N° d'ordre : 167-99 Année 1999

THÈSE
présentée
devant l'UNIVERSITÉ CLAUDE BERNARD – LYON 1
pour l'obtention
du DIPLÔME de DOCTORAT
(arrêté du 30 mars 1992)

présentée et soutenue publiquement le 15 juin 1999

par

Nicolas M. THIÉRY

Invariants algébriques de graphes et reconstruction. Une étude expérimentale.

Rapporteurs :

Adriano Garsia	Professeur, University of California at San-Diego
William Kocay	Professeur, University of Manitoba, Winnipeg

Jury :

Adrian Bondy	Professeur, Université Lyon I
Marc Giusti	Directeur de recherche, École Polytechnique
Michel Habib	Professeur, Université de Montpellier
Daniel Krob	Directeur de recherche, Université Paris VII
Maurice Pouzet	Professeur, Université Lyon I

Remerciements

Mes premiers remerciements vont à Maurice Pouzet pour l'esprit dans lequel il a encadré mon stage de DEA, puis ma thèse. Après m'avoir redonné le goût des mathématiques avec son cours de DEA de théorie des ordres, il m'a guidé progressivement vers ma propre voie, me faisant aborder des sujets aussi divers que passionnants, où mathématiques et informatique s'enrichissent mutuellement. J'ai particulièrement apprécié la grande liberté qu'il m'a toujours laissée, en particulier dans le choix du lieu et du rythme de travail, des méthodes utilisées, des congrès et autres écoles d'été. Je le remercie pour ses nombreux conseils éclairés, et pour les innombrables heures de discussion, au téléphone ou chez lui, autour d'un thé ou d'un bon repas. Je le remercie enfin de m'avoir fait entièrement confiance pour la gestion des ressources informatiques du laboratoire.

De fil en aiguille, une simple petite question a embrayé sur une longue discussion avec Adriano Garsia, d'abord par courrier électronique, puis sur la plage de San Diego. Ses réponses très détaillées, et les calculs qu'il a menés avec N. Wallach m'ont grandement aidé. Je voudrais le remercier ici pour son invitation, son accueil chaleureux, et surtout pour le temps qu'il a consacré, dans des circonstances difficiles, au rapport de ma thèse.

Je voudrais exprimer ma gratitude envers William Kocay pour avoir accepté de rapporter ma thèse, et pour les deux jours de discussions à bâtons rompus qu'il m'a consacrés lors de son court séjour en France. Ses suggestions seront certainement cruciales dans le développement futur de ce sujet.

J'ai été très honoré que Michel Habib accepte de présider le jury de ma thèse.

Durant mon séjour au laboratoire de mathématiques discrètes, j'ai beaucoup apprécié la grande rigueur scientifique d'Adrian Bondy. La clarté de ses articles de synthèse sur la reconstruction, et les conseils avisés qu'il a pris le temps de me prodiguer, m'ont considérablement aidé. Sa présence dans mon jury de thèse a été un grand honneur pour moi.

Je tiens à remercier Daniel Krob, membre du jury, pour nos discussions privées et pour son excellent cours de combinatoire.

Un grand merci à Marc Giusti, pour avoir accepté de participer au jury de ma thèse, pour ses nombreux commentaires constructifs, et pour l'énergie qu'il consacre au développement du centre de calcul Médicis.

L'ouvrage *Algorithms in Invariant Theory* de Bernd Sturmfels a été le point de départ de mon travail de recherche, et une référence constante depuis. Son auteur a répondu avec beaucoup de patience et de précision à mes multiples questions, tant par courrier électronique que lors de congrès. Qu'il en soit chaleureusement remercié.

Philippe Flajolet a effectué pour moi un bon nombre de calculs avec `Maple`. Les feuilles de travail correspondantes, toujours très bien commentées, ont été un formidable outil pédagogique pour apprendre à effectuer moi-même ces calculs.

Je remercie Brendan Mc Kay pour son logiciel `nauty`, pour les calculs qu'il a effectués pour moi, et pour ses réponses rapides et claires à mes questions.

Un grand merci à tous les chercheurs de par le monde qui m'ont aidé en répondant à mes questions, en particulier, Anders Björner, Michel Brion, Hanspeter Kraft, Ilia Ponomarenko, Gerarld Schwarz, Richard Stanley et Paul Zimmermann.

J'ai beaucoup apprécié les conditions de travail, et la liberté dont j'ai bénéficié dans les établissements où j'ai effectué ma thèse, l'École Normale Supérieure de Paris et l'Université Lyon 1. Je voudrais remercier Alexis Bienvenu, Vincent Bouchitté, Philippe Caldero, Thierry Dumont, Jérome Germoni, Philippe Graftiaux, Frédéric Havet, Josette Lefranc, Arlette Mayer, Bernard Roux, Lydia Szyszko, Stéphan Thomassé et tous les collègues qui m'ont aidé et soutenu durant ma thèse.

Le support financier de la Région Rhône-Alpes et le centre de calcul Médicis m'ont permis d'utiliser des moyens de calcul modernes et performants. Ces calculs n'auraient pas non plus été possibles sans une myriade de logiciels libres, et surtout sans l'aide constante de leurs développeurs. Je voudrais remercier Ralph Hillebrand et toute l'équipe de `MuPAD`, Gregor Kemper pour les différentes incarnations d' `Invar`, Jean-Charles Faugère et Fabrice Rouiller pour `GB` et son intégration dans `MuPAD`, Michael Himsolt et toute l'équipe de `Graphlet` et Neil Sloane pour l'encyclopédie électronique en ligne des suites d'entiers ; plus généralement, merci à tous ceux qui œuvrent pour mettre à disposition du plus grand nombre des logiciels de qualité, sous la seule forme de développement informatique scientifique et durable.

Je dois mon goût pour les sciences et en particulier les mathématiques à mes anciens professeurs, Guy Reboul, Yves Fondannier, Michel Wigneron et Zoom. Je ne saurais rien en informatique sans les grands anciens de la salle S, Efgé, Ferminaze, K, K.B., Loïc, Max, Ptiboul et tous les autres.

Je remercie mes parents pour leur soutien sans faille, les relectures interminables de verbiage cryptique, et le havre de paix où j'ai pu rédiger sous le soleil de provence.

Le soutien moral a été assuré pendant l'agrégation par Dominique (longues heures de sueur commune et de 1848 menthe) et Verzi (longues heures d'acros), et pendant ma thèse par tous les jongleurs et voltigeuses de Paris, de Lyon et d'ailleurs (vive la SNCF), tout particulièrement Ariane, Geneviève, Gaëlle et Julie.

Chère Émilia, cher Jean-Christophe, cher Florent, pour tout ce que nous avons partagé, et tout ce que nous partagerons encore, merci !

Au soleil de ma vie, qui rayonne par delà les océans.

Table des matières

Liste des figures

Liste des tableaux

Introduction

Cette thèse porte sur les invariants algébriques de graphes et leurs rapports avec le problème d'isomorphie de graphes et, en particulier, le problème de reconstruction de Ulam.

Étant donné un entier n, on considère un ensemble $\mathbf{x}_{\{i,j\}} := \{x_{\{1,2\}}, \ldots, x_{\{n-1,n\}}\}$ de C_n^2 variables indexées par les paires $\{i,j\}$ de $\{1,\ldots,n\}$, puis l'algèbre $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$ des polynômes en ces variables. On définit alors la sous-algèbre $\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$ composée des polynômes qui restent invariants par une permutation de $\{1,\ldots,n\}$. Dans [Stu93], Sturmfels propose comme exercice de trouver un système générateur minimal de cette algèbre dans le cas $n = 4$. La solution est donnée par Aslaksen, Chan et Gulliksen [ACG96]. Le problème se pose pour tout n, et il ne semble pas avoir été traité dans l'énorme littérature consacrée à la théorie des invariants. Si celle-ci indique que l'algèbre est finiment engendrée, et donne des bornes sur les degrés des polynômes d'un système générateur minimal, les implémentations les plus récentes [Kem93, Kem98b, Der99] des algorithmes classiques [Stu93] ne donnent pas de résultat, même pour $n = 5$, en raison de la taille des calculs. Une réimplémentation spécialisée de ces algorithmes nous a donné des résultats partiels jusqu'à $n = 8$.

Ce problème est lié au problème d'isomorphie de graphes, central en algorithmique. Un graphe non orienté $\mathbf{g}$, ayant pour sommets les entiers $\{1,\ldots,n\}$, peut être vu comme une fonction qui associe à chaque paire $\{i,j\}$ la valuation $g_{\{i,j\}}$, cette valuation étant soit 0, soit 1 si $\mathbf{g}$ est un graphe simple. Ainsi, P étant un polynôme invariant de $\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$, on peut calculer sa valeur $P(\mathbf{g})$. Par exemple, si $P := \sum_{\{i,j\}\subset\{1,\ldots,n\}} x_{\{i,j\}}$, sa valeur pour un graphe simple $\mathbf{g}$ est le nombre d'arêtes de $\mathbf{g}$. Deux graphes isomorphes donnent évidemment la même valeur à tous les polynômes invariants. La réciproque est vraie (c'est un cas particulier d'un résultat de base de la théorie des invariants des groupes finis). On a donc un test algébrique pour l'isomorphie de graphes.

Cependant, pour des répercussions algorithmiques, il conviendrait de connaître les degrés, les tailles et le nombre de polynômes d'un système générateur minimal. Ces paramètres étant mal connus, la question se pose alors de savoir quelles sont les formes possibles des polynômes d'un tel système. Cette question est liée à la conjecture de reconstruction de graphes formulée par Ulam [Ula60]. Étant donné un graphe $\mathbf{g}$, on appelle *jeu* de $\mathbf{g}$ la famille des sous-graphes obtenus en retirant un sommet de $\mathbf{g}$, considérés à l'isomorphie près et comptés avec leur multiplicité. La conjecture de reconstruction de Ulam affirme alors que deux graphes simples ayant le même jeu sont isomorphes.

Disons qu'un polynôme invariant P est *reconstructible* s'il prend la même valeur sur deux graphes ayant le même jeu. Le test algébrique d'isomorphie indique que,

si tous les polynômes invariants sont reconstructibles, la conjecture de Ulam est résolue positivement, pour les graphes simples comme pour les graphes valués.

La notion de polynôme reconstructible n'est pas algébrique, car elle fait intervenir une évaluation. Associons à tout multigraphe $\mathbf{g}$ un polynôme invariant p. Ainsi, les polynômes invariants s'identifient aux combinaisons linéaires formelles de multigraphes non étiquetés. Si $\mathbf{g}$ est un graphe simple, $p(\mathbf{g}')$ compte précisément le nombre de sous-graphes de $\mathbf{g}'$ isomorphes à $\mathbf{g}$. La plupart des résultats sur la conjecture de Ulam sont basés sur des dénombrements de sous-graphes ; en particulier, si $\mathbf{g}$ a un sommet isolé, p est reconstructible (lemme de Kelly [Kel57]). Ce fait s'étend à tout multigraphe $\mathbf{g}$ ayant un sommet isolé. Appelons *polynômes algébriquement reconstructibles* tous les polynômes associés aux multigraphes ayant des sommets isolés, ainsi que leurs combinaisons polynomiales. On note que deux graphes ont même jeu si, et seulement si, ils donnent la même valeur à tous les polynômes algébriquement reconstructibles. À la suite des résultats de Tutte [Tut76, Tut79] sur la reconstructibilité du polynôme caractéristique, Pouzet [Pou77] a proposé une conjecture entraînant la conjecture de Ulam et susceptible d'un traitement algébrique :

« La sous-algèbre des polynômes algébriquement reconstructibles coïncide avec l'algèbre des invariants ».

C'est dans ce cadre que se situe notre travail.

Deux approches de même nature, l'une pour l'isomorphisme et l'autre pour la reconstruction, ont été étudiées. Grigoriev [Gri79] considère l'algèbre $\mathbb{C}[x_{(i,j)}]^{\mathfrak{S}_n}$ dans laquelle les n^2 variables sont indexées par les couples d'éléments de $\{1,\ldots,n\}$ (non nécessairement distincts). Il montre que le corps des fractions est engendré par n^2+1 polynômes, les n^2 premiers pouvant, par exemple, être les fonctions symétriques élémentaires en les variables $x_{(i,j)}$. Kocay [Koc82, Mnu92, Cam96] définit une structure d'algèbre sur les graphes simples (l'algèbre des sous-graphes), et l'utilise pour montrer de manière élémentaire les résultats de Tutte sur la reconstruction. Dans ce cadre, Kocay considère le problème de la reconstruction du nombre d'arbres couvrants par type d'isomorphie.

Nous avons fait une recherche expérimentale sur l'algèbre des invariants. Pour cela, nous avons implémenté les algorithmes classiques pour contourner au mieux les difficultés considérables liées à l'explosion combinatoire des objets manipulés. De cette recherche sont issues des hypothèses sur les systèmes générateurs, leur vérification dans certains cas, des contre-exemples, une réponse négative à la conjecture de Pouzet, ainsi que des résultats sur la reconstruction, notamment sur le problème de Kocay. Au fur et à mesure, nous avons constitué une bibliothèque `PerMuVAR` pour `MuPAD` et `Perl`. Elle est distribuée librement aux utilisateurs intéressés.

Notre thèse est organisée selon les trois parties décrites ci-dessous.

Partie I : Espace vectoriel des parties d'un ensemble

L'action d'un groupe sur un ensemble donne lieu à une action sur les parties de cet ensemble. Ainsi, le groupe symétrique $\mathfrak{S}_n$ agissant sur $\{1,\ldots,n\}$ agit également sur l'ensemble E des parties à 2 éléments de $\{1,\ldots,n\}$, puis sur les parties à k éléments de E. Les orbites pour cette action ne sont autres que les graphes simples à k arêtes, considérés à l'isomorphie près. Si p et q sont deux entiers, $p \leq q \leq |E|$, la matrice d'incidence des parties à p éléments de E versus les parties à q éléments

de E est de rang plein [Kan72]. D'importants résultats connus antérieurement découlent de ce fait élémentaire comme le théorème de Livingstone et Wagner [LW65] (croissance jusqu'à $\frac{|E|}{2}$ du nombre d'orbites des parties à k éléments) ou le résultat de Lovász [Lov72] sur la reconstruction par arêtes. Plusieurs travaux récents en combinatoire en sont issus.

L'opérateur associé à cette matrice peut être vu comme une dérivation. Intervenant dans les problèmes de reconstruction et notamment de reconstruction algébrique, il joue un rôle crucial dans l'approche de la reconstruction algébrique des arbres. Nous donnons une base du noyau de cet opérateur, lorsqu'il n'est pas réduit à $\{0\}$. Celle-ci est un peu différente de celle donnée par la théorie des représentations du groupe symétrique. Dans le cas où E est l'ensemble des paires de $\{1,\ldots,n\}$, ($q=2$, $p=1$), ce noyau est constitué des graphes 0-réguliers. Nous montrons qu'un graphe simple est déterminé, à l'isomorphie près, par sa partie régulière et les degrés de ses sommets, à l'exception d'une famille que nous caractérisons complètement.

Partie II : Invariants algébriques de graphes

Nous avons cherché à estimer les degrés dans un système générateur minimal, et en particulier le degré δ maximal. Nous montrons que $\delta \geq \lfloor \frac{n}{2} \rfloor$. Comme le groupe agit par permutation, la théorie donne la majoration $\delta \leq \mathrm{C}^2_{\mathrm{C}^2_n}$. Cette majoration est obtenue en considérant certains types d'ensembles générateurs composés d'invariants primaires et secondaires, pour lesquels les degrés des secondaires sont déterminés par les degrés des primaires. Nous proposons un nouveau système de primaires dont les degrés sont plus faibles. Pour $n \leq 5$, nous avons démontré par le calcul qu'il s'agissait effectivement de primaires. Au delà, nous avons étayé notre conjecture sur une étude de la série de Hilbert de l'algèbre des invariants et sur une conjecture de Mallows et Sloane. Nous obtiendrions alors une meilleure majoration : $\delta \leq \mathrm{C}^2_{\mathrm{C}^2_{n-1}} + \mathrm{C}^2_n$. Il semblerait d'après nos résultats expérimentaux que cette borne puisse être ramenée à $\mathrm{C}^2_n - 1$.

Via l'identification entre polynôme invariant et combinaison linéaire formelle de multigraphes, l'algèbre des invariants est engendrée par les multigraphes. Nous montrons que cette algèbre est engendrée par les multigraphes ayant une seule composante connexe non triviale. Dans le cas $n = \infty$, ces multigraphes sont algébriquement indépendants, et il s'agit donc d'un système générateur minimal. Nous en déduisons, pour n fini, un système générateur partiel minimal jusqu'au degré $\lfloor \frac{n}{2} \rfloor$.

Les résultats de [ACG96] entraînent que, pour $n \leq 4$, l'algèbre des invariants est engendrée par les graphes simples. Nous montrons que ce n'est plus le cas pour $n \geq 5$, en donnant un contre-exemple de degré 4.

Nous montrons de même que, pour $n \geq 3$, l'algèbre des invariants sur les digraphes n'est pas engendrée par les digraphes simples, en donnant un contre-exemple de degré 3. Ceci infirme un lemme de Grigoriev [Gri79, Lemma I].

Enfin, nous avons cherché expérimentalement des systèmes générateurs. Sauf pour $n = 4$, la plupart des implémentations récentes [Kem98b, Der99] des algorithmes usuels ne donnent aucun résultat car elles utilisent un calcul de base de Gröbner extrêmement coûteux. L'une d'entre elles [Kem93], utilisant seulement des techniques d'algèbre linéaire, permet d'obtenir quelques résultats partiels. Nous

avons implémenté ces algorithmes en les optimisant pour les représentations par permutation. Cela nous a permis d'obtenir des résultats partiels jusqu'à $n = 8$. Pour $n \leq 6$, nous en déduisons que les graphes simples sont algébriquement reconstructibles. Pour $n = 5$, la forme du système générateur partiel que nous obtenons suggère très fortement qu'il s'agit d'un système générateur complet. Tous les polynômes invariants seraient alors algébriquement reconstructibles, pour $n \leq 5$.

Nous introduisons plusieurs algèbres proches (algèbres des graphes bipartis, des graphes simples et des forêts), pour lesquelles nous obtenons des résultats analogues.

Partie III : Invariants algébriques de graphes et conjecture de reconstruction de Ulam

Soit $\mathbf{g}$ un multigraphe, et p le polynôme associé. On a facilement les implications suivantes :

$$p \text{ algébriquement reconstructible} \Rightarrow p \text{ reconstructible} \Rightarrow \mathbf{g} \text{ reconstructible}.$$

Nous étudions leurs réciproques dans quelques cas. Nous montrons en particulier qu'il existe des graphes simples de degré 13 à 17 arêtes non algébriquement reconstructibles, alors que McKay [McK97] a pu vérifier que ces graphes étaient tous reconstructibles. La démonstration, non constructive, repose sur un calcul de la série de Hilbert et une énumération de Pólya, le point essentiel étant que l'algèbre des invariants est graduée. Nous récapitulons les relations entre les différentes notions de reconstruction, comme la reconstruction algébrique et la reconstruction dans l'algèbre des sous-graphes de Kocay.

Certaines opérations, comme le passage au complémentaire, préservent la reconstructibilité. Nous montrons que, pour la plupart, ces opérations préservent aussi la reconstructibilité algébrique. Nous en déduisons que, si un multigraphe $\mathbf{g}$ est non algébriquement reconstructible, il existe des multigraphes de tous degrés supérieurs non algébriquement reconstructibles. De même, si $\mathbf{g}$ est un graphe simple non algébriquement reconstructible à d arêtes, il existe des graphes simples non algébriquement reconstructibles de tous degrés entre d et $\mathrm{C}_n^2 - d$.

Un grand nombre de paramètres sur les graphes sont connus comme étant reconstructibles, par exemple, le nombre d'arbres couvrants, le nombre de cycles hamiltoniens, le polynôme chromatique ou le polynôme caractéristique. Nous montrons que ces paramètres sont en fait algébriquement reconstructibles, par des méthodes élémentaires semblables à celles utilisée par Kocay [Koc82] dans l'algèbre des sous-graphes. Cette approche met en évidence les points-clefs (non-connexité par exemple) qui sous-tendent les démonstrations. Cela nous permet de montrer la reconstructibilité algébrique, et donc la reconstructibilité, de toute une famille de nouveaux paramètres : nombres chromatique et cochromatique raffinés par taille, *point arboricity linear point arboricity* , *k-point partition number*, etc.

La reconstructibilité des arbres [Kel57] est à l'origine des recherches sur le problème de Ulam. Nous abordons le problème de la reconstruction algébrique des arbres, qui contient celui de Kocay sur la reconstruction du nombre d'arbres couvrants d'un graphe, comptés par type d'isomorphie. Ce problème se restreint à une algèbre quotient de l'algèbre des invariants, et s'exprime alors au moyen d'algèbre linéaire seulement. Nous montrons, par le calcul, que les arbres sont algébriquement

reconstructibles jusqu'à $n = 13$, et nous vérifions, par une étude asymptotique, qu'il n'y a pas d'incohérence immédiate avec des considérations de dimension. Enfin, nous donnons une famille infinie d'arbres algébriquement reconstructibles, incluant tous les arbres de diamètre 4.

Partie I

Espaces vectoriels sur les parties d'un ensemble

Chapitre 1

Introduction

Nous considérons l'espace vectoriel V_n ayant pour vecteurs de base les parties de l'ensemble $\{1, \ldots, n\}$. Cet espace est muni du produit scalaire canonique associé à cette base, et de deux opérateurs Div et Etoile adjoints l'un de l'autre traduisant l'ordre d'inclusion sur les parties. L'espace V_n est la somme directe des sous-espaces V_n^k, où V_n^k est le sous-espace engendré par les parties à k éléments. Un résultat de base, dû à Kantor [Kan72], affirme que si $i \leq k \leq n - i$, l'opérateur Div induit une surjection V_n^k sur V_n^i. Il en découle une décomposition de V_n^k en sous-espaces orthogonaux pour le produit scalaire canonique.

L'action du groupe symétrique $\mathfrak{S}_n$ sur $\{1, \ldots, n\}$, naturellement étendue aux parties de $\{1, \ldots, n\}$, induit une représentation linéaire de $\mathfrak{S}_n$ sur V_n. Il s'avère que la décomposition ci-dessus est en fait la décomposition en irréductibles de cette représentation. Nous en donnons une première démonstration basée sur le lemme de Schur, que nous vérifions par un calcul sur les caractères. Nous montrons ensuite que cette approche naïve revient précisément à la construction classique, via les modules de Specht, des représentations irréductibles du groupe symétrique paramétrées par les partitions $[n-k, k]$. Les bases de ces modules irréductibles sont paramétrées par les tableaux standard. Nous rappelons la construction classique donnée par la théorie des représentations du groupe symétrique. Nous présentons ensuite une nouvelle base, dont la construction plus combinatoire met en jeu les mots de Dyck.

Un graphe simple non orienté peut être vu comme collection de parties à deux éléments d'un ensemble à n éléments. On peut voir un élément $\mathbf{g}$ de V_n^2 comme un graphe valué, la valuation de l'arête $\{i, j\}$ étant le coefficient de la paire $\{i, j\}$ dans le vecteur $\mathbf{g}$. Le noyau de Div est ce que nous appelons l'espace des graphes 0-*réguliers*, l'image de V_n^1 par l'opérateur Etoile, l'*espace des étoiles*. Chaque graphe valué est la somme de sa partie étoilée et de sa partie régulière. Tout ceci s'étend à V_n^k et s'exprime dans le langage des hypergraphes. Nous étudions les extensions de graphes par adjonction d'un sommet et les propriétés particulières des graphes valués dans $\mathbb{Z}$ vis-à-vis de la décomposition en partie régulière et étoilée. Nous déduisons de ce dernier point qu'un graphe simple est essentiellement déterminé à l'isomorphie près par sa partie régulière. Cette information est cruciale pour mieux localiser la difficulté du problème de reconstruction pour les graphes simples.

On peut aussi considérer un graphe simple $\mathbf{g}$ comme un ensemble de k arêtes. Donc, au lieu des parties de $\{1, \ldots, n\}$, on peut considérer les parties de $\{1, \ldots, m\}$ où $m = \mathrm{C}_n^2$, et identifier $\mathbf{g}$ à l'un des vecteurs de la base de V_m. Ici l'action qui

nous intéresse n'est pas celle de $\mathfrak{S}_m$, mais celle induite par $\mathfrak{S}_n$ par permutation des sommets. Le théorème de Kantor reste valide dans le quotient de l'espace V_m par $\mathfrak{S}_n$ (c'est-à-dire sur l'espace vectoriel ayant comme base les graphes simples à isomorphie près). Nous rappelons quelques résultats fondamentaux qui en découlent : théorème de Livingstone-Wagner sur les orbites [LW65, Kan72], propriété de Sperner [Pou76, PR86] et théorème de Lovász sur la reconstruction par arête [Lov72, Sta84].

Enfin, nous étudions une généralisation du théorème de Kantor aux matrices d'incidence des arbres. Ces résultats seront essentiels dans les parties suivantes, en particulier pour l'étude de la reconstruction algébrique des arbres.

Chapitre 2

Matrices d'incidence

2.1 Définitions

Soit n un entier. Nous notons $\mathcal{P}_n$ l'ensemble des parties de $\{1,\dots,n\}$, et $\mathcal{P}_n^k$ le sous-ensemble des parties de taille k ; ainsi, $\mathcal{P}_n$ est la réunion disjointe des $\mathcal{P}_n^k$. Par exemple, $\mathcal{P}_n^0 = \{\emptyset\}$ et $\mathcal{P}_n^n = \{\{1,\dots,n\}\}$. Par convention nous posons $\mathcal{P}_n^k := \emptyset$ lorsque $k < 0$ ou $k > n$.

Espace vectoriel des parties d'un ensemble

Soit $\mathbb{K}$ un corps. Sauf mention explicite du contraire, nous supposons que $\mathbb{K}$ est de caractéristique 0, et lorsque le corps de base est clair, nous l'omettons de nos notations. Nous désignons par V_n l'espace vectoriel $\mathbb{K}^{\mathcal{P}_n}$ des applications f de $\mathcal{P}_n$ dans $\mathbb{K}$. Nous écrivons plutôt un élément f comme une combinaison linéaire formelle de parties de $\{1,\dots,n\}$; par exemple, $f = 3.\{1,4\} + 2.\{1,5,7\} - \frac{1}{4}.\{3\}$. L'espace V_n est de dimension $|\mathcal{P}_n| = 2^n$. Il se décompose en la somme directe des sous-espaces $V_n^k, k = 0,\dots,n$, chaque V_n^k étant le sous-espace de dimension C_n^k engendré par $\mathcal{P}_n^k$.

Voici quelques exemples :

- $k < 0$ ou $k > n+1$. Étant donnée notre convention, $V_n^k = \langle\rangle$ est réduit à l'espace vectoriel trivial $\{0\}$.
- $k = 0$. Les éléments de V_n^0 sont de la forme $\lambda \cdot \emptyset$. Donc V_n^0 est la droite $\mathbb{K} \cdot \emptyset$ et sera identifié avec $\mathbb{K}$.
- $k = 1$. Comme exemple d'élément de V_n^1 on a $4.\{1\} - 2.\{2\} + \frac{3}{4}.\{5\}$. Noter que V_n^1 est isomorphe à $\mathbb{K}^n$.
- $k = 2$. On peut identifier le vecteur $4.\{1,2\} + \{2,3\}$ à un graphe valué non orienté dont l'arête $\{1,2\}$ est valuée 4, l'arête $\{2,3\}$ est valuée 1, et les autres arêtes sont valuées 0. Ainsi, V_n^2 est l'ensemble des graphes non orientés sur $\{1,\dots,n\}$ valués dans $\mathbb{K}$.
- Plus généralement, on peut considérer chaque élément de V^k comme un hypergraphe k-uniforme valué dans $\mathbb{K}$.

Remarque 2.1.1: Si $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, les éléments de V_n^k s'identifient aux hypergraphes k-uniformes non orientés de $\{1,\dots,n\}$.

2.2 Opérateurs Div et Etoile

2.2.1 Définition

Deux opérateurs linéaires adjoints, la dérivation Div et l'étoile Etoile, traduisent sur l'espace V_n l'ordre d'inclusion des parties.

Définition 2.2.1 (Opérateurs Div et Etoile).
On appelle dérivation *(noté* Div*) l'opérateur linéaire qui associe à une partie A la somme formelle de ses sous-parties de taille $|A|-1$:*

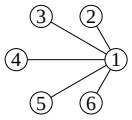
$$\begin{aligned} \mathrm{Div}(\emptyset) &:= 0 \\ \mathrm{Div}(A) &:= \sum_{a\in A} A - \{a\} \end{aligned}$$

On appelle étoile *(noté* Etoile*) l'opérateur linéaire qui associe à une partie A la somme formelle de ses sur-parties de taille $|A|+1$.*

$$\begin{aligned} \mathrm{Etoile}(\{1,\ldots,n\}) &:= 0 \\ \mathrm{Etoile}(A) &:= \sum_{a\in\{1,\ldots,n\}\setminus A} A\cup\{a\} \end{aligned}$$

Le nom de l'opérateur Etoile est suggéré par l'exemple suivant :

$$\mathrm{Etoile}(\{1\}) = \sum_{j\neq 1}\{1,j\} =$$



L'opérateur Div induit une application $\mathrm{Div}^{k+1\to k}$ de V^{k+1} dans V^k. Réciproquement, l'opérateur Etoile induit une application $\mathrm{Etoile}^{k\to k+1}$ de V^k dans V^{k+1}. Nous verrons plus loin à quelles conditions ces applications sont injectives ou surjectives. Nous verrons aussi que ce sont essentiellement les seules applications de ce type qui préservent les symétries.

2.2.2 Matrices d'incidence

Définition 2.2.2 (Matrice d'incidence [Kan72]).
On appelle matrice d'incidence des parties de taille i versus les parties de taille k *la matrice $M^{i\to k}$ de dimension $\mathrm{C}_n^k \times \mathrm{C}_n^i$ dont les colonnes sont indexées par les parties de taille i, les lignes par les parties de taille k, et telle que le coefficient $M^{i\to k}(A,B)$ vaut 1 si $A\subset B$ et 0 sinon :*

$$M^{i\to k} := \begin{array}{c} A \\ \left[\begin{array}{ccc} & \vdots & \\ \ldots & M^{i\to k}(A,B) & \ldots \\ & \vdots & \end{array}\right] \\ B \end{array}$$

Voici quelques exemples de matrices d'incidence.

Exemple 2.2.3.

$$M_3^{0\to 1} = \begin{array}{c} \emptyset \\ \left[\begin{array}{c} 1 \\ 1 \\ 1 \end{array}\right] \\ \end{array} \begin{array}{l} \\ \{1\} \\ \{2\} \\ \{3\} \end{array}$$

$$M_3^{1\to 2} = \begin{array}{c} \begin{array}{ccc} \{1\} & \{2\} & \{3\} \end{array} \\ \left[\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right] \end{array} \begin{array}{l} \\ \{1,2\} \\ \{1,3\} \\ \{2,3\} \end{array}$$

$$M_3^{2\to 3} = \begin{array}{c} \begin{array}{ccc} \{1,2\} & \{1,3\} & \{2,3\} \end{array} \\ \left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right] \end{array} \begin{array}{l} \\ \{1,2,3\} \end{array}$$

$$M_4^{1\to 2} = \begin{array}{c} \begin{array}{cccc} \{1\} & \{2\} & \{3\} & \{4\} \end{array} \\ \left[\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right] \end{array} \begin{array}{l} \\ \{1,2\} \\ \{1,3\} \\ \{2,3\} \\ \{1,4\} \\ \{2,4\} \\ \{3,4\} \end{array}$$

Remarque 2.2.4: La matrice $M^{k\to k+1}$ est la matrice de l'opérateur Etoile$^{k\to k+1}$. Réciproquement sa transposée ${}^tM^{k\to k+1}$ est la matrice de l'opérateur Div$^{k+1\to k}$. Ces deux opérateurs sont donc adjoints. On note que la matrice M_n de l'opérateur Etoile dans V_n est la matrice d'adjacence du diagramme de Hasse de l'ordre d'inclusion sur $\mathcal{P}_n$. On l'obtient en recollant les $M^{k\to k+1}$ comme dans l'exemple 2.2.5.

Exemple 2.2.5 (Matrice d'incidence globale).

$$M_3 = \begin{array}{c} \begin{array}{cccccccc} \emptyset & \{1\} & \{2\} & \{3\} & \{1,2\} & \{1,3\} & \{2,3\} & \{1,2,3\} \end{array} \\ \left[\begin{array}{cccccccc} 0 & & 0 & & & 0 & & 0 \\ 1 & & & & & & & \\ 1 & & 0 & & & 0 & & 0 \\ 1 & & & & & & & \\ & 1 & 1 & 0 & & & & \\ 0 & 1 & 0 & 1 & & 0 & & 0 \\ & 0 & 1 & 1 & & & & \\ 0 & & 0 & & 1 & 1 & 1 & 0 \end{array}\right] \end{array} \begin{array}{l} \emptyset \\ \{1\} \\ \{2\} \\ \{3\} \\ \{1,2\} \\ \{1,3\} \\ \{2,3\} \\ \{1,2,3\} \end{array}$$

2.2.3 Passage au complémentaire, opérations ensemblistes

On peut définir des opérateurs correspondant aux autres opérations ensemblistes. Par exemple, le complémentaire $\complement$, défini sur $\mathcal{P}_n$, s'étend linéairement à V_n. Par exemple, si $n = 4$,

$$\complement(\{1,2\} + \frac{1}{2}\{4\}) = \complement\{1,2\} + \frac{1}{2}\complement\{4\} = \{3,4\} + \frac{1}{2}\{1,2,3\}.$$

On note que, comme le passage au complémentaire $\complement$ est une involution entre $\mathcal{P}_n^k$ et $\mathcal{P}_n^{n-k}$, l'opérateur $\complement$ définit un isomorphisme involutif de V_n^k dans V_n^{n-k}. On étend aussi la réunion en un opérateur bilinéaire, de sorte que

$$(\{1,2\} + 2\{3,4\}) \cup \{1,5\} = \{1,2,5\} + 2\{1,3,4,5\}.$$

On peut bien sûr faire de même pour chaque opération classique sur les parties d'un ensemble (intersection : $\cap$, différence : $\setminus$, différence symétrique : Δ).

Remarque 2.2.6: Le passage au complémentaire induit une dualité supplémentaire entre les deux opérateurs Div et Etoile. En effet, pour $\mathbf{v} \in V_n$, on a :

$$\mathrm{Div}\, {}^{\complement}\mathbf{v} = {}^{\complement}\,\mathrm{Etoile}\,\mathbf{v}.$$

Démonstration. Par linéarité, il suffit de le montrer pour une partie A de $\{1,\dots,n\}$:

$$\mathrm{Div}\, {}^{\complement}A = \sum_{a \in {}^{\complement}A} {}^{\complement}A \setminus \{a\} = \sum_{a \in {}^{\complement}A} {}^{\complement}(A \cup \{a\}) = {}^{\complement} \sum_{a \in {}^{\complement}A} A \cup \{a\} = {}^{\complement}\,\mathrm{Etoile}\, A. \quad \square$$

2.2.4 Itérés des opérateurs Div et Etoile

Définition 2.2.7.
Soit $i \leq k$. On note $\mathrm{Div}^{k\to i}$ l'opérateur linéaire qui à un ensemble A de taille k associe la somme de ses sous-ensembles de taille i. De même, on note $\mathrm{Etoile}^{i\to k}$ l'opérateur linéaire qui à un ensemble A de taille i associe la somme de ses sur-ensembles de taille k

$$\mathrm{Div}^{k\to i} = \begin{cases} V_n^k \to V_n^i \\ A \mapsto \displaystyle\sum_{A' \subset A, |A'|=i} A' \end{cases}; \qquad \mathrm{Etoile}^{i\to k} = \begin{cases} V_n^i \to V_n^k \\ A \mapsto \displaystyle\sum_{A' \supset A, |A'|=i} A'. \end{cases}$$

Propriétés 2.2.8.
Les opérateurs $\mathrm{Div}^{k\to i}$ et $\mathrm{Etoile}^{i\to k}$ sont adjoints, de matrices respectives ${}^tM^{i\to k}$ et $M^{i\to k}$, et on a :

$$\mathrm{Div}^{k\to i} = \frac{1}{(k-i)!}\,\mathrm{Div}^{k-i}; \qquad \mathrm{Etoile}^{i\to k} = \frac{1}{(k-i)!}\,\mathrm{Etoile}^{k-i}.$$

Démonstration. Par passage au complémentaire, il suffit de le montrer pour Div. Soit A une partie de taille k :

$$\begin{aligned} \mathrm{Div}^{k-i} A &= \sum_{a_1 \in A} \sum_{a_2 \in A\setminus\{a_1\}} \cdots \sum_{a_i \in A\setminus\{a_1,\dots,a_{k-i-1}\}} A \setminus \{a_1,\dots,a_{k-i}\} \\ &= \sum_{A' \subset A, |A'|=|A|-i} \; \sum_{(a_1,\dots,a_{k-i}),\{a_1,\dots,a_{k-i}\}=A\setminus A'} A' \\ &= \sum_{A' \subset A, |A'|=i} i!A' = i!\,\mathrm{Div}^{k\to i} A. \quad \square \end{aligned}$$

Corollaire 2.2.9.
Soit A une partie de taille k. On a :

$$\mathrm{Div}^k A = k!\,\mathrm{Div}^{k\to 0} A = k!\emptyset = k!;$$
$$\mathrm{Div}^{k+1} A = k!\,\mathrm{Div}^{k\to -1} A = k!0 = 0.$$

2.2.5 Interprétation algébrique de l'opérateur Div

L'opérateur Div a les propriétés d'une dérivation. Cela se justifie par l'interprétation algébrique proposée par Pouzet [Pou76]. On identifie une partie $\{1, 3, 7\}$ et un monôme $x_1x_3x_7$ via l'application linéaire

$$\Phi \begin{cases} V_n \to \mathbb{K}[x_1, \ldots, x_n] \\ \emptyset \mapsto 1 \\ A \mapsto \prod_{i \in A} x_i \end{cases} .$$

Le polynôme $\Phi(A)$ est élémentaire, c'est-à-dire que les monômes qui le composent sont sans carrés. L'application Φ est évidemment un isomorphisme entre V_n et le sous-espace des polynômes élémentaires de $\mathbb{K}[x_1, \ldots, x_n]$. La remarque suivante indique qu'il s'agit partiellement d'un morphisme d'algèbres.

Remarque 2.2.10: Si A et B sont des parties disjointes, $\Phi(A \cup B) = \Phi(A).\Phi(B)$.

Sur les polynômes, l'opérateur Div s'écrit : $\mathrm{Div} = \sum \frac{\partial}{\partial x_i}$. Lorsqu'il n'y a pas d'ambiguïté, on note

$$p' = \mathrm{Div}(p), \qquad p^{(k)} = \mathrm{Div}^k(p).$$

Nous allons étudier plus précisément les propriétés de cet opérateur sur les polynômes. D'une part, nous en déduirons une propriété cruciale de l'opérateur Div sur les parties et, d'autre part, cet opérateur sera fondamental dans l'étude de la reconstruction algébrique des polynômes (voir § 16.4).

Proposition 2.2.11.
L'opérateur Div *sur les polynômes est une dérivation, c'est-à-dire qu'il vérifie la formule :*

$$(pq)' = p'q + pq'. \tag{2.1}$$

Démonstration.

$$\begin{aligned}(pq)' &= \sum \frac{\partial}{\partial x_i} pq = \sum p \frac{\partial}{\partial x_i} q + \sum q \frac{\partial}{\partial x_i} p = p \sum \frac{\partial}{\partial x_i} q + q \sum \frac{\partial}{\partial x_i} p \\ &= pq' + qp'. \quad \square\end{aligned}$$

On peut réitérer cette formule, pour obtenir la formule de Leibniz sur les dérivations d'ordre supérieur d'un produit :

$$(pq)^{(l)} = \sum_{k=0}^{l} \mathrm{C}_l^k \, p^{(l-k)} q^{(k)}, \tag{2.2}$$

puis sur un produit quelconque :

$$(p_1 \ldots p_k)^{(l)} = \sum_{i_1 + \cdots + i_k = l} \frac{n!}{i_1! \ldots, i_k!} p_1^{(i_1)} \ldots p_k^{(i_k)} \tag{2.3}$$

Corollaire 2.2.12.
Soit A et B deux parties disjointes. On a :

$$\mathrm{Div}(A \cup B) = (\mathrm{Div}\, A) \cup B + A \cup (\mathrm{Div}\, B).$$

On peut en tirer une formule plus générale lorsque A et B ne sont pas disjointes. Nous l'avons omise ici car nous ne l'utiliserons pas.

Soit ϕ la forme linéaire qui à un polynôme p homogène de degré $d = \deg p$ associe la constante $\frac{1}{d!}p^{(d)}$. On étend ϕ par linéarité à tous les polynômes.

Lemme 2.2.13.
(i) $\phi(p)$ est égale à la somme des coefficients des termes de degré $\deg p$ du polynôme p.
*(ii) ϕ est un morphisme d'anneaux (*i.e. $\phi(pq) = \phi(p)\phi(q)$*).*
(iii) L'ensemble I des polynômes p tels que $\phi(p) = 0$ est un idéal premier de $\mathbb{K}[x_1, \ldots, x_n]$.
Soient G un groupe agissant par permutation des variables $x_1, \ldots, x_n$, et $\mathbb{K}[x_1, \ldots, x_n]$ l'algèbre des polynômes invariants par l'action de ce groupe (voir partie I pour les définitions).
*(iv) ϕ est un invariant pour l'action de G (*i.e. $\phi(\sigma p) = \phi(p)$*).*
(v) L'ensemble des polynômes p invariants tels que $\phi(p) = 0$ est l'image I^G de l'idéal I par l'opérateur de Reynolds. C'est un idéal premier de $\mathbb{K}[x_1, \ldots, x_n]^G$.

Démonstration.

(i) Il suffit de le vérifier pour les monômes, ce qui se fait simplement par récurrence. Soit $x_{i_1} \ldots x_{i_d}$ un monôme de degré d. On note que les i_j ne sont pas forcément distincts.

$$\begin{aligned}\frac{1}{d!}(x_{i_1} \ldots x_{i_d})^d = \frac{1}{d!}\left((x_{i_1} \ldots x_{i_d})'\right)^{d-1} &= \frac{1}{d!}\left(\sum_{j=1}^{d} x_{i_1} \ldots x_{i_{j-1}} x'_{i_j} x_{i_{j+1}} \ldots x_{i_d}\right)^{(d-1)} \\ &= \frac{1}{d}\sum_{j=1}^{d} \frac{1}{(d-1)!}(x_{i_1} \ldots x_{i_{j-1}} x_{i_{j+1}} \ldots x_{i_d})^{(d-1)} = \frac{1}{d}d = 1\end{aligned}$$

(ii) On applique la formule de Leibniz (équation 2.2). Parmi tous les termes $p^{(i)} \ldots q^{(j)}$ avec $i + j = \deg pq$, seul $p^{(\deg p)}q^{(\deg q)}$ sera non nul. En effet, dans les autres termes, soit $i > \deg p$ et on a $p^{(i)} = 0$, soit $j \geq >$ et on a $q^{(j)} = 0$.
On peut aussi se contenter de remarquer que la somme des coefficients dans le produit pq est égale au produit de la somme des coefficients dans p, par la somme des coefficients dans q (on ne considère que les coefficients des termes de plus haut degré).
(iii) L'ensemble I est le noyau de ϕ. C'est donc un idéal premier, puisque l'image de ϕ est le corps $\mathbb{K}$ qui est intègre.
(iv) Comme le groupe G agit par permutation des variables, chaque monôme est transformé en un monôme de même degré. Il est donc clair que la somme des coefficients de plus haut degré de p est invariante.

(v) D'après (iv), si $p^* := \frac{1}{|G|}\sum \sigma.g$ est l'image du polynôme p par l'opérateur de Reynolds, alors $\phi(p^*) = \phi(p)$. Il est alors clair que l'ensemble des polynômes invariants p tels que $\phi(p) = 0$ est l'image I^G de I par l'opérateur de Reynolds. On procède de même que pour I pour montrer qu'il s'agit d'un idéal premier de l'algèbre des invariants $\mathbb{K}[x_1, \ldots, x_n]^G$.

□

Théorème 2.2.14.
Soit $\mathbb{K}[x_1, \ldots, x_n]_d$ l'ensemble des polynômes homogènes de degré d. L'opérateur $\mathrm{Div} = \sum \frac{\partial}{\partial x_i}$ *induit une application surjective de $\mathbb{K}[x_1, \ldots, x_n]_{d+1}$ dans $\mathbb{K}[x_1, \ldots, x_n]_d$. L'opérateur adjoint* $\mathrm{Etoile} = \sum \int_0^{x_i} dx_i$ *est une application injective de $\mathbb{K}[x_1, \ldots, x_n]_d$ dans $\mathbb{K}[x_1, \ldots, x_n]_{d+1}$.*

Démonstration. Le principe de la démonstration est de se servir de x_1 pour faire une intégration par parties. On note $<$ l'ordre sur les monômes défini par $\prod x_i^{d_i} < \prod x_i^{d'_i}$ si $d_1 < d'_1$. Le monôme x_1^d est maximal parmi tous les monômes de degré d et est dans l'image de Div : $x_1^d = \frac{1}{d+1}\,\mathrm{Div}\, x_1^{d+1}$. Raisonnons par récurrence descendante sur l'ordre $<$ pour montrer que tous les autres monômes sont aussi dans l'image de Div. Soit $m = \prod x_i^{d_i}$. Posons $p = \mathrm{Div}\, x_1 m$. On a :

$$p = \frac{\partial}{\partial x_1}\mathrm{Div}\, x_1^{d_1+1}\prod_{i>1} x_i^{d_i} + \sum_{i>1}\frac{\partial}{\partial x_i} x_1^{d_1+1}\prod_{i>1} x_i^{d_i} = (d_1+1)m + x_1^{d_1+1}\sum_{i>1}\frac{\partial}{\partial x_i}\prod_{i>1} x_i^{d_i}.$$

Le monôme m s'exprime alors en fonction de $\mathrm{Div}\, x_1 m$ et de monômes strictement plus grands, et est donc dans l'image de Div. Enfin, par transposition, Etoile est injectif. □

On pourrait aussi constater qu'avec un changement de variables approprié, Div se ramène à une dérivation $\frac{d}{dy}$ sur une seule variable. La propriété précédente affirme donc simplement l'existence d'une intégrale.

2.2.6 Injectivité et surjectivité des opérateurs Div et Etoile

Nous avons maintenant suffisamment d'outils pour démontrer simplement les propriétés des opérateurs $\mathrm{Div}^{k\to i}$ et $\mathrm{Etoile}^{i\to k}$.

Théorème 2.2.15 ([Kan72]).
Soient i, k et n trois entiers.

- *Si $i \le k \le n-i$, alors l'opérateur $\mathrm{Div}^{k\to i}$ est surjectif et l'opérateur $\mathrm{Etoile}^{i\to k}$ est injectif ;*
- *Si $k \ge n-i$, alors l'opérateur $\mathrm{Etoile}^{i\to k}$ est surjectif et l'opérateur $\mathrm{Div}^{k\to i}$ est injectif.*

Cela correspond à l'intuition donnée par la dimension des espaces V_n^k. Si $i \le k \le n-i$, il y a moins de parties de taille i que de parties de taille k. Donc Etoile permet de plonger V_n^i comme sous-espace de V_n^k.

Nous nous contenterons de montrer que, lorsque $i \le k \le n-i$, l'opérateur $\mathrm{Div}^{k\to i}$ est surjectif. On en déduit que l'opérateur $\mathrm{Etoile}^{i\to k}$ est injectif, car c'est l'adjoint de $\mathrm{Div}^{k\to i}$. Le cas $k \le n-i$ s'obtient alors par passage au complémentaire.

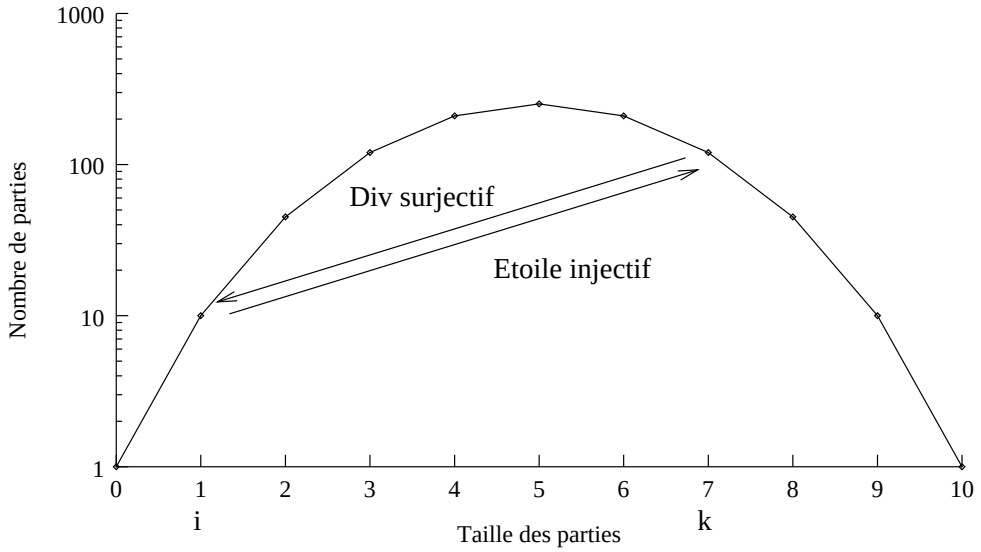


FIG. 2.1 – Nombre de parties de taille k de $\{1,\dots,n\}$, et opérateurs $\mathrm{Div}^{k\to i}$ et $\mathrm{Etoile}^{i\to k}$

La démonstration que nous donnons est inspirée de [Pou76, p. 125]. Le principe est le même que pour le théorème 2.2.14. Nous considérons une partie X de taille i, et nous montrons qu'elle est dans l'image de $\mathrm{Div}^{k\to i}$; en quelque sorte, nous intégrons X. Pour cela, nous écrivons X sous la forme $X \cup 1$ et nous faisons une succession d'intégrations par parties. Contrairement au cas des polynômes, la formule de dérivation n'est valable que pour des parties disjointes. Aussi, nous avons besoin d'une partie Y, disjointe de X, suffisamment grande pour intégrer la constante 1. C'est là qu'intervient la condition $k \le n-i$. Au final, lorsque $k = i+1$, nous exprimons X sous forme d'une somme alternée très proche d'une inversion de Möbius.

Démonstration. Soit X une partie de taille i. Comme $i+k \le n$, on peut prendre une partie Y de taille k disjointe de X. Posons $A_l := \mathrm{Div}^l X \,\mathrm{Div}^{k-l} Y$, pour $l \in \{1,\dots,k\}$. Le vecteur A_l est dans V_n^i, et, en utilisant le corollaire 2.2.9, on obtient :

$$\begin{aligned}
A_0 &= \mathrm{Div}^0 X \,\mathrm{Div}^k Y = k!X;\\
A_i &= \mathrm{Div}^i X \,\mathrm{Div}^{k-i} Y = i!\,\mathrm{Div}^{k-i} Y = i!(k-i)!\,\mathrm{Div}^{k\to i} Y;\\
A_l &= 0 \qquad \text{si } l > i.
\end{aligned}$$

En particulier, on note que A_i est dans l'image de $\mathrm{Div}^{k\to i}$. Procédons par récurrence sur $i-l$. Soit l_0, $0 \le l_0 < i$ tel que pour tout l, $l_0 < l \le i$, la partie A_l soit dans l'image de $\mathrm{Div}^{k\to i}$. On utilise le lemme 2.2.12 pour faire une intégration par parties de A_{l_0} :

$$\begin{aligned}
A_{l_0} &= \mathrm{Div}^{l_0} X \cup \mathrm{Div}^{k-l_0} Y\\
&= \mathrm{Div}^{k-i}(\mathrm{Div}^{l_0} X \cup \mathrm{Div}^{i-l_0} Y) - \sum_{j=1}^{k-i} \mathrm{C}_{k-i}^{j}\,\mathrm{Div}^{l_0+j} X \cup \mathrm{Div}^{k-l_0-j} Y\\
&= \mathrm{Div}^{k-i}(\mathrm{Div}^{l_0} X \cup \mathrm{Div}^{i-l_0} Y) - \sum_{j=1}^{k-i} \mathrm{C}_{k-i}^{j}\, A_{l_0+j}.
\end{aligned}$$

Donc le vecteur A_{l_0} est dans l'image de $\mathrm{Div}^{k\to i}$. On en déduit que $X = \frac{1}{k!}A_0$ est dans l'image de $\mathrm{Div}^{k\to i}$. Enfin, lorsque $k = i+1$, on obtient pour X l'expression directe :

$$X = \frac{1}{(i+1)!}\,\mathrm{Div}\left(\sum_{j=0}^{i}(-1)^{i-j}\,\mathrm{Div}^{i-j}\,X \cup \mathrm{Div}^{j}\,Y\right). \quad \square$$

Généralisations à d'autres scalaires

La seule propriété du corps $\mathbb{K}$ que nous avons utilisée est la possibilité de diviser par $k!$. Ce théorème se généralise donc aux corps de caractéristique $> k$, voire aux anneaux où $\{1,\dots,k\}$ sont tous inversibles. Les exemples suivants montrent les difficultés rencontrées lorsque $k!$ n'est pas inversible.

Exemple 2.2.16.
Dans le cas où $\mathbb{K} = \mathbb{Z}$, l'image de $\mathrm{Div}^{k\to i}$ est un sous-réseau de V_n^i contenant $k!\,V_n^i$. Nous conjecturons que $p := k!$ est le plus petit entier p strictement positif tel que l'image de $\mathrm{Div}^{k\to i}$ contient $p\,V_n^i$.

Exemple 2.2.17.
Dans le cas où $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, l'opérateur Div *définit un opérateur bord. On a en particulier* $\mathrm{Div}\circ\mathrm{Div} = 0$ *et* $\mathrm{Div} \neq 0$. *En aucun cas,* Div *ne peut être surjectif.*

Exemple 2.2.18.
En caractéristique p, et lorsque p divise n, le noyau de Div *et l'image de* Etoile *ne sont plus en somme directe. En effet, on a un vecteur non nul qui est à la fois dans l'image de* $\mathrm{Etoile}^{0\to 1}$ *et dans le noyau de* $\mathrm{Div}^{1\to 0}$ *:*

$$\sum_{i\in\{1,\dots,n\}}\{i\} = \mathrm{Etoile}^{0\to 1}\,\emptyset \qquad \textit{et} \qquad \mathrm{Div}^{1\to 0}\left(\sum_{i\in\{1,\dots,n\}}\{i\}\right) = n.\emptyset = 0.$$

2.3 Décomposition

Le théorème 2.2.15 montre que, si $i \leq k \leq n-i$t, alors on peut plonger V_n^i dans V_n^k. Nous allons nous servir de ce fait pour décomposer V_n^k en deux sous-espaces orthogonaux, puis en somme de $k+1$ sous-espaces orthogonaux. Nous verrons au § 3 le rôle de cette décomposition dans l'étude de l'action du groupe symétrique $\mathfrak{S}_n$ sur V_n^k. Nous avons besoin d'un produit scalaire pour définir la notion d'orthogonalité.

Nous munissons V_n du *produit scalaire canonique* tel que, pour deux parties distinctes A et B, $\langle A|A\rangle = 1$ et $\langle A|B\rangle = 0$. Dans la suite, nous supposons toujours qu'il est possible de définir un tel produit scalaire (voir [AB95] pour des conditions sur le corps $\mathbb{K}$). Par exemple, si le corps est $\mathbb{Q}$ ou $\mathbb{R}$, nous prenons le produit scalaire usuel. De même, sur $\mathbb{C}$, nous prenons le produit Hermitien. La plupart des résultats restent valables dans un corps quelconque de caractéristique zéro, et nous indiquons au cas par cas les difficultés éventuelles.

Théorème 2.3.1.
Soit i et k tels que $i \leq k$ et $2k-1 \leq n$. Alors,

$$V_n^k = \mathrm{Im}\,\mathrm{Etoile}^{i\to k} \oplus^{\perp} \mathrm{Ker}\,\mathrm{Div}^{k\to i},$$

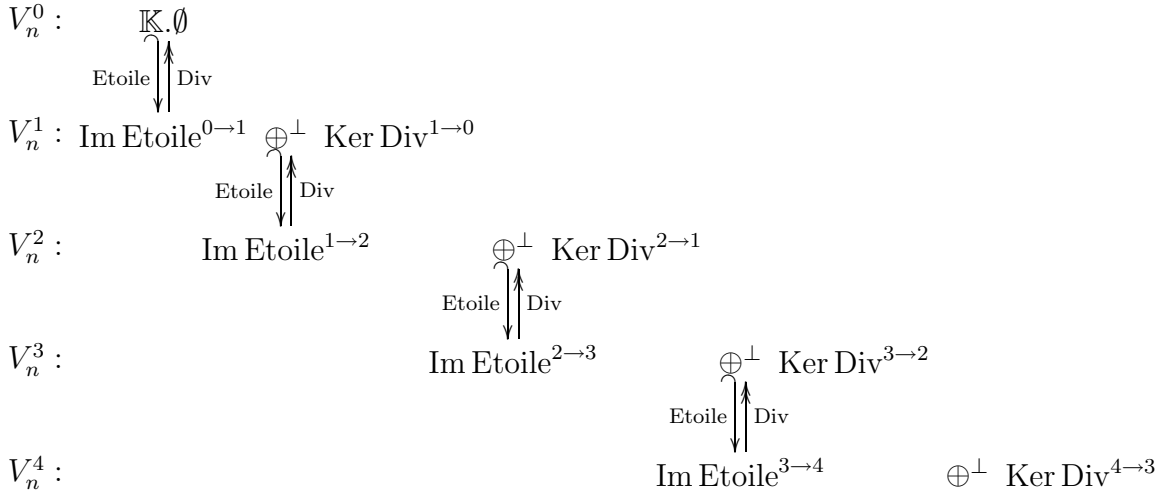
où $\operatorname{Im}\text{Etoile}^{i\to k}$ *est l'image de l'opérateur* $\text{Etoile}^{i\to k}$ *et* $\operatorname{Ker}\text{Div}^{k\to i}$ *le noyau de l'opérateur* $\text{Div}^{k\to i}$.

Démonstration. Comme les opérateurs $\text{Div}^{k\to i}$ et $\text{Etoile}^{i\to k}$ sont adjoints, les espaces $\operatorname{Im}\text{Etoile}^{i\to k}$ et $\operatorname{Ker}\text{Div}^{k\to i}$ sont en somme directe orthogonale. De plus, comme $2k-1 \leq n$, $\text{Div}^{k\to i}$ est surjective et $\text{Etoile}^{i\to k}$ est injective. L'argument de dimension suivant permet alors de conclure :

$$\begin{aligned}\dim V_n^k &= \dim \operatorname{Ker}\text{Div}^{k\to i} + \dim \operatorname{Im}\text{Div}^{k\to i} \\ &= \dim \operatorname{Ker}\text{Div}^{k\to i} + \dim V_n^i \\ &= \dim \operatorname{Ker}\text{Div}^{k\to i} + \dim \operatorname{Im}\text{Etoile}^{i\to k}\,.\end{aligned}$$

On a donc des plongements successifs comme dans l'exemple suivant :

Exemple 2.3.2.



Or, on remarque que $\operatorname{Ker}\text{Div}^{k\to i} \subset \operatorname{Ker}\text{Div}^{k\to i+1}$ et $\operatorname{Ker}\text{Etoile}^{i\to k} \subset \operatorname{Ker}\text{Etoile}^{i+1\to k}$. En effet, à un coefficient près, $\text{Div}^{k\to i+1} = \text{Div} \circ \text{Div}^{k\to i}$ et $\text{Etoile}^{i\to k} = \text{Etoile}^{i+1\to k} \circ \text{Etoile}$. Nous pouvons donc décomposer successivement chaque V_n^k comme dans l'exemple suivant :

Exemple 2.3.3.

$$\textit{dimension}: \quad \mathrm{C}_n^0 \qquad \mathrm{C}_n^1 - \mathrm{C}_n^0 \qquad \mathrm{C}_n^2 - \mathrm{C}_n^1 \qquad \mathrm{C}_n^3 - \mathrm{C}_n^2 \qquad \mathrm{C}_n^4 - \mathrm{C}_n^3 \quad .$$

$$\begin{array}{lccccccccc}
V_n^0: & \mathbb{K}.\emptyset & & & & & & & & \\
& \Big\downarrow \mathrm{Etoile} \;\; \Big\uparrow \mathrm{Div} & & & & & & & & \\
V_n^1: & \sim & \oplus^\perp & \mathrm{Ker\,Div}^{1\to 0} & & & & & & \\
& \Big\downarrow \mathrm{Etoile} \;\; \Big\uparrow \mathrm{Div} & & \Big\downarrow \mathrm{Etoile} \;\; \Big\uparrow \mathrm{Div} & & & & & & \\
V_n^2: & \sim & \oplus^\perp & \sim & \oplus^\perp & \mathrm{Ker\,Div}^{2\to 1} & & & & \\
& \Big\downarrow \mathrm{Etoile} \;\; \Big\uparrow \mathrm{Div} & & \Big\downarrow \mathrm{Etoile} \;\; \Big\uparrow \mathrm{Div} & & \Big\downarrow \mathrm{Etoile} \;\; \Big\uparrow \mathrm{Div} & & & & \\
V_n^3: & \sim & \oplus^\perp & \sim & \oplus^\perp & \sim & \oplus^\perp & \mathrm{Ker\,Div}^{3\to 2} & & \\
& \Big\downarrow \mathrm{Etoile} \;\; \Big\uparrow \mathrm{Div} & & \Big\downarrow \mathrm{Etoile} \;\; \Big\uparrow \mathrm{Div} & & \Big\downarrow \mathrm{Etoile} \;\; \Big\uparrow \mathrm{Div} & & \Big\downarrow \mathrm{Etoile} \;\; \Big\uparrow \mathrm{Div} & & \\
V_n^3: & \sim & \oplus^\perp & \sim & \oplus^\perp & \sim & \oplus^\perp & \sim & \oplus^\perp & \mathrm{Ker\,Div}^{4\to 3}
\end{array}$$

Théorème 2.3.4.
Si $2k-1 \leq n$, V_n^k *se décompose comme suit :*

$$\begin{array}{lcccccc}
V_n^k = \mathrm{Im\,Etoile}^{0\to k} & \oplus^\perp & \mathrm{Im\,Etoile}^{1\to k} & \cap & \mathrm{Ker\,Div}^{k\to 0} & & \\
& \oplus^\perp & & \cdots & & & \\
& \oplus^\perp & \mathrm{Im\,Etoile}^{k-1\to k} & \cap & \mathrm{Ker\,Div}^{k\to k-2} & \oplus^\perp & \mathrm{Ker\,Div}^{k\to k-1}
\end{array}$$

De plus, on a une décomposition duale lorsque $2k+1 \geq n$, qui s'obtient par passage au complémentaire. Nous nous contentons donc d'étudier le cas $2k-1 \leq n$. On note que la forme de cette décomposition est cohérente avec la croissance puis la décroissance des dimensions des espaces V_n^k (figure 2.1).

Le sous-espace $\mathrm{Ker\,Div}^{k\to k-1}$ représente la composante nouvelle dans les parties de taille k par rapport à celles de taille $k-1$. Nous l'appellerons *espace des k-hypergraphes 0-réguliers* et nous le noterons $\mathrm{Réguliers}_n^k$. Cette dénomination vient de la terminologie classique pour les graphes ($k=2$) : l'opérateur Div peut alors être vu comme l'application qui associe à un graphe la liste des degrés de ses sommets ; si un graphe est dans le noyau de l'opérateur Div, tous ses sommets sont de même degré 0. Il est donc 0-régulier. Au § 4, nous chercherons des bases des sous-espaces apparaissant dans cette décomposition. Pour cela, il suffira de chercher des bases des espaces $\mathrm{Réguliers}_n^k$.

Chapitre 3

Représentations du groupe symétrique

Nous considérons l'action naturelle du groupe symétrique sur l'espace V_n. La décomposition obtenue dans le chapitre précédent est en fait la décomposition en sous-modules irréductibles pour cette action. C'est une conséquence relativement immédiate de la théorie des représentations du groupe symétrique et nous en donnons plusieurs démonstrations.

3.1 Décomposition en irréductibles de V_n

Soit $\mathfrak{S}_n$ le groupe des permutations de $\{1, \ldots, n\}$. Chaque permutation σ de $\mathfrak{S}_n$ induit une permutation $\pi(\sigma)$ de l'ensemble $\mathcal{P}_n$ des parties de $\{1, \ldots, n\}$, définie par

$$\pi(\sigma)(A) = \{\sigma(a),\, a \in A\}$$

Cette transformation $\sigma \mapsto \pi\sigma$ est l'*action naturelle du groupe symétrique sur* $\mathcal{P}_n$. Lorsqu'il n'y a pas ambiguïté, nous omettons π pour alléger les notations. Ainsi, on notera $\sigma \cdot A = \pi(\sigma)(A)$. On note que cette action est *transitive* sur chacun des $\mathcal{P}_n^k$, c'est-à-dire que pour toutes parties A et B de même taille k, il existe une permutation σ telle que $\sigma.A = B$.

On étend cette action à l'espace V_n, en étendant chaque $\pi(\sigma)$ en une transformation linéaire de V_n. On obtient ainsi une *représentation linéaire* de $\mathfrak{S}_n$. Comme l'action naturelle π laisse $\mathcal{P}_n^k$ stable, elle laisse stable le sous-espace V_n^k, qui est donc un *sous-module*. La décomposition en somme directe orthogonale $V_n = \oplus^{\perp} V_n^k$ est donc une décomposition en *sous-modules* de V_n. Notre objectif est de décomposer à nouveau chaque V_n^k en sous-modules irréductibles. La finitude du groupe nous assure de l'existence d'une telle décomposition.

On note que ces sous-modules irréductibles sont en somme directe orthogonale, car le produit scalaire canonique est *invariant* (*i.e.* $\langle \sigma\mathbf{v} | \sigma\mathbf{w} \rangle = \langle \mathbf{v} | \mathbf{w} \rangle$). De plus, l'orthogonal d'un sous-module est aussi un sous-module (voir [FH96, § 1.2]).

Théorème 3.1.1.
Soit k tel que $2k \leq n$. La décomposition de V_n^k

$$\begin{array}{lcccl} V_n^k = \operatorname{Im}\operatorname{Etoile}^{0\to k} & \oplus^\perp & \left(\operatorname{Im}\operatorname{Etoile}^{1\to k} \right. & \cap & \left. \operatorname{Ker}\operatorname{Div}^{k\to 0}\right) \\ & \oplus^\perp & & \cdots & \\ & \oplus^\perp & \left(\operatorname{Im}\operatorname{Etoile}^{k-1\to k} \right. & \cap & \left. \operatorname{Ker}\operatorname{Div}^{k\to k-2}\right) \quad \oplus^\perp \quad \operatorname{Ker}\operatorname{Div}^{k\to k-1} \end{array}$$

est une décomposition en sous-modules irréductibles. Ces sous-modules sont deux à deux non-isomorphes et cette décomposition est donc unique.

Nous indiquerons plus précisément de quelles représentations irréductibles du groupe symétrique il s'agit dans le théorème 3.4.1. Ce théorème indique que l'opérateur Div est essentiellement le seul morphisme de V_n^k dans V_n^{k-1} préservant les symétries. Plus précisément, si f est un autre morphisme, alors sur chaque composante irréductible, f est de la forme $\lambda_i \operatorname{Div}$. Il en est, bien sûr, de même pour l'opérateur Etoile. Enfin, sur chaque composante irréductible, l'endomorphisme $\operatorname{Div} \circ \operatorname{Etoile}$ est de la forme $\lambda.\operatorname{Id}$, le coefficient λ dépendant évidemment de la composante.

Lemme 3.1.2.
Les opérateurs Div *et* Etoile *sont des $\mathfrak{S}_n$-morphismes.*

La démonstration est immédiate, et nous ne la donnons que pour Div, à titre d'exemple.

Démonstration.

$$\begin{aligned} \sigma \cdot \operatorname{Div}(A) &= \sigma \cdot \left(\sum_{a\in\{1,\dots,n\}/A} A \cup \{a\} \right) = \sum_{a\in\{1,\dots,n\}/A} \sigma \cdot A \cup \{\sigma(a)\} \\ &= \sum_{a\in\{1,\dots,n\}/\sigma\cdot A} \sigma \cdot A \cup \{a\} = \operatorname{Div}(\sigma \cdot A) \quad \square \end{aligned}$$

On en déduit que les espaces $\operatorname{Im}\operatorname{Etoile}^{i\to k}$ et $\operatorname{Ker}\operatorname{Div}^{k\to i}$ sont des sous-modules de V_n^k, ainsi que leurs intersections. La décomposition

$$\begin{array}{lcccl} V_n^k = \operatorname{Im}\operatorname{Etoile}^{0\to k} & \oplus^\perp & \left(\operatorname{Im}\operatorname{Etoile}^{1\to k} \right. & \cap & \left. \operatorname{Ker}\operatorname{Div}^{k\to 0}\right) \\ & \oplus^\perp & & \cdots & \\ & \oplus^\perp & \left(\operatorname{Im}\operatorname{Etoile}^{k-1\to k} \right. & \cap & \left. \operatorname{Ker}\operatorname{Div}^{k\to k-2}\right) \quad \oplus^\perp \quad \operatorname{Ker}\operatorname{Div}^{k\to k-1} \end{array}$$

est donc une décomposition de V_n^k en sous-modules.

Il ne reste qu'à montrer que ces sous-modules sont irréductibles. Comme le suggère l'exemple 2.3.3, le sous-module $\operatorname{Im}\operatorname{Etoile}^{i\to k} \cap \operatorname{Ker}\operatorname{Div}^{k\to i-1}$ est isomorphe via $\operatorname{Etoile}^{i\to k}$ au sous-module $\operatorname{Ker}\operatorname{Div}^{i\to i-1} = \text{Réguliers}_n^i$ des k-hypergraphes 0-réguliers. Il suffit donc de montrer que, pour tout k, les sous-modules Réguliers_n^k sont irréductibles et qu'ils sont deux à deux non-isomorphes.

3.2 Démonstration élémentaire de l'irréductibilité

Nous n'utilisons ici que le premier résultat de la théorie des représentations.

Lemme 3.2.1 (de Schur [FH96]).
Soit V une représentation linéaire d'un groupe fini G. Alors V est une représentation irréductible de G si, et seulement si, les seuls G-morphismes de V dans V sont les homothéties.

Nous allons étudier les $\mathfrak{S}_n$-morphismes de V_n^k dans Réguliers_n^k. Pour cela, on définit une distance sur $\mathcal{P}_n^k$, mesurant le nombre d'éléments non communs aux deux parties.

Définition 3.2.2 (Distance sur $\mathcal{P}_n^k$).
Pour A et B dans $\mathcal{P}_n^k$, on pose :

$$d(A,B) = k - |A \cap B| \quad \left(= |B \setminus A| = |A \setminus B| = \frac{|A \,\Delta\, B|}{2} \right)$$

où $|C|$ dénote le cardinal de l'ensemble C.

On remarque que $d(A,A) = 0$ et on peut vérifier simplement que d est bien une distance. Nous aurons besoin du lemme suivant qui nous donnera comme sous-produit les formules de projections de V_n^k sur Réguliers_n^k.

Lemme 3.2.3.
Soient f un $\mathfrak{S}_n$-morphisme de V_n^k dans Réguliers_n^k et A une partie de taille k de $\{1,\dots,n\}$. Alors $f(A)$ est de la forme

$$f(A) = \lambda_f \sum_{B \in \mathcal{P}_n^k} \alpha_{d(A,B)}\, B$$

où les coefficients α_d ne dépendent ni de A ni du morphisme et le coefficient λ_f ne dépend que du morphisme f. De fait, pour tout d tel que $0 \leq d \leq k$, on a :

$$\alpha_d = \frac{(-1)^l}{\mathrm{C}_{n-k}^d}.$$

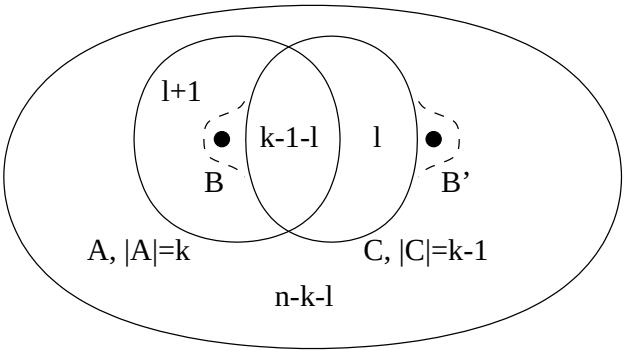
En particulier, α_0=1.

Démonstration. Nous allons d'abord montrer que les symétries du problème, modélisées par l'action de $\mathfrak{S}_n$, imposent que $f(A)$ soit de la forme

$$f(A) = \lambda \sum_{B \in \mathcal{P}_n^k} \alpha_{d(A,B)}\, B.$$

Soit $\mathfrak{S}_{A,\complement A}$ le sous-groupe des permutations de $\mathfrak{S}_n$ stabilisant A ; clairement $\mathfrak{S}_{A,\complement A}$ est isomorphe au produit direct $\mathfrak{S}_A \times \mathfrak{S}_{\complement A}$. Comme f est un $\mathfrak{S}_n$-morphisme, si $\sigma \in \mathfrak{S}_{A,\complement A}$ alors $\sigma \cdot f(A) = f(\sigma \cdot A) = f(A)$. Fixons un $d \in \{0,\dots,k\}$. On voit que l'action de $\mathfrak{S}_{A,\complement A}$ sur $\{B, d(A,B) = d\}$ est transitive. Il faut donc que les coefficients de chacun de ces B dans $f(A)$ soient tous identiques. D'où la forme requise.

Maintenant, nous allons utiliser le fait que l'image $f(A)$ est dans Réguliers_n^k (*i.e.*, $\text{Div}(f(A)) = 0$) pour trouver les contraintes sur les coefficients que nous avons annoncées. Pour cela, nous allons donner une relation de récurrence entre les α_d. Soit $d \in \{0, k-1\}$. Soit C une partie à $k-1$ éléments telle que $|C \cap {}^{\complement}A| = d$ et donc $|C \cap A| = k-1-d$. Le coefficient de C dans $\text{Div}(f(a))$ doit être nul. Évaluons-le. Soit B une partie de taille k contenant C. Selon que l'élément supplémentaire de B est dans A ou dans ${}^{\complement}A$, la distance $d(A, B)$ vaut d ou $d+1$. On a $d+1$ choix pour B dans le premier cas, et $n-k-d$ dans le second.



On en déduit la relation :

$$(d+1)\,\alpha_d + (n-k-d)\alpha_{d+1} = 0,$$

qui donne par récurrence :

$$\alpha_d = \frac{(-1)^d}{\text{C}_{n-k}^d}\alpha_0.$$

Quitte à multiplier λ et les α_d par une constante, on peut se ramener à $\alpha_0 = 1$. Nous obtenons alors bien l'expression annoncée pour les α_d qui ne dépend ni du choix de A, ni du morphisme f. Le coefficient λ est alors le coefficient de A dans $f(A)$.

Il ne reste plus qu'à montrer que le coefficient λ ne dépend pas de A. Soient A et B deux parties de taille k et λ_A et λ_B leurs coefficients respectifs. Soit σ une permutation telle que $\sigma \cdot A = B$. Comme $f(B) = f(\sigma \cdot A) = \sigma \cdot f(A)$, le coefficient de B dans $f(B)$ est égal au coefficient de A dans $f(A)$. Donc $\lambda_A = \lambda_B = \lambda_f$ comme voulu. □

Nous noterons R_A l'expression $\sum_B \alpha_{d(A,B)} B$ obtenue.

Démonstration du théorème 3.1.1. Le lemme 3.2.3 montre en fait que l'espace des $\mathfrak{S}_n$-morphismes de V_n^k dans f est de dimension 1. Cela implique en particulier que l'espace des automorphismes de Réguliers_n^k est de dimension 1. Donc, d'après le lemme de Schur, le module Réguliers_n^k est irréductible. De plus, il n'y a dans V_n^k qu'un seul sous-module isomorphe à Réguliers_n^k, qui est donc Réguliers_n^k lui-même. □

On déduit aussi du lemme 3.2.3 les formules de projections sur Réguliers_n^k et $\text{Im Etoile}^{k-1\to k}$.

Corollaire 3.2.4.
Soit $\pi_{\text{Réguliers}_n^k}$ *la projection orthogonale sur l'espace* Réguliers_n^k *et* $\pi_{\text{Im Etoile}^{k-1\to k}}$ *la*

projection sur son orthogonal.

$$\pi_{\text{Réguliers}_n^k}(A) = \frac{n-2k+1}{n-k+1}\sum_{l=0}^{k}\frac{(-1)^l}{\mathrm{C}_{n-k}^l}\sum_{B\in\mathcal{P}_n^k, d(A,B)=l} B$$

$$\pi_{\text{Im Etoile}^{k-1\to k}}(A) = A - \frac{n-2k+1}{n-k+1}\sum_{l=0}^{k}\frac{(-1)^l}{\mathrm{C}_{n-k}^l}\sum_{B\in\mathcal{P}_n^k, d(A,B)=l} B$$

Démonstration. Soit $\pi = \pi_{\text{Réguliers}_n^k}$. D'après le lemme 3.2.3, il suffit d'évaluer λ_π. En utilisant l'orthogonalité de $\pi(A)$ et $A-\pi(A)$ on obtient l'équation

$$0 = \langle A-\pi(A)|\pi(A)\rangle = \langle A|\pi(A)\rangle - \langle \pi(A)|\pi(A)\rangle = \lambda - \lambda^2\langle R_A|R_A\rangle$$

(On rappelle que le coefficient de A dans $\pi(A)$ est λ). Calculons ce dernier produit scalaire :

$$\begin{aligned}
\langle R_A|R_A\rangle &= \sum_B \alpha_{d(A,B)}^2 = \sum_{d=0}^{k}\alpha_d^2|\{B,\, d(A,B)=d\}| \\
&= \sum_{d=0}^{k}\left(\frac{(-1)^d}{\mathrm{C}_{n-k}^d}\right)^2 \mathrm{C}_k^{k-d}\,\mathrm{C}_{n-k}^d \\
&= \sum_{d=0}^{k}\frac{d!^2(n-k-d)!^2}{(n-k)!^2}\frac{k!}{d!(k-d)!}\frac{(n-k)!}{d!(n-k-d)!} \\
&= \sum_{d=0}^{k}\frac{k!(n-k-d)!}{(n-k)!(k-d)!} \\
&= \sum_{d=0}^{k}\frac{k!(n-2k)!}{(n-k)!}\frac{(n-k-d)!}{(k-d)!(n-2k)!} \\
&= \sum_{d=0}^{k}\frac{\mathrm{C}_{n-k-d}^{k-d}}{\mathrm{C}_{n-k}^k} \\
&= \frac{1}{\mathrm{C}_{n-k}^k}\sum_{d=0}^{k}\mathrm{C}_{n-2k+d}^d
\end{aligned}$$

Nous avons besoin pour conclure du petit lemme combinatoire suivant

Lemme 3.2.5.

$$\mathrm{C}_{(m+1)+k}^k = \sum_{d=0}^{k}\mathrm{C}_{m+d}^d$$

Démonstration. Le coefficient $\mathrm{C}_{(m+1)+k}^k$ compte le nombre de façons de répartir k objets identiques parmi $m+2$ cases. Pour obtenir le même résultat, on peut aussi répartir d objets dans les $m+1$ premières cases (C_{m+d}^d possibilités), puis mettre les $k-d$ objets restants dans la dernière case. □

Conclusion :

$$\langle R_A|R_A\rangle = \frac{\mathrm{C}_{n-2k+1}^k}{\mathrm{C}_{n-2k}^k} = \frac{n-k+1}{n-2k+1}.$$

et donc, comme la solution $\lambda = 0$ ne nous intéresse pas,

$$\lambda = \frac{n-2k+1}{n-k+1}. \quad \square$$

3.3 Démonstration utilisant les caractères

Lemme 3.3.1.
Soit $\chi_{V_n^k}$ le caractère de la représentation naturelle du groupe symétrique sur V_n^k. Si $2k \leq n$, on a

$$\langle \chi_{V_n^k} | \chi_{V_n^k} \rangle = k+1.$$

Démonstration. Le calcul que nous allons faire porte sur la k-ième puissance symétrique de la représentation naturelle de $\mathfrak{S}_n$. Nous nous sommes inspirés d'un calcul similaire sur la k-ième puissance extérieure apparaissant dans [FH96, Proposition 3.2, p. 31].

$$\begin{aligned}
\langle \chi_{V_n^k} | \chi_{V_n^k} \rangle &= \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \chi_{V_n^k}(\sigma)^2 = \frac{1}{n!} \sum_{\sigma} |\{\text{pts fixes de } \sigma\}|^2 \\
&= \frac{1}{n!} \sum_{\sigma} \left(\sum_{A \in \mathcal{P}_n^k, \sigma \cdot A = A} 1 \right)^2 = \frac{1}{n!} \sum_{\sigma} \sum_{B, \sigma \cdot B = B} \sum_{C, \sigma \cdot C = C} 1 \\
&= \frac{1}{n!} \sum_{(B,C)} \sum_{\sigma, \sigma \cdot B = B, \sigma \cdot C = C} 1 \\
&= \frac{1}{n!} \sum_{(B,C)} |\{\sigma, \sigma \cdot B = B, \sigma \cdot C = C\}| \\
&= \sum_{(B,C)} \frac{|B \cap C|! \, |B \setminus C|! \, |C \setminus B|! \, |\complement(B \cup C)|!}{n!} \\
&= \sum_{l, 0 \leq l \leq k} \sum_{(B,C), |B \cap C| = l} \frac{l!(k-l)!(k-l)!(n-2k+l)!}{n!}
\end{aligned}$$

Or, le nombre de couples (B, C) de parties de taille k ayant une intersection de taille l est justement le multinomial

$$\frac{n!}{l!(k-l)!(k-l)!(n-2k+l)!},$$

puisqu'il faut répartir n éléments entre $B \cap C$, $B \setminus C$, $C \setminus B$ et $\complement(B \cup C)$. Nous concluons donc que :

$$\langle \chi_{V_n^k} | \chi_{V_n^k} \rangle = \sum_{l, 0 \leq l \leq k} 1 = k+1. \quad \square$$

Nous rappelons le théorème suivant [FH96, Corollary 2.15, p.17] :

Théorème 3.3.2.
Soit W une représentation d'un groupe fini. Soit $W_1, \ldots, W_l$ les composantes irréductibles de G deux à deux non-isomorphes apparaissant dans W et $a_1, \ldots, a_l$ leurs multiplicités. ($W \cong W_1^{\oplus a_1} \oplus \cdots \oplus W_l^{\oplus a_l}$). On a :

$$\langle \chi_W | \chi_W \rangle = a_1^2 + \cdots + a_l^2.$$

Nous avons maintenant tous les éléments pour démontrer le théorème 3.1.1.

Démonstration. Soient $a_1, \ldots, a_l$ les multiplicités des représentations de $\mathfrak{S}$ apparaissant dans V_n^l. Nous allons montrer que $l = k$ et que les a_i sont tous égaux à 1. D'après le lemme 3.3.1 et le théorème 3.3.2, $\sum a_i^2 = k$. De plus on sait que V_n se décompose en au moins k modules irréductibles, donc $\sum a_i \geq k$. Nous rappelons que les a_i sont des entiers supérieurs ou égaux à 1 et donc $a_i \leq a_i^2$. Mais alors on a aussi

$$a_i^2 = k - \sum_{j \neq i} a_j^2 \leq k - \sum_{j \neq i} a_j \leq a_i,$$

et donc $a_i = 1$.

Conclusion : V_n^k est la somme de k sous-modules irréductibles deux à deux non-isomorphes. La décomposition étant alors unique, ce sont forcément les k sous-modules de notre décomposition. □

3.4 Démonstration utilisant la théorie des représentations du groupe symétrique

Nous supposerons ici que le lecteur est familier avec les constructions des représentations irréductibles du groupe symétrique. En particulier, nous ne rappellerons que les définitions qui seront utiles pour comprendre les liens avec notre propos principal. Nous utiliserons la construction basée sur les modules de Specht et les tabloïdes. Le lecteur pourra se rapporter à [FH96, Problem 4.47, p .60] et surtout à [Sag91, Chapitre 2], dont nous utiliserons les notations.

Les représentations irréductibles du groupe symétrique $\mathfrak{S}_n$ sont paramétrées par les partitions de n. Étant donnée une telle partition $\lambda = [\lambda_1, \ldots, \lambda_l]$ on peut en effet construire un module irréductible appelé module de Specht S^λ. On obtient de cette façon et de manière unique toutes les représentations irréductibles du groupe symétrique. De manière usuelle, nous noterons aussi S^λ par $[\lambda_1, \ldots, \lambda_l]$. Nous allons démontrer le théorème suivant :

Théorème 3.4.1.
Si $2k+1 \leq n$ alors $V_n^k \cong [n] \oplus [n-1,1] \oplus \cdots \oplus [n-k,k]$. De plus, le module $[n-i,i]$ est isomorphe au module $\operatorname{Im}\text{Etoile}^{i \to k} \cap \operatorname{Ker}\text{Div}^{k \to i-1}$ de notre décomposition. En particulier, $[n-k,k]$ est isomorphe au module Réguliers_n^k des k-hypergraphes 0-réguliers.

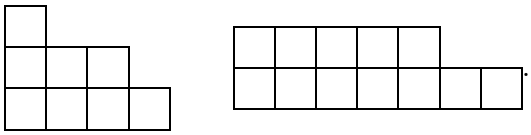
Exemple 3.4.2.
L'espace des graphes V_n^2 se décompose comme suit :

$$V_n^2 = [n] \oplus [n-1,1] \oplus [n-2,2].$$

La composante $[n]$ *correspond à la droite vectorielle engendrée par le graphe complet. L'espace* $[n] \oplus [n-1,1]$ *correspond à l'espace vectoriel engendré par les* n *étoiles* $(\text{Etoile}\{1\}, \ldots, \text{Etoile}\{n\})$. *L'action sur cet espace est l'action naturelle du groupe symétrique par permutation de ces étoiles. Enfin, l'espace* $[n-2,2]$ *est l'espace des graphes* 0*-réguliers.*

Démonstration. Nous rappelons grossièrement la construction des modules de Specht, basée sur les tabloïdes. Nous avons besoin des objets combinatoires suivants :

Définitions 3.4.3 (Diagramme de Ferrers, Tableau et Tabloïde).
Soit λ *une partition d'un entier* n, *par exemple* $\lambda := (4,3,1)$ *ou* $\lambda := (7,5)$. *On associe à* λ *un* diagramme de Ferrers *:*



Si l'on remplit les cases d'un de ces diagrammes avec les entiers de 1 *à* n, *on obtient un* tableau de Young *ou* λ-tableau *:*

4						
3	8	7				
5	1	6	2			

3	5	6	8	12		
1	2	4	7	9	10	11

Si les entrées d'un tableau de Young sont croissantes selon les lignes et les colonnes, le tableau est dit standard. *Le premier tableau n'est pas standard, mais le second l'est. Deux* λ*-tableaux sont dits* ligne-équivalents *si les lignes de chacun des deux tableaux contiennent les mêmes éléments. Par exemple, les deux tableaux suivants sont ligne-équivalents :*

4			
3	8	7	
5	1	6	2

4			
7	3	8	
1	6	5	2

Un λ*-tabloïde ou tabloïde est une classe d'équivalence pour cette relation. Nous noterons comme suit le tabloïde correspondant à la classe d'équivalence du tableau précédent*

4			
3	8	7	
5	1	6	2

Le groupe symétrique agit naturellement sur les tabloïdes en appliquant la permutation à chacun des éléments du tabloïde. Par exemple :

$$(1,2,3,4).\begin{array}{|c|c|c|c|}\hline 4 & & & \\ \hline 3 & 8 & 7 & \\ \hline 5 & 1 & 6 & 2 \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline 1 & & & \\ \hline 4 & 8 & 7 & \\ \hline 5 & 2 & 6 & 3 \\ \hline \end{array}.$$

On peut aussi voir un tabloïde comme une partition de $\{1, \ldots, n\}$ en l sous-ensembles $A_1, \ldots, A_l$ avec $|A_i| = \lambda_i$. En particulier si $l = 2$ (partition de la forme

$[n-k,k]$), cela revient à considérer une partition de $\{1,\dots,n\}$ en deux ensembles de tailles respectives $n-k$ et k. En jetant la première de ces parties nous obtenons une bijection entre les tabloïdes de forme $[n-k,k]$ et les parties de taille k. On remarque que le groupe symétrique agit de façon similaire sur les $[n-k,k]$-tabloïdes et les parties de taille k. Cette bijection est donc un isomorphisme pour l'action du groupe symétrique.

Exemple 3.4.4.

$$(1,2,3,4)\cdot\overline{\begin{array}{|c|c|c|}\hline 4&1&7\\\hline\end{array}\begin{array}{|c|c|c|c|}\hline 5&2&6&3\\\hline\end{array}}=\overline{\begin{array}{|c|c|c|}\hline 1&2&7\\\hline\end{array}\begin{array}{|c|c|c|c|}\hline 5&3&6&4\\\hline\end{array}},$$

$$(1,2,3,4)\cdot\{4,1,7\}=\{1,2,7\}.$$

La suite de la construction consiste à définir le module de permutation M^λ.

Définition 3.4.5.
Soit M^λ l'espace vectoriel sur $\mathbb{K}$ ayant pour base les tabloïdes de forme λ. On munit M^λ de la représentation linéaire correspondant à l'action de $\mathfrak{S}_n$ sur les tabloïdes. L'espace M^λ est appelé module de permutation associé à λ.

On note que, du fait de l'identification entre les tabloïdes à deux lignes et les ensembles, le module $M^{[n-k,k]}$ est exactement le module V_n^k que nous étudions !

Nous rappelons la fin de la construction de S^λ. On a préalablement défini l'ordre de dominance $\lhd$ sur les partitions et on suppose avoir déjà construit les modules S^μ avec $\mu \lhd \lambda$. On peut alors montrer que si l'on décompose M^λ en sous-modules irréductibles, on obtient des modules irréductibles S^μ avec $\mu \lhd \lambda$ plus un unique nouveau module irréductible. On définit S^λ comme étant ce module. La dimension de cet espace est le nombre de tableaux standard de forme λ. On peut donner des formules de projections explicites de M^λ sur S^λ.

Pour démontrer le théorème 3.4.1, il suffit d'appliquer les outils de cette théorie. Ici, nous allons utiliser la règle de Young qui ramène le problème à un dénombrement de tableaux semi-standard. Il s'agit d'une généralisation des tableaux standard dans lesquels on autorise la répétition de certains entiers.

Définition 3.4.6 (Tableau semi-standard).
Soit λ une partition de n. On appelle tableau semi-standard de forme λ *un remplissage t du de forme λ par des nombres entiers, tels que les lignes soient croissantes au sens large et les colonnes croissantes au sens strict. On appelle* contenu *de t la composition μ de n, telle que μ_i compte le nombre d'entiers égaux à i dans t. Par exemple, le tableau semi-standard suivant est de forme $[4,3,1]$ et de contenu $[2,2,3,0,1]$:*

$$\begin{array}{|c|c|c|c|}\hline 5&&&\\\hline 2&3&3&\\\hline 1&1&2&3\\\hline\end{array}\ .$$

Théorème 3.4.7 (Règle de Young [Sag91]).
Soit μ une partition de n. La décomposition en irréductibles du module de permutation M^μ est :

$$M^\mu \cong \bigoplus_\lambda K_{\lambda\mu} S^\lambda$$

où $K_{\lambda\mu}$ est le nombre de Kostka pour (λ, μ), c'est-à-dire le nombre de tableaux semi-standard de forme λ et de contenu μ.

Partons de V_n^k ; cet espace étant isomorphe à $M^{[n-k,k]}$, évaluons les $K_{\lambda\mu}$, avec $\mu := [n-k, k]$ (par exemple, $\mu := [5, 3]$). Soit λ une partition de n. Il faut trouver combien de tableaux semi-standard on peut former en remplissant le de forme λ de $n-k$ zéros et k uns de façon à ce que les lignes soient croissantes et les colonnes strictement croissantes.

Si λ a plus de trois lignes c'est impossible, car il faudrait au moins trois valeurs différentes :

1				
1	1			
0	0	0	0	0

.

Donc, λ est de la forme $[n-i, i]$. Si la deuxième ligne contient des 0, le tableau n'est pas semi-standard :

0	1	1	1	
0	0	0	0	

.

Donc $i \leq k$. Enfin, pour respecter les croissances, il n'y a qu'un seul remplissage possible :

1	1					
0	0	0	0	0	1	

.

Remarquons que nous avons utilisé implicitement le fait que $k \leq n-k$, pour interdire la situation suivante :

1	1	1		
0	0	1	1	

.

Conclusion :

$$M^{[n-k,k]} \cong \bigoplus_{i \leq k} S^{[n-i,i]}$$

ou, autrement dit,

$$V_n^k \cong [n] \oplus [n-1, 1] \oplus \cdots \oplus [n-k, k].$$

Par récurrence, chacun des $[n-i, i]$ avec $i < k$ correspond à l'image de l'espace Réguliers_n^i par $\text{Etoile}^{i \to k}$. Le dernier module restant $[n-k, k]$ correspond donc bien à l'espace Réguliers_n^k des k-hypergraphes 0-réguliers. □

Chapitre 4

Bases des k-hypergraphes 0-réguliers

4.1 Introduction

Nous avons vu que la dimension de l'espace Réguliers_n^k est $\text{C}_n^k - \text{C}_n^{k-1}$. Pour $n = 2k$, elle vaut $\frac{1}{k+1}\,\text{C}_{2k}^k$. C'est le très classique nombre c_k de Catalan, qui compte des objets combinatoires divers : bons parenthésages ou mots de Dyck à k parenthèses ouvrantes et fermantes, tableaux standard de forme $[k, k]$, arbres ordonnés à $k+1$ sommets, arbres binaires à k sommets, arbres binaires complets à $2k+1$ sommets (voir, par exemple, [SW86]). Dans le cas général, la dimension de l'espace Réguliers_n^k est liée aux préfixes de mots de Dyck et aux tableaux standard à deux lignes.

4.2 Préliminaires combinatoires : mots de Dyck et tableaux

Définition 4.2.1 (Parenthésage).
Un parenthésage *est un mot $u = u_1 \dots u_n$ composé de parenthèses ouvrantes « (» et fermantes «) ». L'entier n est la* longueur *du mot.*

Définition 4.2.2 (Préfixe de mot de Dyck).
Un mot de Dyck *est un parenthésage tel que :*

(i) u contient autant de parenthèses ouvrantes que de parenthèses fermantes.

(ii) Tout préfixe de u contient au moins autant de parenthèses ouvrantes que de parenthèses fermantes.

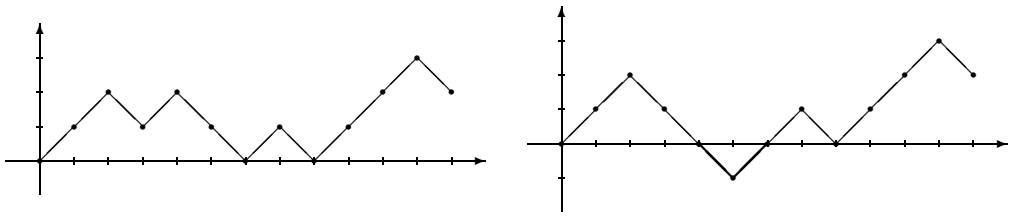
Un préfixe de mot de Dyck *est un parenthésage pour lequel on impose seulement la deuxième condition. Nous notons Dyck_n^k l'ensemble des mots de longueur n ayant k parenthèses fermantes et qui sont préfixes de mots de Dyck. Ainsi, Dyck_{2k}^k est l'ensemble des mots de Dyck de longueur $2k$.*

Définition 4.2.3 (Représentation par des chemins).
Soit u un parenthésage et i une position dans u. On définit y_i comme le nombre de parenthèses ouvrantes moins le nombre de parenthèses fermantes dans le préfixe $u_1 \dots u_i$. On peut maintenant représenter un parenthésage comme un chemin dans $\mathbb{Z}^2$ partant de l'origine :

$$(0,0), (1,y_1), \dots, (i,y_i), \dots, (n,y_n)$$

Pour chaque i, on fait un pas à droite, en montant si u_i est une parenthèse ouvrante et en descendant si u_i est une parenthèse fermante. Comme on peut le voir dans les exemples suivants, les mots de Dyck_n^k *correspondent aux chemins de* $(0,0)$ *à* $(n, n-2k)$ *qui ne passent pas sous l'axe des abscisses.*

Exemple 4.2.4.
« (()())()((() » est un préfixe de mot de Dyck (dans Dyck_{12}^5*), mais pas « ()))(()((() ». Voici les chemins correspondants :*



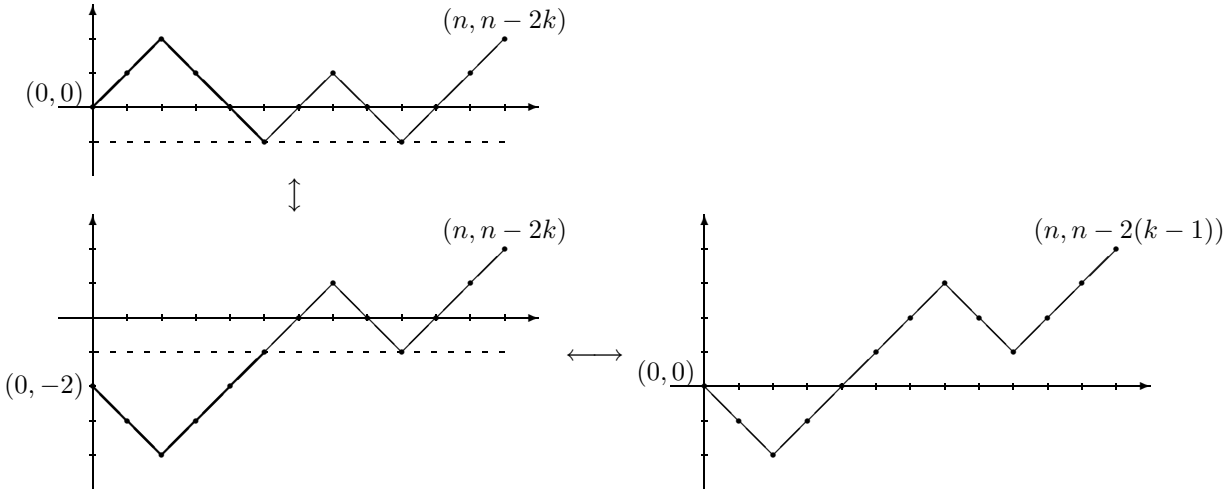
Nous utiliserons alternativement les représentations sous forme de mot ou de chemin, en choisissant la plus visuelle.

Le théorème suivant a motivé notre recherche de constructions de bases de $\mathrm{Réguliers}_n^k$ à partir de ces objets.

Théorème 4.2.5 ([SW86]).
Soient n et k deux entiers tels que $2k \leq n$. Les quantités suivantes valent toutes $\mathrm{C}_n^k - \mathrm{C}_n^{k-1}$:
- *nombre d'éléments de* Dyck_n^k,
- *nombre de tableaux standard de forme* $[n-k, k]$,
- *dimension de l'espace* $\mathrm{Réguliers}_n^k$.

Nous montrons d'abord que $|\,\mathrm{Dyck}_n^k\,| = \mathrm{C}_n^k - \mathrm{C}_n^{k-1}$. La démonstration est basée sur le [And97]. Puis nous donnons la bijection usuelle entre mots de Dyck et tableaux standard.

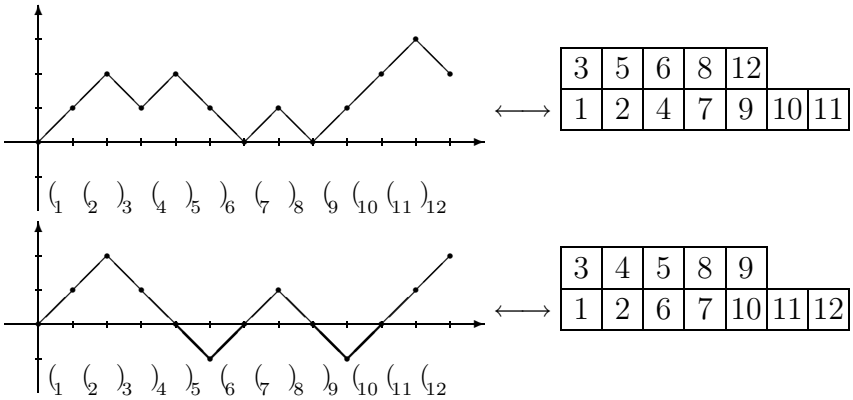
Démonstration. Le nombre de mots à k parenthèses fermantes parmi n est évidemment C_n^k. Parmi ceux-là, il faut montrer qu'il y en a C_n^{k-1} qui ne sont pas des préfixes de mots de Dyck. Pour cela, on met en bijection ces mauvais mots avec les mots à $k-1$ parenthèses fermantes. L'idée, simple mais astucieuse, se visualise mieux sur les chemins. Un mauvais chemin passe en dessous de l'axe des abscisses et croise donc forcément l'horizontale -1. On prend alors le début du chemin jusqu'au premier croisement et on en fait une symétrie par rapport à l'horizontale -1. On obtient un chemin partant de $(0,-2)$ et arrivant à $(n, n-2k)$, que l'on peut remonter en un chemin de $(0,0)$ à $(n, n-2(k-1))$ par symétrie relative à l'horizontale -1.



Réciproquement, soit m un mot avec $k-1$ parenthèses fermantes. On prend le chemin correspondant de $(0,0)$ à $(n, n-2(k-1))$, et on le décale vers le bas de deux crans. Le chemin obtenu va de $(0,-2)$ à $(n, n-2k)$ et donc croise au moins une fois l'horizontale -1. En symétrisant le début du mot jusqu'au croisement avec cette horizontale, on obtient un mauvais chemin.

Il est clair que ces deux opérations sont inverses l'une de l'autre. □

Démonstration de la bijection entre préfixes de mot de Dyck et tableaux standard. Il y a une bijection très simple entre les mots avec k parenthèses fermantes parmi n et les tableaux de Young de forme $[n-k, k]$ dont les lignes sont croissantes. On met dans les cases du haut du tableau et dans l'ordre croissant les positions des parenthèses fermantes et de même dans les cases du bas les positions des parenthèses ouvrantes. Par exemple :



3	5	6	8	12		
1	2	4	7	9	10	11

3	4	5	8	9		
1	2	6	7	10	11	12

Maintenant le tableau est standard si, et seulement si, ses colonnes sont elles aussi croissantes, c'est-à-dire si la i-ième parenthèse fermante est toujours positionnée après la i-ième parenthèse ouvrante ; autrement dit, si le mot est bien parenthésé. □

4.3 Base des tableaux standard projetés orthogonalement

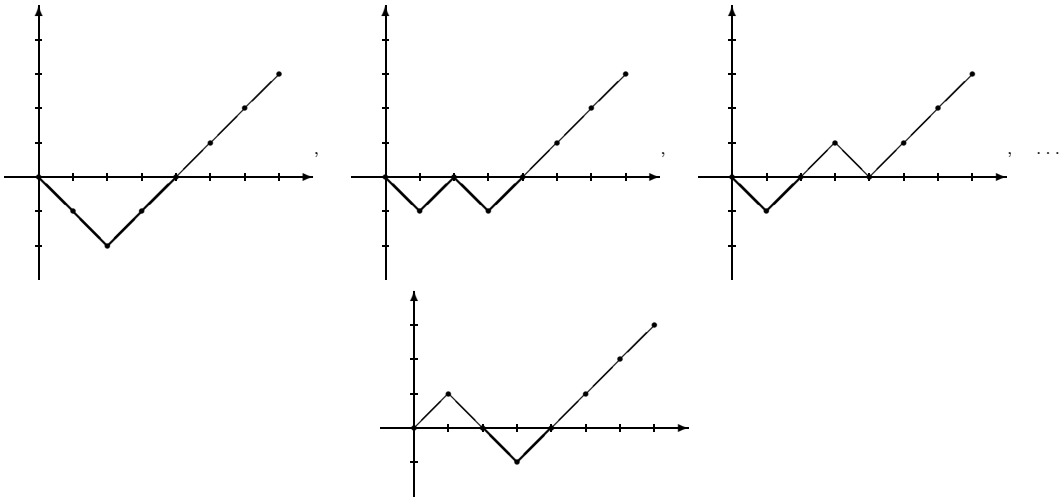
La manière la plus simple de construire des éléments de Réguliers_n^k est de projeter orthogonalement des vecteurs de V_n^k sur ce sous-espace. Or, les parties de taille k

engendrent V_n^k. Donc si l'on considère leurs projections sur Réguliers$_n^k$, on obtient un ensemble générateur. Il est donc tentant d'essayer d'en extraire une base.

On peut associer à tout tableau de forme $[n-k,k]$ une partie à k éléments, et ce, en prenant la partie formée des k nombres de la ligne du haut.

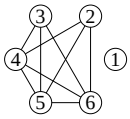
Problème 4.3.1.
Les projections orthogonales de ces parties forment-elles une base de Réguliers$_n^k$ *?*

Pour $k=0$ ou $k=1$ la conjecture se vérifie simplement. Nous allons montrer qu'elle est vraie pour Réguliers$_n^2$, c'est-à-dire pour les graphes 0-réguliers. Les seuls mauvais mots à 2 parenthèses fermantes sont alors les n suivants :



Ils correspondent aux arêtes $\{1,2\},\{1,3\},\ldots,\{1,n\}$ et $\{2,3\}$.

Proposition 4.3.2.
Les projections orthogonales des arêtes $\{i,j\}$ *avec* $2\le i<j\le n$ *et* $\{i,j\}\neq\{2,3\}$ *forment une base de* Réguliers$_n^2$.



Démonstration. Comme les $\pi(\{i,j\})$ engendrent Réguliers$_n^2$, il suffit de montrer que les projections correspondant aux mauvais mots s'expriment en fonction des autres.

Pour les arêtes $\{1,i\}$, c'est très simple :

$$\{1,i\}=\{1,i\}-\text{Etoile}(\{i\})+\text{Etoile}(\{i\})=-\sum_{j,\,2\le j\le n,\,j\neq i}\{i,j\}+\text{Etoile}(\{i\})$$

et donc

$$\pi(\{n,i\})=-\sum_{j,\,2\le j\le n,\,j\neq i}\pi(\{i,j\}).$$

On remarque que l'expression ci-dessus peut encore contenir l'arête $\{2,3\}$, qu'il faut donc éliminer. Pour cela, nous utilisons le vecteur suivant de l'orthogonal de Réguliers$_n^k$:

$$\sum_{i>1}\text{Etoile}(\{i\})-\text{Etoile}(\{1\})=2\sum_{2\le i<j\le n}\{i,j\}.$$

On a :

$$\begin{aligned}\pi(\{2,3\}) &= \pi(\{2,3\} - \frac{1}{2}\left(\sum_{2\leq i}\text{Etoile}(\{i\}) - \text{Etoile}(\{1\})\right)\\ &= -\sum_{2\leq i<j\leq n,\,\{i,j\}\neq\{2,3\}}\pi(\{i,j\}) \quad \square\end{aligned}$$

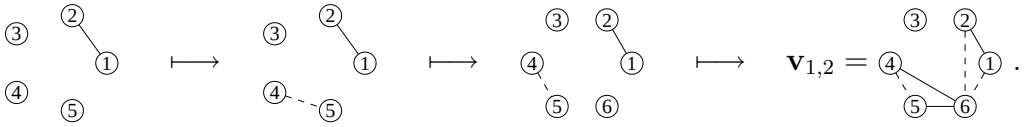
4.4 Base de régularisation

Pour l'espace Réguliers_n^2, on peut définir une autre base. Elle est très fortement liée à l'isomorphisme entre les graphes sur $n-1$ sommets et les graphes réguliers sur n sommets que nous verrons plus en détail au § 5.4.2. Lorsque nous avons eu besoin d'une base des graphes 0-réguliers pour faire des calculs sur les polynômes invariants, nous avons souvent utilisé celle-ci, car elle est la plus simple à manipuler. De fait, c'est celle qui s'est avérée la plus efficace pour les calculs de bases de Gröbner, par exemple pour chercher des systèmes de paramètres (voir § 11.3.1).

On définit pour toute paire $\{i,j\}$ telle que $1 \leq i < j \leq n-1$, $\{i,j\} \neq \{n-1,n-2\}$ le vecteur $\mathbf{v}_{i,j}$ de Réguliers_n^2 :

$$\mathbf{v}_{i,j} := \{i,j\} - \{n,i\} - \{n,j\} - \{n-1,n-2\} + \{n,n-1\} + \{n,n-2\}.$$

Le principe est le suivant : on se sert de l'arête $\{n-1,n-2\}$ pour avoir un graphe sur $\{1,\ldots,n-1\}$ avec une somme des arêtes nulle, puis on se sert du sommet n pour régulariser :



Proposition 4.4.1.
Les $v_{i,j}$ forment une base de Réguliers_n^2*, que l'on appelle* base de régularisation.

Démonstration. Ils sont forcément linéairement indépendants puisque $v_{i,j}$ est le seul d'entre eux à contenir l'arête $\{i,j\}$ et il y en a le bon nombre. $\square$

4.5 Une nouvelle base

Avec Christian Delhommé, nous avons construit une nouvelle base de Réguliers_n^k. Il s'est avéré *a posteriori* que notre construction ressemble beaucoup à la construction classique donnée par la théorie des représentations de S_n. Notre base a la même forme générale, mais n'est pas exactement identique à celle classique.

Tout d'abord, elle sera probablement plus visuelle pour le lecteur familier avec la théorie des graphes. Ensuite notre démonstration, même si elle utilise le même type d'idées que la démonstration classique, a quelques originalités. D'une part, pour montrer que la matrice des vecteurs de la base est libre, nous travaillons sur ses lignes et non ses colonnes. D'autre part, nous avons été amenés à définir un

ordre partiel sur les mots de Dyck qu'il pourrait être intéressant d'approfondir. La note 4.5.4 présente quelques commentaires supplémentaires sur la comparaison de ces bases.

Nous allons commencer par donner un autre moyen de construire un k-hypergraphe 0-régulier en partant cette fois d'un couplage. Soit $E := \{1, \dots, n\}$, soit k avec $0 \leq 2k \leq n$, et $A \subset E$ avec $|A| = k$. Soit $A' = E \setminus A$. Les parties D à k éléments de E sont en bijection avec les couples (B, B') tels que $B \subset A$, $B' \subset A'$ et $|B| = |B'|$. En effet, les deux applications ϕ et ψ définies par :

$$\phi(D) := (A \setminus (D \cap A), D \cap A') \qquad \text{et} \qquad \psi(B, B') := (A \setminus B) \cup B',$$

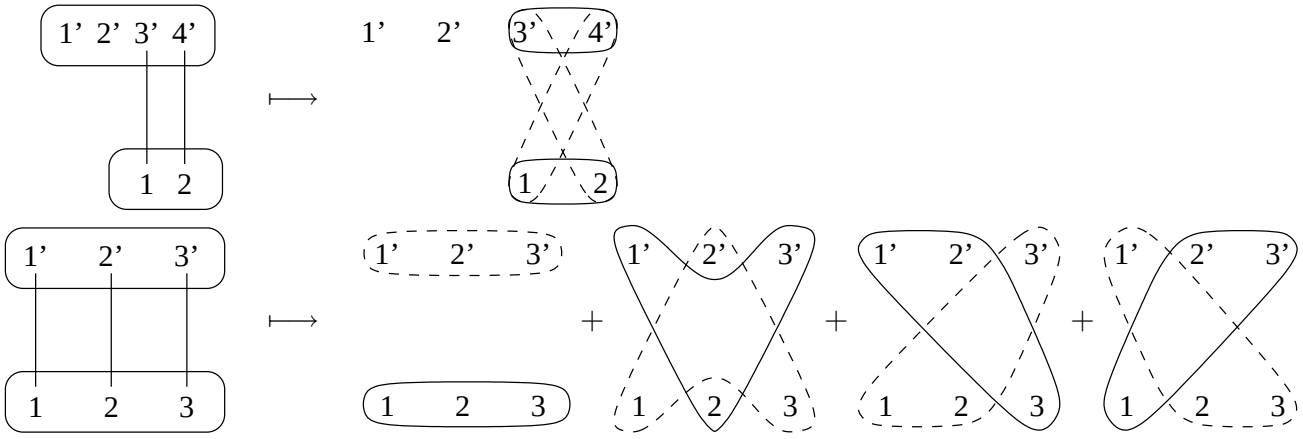
sont inverses l'une de l'autre. Pour chaque couple (B, B'), tels que $B \subset A$, $B' \subset A'$ et $|B| = |B'|$, soit $e_{B,B'}$ l'élément de V_n^k défini par

$$\mathbf{e}_{B,B'} := (-1)^{|B|}(A \setminus B) \cup B';$$

enfin soit $\mathcal{B}$ l'ensemble des $e_{B,B'}$. Les vecteurs $e_{B,B'}$ sont, à coefficient -1 près, les vecteurs de la base canonique de V_n^k. Ils forment donc une base de V_n^k.

Soit f une injection de A dans A', c'est-à-dire un couplage entre les éléments de A et certains éléments de A'. On pose $\mathbf{v}(f) := \sum_{B \subset A} \mathbf{e}_{B,f(B)}$. Ainsi, $\mathbf{v}(f) = \sum_{B \subset A}(-1)^{|B|}(A \setminus B) \cup f(B)$.

Exemples 4.5.1.
Voici quelques couplages et les vecteurs correspondants. Les parties en plein sont valuées 1*, celles en pointillés* -1 *et les autres* 0*.*

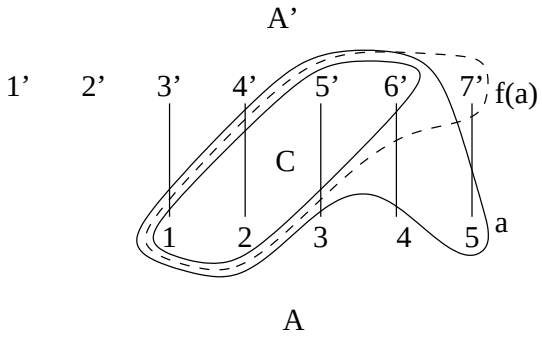


Lemme 4.5.2.
Le vecteur $\mathbf{v}(f)$ *est* 0*-régulier.*

Démonstration. Il faut montrer que pour toute partie C à $k-1$ éléments, la somme des coefficients des parties contenant C dans l'expression de $\mathbf{v}(f)$ est nulle.

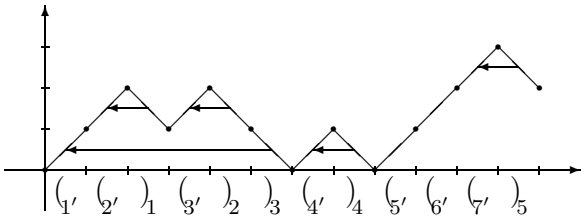
Remarque préliminaire : Soit $D := (A \setminus B) \cup B'$ une partie apparaissant dans l'expression de $\mathbf{v}(f)$. Pour tout a dans A, D contient soit a soit $f(a)$, mais pas les deux.

Soit donc C une partie à $k-1$ éléments. On suppose qu'elle contient $k-1-i$ éléments dans A, et i éléments dans A'. Si C contient à la fois a et $f(a)$ pour un certain a de A, alors aucune partie contenant C n'apparaîtra dans $\mathbf{v}(f)$. Sinon, il y a au plus un sommet a tel que C ne contienne ni a, ni $f(a)$. Les parties contenant C apparaissant dans $\mathbf{v}(f)$ sont donc $C \cup \{a\}$ et $C \cup \{f(a)\}$. La première est valuée $(-1)^i$ et la deuxième $(-1)^{i+1}$ ce qui donne bien une somme des coefficients nulle.

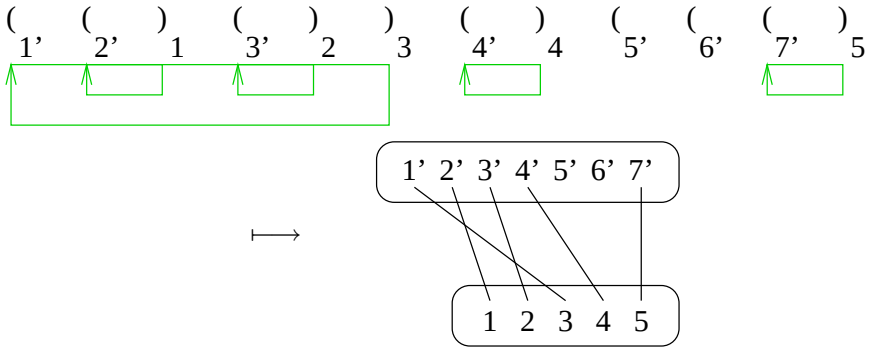


□

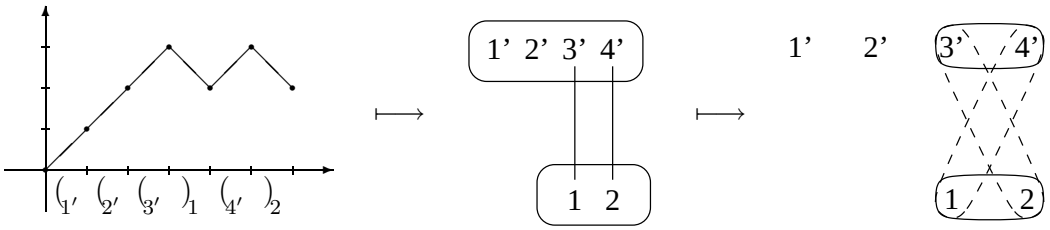
On peut associer à chaque mot $m \in \mathrm{Dyck}_n^k$ une injection de A dans A', et ce de manière univoque. Pour cela, on fixe une énumération des éléments de A et une énumération des éléments A'. Par commodité, nous supposerons que $A := \{1, \ldots, k\}$, et nous appellerons $\{1', \ldots, (n-k)'\}$ les éléments de A'. Soit $m \in \mathrm{Dyck}_n^l$. La propriété cruciale de m est que l'on peut associer une parenthèse ouvrante à chaque parenthèse fermante : il suffit de prendre la parenthèse qu'elle ferme !



Pour construire le couplage f_m entre $A := \{1, \ldots, k\}$ et $A' := \{1', \ldots, (n-k)'\}$, on numérote les parenthèses ouvrantes par $\{1', \ldots, (n-k)'\}$ de la gauche vers la droite, puis de même les parenthèses fermantes par $\{1, \ldots, k\}$. Enfin, on pose $f_m(i) := j'$ lorsque la parenthèse i ferme la parenthèse j'. Voilà ce que cela donne pour le mot précédent :



En rassemblant les deux constructions précédentes, nous obtenons à partir de chaque mot m de Dyck_n^k un couplage f_m, puis un vecteur $\mathbf{v}_m = v(f_m)$ de $\mathrm{Réguliers}_n^k$:



Nous avons alors le théorème :

Théorème 4.5.3 (Delhommé, Thiéry).
L'ensemble des $\mathbf{v}_m$ *avec* m *dans* Dyck_n^k *est une base de* $\mathrm{Réguliers}_n^k$.

On note que les vecteurs de cette base (et de la base classique) sont à coefficients entiers $\{-1, 1\}$. Cette famille est donc définie pour n'importe quel corps. Cependant, en caractéristique non nulle, elle peut n'être qu'une famille libre de l'espace $\mathrm{Réguliers}_n^k$.

Note 4.5.4 (pour les spécialistes de combinatoire): La construction du vecteur $\mathbf{v}_m$ est très proche de celle d'un polytabloïde (voir [Sag91]). La différence par rapport à la base classique réside dans le choix de ces polytabloïdes. Dans la construction classique, on prend directement le polytabloïde associé au tableau standard. Ici, nous partons du tableau standard et, via le mot de Dyck associé, on obtient un couplage. On peut considérer ce couplage comme un tableau en groupant les parenthèses associées par colonnes. Le vecteur que nous construisons est alors exactement le polytabloïde associé à ce tableau. (Il y aurait en fait le choix entre plusieurs tableaux, mais le polytabloïde final est de toute façon le même). Cette construction ne fonctionne que pour les représentations $[n-k, k]$. Pour $k = 0$ et $k = 1$, les deux bases coïncident.

Une propriété de cette base qui pourrait s'avérer utile est qu'il y a une partie A telle que chaque vecteur de cette base contient A avec un coefficient 1.

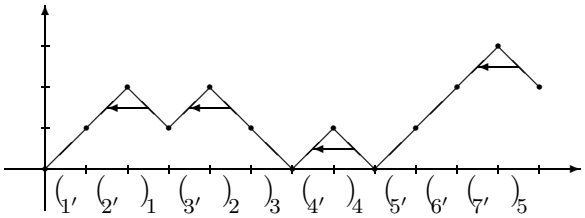
Démonstration du théorème. Fixons n et k. Comme le nombre de vecteurs est égal à la dimension, il suffit de vérifier qu'ils sont linéairement indépendants. Pour cela, prenons la matrice M des $\mathbf{v}_m$ dans la base $\mathcal{B}$ des vecteurs $\mathbf{e}_{B,B'}$. La matrice M a $\mathrm{C}_n^k - \mathrm{C}_n^{k-1}$ colonnes, C_n^k lignes et est composée de 0 et de 1. Nous allons montrer qu'à condition d'ordonner les mots m convenablement on peut, en extrayant certaines de ses lignes, obtenir une matrice triangulaire supérieure à coefficients 1 sur la diagonale.

Définition 4.5.5 (Ordre sur les mots).
On ordonne les mots de Dyck_n^k *lexicographiquement, en considérant que « (» est plus petit que «) ». Par exemple, le plus petit élément de* Dyck_8^4 *est «* ((()())) *» et le plus grand «* ()()()() *».*

Fixons un couple (B, B'). Le terme $\mathbf{e}_{B,B'}$ apparaît dans tous les $\mathbf{v}_m$ tels que $f_m(B) = (B')$. Intuitivement le couplage induit par m est « plus fin » que $B \mapsto B'$. Le principe de la démonstration va être d'exhiber pour chaque mot m un couple (B_m, B'_m) tel que m est le plus grand des mots m' vérifiant $f_{m'}(B_m) = B_m$.

Exemple 4.5.6.
Pour le mot « ((((())) », c'est simple. En effet, il s'agit du seul parenthésage pour lequel la première parenthèse fermante ferme la dernière parenthèse ouvrante. Le couple $(\{1\}, \{(n-k)'\})$ *impose exactement cette condition et donc convient.*

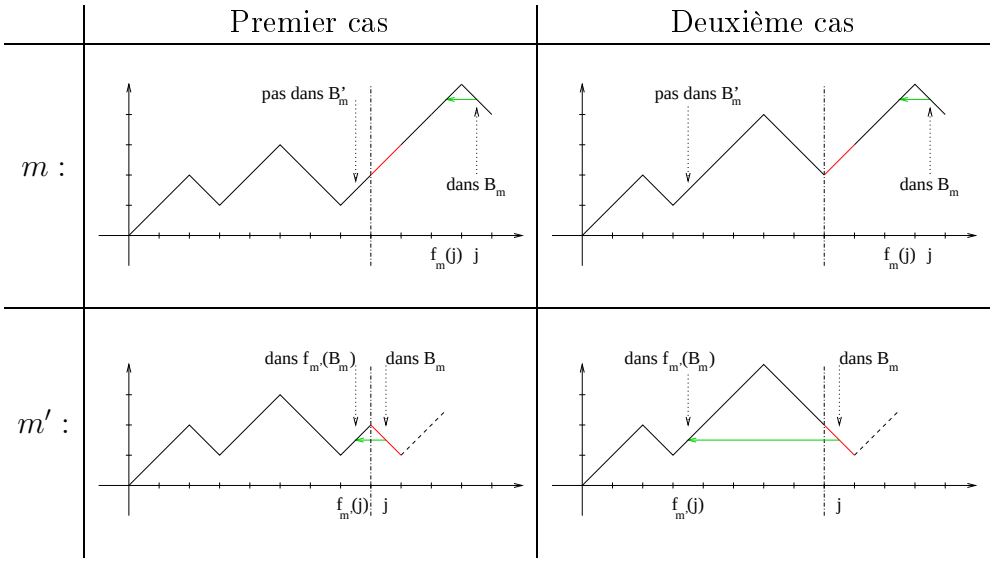
Après quelques essais avec MuPAD, nous avons constaté que la bonne idée est, comme dans l'exemple précédent, de se servir des pics. On note B_m l'ensemble des numéros des parenthèses fermantes immédiatement à droite d'un pic et B'_m l'ensemble des numéros des parenthèses ouvrantes correspondantes. On obtient par exemple $(\{2', 3', 4', 7'\}, \{1, 2, 4, 5\})$ pour le mot



Lemme 4.5.7.
Pour tous mots m *et* m', *si* $f_{m'}(B_m) = B'_m$ *alors* $m' \leq m$.

Démonstration. Soit m un mot, et $m' \neq m$ tel que $f_{m'}(B_m) = B'_m$. Soit i la première position telle que $m'_i \neq m_i$. Supposons que $m'_i > m_i$, *i.e.* $m'_i = ')'$ et $m_i = '('$. Soit j le numéro de la parenthèse fermante m'_i. Comme m et m' coïncident auparavant et étant donnée notre numérotation, cette parenthèse est située dans m un peu plus loin à droite, avec seulement des parenthèses ouvrantes entre-temps. En particulier, elle est au niveau d'un pic et fait donc partie de B_m. Nous allons montrer que $f_{m'}(j)$ n'est pas dans B'_m, ce qui sera contradictoire.

Il y a deux cas voisins illustrés ci-dessous. Dans les deux cas, $f_{m'}(j)$ n'est pas refermée immédiatement dans m. Ne faisant pas partie d'un pic, elle ne peut pas appartenir à B'_m.



Conclusion : $m'_i < m_i$ et donc m' est strictement plus petit lexicographiquement que m. □

Cela clôt la démonstration du théorème. Si on extrait de M les lignes correspondant aux couples (B_m, B'_m), on obtient une matrice T triangulaire supérieure à coefficient 0 ou 1 avec des 1 sur la diagonale. Donc M est de rang $|\operatorname{Dyck}_n^k|$ et les vecteurs $\mathbf{v}_m$ sont linéairement indépendants. □

Remarque 4.5.8: La matrice T obtenue s'inverse trivialement et on peut déduire de cette démonstration un algorithme (voire une formule) pour écrire tout hypergraphe 0-régulier sur cette base.

Remarque 4.5.9: Il y a visiblement un ordre partiel sous-jacent sur les préfixes de mots de Dyck. On pose $m \succ m'$ si $f_{m'}(B_m) = B'_m$. On obtient un graphe orienté acyclique puisque le lemme 4.5.7 indique précisément que l'ordre lexicographique en est une extension linéaire. Il ne reste donc plus qu'à en prendre la clôture transitive.

Il se trouve que l'existence d'une extension linéaire nous suffisait et nous n'avons donc pas exploré plus loin les propriétés de cet ordre partiel.

Sa matrice d'adjacence ressemble à T avec probablement des 1 de transitivité supplémentaires strictement au-dessus de la diagonale. La formule envisagée dans la remarque précédente est proche d'une inversion de Möbius.

4.6 Bases orthogonales/orthonormées

Les bases précédentes ne sont pas orthonormées. Nous verrons plus loin qu'en plus du point de vue purement esthétique, il serait utile d'avoir des bases de V_n^k orthogonales (ou mieux orthonormées) et qui respectent la décomposition. Nous allons donner, pour certains cas particuliers, des constructions *ad hoc* de telles bases.

4.6.1 Bases orthonormées de l'image de $\operatorname{Etoile}^{i\to k}$.

Nous allons d'abord regarder le cas particulier de l'espace $\operatorname{Im}\operatorname{Etoile}^{1\to 2}$. L'ensemble des étoiles $\mathbf{E}_i := \operatorname{Im}\operatorname{Etoile}^{1\to 2}(\{i\}) = \sum_j \mathbf{e}_{i,j}$ forme une base de ce sous-espace de V_n^2. Elle n'est pas orthonormée, mais on peut la modifier pour qu'elle le soit.

Proposition 4.6.1.
On peut choisir α et β réels tels que la famille suivante soit une base orthonormée :

$$(\mathbf{E}'_i = \alpha\mathbf{E}_i + \beta\mathbf{C})_i$$

La base duale forme alors une base orthonormée des formes linéaires.

On a 4 choix pour α et β, dont :

$$\alpha = 1/\sqrt{(n-2)},$$
$$\beta = -\frac{\sqrt{2}}{\sqrt{n-1}\sqrt{n-2}(\sqrt{n-2}+\sqrt{2}\sqrt{n-1})}.$$

Démonstration. Pour trouver α et β, il suffit de résoudre le système d'équations suivant :

$$\mathbf{E}'_i.\mathbf{E}'_i = 1 \qquad\qquad \mathbf{E}'_i.\mathbf{E}'_j = 0$$

or on a

$$\begin{aligned} \mathbf{E}_i.\mathbf{E}_i &= n-1, & \mathbf{E}_i.\mathbf{E}_j &= 1, \\ \mathbf{E}_i.\mathbf{C} &= n-1, & \mathbf{C}.\mathbf{C} &= \frac{n(n-1)}{2}. \end{aligned}$$

On obtient finalement comme système d'équations

$$\begin{aligned} (n-1)*\alpha^2 + 2\alpha\beta(n-1) + \beta^2 * \frac{n(n-1)}{2} &= 1, \\ \alpha^2 + 2\alpha\beta(n-1) + \beta^2 * \frac{n(n-1)}{2} &= 0. \end{aligned}$$

Ce système se triangularise immédiatement en deux équations de degré 2 à une inconnue

$$\begin{aligned} (n-2)*\alpha^2 &= 1, \\ \alpha^2 + 2\alpha\beta(n-1) + \beta^2 * \frac{n(n-1)}{2} &= 0. \end{aligned}$$

que l'on résout aisément. □

Il devrait être possible de généraliser cela à $\mathrm{Im}\,\mathrm{Etoile}^{k\to k+1}$, voire $\mathrm{Im}\,\mathrm{Etoile}^{i\to k}$ sous la forme

$$\mathbf{E}_A = \sum_{B\in\mathcal{P}_n^k} \alpha_{d(A,B)} B$$

avec $d(A,B)$ la distance entre A et B définie au § 3.2.2.

Conjecture 4.6.2.
On peut choisir convenablement les α_i de sorte que $\{\mathrm{Etoile}^{k\to k+1}(o(A)), A\in\mathcal{P}_n^k\}$ soit une base orthonormée de $\mathrm{Im}\,\mathrm{Etoile}^{k\to k+1}$.

Pour prouver cette conjecture, il doit suffire d'écrire le système d'équations, probablement triangulaire, comme dans le cas précédent.

4.6.2 Bases orthonormées des 0-réguliers

Commençons par le plus simple. $\mathrm{Réguliers}_n^0$ est de dimension 1 et a donc une base orthonormée triviale.

Nous allons maintenant donner des bases orthonormées de $\mathrm{Réguliers}_n^1$.

Première construction : posons pour $i\in\{2,\dots,n\}$:

$$\mathbf{g}_i := (a, b, \dots, b, c, b, \dots, b)$$

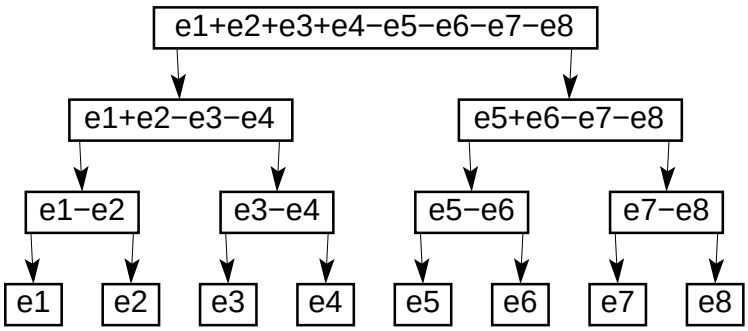
avec $a := 1$, $b := -\frac{\sqrt{n}+1}{n-1}$, $c := \frac{\sqrt{n}(n-2)-1}{n-1}$.

Théorème 4.6.3.
La famille $\{\mathbf{g}_i\}_{i\in\{2,\dots,n\}}$ *est une base orthogonale de* Réguliers$_n^1$, *tandis que la famille* $\{\frac{1}{\sqrt{n}}\mathbf{g}_i\}_{i\in\{2,\dots,n\}}$ *en est une base orthonormée.*

La démonstration est un simple calcul direct. L'inconvénient de cette base est qu'elle nécessite que $\sqrt{n}$ soit défini dans le corps. $\mathbb{R}$ conviendra, mais la plupart du temps $\mathbb{Q}$ ne conviendra pas.

Dans le cas où $n = 2^l$, on a une base élégante à coefficients ± 1. On la construit comme suit à partir de l'arbre binaire complet à n feuilles. On étiquette les feuilles par $\mathbf{e}_i$. Ensuite on étiquette les noeuds internes par la somme des étiquettes des feuilles en dessous à gauche moins la somme des étiquettes des feuilles en dessous à

droite. On pose B l'ensemble des étiquettes des noeuds internes.



Théorème 4.6.4.
B est une base orthogonale de Réguliers_n^1 *à coefficients entiers. Elle peut se normaliser sans problème sur* $\mathbb{R}$ *par exemple.*

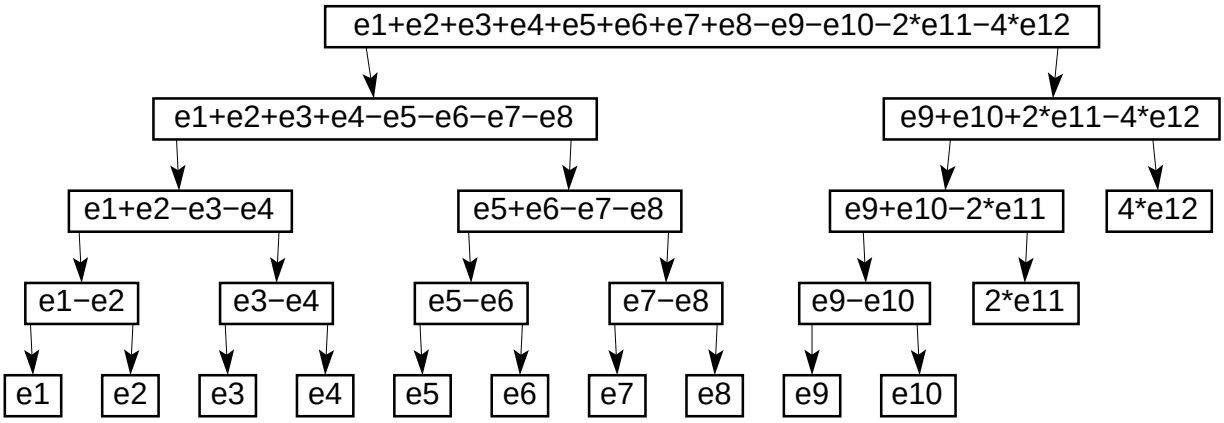
Démonstration. Soit n un noeud interne de l'arbre de niveau l. Il y a autant de feuilles en dessous à gauche qu'en dessous à droite. Le vecteur de la base correspondant est donc bien 0-régulier.

Soit n_1 et n_2 deux noeuds internes de l'arbre. S'ils n'ont aucune feuille en commun, il est clair qu'ils sont orthogonaux. Sinon, on peut supposer par exemple que n_1 est un descendant à gauche de n_2. Soient $\{g_j\}_j$ les étiquettes des feuilles à gauche de n_1 et $\{d_j\}_j$ les étiquettes des feuilles à droite de n_1.

$$\begin{aligned}\langle n_1|n_2\rangle &= \langle \sum g_j - \sum d_j | \sum g_j + \sum d_j + \ldots \rangle \\ &= \sum \langle g_j|g_j\rangle - \langle d_j|d_j\rangle = |\{g_j\}| - |\{d_j\}| = 0\end{aligned}$$

□

Nous ne savons pas si cela se généralise. Pour $2^n + 1$, par exemple, c'est possible en choisissant un coefficient convenable à la feuille surnuméraire. Mais le schéma tentant


e1+e2+e3+e4+e5+e6+e7+e8−e9−e10−2*e11−4*e12
e1+e2+e3+e4−e5−e6−e7−e8
e9+e10+2*e11−4*e12
e1+e2−e3−e4
e5+e6−e7−e8
e9+e10−2*e11
4*e12
e1−e2
e3−e4
e5−e6
e7−e8
e9−e10
2*e11
e1
e2
e3
e4
e5
e6
e7
e8
e9
e10

ne fonctionne pas. Les vecteurs $e9+e10-2*e11$ et $e9+e10+2*e11+4*e12$ sont bien réguliers, mais non orthogonaux.

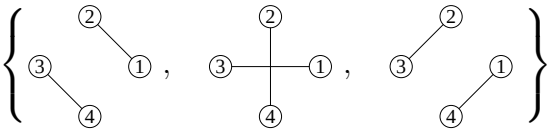
Pour $n=3$ et si l'on se place sur $\mathbb{C}$ avec $j=e^{\frac{i2\pi}{3}}$, il y a une autre base orthogonale :

$$\{\mathbf{e}_1+j.\mathbf{e}_2+j^2.\mathbf{e}_3, \mathbf{e}_1+j^2.\mathbf{e}_2+j.\mathbf{e}_3\}.$$

Enfin, nous allons donner pour $n=4,5$ des constructions *ad hoc* de bases orthonormées de Réguliers$_n^2$. Pour $n<4$, l'espace Réguliers$_n^2$ est réduit à $\{0\}$, et nous n'avons pas réussi à généraliser ces constructions pour $n>5$. Pour $n=4$, on peut adapter deux des idées des bases de Réguliers$_3^1$.

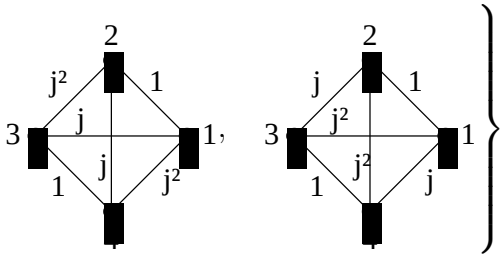
(i) L'ensemble

$$\{\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3\} := \left\{ \right. \quad , \quad , \quad \left. \right\} \tag{4.1}$$



est une base de l'espace des graphes réguliers. Si on se place sur $\mathbb{C}$, on peut construire la base orthonormée suivante de l'espace Réguliers$_4^2$ des graphes 0-réguliers :

$$\{\mathbf{g}_1+j.\mathbf{g}_2+j^2.\mathbf{g}_3, \mathbf{g}_1+j.\mathbf{g}_2+j^2.\mathbf{g}_3\} = \left\{ \right. \quad , \quad \left. \right\}$$



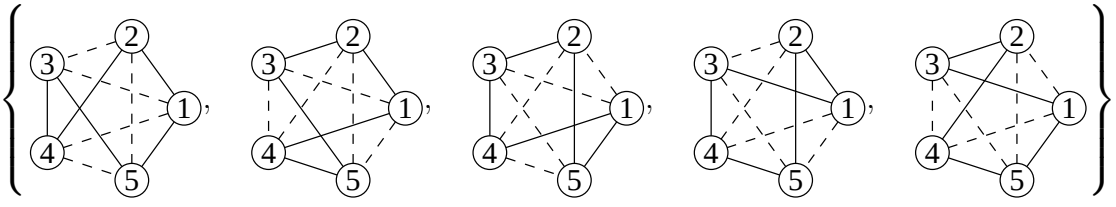
(ii) sans restriction sur le corps on peut prendre la base orthogonale

$$\{\mathbf{g}_1-\mathbf{g}_2, \mathbf{g}_1+\mathbf{g}_2-2*\mathbf{g}_3\}$$

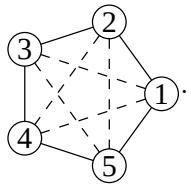
qui se normalise sans problème sur $\mathbb{R}$:

$$\{\frac{1}{\sqrt{2}}(\mathbf{g}_1-\mathbf{g}_2), \frac{1}{\sqrt{6}}(\mathbf{g}_1+\mathbf{g}_2-2*\mathbf{g}_3)\}$$

Pour $n=5$, on peut aussi construire une base orthogonale *ad hoc*, en utilisant l'existence de 12 cycles de longueur 5 qui se regroupent par paires. La dimension de Réguliers$_5^2$ est 5. On remarque alors que si l'on prend les 5 vecteurs $\{\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3,\mathbf{g}_4,\mathbf{g}_5\}$ qui correspondent aux 5 premières paires de cycles,



leur produit scalaire deux à deux est constant et vaut -2. La dernière paire de cycles nous donne un vecteur supplémentaire qui joue un rôle symétrique par rapport à tous les autres.

$\mathbf{g}_0 =$ 

.

Ce vecteur nous permet de modifier légèrement les vecteurs $\{\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3, \mathbf{g}_4, \mathbf{g}_5\}$ de façon à obtenir une base orthonormée.

Proposition 4.6.5.
Il existe α et β réels tels que la famille suivante soit une base orthonormée :

$$(\mathbf{g}'_i = \alpha \mathbf{g}_i + \beta \mathbf{g}_0)_{i \in \{1,2,3,4,5\}}$$

On a en fait 4 choix :

$$\alpha = \pm \frac{1}{2\sqrt{3}} \qquad\qquad \beta = \alpha \frac{1}{1 \pm \sqrt{6}}.$$

Démonstration. Pour trouver α et β, il suffit de résoudre le système d'équations suivant :

$$\mathbf{g}'_i.\mathbf{g}'_i = 1, \qquad\qquad \mathbf{g}'_i.\mathbf{g}'_j = 0;$$

or on a :

$$\mathbf{g}_i.\mathbf{g}_i = 10, \qquad \mathbf{g}_i.\mathbf{g}_j = -2, \qquad \mathbf{g}_i.\mathbf{g}_0 = 2, \qquad \mathbf{g}_0.\mathbf{g}_0 = 10.$$

On obtient finalement comme système d'équations :

$$10 * \alpha^2 + 4\alpha\beta + 10\beta^2 = 1, \qquad -2 * \alpha^2 + 4\alpha\beta + 10\beta^2 = 0,$$

qui se triangularise immédiatement en deux équations à une inconnue de degré deux et d'où l'on tire les solutions indiquées dans l'énoncé. □

Chapitre 5

Applications aux graphes

5.1 Introduction

Dans ce chapitre, nous nous intéressons plus particulièrement à l'espace V_n^2, que nous interprétons comme l'ensemble des graphes non orientés valués sur $\mathbb{K}$. Ces graphes se décomposent en partie régulière et partie étoilée. Nous donnons les formules de projections permettant de calculer ces deux parties. Deux graphes ont même liste de degrés si, et seulement si, ils ont la même partie étoilée. Nous étudions plus précisément la décomposition des graphes valués dans $\mathbb{Z}$, et nous montrons qu'un graphe simple est essentiellement déterminé à l'isomorphie près par sa partie régulière et la liste de ses degrés. Enfin, nous caractérisons les extensions de V_{n-1}^2 dans V_n^2 qui préservent les symétries.

5.2 Espace vectoriel des graphes

On peut identifier un vecteur $\mathbf{v}$ de l'espace V_n^2 avec le graphe valué tel que la valuation de l'arête $\{i,j\}$ est le coefficient de la partie $\{i,j\}$ dans $\mathbf{v}$. On note $x_{\{i,j\}}$ la forme linéaire telle que $x_{\{i,j\}}(\mathbf{g})$ est la valuation de l'arête $\{i,j\}$ de $\mathbf{g}$. On appelle *degré* de $\mathbf{g}$ au sommet i la somme $d_i(\mathbf{g}) := \sum_{j\neq i} x_{\{i,j\}}(\mathbf{g})$ des valuations des arêtes de $\mathbf{g}$ adjacentes au sommet i. Un graphe $\mathbf{g}$ est dit *simple* si les valuations sont soit 0 (absence d'arête), soit 1 (une arête). Il est appelé *multigraphe* si ses valuations sont dans $\mathbb{N}$. Sauf indication du contraire, les graphes considérés ici sont tous valués.

On note que le vecteur $\mathbf{E}_i := \mathrm{Etoile}^{1\to 2}\{i\}$ est l'étoile centrée sur i, et que le vecteur $\mathbf{C} := \mathrm{Etoile}^{0\to 2}\,\emptyset$ est le graphe complet. On appelle *espace des étoiles* le sous-espace engendré par les étoiles, c'est-à-dire $\mathrm{Im}\,\mathrm{Etoile}^{1\to 2}$. Un graphe de ce sous-espace est dit *étoilé*. Réciproquement un graphe est dit 0-*régulier* s'il est dans le noyau $\mathrm{Réguliers}_n^2$ de l'opérateur $\mathrm{Div}^{2\to 1}$. Cela revient à dire que les degrés de ses sommets sont tous nuls. L'espace des étoiles et l'espace des graphes 0-réguliers sont en somme directe orthogonale.

Proposition 5.2.1.
Soit $\mathbf{g}$ *un graphe* 0*-régulier non nul. Alors la collection* $\{\sigma.g, \sigma \in \mathfrak{S}_n\}$ *des graphes de son orbite engendre tout l'espace des graphes* 0*-réguliers.*
Un graphe $\mathbf{g}$ *non étoilé et non* 0*-régulier engendre, avec les éléments de son orbite, tout l'espace* V_n^2*.*

Démonstration. Le sous-espace engendré par l'orbite de $\mathbf{g}$ est un sous-module de Réguliers_n^2. Comme ce dernier est irréductible, il y a forcément égalité entre ces deux espaces. On procède de même dans le deuxième cas. □

On note respectivement $\pi_{\text{étoiles}}$ et $\pi_{\text{0-réguliers}}$ les projections orthogonales de V_n^2 sur l'espace des étoiles et l'espace des 0-réguliers. Étant donné un graphe $\mathbf{g}$, on appelle respectivement *partie étoilée* et *partie régulière* de $\mathbf{g}$ ses projetés $\mathbf{g}_{\text{et}} := \pi_{\text{étoiles}}(\mathbf{g})$ et $\mathbf{g}_{\text{reg}} := \pi_{\text{0-réguliers}}(\mathbf{g})$.

5.3 Formules de projection

Les formules suivantes permettent des calculs informatiques et seront cruciales au § 5.5. On en déduit que *la partie étoilée d'un graphe* $\mathbf{g}$ *est entièrement déterminée par la liste des degrés* d_i *de ses sommets*. La réciproque est claire, puisque $d_i(\mathbf{g}) = d_i(\mathbf{g}_{\text{et}})$.

Proposition 5.3.1 (Formules de projections).
Soit $\mathbf{g}$ *un graphe, et soit* $d_i := d_i(\mathbf{g})$ *le degré de* $\mathbf{g}$ *au sommet* i. *On a :*

$$x_{\{i,j\}}(\mathbf{g}_{et}) = \frac{d_i + d_j}{n-2} - \frac{\sum d_k}{(n-1)(n-2)};$$
$$x_{\{i,j\}}(\mathbf{g}_{reg}) = x_{\{i,j\}}(\mathbf{g}) - \frac{d_i + d_j}{n-2} + \frac{\sum d_k}{(n-1)(n-2)}.$$

On note que $\sum d_k$ vaut deux fois la somme des valuations de toutes les arêtes du graphe $\mathbf{g}$.

Démonstration. Soient $\mathbf{h}_{\text{et}}$ et $\mathbf{h}_{\text{reg}}$ tels que :

$$x_{\{i,j\}}(\mathbf{h}_{\text{et}}) := \frac{d_i + d_j}{n-2} - \frac{\sum d_k}{(n-1)(n-2)},$$
$$x_{\{i,j\}}(\mathbf{h}_{\text{reg}}) := x_{\{i,j\}}(\mathbf{g}) - \frac{d_i + d_j}{n-2} + \frac{\sum d_k}{(n-1)(n-2)}.$$

Clairement $\mathbf{g} = \mathbf{h}_{\text{et}} + \mathbf{h}_{\text{reg}}$ et $\mathbf{h}_{\text{et}}$ est étoilé puisque

$$\mathbf{h}_{\text{et}} = \sum_{i=1}^{n} \frac{d_i}{n-2}\mathbf{E}_i - \frac{\sum d_k}{(n-1)(n-2)}\mathbf{C}.$$

Il suffit donc de vérifier que $\mathbf{h}_{\text{reg}}$ est 0-régulier. Or, pour chaque sommet i :

$$\begin{aligned} d_i(\mathbf{h}_{\text{reg}}) &= \sum_{j,\, j\neq i} x_{\{i,j\}}(\mathbf{h}_{\text{reg}}) \\ &= \sum_{j,\, j\neq i} x_{\{i,j\}}(\mathbf{g}) - (n-1)\frac{d_i}{n-2} + \sum_{j,\, j\neq i} \frac{d_j}{n-2} + (n-1)\frac{\sum d_k}{(n-1)(n-2)} \\ &= d_i - (n-1)\frac{d_i}{n-2} - \sum_{j,\, j\neq i} \frac{d_j}{n-2} + \sum \frac{d_k}{(n-2)} = 0. \quad \square \end{aligned}$$

5.4 Extensions de graphes

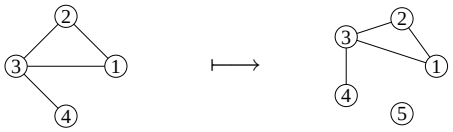
Nous avons vu comment on peut utiliser l'opérateur Etoile pour plonger des hypergraphes dans des hypergraphes dont les arêtes sont de plus en plus grandes, et nous avons remarqué que ces plongements respectaient les symétries.

Ici, nous cherchons comment on peut étendre un graphe $\mathbf{g}$ sur $n-1$ sommets en un graphe sur n sommets. Cela définit un plongement ϕ de V^2_{n-1} dans V^2_n. Nous voulons de plus que ce plongement préserve les symétries, c'est-à-dire que si l'on permute les sommets de $\mathbf{g}$, les $n-1$ premiers sommets de son extension sont permutés de la même façon. Ainsi, deux graphes isomorphes ont des extensions isomorphes.

Formellement, $\mathfrak{S}_{n-1}$ agit sur V^2_n par restriction de l'action de $\mathfrak{S}_n$ (on ne permute que les $n-1$ premiers sommets). Nous cherchons donc les $\mathfrak{S}_{n-1}$-morphismes ϕ de V^2_{n-1} dans V^2_n qui préservent les arêtes entre les $n-1$ premiers sommets. Nous appelons *extensions* ces morphismes. Nous en donnons deux naturelles. Puis, en nous servant d'un tout petit peu de théorie, nous les cherchons systématiquement. Nous constatons alors qu'elles s'expriment toutes en fonction des deux premières, et d'une troisième sans grand intérêt.

5.4.1 Extension simple

L'extension la plus simple consiste à rajouter un sommet isolé au graphe !

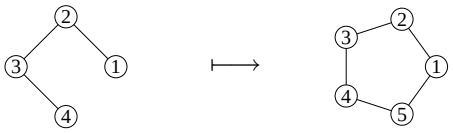


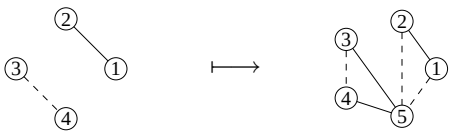
Formellement, elle correspond au plongement canonique de V^2_{n-1} dans V^2_n. Cette extension permet de considérer indifféremment un graphe à n sommets comme graphe sur $m \geq n$ sommets. On peut l'utiliser pour définir la notion d'isomorphie indépendamment de n.

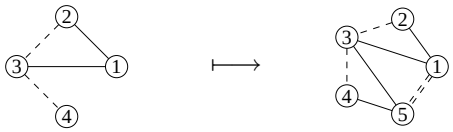
Bien entendu, cette extension se généralise au cas des hypergraphes.

5.4.2 Extension régulière

L'idée pour construire la deuxième extension est la même que celle que nous avons utilisée pour construire la base de régularisation au § 4.4. On se sert du sommet supplémentaire pour rendre le graphe régulier comme dans les exemples suivants.







Pour cela, on recherche les valuations α_i à mettre sur les arêtes $\{i, n\}$, de manière à ce que le graphe obtenu soit régulier. On obtient alors les équations

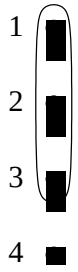
$$d = \sum d_i + \alpha_i$$
$$d = \sum \alpha_i$$

où d est le degré du graphe obtenu, et d_i le degré du sommet i dans le graphe de départ. Ces équations ont alors comme solution

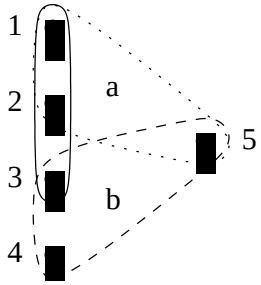
$$d = \frac{\sum d_i}{n-2}$$
$$\alpha_i = d - d_i$$

On remarque que l'image d'un graphe pour lequel la somme des valuations est nulle est un graphe 0-régulier. Enfin, on note qu'il n'est pas possible de définir d'extension régulière pour les hypergraphes. Voici un exemple de problème rencontré.

Exemple 5.4.1.
Soit $\mathbf{h}$ *l'hypergraphe de* V_4^3 *à une arête* $\{1, 2, 3\}$.



Essayons de l'étendre en $\mathbf{h}'$ *en rajoutant un sommet* 5. *Par symétrie, les arêtes* $\{1, 2, 5\}$, $\{1, 3, 5\}$ *et* $\{2, 3, 5\}$ *ont même coefficient* a. *De même, les arêtes* $\{1, 4, 5\}$, $\{2, 4, 5\}$ *et* $\{3, 4, 5\}$ *ont même coefficient* b.



Calculons les degrés de chaque paire dans $\mathbf{h}'$.

$$\{1,2\} : 1 + a \qquad \{3,4\} : b$$
$$\{1,5\} : 2a + b \qquad \{4,5\} : 3b$$

Il faut que ces degrés soient tous égaux. On en déduit successivement : $b = 0$, *le degré est* 0 *et* $a = 0$. *Mais alors le degré de* $\{1, 2\}$ *vaut* 1, *ce qui est impossible.*

5.4.3 Recherche systématique des extensions

Nous allons décomposer, dans le cas général, l'espace V_n^k en sous-modules irréductibles pour l'action du groupe symétrique $\mathfrak{S}_{n-1}$ sur les $n-1$ premiers sommets. L'espace V_n^k se décompose déjà en deux sous-modules, car on peut séparer les parties selon qu'elles contiennent n ou pas (triangle de Pascal). Soit U le sous-espace engendré par les arêtes ne contenant pas n. Il est isomorphe à V_{n-1}^k. Soit W le sous-espace engendré par les arêtes contenant n. Il est isomorphe à V_{n-1}^{k-1}. On connaît la décomposition de U et W en $\mathfrak{S}_{n-1}$-modules irréductibles, et on en déduit la décomposition voulue de V_n^k.

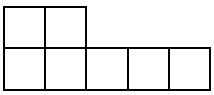
Théorème 5.4.2.
La décomposition de V_n en sous-modules irréductibles pour l'action de $\mathfrak{S}_{n-1}$ est donnée par :

$$\begin{aligned} V_n^k &= U \oplus^\perp W \\ &\cong_{\mathfrak{S}_{n-1}} \quad ([n-1] \oplus^\perp [n-2,1] \oplus^\perp \ldots \oplus^\perp [n-1-k,k]) \\ &\qquad \oplus^\perp ([n-1] \oplus^\perp [n-2,1] \oplus^\perp \ldots \oplus^\perp [n-k,k-1]). \end{aligned}$$

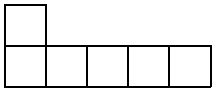
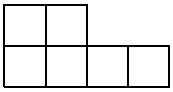
Nous vérifions que ce résultat est en accord avec la règle de branchement. Pour un énoncé précis et la démonstration de cette règle, nous renvoyons à [Sag91, 2.8 The Branching Rule, p.76].

Théorème 5.4.3 (Branching Rule).
Soit S^λ une représentation irréductible de $\mathfrak{S}_n$ paramétrée par le diagramme λ. La restriction de S^λ à $\mathfrak{S}_{n-1}$ est isomorphe à la somme directe des S^{λ^-} où les λ^- sont les diagrammes de $n-1$ obtenus en enlevant un coin interne de λ.

Par exemple, si l'on considère le diagramme

$\lambda = [5,2] =$  ,

alors les λ^- sont

$[5,1] =$  et $[4,2] =$  .

$S^{[5,2]}$ restreint à $\mathfrak{S}_6$ sera donc isomorphe à $S^{[5,1]} \oplus^\perp S^{[4,2]}$. D'après le théorème 3.1.1, la décomposition de l'espace V_n^k en $\mathfrak{S}_n$-modules irréductibles est :

$$V_n^k \cong_{\mathfrak{S}_n} [n] \oplus^\perp [n-1,1] \oplus^\perp \ldots \oplus^\perp [n-k,k].$$

En appliquant la règle 5.4.3, chaque $[n-i,i]$ se décompose sous l'action de $\mathfrak{S}_{n-1}$ en $[n-i-1,i] \oplus^\perp [n-i,i-1]$ tandis que $[n]$ se transforme en $[n-1]$. La décomposition finale est alors bien en accord avec le théorème 5.4.2.

En revenant au cas des graphes, cette décomposition permet de caractériser complètement les extensions.

Proposition 5.4.4.
Soit ϕ une extension. Elle se décompose en $\phi = \phi_U + \phi_W$, où ϕ_U est l'extension simple, et ϕ_W est de la forme :

$$\phi_W = \alpha \sum_i d_i^* \{i, n\} + \beta \left(\sum_i d_i^* \right) \left(\sum_i \{i, n\} \right),$$

où d_i^* est la fonction degré du sommet i.

L'extension simple correspond au cas $\alpha = \beta = 0$. L'extension régulière correspond au cas $\alpha = -1$, $\beta = \frac{1}{n-2}$. Enfin, si $\alpha = 0$ et $\beta = -\frac{1}{2(n-1)}$, on obtient une troisième extension qui transforme un graphe $\mathbf{g}$ sur $n-1$ sommets en graphe sur n sommets dont la somme des valuations est nulle, en rajoutant toutes les arêtes $\{i, n\}$ avec la même valuation. Toutes les autres extensions sont des combinaisons linéaires de ces trois là.

Démonstration. Pour que ϕ soit une extension, il faut qu'elle ne modifie pas les arêtes sur $\{1, \ldots, n-1\}$, autrement dit que ϕ_U soit l'extension simple. D'autre part, ϕ_W doit être un morphisme de $[n-1] \oplus [n-2, 1] \oplus [n-3, 2]$ vers $[n-1] \oplus [n-2, 1]$. D'après le lemme de Schur, les composantes sont envoyées homothétiquement les unes sur les autres. Par exemple, ϕ_W sera nulle sur les graphes 0-réguliers (pas de composante $[n-3, 2]$ dans W). On en déduit la forme voulue. □

5.5 Décomposition des graphes

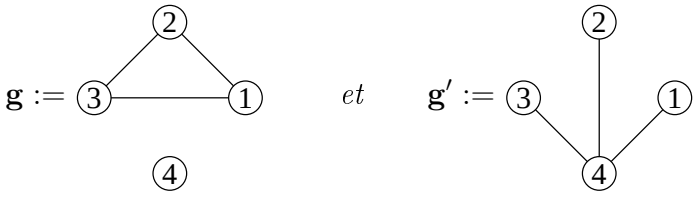
5.5.1 Décomposition des graphes simples

La motivation de l'étude qui va suivre est la suivante : suffit-il de connaître les parties régulière et étoilée d'un graphe pour connaître le graphe lui-même à l'isomorphie près ? Pour un graphe valué quelconque, la réponse est *a priori* non. En effet, étant donné un graphe $\mathbf{g} := \mathbf{g}_{\text{reg}} + \mathbf{g}_{\text{et}}$, et une permutation σ, le graphe $\mathbf{g}_{\text{reg}} + \sigma.\mathbf{g}_{\text{et}}$ a les mêmes parties régulière et étoilée à isomorphie près et pourtant n'est pas forcément isomorphe à $\mathbf{g}$. Par contre, pour un graphe simple, les valuations 0 ou 1 imposent des contraintes très fortes sur le recollement des deux parties.

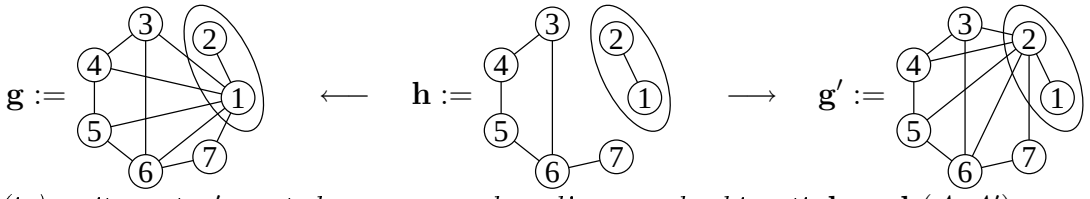
Théorème 5.5.1.
Soient $\mathbf{g}$ et $\mathbf{g}'$ deux graphes simples ayant même partie régulière et même nombre d'arêtes. Alors,

(i) soit $\mathbf{g} = \mathbf{g}'$;

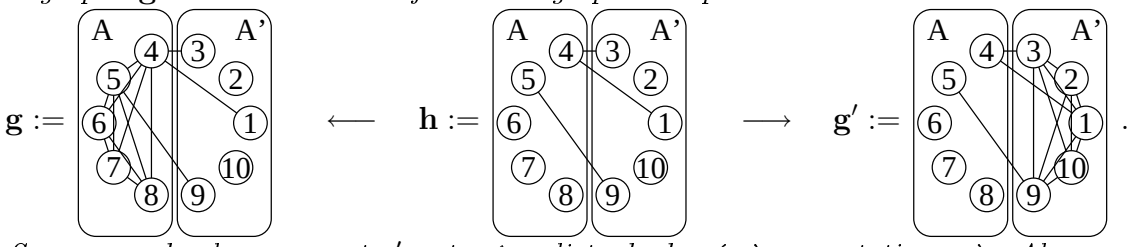
(ii) soit :



(iii) soit $\mathbf{g}$ *et* $\mathbf{g}'$ *sont deux sur-graphes d'un graphe* $\mathbf{h}$*, union disjointe d'un graphe sur deux sommets* $\{i, i'\}$ *et d'un graphe sur* $n-2$ *sommets* $X := \{1, \ldots, n\} - \{i, i'\}$ *; le graphe* $\mathbf{g}$ *étant obtenu en reliant le sommet* i *à tous les sommets de* X *et le graphe* $\mathbf{g}'$ *étant obtenu en reliant le sommet* i' *à tous les sommets de* X *:*



(iv) soit $\mathbf{g}$ *et* $\mathbf{g}'$ *sont deux sur-graphes d'un graphe biparti* $\mathbf{b} = \mathbf{b}(A, A')$ *avec* $|A| = |A'|$ *; le graphe* $\mathbf{g}$ *étant obtenu en ajoutant le graphe complet sur* A *et le graphe* $\mathbf{g}'$ *étant obtenu en ajoutant le graphe complet sur* A' *:*



Supposons de plus que $\mathbf{g}$ *et* $\mathbf{g}'$ *ont même liste de degrés à permutation près. Alors le cas (ii) est impossible et, dans le cas (iv), les degrés des sommets de* A *et de* A' *dans le graphe* $\mathbf{b}$ *sont identiques à permutation près.*

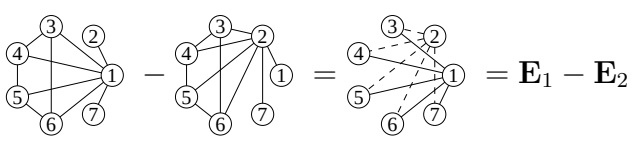
On remarque que, dans le cas (iii), $\mathbf{g}$ est isomorphe à $\mathbf{g}'$. En fait, deux graphes $\mathbf{g}$ et $\mathbf{g}'$ ayant même partie régulière et même liste de degrés ne peuvent être non-isomorphes que dans le cas (iv). Il est possible (mais non trivial !) de construire de tels graphes. Le plus petit contre-exemple que nous connaissons a une vingtaine de sommets.

Corollaire 5.5.2.
Si n *est impair, deux graphes ayant des parties régulières isomorphes et même nombre d'arêtes sont isomorphes.*

On note que, pour le problème de reconstruction comme pour de nombreux autres problèmes d'isomorphie, le nombre d'arêtes et la liste des degrés sont des informations faciles à obtenir. *Aux quelques rares exceptions près ci-dessus, il est équivalent de reconstruire la partie régulière d'un graphe* $\mathbf{g}$ *ou le graphe* $\mathbf{g}$ *lui-même.*

5.5.2 Décomposition des graphes valués dans $\mathbb{Z}$

Soient $\mathbf{g}$ et $\mathbf{g}'$ deux graphes simples. Ils ont même partie régulière si, et seulement si, leur différence $\mathbf{g} - \mathbf{g}'$ est un graphe étoilé. Cette différence est alors valuée dans $\{0, 1, -1\}$. Par exemple :



Pour démontrer le théorème 5.5.1, nous allons caractériser les graphes étoilés valués dans $\{0, 1, -1\}$ et, plus généralement, valués dans $\mathbb{Z}$.

Proposition 5.5.3.
Soit $\mathbf{g} := \sum \lambda_i \mathbf{E}_i$ *un graphe étoilé. Si* $n \geq 3$, *le graphe* $\mathbf{g}$ *est valué dans* $\mathbb{Z}$ *si, et seulement si,*

- *soit tous les coefficients* λ_i *sont entiers relatifs,*
- *soit tous les coefficients* λ_i *sont de la forme* $n_i + \frac{1}{2}$ *avec* n_i *entier relatif.*

Démonstration. La valuation de l'arête $\{i, j\}$ dans $\mathbf{g}$ est $\lambda_i + \lambda_j$. Il faut donc caractériser les $n-uplets$ de scalaires $(\lambda_1, \ldots, \lambda_n)$ tels que pour tout (i, j) $\lambda_i + \lambda_j \in \mathbb{Z}$. Pour $n = 2$, il n'y a qu'une seule arête, valuée par un entier. La décomposition en étoiles n'a plus de véritable sens, car elle n'est pas unique. Par exemple, $\mathbf{E}_1 = \mathbf{E}_2 = \lambda \mathbf{E}_1 + (1 - \lambda)\mathbf{E}_2$. Supposons $n \geq 3$. On a :

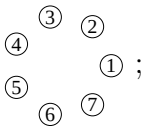
$$\lambda_1 + \lambda_2 \in \mathbb{Z}, \qquad \lambda_1 + \lambda_3 \in \mathbb{Z}, \qquad \lambda_2 + \lambda_3 \in \mathbb{Z},$$

d'où l'on déduit que $2\lambda_1 \in \mathbb{Z}$. Comme voulu, soit λ_1 est entier, soit il est de la forme $n_1 + \frac{1}{2}$. On aurait pu faire de même pour n'importe quel λ_i. Il ne reste plus qu'à vérifier qu'ils sont tous synchronisés. Si $\lambda_1 \in \mathbb{Z}$, comme $\lambda_1 + \lambda_i \in \mathbb{Z}$, alors $\lambda_i \in \mathbb{Z}$. De même si λ_1 est de la forme $n_1 + \frac{1}{2}$. □

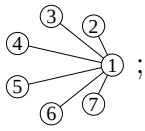
Nous obtenons alors la caractérisation recherchée des graphes étoilés valués dans $\{0, 1, -1\}$.

Théorème 5.5.4.
Un graphe $\mathbf{g}$ *est étoilé à valuation dans* $\{0, 1, -1\}$ *si, et seulement si, il vérifie l'une des conditions suivantes.*

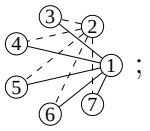
(i) $\mathbf{g}$ *est le graphe vide :*

$\mathbf{g} :=$  ;

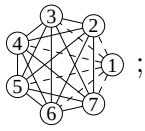
(ii) $\mathbf{g}$ *est une étoile* $\mathbf{E}_i$, *ou son opposé :*

$\mathbf{g} := \pm$  ;

(iii) $\mathbf{g}$ *est la différence de deux étoiles distinctes* $\mathbf{E}_i - \mathbf{E}_j$ *:*

$\mathbf{g} :=$  ;

(iv) $\mathbf{g}$ *est égal à* $\mathbf{C} - 2\mathbf{E}_i$ *ou* $2\mathbf{E}_i - \mathbf{C}$, *où* $\mathbf{C}$ *est le graphe complet :*

$\mathbf{g} := \pm$  ;

(v) $\mathbf{g}$ *est la réunion disjointe de deux graphes complets (éventuellement triviaux) ; les arêtes du premier sont toutes valuées* 1*, et les arêtes du second sont toutes valuées* -1 *:*

$$\mathbf{g} := \quad = \frac{1}{2}\left(\sum_{i\in A}\mathbf{E}_i - \sum_{i\in A'}\mathbf{E}_i\right),$$

où A *est l'ensemble des sommets du premier graphe complet, et* A' *l'ensemble des sommets du second.*

On note que le cas (v) contient les cas dégénérés du graphe complet, du graphe complet sur $n-1$ sommets et de leurs opposés :

$$\mathbf{g} := \pm \quad , \qquad\qquad \mathbf{g} := \pm \quad .$$

Démonstration. Par construction, si $\mathbf{g}$ vérifie l'une des conditions (i), (ii), (iii), (iv) ou (v), il est étoilé et valué dans $\{0, 1, -1\}$. Il faut vérifier la réciproque. Si $n = 2$, il n'y a qu'une seule arête, valuée par 0, 1 ou -1. Le graphe $\mathbf{g}$ est donc soit 0, soit le graphe complet, soit son opposé (conditions (i) ou (v)). Sinon, $n \geq 3$ et on peut appliquer la proposition 5.5.3 :

- Premier cas : tous les λ_i sont entiers.
  Supposons que, pour au moins un i, $\lambda_i \geq 2$. Comme $\lambda_i + \lambda_j \in \{0, 1, -1\}$ on a $\lambda_j \leq -1$. De même $\lambda_k \leq -1$. D'où $\lambda_j + \lambda_k \leq -2 < -1$, ce qui est contradictoire. Par symétrie, on élimine aussi la possibilité $\lambda_i \leq -2$.
  En conséquence, pour tout i, $\lambda_i \in \{0, 1, -1\}$. De plus, il est impossible que λ_i et λ_j soient simultanément égaux à 1. On a donc $|\{i, \lambda_i = 1\}| \leq 1$ et $|\{i, \lambda_i = -1\}| \leq 1$, les autres λ_j étant nuls. Le graphe $\mathbf{g}$ vérifie donc l'une des conditions (i), (ii) ou (iii) :

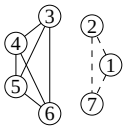
$$\mathbf{g} \in \left\{ \quad , \pm \quad , \quad \right\}.$$

- Second cas : les λ_i sont tous de la forme $n_i + \frac{1}{2}$.
  Si $\lambda_i > 1 + \frac{1}{2}$ alors $\lambda_j < -\frac{1}{2}$ et $\lambda_k < -\frac{1}{2}$ d'où $\lambda_i + \lambda_k < -1$, ce qui est contradictoire. De même, par symétrie si $\lambda_i < -1 - \frac{1}{2}$.
  Si $\lambda_i = 1 + \frac{1}{2}$ alors $\lambda_j \leq -\frac{1}{2}$ et $\lambda_k \leq -\frac{1}{2}$. Comme $\lambda_j + \lambda_k \geq -1$, on a $\lambda_j = -\frac{1}{2}$. De même que dans le cas symétrique lorsque $\lambda_i = -1 - \frac{1}{2}$, le graphe $\mathbf{g}$ vérifie alors la condition (iv) :

$$\mathbf{g} = \pm \quad .$$

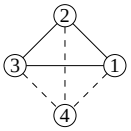
  Il ne reste plus que $\{+\frac{1}{2}, -\frac{1}{2}\}$ comme choix pour les λ_i. Séparons les sommets en V^+ où $\lambda_i = +\frac{1}{2}$ et V^- où $\lambda_i = -\frac{1}{2}$. Entre V^+ et V^- il n'y a pas d'arêtes,

puisque $\lambda_i + \lambda_j = 0$. Les arêtes valent 1 dans V^+ et symétriquement -1 dans V^-. Donc $\mathbf{g}$ vérifie la condition (v) :

$\mathbf{g} :=$  . $\square$

Nous avons maintenant tous les outils pour caractériser les graphes simples ayant même partie régulière.

Démonstration du théorème 5.5.1. Soient $\mathbf{g}$ et $\mathbf{g}'$ deux graphes simples ayant même partie régulière et même nombre d'arêtes. La somme des valuations des arêtes de $\mathbf{g} - \mathbf{g}'$ est zéro, et le théorème 5.5.4 indique que $\mathbf{g} - \mathbf{g}'$ vérifie les conditions (i), (ii) ou (v) avec $|A| = |A'|$. Si $n = 4$, le graphe $\mathbf{g} - \mathbf{g}'$ peut aussi vérifier la condition (iv) :

$\mathbf{g} - \mathbf{g}' :=$ 

De plus, si l'arête $\{i, j\}$ est valuée 1 dans $\mathbf{g} - \mathbf{g}'$, alors $\{i, j\}$ est une arête de $\mathbf{g}$ mais pas de $\mathbf{g}'$. Réciproquement si $\{i, j\}$ est valuée -1 dans $\mathbf{g} - \mathbf{g}'$, alors $\{i, j\}$ est une arête de $\mathbf{g}'$ mais pas de $\mathbf{g}$. Enfin, $\mathbf{g}$ et $\mathbf{g}'$ coïncident sur les autres arêtes. On en déduit les formes possibles de $\mathbf{g}$ et $\mathbf{g}'$.

Soient maintenant $\mathbf{g}$ et $\mathbf{g}'$ deux graphes dans la situation (v) et ayant même liste de degrés. Il faut vérifier que, dans le graphe $\mathbf{b}$, il y a autant de sommets de degré d dans A et dans A' (d variant de 0 à $\frac{n}{2}\}$, puisque $\mathbf{b}$ est biparti et $|A| = |A'|$). On note respectivement $d(v)$ et $d'(v)$ le degré d'un sommet v dans $\mathbf{g}$ et dans g'. On remarque que, si $v \in A$, on a $d(v) = d'(v) + \frac{n}{2} - 1$, et $d'(v)$ est le degré de v dans $\mathbf{b}$; enfin $d'(v) \leq \frac{n}{2}$. De même, si $v \in A'$, on a $d'(v) = d(v) + \frac{n}{2} - 1$, et $d(v)$ est le degré de v dans $\mathbf{b}$; enfin $d(v) \leq \frac{n}{2}$.

Soit $d < \frac{n}{2} - 1$. En utilisant la remarque précédente, et le fait que $\mathbf{g}$ et $\mathbf{g}'$ ont même liste de degrés, on obtient :

$$|\{v \in A,\, d'(v) = d\}| = |\{v,\, d'(v) = d\}| = |\{v,\, d(v) = d\}| = |\{v \in A',\, d(v) = d\}|.$$

Soit maintenant $d := \frac{n}{2}$. On a :

$$\begin{aligned} |\{v \in A,\, d'(v) = \frac{n}{2}\}| &= |\{v \in A,\, d(v) = n - 1\}| = |\{v,\, d(v) = n - 1\}| \\ &= |\{v,\, d'(v) = n - 1\}| = |\{v \in A',\, d'(v) = n - 1\}| \\ &= |\{v \in A',\, d(v) = \frac{n}{2}\}|. \end{aligned}$$

Enfin, soit $d := \frac{n}{2} - 1$. On a :

$$|\{v \in A,\, d'(v) = \frac{n}{2} - 1\}| = |\{v,\, d'(v) = \frac{n}{2} - 1\}| - |\{v \in A',\, d'(v) = \frac{n}{2} - 1\}|.$$

Or, on a

$$\begin{aligned}|\{v \in A',\, d'(v) = \frac{n}{2} - 1\}| &= |\{v \in A',\, d(v) = 0\}| = |\{v,\, d(v) = 0\}| \\ &= |\{v,\, d'(v) = 0\}| = |\{v \in A,\, d(v) = \frac{n}{2} - 1\}| \\ |\{v,\, d'(v) = \frac{n}{2} - 1\}| &= |\{v,\, d(v) = \frac{n}{2} - 1\}|,\end{aligned}$$

et donc

$$\begin{aligned}|\{v \in A,\, d'(v) = \frac{n}{2} - 1\}| &= |\{v,\, d(v) = \frac{n}{2} - 1\}| - |\{v \in A,\, d(v) = \frac{n}{2} - 1\}| \\ &= |\{v \in A',\, d(v) = \frac{n}{2} - 1\}|.\end{aligned}$$

Dans les trois cas, on en déduit que, dans le graphe $\mathbf{b}$, il y a autant de sommets de degré d dans A que dans A'. □

On note que, même sans savoir que $\mathbf{g}$ et $\mathbf{g}'$ ont même nombre d'arêtes, la caractérisation de $\mathbf{g} - \mathbf{g}'$ par le théorème 5.5.4 donne des conditions assez fortes sur $\mathbf{g}$ et $\mathbf{g}'$.

Pour un graphe simple $\mathbf{g}$, il suffit de connaître la liste des degrés de ses sommets pour connaître son nombre d'arêtes, et donc la liste des valuations de ses arêtes. Ce n'est plus le cas pour un graphe valué quelconque. On peut donc se demander dans quelle mesure un graphe valué est déterminé à l'isomorphie près par la liste des valuations de ses arêtes, la liste des degrés de ses sommets et sa partie régulière.

Chapitre 6

Quotients de l'espace vectoriel des parties

6.1 Introduction

Soit G un groupe agissant sur $E := \{1, \ldots, n\}$, c'est-à-dire un sous-groupe du groupe symétrique $\mathfrak{S}_n$. L'action de G s'étend à l'ensemble $\mathcal{P}_n$ des parties de E. Étant donnée une partie A de E, on appelle *orbite de* A sous l'action de G l'ensemble $\overline{A} := \{\sigma.A,\, \sigma \in G\}$. Par exemple, si l'on prend pour E l'ensemble des paires de $\{1, \ldots, n\}$, les parties de E sont les graphes simples étiquetés. L'action du groupe symétrique sur les sommets se traduit par une action sur les arêtes. Une orbite correspond alors à un *graphe simple non-étiqueté* (ou *graphe simple à isomorphie près*).

On étend l'ordre d'inclusion des parties aux orbites comme suit. On dit qu'une orbite $\overline{A}$ est incluse dans une orbite $\overline{B}$ si l'un des représentants de $\overline{A}$ est inclus dans un des représentants de B. Par symétrie, on en déduit que pour tout représentant de $\overline{A}$ il existe un représentant de $\overline{B}$ le contenant, et réciproquement. L'ordre partiel obtenu est le *quotient du treillis booléen par le groupe* G. Nous rappelons quelques propriétés de cet ordre partiel que l'on peut obtenir *via* l'algèbre linéaire et le théorème de Kantor.

6.2 Espace vectoriel des orbites

Soient A et A' deux parties de E. Ces parties A et A' sont *isomorphes* (noté $A \approx A'$) si elles sont dans la même orbite. On note $\operatorname{Aut} A := \{\sigma \in G,\, \sigma.A = A\}$ le *groupe d'automorphismes* de A. Si A et B sont deux parties de E, on note $s(A, B)$ le nombre de sous-parties A' de B isomorphes à A, et $S(A, B)$ le nombre de sur-parties B' de A isomorphes à B. Bien entendu, l'orbite de A est incluse dans l'orbite de B si, et seulement si, $s(A, B) \neq 0$.

Proposition 6.2.1.
Les quantités $s(A, B)$ et $S(A, B)$ sont liées par la relation :

$$|\operatorname{Aut} A|\, s(A, B) = |\operatorname{Aut} B|\, S(A, B).$$

Démonstration.

$$\begin{aligned}|\operatorname{Aut} A|\, s(A,B) &= |\operatorname{Aut} A|\, |\{A',\, A' \subset A,\, A' \approx A\}| \\ &= |\operatorname{Aut} A| \sum_{A' \approx A} \chi_{A' \subset B} = \sum_{\sigma \in G} \chi_{\sigma.A \subset B} = \sum_{\sigma \in G} \chi_{A \subset \sigma.B} = |\operatorname{Aut} B| \sum_{B' \approx B} \chi_{A \subset B'} \\ &= |\operatorname{Aut} B|\, |\{B',\, A \subset B',\, B' \approx A\}| = |\operatorname{Aut} B|\, S(A,B)\end{aligned}$$

où, $\chi_{A \subset B}$ est la fonction caractéristique de $A \subset B$. □

Représentation linéaire de G sur V_n et invariants

L'action de G sur l'ensemble $\mathcal{P}_n$ des parties de E s'étend en une représentation linéaire de $\mathbf{g}$ dans l'espace V_n. Par exemple, si σ est dans G, on a :

$$\sigma.(\{1,3\} + 4\{2,5\}) = \{\sigma(1), \sigma(3)\} + 4\{\sigma(2), \sigma(5)\}.$$

On appelle *invariant* un vecteur $\mathbf{v}$ de V_n fixé par toute permutation σ de G (*i.e.* $\forall \sigma \in G$, $\sigma.\mathbf{v} = \mathbf{v}$). On appelle *sous-espace des invariants* le sous-espace V_n^G des vecteurs de V_n invariants par G. On rappelle que l'*opérateur de Reynolds* est l'application linéaire

$$\mathbf{v} \mapsto \mathbf{v}^* = \frac{1}{|G|} \sum_{\sigma \in G} \sigma.\mathbf{v}.$$

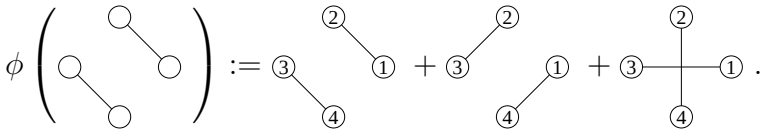
C'est une projection de V_n sur V_n^G.

Identification invariants/espace vectoriel des orbites

Soit A une partie de $\{1, \ldots, n\}$ et $\overline{A}$ son orbite sous l'action de G. On peut identifier cette orbite à un vecteur $\phi(\overline{A})$ de V_n^G :

$$\phi(\overline{A}) := \sum_{B \in \overline{A}} B.$$

Par exemple, dans le cas des graphes, on identifie un graphe non étiqueté et la somme formelle des graphes simples étiquetés le représentant :



Proposition 6.2.2.
Les vecteurs associés aux orbites des parties de $\{1, \ldots, n\}$ *forment une base de* V_n^G. *Autrement dit, le sous-espace des vecteurs invariants s'identifie à l'espace vectoriel engendré par les orbites.*

Démonstration. On vérifie d'abord que les vecteurs $\phi(\overline{A})$ sont indépendants. Soit $\sum \lambda_i \phi(\overline{A_i}) = 0$ une combinaison linéaire nulle d'orbites distinctes. La partie A_i apparaît dans le vecteur $\phi(\overline{A_i})$ et dans aucun des autres vecteurs $\phi(\overline{A_j}), j \neq i$. On en déduit, comme voulu, que tous les λ_i sont nuls.

Étant donné un vecteur $\mathbf{v} \in V_n$, on appelle *terme* de $\mathbf{v}$ une partie A telle que le coefficient de A dans $\mathbf{v}$ soit non-nul. Pour montrer que les vecteurs $\phi(\overline{A})$ engendrent

le sous-espace des invariants, on raisonne par récurrence sur le nombre de termes d'un vecteur invariant $\mathbf{v}$. Si $\mathbf{v}$ a zéro terme, $\mathbf{v} = 0$ et donc $\mathbf{v}$ est bien engendré. Sinon, soit A une des parties apparaissant dans l'expression de $\mathbf{v}$ et α le coefficient correspondant. Comme $\mathbf{v}$ est invariant, pour toute partie B de l'orbite de A, le coefficient de B dans $\mathbf{v}$ vaut aussi α. Soit alors $\mathbf{v}' = \mathbf{v} - \alpha \sum_{B \in \overline{A}} B$. Par construction, $\mathbf{v}'$ a strictement moins de termes que $\mathbf{v}$. On en déduit que $\mathbf{v}'$ et donc $\mathbf{v}$ sont engendrés. □

6.3 Opérateurs Div et Etoile

Comme précédemment, on traduit la structure d'ordre partiel par deux opérateurs linéaires adjoints. Comme les opérateurs Etoile et Div de V_n sont des morphismes pour l'action de G (lemme 3.1.2), l'image d'un vecteur invariant est un vecteur invariant. Ils définissent donc chacun un morphisme de V_n^G dans V_n^G, que l'on note respectivement Etoile et Div.

On appelle *matrice d'incidence des orbites à i éléments versus les orbites à k éléments* la matrice $\overline{M}$ de $\overline{\text{Etoile}}^{i \to k}$ dans la base des orbites. Soit de même $\overline{N}$ la matrice de $\overline{\text{Div}}^{k \to i}$ dans la base des orbites. On peut les décrire plus précisément. Soit A une partie à i éléments et B une partie à k éléments. Le coefficient de $\overline{M}$, sur la colonne correspondant à l'orbite de A et la ligne correspondant à l'orbite de B, est le nombre $s(A, B)$ de parties A' isomorphes à A et contenues dans B. Le coefficient de $\overline{N}$, sur la ligne correspondant à l'orbite de A et la colonne correspondant à l'orbite de B, est le nombre $S(A, B)$ de parties B' isomorphes à B et contenant A.

Les deux matrices $\overline{M}$ et $\overline{N}$ ne sont donc pas adjointes, mais vérifient cependant une certaine relation de dualité.

Proposition 6.3.1.
Soit X le vecteur colonne indexé par les orbites des parties de taille i défini comme suit : le coefficient correspondant à l'orbite $\overline{A}$ est la taille $|\operatorname{Aut} A|$ du groupe d'automorphismes de A. Soit Y le vecteur colonne indexé par les orbites des parties de taille k défini comme suit : le coefficient correspondant à l'orbite $\overline{B}$ est la taille $|\operatorname{Aut} B|$ du groupe d'automorphismes de B. On a alors :

$$\overline{M}X = {}^t(\overline{N}Y)$$

Démonstration. Les colonnes des deux matrices $\overline{M}X$ et ${}^t(\overline{N}Y)$ sont indexées par les parties A de taille i, et les lignes par les parties B de taille k. On vérifie que les coefficients de $\overline{M}X$ sont de la forme $|\operatorname{Aut} A|\, s(A, B)$, et ceux de ${}^t(\overline{N}Y)$ de la forme $|\operatorname{Aut} B|\, S(A, B)$. Enfin, on applique la proposition 6.2.1. □

Le théorème de Kantor se généralise à ces matrices.

Théorème 6.3.2.
- *Si $i \leq k \leq n - i$, l'opérateur $\overline{\text{Div}}^{k \to i}$ est surjectif et l'opérateur $\overline{\text{Div}}^{k \to i}$ est injectif ;*
- *Si $k \geq n - i$, l'opérateur $\overline{\text{Etoile}}^{i \to k}$ est surjectif et l'opérateur $\overline{\text{Div}}^{k \to i}$ est injectif.*

Démonstration. Supposons que $i \leq k \leq n-i$ et montrons que $\overline{\text{Div}}^{k\to i}$ est surjectif. Soit $\mathbf{v}$ un vecteur de V_n^i. D'après le théorème 2.2.15, l'opérateur $\text{Div}^{k\to i}$ est surjectif et il existe donc $\mathbf{w} \in V_n^k$ tel que $\text{Div}^{k\to i}\,\mathbf{w} = v$. Soit $\mathbf{w}^* = \frac{1}{|G|}\sum_{\sigma\in G}\sigma.\mathbf{w}$ le projeté de $\mathbf{w}$ sur V_n^{iG}. Comme $\text{Div}^{k\to i}$ est un morphisme, $\text{Div}^{k\to i}\,\mathbf{w}^* = (\text{Div}^{k\to i}\,\mathbf{w})^* = \mathbf{v}^* = \mathbf{v}$. Conclusion : $\mathbf{v}$ est dans l'image de $\overline{\text{Div}}^{k\to i}$.

Par dualité, l'opérateur $\overline{\text{Etoile}}^{i\to k}$ est injectif. Enfin, dans le cas $k \geq n-i$, on procède de même en montrant que l'opérateur $\overline{\text{Etoile}}^{i\to k}$ est surjectif. □

6.4 Applications

6.4.1 Théorème de Livingstone-Wagner

Théorème 6.4.1 ([LW65], [Rob67]).
Soit G un groupe agissant sur un ensemble fini E de taille n. Soit p_i le nombre d'orbites des parties de taille i de E. Ce nombre p_i croît jusqu'à $\frac{n}{2}$, puis décroît.

Démonstration. Soit i tel que $2i+1 \leq n$. Comme l'opérateur $\overline{\text{Etoile}}^{i\to i+1}$ est injectif, la dimension de V_n^{iG} est plus petite que celle de V_n^{iG}. Donc, comme voulu, $p_i \leq p_{i+1}$. □

On peut être plus précis : *à chaque orbite d'une partie X de taille i on peut associer, et ce de manière injective, l'orbite d'une partie Y contenant X et de taille $i+1$.* En effet, on peut extraire de la matrice de $\text{Etoile}^{i\to i+1}$ une matrice carrée $\overline{M}$ inversible en éliminant certaines colonnes. Le déterminant de $\overline{M}$ est non nul et donc au moins un des termes $\prod \overline{M}_{k,\sigma(k)}$ de son expansion est non nul. On en déduit que pour cette permutation σ tous les $\overline{M}_{k,\sigma(k)}$ sont non-nuls, autrement dit que, si l'on associe à l'orbite $\overline{A}$ correspondant à la ligne k l'orbite $\overline{B}$ correspondant à la ligne σk, alors $\overline{A}$ est inclus dans $\overline{B}$.

Rappelons qu'un ensemble ordonné a la *propriété de Sperner* si l'un de ses niveaux constitue une antichaîne de taille maximale. Avec l'observation ci-dessus, il vient :

Théorème 6.4.2 (Pouzet et Rosenberg [PR86]).
Le quotient de l'ensemble des parties d'un ensemble E par un groupe de permutation a la propriété de Sperner. Plus précisément, le niveau de hauteur $\lfloor\frac{|E|}{2}\rfloor$ est une antichaîne de taille maximale.

Ce résultat contient le fameux théorème de Sperner (prendre G réduit à l'identité). Il contient beaucoup plus. Étant donné un entier k, on dit qu'un ensemble ordonné P a la propriété de k-Sperner si la réunion de k niveaux est une k-antichaîne de taille maximum (une k-antichaîne est la réunion d'au plus k antichaînes). Enfin, on rappelle que P a la propriété de k-Sperner dès que le produit direct $P \times K$ où K est la chaîne à k éléments a la propriété de Sperner.

La collection des ordres quotients est stable par produit et contient les chaînes. (Si P est l'ensemble ordonné associé à G et P' l'ensemble ordonné associé à G' alors le produit cartésien $P \times P'$ est associé à $G \times G'$). On obtient ainsi :

Théorème 6.4.3 (Pouzet et Rosenberg [PR86]).
Le quotient de l'ensemble des parties d'un ensemble a la propriété de k-Sperner, pour tout k.

En prenant, comme ci-dessus, G réduit à l'identité on retrouve le théorème d'Erdös-De Bruijn.

6.4.2 Reconstruction par arêtes / Lovász

Stanley [Sta84] a utilisé la même approche pour donner une démonstration élémentaire du théorème de Lovász sur la reconstruction par arêtes. Soient E et G comme précédemment. Soit B une partie à k éléments. On appelle *jeu* de B l'ensemble des orbites $\overline{A}$, où A est une partie de taille $k-1$ incluse dans B. Ces orbites sont comptées avec multiplicités. La partie B est dite *reconstructible* si toute autre partie B' ayant même jeu est dans l'orbite de B.

Théorème 6.4.4 (Stanley [Sta84]).
Si $k > \frac{m}{2}$ alors toutes les parties à k éléments sont reconstructibles.

Démonstration. On peut représenter le jeu d'une partie B par le vecteur colonne dont chaque ligne, indexée par une orbite $\overline{A}$ de taille $k-1$ contient le nombre $S(A,B)$ d'éléments A' de l'orbite $\overline{A}$ qui sont inclus dans B. En prenant pour chaque orbite $\overline{B}$ le vecteur colonne correspondant, on obtient la matrice de $\mathrm{Div}^{k\to k-1}$. Si $k > \frac{m}{2}$, cet opérateur est injectif, ce qui implique que tous les vecteurs colonnes de la matrice sont linéairement indépendants et donc *a fortiori* distincts. Conclusion : chaque orbite $\overline{B}$ est caractérisée par son jeu. □

Si E est l'ensemble des paires de $\{i,\ldots,n\}$ et G le groupe symétrique $\mathfrak{S}_n$, une partie B de E peut être vue comme un graphe simple. Le fait que B soit reconstructible au sens ci-dessus, revient à dire qu'il est *reconstructible par arête*. Plus précisément, B et B' sont isomorphes dès qu'il existe une bijection σ des arêtes B sur celles de B' telle que pour toute arête e de B les graphes $B\setminus e$ et $B'\setminus\sigma(e)$ sont isomorphes.

Corollaire 6.4.5 (Lovász [Lov72]).
Tout graphe sur n sommets ayant strictement plus de $\frac{n(n-1)}{4}$ arêtes est reconstructible par arêtes.

6.5 Matrices d'incidence sur les forêts

On rappelle qu'une *forêt* est un graphe acyclique, et qu'un *arbre* est une forêt connexe. Au § 19, l'étude de la reconstructibilité algébrique des arbres soulève le problème suivant.

Problème 6.5.1.
Soit n un entier. Soit $\overline{M}$ la matrice d'incidence des graphes non étiquetés à $n-1$ arêtes versus les graphes non étiquetés à $n-2$ arêtes (c'est-à-dire la matrice de $\overline{\mathrm{Div}}^{n-1\to n-2}$). D'après le théorème 6.3.2, les lignes de cette matrice sont indépendantes. Soit $\overline{T}$ la sous-matrice obtenue par extraction des colonnes correspondant

aux arbres et des lignes correspondant aux forêts. Les lignes de cette matrice $\overline{T}$ sont-elles indépendantes ?

Au § 19.2.2, nous décrivons comment nous avons vérifié par calcul sur ordinateur que, jusqu'à $n = 13$, les lignes de $\overline{T}$ étaient indépendantes (matrice 1121×1302). Nous considérons ici le cas étiqueté. Soit T la matrice d'incidence des arbres étiquetés versus les forêts étiquetées à $n-2$ arêtes. Les lignes de T sont-elles indépendantes ? Si la réponse est oui, il s'ensuit immédiatement que les lignes de la matrice $\overline{T}$ sont aussi indépendantes. La réciproque n'est pas claire, et on risque donc d'étudier un problème plus difficile.

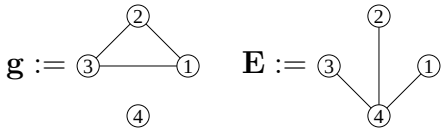
6.5.1 Petits cas

Proposition 6.5.2.
Lorsque le nombre de sommets n est inférieur à ou égal à 6, la matrice T est de rang plein.

Notons qu'un calcul sur ordinateur ne donne pas de meilleur résultat. En effet, le nombre d'arbres étiquetés croît très rapidement avec n (il y a n^{n-2} arbres étiquetés sur n sommets), et nous n'avons pu mener le calcul que jusqu'à $n = 6$ (matrice 1296×1080). Pour $n = 7$, il faudrait calculer le rang d'une matrice 16807×13377. La démonstration de cette proposition est basée sur le lemme suivant. Il utilise la construction de vecteurs 0-réguliers à partir de couplages que nous avons vue au § 4.5 (lemme 4.5.2).

Lemme 6.5.3.
Soit $\mathbf{g}$ un graphe à $n-1$ arêtes tel que chaque composante connexe non réduite à un sommet contienne un cycle. Le graphe $\mathbf{g}$ a au moins un sommet isolé et, en tant qu'élément de V_m^{n-1} ($m := \mathrm{C}_n^2$), s'écrit comme combinaison linéaire d'un vecteur 0-régulier $\mathbf{v}_f$ et de graphes ayant strictement moins de sommets isolés que $\mathbf{g}$.

Démonstration. Commençons par un exemple sur 4 sommets. Soit $\mathbf{g}$ le cycle sur les sommets $\{1, 2, 3\}$ et $\mathbf{E}$ l'étoile centrée sur le sommet 4 :

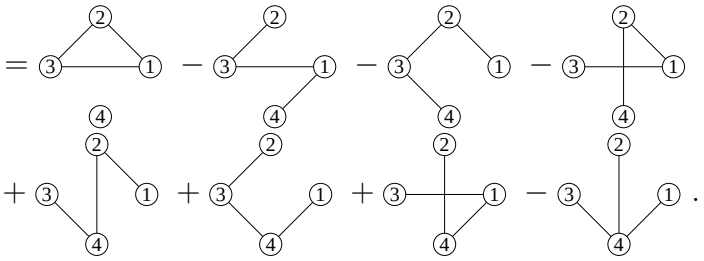


On considère le couplage f, entre l'ensemble A des arêtes de ce cycle et l'ensemble A' des arêtes de l'étoile, défini par :

$$f(\{1,2\}) := \{1,4\}, \quad f(\{2,3\}) := \{2,4\}, \quad f(\{3,1\}) := \{3,4\}.$$

Enfin, on construit le vecteur :

$$\mathbf{v}_f := \sum_{B \subset A} (-1)^{|B|} (A \setminus B) \cup f(B)$$



D'après le lemme 4.5.2, le vecteur $\mathbf{v}_f$ est dans le noyau de l'opérateur $\mathrm{Div}^{n-1 \to n-2}$. Nous avons construit ce couplage de sorte qu'il ait les deux propriétés suivantes :

(i) Pour chaque sommet v non isolé dans le cycle $\mathbf{g}$, il y a une arête e de $\mathbf{g}$ telle que e et $f(e)$ sont adjacentes à v.

(ii) Toutes les arêtes $f(e)$ sont adjacentes à un sommet isolé de $\mathbf{g}$.

Par exemple, le sommet 1 est adjacent à $\{1,3\}$ et à $f(\{1,3\}) = \{1,4\}$, et 4 est adjacent à $f(\{1,3\}) = \{1,4\}$. On en déduit que, en dehors du cycle $\mathbf{g}$ d'origine, aucun des graphes apparaissant dans l'expression $\mathbf{v}_f$ n'a de sommet isolé. Donc, comme voulu, on peut exprimer $\mathbf{g}$ comme combinaison linéaire du graphe 0-régulier $\mathbf{v}_f$ et de graphes avec au moins un sommet isolé en moins.

Soit maintenant $\mathbf{g}$ un graphe dont chaque composante connexe non triviale contient un cycle. On vérifie facilement que $\mathbf{g}$ a au moins un sommet isolé. Soit i un tel sommet et soit $\mathbf{E}$ l'étoile centrée en i. De même que dans l'exemple, nous allons construire un couplage f entre les arêtes de $\mathbf{g}$ et celles de l'étoile $\mathbf{E}$. Soit C une composante connexe non triviale de $\mathbf{g}$ et $(v_1, v_2, ..., v_k)$ un cycle de C. Pour v_1, on prend l'arête $\{v_1, v_2\}$ de $\mathbf{g}$ et on lui associe l'arête $f(\{v_1, v_2\}) := \{v_1, i\}$ de $\mathbf{E}$; on procède de même pour tous les sommets du cycle jusqu'à v_k pour lequel on prend l'arête $\{v_k, v_1\}$ de $\mathbf{g}$ et on lui associe l'arête $f(\{v_k, v_1\}) := \{v_k, i\}$ de $\mathbf{E}$. Ensuite, pour chaque sommet v de C à distance 1 du cycle, on prend une arête e qui relie v au cycle, et on lui associe l'arête $f(e) := \{v, i\}$ de $\mathbf{E}$. De même, pour chaque sommet à distance $d+1$ du cycle, on prend une arête e de $\mathbf{g}$ qui relie v à un sommet à distance d du cycle et on lui associe l'arête $f(e) := \{v, i\}$ de $\mathbf{E}$.

Enfin, on associe par un couplage quelconque les arêtes restantes de $\mathbf{E}$ aux arêtes restantes de $\mathbf{g}$. Par construction, le couplage f réalisé vérifie les propriétés (i) et (ii). Donc, en dehors de $\mathbf{g}$, tous les graphes apparaissant dans $\mathbf{v}_f$ ont au moins un sommet isolé en moins. En conclusion, $\mathbf{g}$ s'exprime comme combinaison linéaire du graphe 0-régulier $\mathbf{v}_f$ et de graphes avec au moins un sommet isolé en moins. □

Démonstration de la proposition 6.5.2. Soit n un entier. On considère la matrice M d'incidence entre les parties de taille $n-1$ (sur les colonnes) et les parties $n-2$ (sur les lignes). Soient respectivement l et c le nombre de lignes et de colonnes de M. Soit n_F le nombre de forêts à $n-2$ arêtes et n_A le nombre d'arbres.

On regroupe les colonnes correspondant aux arbres et celles aux graphes non-acycliques, ainsi que les lignes correspondant aux forêts et celles aux graphes non-acycliques. Comme les sous-graphes d'un arbre sont certainement des forêts, la ma-

trice M est de la forme :

$$M = \begin{bmatrix} T & * \\ 0 & * \end{bmatrix}$$

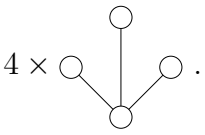
où T est la matrice d'incidence des arbres versus les forêts à $n-2$ arêtes qui nous intéresse. On note que, si $n \leq 3$, les matrices T et M sont égales, puisqu'il n'y a pas de graphes non-acycliques.

Il faut montrer qu'il y a n_F colonnes indépendantes dans T, ou de manière équivalente dans les colonnes de gauche de M. Comme la matrice M est de rang plein, on sait qu'il y a en tout l colonnes indépendantes dans M.

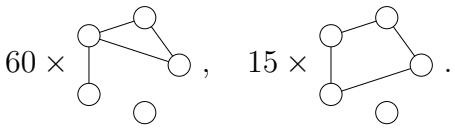
Soit $\mathbf{g}$ un graphe dans les conditions du lemme 6.5.3. Il s'exprime comme combinaison linéaire d'un vecteur $\mathbf{v}$ 0-régulier et de graphes avec un sommet isolé en moins. Cela se traduit par le fait que la colonne de M correspondant à $\mathbf{g}$ est une combinaison linéaire de colonnes de M correspondant à des graphes avec un sommet isolé en moins. En effet, $\mathbf{v}$ étant 0-régulier, il est dans le noyau de l'opérateur Div dont la matrice est précisément M. Donc la combinaison linéaire de colonnes correspondant à $\mathbf{v}$ est nulle.

On procède alors par récurrence descendante sur le nombre de sommets isolés pour retirer toutes les colonnes correspondant à des graphes dans les conditions du lemme 6.5.3. Chaque opération préserve le rang de la matrice, et la matrice finale est encore de rang l. Supposons que l'on ait ainsi enlevé k colonnes. Toutes ces colonnes ont été enlevées dans la partie droite de M, et il n'en reste donc que $c-n_A-k$. On en déduit qu'il y a au moins $l-(c-n_A-k) = l-c+n_A+k$ colonnes indépendantes dans la partie gauche, c'est-à-dire dans T. Autrement dit, si $k \geq (l-n_F)-(c-n_A)$, la matrice T est de rang plein. Lorsque $4 \leq n \leq 6$, cette condition est vérifiée.

Pour $n = 4$, on a : $c - n_A - (l - n_F) = (20 - 16) - (15 - 15) = 4$. Or, comme voulu, $k = 4$, car on peut retirer les colonnes des graphes suivants (nombre par type d'isomorphie) :

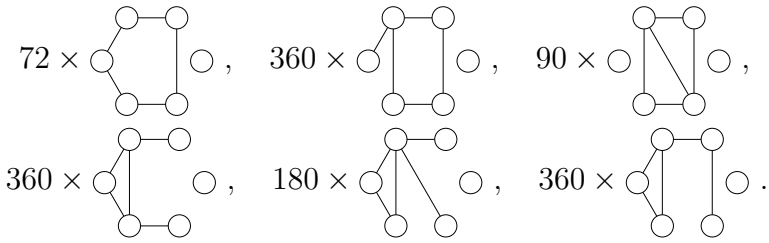


Pour $n = 5$, on a : $c - n_A - (l - n_F) = 210 - 125 - (120 - 110) = 75$. Or, comme voulu, $k = 75$, car on peut retirer les colonnes des graphes suivants (nombre par type d'isomorphie) :



Pour $n = 6$, on a : $c - n_A - (l - n_F) = 3003 - 1296 - (1365 - 1080) = 1422$. Or, comme voulu, $k = 1422$, car on peut retirer les colonnes des graphes suivants

(nombre par type d'isomorphie) :



Pour $n = 7$, on a $c - n_A - (l - n_F) = 54264 - 16807 - (20349 - 13377) = 30485$. Comme $k = 30030$, il faudrait encore retirer 455 colonnes. De même, pour $n = 8$ et $n = 9$, il faudrait encore retirer respectivement 28980 et 1393686 colonnes. □

6.5.2 Forêts avec un sommet isolé

Nous allons montrer que, lorsque n est impair une certaine sous-matrice de la matrice des arbres versus les forêts a des lignes indépendantes.

Théorème 6.5.4.
Soit T la matrice d'incidence des arbres étiquetés versus les forêts à $n-2$ arêtes avec un sommet isolé. Si n est impair, alors les lignes de cette matrice sont indépendantes.

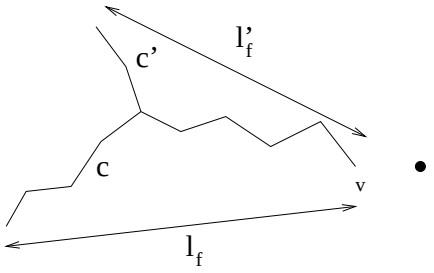
Démonstration. Tout au long de cette démonstration nous appelons forêt une forêt avec $n-2$ arêtes et un sommet isolé. Soit $L := \lambda_{\mathbf{f}_1} l_{\mathbf{f}_1} 1 + \cdots + \lambda_{\mathbf{f}_k} l_{\mathbf{f}_k}$ une combinaison linéaire nulle de lignes $l_{\mathbf{f}_i}$ de T indexées par des forêts $\mathbf{f}_i$. Nous allons d'abord montrer que, si $\mathbf{f}_i$ est un chemin de longueur $n-2$, alors le coefficient λ_i est nul, puis nous procéderons par induction sur une statistique bien choisie sur les arbres. C'est dans la première étape qu'intervient la condition n impair. Si l'on pouvait démontrer ce premier point dans le cas pair, alors l'induction s'appliquerait.

Soit donc $\mathbf{c}_1$ un chemin de longueur $n-2$, et $v_1, \ldots, v_{n-1}$ une énumération de ses sommets en partant d'une extrémité jusqu'à l'autre. Enfin, soit v_n le chemin restant. On construit $\mathbf{c}_2$ le chemin $v_2, \ldots, v_n$, puis $\mathbf{c}_3$ le chemin $v_3, \ldots, v_n, v_1$, et ainsi de suite jusqu'à $\mathbf{c}_n$ le chemin $v_n, v_1, \ldots, v_{n-2}$. On note λ_i le coefficient de $\mathbf{c}_i$ dans la combinaison linéaire L, en prenant par défaut $\lambda_i := 0$ si $\mathbf{c}_i$ n'apparaît pas dans L. Soit $\mathbf{g}$ le chemin $v_1, \ldots, v_n$. C'est un arbre qui ne contient que $\mathbf{c}_1$ et $\mathbf{c}_2$ comme sous-forêt avec un sommet isolé. On en déduit que $\lambda_1 + \lambda_2 := 0$, car la combinaison linéaire L de lignes est nulle. De même, $\lambda_2 + \lambda_3 := 0$, et ainsi de suite jusqu'à $\lambda_n + \lambda_1 := 0$. Comme n est impair, il s'ensuit que $\lambda_1 = -\lambda_1$ et donc $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$ comme voulu.

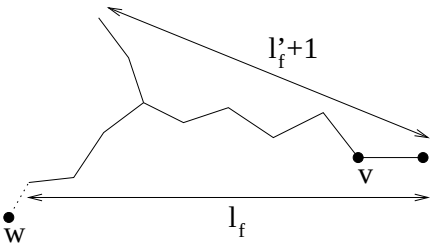
Procédons maintenant par induction. Nous associons à chaque forêt $\mathbf{f}$ un compteur $(l_{\mathbf{f}}, l'_{\mathbf{f}})$ défini comme suit : $l_{\mathbf{f}}$ est la taille du plus grand chemin $\mathbf{c}$ de $\mathbf{f}$, et $l'_{\mathbf{f}}$ est la taille du plus grand chemin $\mathbf{c}'$ non inclus dans $\mathbf{c}$. Si $\mathbf{f}$ est un chemin, on pose $l'_{\mathbf{f}} := 0$. On ordonne alors les forêts en comparant lexicographiquement leurs compteurs. La plus grande forêt $\mathbf{f}$ est le chemin $(\lambda_{\mathbf{f}}, \lambda'_{\mathbf{f}}) = (n-2, 0)$, et la plus petite l'étoile $(\lambda_{\mathbf{f}}, \lambda'_{\mathbf{f}}) = (1, 1)$.

Soit $\mathbf{f}$ une forêt. Si $\lambda_f = n-2$, alors $\mathbf{f}$ est un chemin, et on a terminé. Sinon, $\lambda'_f > 1$. Soit $\mathbf{c}$ un chemin de $\mathbf{f}$ de longueur $\mathbf{c}_f$, et $\mathbf{c}'$ un chemin de $\mathbf{f}$ de longueur $\mathbf{c}'_f$

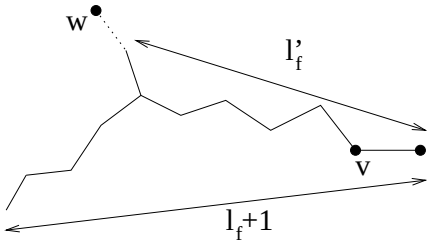
non inclus dans $\mathbf{c}$. Il est possible de choisir $\mathbf{c}$ et $\mathbf{c}'$ de sorte qu'ils aient une extrémité v en commun.



Soit $\mathbf{g}$ l'arbre obtenu en reliant dans $\mathbf{f}$ le sommet v au sommet isolé de $\mathbf{f}$. Soit $\mathbf{f}'$ une autre sous-forêt de $\mathbf{g}$. Cette forêt, ayant un sommet isolé, est obtenue en retirant une arête à une extrémité de l'arbre $\mathbf{g}$. Si on a enlevé l'arête adjacente à v, on réobtient $\mathbf{f}$. Si on a enlevé l'autre extrémité du chemin $\mathbf{c}'$, il y a dans $\mathbf{f}'$ un chemin de longueur $\lambda + 1$, obtenu en ajoutant v à $\mathbf{c}$. Donc $(l_{\mathbf{f}'}, l'_{\mathbf{f}'}) > (l_{\mathbf{f}}, l'_{\mathbf{f}})$.



Enfin, si l'on a enlevé l'autre extrémité w du chemin $\mathbf{c}$, il y a dans $\mathbf{f}$ un chemin de longueur $l_{\mathbf{f}}$, et un chemin disjoint de longueur $\lambda'_f + 1$. Donc, là encore $(l_{\mathbf{f}'}, l'_{\mathbf{f}'}) > (l_{\mathbf{f}}, l'_{\mathbf{f}})$.



Dans la combinaison linéaire L, la somme des coefficients des sous-forêts de $\mathbf{g}$ est nulle, le coefficient $\lambda_{\mathbf{f}}$ de $\mathbf{f}$ s'exprime sous la forme $\lambda_{\mathbf{f}} := -\sum_{\mathbf{f}'} \lambda_{\mathbf{f}'}$, où les forêts $\mathbf{f}'$ sont strictement plus grandes. Par induction, $\lambda_{\mathbf{f}} = 0$. □

6.5.3 Lien avec les matroïdes

Les considérations sur les matrices d'incidence s'étendent aux matroïdes. Nous renvoyons à [Wel76] pour les définitions de base.

Problème 6.5.5.
Pour quels matroïdes M, la matrice d'incidence des indépendants de taille i versus les indépendants de taille k est-elle de rang plein ?

Le matroïde des cycles associé au graphe complet est connexe. Ses bases sont les arbres, tandis que ses points sont les arêtes $\{i, j\}$. Le théorème 6.5.6 affirme alors que la matrice d'incidence des arbres versus les arêtes est de rang plein. Nous ne savons pas à quelles conditions ce résultat se généralise pour des indépendants de taille plus grande.

Théorème 6.5.6 ([Whi77, BK92]).
Soit M un matroïde de rang r ayant n éléments. Soit $\mathbb{K}$ un corps de caractéristique zéro ou supérieure à r. La matrice d'incidence des bases versus les points de M est de rang $n - k + 1$ où k est le nombre de composantes connexes de M.

Démonstration. Nous proposons une démonstration plus simple, nous contentant de montrer que la matrice M est de rang n lorsque le matroïde est connexe.

1) Soit $\mathcal{B}$ un ensemble de parties A d'un ensemble E. La matrice d'incidence des éléments de $\mathcal{B}$ versus les éléments de E est de rang plein si le graphe $c(\mathcal{B})$ défini comme suit est connexe : $c(\mathcal{B})$ a E comme ensemble de sommets et pour arêtes les paires d'éléments $\{x, y\}$ de E telles qu'il existe une partie N (ne contenant ni x ni y) de sorte que N augmenté de x et N augmenté de y soient dans $\mathcal{B}$. En effet, si l'on met sur les éléments de E une distribution de valeurs de sorte que pour chaque élément de $\mathcal{B}$ la somme soit nulle, alors deux sommets liés par une arête portent la même valeur ; le graphe étant connexe, toutes ces valeurs sont égales et donc nulles.

2) Si $\mathcal{B}$ est l'ensemble des bases d'un matroïde connexe, alors $c(\mathcal{B})$ est le graphe complet. En effet, soient x et y deux éléments et C un circuit les contenant ; alors, comme $C \setminus x$ est indépendant, y n'est pas dans la clôture F de $C \setminus \{x, y\}$. Ainsi, ni x ni y ne sont dans F. Soit G un sous espace clos contenant F, excluant x et y et maximal pour l'inclusion. On montre que F est un hyperplan : sur $E \setminus F$ la relation binaire, composée des couples (u, v) tels que u est dans la clôture de F augmenté de v, est une équivalence (Axiome de Steinitz). Puisque C est un circuit, et $C \setminus \{x, y\}$ est dans F, les éléments x et y sont équivalents. En fait, tous les éléments de $E \setminus F$ sont équivalents. En effet, si z est inéquivalent à x, alors la clôture de F augmenté de z exclut x et y, ce qui contredit la maximalité de F. Ainsi, si N est une base de F, alors N augmenté de x engendre E, et de même N augmenté de y. □

Définition 6.5.7 (Transformée de Radon discrète).
Soit E un ensemble à n éléments, et $\mathcal{A}$ une collection de parties de E. À chaque fonction f de E dans $\mathbb{K}$, on associe la fonction T_f de $\mathcal{A}$ dans $\mathbb{K}$ définie par :

$$T_f(A) := \sum_{a \in A} f(a).$$

T_f est appelée la transformée de Radon *de f.*

La matrice de la transformation de Radon n'est autre que la matrice d'incidence des parties de $\mathcal{A}$ versus les éléments de E. Le problème de reconstruction de la transformée de Radon discrète est le suivant : est-ce qu'une fonction f peut être reconstruite à partir de sa transformée de Radon T_f. Cela revient à se demander si la transformation T est injective. Lorsque $\mathcal{A}$ est l'ensemble des bases d'un matroïde, le théorème 6.5.6 donne une réponse positive à ce problème de reconstruction. Pour des applications de la transformée de Radon discrète en combinatoire, et en particulier pour une discussion sur la reconstruction de fonctions à partir de leur transformée de Radon, voir [Kun86].

Partie II

Invariants algébriques de graphes

Chapitre 7

Introduction

7.1 Motivations

Cette partie est consacrée à une étude approfondie de l'algèbre des polynômes invariants sur les graphes. La principale motivation de cette étude est la recherche de systèmes d'invariants fondamentaux, avec comme objectif lointain la conjecture de reconstruction de Ulam. Pour $n = 4$, nous connaissions un tel système et il nous a suffi de montrer que les polynômes de ce système étaient algébriquement reconstructibles. Nous en avons déduit la reconstructibilité algébrique de tous les invariants et donc des graphes valués (voir théorème 17.1.1). Selon les résultats expérimentaux obtenus dans cette partie, il est très probable que ce soit aussi le cas pour $n = 5$ (voir § 17.2). Nous présentons aussi les outils qui serviront dans la partie III à montrer que pour $n = 13$ il existe des graphes simples non-reconstructibles.

Plus généralement Read et Corneil [RC77, p344] proposent la recherche d'invariants comme approche du problème d'isomorphisme de graphes. La connaissance d'un système fondamental d'invariants permettrait de déduire des propriétés de tous les invariants en ne les montrant que sur ce système. Notons cependant qu'ils considèrent des graphes simples et des fonctions et paramètres invariants quelconques. Notre notion d'invariant est plus restrictive. Il se pourrait par exemple que nos systèmes d'invariants soient bien plus grands que réellement nécessaire.

Pas d'application algorithmique

En particulier, notre approche ne permettra probablement pas de résoudre de problèmes algorithmiques ou de complexité selon la suggestion de Read et Corneil [RC77, p344] :

« The discovery of a sufficient graph invariant (called a complete graph invariant) would solve the isomorphism problem completely, provided that the invariant was computable in polynomial time. »

« La découverte d'un invariant suffisant sur les graphes (appelé invariant complet sur les graphes) résoudrait complètement le problème d'isomorphisme, à condition que cet invariant soit calculable en temps polynômial. »

En effet, nos estimations indiquent qu'un système fondamental d'invariants polynômiaux aurait nettement plus de $n!$ termes. D'un autre côté, notre cadre restrictif

nous permet d'obtenir un certain nombre d'informations *a priori* et fournit des méthodes systématiques de recherche.

Aspects géométriques de l'algèbre des invariants

Il est clair que l'algèbre des invariants sur les graphes est aussi l'algèbre des invariants sur les matrices symétriques à diagonale nulle (ou constante), à permutation simultanée des colonnes et des lignes près. On peut en effet identifier une telle matrice avec un graphe valué, et réciproquement. Cela permet d'utiliser cette algèbre pour étudier les configurations géométriques d'ensembles de vecteurs [Pou77]. Ce fait a des applications dans l'étude des réseaux de neurones, et a motivé l'étude de l'algèbre des invariants $\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n} n$ par Aslaksen et al. [ACG96]. La présentation qui suit est fortement inspirée de leur article.

Soient K et L deux ensembles de n vecteurs de $\mathbb{R}^m$. On dit que K et L ont *même forme* s'il existe une transformation orthogonale f qui transforme K en L. Considérant les éléments non ordonnés de K comme les colonnes d'une matrice $n \times m$, on est amené à la définition suivante. Soient A et B deux matrices $n \times m$. On dit que A et B sont *congruentes* s'il existe une matrice orthogonale U et une matrice de permutation P telle que

$$B = UAP.$$

Ainsi, si les matrices A et B correspondent aux ensembles de vecteurs K et L, alors K et L ont même forme si, et seulement si, A et B sont congruentes. Pour étudier la congruence de deux matrices, nous allons montrer le lemme suivant.

Lemme 7.1.1.
Soient C et D deux matrices réelles de même dimension. Il existe une matrice orthogonale U telle que $D = UC$ si, et seulement si, $C^tC = D^tD$.

Démonstration. Une des implications est triviale. Supposons maintenant que $C^tC = D^tD$. Soient $c_1, \ldots, c_n$ et $d_1, \ldots, d_n$ les colonnes respectives de C et D. Soit $R = (r_1, \ldots, r_n)$ un vecteur colonne de nombres réels. On a

$$\|CR\|^2 = {}^tR^tCCR = {}^tR^tDDR = \|DR\|,$$

d'où l'on déduit que

$$\sum r_i c_i = 0 \Leftrightarrow \sum r_d d_i = 0.$$

Il s'ensuit que les équations $f(c_i) := d_i$, pour $i = 1 \ldots n$ déterminent une application linéaire f bien définie depuis l'espace des colonnes de C vers celui de D. Il est clair que f préserve la norme, et qu'il est possible d'étendre f en une transformation orthogonale U de $\mathbb{R}^m$. □

Les coefficients $a_{i,j}$ de la matrice ${}^tAA$ sont les produits scalaires des vecteurs de K. D'après le lemme 7.1.1, les matrices A et B sont congruentes si, et seulement si, il existe une matrice de permutation telle que

$${}^tP^tAAP = {}^tBB,$$

c'est-à-dire si les matrices symétriques ${}^tAA$ et ${}^tBB$ sont égales à permutation simultanée des lignes et des colonnes près. Lorsque les vecteurs des ensembles K et L sont tous de même norme, les coefficient diagonaux de ${}^tAA$ et ${}^tBB$ sont constants, et on peut utiliser l'algèbre des invariants $\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n} n$ pour tester si K et L ont même forme. Ainsi, si l'étude de l'algèbre $\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n} n$ des invariants sur les graphes donne un système complet d'invariants, ce système pourra aussi être utilisé pour tester si des ensembles de n vecteurs de même norme ont même forme.

Réciproquement, il est probable que ce point de vue géométrique puisse faciliter l'étude de l'algèbre des invariants $\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n} n$, en particulier en ce qui concerne la reconstruction : Pouzet [Pou77, Rev84] a proposé une version géométrique du problème de reconstruction de Ulam, équivalente au problème de reconstruction des graphes valués.

Conjecture 7.1.2.
Soient $n \geq 3$ et $K := \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ et $L := \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ deux ensembles de n vecteurs de $\mathbb{R}^m$. Si pour tout i les ensembles de $n-1$ vecteurs $K \setminus \{\mathbf{v}_i\}$ et $L \setminus \{\mathbf{w}_i\}$ ont la même forme, alors K et L eux-mêmes ont la même forme.

7.2 Littérature

Nous avons vu que cet anneau d'invariants apparaît naturellement dans différents domaines. Pourtant on ne trouve que très peu d'informations à son propos dans la littérature. Lors du congrès MEGA'98 à St-Malo, nous en avons discuté avec Sturmfels. Il nous a indiqué que, après la publication de son livre [Stu93], plusieurs personnes l'avaient contacté pour savoir ce qui était connu sur cet anneau d'invariants. Il avait en effet proposé le cas $n = 4$ comme « exercice » (exercice 3, page 28). La seule référence qu'il a pu leur fournir est [ACG96], dans lequel l'« exercice » est traité en 5 pages denses et utilisant des propriétés non triviales de théorie des invariants et des représentations.

L'échelle suivante présente, par ordre croissant de difficulté, les informations que l'on peut avoir sur un anneau d'invariants. Nous reviendrons plus loin sur les définitions précises.

1. Série de Hilbert
2. Système de paramètres (invariants primaires)
3. Invariants secondaires
4. Système fondamental d'invariants (système générateur minimal)
5. Syzygies entre les générateurs
6. Algorithme de réécriture d'un invariant en fonction des générateurs

Les recherches respectives de 4, 5 et 6 sont traditionnellement appelées les problèmes fondamentaux de la théorie des invariants. Au moins du point de vue algorithmique, 3 et 4 sont du même ordre de difficulté.

Nous avons trouvé les résultats suivants dans la littérature. Pour $n = 4$, Aslaksen et al.. [ACG96] présentent un système générateur minimal et indiquent que les

syzygies s'obtiennent sans difficulté avec les algorithmes habituels. Pour $n = 5$, ils donnent un système de paramètres en utilisant [Dix91], assorti du commentaire :

« When we computed the Poincaré series, we got 720 terms in the numerator, so it seems difficult to give a simple description of the ring of invariants. »

« Lorsque nous avons calculé la série de Poincaré, nous avons obtenu 720 termes au numérateur. Il semble donc difficile de donner une description simple de l'anneau des invariants. »

Le calcul pour $n = 4$ a aussi été traité par ordinateur par Kemper [Kem98b, p. 11]. En dehors de cela, nous n'avons trouvé qu'un article de Grigoriev [Gri79] contenant des résultats sur une algèbre proche, l'algèbre des invariants sur les digraphes, et surtout sur le corps des invariants sur les digraphes. La plupart de ces résultats sont des propriétés générales du corps des invariants d'un groupe fini (voir § 9). Nous montrons au § 12.1 que le principal résultat spécifique aux digraphes est faux.

En fait, contrairement à ce que nous pensions, autant les représentations du groupe symétrique sont parfaitement connues, autant les anneaux d'invariants correspondants le sont peu. Par exemple, pour les représentations irréductibles de $\mathfrak{S}_n$, et en dehors des cas triviaux comme les polynômes à une variable ou les polynômes symétriques, seul le cas de $\mathfrak{S}_5$ semble avoir été approfondi. Nous citons Dixmier [Dix91] :

« Je n'ai pu régler le cas de $[3, 1^2]$. Le but principal du présent mémoire est d'obtenir, pour $\mathbb{C}[[3, 2]]^{\mathfrak{S}_5}$ et $\mathbb{C}[[2^2, 1]]^{\mathfrak{S}_5}$, un système de paramètres et un système générateur minimal. Cet objectif, bien que modeste, va demander du travail. »

Comme l'indiquent Aslaksen et al. [ACG96], la première difficulté de cette étude vient de l'explosion combinatoire qui restreint considérablement le champ exploratoire. Pour donner un ordre de grandeur, pour $n = 5$ on est amené à rechercher 720 polynômes à 10 variables de degré allant jusqu'à 22. Certains d'entre eux peuvent occuper quelques centaines de kO sur le disque. Par exemple, le test classique pour vérifier si un ensemble de polynômes forme un système de paramètres, n'est pas toujours praticable. Il utilise un calcul de base de Gröbner qui, si les polynômes ne s'y prêtent pas, explose en temps et en mémoire, même sur des machines récentes. Pour $n = 5$, il ne fonctionne qu'à condition de prendre des précautions. Pour $n = 6$, il est inutile d'essayer.

Nous avons donc très peu de marge de manoeuvre pour tester des conjectures, d'autant plus que les cas $n \leq 3$ sont dégénérés. Les polynômes invariants coïncident en effet avec les polynômes symétriques. Même le cas $n = 4$ présente des particularités. Nous avons donc plusieurs fois basé des conjectures sur le seul cas $n = 5$, espérant qu'il soit assez générique. Heureusement certains calculs (série de Hilbert, ...) peuvent aller nettement plus loin. À ce titre, l'étude de l'anneau des invariants pour les graphes bipartis paraît intéressante, car l'explosion est moins brutale et devrait ouvrir un plus grand champ d'expérimentation.

L'autre difficulté vient de la très grande généralité des outils utilisés, autant théoriques que pratiques. En effet ceux-ci n'exploitent pas toutes les spécificités du problème et se révèlent souvent peu efficaces. Par exemple, nous avons essayé plusieurs systèmes récents de calcul de bases d'algèbres d'invariants (`Invar` et `Invar 2` sous `Maple` et `RngInvar` sous `Magma` de Kemper [Kem96], `FINVAR.LIB`

sous `Singular` [Hey96]. La plupart du temps, le cas $n = 4$ était traité correctement. En revanche, aucun des systèmes n'a réussi à trouver des invariants primaires pour $n = 5$. Même en leur fournissant nos invariants primaires, aucun d'entre eux n'a pu construire les invariants secondaires au-delà du degré 5. Nous avons donc dû réimplémenter ces algorithmes en les optimisant pour notre problème. Cela ne nous a pas suffi pour régler complètement le cas 5, mais nous a déjà donné des informations partielles intéressantes pour $n = 5, 6, 7$ (voir section 11.4.3).

7.3 Plan

Le chapitre 8 décrit les propriétés générales de l'algèbre des invariants. Notre objectif n'est pas de réécrire une énième introduction à la théorie des invariants, mais de faire une synthèse des résultats généraux à notre disposition dans la littérature. Nous n'avons pas particulièrement cherché à retrouver les auteurs originaux, mais nous nous sommes efforcés de donner comme références les textes les plus accessibles et les plus clairs (cette appréciation étant forcément subjective).

Notre représentation a un certain nombre de caractéristiques particulières et nous indiquons ce que chacune d'entre elles peut nous apporter. Tout d'abord, c'est une représentation linéaire d'un groupe fini. Ce groupe agit par permutation des vecteurs de la base, mais c'est aussi une représentation du groupe symétrique. Ces deux dernières caractéristiques suggèrent des approches très différentes, voire incompatibles et il est difficile de dire laquelle est la plus importante. Tout au long de cette partie, nous serons amenés à exploiter tantôt l'une, tantôt l'autre, selon les problèmes abordés. Enfin, lorsque n est pair, c'est un sous-groupe du groupe spécial linéaire $SL_{C_n^2}(\mathbb{C})$.

Le chapitre 11 est consacré à la recherche de systèmes fondamentaux d'invariants. Nous commençons par présenter les principales techniques et outils que nous avons à notre disposition. Nous montrons en particulier que « les graphes simples n'engendrent pas tous les multigraphes ». Ceci répond par la négative à une question posée par Pouzet. Comme nous l'avons dit, il est difficile d'obtenir des informations *a priori* sur les systèmes générateurs minimaux. De plus, il n'existe pas de méthode générale de recherche, et les algorithmes sont très coûteux. En revanche, il existe d'autres systèmes générateurs qui exploitent beaucoup mieux la structure de l'algèbre. Un tel système est composé d'invariants primaires et secondaires, en fonction desquels tout polynôme invariant s'exprime de manière canonique. Dans la plupart des cas ce système est loin d'être minimal. D'un autre côté, on peut avoir beaucoup d'informations *a priori* sur eux uniquement en étudiant la série de Hilbert. Cela permet en particulier d'obtenir des bornes sur la taille et les degrés d'un système générateur minimal. Enfin, il existe des outils et des algorithmes de construction. Certaines variantes de ces algorithmes permettent d'extraire un système générateur minimal au fur et à mesure de la construction.

Nous nous intéressons d'abord aux invariants primaires. Le choix classique (les polynômes symétriques élémentaires) est sous-optimal, car il impose un très grand nombre d'invariants secondaires. Nous proposons un autre ensemble de polynômes qui, selon notre conjecture, devrait être un système d'invariants primaires. Si c'est le cas, cela réduit considérablement le nombre d'invariants secondaires. On obtient

alors une bien meilleure majoration de la taille d'un système fondamental d'invariants, et surtout des degrés des polynômes d'un tel système. Nous avons pu montrer notre conjecture, par le calcul, jusqu'à $n = 5$. Au delà, nous étayons notre conjecture sur une étude de la série de Hilbert, en nous appuyant sur une conjecture de Mallows et Sloane [MS73, Dix91].

Dans la section 11.4,nous détaillons les voies que nous avons suivies pour rechercher des invariants secondaires. Nous nous sommes en particulier intéressés à une recherche par ordinateur dans les petits cas. Comme nous l'avons mentionné ci-dessus, le cas $n = 4$ (6 variables, 6 invariants secondaires de degré allant jusqu'à 9[1]) ne pose pas de problème particulier et a déjà été traité dans la littérature. Il est probablement impossible d'obtenir par le calcul de résultat complet pour $n = 6$ (15 variables, 3628800 invariants secondaires de degré allant jusqu'à 60) et au delà. Nous nous sommes donc concentrés sur le cas limite $n = 5$ (10 variables, 720 invariants secondaires de degré jusqu'à 22).

Une application directe des logiciels existants ne permet pas d'aller très loin. Nous avons donc réimplémenté les algorithmes pour utiliser certaines propriétés spécifiques de notre algèbre d'invariants. Nous ne pensons pas pouvoir donner un système complet d'invariants secondaires pour $n \geq 5$. En revanche, nous avons déjà des résultats partiels intéressants. En particulier, pour $n = 5$, nous avons construit un système de polynômes invariants, composé uniquement de multigraphes avec des sommets isolés, qui est très certainement un système générateur minimal ; cela prouverait que les polynômes invariants sont tous algébriquement reconstructibles.

Nous présentons au chapitre 9 quelques propriétés du corps des fractions invariantes, et nous expliquons pourquoi nous avons plutôt travaillé sur l'anneau des polynômes invariants.

Enfin, dans le chapitre 12, nous étudions certaines algèbres d'invariants proches (algèbre des invariants sur les digraphes, algèbre des graphes simples, algèbre des forêts, etc.). Nous montrons en particulier que de même que l'algèbre des invariants sur les graphes, l'algèbre des invariants sur les digraphes n'est pas engendrée par les digraphes simples. Ceci infirme un lemme de Grigoriev [Gri79, Lemma I].

[1] Cf. annexe A pour quelques statistiques sur l'algèbre des invariants, sous forme de tables et de graphiques

Chapitre 8

Généralités sur les algèbres d'invariants

Ce chapitre présente une synthèse des principales propriétés de l'algèbre des invariants sur les graphes que l'on définit comme suit. Soient $(\{x_{\{1,2\}}, x_{\{1,3\}}, \ldots, x_{\{n,n-1\}})$ un ensemble de C_n^2 variables indexées par les paires de $\{1, \ldots, n\}$. Le groupe symétrique $\mathfrak{S}_n$ agit naturellement sur ces variables par $\sigma x_{\{i,j\}} = x_{\{\sigma(i),\sigma(j)\}}$. Cette action est le pendant de la représentation du groupe symétrique sur l'espace vectoriel des graphes valués que nous avons vu dans la première partie. Soit $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$ l'algèbre des polynômes en ces variables. L'action de $\mathfrak{S}_n$ sur ces variables s'étend sur $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$, et on considère le sous-ensemble $\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$ des polynômes de $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$ invariants par l'action de $\mathfrak{S}_n$. Comme la somme et le produit de deux polynômes invariants sont clairement invariants, l'ensemble $\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$ est une algèbre, que l'on appelle *algèbre des invariants sur les graphes* .

Nous avons cherché dans la littérature ce que l'on pouvait déduire de chaque caractéristique de la représentation de $\mathfrak{S}_n$ sur les graphes valués : représentation linéaire d'un groupe fini, représentation par permutation, représentation du groupe symétrique, etc. L'objectif de notre exposé est de rester simple, en évitant autant que possible le formalisme non indispensable. Pour cela, nous avons omis un certain nombre de détails techniques. En revanche, nous proposons au fur et à mesure des références auxquelles le lecteur pourra se reporter. De nombreux points seront aussi repris dans les chapitres ultérieurs.

Dans toute cette partie, nous prenons $\mathbb{C}$ comme corps de base. La plupart des résultats s'étendent à n'importe quel corps de caractéristique zéro. Lorsque ce n'est pas le cas, par exemple lorsque le corps doit être algébriquement clos, nous le mentionnons explicitement.

8.1 Invariants d'une représentation d'un groupe fini

8.1.1 Introduction et références

La première caractéristique de la représentation du groupe symétrique sur les graphes est d'être une représentation linéaire d'un groupe fini. Fixons les notations. Soient $V = \langle \mathbf{e}_1, \ldots, \mathbf{e}_m \rangle_{\mathbb{C}}$ un espace vectoriel de dimension m, et G un groupe fini agissant linéairement sur V. Soit $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_m]$ l'anneau des polynômes sur V. On considère l'ensemble $\mathbb{C}[\mathbf{x}]^G$ des polynômes de $\mathbb{C}[\mathbf{x}]$ invariants par l'action de

G. Cet ensemble est naturellement stable par addition et multiplication et forme donc une sous-algèbre de $\mathbb{C}[\mathbf{x}]$, que l'on appelle *algèbre des invariants*. Dans notre cas, G est le groupe symétrique $\mathfrak{S}_n$, les $\mathbf{e}_i$ sont les arêtes du graphe complet que l'on a énuméré dans un ordre quelconque et $m = \mathrm{C}_n^2$.

Pour une introduction aux algèbres d'invariants de groupes finis, nous conseillons [CLO97, Chapitre 7]. Nous avons apprécié l'article de synthèse [Sta79] qui est accessible et très complet. [Smi97] est un autre article de synthèse plus récent. Pour une approche algorithmique, il y a l'incontournable livre de Sturmfels [Stu93], mais aussi les articles de Kemper [Kem96, Kem98b] qui a implémenté concrètement ces algorithmes [Kem93]. Enfin, Dixmier [Dix91] propose plusieurs études à la main de petits cas.

8.1.2 Graduation et série de Hilbert

Graduation

De nombreux problèmes sur l'algèbre des invariants peuvent se ramener à de l'algèbre linéaire en dimension finie. Soient en effet P un polynôme de degré d et σ un élément du groupe. Comme l'action de σ est linéaire, le degré de P est préservé : $d(P) = d(\sigma.P)$. Par exemple, si P est le polynôme xy^2 et σ la transformation linéaire $x = u + v, y = u - v$, on a

$$\sigma.P = \sigma.xy^2 = (u+v)(u-v)^2 = u^3 + v^3 - uv^2 - u^2v.$$

L'action du groupe sur l'algèbre des polynômes $\mathbb{C}[\mathbf{x}]$ se décompose donc sur chaque composante homogène $\mathbb{C}[\mathbf{x}]_d$ de degré d. On en déduit, en particulier, qu'un polynôme est invariant si, et seulement si, toutes ses composantes homogènes le sont. Soit $\mathbb{C}[\mathbf{x}]_d^G$ l'ensemble des polynômes invariants homogènes de degré d. C'est un sous-espace vectoriel de $\mathbb{C}[\mathbf{x}]_d$, donc de dimension finie, et on a la proposition :

Proposition 8.1.1.
L'algèbre des invariants est une sous-algèbre graduée de $\mathbb{C}[\mathbf{x}]$ *:*

$$\mathbb{C}[\mathbf{x}]^G = \bigoplus_d \mathbb{C}[\mathbf{x}]_d^G.$$

Série de Hilbert

L'algèbre des invariants commence déjà à prendre un peu de structure. En particulier, nous pouvons la mesurer, en considérant la dimension de chacun des espaces vectoriels $\mathbb{C}[\mathbf{x}]_d^G$. La série de Hilbert n'est rien d'autre que la série génératrice de ces dimensions.

Définition 8.1.2 (Série de Hilbert).
Soit $A = \bigoplus_{d\geq 0} A_d$ *une algèbre graduée. On appelle* série de Hilbert *de* A *la série génératrice des dimensions des composantes homogènes de* A *:*

$$H(A, z) = \sum \dim(A_d)\, z^d$$

Lorsque A *est une algèbre d'invariants, on appelle aussi cette série,* série de Molien *ou* série de Poincaré*.*

Le théorème suivant indique qu'il suffit de connaître les matrices de représentation des éléments du groupe pour calculer la série de Hilbert !

Théorème 8.1.3 (Molien 1897).

$$H(\mathbb{C}[\mathbf{x}]^G, z) = \frac{1}{|G|} \sum_{M \in G} \frac{1}{\det(\mathrm{Id} - zM)}$$

Cette formule peut être raffinée pour obtenir un calcul efficace (voir section 10.3).

8.1.3 Opérateur de Reynolds

Le calcul de la série de Hilbert, et plus généralement les calculs de caractères de groupe fini, reposent sur une idée de moyenne sur le groupe. Cette idée peut aussi être utilisée pour construire les polynômes invariants par symétrisation de polynômes quelconques.

Définition 8.1.4 (Opérateur de Reynolds).
On appelle opérateur de Reynolds *l'application :*

$$\text{« * »} : \begin{cases} \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G \\ \quad p \to p^* = \dfrac{1}{|G|} \displaystyle\sum_{\sigma \in G} \sigma.p \end{cases}$$

On note que la caractéristique zéro est essentielle pour pouvoir définir cet opérateur (on pourrait cependant se contenter d'une caractéristique ne divisant pas l'ordre du groupe). L'opérateur de Reynolds a les propriétés suivantes

Propriétés 8.1.5.

- *« * » est linéaire,* i.e. $(\lambda_1 p_1 + \lambda_2 p_2)^* = \lambda_1 p_1^* + \lambda_2 p_2^*$ *pour tout* $p_1, p_2 \in \mathbb{C}[\mathbf{x}]$ *et* $\lambda_1, \lambda_2 \in \mathbb{C}$,
- *« * » est une projection sur* $\mathbb{C}[\mathbf{x}]^G$, i.e. $p^{**} = p^*$ *et* $\mathrm{Im}(*) = \mathbb{C}[\mathbf{x}]^G$,
- *« * » est un homomorphisme de* $\mathbb{C}[\mathbf{x}]^G$*-modules,* i.e. $(I.p)^* = I.p^*$ *si* $I \in \mathbb{C}[\mathbf{x}]^G$ *et* $p \in \mathbb{C}[\mathbf{x}]$.

8.1.4 Systèmes générateurs, syzygies et géométrie des orbites

Finitude des systèmes générateurs

Nous allons maintenant énoncer le théorème fondamental de la théorie des invariants.

Définition 8.1.6 (Algèbre de type fini).
Une algèbre est de type fini *si elle admet un système générateur fini.*

Théorème 8.1.7 (Hilbert 1890 / Noether 1916 [Stu93, p. 26–27]).
L'algèbre des invariants est de type fini. Elle est engendrée par les $C^m_{m+|G|}$ *polynômes invariants homogènes de degré inférieur à* $|G|$.

La démonstration originale de Hilbert repose essentiellement sur la graduation de l'algèbre et l'opérateur de Reynolds (voir § 11.1.2) ; elle ne donne pas la borne sur le degré. La démonstration de Noether est basée sur l'opérateur de Reynolds et le théorème fondamental des fonctions symétriques. Cette démonstration s'applique en fait de manière plus générale, la graduation ne servant en effet qu'à obtenir la borne sur le degré.

Théorème 8.1.8 (Noether[VdW91, p. 279]).
Soit $\mathcal{A}$ une algèbre de type fini sur un corps $\mathbb{K}$, et G un groupe fini d'automorphismes de $\mathcal{A}$ tel que la caractéristique de $\mathbb{K}$ ne divise pas l'ordre du groupe G. Alors la sous-algèbre $\mathcal{A}^G$ des invariants est de type fini.

Définition 8.1.9.
On appelle borne sur les degrés d'un système générateur *l'entier*

$$\beta(\mathbb{C}[\mathbf{x}]^G) = \min\left\{d,\ \mathbb{C}[\mathbf{x}]^G \text{ est engendré par les polynômes de degré } \leq d\right\}.$$

On vérifie qu'il s'agit du plus grand degré d'un polynôme dans un système générateur minimal. Dans le cas de l'algèbre des invariants sur les graphes, nous le noterons $\beta(n) := \delta\left(\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}\right)$.

Il est très important d'obtenir une majoration fine de $\beta(n)$, en particulier pour des raisons algorithmiques. Dans le cas général d'un groupe fini, la borne donnée par le théorème 8.1.7 est optimale, car elle est atteinte pour les groupes cycliques. On peut l'améliorer pour les groupes non cycliques (voir [Sch91] et [DK97]). Dans notre cas, cette borne est très grossière ($\beta(n) \leq |G| = n!$), et nous pourrons l'améliorer drastiquement.

Systèmes minimaux de générateurs

La qualité d'algèbre graduée de type fini suffit pour donner une certaine canonicité aux ensembles minimaux de générateurs homogènes. Tout ce qui est dit ici est valable dans n'importe quelle algèbre graduée $\mathcal{A}$ sur un corps $\mathbb{K}$ de caractéristique quelconque, telle que $\mathcal{A}_0 = \mathbb{K}$.

Définition 8.1.10 (Ensemble minimal de générateurs).
Soit B un ensemble de polynômes invariants. B est un système minimal de générateurs *si $\mathbb{C}[\mathbf{x}]^G$ est engendré par B, mais par aucun sous-ensemble strict de B.*

Par la suite, et sauf mention contraire, tous les systèmes de générateurs que nous considérerons seront des systèmes de générateurs homogènes. Dans un espace vectoriel, il n'y a pas unicité de la base, mais par contre la taille d'une base est fixée. De même ici, le nombre et les degrés des polynômes dans un système minimal de générateurs sont entièrement déterminés. Cependant, il n'existe pas de méthode générale pour connaître ces degrés *a priori*, sans calculer explicitement un système de générateurs minimal.

Proposition 8.1.11.
Soient $\{p_1, \ldots, p_k\}$ et $\{q_1, \ldots, q_l\}$ deux systèmes minimaux de générateurs. On suppose de plus qu'ils sont triés par degré croissant. Alors, $k = l$ et pour tout i, les polynômes p_i et q_i sont de même degré.

Nous reviendrons de manière plus approfondie sur cette proposition au § 11.1. Nous verrons que l'opérateur de Reynolds et la connaissance d'une borne sur le degré permet de définir un premier algorithme de recherche d'invariants minimaux (voir § 11.1.1). Notons que cet algorithme termine en théorie, mais qu'il est inutilisable dans la pratique. Par contre, il existe des algorithmes beaucoup plus efficaces, qui exploitent la structure très forte de l'algèbre des invariants (voir § 8.1.5).

Relations entre les générateurs

Pour étudier plus précisément la façon dont l'algèbre est engendrée, il faut étudier les syzygies entre les générateurs.

Définition 8.1.12 (Syzygie).
Soit $F = (f_1, \ldots, f_k)$ un ensemble de générateurs de l'algèbre $\mathbb{C}[\mathbf{x}]^G$ des invariants. On appelle syzygie *ou* relation algébrique *entre les f_i un polynôme h tel que*

$$h(f_1, \ldots, f_k) = 0$$

On note I_F l'ensemble des syzygies entre les f_i.

Théorème 8.1.13 ([CLO97, ch. 7, § 4]).
- *L'ensemble I_F des syzygies entre les f_i est un idéal premier.*
- *Soit p un polynôme de $\mathbb{C}[\mathbf{x}]^G$. Supposons que $p = h(f_1, \ldots, f_k)$ soit une expression de p en fonction des générateurs. Alors, toutes les expressions de p en fonction des générateurs sont de la forme*

  $$p = h(f_1, \ldots, f_k) + g(f_1, \ldots, f_k)$$

  où $\mathbf{g}$ est dans I_F.

Considérons le morphisme de l'algèbre libre $\mathbb{C}[y_1, \ldots, y_k]$ sur k variables dans $\mathbb{C}[\mathbf{x}]^G$ qui associe f_i à y_i :

$$\phi_F = \begin{cases} \mathbb{C}[y_1, \ldots, y_k] \to \mathbb{C}[\mathbf{x}]^G \\ y_i \mapsto f_i \end{cases}$$

Par définition, ce morphisme est surjectif et son noyau est l'idéal des syzygies I_F. L'algèbre des invariants est donc isomorphe au quotient de l'algèbre libre par l'idéal des syzygies I_F.

Géométrie de l'espace des orbites

La connaissance d'un système générateur et de ses relations a une conséquence géométrique très intéressante. Elle permet en effet de donner une structure de variété algébrique à l'espace des orbites. Il sera ici essentiel que le corps soit algébriquement clos, de sorte que la dualité algèbre/géométrie fonctionne correctement.

Le théorème suivant indique que l'algèbre des invariants sépare les orbites de V.

Théorème 8.1.14 ([CLO97, ch. 7, § 4], [Stu93, p. 16]).
Soient $\mathbf{v}$ et $\mathbf{v}'$ deux vecteurs de V. Si $\mathbf{v}$ et $\mathbf{v}'$ sont dans la même orbite, ils donnent la même valeur à tous les polynômes invariants. La réciproque est aussi vraie, c'est-à-dire que si $\mathbf{v}$ et $\mathbf{v}'$ ne sont pas dans la même orbite, il existe un polynôme invariant p tel que $p(\mathbf{v}) \neq p(\mathbf{v}')$.

La finitude du groupe est ici essentielle. L'idée de la démonstration est que, étant donnés deux ensembles finis de vecteurs $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ et $\{\mathbf{w}_1, \ldots, \mathbf{w}_l\}$, on peut construire un polynôme nul sur les $\mathbf{v}_i$ et valant 1 sur les $\mathbf{w}_i$. On applique alors l'opérateur de Reynolds pour obtenir un polynôme invariant. En termes algébriques on peut aussi se contenter de rappeler qu'un ensemble fini de points est un fermé pour la topologie de Zariski.

Bien entendu, ce théorème reste vrai pour une famille (f_i) quelconque qui engendre l'algèbre des invariants : deux vecteurs sont dans la même orbite si, et seulement si, ils donnent la même valeur à tous les polynômes f_i. Les f_i forment donc un système complet d'invariants dans le sens usuel de la théorie des graphes (voir [RC77]). Dans ce contexte, le théorème fondamental de la théorie des invariants 8.1.7 nous assure de l'existence d'un système d'invariants polynomiaux complet et fini.

De plus, les f_i permettent de définir l'espace des orbites comme une variété algébrique. Soit Ψ l'application qui, à un vecteur $\mathbf{v}$, associe la liste des k valeurs que prennent les f_i sur $\mathbf{v}$.

$$\Psi = \begin{cases} V \to \mathbb{C}^k \\ \mathbf{v} \mapsto (f_1(\mathbf{v}), \ldots, f_k(\mathbf{v})) \end{cases}$$

Les polynômes f_i sont invariants et Ψ est donc définie sur les orbites de V. L'application Ψ est alors injective. Soit maintenant V_F la sous-variété de $\mathbb{C}^k$ définie par l'idéal des syzygies de F. Si h est une syzygie et $\mathbf{v}$ un vecteur de V, on remarque que

$$h(\Psi(\mathbf{v})) = h(f_1(\mathbf{v}), \ldots, f_k(\mathbf{v})) = h(f_1, \ldots, f_k)(\mathbf{v}) = 0.$$

Donc l'image de Ψ est inclue dans la variété V_F. Le théorème suivant décrit alors complètement la structure de l'image de Ψ dans $\mathbb{C}^k$.

Théorème 8.1.15 ([CLO97, ch. 7, § 4]).
Ψ est une bijection des orbites de V sur V_F. De plus, V_F est une variété irréductible.

Notons qu'il est indispensable que le corps soit algébriquement clos pour que Ψ soit surjective. Sur $\mathbb{R}$, par exemple, ce n'est plus le cas. L'image de Ψ est alors un sous-ensemble de V_F défini par un ensemble d'inégalités larges. On pourra consulter [Sch96] pour plus de détails, en particulier sur les techniques pour établir ces inégalités.

En conclusion, cette machinerie permet de plonger l'espace des orbites comme sous-variété irréductible d'un $\mathbb{C}^k$. L'algèbre des invariants est l'anneau des coordonnées de cette sous-variété. De plus, nous avons vu (proposition 8.1.11) que tous les systèmes générateurs minimaux ont même cardinal. On en déduit que l'on peut définir de manière canonique le plus petit k tel que l'espace des orbites se plonge comme sous-variété algébrique de $\mathbb{C}^k$.

Généralisations

On remarque que, pour pouvoir définir l'opérateur de Reynolds, il suffit que la caractéristique du corps ne divise pas $|G|$. Tant que cette condition est vérifiée, la

plupart des théorèmes se généralisent sans problème sur des corps autres que $\mathbb{C}$, car ils sont essentiellement basés sur l'existence de cet opérateur. Il existe maintenant aussi une théorie assez complète pour le cas modulaire, mais elle est plus complexe. Nous avons pris le parti de ne pas l'aborder et, comme notre groupe est d'ordre $n!$, de nous placer directement en caractéristique 0. Nous préciserons les théorèmes pour lesquels nous avons besoin d'éventuelles propriétés supplémentaires (clôture algébrique, etc.).

Notons aussi que l'opérateur de Reynolds peut aussi être défini sur certains groupes infinis à l'aide d'une mesure et d'intégrales. Voir par exemple [Stu93, p. 27] pour plus de détails.

Invariants relatifs

Nous renvoyons à [Sta79] pour une définition précise des composantes isotypiques de l'algèbre des polynômes. L'idée est simplement de décomposer cette algèbre en composantes irréductibles vis-à-vis de l'action de G, puis de regrouper entre elles les composantes isomorphes.

Notation 8.1.16 (Composantes isotypiques de l'algèbre des polynômes). *Soient U un G-module et χ un caractère irréductible de G. Ce caractère χ définit une représentation irréductible de G à isomorphie près. On note $\mathbb{C}[U]^G_\chi$ la* composante isotypique *correspondante de $\mathbb{C}[U]$. Les polynômes de $\mathbb{C}[U]^G_\chi$ sont dits* invariants relatifs au caractère χ.

Par exemple, si ϵ est le caractère de la représentation triviale du groupe, la composante isotypique correspondante est tout simplement l'algèbre des polynômes invariants :

$$\mathbb{C}[U]^G_\epsilon = \mathbb{C}[U]^G.$$

On note que la décomposition en composantes isotypiques $\mathbb{C}[U] = \bigoplus_\chi \mathbb{C}[U]^G_\chi$ est unique. Les propriétés de ces composantes sont étudiées en détail dans [Sta79]. On y trouve en particulier une généralisation de la formule de Molien pour calculer leurs séries de Hilbert [Sta79, p. 479] :

$$H(\mathbb{C}[\mathbf{x}]^G_\chi, z) = \chi(1)\frac{1}{|G|}\sum_{M\in G}\frac{\overline{\chi}(M)}{\det(\mathrm{Id} - zM)}.$$

Nous verrons plus loin (théorème 8.3.5) que l'étude de ces séries de Hilbert permet de montrer que la répartition entre les composantes isotypiques est bien caractérisée. De fait, l'espace des polynômes est une somme directe de copies de la représentation régulière du groupe.

Il y a une dualité entre les invariants et les invariants relatifs au caractère $\epsilon := \det^{-1}$. Cette dualité apparaît dans l'expression de la série de Hilbert [Sta79, p. 479] :

$$H(\mathbb{C}[\mathbf{x}]^G, \frac{1}{z}) = (-1)^m z^m H(\mathbb{C}[\mathbf{x}]^G_{\det^{-1}}, z). \tag{8.1}$$

8.1.5 L'algèbre des invariants est de Cohen-Macaulay

L'article de synthèse de Kemper [Kem98b] donne une très bonne présentation de ce qui va suivre, en particulier d'un point de vue algorithmique.

Dimension de Krull de l'algèbre des invariants

On rappelle que la *dimension de Krull* d'une algèbre $\mathcal{A}$ est le plus grand entier k tel qu'il existe k éléments $p_1, \ldots, p_k$ de $\mathcal{A}$ algébriquement indépendants. Par exemple, la dimension de Krull de l'anneau $\mathbb{C}[\mathbf{x}]$ des polynômes est le nombre m de variables de $\mathbb{C}[\mathbf{x}]$.

Théorème 8.1.17 (Noether 1916).
La dimension de Krull de l'algèbre des invariants est la dimension m de l'espace vectoriel V ou, autrement dit, le nombre de variables de $\mathbb{C}[\mathbf{x}]$.

Une algèbre $\mathcal{A}$ est *entière* sur une sous-algèbre $\mathcal{B}$ si tout élément p de $\mathcal{A}$ vérifie une équation de la forme

$$p^k + \alpha_1 p^{k-1} + \cdots + \alpha_k = 0,$$

où les α_i sont dans $\mathcal{B}$. En particulier, les éléments p de $\mathcal{A}$ sont algébriques sur $\mathcal{B}$. Une des propriétés fondamentales de la dimension de Krull est que, si une algèbre $\mathcal{A}$ est entière sur une sous-algèbre $\mathcal{B}$, alors $\mathcal{A}$ et $\mathcal{B}$ ont même dimension de Krull.

Lemme 8.1.18.
L'algèbre $\mathbb{C}[\mathbf{x}]$ des polynômes est entière sur l'algèbre $\mathbb{C}[\mathbf{x}]^G$ des polynômes invariants.

Démonstration. La démonstration de ce lemme utilise le même artefact que la démonstration du théorème 8.1.7. Soit p un polynôme quelconque de $\mathbb{C}[\mathbf{x}]$. On considère le polynôme P en la variable t

$$P := \prod_{\sigma \in G} (t - \sigma.p).$$

On développe P par rapport à t pour le mettre sous la forme :

$$P = t^{|G|} + \alpha_1 t^{|G|-1} + \cdots + \alpha_{|G|}.$$

Comme P est clairement invariant par l'action de G, chacun des coefficient α_i est un polynôme invariant de $\mathbb{C}[\mathbf{x}]^G$. De plus, par construction, $P(p) = 0$. □

Dans notre cas, comme le groupe G agit par permutation des variables, on peut aussi se contenter de remarquer que les m polynômes symétriques élémentaires en les variables $x_1, \ldots, x_m$ sont, d'une part, invariants et, d'autre part, algébriquement indépendants.

Décomposition de Hironaka

Nous avons vu qu'il était difficile d'avoir *a priori* des informations sur la taille et les degrés d'un système générateur minimal. Il existe des systèmes générateurs, habituellement plus grands, mais sur lesquels on peut recueillir beaucoup d'informations *a priori*. De plus, ces systèmes donnent une structure très forte à l'algèbre des invariants. Un polynôme invariant quelconque peut s'écrire de manière canonique en fonction des générateurs. En outre, les relations entre les générateurs ont une forme bien déterminée. Enfin, on peut exploiter cette structure pour accélérer considérablement la construction d'un système générateur.

Dans le cas le plus simple, l'algèbre des invariants est engendrée par m polynômes invariants algébriquement indépendants. Par exemple, les polynômes symétriques en m variables sont engendrés par les polynômes symétriques élémentaires. Il n'y a alors pas de relations entre les générateurs, et l'écriture d'un polynôme en fonction des générateurs est unique, comme souhaité. Les groupes de matrices dont les algèbres d'invariants ont cette propriété sont entièrement caractérisés.

Définition 8.1.19 (Pseudo-réflexion).
Une pseudo-réflexion *est une matrice ayant exactement une valeur propre simple différente de* 1.

Théorème 8.1.20 (Shepard, Todd, Chevalley et Serre [Sta79, p. 486]).
Soit G un groupe de matrices fini. L'anneau des invariants de G est engendré par des polynômes invariants algébriquement indépendants si, et seulement si, G est engendré par des pseudo-réflexions.

Nous verrons que, pour $n \geq 4$, le groupe de matrices correspondant à la représentation de $\mathfrak{S}_n$ sur les graphes valués ne contient pas de pseudo-réflexions (voir lemme 8.4.2). L'algèbre des invariants sur les graphes n'est donc pas engendrée par des invariants algébriquement indépendants. En revanche, à défaut d'être de la forme $\mathbb{C}[\theta_1, \ldots, \theta_m]$, l'algèbre des invariants admet une décomposition dite *décomposition de Hironaka*

$$\mathbb{C}[\mathbf{x}]^G = \bigoplus_{i=1}^{t} \eta_i.\mathbb{C}[\theta_1, \ldots, \theta_m]$$

où les θ_i et les η_i sont homogènes et les θ_i algébriquement indépendants (voir figure 8.1 page suivante). Autrement dit, si l'on considère les polynômes de $\mathbb{C}[\theta_1, \ldots, \theta_m]$ comme des scalaires, l'algèbre des invariants est la somme directe finie des « droites » engendrées par les η_i. On dit que $\mathbb{C}[\mathbf{x}]^G$ est un module libre de type fini sur la sous-algèbre $\mathbb{C}[\theta_1, \ldots, \theta_m]$. Les polynômes $\theta_1, \ldots, \theta_m$ sont appelés *invariants primaires* et les polynômes $\eta_1, \ldots, \eta_t$ *invariants secondaires*. Notons tout de suite que ni les invariants primaires, ni les invariants secondaires ne sont canoniques.

Pour résumer :

Définition 8.1.21 (Algèbre de Cohen-Macaulay).
Une algèbre est dite de Cohen-Macaulay si elle admet une décomposition de Hironaka.

Théorème 8.1.22 ([Sta79, p. 481], [Stu93, ch. 2.3]).
L'algèbre des polynômes invariants $\mathbb{C}[\mathbf{x}]^G$ est de Cohen-Macaulay.

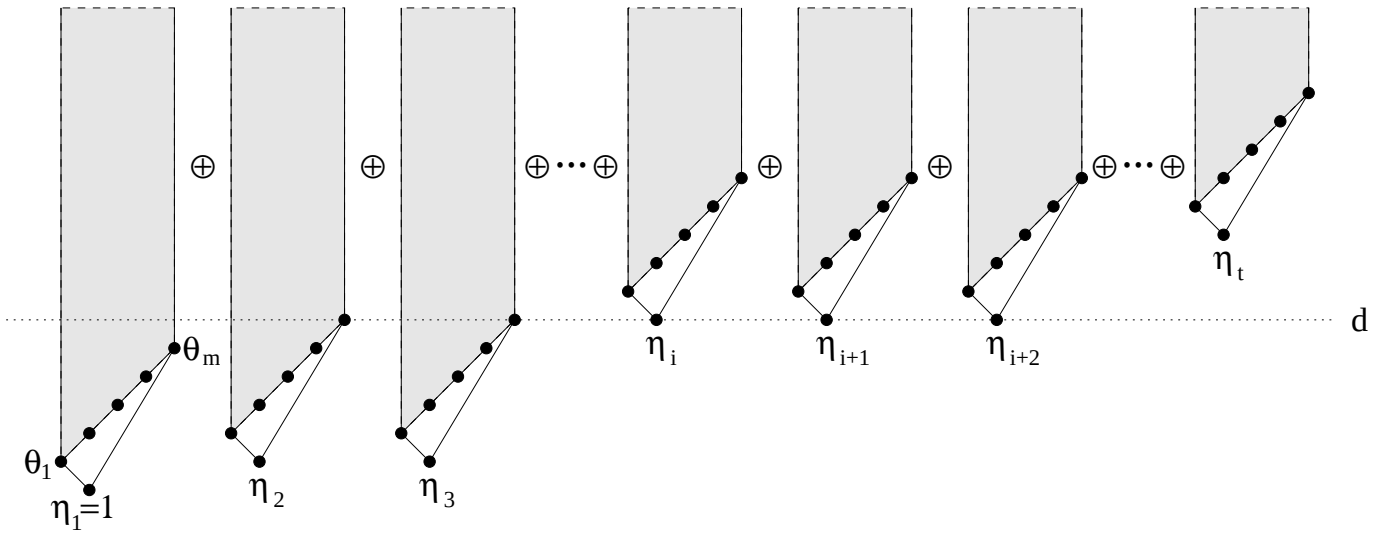


FIG. 8.1 – Décomposition de Hironaka de l'algèbre des invariants
Le bloc le plus à gauche est l'algèbre engendrée par les primaires. L'idéal engendré par les primaires est en grisé. Les polynômes n_i, n_{i+1}, n_{i+2} sont une base d'un supplémentaire de cet idéal dans l'espace des polynômes invariants homogènes de degré d.

Calculs dans une algèbre de Cohen-Macaulay

La connaissance d'une décomposition de Hironaka présente plusieurs avantages. Tout d'abord, comme la somme est directe, tout polynôme invariant p s'écrit de manière unique sous la forme

$$P_1(\theta_1, \ldots, \theta_m).\eta_1 + \cdots + P_t(\theta_1, \ldots, \theta_m).\eta_t$$

où $P_1, \ldots, P_t$ sont des polynômes. En quelque sorte, les η_i forment une base des polynômes invariants et les coordonnées de p sont les polynômes P_i. Le calcul dans cette base de la somme de deux polynômes p et q est bien entendu trivial :

$$\begin{aligned} p + q &= P_1(\theta_1, \ldots, \theta_m).\eta_1 + \cdots + P_t(\theta_1, \ldots, \theta_m).\eta_t \\ &\quad + Q_1(\theta_1, \ldots, \theta_m).\eta_1 + \cdots + Q_t(\theta_1, \ldots, \theta_m).\eta_t \\ &= (P_1 + Q_1)(\theta_1, \ldots, \theta_m).\eta_1 + \cdots + (P_t + Q_t)(\theta_1, \ldots, \theta_m).\eta_t \end{aligned}$$

De même, comme pourra le vérifier le lecteur, il suffit de connaître la table de multiplication des η_i pour pouvoir calculer n'importe quel produit dans cette base. Il est en effet aisé de calculer pq si l'on connaît l'écriture des produits $\eta_i\eta_j$ dans cette décomposition :

$$\eta_i\eta_j = P_{i,j,1}(\theta_1, \ldots, \theta_m).\eta_1 + \cdots + P_{i,j,t}(\theta_1, \ldots, \theta_m).\eta_t. \tag{8.2}$$

Enfin, ces règles de multiplication définissent certaines syzygies (relations algébriques) entre les générateurs. On montre facilement qu'elles s'obtiennent toutes de cette façon ! Pour être précis, l'idéal des syzygies est engendré par les relations 8.2.

En résumé, la connaissance d'une décomposition de Hironaka et de la table de multiplication correspondante donne une description très complète de l'algèbre.

Systèmes de paramètres

Voyons maintenant comment se caractérisent les invariants primaires et secondaires d'une décomposition de Hironaka. Pour cela, nous avons besoin d'une dernière définition.

Définition 8.1.23 (Système de paramètres homogènes).
Un ensemble de m polynômes invariants homogènes $\theta_1, \ldots, \theta_m$ est un système de paramètres homogènes *ou* système de paramètres*, si l'algèbre des invariants est un module libre de type fini sur $\mathbb{C}[\theta_1, \ldots, \theta_m]$, autrement dit, si $\theta_1, \ldots, \theta_m$ apparaissent comme invariants primaires dans une décomposition de Hironaka de $\mathbb{C}[\mathbf{x}]^G$.*

On peut caractériser comme suit les systèmes de paramètres :

Caractérisation 8.1.24.
Un ensemble de m polynômes invariants homogènes est un système de paramètres si, et seulement si, 0 est la seule solution dans $\mathbb{C}^m$ commune à tous les polynômes.

Sturmfels propose un test mécanique basé sur un calcul de base de Gröbner.

Proposition 8.1.25 ([Stu93, Subroutine 2.5.2]).
Soit $p_1, \ldots, p_m$ un ensemble de polynômes invariants homogènes. Soit G une base de Gröbner de l'idéal $\langle p_1, \ldots, p_m \rangle_{\mathbb{C}[\mathbf{x}]}$, pour un ordre monomial quelconque. La seule solution de $p_1 = p_2 = \cdots = p_m = 0$ est 0 si, et seulement si, pour toute variable x_i, un monôme de la forme $x_i^{d_i}$ apparaît parmi les monômes initiaux de G.

Notons tout de même que, si cette caractérisation est simple sur le papier, elle est coûteuse dans la pratique. Le calcul de base de Gröbner peut en effet devenir rapidement impraticable (il y aura au § 11.3.1 une discussion sur le sujet, basée sur notre expérience avec l'algèbre des invariants sur les graphes). En dehors de cela, il n'y a pas de méthode générale pour traiter ce genre de problèmes.

Invariants secondaires

Fixons maintenant un système de paramètres $(\theta_1, \ldots, \theta_m)$. Il suffit de connaître les degrés des polynômes qui le composent, pour avoir des informations *a priori* sur les secondaires. On peut par exemple calculer leur nombre et leurs degrés à partir de la série de Hilbert.

Théorème 8.1.26 ([Sta79, § 3]).
Soit $(\theta_1, \ldots, \theta_m)$ un système de paramètres de degrés respectifs $d_1, \ldots, d_m$, et soit $(\eta_1, \ldots, \eta_t)$ un système d'invariants secondaires de degrés respectifs $e_1, \ldots, e_t$. Enfin, soit μ le plus petit degré d'un polynôme invariant relatif au caractère $\det^{-1}$. On a :

$$\sum_{i=1}^{t} z^{e_i} = H(\mathbb{C}[V]^G, z)(1 - z^{d_1}) \cdots (1 - z^{d_m})$$

$$t = \frac{d_1 d_2 \ldots d_m}{|G|}$$

$$e_t = d_1 + d_2 + \cdots + d_m - m - \mu$$

On montre la première formule en remarquant que la série de Hilbert de la composante $\eta_i.\mathbb{C}[\theta_1, \ldots, \theta_m]$ est

$$\frac{z^{e_i}}{(1-z^{d_1})\cdots(1-z^{d_m})}$$

et que la série de Hilbert d'une somme directe d'espaces est la somme des séries de Hilbert de ces espaces. La seconde formule se déduit de l'étude asymptotique de la série de Hilbert lorsque z tend vers 1. Pour la dernière formule on utilise la dualité entre invariants et invariants relatifs au caractère $\det^{-1}$, donnée par l'équation 8.1. Pour plus de détails, voir [Sta79, § 3].

Ce théorème donne une majoration de la borne sur les degrés d'un système générateur

$$\beta(\mathbb{C}[\mathbf{x}]^G) \leq \min(d_i, d_1 + d_2 + \cdots + d_m - m). \tag{8.3}$$

Les secondaires sont caractérisés comme suit :

Caractérisation 8.1.27.
Soit $(\theta_1, \ldots, \theta_m)$ un système de paramètres de $\mathbb{C}[\mathbf{x}]^G$. Soit $\langle\theta_1, \ldots, \theta_m\rangle$ l'idéal qu'ils engendrent dans $\mathbb{C}[\mathbf{x}]^G$. Les polynômes $(\eta_1, \ldots, \eta_t)$ forment un système d'invariants secondaires si, et seulement si, $(\eta_1, \ldots, \eta_t)$ est une base de l'espace vectoriel quotient $\mathbb{C}[\mathbf{x}]^G/\langle\theta_1, \ldots, \theta_m\rangle$.

Démonstration. On procède degré par degré, le principe de la démonstration apparaissant clairement sur la figure 8.1 page 104. □

Il existe des algorithmes pour calculer des systèmes d'invariants secondaires (voir [Stu93, Kem98b]). Ces algorithmes sont implémentés dans la plupart des systèmes de calculs dans les anneaux d'invariants [Kem93, Kem96]. De plus, il est possible d'extraire de ces systèmes, des systèmes générateurs presque minimaux :

Définition 8.1.28 (Système d'invariants secondaires irréductibles).
On appelle système d'invariants secondaires irréductibles *un sous-ensemble S d'un système d'invariants secondaires, minimal pour l'inclusion, tel que tous les autres polynômes secondaires s'expriment comme combinaison polynomiale des éléments de S et des primaires.*

Soit S la réunion d'un système $(\theta_1, \ldots, \theta_m)$ d'invariants primaires et d'un système d'invariants secondaires irréductibles correspondant. C'est un système générateur de l'algèbre des invariants, qui est minimal pour l'inclusion parmi tous les systèmes générateurs contenant $(\theta_1, \ldots, \theta_m)$. On peut modifier, sans surcoût notable, les algorithmes de calculs d'invariants secondaires pour qu'ils donnent un tel système d'invariants secondaires irréductibles comme sous-produit (voir [Kem96]).

8.2 Invariants d'une représentation par permutation

8.2.1 Introduction et références

La deuxième caractéristique fondamentale de notre représentation est d'être une représentation par permutation. *A priori*, l'intérêt de l'utilisation des polynômes

invariants est de traduire et de traiter algébriquement des problèmes sur certains objets combinatoires (ici les graphes). Nous allons voir que, réciproquement, un certain nombre de questions sur l'algèbre des invariants ont des interprétations combinatoires et peuvent être traitées avec des outils combinatoires. Ne risquons-nous pas de tourner en rond ? Probablement pas. Ce va-et-vient entre les deux langages permet d'envisager les questions sous plusieurs angles ; il permet aussi de trouver des liens entre des problèmes à l'intérieur d'un même langage, que l'on n'aurait pas remarqués sans ce détour.

Cette interaction entre algèbre et combinatoire est bien mise en valeur dans les articles [Sta79, § 10] et [GS84]. Dans [Stu93], Sturmfels consacre aussi quelques pages aux algorithmes particuliers pour les représentations par permutation.

8.2.2 Définitions et propriétés

Définition 8.2.1 (Représentation par permutation).
Soit V une représentation d'un groupe G. La représentation V est dite par permutation *s'il existe une base $(\mathbf{e}_1, \dots, \mathbf{e}_m)$ de V telle que G agisse en permutant les éléments de cette base. G est alors un sous-groupe du groupe $\mathfrak{S}_m$ de toutes les permutations de $\{1, \dots, m\}$, et on dit que G est un* groupe de permutations*.*

Par exemple, la représentation naturelle du groupe symétrique $\mathfrak{S}_m$ sur $\mathbb{C}^m$ est une représentation par permutation des vecteurs de la base canonique. De même, la représentation du groupe symétrique $\mathfrak{S}_n$ sur l'espace vectoriel des graphes $\langle \mathbf{e}_{\{i,j\}} \rangle_{\mathbb{C}}$ est une représentation par permutation de la base des arêtes.

Nous allons commencer par une remarque très simple, mais fondamentale, car elle donne une interprétation combinatoire des polynômes et des polynômes invariants. En particulier, cela nous donnera une écriture concise et visuelle des polynômes invariants et donc un support concret à l'intuition. On peut identifier un monôme $x_1^{\lambda_1} \dots x_m^{\lambda_m}$ avec le vecteur à coordonnées entières positives $\lambda_1.\mathbf{e}_1 + \dots + \lambda_m.\mathbf{e}_m$. Dans notre cas, un monôme est donc un multigraphe. De ce point de vue, un polynôme invariant devient une combinaison linéaire de multigraphes à isomorphie près. Cette identification se comporte par exemple bien avec l'action du groupe.

On définit la *forme d'un multigraphe* comme la liste $(\lambda_0, \lambda_1, \lambda_2, \dots)$ où λ_i compte le nombre d'arêtes valuées i du multigraphe. Cette forme est préservée par l'action du groupe symétrique.

Polynômes symétriques

Définition 8.2.2 (Polynôme symétrique).
On appelle polynôme symétrique *un polynôme qui reste inchangé par toute permutation des variables. Nous insistons sur la différence avec polynôme invariant pour lequel on ne considère que les permutations qui sont dans G. Bien entendu un polynôme symétrique est* a fortiori *invariant.*

Voici quelques exemples de polynômes symétriques.

Exemples 8.2.3.
– *Fonctions symétriques puissances :* $p_d = \sum x_i^d$;

– *Polynômes symétriques élémentaires :* $e_d = \sum_{i_1<i_2,\dots,i_d} x_{i_1}x_{i_2}\dots x_{i_d}$.

On rappelle le théorème fondamental des polynômes symétriques.

Théorème 8.2.4 ([Stu93, théorème 1.1.1, p. 2]).
Les polynômes symétriques élémentaires de degrés $1,\dots,m$ *sont algébriquement indépendants, et engendrent l'algèbre* $\mathbb{C}[\mathbf{x}]^{\mathfrak{S}_m}$ *des polynômes symétriques. Il en est de même pour les fonctions symétriques puissance de degré* $1,\dots,m$.

On remarque que l'on peut interpréter le polynôme e_d comme la somme de toutes les exponentielles symétrisées de graphes à d arêtes. De même, si l'on se fixe une forme λ, la somme de toutes les exponentielles symétrisées de multigraphes de forme λ est un polynôme symétrique.

Proposition 8.2.5 ([Stu93, théorème 2.7.6, p 72]).
Les m *polynômes symétriques élémentaires forment un système de paramètres. De plus, on a*

$$t = \frac{m!}{|G|} \qquad et \qquad e_t = \mathrm{C}_m^2 - m,$$

où t *est le nombre d'invariants secondaires,* e_t *est le plus haut degré d'un invariant secondaire, et* m *est le plus petit degré d'un polynôme invariant relatif au signe (* i.e. *tel que* $\sigma.P = \mathrm{sign}(\sigma)P$ *pour* $\sigma \in G$*).*

La borne $\beta(\mathbb{C}[\mathbf{x}]^G)$ *sur les degrés des générateurs est majorée par* C_m^2.

Démonstration. Les polynômes symétriques élémentaires sont invariants, et vérifient la caractérisation 8.1.24. Il suffit d'appliquer le théorème 8.1.26 pour obtenir le nombre et le degré maximal des secondaires. On en déduit immédiatement la majoration de la borne sur les degrés des générateurs. □

On peut donner concrètement un ensemble générateur. On appelle *monôme sous l'escalier* un monôme $x_1^{\nu_1}\dots x_m^{\nu_m}$ avec $0 \le \nu_i < i$. Il y en a $n!$, tous de degré inférieur à C_m^2.

Théorème 8.2.6 ([Stu93, théorème 2.7.8, p. 73]).
L'algèbre des invariants est engendrée par $m!+m$ *polynômes de degré inférieur à* C_m^2. *Il s'agit, d'une part, des* m *polynômes symétriques élémentaires de degré* 1 *à* m *et, d'autre part, des monômes sous l'escalier symétrisés par l'opérateur de Reynolds.*

Nous verrons aussi au § 10.3 que l'on peut calculer la série de Hilbert beaucoup plus efficacement pour les groupes de permutations, en se ramenant à une énumération de Pólya.

8.3 Invariants d'une représentation non irréductible du groupe symétrique

8.3.1 Introduction et références

Nous connaissons bien la représentation du groupe symétrique sur l'espace vectoriel des graphes, et, en particulier, la décomposition en étoiles et graphes 0-réguliers.

Or, la théorie des représentations nous a habitués à appliquer l'adage « diviser pour régner ». La démarche est de décomposer l'espace en composantes irréductibles, d'obtenir des informations sur les invariants de chacune d'entre elles et enfin de les regrouper. Cependant, pour les invariants, il n'est pas trivial de rassembler les irréductibles et de maintenir la cohésion. Par exemple, Sturmfels pensait que l'on ne pouvait pas exploiter cette décomposition. À notre connaissance, il n'y a que dans l'article d'Aslaksen et al. [ACG96] que ce genre de technique a été utilisé.

Soit G un groupe et V un G-module. Supposons que V se décompose en deux sous-G-modules : $V = V_1 + V_2$. Soient $n, n1, n2$ les dimensions respectives des espaces V, V_1 et V_2. On obtient l'algèbre de tous les polynômes sur V en faisant le produit tensoriel de l'algèbre des polynômes sur V_1 par celle des polynômes sur V_2 :

$$\mathbb{C}[V] = \mathbb{C}[V_1] \otimes \mathbb{C}[V_2].$$

Invariants primaires

Pour les invariants primaires, la démarche fonctionne bien, comme l'indique la remarque suivante.

Remarque 8.3.1: Supposons que $(\theta_{1,1}, \ldots, \theta_{1,n_1})$ (resp. $(\theta_{2,1}, \ldots, \theta_{2,n_1})$) soit un ensemble d'invariants primaires pour V_1 (resp. V_2). Alors $(\theta_{1,1}, \ldots, \theta_{1,n_1}, \theta_{2,1}, \ldots, \theta_{2,n_2})$ est un ensemble d'invariants primaires pour V.

Démonstration. Il suffit d'appliquer la caractérisation 8.1.24. Soit $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2 \in V$ tel que

$$\theta_{1,1}(\mathbf{x}) = \cdots = \theta_{1,n_1}(\mathbf{x}) = \theta_{2,1}(\mathbf{x}) = \ldots, \theta_{2,n_2}(\mathbf{x}) = 0$$

On a alors $\theta_{1,1}(\mathbf{x}_1) = \cdots = \theta_{1,n_1}(\mathbf{x}_1) = 0$ donc $\mathbf{x}_1 = 0$. De même $\mathbf{x}_2 = 0$. Donc $\mathbf{x} = 0$. Enfin, le nombre total d'invariants $n_1 + n_2 = n$ est bien égal à la dimension de V. □

Dans la section 11.3.1, nous utiliserons cette décomposition pour la recherche d'invariants primaires.

Invariants secondaires

En revanche, cela ne se passe pas aussi bien pour le reste des polynômes invariants. Le produit d'un invariant sur V_1 par un invariant sur V_2 donne bien un invariant sur V.

Remarque 8.3.2: Si la représentation sur V_1 est la représentation triviale, on obtient tous les polynômes invariants de V par produit tensoriel des invariants de V_1 et de V_2 :

$$\mathbb{C}[V]^G = \mathbb{C}[V_1]^G \otimes \mathbb{C}[V_2]^G = \mathbb{C}[V_1] \otimes \mathbb{C}[V_2]^G.$$

Par contre, si V_1 n'est pas la représentation triviale, on n'obtient pas forcément tous les invariants de la sorte. Voici un exemple symptomatique :

Exemple 8.3.3.
Soit $\mathfrak{S}_2 = (\mathrm{id}, t)$ le groupe symétrique sur deux éléments. Soit V et W deux espaces vectoriels de dimension 1 engendrés par $\mathbf{v}$ et $\mathbf{w}$. Prenons la représentation alternée

de $\mathfrak{S}_2$ sur V, c'est-à-dire la représentation telle que $\mathrm{id}.\mathbf{v} = \mathbf{v}$ *et* $t.\mathbf{v} = -\mathbf{v}$. *De même pour W. Soient $\mathbb{C}[\mathbf{x}]$ et $\mathbb{C}[\mathbf{y}]$ les algèbres des polynômes sur V et W. Les polynômes invariants de $\mathbb{C}[\mathbf{x}]$ sont 1, x^2, x^4, ... De même les polynômes invariants de $\mathbb{C}[\mathbf{y}]$ sont 1, y^2, y^4, ... Par produit, on obtient les polynômes x^2y^2, x^4y^2, ... qui sont bien invariants sur $V \oplus W$. En revanche, le polynôme xy est invariant sur $V \oplus W$, mais ne peut pas être obtenu à partir des invariants sur V et W.*

8.3.2 Une méthode de construction des invariants à partir de la décomposition en irréductibles

En nous inspirant de [ACG96], nous proposons une méthode de construction des invariants. Nous n'avons cependant pas encore réussi à l'appliquer complètement à l'algèbre des invariants sur les graphes. De manière informelle, le principe est le suivant. Soit p_1 (resp. p_2) un polynôme sur l'espace vectoriel V_1 (resp. V_2). Supposons que le groupe agisse de la même façon sur p_1 et p_2. On peut alors faire une convolution entre p_1 et p_2, de sorte que les deux actions s'annihilent. Le résultat de cette convolution est un polynôme invariant, et on peut obtenir de cette façon tous les polynômes invariants.

Les représentations du groupe sur V_1 et V_2 induisent respectivement des représentations sur les espaces de polynômes $\mathbb{C}[V_1]$ et $\mathbb{C}[V_2]$.

Théorème 8.3.4.
Les invariants de V sont en bijection avec les morphismes de G-modules de $\mathbb{C}[V_1]$ dans $\mathbb{C}[V_2]$.

Démonstration. Soient U_1 et U_2 deux G-modules. On recherche les éléments invariants de $U_1 \otimes U_2$. On rappelle que l'on peut toujours munir U_1 (et U_2) d'un produit scalaire invariant. Pour cela, il suffit de prendre un produit scalaire $\langle .|. \rangle$ quelconque sur U_i et de le rendre invariant en posant

$$\langle \mathbf{v}|\mathbf{w}\rangle^* := \frac{1}{|G|}\sum_{\sigma\in G}\langle \sigma\mathbf{v}|\sigma\mathbf{w}\rangle.$$

Soit $\overline{U}_1$ le dual de U_1, que l'on munit de l'action $\sigma.v = v \circ \sigma^{-1}$. Le produit scalaire invariant fournit un isomorphisme de G-modules entre U_1 et $\overline{U}_1$. On a donc un isomorphisme de G-modules :

$$\begin{cases} U_1 \otimes U_2 \to \overline{U}_1 \otimes U_2 \\ \mathbf{v}_1 \otimes \mathbf{v}_2 \mapsto \overline{\mathbf{v}}_1 \otimes \mathbf{v}_2 \end{cases}.$$

Or, un élément f de $\overline{U}_1 \otimes U_2$ représente une application linéaire de U_1 dans U_2. Comme $\sigma.f = \sigma \circ f \circ \sigma^{-1}$, l'application f est invariante si, et seulement si, f commute avec l'action du groupe. Autrement dit, si f est un morphisme de G-modules de U_1 dans U_2. □

Il nous faut donc chercher les morphismes de G-modules de $\mathbb{C}[V_1]$ dans $\mathbb{C}[V_2]$. Pour cela, il faut décomposer ces deux espaces en composantes isotypiques (voir section 8.1.4). Le lemme de Schur assure alors que les composantes isotypiques de $\mathbb{C}[V_1]$ sont envoyées sur celles de $\mathbb{C}[V_2]$.

Il n'est pas nécessaire de décomposer toute l'algèbre $\mathbb{C}[V]$ des polynômes. De fait, les composantes isotypiques ont des propriétés proches de celles de l'algèbre des invariants. En particulier, elles admettent aussi une décomposition de Hironaka sur les invariants primaires (θ_i). On peut donc se contenter de décomposer $\mathbb{C}[V]/\langle\theta_i\rangle$ en composantes isotypiques. Le théorème suivant décrit complètement à isomorphie près ce quotient.

Théorème 8.3.5 ([Sta79, p.489]).
L'algèbre des polynômes quotientée par les primaires, $\mathbb{C}[V]/\langle\theta_i\rangle$, est isomorphe à t fois la représentation régulière du groupe de matrices G, où t est le nombre d'invariants secondaires.

Note 8.3.6: La précision « groupe de matrices » est essentielle ici. Par exemple, pour $n = 4$, la représentation de $\mathfrak{S}_4$ sur les graphes 0-réguliers n'est pas fidèle. Le groupe de matrices que l'on obtient est en fait isomorphe à $\mathfrak{S}_3$. On obtient donc la représentation régulière de $\mathfrak{S}_3$ et non celle de $\mathfrak{S}_4$.

Cela fait partie des particularités du cas $n = 4$. À partir de $n \geq 5$, la représentation est fidèle sur les étoiles et les graphes 0-réguliers.

La démonstration de ce théorème n'est pas constructive. Elle repose entièrement sur des considérations de dimensions, via l'étude des séries de Hilbert des invariants relatifs.

La fin de la méthode consiste à localiser ces composantes isotypiques dans $\mathbb{C}[V_1]$ et $\mathbb{C}[V_2]$, en donner des bases adaptées, construire les G-morphismes et, enfin, traduire ces derniers en invariants avec le théorème 8.3.4.

Quelques remarques sur l'application aux graphes

Dans notre cas, on prendrait *a priori* $V_1 = [n] \oplus [n-1,1]$ et $V_2 = [n-2,2]$. La composante $[n]$ correspondant au graphe complet est sans grande importance. La représentation étant triviale, la rajouter revient simplement à prendre le produit tensoriel des invariants par $\mathbb{C}[\mathbf{x}]$ (voir remarque 8.3.2).

Au § 10.3 nous raffinerons le calcul de la série de Hilbert en une série multigraduée, de façon à obtenir plus d'informations sur la répartition des invariants entre les deux composantes.

Nous pouvons donner quelques informations supplémentaires sur la composante $[n] \oplus [n-1,1]$. Il s'agit bien sûr de la représentation naturelle du groupe symétrique par permutation des étoiles. Les polynômes invariants sont les polynômes symétriques. On peut choisir comme invariants primaires les polynômes symétriques élémentaires et le seul invariant secondaire est 1. Soit A le quotient de $\mathbb{C}[\mathbf{x}]$ par les primaires. D'après le théorème 8.3.5, A est isomorphe à la représentation régulière de $\mathfrak{S}_n$. Il existe plusieurs bases simples de A en tant qu'espace vectoriel : monômes sous l'escalier, monômes de descentes (voir [GS84], repris dans [Stu93, p. 73]). Cependant, ces bases ne sont pas adaptées à la décomposition en composantes isotypiques. Garsia et Stanton [GS84, p. 195] donnent un algorithme permettant de calculer une base adaptée. Cet algorithme fonctionne en fait pour n'importe quelle représentation par permutation de $\mathfrak{S}_n$. Mais nous ne savons pas s'il peut être implémenté efficacement.

Quelques pistes pour construire cette base : utiliser comme guide le théorème de Lusztig [Sta79, p.490], permettant d'exprimer combinatoirement la dimension de

chaque composante isotypique par degré, et chercher les relations avec les polynômes de Schubert [Mac91, Ker91].

8.4 Sous-groupes de $SL_m(\mathbb{C})$ et algèbres de Gorenstein

8.4.1 Introduction et références

En plus des propriétés précédentes, nous avons remarqué que, lorsque n est pair, notre représentation est un sous-groupe de $SL_m(\mathbb{C})$. En revanche, lorsque n est impair, c'est la représentation sur les graphes 0-réguliers qui est un sous-groupe de $SL_m(\mathbb{C})$. La théorie nous indique alors que l'algèbre des invariants correspondants est de Gorenstein.

C'est – paraît-il – une très jolie propriété. Elle exprime une dualité dans cette algèbre, qui s'exprime apparaît à plusieurs niveaux. Pour le moment, nous n'en avons pas trouvé d'applications concrètes et ce qui suit est essentiellement d'ordre esthétique. Nous indiquons cependant quelques conséquences qui pourraient s'avérer utiles, en particulier pour la recherche d'invariants secondaires.

8.4.2 Quelques propriétés de la représentation sur les graphes

Nous avons besoin de quelques informations techniques sur la représentation sur les graphes. Elles sont résumées dans les lemmes suivants.

Lemme 8.4.1.
Soit $\sigma \in \mathfrak{S}_n$ une permutation des sommets. Le déterminant de sa matrice de représentation vaut

sur les graphes :

$$\det(\sigma) = \begin{cases} 1 & \text{si } n \text{ est pair}, \\ \operatorname{sign}(\sigma) & \text{si } n \text{ est impair}; \end{cases} \tag{8.4}$$

sur les étoiles :

$$\det(\sigma) = \operatorname{sign}(\sigma); \tag{8.5}$$

sur les graphes 0-réguliers :

$$\det(\sigma) = \begin{cases} \operatorname{sign}(\sigma) & \text{si } n \text{ est pair}, \\ 1 & \text{si } n \text{ est impair}. \end{cases} \tag{8.6}$$

Démonstration. Soit U une représentation du groupe symétrique. L'application qui associe à chaque permutation le déterminant de sa matrice de représentation est un morphisme de $\mathfrak{S}_n$ dans $\mathbb{C}$. Or, il n'existe que deux morphismes de $\mathfrak{S}_n$ dans $\mathbb{C}$:

l'application constante 1 et la signature sign. Pour les distinguer, il suffit d'étudier le cas d'une transposition élémentaire.

Soit t la transposition des sommets 1 et 2. L'arête $\{1,2\}$ et les arêtes à sommets dans $\{3,\ldots,n\}$ sont fixes. Les arêtes $\{1,i\}$ et $\{2,i\}$ avec $i \geq 3$ sont échangées. Il y a donc $n-2$ cycles de longueur 2. La signature de la permutation correspondante des arêtes est donc $(-1)^{n-2}$. En conclusion : si n est pair, $det(\sigma) = 1$, sinon $\det(\sigma) = \mathrm{sign}(\sigma)$.

Sur les étoiles, le déterminant est $\mathrm{sign}(\sigma)$ puisqu'il s'agit de la représentation naturelle de $\mathfrak{S}_n$.

Enfin, pour calculer le déterminant sur les graphes 0-réguliers, il suffit de remarquer que les étoiles et les graphes 0-réguliers sont supplémentaires dans l'ensemble des graphes. Le déterminant total est donc égal au produit des déterminants sur chaque composante. □

Lemme 8.4.2.
Pour $n > 3$, le groupe de matrices de la représentation sur les graphes à n sommets ne contient pas de pseudo-réflexion.

Démonstration. Les seules matrices de permutations qui sont des pseudo-réflexions correspondent aux transpositions. En effet, le polynôme caractéristique d'un cycle de longueur k est $1 - X^k$. Donc chaque cycle de longueur $k > 1$ de la permutation induit $k-1$ valeurs propres différentes de 1. Pour qu'il n'y ait en tout qu'une seule valeur propre différente de 1, il faut qu'il y ait exactement 1 cycle de longueur 2, tous les autres cycles étant de longueur 1.

Lorsque $n > 3$, on vérifie aisément qu'aucune permutation des sommet n'induit une transposition de deux arêtes. □

8.4.3 Caractérisations des algèbres de Gorenstein et applications

Pour une définition précise d'une algèbre de Gorenstein, nous renvoyons à [Sta79, § 8] d'où proviennent les théorèmes et caractérisations qui suivent. Pour les algébristes, un traitement complet peut être trouvé dans [Eis95, ch. 21]. Cette définition est basée essentiellement sur une auto-dualité de la résolution libre minimale d'une algèbre (les syzygies de première espèce sont isomorphes aux syzygies de dernière espèce, et ainsi de suite). Pour ce qui nous intéresse, voici quelques caractérisations des algèbres d'invariants de Gorenstein :

Caractérisation 8.4.3 ([Sta79]).
Les propositions suivantes sont équivalentes :
(i) $\mathbb{C}[V]^G$ est de Gorenstein ;
(ii) La série de Hilbert est réciproque :

$$H(C[x]^G, \frac{1}{z}) = (-1)^m z^{m+r} H(C[x]^G, z),$$

où m est la dimension de V et r le nombre de pseudo-réflexions dans le groupe de matrices G ;

(iii) Pour tout choix d'invariants primaires, la série génératrice des secondaires est un polynôme réciproque.

Théorème 8.4.4 (Watanabee 1974 [Sta79]).
Si G est un sous-groupe de $SL_m(\mathbb{C})$ – i.e. *$det(M) = 1$ pour tout $M \in G$* – *alors l'algèbre des invariants $\mathbb{C}[V]^G$ est de Gorenstein.*

Réciproquement, si $\mathbb{C}[V]^G$ est de Gorenstein et si G ne contient pas de pseudo-réflexions, alors G est un sous-groupe de $SL_m(\mathbb{C})$.

Corollaire 8.4.5.
L'algèbre des polynômes invariants sur les graphes est de Gorenstein si, et seulement si, n est pair.

L'algèbre des polynômes invariants sur les graphes 0-réguliers est de Gorenstein si, et seulement si, n est impair.

8.4.4 Conséquences

Ce corollaire donne des informations assez spécifiques sur les polynômes secondaires. Tout d'abord, le caractère $\det^{-1}$ et le caractère trivial coïncident. Donc $\mathbb{C}[V]^G = \mathbb{C}[V]^G_{\det^{-1}}$. La dualité donnée par l'équation 8.1 est donc une auto-dualité. En particulier, il y a un invariant relatif à $\det^{-1}$ de degré 0, ce qui permet de simplifier l'expression du degré e_t maximal d'un invariant secondaire (théorème 8.1.26).

$$e_t = d_1 + d_2 + \cdots + d_m - m \tag{8.7}$$

La caractérisation 8.4.3 nous indique qu'il y a autant d'invariants secondaires de degré d que d'invariants secondaires de degré $e_t - d$. En particulier, il y a exactement un invariant secondaire de degré e_t. De fait, il est important de pouvoir construire effectivement une bijection, car d'un point de vue algorithmique, les conséquences sont considérables. Il suffit en effet de construire les invariants secondaires jusqu'au degré $e_t/2$, et les autres s'obtiennent immédiatement. Le gain est bien plus que de la moitié, puisque cela permet de travailler uniquement dans les petits degrés. Pour donner un ordre de grandeur, voici quelques statistiques pour $n = 6$. Le degré maximal d'un invariant secondaire est $e_t = 60$. Au niveau 30 le nombre total d'invariants est de l'ordre de $1,6.10^8$ contre $6,3.10^{11}$ au niveau 60. On note cependant que cette technique permet seulement de construire les secondaires de hauts degrés, et non pas les générateurs minimaux.

Dualité et opérateurs différentiels

On construit cette bijection de la manière suivante : soit ∂_i l'opérateur $\frac{\partial}{\partial x_i}$ de différentiation par rapport à la variable x_i. On note que les opérateurs ∂_i commutent : $\partial_1\partial_2 = \partial_2\partial_1$. Étant donné un polynôme p, on note $p(\partial)$ l'opérateur différentiel obtenu en substituant x_i par ∂_i. On vérifie alors que si p et q sont deux polynômes invariants, alors $p(\partial)q$ est aussi un polynôme invariant. Si p et q sont homogènes alors $\deg p(\partial)q = \deg q - \deg p$. Soit $\Delta := \prod_{i<j}(x_i - x_j)$ le déterminant de Vandermonde des variables. Par construction, Δ est antisymétrique. Comme la représentation est par permutation et que toutes les permutations sont paires, Δ est un polynôme invariant. Donc, pour tout p, le polynôme $p(\partial)\Delta$ est invariant.

Théorème 8.4.6.
L'application $p \mapsto p(\partial)\Delta$ est un automorphisme de $\mathbb{C}[\mathbf{x}]^G/\langle\theta_1,\ldots,\theta_m\rangle$ qui envoie la composante homogène de degré d sur la composante homogène de degré $e_t - d$.

Nous n'avons pas encore utilisé concrètement ce type d'outils, et nous renvoyons donc à [GH94] pour plus de détails.

Dualité et produit scalaire

Cette dualité apparaît aussi sous la forme d'un produit scalaire entre les niveaux d et $e_t - d$. Soit η_i et η_j deux invariants secondaires de degrés respectifs d et $e_t - d$. Le polynôme $\eta_i\eta_j$ est un invariant de degré e_t, et s'écrit comme suit dans la décomposition de Hironaka :

$$\eta_i\eta_j = p_1(\theta_i)\eta_1 + p_2(\theta_i)\eta_2 + \cdots + p_t(\theta_i)\eta_t$$

En raison du degré, le coefficient $\lambda := p_t(\theta_i)$ est une constante. Posons $\langle\eta_i|\eta_j\rangle := \lambda$. Cela définit une forme bilinéaire. La théorie des anneaux de Gorenstein nous indique qu'elle est bien non dégénérée [Eis95, Ch. 21, Ex. 21.9, p. 547-548].

Enfin, pour conclure, cette propriété peut permettre de construire des arguments *ad hoc* pour montrer qu'un ensemble de générateurs est minimal (voir [Dix91, Lemme 1.6 et applications]).

8.5 Quelques propriétés de la représentation de $\mathfrak{S}_n$ sur les graphes

Nous concluons avec quelques propriétés de notre groupe que nous n'avons pas eu l'occasion d'exploiter jusqu'ici. Soit $\mathfrak{S}_m$, $m := \mathrm{C}_n^2$, le groupe des permutations τ des arêtes du graphe complet à n sommets (c'est-à-dire des paires $\{i,j\}$ de $\{1,\ldots,n\}$). Soit G le sous-groupe des permutations $\tilde{\sigma}$ induites par les permutations σ des sommets.

On dit qu'une permutation τ des arêtes *préserve l'adjacence* si les images par τ de deux arêtes adjacentes sont adjacentes. Il est clair qu'une permutation des arêtes induite par une permutation des sommets préserve l'adjacence. De plus, l'ensemble des permutations qui préservent l'adjacence est un sous-groupe de $\mathfrak{S}_m$. La stabilité par composition est claire. Soit τ une permutation préservant l'adjacence. Elle fournit une injection f de l'ensemble des couples d'arêtes adjacentes dans lui-même. Cette application f est forcément bijective, c'est-à-dire que l'image réciproque par τ^{-1} d'un couple d'arêtes adjacentes est un couple d'arêtes adjacentes. Donc l'inverse de τ préserve aussi l'adjacence.

Proposition 8.5.1.
On se place dans le cas $n \geq 5$.

(i) G est exactement le sous-groupe des permutations de $\mathfrak{S}_m$ qui préservent l'adjacence.

(ii) G est son propre normalisateur. En particulier, G n'est pas un sous-groupe distingué de $\mathfrak{S}_m$.

(iii) Soit H un sous-groupe de $\mathfrak{S}_m$. Si $G \subset H \subset \mathfrak{S}_m$ et si H est engendré par des pseudo-réflexions, alors $H = \mathfrak{S}_m$.

Pour $n = 3$, les groupes G et $\mathfrak{S}_m$ sont de même cardinal 6, donc toutes les permutations des arêtes préservent l'adjacence, et G est distingué dans $\mathfrak{S}_m$. Par contre, pour $n = 4$, la transposition des arêtes $\{1, 2\}$ et $\{3, 4\}$ préserve l'adjacence, mais n'est pas induite par une permutation des sommets.

Dans (iii), on voit $\mathfrak{S}_m$ comme un groupe de matrices de permutations. Une pseudo-réflexion est donc une permutation dont la matrice de permutation est une pseudo-réflexion. En utilisant les propriétés du corps des fractions invariantes (cf §Inv.fractions, corollaire 9.1.7), on peut déduire de (iii) qu'il n'y a pas d'algèbre d'invariants engendrée par des polynômes algébriquement indépendants intermédiaire entre l'algèbre des polynômes symétriques et l'algèbre des invariants sur les graphes.

Démonstration de (i). Supposons $n \geq 5$. Soient i un sommet, E_i l'ensemble des $n-1$ arêtes adjacentes à i, et $\tau(E)$ les images par τ de ces arêtes. Les arêtes de $\tau(E)$ sont deux à deux adjacentes, et en nombre supérieur à 4. Elles ont donc un sommet j commun (c'est clair sur un dessin, ou en utilisant la propriété de Helly). Ce sommet est unique, puisque l'intersection de deux arêtes distinctes contient au plus un sommet. On a donc $\tau(E_i) = E_j$. Posons $\sigma(i) = j$. La permutation σ est clairement bijective, puisque l'on peut construire son inverse, en utilisant $\tau^{-1}(E_j)$, pour j un sommet quelconque. Comme l'arête $\{i, j\}$ appartient aux deux ensembles E_i et E_j, son image $\tau(\{i, j\})$ appartient aux deux ensembles $E_{\sigma(i)}$ et $E_{\sigma(j)}$. On en déduit que $\tau(\{i, j\}) = \{\sigma(i), \sigma(j)\}$, c'est-à-dire que τ est la permutation $\tilde{\sigma}$ des arêtes induite par σ. □

Démonstration de (ii). Soit τ une permutation des arêtes qui n'est pas dans G. Il faut montrer qu'il existe une permutation $\tilde{\sigma}$ de G telle que la permutation $\tau\tilde{\sigma}\tau^{-1}$ n'appartient pas à G.

D'après (i), τ ne préserve pas l'adjacence. Soient e et e' deux arêtes adjacentes distinctes dont les images ne sont pas adjacentes, et soit i le sommet commun à e et e'. Soit E_i l'ensemble des arêtes adjacentes à i, et $\tau(E)$ l'image de ces arêtes. Par construction, c'est un graphe à $n-1$ arêtes tel qu'il existe deux arêtes non-adjacentes. D'un autre côté, toutes les arêtes de ce graphe ne peuvent pas être disjointes, car $2(n-1) > n$. On peut donc choisir 3 arêtes f_1, f_2, f_3 dans $\tau(E)$ telles que f_1 est adjacente à f_2, et f_1 n'est pas adjacente à f_3. Soient $e_1 = \{i, j_1\}, e_2 = \{i, j_2\}, e_3 = \{i, j_3\}$ les antécédents de ces arêtes. Enfin, soit σ la transposition (i_2, i_3) des sommets. On a alors (voir figure 8.2 page ci-contre) :

$$\tau\tilde{\sigma}\tau^{-1}(f_1) = f_1 \qquad\qquad \tau\tilde{\sigma}\tau^{-1}(f_2) = f_3$$

Donc $\tau\tilde{\sigma}\tau^{-1}$ ne préserve pas l'adjacence, comme voulu. □

Nous avons noté dans la démonstration du lemme 8.4.2 que les seules permutations de $\mathfrak{S}_m$, dont les matrices de permutation sont des pseudo-réflexions, sont les transpositions (i, j). La démonstration de (iii) se ramène donc au lemme suivant :

Lemme 8.5.2.
Soit H un sous-groupe de $\mathfrak{S}_m$ engendré par des transpositions et agissant transitivement. Alors, $H = \mathfrak{S}_m$.

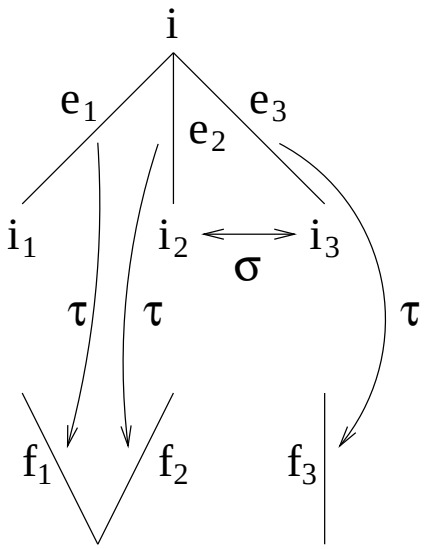


FIG. 8.2 – Construction d'une transposition $\sigma = (i_1, i_2)$ telle que $\tau\tilde{\sigma}\tau^{-1}$ ne préserve pas l'adjacence

Démonstration. Comme le groupe H agit transitivement, l'ensemble $\{1\}$ n'est pas stable par H. Donc H contient une transposition de la forme $(1, i)$. Par symétrie, on peut supposer $i = 2$. Comme $\{1, 2\}$ n'est pas stable, H doit contenir une transposition de forme $(1, i)$ ou $(2, i)$ avec $i > 2$. Par symétrie, on peut supposer $i = 3$. Cette transposition et la transposition $(1, 2)$ engendrent le sous-groupe $\mathfrak{S}_3$ des permutations de $\{1, 2, 3\}$, qui est donc contenu dans H. On montre ainsi de suite que H doit contenir les sous-groupes $\mathfrak{S}_4, \mathfrak{S}_5, \ldots$ et enfin $\mathfrak{S}_m$. □

Ces propriétés suggèrent qu'il existe peu de groupes intermédiaires entre G et $\mathfrak{S}_m$ (bien entendu, si n est pair, G est inclus dans le groupe alterné $\mathcal{A}_m$). De fait, à quelques exceptions près, G est maximal.

Théorème 8.5.3 ([FIKW94]).
Soit $n \notin \{4, 5, 6, 8\}$. Si n est impair (resp. pair), alors le groupe G des permutations des arêtes induites par des permutations des sommets est un sous-groupe maximal de $\mathfrak{S}_m$ (resp. $\mathcal{A}_m$).

L'énoncé originel est plus général et caractérise entièrement les valeurs de n et k pour lesquelles l'action naturelle de $\mathfrak{S}_n$ sur les parties de taille k de $\{1, \ldots, n\}$ induit un sous-groupe maximal de $\mathfrak{S}_{\mathrm{C}_n^k}$ ou $\mathcal{A}_{\mathrm{C}_n^k}$.

En utilisant les propriétés du corps des fractions invariantes (cf §Inv.fractions, corollaire 9.1.7), on en déduit le corollaire suivant :

Corollaire 8.5.4.
Pour $n \neq 4, 5, 6, 8$, il n'existe pas d'algèbre d'invariants intermédiaire entre l'algèbre des polynômes symétriques (resp. alternés, lorsque n est pair) et l'algèbre des invariants sur les graphes.

Chapitre 9

Le corps des fractions invariantes

Il paraît restrictif de ne considérer que des invariants polynomiaux, et non pas, par exemple, des fractions invariantes. Soient $\mathbb{C}(\mathbf{x})$ le corps des fractions de $\mathbb{C}[\mathbf{x}]$, et $\mathbb{C}(\mathbf{x})^G$ le sous-ensemble des fractions invariantes par l'action de G. Il s'agit bien évidemment d'un sous-corps de $\mathbb{C}(\mathbf{x})$, que l'on appelle *corps des fractions invariantes* ou simplement *corps des invariants*. Nous donnons dans cette section une description assez précise de ce corps. En particulier, nous donnons une construction simple d'un système générateur. Enfin, nous montrons qu'on ne peut pas, *a priori*, tirer de cette construction des informations spécifiques sur le problème d'isomorphie, et en particulier sur le problème de reconstruction.

9.1 Corps des fractions invariantes d'un groupe fini

Le théorème suivant donne une première description du corps des invariants.

Théorème 9.1.1 ([Bri96]).
Le corps des fractions invariantes $\mathbb{C}(\mathbf{x})^G$ est le corps des fractions de $\mathbb{C}[\mathbf{x}]^G$. C'est-à-dire que toute fraction invariante s'écrit comme fraction de deux polynômes invariants.

Cet énoncé n'est pas forcément vrai pour un groupe infini. Prenons $\mathbb{C}(x, y)$ sur lequel on fait agir l'application $t : x \mapsto 2x, y \mapsto 2y$. Soit G le groupe (infini) engendré par t. La fraction $\frac{x+y}{x-y}$ est clairement invariante, alors que les seuls polynômes invariants sont les constantes.

La démonstration du théorème, toute simple, utilise à nouveau une moyenne bien choisie sur le groupe.

Démonstration. Soit $f = \frac{p}{q}$ une fraction de $\mathbb{C}(\mathbf{x})$. Supposons que f est invariante. On va montrer que f est le quotient de deux polynômes invariants. On a :

$$f = \frac{p}{q} = \frac{p \prod_{\sigma \in G, \sigma \neq \mathrm{id}} \sigma.q}{\prod_{\sigma \in G} \sigma.q}$$

Soit q' le dénominateur de cette dernière fraction. Par construction, c'est un polynôme invariant. Quant au numérateur, il est égal à $f.q'$ et est donc aussi invariant. □

La recherche de générateurs de $\mathbb{C}[\mathbf{x}]^G$ fournit donc des générateurs de $\mathbb{C}(\mathbf{x})^G$. Pour le corps des fractions invariantes, il existe des systèmes générateurs beaucoup plus petits que pour l'algèbre des invariants. Nous avons rencontré l'énoncé suivant pour la première fois dans [Gri79] à propos du corps des fractions invariantes sur les digraphes, mais il est valable pour le corps des fractions invariantes d'un groupe fini quelconque. Nous rappelons (voir théorème 8.1.17) que la dimension de Krull de l'algèbre des invariants et donc du corps des invariants est m, c'est-à-dire qu'il existe m fractions invariantes algébriquement indépendantes, mais pas $m+1$.

Théorème 9.1.2.

(i) Le corps des fractions invariantes est engendré par $m+1$ fractions invariantes.

(ii) Soit $\theta_1, \ldots, \theta_m$ un système de paramètres de l'algèbre des polynômes invariants. Soit t le nombre total d'invariants secondaires, et soit S un système d'invariants secondaires irréductibles. Alors, il existe un polynôme invariant q combinaison linéaire des polynômes de S tel que la famille $(\theta_1, \ldots, \theta_m, q)$ engendre le corps des fractions invariantes :

$$\mathbb{C}(\mathbf{x})^G = \mathbb{C}(\theta_1, \ldots, \theta_m)[q].$$

Le polynôme q est de degré d au plus égal à la borne $\beta(\mathbb{C}[\mathbf{x}]^G)$. Son polynôme minimal est de degré au plus égal au nombre t d'invariants secondaires.

Ce résultat, essentiellement non-constructif, est un corollaire du théorème de l'élément primitif (théorème 9.1.5, voir aussi [Esc97, p. 90]), et du théorème de Noether sur la dimension de Krull de l'algèbre des invariants (théorème 8.1.17). Donnons les grandes lignes de la démonstration de (i). Soit $(f_1, \ldots, f_m)$ une famille de m fractions invariantes algébriquement indépendantes. Comme le corps $\mathbb{C}(\mathbf{x})^G$ des fractions invariantes et le sous-corps $\mathbb{C}(p_1, \ldots, p_m)$ ont même dimension de Krull, le premier est une extension purement algébrique du second. Le théorème de l'élément primitif affirme alors qu'il existe un élément q, dit *élément primitif* , tel que le corps des fractions invariantes $\mathbb{C}(\mathbf{x})^G$ est engendré par q sur le corps $\mathbb{C}(p_1, \ldots, p_m)$.

$$\mathbb{C}(\mathbf{x})^G = \mathbb{C}(f_1, \ldots, f_m)(q)$$

Il n'existe pas, à notre connaissance, d'algorithme pour construire un tel élément primitif q pour un groupe fini quelconque. Nous allons maintenant détailler la démonstration de (ii), car on peut glaner quelques informations *a priori* sur la forme des systèmes générateurs de $\mathbb{C}(\mathbf{x})^G$, et en particulier sur l'élément primitif q. Nous admettons le lemme suivant, qui est équivalent à la formulation usuelle du théorème de l'élément primitif (voir [Esc97]).

Lemme 9.1.3.
Soit $\mathbf{L}$ une extension de degré fini d'un corps $\mathbf{K}$ de caractéristique zéro. Il n'existe qu'un nombre fini de corps intermédiaires entre $\mathbf{K}$ et $\mathbf{L}$.

Le lemme suivant est élémentaire et a pour but principal de montrer que le corps $C(\mathbf{x})^G$ est une extension de degré fini du corps $\mathbb{C}(\theta_1, \ldots, \theta_m)$.

Lemme 9.1.4.
Soit $(\theta_1, \ldots, \theta_m)$ un système de paramètres de l'algèbre des invariants, et soit $(\eta_1, \ldots, \eta_t)$ un système d'invariants secondaires. La famille $(\eta_1, \ldots, \eta_t)$ engendre $\mathbb{C}(\mathbf{x})^G$ en tant qu'espace vectoriel sur $\mathbb{C}(\theta_1, \ldots, \theta_m)$. En particulier, la dimension de $\mathbb{C}(\mathbf{x})^G$ sur le corps $\mathbb{C}(\theta_1, \ldots, \theta_m)$ est au plus égal au nombre t d'invariants secondaires.

Démonstration. Soit f une fraction invariante. D'après le théorème 9.1.1, elle se met sous la forme $\frac{p}{q}$ où p et q sont deux polynômes invariants. Comme $\mathbb{C}[\mathbf{x}]^G$ est un module libre de type fini sur $\mathbb{C}[\theta_1, \ldots, \theta_m]$, le polynôme q est algébrique sur $\mathbb{C}[\theta_1, \ldots, \theta_m]$, c'est-à-dire qu'il vérifie une équation de la forme

$$\alpha_k q^k + \alpha_{k-1} q^{k-1} + \cdots + \alpha_1 q + \alpha_0 = 0,$$

où les coefficients α_i sont dans $\mathbb{C}[\theta_1, \ldots, \theta_m]$, le coefficient α_0 est non nul et $k > 1$. On en déduit que

$$\frac{1}{q} = -\frac{1}{\alpha_0}(\alpha_k q^{k-1} + \alpha_{k-1} q^{k-2} + \cdots + \alpha_1),$$

et donc que

$$\frac{p}{q} = \frac{1}{\alpha_0}(-\alpha_k p q^{k-1} - \alpha_{k-1} p q^{k-2} - \cdots - p\alpha_1).$$

Le terme entre parenthèses est un polynôme invariant et s'écrit sous la forme $\beta_1\eta_1 + \cdots + \beta_t\eta_t$, où les β_i sont dans $\mathbb{C}[\theta_1, \ldots, \theta_m]$. Donc :

$$f = \frac{p}{q} = \frac{\beta_1}{\alpha_0}\eta_1 + \cdots + \frac{\beta_t}{\alpha_0}\eta_t.$$

Comme les coefficients $\frac{\beta_i}{\alpha_0}$ sont dans le corps $\mathbb{C}(\theta_1, \ldots, \theta_m)$, la fraction invariante f est dans l'espace vectoriel engendré par $\eta_1, \ldots, \eta_t$. □

L'énoncé suivant est une variante de l'énoncé usuel du théorème de l'élément primitif, dans laquelle on précise la forme de q.

Théorème 9.1.5 (de l'élément primitif, variante).
Soit $\mathbf{L}$ une extension de degré fini d'un corps $\mathbf{K}$ de caractéristique zéro tel que $\mathbf{L} = \mathbf{K}(p_1, \ldots, p_k)$. Alors, il existe un élément q, combinaison linéaire des p_i tel que $\mathbf{L} = \mathbf{K}(q) = \mathbf{K}[q]$. Un tel élément est dit primitif.

Démonstration. On rappelle d'abord que, si un élément q est algébrique sur $\mathbf{K}$, alors $\mathbf{K}(q) = \mathbf{K}[q]$. Soit en effet $P = \alpha_k X^k + \cdots + \alpha_1 X + \alpha_0$ le polynôme minimal de q. Par minimalité, P n'est pas divisible par X, et donc $\alpha_0 \neq 0$. On en déduit que $\frac{1}{q}$ est dans $\mathbf{K}[q]$ puisque :

$$\frac{1}{q} = -\frac{\alpha_k}{\alpha_0} q^{k-1} - \cdots - \frac{\alpha_1}{\alpha_0}$$

Supposons que $\mathbf{L} = \mathbf{K}(p_1, p_2)$. Soit $q_\lambda = p_1 + \lambda p_2$ une combinaison linéaire de p_1 et p_2 à coefficients dans K. Le corps $\mathbf{K}(q_\lambda)$ est un corps intermédiaire entre $\mathbf{K}$

et $\mathbf{L}$. Le corps $\mathbf{K}$ étant infini (caractéristique 0), on peut construire une infinité de telles combinaisons linéaires q_λ. Comme il n'y a qu'un nombre fini d'extensions intermédiaires entre $\mathbf{K}$ et $\mathbf{L}$, on peut trouver $q := q_\lambda$ et $q' := q_{\lambda'}$ distincts tels que $\mathbf{K}(q) = \mathbf{K}(q')$. Donc q' s'exprime sous la forme $P(q)$, et on a :

$$p_1 + \lambda p_2 = q \qquad\qquad p_1 + \lambda' p_2 = P(q).$$

Il s'ensuit que $\mathbf{L} = \mathbf{K}(p_1, p_2) = \mathbf{K}(q)$, car p_1 et p_2 s'expriment en fonction de q.

On procède ensuite par récurrence sur k. Supposons que

$$\mathbf{L} = \mathbf{K}(p_1, \ldots, p_k) = \mathbf{K}(p_1, \ldots, p_{k-1})(p_k).$$

Par hypothèse, il existe q', combinaison linéaire de $p_1, \ldots, p_{k-1}$, tel que

$$\mathbf{K}(p_1, \ldots, p_{k-1}) = \mathbf{K}(q')$$

. En raisonnant comme précédemment sur $\mathbf{L} = \mathbf{K}(q', p_k)$, on montre qu'il existe q, combinaison linéaire de q' et de p_k, tel que $\mathbf{L} = \mathbf{K}(q)$.

En fait, tout élément q, combinaison linéaire suffisamment générique de $p_1, \ldots, p_k$, est un élément primitif. □

Démonstration du théorème 9.1.2. Soit $(\theta_1, \ldots, \theta_m)$ un système de paramètres de l'algèbre $\mathbb{C}[\mathbf{x}]^G$ des invariants, et soit $(p_1, \ldots, p_k)$ un système de secondaires irréductibles. Comme $\{\theta_1, \ldots, \theta_m, p_1, \ldots, p_k\}$ est un système générateur de $\mathbb{C}[\mathbf{x}]^G$, on a $\mathbb{C}(\mathbf{x})^G = \mathbb{C}(\theta_1, \ldots, \theta_m)(p_1, \ldots, p_k)$. En appliquant le théorème de l'élément primitif, on en déduit qu'il existe un polynôme q, combinaison linéaire de $(p_1, \ldots, p_k)$, tel que $\mathbb{C}(\mathbf{x})^G = \mathbb{C}(\theta_1, \ldots, \theta_m, q)$. Enfin, comme les p_i sont tous de degré inférieur à $\beta(\mathbb{C}[\mathbf{x}]^G)$ – sinon, ils ne seraient pas irréductibles –, le degré d de q est inférieur à $\beta(\mathbb{C}[\mathbf{x}]^G)$. □

Bien entendu, la théorie de Galois est l'outil principal pour étudier le corps des fractions invariantes, le point central étant la correspondance de Galois [Esc97] :

Théorème 9.1.6.
Soit G un groupe fini. Le corps $\mathbb{C}(\mathbf{x})$ des fractions est une extension normale du corps $\mathbb{C}(\mathbf{x})^G$ des fractions invariantes ; le groupe de Galois de cette extension est le groupe G lui-même. $\mathbb{C}(\mathbf{x})$ est de dimension $|G|$ en tant qu'espace vectoriel sur $\mathbb{C}(\mathbf{x})^G$.

La correspondance $G \mapsto \mathbb{C}(\mathbf{x})^G$ est bijective et contravariante, c'est-à-dire que $G \subset G' \Leftrightarrow \mathbb{C}(\mathbf{x})^G \supset \mathbb{C}(\mathbf{x})^{G'}$.

Dans le cas de l'algèbre des invariants, il est clair que si G et G' sont deux groupes avec $G \subset G'$, l'algèbre des invariants $\mathbb{C}[\mathbf{x}]^G$ contient $\mathbb{C}[\mathbf{x}]^{G'}$. La correspondance de Galois permet de montrer que la réciproque est vraie.

Corollaire 9.1.7.
Soient G et G' deux groupes de matrices de $\mathbb{C}^m$, avec G' fini. Alors G est un sous-groupe de G' si, et seulement si, l'algèbre des invariants $\mathbb{C}[\mathbf{x}]^G$ de G contient l'algèbre des invariants $\mathbb{C}[\mathbf{x}]^{G'}$ de G'.

Le foncteur $G \mapsto \mathbb{C}[\mathbf{x}]^G$ entre les groupes finis de matrices et leurs algèbres d'invariants est une correspondance bijective et contravariante.

Démonstration. On se ramène au corps des fractions invariantes pour appliquer la correspondance de Galois. Le groupe G est un sous-groupe du groupe de Galois $\mathrm{Gal}(\mathbb{C}(\mathbf{x}) \,|\, \mathbb{C}(\mathbf{x})^G)$ du corps des fractions sur le corps des fractions invariantes. Il y a en fait égalité entre ces deux groupes, mais comme on n'a pas supposé que G était fini, on ne peut pas encore l'assurer. Le corps $\mathbb{C}(\mathbf{x})^G$ des fractions invariantes de G contient l'anneau $\mathbb{C}[\mathbf{x}]^{G'}$ des polynômes invariants de G' et donc aussi le corps $\mathbb{C}(\mathbf{x})^{G'}$ des fractions invariantes de G' (on utilise le théorème 9.1.1). Le corps $\mathbb{C}(\mathbf{x})^G$ est alors une extension intermédiaire entre le corps $\mathbb{C}(\mathbf{x})^{G'}$ et le corps $\mathbb{C}(\mathbf{x})$ de toutes les fractions. D'après la correspondance de Galois, le groupe $\mathrm{Gal}(\mathbb{C}(\mathbf{x}) \,|\, \mathbb{C}(\mathbf{x})^G)$ est inclus dans le groupe $\mathrm{Gal}(\mathbb{C}(\mathbf{x}) \,|\, \mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}) = G'$, d'où l'on déduit que $G \subset G'$.

Le foncteur $G \mapsto \mathbb{C}[x]^G$ est surjectif par définition et injectif puisque :

$$\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[\mathbf{x}]^{G'} \Rightarrow \mathbb{C}(\mathbf{x})^G = \mathbb{C}(\mathbf{x})^{G'} \Rightarrow G = G'$$

Enfin, nous venons de montrer qu'il est contravariant. □

9.2 Corps des fractions invariantes d'une représentation par permutation

Dans le cas d'un groupe de permutation, la correspondance de Galois permet d'obtenir une caractérisation simple des éléments primitifs et la construction de l'un d'entre eux.

Corollaire 9.2.1.
Soit $\mathbf{f}$ *une fraction invariante. Les propositions suivantes sont équivalentes :*

(i) f *est un élément primitif de* $\mathbb{C}(\mathbf{x})^G$ *sur* $\mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}$ *;*

(ii) L'orbite de f *par* $\mathfrak{S}_m$ *est de taille* $\frac{m!}{|G|}$ *;*

(iii) Le groupe des permutations laissant f *invariante est réduit à* G*.*

En particulier, si $\mathbf{m}$ *est un vecteur valué dans* $\mathbf{N}$ *dont toutes les valuations sont distinctes (par exemple* $(0, 1, \ldots, m-1)$*), le polynôme invariant* q *correspondant est un élément primitif.*

Nous allons donner une démonstration très élémentaire de ce théorème et de son corollaire, en n'utilisant que des rudiments de théorie de Galois (voir [Esc97]). En particulier, nous n'utilisons pas le théorème 9.1.2. Nous n'utilisons la correspondance de Galois que pour obtenir la deuxième caractérisation des éléments primitifs. Le lemme suivant énumère toutes les étapes intermédiaires jusqu'aux énoncés du théorème et du corollaire. Ces étapes intermédiaires donnent des informations intéressantes en soi sur le corps des invariants.

Lemme 9.2.2.
Soient $\mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}$ *le corps des fractions symétriques, et* $\mathbb{C}(\mathbf{x})^G$ *le corps des fractions invariantes de* G*. Soit* T *un ensemble de représentants des cosets à droites de* G *dans* $\mathfrak{S}_m$*. Enfin, soient* $\mathbf{m}$ *et* q *comme dans le corollaire 9.2.1.*

(i) Le nombre $|T| = \frac{m!}{|G|}$ *de cosets est égal au nombre* t *d'invariants secondaires ;*

(ii) Les permutations $\sigma \in T$ *induisent* t *distincts* $\mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}$*-homomorphismes de* $\mathbb{C}(\mathbf{x})^G$ *dans* $\mathbb{C}(\mathbf{x})$ *;*

(iii) La dimension de $\mathbb{C}(\mathbf{x})^G$ *sur* $\mathbb{C}(\mathbf{x})$ *est* t *;*
(iv) Le polynôme q *est un élément primitif de* $\mathbb{C}(\mathbf{x})^G$ *sur* $\mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}$ *;*
(v) Une fraction invariante est un élément primitif de $\mathbb{C}(\mathbf{x})^G$ *sur* $\mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}$ *si, et seulement si, son orbite par* $\mathfrak{S}_m$ *est de taille* t *;*
(vi) $\mathbb{C}(\mathbf{x})$ *est la clôture normale de* $\mathbb{C}(\mathbf{x})^G$*, et le groupe de Galois de* $\mathbb{C}(\mathbf{x})/\mathbb{C}(\mathbf{x})^G$ *est* G *lui-même ;*
(vii) Une fraction invariante est un élément primitif de $\mathbb{C}(\mathbf{x})^G$ *sur* $\mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}$ *si, et seulement si, les seules permutations la laissant invariante sont dans* G*.*

Démonstration. On note, pour abréger, $\mathbf{K} := \mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}$ le corps des fractions symétriques, $\mathbf{L} := \mathbb{C}(\mathbf{x})^G$ le corps des fractions invariantes et $\mathbf{N} := \mathbb{C}(\mathbf{x})$ le corps des fractions. On obtient (i) par une application immédiate de la proposition 8.2.5 : $t = \frac{m!}{|G|} = |T|$.

Comme les valuations de $\mathbf{m}$ sont distinctes, on peut identifier chaque élément de l'orbite de $\mathbf{m}$ par G à une permutation de $\mathfrak{S}_m$. Par exemple, si $\mathbf{m}$ est le vecteur $(1, 2, \ldots, n)$, on identifie le vecteur $(5, 1, n, \ldots, 3)$ de l'orbite de $\mathbf{m}$ avec la permutation $\sigma = (5, 1, n, \ldots, 3)$. L'action de $\mathfrak{S}_m$ sur l'orbite de $\mathbf{m}$ correspond donc à l'action à droite du groupe $\mathfrak{S}_m$ sur lui-même. Le polynôme invariant $q := \mathbf{x}^{\mathbf{m}\circledast} = \sum_{\sigma\in G} \mathbf{x}^{\sigma.\mathbf{m}}$ associé à $\mathbf{m}$ s'identifie avec l'ensemble des permutations du groupe G (on pourrait directement voir ce polynôme comme un vecteur de l'algèbre du groupe symétrique). Si σ est une permutation de $\mathfrak{S}_m$, le polynôme $\sigma.\mathbf{x}^{\mathbf{m}\circledast}$ s'identifie de même avec le coset à droite $G.\sigma$. Comme T est un ensemble de représentants de ces cosets à droite, les polynômes $\sigma.q$ où σ parcourt T sont distincts.

Soit σ une permutation σ de $\mathfrak{S}_m$, et f_σ l'application induite de $\mathbf{L}$ dans $\mathbf{N}$ définie par $f_\sigma(p) := \sigma.p$. Cette application est un morphisme d'anneaux unitaire qui laisse invariants les polynômes symétriques. C'est donc un $\mathbf{K}$-homomorphisme. Cela montre le point (ii) : les permutations σ de T induisent t homomorphismes distincts.

Soit $P := a_k X^k + \cdots + a_1 X + X_0$, où les a_i sont des fractions symétriques, le polynôme minimal de q sur $\mathbf{K}$. On rappelle qu'un *conjugué de* q sur $\mathbf{K}$ est l'image de q par un $\mathbf{K}$-homomorphisme quelconque, et qu'un tel conjugué est aussi racine du polynôme minimal de q :

$$\begin{aligned} 0 = \sigma.P(q) &= \sigma.(a_k q^k + \cdots + a_1 q + a_0) = \sigma.a_k(\sigma.q)^k + \cdots + \sigma.a_1\sigma q + \sigma a_0 \\ &= a_k(\sigma.q)^k + \cdots + a_1\sigma q + a_0 = P(\sigma.q). \end{aligned}$$

Les t polynômes invariants $\mathbf{f}_\sigma(q) = \sigma.q$ où σ parcourt T sont conjugués de q, et sont t racines distinctes du polynôme minimal P, qui est donc de degré au moins t. On en déduit que les polynômes $1, q, q^2, \ldots q^{t-1}$ sont linéairement indépendants, et que la dimension de $\mathbf{L}$ en tant qu'espace vectoriel sur $\mathbf{K}$ est supérieure à t. Comme le lemme 9.1.4 indique que la dimension de $\mathbf{L}$ sur $\mathbf{K}$ est inférieure à t, (iii) et (iv) en découlent ; $1, q, q^2, \ldots, q^{t-1}$ est une base de $\mathbf{L}$ en tant que $\mathbf{K}$-espace vectoriel, le polynôme minimal de q est de degré t, la dimension de $\mathbf{L}$ sur $\mathbf{K}$ est t, et enfin q est un élément primitif : $\mathbf{L} = \mathbf{K}[q]$. On montre de même le point (v) : toute fraction invariante f dont l'orbite par $\mathfrak{S}_m$ est de taille t est un élément primitif de $\mathbf{L}$ sur $\mathbf{K}$.

Le polynôme invariant q a exactement t conjugués. Comme un $\mathbf{K}$-homomorphisme f de $\mathbf{L}$ dans une clôture normale de $\mathbf{L}$ est déterminé par sa valeur $f(q)$ sur l'élément primitif, et que cette valeur $f(q)$ est un conjugué de q, il y en a au plus t. Ces $\mathbf{K}$-homomorphismes sont donc exactement les $\mathbf{K}$-homomorphismes induits par les

permutations de T. En particulier, les conjugués d'une fraction f invariante quelconque sont tous dans le corps des fractions $\mathbf{N}$, qui est donc la clôture normale de $\mathbf{L}$.

En prenant $G = \mathfrak{S}_m$, on obtient que $\mathbf{N}$ est aussi une extension normale de $\mathbf{K}$. Prenons maintenant G réduit à l'identité. Les $\mathbf{K}$-automorphismes de $\mathbf{N}$ dans lui-même sont induits par les $m!$ permutations de $\mathfrak{S}_m$, de sorte que le groupe de Galois de $\mathbf{N}$ sur $\mathbf{L}$ est exactement $\mathfrak{S}_m$.

Revenons à un sous-groupe G quelconque de $\mathfrak{S}_m$. Les $\mathbf{L}$-automorphismes de $\mathbf{N}$ sont exactement les $\mathbf{K}$-homomorphismes qui laissent $\mathbf{L}$ invariant. On montre aisément que les seules permutations laissant $\mathbf{L}$ invariant sont les permutations de G (sinon l'exponentielle q du vecteur $\mathbf{m}$ n'est pas invariante). Donc le groupe de Galois de $\mathbf{N}$ sur $\mathbf{K}$ est précisément G, ce qui clôt la démonstration de (vi).

Soit f une fraction invariante par G, soit $\mathbf{L}' \subset \mathbf{L}$ le sur-corps de $\mathbf{K}$ qu'elle engendre, et soit $G' \supset G$ le groupe de Galois de ce corps. On vérifie que G' est le groupe des permutations laissant f invariante. D'après la correspondance de Galois, les points suivants sont alors équivalents :

- f est un élément primitif ;
- $\mathbf{L}' = \mathbf{L}$;
- $G = G'$;
- Les seules permutations laissant invariante f sont dans G.

□

Ces résultats donnent quelques informations sur la forme possible des systèmes générateurs de l'algèbre des invariants.

Corollaire 9.2.3.
Soit q un polynôme, élément primitif de $\mathbb{C}(\mathbf{x})^G$ (par exemple celui du corollaire 9.2.1), et soit t comme ci-dessus. L'anneau des polynômes invariants est engendré par les polynômes symétriques élémentaires et un ensemble fini de polynômes invariants $p_1, \ldots, p_k$ de la forme :

$$p_i = \frac{\alpha_{i,0} + \alpha_{i,1} q + \cdots + \alpha_{i,t-1} q^{t-1}}{\beta_i},$$

où les $\alpha_{i,d}$, et β_i sont des polynômes symétriques.

Démonstration. On prend, par exemple, pour les p_i un système d'invariants secondaires. Ils se mettent sous la forme voulue, car $1, q, \ldots, q^{t-1}$ est une base de l'espace vectoriel $\mathbb{C}(\mathbf{x})^G$ sur le corps $\mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}$.

On note que $1, q, \ldots, q^{t-1}$ est une base d'un sous-module M libre de $\mathbb{C}[\mathbf{x}]^G$ sur $\mathbb{C}[\mathbf{x}]^{\mathfrak{S}_m}$. Cependant, même si les modules libres M et $\mathbb{C}[\mathbf{x}]^G$ ont même dimension, il n'y a que rarement égalité. □

En utilisant le corollaire 9.2.1, on obtient un système générateur particulièrement simple du corps des fractions invariantes sur les graphes.

Corollaire 9.2.4.
Soit $n \geq 5$; soit $\mathbf{g}$ le graphe simple composé de deux arêtes adjacentes et $q := \mathbf{x}^{\mathbf{g}\circledast}$ le polynôme invariant associé ; enfin, soit e_d le polynôme symétrique élémentaire de degré d. Le corps $\mathbb{C}(\mathbf{x})^G$ des fractions invariantes sur les graphes est engendré par les polynômes $(e_1, \ldots, e_m, q)$.

Démonstration. Il est clair que q n'est invariant que par les permutations des arêtes qui préservent l'adjacence. Si $n \geq 5$, d'après la proposition 8.5.1, l'ensemble de ces permutations est exactement notre groupe G des permutations induites par les permutations des sommets. Donc, d'après le corollaire 9.2.1, q est un élément primitif du corps $\mathbb{C}(\mathbf{x})^G$ des fractions invariantes sur les graphes, sur le corps $\mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}$ des fractions symétriques. □

On pourrait en fait choisir pour q quasiment n'importe quel polynôme invariant.

Corollaire 9.2.5.
Soit $n \notin \{4, 5, 6, 8\}$. Si n est impair (resp. pair) et q est un polynôme invariant non symétrique (resp. non alterné), alors q est un élément primitif du corps $\mathbb{C}(\mathbf{x})^G$ des fractions invariantes sur les graphes sur le corps $\mathbb{C}(\mathbf{x})^{\mathfrak{S}_m}$ des fractions symétriques.

Démonstration. Voyons le cas n pair. Supposons que q soit invariant par une permutation σ qui n'est pas dans G. Clairement q est invariant par toute permutation dans le groupe G' engendré par G et σ. Or, d'après le théorème 8.5.3, G est un sous-groupe maximal de $\mathfrak{S}_m$, et donc $G' = \mathfrak{S}_m$, c'est-à-dire que q est un polynôme symétrique. Réciproquement, si q n'est pas symétrique, les seules permutations le laissant invariant sont dans G. Donc, d'après le corollaire 9.2.1 (viii), q est primitif.

Le cas n impair se traite de manière analogue en remplaçant symétrique par antisymétrique □

9.3 Systèmes générateurs et systèmes complets d'invariants

Dans [Gri79], Grigoriev déduit de l'existence d'un système générateur de taille $m+1$ (théorème 9.1.2) qu'il existe un système complet d'invariants de taille $m+1$. Il est effectivement tentant de considérer que, comme pour l'algèbre des invariants, un système générateur du corps des fractions invariantes est un système complet d'invariants. Ce n'est pas vrai.

Prenons, par exemple, le système générateur $(e_1, \ldots, e_m, q)$ de l'algèbre des invariants sur les graphes donné par le corollaire 9.2.4. Pour un graphe simple $\mathbf{g}'$, les évaluations $(e_1(\mathbf{g}), \ldots, e_m(\mathbf{g}))$ sont déterminées par le nombre d'arêtes de $\mathbf{g}'$, tandis que $q(\mathbf{g})$ compte le nombre de paires d'arêtes adjacentes de $\mathbf{g}'$. On constate alors que le triangle et l'étoile à trois branches donnent la même évaluation à tous les polynômes du système générateur, alors qu'ils ne sont pas isomorphes. On pourrait, bien entendu, construire un exemple équivalent dans l'algèbre des invariants sur les digraphes.

Le problème apparaît nettement dans l'exemple suivant. Soit $\mathbf{L} := \mathbb{C}(x, y)$ le corps des fractions à deux variables, et $\mathbf{K} := \mathbb{C}(x^2, y^2)$. Enfin, soit q le polynôme $x + y$. Les polynômes x^2, y^2 et $x + y$ engendrent le corps $\mathbf{L}$. En effet,

$$x = \frac{1}{2}\left(x + y + \frac{x^2 - y^2}{x + y}\right) \qquad \text{et} \qquad y = \frac{1}{2}\left(x + y - \frac{x^2 - y^2}{x + y}\right).$$

Par contre, les vecteurs $\mathbf{v} := (1, -1)$ et $\mathbf{v}' := (-1, 1)$ donnent la même évaluation à x^2, y^2 et $x+y$. Le problème est que, en $\mathbf{v}$ et en $\mathbf{v}'$, on ne peut pas calculer l'évaluation

du polynôme $x - y$ à partir des évaluations des générateurs x^2, y^2 et $x + y$ car

$$x - y = \frac{x^2 - y^2}{x - y} = \frac{0}{0}.$$

On a cependant le résultat suivant :

Proposition 9.3.1.
Soit $(f_1, \ldots, f_k)$ un système fini générateur du corps des invariants. Il existe un ouvert U dense, dont le complémentaire est un ensemble algébrique, tel que $(f_1, \ldots, f_k)$ est un système complet d'invariants sur U.

Démonstration. Soit $(p_1, \ldots, p_l)$ un système fini de polynômes invariants qui engendrent (par somme et produit) l'algèbre des invariants. Chaque p_i s'exprime comme une fraction rationnelle $\frac{r_i}{q_i}$, où r_i et q_i sont des combinaisons polynomiales des éléments du système générateur S, et $q_i \neq 0$.

Soit S l'ensemble des polynômes q_i et des dénominateurs des fractions q_i. Soient U l'ensemble des vecteurs $\mathbf{v}$ qui n'annulent aucun des polynômes de S, et V son complémentaire. On note que V étant défini par un nombre fini d'équations polynomiales est un ensemble algébrique. Clairement, en chaque vecteur $\mathbf{v}$ de U, on peut calculer l'évaluation de tous les p_i et donc de tous les polynômes invariants en fonction des évaluations des fractions f_i. Comme l'algèbre des invariants est un système complet d'invariants, on en déduit que $(f_1, \ldots, f_k)$ est aussi un système complet d'invariants sur U.

Soit q un polynôme de S. L'ensemble Z_q des zéros de q est un fermé car q est continu. De plus Z_q ne contient pas de boule ouverte de rayon > 0, car sinon q serait uniformément nul. Le complémentaire de Z_q est donc un ouvert dense. Comme U est une réunion finie de tels complémentaires, U est un ouvert dense. □

Il faut un peu de prudence pour généraliser cette proposition à d'autres corps de base que $\mathbb{Q}$, $\mathbb{R}$ où $\mathbb{C}$, puisqu'on utilise certaines de leur propriétés topologiques.

9.4 Applications aux problèmes d'isomorphie et de reconstruction

Nous renvoyons à la partie III pour la définition de la reconstructibilité algébrique. Soit $(e_1, \ldots, e_m, q)$ le système générateur du corps des invariants sur les graphes donné par le corollaire 9.2.4. Les polynômes de ce système générateur sont tous algébriquement reconstructibles. On sait aussi qu'il existe des polynômes invariants non algébriquement reconstructibles (théorème 18.0.1). On en déduit que la reconstructibilité algébrique n'est pas préservée par fraction. Nous avions été tenté de définir une notion affaiblie de reconstructibilité algébrique, autorisant les fractions, de façon à contourner les restrictions de la proposition 16.5.1. Les considérations ci-dessus montrent que cette notion est sans intérêt, puisque tous les polynômes invariants sont alors trivialement algébriquement reconstructibles.

Soit maintenant $\mathbf{m}$ un polynôme invariant reconstructible (en tant que fonction), et $q := \mathbf{x}^{\mathbf{m}\circledast}$ le polynôme invariant associé. On déduit de la proposition 9.3.1 qu'il existe un ouvert dense U dans l'espace vectoriel des graphes valués tel que tous

les graphes de U sont reconstructibles. Ceci résulte bien plus simplement de la proposition suivante.

Proposition 9.4.1.
Tout graphe valué $\mathbf{g}$ *dont les valuations sont distinctes (on suppose en particulier que* $\mathbf{g}$ *a au plus une non-arête) est reconstructible.*

Démonstration. Cela est clair si $n = 3$. Pour $n \geq 4$, on constate que chaque sommet est identifié uniquement dès que l'on connaît les valuations de deux arêtes adjacentes. Cela permet de recoller sans difficulté les cartes du jeu de $\mathbf{g}$. □

En effet, la proposition 9.4.1 nous dit que l'ensemble des graphes non-reconstructibles dans la réunion des hyperplans $x_{\{i,j\}} = x_{\{i',j'\}}$. Le complémentaire de ces $\mathrm{C}^2_{\mathrm{C}^2_n}$ est un ouvert dense.

Pour aller plus loin, il serait nécessaire de connaître plus précisément U, et en particulier les équations polynomiales qui le définissent. Cela nécessite *a priori* de connaître un système générateur $p_1, \ldots, p_k$ de l'algèbre des invariants, pour en déduire les dénominateurs des expressions des p_i en fonction des générateurs du corps des fractions. Pour le moment, nous ne connaissons qu'un système générateur de l'algèbre des invariants très grossier (voir 8.2.6), et surtout dont la structure ne contient pas vraiment d'information spécifique aux graphes. Il est donc peu probable que l'ouvert U correspondant contienne des classes de graphes intéressantes.

Au vu de ces résultats, nous ne pensons pas que l'étude du corps des invariants puisse apporter des informations sur le problème d'isomorphisme de graphes, et en particulier sur le problème de reconstruction.

Chapitre 10

Manipulation concrète de l'algèbre des invariants

10.1 Représentation combinatoire et informatique des polynômes invariants

Les remarques de cette section sont valables pour n'importe quelle représentation par permutation. Cependant, pour en avoir une représentation concrète, nous les développerons dans le cadre des graphes. Pour généraliser, il suffira de remplacer graphe par vecteur à coordonnées $\{0,1\}$ et multigraphe par vecteur à coordonnées entières positives. Pour aider cette généralisation, nous supposerons fixée une énumération des arêtes que nous noterons $\mathbf{e}_1, \ldots, \mathbf{e}_m$.

10.1.1 Représentation combinatoire

On peut identifier un multigraphe et un monôme. L'idée, qui apparaît par exemple dans Stanley[Sta79, p. 509], est très naturelle.

Définition 10.1.1 (Exponentielle).
Soit $\mathbf{v} = \sum v_1\mathbf{e}_1 + \cdots + v_m\mathbf{e}_m$ *un multigraphe. On appelle* exponentielle de $\mathbf{v}$ *le monôme*

$$\mathbf{x}^{\mathbf{v}} = x_1^{v_1} \ldots x_m^{v_m}.$$

On appelle exponentielle *l'application qui associe à chaque multigraphe le monôme correspondant.*

Comme souhaité, cette application permet d'identifier multigraphes et monômes. Elle transforme l'addition en multiplication et préserve l'action du groupe :

$$\mathbf{x}^{\mathbf{v}+\mathbf{v}'} = \mathbf{x}^{\mathbf{v}} \times \mathbf{x}^{\mathbf{v}'};$$
$$\sigma.\mathbf{x}^{\mathbf{e}} = \mathbf{x}^{\sigma.\mathbf{e}}.$$

Un polynôme est donc tout simplement une combinaison linéaire formelle de multigraphes avec certains coefficients. Nous allons maintenant identifier un multigraphe à isomorphie près avec un polynôme invariant, par sommation sur l'orbite.

Définition 10.1.2 (Exponentielle symétrisée).
Soit $\mathbf{v}$ *un multigraphe et* $\overline{\mathbf{v}}$ *son orbite. On appelle* exponentielle symétrisée de $\mathbf{v}$ *le polynôme invariant*

$$\mathbf{x}^{\mathbf{v}^{\circledast}} = \sum_{\mathbf{v}' \in \overline{\mathbf{v}}} \mathbf{x}^{\mathbf{v}'}$$

On remarque que, à une constante près, cela revient à appliquer l'opérateur de Reynolds à $\mathbf{x}^{\mathbf{v}}$:

$$\mathbf{x}^{\mathbf{v}^{\circledast}} = |\overline{\mathbf{v}}| \, (\mathbf{x}^{\mathbf{v}})^*$$

En effet :

$$\begin{aligned} \mathbf{x}^{\mathbf{v}^*} &= \frac{1}{|G|} \sum_{\sigma} \sigma.\mathbf{x}^{\mathbf{v}} = \frac{1}{|G|} \sum_{\sigma} \mathbf{x}^{\sigma.\mathbf{v}} = \frac{1}{|G|} \sum_{\mathbf{v}' \in \overline{\mathbf{v}}} |\{\sigma : \sigma\mathbf{v} = \mathbf{v}'\}| \, \mathbf{x}^{\mathbf{v}'} \\ &= \frac{|G_{\mathbf{v}}|}{|G|} \sum_{\mathbf{v}' \in \overline{\mathbf{v}}} \mathbf{x}^{\mathbf{v}'} = \frac{1}{|\overline{\mathbf{v}}|} \sum_{\mathbf{v}' \in \overline{\mathbf{v}}} \mathbf{x}^{\mathbf{v}'} = \frac{1}{|\overline{\mathbf{v}}|} \mathbf{x}^{\mathbf{v}^{\circledast}} \end{aligned} \tag{10.1}$$

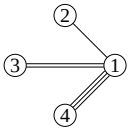
où $G_{\mathbf{v}}$ est le groupe d'automorphismes de $\mathbf{v}$, *i.e.* $\{\sigma : \sigma\mathbf{v} = \mathbf{v}'\}$. C'est pourquoi nous avons utilisé une notation proche.

Représentation semi-graphique

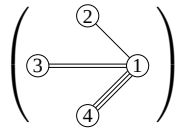
Nous pouvons donc maintenant voir tout polynôme invariant comme combinaison linéaire formelle de multigraphes à isomorphie près. Nous allons utiliser cela pour représenter ces polynômes de manière semi-graphique. L'exemple suivant permet de fixer nos notations.

Exemple 10.1.3.
Soit $\mathbf{g}$ *le multigraphe* $\mathbf{e}_{1,2} + 2\mathbf{e}_{1,3} + 3\mathbf{e}_{1,4}$. *On le représentera comme suit*

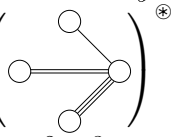
– *Vecteur :*

$\mathbf{g} =$  $= \mathbf{e}_{1,2} + 2\mathbf{e}_{1,3} + 3\mathbf{e}_{1,4}$

– *Exponentielle :*

$\mathbf{x}^{\mathbf{g}} =$  $= x_{1,2}x_{1,3}^2x_{1,4}^3$

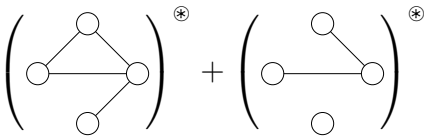
– *Exponentielle symétrisée :*

$\mathbf{x}^{\mathbf{g}^{\circledast}} =$ 

$$\begin{aligned} &= x_{1,2}x_{1,3}^2x_{1,4}^3 + x_{1,2}x_{1,3}^3x_{1,4}^2 + x_{1,2}^2x_{1,3}x_{1,4}^3 + x_{1,2}^2x_{1,3}^3x_{1,4} + x_{1,2}^3x_{1,3}x_{1,4}^2 + x_{1,2}^3x_{1,3}^2x_{1,4} \\ &+ x_{1,2}x_{2,3}^2x_{2,4}^3 + x_{1,2}x_{2,3}^3x_{2,4}^2 + x_{1,2}^2x_{2,3}x_{2,4}^3 + x_{1,2}^2x_{2,3}^3x_{2,4} + x_{1,2}^3x_{2,3}x_{2,4}^2 + x_{1,2}^3x_{2,3}^2x_{2,4} \\ &+ x_{1,3}x_{2,3}^2x_{3,4}^3 + x_{1,3}x_{2,3}^3x_{3,4}^2 + x_{1,3}^2x_{2,3}x_{3,4}^3 + x_{1,3}^2x_{2,3}^3x_{3,4} + x_{1,3}^3x_{2,3}x_{3,4}^2 + x_{1,3}^3x_{2,3}^2x_{3,4} \\ &+ x_{1,4}x_{2,4}^2x_{3,4}^3 + x_{1,4}x_{2,4}^3x_{3,4}^2 + x_{1,4}^2x_{2,4}x_{3,4}^3 + x_{1,4}^2x_{2,4}^3x_{3,4} + x_{1,4}^3x_{2,4}x_{3,4}^2 + x_{1,4}^3x_{2,4}^2x_{3,4} \end{aligned}$$

Encore un dernier exemple pour se convaincre que, sans cette représentation, il serait impossible de manipuler concrètement le moindre polynôme invariant.

Exemple 10.1.4.



$$
\begin{aligned}
&= x_{1,2}x_{1,4} + x_{1,2}x_{1,3} + x_{1,3}x_{1,4} + x_{1,2}x_{2,4} + x_{1,2}x_{2,3} + x_{2,3}x_{2,4} \\
&+ x_{1,3}x_{3,4} + x_{1,3}x_{2,3} + x_{2,3}x_{3,4} + x_{1,4}x_{3,4} + x_{1,4}x_{2,4} + x_{2,4}x_{3,4} \\
&+ x_{1,3}x_{1,4}x_{2,3}x_{2,4}x_{3,4} + x_{1,2}x_{1,4}x_{2,3}x_{3,4}x_{2,4} + x_{1,2}x_{1,3}x_{2,4}x_{3,4}x_{2,3} \\
&+ x_{1,2}x_{2,4}x_{1,3}x_{3,4}x_{1,4} + x_{1,2}x_{2,3}x_{1,4}x_{3,4}x_{1,3} + x_{1,3}x_{2,3}x_{1,4}x_{2,4}x_{1,2}
\end{aligned}
$$

Par la suite, lorsque le contexte sera clair, on ne précisera pas si l'on considère un multigraphe comme un vecteur, un monôme ou un polynôme invariant.

Parallèle avec les fonctions symétriques

Notons que c'est la même approche qui permet de considérer tout polynôme de $\mathbb{C}[x_1, \ldots, x_m]$ comme une somme formelle de compositions et un polynôme symétrique comme une somme formelle de partitions.

10.1.2 Représentants canoniques des orbites

Dans le cas des polynômes symétriques, la tâche est simplifiée, car on peut représenter canoniquement une orbite de compositions avec l'unique partition qu'elle contient. De manière générale, pour toute représentation par permutation, il est possible de définir de manière canonique un représentant de chaque orbite.

Ce type de technique, proche d'un codage, est utile pour étudier des structures combinatoires à isomorphie près [RC77, p. 352] et en particulier pour engendrer des catalogues de représentants (voir [Ker91] et [CCRW85])

Définition 10.1.5 (Canonisation).
Une canonisation *est une fonction qui, à un vecteur, associe un* représentant canonique *de son orbite.*

Lorsqu'il y a un ordre total sur les coefficients, on peut toujours définir une telle canonisation, comme par exemple la suivante.

Définition 10.1.6 (Canonisation lexicographique).
Soit $(e_1, \ldots, e_m)$ *une énumération des vecteurs de la base. Tout vecteur peut maintenant être identifié avec la liste de ses coefficients. On définit alors un ordre total* $<_{lex}$ *sur les vecteurs de sorte que* $\mathbf{v} <_{lex} \mathbf{v}'$*, si la liste correspondant à* $\mathbf{v}$ *est lexicographiquement plus petite que celle correspondant à* $\mathbf{v}'$*.*

On prend comme représentant canonique de $\mathbf{v}$ *le plus grand vecteur* $\mathbf{v}'$ *de l'orbite de* $\mathbf{v}$ *pour cet ordre total.*

On remarque que cet ordre total sur les vecteurs à coefficients entiers positifs coïncide avec l'ordre lexicographique habituel sur les monômes. Cela renforce notre

identification vecteur/monôme. De manière générale, on aurait pu utiliser n'importe quel ordre classique sur les monômes, comme l'ordre lexicographique par degré (DegLex), l'ordre lexicographique inverse (InvLex) ou (DegRevLex). On remarque aussi que, les vecteurs d'une même orbite ayant même degré, le choix de l'ordre lexicographique ou de l'ordre lexicographique par degré ne change pas la canonisation.

Codage des graphes simples par des entiers

On note que cela permet de coder un graphe simple non étiqueté de manière canonique par un entier. Sa forme canonique est en effet une suite de 0 et de 1 que l'on peut considérer comme un entier écrit en binaire. Les algorithmes simples pour engendrer des graphes non étiquetés sont basés sur ce codage (voir [Rea81, p. 79]). Ce codage permet de stocker le graphe de manière compacte, et il est immédiat de tester si deux graphes sous forme canonique sont égaux. On peut aussi l'utiliser dans des algorithmes de type crible d'Eratostène. Cependant, pour aller au-delà de 7 sommets il faut utiliser des techniques plus sophistiquées (voir [CCRW85] pour les graphes sur 10 sommets).

Canonisations spécifiques

Dans certains cas, il est possible de définir des canonisations qui exploitent les propriétés particulières de la représentation. Cela peut être intéressant pour plusieurs raisons, comme tenir compte de symétries ou pour avoir un algorithme de calcul considérablement plus rapide de la forme canonique. Jusqu'à la fin de cette sous-section, nous allons développer cette idée dans le cas spécifique des graphes.

Canonisation indépendante du nombre de sommets

Il est parfois intéressant d'avoir une forme canonique qui ne change pas lorsqu'on rajoute des sommets isolés au graphe. De cette façon on peut identifier deux graphes qui ne diffèrent que par leur nombre de sommets. Nous allons construire une canonisation qui respecte cette règle. On considère l'énumération suivante des arêtes

$$(\mathbf{e}_{1,2}, \quad \mathbf{e}_{1,3}, \mathbf{e}_{2,3}, \quad \mathbf{e}_{1,4}, \mathbf{e}_{2,4}, \mathbf{e}_{3,4}, \quad \ldots, \quad \mathbf{e}_{n-1,n})$$

et on prend l'ordre DegRevLex. À degré égal, cet ordre privilégie les vecteurs dont les zéros sont à la fin. On remarque alors que, dans un graphe $\mathbf{g}$ sous forme canonique, tous les sommets isolés sont regroupés à la fin. De même, rajouter des sommets isolés $(n+1, n+2, \ldots)$ à $\mathbf{g}$ le laisse sous forme canonique. Il ne nous reste donc plus qu'à ôter tous les sommets isolés à la fin de $\mathbf{g}$.

Digression sur les énumérations d'arêtes

Il y a essentiellement deux façons naturelles d'énumérer les arêtes du graphe complet, celle que nous venons de voir et la suivante :

$$(\mathbf{e}_{1,2}, \mathbf{e}_{1,3}, \ldots, \mathbf{e}_{1,n}, \quad \mathbf{e}_{2,3}, \ldots \mathbf{e}_{2,n}, \quad \ldots \quad \mathbf{e}_{n-1,n})$$

Cela revient à parcourir une matrice symétrique au dessous de la diagonale, soit ligne par ligne, soit colonne par colonne. L'intérêt du premier cas est qu'il n'est pas nécessaire de connaître *a priori* le nombre final de sommets. Toujours est-il que dans les programmes de manipulation de matrices symétriques les deux conventions sont utilisées. La permutation permettant de passer d'une représentation à l'autre a donc été découverte et étudiée [Sou91]. Il se trouve qu'elle a des propriétés algorithmiques intéressantes. En particulier, le calcul de son ordre par itérations successives a été utilisé pour des tests comparatifs de vitesse de calcul en entiers d'ordinateurs, depuis le PDP-11 jusqu'aux derniers CRAYs.

Canonisations algorithmiquement efficaces

Revenons à des applications informatiques nous concernant. La mise sous forme canonique d'un vecteur est une opération que nous utiliserons très souvent et qui doit donc être la moins coûteuse possible. Avec les canonisations que nous avons vues jusqu'ici, il n'y a guère d'autre algorithme que de parcourir toute l'orbite d'un graphe et de prendre le plus petit représentant (voir cependant [Ker91] pour des optimisations). En s'inspirant de [RC77] on peut trouver des canonisations beaucoup moins coûteuses, au moins en moyenne.

La stratégie générale est d'éviter de parcourir toutes les permutations des sommets en groupant ensemble les sommets ayant des caractéristiques communes. Il suffit alors de tester les permutations à l'intérieur de chacun des groupes. Par exemple, pour obtenir la forme canonique d'un graphe $\mathbf{g}$, on commence par trier les sommets par degrés décroissants, puis on teste toutes les permutations qui ne changent pas ces degrés. Enfin, on sélectionne le graphe obtenu le plus grand pour l'ordre lexicographique. On ne parcourt donc que $\lambda_1!\lambda_2!\ldots\lambda_k!$ permutations où λ_i est le nombre de sommets de $\mathbf{g}$ de degré i. On remarque que, avec cette canonisation, les sommets isolés se retrouvent à la fin. Elle est donc indépendante du nombre de sommets.

Il est possible de raffiner pour diminuer encore le nombre de permutations parcourues. On peut, par exemple, caractériser chaque sommet non seulement par son degré, mais aussi par la liste décroissante des degrés des sommets adjacents.

Bien évidemment, ce genre de méthode fonctionne mal sur les graphes réguliers. De toute façon, quelle que soit la méthode utilisée, il y a toujours des graphes pour lesquels on est obligé de parcourir quasiment toutes les permutations (voir à ce sujet la discussion dans [RC77, 13. Advice to the user]). Dans notre cas, nous avons besoin de traiter beaucoup de petits graphes et, en moyenne, l'efficacité est suffisante. Dans la plupart des cas, nous nous sommes contentés du raffinement par degré. Pour traiter les arbres sur 14 sommets (19) nous avons dû utiliser le raffinement par degrés des sommets adjacents. Si cela avait été vraiment nécessaire, nous aurions pu utiliser un algorithme spécifique aux arbres.

10.1.3 Interprétation combinatoire du produit

Nous allons voir maintenant que le produit de deux polynômes invariants a aussi une interprétation simple. Il suffit de regarder ce qu'il se passe pour le produit de

deux multigraphes :

$$\mathbf{x}^{\mathbf{g}_1{}^{\circledast}}.\mathbf{x}^{\mathbf{g}_2{}^{\circledast}} = \sum_{\mathbf{g}'_1 \in \overline{\mathbf{g}_1}} \mathbf{x}^{\mathbf{g}'_1}. \sum_{\mathbf{g}'_2 \in \overline{\mathbf{g}_2}} \mathbf{x}^{\mathbf{g}'_2} = \sum_{\mathbf{g}'_1 \in \overline{\mathbf{g}_1}, \mathbf{g}'_2 \in \overline{\mathbf{g}_2}} \exp \mathbf{g}'_1 + \mathbf{g}'_2 \tag{10.2}$$

Cela revient donc à superposer les deux graphes de toutes les façons possibles et à considérer la somme formelle de ces superpositions.

Lien avec l'opérateur Etoile

On remarque alors que la multiplication par un polynôme symétrique élémentaire donne un opérateur sur les graphes simples proche de l'opérateur Etoile de la partie I (§ 6.3).

Proposition 10.1.7.
Soient $\mathbf{g}$ *et* $\mathbf{h}$ *deux graphes simples tels que* $\mathbf{g}$ *possède* d *arêtes de plus que* $\mathbf{h}$. *Soit* e_d *le polynôme symétrique élémentaire de degré* d *en les* $x_{\{i,j\}}$. *Le coefficient de* $\mathbf{x}^{\mathbf{g}^{\circledast}}$ *dans* $\mathbf{x}^{\mathbf{h}^{\circledast}} e_d$ *vaut* $s(\mathbf{h}, \mathbf{g})$.

Démonstration. Comme $\mathbf{x}^{\mathbf{g}^{\circledast}} = \sum_{\mathbf{g}' \approx \mathbf{g}} \mathbf{x}^{\mathbf{g}}$, les coefficients de $\mathbf{x}^{\mathbf{g}^{\circledast}}$ et de $\mathbf{x}^{\mathbf{g}}$ dans $\mathbf{x}^{\mathbf{h}^{\circledast}} e_d$ coïncident. Soit $\mathbf{h}'$ un graphe isomorphe à $\mathbf{h}$. Les termes de $\mathbf{x}^{\mathbf{h}'} e_d$ correspondent à toutes les façons possibles de rajouter d arêtes disjointes à $\mathbf{h}'$ (éventuellement en doublant certaines arêtes de $\mathbf{h}'$). Le coefficient de $\mathbf{x}^{\mathbf{g}}$ dans $\mathbf{x}^{\mathbf{h}'} e_d$ est donc 1 si $\mathbf{h}'$ est un sous-graphe de $\mathbf{g}$ et 0 sinon. On en déduit que le coefficient de $\mathbf{g}$ dans $\mathbf{x}^{\mathbf{h}^{\circledast}} e_d$ est le nombre de graphes $\mathbf{h}'$ isomorphes à $\mathbf{h}$ qui sont sous-graphes de $\mathbf{g}$, c'est-à-dire $s(\mathbf{h}, \mathbf{g})$. □

Le polynôme $e_d.\mathbf{x}^{\mathbf{g}^{\circledast}}$ est donc la somme d'un terme correspondant à Etoile($\mathbf{g}$) et de termes avec des arêtes multiples. Nous définissons au § 12.2.1 l'algèbre des graphes simples, qui est obtenue en éliminant ces termes. Dans cette nouvelle algèbre, les deux opérateurs coïncident alors complètement. Il en sera de même dans l'algèbre des forêts que l'on définit de manière analogue.

10.1.4 Représentation informatique

Représentation

Nous avons vu que ces considérations permettent d'obtenir des représentations graphiques compactes pour l'humain. De même, il est possible de s'en servir pour manipuler informatiquement des polynômes invariants. On code tout d'abord un multigraphe par la liste de ses coefficients. Un multigraphe à isomorphie près est alors codé par son représentant canonique (cf.§ 10.1.2). Enfin un polynôme invariant est une combinaison linéaire de multigraphes à isomorphie près. On ne stocke donc qu'un terme du polynôme par classe d'équivalence, ce qui permet un gain en mémoire considérable, de l'ordre de $n!$.

Calcul du produit

Il faut maintenant vérifier que l'on peut calculer le produit de deux polynômes dans cette représentation. On veut éviter de calculer toutes les superpositions possibles des deux graphes, car il risque d'y en avoir jusqu'à $n!^2$. Par symétrie, il suffit de fixer un des deux graphes et de faire les superpositions avec tous les permutés de l'autre. Il faut mettre sous forme canonique toutes les superpositions obtenues. Enfin, il y a un coefficient que l'on ajuste aisément.

$$\mathbf{x}^{\mathbf{v}_1{}^{\circledast}}.\mathbf{x}^{\mathbf{v}_2{}^{\circledast}} = |\overline{\mathbf{v}_1}| \sum_{v_2' \in \overline{\mathbf{v}_2}} \frac{1}{|\overline{\mathbf{v}_1 + \mathbf{v}_2}|} \mathbf{x}^{\mathrm{canonic}(\mathbf{v}_1 + \mathbf{v}_2')^{\circledast}} \tag{10.3}$$

Remarques 10.1.8:

- La taille de $\overline{\mathbf{v}_1 + \mathbf{v}_2}$ peut être obtenue comme sous-produit de la recherche de sa forme canonique.
- Il est raisonnable de conserver dans la représentation de chaque multigraphe la taille de son orbite de façon à ne pas avoir à la recalculer ultérieurement.
- On peut choisir, pour la sommation, entre $\mathbf{v}_1$ et $\mathbf{v}_2$ celui qui a la plus petite orbite.

Implémentation

Le domaine `Dom::InvariantAlgebra` permet de manipuler des polynômes invariants comme indiqué ci-dessus pour toute représentation par permutation (domaines dans la catégorie `Cat::PermutationGroup`). Par défaut, la forme canonique est définie en utilisant l'ordre lexicographique. Lorsque c'est possible, il est vivement recommandé de définir une méthode de canonisation plus efficace. Il peut être rentable de mémoriser (option `remember` ou autre) les formes canoniques au fur et à mesure. Il y a alors un compromis temps/mémoire à trouver.

Un des avantages de `MuPAD`, est qu'il est possible de faire appel à des bibliothèques extérieures, par exemple écrites en C, et chargées dynamiquement. Dans le cas des graphes, nous comptons à court terme utiliser la bibliothèque `nauty` de McKay [McK90] pour les calculs de forme canonique. Cela permettra probablement de gagner plusieurs ordres de grandeur dans le temps de calcul des formes canoniques. Nous escomptons aussi un gain en mémoire, puisqu'il ne sera plus vraiment nécessaire de conserver les formes canoniques déjà calculées.

10.1.5 Représentation par des chaînes de graphes

Pour conclure, nous allons donner une autre interprétation combinatoire des polynômes invariants, inspirée de l'article de Garsia et Stanton [GS84]. Étant donné un ordre partiel (ou plus généralement un complexe simplicial) on peut construire une algèbre dite de Stanley-Reisner, dont la structure algébrique est très liée à la structure combinatoire de l'ordre sous-jacent [Gar80, BGS82]. Or, lorsqu'un groupe agit par permutation, on peut choisir un ordre partiel de sorte que son algèbre de Stanley-Reisner ait des propriétés proches de l'algèbre des invariants. En particulier, il sera possible de transférer des systèmes générateurs de la première vers la

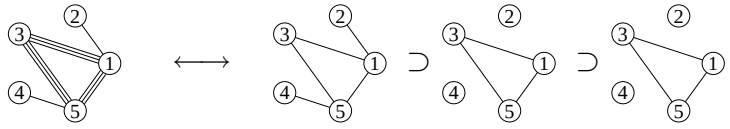
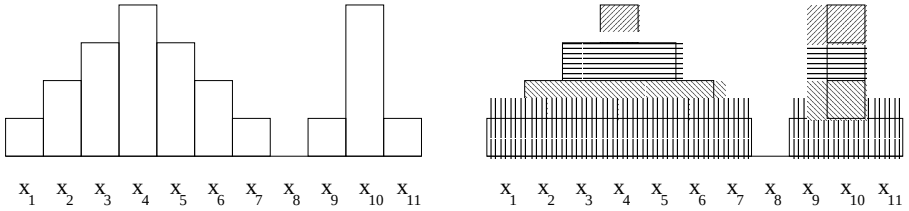


FIG. 10.1 – Un multigraphe et sa décomposition en couches



(a) Par coordonnées (b) Par couches

FIG. 10.2 – Les deux façons orthogonales de considérer un monôme

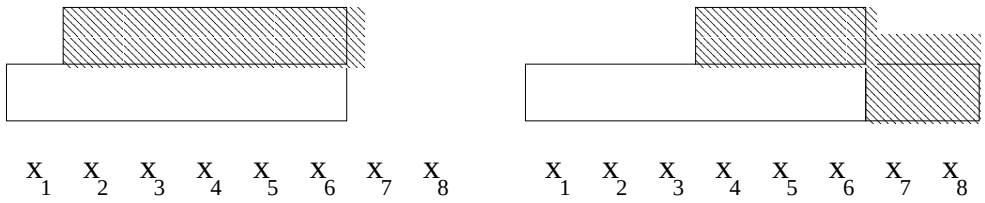
seconde. Dans notre cas, on ordonne l'ensemble des graphes simples par inclusion. L'ordre partiel à considérer est alors le complexe des chaînes de tels graphes, que l'on a quotienté par l'action du groupe. Il y a donc de fortes chances pour que cette approche permette d'appliquer en retour des outils combinatoires pour étudier l'algèbre des invariants. En particulier, on peut espérer obtenir une forme intéressante pour les invariants secondaires. Pour le moment, nous n'avons exploité que des idées élémentaires de cette approche, et ce, essentiellement pour le calcul informatique des secondaires. Nous pourrons donc nous contenter d'une présentation simple, sans avoir à introduire le formalisme du cadre général.

Décomposition d'un multigraphe en couches

Jusqu'ici nous avons considéré un multigraphe comme une juxtaposition d'arêtes valuées. De manière orthogonale, on peut aussi considérer ce multigraphe comme un empilement de graphes simples emboîtés de plus en plus petits (voir figure 10.1). La figure 10.2 a été réalisée en représentant un multigraphe par une suite d'entiers. Elle montre que cette décomposition est utilisable pour n'importe quelle représentation par permutation. Bien entendu, ceci est une simple généralisation de la notion de partition duale d'une partition.

Soit T le treillis booléen des graphes ordonnés par inclusion. Un multigraphe est donc une *multichaîne* de T. Par multichaîne, nous indiquons qu'il peut y avoir répétition de certaines couches. On considère $\mathcal{C}$ l'ensemble de ces multichaînes, que l'on a quotienté par l'action du groupe symétrique. On peut identifier les éléments de $\mathcal{C}$ avec les multigraphes à isomorphie près. On ordonne $\mathcal{C}$, par inclusion, c'est-à-dire qu'un multigraphe $\mathbf{m}$ est plus grand qu'un autre $\mathbf{m}'$, s'il contient les couches de $\mathbf{m}'$, plus éventuellement d'autres.

Ceci est l'ordre partiel voulu. On voit que, au moins en tant qu'espace vectoriel, les polynômes invariants et les combinaisons linéaires formelles d'éléments de $\mathcal{C}$



(a) Emboîtement correct (b) Emboîtement incorrect

FIG. 10.3 – Emboîtements des couches lors d'un produit

coïncident. Reste à définir un produit.

Définition 10.1.9.
On appelle forme *d'un multigraphe* $\mathbf{m}$ *la liste décroissante des tailles des couches qui le composent.*

Produit de chaînes

Lorsque l'on effectue le produit de deux graphes, on peut obtenir deux types de termes. Dans les premiers, les couches se superposent correctement (figure 10.3(a)). En revanche, dans les seconds, les couches ne s'emboîtent pas et une partie de la deuxième couche s'effondre à l'étage inférieur (figure 10.3(b)). Nous allons définir sur l'anneau des polynômes un deuxième produit qui évitera cet inconvénient en annulant les termes pour lesquels il y a eu un effondrement.

Définition 10.1.10 (Produit de chaînes).
Soient $\mathbf{m}$ *et* $\mathbf{m}'$ *deux chaînes de graphes* $c_1 \subseteq c_2 \subseteq \dots c_d$ *et* $c'_1 \subseteq c'_2 \subseteq \dots c'_{d'}$. *On définit comme suit leur* produit de chaînes

$$m \star m' = \begin{cases} m.m' & \text{si l'ensemble des graphes } \{c_1, \dots, c_d, c'_i, \dots, c'_d\} \text{ est une chaîne} \\ 0 & \text{sinon} \end{cases}$$

L'espace des combinaisons linéaires formelles d'éléments de $\mathcal{C}$, muni du produit de chaînes, est l'algèbre de Stanley-Reisner annoncée. Dans notre vision simpliste, nous considérons seulement que nous avons muni l'espace vectoriel des polynômes invariants d'un nouveau produit. En voici les propriétés principales :

Propriétés 10.1.11.
(i) $\star$ *n'est pas intègre ;*
(ii) $\star$ *préserve la graduation et plus précisément la graduation fine par forme de* $\mathbb{C}[\mathbf{x}]$ *; L'algèbre des invariants* $(\mathbb{C}[\mathbf{x}]^G, \star)$ *est donc finement graduée ;*
(iii) L'algèbre des invariants $(\mathbb{C}[\mathbf{x}]^G, \star)$ *est de type fini ;*
(iv) Un ensemble B *de générateurs pour le produit de chaînes est aussi générateur pour le produit usuel ;*
(v) L'algèbre des invariants est de Cohen-Macaulay ;
(vi) Les polynômes symétriques élémentaires forment un système d'invariants primaires ;

(vii) Un système de primaires et de secondaires pour le produit de chaînes est aussi un système de primaires et de secondaires pour le produit usuel.

Le point (ii) est clair. Le produit de chaînes a été construit pour éviter tout effondrement et donc, dans ce cas, la forme du produit est déterminée par la forme des opérandes. En revanche, on perd forcément l'intégrité du produit, même dans la sous-algèbre $\mathbb{C}[\mathbf{x}]^G$ (point (i)). Par exemple, le produit de deux arêtes adjacentes par deux arêtes disjointes est nul.

Le point (iii) est une conséquence de la remarque suivante :

Remarque 10.1.12: Soit $\mathbf{m}$ un multigraphe dans lequel une couche $\mathbf{g}$ de taille k est répétée plusieurs fois. Soit $\mathbf{m}'$ le multigraphe dans lequel on a enlevé un des exemplaires de cette couche. Soit enfin e_k le k^{e} polynôme symétrique élémentaire. On a :

$$\mathbf{m} = \mathbf{m}' \star e_k$$

Démonstration. La démonstration est simple : e_k est la somme de tous les graphes de taille k. Il contient donc entre autres $\mathbf{g}$, et le multigraphe $\mathbf{m}$ apparaît comme terme dans le produit. En revanche, si $\mathbf{g}'$ est un autre graphe de taille k, il est incomparable pour l'inclusion avec $\mathbf{g}$. Comme $\mathbf{m}'$ contient $\mathbf{g}$ comme couche, $\mathbf{m}' \star g' = 0$. On note que le même argument fonctionne si l'on considère $\mathbf{m}$ à isomorphie près, c'est-à-dire comme la somme des multigraphes de son orbite. □

L'algèbre des invariants est donc engendrée par les m fonctions symétriques élémentaires et les multigraphes sans répétition de couches. Ceux-ci sont en nombre fini.

Le point (iv) n'est pas énoncé explicitement dans [Gar80], mais s'obtient en appliquant les méthodes qui y sont décrites. Le point clef est que, dans un empilement incorrect, les couches inférieures grossissent et les couches supérieures diminuent à cause de l'effondrement. Il est alors possible de mettre un ordre total sur les formes comme suit : $\mathbf{m}$ est plus petit que $\mathbf{m}'$ si pour tout i la somme des tailles des couches de $\mathbf{m}$ en dessous de i est plus petite que celle de $\mathbf{m}'$. De la sorte, étant donnés deux multigraphes $\mathbf{m}$ et $\mathbf{m}'$, les deux produits $\mathbf{m}\mathbf{m}'$ et $\mathbf{m} \star \mathbf{m}'$ ne diffèrent que par des termes où il y a eu un effondrement et qui sont donc strictement inférieurs aux termes principaux. On peut alors procéder par induction.

Nous obtenons comme corollaire le fait que, pour le produit usuel, l'algèbre des invariants est engendrée par les multigraphes sans répétition de couche. Nous avons essayé de l'exploiter, pour accélérer le calcul par ordinateur d'un système minimal de générateurs.

Les points restants, que nous n'avons pas utilisés intensivement, sont traités en détail dans [Gar80] ou [GS84].

Évaluation de l'apport du produit de chaînes

Le point (iv) nous permet de rechercher des systèmes générateurs dans l'algèbre des invariants avec le produit de chaînes, puis de les retransférer sur l'algèbre usuelle des invariants. De même, de nombreuses identités algébriques peuvent être transférées [Gar80]. Cela suggère donc de travailler avec le produit de chaînes. D'un point de vue théorique, on peut espérer pouvoir exploiter son interprétation combinatoire

forte. Nous allons montrer ici que ce produit peut avoir aussi des répercussions très intéressantes d'un point de vue algorithmique. En revanche, il présente aussi quelques inconvénients majeurs, en particulier vis à vis de nos objectifs concernant le problème de reconstruction.

Un grand intérêt algorithmique,...

D'un point de vue concret, le premier avantage de ce produit est qu'il génère beaucoup moins de termes. Or, le coût principal d'un calcul de produit est la recherche de la forme canonique de chaque terme obtenu (cf. § 10.1.4). De plus, la plupart des algorithmes de recherche de systèmes générateurs minimaux sont basés sur la construction d'une matrice dont les entrées sont des produits. Si ces produits ont peu de termes, la matrice est relativement creuse. Son inversion nécessite donc nettement moins de mémoire et de temps. Les figures comparatives 11.3 page 177 et 11.4 page 178 sont édifiantes à ce point de vue.

La graduation fine de l'algèbre permet encore un gain supplémentaire. En effet, elle permet de découper $\mathbb{C}[x]_d^G$ en plusieurs sous-espaces vectoriels et de travailler indépendamment dans chacun d'entre eux. Premier gain, cela permet de manipuler plusieurs petites matrices plutôt qu'une grosse, ce qui est très important puisque le coût d'inversion d'une matrice est de l'ordre de n^3. Deuxième gain, on peut éliminer directement tous les sous-espaces correspondant à des multigraphes avec répétition de couches. Enfin, cela donne un algorithme fortement parallélisable. Tout cela devrait permettre d'envisager de traiter des cas nettement plus conséquents.

... mais des objections majeures

Hélas, il y a un mais. En effet, le point (iv) n'a pas de réciproque, c'est-à-dire qu'un système générateur pour le produit usuel peut ne pas être générateur pour le produit de chaînes. En conséquence, un système générateur minimal pour le produit de chaînes peut perdre sa minimalité quand on le transfère pour le produit usuel. Dans la pratique et sur nos exemples, les systèmes obtenus par ce biais sont de tailles et surtout de degrés considérablement plus grands que nécessaire. Nous avions espéré pouvoir utiliser cette technique, au moins comme prétraitement, pour obtenir une borne sur les degrés. Mais finalement cette borne ne semble pas bien meilleure que celle donnée par le calcul du degré maximal des secondaires (théorème 11.4.1).

En fait, il semblerait qu'il n'y ait pas de systèmes d'invariants primaires de degrés relativement petits, comme pour le produit usuel (Cf. § 11.3.1). Si on essaye de prendre de tels primaires, on peut calculer le nombre de secondaires par degré et cela permet de borner le nombre de générateurs par degré dans un système générateur minimal (rappelons que grâce à la proposition 11.1.4, ce nombre est indépendant du système générateur minimal). Or, nous avons pu calculer effectivement un tel système minimal pour $n = 4, 5$ et les bornes sont dépassées, de beaucoup. Il sera donc probablement obligatoire d'utiliser les fonctions symétriques comme primaires avec tous les problèmes que cela pose (cf. §11.3.1).

Il y a aussi un autre inconvénient de ce produit, vis-à-vis de notre intérêt pour le problème de reconstruction. Notre objectif lointain est de montrer que l'algèbre des invariants est engendrée par les multigraphes ayant au moins un sommet isolé. Or, ce

n'est pas le cas avec le produit de chaînes. En effet, si l'on fait le produit de chaînes de deux multigraphes avec des sommets isolés, on n'obtient que des multigraphes avec des sommets isolés. L'idée étant qu'avec ce produit on ne fait qu'empiler des couches existantes, sans en créer de nouvelles. En particulier, un système générateur devra contenir toutes les couches simples, c'est-à-dire tous les graphes.

10.2 Relations entre les algèbres d'invariants sur les graphes

Notons, pour abréger, $\mathcal{I}_n$ l'algèbre des polynômes invariants sur les graphes à n sommets. Dans cette section, nous étudions les relations entre les algèbres des invariants $\mathcal{I}_n$ et $\mathcal{I}_{n'}$ sur les graphes à respectivement n et n' sommets. Nous regardons en particulier le cas $\mathcal{I}_{n-1}$ et $\mathcal{I}_n$, ce qui donne une construction formelle des polynômes algébriquement reconstructibles de la partie III. Enfin, nous construisons l'algèbre limite $\mathcal{I}_\infty$ sur un nombre infini de sommets, et nous tirons de son étude des informations sur $\mathcal{I}_n$.

10.2.1 Relations entre $\mathcal{I}_{n-1}$ et $\mathcal{I}_n$

Nous présentons ici une construction plus abstraite des polynômes algébriquement reconstructibles que nous étudierons dans la partie III.

Généralités sur la puissance symétrique d'une algèbre

Soit $\mathcal{A}$ un espace vectoriel, et n un entier. On appelle $\mathrm{Sym}^n \mathcal{A}$ la énième puissance symétrique de $\mathcal{A}$, c'est-à-dire le sous-espace de $\bigotimes^n \mathcal{A}$ engendré par les éléments de la forme

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n := \sum_{\sigma \in \mathfrak{S}_n} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(n)},$$

où $a_1, \ldots, a_n \in \mathcal{A}$ (voir, par exemple, [FH96, Appendix B]). Supposons que $\mathcal{A}$ soit une algèbre avec une unité que nous notons 1. Alors $\bigotimes^n \mathcal{A}$ a aussi une structure d'algèbre (multiplication terme à terme) et une unité : $1 \otimes \cdots \otimes 1$.

Soit $j \in \{1, \ldots, n\}$ et $a \in \mathcal{A}$; on pose $\Phi_j(a) := \alpha_1 \otimes \cdots \otimes \alpha_n$, où $\alpha_j = a$ et $\alpha_k = 1$ si $k \neq j$. Enfin, soit

$$\begin{aligned}\Phi(a) &:= \sum_{j=1}^{n} \Phi_j(a) = a \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes a \otimes \cdots \otimes 1 + \cdots + 1 \otimes \cdots \otimes 1 \otimes a \\ &= \frac{1}{(n-1)!} a \cdot 1 \cdot \ldots \cdot 1\end{aligned}$$

Théorème 10.2.1.
$\mathrm{Sym}^n \mathcal{A}$ *est la sous-algèbre de* $\bigotimes^n \mathcal{A}$ *engendrée par l'image de* $\mathcal{A}$ *par* Φ.

Démonstration. Nous allons raisonner par récurrence sur le nombre k de termes différents de 1 dans un produit symétrique $p := a_1 \cdot \ldots \cdot a_n$. Si $k = 1$, ce produit

est de la forme $p = a_1 \cdot 1 \cdot \ldots \cdot 1$ qui est bien dans l'image de $\mathcal{A}$ par Φ. Soit $p := a_1 \cdot a_2 \cdot \ldots \cdot a_k \cdot 1 \cdot \ldots \cdot 1$ un produit symétrique ayant k termes distincts de 1. Par récurrence, les produits $q := a_1 \ldots . a_{k-1} \cdot 1 \cdot \ldots \cdot 1$ et $r := a_1 \cdot 1 \cdot \ldots \cdot 1$ sont engendrés par $\Phi(\mathcal{A})$. Notons, par commodité, $b_1 = a_1, \ldots, b_{k-1} = a_{k-1}$, $b_k = b_{k+1} = \cdots = b_n = 1$ les termes du produit q, et développons l'expression qr :

$$\begin{aligned} qr &= (a_1 \cdot \ldots \cdot a_{k-1} \cdot 1 \cdot \ldots \cdot 1)(a_k \cdot 1 \cdot \ldots \cdot 1) \\ &= \left(\sum_{\sigma \in \mathfrak{S}_n} b_{\sigma(1)} \otimes \cdots \otimes b_{\sigma(n)} \right) (a \otimes 1 \otimes \cdots \otimes 1 + \cdots + 1 \otimes \cdots \otimes 1 \otimes a) \\ &= (a_1 a_k) \cdot \ldots \cdot a_{k-1} \cdot 1 \cdot \ldots \cdot 1 + a_1 \cdot \ldots \cdot (a_{k-1} a_k) \cdot 1 \cdot \ldots \cdot 1 + a_1 \cdot \ldots \cdot a_k \cdot 1 \cdot \ldots \cdot 1 \end{aligned}$$

En dehors $(a_1 \cdot \ldots \cdot a_k \cdot 1 \cdot \ldots \cdot 1)$, tous les produits apparaissant dans qr ont strictement moins de k termes distincts de 1. On peut donc exprimer p à partir de tels produits et, par récurrence, on obtient $p \in \Phi(\mathcal{A})$. □

Prenons, par exemple, $\mathcal{A} := \mathbb{C}[x]$. Dans ce cas, $\bigotimes^n \mathcal{A}$ s'identifie avec $\mathbb{C}[x_1, \ldots, x_n]$ et $\mathrm{Sym}^n \mathcal{A}$ avec la sous-algèbre $\mathbb{C}[x_1, \ldots, x_n]^{\mathfrak{S}_n}$ des polynômes symétriques ; le théorème 10.2.1 affirme que les polynômes symétriques sont engendrés par les fonctions symétriques puissances $p_k := x_1^k + \cdots + x_n^k$, pour $k \in \mathbb{N}$.

Prenons maintenant $\mathcal{A} := \mathbb{C}[x_1, \ldots, x_r]$. Dans ce cas, $\bigotimes^n \mathcal{A}$ s'identifie avec $\mathbb{C}[x_{i,j}], i \in \{1, \ldots, r\}, j \in \{1, \ldots, n\}$, et $\mathrm{Sym}^n \mathcal{A}$ avec la sous-algèbre des *polynômes multisymétriques*, c'est-à-dire les polynômes $P(x_{i,j})$ tels que $P(x_{i,j}) = P(x_{i,\sigma(j)})$ pour toute permutation de $\mathfrak{S}_n$. Considérons l'expression suivante :

$$\prod_{i=1}^{n} (1 + x_{i,1} U_1 + x_{i,2} U_2 + \cdots + x_{i,r} U_r) .$$

On appelle *polynômes multisymétriques élémentaires* les coefficients des monômes en les variables U_i dans cette expression. On rappelle la généralisation du théorème fondamental des fonctions symétriques (théorème 8.2.4).

Théorème 10.2.2.
L'algèbre des polynômes multisymétriques est engendrée par les polynômes multisymétriques élémentaires. Ces derniers sont de degré au plus n.

Corollaire 10.2.3.
Soit $\mathcal{A}$ une algèbre graduée de type fini, engendrée par des éléments de degré au plus d. Alors $\mathrm{Sym}^n \mathcal{A}$ est une algèbre graduée finiment engendrée par des éléments de degré au plus nd.

Démonstration. Soit $a_1, \ldots, a_r$ des générateurs de $\mathcal{A}$. Soit Ψ le morphisme surjectif d'anneaux de l'algèbre des polynômes multisymétriques de $\mathbb{C}[\mathbf{x}_{\{i,j\}}], i \in \{1, \ldots, r\}, j \in \{1, \ldots, n\}$ dans $\mathrm{Sym}^n \mathcal{A}$ défini par $\Psi(x_{i,j}) = \Phi_j(a_i)$. Soient $p_1, \ldots, p_k$ les polynômes multisymétriques élémentaires. On déduit de la proposition 10.2.2, que l'algèbre $\mathrm{Sym}^n \mathcal{A}$ est engendrée par les polynômes $(\Phi(p_1), \ldots, \Phi(p_k))$. Ceux-ci sont en nombre fini, et de degré inférieur à nd. □

Application à la reconstructibilité algébrique

Revenons maintenant aux algèbres des invariants sur les graphes. Soit $\mathcal{A} := \mathcal{I}_{n-1}$. Pour $j \in \{1, \ldots, n\}$ et $p \in \mathcal{I}_{n-1}$, soit $\Theta_j(p)$ le polynôme de $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$ obtenu en renumérotant les sommets dans $\{1, \ldots, n\}$ de sorte que $\Theta_j(p)$ ne contienne aucune des variables $x_{\{j,k\}}$. On peut, par exemple, renuméroter les sommets en utilisant la transposition $\sigma = (i, n)$. Cependant, comme p est invariant par rapport à $\mathfrak{S}_{n-1}$, toute autre permutation σ des sommets telle que $\sigma(n) = i$ donnera le même résultat. On note que $\Theta_n(p) = p$. Posons finalement

$$\Theta(p) := \Theta_1(p) + \cdots + \Theta_n(p).$$

Proposition 10.2.4.
Il y a un morphisme naturel de $\mathrm{Sym}^n \mathcal{I}_{n-1}$ *dans* $\mathcal{I}_n$. *L'image* $\mathbb{C}[\Theta(\mathcal{I}_{n-1})]$ *de* $\mathrm{Sym}^n \mathcal{I}_{n-1}$ *est engendrée par l'ensemble* $\Theta(\mathcal{I}_{n-1})$ *des polynômes de la forme* $\Theta(p)$ *où* $p \in \mathcal{I}_{n-1}$. *Cette algèbre est finiment engendrée, et on a la borne suivante sur les degrés d'un système générateur :*

$$\delta\left(\mathbb{C}[\Theta(\mathcal{I}_{n-1})]\right) \leq n\delta\left(\mathcal{I}_{n-1}\right).$$

Démonstration. Soit Ψ l'application linéaire de $\bigotimes^n \mathcal{I}_{n-1}$ dans $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$ définie par

$$\Psi(p_1 \otimes \cdots \otimes p_n) := \Theta_1(p_1) \ldots \Theta_n(p_n).$$

L'image d'un élément de $\mathrm{Sym}^n \mathcal{I}_{n-1}$ est donc de la forme

$$\Psi\left(\sum_{\sigma \in \mathfrak{S}_n} p_{\sigma(1)} \otimes \cdots \otimes p_{\sigma(n)}\right) = \sum_{\sigma \in \mathfrak{S}_n} \Theta_1(p_{\sigma(1)}) \cdots \Theta_n(p_{\sigma(n)})$$

et on vérifie que c'est un polynôme invariant. Comme de plus les Θ_i sont des morphismes, l'application Ψ se restreint en un morphisme de $\mathrm{Sym}^n \mathcal{I}_{n-1}$ dans $\mathcal{I}_n$. Le diagramme suivant résume la situation.

$$\begin{array}{ccccc}
\mathcal{I}_{n-1} & \xhookrightarrow{\Phi} & \mathrm{Sym}^n \mathcal{I}_{n-1} & \xleftarrow{\pi} & \bigotimes^n \mathcal{I}_{n-1} \\
 & \searrow^{\Theta} & \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \Psi} \\
 & & \mathcal{I}_n & \xleftarrow{\text{« * »}} & \mathbb{C}[\mathbf{x}_{\{i,j\}}]
\end{array}$$

Ce diagramme commute. En effet, si $p \in \mathbb{R}[n-1]$, on a :

$$\begin{aligned}
\Psi(\Phi(p)) &= \Psi(\Phi_1(p) + \cdots + \Phi_n(p)) \\
&= \Psi(p \otimes 1 \otimes \cdots \otimes 1) + \cdots + \Psi(1 \otimes \cdots \otimes 1 \otimes p) \\
&= \Theta_1(p)\Theta_2(1) \cdots \Theta_n(1) + \cdots + \Theta_1(1) \cdots \Theta_{n-1}(1)\Theta_n(p) \\
&= \Theta_1(p) + \cdots + \Theta_n(p) = \Theta(p)
\end{aligned}$$

Comme d'après le théorème 10.2.1, l'algèbre $\mathrm{Sym}^n \mathcal{I}_{n-1}$ est engendrée par $\Phi(\mathcal{I}_{n-1})$, son image $\mathbb{C}[\Theta(\mathcal{I}_{n-1})]$ par Ψ est engendrée par $\Theta(\mathcal{I}_{n-1}) = \Psi(\Phi(\mathcal{I}_{n-1}))$, comme voulu. □

Justifions ce formalisme. Soit $\mathbf{m}$ un multigraphe sur $n-1$ sommets, où, de manière équivalente, un multigraphe sur n sommets avec un sommet isolé. Soit p l'exponentielle symétrisée de $\mathbf{m}$ sur $n-1$ sommets. À une constante près, le polynôme invariant $\Theta(p)$ est l'exponentielle symétrisée de $\mathbf{m}$ sur n sommets. On en déduit que $\Theta(\mathcal{I}_{n-1})$ est le sous-espace vectoriel de $\mathcal{I}_n$ engendré par les exponentielles de multigraphes ayant un sommet isolé. Les polynômes de $\mathbb{C}[\Theta(\mathcal{I}_{n-1})]$ sont donc précisément les polynômes invariants algébriquement reconstructibles, tels que nous les définissons dans la partie III.

La construction des polynômes algébriquement reconstructibles permet d'obtenir un certain nombre d'informations sur ceux-ci. Par exemple, si p est un polynôme invariant de $\mathcal{I}_{n-1}$, on sait immédiatement que non seulement $\Theta_1(p)+\cdots+\Theta_n(p)$ est algébriquement reconstructible, mais aussi $\Theta_1(p)\cdots\Theta_n(p)$, ou toute autre combinaison symétrique des $\Theta_i(p)$, ce qui est moins évident avec l'autre définition des polynômes algébriquement reconstructibles. On peut de même construire toutes sortes d'autres polynômes algébriquement reconstructibles. Une autre conséquence est que l'algèbre des polynômes invariants algébriquement reconstructibles est finiment engendrée, avec une borne connue sur le degré des générateurs.

10.2.2 Relations entre $\mathcal{I}_n$ et $\mathcal{I}_\infty$

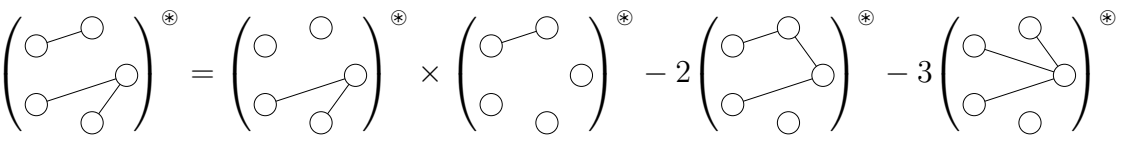
Nous considérons ici un graphe indépendamment de son nombre de sommets isolés. Comme la notion de connexité n'a alors pas vraiment de sens, on définit la quasi-connexité.

Définition 10.2.5 (graphe quasi-connexe).
On appelle graphe quasi-connexe un graphe qui n'a qu'une composante connexe non triviale. Un graphe quasi-connexe est constitué d'un graphe connexe et éventuellement de sommets isolés.

On a alors la proposition suivante.

Proposition 10.2.6.
L'algèbre des invariants est engendrée par les multigraphes quasi-connexes.

Démonstration. Le principe est le même que pour montrer que les multigraphes non-connexes sont algébriquement reconstructibles (théorème 15.1.1). On raisonne par récurrence sur le nombre total de composantes connexes non triviales. Soit $\mathbf{g}$ un multigraphe ayant au moins deux composantes connexes non triviales, soit $\mathbf{g}_1$ une de ces composantes connexes et $\mathbf{g}_2$ le reste du multigraphe. Dans le produit de $\mathbf{g}_1$ par $\mathbf{g}_2$, il y a deux types de termes. Dans les premiers la composante $\mathbf{g}_1$ est restée indépendante des autres ; ces termes sont donc isomorphes à $\mathbf{g}$. Dans les seconds, $\mathbf{g}_1$ touche au moins une autre composante connexe non triviale de $\mathbf{g}_2$; le nombre total de composantes connexes non triviales a donc diminué et on applique la récurrence pour les éliminer. Par exemple :



□

On peut étendre la définition de l'algèbre des polynômes invariants à un nombre infini de sommets. Pour cela, on considère l'espace vectoriel ayant pour base les multigraphes sans sommets isolés, sur un nombre fini quelconque de sommets. On munit sans difficulté cet espace d'un produit similaire à celui du cas fini.

Proposition 10.2.7.

(i) Lorsque le nombre de sommets est infini, les multigraphes quasi-connexes sont algébriquement indépendants. L'algèbre des invariants est l'algèbre libre sur les multigraphes quasi-connexes ;

(ii) Les multigraphes quasi-connexes forment un système générateur minimal partiel de l'algèbre des invariants sur n sommets jusqu'au degré $\lfloor \frac{n}{2} \rfloor$.

Démonstration. (i) Soit $p := p(\mathbf{x}^{\mathbf{m}_1^{\circledast}}, \ldots, \mathbf{x}^{\mathbf{m}_k^{\circledast}})$ une combinaison polynomiale nulle des polynômes $\mathbf{x}^{\mathbf{m}_1^{\circledast}}, \ldots, \mathbf{x}^{\mathbf{m}_k^{\circledast}}$ où les multigraphes $\mathbf{m}_i$ sont quasi-connexes et définis sur un nombre infini de sommets. Supposons que p ne soit pas le polynôme nul. Soit $\alpha \mathbf{x}^{\mathbf{m}_{i_1}{}^{\circledast}} \ldots \mathbf{x}^{\mathbf{m}_{i_l}{}^{\circledast}}$ un monôme de p, avec $\alpha \neq 0$, $i_1 \leq i_2 \leq \cdots \leq i_l$ et l maximal. Dans l'expansion de p, on trouve le polynôme $\mathbf{x}^{\mathbf{m}^{\circledast}}$ où $\mathbf{m}$ est le multigraphe obtenu par réunion disjointe des composantes connexes non triviales de chaque $\mathbf{m}_i$. On constate que, par maximalité de l, aucun autre monôme de p n'a pu produire ce polynôme $\mathbf{x}^{\mathbf{m}^{\circledast}}$. Le coefficient α est donc nul, ce qui est contradictoire.

De fait, on peut définir naturellement un autre produit dans l'algèbre des invariants sur un nombre infini de sommets consistant simplement à prendre pour $\mathbf{m}_1.\mathbf{m}_2$ le multigraphe $\mathbf{m}$ union disjointe sur les sommets des multigraphes $\mathbf{m}_1$ et $\mathbf{m}_2$. Notre produit peut alors être vu comme un déformé de ce produit disjoint.

(ii) Jusqu'au degré $\lfloor \frac{n}{2} \rfloor$, l'algèbre des invariants sur n sommets coïncide avec l'algèbre des invariants sur un nombre infini de sommets. Il est donc clair que les multigraphes quasi-connexes forment un système générateur minimal jusqu'au degré $\lfloor \frac{n}{2} \rfloor$.

□

10.3 Calcul de la série de Hilbert

10.3.1 Introduction

Nous allons nous intéresser ici au calcul de la série de Hilbert de l'algèbre des invariants sur les graphes et, en particulier, à son calcul explicite. Dans la pratique, on peut la calculer sans problème jusqu'à plus d'une quinzaine de sommets (1 heure de calcul et 20 Mo). L'étude attentive de cette série nous a été très utile. Elle nous a, par exemple, permis de remarquer que l'algèbre était de Gorenstein (§ 8.4), de conjecturer l'existence d'invariants primaires de certains degrés (§ 11.3.1), ou de résoudre par la négative un problème de Pouzet (§ 11.2, conjecture 11.2.1). Elle est essentielle aussi dans la recherche des invariants secondaires (§ 11.4), pour avoir rapidement des ordres de grandeur et des conditions d'arrêt.

Nous avons donc cherché un algorithme de calcul rapide, avec de plus des raffinements multigradués ou par forme.

Nous rappelons succinctement les propriétés que nous avons énoncées au cours de la section 8. Pour un groupe G fini quelconque, une formule générale de calcul de la série de Hilbert est donnée par :

Théorème 10.3.1 (Molien 1897).

$$H(\mathbb{C}[V]^G, z) = \frac{1}{|G|} \sum_{M \in G} \frac{1}{\det(\mathrm{Id} - zM)}$$

Optimisation : Calcul par classe de conjugaison

On remarque que le polynôme caractéristique est constant sur les classes de conjugaison de G. Il est intéressant de sommer par classe. Nous rappelons que pour le groupe symétrique, les classes de conjugaison sont paramétrées par les partitions de n. La classe de conjugaison correspondant à la partition $c_1, \ldots, c_k$ contient les $\frac{n!}{c_1! \ldots c_k!}$ permutations ayant des cycles de longueur $c_1, \ldots, c_k$. Le gain est considérable, car le nombre de partitions croît relativement lentement, de l'ordre de $\exp(\sqrt{n}))$. Par exemple, pour 15 sommets, il y a seulement 176 partitions contre $1,3.10^{12}$ permutations.

Optimisation : utilisation du type cyclique

Comme notre représentation est une représentation par permutation, les polynômes caractéristiques se calculent facilement.

Proposition 10.3.2.
Soit M une matrice de permutation et (l_i) le type cyclique correspondant (autrement dit, l_i est le nombre de cycles de longueur i de la permutation).

$$\det(\mathrm{Id} - zM) = \prod_i (1 - z^i)^{l_i}$$

Corollaire 10.3.3.
Soit G un groupe de permutations de $\{1, \ldots, m\}$, la série de Hilbert de l'algèbre des invariants $\mathbb{C}[\mathbf{x}]^G$ s'exprime sous la forme :

$$H(\mathbb{C}[\mathbf{x}]^G, z) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\prod (1 - z^i)^{l_i(\sigma)}},$$

où $l_i(\sigma)$ compte le nombre de cycles de longueur i de σ.

Étant donnée une permutation σ des sommets, il suffit donc de calculer le type cyclique de la permutation correspondante des arêtes, comme décrit par la proposition suivante.

Proposition 10.3.4 ([HP73][Ker91, p. 43]).
Soit σ une permutation des sommets.

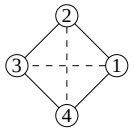
(i) Un cycle de σ de longueur c impaire concourt à $\frac{c-1}{2}$ cycles de longueur c (arêtes entre les sommets du cycle).

(ii) Un cycle de σ de longueur c paire concourt à $\frac{c}{2} - 1$ cycles de longueur c (arêtes entre les sommets du cycle).

(iii) Deux cycles de σ de longueurs c et c' concourent à $c \wedge c'$ cycles de longueur $c \vee c'$ (arêtes entre les sommets des deux cycles).

Exemple 10.3.5.
Le cycle $(1,2,3,4)$ sur 4 sommets engendre les cycles suivants sur les arêtes

$(\{1,2\},\{2,3\},\{3,4\},\{4,5\})$ *et* $(\{1,3\},\{2,4\})$:



Énumération de Pólya

Le corollaire 10.3.3 peut aussi être obtenu comme conséquence du théorème d'énumération par poids de Pólya. Soit G un groupe de permutation. Nous avons vu au 10.1 que les polynômes $\mathbf{x}^{\mathbf{m}\circledast}$ où $\mathbf{m}$ est un vecteur à coefficients entiers forment une base d'espace vectoriel de $\mathbb{C}[\mathbf{x}]^G$. Donc, la dimension de la composante homogène $\mathbb{C}[\mathbf{x}]^G_d$ de degré d de l'algèbre des invariants est précisément le nombre de vecteurs à coefficients entiers, tels que la somme des coefficients vaut d, comptés à l'isomorphie près. Ce lien entre série de Hilbert et théorème de Pólya est déjà explicité dans [Sta79]. Nous nous contentons de rappeler sans démonstration le théorème de Pólya, et de présenter quelques unes de ses applications. En effet, nous nous en sommes aussi servi à diverses reprises, pour compter les graphes simples à l'isomorphie près, etc. (voir, par exemple, § 18).

Soient X et Y deux ensembles avec $m := |X|$ et $k := |Y|$. On suppose X fini. À chaque élément y de Y, on associe un poids $\omega(y)$ et à chaque fonction de Y^X le poids $w(f) := \prod_{x\in X} \omega(f(x))$. Par exemple, si $Y := \{y_1,\ldots,y_k\}$, si chaque y_i est vu comme une indéterminée avec $\omega(y) = y$, et si $f \in Y^X$, alors $\omega(f)$ est un monôme de degré $m = |X|$. Soit G un groupe agissant sur X, que l'on fait agir sur Y^X par $\sigma.f := f \circ \sigma^{-1}$.

Fait 10.3.6.
Si f et f' sont dans la même orbite O par l'action de G sur Y^X, alors $\omega(f) = \omega(f')$.

On définit le poids d'une orbite O (pour l'action de G sur Y^X) comme le poids de n'importe quel élément de cette orbite.

Le théorème de Pólya permet d'exprimer le nombre d'orbites de poids donné. On appelle *polynôme énumérateur des cycles*, ou *cycle-index* de G le polynôme

$$Z(G,X) := \frac{1}{|G|}\sum_{\sigma\in G}\prod_{i=1}^{|E|} Z_i^{l_i(\sigma)},$$

où $(Z_1,\ldots,Z_{|E|})$ sont des variables et $l_i(\sigma)$ compte le nombre de cycles de longueur i de la permutation σ. On note $S(Y) := \sum_{y\in Y} w(y)$ la série génératrice par poids de Y. Plus généralement, on note $S_i(Y) := \sum_{y\in Y} w(y)^i$ la série génératrice des i-uples $(y,\ldots,y)$ d'éléments identiques de Y.

Théorème 10.3.7 (Pólya [HP73], [FR]).
La série génératrice par poids des orbites de Y^X s'obtient en substituant Z_i par $S_i(Y)$ dans le cycle-index $Z(G,X)$ de G.

Par exemple, si l'on veut énumérer par nombre d'arêtes les graphes simples à l'isomorphie près, on prend pour X l'ensemble des paires de $\{1,\dots,n\}$, pour Y l'ensemble $\{0,1\}$ et pour poids $\omega(0)=1$ et $\omega(1)=t$. Enfin, on fait agir naturellement le groupe $\mathfrak{S}_n$ sur l'ensemble X des paires de $\{1,\dots,n\}$. Le nombre de graphes à l'isomorphie près à d arêtes est précisément le nombre d'orbites dans Y^X de poids y^d. La série génératrice $S_i(y)$ vaut alors $1+y^i$. Lorsque l'on substitue Z_i par $S_i(y)$ dans $Z(G,X)$, on obtient un polynôme $a_0+a_1t+\cdots+a_{\mathrm{C}_n^2}t^{\mathrm{C}_n^2}$ où a_d compte le nombre de graphes simples à d arêtes. Si l'on veut se contenter d'obtenir le nombre total de graphes simples, il suffit de prendre pour poids $\omega(0)=\omega(1)=1$.

Pour compter par nombre total d'arêtes les multigraphes à l'isomorphie près, on prend $Y:=\mathbb{N}$, avec $\omega(d)=t^d$. À priori les séries génératrices $S_i(Y):=1+t^i+t^{2i}+\cdots+t^{di}+\dots$ sont infinies. Cependant, en les mettant sous la forme $S_i(Y)=\frac{1}{1-t^i}$ la substitution ne pose pas de problème. On retrouve alors l'expression de la série de Hilbert de l'algèbre des invariants du corollaire 10.3.3 :

$$H(\mathbb{C}[\mathbf{x}]^G,z)=\frac{1}{|G|}\sum_{\sigma\in G}\frac{1}{\prod(1-z^i)^{l_i}}$$

On note pour finir que, dans le cadre de la théorie des représentations, l'énumération par poids de Pólya peut être vue comme un calcul de caractère de la représentation du groupe G. En particulier, lorsque $Y=\{y_1,\dots,y_k\}$, on peut exprimer la série génératrice par poids des orbites Y^X comme combinaison linéaire à coefficients entiers des polynômes symétriques de Schur en les variables $(y_1,\dots,y_k)$ [Ker91, Corollaire 5.1.5].

10.3.2 Raffinement par forme

Nous allons voir maintenant un premier raffinement de la série de Hilbert. Comme le groupe agit par permutation des arêtes, son action sur un multigraphe ne change pas, par exemple, le nombre d'arêtes valuées 3 du multigraphe. On appelle *forme d'un multigraphe* la suite $\sigma=(\sigma_1,\sigma_2,\dots)$ où σ_i est le nombre d'arêtes valuées i du multigraphe. Cela définit une graduation fine sur l'espace vectoriel des polynômes. On remarque que ce n'est pas une graduation d'algèbre. En effet, la graduation fine d'un produit $p*q$ ne dépend pas uniquement des graduations fines de p et q. Par exemple, si l'on multiplie deux arêtes entre elles ($\sigma=(1,0,\dots)$), on peut soit obtenir une double arête ($\sigma=(0,1,0,\dots)$), soit deux arêtes simples ($\sigma=(2,0,\dots)$). Comme cette graduation est respectée par l'action du groupe, elle se transmet à l'algèbre des invariants. On note $\mathbb{C}[\mathbf{x}]^G_\sigma$ l'espace vectoriel des polynômes invariants de forme σ.

Il est alors possible de calculer une série de Hilbert fine en utilisant une énumération de Pólya. En effet, on est exactement en train d'énumérer par poids les multigraphes à isomorphie près.

La série de Hilbert fine est très utile pour la recherche d'invariants secondaires en s'inspirant des résultats de Garsia et Stanton [GS84]. Le principe est de définir un deuxième produit sur l'algèbre des invariants, dit produit de chaînes. L'intérêt de ce produit est qu'il préserve la graduation fine. Si l'on choisit les polynômes symétriques élémentaires comme invariants primaires, cette graduation fine passe

au quotient par l'idéal engendré par les primaires. On peut alors calculer la série génératrice fine des secondaires à partir de la série de Hilbert fine par une inversion de Möbius [GS84, p. 117].

10.3.3 Raffinement multigradué

Comme notre représentation se scinde en sous-représentations, il est possible de calculer une série de Hilbert multigraduée (voir [Sch91]). Cela permet d'avoir plus d'informations sur la répartition des polynômes invariants entre les étoiles et les graphes 0-réguliers. Cela nous sera particulièrement utile pour la recherche d'invariants primaires(§ 11.3.1). Nous verrons réciproquement que cette recherche d'invariants primaires a abouti à une amélioration du calcul de la série de Hilbert multigraduée.

Pour le calcul, il suffit de remarquer que les matrices de la représentation s'écrivent par blocs et de calculer le polynôme caractéristique sur chaque bloc.

$$H(\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}, z_1, z_2) = \frac{1}{|G|} \sum_{M \in G} \frac{1}{\det(\mathrm{Id} - z_1 M_1) \det(\mathrm{Id} - z_2 M_2)} \tag{10.4}$$

Où M_1 et M_2 sont les blocs de M correspondant respectivement aux étoiles et aux graphes 0-réguliers. Dans la pratique, comme V et V_1 sont des représentations par permutation, il est intéressant d'utiliser :

$$H(\mathbb{C}[V], z_1, z_2) = \frac{1}{|G|} \sum_{M \in G} \frac{\det(\mathrm{Id} - z_2 M_1)}{\det(\mathrm{Id} - z_1 M_1) \det(\mathrm{Id} - z_2 M)} \tag{10.5}$$

sachant que les polynômes caractéristiques se calculent rapidement à partir des types cycliques (proposition 10.3.2).

Le lemme 11.3.4 permet une dernière optimisation. Il montre en effet que pour chaque terme

$$\frac{\det(\mathrm{Id} - z_2 M_1)}{\det(\mathrm{Id} - z_1 M_1) \det(\mathrm{Id} - z_2 M)} (1 - z_1) \dots (1 - z_1^n)(1 - z_2^2) \dots (1 - z_2^{\mathrm{C}_{n-1}^2})$$

est un polynôme P. Le calcul direct de la série génératrice des invariants secondaires permet donc de ne manipuler que des polynômes et non des fractions. Cela est nettement plus rapide, d'autant que le polynôme P peut se calculer directement avec une variante de la proposition 10.3.4. Pour obtenir la série de Hilbert, il suffit alors de diviser le résultat obtenu par

$$(1 - z_1) \dots (1 - z_1^n)(1 - z_2^2) \dots (1 - z_2^{\mathrm{C}_{n-1}^2})$$

.

10.3.4 Implémentation

La bibliothèque `PerMuVAR` pour `MuPAD` permet le calcul de la série de Hilbert d'un groupe fini avec plusieurs algorithmes suivant la connaissance que l'on a du

groupe. Pour cela, l'approche orientée objet de `MuPAD` est très pratique. Dans le cas général (catégorie `Cat::FiniteGroupModule`), il appliquera la formule basique utilisant les polynômes caractéristiques. Si l'action est par permutation (catégorie `Cat::PermutationGroupModule`), il calcule le type cyclique des permutations. Pour optimiser, on peut définir une méthode `cycleTypes` renvoyant pour chaque classe de conjugaison le type cyclique et la taille. Enfin, on peut définir sa propre méthode de calcul s'il y a des optimisations très spécifiques, ou pour obtenir des multigraduations.

Dans le cas d'une action par permutation, on obtient le polynôme énumérateur des cycles comme résultat intermédiaire. La Pólya-substitution est partiellement implémentée : on peut faire de l'énumération par poids sur un ensemble fini de valuations. Ceci nous a aussi servi à différentes occasions, par exemple pour énumérer les graphes simples ou les graphes valués dans $\{0, 1, 2\}$. Enfin, on peut obtenir l'énumération fine des chaînes et des secondaires (§ 10.3.2). Dans l'implémentation courante cette énumération fine est très coûteuse. On ne peut par exemple pas traiter le cas des graphes sur 6 sommets. Il doit être possible de l'améliorer, mais une partie de ce coût semble structurel, la série obtenue étant de taille conséquente (≈ 30 termes pour 4 sommets, ≈ 500 termes pour 5 sommets et ≈ 16000 termes pour 6 sommets).

10.3.5 Estimations de la complexité

Pour conclure, nous donnons ici quelques estimations de la complexité du calcul de la série de Hilbert pour les graphes, dans les cas mono et bigradué. Pour cela, nous avons fait des mesures expérimentales avec `MuPAD` sur un PC pentium 450 MHz sous `Linux`, puis nous avons cherché le comportement par ajustement avec `gnuplot`. Le principal intérêt est d'avoir rapidement un ordre de grandeur des ressources nécessaires avant de démarrer un calcul.

Complexité en temps

La figure 10.4 page suivante donne le temps de calcul de la série de Hilbert. Il ne varie guère selon que l'on recherche la série monograduée ou bigraduée. L'essentiel de l'algorithme est une boucle sur toutes les partitions de n. Hardy et Ramajuan [HR18] ont donné l'évaluation asymptotique suivante du nombre $p(n)$ de partitions de n :

$$p(n) \approx \frac{1}{4\sqrt{3}n} \exp \pi \sqrt{\frac{2n}{3}}$$

Il doit donc y avoir dans notre cas un terme principal de cet ordre. Un ajustement par une courbe de la forme $an^b \exp(n^c)$ donne une complexité de l'ordre de $n^4 \exp(n^{0,8})$.

Complexité en mémoire

La figure 10.5 page 151 donne la mémoire utilisée pour le calcul de la série de Hilbert. Cette mémoire sert essentiellement à stocker le polynôme générateur des

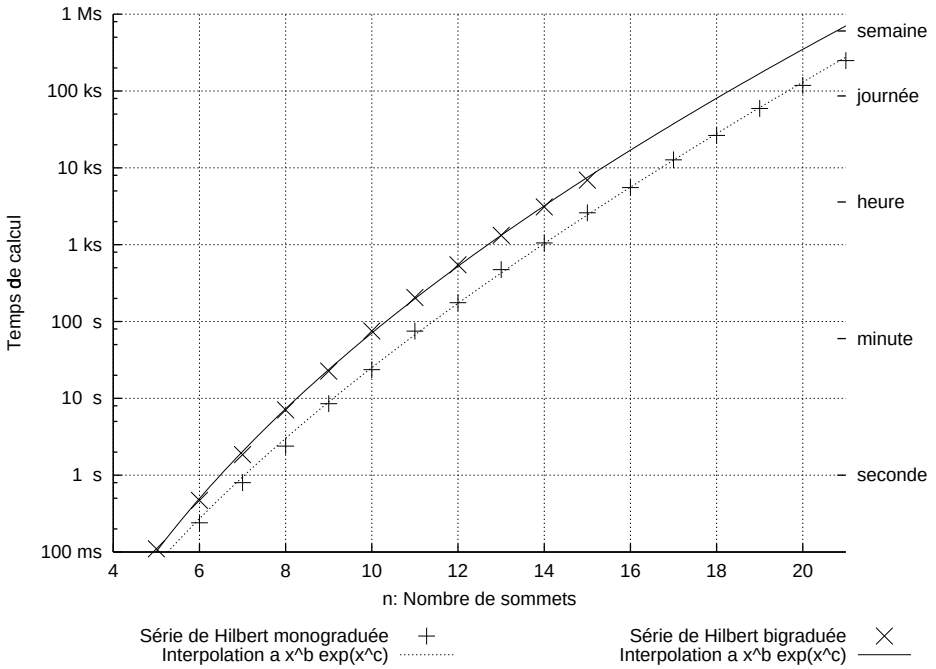


FIG. 10.4 – Temps de calcul de la série de Hilbert en fonction du nombre de sommets

secondaires. Dans le cas monogradué, son nombre de termes est de l'ordre de son degré

$$\mathrm{C}^2_{\mathrm{C}^2_{n-1}} + \mathrm{C}^2_n \approx n^4.$$

Dans le cas bigradué, son nombre de termes est de l'ordre de son degré sur les étoiles, multiplié par son degré sur les graphes 0-réguliers :

$$\mathrm{C}^2_{\mathrm{C}^2_{n-1}} \,.\, \mathrm{C}^2_n \approx n^6.$$

Il faut encore tenir compte de la taille des coefficients qui croît vite, surtout dans le cas monogradué. L'ajustement donne un comportement asymptotique de l'ordre de n^5 en monogradué et n^8 en bigradué. Ceci dit, le comportement est assez irrégulier, et la qualité de l'ajustement est très moyenne.

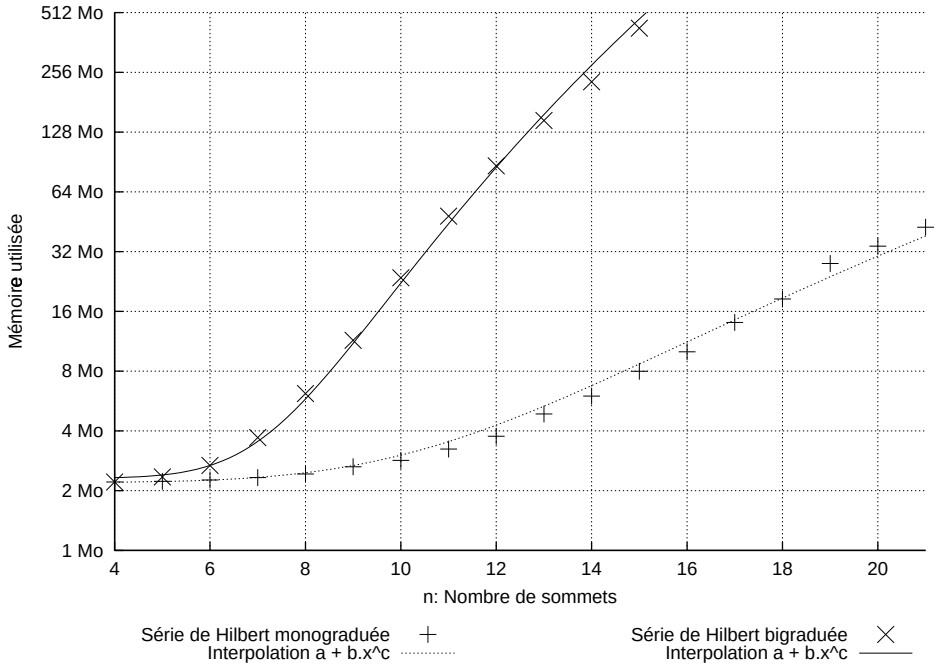


FIG. 10.5 – Mémoire utilisée pour le calcul de la série de Hilbert mono et bigraduée en fonction du nombre de sommets

Chapitre 11

Recherche de générateurs de l'algèbre des invariants

11.1 Préliminaires

Nous allons commencer par examiner les outils dont nous disposons pour montrer qu'un ensemble d'invariants engendre (ou n'engendre pas !) l'algèbre des invariants. Nous omettrons la plupart des démonstrations, que le lecteur pourra trouver traitées en détail dans les introductions classiques [Stu93].

11.1.1 D'un problème d'algèbre à un problème d'algèbre linéaire

Grâce à la graduation de l'algèbre des polynômes invariants, on peut entièrement caractériser un système générateur et un système générateur minimal au moyen d'algèbre linéaire. L'idée sous-jacente est contenue dans la remarque suivante. En quelque sorte, un polynôme homogène de degré d n'a aucune influence sur ceux de degré $< d$. Les remarques et propositions ci-dessous expriment cette idée sous différentes formes, relativement redondantes, mais que nous utiliserons toutes par la suite.

Remarque 11.1.1: Soit B un ensemble de polynômes invariants homogènes. Soit p un polynôme de degré d et $B_{\leq d}$ le sous-ensemble des polynômes de B de degré $\leq d$. Le polynôme p est dans l'algèbre engendrée par B si, et seulement si, il est dans l'algèbre engendrée par $B_{\leq d}$.

Démonstration. Une des implications est triviale. Pour l'autre, on suppose que p est dans l'algèbre engendrée par B, c'est-à-dire

$$p = Q(b_1, \ldots, b_n)$$

Maintenant, comme p est de degré d, il est égal à la somme de ses composantes homogènes de degré $\leq d$. Il en est donc de même pour $Q(b_1, \ldots, b_n)$. Supposons que b_1 soit de degré $> d$. Tous les termes contenant b_1 sont aussi de degré $> d$, et sont

donc éliminés lorsque l'on sélectionne les composantes homogènes de degré $\leq d$ de $Q(b_1, \ldots, b_n)$. Conclusion :

$$p = Q(b_1, \ldots, b_n) = R(b_2, \ldots, b_n).$$

□

Définition 11.1.2 (Système générateur partiel).
Un ensemble B de polynômes invariants homogènes est un système générateur partiel jusqu'au degré *d de l'algèbre des invariants si la sous-algèbre engendrée par B contient tous les polynômes invariants de degré $\leq d$.*

On note que d'après la remarque précédente il est équivalent que B ou $B_{\leq d}$ soit un système générateur partiel jusqu'au degré d.

Proposition 11.1.3.
Soit B un ensemble de polynômes invariants homogènes. On note B_d le sous-ensemble des polynômes de B de degré d. On note E_d le sous-espace vectoriel de $\mathbb{C}[\mathbf{x}]^d$ engendré par des sommes et produits de polynômes invariants de degré $< d$. Les conditions suivantes sont équivalentes :

- *B engendre toute l'algèbre des invariants ;*
- *pour tout d, B_d et E_d engendrent $\mathbb{C}[\mathbf{x}]^d$ en tant qu'espace vectoriel.*

De plus, les conditions suivantes sont encore équivalentes :

- *B est un système minimal de générateurs ;*
- *pour tout d, B_d est une base d'un supplémentaire de E_d dans $\mathbb{C}[\mathbf{x}]^d$.*

Notons que cette proposition et ses corollaires sont valables pour n'importe quelle algèbre graduée A sur un corps $\mathbb{K}$ telle que $A_0 = \mathbb{K}$ et A_d est de dimension finie pour tout d.

La situation est illustrée par la figure 11.1 page suivante. La démonstration de cette proposition est élémentaire. Cependant, nous conseillons au lecteur d'en vérifier soigneusement les détails, car elle est symptomatique de l'utilisation de la graduation pour étudier les polynômes invariants. Comme premier corollaire nous obtenons la proposition 8.1.11 énoncée au § 8. Elle indique que la liste des degrés d'un système générateur minimal ne dépend que de l'algèbre des invariants.

Corollaire 11.1.4.
Soient $\{p_1, \ldots, p_k\}$ et $\{q_1, \ldots, q_l\}$ deux systèmes minimaux de générateurs. On suppose de plus qu'ils sont triés par degré croissant. Alors, $k = l$ et pour tout i, les polynômes p_i et q_i ont même degré.

Corollaire 11.1.5.
B est un système générateur minimal si, et seulement si, pour tout d, l'ensemble $B_{\leq d}$ est un système générateur partiel jusqu'au degré d minimal.

Cela nous donne aussi un algorithme pour extraire un ensemble générateur minimal d'un ensemble générateur B quelconque. On note $B_{<d}$ l'ensemble des éléments de B de degré strictement inférieur à d.

Procédure `Fondamental`(B)

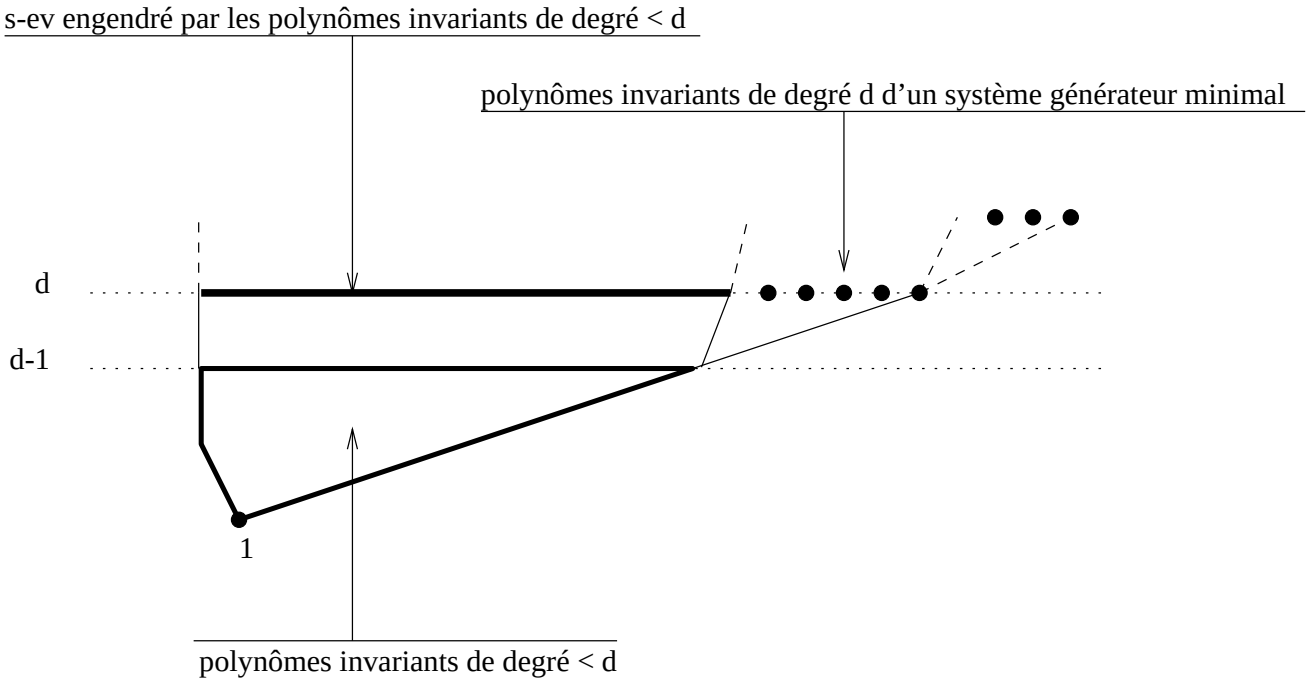


FIG. 11.1 – Disposition au degré d d'un système générateur minimal

$Bmin := 1$

Pour d de 1 jusqu'au plus haut degré de B **Faire**

$L := \{q, q$ produit de degré d d'élément de $B_{<d}\}$

Pour $p \in B_d$ **Faire**

Si p n'est pas dans l'espace vectoriel engendré par L **Alors**

$L := L \cup \{p\}$

$Bmin := Bmin \cup \{p\}$

Fin Si

Fin Pour

Fin Pour

L'étape principale de cet algorithme est un problème d'algèbre linéaire. Heureusement, pour une implémentation réelle, il n'est pas nécessaire d'inverser une matrice à chaque étape. On peut maintenir L sous forme triangulaire en appliquant dessus un pivot de Gauss partiel à chaque fois que l'on insère dedans un nouveau polynôme. Le test d'appartenance à l'espace vectoriel engendré par L est alors relativement rapide. On note que le choix des polynômes dans $Bmin_{<d}$ n'a aucune influence sur le choix de ceux de $Bmin_d$. En effet, les produits dépendent de $Bmin_{<d}$, mais pas le sous-espace vectoriel engendré par ces produits.

Bien entendu, cet algorithme ne peut terminer que si l'on a une borne sur le degré des éléments de B ou, de manière équivalente, si $\mathbb{C}[\mathbf{x}]^d$ est de type fini. Le théorème 8.1.7 nous l'assure et donne une borne D. Nous pourrons l'améliorer considérablement. D'autre part, grâce à l'opérateur de Reynolds on peut avoir un ensemble

de générateurs de l'algèbre. On a donc ce premier algorithme brutal de construction de système minimal d'invariants :

$B := \{m^* : m \text{ monômes de degré } < D\}$

fondamental(B).

Cet algorithme a deux inconvénients principaux. Le premier est que la quantité de produits à engendrer est vite démesurée. De fait, ils ne sont *a priori* pas linéairement indépendants et il y a donc beaucoup de redites. Il serait intéressant de pouvoir en extraire un sous-ensemble minimal. Le second inconvénient est que l'on est obligé de parcourir tous les éléments de B. On aimerait pouvoir appliquer pour chaque d un argument de dimension comme règle d'arrêt. Nous verrons en 11.4 que la structure de Cohen-Macaulay de l'algèbre des invariants permet de passer en bonne partie outre ces inconvénients. On obtiendra alors des algorithmes utilisables dans la pratique, contrairement à celui-là.

11.1.2 D'un problème d'algèbre à un problème d'idéal

Nous allons voir une caractérisation supplémentaire des ensembles générateurs. Cette caractérisation a été découverte par Hilbert pour montrer que l'algèbre des invariants est de type fini.

Théorème 11.1.6 (Hilbert).
Soit $\{p_1, \ldots, p_k\}$ un ensemble fini d'invariants homogènes de degrés strictement positifs. Les conditions suivantes sont équivalentes :
(i) L'algèbre $\mathbb{C}[p_1, \ldots, p_k]$ contient tout l'anneau des invariants ;
(ii) L'idéal $\langle p_1, \ldots, p_k \rangle_{\mathbb{C}[\mathbf{x}]}$ contient tout l'anneau des invariants ;
(iii) L'idéal $\langle p_1, \ldots, p_k \rangle_{\mathbb{C}[\mathbf{x}]^G}$ contient tout l'anneau des invariants.

Nous esquissons la démonstration de ce théorème, car elle illustre bien les techniques usuelles. Elle repose fondamentalement sur l'existence de l'opérateur de Reynolds et sur la graduation de l'anneau des invariants.

Démonstration. Les implications (i) $\Rightarrow$ (ii) et (i) $\Rightarrow$ (iii) sont triviales.

Supposons que l'algèbre des invariants $\mathbb{C}[\mathbf{x}]^G$ soit bien contenue dans l'idéal $\langle p_1, \ldots, p_k \rangle_{\mathbb{C}[\mathbf{x}]}$ mais pas dans l'algèbre $\mathbb{C}[p_1, \ldots, p_k]$. Soit p un polynôme invariant de plus petit degré non contenu dans $\mathbb{C}[p_1, \ldots, p_k]$. Les algèbres considérées étant graduées, on peut supposer que p est homogène. Comme p est dans l'idéal $\langle p_1, \ldots, p_k \rangle_{\mathbb{C}[\mathbf{x}]}$, p s'écrit sous la forme

$$p = I_1 p_1 + \cdots + I_k p_k$$

où $I_1, \ldots, I_k$ sont des polynômes homogènes.

On applique alors l'opérateur de Reynolds et on utilise ses propriétés (propriétés 8.1.5), sachant que p et les p_i sont invariants :

$$p^* = (I_1 p_1)^* + \cdots + (I_k p_k)^* = I_1^* p_1 + \cdots + I_k^* p_k$$

Comme les p_i sont de degrés strictement positifs, les polynômes invariants homogènes $I_1^*, \ldots, I_k^*$ sont de degrés strictement inférieurs à p. Par minimalité du degré de p, ils sont dans $\mathbb{C}[p_1, \ldots, p_k]$ et donc p aussi. Contradiction.

Enfin, pour montrer (ii) $\Rightarrow$ (iii), on peut vérifier en utilisant de manière équivalente l'opérateur de Reynolds que

$$\langle p_1, \ldots, p_k \rangle_{\mathbb{C}[\mathbf{x}]^G} = \langle p_1, \ldots, p_k \rangle_{\mathbb{C}[\mathbf{x}]} \cap \mathbb{C}[\mathbf{x}]^G \tag{11.1}$$

Notons que l'on peut aussi montrer directement par récurrence (iii) $\Rightarrow$ (i) en remarquant que les sous-espaces de $\mathbb{C}[\mathbf{x}]^d$ engendrés par $B_{<d}$ en tant qu'idéal sur $\mathbb{C}[\mathbf{x}]^d$ et en tant qu'algèbre coïncident. □

Cette propriété remarquable permet de se ramener d'un problème d'anneau à un problème d'idéal de $\mathbb{C}[\mathbf{x}]$, ce qui est un progrès considérable. En effet, on a des théorèmes généraux sur les idéaux dont, par exemple, le fameux

Théorème 11.1.7 (dit de la base de Hilbert).
Tout idéal de $\mathbb{C}[\mathbf{x}]$ *est finiment engendré.*

On en déduit que $\mathbb{C}[\mathbf{x}]^d$ est de type fini, comme annoncé par le théorème 8.1.7. De plus, depuis l'apparition des méthodes de calculs de bases de Gröbner, il existe des procédés mécaniques pour traiter la plupart des problèmes sur les idéaux : recherche de générateurs, test d'égalité de deux idéaux, test d'appartenance à un idéal, forme normale modulo un idéal, ... Enfin, le (iii) permet de travailler dans l'idéal engendré dans $\mathbb{C}[\mathbf{x}]^G$ plutôt que dans $\mathbb{C}[\mathbf{x}]$, ce qui évite de casser les symétries. En particulier, à un degré d fixé, la dimension en tant qu'espace vectoriel est beaucoup plus petite. En revanche, il n'y a pas à notre connaissance d'équivalent des procédures de calculs de bases de Gröbner.

11.1.3 Bases SAGBI

Des outils équivalents aux bases de Gröbner ont été développés pour les algèbres (base SAGBI : Subalgebra Analogue to Gröbner Basis for Ideals). Cependant, leur utilisation est plus délicate. En particulier, contrairement aux idéaux, de nombreuses algèbres n'ont pas de base SAGBI finie. Nous renvoyons à [Stu93, p. 91], [Stu96, chap. 11] et [RS90] pour plus de détails. Dans notre cas, nous avons pu montrer que, pour la plupart des ordres usuels sur les monômes, il n'y a pas de base SAGBI finie. Nous ne savons pas s'il existe des ordres pour lesquels la base serait finie.

Théorème 11.1.8.
(i) Soit $<$ *un ordre total quelconque sur les variables* $(x_{1,2}, \ldots, x_{n-1,1})$. *Si* $n \geq 5$, *il n'y a pas de base SAGBI finie pour les ordres lexicographique* $<_{\text{Lex}}$ *ou degré lexicographique* $<_{\text{DegLex}}$ *correspondants sur les monômes.*
(ii) Soit $<$ *un ordre total sur les variables* $(x_{1,2}, \ldots, x_{n-1,1})$ *tel que les* $n-1$ *plus petites variables correspondent à des arêtes adjacentes à un même sommet* v. *Il n'y a pas de base SAGBI finie pour l'ordre* $<_{\text{DegRevLex}}$ *correspondant.*

Le principe de la démonstration est le même dans les deux cas. Nous aurons besoin de la définition suivante.

Définition 11.1.9 (Monôme initial irréductible).
Un monôme initial m *est* irréductible *s'il n'est pas le produit de deux monômes initiaux non triviaux.*

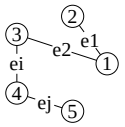
Nous allons construire des familles infinies de monômes initiaux irréductibles. On en déduira que l'algèbre initiale n'est pas finiment engendrée, et qu'il n'y a donc pas de base SAGBI finie.

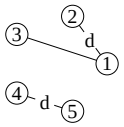
Démonstration. Commençons par traiter le point (i). Soit $e_1, \ldots, e_m$ l'énumération choisie des arêtes, et $x_1, \ldots, x_m$ les variables correspondantes. Soit $<_{\text{Lex}}$ l'ordre lexicographique correspondant sur les monômes (ce qui suit reste valable pour l'ordre degré lexicographique $<_{\text{DegLex}}$, car les monômes initiaux sont les mêmes). Nous montrerons que, à condition de choisir convenablement j, les monômes $m_d = x_1^d x_2 x_j^d$ avec $d > 1$ sont initiaux, tandis que les monômes $x_1^d x_j^d$ ne le sont pas.

Voyons que cela suffit pour conclure : supposons que m_d soit le produit de deux monômes. Par symétrie, ils sont de la forme $m' = x_1^k x_i^l$ et $m'' = x_1^{d-k} x_2 x_i^{d-l}$. Si $k < l$ alors m' n'est pas initial. De même si $k > l$ alors m'' n'est pas initial. On en déduit que $m' = x_1^k x_i^k$ avec $k > 1$ et donc que m' n'est pas initial.

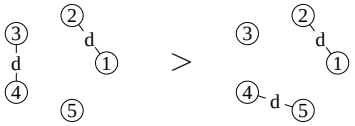
Soit $e_1, \ldots, e_m$ l'énumération choisie des arêtes.

- Premier cas : les arêtes e_1 et e_2 sont adjacentes. Soit $i > 2$ minimal tel que e_i n'est pas adjacente à e_1.
  - (i) e_i et e_2 sont adjacentes. Soit $j > i$ minimal tel que e_j n'est adjacente ni à e_1, ni à e_2. Soit $m_d := x_1^d x_2 x_j^d$.

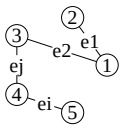


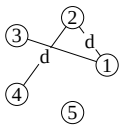
,
$m_d :=$


    On constate que m_d est initial. Par exemple, si l'arête e_j est envoyée sur e_1, les arêtes e_1 et e_2 seront envoyées après e_3, pour préserver l'adjacence. Donc x_2 aura une puissance nulle, et le monôme sera plus petit. De même, si e_1 et e_2 sont fixes, on ne peut pas déplacer e_j avant, puisque j a été choisi minimal.
    En revanche, $x_1^d x_j^d$ n'est pas initial puisque $x_1^d x_i^d$ est plus grand :



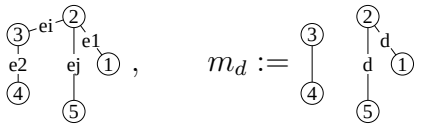
    Les autres cas se traitent de même. Nous nous contentons de donner la construction.
  - (ii) e_i et e_2 ne sont pas adjacentes. Soit $j > i$ minimal tel que e_j est adjacente à e_2 mais pas à e_1. Là encore, on pose $m_d := x_1^d x_2 x_j^d$.



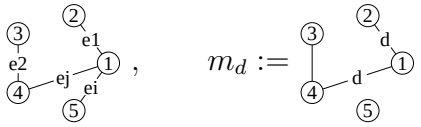
,
$m_d :=$


- Deuxième cas : les arêtes e_1 et e_2 ne sont pas adjacentes. Soit $i > 2$ minimal tel que e_i est adjacente à e_1.

– (i) e_i et e_2 sont adjacentes. Soit $j > i$ minimal tel que e_j est adjacente à e_1, mais pas à e_2.



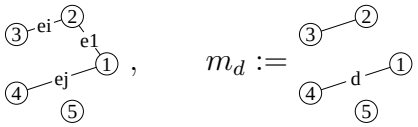
– (ii) e_i et e_2 ne sont pas adjacentes. Soit $j > i$ minimal tel que l'arête e_j est adjacente à e_2 et à e_1.



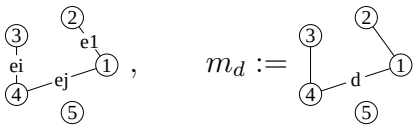
Remarque : la condition $n \geq 5$ a servi implicitement pour assurer l'existence des arêtes lors des constructions.

La démonstration du (ii) suit le même principe et, comme précédemment, on se contente de donner la construction idoine dans chaque cas. On suppose que le point commun aux $n-1$ plus petites arêtes est 1. Soit e_i la plus petite arête non adjacente à 1.

– Premier cas : l'arête la plus petite e_1 est adjacente à e_i. Soit e_j la plus petite arête adjacente à v non-adjacente à e_i.



– Deuxième cas : l'arête la plus petite e_1 n'est pas adjacente à e_i. Soit e_j la plus petite arête adjacente à v et à e_i.



Il est très certainement possible de traiter d'autres cas de façon similaire □

11.1.4 Produit de chaînes

Nous avons vu à la section 10.1.5 que l'on peut définir un deuxième produit à forte connotation combinatoire (dit produit de chaînes) sur l'algèbre des invariants. Un système générateur pour ce produit est générateur pour le produit usuel. Nous renvoyons à la section 10.1.5 pour une discussion sur l'apport de ce produit.

11.1.5 Considérations de dimension

Pour conclure, la série de Hilbert fournit un outil très utile pour la recherche de générateurs. Cette approche est naturelle, puisqu'elle généralise les arguments de dimensions en algèbre linéaire. Cependant, ici il n'existe pas toujours de famille

à la fois libre et génératrice. Aussi, la plupart du temps, cette approche ne pourra donner qu'une condition nécessaire.

Soit $A = \bigoplus A_d$ une sous-algèbre graduée de l'algèbre des invariants. On peut définir sa série de Hilbert $H(A,z) = \sum \dim(A_d) z^d$. Nous appellerons informellement $H(A,z)$ la dimension de A. Une série H sera *dominée* par une série H' si chaque coefficient de H est majoré par le coefficient correspondant de H'. Nous dirons alors que la dimension de A est plus petite que la dimension de A'.

Soit $P = \{p_1, \ldots, p_k\}$ un ensemble fini de polynômes invariants homogènes. On voudrait savoir s'ils engendrent toute l'algèbre des invariants. L'algèbre $\mathbb{C}[p_1, \ldots, p_k]$ engendrée par P est graduée et il suffirait *a priori* de montrer qu'elle est de même dimension que l'algèbre complète des invariants. Comme nous connaissons la dimension totale (cf. 10.3), il suffit d'évaluer la dimension de l'algèbre engendrée. Lorsque les éléments de P sont algébriquement indépendants, on a

$$H(\mathbb{C}[p_1, \ldots, p_k], z) = \frac{1}{\prod_i (1 - z^{d_i})},$$

où d_i est le degré de p_i.

Cependant, nous avons vu au § 8.5 que l'algèbre des invariants ne peut pas être engendrée par des polynômes algébriquement indépendants. Lorsqu'il y a des relations algébriques entre les p_i, la situation est plus complexe. Une relation algébrique entre les p_i (*i.e.* un polynôme P de $\mathbb{C}[Y_1, \ldots, Y_k]$ tel que $P(p_1, \ldots, p_k) = 0$) est appelée *syzygie de première espèce*, ou syzygie. L'ensemble des syzygies sur les p_i forme un idéal I_P de $\mathbb{C}[Y_1, \ldots, Y_k]$. L'algèbre graduée $\mathbb{C}[p_1, \ldots, p_k]$ est isomorphe au quotient de l'algèbre libre $\mathbb{C}[Y_1, \ldots, Y_k]$ sur les p_i par l'idéal I_P. Il faut donc calculer la série de Hilbert de I_P. C'est en théorie possible en déterminant un ensemble de générateurs de I_P. Ces générateurs pourront avoir à leur tour des relations que l'on appellera syzygies de deuxième espèce. Et ainsi de suite, on obtient les syzygies de troisième, quatrième, ... espèces. Le théorème des Syzygies de Hilbert [Sta79, p. 95],[ZS75, Chapitre VII, § 13] assure que ce processus termine. La suite obtenue est appelée résolution libre des p_i.

Des logiciels comme `Macaulay` permettent de déterminer des résolutions libres en utilisant un calcul de base de Gröbner pour trouver des générateurs de l'idéal des relations. Cependant, concrètement on ne peut pas aller au delà de quelques polynômes de petit degré et cela s'est avéré impraticable dans notre cas pour $n \geq 5$. Nous n'avons pas eu non plus l'occasion d'utiliser ce genre de technique d'un point de vue théorique.

Une condition nécessaire

Cependant, à défaut de nous donner une condition suffisante pour que les p_i engendrent $\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$, cela nous fournit une condition nécessaire. Cette condition est valide pour n'importe quelle algèbre graduée, et nous l'énonçons dans ce cadre là.

Condition 11.1.10.
Soient $A := \sum_{d=0}^{\infty} A_d$ une algèbre graduée et $(p_1, \ldots, p_k)$ une famille de k éléments homogènes de degrés strictement positifs $(d_1, \ldots, d_k)$. Si la famille des p_i engendre l'algèbre A, alors la série de Hilbert $H(A,z) = \sum \dim A_d z^d$ est dominée par $\frac{1}{\prod_i (1 - z^{d_i})}$.

Cette condition paraît plutôt faible. Mais toujours est-il qu'elle donne un test simple permettant d'écarter rapidement certaines hypothèses. Ainsi, nous avons pu l'utiliser pour résoudre par la négative une question de Pouzet (voir § 11.2), pour nous guider vers un contre-exemple à un lemme de Grigoriev (voir § 12.1), ou pour montrer qu'il existait des multigraphes et même des graphes simples non algébriquement reconstructibles (voir § 18).

On peut donner une autre condition du même style.

Condition 11.1.11.
Soient $A := \sum_{d=0}^{\infty} A_d$ *une algèbre graduée et* $(p_1, \ldots, p_k)$ *une famille de* k *éléments homogènes de degrés respectifs* $(d_1, \ldots, d_k)$. *Soit* $s(z) := z^{d_1} + \cdots + z^{d_k}$ *leur série génératrice. Si la famille des* p_i *engendre l'algèbre* A, *alors la série de Hilbert* $H(A, z) = \sum \dim A_d z^d$ *est dominée par la série* $H(A, z)s(z)$.

Démonstration. Si la famille $(p_1, \ldots, p_k)$ engendre A en tant qu'algèbre, elle engendre aussi A en tant qu'idéal. Tout élément p de degré d se met donc sous la forme

$$p = f_1 p_1 + \cdots + f_k p_k,$$

où f_i est un élément de A de degré $d - d_i$. On en déduit que la dimension de A_d est majorée par

$$c_d := \dim A_{d-d_1} + \dim A_{d-d_2} + \cdots + \dim A_{d-d_k}.$$

Ce coefficient est précisément le coefficient de degré d du produit $H(A, z)s(z)$. □

D'après notre expérience, la première condition donne généralement des résultats plus fins, surtout lorsqu'il y a peu de relations entre les générateurs. Cependant la deuxième condition peut se révéler intéressante, car on peut, dans certains cas, en tirer des informations supplémentaires, comme une minoration du nombre de générateurs de tel ou tel degré (voir, par exemple, § 19.3).

11.2 Les graphes simples n'engendrent pas tous les invariants

Une approche pour essayer de trouver des générateurs est de tenter de généraliser les propriétés des polynômes symétriques. Or, ceux-ci sont engendrés par les polynômes symétriques élémentaires, c'est-à-dire les polynômes symétriques dans lesquels les variables sont élevées seulement à des puissances 0 ou 1. Par analogie, appelons *polynômes invariants élémentaires* les polynômes invariants $\mathbf{x}^{\mathbf{g}\circledast}$ associés aux graphes simples $\mathbf{g}$. Pouzet avait soulevé le problème suivant :

Problème 11.2.1.
L'algèbre des invariants sur les graphes est-elle engendrée par les polynômes invariants élémentaires.

Pour alléger, nous confondons ici chaque graphe simple ou multigraphe $\mathbf{m}$ avec le polynôme invariant $\mathbf{x}^{\mathbf{m}\circledast}$ correspondant. Ce problème se reformule comme suit : les multigraphes sont engendrés par les graphes simples.

Observation 11.2.2.
Le polynôme symétrique élémentaire de degré d sur les arêtes est la somme des graphes simples à d arêtes. Donc les graphes simples engendrent tous les polynômes symétriques sur les arêtes.

Théorème 11.2.3.
Pour $n = 2, 3, 4$, tous les multigraphes sont engendrés par les graphes simples.

Démonstration. Pour $n = 2$ ou 3, les polynômes invariants coïncident avec les polynômes symétriques et la proposition est donc trivialement vraie.

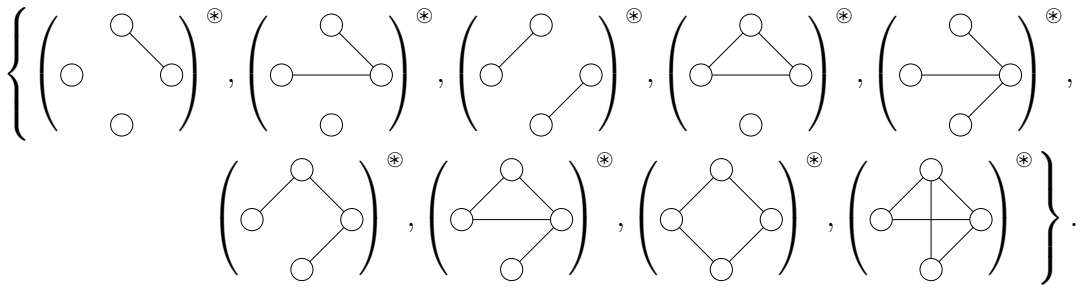
Pour $n = 4$, cela demande plus de travail.

Dans le cadre de notre DEA, nous l'avions montré par un calcul brutal en utilisant `Maple`. Ce calcul n'était à l'époque pas parfaitement terminé. Nous l'avons repris un peu plus tard avec `CoCoA` et avec quelques optimisations. Voici la méthode : le théorème 8.2.6 donne un ensemble fini P de multigraphes qui engendrent tous les multigraphes. Nous avons alors calculé une base de Gröbner de l'idéal engendré par les graphes simples et vérifié que chaque multigraphe de P était dans l'idéal. Donc les graphes simples engendrent, au sens d'idéal, tous les multigraphes et on conclut en utilisant le théorème 11.1.6. Pour donner un ordre de grandeur, la base de Gröbner comporte 33 polynômes et il faut tester 120 polynômes de degré ≤ 15. Sur un Pentium 133 et avec `CoCoA` le calcul dure environ 3 heures, dont $\frac{1}{2}$ heure pour le calcul de base de Gröbner.

Note 11.2.4: Pour 5 sommets et plus, ce type de méthode est complètement impraticable. Même avec `GB` le calcul de la base de Gröbner explose très rapidement. De toutes façons, il faudrait tester 3 millions de polynômes de degré ≤ 45.

En utilisant les algorithmes de constructions d'invariants secondaires (voir section 11.4) on peut réduire le calcul à moins de 20 secondes pour $n = 4$. Ces algorithmes utilisent au mieux la décomposition de Hironaka de l'algèbre des invariants. Cependant, pour $n = 5$ le calcul est encore impraticable, du moins tant que l'on n'aura pas une meilleure majoration de la borne $\beta(n)$ sur les degrés des générateurs.

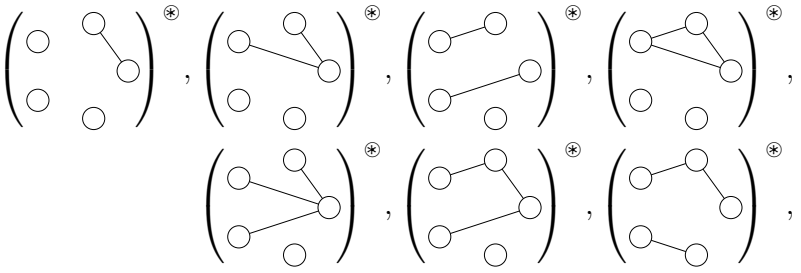
À peu près à la même époque, Aslaksen et al. [ACG96] ont aussi montré indépendamment ce théorème en donnant l'ensemble suivant de générateurs :



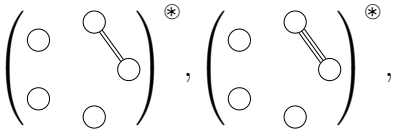
Leur démonstration réduit considérablement la quantité de calculs nécessaires en utilisant convenablement la décomposition des graphes en étoiles et graphes 0-réguliers et la décomposition de Hironaka de l'algèbre des invariants. Notons que Aslaksen et al. étudiaient cette algèbre dans un cadre très différent (étude d'ensembles de vecteurs à isométrie près) et l'interprétation de leurs invariants sous forme de graphes simples n'apparaît pas dans leur article. □

Nous allons voir maintenant que cela ne se généralise pas au delà, c'est-à-dire pour 5 sommets ou plus. En fait l'argument est très simple, puisque la condition nécessaire 11.1.10 n'est pas vérifiée. Convaincu de la faiblesse de ce test, nous ne l'avons appliqué que tardivement et nous avons été surpris par la réponse.

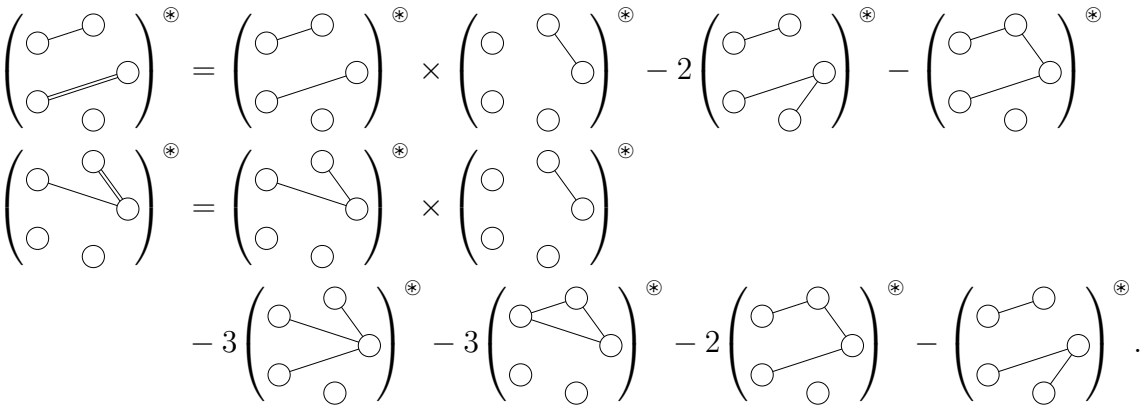
Pour les multigraphes de degrés $1, 2, 3$, il n'y a pas de problème. Il y a d'abord les graphes simples eux mêmes :



puis les polynômes symétriques :



et enfin deux exponentielles symétrisées de multigraphes qui s'obtiennent aisément :



En revanche, dès le degré 4 la situation change :

Théorème 11.2.5.
Pour tout $n \geq 5$, il y a au moins un multigraphe de degré 4 sur n sommets qui n'est pas engendré par les graphes simples.

Démonstration. Comme annoncé, l'argument de dimension va pouvoir s'appliquer. L'homogénéité des polynômes est ici encore un point clef. Elle nous permet d'être assurés que les polynômes de degré 4 ne peuvent être engendrés que par des graphes comportant au plus 4 arêtes. Il y en a 1 de degré 1, 2 de degré 2, 4 de degré 3 et 6 de degré 4. S'ils étaient algébriquement indépendants, la série de Hilbert de l'algèbre engendrée serait :

$$\begin{aligned} F_5(z) &= \frac{1}{(1-z)\,(1-z^2)^2\,(1-z^3)^4\,(1-z^4)^6} \\ &= 1 + z + 3z^2 + 7z^3 + 16z^4 + O(z^5). \end{aligned}$$

En comparant avec la série de Hilbert des polynômes invariants,

$$H(\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_5}, z) = 1 + z + 3z^2 + 7z^3 + 17z^4 + O(z^5),$$

on voit qu'au moins un multigraphe de degré 4 n'est pas engendré.

On peut opérer de même pour $6, 7, 8$ sommets. Il n'est pas nécessaire d'aller plus loin. En effet, à partir de $n = 8$, le nombre de graphes simples et de multigraphes de degré au plus 4 ne change plus. Pour des détails sur le calcul des séries de Hilbert et du nombre de graphes simples par degré, voir la section 10.3.

$$\begin{aligned} F_6(z) &= 1 + z + 3z^2 + 8z^3 + 20z^4 + O(z^5), \\ H\left(\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_6}, z\right) &= 1 + z + 3z^2 + 8z^3 + 21z^4 + O(z^5), \end{aligned}$$

$$\begin{aligned} F_7(z) &= 1 + z + 3z^2 + 8z^3 + 21z^4 + O(z^5), \\ H\left(\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_7}, z\right) &= 1 + z + 3z^2 + 8z^3 + 22z^4 + O(z^5), \end{aligned}$$

$$\begin{aligned} F_8(z) &= 1 + z + 3z^2 + 8z^3 + 22z^4 + O(z^5), \\ H\left(\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_7}, z\right) &= 1 + z + 3z^2 + 8z^3 + 23z^4 + O(z^5). \end{aligned}$$

□

Généralisations

Jusqu'ici, on s'est restreint à des valuations 0 et 1 sur chaque arête. Peut-être suffirait-il d'autoriser quelques valuations supplémentaires pour engendrer tous les multigraphes.

Problème 11.2.6.
L'algèbre des invariants est-elle engendrée par les multigraphes valués dans $\{0, 1, 2\}$ *?*

Sinon, quel est le plus petit entier d *tel que l'algèbre des invariants est engendrée par les multigraphes valués dans* $\{0, 1, \ldots, d\}$ *?*

D'après ce que nous venons de voir, $d = 1$ si $n \leq 3$ et $d \geq 2$ si $n \geq 5$. De plus, on déduit du théorème 8.2.6 que $d < \mathrm{C}_n^2$. Pour $n = 5$, nous avons pu vérifier que les multigraphes valués dans $\{0, 1, 2\}$ engendrent tous les multigraphes jusqu'au degré 10 (voir § 11.4). Un résultat général de cette nature serait très intéressant pour le problème de reconstruction, car il réduit le problème de reconstructibilité algébrique des polynômes invariants aux seuls polynômes invariants de degré $\leq \mathrm{C}_n^2$. En particulier, cela clôturerait le cas $n = 5$.

Dans [Gri79], le lemme I indique que l'algèbre des invariants sur les digraphes est engendrée par les polynômes invariants élémentaires, et nous aurions pu en déduire que $d = 2$, comme voulu. Cependant, ce lemme s'est avéré faux (voir § 12.1).

Nos calculs indiquent que, pour le produit de chaînes, il est nécessaire de considérer des multigraphes valués 3 ou plus.

À défaut de mieux, nous avons le résultat partiel suivant :

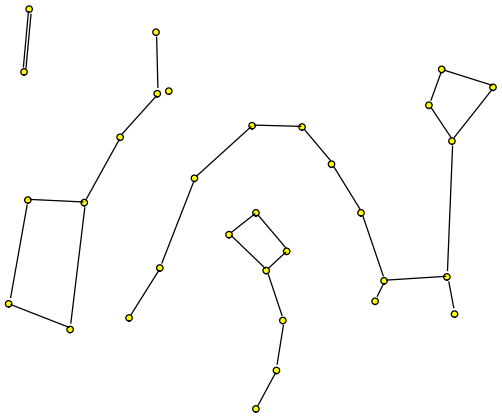


FIG. 11.2 – Exemple de multigraphe obtenu dans le développement des polynômes élémentaires en les étoiles

Proposition 11.2.7.
Les polynômes symétriques en les étoiles sont engendrés par les multigraphes valués dans $\{0,1,2\}$. *Plus précisément, les polynômes symétriques en les étoiles sont engendrés par les graphes avec au plus* n *arêtes et au plus un cycle dans chaque composante connexe. Le cycle peut être réduit à deux sommets, donnant une double arête. La figure 11.2 en donne un exemple.*

Démonstration. On rappelle que les polynômes symétriques en les étoiles sont les polynômes symétriques en les n variables E_i où $E_i := \sum_{h \neq i} x_{\{i,j\}}$. Ces polynômes sont engendrés par les polynômes symétriques élémentaires. Soit e_k le k-ième polynôme symétrique élémentaire en les étoiles :

$$e_k := \sum_{i_1 < i_2 < \cdots < i_k} E_{i_1} E_{i_2} \ldots . E_{i_k}$$

Soit $\mathbf{g}$ un graphe dont le monôme $\mathbf{x}^{\mathbf{g}^{\circledast}}$ apparaît dans le développement d'un des produits $E_{i_1} E_{i_2} \ldots . E_{i_k}$. $\mathbf{g}$ a k arêtes, chacune prise dans une étoile E_i. On peut donc associer de manière unique à chaque arête de $\mathbf{g}$ un de ses sommets adjacents. Sur une composante connexe il y a donc au moins autant de sommets que d'arêtes, ce qui permet au plus un cycle. □

Notons que les doubles arêtes sont réellement nécessaires. Un petit calcul avec `MuPAD` montre que, sur 5 sommets, le polynôme e_4 symétrique élémentaire de degré 4 en les étoiles n'est pas engendré par les graphes. Pour cela, il nous a suffi de considérer l'ensemble des produits de graphes donnant un polynôme de degré 4 et de vérifier que e_4 n'était pas dans l'espace vectoriel engendré par ces produits.

11.3 Invariants primaires

11.3.1 Motivations

Comme nous l'avons vu au § 8.2 les polynômes symétriques élémentaires fournissent immédiatement un système d'invariants primaires. De plus, ces invariants primaires ont de très bonnes propriétés. Tout d'abord, ils se comportent bien vis à vis du type de problèmes auxquels nous nous intéressons. Il est par exemple trivial de montrer qu'ils sont algébriquement reconstructibles ou engendrés par les graphes.

Ensuite, ils se prêtent bien à la recherche d'invariants secondaires. On connaît parfaitement l'algèbre engendrée ; on connaît une base de Gröbner de l'idéal engendré, ce qui permet de faire aisément des calculs dans le quotient. Enfin, Garsia et Stanton [GS84] ont développé un certain nombre de techniques dans ce cas là (cf. § 10.1.5). Ces techniques sont d'autant plus intéressantes qu'elles créent un lien explicite avec la structure combinatoire sous-jacente.

Cependant, il apparaît nécessaire de trouver d'autres invariants primaires, pour diminuer la complexité des invariants secondaires, et pour améliorer la majoration de la borne $\beta(n)$. Nous rappelons que le nombre et les degrés des invariants secondaires sont uniquement déterminés par les degrés des invariants primaires (proposition 8.1.11) :

$$t = \frac{\prod d_i}{|G|} \qquad \text{et} \qquad e_t = \sum (d_i - 1) - \mu_n,$$

où μ_n est le degré du plus petit polynôme antisymétrique pour l'action du groupe. Or, si l'on utilise les polynômes symétriques élémentaires, t et e_t sont vite élevés :

n	$t = \frac{\mathrm{C}_n^2!}{n!}$	$e_t = \mathrm{C}^2_{\mathrm{C}_n^2} - \mu_n$
4	30	15
5	30240	42
6	$1,8.10^9$	106

où t est le nombre d'invariants secondaires et e_t leur plus haut degré. Le terme correctif μ_n est nul si n est pair et vaut $\mu_n = \left\lceil \frac{3}{4}(n-1) \right\rceil$ si n est impair (théorème 11.4.1).

Dans la suite, nous allons proposer un autre système d'invariants primaires pour lesquels on obtiendrait :

n	$t = \mathrm{C}^2_{n-1}!$	$e_t = \mathrm{C}^2_n + \mathrm{C}^2_{\mathrm{C}^2_{n-1}} - \mu_n$
4	6	9
5	720	22
6	$3,6.10^6$	60

La différence est considérable ! De plus, si l'on ne recherche que les invariants sur les graphes 0-réguliers[1], ce système d'invariants primaires donne :

n	$t = \frac{C_{n-1}^2!}{n!}$	$e_t = C_{C_{n-1}^2}^2 - \mu_n$
4	1	0
5	6	15
6	5040	40

Notre principale motivation a été de chercher des invariants primaires pour lesquels la construction par ordinateur des invariants secondaires soit envisageable dans le cas $n = 5$. On ne connaît pas de système d'invariants primaires raisonnablement optimal pour les représentations irréductibles du groupe symétrique, en dehors des cas triviaux ($[n]$, $[n-1,1]$, etc.) et des petits cas [Dix91]. Par « raisonnablement optimal », nous entendons de petits degrés. Nous espérons en fournir pour la représentation $[n-2,2]$. Notons qu'il existe des algorithmes de recherche d'invariants primaires optimaux [Kem98a], mais ceux-ci ne parviennent pas à traiter le cas $n = 5$. Enfin, Dixmier [Dix91] a construit un système *ad hoc* d'invariants primaires pour la représentation $[3,2]$ de degrés identiques à ceux que nous proposerons, mais nous n'avons pas réussi à le généraliser.

Nous allons présenter les méthodes que nous avons utilisées pour rechercher des candidats. Puis, nous proposerons, pour tout n, un système d'invariants. Nous conjecturons qu'il s'agit d'un système d'invariants primaires. Nous avons pu le montrer jusqu'à $n = 5$ par le calcul. Au delà, nous étayerons cette conjecture sur une étude de la série de Hilbert, en nous appuyant sur une conjecture de Mallows et Sloane.

11.3.2 Degrés des invariants primaires

Utilisation de la série de Hilbert

Nous cherchons donc m polynômes invariants $(\theta_1, \ldots, \theta_m)$ de sorte que $\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$ soit un module libre sur $\mathbb{C}[\theta_1, \ldots, \theta_m]$. Le théorème 8.1.24 nous donne une caractérisation : il faut et il suffit que $\mathbf{x}_{\{i,j\}} = 0$ soit la seule solution au système d'équations

$$\theta_1(\mathbf{x}_{\{i,j\}}) = \cdots = \theta_m(\mathbf{x}_{\{i,j\}}) = 0.$$

Pour orienter les recherches, il serait utile d'avoir des informations supplémentaires sur d'éventuels candidats. L'étude de la série de Hilbert va nous fournir ici de précieuses informations. En effet, si $(\theta_1, \ldots, \theta_m)$ est un système d'invariants primaires de degrés respectifs $(d_1, \ldots, d_m)$, on peut calculer la série génératrice des degrés $e_1, \ldots, e_t$ des invariants secondaires :

$$\sum_{i=1}^{t} z^{e_i} = H(\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}, z)(1 - z^{d_1})(1 - z^{d_2}) \cdots (1 - z^{d_m}).$$

[1] Nous rappelons que la reconstruction de ces derniers polynômes suffirait presque à montrer la conjecture de Ulam pour les graphes simples ! En effet, cela montrerait la reconstructibilité de la partie régulière d'un graphe. Le théorème 5.5.1 nous assure alors que, à quelques exceptions près, cela suffit pour déterminer un graphe simple.

Cela montre que n'importe quel choix de degrés ne peut pas convenir, puisqu'il serait bienvenu que le résultat obtenu soit un polynôme à coefficients entiers positifs. Cela nous donne une condition nécessaire. Est-elle suffisante ? Autrement dit, étant donnés m entiers $d_1, \ldots, d_m$, si le polynôme obtenu est à coefficients entiers positifs, existe-t-il un système d'invariants primaires ayant les d_i comme degrés ? Il s'agit d'une conjecture de Mallows et Sloane [MS73]. Depuis des contre-exemples ont été trouvés, mais la conjecture est encore ouverte dans le cas de représentations irréductibles. Pour une discussion plus approfondie, voir [Dix91, p. 5].

On notera que, pour une représentation réductible, il suffit de travailler sur la série de Hilbert multigraduée au lieu de la série de Hilbert classique. Prenons un exemple. Supposons que notre espace V se décompose en deux irréductibles V_1 et V_2. Soit $H = H(V, z_1, z_2)$ la série de Hilbert bigraduée de V. Soient $(d_{1,1}, \ldots, d_{1,m_1})$ et $(d_{2,1}, \ldots, d_{2,m_2})$ deux suites d'entiers de sorte que

$$P := H(1 - z_1^{d_{1,1}}) \ldots (1 - z_1^{d_{1,m_1}})(1 - z_2^{d_{2,1}}) \ldots (1 - z_2^{d_{2,m_2}})$$

soit un polynôme à coefficients entiers positifs. Plaçons nous sur la première composante irréductible. Si on substitue $z_2 = 0$ dans H, on obtient la série de Hilbert $H_1 = H(\mathbb{C}[V_1]^G, z_1)$ des invariants de V_1. Si on substitue de même $z_2 = 0$ dans P, on obtient

$$P_1 := H_1(1 - z_1^{d_{1,1}}) \ldots (1 - z_1^{d_{1,m_1}}),$$

qui est donc aussi un polynôme à coefficients entiers positifs. La conjecture de Mallows et Sloane nous donnerait alors des invariants primaires sur V_1 et de même sur V_2. Grâce à la remarque 8.3.1, on obtient alors des invariants primaires de V de degrés $(d_{1,1}, \ldots, d_{1,m_1}, d_{2,1}, \ldots, d_{2,m_2})$.

Une proposition de degrés

Nous avons donc étudié les séries de Hilbert jusqu'à $n = 16$. Nous avons trouvé que la suite de degrés suivante convenait :

$$(1, \ldots, n, 2, \ldots, \mathrm{C}_{n-1}^2).$$

Pour certains entiers, on peut faire un peu mieux (remplacement d'un 14 par un 7 par exemple), mais ce n'est pas systématique. Le $(1, \ldots, n)$ correspond à l'espace des étoiles $([n] \oplus [n-1, 1])$. On peut effectivement prendre les n polynômes symétriques élémentaires en les étoiles comme invariants primaires. Cela nous a suggéré la conjecture suivante :

Conjecture 11.3.1.
Il existe un système d'invariants primaires sur les graphes 0-réguliers $([n-2, 2])$ de degrés $(1, \ldots, \mathrm{C}_{n-1}^2)$.

Cohérence avec la série de Hilbert pour tout n

Pour étayer cette conjecture il serait bon d'être assurés de la cohérence avec la série de Hilbert pour tout n, c'est-à-dire que nous obtenons bien un polynôme à

coefficients entiers positifs pour la série génératrice des secondaires. Nous l'avons vérifié par ordinateur jusqu'à $n = 12$ pour la série bigraduée et jusqu'à $n = 15$ pour la série monograduée. Au delà, nous avons montré un résultat partiel.

Théorème 11.3.2.
Le produit suivant est un polynôme. Ses coefficients sont de la forme $\frac{i}{n!}$ *où* $i \in \mathbb{Z}$.

$$H\left(\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}, z_1, z_2\right)\ (1-z_1)\dots(1-z_1^n)(1-z_2^2)\dots(1-z_2^{\mathrm{C}_{n-1}^2}).$$

Démonstration. On utilise la formule 10.5 pour calculer la série de Hilbert.

$$\begin{aligned}&H\left(\mathbb{C}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}, z_1, z_2\right)\ (1-z_1)\dots(1-z_1^n)(1-z_2^2)\dots(1-z_2^{\mathrm{C}_{n-1}^2})\\ &= \frac{1}{|\mathfrak{S}_n|}\sum_{\sigma\in\mathfrak{S}_n}\frac{\det(\mathrm{Id}-z_2M_1)}{\det(\mathrm{Id}-z_1M_1)\det(\mathrm{Id}-z_2M)}(1-z_1)\dots(1-z_1^n)(1-z_2^2)\dots(1-z_2^{\mathrm{C}_{n-1}^2}),\end{aligned}$$

où M_1 et M sont les matrices respectives de chaque permutation σ sur les étoiles et les graphes.

Le lemme qui suit nous montrera que chaque terme de la somme donne un polynôme à coefficients entiers, ce qui terminera la démonstration. □

Lemme 11.3.3.
Soient σ *une permutation et* M_1 *et* M *les matrices respectives des représentations de* σ *sur les étoiles et les graphes. L'expression suivante est un polynôme à coefficients entiers.*

$$\frac{\det(\mathrm{Id}-z_2M_1)}{\det(\mathrm{Id}-z_1M_1)\det(\mathrm{Id}-z_2M)}(1-z_1)\dots(1-z_1^n)(1-z_2^2)\dots(1-z_2^{\mathrm{C}_{n-1}^2}).$$

On a besoin du sous-lemme suivant :

Lemme 11.3.4.
Soient n *un entier et* $\lambda = (\lambda_1 \geq \lambda_2 \geq \dots \geq l_k)$ *avec* $\lambda_1 + \dots + \lambda_k \leq n$. *La fraction suivante est un polynôme à coefficients entiers :*

$$\frac{(1-z^{1+l})(1-z^{2+l})\dots(1-z^{n+l})}{(1-z^{\lambda_1})(1-z^{\lambda_2})\dots(1-z^{\lambda_k})}$$

Si de plus $\lambda \neq (\underbrace{1,\dots,1}_{n})$, *la fraction suivante reste encore un polynôme à coefficients entiers.*

$$\frac{(1-z^{2+l})\dots(1-z^{n+l})}{(1-z^{l_1})(1-z^{\lambda_2})\dots(1-z^{\lambda_k})}$$

Démonstration. On va assigner de manière unique à chaque i un entier d_i de $1+l,\dots,n+l$ de sorte que λ_i divise d_i. On aura alors pour chaque i

$$\frac{(1-z^{d_i})}{(1-z^{\lambda_i})} = 1 + z^{\lambda_i} + z^{2\lambda_i} + \dots + z^{d_i-\lambda_i}$$

La fraction totale sera donc un polynôme à coefficients entiers.

Commençons par 1. Soit d le plus grand multiple de λ_1 dans $1+l,\dots,n+l$. On pose $d=l$.

Supposons que $d_1,\dots,d_{i-1}$ soient déjà définis. Dans $1+l,\dots,n+l$, il y a $\lfloor\frac{n}{\lambda_i}\rfloor$ multiples de λ_i. Or, $\lambda_1+\cdots+\lambda_{i-1}\leq n$, donc comme les λ_j sont rangés par ordre décroissant, $(i-1)\lambda_i\leq n$, d'où $i\leq\lfloor\frac{n}{\lambda_i}\rfloor-1$. Il y a donc au moins un multiple de λ_i qui n'a pas déjà été assigné. Soit d le plus grand d'entre eux. On pose $d_i=d$.

Et ainsi de suite jusqu'au dernier.

Étant donné qu'à chaque étape on prend le plus grand multiple disponible, $1+l$ ne sera assigné que si $\lambda=(1,\dots,1)$. En dehors de ce cas, on peut donc enlever le terme $(1-z)^{1+l}$ et continuer d'obtenir un polynôme à coefficients entiers. □

Démonstration. Soient $\sigma\in\mathfrak{S}_n$ et $(c_1,\dots,c_k)$ les longueurs des cycles de σ. Comme M_1 et M sont des matrices de permutations, leurs polynômes caractéristiques se calculent aisément. On a

$$\det(\mathrm{Id}-zM_1)=\prod_i(1-z^{c_i})$$

et, en utilisant la proposition 10.3.4,

$$\det(\mathrm{Id}-zM)=\prod_{c_i\text{pair}}(1-z^{c_i})^{\frac{c_i}{2}-1}(1-z^{\frac{c_i}{2}})\prod_{c_i\text{impair}}(1-z^{c_i})^{\frac{i-1}{2}-1}\prod_{i,j}(1-z^{c_i\vee c_j})^{c_i\wedge c_j}$$

Nous n'aurons pas besoin de regarder précisément tous les termes. En posant a_1 et a_2 le nombre de cycles de longueur 1 et 2, on factorise l'expression précédente comme suit

$$\det(\mathrm{Id}-zM)=\prod_{c_i>2}(1-z^{c_i})(1-z)^{a_2}(1-z)^{\mathrm{C}^2_{a_1}}(1-z^2)^{\mathrm{C}^2_{a_2}}(1-z^2)^{a_1a_2}P$$

où P est un polynôme de la forme $\prod_i(1-z^{d_i})$. On calcule alors le terme correspondant à σ :

$$\begin{aligned}H_\sigma&=\frac{\det(\mathrm{Id}-z_2M_1)}{\det(\mathrm{Id}-z_1M_1)\det(\mathrm{Id}-z_2M)}(1-z_1)\dots(1-z_1^n)(1-z_2^2)\dots(1-z_2^{\mathrm{C}^2_{n-1}})\\&=\frac{(1-z_1)\dots(1-z_1^n)}{\prod_i(1-z_1^{c_i})}\frac{\prod_i(1-z_2^{c_i})}{\prod_{c_i>2}(1-z_2^{c_i})}\frac{(1-z_2^2)\dots(1-z_2^{\mathrm{C}^2_{n-1}})}{(1-z_2)^{a_2}(1-z_2)^{\mathrm{C}^2_{a_1}}(1-z_2^2)^{\mathrm{C}^2_{a_2}}(1-z_2^2)^{a_1a_2}P}\\&=\frac{(1-z_1)\dots(1-z_1^n)}{\prod_i(1-z_1^{c_i})}\quad\frac{(1-z_2)^{a_1}(1-z_2^2)^{a_2}\quad(1-z_2^2)\dots(1-z_2^{\mathrm{C}^2_{n-1}})}{(1-z_2)^{\mathrm{C}^2_{a_1}+a_2}(1-z_2^2)^{\mathrm{C}^2_{a_2}+a_1a_2}P}\end{aligned}$$

Le lemme 11.3.4 s'applique immédiatement au premier terme qui est donc un polynôme. Soit T l'autre terme.

Dans les deux cas extrêmes suivants, on vérifie que le dénominateur est de degré $\mathrm{C}^2_{n-1}-1$, ce qui permet d'appliquer le lemme 11.3.4 :

– $a_1=n\geq 3$:

$$\frac{(1-z_2^2)\dots(1-z_2^{\mathrm{C}^2_{n-1}})}{(1-z_2)^{\mathrm{C}^2_n-n}},$$

– $a_1 = a_2 = 0$:

$$\frac{(1-z_2^2)\dots(1-z_2^{\mathrm{C}^2_{n-1}})}{P}.$$

Dans les deux cas restant, on factorise T de telle sorte qu'apparaisse au dénominateur du deuxième facteur un polynôme de degré C^2_{n-1}. On appliquera alors la deuxième version du lemme 11.3.4.

– $a_1 = 0$ et $a_2 \geq 1$:

$$(1+z_2)\,\frac{(1-z_2^2)\dots(1-z_2^{\mathrm{C}^2_{n-1}})}{(1-z_2)^{a_2-1}(1-z_2^2)^{\mathrm{C}^2_{a_2}-a_2+1}P},$$

– $n > a_1 \geq 1$:

$$(1-z_2)\,\frac{(1-z_2^2)\dots(1-z_2^{\mathrm{C}^2_{n-1}})}{(1-z_2)^{\mathrm{C}^2_{a_1}+a_2-a_1+1}(1-z_2^2)^{\mathrm{C}^2_{a_2}+a_1a_2-a_2}P}.$$

□

11.3.3 Une proposition d'invariants primaires

Après quelques tâtonnements, nous avons proposé le système suivant d'invariants primaires.

Conjecture 11.3.5.
Symétriques en les étoiles + symétriques projetés ou pas.

Proposition 11.3.6.
La conjecture 11.3.5 est vérifiée pour $n \leq 5$.

Démonstration. On note que les polynômes symétriques en les étoiles forment bien un système d'invariants primaires pour l'espace des Étoiles. D'après la remarque 8.3.1, il suffit donc de vérifier que les polynômes symétriques de degré $2, \dots, \mathrm{C}^2_{n-1}$ forment un système de paramètres pour les graphes 0-réguliers.

Pour $n \leq 3$, cette conjecture est triviale, puisque le seul graphe 0-régulier est 0. Pour $n = 4$, on utilise la caractérisation 8.1.24. Il faut vérifier qu'un graphe 0-régulier tel que $\sum x^2_{\{i,j\}} = 0$ et $\sum x^3_{\{i,j\}} = 0$ est le graphe nul. Pour cela, on écrit ces deux polynômes dans la base de régularisation (proposition 4.4.1), c'est-à-dire que l'on substitue $x_{i,n}$ par $-\sum_{j\neq i, j\neq n} x_{\{i,j\}}$. On obtient alors comme système d'équations

$$\begin{aligned} x_{1,2} + x_{2,3} + x_{1,3} &= 0,\\ x_{1,2}^2 + x_{2,3}^2 + x_{1,3}^2 + (-x_{1,2} - x_{1,3})^2 + (-x_{1,2} - x_{2,3})^2 + (-x_{1,3} - x_{2,3})^2 &= 0,\\ x_{1,2}^3 + x_{2,3}^3 + x_{1,3}^3 + (-x_{1,2} - x_{1,3})^3 + (-x_{1,2} - x_{2,3})^3 + (-x_{1,3} - x_{2,3})^3 &= 0. \end{aligned}$$

On constate que les trois polynômes sont symétriques, ce qui n'est pas étonnant, vu que pour $n = 4$ la représentation sur les graphes réguliers est la représentation naturelle du groupe symétrique $\mathfrak{S}_3$ (par permutation des trois vecteurs de la base

donnée dans l'équation 4.1). On montre alors aisément à la main que les sommes de puissances des $x_{\{i,j\}}$ sont nulles et donc que les $x_{\{i,j\}}$ sont nuls.

Pour $n = 5$, on obtient un système de degré 6, composé de polynômes non-symétriques qu'il n'est pas envisageable de résoudre à la main. Nous avons donc utilisé le test mécanique de la proposition 8.1.25. Le problème de ce test réside dans le calcul de la base de Gröbner. Si on l'applique directement au système complet de paramètres, ce calcul ne termine pas, du moins pas dans un temps raisonnable. Il en est de même avec le système partiel de paramètres si le choix de la base et de l'ordre sur les monômes n'est pas convenable. Cela explique pourquoi les systèmes usuels de calculs d'invariants sont incapables de trouver un ensemble de paramètres. En utilisant la base de régularisation, et avec un système de calcul de base de Gröbner efficace (`GB` par exemple), il est possible de mener à bien ce calcul en quelques minutes. Nous avons même pu obtenir une base de Gröbner du système complet de paramètres. □

Pour $n \geq 6$, le test mécanique semble définitivement impraticable. Même en utilisant `FGB` (la toute dernière version encore expérimentale de *GB*, qui permet de gagner un, voire plusieurs ordres de grandeur) et une base convenable, le calcul a littéralement explosé.

Pour $n = 6, 7, 8$, nous avons utilisé ce système de paramètres pour rechercher des invariants secondaires. Nous avons alors vérifié que, au moins pour les petits degrés, l'algèbre des invariants est un module libre sur l'algèbre engendrée par ce système de paramètres.

11.4 Invariants secondaires

Dans toute cette partie, nous supposons vraie notre conjecture 11.3.5 sur les invariants primaires. Tout au moins, nous supposons qu'il existe un système d'invariants primaires dont les degrés sont $1, \ldots, n, 2, \ldots, \mathrm{C}^2_{n-1}$. Notons que la justesse de nos calculs utilisant ces invariants primaires ne dépend pas de cette conjecture, car ils peuvent vérifier au fur et à mesure la cohérence des résultats. De fait, un sous-produit de ces calculs est que, pour les petits degrés, l'algèbre des invariants est bien un module libre sur l'algèbre engendrée par les invariants primaires.

11.4.1 Degrés des invariants secondaires

Avant toute recherche, il peut être intéressant de connaître précisément le plus haut degré d'un secondaire. Nous rappelons la formule du théorème 8.1.26 :

$$e_t = \sum_i (d_i - 1) - \mu,$$

où e_t est le degré du dernier polynôme secondaire, d_i sont les degrés des primaires et μ est le plus petit degré d'un polynôme invariant relatif au caractère $\det^{-1}$. On peut calculer μ pour tout n.

Théorème 11.4.1.
Avec les notations ci-dessus,

$$\mu = \begin{cases} 0 & \text{si } n \text{ est pair,} \\ \lceil \frac{3}{4}(n-1) \rceil & \text{si } n \text{ est impair;} \end{cases} \quad e_t = \begin{cases} \mathrm{C}_n^2 + \mathrm{C}_{\mathrm{C}_{n-1}^2}^2 & \text{si } n \text{ pair,} \\ \mathrm{C}_n^2 + \mathrm{C}_{\mathrm{C}_{n-1}^2}^2 - \lceil \frac{3}{4}(n-1) \rceil & \text{si } n \text{ est impair,} \end{cases}$$

où $\lceil x \rceil$ est la partie entière supérieure de x.

Démonstration. Lorsque n est pair, d'après le lemme 8.4.1 $\epsilon := \det^{-1}$ est le caractère trivial car l'algèbre est de Gorenstein (corollaire 8.4.5). Donc le polynôme 1 est un invariant relatif et est de degré 0.

Nous supposerons par la suite n impair. Dans ce cas, toujours d'après le lemme 8.4.1, $\det^{-1}(\sigma) = \mathrm{sign}(\sigma)$. Nous appellerons ici polynôme antisymétrique un polynôme invariant relatif au caractère $\epsilon := \det^{-1}$. Cette notion est différente de celle, usuelle, de polynôme antisymétrique, car notre action du groupe symétrique n'est pas l'action naturelle du groupe symétrique $\mathfrak{S}_m$ en entier.

Il s'agit donc de trouver quel est le plus petit degré d'un polynôme p tel que $\sigma p = \mathrm{sign}(\sigma) p$. Le lemme suivant va nous permettre de nous ramener à un problème sur les multigraphes :

Lemme 11.4.2.
Il existe un polynôme antisymétrique de degré d si, et seulement si, il existe un multigraphe à d arêtes (comptées avec multiplicité) sans automorphisme impair.

Démonstration. Soit $\mathbf{g}$ un multigraphe à d arêtes sans automorphisme impair. C'est à dire qu'il n'y a pas de permutation σ des sommets de $\mathbf{g}$ telle que σ soit de signe -1 et laisse $\mathbf{g}$ invariant.

Soit donc $\overline{\mathbf{g}}^+ = \{\sigma.\mathbf{g} | \, \mathrm{sign}(\sigma) = 1\}$ l'ensemble des graphes obtenus à partir de $\mathbf{g}$ par une permutation paire. On définit de même $\overline{\mathbf{g}}^- = \{\sigma.\mathbf{g} | \, \mathrm{sign}(\sigma) = -1\}$. Supposons que ces deux ensembles soient d'intersection non vide. Il existe alors $\mathbf{g}'$, σ^+ et σ^- tels que $\sigma^+ \mathbf{g} = \mathbf{g}' = \sigma^- \mathbf{g}$ avec $\mathrm{sign}(\sigma^+) = 1$ et $\mathrm{sign}(\sigma^-) = -1$. Mais alors $(\sigma^-)^{-1} \circ \sigma^+$ est un automorphisme impair de $\mathbf{g}$, ce qui est contraire à nos hypothèses. Donc $\overline{\mathbf{g}}^+$ et $\overline{\mathbf{g}}^-$ sont disjoints.

On peut alors définir le polynôme antisymétrique de degré d

$$p = \sum_{\mathbf{g} \in \overline{\mathbf{g}}^+} \mathbf{x}_{\{i,j\}}^{\mathbf{g}'} - \sum_{\mathbf{g}' \in \overline{\mathbf{g}}^-} \mathbf{x}_{\{i,j\}}^{\mathbf{g}'}.$$

Le lecteur pourra vérifier que ce polynôme est bien antisymétrique en constatant qu'une permutation paire laisse stable $\overline{\mathbf{g}}^+$ et $\overline{\mathbf{g}}^-$ tandis qu'une permutation impaire échange $\overline{\mathbf{g}}^+$ et $\overline{\mathbf{g}}^-$.

Nous allons voir que réciproquement, on peut extraire un graphe sans automorphisme pair d'un polynôme antisymétrique.

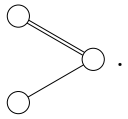
Soit donc p un polynôme antisymétrique de degré d. Soit m un monôme de degré d de p. Soit $\mathbf{g}$ le multigraphe correspondant et c le coefficient du monôme. Supposons que $\mathbf{g}$ ait un automorphisme σ impair. Comme p est antisymétrique, $\sigma.p = -p$ et donc le coefficient de $\mathbf{g}$ dans $\sigma.p$ doit être égal à $-c$. D'un autre côté, puisque que $\mathbf{g}$ est envoyé sur lui même par σ, le coefficient de $\mathbf{g}$ dans $\sigma.p$ doit être c. On aurait alors $c = 0$.

Conclusion : $\mathbf{g}$ est un multigraphe de degré d sans automorphisme impair. □

Il ne nous reste donc plus qu'à vérifier le lemme suivant :

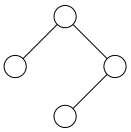
Lemme 11.4.3.
Si $n > 3$, le degré minimal d'un multigraphe $\mathbf{g}$ *sur n sommets sans automorphisme impair est $\lceil \frac{3}{4}(n-1) \rceil$.*

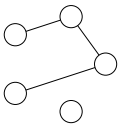
Démonstration. On note que pour $n = 1$ et $n = 2$, il n'y a pas de graphe sans automorphisme impair, et que pour $n = 3$, le plus petit graphe sans automorphisme impair a $3 > \lceil \frac{3}{4}(3-1) \rceil$ arêtes

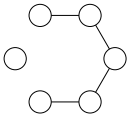


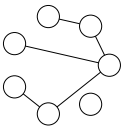
.

Nous allons d'abord construire une famille de multigraphes sans automorphisme impair et de degré $\lceil \frac{3}{4}(n-1) \rceil$.

$n = 4 : g_4 =$ 

$n = 5 : g_5 =$ 

$n = 6 : g_6 =$ 

$n = 7 : g_7 =$ 

De manière générale on définit g_n comme suit :
- Si $n = 4k$, on prend k copies de g_4 (degré $3k$) ;
- Si $n = 4k + 1$, on rajoute un sommet isolé (degré $3k$) ;
- Si $n = 4k + 2$, on prend $k - 1$ copies de g_4 et une copie de g_6 (degré $3k + 1$) ;
- Si $n = 4k + 3$, on prend $k - 1$ copies de g_4 et une copie de g_7 (degré $3k + 2$).

Il faut maintenant vérifier que tout graphe n'ayant pas d'automorphisme impair est de degré supérieur à $\lceil \frac{3}{4}(n-1) \rceil$. Nous allons le faire par récurrence forte sur le nombre de sommets.

Hypothèse de récurrence : Pour tout $n' < n$, si $\mathbf{g}$ à n' sommets et m' arêtes n'a pas d'automorphisme impair, alors $m' \geq \frac{3}{4}(n'-1)$.

Pour $n = 0, 1, 2, 3$, l'hypothèse est vérifiée (cf. remarque en début de démonstration).

Soit donc $\mathbf{g}$ un multigraphe à n sommets et m arêtes. Si $\mathbf{g}$ n'est constitué que de sommets isolés, comme $n \geq 2$, $\mathbf{g}$ a des automorphismes impairs. De même, si $\mathbf{g}$ a des composantes connexes avec 1 ou 2 arêtes.

Soit donc c une composante connexe de $\mathbf{g}$ avec $k \geq 3$ arêtes. Soit $\mathbf{g}'$ le graphe obtenu en enlevant cette composante connexe. Soient n' et m' son nombre de sommets et d'arêtes. La composante c étant connexe a au plus $k + 1$ sommets. Donc

$m = m' + k$ et $n \leq n' + k + 1$. Le graphe $\mathbf{g}'$ n'a pas d'automorphisme impair et donc par récurrence, $m' \geq \frac{3}{4}(n' - 1)$. Il ne reste plus qu'à vérifier que $m \geq \frac{3}{4}(n - 1)$.

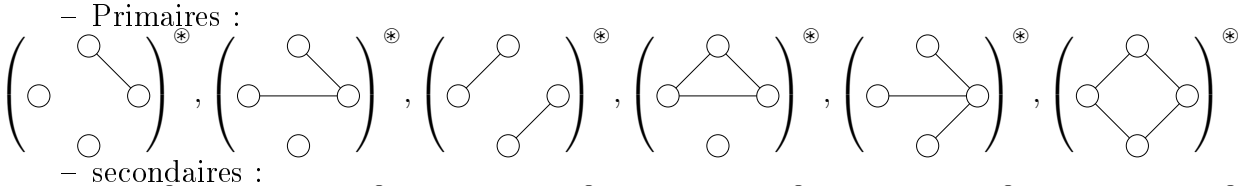
$$m - \frac{3}{4}(n-1) \geq m' + k - \frac{3}{4}(n' + k) \geq m' - \frac{3}{4}(n' - 1) + k - \frac{3}{4}(k+1) \geq \frac{k-3}{4} \geq 0$$

□

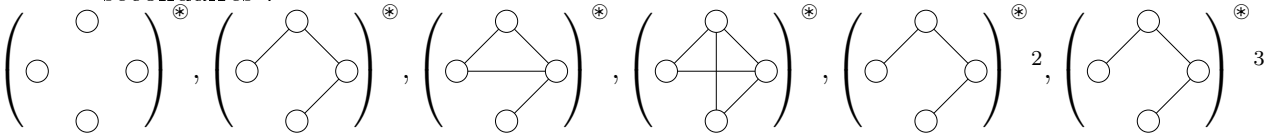
Ceci conclut la preuve du théorème 11.4.1. □

11.4.2 Base donnée par Aslaksen et al.pour $n = 4$

– Primaires :



– secondaires :



11.4.3 Résultats expérimentaux

Le tableau 11.1 page suivante résume les résultats que l'on a pu obtenir en essayant différents systèmes de calcul d'invariants. Les temps sont donnés à titre d'ordre de grandeur. La plupart des calculs ont été effectués sur un PC Linux 300 MHz avec 128 Mo de mémoire. Certains ont été faits sur une machine personnelle (PC Linux 133 MHz, 64 Mo) et nous avons alors appliqué un facteur correctif grossier.

Suivant l'ordre dans lequel on injecte les polynômes invariants, on peut vérifier si certains ensembles de polynômes invariants sont générateurs. Nous allons présenter quelques résultats obtenus de la sorte. Lorsque nous indiquons qu'un système est générateur, nous entendons générateur pour les nombres de sommets et d'arêtes pour lesquels les calculs ont été menés (voir table 11.1 page suivante). Pour l'algèbre des invariants sur les graphes avec le produit usuel et $n = 4$ sommets, cela permet de conclure que ces systèmes sont bien générateurs. Pour $n = 5$ sommets, la meilleure borne théorique sur le degré à notre disposition est $d = 22$. Les calculs n'ayant été menés que jusqu'au degré 10 ne permettent *a priori* pas de conclure. Cependant, au vu de la régularité et de l'évolution de la taille du système générateur minimal en fonction du degré (voir figure A.6 page 266), il nous paraît très probable que les systèmes générateurs minimaux ne contiennent pas de polynômes de degré > 10.

- Produit usuel :
  - Les graphes simples ne sont pas générateurs,
  - Les multigraphes valués $\{0, 1, 2\}$ sont générateurs,
  - Les multigraphes avec au moins un sommet isolé sont générateurs ;
- Produit de chaîne :
  - Les multigraphes valués $\{0, 1, 2\}$ ne sont pas générateurs (n=4, d=4 ; n=5, d=6, ...) ;

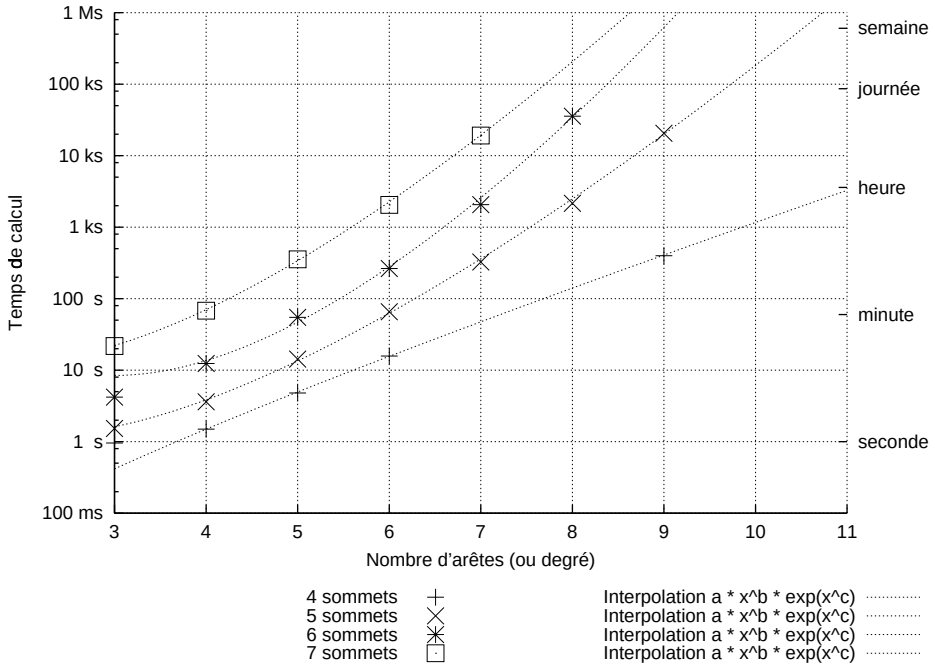
n		à la main	`Invar`	`Invar` 2	`Magma`	`MuPAD`	`MuPAD` fin
4	primaires	$\surd$	$\surd$	∞^{cgf}	$\surd$	fournis	symétriques
	secondaires	$\surd$[ACG96]	$\surd$(5 min, 10 Mo)^{a}	$\rightarrow$6 (1 min)^{bj}	1 s	$\surd$(7 min, 4 Mo)^{a}	$\surd$(20 s)
5	primaires	$\surd^{h}$	∞^{cg}	∞^{cgf}	∞^{cgf}	fournis	symétriques
	secondaires	?	? ^{e}	$\rightarrow$5 (8 min)^{bk}	∞^{ce}	$\rightarrow$9 (7 h, 40 Mo)^{b}	$\rightarrow$20 (36 h, 200 Mo)^{b}
6	primaires	$\surd^{i}$	∞^{cg},	∞^{cgf}	∞^{cgf}	fournis	symétriques
	secondaires	?	? ^{e}	$\rightarrow$4 (5 min)^{bl}	∞^{cg}	$\rightarrow$8 (10 h, 107 Mo)^{b}	?
7	primaires	$\surd^{i}$	∞^{cg},	∞^{cgf}	∞^{cgf}	fournis	symétriques
	secondaires	?	? ^{e}	∞^{cm}	∞^{cg}	$\rightarrow$7 (5 h, 72 Mo)^{b}	?
8	primaires	$\surd^{i}$	∞^{cg},	∞^{cgf}	∞^{cgf}	fournis	symétriques
	secondaires	?	? ^{e}	∞^{cn}	∞^{cg}	$\rightarrow$???? (??? h, ?? Mo)^{b}	?

[a] « $\surd$(1 min, 5 Mo) » : calcul mené à terme, en 1 minute et en utilisant 5 Mo de mémoire
[b] « $\rightarrow$6 (10 h, 107 Mo) » : calcul non mené à terme, mais donnant des résultats partiels jusqu'au degré 6, au bout de 10 heures et en utilisant 107 Mo
[c] « ∞ » : calcul non mené à terme (calcul trop long et interrompu, arrêt par saturation de la mémoire ou autres)
[g] Calcul de base de Gröbner divergent
[d] « ? » : Non essayé
[e] Primaires difficiles à fournir
[f] Primaires fournis
[h] Primaires vérifiés avec GB
[i] Primaires non vérifiés (voir conjecture 11.3.5)
[j] Crash pour 9 : « Error : object too large »
[k] Crash pour 6 : « Error : object too large »
[l] Crash pour 5 : « Error : object too large »
[m] Crash pour 3 (>60 Mo) : « segmentation fault (core dumped) maple »
[n] Crash pour 3 (>60 Mo) : « segmentation fault (core dumped) maple »

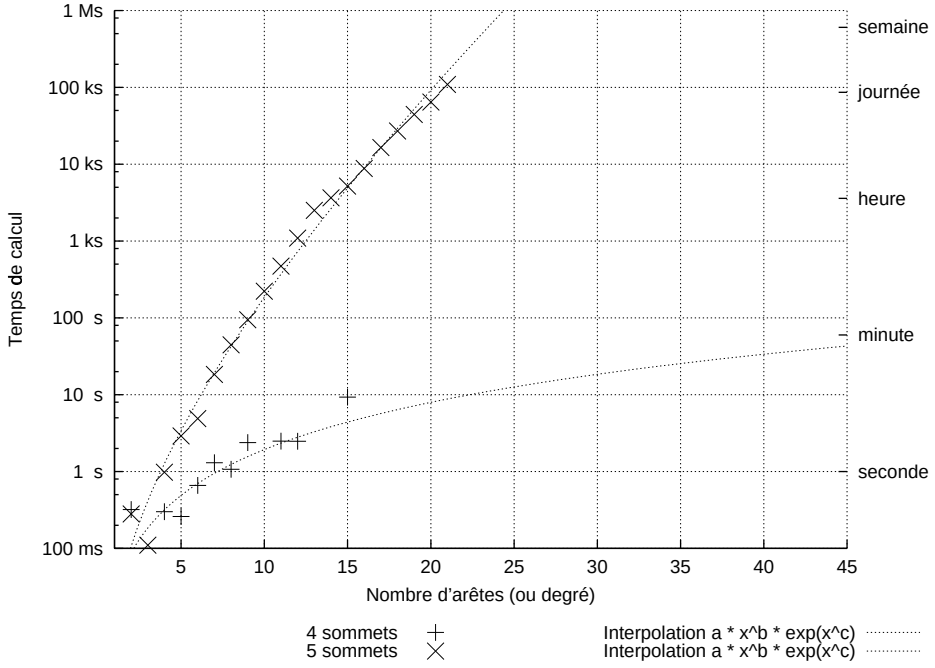
TAB. 11.1 – Synthèse des résultats obtenus avec différents programmes de calculs d'invariants

– Algèbre des digraphes (avec ou sans boucles) :
  – Les digraphes simples ne sont pas générateurs (n=3, d=3).

Nous concluons par quelques statistiques sur le temps et la mémoire nécessaires pour la recherche des invariants secondaires sur $4, 5, 6, 7$ et 8 sommets avec notre implémentation.

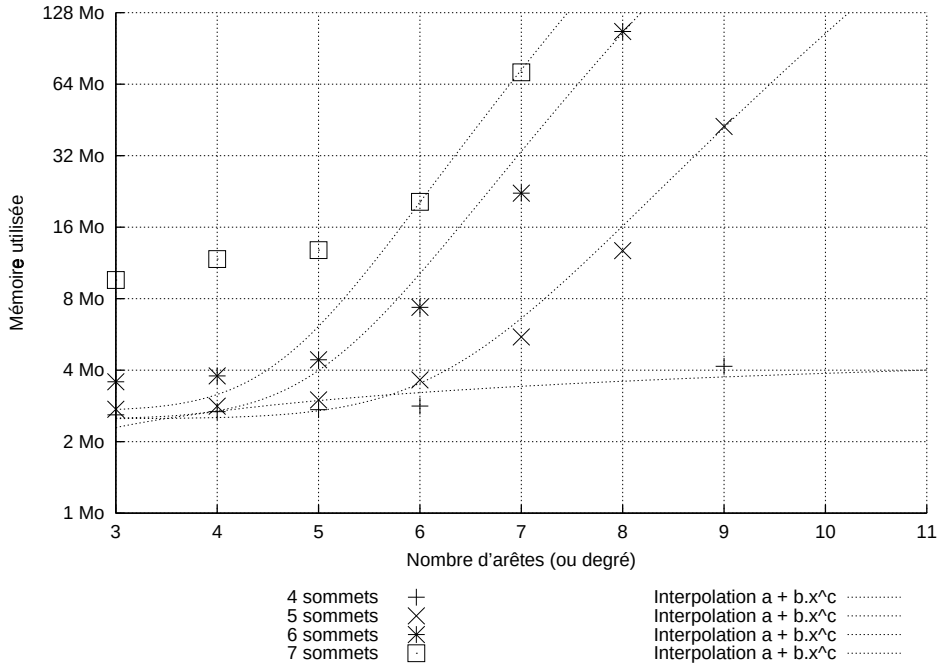


(a) Produit classique

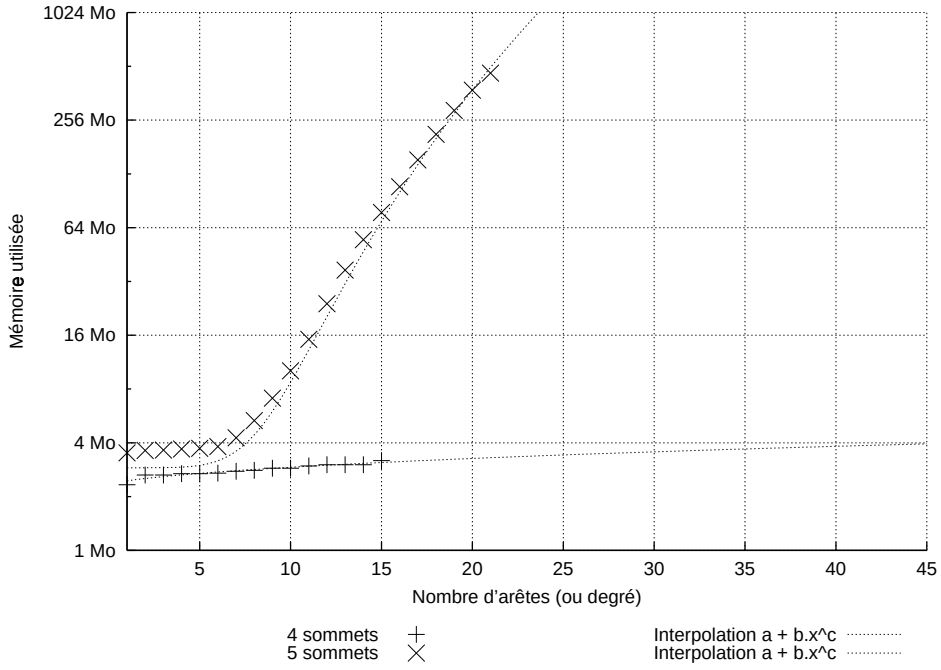


(b) Produit de chaînes

FIG. 11.3 – Temps de calcul des secondaires en fonction du nombre de sommets et d'arêtes



(a) Produit classique



(b) Produit de chaînes

FIG. 11.4 – Mémoire nécessaire pour le calcul des secondaires en fonction du nombre de sommets et d'arêtes

Chapitre 12

Autres algèbres d'invariants

Dans ce chapitre, nous discutons d'une part d'une autre algèbre introduite par Grigoriev pour traiter le problème d'isomorphie de graphes, ainsi que d'autres algèbres d'invariants en relation avec ce problème, par exemple les algèbres des graphes simples et des forêts, que nous utiliserons dans la partie III.

12.1 Algèbre des invariants sur les digraphes

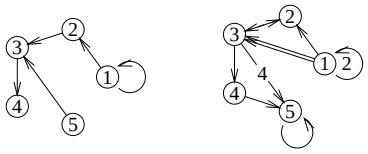
L'approche algébrique des problèmes d'isomorphie de graphes a été considérée par Grigoriev [Gri79]. Il utilise une autre algèbre ; au lieu de graphes non orientés, il considère des relations d'arité k. Pour $k = 2$, on peut voir ces relations comme des digraphes ayant éventuellement des boucles ; les n^2 variables sont indexées par les couples de $\{1, \ldots, n\}$ au lieu des paires dans notre cas. Un de ses résultats indique que l'anneau des invariants est engendré par les polynômes invariants associés aux digraphes simples. Ce résultat est erroné. Nous donnons ci-dessous un exemple de polynôme de degré 3 qui n'est pas ainsi engendré.

Dans notre contexte, de l'exactitude du résultat de Grigoriev, nous aurions obtenu que l'algèbre d'invariants sur les graphes est engendrée par les polynômes invariants associés aux graphes valués dans $\{0, 1, 2\}$, énoncé dont nous ne connaissons pas le statut. Si cet énoncé est exact, cela permet de réduire le test d'égalité de l'algèbre des invariants et de l'algèbre des polynômes algébriquement reconstructibles aux seuls polynômes de degré $\leq 2\,\mathrm{C}_n^2$. En fait, par passage au complémentaire pour les polynômes invariants associés aux graphes valués dans $\{0, 1, 2\}$, on peut encore réduire cette borne à C_n^2. Dans le cas $n = 5$, cette borne vaut 10, ce qui nous permettrait de conclure puisque nous avons vérifié par le calcul que jusqu'au degré 10, les polynômes invariants sont algébriquement reconstructibles. Mais, même pour $n = 5$, nous ne savons pas si l'énoncé ci-dessus est correct.

12.1.1 Digraphes et algèbre des invariants sur les digraphes

Soit W l'espace vectoriel sur $\mathbb{C}$ dont les n^2 vecteurs de base $(\mathbf{e}_{(1,2)}, \mathbf{e}_{(1,3)}, \ldots, \mathbf{e}_{(n,n-1)})$ sont indexés par les couples de $\{1, \ldots, n\}$. De manière analogue au cas des graphes, on peut considérer un vecteur de cet espace comme un *digraphe* valué dans $\mathbb{C}$, avec

éventuellement des boucles, et des arêtes en sens opposé :



On appelle cet espace *espace vectoriel des digraphes*. Un *digraphe simple* est un digraphe valué dans $\{0,1\}$. Un *multidigraphe* est un digraphe valué dans $\mathbb{N}$. Sauf mention explicite du contraire, tous les digraphes considérés plus loin sont valués. On munit cet espace de la représentation par permutation du groupe symétrique $\mathfrak{S}_n$ définie par : $\sigma \mathbf{e}_{(i,j)} := \mathbf{e}_{(\sigma(i),\sigma(j))}$.

Soit $\mathbb{C}[\mathbf{x}_{(i,j)}] := \mathbb{C}[x_{(1,2)}, x_{(1,3)}, \ldots, x_{(n,n-1)}]$ l'algèbre des polynômes sur les digraphes. On note qu'ici les variables $x_{(i,j)}$ et $x_{(j,i)}$ sont distinctes, et que l'on considère les variables $x_{(i,i)}$. L'action de $\mathfrak{S}_n$ sur l'espace W s'étend en une action sur ces polynômes, par $\sigma x_{(i,j)} := x_{(\sigma(i),\sigma(j))}$. On appelle *algèbre des invariants sur les digraphes* la sous-algèbre $\mathbb{C}[x_{(i,j)}]^{\mathfrak{S}_n}$ des polynômes de $\mathbb{C}[x_{(i,j)}]$ invariants par l'action de $\mathfrak{S}_n$.

La représentation est par permutation et, comme au §10.1, on peut définir l'exponentielle $\mathbf{x}^{\mathbf{g}}$ et l'exponentielle symétrisée de $\mathbf{x}^{\mathbf{g}^{\circledast}}$ d'un multidigraphe $\mathbf{g}$. Ainsi, un monôme m de $\mathbb{C}[x_{(i,j)}]$ peut être identifié avec un multidigraphe étiqueté, et un polynôme invariant peut être interprété comme une combinaison linéaire de multidigraphes non étiquetés.

Digraphes, graphes et graphes orientés

On peut formaliser la construction de l'espace vectoriel des digraphes valués comme suit. Soit V l'espace vectoriel de base $\mathbf{v}_1, \ldots, \mathbf{v}_n$ où $\mathbf{v}_i$ représente le sommet i. En identifiant $\mathbf{e}_{(i,j)}$ et $\mathbf{v}_i \otimes \mathbf{v}_j$, l'espace W est isomorphe au produit tensoriel $V \otimes V$ de V par lui-même. La représentation du groupe symétrique sur les digraphes est donc le produit tensoriel de la représentation naturelle du groupe symétrique par elle-même.

L'espace vectoriel des graphes valués peut être construit comme produit symétrique $V.V$ de V par lui-même. Pour cela, on identifie l'arête non orientée $\{i,j\}$ et le produit symétrique $\mathbf{v}_i.\mathbf{v}_j$. On peut alors plonger l'espace des graphes comme sous-module de W par le morphisme

$$\phi : \quad \mathbf{e}_{\{i,j\}} = \mathbf{v}_i.\mathbf{v}_j \quad \mapsto \quad \mathbf{v}_i \otimes \mathbf{v}_j + \mathbf{v}_j \otimes \mathbf{v}_i = \mathbf{e}_{(i,j)} + \mathbf{e}_{(j,i)}$$

(voir par exemple [FH96, Appendix B]). De même l'espace vectoriel des graphes orientés peut être construit comme produit extérieur $V \wedge V$ de V par lui-même. Pour cela, on identifie l'arête orientée $i \to j$ et le produit extérieur $\mathbf{v}_i \wedge \mathbf{v}_j$. On peut plonger cet espace comme sous-module de W par le morphisme

$$\phi : \quad \mathbf{e}_{i \to j} = \mathbf{v}_i \wedge \mathbf{v}_j \quad \mapsto \quad \mathbf{v}_i \otimes \mathbf{v}_j - \mathbf{v}_j \otimes \mathbf{v}_i = \mathbf{e}_{(i,j)} - \mathbf{e}_{(j,i)}.$$

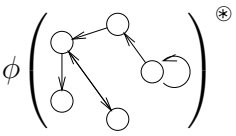
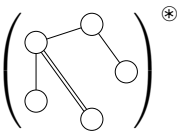
On en déduit que l'espace vectoriel des digraphes valués se décompose comme $\mathfrak{S}$-module en la somme directe de l'espace des graphes valués, de l'espace des graphes

orientés, et d'une copie de V formée des boucles $\mathbf{v}_i \otimes \mathbf{v}_i$. La décomposition en irréductibles de V en découle immédiatement. Tout ceci revient à dire que l'espace des matrices carrées (digraphes) est la somme directe des espaces des matrices symétriques à diagonale nulle (graphes), des matrices antisymétriques (graphes orientés) et des matrices diagonales (boucles).

Les calculs dans l'algèbre des invariants sur les digraphes sont souvent difficiles du fait de la croissance très rapide de sa taille. On définit alors *l'espace des digraphes sans boucles* et l'*algèbre des invariants sur les digraphes sans boucles* . La seule différence est que l'on ne considère pas les arêtes (i,i) et les variables $x_{(i,i)}$ correspondantes. On peut obtenir cette dernière algèbre comme quotient de l'algèbre des invariants sur les digraphes, via le morphisme d'algèbres ϕ défini par $\phi(x_{(i,i)}) := 0$ et $\phi(x_{(i,j)}) := x_{(i,j)}$. Cela permet de ramener de nombreux calculs dans l'algèbre des invariants sur les digraphes à des calculs dans l'algèbre des invariants sur les digraphes sans boucles, dont la croissance de la taille est moins rapide. Pour donner un ordre de comparaison, on donne, pour $n = 5$ sommets, les premiers termes des deux séries de Hilbert de ces algèbres

- Avec boucles : $1 + 2z + 11z^2 + 51z^3 + 269z^4 + 1270z^5 + 5776z^6 + 24z^7032 + 93067z^8 + 333948z^9 + 1121419z^10 + O(z^11)$
- Sans boucles : $1+z+6z^2+23z^3+110z^4+427z^5+1681z^6+5881z^7+19448z^8+59305z^9+170583z^10+O(z^11)$

L'algèbre des invariants sur les graphes s'exprime comme quotient de l'algèbre des invariants sur les digraphes, via le morphisme d'algèbres ϕ défini par $\phi(x_{(i,i)}) := 0$ et $\phi(x_{(i,j)}) := \phi(x_{(j,i)}) := x_{\{i,j\}}$. Par exemple,

ϕ  $=$ 

On note dès maintenant que l'image d'un digraphe simple est un graphe valué dans $\{0,1,2\}$.

Calcul de la série de Hilbert

Comme la représentation est une représentation par permutation du groupe symétrique $\mathfrak{S}_n$, le calcul de la série de Hilbert se réduit au calcul, à partir du type cyclique d'une permutation σ des sommets, du type cyclique de la permutation des arêtes induite par σ (voir § 10.3).

Proposition 12.1.1.
Soit σ une permutation des sommets. Alors :

(i) Un cycle de σ de longueur c induit c cycles de longueur c (arêtes internes au cycle, y compris les boucles) ;

(ii) Deux cycles de σ de longueurs c et c' concourent à $2*c\wedge c'$ cycles de longueur $c \vee c'$ (arêtes entre les sommets des deux cycles).

Pour les digraphes sans boucles, il faut modifier légèrement l'énoncé du (i) : un cycle de σ de longueur c n'induit que $c-1$ cycles de longueur c.

La complexité du calcul effectif de cette série de Hilbert est du même ordre que pour les graphes (voir 10.3.5). Ceci peut être utilisé pour calculer efficacement

la série de Hilbert de l'algèbre des invariants sur les graphes orientés, alors même que la représentation du groupe symétrique $\mathfrak{S}_n$ sur les graphes orientés n'est pas une représentation par permutation. Soit en effet σ une permutation de $\mathfrak{S}_n$ dont on connaît le type cyclique. Le polynôme caractéristique de la matrice de représentation M_σ de σ sur les graphes orientés vaut

$$\det(\mathrm{Id} - zM) = \frac{\det(\mathrm{Id} - zM')}{\det(\mathrm{Id} - zM'')} = \frac{\prod_i (1-z^i)^{l'_i}}{\prod_i (1-z^i)^{l''_i}},$$

où M' et M'' sont les matrices de représentation de σ sur l'espace des digraphes et l'espace des graphes, et l' et l'' les types cycliques correspondants. Ces types cycliques sont entièrement décrits par les propositions 12.1.1 et 10.3.4.

12.1.2 Systèmes générateurs

Dans [Gri79], Grigoriev étudie les propriétés de cette algèbre. Il se place dans un cadre plus général et considère l'espace vectoriel de dimension n^k :

$$G_{k,n} := \underbrace{V \otimes \cdots \otimes V}_{k}$$

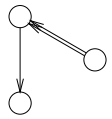
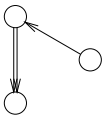
Il interprète un vecteur $\mathbf{v}_{i_1} \otimes \cdots \otimes \mathbf{v}_{i_k}$ de la base canonique de cet espace comme une hyperarête orientée $(i_1, \ldots, i_k)$, et un vecteur quelconque $\mathbf{h}$ comme un k-hypergraphe orienté et valué. Il définit alors de manière usuelle l'action du groupe symétrique $\mathfrak{S}_n$ sur cet espace, puis les polynômes et les polynômes invariants.

Grigoriev démontre que le corps des fractions invariantes est engendré par n^k+1 polynômes invariants, et en déduit qu'il existe un système complet d'invariants de taille $n^k + 1$. Ce résultat, non constructif, est en fait un résultat général sur les invariants de groupes finis (voir théorème 9.1.2). Il raffine ensuite ce résultat en précisant que l'on peut prendre ces n^k+1 polynômes invariants parmi les polynômes de degré $\leq n^k$. Pour cela, il s'appuie sur un lemme [Gri79, Lemma I] que l'on référencera par la suite par lemme I.

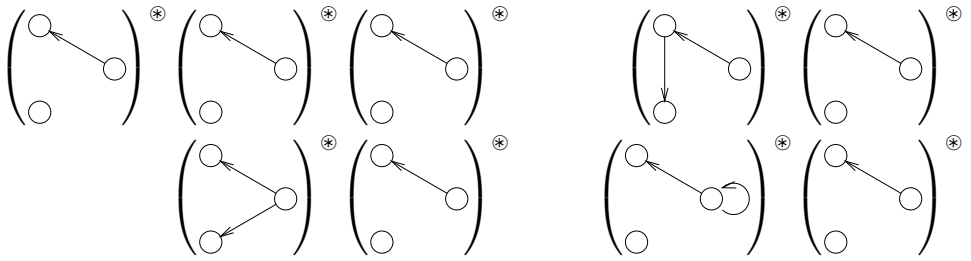
Appelons *polynôme invariant élémentaire* le polynôme invariant associé à un digraphe simple. Cette notion est analogue à celle de polynôme symétrique élémentaire. Le théorème fondamental des fonctions symétriques indique que les polynômes symétriques sont engendrés par les polynômes symétriques élémentaires. Dans le lemme I, Grigoriev propose la généralisation suivante de ce théorème : l'algèbre $\mathbb{C}[x_{(i,j)}]^{\mathfrak{S}_n}$ des invariants sur les digraphes est engendrée par les polynômes invariants élémentaires (ce lemme est en fait énoncé dans le cadre plus général des hypergraphes). La démonstration indique de procéder comme pour le théorème fondamental des fonctions symétriques (c'est-à-dire en fait de démontrer que les polynômes invariants élémentaires sont une base SAGBI de l'algèbre des invariants). Ceci nous a intrigués, car nous avons montré que, dans le cas des graphes, l'analogue du lemme I était faux (théorème 11.2.5). De plus, toujours dans le cas des graphes, il n'y a pas de base SAGBI finie pour l'ordre sur les monômes utilisé dans la démonstration du théorème fondamental des fonctions symétriques (théorème 11.1.8), et en fait probablement pas de bases SAGBI finie du tout.

Comme dans le cas des graphes (voir § 11.2), on peut appliquer le test sur la série de Hilbert. Il nous indique qu'il y a au moins un multidigraphe de degré ≤ 6 qui n'est pas engendré par les digraphes simples. Le même test appliqué aux digraphes sans boucles réduit ce degré à 3.

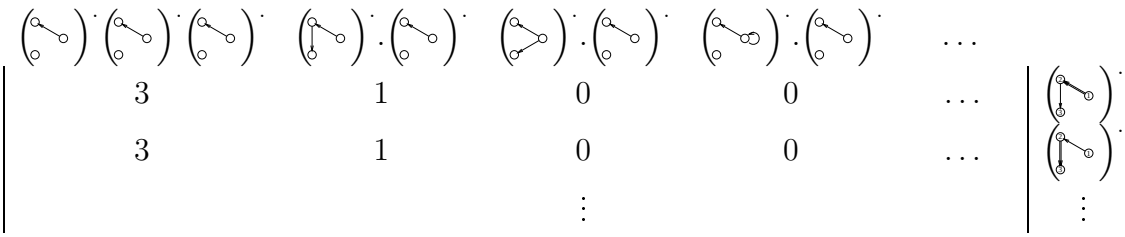
Proposition 12.1.2.
Pour $n \leq 3$, les multidigraphes suivants de degré 3 ne sont pas engendrés par les digraphes simples.

$\mathbf{g}_1 :=$  $\mathbf{g}_2 :=$ 

Démonstration. Les polynômes invariants associés aux graphes simples étant homogènes, on peut se ramener à un problème d'algèbre linéaire de la façon suivante. On considère tous les produits de graphes simples dont le degré final est 3. Par exemple :



Chacun de ces produits donne un polynôme homogène de degré 3. Soit M la matrice de ces polynômes dans la base des multigraphes.



Il est clair que seuls les deux premiers produits ont un coefficient non nul sur $\mathbf{g}_1$ et $\mathbf{g}_2$, car il faut que tous les digraphes apparaissant dans le produit soient des « sous-digraphes » de $\mathbf{g}_1$ ou $\mathbf{g}_2$. Les deux lignes correspondant à $\mathbf{g}_1$ et $\mathbf{g}_2$ sont donc égales, ce qui veut dire que toute combinaison linéaire de produits de digraphes simples a le même coefficient sur $\mathbf{g}_1$ et $\mathbf{g}_2$. Donc ni $\mathbf{g}_1$ ni $\mathbf{g}_2$ ne sont engendrés par les digraphes simples.

Nous avons aussi vérifié ce contre-exemple en utilisant notre bibliothèque `PerMuVAR` pour `MuPAD`. De fait, il est possible d'utiliser ce paquet pour construire systématiquement des contre-exemples de degrés 4 ou 5. □

On note que Grigoriev a énoncé ce lemme en prenant comme corps de base un corps de caractéristique 0 ou bien $\mathbb{F}_q$. On vérifie que, même en caractéristique $q > 0$, la démonstration ci-dessus reste valide, et que les multidigraphes $\mathbf{g}_1$ et $\mathbf{g}_2$ ne sont donc pas engendrés par les digraphes simples.

12.2 Quotients de l'algèbre des invariants

Nous étudions maintenant les propriétés générales de certains quotients de l'algèbre des invariants, l'algèbre des graphes simples et l'algèbre des forêts. Les résultats obtenus ici serviront dans la partie III.

12.2.1 Algèbre des graphes simples

Définition

Soit I l'espace vectoriel engendré par les multigraphes avec des arêtes multiples. On constate aisément que I est un idéal de l'algèbre $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$ des polynômes. Comme de plus cet idéal est stable par l'action du groupe $\mathfrak{S}_n$, il définit un idéal $I^{\mathfrak{S}_n}$ de l'algèbre des invariants. Cet idéal est engendré par les polynômes $x_{\{i,j\}}^2 = 0$.

Définition 12.2.1 (Algèbre des graphes simples).
On appelle algèbre des graphes simples *ou* algèbre des graphes *le quotient de l'algèbre des invariants par $I^{\mathfrak{S}_n}$. En tant qu'espace vectoriel, il est engendré par les expressions $\mathbf{x}^{\mathbf{g}^{\circledast}}$ où $\mathbf{g}$ est un graphe simple. On a donc muni d'une structure d'algèbre l'espace vectoriel $V_{\mathrm{C}_n^2}^{\mathfrak{S}_n}$ des graphes simples non étiquetés du § 6.*

Le produit de deux graphes $\mathbf{g}_1$ et $\mathbf{g}_2$ est la somme des graphes obtenus par union disjointe des arêtes de $\mathbf{g}_1$ et de $\mathbf{g}_2$. On l'appelle donc *produit disjoint* de $\mathbf{g}_1$ et $\mathbf{g}_2$. Bien entendu, le produit disjoint n'est pas intègre, mais l'algèbre est graduée, de 0 à C_n^2, chaque composante homogène de degré d correspondant à l'espace vectoriel des graphes simples non étiquetés à d arêtes. On peut donc appliquer les résultats du § 11.1.1 sur les systèmes générateurs minimaux. Le point principal est que deux systèmes générateurs minimaux ont même taille et mêmes degrés. En particulier, le degré maximal $\beta(V_{\mathrm{C}_n^2}^{\mathfrak{S}_n})$ dans un système générateur minimal ne dépend que de l'algèbre. L'étude des polynômes symétriques de cette algèbre va nous permettre de donner une majoration de $\beta(V_{\mathrm{C}_n^2}^{\mathfrak{S}_n})$.

Polynômes symétriques

Soit ϕ la projection canonique de l'algèbre des invariants dans l'algèbre des graphes simples. C'est un morphisme d'algèbres.

Définition 12.2.2.
On appelle polynôme symétrique de l'algèbre des graphes simples *l'image par ϕ d'un polynôme symétrique de l'algèbre $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$.*

Propriétés 12.2.3.
À un scalaire près, il n'y a qu'un seul polynôme symétrique élémentaire de degré d dans l'algèbre des graphes simples. Il s'agit de l'image $\phi(e_d)$ du polynôme symétrique élémentaire e_d de $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$. Ce polynôme est la somme des graphes simples à d arêtes. Lorsqu'il n'y a pas ambiguïté, on le note simplement e_d. Il s'exprime très simplement en fonction de e_1 :

$$e_d = d!\, e_1^d.$$

Démonstration. Soit p_λ le polynôme symétrique $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$ correspondant à la partition λ de d. Il s'agit de la somme de tous les multigraphes dont la forme est λ. Par exemple, si $\lambda = (3,1,1,1)$ p_λ est la somme des multigraphes ayant une arête valuée 3 et 3 arêtes valuées 1. Calculons sa projection $\phi(p_\lambda)$ sur l'algèbre des invariants. Si λ contient une valuation plus grande que 2, il y a une arête multiple et donc $\phi(p_\lambda) = 0$. Sinon, p_λ est le polynôme symétrique élémentaire e_d. De même que e_d, le polynôme $\phi(e_d)$ est la somme des graphes simples à d arêtes.

Comme $\phi(e_1)^d = \phi(e_1^d)$ est un polynôme symétrique de degré d, il s'écrit sous la forme $\phi(e_1)^d = \alpha\phi(e_d)$. Le coefficient α compte de combien de façons on peut choisir une arête dans chaque $\phi(e_1)$ pour obtenir un graphe donné à partir du produit $\phi(e_1)^d$. Donc $\alpha = d!$. □

Une application directe de la proposition 10.1.7 donne alors une interprétation combinatoire du produit pas un polynôme symétrique dans l'algèbre des graphes simples.

Remarque 12.2.4: La multiplication par e_1 dans l'algèbre des graphes simples correspond exactement à l'opérateur Etoile du § 6.3.

Majoration des degrés dans un système générateur minimal

On en déduit que, si d est supérieur à $\lfloor \frac{\mathrm{C}_n^2}{2} \rfloor$, la multiplication par e_1 donne un opérateur linéaire surjectif de la composante homogène de degré d vers la composante homogène de degré $d+1$ (théorème 6.3.2). Autrement dit, on peut exprimer un graphe simple à $d+1$ arêtes comme combinaison linéaire de produits de graphes simples à d arêtes par e_1. On en déduit le théorème suivant.

Proposition 12.2.5.
L'algèbre des graphes simples est engendrée par les graphes avec moins de $\lfloor \frac{\mathrm{C}_n^2}{2} \rfloor$ *arêtes :*

$$\beta(V_{\mathrm{C}_n^2}^{\mathfrak{S}_n}) \leq \lfloor \frac{\mathrm{C}_n^2}{2} \rfloor$$

Notons que l'on peut faire la même construction pour n'importe qu'elle représentation par permutation, et que les résultats précédents restent valables. Dans le cas des graphes, on peut raffiner cette proposition en utilisant un raisonnement analogue à celui de la proposition 10.2.6.

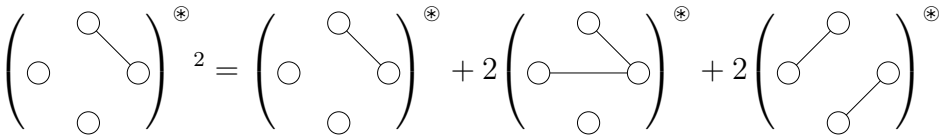
Proposition 12.2.6.
L'algèbre des graphes simples est engendrée par les graphes simples quasi-connexes avec moins de $\lfloor \frac{\mathrm{C}_n^2}{2} \rfloor$ *arêtes.*

De même que dans le cas des multigraphes, on peut considérer le cas $n = \infty$. L'algèbre des invariants est alors isomorphe à l'algèbre libre sur les graphes simples quasi-connexes.

Algèbre des graphes simples pour la réunion

On peut aussi définir une algèbre sur les graphes simples en prenant comme produit de deux graphes étiquetés $\mathbf{g}$ et $\mathbf{g}'$ la réunion $\mathbf{g} \cup \mathbf{g}'$ de ces deux graphes. Cela revient à quotienter l'algèbre des invariants par l'idéal engendré par $x_{\{i,j\}}^2 = x_{\{i,j\}}$. Pour distinguer entre les deux produits, on appelle ce produit *produit de réunion*, et l'autre *produit disjoint*. Cette algèbre a été utilisée par Kocay [Koc82] sous le nom d'algèbre des sous-graphes pour étudier le problème de reconstruction (voir § 15).

On note que ce n'est pas une algèbre graduée ! Par exemple,



Soient $\mathbf{v}$ et $\mathbf{v}'$ deux vecteurs homogènes de $V_{\mathrm{C}_n^2}^{\mathfrak{S}_n}$. Soient $\mathbf{v} \times \mathbf{v}'$ leur produit disjoint et $\mathbf{v} \cup \mathbf{v}'$ leur produit de réunion. On vérifie que $\mathbf{v} \times \mathbf{v}'$ est la composante homogène de degré maximal de $\mathbf{v} \cup \mathbf{v}'$. En effet, tous les autres termes de $\mathbf{v} \cup \mathbf{v}'$ correspondent à des unions non disjointes de graphes, qui sont donc de degré strictement plus petit (c'est-à-dire qui ont moins d'arêtes). On en déduit que le vecteur $\mathbf{v} \times \mathbf{v}' - \mathbf{v} \cup \mathbf{v}'$ est de degré strictement inférieur au vecteur $\mathbf{v} \times \mathbf{v}'$.

Ce fait permet de comparer le comportement des deux algèbres vis-à-vis des systèmes générateurs. La démarche est la même que lorsque nous comparons le produit de chaînes et le produit usuel de l'algèbre des invariants (voir § 10.1.5).

Proposition 12.2.7.
Soit B une famille de vecteurs homogènes de l'espace vectoriel $V_{\mathrm{C}_n^2}^{\mathfrak{S}_n}$ des graphes simples, qui est génératrice pour le produit disjoint. Alors, elle est génératrice pour le produit de réunion.

Démonstration. Supposons, par hypothèse de récurrence, que B engendre tous les vecteurs de degré $< d$ pour le produit d'union. Soit ω un vecteur de degré d. Il s'écrit comme combinaison linéaire de produits disjoints d'éléments de B. Comme le produit $\times$ préserve le degré, on peut se ramener par linéarité au cas où ω est de la forme $\mathbf{v} \times \mathbf{v}'$, avec $\mathbf{v}$ et $\mathbf{v}'$ deux vecteurs de degré $< d$. On a alors $\omega = \mathbf{v} \times \mathbf{v}' + (\mathbf{v} \cup \mathbf{v}' - \mathbf{v} \times \mathbf{v}')$. Le deuxième terme est de degré $< d$. Par hypothèse de récurrence, il est donc engendré par B pour le produit d'union, ainsi que $\mathbf{v}$ et $\mathbf{v}'$. Donc ω est engendré par B pour le produit d'union, comme voulu. □

Comme entre le produit de chaînes et le produit usuel, la réciproque est fausse. En effet, le produit d'union ne préservant pas le degré, on peut obtenir des vecteurs de degré d par des différences de la forme $\mathbf{v} \cup \mathbf{v}' - \omega \cup \omega'$, alors que les deux termes $\mathbf{v} \cup \mathbf{v}'$ et $\omega \cup \omega'$ sont de degré $> d$.

12.2.2 Algèbre des forêts

Introduction

Nous allons définir de manière analogue l'algèbre des forêts comme quotient de l'algèbre des invariants. Cette algèbre est utilisée au § 19.1.3, pour étudier la reconstructibilité algébrique des arbres. Ceci est possible grâce à la proposition 19.1.4 qui

assure que la reconstructibilité algébrique dans l'une ou l'autre algèbre est équivalente.

Soit I l'espace vectoriel engendré par les multigraphes cycliques, c'est-à-dire avec au moins une arête multiple ou un cycle. On constate que I est un idéal stable par l'action du groupe $\mathfrak{S}_n$. (Si un monôme m est cyclique, tout monôme obtenu par produit de m par un autre monôme est aussi cyclique. De même, les éléments de l'orbite de m sont cycliques).

Définition 12.2.8 (Algèbre des forêts).
On appelle algèbre des forêts *le quotient de l'algèbre des invariants par l'idéal* $I^{\mathfrak{S}_n}$. *En tant qu'espace vectoriel, il est engendré par les expressions* $\mathbf{x}^{\mathbf{f}^{\circledast}}$ *où* $\mathbf{f}$ *est une forêt. On a donc muni d'une structure d'algèbre l'espace vectoriel* $\langle forêts_n \rangle$ *des forêts non étiquetées.*

On note que l'algèbre des forêts est de dimension finie, graduée de 0 à $n-1$. Le produit n'est bien entendu pas intègre. Par exemple, si l'on multiplie un arbre par une arête, on obtient forcément un cycle.

Évaluation de la série de Hilbert

La série de Hilbert de cette algèbre compte les forêts à n sommets par nombre d d'arêtes. On note f_d le nombre total de forêts non étiquetées sans sommets isolés et avec d arêtes. On vérifie que f_d est un majorant de $\dim(\langle \text{forêts}_n \rangle_d)$, avec égalité lorsque $n \geq 2d$.

Le calcul de f_d se fait sans difficulté au moyen de séries génératrices (voir [FR, § 1], [Knu69] ou [HP73]). On peut obtenir plusieurs centaines de termes en quelques secondes (table 12.1 page suivante et figure A.7 page 267). L'évaluation asymptotique du nombre a_n d'arbres à n sommets ($d = n-1$ arêtes) est donnée par

$$a_n = 0,5349485 \frac{1}{\rho^n} \frac{1}{n^{5/2}} + O(\frac{1}{\rho^n} \frac{1}{n^{7/2}}) \tag{12.1}$$

où ρ est de l'ordre de $0,3383219$ ([HP73]). Elle est obtenue par une étude analytique de la série génératrice (voir aussi [FR, § II]). On en déduit que l'évaluation asymptotique de f_d doit être de la forme :

$$f_d \approx C \frac{1}{\rho}^d \frac{1}{d^{5/2}} \tag{12.2}$$

(communication personnelle de Flajolet). Un ajustement rapide avec `gnuplot` indique que C est de l'ordre de $1,21$, et que $C = 3$ est une majoration stricte. La figure A.10 page 268 présente le rapport r_d entre le nombre de forêts et d'arbres à d jusqu'à $n = 250$. Ce rapport tend asymptotiquement vers une constante r, avec une vitesse de convergence de l'ordre de $\frac{1}{n}$. Un ajustement équivalent par `gnuplot` donne r de l'ordre de $2,13$.

Pour $n \leq 2d$, le calcul peut aussi se faire par nombre de sommets et nombre de composantes connexes, mais on ne peut guère aller au delà de 14 composantes connexes (figure A.8 page 267). Enfin, on peut avoir des équivalents asymptotiques de ces quantités.

Note 12.2.9: L'évaluation la plus intéressante est que, lorsque n tend vers l'infini, le quotient du nombre de forêts à k composantes connexes par le nombre d'arbres tend vers une quantité de l'ordre de $\frac{1}{k-1!}$ (communication personnelle de Flajolet). Le nombre de forêts décroît donc très rapidement par rapport au nombre d'arbres.

d	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
# forêts	1	1	2	4	8	16	34	71	154	341	768	1765	4134	9838	23766

TAB. 12.1 – Nombre de forêts à d arêtes, ou dimension de la composante homogène de degré d de l'algèbre des forêts lorsque n est grand par rapport à d

Systèmes générateurs et comportement asymptotique

Les propriétés suivantes de l'algèbre des forêts se montrent de manière analogue au cas des multigraphes ou des graphes simples. On note qu'une forêt quasi-connexe est constituée d'un arbre et de sommets isolés. On l'appelle donc quasi-arbre.

Propriétés 12.2.10.
L'algèbre des forêts est engendrée par les quasi-arbres.

Sur un nombre infini de sommets, les quasi-arbres sont algébriquement indépendants. L'algèbre des forêts est alors l'algèbre libre sur les quasi-arbres.

Comme l'algèbre sur n sommets coïncide avec l'algèbre sur un nombre infini de sommets jusqu'au degré $\lfloor \frac{n}{2} \rfloor$, les quasi-arbres forment un système générateur minimal partiel de l'algèbre des forêts sur n sommets jusqu'au degré $\lfloor \frac{n}{2} \rfloor$.

Polynômes symétriques

De même que dans l'algèbre des graphes simples, on peut aussi définir les polynômes symétriques dans l'algèbre des forêts. On montre de manière analogue les propriétés suivantes.

Propriétés 12.2.11.
À un scalaire près, il n'y a qu'un seul polynôme symétrique élémentaire de degré d dans l'algèbre des forêts. Il s'agit de l'image $\phi(e_d)$ du polynôme symétrique élémentaire e_d de $\mathbb{C}[\mathbf{x}_{\{i,j\}}]$. Ce polynôme est la somme des forêts à d arêtes. Lorsqu'il n'y a pas ambiguïté, on le note simplement e_d. Il s'exprime très simplement en fonction de e_1 :

$$e_d = d!\, e_1^d.$$

Remarque 12.2.12: Ici aussi, la multiplication par le polynôme symétrique élémentaire e_1 peut être interprétée comme l'opérateur Etoile. Cependant, contrairement aux graphes simples non étiquetés, les forêts non étiquetées ne peuvent pas être définies comme quotient du treillis booléen par un groupe de permutation. On ne peut donc pas appliquer directement les résultats du § 6 pour étudier l'injectivité de cet opérateur.

12.2.3 Généralisations

Soit $\mathcal{P}$ une propriété de multigraphe, indépendante de l'étiquetage des sommets et stable par sous-graphe. On peut définir de manière analogue une algèbre gradué $A_{\mathcal{P}}$ en quotientant l'algèbre des polynômes invariants par l'idéal des multigraphes ne vérifiant pas $\mathcal{P}$. Par exemple, on retrouve respectivement l'algèbre des graphes simples et l'algèbre des forêts avec les propriétés « être un graphe simple » et « être une forêt ». On peut ainsi définir des algèbres des graphes bipartis, des graphes sans P_4, des graphes sans triangles, etc. L'intérêt d'une construction de ce type peut être de fournir une condition supplémentaire pour qu'un ensemble donné de multigraphes engendre l'algèbre des invariants. En effet il faut que le sous-ensemble des multigraphes vérifiant $\mathcal{P}$ engendre l'algèbre $A_{\mathcal{P}}$, et l'on peut alors essayer d'appliquer le critère 11.1.10 de dimension.

12.3 Hypergraphes et graphes bipartis

Nous définissons ici les algèbres d'invariants sur les multigraphes et sur les graphes bipartis, et nous récapitulons les propriétés de ces algèbres similaires à celles de l'algèbre sur les graphes.

12.3.1 Hypergraphes

Soit $k \leq n$ un entier. On considère l'espace vectoriel dont les C_n^k vecteurs $\mathbf{e}_A$ de base sont indexés par les parties de taille k de $\{1, \ldots, n\}$. Un élément de cet espace vectoriel peut être interprété comme un k-hypergraphe valué. Le groupe symétrique $\mathfrak{S}_n$ agit de manière usuelle sur ces vecteurs par $\sigma\mathbf{e}_A := \mathbf{e}_{\{\sigma(a), a\in A\}}$. Cette action s'étend à l'anneau $\mathbb{C}[\mathbf{x}_A]$ des polynômes sur cet espace, et on appelle *algèbre des polynômes invariants sur les multigraphes* la sous-algèbre $\mathbb{C}[\mathbf{x}_A]^G$ des polynômes invariants. Bien entendu, pour $k = 1$, on obtient l'algèbre des fonctions symétriques, et pour $k = 2$ l'algèbre des polynômes invariants sur les graphes.

Calcul de la série de Hilbert

Comme dans le cas des graphes, on peut calculer efficacement la série de Hilbert en sommant par classes C de conjugaisons de $\mathfrak{S}_n$ et, étant donnée une permutation des sommets $\sigma \in C$, en exprimant le polynôme caractéristique de la matrice M_σ de représentation à partir du type cyclique de la permutation des hyperarêtes correspondante (voir § 10.3). Par contre, il semble difficile d'exprimer directement le type cyclique de la permutation des arêtes à partir du type cyclique de la permutation des sommets. La difficulté vient du fait que les arêtes sont non orientées. Si l'on considère des variables indexées par les k-uples et non les parties de taille k, ce calcul est plus facile. Cela peut se voir dès $n = 2$, l'expression étant déjà plus simple pour les digraphes que pour les graphes (voir 10.3.4 et 12.1.1).

Dans notre implémentation, nous construisons donc explicitement pour chaque classe de conjugaison de $\mathfrak{S}_n$ une permutation σ de cette classe, puis la permutation correspondante des hyperarêtes, et enfin, le type cyclique de cette permutation.

De même que pour les graphes, on montre que pour $k \geq 2$, il n'y a pas de pseudo-réflexions (voir lemme 8.4.2). Enfin, l'algèbre des invariants sur les digraphes est de Gorenstein si, et seulement si, C_{n-2}^{k-1} est pair. Prenons en effet une transposition i, j ; les parties contenant i et j, ou ni i ni j, sont fixes. Les autres se groupent par cycles de longueur 2 de la forme $(A \cup \{i\}, A \cup \{j\})$, où A est une partie de taille $k-1$ parmi les sommets restants. Le signe de la permutation des hyperarêtes correspondant à cette transposition vaut donc $(-1)^{C_{n-2}^{k-1}}$.

12.3.2 Graphes bipartis

Soit n_1 et n_2 deux entiers. On considère l'espace vectoriel dont les $n_1 n_2$ vecteurs $\mathbf{e}_(i,j)$ de base sont indexés par les couples (i,j) où i parcourt $\{1,\ldots,n_1\}$ et j parcourt $\{1,\ldots,n_2\}$. Un élément de cet espace peut être interprété comme un graphe biparti $A_1 \times A_2$ valué, où comme une matrice $n_1 \ldots n_2$. Le groupe symétrique $\mathfrak{S}_{n_1}$ agit sur ces variables par $\sigma_1.\mathbf{e}_{(i,j)} := \mathbf{e}_{(\sigma(i),j)}$. De même, le groupe symétrique $\mathfrak{S}_{n_2}$ agit par $\sigma_2.\mathbf{e}_{(i,j)} := \mathbf{e}_{(i,\sigma(j))}$. De plus, si $n_1 = n_2$, on considère l'action de $\mathfrak{S}_2 := (\mathrm{id}, t)$ définie par $t.\mathbf{e}_{(i,j)} = \mathbf{e}_{(j,i)}$. On considère le groupe engendré par toutes ces opérations. Par exemple, dans le cas $n_1 \neq n_2 = n$, cela revient à considérer des matrices à permutations indépendantes des lignes et des colonnes près. Lorsque $n_1 = n_2$, on rajoute de plus la transposition.

On définit de manière usuelle l'algèbre des polynômes $\mathbb{C}[x_{(i,j)}]$ puis l'*algèbre des polynômes invariants sur les graphes bipartis* .

Il peut être intéressant d'étudier cette algèbre pour deux raisons. D'une part sa taille croît plus lentement que pour les graphes. Ainsi, on a à sa disposition un certain nombre de petites algèbres d'invariants sur lesquelles on peut faire des calculs explicites et des expérimentations, et on peut supposer que les propriétés de ces algèbres ne sont pas sans rapport avec celles de l'algèbre des invariants sur les graphes. D'autre part, on peut définir une notion de reconstructibilité algébrique dans cette algèbre et montrer, que si un graphe simple biparti non séparable est algébriquement reconstructible, alors il est reconstructible. Ceci pourrait fournir une approche pour l'étude de la reconstructibilité des graphes bipartis.

Pour calculer efficacement la série de Hilbert de cette algèbre d'invariants, on peut donner une description complète des classes de conjugaison, de leurs tailles et des types cycliques correspondants.

Théorème 12.3.1.

- *Premier cas : $n_1 \neq n_2$. Le groupe qui agit est $\mathfrak{S}_{n_1} \times \mathfrak{S}_{n_2}$. Une classe de conjugaison est caractérisée par un couple de partition. On peut alors calculer comme suit le type cyclique d'un élément (σ_1, σ_2) de cette classe de conjugaison : un cycle de longueur c_1 de σ_1 et un cycle de longueur c_2 de σ_2 concourent à $c_1 \wedge c_2$ cycles de longueur $c_1 \vee c_2$.*
- *Deuxième cas : $n_1 = n_2$. Ici, les classes de conjugaison sont un peu plus complexes. Ce qui suit décrit une liste complète de représentants de ces classes, avec la taille de la classe et le type cyclique correspondant.*
  Soient $\{p_1, p_2\}$ une paire de partitions, éventuellement égales, et soient $|p_1|$ et $|p_2|$ les tailles des classes de conjugaison correspondantes. Enfin, soient σ_1, σ_2 deux représentants de ces classes de conjugaison. Il y a $|p_1| * |p_2|$ éléments dans

la classe de conjugaison de (σ_1, σ_2)*. Le type cyclique se calcule comme dans le premier cas.*
Soit p_1 *une partition de* n_1 *et soient* $|p_1|$*,* σ_1 *comme ci-dessus. Il y a* $|p_1| * n_1!$ *éléments dans la classe de conjugaison de* $(\sigma_1, \mathrm{id}) \circ t$*. Son type cyclique se calcule comme suit :*
(i) Un cycle de longueur c *de* σ_1 *concourt à des cycles de longueurs respectives* $3, 5, \ldots, 2n-3, 2n$*.*
(ii) Deux cycles de σ_1 *de longueurs* c *et* c' *concourent à* $c \wedge c'$ *cycles de longueur* $2 \vee c'$*.*

Démonstration.

- Premier cas, $n_1 \neq n_2$. Calculons les conjugués de (σ_1, σ_2).

$$(\tau_1, \tau_2) \circ (\sigma_1, \sigma_2) \circ (\tau_1, \tau_2)^{-1} = (\tau_1 \circ \sigma_1 \circ \tau_1^{-1}, \tau_2 \circ \sigma_2 \circ \tau_2^{-1})$$

  Conclusion : la classe de conjugaison de (σ_1, σ_2) est composée des éléments (σ_1', σ_2') tels que σ_1' est conjugué de σ_1 et σ_2' conjugué de σ_2. Son type cyclique se déduit des types cycliques de σ_1 et σ_2 comme dans le point (iii) de la proposition 10.3.4. On en déduit la paramétrisation et la description voulues des classes de conjugaison.
- Deuxième cas, plus complexe, $n_1 = n_2$. Le groupe est engendré par la transposition t et les éléments de la forme (σ_1, σ_2). Comme $t \circ (\sigma_1, \sigma_2) = (\sigma_2, \sigma_1) \circ t$, tout élément du groupe est d'une des formes suivantes : (σ_1, σ_2) ou $(\sigma_1, \sigma_2) \circ t$. Nous allons commencer par déterminer les classes de conjugaison.
  Calculons les conjugués de (σ_1, σ_2).

$$\begin{aligned}(\tau_1, \tau_2) \circ (\sigma_1, \sigma_2) \circ (\tau_1, \tau_2)^{-1} &= (\tau_1 \circ \sigma_1 \circ \tau_1^{-1}, \tau_2 \circ \sigma_2 \circ \tau_2^{-1}) \\ ((\tau_1, \tau_2) \circ t) \circ (\sigma_1, \sigma_2) \circ ((\tau_1, \tau_2) \circ t)^{-1} &= (\tau_1 \circ \sigma_2 \circ \tau_1^{-1}, \tau_2 \circ \sigma_1 \circ \tau_2^{-1})\end{aligned}$$

  Conclusion : La classe de conjugaison de (σ_1, σ_2) est composée des éléments (σ_1', σ_2') tels que : ou bien σ_1' est conjugué de σ_1 et σ_2' conjugué de σ_2, ou bien σ_1' est conjugué de σ_2 et σ_2' conjugué de σ_1. Le calcul du type cyclique se fait toujours comme dans le point (iii) de la proposition 10.3.4.
  Calculons les conjugués de $(\sigma_1, \sigma_2) \circ t$.

$$\begin{aligned}(\tau_1, \tau_2) \circ (\sigma_1, \sigma_2) \circ t \circ (\tau_1, \tau_2)^{-1} &= (\tau_1 \circ \sigma_1 \circ \tau_2^{-1}, \tau_2 \circ \sigma_2 \circ \tau_1^{-1}) \circ t \\ ((\tau_1, \tau_2) \circ t) \circ (\sigma_1, \sigma_2) \circ t \circ ((\tau_1, \tau_2) \circ t)^{-1} &= (\tau_1 \circ \sigma_2 \circ \tau_2^{-1}, \tau_2 \circ \sigma_1 \circ \tau_1^{-1}) \circ t\end{aligned}$$

  Conclusion : $(\sigma_1, \sigma_2) \circ t$ est conjugué avec n'importe quel élément de la forme $(\sigma_1', \mathrm{id}) \circ t$, où σ_1' est conjugué de $\sigma_1 \circ \sigma_2^{-1}$. On en déduit la paramétrisation et la description voulues des classes de conjugaison.
  Il ne reste plus qu'à déterminer le type cyclique de $(\sigma_1, \mathrm{id}) \circ t$, à partir du type cyclique de σ_1. Pour cela, on peut choisir σ_1 de sorte qu'elle agisse comme sur la figure 12.1 page suivante. On constate que les blocs diagonaux sont stabilisés par $(\sigma_1', \mathrm{id}) \circ t$, alors que les autres blocs sont échangés de part et d'autre de la diagonale principale. Il nous suffit donc d'étudier ces deux cas.
  - La figure 12.2 page suivante illustre l'action d'un cycle de σ_1 sur un bloc diagonal. On vérifie que les cycles obtenus sont de longueur $3, 5, \ldots, 2n-3, 2n$.

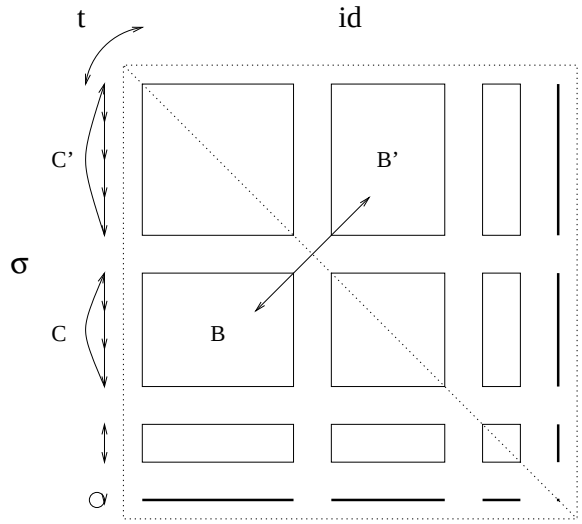


FIG. 12.1 – Action de $(\sigma_1, \mathrm{id}) \circ t$ sur la matrice d'un graphe biparti

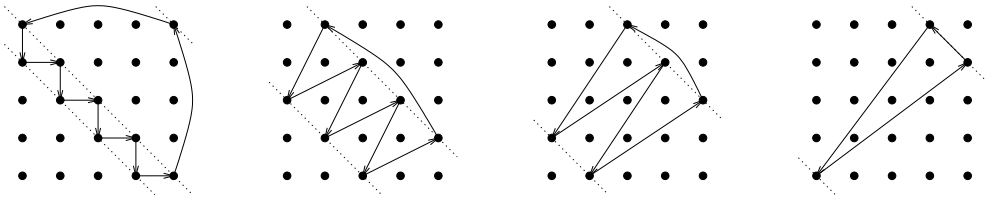


FIG. 12.2 – Action de $(\sigma_1, \mathrm{id}) \circ t$ sur un bloc diagonal de la matrice d'un graphe biparti

– Soit B un bloc non diagonal et B' le bloc symétrique par rapport à la diagonale (Voir figure 12.2). Soit C et C' de longueur c et c' les cycles correspondants. Soit $\tau = ((\sigma_1, \mathrm{id}) \circ t)^2$. B est stabilisé par τ. De plus, on obtient la même action que si on avait appliqué C sur les lignes et C' sur les colonnes. Il y a donc $c \wedge c'$ cycles de longueurs $c \vee c'$ pour l'action de τ. Comme B est disjoint de B', on double la longueur des cycles lorsque l'on applique seulement $(\sigma_1, \mathrm{id}) \circ t$. D'où un nombre total de $c \wedge c'$ cycles de longueurs $2 \vee c'$ dans $B \cup B'$.

□

Partie III

Invariants algébriques de graphes et reconstruction

Chapitre 13

Introduction

Dans cette partie, nous considérons le problème de reconstruction de Ulam. Le cadre algébrique dans lequel nous nous plaçons met en évidence une nouvelle notion concernant aussi bien les polynômes que les multigraphes : la reconstruction algébrique. Nous présentons les relations entre la reconstructibilité algébrique, la notion usuelle de reconstruction et d'autres notions proches, comme celle de Kocay [Koc82].

Nous étudions le comportement de cette notion vis-à-vis d'un certain nombre d'opérations élémentaires. Par exemple, il est clair que le complémentaire d'un graphe reconstructible est reconstructible. Nous montrons que cela reste vrai dans le cas algébrique, mais ceci nécessite une véritable démonstration. Nous montrons aussi qu'un certain nombre d'invariants reconstructibles classiques sont algébriquement reconstructibles.

Ce que nous venons de mentionner montre que la notion de reconstruction algébrique n'est pas vide de sens. Elle était motivée par l'hypothèse que tous les invariants soient algébriquement reconstructibles. L'intérêt de cette hypothèse est l'existence d'outils algébriques et algorithmiques pour la traiter. Dans la section 18, nous montrons, par un calcul de dimension, que cette hypothèse est fausse pour les graphes simples à 13 sommets et 17 arêtes.

Cependant, en utilisant les calculs de systèmes générateurs de l'algèbre des invariants de la partie II, on montre que pour $n = 3, 4$ tous les multigraphes sont algébriquement reconstructibles. Pour $n = 5$, il semble ne manquer qu'un argument de degré. Enfin, pour $n = 6$, tous les graphes simples sont algébriquement reconstructibles.

Dans un dernier chapitre, nous étudions la reconstruction algébrique des arbres, dans le but de répondre à une conjecture de Kocay [Koc82]. Nous montrons, par le calcul, que les arbres sont algébriquement reconstructibles jusqu'à 13 sommets, et nous donnons une famille infinie d'arbres algébriquement reconstructibles, incluant les arbres de diamètres ≤ 4.

Dans toute cette partie, nous utilisons intensivement les résultats des deux premières parties. Enfin, pour l'agrément du lecteur, la figure 13.1 page suivante récapitule les rapports entre les différentes notions de reconstructibilité, pour les multigraphes, les graphes simples et les arbres.

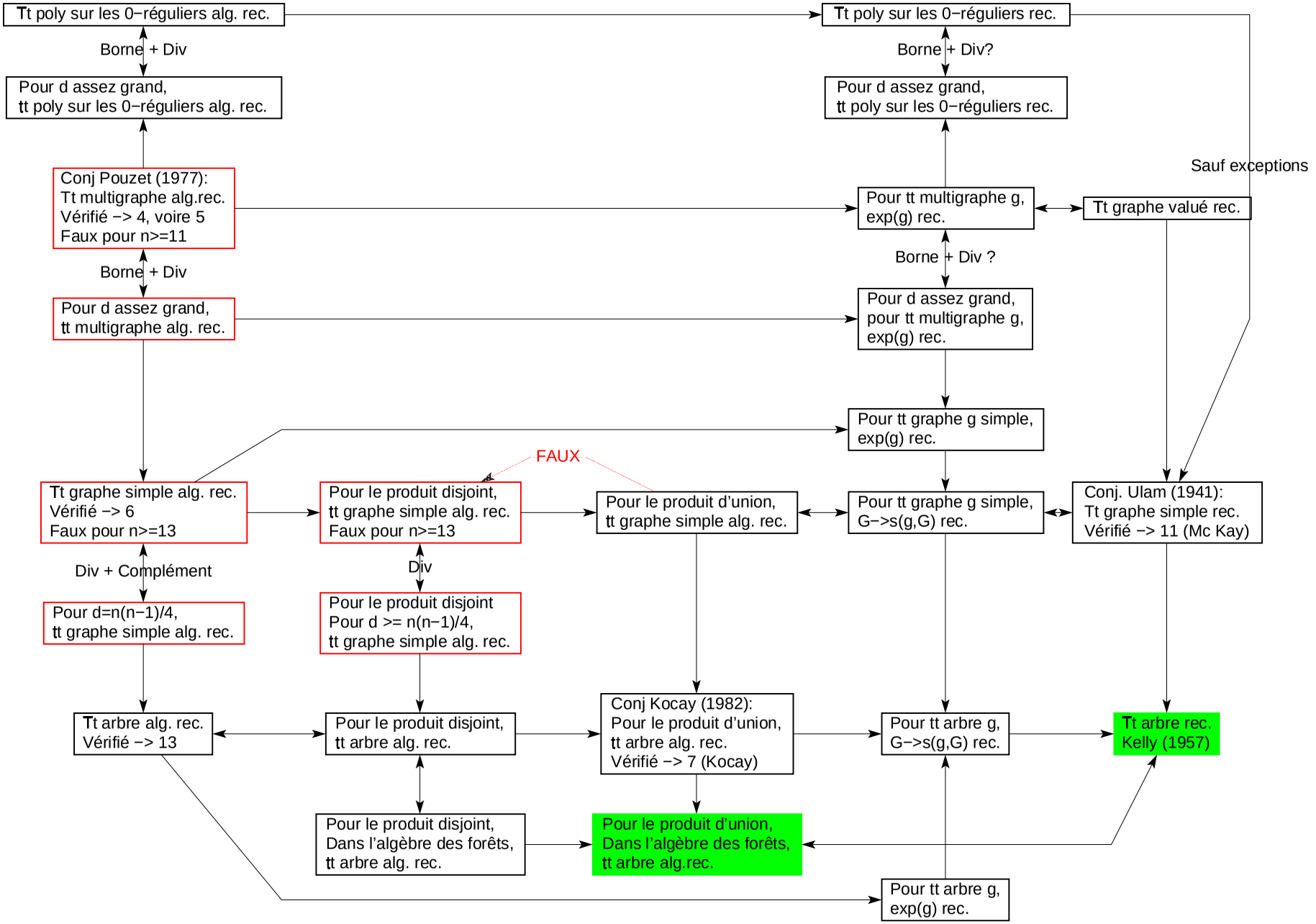


FIG. 13.1 – Récapitulatif des conjectures pour les différentes notions de reconstructibilité, et de leurs relations
Nous ne connaissons pas le statut des réciproques non indiquées. Abréviations : rec.=reconstructible ; alg. rec.=algébriquement reconstructible ; exp(g)= polynôme invariant associé à g.

Chapitre 14

Reconstructibilité et reconstructibilité algébrique

14.1 Graphes reconstructibles

Un *graphe simple* sur n sommets est un ensemble de paires d'un ensemble V de taille n. Pour un graphe $\mathbf{g}$ et un sommet v de $\mathbf{g}$, on note $\mathbf{g}_{\setminus v}$ le *sous-graphe induit* obtenu en retirant de $\mathbf{g}$ le sommet v et toutes les arêtes adjacentes à v. Étant donnée une permutation σ des sommets de $\mathbf{g}$, on note $\sigma\mathbf{g}$ le graphe obtenu en transformant chaque arête $\{v, w\}$ de $\mathbf{g}$ en l'arête $\{\sigma(v), \sigma(w)\}$. Deux graphes $\mathbf{g}$ et $\mathbf{g}'$ sont dits *isomorphes* s'il existe une bijection σ entre les sommets de $\mathbf{g}$ et ceux de $\mathbf{g}'$ telle que $\mathbf{g}' = \sigma\mathbf{g}$.

Le problème de reconstruction original s'énonce comme suit.

Conjecture 14.1.1 (Ulam [Ula60]).
Soient $\mathbf{g}$ *et* $\mathbf{g}'$ *deux graphes simples sur* n *sommets* ($n \geq 3$) *tels que, pour tout sommet* v, *les sous-graphes induits* $\mathbf{g}_{\setminus v}$ *et* $\mathbf{g}'_{\setminus v}$ *soient isomorphes. Alors* $\mathbf{g}$ *et* $\mathbf{g}'$ *sont isomorphes.*

La condition $n \geq 3$ est nécessaire, car les deux graphes suivants sont clairement non-isomorphes, alors que leurs sous-graphes induits vérifient les conditions voulues.

$$\mathbf{g} := \textcircled{2} \qquad \textcircled{1} \qquad\qquad \mathbf{g}' := \textcircled{2}\text{———}\textcircled{1} \tag{14.1}$$

Dans toute la suite de cette partie, nous fixons un entier $n \geq 3$. Un *graphe valué dans un ensemble* E est une fonction de l'ensemble des paires de V dans E. *Sauf mention du contraire, tous les graphes considérés dans cette partie sont valués* . On généralise immédiatement les notions d'isomorphie et de sous-graphes induits. Le même problème de reconstruction se pose pour les graphes valués.

Conjecture 14.1.2.
Soient $\mathbf{g}$ *et* $\mathbf{g}'$ *deux graphes sur* n *sommets valués dans un ensemble* E. *On suppose qu'il existe une bijection* σ *entre les sommets de* $\mathbf{g}$ *et ceux de* $\mathbf{g}'$ *telle que, pour tout sommet* v *de* $\mathbf{g}$, *les deux sous-graphes induits* $\mathbf{g}_{\setminus v}$ *et* $\mathbf{g}'_{\setminus \sigma(v)}$ *sont isomorphes. Alors* $\mathbf{g}$ *et* $\mathbf{g}'$ *sont isomorphes.*

Le fait d'introduire la bijection σ entre les sommets ne change pas la teneur du problème. Si, par exemple, pour $\mathbf{g}$ et $\mathbf{g}'$ il existe une bijection des sommets telle que $\mathbf{g}_{\setminus v}$ et $\mathbf{g}'_{\setminus \sigma(v)}$ sont isomorphes, on se ramène au problème sans bijection en considérant $\mathbf{g}$ et $\sigma^{-1}\mathbf{g}'$.

Il sera pratique de reformuler la condition sur les sous-graphes de $\mathbf{g}$ et $\mathbf{g}'$ sous la forme suivante. Étant donné un graphe $\mathbf{g}$ sur n sommets, on appelle *carte de* $\mathbf{g}$ un sous-graphe induit $\mathbf{g}_{\setminus v}$ considéré à l'isomorphie près. On appelle alors *jeu de* $\mathbf{g}$ la collection de ces n cartes, une même carte pouvant apparaître plusieurs fois. Dire que $\mathbf{g}$ et $\mathbf{g}'$ ont le même jeu est équivalent à dire qu'il existe une bijection σ entre les sommets de $\mathbf{g}$ et ceux de $\mathbf{g}'$ telle que, pour tout sommet v de $\mathbf{g}$, les deux sous-graphes induits $\mathbf{g}_{\setminus v}$ et $\mathbf{g}'_{\setminus \sigma(v)}$ sont isomorphes.

Définition 14.1.3.
Un graphe $\mathbf{g}$ *est dit* reconstructible *s'il est déterminé à l'isomorphie près par son jeu, c'est-à-dire si tout graphe* $\mathbf{g}'$ *ayant le même jeu que* $\mathbf{g}$ *est isomorphe à* $\mathbf{g}$.

Par exemple, la conjecture de Ulam affirme que tous les graphes simples sur $n \geq 3$ sommets sont reconstructibles.

Il est très important de noter que, dans ce problème, les valeurs précises des valuations sont sans importance réelle. Ce qui compte, c'est la partition des arêtes que ces valeurs déterminent. Supposons, par exemple, que les graphes $\mathbf{g}$ et $\mathbf{g}'$ soient valués dans un ensemble E. Soit f une injection de E dans un autre ensemble F, et notons $f(\mathbf{g})$ et $f(\mathbf{g}')$ les graphes obtenus en substituant chaque valuation x par $f(x)$. On voit que les graphes $\mathbf{g}$ et $\mathbf{g}'$ sont isomorphes si, et seulement si, les graphes $f(\mathbf{g})$ et $f(\mathbf{g}')$ sont isomorphes. De même, les sous-graphes induits $\mathbf{g}_{\setminus v}$ et $\mathbf{g}'_{\setminus v}$ sont isomorphes si, et seulement si, les sous-graphes correspondants $f(\mathbf{g}_{\setminus v})$ et $f(\mathbf{g}'_{\setminus v})$ sont isomorphes. Le problème de reconstruction ne dépend que du nombre total de valuations possibles, c'est-à-dire de la taille de E. En particulier, dès que les tailles de deux ensembles E et F dépassent le nombre total d'arêtes C_n^2, les problèmes de reconstruction pour des graphes valués dans E ou dans F sont équivalents. Par la suite, nous ne considérerons que les deux cas extrêmes : d'une part les graphes simples (E de taille 2) et d'autre part les graphes valués dans un ensemble de taille plus grande que C_n^2. Il sera alors pratique de prendre pour E un corps $\mathbb{K}$ de caractéristique nulle, par exemple $\mathbb{C}$.

14.2 Fonctions et polynômes reconstructibles

Définition 14.2.1 (Fonction invariante et fonction reconstructible).
Une fonction qui attribue à chaque graphe valué une valeur dans un certain ensemble est dite invariante *si elle donne la même valeur à deux graphes isomorphes.*

Une fonction est dite reconstructible *si elle donne la même valeur à deux graphes valués ayant même jeu.*

Parmi toutes les fonctions invariantes possibles, nous nous intéresserons plus particulièrement aux fonctions polynomiales invariantes. On considère un ensemble de variables $x_{\{i,j\}}$ indexées par les paires de $\{1, \ldots, n\}$, et $\mathbb{K}[\mathbf{x}_{\{i,j\}}]$ l'algèbre des polynômes en ces variables. Pour chaque graphe $\mathbf{g}$ sur les sommets $1, \ldots, n$ valué

dans $\mathbb{K}$, on définit l'évaluation $x_{\{i,j\}}(\mathbf{g})$ de la variable $x_{\{i,j\}}$ sur $\mathbf{g}$ comme étant la valuation de $\mathbf{g}$ sur l'arête $\{i,j\}$. On peut alors calculer l'évaluation $p(\mathbf{g})$ de tout polynôme p de $\mathbb{K}[\mathbf{x}_{\{i,j\}}]$ sur $\mathbf{g}$.

Définition 14.2.2 (Polynôme invariant).
On appelle polynôme invariant *un polynôme donnant la même évaluation sur deux graphes isomorphes. Clairement la somme et le produit de deux polynômes invariants sont invariants. On appelle* algèbre des polynômes invariants *l'ensemble* $\mathbb{K}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$ *des polynômes invariants.*

L'algèbre des polynômes invariants est étudiée en détail dans la partie II. Notons que, avec la définition que nous venons de donner, un polynôme est invariant s'il est invariant en tant que fonction. D'un autre côté, dans la partie II, nous utilisons une définition syntaxique d'invariant, en faisant agir $\mathfrak{S}_n$ directement sur les polynômes par permutation des variables. Un polynôme est alors invariant si $\sigma.P = P$ pour toute permutation σ de $\mathfrak{S}_n$. En fait, comme le corps $\mathbb{K}$ de base est infini, ces deux notions sont équivalentes. En effet, en utilisant le fait qu'un polynôme à plusieurs variables identiquement nul est nul, on a :

$$\forall \mathbf{g},\, \mathcal{P}_n(\sigma\mathbf{g}) = P(\mathbf{g}) \Leftrightarrow \forall \mathbf{g},\, \mathcal{P}_n(\sigma\mathbf{g}) - P(\mathbf{g}) = 0 \Leftrightarrow \sigma P - P = 0 \Leftrightarrow \sigma P = P.$$

Le résultat fondamental est qu'il existe un système d'invariants complet composé d'un nombre fini de polynômes invariants.

Théorème 14.2.3.
Il existe un ensemble fini $\{p_1, \ldots, p_k\}$ *de polynômes invariants tels que deux graphes* $\mathbf{g}$ *et* $\mathbf{g}'$ *sont isomorphes si, et seulement si, pour tout* i *on a* $p_i(\mathbf{g}) = p_i(\mathbf{g}')$.

Démonstration. D'après le théorème 8.1.7 il existe un ensemble fini $\{p_1, \ldots, p_k\}$ qui engendre l'algèbre des invariants. Pour tout polynôme invariant p la valeur $p(\mathbf{g})$ est donc déterminée par les valeurs $p_1(\mathbf{g}), \ldots p_k(\mathbf{g})$. De plus, d'après le théorème 8.1.14, deux graphes sont isomorphes si, et seulement si, ils donnent la même valeur à tous les polynômes invariants. □

On dit qu'un polynôme invariant p est *reconstructible* si, vu en tant que fonction, il est reconstructible. Dans certains cas, nous parlerons alors de reconstructibilité fonctionnelle, pour lever toute ambiguïté. La somme et le produit de deux polynômes reconstructibles sont clairement reconstructibles. L'ensemble des polynômes reconstructibles est donc une sous-algèbre de $\mathbb{K}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$.

Proposition 14.2.4.
Les deux problèmes suivants sont équivalents :
(i) Tous les graphes (valués) sur n *sommets sont reconstructibles ;*
(ii) Tous les polynômes invariants de $\mathbb{K}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$ *sont reconstructibles.*

Démonstration. Supposons (i). Soient p un polynôme invariant et $\mathbf{g}$ et $\mathbf{g}'$ deux graphes ayant même jeu. Comme $\mathbf{g}$ est reconstructible, $\mathbf{g}'$ est isomorphe à $\mathbf{g}$ et donc $p(\mathbf{g}) = p(\mathbf{g}')$. Donc p est reconstructible.

Supposons (ii). D'après le théorème 8.1.14, l'algèbre des invariants sépare les graphes à isomorphie près, c'est-à-dire que deux graphes sont isomorphes si, et seulement si, ils donnent la même valeur à tous les polynômes invariants. Soient alors $\mathbf{g}$

et $\mathbf{g}'$ deux graphes ayant même jeu. Par hypothèse, pour tout polynôme invariant p on a $p(\mathbf{g}) = p(\mathbf{g}')$ car p est reconstructible. Donc, $\mathbf{g}$ et $\mathbf{g}'$ sont isomorphes comme voulu. □

Pour pouvoir calculer l'évaluation d'un polynôme p de $\mathbb{K}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$ sur un graphe $\mathbf{g}$, il suffit que $\mathbf{g}$ soit valué dans une $\mathbb{K}$-algèbre. On pourrait imaginer que la définition de reconstructibilité de p puisse dépendre de l'espace précis dans lequel sont valués les graphes. Du fait que l'on a supposé que la caractéristique de $\mathbb{K}$ était nulle, la proposition suivante clarifie la situation.

Proposition 14.2.5.
Soit p un polynôme invariant $\mathbb{K}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$. Les deux propositions suivantes sont équivalentes :

(i) p est reconstructible sur les graphes valués dans $\mathbb{K}$

(ii) p est reconstructible sur les graphes valués dans toute $\mathbb{K}$-algèbre.

Démonstration. Le sens (ii) $\Rightarrow$ (i) est clair. Montrons la réciproque. Soit p un polynôme reconstructible sur les graphes valués dans $\mathbb{K}$. Soient $\mathbf{g}$ et $\mathbf{g}'$ deux graphes valués dans une $\mathbb{K}$-algèbre $\mathbb{L}$ et ayant même jeu. Soit $(\lambda_1, \ldots, \lambda_k)$ l'ensemble des valuations apparaissant dans $\mathbf{g}$ (sans répétition). Comme $\mathbf{g}$ et $\mathbf{g}'$ ont même jeu, les valuations apparaissant dans $\mathbf{g}'$ sont les mêmes. Soit $(y_1, \ldots, y_k)$ une liste de k variables. On considère maintenant les graphes $\tilde{\mathbf{g}}$ et $\tilde{\mathbf{g}}'$ valués dans $\mathbb{K}[y_1, \ldots, y_k]$ obtenus en substituant pour chaque arête la valuation λ_i par la variable y_i. Soit $q := p(\tilde{\mathbf{g}})$ l'évaluation de p sur $\tilde{\mathbf{g}}$. C'est un polynôme de $\mathbb{K}[y_1, \ldots, y_k]$. On pose de même $q' := p(\tilde{\mathbf{g}}')$.

Soit $a_1, \ldots, a_k$ une liste de k éléments de $\mathbb{K}$. Si l'on substitue $y_1, \ldots, y_k$ par $a_1, \ldots, a_k$ dans $\tilde{\mathbf{g}}$ et $\tilde{\mathbf{g}}'$, les deux graphes obtenus sont valués dans $\mathbb{K}$ et ont même jeu. Comme p est reconstructible, on en déduit que $q(a_1, \ldots, a_k) = q'(a_1, \ldots, a_k)$.

Comme $q - q'$ est un polynôme à plusieurs variables identiquement nul sur $\mathbb{K}^k$, c'est le polynôme nul ($\mathbb{K}$ est infini). Donc $p(\tilde{\mathbf{g}}) = p(\tilde{\mathbf{g}}')$. En resubstituant y_i par λ_i, on en déduit que $p(\mathbf{g}) = p(\mathbf{g}')$, comme voulu. □

On note que cette proposition se généralise en prenant seulement pour $\mathbb{K}$ un anneau intègre infini et pour $\mathbb{L}$ un $\mathbb{K}$-module.

14.3 Polynômes algébriquement reconstructibles

Soit $\mathbf{m}$ un *multigraphe* c'est-à-dire un graphe valué par les entiers $0, 1, 2, \ldots$. Soit $m_{\{i,j\}}$ la valuation de l'arête $\{i, j\}$ dans $\mathbf{m}$. On rappelle que l'on peut associer à $\mathbf{m}$ un monôme $\mathbf{x}^{\mathbf{m}} := \prod x_{\{i,j\}}^{m_{\{i,j\}}}$, puis un polynôme invariant $\mathbf{x}^{\mathbf{m}\circledast} := \sum_{\mathbf{m}' \in \overline{\mathbf{m}}} \mathbf{x}^{\mathbf{m}'}$, où la somme est prise sur l'orbite $\overline{\mathbf{m}}$ de $\mathbf{m}$ (voir § 10.1). La proposition suivante est fondamentale, car elle indique que l'on peut utiliser les polynômes invariants pour compter des sous-graphes.

Proposition 14.3.1.
Soient $\mathbf{g}$ et $\mathbf{h}$ deux graphes simples, et soit $\mathbf{x}^{\mathbf{g}\circledast}$ le polynôme invariant associé à $\mathbf{g}$. Le nombre $\mathbf{x}^{\mathbf{g}\circledast}(\mathbf{h})$ compte les sous-graphes de $\mathbf{h}$ isomorphes à $\mathbf{g}$.

Démonstration. Comme $\mathbf{x}^{\mathbf{g}} = \prod_{\{i,j\} \text{ arête de } \mathbf{g}} x_{\{i,j\}}$, on voit que $\mathbf{x}^{\mathbf{g}}(\mathbf{h})$ vaut 1 si $\mathbf{g}$ est un sous-graphe de $\mathbf{h}$ et 0 sinon. Comme $\mathbf{x}^{\mathbf{g}^{\circledast}}$ est la somme des $\mathbf{x}^{\mathbf{g}'}$ sur l'orbite de $\mathbf{g}$, la quantité $\mathbf{x}^{\mathbf{g}^{\circledast}}(\mathbf{h})$ est précisément le nombre d'éléments de l'orbite de $\mathbf{g}$ qui sont sous-graphes de $\mathbf{h}$, c'est-à-dire le nombre de sous-graphes de $\mathbf{h}$ isomorphes à $\mathbf{g}$. □

Notre définition de la reconstructibilité algébrique repose sur la proposition suivante, qui est une généralisation du lemme de Kelly [Kel57].

Proposition 14.3.2.
Soit $\mathbf{m}$ *un multigraphe avec au moins un sommet isolé. Le polynôme invariant* $\mathbf{x}^{m^{\circledast}}$*, vu en tant que fonction de l'ensemble des graphes valués dans* $\mathbb{K}$ *est reconstructible.*

Démonstration. Soient $p := \mathbf{x}^{\mathbf{m}^{\circledast}}$ et i un sommet isolé de $\mathbf{m}$. Soit $\mathbf{g}$ un graphe valué quelconque.

$$p(\mathbf{g}) = \sum_{\mathbf{m}' \in \overline{\mathbf{m}}} \mathbf{x}^{\mathbf{m}'}(\mathbf{g}) = \frac{1}{|\operatorname{Aut} \mathbf{m}|} \sum_{\sigma \in \mathfrak{S}_n} \mathbf{x}^{\sigma \mathbf{m}}(\mathbf{g}) = \frac{1}{|\operatorname{Aut} \mathbf{m}|} \sum_{j} \sum_{\sigma, \sigma(i)=j} \mathbf{x}^{\sigma \mathbf{m}}(\mathbf{g})$$

Pour chaque sommet j, on pose $p_j := \sum_{\sigma, \sigma(i)=j} \mathbf{x}^{\sigma \mathbf{m}}(\mathbf{g})$. Ce polynôme vérifie les propriétés suivantes :

(i) p_j est invariant par permutation des sommets laissant fixe j.

(ii) p_j ne contient aucune des variables $x_{\{j,k\}}$.

D'après (ii), $p_j(\mathbf{g}) = p_j(\mathbf{g}_{\setminus j})$. Soient $\mathbf{g}$ et $\mathbf{g}'$ deux graphes sur les sommets $1, \ldots, n$ et ayant même jeu. Il existe alors une permutation σ des sommets de $\mathbf{g}$ telle que pour tout sommet j de $\mathbf{g}$, les graphes $\mathbf{g}_{\setminus j}$ et $\mathbf{g}'_{\setminus \sigma(j)}$ sont isomorphes. Comme p est invariant, $p(\mathbf{g}') = p(\sigma^{-1}\mathbf{g}')$. On peut donc se ramener au cas où σ est l'identité, c'est-à-dire que $\mathbf{g}_{\setminus j}$ et $\mathbf{g}'_{\setminus j}$ sont isomorphes.

D'après (ii), $p_j(\mathbf{g}) = p_j(\mathbf{g}_{\setminus j})$. En utilisant (i), on obtient alors :

$$p_j(\mathbf{g}) = p_j(\mathbf{g}_{\setminus j}) = p_j(\mathbf{g}'_{\setminus j}) = p_j(\mathbf{g}'),$$

puis :

$$p(\mathbf{g}) = \frac{1}{|\operatorname{Aut} \mathbf{m}|} \sum p_j(\mathbf{g}) = \frac{1}{|\operatorname{Aut} \mathbf{m}|} \sum p_j(\mathbf{g}') = p(\mathbf{g}').$$

On en conclut que p est reconstructible. □

Ceci est bien une généralisation du lemme de Kelly.

Lemme 14.3.3 (Kelly [Kel57]).
Soit $\mathbf{g}$ *un graphe simple sur* k *sommets avec* $k < n$ *(ou, de manière équivalente, un graphe sur* n *sommets avec au moins un sommet isolé). Le nombre de sous-graphes de* $\mathbf{h}$ *isomorphes à* $\mathbf{g}$ *est reconstructible.*

Démonstration. D'après la proposition 14.3.2, le polynôme $\mathbf{x}^{\mathbf{g}^{\circledast}}$ est reconstructible, et d'après la proposition 14.3.1 l'expression $\mathbf{x}^{\mathbf{g}^{\circledast}}(\mathbf{h})$ compte précisément le nombre de sous-graphes de $\mathbf{h}$ isomorphes à $\mathbf{g}$. □

Définition 14.3.4 (Reconstructibilité algébrique).
Un polynôme invariant est dit algébriquement reconstructible *s'il s'exprime comme somme et produit de polynômes* $\mathbf{x}^{\mathbf{m}_i{}^{\circledast}}$*, où chaque* $\mathbf{m}_i$ *est un multigraphe avec au moins un sommet isolé.*

Par construction, l'ensemble des polynômes algébriquement reconstructibles forme une algèbre. Au § 10.2.1, nous en donnons une construction formelle en termes de quotient de la puissance symétrique énième de l'algèbre des invariants sur $n-1$ sommets, et nous en déduisons quelques propriétés.

Proposition 14.3.5.
Un polynôme algébriquement reconstructible est reconstructible.

Démonstration. D'après la proposition 14.3.2 les polynômes associés aux multigraphes avec au moins un sommet isolé sont reconstructibles. Comme la reconstructibilité de polynômes est stable par somme et produit, tout polynôme algébriquement reconstructible est reconstructible. □

Corollaire 14.3.6.
Tous les polynômes symétriques en les $x_{\{i,j\}}$ sont algébriquement reconstructibles.

Démonstration. En effet, la k-ième fonction puissance $\sum x_{\{i,j\}}^k$ est le polynôme invariant associé au multigraphe composé d'une seule arête valuée k. Ce multigraphe a un sommet isolé (car $n \geq 3$) et est donc algébriquement reconstructible. Enfin, les fonctions puissances engendrent tous les polynômes symétriques. □

On déduit de ce fait que la liste des valuations des arêtes, considérée à permutation près, est reconstructible (une liste de valeurs λ_i est déterminée à permutation près par ses sommes de puissances $\sum \lambda_i^k$).

Le théorème suivant est un résultat de complétude, dans le sens où les polynômes algébriquement reconstructibles sont suffisants pour caractériser les graphes ayant même jeu.

Théorème 14.3.7.
Deux graphes ont même jeu si, et seulement si, ils donnent la même évaluation à tous les polynômes algébriquement reconstructibles.

Démonstration. D'après la proposition 14.3.5 les polynômes algébriquement reconstructibles sont reconstructibles. Il est donc clair que deux graphes ayant même jeu donnent la même évaluation à tous les polynômes algébriquement reconstructibles. Montrons la réciproque.

D'après le théorème 14.2.3, on sait qu'il existe un système fini $p_0, \ldots, p_k$ d'invariants sur les graphes à $n-1$ sommets tel que deux graphes sur $n-1$ sommets sont isomorphes si, et seulement si, ils donnent la même valeur à tous les p_i. Soit λ une variable supplémentaire, et $P := p_0 + \lambda p_1 + \cdots + \lambda^k p_k$.

Remarque 14.3.8: Soient $\mathbf{g}$ et $\mathbf{g}'$ deux graphes sur $n-1$ sommets. Soient aussi $P(\mathbf{g}) := p_0(\mathbf{g}) + \lambda p_1(\mathbf{g}) + \cdots + \lambda^k p_k(\mathbf{g})$ et $P(\mathbf{g}') := p_0(\mathbf{g}') + \lambda p_1(\mathbf{g}') + \cdots + \lambda^k p_k(\mathbf{g}')$ les polynômes de $\mathbb{C}[\lambda]$ correspondants. Alors, les graphes $\mathbf{g}$ et $\mathbf{g}'$ sont isomorphes si, et seulement si, $P(\mathbf{g}) = P(\mathbf{g}')$.

Revenons aux graphes sur n sommets, et soit v un de ces sommets. On rappelle que l'on note $\mathbf{g}_v$ le graphe obtenu en enlevant le sommet v du graphe $\mathbf{g}$. En renumérotant convenablement les sommets, on peut définir un polynôme $P_v := p_{v,0} + \lambda p_{v,1} + \cdots + \lambda^k p_{v,k}$ sur les graphes à n sommets de sorte que pour tout graphe $\mathbf{g}$, on ait $P_v(\mathbf{g}) = P(\mathbf{g}_v)$.

Considérons le polynôme $q := {P_v}^l$. On peut l'écrire sous la forme $q = c_{v,0} + c_{v,1}\lambda^1 + \cdots + c_{v,d}\lambda^d$, où chaque $c_{v,i}$ est un polynôme en les variables $x_{\{i,j\}}$ dans lequel aucune des variables $x_{\{v,j\}}$ n'apparaît. Soit $s_l := \sum_{v=1}^n P_v^l$. Il s'écrit sous la forme :

$$(\sum_{v=1}^{n} c_{v,0}) + (\sum_{v=1}^{n} c_{v,1})\lambda + \cdots + (\sum_{v=1}^{n} c_{v,d})\lambda^d.$$

Chacun des coefficients $\sum_{v=1}^n c_{v,d})$ est un polynôme invariant ; il est de plus algébriquement reconstructible, car chaque $c_{v,d}$ ne contient aucune des variables $x_{\{i,j\}}$.

Soient $\mathbf{g}$ et $\mathbf{g}'$ deux graphes donnant la même valeur à tous les polynômes invariants algébriquement reconstructibles. D'après ce qui précède, $s_l(\mathbf{g})$ et $s_l(\mathbf{g}')$ sont deux polynômes de $\mathbb{C}[\lambda]$ donnés dont les coefficients sont égaux. On en déduit que, pour tout l,

$$\sum_{v=1}^{n} \left(P_v(\mathbf{g})\right)^l = s_l(\mathbf{g}) = s_l(\mathbf{g}') = \sum_{v=1}^{n} \left(P_v(\mathbf{g}')\right)^l.$$

Il en résulte, d'après le théorème classique sur les fonctions symétriques, qu'il existe une permutation σ des sommets telle que $P_v(\mathbf{g}) = P_{\sigma(v)}(\mathbf{g}')$, pour tout v. Il s'ensuit, selon la remarque 14.3.8, que les graphes $\mathbf{g}_{\setminus v}$ et $\mathbf{g}_{\setminus \sigma(v)}$ sont isomorphes. Conclusion : $\mathbf{g}$ et $\mathbf{g}'$ ont même jeu. □

Problème 14.3.9 (Pouzet [Pou77]).
Pour $n \geq 3$, tous les polynômes invariants sont-ils algébriquement reconstructibles ?

En termes algébriques, cela revient à se demander si l'algèbre des invariants est engendrée par les polynômes invariants $\mathbf{x}^{\mathbf{m}\circledast}$ où $\mathbf{m}$ est un multigraphe avec un sommet isolé.

Notre approche a été guidée par l'étude de ce problème. En effet, d'après les théorèmes 14.2.3 et 14.3.7, une réponse positive aurait entraîné la reconstructibilité de tous les graphes, simples ou valués, et donc la conjecture de Ulam.

14.4 Multigraphes algébriquement reconstructibles

La notion de reconstruction algébrique permet une approche globale du problème de reconstruction. Il est heureusement possible de l'utiliser pour une approche plus locale, de façon à pouvoir obtenir des résultats partiels, comme par exemple montrer que certaines classes de graphes sont reconstructibles.

Lemme 14.4.1.
Soit $\mathbf{m}$ un multigraphe dont le polynôme invariant $\mathbf{x}^{\mathbf{m}\circledast}$ est reconstructible. Alors, $\mathbf{m}$ est un multigraphe reconstructible.

Démonstration. Le principe de la démonstration ressort mieux dans le cas des graphes simples. Soit $\mathbf{g}$ un graphe simple tel que le polynôme invariant $p := \mathbf{x}^{\mathbf{g}\circledast}$ est reconstructible. Soit $\mathbf{g}'$ un graphe ayant même jeu. Comme la liste des valuations des arêtes est reconstructible, $\mathbf{g}'$ est aussi un graphe simple. La proposition 14.3.1 affirme alors que $p(\mathbf{g}')$ est le nombre $s(\mathbf{g}, \mathbf{g}')$ de sous graphes de $\mathbf{g}'$ isomorphes à $\mathbf{g}$.

On a $s(\mathbf{g}, \mathbf{g}') = p(\mathbf{g}') = p(\mathbf{g}) = s(\mathbf{g}, \mathbf{g})$, et ce dernier nombre est strictement positif. On en déduit que $\mathbf{g}'$ a un sous-graphe isomorphe à $\mathbf{g}$. Ce sous-graphe est forcément $\mathbf{g}'$ lui-même, puisque $\mathbf{g}$ et $\mathbf{g}'$ ont le même nombre d'arêtes.

Pour un multigraphe $\mathbf{m}$, la démonstration repose essentiellement sur la même idée, mais est nettement plus technique. On considère l'ensemble $\{\lambda_1, \lambda_2, \ldots, \lambda_k\}$ des valuations apparaissant sur les arêtes de $\mathbf{m}$ (on suppose $\lambda_1 < \lambda_2 < \cdots < \lambda_k$). Par exemple, pour le graphe vide c'est l'ensemble $\{0\}$, pour le graphe complet c'est $\{1\}$ et pour un autre graphe simple, $\{0, 1\}$.

Nous allons donc substituer les valeurs $\lambda_1, \ldots, \lambda_k$ par des variables indépendantes $y_1, \ldots, y_k$. Le graphe $\tilde{\mathbf{m}}$ est un graphe valué dans le corps des fractions $\mathbb{K}(\lambda_1, \ldots, \lambda_k)$. Étant donné un polynôme p invariant, son évaluation $p(\mathbf{m})$ est un polynôme de $\mathbb{K}[\lambda_1, \ldots, \lambda_k]$. Soit $\mathbf{m}'$ un multigraphe ayant le même jeu que $\mathbf{m}$. Ils ont la même liste de valuations à permutation près. En particulier, le nombre d'arêtes valuées λ_i dans $\mathbf{m}$ et dans $\mathbf{m}'$ coïncident. Soit n_i ce nombre. De même que pour $\mathbf{m}$, on substitue dans $\mathbf{m}'$ les valuations λ_i par les variables y_i.

Soit $p := \mathbf{x}^{\mathbf{m}\circledast}$ le polynôme invariant associé à $\mathbf{m}$. On suppose p reconstructible. On a vu qu'il restait reconstructible pour des graphes valués dans toute sur-algèbre de $\mathbb{K}$, et donc en particulier pour $\mathbb{K}[y_1, \ldots, y_k]$ (proposition 14.2.5). Donc, comme $\tilde{\mathbf{m}}$ et $\tilde{\mathbf{m}}'$ ont même jeu, $p(\tilde{\mathbf{m}}) = p(\tilde{\mathbf{m}}')$. Nous allons en déduire que $\tilde{\mathbf{m}}$ est isomorphe à $\tilde{\mathbf{m}}'$.

L'évaluation du monôme $\mathbf{x}^{\mathbf{m}}$ en $\tilde{\mathbf{m}}$, vaut $q := \prod y_i^{n_i \lambda_i}$ (chaque arête $\{v, v'\}$ valuée y_i de $\tilde{\mathbf{m}}$ est élevée à la puissance de la variable $x_{\{v,v'\}}$ dans $\mathbf{x}^{\mathbf{m}}$, c'est-à-dire λ_i). Ce monôme apparaît donc dans $p(\tilde{\mathbf{m}})$ avec un coefficient entier strictement positif ($\mathbb{K}$ est de caractéristique 0 !). Comme $p(\tilde{\mathbf{m}}') = p(\tilde{\mathbf{m}}')$, il apparaît aussi dans $p(\tilde{\mathbf{m}}')$, et il existe donc une permutation σ telle que $\mathbf{x}^{\sigma\mathbf{m}}(\tilde{\mathbf{m}}') = q$.

Il ne reste plus qu'à montrer que $\sigma\mathbf{m} = \mathbf{m}'$. Soit V_k l'ensemble des arêtes valuées λ_k de $\mathbf{m}'$. Comme λ_k est strictement plus grand que les autres λ_i, les variables $x_{\{v,v'\}}$ sont au maximum élevées à la puissance λ_k dans $\mathbf{x}^{\sigma\mathbf{m}}$. Donc la puissance de y_k dans $\mathbf{x}^{\sigma\mathbf{m}}(\tilde{\mathbf{m}}')$ est au maximum $|V_k|\lambda_k$, avec égalité si, et seulement si, chaque arête $\{v, v'\}$ de V_k est valuée λ_k dans $\sigma\mathbf{m}$. C'est le cas, car $|V_k| = n_k$. Comme le nombre d'arêtes valuées λ_k dans $\sigma\mathbf{m}$ est aussi n_k, pour toute arête $\{v, v'\}$ restante de $\mathbf{m}$, la variable $x_{\{v,v'\}}$ est élevée au maximum à la puissance λ_{k-1}. On procède alors de même pour λ_{k-1}, puis par récurrence jusqu'à λ_1. Conclusion : les arêtes valuées λ_i dans $\mathbf{m}'$ sont aussi valuées λ_i dans $\sigma\mathbf{m}'$. Autrement dit, $\mathbf{m}$ et $\mathbf{m}'$ sont isomorphes, comme voulu. □

Définition 14.4.2 (Multigraphe algébriquement reconstructible).
Du fait du lemme 14.4.1, on appelle algébriquement reconstructible *un multigraphe* $\mathbf{m}$ *dont le polynôme invariant* $\mathbf{x}^{\mathbf{m}\circledast}$ *est algébriquement reconstructible.*

On a alors :

$$\mathbf{m} \text{ algébriquement reconstructible } \Rightarrow \mathbf{x}^{\mathbf{m}\circledast} \text{ reconstructible } \Rightarrow \mathbf{m} \text{ reconstructible}$$

On peut donc utiliser la notion de reconstruction algébrique pour montrer que certaines classes de graphes sont reconstructibles. On note qu'au moins une des réciproques des implications ci-dessus est fausse. De fait, il existe des graphes simples à 13 sommets et 17 arêtes non-algébriquement reconstructibles, alors que tous ces graphes simples sont reconstructibles (voir § 18).

Par exemple, si l'on montre qu'un graphe simple est algébriquement reconstructible, on montre qu'il est reconstructible au sens usuel. Cependant on montre aussi que, pour tout autre graphe simple $\mathbf{g}'$, le nombre $s(\mathbf{g}, \mathbf{g}')$ de sous-graphes de $\mathbf{g}'$ isomorphes à $\mathbf{g}$ est aussi reconstructible, ce qui est *a priori* beaucoup plus fort.

Chapitre 15

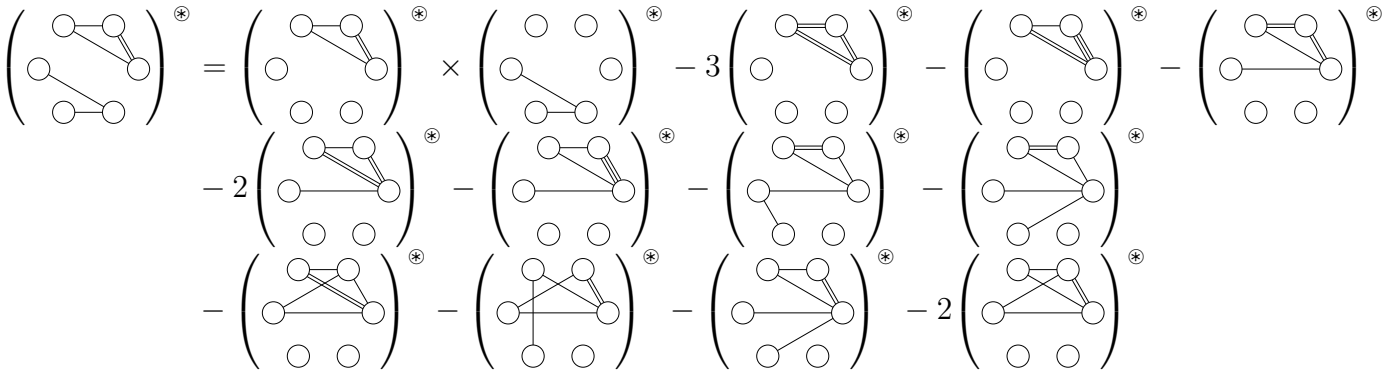
Expression des principaux résultats classiques dans ce cadre

Notre exposé sera parallèle à celui de Kocay [Koc82]. Dans la plupart des cas, les arguments seront très semblables. Cependant, dans notre cas, nous les appliquons dans l'algèbre des polynômes invariants, c'est-à-dire des multigraphes, et non seulement dans l'algèbre des sous-graphes simples. Nous en déduirons dans certains cas des résultats plus généraux sur les graphes valués.

15.1 Connexité

Théorème 15.1.1.
Les multigraphes non-connexes sont algébriquement reconstructibles.

Démonstration. Soit $\mathbf{m}$ un multigraphe sur n sommets union disjointe de deux composantes connexes $\mathbf{m}_1$ et $\mathbf{m}_2$ de tailles respectives $n_1 > 0$ et $n_2 > 0$, avec $n_1 + n_2 = n$. On veut montrer que le polynôme $\mathbf{x}^{\mathbf{m}\circledast}$ est algébriquement reconstructible. On étend $\mathbf{m}_1$ et $\mathbf{m}_2$ en des graphes sur n sommets en rajoutant à chacun des sommets isolés. Comme $n_1 < n$ et $n_2 < n$, leurs polynômes invariants associés $\mathbf{x}^{\mathbf{m}_1\circledast}$ et $\mathbf{x}^{\mathbf{m}_2\circledast}$ sont algébriquement reconstructibles. De même pour $\mathbf{m}_2$. On considère le produit $p := \mathbf{x}^{\mathbf{m}_1\circledast}\mathbf{x}^{\mathbf{m}_2\circledast}$. Ce produit consiste à prendre toutes les superpositions de $\mathbf{m}_1$ et $\mathbf{m}_2$. Dans les termes obtenus, $\mathbf{m}_1$ et $\mathbf{m}_2$ peuvent soit être disjoints, soit avoir au moins un sommet en commun. Dans le premier cas, on obtient un multigraphe avec comme composantes connexes $\mathbf{m}_1$ et $\mathbf{m}_2$, qui est donc isomorphe à $\mathbf{m}$. Dans le deuxième cas, $\mathbf{m}_1$ et $\mathbf{m}_2$ couvrent strictement moins de $n_1 + n_2$ sommets. Le multigraphe obtenu a donc forcément un sommet isolé et est algébriquement reconstructible. On peut donc le retirer du produit p. Au final, on a exprimé $\mathbf{x}^{\mathbf{m}\circledast}$ comme somme et produit de polynômes algébriquement reconstructibles, comme voulu. Par exemple :



□

En appliquant le lemme 14.4.1, on en déduit immédiatement que les multigraphes non-connexes (et donc tous les graphes valués non-connexes) sont reconstructibles. En particulier, les graphes non-connexes sont reconstructibles [Kel57].

Proposition 15.1.2 (Tutte [Tut79]).
Soit $\mathbf{h}$ *un graphe simple. Le nombre de sous-graphes couvrants de* $\mathbf{h}$ *avec* k *composantes connexes isomorphes à* $\mathbf{f}_1, \ldots, \mathbf{f}_k$ *est reconstructible.*

Démonstration. Soit $\mathbf{g}$ la réunion disjointe des f_i, et $p := \mathbf{x}^{\mathbf{g}^{\circledast}}$. D'après le lemme 14.3.1, le nombre $p(\mathbf{h})$ compte précisément les sous-graphes couvrants de $\mathbf{h}$ avec k composantes connexes isomorphes à $\mathbf{f}_1, \ldots, \mathbf{f}_k$ N. Comme le graphe $\mathbf{g}$ est non-connexe, il est algébriquement reconstructible, et donc p est reconstructible, ce qui permet de conclure. □

Corollaire 15.1.3.
La taille maximale d'un couplage d'un graphe simple $\mathbf{h}$ *est reconstructible.*
Le nombre d'arbres couvrants de $\mathbf{h}$ *est reconstructible.*

Démonstration. Soit $\mathbf{g}$ le graphe composé de k arêtes disjointes. Il est clair que $\mathbf{g}$ est algébriquement reconstructible, et que $\mathbf{g}(\mathbf{h})$ compte le nombre de couplages à k arêtes de $\mathbf{g}$. Ce dernier nombre est donc reconstructible pour tout k. On en déduit, entre autres, que le nombre de couplages maximaux de $\mathbf{h}$ est reconstructible.

Soit e_{n-1} le polynôme symétrique élémentaire de degré $n-1$ en les variables $x_{\{i,j\}}$. Il peut être interprété comme la somme de tous les polynômes $\mathbf{x}^{\mathbf{g}^{\circledast}}$, où $\mathbf{g}$ est un graphe simple avec $n-1$ arêtes. On élimine de e_{n-1} tous les graphes non-connexes. Comme ils sont algébriquement reconstructibles, le polynôme p restant est algébriquement reconstructible. De plus p est la somme de tous les $\mathbf{x}^{\mathbf{g}^{\circledast}}$ où $\mathbf{g}$ est un arbre couvrant. On en déduit que $p(\mathbf{h})$ est le nombre d'arbres couvrants de $\mathbf{h}$, nombre qui est donc reconstructible. □

Par extension, on dira qu'un polynôme invariant est *non-connexe* s'il s'exprime comme combinaison linéaire de polynômes invariants $\mathbf{x}^{\mathbf{m}^{\circledast}}$ associés à des multigraphes $\mathbf{m}$ non-connexes. De tels polynômes invariants sont clairement algébriquement reconstructibles. De nombreux invariants sur les graphes simples sont reconstructibles car ils s'expriment au moyen de polynômes invariants non-connexes. Prenons comme exemple le *nombre!chromatique* (voir [Ber83] pour la définition).

Proposition 15.1.4.

(i) Soient $\lambda_1, \ldots, \lambda_k$ k couleurs et $n_1 + n_2 + \cdots + n_k$ une partition de n. Le nombre de bonnes colorations des sommets d'un graphe simple $\mathbf{g}$ telles qu'il y a n_i sommets de couleur λ_i est algébriquement reconstructible.

(ii) Le nombre chromatique et le polynôme chromatique d'un graphe sont reconstructibles.

Le point (ii) est connu (voir [Bon91, p. 230]). En revanche nous n'avons pas vu énoncé le point (i).

Démonstration. Soit $\mathbf{V} = \{V_1, \ldots, V_k\}$ une partition des sommets telle que $|V_i| = n_i$. On note $v \approx v'$, si v et v' sont dans un même V_i. Soit

$$p_{\mathbf{V}} := \prod_{v \approx v'} (1 - x_{\{v,v'\}}).$$

Soit $\mathbf{g}$ un graphe simple. On considère la coloration de $\mathbf{g}$ obtenue en colorant les sommets de V_i par λ_i. On constate que $p_{\mathbf{V}}(\mathbf{g})$ vaut 1 si $\mathbf{g}$ n'a aucune arête à l'intérieur des V_i, (c'est-à-dire si la coloration est bonne) et 0 sinon.

Soit maintenant q la somme des $p_{\mathbf{V}}$ lorsque $\mathbf{V}$ parcourt les partitions des sommets avec des parts de taille $n_1, \ldots, n_k$. La quantité $q(\mathbf{g})$ compte le nombre de bonnes colorations voulues dans l'énoncé. Si $\mathbf{V}$ ne contient qu'une part, q est le polynôme invariant obtenu en substituant $x_{\{i,j\}}$ par $(1 - x_{\{i,j\}})$ dans le polynôme symétrique $\prod x_{\{i,j\}}$. Donc p est algébriquement reconstructible (corollaire 14.3.6 et proposition 16.2.1). Sinon, q est un polynôme non-connexe, et est donc algébriquement reconstructible. Cela clôt la démonstration du (i).

Soit P le polynôme chromatique d'un graphe $\mathbf{g}$. Par définition, $P(k)$ est le nombre de colorations de $\mathbf{g}$ en k parts. Si l'on considère $q_k := \sum p_{\mathbf{V}}$, où la somme est prise sur toutes les partitions des sommets en k parts non vides, on a $P(k) := q_k(\mathbf{g})$. On en déduit d'après le point (i) que $P(k)$ est reconstructible pour tout k. Donc, le polynôme chromatique est reconstructible. Enfin, le nombre chromatique est le plus petit $k \geq 0$ tel que $P(k) > 0$, il est lui aussi reconstructible. □

Cette méthode se généralise à toute une classe d'invariants sur les graphes. Soit $\mathcal{P}$ une propriété invariante sur les graphes simples, par exemple « être le graphe vide ». On dit qu'une partition $\mathbf{V} = \{V_1, \ldots, V_k\}$ des sommets d'un graphe simple $\mathbf{g}$ est *bonne* si tous les graphes induits par $\mathbf{g}$ sur les parts $V_1, \ldots, V_k$ vérifient la propriété $\mathcal{P}$. Pour toute partition $n_1, n_2, \ldots, n_k$ de n, on note $N_{\mathcal{P},n_1,\ldots,n_k}(\mathbf{g})$ le nombre de bonnes partitions des sommets de $\mathbf{g}$ en parts de taille $n_1, \ldots, n_k$. Enfin, on note $N_{\mathcal{P}}(\mathbf{g})$ le plus petit k tel qu'il existe une partition $n_1, \ldots, n_k$ de sorte que $N_{\mathcal{P},n_1,\ldots,n_k}$ est non nul.

Par exemple, si $\mathcal{P}$ est la propriété « être le graphe vide », $N_{\mathcal{P}}(\mathbf{g})$ est le nombre chromatique du graphe $\mathbf{g}$.

Théorème 15.1.5.
Soit $\mathcal{P}$ une propriété sur les graphes simples. On définit comme ci-dessus l'entier $N_{\mathcal{P}}$, et pour pour toute partition $n_1, \ldots, n_k$ de n l'entier $N_{\mathcal{P},n_1,\ldots,n_k}(\mathbf{g})$. Alors, si $k \geq 2$, le nombre $N_{\mathcal{P},n_1,\ldots,n_k}(\mathbf{g})$ est reconstructible. En particulier, si la propriété $\mathcal{P}$ est reconstructible (c'est-à-dire si l'on peut tester si le graphe non-partitionné lui-même vérifie la propriété), alors le nombre $N_{\mathcal{P}}(\mathbf{g})$ est reconstructible.

Démonstration. Soit $\mathbf{V} = \{V1, \ldots, V_k\}$ une partition des sommets telle que $|V_i| = n_i$. Il n'y a qu'un nombre fini de graphes simples sur les sommets V_1. On peut donc construire un polynôme p_1 en les variables $x_{\{i,j\}}, i, j \in V_1$, de sorte que pour tout graphe simple $\mathbf{g}$ sur ces sommets, $p_1(\mathbf{g})$ vaut 1 si $\mathbf{g}$ vérifie la propriété $\mathcal{P}$, et 0 sinon. On peut de même construire un polynôme p_2 qui teste la propriété $\mathcal{P}$ pour les graphes sur les sommets V_2, et ainsi de suite. Soit $p_{\mathbf{V}}$ le produit $p_1 \cdots p_k$ de ces polynômes. Clairement, pour tout graphe simple $\mathbf{g}$ sur $\{1, \ldots, n\}$, on a $p(\mathbf{g}) = 1$ si, et seulement si, la partition $\mathbf{V}$ est bonne.

Soit q la somme des $p_{\mathbf{V}}$, où $\mathbf{V}$ parcourt toutes les partitions des sommets avec des parts de taille $n_1, \ldots, n_k$. C'est un polynôme invariant tel que $q(\mathbf{g})$ compte le nombre recherché $N_{\mathcal{P},n_1,\ldots,n_k}(\mathbf{g})$ de bonnes partitions. De plus, si $k \geq 2$, le polynôme q est non-connexe, et donc algébriquement reconstructible. Il en découle que $N_{\mathcal{P},n_1,\ldots,n_k}(\mathbf{g})$ est reconstructible.

Si de plus la propriété $\mathcal{P}$ est reconstructible, $N_{\mathcal{P},n}$ est aussi reconstructible. Donc $N_{\mathcal{P}}$ est reconstructible, ce qui clôt la démonstration. □

Bien entendu, ce théorème se généralise aux multigraphes, pour toute propriété que l'on peut tester par un (ou plusieurs) polynômes.

En plus du nombre chromatique, plusieurs paramètres classiques sur les graphes simples s'expriment dans le cadre de ce théorème, et sont donc reconstructibles. Si $\mathcal{P}$ est la propriété « être le graphe complet », $N_{\mathcal{P}}(\mathbf{g})$ est appelé *nombre cochromatique* de $\mathbf{g}$ [Ber83]. Si $\mathcal{P}$ est la propriété « être un arbre », $N_{\mathcal{P}}(g)$ est appelé *point arboricity* de $\mathbf{g}$ [Har83]. Si $\mathcal{P}$ est la propriété « être un chemin », $N_{\mathcal{P}}(g)$ est appelé *linear point arboricity* de $\mathbf{g}$ [Che94]. On dit qu'un graphe est k-dégénéré si dans tout sous-graphe $\mathbf{g}'$ de $\mathbf{g}$ le degré minimal des sommets de $\mathbf{g}'$ est inférieur à k. Un graphe 0-dégénéré est le graphe vide, et un graphe 1-dégénéré est un arbre. Si $\mathcal{P}$ est la propriété « être k-dégénéré », $N_{\mathcal{P}}(\mathbf{g})$ est appelé *k-point partition number* de $\mathbf{g}$ [LW74].

Corollaire 15.1.6.
Les quantités suivantes sont reconstructibles :
- *nombre chromatique*
- *nombre cochromatique*
- point arboricity
- linear point arboricity
- k-point partition number

Démonstration. Il suffit de vérifier que les propriétés sous-jacentes sont reconstructibles. On rappelle que la liste des degrés des sommets d'un graphe est reconstructible. Il en découle immédiatement que les propriétés « être le graphe vide », « être le graphe complet » et « être un chemin » sont reconstructibles. Il en est de même pour la propriété « être k-dégénéré », puisqu'elle n'impose des conditions que sur les degrés des sommets et sur les sous-graphes induits stricts. Enfin, la propriété « être un arbre » est équivalente à la propriété « être 1-dégénéré ». □

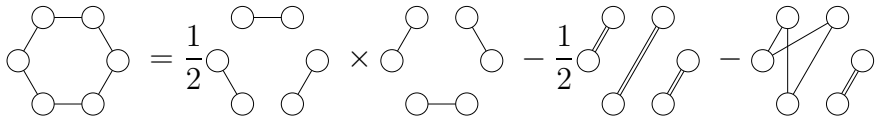
Un autre paramètre, appelé *k-point arboricity* [Lic76] rentre dans ce cadre, mais nous ne savons pas si la propriété sous-jacente « être k-acyclic » est reconstructible.

15.2 Cycles hamiltoniens et polynôme caractéristique

Théorème 15.2.1 (Tutte [Tut79]).
Le nombre de cycles hamiltoniens d'un graphe $\mathbf{g}$ *simple est reconstructible.*

Démonstration. Soit $\mathbf{c}$ un cycle sur n sommets. Il est clair que $\mathbf{x}^{\mathbf{c}\circledast}(\mathbf{h})$ compte le nombre de cycles hamiltoniens de $\mathbf{c}$.

- Cas n pair : On peut court-circuiter légèrement la démonstration de Kocay [Koc82] comme suit. Soit $\mathbf{g}$ le couplage maximal, composé de $\frac{n}{2}$ arêtes disjointes, et soit $p := (\mathbf{x}^{\mathbf{c}\circledast})^2$. Soit $\mathbf{m}$ un multigraphe apparaissant dans p. Il est obtenu par superposition de deux permutés de $\mathbf{g}$. Comme les sommets de $\mathbf{g}$ sont tous de degré 1, les sommets de $\mathbf{m}$ sont de degré 2. Donc $\mathbf{m}$ est soit un cycle sur n sommets, isomorphe à $\mathbf{g}$, soit la réunion disjointe de plusieurs cycles, éventuellement réduits à une double arête. Par non-connexité, le graphe $\mathbf{g}$ et donc le polynôme p sont algébriquement reconstructibles, ainsi que tous les termes $\mathbf{m}$ qui ne sont pas des cycles sur n sommets. On en déduit que $\mathbf{x}^{\mathbf{c}\circledast}$ est algébriquement reconstructible. Par exemple :



- Dans le cas impair, on procède comme dans [Koc82]. Pour $k \in 1, \ldots, \mathrm{C}_n^2$, on définit e_k le polynôme symétrique élémentaire de degré k en les variables $x_{\{i,j\}}$. Comme tout polynôme symétrique, ce polynôme est algébriquement reconstructible. On peut interpréter e_n comme la somme de tous les polynômes $\mathbf{x}^{\mathbf{g}\circledast}$ où $\mathbf{g}$ est un graphe simple avec n arêtes. Ces graphes sont soit
  (i) des cycles hamiltoniens,
  (ii) des graphes simples avec un cycle, de taille $< n$
  (iii) des graphes non-connexes.
  Les graphes dans (iii) sont algébriquement reconstructibles, et le polynôme $\tilde{e}_n$ obtenu en les retirant de e_n est algébriquement reconstructible.
  Soit c_k un cycle de longueur k, avec $k < n$, et $p_k := \mathbf{x}^{c_k\circledast} e_n - k$. Ce polynôme est algébriquement reconstructible. On en retire tous les termes correspondant à des multigraphes non-connexes. Le polynôme $\tilde{p}_k$ restant est la somme de tous les $\mathbf{x}^{\mathbf{g}\circledast}$ où $\mathbf{g}$ est un graphe simple contenant un seul cycle (de longueur k). Au final, lorsque l'on soustrait chaque $\tilde{p}_k$ de $\tilde{e}_n$, on obtient $\mathbf{x}^{\mathbf{c}\circledast}$. On en déduit que ce dernier est algébriquement reconstructible. □

Un graphe $\mathbf{g}$ est dit *séparable* s'il existe un sommet v tel que $\mathbf{g}$ privé du sommet v est non-connexe. Nous ne rentrons pas dans les détails, mais ceci définit une partition des arêtes de $\mathbf{g}$ en blocs, deux blocs ayant au maximum un sommet en commun. De plus ces blocs ne forment pas de cycles.

Théorème 15.2.2.
Soit $\mathbf{h}$ *un graphe simple. Le nombre de sous-graphes séparables de* $\mathbf{h}$*, avec* k *blocs isomorphes à* $\mathbf{f}_1, \ldots, \mathbf{f}_k$ *est reconstructible.*

Démonstration. Comme pour la connexité, on considère $p := \mathbf{x}^{f_1{}^{\circledast}}, \ldots, \mathbf{x}^{f_k{}^{\circledast}}$, et on construit $\tilde{p}$ en retirant tous les multigraphes avec un sommet isolé. Tous les termes de $\tilde{p}$ correspondent à des graphes simples avec k blocs isomorphes à $f_1, \ldots, f_k$. Donc $\tilde{p}(\mathbf{h})$ compte le nombre voulu, et est reconstructible. □

Soit $\mathbf{h}$ un graphe valué. On considère la matrice symétrique M à diagonale nulle dont le coefficient $M_{i,j}$ est la valuation de l'arête $\{i, j\}$ de $\mathbf{h}$. On appelle *déterminant* et *polynôme caractéristique* de $\mathbf{h}$ le déterminant $\det(M)$ et le polynôme caractéristique $\det(M - \lambda Id)$ de M. D'après Tutte [Tut76, Tut79], pour un graphe simple ces deux quantités sont reconstructibles.

Théorème 15.2.3 ([Pou77]).
Le déterminant et le polynôme caractéristique d'un graphe valué sont algébriquement reconstructibles.

Plus précisément, les coefficients c_k du polynôme caractéristique peuvent s'exprimer comme des polynômes invariants en les $x_{\{i,j\}}$ qui sont algébriquement reconstructibles.

Démonstration. Considérons la matrice symétrique générique M dont les entrées sur la diagonale sont $-\lambda$ et les entrées en dehors de la diagonale sont les variables $x_{\{i,j\}}$. Si l'on développe complètement l'expression $\det(M)$, on obtient des termes de la forme $\lambda^k \prod x_{i,\sigma(i)}$. Chaque $\prod x_{i,\sigma(i)}$ peut être vu sous la forme $\mathbf{x}^{\mathbf{g}}$, où $\mathbf{g}$ est un graphe simple composé d'un ou plusieurs cycles disjoints. On en déduit que le coefficient de λ^k est une somme de polynômes invariants $\mathbf{x}^{\mathbf{g}^{\circledast}}$ où $\mathbf{g}$ est un graphe simple composé d'un ou plusieurs cycles disjoints. Cela permet de conclure, car nous avons vu dans la démonstration du théorème 15.2.1 que ces graphes étaient algébriquement reconstructibles. □

15.3 Graphes étoilés et 0-réguliers

Proposition 15.3.1.
Tout polynôme invariant coïncide sur les graphes 0-réguliers avec un polynôme algébriquement reconstructible.

Démonstration. Soit P un polynôme invariant. Soit Q le polynôme obtenu en substituant $x_{i,n}$ par $-\sum_{j<n j\neq i} x_{i,j}$. Le sommet n est isolé dans Q, puisqu'il ne contient plus de variable de la forme $x_{i,n}$. On en déduit que Q^* est un polynôme invariant algébriquement reconstructible. Il ne reste plus qu'à montrer que P et Q^* coïncident sur les graphes 0-réguliers.

Soit $\mathbf{g}$ un tel graphe. On vérifie que $x_{i,n}(\mathbf{g}) = -\sum_{j,j<n,j\neq i} x_{i,j}(\mathbf{g})$. Donc par construction $Q(\mathbf{g}) = P(\mathbf{g})$, et on conclut comme suit.

$$\begin{aligned} Q^*(\mathbf{g}) &= \frac{1}{n!} Q(\sigma^{-1}.\mathbf{g}) = \sum_{\sigma} P(\sigma^{-1}.\mathbf{g}) && (\sigma.\mathbf{g} \text{ est 0-régulier}) \\ &= P^*(\mathbf{g}) = P(\mathbf{g}) && (P \text{ est invariant}). \end{aligned}$$

□

Corollaire 15.3.2.
Les graphes 0*-réguliers sont reconstructibles.*

Démonstration. Soit $\mathbf{g}$ un graphe 0-régulier, et $\mathbf{g}'$ tel que $\mathrm{Jeu}(g') = \mathrm{Jeu}(g)$. Le graphe $\mathbf{g}'$ est aussi 0-régulier. Pour tout polynôme invariant P sur les graphes 0-réguliers, P coïncide sur les graphes 0-réguliers avec un polynôme Q reconstructible, donc $P(g) = P(g')$. On conclut, puisqu'un $\mathfrak{S}_n$-module est séparé par ses polynômes invariants. □

Chapitre 16

Opérateurs préservant la reconstructibilité algébrique

Dans ce chapitre, nous recherchons les opérations qui préservent la reconstructibilité algébrique. Nous montrons en particulier qu'elle est préservée par composition et substitution polynomiale et par dérivation. Nous en déduisons qu'elle est préservée par passage au complémentaire et, sous certaines conditions, par fraction et racine. Pour les graphes simples, elle est aussi préservée par l'opérateur Etoile. Cela nous permet de montrer que, si les graphes simples à $\lfloor \frac{C_n^2}{2} \rfloor$ arêtes sont algébriquement reconstructibles, alors tous les graphes simples sont algébriquement reconstructibles.

Nous introduisons aussi la notion de i-reconstructibilité qui nous permet, entre autres, de montrer que les étoiles valuées et les polynômes symétriques en les étoiles sont algébriquement reconstructibles. Cette notion sera centrale au § 19.

Enfin, nous montrons que les constructions de polynômes reconstructibles au moyen d'autres moyennes symétriques sur le groupe se ramènent à la reconstructibilité algébrique.

Tous ces résultats indiquent que la notion de reconstructibilité algébrique n'est pas trop restrictive.

16.1 Composition à gauche

On remarque que la reconstructibilité fonctionnelle est naturellement préservée par composition à gauche.

Proposition 16.1.1.
Soient h une fonction d'une variable complexe et f une fonction reconstructible. Alors, la fonction $h \circ f$ est reconstructible.

On voudrait essayer de généraliser ceci aux polynômes algébriquement reconstructibles. Bien entendu, on impose que le résultat $h \circ p$ soit un polynôme, ce qui est *a priori* une contrainte très forte !

Problème 16.1.2.
Soit h une fonction de $\mathbb{K}$ dans $\mathbb{K}$. Soit p un polynôme algébriquement reconstructible. Si $h \circ p$ est un polynôme (nécessairement invariant), est-ce que $h \circ p$ est algébriquement reconstructible ?

Par exemple, si h est un polynôme de $\mathbb{K}[x]$ et p est algébriquement reconstructible, alors $h \circ p$ est algébriquement reconstructible. En effet, les sommes et produits préservent la reconstructibilité algébrique. Il est peu probable que l'on puisse donner une réponse au problème général 16.1.2. En particulier nous n'avons pas de contre-exemple, puisque nous conjecturons que tous les polynômes invariants sont algébriquement reconstructibles. Dans la suite nous obtiendrons des réponses dans quelques cas particuliers, par exemple lorsque h est de la forme $p \mapsto \frac{p}{q}$, où q est un polynôme algébriquement reconstructible vérifiant certaines hypothèses.

Un cas particulier de ce problème concerne la préservation de la reconstructibilité algébrique lorsque l'on prend la racine énième d'un polynôme.

Problème 16.1.3.
Soit p un polynôme invariant tel que p^n soit reconstructible (resp. algébriquement reconstructible). Est-ce que p est reconstructible (resp. algébriquement reconstructible) ?

16.2 Substitution

Nous allons maintenant regarder l'opération duale, qui consiste à composer à droite. Il faut prendre quelques précautions pour que l'opération commute avec l'action du groupe, de façon à préserver l'invariance. Nous allons ici nous contenter des opérations qui consistent à prendre un graphe $\mathbf{g}$, et à le transformer en appliquant une fonction h sur la valuation de chaque arête de $\mathbf{g}$.

Reconstructibilité

Soit f une fonction reconstructible. Soit h une fonction de $\mathbb{K}$ dans $\mathbb{K}$. Enfin, soit $\overline{h}$ la fonction obtenue en appliquant h sur chaque arête :

$$\overline{h}\left(\sum \lambda_{\{i,j\}}\mathbf{e}_{\{i,j\}}\right) = \sum h(\lambda_{\{i,j\}})\mathbf{e}_{\{i,j\}} \tag{16.1}$$

On considère la fonction $f \circ \overline{h}$, qui est naturellement invariante. Si f est un polynôme, cela revient à substituer $\mathbf{x}_{\{i,j\}}$ par $h(\mathbf{x}_{\{i,j\}})$. On remarque que $f \circ \overline{h}$ est reconstructible. Supposons en effet que $\mathbf{g}$ et $\mathbf{g}'$ ont même jeu. Les graphes $\overline{h}(\mathbf{g})$ et $\overline{h}(\mathbf{g}')$ ont alors aussi même jeu et alors

$$(f \circ \overline{h})(\mathbf{g}) = f(\overline{h}(\mathbf{g})) = f(\overline{h}(\mathbf{g}') = (f \circ \overline{h})(\mathbf{g}').$$

En particulier, la reconstructibilité est préservée lorsque l'on substitue $x_{\{i,j\}}$ par $f(x_{\{i,j\}})$ dans un polynôme invariant.

Reconstructibilité algébrique

Nous allons vérifier que la reconstructibilité algébrique est aussi préservée. Bien entendu, nous voulons rester dans l'algèbre des polynômes invariants et nous ne considérerons que des substitutions algébriques, c'est-à-dire telles que h est un polynôme de $\mathbb{K}[x]$.

Proposition 16.2.1.
Soit p un polynôme invariant algébriquement reconstructible. Soit h un polynôme de $\mathbb{K}[x]$, et soit $\overline{h}$ définie comme ci-dessus. Le polynôme $p \circ \overline{h}$ est algébriquement reconstructible.

Démonstration. Par définition, p s'écrit sous la forme

$$p = P(q_1, \ldots, q_k)$$

où P est un polynôme et les q_i sont des multigraphes avec des sommets isolés. Soit m un monôme apparaissant dans q_1, et soit v un sommet isolé de m. Substituons dans m chaque $x_{\{i,j\}}$ par $h(x_{\{i,j\}})$. En développant, on obtient une somme de monômes dans lesquels v est encore isolé. Donc $q_1 \circ \overline{h}$ est une somme de multigraphes avec des sommets isolés. Il en est de même pour les autres q_i. Comme

$$p \circ \overline{h} = P(q_1 \circ \overline{h}, \ldots, q_k \circ \overline{h}),$$

le polynôme $p \circ \overline{h}$ est algébriquement reconstructible. □

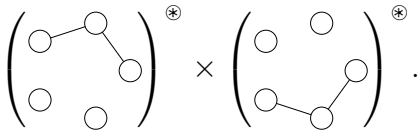
Généralisations

On peut essayer de généraliser ceci à des substitutions où h n'est pas un polynôme, mais telles que $p \circ \overline{h}$ soit un polynôme. Ce n'est possible que si l'on peut montrer que chaque $q_i \circ \overline{h}$ est un polynôme. Nous utiliserons cette idée pour le passage au complémentaire.

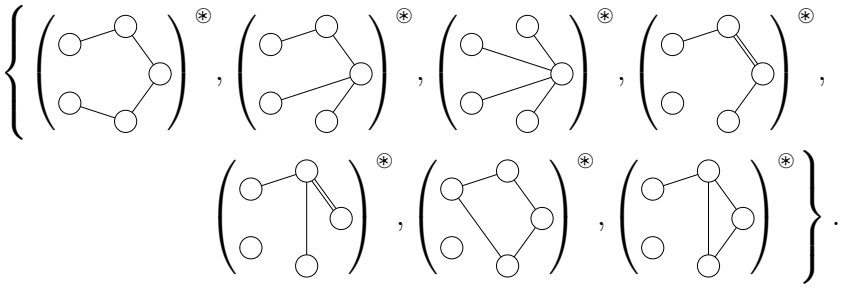
16.3 i-reconstructibilité

Motivations

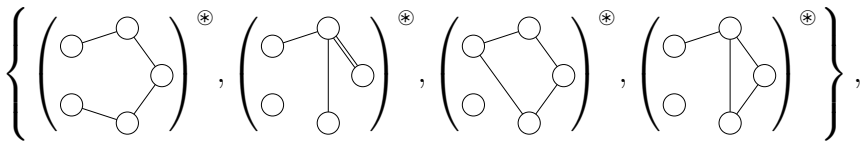
Nous allons maintenant introduire une notion qui permet de montrer que certains polynômes sont algébriquement reconstructibles. L'objectif est le suivant. Lorsque l'on fait le produit de deux multigraphes, on obtient toutes les superpositions possibles de ces deux multigraphes. Dans certains cas, on voudrait forcer la superposition de deux sommets précis des multigraphes. Prenons par exemple le produit de deux chemins de longueur deux



On obtient une combinaison linéaire de tous les multigraphes suivants



Si on pouvait forcer les deux chemins à se toucher par une extrémité, on n'obtiendrait plus que les multigraphes



qui, en dehors du premier, ont tous un sommet isolé. On en déduirait que le premier est algébriquement reconstructible. La i-reconstructibilité va permettre cela, en distinguant un sommet particulier, et en considérant des polynômes invariants par permutation des autres sommets.

Définition et propriétés

Définition 16.3.1.
Soit i un sommet. On définit récursivement l'algèbre des polynômes i-reconstructibles comme suit : un polynôme est i-reconstructible *si l'une des conditions suivantes est vérifiée :*

(i) p est invariant et algébriquement reconstructible ;

(ii) i est un sommet isolé de p ;

(iii) p est une combinaison algébrique de polynômes i-reconstructibles.

On dit alors qu'un multigraphe $\mathbf{g}$ pointé en i est i-reconstructible *si le polynôme $\mathbf{x}^{\mathbf{g}}{}_i^{\circledast}$ obtenu en symétrisant $\mathbf{x}^{\mathbf{g}}$ par permutation des sommets différents de i est i-reconstructible.*

Cette définition permet une généralisation du corollaire suivant du lemme de Kelly.

Proposition 16.3.2 ([Kel57], [Bon91, Corollaire 2.5]).
Soit $\mathbf{g}$ un graphe simple sur n sommets et $\mathbf{f}$ un graphe simple sur moins de $n-1$ sommets. Le nombre de sous-graphes de $\mathbf{g}$ isomorphes à $\mathbf{f}$ et passant par un sommet donné i est reconstructible.

On a en effet les deux lemmes suivants :

Lemme 16.3.3.
Soit $\mathbf{f}$ un multigraphe avec au moins un sommet isolé. Soit p la somme des $\mathbf{x}^{\mathbf{f}'\circledast}$, où $\mathbf{f}'$ est isomorphe à $\mathbf{f}$ et i n'est pas un sommet isolé de $\mathbf{f}'$. Le polynôme p est i-reconstructible.

Démonstration. Comme dans la démonstration de la proposition originale 16.3.2, il suffit de constater que $p = \mathbf{x}^{\mathbf{f}'} - q$, où q est la somme des $\mathbf{x}^{\mathbf{f}'\circledast}$, avec $\mathbf{f}'$ isomorphe à $\mathbf{f}$ et i sommet isolé de $\mathbf{f}'$. Comme $\mathbf{f}$ a un sommet isolé, $\mathbf{x}^{\mathbf{f}'}$ est algébriquement et donc i-reconstructible. Enfin, q est i-reconstructible et donc p aussi. □

Lemme 16.3.4.
Soit p un polynôme i-reconstructible et invariant par permutation des sommets différents de i. La quantité $p(\mathbf{g})$ où $\mathbf{g}$ est un graphe quelconque est reconstructible.

Démonstration. Il suffit de le montrer dans les deux premiers cas de la définition 16.3.1.

- Cas (i). Le sommet i est un sommet isolé de p. On peut appliquer p sur la carte $\mathbf{g}_{\setminus i}$. En effet, p est invariant par permutation des sommets de i, et ne dépend donc pas de l'étiquetage de $\mathbf{g}_{\setminus i}$.
- Cas (ii). Le polynôme p est algébriquement reconstructible, et donc reconstructible.

□

Le principal intérêt de la i-reconstructibilité vient de la proposition suivante.

Proposition 16.3.5.
Soit p un polynôme i-reconstructible. Le polynôme invariant p^* obtenu en appliquant l'opérateur de Reynolds est algébriquement reconstructible.

Démonstration. Par linéarité, on peut se ramener au cas où p est de la forme

$$p = q_1 \dots q_k r_1 \dots r_l$$

avec les q_j vérifiant la condition (i) et les r_j vérifiant la condition (ii). Soit $q = q_1 \dots q_k$ et $r = r_1 \dots r_k$. On constate que q est invariant et algébriquement reconstructible. En utilisant les propriétés de l'opérateur de Reynolds 8.1.5, on a alors :

$$p^* = (qr)^* = qr^*$$

Il ne reste donc plus qu'à montrer que le polynôme invariant r^* est algébriquement reconstructible. Comme les r_j vérifient la condition (ii), le sommet i est aussi isolé dans r. Donc tous les monômes apparaissant dans r^* ont un sommet isolé, ce qui suffit. □

Applications aux polynômes symétriques en les étoiles

Voyons maintenant comment cette notion peut être utilisée. On rappelle que les polynômes symétriques en les étoiles sont les polynômes symétriques en les variables E_i où $E_i = \sum_j x_{\{i,j\}}$. (Pour alléger, nous omettons l'ensemble $\{1 \dots n\} \setminus \{i\}$ sur lequel la somme porte).

Proposition 16.3.6.
Les polynômes symétriques en les étoiles sont algébriquement reconstructibles.

Démonstration. Soit i un sommet quelconque. D'après le lemme 16.3.3 E_i est i-reconstructible car E_i est la somme des arêtes adjacentes à i. On en déduit que les puissances E_i^k de E_i sont aussi i-reconstructibles. Or, à un coefficient $(n-1)!$ près, $(E_i^k)^*$ n'est autre que la k-ième fonction symétrique puissance en les étoiles. Cette dernière est donc algébriquement reconstructible. On conclut alors en appliquant le théorème fondamental des fonctions symétriques (théorème 8.2.4), qui indique que les polynômes symétriques sont engendrés par les fonctions puissances. □

Variations

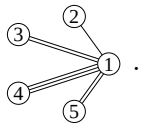
Le lemme suivant servira plus loin pour le passage au complémentaire.

Lemme 16.3.7.
Soit i un sommet fixé. On considère les $n-1$ variables $\{x_{\{i,j\}} \mid j \neq i\}$. Les polynômes symétriques en ces variables sont i-reconstructibles. En particulier, $\prod_j x_{\{i,j\}}$ est i-reconstructible.

Démonstration. Soit $s_k = \sum_j x_{\{i,j\}}^k$ la k-ième fonction symétrique puissance en les $x_{\{i,j\}}$. D'après le lemme 16.3.3, le polynôme s_k est i-reconstructible. En effet, chaque arête multiple $k.\mathbf{e}_{\{i,j\}}$ a un sommet isolé, et s_k est la somme de ces arêtes passant par i. On conclut en utilisant le théorème fondamental des fonctions symétriques (théorème 8.2.4), qui assure que les s_k engendrent tous les polynômes symétriques. □

On note que l'on peut déduire de ce lemme une généralisation du théorème 16.3.6.

Corollaire 16.3.8.
Soit $\mathbf{m}$ un multigraphe dont toutes les arêtes sont adjacentes en un même sommet, comme par exemple



Alors, le multigraphe $\mathbf{m}$ est algébriquement reconstructible.

Démonstration. Soit i le sommet commun à toutes les arêtes du multigraphe $\mathbf{m}$ et $\mathbf{x}^{\mathbf{m}}$ l'exponentielle de $\mathbf{m}$. Soit $p_i := \sum_\sigma \sigma \mathbf{x}^{\mathbf{m}}$ le polynôme obtenu en symétrisant $\mathbf{x}^{\mathbf{m}}$ par toutes les permutations σ de $\{1, \ldots, i-1, i+1, \ldots, n\}$. Ce polynôme p_i est un polynôme symétrique en les variables $\{x_{\{i,j\}} \mid j \neq i\}$ et est donc i-reconstructible. On en déduit d'après le lemme 16.3.7 que le polynôme invariant $p := p_i^*$ obtenu en appliquant l'opérateur de Reynolds est algébriquement reconstructible. Or, à un scalaire près, ce polynôme p n'est autre que l'exponentielle symétrisée $\mathbf{x}^{\mathbf{m}^\circledast}$ de $\mathbf{m}$. On en déduit que ce dernier est algébriquement reconstructible. □

16.4 Opérateur Div

Au § 2.2.5 nous avons introduit l'opérateur Div sur les polynômes, défini par $\mathrm{Div} := \sum \frac{\partial}{\partial x_i}$, et nous avons observé qu'il s'agissait d'une dérivation. Lorsqu'il n'y a pas d'ambiguïté, on note

$$p' := \mathrm{Div}(p), \qquad p^{(k)} := \mathrm{Div}^k(p).$$

Nous montrons que cet opérateur préserve la reconstructibilité algébrique. Nous utiliserons ce fait pour en quelque sorte intégrer par parties les polynômes algébriquement reconstructibles. Cela nous servira, par exemple, pour les fractions et le passage au complémentaire.

Proposition 16.4.1.
Soit p un polynôme algébriquement reconstructible. Le polynôme p' est aussi algébriquement reconstructible.

Démonstration. On dit qu'un monôme q a un sommet i isolé si le multigraphe correspondant a un sommet isolé. Cela revient à dire qu'aucune des variables $x_{\{i,j\}}$ n'apparaît dans q. Soit p un polynôme invariant associé à un multigraphe avec un sommet isolé. Nous allons montrer que p' est algébriquement reconstructible. Soit q un monôme de p, et soit i un sommet isolé de q. Le sommet i est aussi isolé dans tous les monômes apparaissant dans q'. On en déduit que p' est une somme de monômes avec des sommets isolés et qu'il est donc algébriquement reconstructible.

Soit maintenant $p := P(q_1, \ldots, q_k)$ un polynôme algébriquement reconstructible, où chaque q_i est le polynôme invariant associé à un multigraphe avec un sommet isolé. Prenons par exemple $p = q_1 q_2$. En appliquant la formule de dérivation de la proposition 2.2.11, on obtient

$$p' = (q_1 q_2)' = q_1' q_2 + q_1 q_2'.$$

Les polynômes q_1, q_1', q_2 et q_2' sont algébriquement reconstructibles, et donc p' est algébriquement reconstructible. Le cas général se traite de même en appliquant la formule de dérivation à chaque terme $q_1^{d_1} \ldots q_k^{d_k}$ de $p' = (P(q_1, \ldots, q_k))'$ (Les termes obtenus sont de la forme $q_1^{d_1} \ldots q_{i-1}^{d_{i-1}} q_i' q_i^{d_i - 1} q_{i+1}^{d_{i+1}} \ldots q_k^{d_k}$). □

On note qu'il est fastidieux de montrer que cet opérateur préserve la reconstructibilité fonctionnelle, car il faut *a priori* utiliser des propriétés topologiques du corps. On constate qu'avec un changement de variable adéquat, Div s'exprime sous la forme $\frac{\partial}{\partial y}$, où $y := \sum x_{\{i,j\}}$. On peut alors procéder en écrivant les deux graphes $\mathbf{g}$ et $\mathbf{g}'$ ayant même jeu comme limite des graphes $\mathbf{g} + \frac{1}{n}\mathbf{c}$ et $\mathbf{g} + \frac{1}{n}\mathbf{c}$, où $\mathbf{c}$ est le graphe complet. Ces graphes ont encore même jeu. On conclut alors en exprimant $\operatorname{Div} p(\mathbf{g})$ comme limite de $p(\mathbf{g} + \frac{1}{n}\mathbf{c}) - p(\mathbf{g})$.

Application

On rappelle que $\beta(n)$ est le plus haut degré $\beta(n)$ dans un système générateur minimal, et que l'on a des bornes sur $\beta(n)$. Par exemple, on sait que $\beta(n) \leq \mathrm{C}^2_{\mathrm{C}^2_n}$, et il est très probable que l'on puisse réduire cette borne (voir § 11.3.1).

Théorème 16.4.2.
Pour $d \geq \beta(n)$, si tous les polynômes invariants homogènes de degré d sont algébriquement reconstructibles, alors tous les polynômes invariants sont algébriquement reconstructibles.

Démonstration. Supposons que tous les polynômes homogènes de degré d sont algébriquement reconstructibles. La dérivation préserve la reconstructibilité algébrique et, vue comme application de $\mathbb{K}[\mathbf{x}_{\{i,j\}}]_d^{\mathfrak{S}_n}$ dans $\mathbb{K}[\mathbf{x}_{\{i,j\}}]_{d-1}^{\mathfrak{S}_n}$, est surjective (théorème 2.2.14). On en déduit que tous les polynômes de degré $\leq d$ sont reconstructibles. Comme l'algèbre des invariants est engendrée par les polynômes de degré $\leq \beta(n)$, tous les polynômes invariants sont algébriquement reconstructibles. □

16.5 Fractions

Nous allons montrer que, sous certaines conditions, la reconstructibilité algébrique est préservée par fraction. La discussion du § 9.4 à propos du corps des fractions invariantes indique que ce n'est pas toujours le cas, ce qui justifie l'existence de conditions. De plus, l'énoncé équivalent pour la reconstructibilité fonctionnelle des polynômes (toujours sans conditions), entraînerait immédiatement la conjecture de Ulam.

Proposition 16.5.1.
Soit r un polynôme invariant. On suppose que

(i) r est le quotient $\frac{p}{q}$ de deux polynômes invariants p et q algébriquement reconstructibles.

(ii) La constante $q^{(\deg q)}$ est non nulle.

Alors, r est algébriquement reconstructible.

La condition (ii) est en particulier vérifiée si q est à coefficients réels strictement positifs, par exemple pour un multigraphe.

Démonstration. Le principe de la démonstration va être d'utiliser la formule de dérivation de la proposition 2.2.11 pour faire une intégration par parties. On remarque d'abord que si r vérifie les conditions de l'énoncé, alors r' aussi. En effet, $p' = (qr)' = q'r + r'q$ et on a donc la formule usuelle de la dérivée d'un quotient

$$r' = \frac{p'q - q'p}{q^2};$$

grâce à la proposition 16.4.1, les polynômes $p'q - q'p$ et q^2 sont algébriquement reconstructibles. De plus, q^2 vérifie la condition (ii) (lemme 2.2.13).

Procédons par récurrence sur le degré de r. On suppose que tout polynôme de degré $\leq d$ dans les conditions de l'énoncé est algébriquement reconstructible. Comme les constantes sont algébriquement reconstructibles, l'hypothèse de récurrence est vérifiée pour $d = 0$.

Soit $r = \frac{p}{q}$ de degré $d + 1$ dans les conditions de l'énoncé. En appliquant la formule de Leibniz 2.2, on obtient

$$(qr)^{(\deg(q))} = \sum_{k=0}^{\deg(q)} \mathrm{C}^k_{\deg(q)}\, q^{(\deg(q)-k)} r^{(k)},$$

d'où l'on déduit

$$q^{(\deg(q))} r = p^{(\deg(q))} - \deg(q) q^{(\deg(q)-1)} r' - \cdots - \mathrm{C}^k_{\deg(q)}\, q^{(\deg(q)-k)} r^{(k)} - \cdots - q r^{(\deg(q))}.$$

Par récurrence, tous les termes de droite sont algébriquement reconstructibles. Comme $q^{(\deg(q))}$ est une constante non nulle, r est algébriquement reconstructible.

Pour conclure, il faut vérifier que la condition (ii') est plus forte que la condition (ii). Soit q un polynôme à coefficients strictement positifs. Le polynôme $p = q^{2^k}$ est aussi à coefficients strictement positifs. Soit d le degré de p. Lorsque l'on dérive d fois p, on obtient la constante $d!$ multipliée par la somme des coefficients des termes de plus haut degré de p. Ces derniers étant strictement positifs, $p^{(d)}$ est une constante non nulle, comme voulu. □

Corollaire 16.5.2.
Soient p et q deux polynômes tels que $q = p\prod x_{\{i,j\}}$. Les deux conditions suivantes sont équivalentes :
- *p est algébriquement reconstructible,*
- *q est algébriquement reconstructible.*

Démonstration. Un sens est trivial, puisque les polynômes symétriques sont algébriquement reconstructibles. L'autre sens se déduit de la proposition 16.5.1. On peut donc enlever et rajouter le graphe complet à un multigraphe en préservant sa reconstructibilité algébrique. □

16.6 Passage au complémentaire

Ce que nous venons de voir va nous servir pour le passage au complémentaire. On étend comme suit la définition usuelle de complémentaire d'un graphe simple à un multigraphe.

Définition 16.6.1 (Complémentaire).
Soit $\mathbf{m}$ un multigraphe. Soit k la plus grande valuation de $\mathbf{m}$. On appelle complémentaire de $\mathbf{m}$ *le multigraphe*

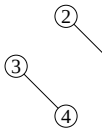
$$\complement\mathbf{m} = k\left(\sum \mathbf{e}_{\{i,j\}}\right) - \mathbf{m}$$

Pour un graphe non nul, cette notion coïncide avec la notion usuelle de complémentaire. En effet, l'opération effectuée revient à retirer les arêtes de $\mathbf{g}$ du graphe complet $\sum \mathbf{e}_{\{i,j\}}$.

Théorème 16.6.2.
Si $\mathbf{m}$ est un multigraphe algébriquement reconstructible, alors, son complémentaire $\complement\mathbf{m}$ de $\mathbf{m}$ est aussi algébriquement reconstructible.

Le point de départ de la démonstration est donné par l'exemple suivant. [1]

Exemple 16.6.3.
Soit $\mathbf{m}$ le graphe sur 4 sommets

$\mathbf{m} =$  $= e_{\{1,2\}} + e_{\{3,4\}}.$

Son exponentielle symétrisée vaut

$$\mathbf{x}^{\mathbf{m}^{\circledast}} = x_{\{1,2\}}x_{\{3,4\}} + x_{\{1,3\}}x_{\{2,4\}} + x_{\{1,4\}}x_{\{2,3\}}.$$

On substitue $x_{\{i,j\}}$ par $\frac{1}{x_{\{i,j\}}}$

$$\mathbf{x}^{\mathbf{m}^{\circledast}} \circ \overline{h} = \frac{1}{x_{\{1,2\}}x_{\{3,4\}}} + \frac{1}{x_{\{1,3\}}x_{\{2,4\}}} + \frac{1}{x_{\{1,4\}}x_{\{2,3\}}}.$$

[1] Nous avons maintenant une démonstration bien plus courte et générale. De plus celle-ci n'utilise pas la notion de i-reconstructibilité (voir [PT00]).

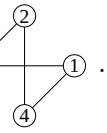
Enfin, on multiplie par

$$\prod x_{\{i,j\}} = x_{\{1,2\}}x_{\{1,3\}}x_{\{1,4\}}x_{\{2,3\}}x_{\{2,4\}}x_{\{3,4\}}$$

et on obtient le polynôme

$$\left(\prod x_{\{i,j\}}\right).\mathbf{x}^{\mathbf{m}^{\circledast}} \circ \overline{h} = x_{\{1,3\}}x_{\{1,4\}}x_{\{2,3\}}x_{\{2,4\}} + x_{\{1,2\}}x_{\{1,4\}}x_{\{2,3\}}x_{\{3,4\}} + x_{\{1,2\}}x_{\{1,3\}}x_{\{2,4\}}x_{\{3,4\}}$$

qui correspond au complémentaire de $\mathbf{m}$ *:*

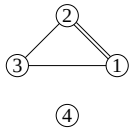
$$^{\complement}\mathbf{m} = $$  .

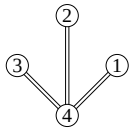
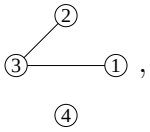
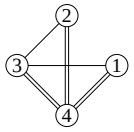
Ceci montre qu'on peut donc obtenir le complémentaire de $\mathbf{m}$ via une substitution bien choisie. Cette substitution n'est pas algébrique, mais nous pourrons tout de même montrer que l'expression finale $\left(\prod x_{\{i,j\}}\right)\mathbf{x}^{\mathbf{m}^{\circledast}} \circ \overline{h}$ est algébriquement reconstructible. Pour cela, nous allons commencer par les multigraphes avec un sommet isolé.

Lemme 16.6.4.
Soit $\mathbf{g}$ *un multigraphe avec un sommet isolé. Son complémentaire* $^{\complement}\mathbf{g}$ *est aussi algébriquement reconstructible.*

Démonstration. Nous allons utiliser la i-reconstructibilité. Soit $\mathbf{g}$ un multigraphe avec un sommet isolé i. Soit k la plus grande valuation de $\mathbf{g}$. Soit $\mathbf{h}$ le complément de $\mathbf{g}$ sur $\{1,\dots,n\}\setminus\{i\}$. Enfin, soit $\mathbf{E}_i = \sum \mathbf{e}_{\{i,j\}}$. On a alors

$$^{\complement}\mathbf{g} = \mathbf{h} + k\mathbf{E}_i$$

Voici ce que cela donne sur l'exemple $\mathbf{g} =$  . On a alors $i = 4$, $k = 2$, et on trouve

$k\mathbf{E}_i =$  , $\mathbf{h} =$  , $^{\complement}\mathbf{g} =$  .

Soient $p = \mathbf{x}^{\mathbf{h}}$ et $q = \mathbf{x}^{\mathbf{E}_i} = \prod_j x_{\{i,j\}}$. On a $\mathbf{x}^{^{\complement}\mathbf{g}} = pq^k$. Puisque par construction $\mathbf{h}$ a un sommet isolé, le polynôme p est i-reconstructible. Le polynôme q l'est aussi, grâce au lemme 16.3.7. Donc $\mathbf{x}^{^{\complement}\mathbf{g}}$ est i-reconstructible. On en déduit (proposition 16.3.5) que $\mathbf{x}^{^{\complement}\mathbf{g}^{*}}$ est algébriquement reconstructible. Les polynômes $\mathbf{x}^{^{\complement}\mathbf{g}^{*}}$ et $\mathbf{x}^{^{\complement}\mathbf{g}^{\circledast}}$ ne diffèrent que par une constante multiplicative, et donc $^{\complement}\mathbf{g}$ est algébriquement reconstructible. □

Avec le corollaire 16.5.2, nous pouvons maintenant traiter les multigraphes sans sommets isolés.

Démonstration de la proposition 16.6.2. Soit $\mathbf{m}$ un multigraphe algébriquement reconstructible et soit k la plus grande valuation de $\mathbf{m}$. Soit $p := \mathbf{x}^{\mathbf{m}^{\circledast}}$ l'exponentielle symétrisée de $\mathbf{m}$. Puisque $\mathbf{m}$ est algébriquement reconstructible, ce polynôme s'écrit $p = P(q_1, \ldots, q_l)$, où chaque q_i est le polynôme invariant associé à un multigraphe avec un sommet isolé. Enfin, soit h définie par $h(x) = \frac{1}{x}$ et $\overline{h}$ définie comme dans l'équation 16.1. On a l'identité

$$\mathbf{x}^{-\mathbf{m}^{\circledast}} = \mathbf{x}^{\mathbf{m}^{\circledast}} \circ \overline{h},$$

d'où l'on déduit que

$$\begin{aligned} \mathbf{x}^{\complement\mathbf{m}^{\circledast}} = \mathbf{x}^{k(\sum \mathbf{e}_{\{i,j\}})-\mathbf{m}^{\circledast}} &= \left(\prod x_{\{i,j\}}\right)^k \left(\mathbf{x}^{\mathbf{m}^{\circledast}} \circ \overline{h}\right) \\ &= \left(\prod x_{\{i,j\}}\right)^k P\left(q_1 \circ \overline{h}, \ldots, q_l \circ \overline{h}\right). \end{aligned} \tag{16.2}$$

Notons que l'on a pu développer $\mathbf{x}^{k(\sum \mathbf{e}_{\{i,j\}})-\mathbf{m}^{\circledast}}$ car l'expression $\mathbf{x}^{k(\sum \mathbf{e}_{\{i,j\}})^{\circledast}}$ ne comporte qu'un seul terme.

Soient $\mathbf{m}_1$ le multigraphe correspondant à q_1 et k_1 la plus grande valuation dans m_1. L'expression $q_1 \circ \overline{h}$ n'est pas directement un polynôme. En revanche, le polynôme

$$\overline{q}_1 = \mathbf{x}^{\complement\mathbf{m}_1{}^{\circledast}} = \left(\prod x_{\{i,j\}}\right)^{k_1} q_1 \circ \overline{h}$$

est algébriquement reconstructible d'après le lemme 16.6.4. On fait de même pour tous les q_i.

Nous affirmons alors que, à condition de choisir k' suffisamment grand, l'expression

$$\left(\prod x_{\{i,j\}}\right)^{k'} P\left(q_1 \circ \overline{h}, \ldots, q_l \circ \overline{h}\right)$$

est un polynôme en les expressions $\overline{q}_1, \ldots \overline{q}_l$ et $\prod x_{\{i,j\}}$. Il suffit pour s'en convaincre de considérer l'exemple suivant. Soit $P(q_1, q_2) = q_1 q_2^2$ et $k' \geq k_1 + 2k_2$. On a

$$\begin{aligned} \left(\prod x_{\{i,j\}}\right)^{k'} P\left(q_1 \circ \overline{h}, q_2 \circ \overline{h}\right) &= \left(\prod x_{\{i,j\}}\right)^{k'} \left(q_1 \circ \overline{h}\right) \left(q_2 \circ \overline{h}\right)^2 \\ &= \left(\prod x_{\{i,j\}}\right)^{k'-k_1-2k_2} \left(\left(\prod x_{\{i,j\}}\right)^{k_1} q_1 \circ \overline{h}\right) \left(\left(\prod x_{\{i,j\}}\right)^{k_2} q_2 \circ \overline{h}\right)^2 \\ &= \left(\prod x_{\{i,j\}}\right)^{k'-k_1-2k_2} \left(\overline{q}_1\right) \left(\overline{q}_2\right)^2. \end{aligned}$$

On en déduit que $\left(\prod x_{\{i,j\}}\right)^{k'} P\left(q_1 \circ \overline{h}, \ldots, q_l \circ \overline{h}\right)$ est algébriquement reconstructible. Cette expression ne diffère que par un facteur $\left(\prod x_{\{i,j\}}\right)^{k'-k}$ de l'expression de $\mathbf{x}^{\complement\mathbf{m}^{\circledast}}$ donnée par l'équation 16.2. On conclut alors que $\complement\mathbf{m}$ est algébriquement reconstructible en utilisant le résultat du corollaire 16.5.2. □

Application aux graphes simples

Dans le cas des graphes simples, on peut combiner les résultats ci-dessus avec ceux du § 6 de la partie I. En effet, la dérivation d'un graphe $\mathbf{g}$ simple est la somme des sous-graphes de $\mathbf{g}$ obtenus en retirant une arête. De même on peut définir l'opérateur Etoile qui à un graphe $\mathbf{g}$ simple associe la somme des graphes obtenus en rajoutant une arête.

Proposition 16.6.5.
Soit $\mathbf{g}$ *un graphe simple avec* d *arêtes. On a*

$$(\mathbf{x}^{\mathbf{g}^{\circledast}})' = \sum_{\mathbf{h}} S(\mathbf{h},\mathbf{g})\mathbf{x}^{\mathbf{h}^{\circledast}} = \sum_{\mathbf{h}} \frac{|\operatorname{Aut}(\mathbf{h})|}{|\operatorname{Aut}(\mathbf{g})|} s(\mathbf{h},\mathbf{g})\mathbf{x}^{\mathbf{h}^{\circledast}},$$

où $\mathbf{h}$ *parcourt les sous-graphes de* $\mathbf{g}$ *à isomorphie près avec* $d-1$ *arêtes.*

Démonstration. On calcule $(\mathbf{x}^{\mathbf{g}^{\circledast}})'$.

$$\begin{aligned}(\mathbf{x}^{\mathbf{g}^{\circledast}})' &= \sum_{\mathbf{g}_1 \approx \mathbf{g}} (\mathbf{x}^{\mathbf{g}_1})' = \sum_{\mathbf{g}_1 \approx \mathbf{g}} \sum_{\mathbf{h}\subset \mathbf{g}_1, |\mathbf{h}|=d-1} \mathbf{x}^{\mathbf{h}} = \sum_{\mathbf{h},|\mathbf{h}|=d-1} |\{\mathbf{g}_1 \,|\, \mathbf{h}\subset \mathbf{g}_1, \mathbf{g}_1 \approx \mathbf{g}\}| \mathbf{x}^{\mathbf{h}} \\ &= \sum_{\mathbf{h},|\mathbf{h}|=d-1} S(\mathbf{h},\mathbf{g})\mathbf{x}^{\mathbf{h}}\end{aligned}$$

On obtient l'expression voulue en ne gardant que les sous-graphes de $\mathbf{g}$ (*i.e.* les graphes $\mathbf{h}$ tels que $S(\mathbf{h},\mathbf{g}) > 0$) et en les regroupant par classes d'isomorphie. On peut alors remplacer $S(\mathbf{h},\mathbf{g})$ par $s(\mathbf{h},\mathbf{g})$ en utilisant la remarque 6.2.1. □

L'énoncé suivant résume les conséquences principales.

Théorème 16.6.6.
(i) Les opérateurs Div *et* Etoile *et* C *préservent la reconstructibilité algébrique.*
(ii) Supposons que les graphes simples à d *arêtes soient tous algébriquement reconstructibles. Si* $d \leq \frac{\mathrm{C}_n^2}{2}$*, alors les graphes simples à* $d-1$ *arêtes sont tous algébriquement reconstructibles. De même, si* $d \geq \frac{\mathrm{C}_n^2}{2}$*, alors les graphes simples à* $d+1$ *arêtes sont tous algébriquement reconstructibles.*
(iii) Si les graphes simples à $\frac{\mathrm{C}_n^2}{2}$ *arêtes sont algébriquement reconstructibles, alors tous les graphes simples sont algébriquement reconstructibles.*

Démonstration. Le (i) se déduit de la proposition 16.4.1 et du théorème 16.6.2 en remarquant que Etoile $= \mathsf{C} \circ \mathrm{Div} \circ \mathsf{C}$. Pour le (ii), on utilise le (i) et la surjectivité de l'opérateur Div des graphes à d arêtes vers ceux à $d-1$ (théorème 6.3.2). Enfin, le (iii) est une conséquence immédiate du (ii). □

Pour $n = 13$, et probablement au delà, on sait qu'il existe des graphes simples à d arêtes non-algébriquement reconstructibles (voir 18.0.1). Ce théorème permet de montrer qu'il en existe pour tout nombre d'arêtes, jusqu'à $\mathrm{C}_n^2 - d$.

Chapitre 17

Étude dans les petits cas de la reconstructibilité algébrique

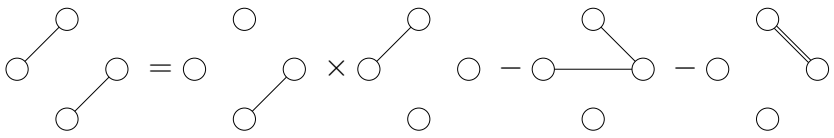
17.1 Vérification à la main de $n = 4$

Théorème 17.1.1.
Sur $n = 4$ sommets, tous les polynômes invariants sont algébriquement reconstructibles.

Ce théorème se déduit du lemme suivant. En effet, le théorème 11.2.3 assure que les graphes simples sur 4 sommets engendrent toute l'algèbre des polynômes invariants.

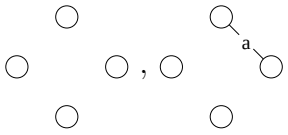
Lemme 17.1.2.
Les graphes simples sur 4 sommets sont algébriquement reconstructibles.

Démonstration. Nous identifions ici complètement un multigraphe avec le polynôme invariant associé. Par exemple, l'équation suivante indique comment on peut exprimer le graphe simple **g** composé de deux arêtes disjointes comme le produit du graphe composé d'une arête avec lui-même, auquel on retire deux multigraphes avec un sommet isolé. On en déduit que le graphe **g** est algébriquement reconstructible.

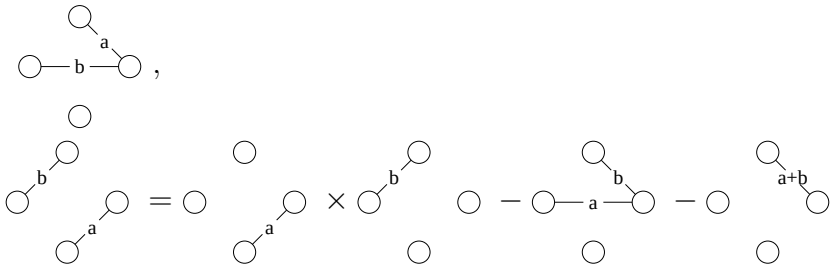


Nous allons montrer de même, à tour de rôle, que tous les graphes simples s'expriment comme sommes et produits de multigraphes ayant un sommet isolé. On note qu'il est nécessaire, comme résultat intermédiaire, de montrer que certains multigraphes sans sommets isolés sont algébriquement reconstructibles.

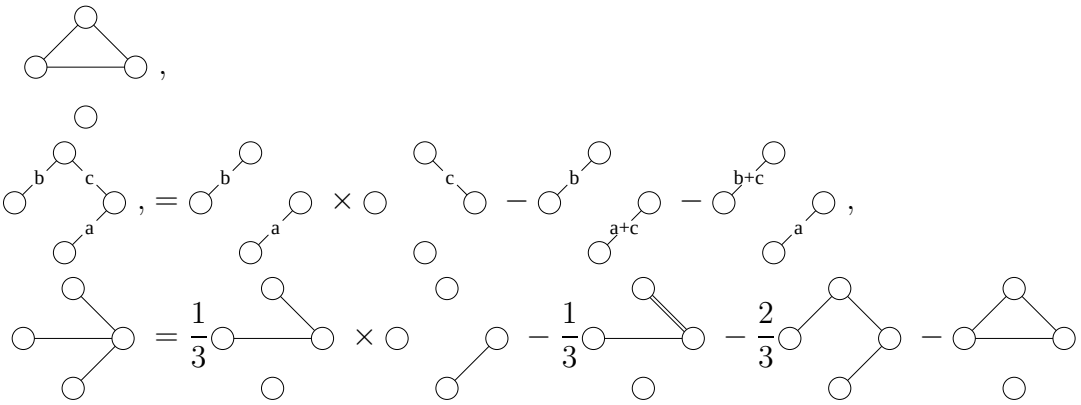
Graphes simples à 0 et 1 arête :



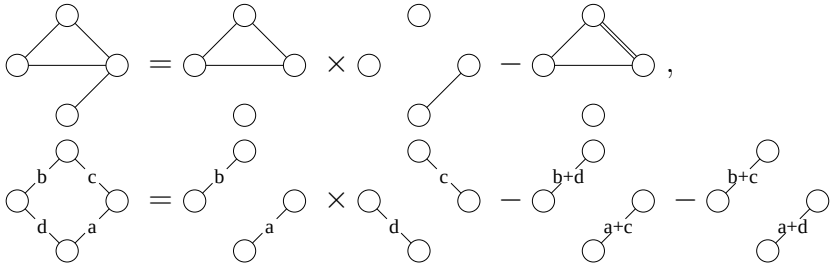
Graphes simples à 2 arêtes :



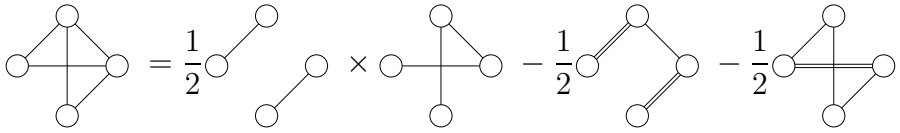
Graphes simples à 3 arêtes :



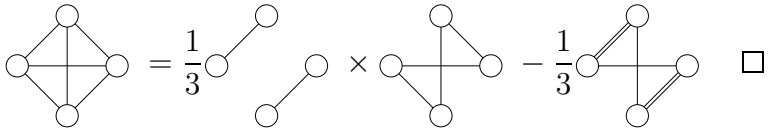
Graphes simples à 4 arêtes :



Graphe simple à 5 arêtes :



Graphe simple à 6 arêtes :



□

17.2 Vérification informatique

Il est possible, dans les petits cas, de tester informatiquement la reconstructibilité algébrique des polynômes invariants en utilisant les algorithmes de construction de système générateurs minimaux de l'algèbre des invariants. Notons cependant que le principe de ces algorithmes est de construire, degré par degré, depuis 0 jusqu'à une borne théorique $\beta(n)$, un système générateur minimal en n'utilisant que des multigraphes avec des sommets isolés. Le calcul devient donc très rapidement difficile du fait de l'explosion combinatoire. Il est bien sûr crucial de réduire le plus possible la borne $\beta(n)$.

Pour $n \leq 4$, le calcul nécessite moins de 5 secondes. Pour $n = 5$, nous avons construit un système générateur partiel jusqu'au degré 10 en n'utilisant que des multigraphes avec des sommets isolés (voir section 11.4.3). Il ne sera probablement pas possible d'aller au delà, sachant que pour l'instant la meilleure borne théorique que nous ayons est $d(5) = 22$. Cependant, la forme du système générateur laisse supposer qu'il est complet, c'est-à-dire que nous ne trouverons pas de générateur de degré plus grand (voir figure A.5 page 265).

Pour $n = 6$, le même calcul a atteint le degré 8. On en déduit en particulier que tous les graphes simples à moins de 8 arêtes sont algébriquement reconstructibles. Comme la reconstruction algébrique est conservée par passage au complémentaire (théorème 16.6.2), ce calcul suffit à montrer que *tous les graphes simples sur* 6 *sommets sont algébriquement reconstructibles* . Pour $n = 7$, le calcul a atteint le degré 7.

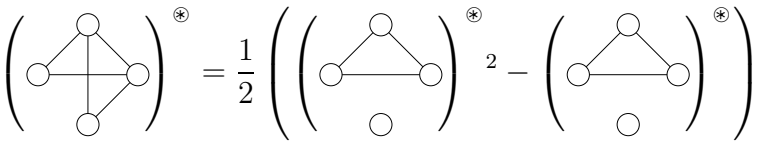
Enfin, nous montrons au § 19 comment nous avons vérifié que les arbres jusqu'à 13 sommets étaient algébriquement reconstructibles.

Chapitre 18

Existence de graphes simples non-algébriquement reconstructibles

Nous allons montrer dans cette section qu'il existe des multigraphes, et plus fortement des graphes simples, qui ne sont pas algébriquement reconstructibles. La démonstration, non-constructive, est basée sur des considérations de dimensions : on utilise la condition nécessaire 11.1.10 sur la série de Hilbert d'une algèbre graduée A pour qu'un système S d'éléments homogènes soit générateur. Le principe est de majorer le nombre d'identités de degré d que l'on peut obtenir par produits d'éléments de S, et de comparer cette majoration avec la dimension de la composante homogène A_d de degré d de A. S'il n'y a pas assez d'identités, le système S ne peut pas être générateur. On rappelle que le même critère nous a, par exemple, permis de montrer que l'algèbre des invariants n'est pas engendrée par les graphes simples (voir § 11.2).

Kocay [Koc82] a utilisé une démarche similaire pour évaluer si les graphes simples étaient algébriquement reconstructibles pour le produit d'union. Dans certains cas, il a constaté qu'il n'y avait pas assez d'identités. Cependant, comme le produit d'union n'est pas gradué, cela ne permet pas de conclure. De fait, il est possible d'obtenir des identités de degré d par combinaison linéaire d'identités d'autres degrés. Ainsi, l'identité suivante n'est pas comptabilisée parmi les identités de degré 5, alors qu'elle permet de montrer que le graphe à 4 sommets et 5 arêtes est algébriquement reconstructible :



La reconstructibilité algébrique des graphes simples pour le produit d'union est donc toujours un problème ouvert.

Théorème 18.0.1.

(i) Il existe des multigraphes sur 11 *sommets et à* 18 *arêtes qui ne sont pas algébriquement reconstructibles.*

(ii) Il existe des graphes simples sur 13 *sommets et à* 17 *arêtes qui ne sont pas algébriquement reconstructibles.*

18.1 Cas des multigraphes

Lemme 18.1.1.
Les multigraphes algébriquement reconstructibles sur n sommets sont engendrés par les multigraphes quasi-connexes dont la composante connexe non triviale est de taille $< n$.

Démonstration. Le principe de la démonstration est exactement le même que pour le théorème 15.1.1 affirmant que les multigraphes non-connexes sont algébriquement reconstructibles. □

Lemme 18.1.2.
Soit $\mathbb{K}[\mathbf{x}_{\{i,j\}}]_d^{\mathfrak{S}_n}$ la composante homogène de degré d de l'algèbre des polynômes invariants sur n sommets. Soit F_n^d le sous-espace vectoriel des polynômes algébriquement reconstructibles de $\mathbb{K}[\mathbf{x}_{\{i,j\}}]_d^{\mathfrak{S}_n}$. Soit $f_{n,d}$ le nombre de multigraphes à d arêtes, sans sommets isolés et dont les composantes connexes sont de taille $< n$.

(i) La dimension de F_n^d est majorée par $f_{n,d}$.

(ii) Le nombre de multigraphes à n sommets et d arêtes algébriquement reconstructibles est majoré par $f_{n,d}$.

(iii) Si $f_{n,d}$ est strictement inférieur au nombre $m_{n,d}$ de multigraphes à n sommets et d arêtes, alors il existe au moins $m_{n,d} - f_{n,d}$ multigraphes sur n sommets à d arêtes non-algébriquement reconstructibles.

Démonstration. D'après le lemme 18.1.1, l'espace F_n^d est dans l'algèbre engendrée par les multigraphes quasi-connexes dont la composante connexe non triviale est de taille $< n$. La condition 11.1.10 permet de majorer la dimension de F_n^d par le nombre de monômes formels de degré total d en ces multigraphes quasi-connexes. On peut associer à chacun de ces monômes $m := \mathbf{x}^{\mathbf{m}_1\circledast} \dots \mathbf{x}^{\mathbf{m}_k\circledast}$ le multigraphe $\mathbf{g}_m$ à d arêtes, sans sommets isolés, union disjointe des composantes connexes non-triviales des multigraphes $\mathbf{m}_i$ apparaissant dans m. Cette correspondance $m \mapsto \mathbf{g}_m$ est clairement bijective, ce qui démontre le (i).

Les polynômes $\mathbf{x}^{\mathbf{m}\circledast}$, associés aux multigraphes à n sommets et d arêtes algébriquement reconstructibles, forment une famille libre de F_n^d. Le nombre de ces multigraphes est donc aussi majoré par $f_{n,d}$. Le (ii) et le (iii) en découlent. □

Démonstration du théorème 18.0.1, (i). Le calcul de la série de Hilbert permet d'évaluer le nombre $m_{n,d}$ de multigraphes à n sommets et d arêtes (voir § 10.3.1). Il reste à évaluer le nombre $f_{n,d}$.

On commence par évaluer le nombre $c_{n',d'}$ de multigraphes connexes à n' sommets et d' arêtes. Pour cela, on suit pas à pas la méthode décrite dans [HP73, § 4.2, p 90] dans le cas des graphes simples. Plus généralement, étant donnée une classe $\mathcal{C}$ d'objets, cette méthode permet de calculer le nombre $g_{n,p}$ de ces objets, comptés selon deux statistiques n et p, à partir des nombres $(g_{n',p'})_{n'\leq n, p'\leq n}$ de multiensembles (*i.e.* ensembles avec répétitions) de ces objets comptés selon les deux mêmes statistiques. Nous avons implémenté cette méthode dans `PerMuVAR`.

Soient $m(x,y) := \sum_{n\geq 1, d\geq 0} m_{n,d} x^n y^d$ et $c(x,y) := \sum_{n\geq 1, d\geq 0} c_{n,d} x^n y^d$ les séries génératrices des multigraphes et des multigraphes connexes non triviaux. On peut considérer un multigraphe quelconque comme un multiensemble de multigraphes

connexes. Ces deux séries génératrices sont donc liées par la relation :

$$1 + m(x, y) = \exp\left(\sum_{k=1}^{\infty} c(x^k, y^k)/k\right).$$

On peut alors inverser cette relation et exprimer les coefficients de la série $c(x, y)$ au moyen de ceux de la série $m(x, y)$, *via* une inversion de Möbius. On rappelle que les coefficients de la série $m(x, y)$ eux-mêmes s'obtiennent via une énumération de Pólya (voir § 10.3.1 ou § 11.2).

Fixons le nombre n de sommets. On note $C_{n,d}$ le nombre de multigraphes connexes à d arêtes et à au plus $n-1$ sommets. Clairement $C_{n,d} := \sum_{n'<n} c_{n',d}$. La série génératrice par nombre d'arêtes des multigraphes sans sommets isolés dont les composantes connexes ont au plus $n-1$ sommets s'écrit alors :

$$\sum_{d=0}^{\infty} f_{n,d} z^d := \prod_{d=1}^{\infty} \frac{1}{(1-z^d)^{C_{n,d}}}$$

Bien entendu, pour calculer, à partir de cette expression, les coefficients $f_{n,d}$ jusqu'à $d := D$ arêtes, on peut restreindre le produit infini de droite au produit fini de $d = 1$ à $d = D$.

La figure 18.1 page 235 présente la courbe du rapport $\frac{f_{n,d}}{m_{n,d}}$ pour différentes valeurs de n. On note que pour $n = 11$, et $d =??$, ce rapport est strictement inférieur à 1, indiquant qu'il existe au moins un multigraphe non algébriquement reconstructible. □

18.2 Cas des graphes simples

Le lemme suivant permet de traiter les graphes simples dans l'algèbre des graphes simples.

Lemme 18.2.1.
Un graphe simple algébriquement reconstructible est aussi algébriquement reconstructible dans l'algèbre des graphes simples.

La démonstration du point (ii) du théorème 18.0.1 est analogue à celle du point (i), et nous nous contentons d'énoncer sans démonstration les lemmes correspondants.

Lemme 18.2.2.
Les graphes simples algébriquement reconstructibles dans l'algèbre des graphes simples sont dans l'algèbre engendrée par les graphes simples quasi-connexes dont la composante connexe non triviale est de taille $< n$.

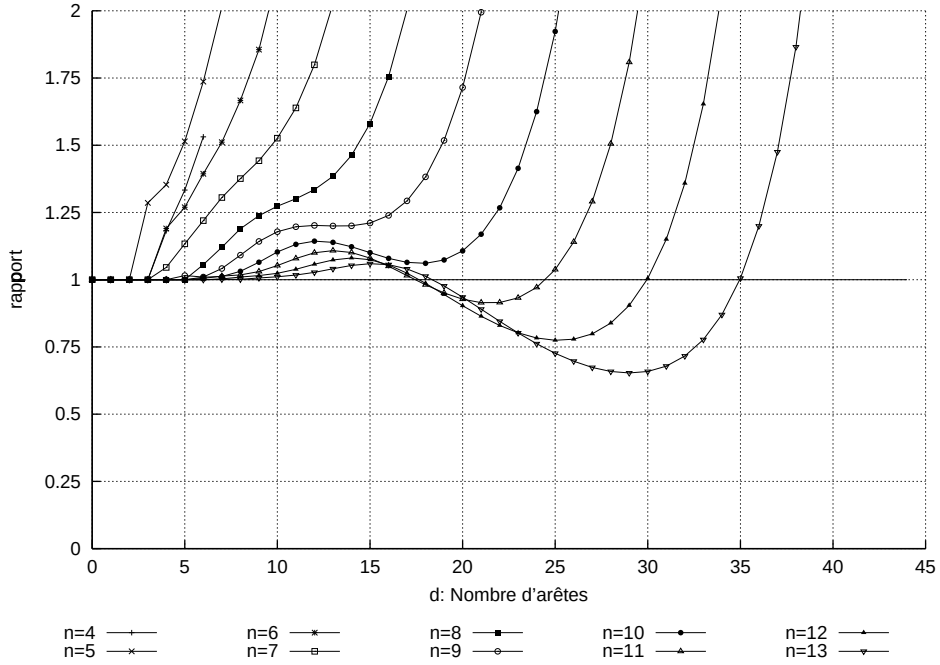
Lemme 18.2.3.
On considère la composante homogène de degré d de l'algèbre des graphes simples sur n sommets. Soit F_n^d le sous-espace des vecteurs algébriquement reconstructibles. Soit $f_{n,d}$ le nombre de graphes simples à d arêtes, sans sommets isolés et dont les composantes connexes sont de taille $< n$.

(i) La dimension de F_n^d est majorée par $f_{n,d}$.
(ii) Le nombre de graphes simples à n sommets et d arêtes algébriquement reconstructibles est majoré par $f_{n,d}$.
(iii) Si $f_{n,d}$ est strictement inférieur au nombre $g_{n,d}$ de graphes simples à n sommets et d arêtes, alors il existe $g_{n,d} - f_{n,d}$ graphes simples sur n sommets à d arêtes non-algébriquement reconstructibles.

La figure 18.4 page 237 présente la courbe du rapport $\frac{f_{n,d}}{g_{n,d}}$ en fonction de d, pour différentes valeurs de n. On note que pour $n = 13$, et $d = 17$, ce rapport est strictement inférieur à 1, indiquant qu'il existe au moins un graphe simple non algébriquement reconstructible. Mc Kay [McK97] ayant vérifié par ordinateur que tous les graphes simples sur 11 sommets sont reconstructibles, nous lui avons demandé s'il pouvait appliquer le même test aux 17422984 graphes simples à 13 sommets et 17 arêtes. Nous avons reçu une réponse positive dans les heures qui suivaient (la performance est impressionnante, et nous le remercions vivement pour ce calcul). Ainsi,

Proposition 18.2.4.
Il existe des graphes simples reconstructibles et non algébriquement reconstructibles.

La figure 18.5 page 238 indique, en fonction de n, la valeur minimale M_n atteinte par le rapport $\frac{f_{n,d}}{g_{n,d}}$ lorsque d varie. Un ajustement rapide avec `gnuplot` semble indiquer que M_n tend rapidement vers 0.04. Cela indique que, lorsque n est grand, il existe un d tel qu'une très faible proportion des graphes simples à n sommets et d arêtes sont algébriquement reconstructibles. Pourrait-on en déduire, par exemple en utilisant la dérivation, que les graphes simples à n sommets sont presque tous non-algébriquement reconstructibles ?



(a) Agrandissement

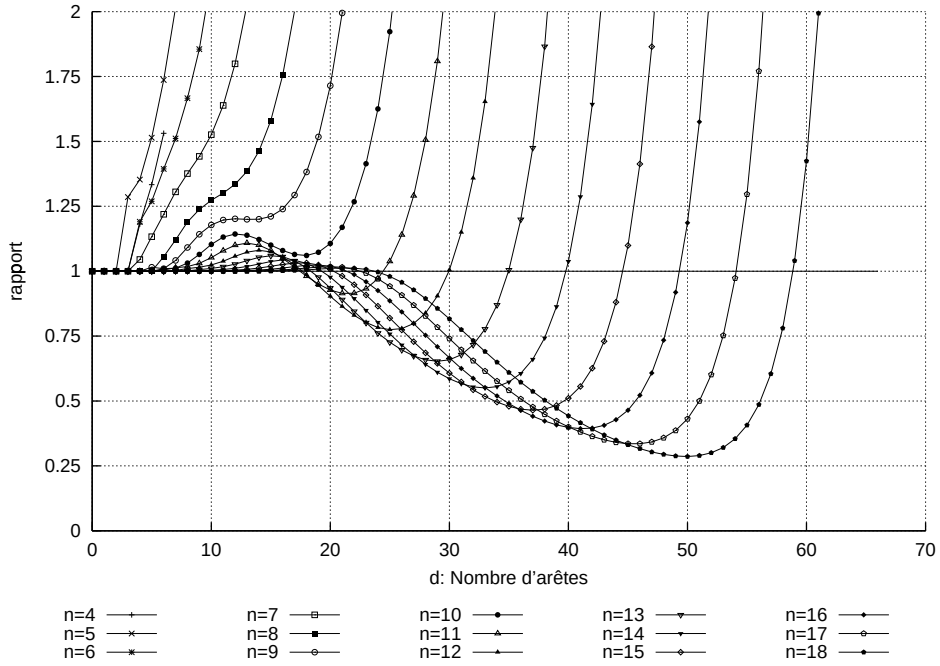


FIG. 18.1 – Majoration de la proportion de multigraphes algébriquement reconstructibles parmi les multigraphes à n sommets et d arêtes
C'est le rapport $\frac{f_{n,d}}{m_{n,d}}$ entre le nombre de multigraphes, à d arêtes, sans sommets isolés et dont les composantes connexes sont de taille $< n$ et le nombre de multigraphes à n sommets et d arêtes

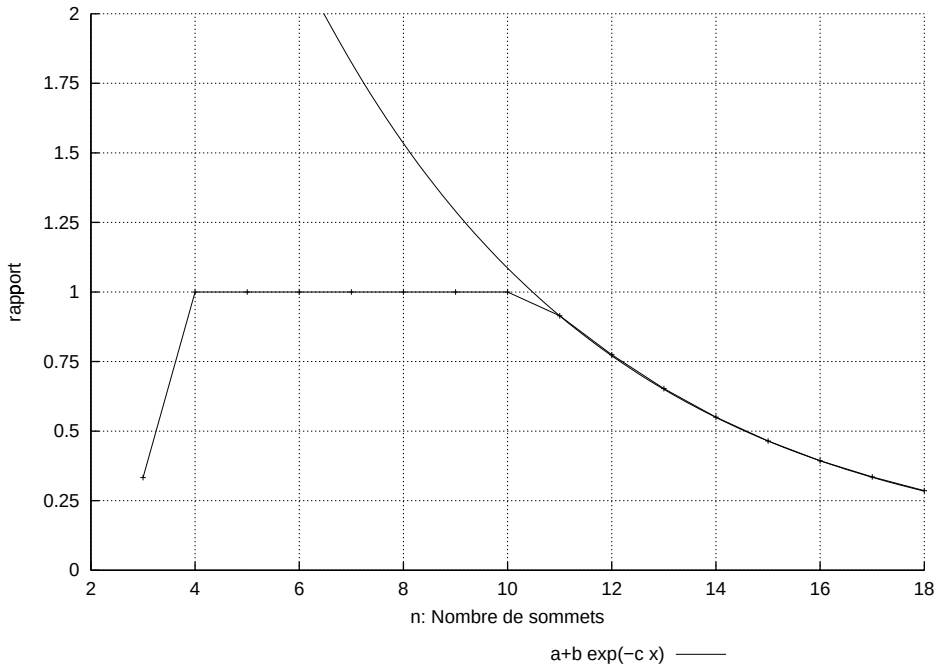


FIG. 18.2 – Minimum, lorsque d varie, du rapport $\frac{f_{n,d}}{m_{n,d}}$, en fonction de n

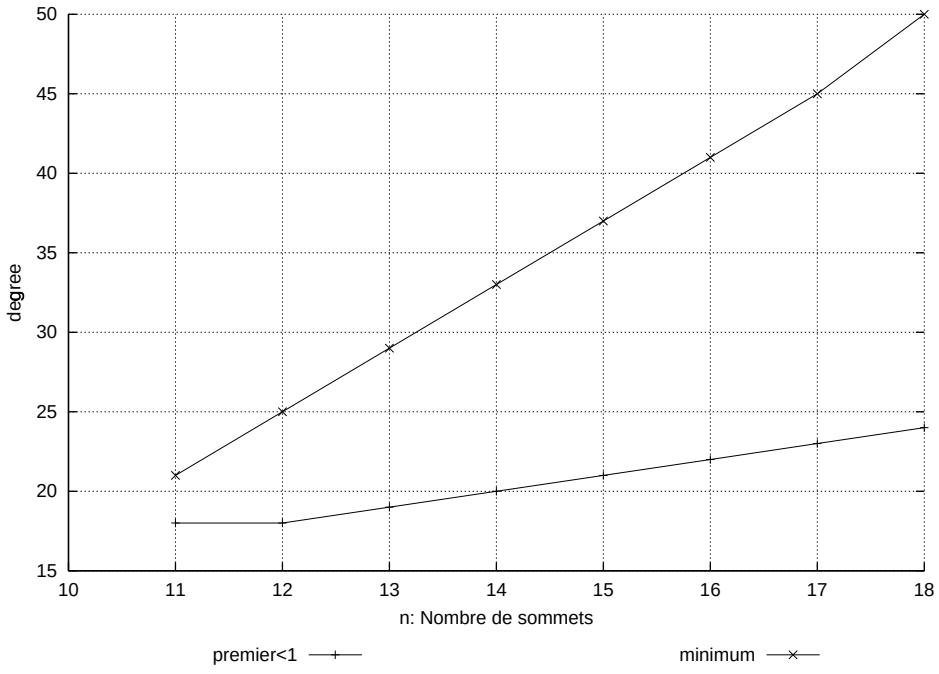
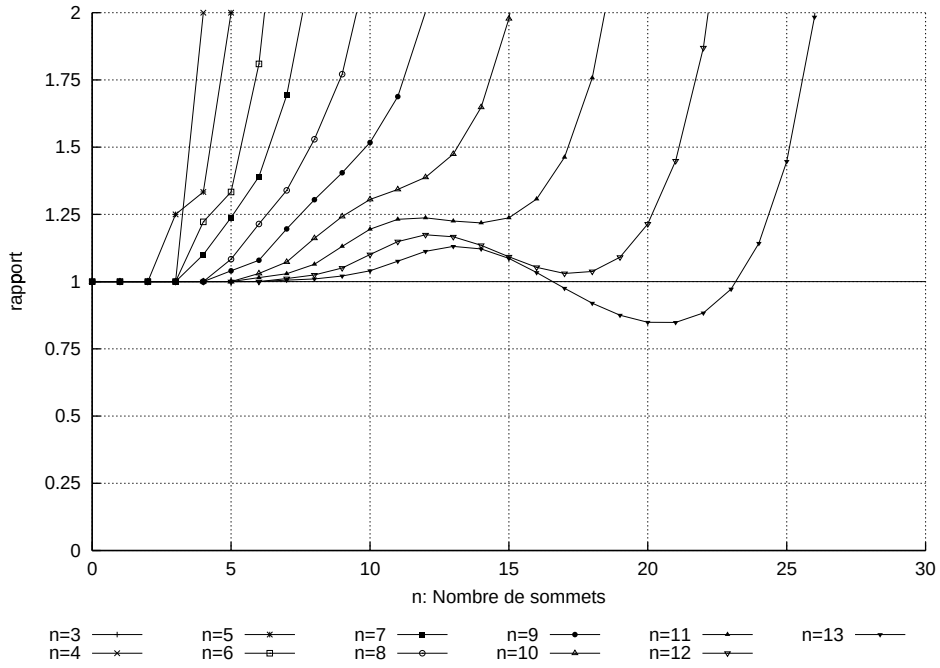


FIG. 18.3 – Degré d minimal tel que le rapport $\frac{f_{n,d}}{m_{n,d}}$ est < 1, et degré pour lequel le rapport est minimal, en fonction de n



(a) Agrandissement

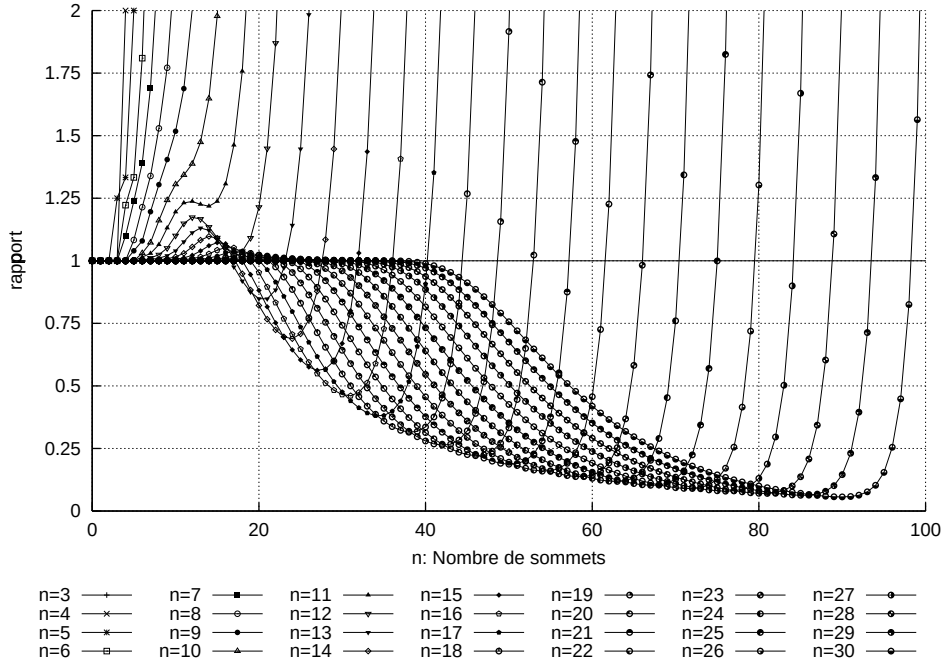


FIG. 18.4 – Majoration de la proportion de graphes algébriquement reconstructibles parmi les graphes simples à n sommets et d arêtes
C'est le rapport $\frac{f_{n,d}}{g_{n,d}}$ entre le nombre de graphes simples, à d arêtes, sans sommets isolés et dont les composantes connexes sont de taille $< n$ et le nombre de graphes simples à n sommets et d arêtes

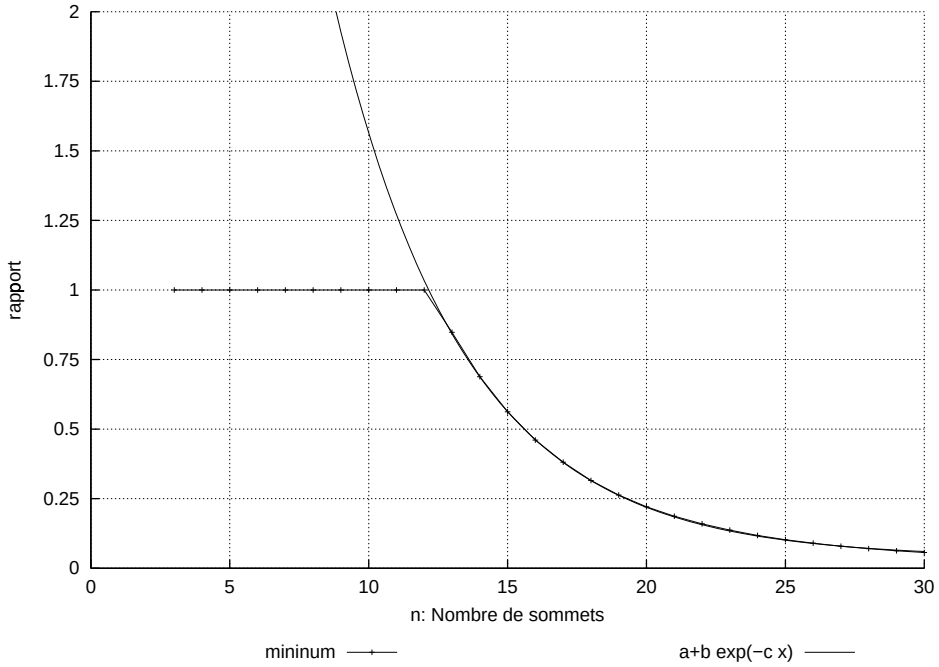


FIG. 18.5 – Minimum, lorsque d varie, du rapport $\frac{f_{n,d}}{g_{n,d}}$, en fonction de n

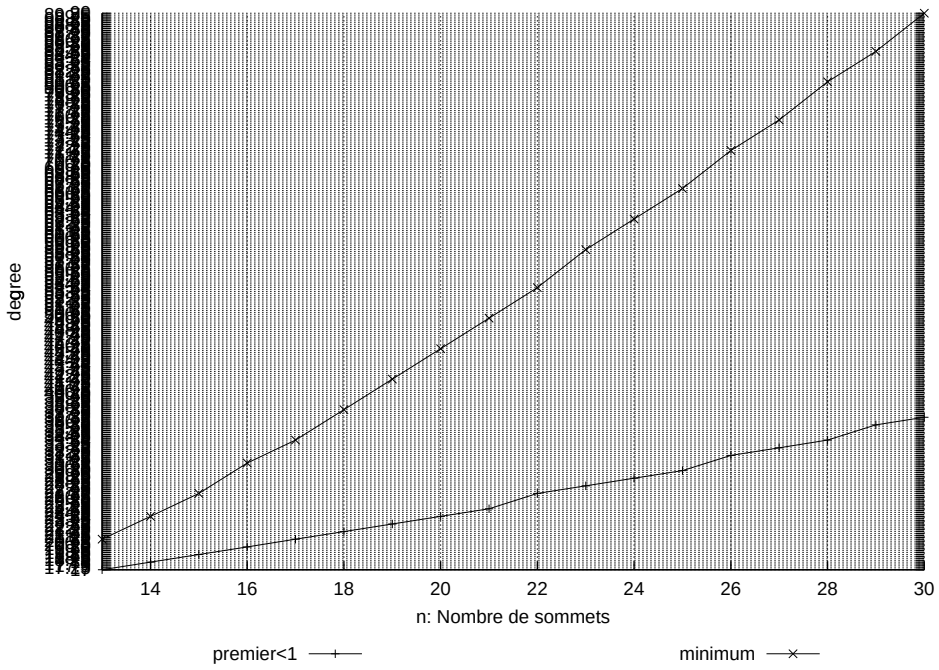


FIG. 18.6 – Degré d minimal tel que le rapport est < 1, et degré pour lequel le rapport est minimal, en fonction de n

Chapitre 19

Reconstruction algébrique des arbres

19.1 Préliminaires

19.1.1 Motivation

Ce chapitre présente différentes approches pour tenter de démontrer l'énoncé suivant.

Conjecture 19.1.1.
Les arbres sont algébriquement reconstructibles.

Nous avons vu que les graphes non-connexes sont algébriquement reconstructibles. Comme les arbres sont les graphes connexes avec le plus petit nombre d'arêtes, il paraît naturel de commencer par eux. Cette idée est renforcée par le théorème 16.6.6 qui indique que si d est petit et les graphes à d arêtes sont reconstructibles, alors les graphes à $d-1$ arêtes sont reconstructibles. Les arbres devraient donc être les graphes simples les moins difficiles à traiter.

Une réponse positive à cette conjecture impliquerait tout d'abord la reconstructibilité des arbres. Cependant, ce résultat est connu depuis fort longtemps ([Kel57]). Plus intéressant, cela résoudrait un problème soulevé par Kocay en 1982 et qui, lui, n'est toujours pas résolu. On rappelle que le nombre total d'arbres couvrants est reconstructible (proposition 15.1.2). Il s'agit ici de raffiner ce dénombrement.

Problème 19.1.2 ([Koc82], [Bon91]).
Démontrer que le nombre d'arbres couvrants de chaque type d'isomorphie est reconstructible.

Nous avons vu au § 15 que les démonstrations de la plupart des résultats classiques s'exprimaient naturellement en utilisant des polynômes invariants. Ces démonstrations sont en effet essentiellement basées sur des dénombrements. Nous avons donc tenté d'adapter de la sorte les démonstrations de la reconstructibilité des arbres en espérant obtenir au moins un point de départ pour la reconstructibilité algébrique. Il serait effectivement possible de traduire mot à mot la démonstration de [BH77, p. 233], mais le point de vue algébrique ne semble pas permettre de généralisation. Nous avons donc cherché d'autres approches.

Pour le moment, nous avons pu montrer informatiquement que tous les arbres jusqu'à 13 sommets étaient algébriquement reconstructibles. À ce propos, la figure A.8

page 267 donne le nombre d'arbres, de forêts, etc. en fonction du nombre de sommets, ce qui permet d'évaluer la difficulté du problème. Nous avons aussi montré que certaines familles infinies d'arbres (les pieuvres) étaient algébriquement reconstructibles.

19.1.2 Petits cas

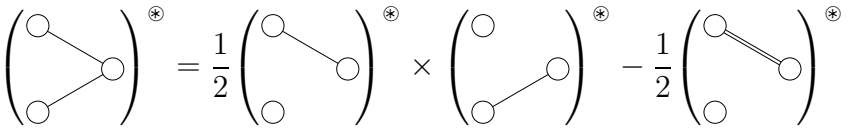
Nous présentons ici quelques petits cas traités à la main. Le principe utilisé est le suivant. On considère deux forêts $\mathbf{f}_1$ et $\mathbf{f}_2$ à respectivement k et $n-1-k$ arêtes. On suppose qu'aucune des deux n'est un arbre (*i.e.* $0 < k < n-1$). Elles sont alors non-connexes et donc algébriquement reconstructibles. Le produit $\mathbf{x}^{\mathbf{f}_1 \circledast}\mathbf{x}^{\mathbf{f}_2 \circledast}$ est aussi algébriquement reconstructible. Parmi les termes qui apparaissent dans ce produit, certains ne sont pas des arbres, car ils ont des cycles ou des arêtes multiples. Nous appelons *cycliques* de tels termes. Il est possible de les éliminer, car ils sont non-connexes, et donc algébriquement reconstructibles. Ainsi, on a construit une combinaison linéaire d'arbres qui est algébriquement reconstructible. Si on arrive à engendrer de cette façon suffisamment d'identités, on peut résoudre le système, et exprimer chaque arbre en fonction d'expressions algébriquement reconstructibles.

On peut exprimer ceci sous forme matricielle. On considère la matrice dont les colonnes sont indexées par les arbres et les lignes sont un certain nombre de combinaisons linéaires d'arbres que l'on aura pu engendrer par produits de forêts. Il faut montrer que la matrice a pour rang son nombre de colonnes. Autrement dit, qu'il y a plus de combinaisons linéaires que d'arbres et que la matrice est de rang plein.

Exemple 19.1.3.
Les arbres sur 3, 4 *et* 5 *sommets sont algébriquement reconstructibles.*

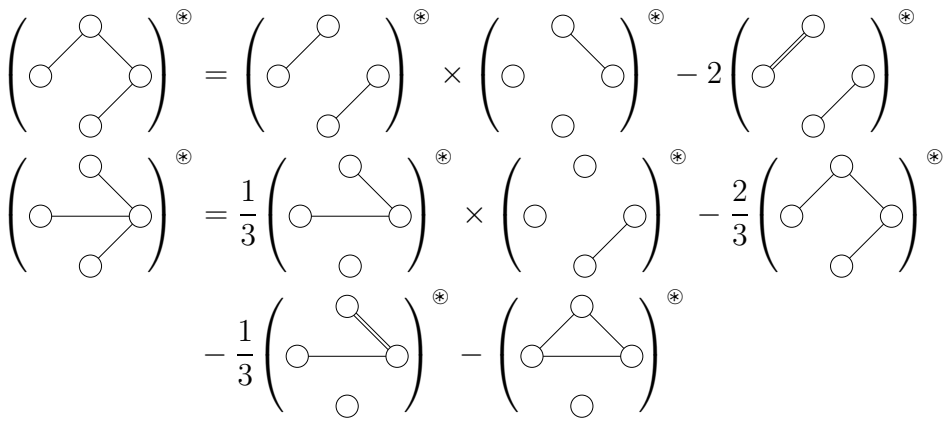
Démonstration. Pour 3 et 4, nous avons montré que tous les graphes simples sont reconstructibles (théorème 17.1.1). Nous allons cependant refaire le calcul car il tient en quelques lignes.

Pour $n = 3$, le seul arbre est le chemin à deux arêtes. On l'exprime à partir du produit de deux arêtes, le terme restant ayant un sommet isolé.

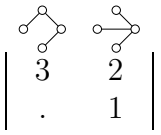


La matrice correspondante est

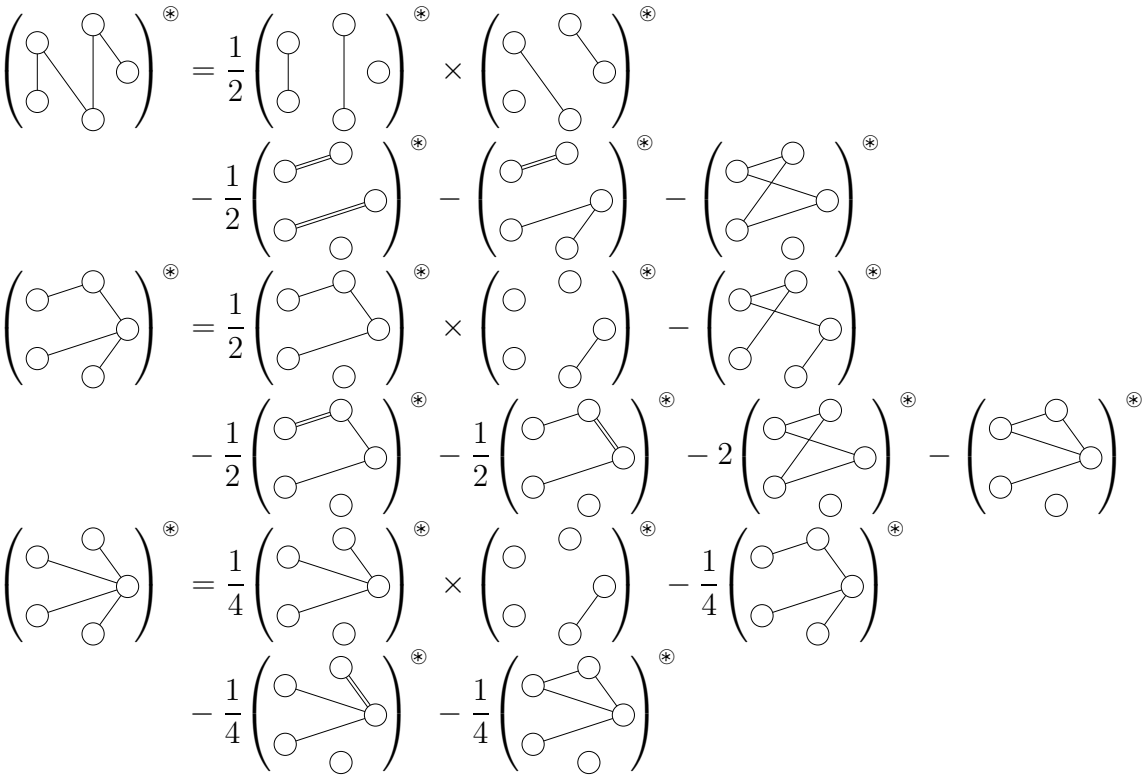
Pour $n = 4$, il y a deux arbres.



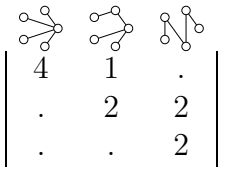
La matrice correspondante est (en remplaçant 0 par . pour plus de lisibilité) :



Pour $n = 5$, il y a 3 arbres.



La matrice correspondante est



□

19.1.3 Algèbre des forêts

Introduction

On peut formaliser la démarche utilisée dans le cadre suivant. On remarque que si un monôme m est cyclique (c'est-à-dire s'il y a un cycle ou une arête multiple) tous les monômes obtenus par produit de m par un autre monôme sont aussi cycliques. De même, si l'on permute les sommets de m, la cyclicité est préservée. L'ensemble des polynômes invariants cycliques est donc un idéal de l'algèbre des polynômes invariants. On considère le quotient de l'algèbre des invariants par cet idéal. Il s'agit d'une algèbre graduée qui, en tant qu'espace vectoriel, est engendrée par les forêts. On l'appelle *algèbre des forêts*. Cette algèbre est définie et étudiée plus précisément au § 12.2.2. Cependant, nous ne savons pas si elle a des propriétés particulières qui permettraient, par exemple, de donner une borne sur les degrés d'un système générateur minimal. Pour le moment, cette construction nous sert essentiellement à éliminer proprement les termes avec des cycles, et à évaluer le nombre d'identités que l'on peut produire.

Application à la reconstructibilité algébrique des arbres

Dans ce cadre, la reconstructibilité algébrique des arbres se ramène à un problème d'algèbre linéaire.

Proposition 19.1.4.
On considère la composante homogène de degré $n-1$ de l'algèbre des forêts, c'est-à-dire l'espace des combinaisons linéaires formelles d'arbres non étiquetés. On le note $\langle arbres \rangle$. Soit $\langle \mathbb{C}[forêts] \rangle$ le sous-espace vectoriel de $\langle arbres \rangle$ engendré par des produits de forêts non-connexes. Soit $\mathbf{g}$ un arbre. Les deux propositions suivantes sont alors équivalentes :

- $\mathbf{g}$ *est algébriquement reconstructible ;*
- $\mathbf{g}$ *est dans le sous-espace vectoriel $\langle \mathbb{C}[forêts] \rangle$.*

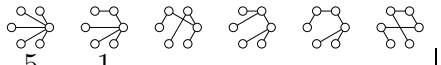
Les arbres sont donc algébriquement reconstructibles si, et seulement si, $\langle \mathbb{C}[forêts] \rangle = \langle arbres \rangle$.

Démonstration. Cela revient à formaliser la démarche utilisée dans les petits cas. Soit ϕ la projection canonique de l'algèbre des invariants dans l'algèbre des forêts. C'est un morphisme d'algèbres. Il faut ici être un peu prudent selon que l'on considère $\mathbf{g}$ comme un graphe non étiqueté, comme un polynôme invariant ou un polynôme de l'algèbre des forêts. On le note $\mathbf{g}$ dans le premier cas et $\phi(\mathbf{g})$ dans le second.

Soit $\mathbf{g}$ un arbre algébriquement reconstructible. En tant que polynôme invariant, $\mathbf{g}$ est de la forme $P(\mathbf{g}_1, \ldots, \mathbf{g}_k)$, où g_1,...,g_k sont des multigraphes avec un sommet isolé :

$$\phi(\mathbf{g}) = \phi(P(\mathbf{g}_1, \ldots, \mathbf{g}_k)) = P(\phi(\mathbf{g}_1), \ldots, \phi(\mathbf{g}_k)).$$

Par définition, si $\mathbf{g}_i$ n'est pas une forêt, $\phi(\mathbf{g}_i) = 0$. De plus $\mathbf{g}_i$ a un sommet isolé et a donc moins de $n-1$ arêtes. Conclusion : dans l'algèbre des forêts, $\mathbf{g}$ est une combinaison algébrique de forêts non-connexes.



5	1	.	.	.	.
.	1	.	.	1	.
.	3	2	4	1	.
.	.	2	.	.	2
.	.	1	.	2	2
.	.	.	1	1	1

FIG. 19.1 – Matrice d'incidence sur 6 sommets des arbres versus les forêts à 4 arêtes

Supposons réciproquement que, dans l'algèbre des forêts, $\phi(\mathbf{g})$ est dans $\langle \mathbb{C}[\text{forêts}] \rangle$. Il est alors de la forme $P(\phi(\mathbf{g}_1), \ldots, \phi(\mathbf{g}_k))$ où $\mathbf{g}_1, \ldots, \mathbf{g}_k$ sont des forêts non connexes. Prenons la même expression dans l'algèbre des invariants : $P(\mathbf{g}_1, \ldots, \mathbf{g}_k)$. Cette expression est algébriquement reconstructible, et on a :

$$\phi(P(\mathbf{g}_1, \ldots, \mathbf{g}_k)) = P(\phi(\mathbf{g}_1), \ldots, \phi(\mathbf{g}_k)) = \phi(\mathbf{g}).$$

Donc $\mathbf{g}$ et $P(\mathbf{g}_1, \ldots, \mathbf{g}_k)$ ne diffèrent que par un polynôme p de degré $n-1$ de l'idéal. Les termes de p ayant soit des cycles, soit des arêtes multiples sont non-connexes. Donc p est algébriquement reconstructible. □

Angle d'attaque

Le principe est maintenant d'engendrer des vecteurs de $\langle \mathbb{C}[\text{forêts}] \rangle$ par produit de forêts non-connexes. Cela donne des identités entre des expressions algébriquement reconstructibles et des combinaisons linéaires d'arbres. Il reste à savoir si l'on peut engendrer suffisamment d'identités pour que le système obtenu soit inversible.

Dans les trois exemples que nous avons vus, nous avons pu ordonner les arbres et construire des identités de façon à obtenir directement un système triangulaire et donc facile à inverser. En revanche, à partir de 6, nous n'avons obtenu que des systèmes non triangulaires comme celui de la figure 19.1. L'inversibilité est alors *a priori* un problème difficile à traiter, à part informatiquement (pivot de Gauss). La section suivante présente une approche possible.

19.2 Utilisation de matrices d'incidence

19.2.1 Introduction

La manière la plus simple d'engendrer une équation consiste à multiplier une forêt $\mathbf{f}$ à $n-2$ arêtes (et donc 2 composantes connexes) par une arête simple. En tant que polynôme, cela revient à multiplier $\mathbf{x}^{\mathbf{f}^{\circledast}}$ par le polynôme e_1 symétrique élémentaire de degré 1. En prenant toutes les identités obtenues de la sorte, on obtient une matrice comme, par exemple, celle de la figure 19.1. Or, d'après la remarque 12.2.12, on peut interpréter cette matrice comme la matrice d'incidence dans le cas non étiqueté des arbres versus les forêts à deux composantes connexes. Le coefficient indexé par l'arbre $\mathbf{g}$ et la forêt $\mathbf{f}$ et $s(\mathbf{f}, \mathbf{g})$. *C'est une sous-matrice de*

la matrice d'incidence des graphes non étiquetés à $n-1$ versus $n-2$ arêtes, qui est de rang plein d'après le théorème 6.3.2. On ne peut pas en déduire immédiatement qu'elle est aussi de rang plein, mais il est probable que l'on puisse appliquer des techniques proches de celles du chapitre 6. Nous avons constaté expérimentalement que cette matrice est de rang plein jusqu'à $n = 13$, c'est-à-dire que les identités sont indépendantes entre elles.

Conjecture 19.2.1.
La matrice d'incidence des arbres (non étiquetés) versus les forêts (non étiquetées) à deux composantes connexes est de rang plein.

Au § 6.5, nous avons essayé d'aborder cette conjecture dans le cas étiqueté.

19.2.2 Vérification informatique

Nous avons pu vérifier informatiquement notre conjecture jusqu'à $n = 13$ (matrice de taille 1302×1121). Cela s'est fait en trois étapes.

1. Génération des arbres non étiquetés sur n sommets ;
2. Génération de la matrice d'incidence ;
3. Calcul du rang de la matrice.

Pour la première étape, nous avons utilisé notre bibliothèque `MathGraph` en `Perl`, qui permet d'engendrer les arbres enracinés non étiquetés, puis les arbres. Il est cependant beaucoup plus rapide d'utiliser le programme `nauty` de McKay [McK90]. Il permet par exemple d'obtenir les arbres sur 14 sommets en moins de 10 secondes.

Génération de la matrice d'incidence

Nous avons en fait engendré la matrice des $S(\mathbf{h}, \mathbf{g})$ au lieu de celle des $s(\mathbf{h}, \mathbf{g})$. Cependant, en utilisant la remarque 6.2.1 on montre que ces deux matrices sont équivalentes par un changement de bases approprié (prendre l'ensemble des $|\operatorname{Aut}(\mathbf{h})|\mathbf{h}$ comme base des forêts et $\frac{\mathbf{g}}{|\operatorname{Aut}(\mathbf{g})|}$ comme base des arbres). Elles sont donc de même rang.

L'algorithme est alors le suivant

Pour $\mathbf{g}$ arbre sur n sommets **Faire**
  Par défaut, $S(\mathbf{h}, \mathbf{g}) := 0$
  Pour $\{i, j\}$ arête $\mathbf{g}$ **Faire**
    $\mathbf{h} := \text{canonic}(\mathbf{g} \setminus \{i, j\})$
    $S(\mathbf{h}, \mathbf{g}) := S(\mathbf{h}, \mathbf{g}) + 1$
  Fin Pour
Fin Pour
Renvoie S

On remarque que la matrice finale est rapidement grande (jusqu'à 3159×2644 pour $n = 14$), mais que chaque colonne ne contient que peu de valeurs non-nulles (moins de $n-1$, puisqu'il y a $n-1$ arêtes dans $\mathbf{g}$). Il est très avantageux de stocker la matrice sous forme de matrice creuse.

Calcul du rang

Pour calculer le rang, nous avons essayé divers systèmes de calcul formel. Le problème est assez coûteux du fait de la taille de la matrice. Au delà de $n = 10$, les systèmes ne gérant pas les matrices creuses (dont `MuPAD` pour le moment) sont éliminés d'office. Or, la plupart des systèmes gérant les matrices creuses sont plutôt spécialisés sur des problèmes de physique, et font donc les calculs en flottants et non en entiers. Il en découle un risque d'erreur de calcul et probablement un coût plus élevé en temps et en mémoire. En utilisant `Scilab` nous avons pu ainsi faire le calcul jusqu'à $n = 13$ (matrice 1301×1121), mais seulement en flottants. En revanche, la toute dernière version (non officielle) de la bibliothèque `C++ LiDIA` sait gérer les matrices creuses à coefficients entiers. Nous n'avons pas encore pu l'essayer, mais il est probable qu'elle puisse traiter la matrice pour $n = 14$. Il faudra aussi reprendre les calculs fait avec `Scilab` pour être absolument certains qu'il n'y a pas eu d'erreurs d'approximation.

19.2.3 Rajouts d'identités

Ce que nous venons de voir est suffisant jusqu'à 8 sommets. En effet, il y a alors autant d'arbres que de forêts à deux composantes connexes (voir table A.14 page 277). Cependant, ce n'est plus le cas à partir de $n = 9$. Il faut donc rajouter de nouvelles identités. Notons qu'il est inutile de multiplier une forêt $\mathbf{f}$ à $k+1$ composantes connexes par le polynôme symétrique e_k. En effet, en utilisant les propriétés 12.2.11 de e_k, l'expression obtenue est une combinaison linéaire des produits que l'on a déjà considérés.

$$\mathbf{x}^{\mathbf{f}^{\circledast}} e_k = \mathbf{x}^{\mathbf{f}^{\circledast}} k!(e_1)^k = \left(k!\mathbf{x}^{\mathbf{f}^{\circledast}}(e_1)^{k-1}\right) e_1$$

Nous avons considéré l'ensemble des produits d'une forêt à 3 composantes connexes par une étoile à 2 branches, et engendré la matrice correspondante. Là encore, nous avons en fait engendré la matrice équivalente obtenue en retirant des étoiles à 2 branches aux arbres. Le calcul jusqu'à $n = 13$ nous a alors donné deux résultats remarquables :

Proposition 19.2.2.
(i) La matrice obtenue est à nouveau de rang plein, c'est-à-dire que toutes les combinaisons linéaires obtenues sont linéairement indépendantes entre elles.
(ii) Si on rajoute ces combinaisons linéaires à celles que l'on avait déjà, on obtient une matrice surjective sur les arbres.

Corollaire 19.2.3.
Les arbres sont algébriquement reconstructibles jusqu'à $n = 13$ sommets.

De manière générale, les matrices obtenues en enlevant une étoile avec un nombre fixé k de branches aux arbres sont de rang plein, et ce au moins jusqu'à $n = 13$.

Conjecture 19.2.4.
Soient n un entier et $k \leq n$. On considère une matrice M dont les colonnes sont indexées par les arbres sur n sommets et les colonnes indexées par les forêts sur

n sommets à $k+1$ composantes connexes; si $\mathbf{g}$ *est un arbre et* $\mathbf{h}$ *une forêt, le coefficient de* $M(\mathbf{g},\mathbf{h})$ *compte le nombre de sous-graphes de* $\mathbf{g}$ *isomorphes à* $\mathbf{h}$ *et obtenus en retirant une étoile à k branches de* $\mathbf{g}$*. On retire éventuellement de M les lignes composées uniquement de 0. Ces lignes correspondent à des forêts qui ne peuvent pas être complétées en un arbre en rajoutant une étoile à k branches. Alors, la matrice M restante est de rang plein.*

19.3 Perspectives

Dénombrements et études asymptotiques

On ne pourra probablement pas continuer ce type d'expérimentation bien au delà de $n = 14$, à cause de la taille des matrices mises en jeu. Cependant, on peut glaner des informations supplémentaires en étudiant l'évolution asymptotique du nombre d'arbres et de forêts. Nous voudrions ici remercier chaleureusement Flajolet pour l'aide précieuse qu'il nous a fournie par mél. En plus des réponses détaillées à nos questions, il nous a fourni des feuilles de travail `Maple` avec des exemples de dénombrement d'arbres qui nous ont permis très rapidement de faire nos propres dénombrements de manière autonome. Il a aussi fait plusieurs études asymptotiques : nombre d'arbres et de forêts par nombre de sommets (identités 12.1 et 12.2), nombre de forêts à k composantes connexes relativement au nombre d'arbres (table 19.1).

Le principe est essentiellement d'utiliser les conditions 11.1.10 et 11.1.11, c'est-à-dire de vérifier que l'on produit suffisamment d'identités.

Nous commençons par utiliser la condition 11.1.11, en la raffinant, pour obtenir des informations plus précises sur les systèmes générateurs potentiels. Dans ce qui précédait, nous avons considéré les identités obtenues par produit des forêts à 2 et 3 composantes connexes par les étoiles à respectivement 1 et 2 branches. Il faut donc qu'il y ait plus de forêts à 2 et 3 composantes connexes que d'arbres. On constate que c'est faux à partir de $n = 35$ (voir table A.14 page 277 ou figure A.9 page 268). Il est alors tentant de rajouter les produits de forêts à 4 composantes connexes par des étoiles à 3 branches et ainsi de suite. L'étude asymptotique menée par Flajolet nous indique que cette approche est vaine. En effet, le quotient du nombre total de forêts non connexes par le nombre d'arbres a une limite asymptotique de l'ordre de $0,913$ (table 19.1). Cela peut aussi se voir sur la figure A.7 page 267. Au delà de 90 sommets, il y a plus d'arbres que de forêts non connexes.

k	1	2	3	4	5	6	7	8
q	1	$0,566$	$0,225$	$0,0802$	$2,76.10^{-2}$	$9,41.10^{-3}$	$3,19.10^{-3}$	$1,08.10^{-4}$
k	9	10	11	12	13	14	15	total
q	$3,65.10^{-4}$	$1,24.10^{-4}$	$4,18.10^{-5}$	$1,41.10^{-5}$	$4,79.10^{-6}$	$1,62.10^{-6}$	$5,48.10^{-7}$	$0,913$

TAB. 19.1 – Limite asymptotique lorsque le nombre de sommets tend vers l'infini du quotient q du nombre de forêts à k composantes connexes par le nombre d'arbres

Cette étude asymptotique combinée avec une étude de l'algèbre des forêts dans les petits degrés permet une étude plus fine des identités à rajouter.

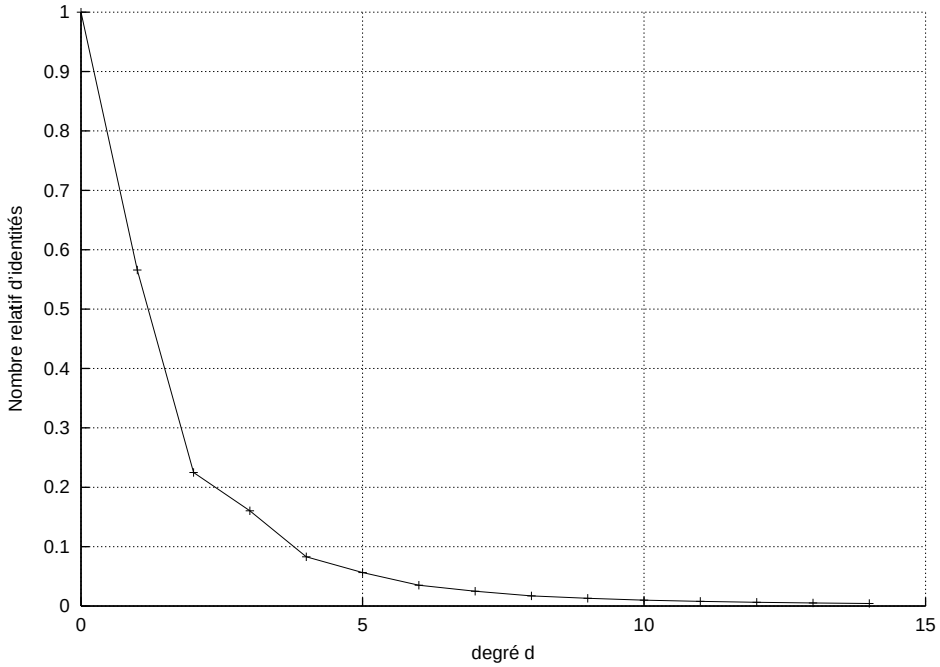
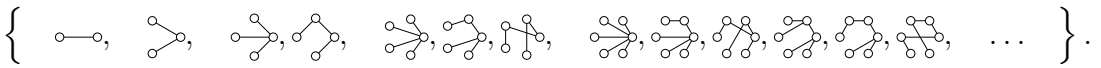


FIG. 19.2 – Nombre d'identités pouvant être produites en multipliant une forêt à d arêtes par une forêt à $n-1-d$ arêtes, relativement au nombre total d'arbres. Évaluation asymptotique pour n grand relativement à d

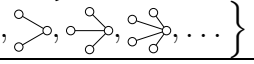
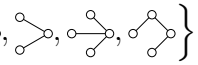
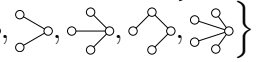
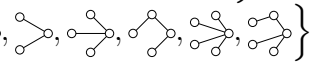
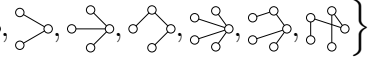
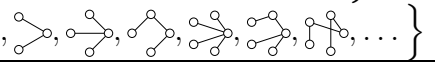
Nous avons vu qu'il était inutile de considérer les produits de la forme $e_k\,\mathbf{x}^{\mathbf{f}^{\circledast}}$, car ils n'apportent rien de plus que les produits $e_1\,\mathbf{x}^{\mathbf{f}^{\circledast}}$ (voir § 19.2.3). Plus généralement, si $A := \cup_d A_d$ est un ensemble minimal de forêts qui engendre par somme et produit toutes les forêts non-connexes, il suffit de considérer les produits de la forme $p\,\mathbf{x}^{\mathbf{f}^{\circledast}}$, où p est un polynôme de degré d dans A et $\mathbf{f}$ une forêt à $n-1-d$ arêtes.

Soit q_d le rapport entre le nombre de forêts à $n-1-d$ arêtes et le nombre d'arbres. Le produit $|A_d|.q_d$ compte le nombre d'identités que l'on peut obtenir par les produits que nous venons de voir, relativement au nombre total d'arbres. Comme les quasi-arbres engendrent toute l'algèbre des forêts (proposition 12.2.10), on peut majorer $|A_d|$ par le nombre d'arbres à d arêtes. En utilisant les évaluations asymptotiques de la table 19.1 page précédente, on peut obtenir une majoration de $|A_d|.q_d$ pour les petites valeurs de d (figure 19.2). On constate que $|A_d|.q_d$ décroît extrêmement rapidement.

La majeure partie des identités va donc être fournie en utilisant les générateurs de A de petit degré d. D'après la remarque 12.2.10, dès que n est grand ($n \geq 2d$), ces générateurs sont exactement les quasi-arbres



Si on considère tous les générateurs de A_d, le quotient entre le nombre d'identités et le nombre d'arbres est de l'ordre de $1,213800$. Il faut donc que les identités soient majoritairement libres. De plus, on sait qu'il faut prendre le générateur de degré 1 et celui de degré 2. Enfin, on peut tester si certaines combinaisons sont plausibles (voir table 19.2 page suivante).

Générateurs	Série génératrice des degrés	Rapport	Plausible
Étoiles			
$\{$  $\}$	z	$0,57$	non
$\left\{$  $\right\}$	$z+z^2$	$0,79$	non
$\left\{$  $\right\}$	$z+z^2+z^3+\ldots$	$0,91$	non
Arbres			
$\left\{$  $\right\}$	$z+z^2+2z^3$	$0,95$	non
$\left\{$  $\right\}$	$z+z^2+2z^3+z^4$	$0,98$	non
$\left\{$  $\right\}$	$z+z^2+2z^3+2z^4$	$1,01$	oui
$\left\{$  $\right\}$	$z+z^2+2z^3+3z^4$	$1,03$	oui
$\left\{$  $\right\}$	$z+z^2+2z^3+3z^4+6z^5\ldots$	$1,21$	oui

TAB. 19.2 – Rapport entre nombre d'identités obtenues et nombre total d'identités nécessaires pour que les arbres soient algébriquement reconstructibles, pour différents choix de générateurs minimaux
Il s'agit d'une estimation asymptotique lorsque le nombre n de sommets est grand. Si la proportion est strictement inférieure à 1, on ne peut pas engendrer tous les arbres sur n sommets par des produits de ces générateurs minimaux et de forêts. Le nombre de générateurs par degré est représenté par sa série génératrice. La série $z+z^2+2z^3$ correspond à 1 générateur de degré 1, 1 de degré 2 et 2 de degré 3.

Nous finissons cette section avec une seconde étude basée sur la condition 11.1.10, semblable à celle que nous avons utilisée pour montrer qu'il existait des graphes simples non-algébriquement reconstructibles. Le lemme suivant est l'équivalent du lemme 18.2.2.

Lemme 19.3.1.
Les forêts algébriquement reconstructibles dans l'algèbre des forêts sont engendrées par les forêts quasi-connexes dont la composante connexe non triviale est de taille $< n$.

Il faut donc évaluer, au degré d, le rapport entre le nombre d'identités de degré d que l'on obtient par produit de forêts quasi-connexes dont la composante connexe non triviale est de taille $< n$, et le nombre de forêts à d arêtes sur n sommets. Comme on sait que les forêts à moins de $n-1$ arêtes sont non-connexes et donc algébriquement reconstructibles, on peut se contenter d'évaluer ce rapport pour $d = n-1$. Les forêts à $n-1$ arêtes sur n sommets sont exactement les arbres. On obtient une expression très simple pour ce ratio.

Proposition 19.3.2.
Soit r_n le rapport entre le nombre d'identités que l'on obtient par produit de forêts quasi-connexes dont la composante connexe est de taille $< n$ et le nombre d'arbres à n sommets. Alors

$$R_n = \frac{f_{n-1}}{a_n} - 1,$$

où f_d est le nombre de forêts à d arêtes, et a_n le nombre d'arbres à n sommets.

Démonstration. Les forêts quasi-connexes dont la composante connexe est de taille $< n$ sont en bijection avec les arbres à strictement moins de n sommets. Les identités de degré $n-1$ obtenues par produit de telles forêts sont donc en bijection avec les forêts à $n-1$ arêtes dont les composantes connexes sont de tailles $< n$ (comme pour les graphes simples, on identifie un produit d'arbres $\mathbf{g}_1, \ldots, \mathbf{g}_k$ avec la forêt réunion sommet-disjointe de ces arbres). Ce sont exactement les forêts à $n-1$ arêtes qui ne sont pas des arbres. Le nombre d'identités est donc simplement $f_{n-1} - a_n$. On en déduit la valeur annoncée pour le rapport r_n. □

Nous pouvons utiliser les résultats du § 12.2.2 pour calculer et évaluer asymptotiquement ce ratio. Jusqu'à $n = 250$, il est strictement supérieur à 1 (voir figure A.10 page 268) ; au delà, il tend asymptotiquement par le haut vers une constante de l'ordre de 1.13. Cette deuxième étude confirme donc la première : il y a tout juste suffisamment d'identités. Il faut donc que ces identités soient presque toutes linéairement indépendantes pour que les arbres soient algébriquement reconstructibles.

19.4 Familles infinies d'arbres algébriquement reconstructibles

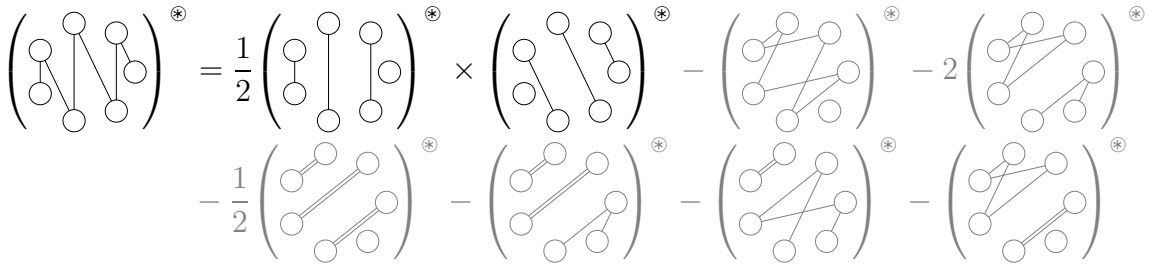
Nous allons conclure ce chapitre en donnant certaines familles d'arbres qui sont algébriquement reconstructibles. Nous commençons par les chemins pour lesquels

on peut donner une démonstration particulière, semblable à celle des cycles hamiltoniens pairs. On appelle la longueur d'un chemin son nombre d'arêtes.

Remarque 19.4.1: Les chemins sont algébriquement reconstructibles.

Démonstration. Soit $\mathbf{g}$ un chemin. On peut supposer qu'il est de longueur $n-1$, car sinon il possède un sommet isolé et est donc algébriquement reconstructible.

Soient $\mathbf{c}_1$ et $\mathbf{c}_2$ les deux couplages obtenus en prenant alternativement une arête sur deux du chemin. On considère leur produit $\mathbf{x}^{\mathbf{c}_1 \circledast}\mathbf{x}^{\mathbf{c}_2 \circledast}$ dans l'algèbre des forêts. Soit t un terme de ce produit. Comme les sommets de $\mathbf{c}_1$ et $\mathbf{c}_2$ sont de degré inférieur à 1, les sommets de t sont de degré inférieur à 2. De plus, t est connexe (sinon il contient au moins un cycle ou une double arête et a donc été éliminé par le produit). Conclusion : t est le chemin de longueur $n-1$, isomorphe au chemin de départ.



□

Définition 19.4.2 (Pieuvre).
On appelle pieuvre *un arbre dont au plus un sommet est de degré supérieur à 2 (voir figure 19.3 page 253). On appelle ce sommet la tête. Dans le cas d'un chemin, la tête peut être n'importe lequel des sommets. On distingue deux pieuvres sur le même chemin mais dont la tête pointe sur des sommets différents.*

On définit la *i-reconstructibilité* dans l'algèbre des forêts de manière analogue à la i-reconstructibilité usuelle. Là aussi, la i-reconstructibilité implique la reconstructibilité algébrique dans l'algèbre des forêts, et donc dans l'algèbre des invariants. Cependant, on note qu'elle n'implique pas la i-reconstructibilité dans l'algèbre des invariants. Ainsi, le chemin de longueur 3 dont une extrémité est en i est i-reconstructible dans l'algèbre des forêts, mais pas dans l'algèbre des invariants (testé informatiquement pour $n = 5$).

Théorème 19.4.3.
Soit $\mathbf{f}$ *une pieuvre et i sa tête. Alors,* $\mathbf{f}$ *est i-reconstructible dans l'algèbre des forêts. Les pieuvres sont algébriquement reconstructibles.*

Démonstration. Le principe est de détacher une des tentacules les plus longues de la pieuvre et de la rattacher de toutes les façons possibles (figures 19.3(b) et 19.3(c) page 253). Nous verrons que cette opération préserve la i-reconstructibilité. Si la tentacule est rattachée par une des deux extrémités, on retombe sur la pieuvre d'origine. Sinon, la tentacule est remplacée par deux tentacules strictement plus courtes. En réitérant l'opération, on obtient la pieuvre la plus simple, c'est-à-dire l'étoile (figure 19.3(d) page 253). Nous avons vu au § 16.3 que cette dernière était i-reconstructible, ce qui permettra de conclure.

On associe à chaque pieuvre la liste décroissante des longueurs de ses tentacules. Pour la pieuvre de la figure 19.3 page 253 cela donne successivement les listes

$$(5,5,5,4,3), \quad (5,5,4,3,3,2), \quad \ldots, \quad (\underbrace{1,\ldots,1}_{22}).$$

On ordonne partiellement les pieuvres en comparant lexicographiquement ces listes. De la sorte, à nombre d'arêtes constant, le chemin pointé en une extrémité est la plus grande pieuvre et l'étoile la plus petite. On raisonne par induction sur cet ordre.

Soit $\mathbf{f}$ une pieuvre et i sa tête. Si $\mathbf{f}$ est une étoile, $\mathbf{f}$ est i-reconstructible d'après le lemme 16.3.7. Sinon, on suppose que toutes les pieuvres plus petites sont i-reconstructibles. Soient $\mathbf{t}$ une tentacule de longueur maximale, et $\mathbf{g}$ la pieuvre obtenue en retirant $\mathbf{t}$ de $\mathbf{f}$. Par induction, $\mathbf{g}$ est i-reconstructible.

Comme $\mathbf{t}$ est un chemin, $\mathbf{t}$ est algébriquement reconstructible. Donc $\mathbf{x}^{\mathbf{t}^{\circledast}}$ est un polynôme i-reconstructible. Soit q la somme de tous les chemins de même longueur que $\mathbf{t}$ passant par i. On va montrer que p est i-reconstructible. Si $\mathbf{t}$ est de longueur $l = n-1$, le polynôme p coïncide avec $\mathbf{x}^{\mathbf{t}^{\circledast}}$ et est donc directement i-reconstructible. Sinon $\mathbf{t}$ a un sommet isolé, et on applique le lemme 16.3.3.

On considère maintenant le produit $p = q\mathbf{x}^{\mathbf{g}^{\circledast}_i}$ qui est i-reconstructible. Soit m un terme de ce produit. Il est obtenu en rajoutant à $\mathbf{g}$ un chemin passant par i de longueur l, sans créer de cycle ni de double arête, car le produit se fait dans l'algèbre des forêts. Si le chemin touche i par une de ses deux extrémités, on obtient une pieuvre isomorphe à $\mathbf{g}$. Sinon, on obtient une pieuvre avec deux tentacules de longueur strictement plus petite que l. Cette pieuvre est alors plus petite que $\mathbf{g}$, et donc i-reconstructible par induction. En conclusion, $\mathbf{x}^{\mathbf{f}^{\circledast}_i}$ s'obtient de $\frac{p}{2}$ en retirant des polynômes i-reconstructibles, et est donc i-reconstructible. □

Généralisations

L'utilisation de la i-reconstructibilité a permis de forcer le comportement du produit en un sommet donné. La remarque suivante donne quelques arbres supplémentaires que l'on obtient de manière analogue.

Théorème 19.4.4.
Les pieuvres auxquelles on a rajouté des étoiles touchant la tête par l'extrémité d'une branche (voir figure 19.4 page 254) sont i-reconstructibles

Démonstration. On commence par montrer qu'une étoile $\mathbf{t}$ pointée en une de ses extrémités est i-reconstructible. Soit $p := \mathbf{x}^{\mathbf{t}^{\circledast}_i}$ le polynôme associé à $\mathbf{t}$, invariant par rapport aux permutations des sommets différents de i, et soit $q := \mathbf{x}^{\mathbf{t}^{\circledast}}$ le polynôme invariant associé à $\mathbf{t}$. D'après le lemme 16.3.7, le polynôme q est algébriquement reconstructible et donc i-reconstructible. On obtient p à partir de q en retirant la somme des étoiles isomorphes à $\mathbf{t}$ centrées sur i de q, et la somme des étoiles isomorphes à $\mathbf{t}$ ne passant pas par i. Comme ces deux quantités sont i-reconstructibles, p est aussi i-reconstructible.

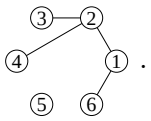
Le principe est ensuite le même que pour les pieuvres, en raisonnant par récurrence sur le nombre d'étoiles (voir figure 19.4 page 254). Soit $\mathbf{f}$ une pieuvre, et i sa tête. Si $\mathbf{f}$ ne contient pas d'étoiles, $\mathbf{f}$ est une pieuvre et on applique le théorème 19.4.3. Sinon, soit $\mathbf{t}$ une des étoiles de $\mathbf{f}$ et $\mathbf{g}$ l'arbre restant lorsque l'on retire

$\mathbf{t}$ (voir figure 19.4(b) page 254). Par récurrence, $\mathbf{g}$ a une étoile en moins et est donc i-reconstructible. Si l'on multiplie le polynôme $\mathbf{x}^{\mathbf{g}}{}_i^{\circledast}$ associé à $\mathbf{g}$ par le polynôme $p := \mathbf{x}^{\mathbf{t}}{}_i^{\circledast}$ associé à $\mathbf{t}$, on obtient le polynôme $\mathbf{x}^{\mathbf{t}}{}_i^{\circledast}$ associé à $\mathbf{f}$. On en déduit que ce dernier est i-reconstructible. □

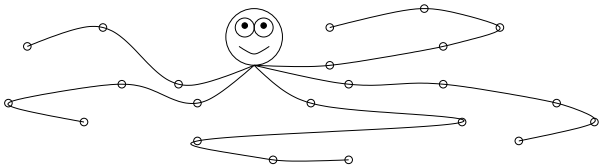
Corollaire 19.4.5.
Les arbres de diamètre inférieur 4 sont algébriquement reconstructibles.

Limites de la i-reconstructibilité

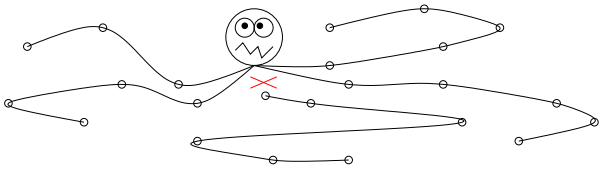
La notion de i-reconstructibilité est très forte, même dans le cadre de l'algèbre des forêts. Aussi, nous ne pensons pas qu'il soit possible d'étendre la méthode utilisée pour les pieuvres et les pieuvres étoilées à d'autres familles substantielles d'arbres. Par exemple, pour $n \geq 6$, la forêt quasi-connexe suivante n'est pas i-reconstructible lorsque l'on pointe i sur l'une quelconque de ses feuilles (sommets 3, 4 ou 6) :



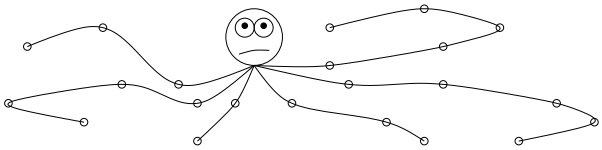
Pour vérifier ce fait, nous avons utilisé notre bibliothèque `PerMuVAR` pour calculer efficacement dans l'algèbre des forêts étiquetées quotientée par l'action du groupe $\mathfrak{S}_{n-1}$ par permutation des sommets distincts de i. Pour chaque forêt $\mathbf{f}$ quasi-connexe sur les sommets $\{1, \ldots, i-1, i+1, \ldots, n\}$ nous avons considéré le polynôme $p_f := \mathbf{x}^{\mathbf{f}}{}_i^{\circledast}$ obtenu par symétrisation de $\mathbf{f}$ sur les sommets distincts de i et le polynôme $q_f := \mathbf{x}^{\mathbf{f}^{\circledast}}$ obtenu par symétrisation de $\mathbf{f}$ sur les n sommets. Une forêt $\mathbf{g}$ pointée au sommet n est n-reconstructible si, et seulement si, le polynôme $r := \mathbf{x}^{\mathbf{g}}{}_i^{\circledast}$ obtenu par symétrisation de $\mathbf{g}$ sur les sommets distincts de i est dans l'algèbre engendrée par l'ensemble des polynômes $p_{\mathbf{f}}$ et q_f. Nous avons alors vérifié que, si $n = 6$, l'arbre $\mathbf{g}$ que nous avons donné ci-dessus n'était pas i-reconstructible. On en déduit facilement qu'il n'est pas i-reconstructible pour $n \geq 6$.



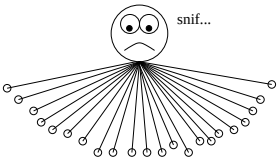
(a) Une pieuvre. Elle sourit car elle vient d'apprendre qu'elle est algébriquement reconstructible. Elle ne connaît pas encore les détails de l'opération...



(b) Début de la première opération ;

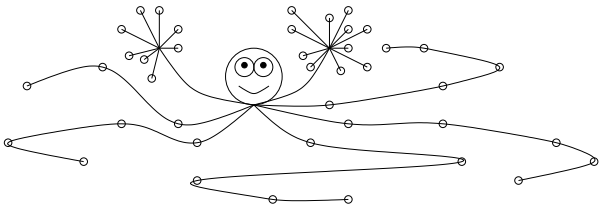


(c) Fin de la première opération ;

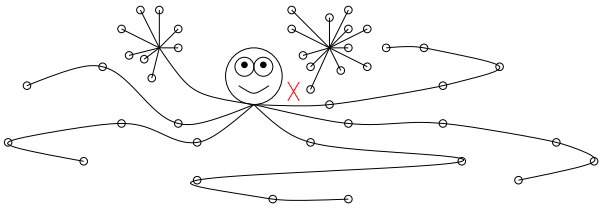


(d) Et au final, on obtient une étoile (de mer).

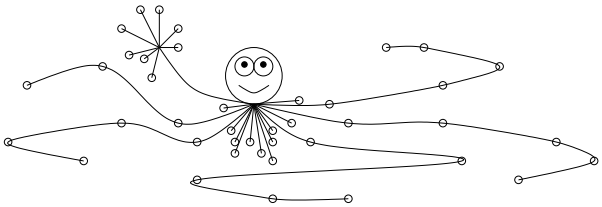
FIG. 19.3 – Reconstruction algébrique des pieuvres



(a) Une pieuvre étoilée



(b) On détache une étoile



(c) Que l'on raccroche

FIG. 19.4 – Rajout d'étoiles à une pieuvre

Conclusion et perspectives

Un des objectifs principaux de cette thèse était d'évaluer la pertinence de l'utilisation d'outils algébriques pour aborder le problème de reconstruction de graphes ; le principe étant d'essayer de montrer que tous les polynômes invariants sont reconstructibles, problème équivalent au problème de reconstruction des graphes valués.

Pouzet [Pou77] avait introduit la notion de reconstructibilité algébrique d'un polynôme, impliquant celle de reconstructibilité, en s'inspirant de la reconstructibilité du polynôme caractéristique montrée par Tutte [Tut76, Tut79]. De fait, nous avons montré qu'elle permet d'obtenir naturellement plusieurs résultats classiques de reconstruction (voir § 15). En particulier, les multigraphes non-connexes, le nombre de cycles hamiltoniens, les nombres chromatique et cochromatique raffinés par taille, ainsi que les paramètres tels que « point arboricity », « linear point arboricity » ou « k-point partition » sont algébriquement reconstructibles.

La reconstructibilité algébrique est préservée par de nombreuses opérations, substitution (proposition 16.2.1), dérivation (proposition 16.4.1), fractions dans certains cas (proposition 16.5.1), et surtout passage au complémentaire (théorème 16.6.2).

Si le polynôme invariant $\mathbf{x}^{\mathbf{m}\circledast}$ associé à un multigraphe $\mathbf{m}$ (et *a fortiori* un graphe simple) est algébriquement reconstructible, alors le multigraphe $\mathbf{m}$ est lui-même reconstructible au sens usuel. Nous avons montré, par des calculs dans l'algèbre des invariants, que tous les graphes simples sont algébriquement reconstructibles jusqu'à $n = 6$, et que les multigraphes sont algébriquement reconstructibles pour $n = 4$ sommets (théorème 17.1.1), et très probablement aussi pour $n = 5$. De même, les arbres sont algébriquement reconstructibles jusqu'à $n = 13$ (corollaire 19.2.3), et nous avons vérifié que, au delà, il y avait *a priori* suffisamment d'identités. Enfin, nous avons construit une famille infinie d'arbres algébriquement reconstructibles, contenant tous les arbres de diamètre ≤ 4. À l'exception de quelques exemples, nous ne savons pas traiter les arbres de diamètre 5.

Au vu de ces résultats, il était plausible que tous les polynômes invariants soient algébriquement reconstructibles. Cependant, nous avons montré, par un calcul de dimension, qu'il existe des graphes simples sur 13 sommets et 17 arêtes dont le polynôme invariant associé n'est pas algébriquement reconstructible, alors que ces graphes sont reconstructibles. Nos résultats expérimentaux suggèrent qu'il existe une constante c telle que pour $n \leq 13$, et $c * n \leq d \leq \mathrm{C}_n^2 - c * n$, la plupart des graphes simples à n sommets et d arêtes, ne soient pas algébriquement reconstructibles.

Une approche est d'affaiblir la notion de reconstructibilité algébrique, par exemple en rajoutant des axiomes de préservation par d'autres opérations que sommes et produits. Il est illusoire de rajouter la préservation par fractions quelconques, car une étude du corps des invariants (voir § 9.4) montre que tout polynôme invariant

s'exprime comme fraction de polynômes algébriquement reconstructibles. Toute la difficulté est donc rejetée dans la propriété « algébriquement reconstructible $\Longrightarrow$ reconstructible ». De même, la stabilité par racine quelconque serait un axiome trop fort, car tout polynôme invariant vérifie une équation polynomiale à coefficients algébriquement reconstructibles.

Une autre voie est d'étudier cette notion dans d'autres algèbres, en particulier dans l'algèbre des graphes simples munie du produit d'union (algèbre des sous-graphes de Kocay [Koc82]). Il est cependant difficile d'étudier cette algèbre, car elle n'est pas graduée (voir § 18).

La figure 13.1 page 196 dresse un bilan des liens entre les différentes notions de reconstructibilité.

Résumé des autres résultats de la thèse

Partie I : Espace vectoriel des parties d'un ensemble

- Nouvelle base de la représentation irréductible $[n-k,k]$ du groupe symétrique ;
- Les graphes simples sont essentiellement déterminés à l'isomorphie près par leur partie régulière ;
- Une hypothèse sur la matrice d'incidence des graphes étiquetés versus les forêts à $n-2$ arêtes, vérifiée pour $n \leq 6$. Le cas non-étiqueté est traité jusqu'à $n = 13$ dans la partie III.
- Pour tout n, les lignes de la matrice d'incidence des arbres étiquetés versus les forêts à $n-2$ arêtes et un sommet isolé sont indépendantes ;

Partie II : Invariants algébriques de graphes

- Calcul de la série de Hilbert de l'algèbre des invariants sur les graphes jusqu'à $n = 12$ en raffiné et $n = 18$ en non-raffiné ;
- L'algèbre des invariants sur les graphes n'est pas engendrée par les graphes simples ;
- L'algèbre des invariants sur les digraphes n'est pas engendrée par les digraphes simples (contre-exemple à un lemme de Grigoriev) ;
- Proposition d'un nouveau système de paramètres pour [n-2,2], de degrés cohérents avec la série de Hilbert. Vérifié pour $n \leq 5$.
- Calcul pour $n = 5$ de systèmes partiels d'invariants secondaires et de systèmes générateurs minimaux jusqu'au degré 10. Cela semble suffisant pour donner un système générateur minimal. On en déduirait la reconstructibilité algébrique de tous les multigraphes à $n = 5$ sommets, et que les graphes valués dans $\{0,1,2\}$ forment un système générateur. Mêmes types de calculs partiels jusqu'à $n = 8$. On en déduit que tous les graphes simples à $n = 6$ sommets sont algébriquement reconstructibles ;
- Calcul pour $n = 5$ de systèmes partiels d'invariants secondaires et de systèmes générateurs minimaux jusqu'au degré 22 avec le produit de chaîne. On en déduit un système générateur (non minimal !) pour $n = 5$. Mêmes types de calculs partiels jusqu'à $n = 8$;

- Les multigraphes (resp. graphes simples, forêts) quasi-connexes sont des générateurs algébriquement indépendants de l'algèbre des invariants (resp. graphes simples, forêts) sur un nombre infini de sommets ;
- Système générateur partiel minimal jusqu'au degré $n/2$.
- Système générateur très simple du corps des fractions invariantes. Contrairement à ce qu'affirme Grigoriev [Gri79], ce n'est pas un système complet d'invariants.
- Étude de la borne $\beta(n)$ sur les degrés d'un système générateur minimal de l'algèbre des invariants sur les graphes :
  - $\beta(n) \leq n!$ (groupe fini) ;
  - $\beta(n) \leq \mathrm{C}^2_{\mathrm{C}^2_n} - \mu(n)$, où la valeur de $\mu(n)$ est parfaitement connue (représentation par permutation et théorème 11.4.1) ;
  - $\beta(n) \leq \mathrm{C}^2_n + \mathrm{C}^2_{\mathrm{C}^2_{n-1}} - \mu(n)$? (conjecture 11.3.1 sur les invariants primaires) ;
  - $\beta(n) \leq 2\,\mathrm{C}^2_n$? (problème 11.2.6 : les multigraphes valués $\{0,1,2\}$ engendrent l'algèbre des invariants) ;
  - $\beta(n) \leq \mathrm{C}^2_n - 1$? (résultats expérimentaux pour $n = 4, 5$).

Bilan des Outils utilisés

Le théorème de Kantor a été central dans cette thèse. Même s'il peut être interprété comme un avatar de la théorie des représentations, nous n'avons pas pu vraiment exploiter cette dernière. Nous avons utilisé quelques notions de base de géométrie algébrique ; en particulier, les considérations de dimensions (dimension de Krull, série de Hilbert/énumération de Pólya) se sont révélées un outil efficace pour éliminer d'office certaines hypothèses. Nos calculs effectifs sur l'algèbre des invariants sont basés sur sa structure (graduation, décomposition de Hironaka) et les algorithmes usuels associés, ainsi que sur quelques idées très rudimentaires tirées de l'étude des invariants de groupes de permutations *via* les algèbres de Stanley-Reisner [GS84]. Enfin, des propriétés élémentaires de théorie de Galois nous ont permis d'extraire des informations sur le corps des fractions invariantes.

Annexes

Annexe A

Statistiques

Cette annexe contient des graphiques et des tables sur le nombre de graphes non étiquetés, le nombre de secondaires nécessaires, etc. Le but des graphiques est d'avoir rapidement des ordres de grandeurs sur la taille des problèmes traités. Le choix des échelles des graphiques a été délicat car les croissances sont très rapides et les variations très grandes d'une famille d'objets à l'autre. Nous avons essayé de réduire au maximum le nombre d'échelles différentes de façon à faciliter les comparaisons. En revanche, certains graphiques paraissent quelque peu tassés. Enfin, certains graphiques ont été repris à deux échelles.

Toutes les valeurs numériques ont été calculées avec `MuPAD` et notre bibliothèque `PerMuVAR`. Les tables complètes seront disponibles par ftp, et vous pouvez dès maintenant les demander par mél à l'auteur `Nicolas.Thiery@jonas.univ-lyon1.fr`.

A.1 Graphiques

A.1.1 Nombre de graphes non étiquetés

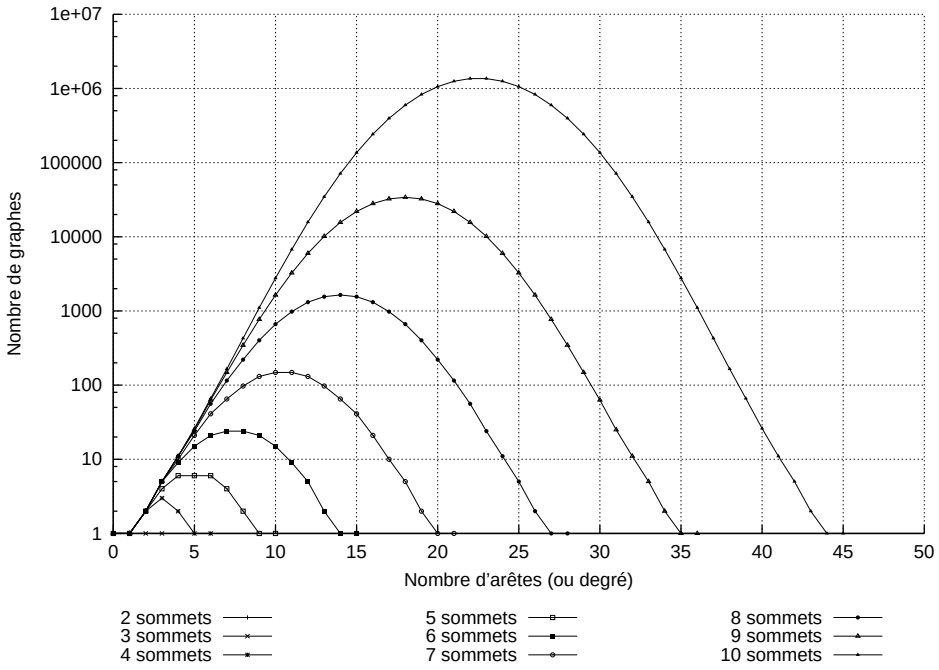


FIG. A.1 – Nombre de graphes non étiquetés, par nombre de sommets et d'arêtes

A.1.2 Nombre de graphes et multigraphes non étiquetés

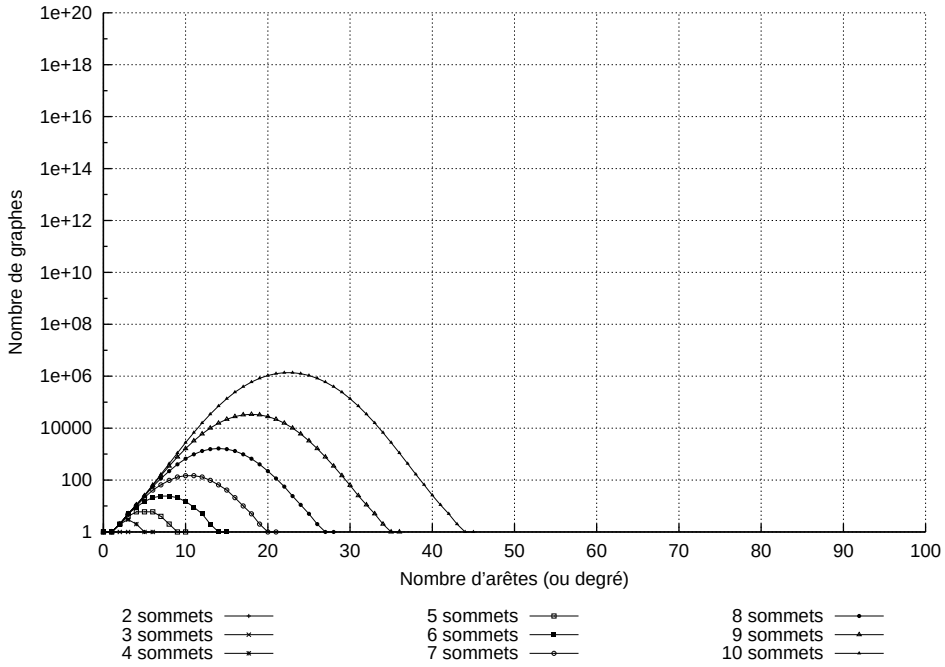


FIG. A.2 – Nombre de graphes non étiquetés, par nombre de sommets et d'arêtes

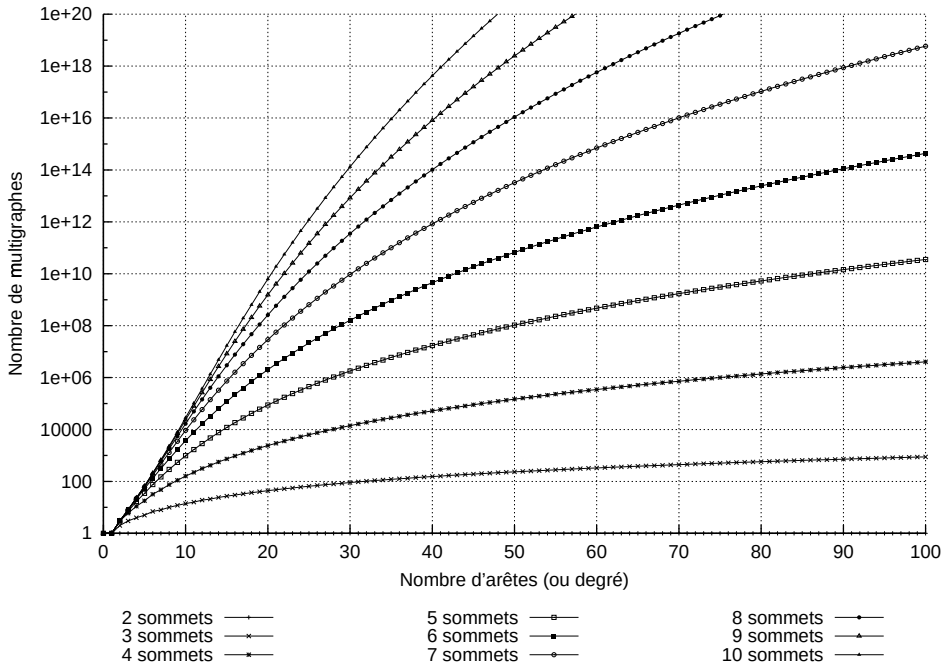
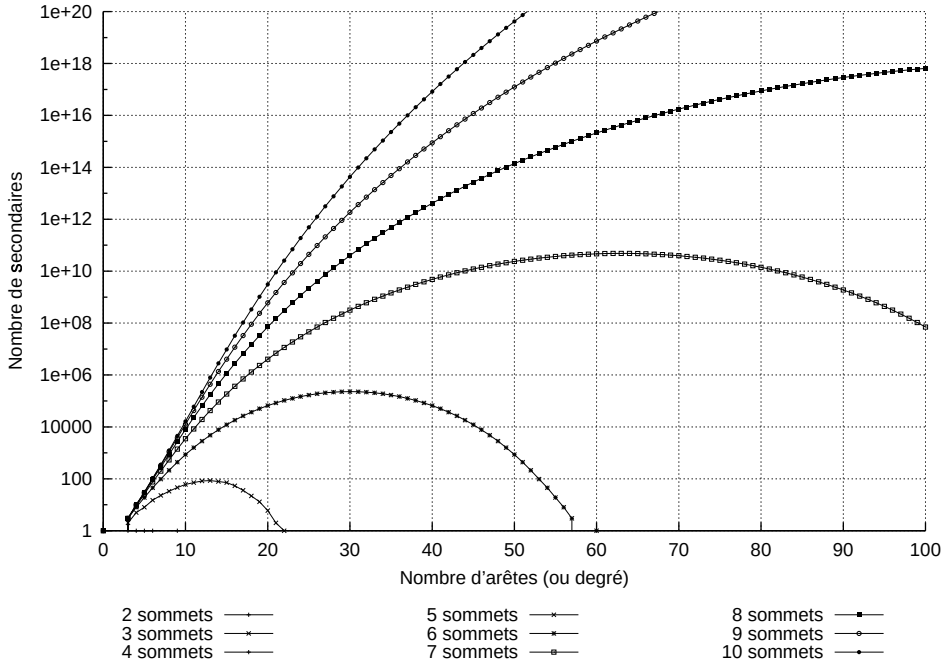
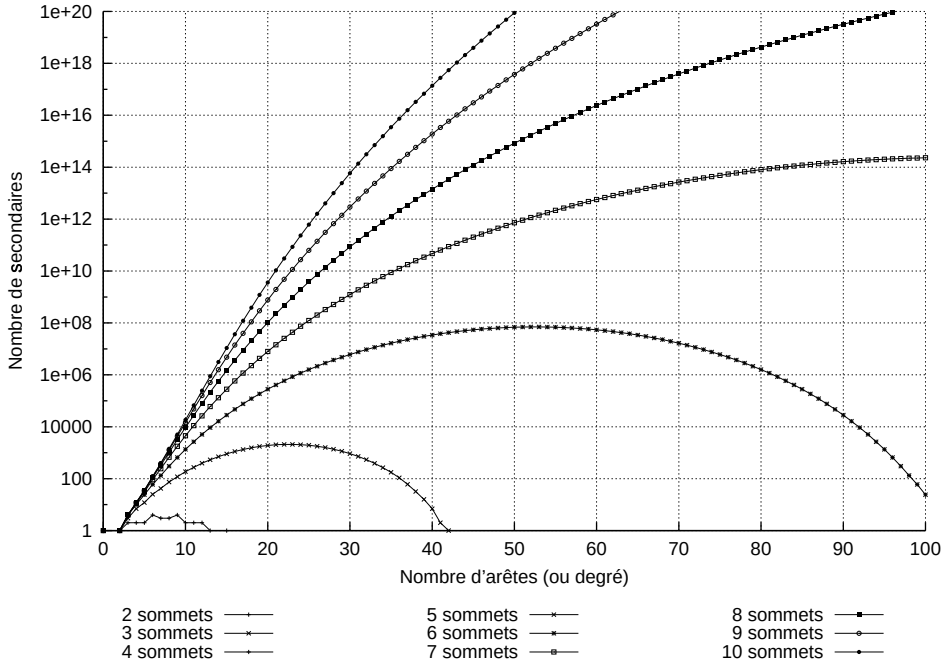


FIG. A.3 – Nombre de multigraphes non étiquetés, par nombre de sommets et d'arêtes

A.1.3 Nombre de secondaires



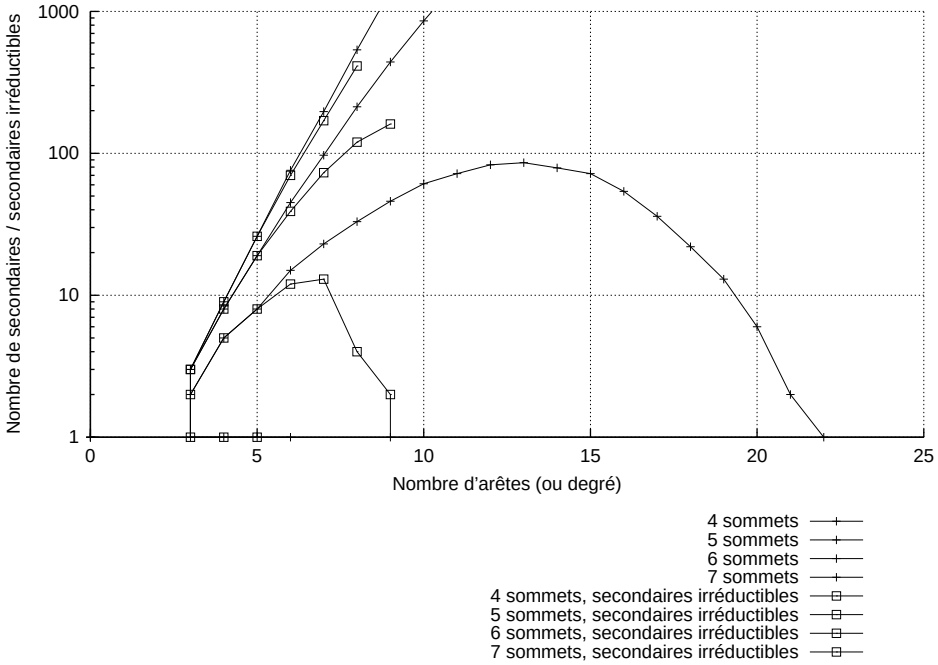
(a) Primaires : polynômes symétriques + symétriques en les étoiles



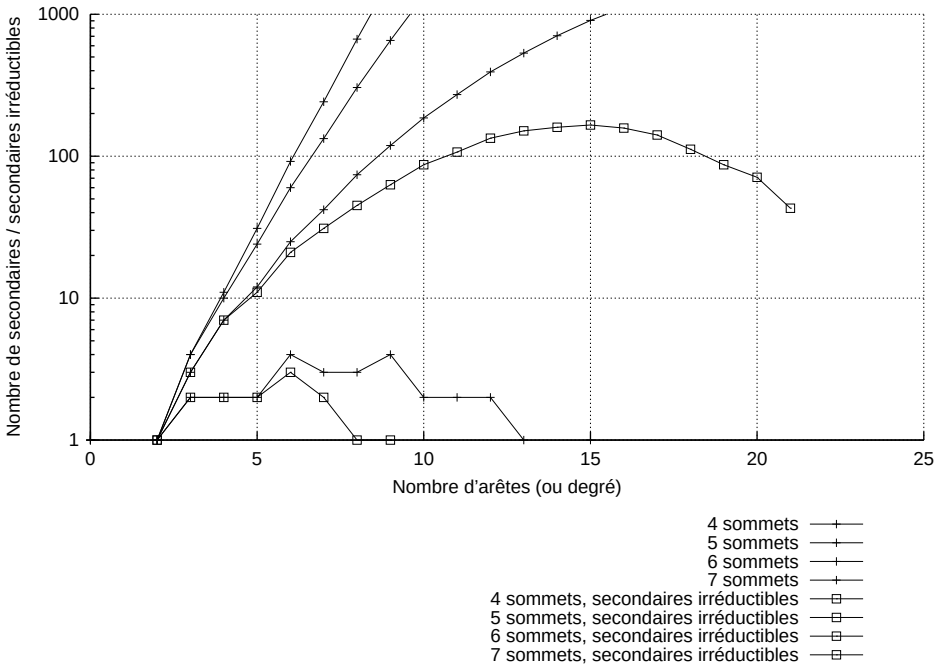
(b) Primaires : polynômes symétriques

FIG. A.4 – Nombre de secondaires, par nombre de sommets et d'arêtes

A.1.4 Nombre de secondaires irréductibles



(a) Produit classique



(b) Produit de chaînes

FIG. A.5 – Nombre de secondaires irréductibles versus nombre total de secondaires par nombre de sommets et d'arêtes

A.1.5 Nombre de générateurs dans un système minimal

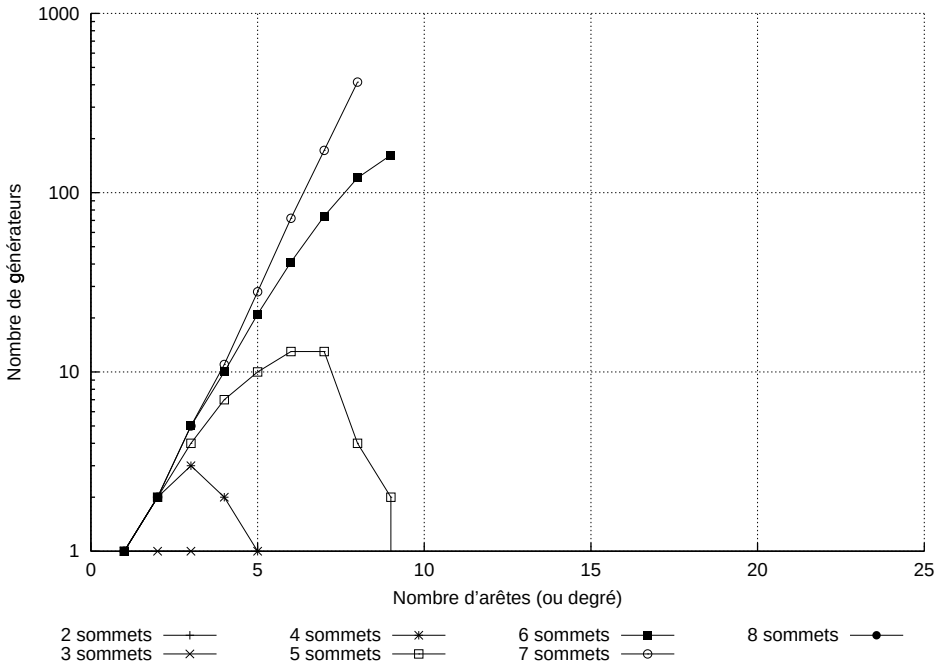


FIG. A.6 – Majoration fine du nombre de générateurs dans un système minimal de générateurs, par nombre de sommets et d'arêtes

A.1.6 Arbres et forêts

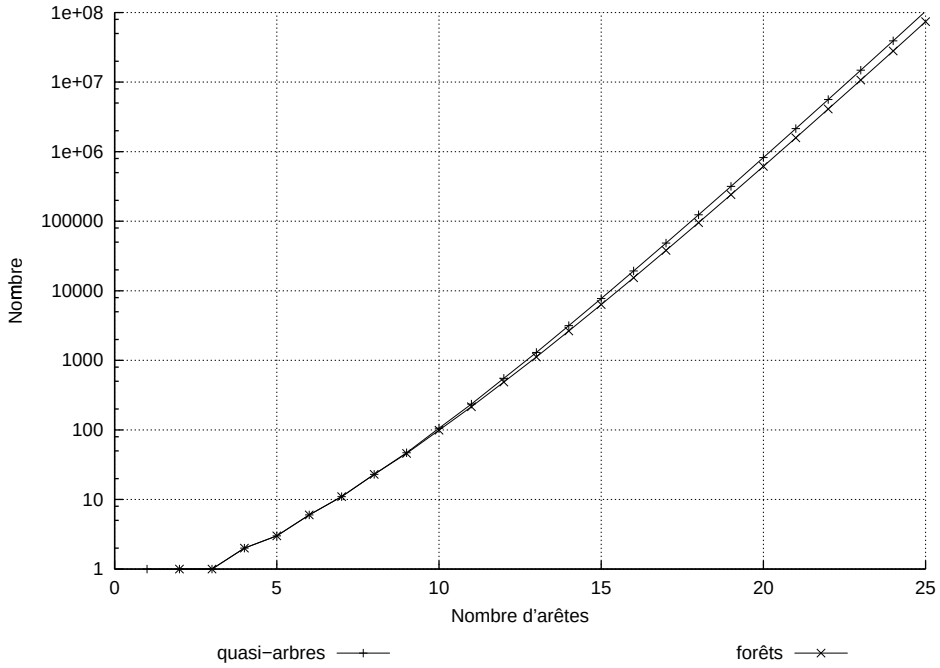


FIG. A.7 – Nombre de forêts et d'arbres par nombre d'arêtes, indépendamment du nombre de sommets

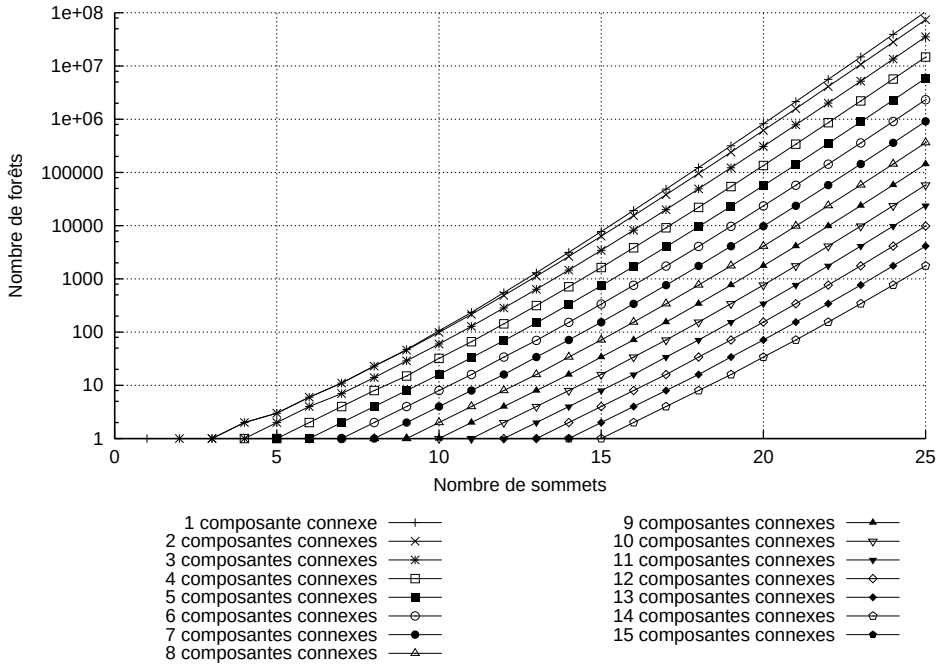


FIG. A.8 – Nombre de forêts par nombre de sommets et de composantes connexes

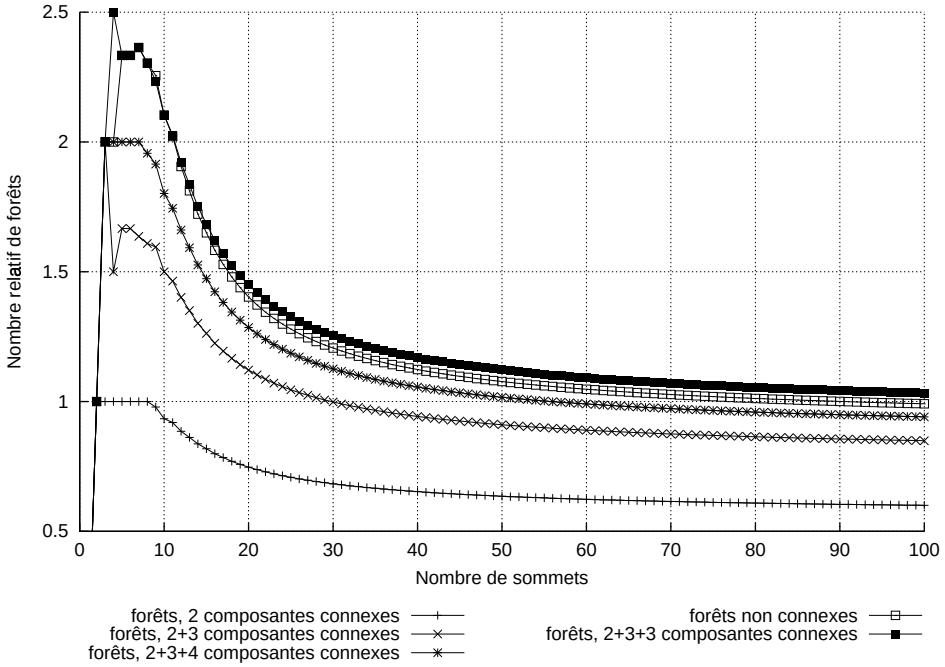


FIG. A.9 – Nombre de forêts relativement au nombre d'arbres, en fonction du nombre de sommets et de composantes connexes

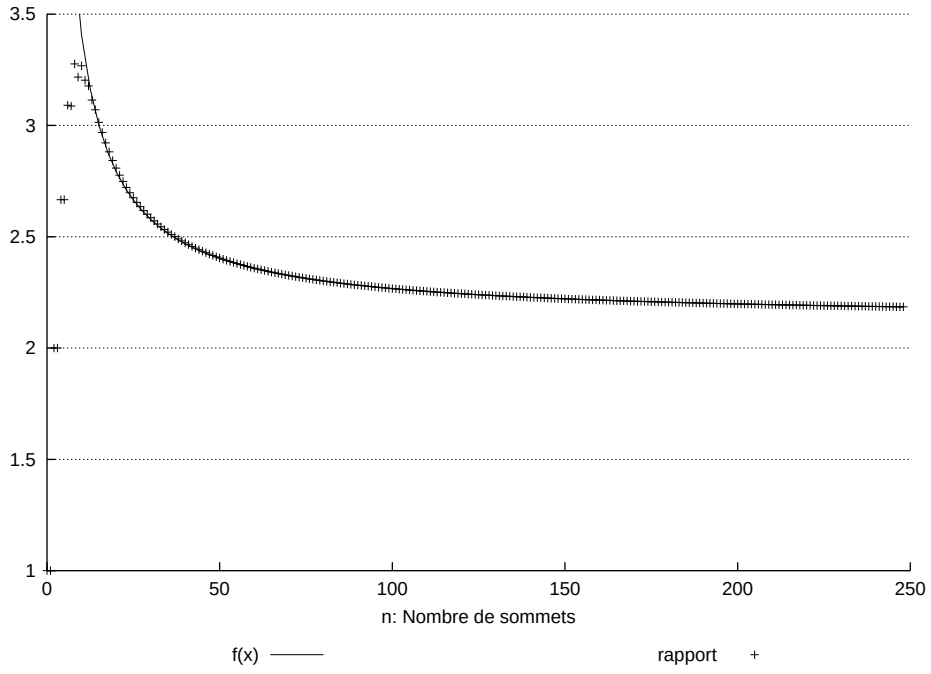


FIG. A.10 – Rapport entre le nombre de forêts à d arêtes et le nombre d'arbres à d arêtes

A.2 Tables de valeurs numériques

			produit usuel			produit de chaînes		
arêtes	graphes	multigraphes	sec.	sec. irréd.	gén. min.	sec.	sec. irréd.	gén. min.
0	1	1	1	0	0	1	0	0
1	1	1	0	1	1	0	1	2
2	1	2	0	1	1	0	1	2
3	1	3	0	1	1	0	1	2
4	0	4	0	0	0	0	0	0
5	0	5	0	0	0	0	0	0
6	0	7	0	0	0	0	0	0
7	0	8	0	0	0	0	0	0
8	0	10	0	0	0	0	0	0
9	0	12	0	0	0	0	0	0
10	0	14	0	0	0	0	0	0
11	0	16	0	0	0	0	0	0
12	0	19	0	0	0	0	0	0
13	0	21	0	0	0	0	0	0
14	0	24	0	0	0	0	0	0
15	0	27	0	0	0	0	0	0
16	0	30	0	0	0	0	0	0
17	0	33	0	0	0	0	0	0
18	0	37	0	0	0	0	0	0
19	0	40	0	0	0	0	0	0
20	0	44	0	0	0	0	0	0
21	0	48	0	0	0	0	0	0
22	0	52	0	0	0	0	0	0
23	0	56	0	0	0	0	0	0
24	0	61	0	0	0	0	0	0
25	0	65	0	0	0	0	0	0
26	0	70	0	0	0	0	0	0
27	0	75	0	0	0	0	0	0
28	0	80	0	0	0	0	0	0
29	0	85	0	0	0	0	0	0
30	0	91	0	0	0	0	0	0

TAB. A.1 – Statistiques sur l'algèbre des invariants sur les graphes à 3 sommets

			produit usuel			produit de chaînes		
arêtes	graphes	multigraphes	sec.	sec. irréd.	gén. min.	sec.	sec. irréd.	gén. min.
0	1	1	1	0	0	1	0	0
1	1	1	0	0	1	0	0	1
2	2	3	0	0	2	1	1	2
3	3	6	1	1	3	2	2	3
4	2	11	1	1	2	2	2	3
5	1	18	1	1	1	2	2	3
6	1	32	1	0	0	4	3	4
7	0	48	0	0	0	3	2	2
8	0	75	0	0	0	3	1	1
9	0	111	1	0	0	4	1	1
10	0	160	0	0	0	2	0	0
11	0	224	0	0	0	2	0	0
12	0	313	0	0	0	2	0	0
13	0	420	0	0	0	1	0	0
14	0	562	0	0	0	0	0	0
15	0	738	0	0	0	1	0	0
16	0	956	0	0	0	0	0	0
17	0	1 221	0	0	0	0	0	0
18	0	1 550	0	0	0	0	0	0
19	0	1 936	0	0	0	0	0	0
20	0	2 405	0	0	0	0	0	0
21	0	2 958	0	0	0	0	0	0
22	0	3 609	0	0	0	0	0	0
23	0	4 368	0	0	0	0	0	0
24	0	5 260	0	0	0	0	0	0
25	0	6 279	0	0	0	0	0	0
26	0	7 462	0	0	0	0	0	0
27	0	8 814	0	0	0	0	0	0
28	0	10 356	0	0	0	0	0	0
29	0	12 104	0	0	0	0	0	0
30	0	14 093	0	0	0	0	0	0

TAB. A.2 – Statistiques sur l'algèbre des invariants sur les graphes à 4 sommets

			produit usuel			produit de chaînes		
arêtes	graphes	multigraphes	sec.	sec. irréd.	gén. min.	sec.	sec. irréd.	gén. min.
0	1	1	1	0	0	1	0	0
1	1	1	0	0	1	0	0	1
2	2	3	0	0	2	1	1	2
3	4	7	2	2	4	3	3	4
4	6	17	5	5	7	7	7	8
5	6	35	8	8	10	12	11	12
6	6	76	15	12	13	25	21	22
7	4	149	23	13	13	42	31	32
8	2	291	33	4	4	74	45	46
9	1	539	46	2	2	119	63	64
10	1	974	61	0	0	186	87	88
11	0	1 691	72	?	?	272	107	107
12	0	2 874	83	?	?	393	134	134
13	0	4 730	86	?	?	533	151	151
14	0	7 620	79	?	?	706	160	160
15	0	11 986	72	?	?	905	166	166
16	0	18 485	54	?	?	1 115	158	158
17	0	27 944	36	?	?	1 332	141	141
18	0	41 550	22	?	?	1 550	112	112
19	0	60 744	13	?	?	1 743	87	87
20	0	87 527	6	?	?	1 907	71	71
21	0	124 338	2	?	?	2 027	43	43
22	0	174 403	1	?	?	2 088	?	?
23	0	241 650	0	0	0	2 097	?	?
24	0	331 153	0	0	0	2 045	?	?
25	0	448 987	0	0	0	1 935	?	?
26	0	602 853	0	0	0	1 775	?	?
27	0	801 943	0	0	0	1 588	?	?
28	0	1 057 615	0	0	0	1 367	?	?
29	0	1 383 343	0	0	0	1 145	?	?
30	0	1 795 578	0	0	0	927	?	?

TAB. A.3 – Statistiques sur l'algèbre des invariants sur les graphes à 5 sommets

			produit usuel			produit de chaînes		
arêtes	graphes	multigraphes	sec.	sec. irréd.	gén. min.	sec.	sec. irréd.	gén. min.
0	1	1	1	0	0	1	0	0
1	1	1	0	0	1	0	0	1
2	2	3	0	0	2	1	?	?
3	5	8	3	3	5	4	?	?
4	9	21	8	8	10	10	?	?
5	15	52	19	19	21	24	?	?
6	21	132	45	39	41	60	?	?
7	24	313	97	73	74	133	?	?
8	24	741	213	120	121	305	?	?
9	21	1 684	440	161	162	654	?	?
10	15	3 711	858	?	?	1 346	?	?
11	9	7 895	1 590	?	?	2 653	?	?
12	5	16 310	2 834	?	?	5 068	?	?
13	2	32 604	4 794	?	?	9 271	?	?
14	1	63 363	7 784	?	?	16 443	?	?
15	1	119 745	12 157	?	?	28 221	?	?
16	0	220 546	18 244	?	?	46 996	?	?
17	0	396 428	26 422	?	?	76 104	?	?
18	0	696 750	37 002	?	?	120 137	?	?
19	0	1 198 812	50 142	?	?	184 979	?	?
20	0	2 022 503	65 905	?	?	278 513	?	?
21	0	3 349 574	84 095	?	?	410 392	?	?
22	0	5 452 496	104 277	?	?	592 669	?	?
23	0	8 732 932	125 830	?	?	839 756	?	?
24	0	13 776 366	147 862	?	?	1 168 725	?	?
25	0	21 423 968	169 274	?	?	1 598 808	?	?
26	0	32 872 642	188 932	?	?	2 151 996	?	?
27	0	49 804 323	205 729	?	?	2 851 901	?	?
28	0	74 560 913	218 549	?	?	3 723 698	?	?
29	0	110 369 469	226 608	?	?	4 793 155	?	?
30	0	161 639 227	229 372	?	?	6 085 985	?	?

TAB. A.4 – Statistiques sur l'algèbre des invariants sur les graphes à 6 sommets

			produit usuel			produit de chaînes		
arêtes	graphes	multigraphes	sec.	sec. irréd.	gén. min.	sec.	sec. irréd.	gén. min.
0	1	1	1	0	0	1	0	0
1	1	1	0	0	1	0	0	1
2	2	3	0	0	2	1	?	?
3	5	8	3	3	5	4	?	?
4	10	22	9	9	11	11	?	?
5	21	60	26	26	28	31	?	?
6	41	173	76	70	72	92	?	?
7	65	471	197	170	172	242	?	?
8	97	1 303	536	413	414	668	?	?
9	131	3 510	1 399	?	?	1 761	?	?
10	148	9 234	3 494	?	?	4 489	?	?
11	148	23 574	8 375	?	?	11 025	?	?
12	131	58 464	19 328	?	?	26 186	?	?
13	97	140 340	42 680	?	?	59 777	?	?
14	65	326 792	90 761	?	?	131 966	?	?
15	41	738 090	185 853	?	?	281 486	?	?
16	21	1 619 321	367 213	?	?	581 500	?	?
17	10	3 455 129	701 621	?	?	1 165 353	?	?
18	5	7 180 856	1 299 107	?	?	2 270 139	?	?
19	2	14 555 856	2 334 525	?	?	4 304 634	?	?
20	1	28 819 926	4 079 931	?	?	7 960 281	?	?
21	1	55 808 840	6 944 813	?	?	14 375 488	?	?
22	0	105 834 657	11 531 367	?	?	25 389 407	?	?
23	0	196 779 279	18 703 466	?	?	43 911 084	?	?
24	0	359 124 362	29 671 980	?	?	74 459 442	?	?
25	0	643 976 482	46 094 069	?	?	123 924 063	?	?
26	0	1 135 731 758	70 193 957	?	?	202 645 284	?	?
27	0	1 971 734 302	104 889 612	?	?	325 884 200	?	?
28	0	3 372 477 533	153 934 933	?	?	515 840 247	?	?
29	0	5 687 370 342	222 062 542	?	?	804 336 466	?	?
30	0	9 463 392 974	315 123 121	?	?	1 236 384 289	?	?

TAB. A.5 – Statistiques sur l'algèbre des invariants sur les graphes à 7 sommets

			produit usuel			produit de chaînes		
arêtes	graphes	multigraphes	sec.	sec. irréd.	gén. min.	sec.	sec. irréd.	gén. min.
0	1	1	1	0	0	1	0	0
1	1	1	0	0	1	0	0	1
2	2	3	0	0	2	1	?	?
3	5	8	3	?	?	4	?	?
4	11	23	10	?	?	12	?	?
5	24	64	29	?	?	34	?	?
6	56	197	94	?	?	111	?	?
7	115	588	282	?	?	331	?	?
8	221	1 806	874	?	?	1 030	?	?
9	402	5 509	2 668	?	?	3 141	?	?
10	663	16 677	7 969	?	?	9 434	?	?
11	980	49 505	23 056	?	?	27 539	?	?
12	1 312	143 761	64 680	?	?	78 230	?	?
13	1 557	406 091	174 889	?	?	214 827	?	?
14	1 646	1 114 890	456 464	?	?	571 132	?	?
15	1 557	2 970 964	1 149 515	?	?	1 468 457	?	?
16	1 312	7 685 972	2 795 984	?	?	3 655 108	?	?
17	980	19 311 709	6 576 066	?	?	8 815 144	?	?
18	663	47 170 674	14 979 117	?	?	20 628 384	?	?
19	402	112 123 118	33 091 351	?	?	46 898 775	?	?
20	221	259 662 333	71 013 194	?	?	103 743 726	?	?
21	115	586 583 731	148 251 796	?	?	223 593 436	?	?
22	56	1 294 143 065	301 525 768	?	?	470 162 410	?	?
23	24	2 791 716 176	598 276 014	?	?	965 794 716	?	?
24	11	5 895 027 869	1 159 555 108	?	?	1 940 454 188	?	?
25	5	12 198 014 683	2 197 930 824	?	?	3 817 680 885	?	?
26	2	24 758 285 639	4 079 050 631	?	?	7 362 785 565	?	?
27	1	49 339 306 519	7 419 618 766	?	?	13 933 696 935	?	?
28	1	96 626 207 776	13 240 566 720	?	?	25 898 823 662	?	?
29	0	186 118 717 992	23 202 229 936	?	?	47 321 948 629	?	?
30	0	352 873 805 078	39 959 534 441	?	?	85 068 470 361	?	?

TAB. A.6 – Statistiques sur l'algèbre des invariants sur les graphes à 8 sommets

			produit usuel			produit de chaînes		
arêtes	graphes	multigraphes	sec.	sec. irréd.	gén. min.	sec.	sec. irréd.	gén. min.
0	1	1	1	0	0	1	0	0
1	1	1	0	0	0	0	0	1
2	2	3	0	0	0	1	?	?
3	5	8	3	?	?	4	?	?
4	11	23	10	?	?	12	?	?
5	25	65	30	?	?	35	?	?
6	63	206	102	?	?	119	?	?
7	148	645	328	?	?	378	?	?
8	345	2 121	1 114	?	?	1 279	?	?
9	771	7 042	3 772	?	?	4 302	?	?
10	1 637	23 615	12 756	?	?	14 525	?	?
11	3 252	78 845	42 477	?	?	48 417	?	?
12	5 995	260 526	138 722	?	?	158 775	?	?
13	10 120	844 911	440 797	?	?	507 866	?	?
14	15 615	2 679 422	1 360 514	?	?	1 581 669	?	?
15	21 933	8 280 672	4 068 874	?	?	4 782 066	?	?
16	27 987	24 900 625	11 784 342	?	?	14 026 394	?	?
17	32 403	72 797 692	33 049 942	?	?	39 900 468	?	?
18	34 040	206 906 004	89 811 583	?	?	110 131 229	?	?
19	32 403	571 913 238	236 672 534	?	?	295 148 822	?	?
20	27 987	1 538 467 541	605 465 553	?	?	768 771 696	?	?
21	21 933	4 031 036 974	1 505 420 147	?	?	1 948 228 994	?	?
22	15 615	10 297 548 027	3 642 323 428	?	?	4 809 097 617	?	?
23	10 120	25 672 985 025	8 585 671 228	?	?	11 576 125 688	?	?
24	5 995	62 529 921 261	19 740 526 222	?	?	27 203 831 574	?	?
25	3 252	148 938 107 490	44 322 724 592	?	?	62 479 706 231	?	?
26	1 637	347 261 349 130	97 286 231 187	?	?	140 393 512 348	?	?
27	771	793 322 686 367	208 969 695 127	?	?	308 950 704 183	?	?
28	345	1 777 372 222 672	439 691 574 207	?	?	666 466 463 847	?	?
29	148	3 908 544 447 069	907 084 055 778	?	?	1 410 601 530 857	?	?
30	63	8 443 326 985 730	1 836 368 666 381	?	?	2 931 806 223 972	?	?

TAB. A.7 – Statistiques sur l'algèbre des invariants sur les graphes à 9 sommets

			produit usuel			produit de chaînes		
arêtes	graphes	multigraphes	sec.	sec. irréd.	gén. min.	sec.	sec. irréd.	gén. min.
0	1	1	1	0	0	1	0	0
1	1	1	0	0	0	0	0	0
2	2	3	0	0	0	1	?	?
3	5	8	3	?	?	4	?	?
4	11	23	10	?	?	12	?	?
5	26	66	31	?	?	36	?	?
6	66	210	105	?	?	122	?	?
7	165	671	348	?	?	399	?	?
8	428	2 283	1 242	?	?	1 411	?	?
9	1 103	7 964	4 481	?	?	5 036	?	?
10	2 769	28 494	16 395	?	?	18 321	?	?
11	6 759	103 220	60 168	?	?	66 995	?	?
12	15 772	375 543	219 851	?	?	244 565	?	?
13	34 663	1 358 128	791 681	?	?	881 857	?	?
14	71 318	4 851 060	2 796 717	?	?	3 126 021	?	?
15	136 433	17 015 285	9 645 441	?	?	10 836 865	?	?
16	241 577	58 389 489	32 388 909	?	?	36 634 304	?	?
17	395 166	195 533 148	105 713 036	?	?	120 532 342	?	?
18	596 191	638 081 578	335 115 535	?	?	385 620 071	?	?
19	828 728	2 027 677 587	1 031 623 309	?	?	1 199 288 770	?	?
20	1 061 159	6 273 874 644	3 084 922 767	?	?	3 626 486 543	?	?
21	1 251 389	18 905 818 588	8 966 417 748	?	?	10 667 498 732	?	?
22	1 358 852	55 513 798 559	25 350 467 725	?	?	30 546 624 596	?	?
23	1 358 852	158 944 901 223	69 780 399 857	?	?	85 221 649 641	?	?
24	1 251 389	444 090 638 818	187 187 255 080	?	?	231 854 766 267	?	?
25	1 061 159	1 211 822 681 944	489 822 553 839	?	?	615 697 711 511	?	?
26	828 728	3 232 382 023 589	1 251 540 560 744	?	?	1 597 397 244 746	?	?
27	596 191	8 435 230 596 037	3 125 436 196 076	?	?	4 052 796 172 946	?	?
28	395 166	21 554 157 159 726	7 635 535 636 228	?	?	10 064 335 512 507	?	?
29	241 577	53 973 976 737 571	18 265 009 834 753	?	?	24 483 993 035 656	?	?
30	136 433	132 557 504 385 361	42 817 718 791 830	?	?	58 399 482 976 674	?	?

TAB. A.8 – Statistiques sur l'algèbre des invariants sur les graphes à 10 sommets

			produit usuel			produit de chaînes		
arêtes	graphes	multigraphes	sec.	sec. irréd.	gén. min.	sec.	sec. irréd.	gén. min.
0	1	1	1	0	0	1	0	0
1	1	0	0	0	1	0	0	1
2	3	0	?	?	?	?	?	?
3	8	3	?	?	?	?	?	?
4	23	10	?	?	?	?	?	?
5	66	31	?	?	?	?	?	?
6	211	106	?	?	?	?	?	?
7	680	356	?	?	?	?	?	?
8	2 347	1 295	?	?	?	?	?	?
9	8 392	4 827	?	?	?	?	?	?
10	31 153	18 499	?	?	?	?	?	?
11	118 662	72 106	?	?	?	?	?	?
12	460 621	284 261	?	?	?	?	?	?
13	1 802 421	1 120 642	?	?	?	?	?	?
14	7 053 679	4 388 899	?	?	?	?	?	?
15	27 396 123	16 958 963	?	?	?	?	?	?
16	104 991 688	64 339 399	?	?	?	?	?	?
17	395 243 518	238 776 414	?	?	?	?	?	?
18	1 457 002 920	864 753 689	?	?	?	?	?	?
19	5 248 431 818	3 051 527 870	?	?	?	?	?	?
20	18 451 338 205	10 484 038 916	?	?	?	?	?	?
21	63 267 199 041	35 060 174 058	?	?	?	?	?	?
22	211 546 181 264	114 137 779 036	?	?	?	?	?	?
23	689 877 613 525	361 863 517 031	?	?	?	?	?	?
24	2 195 041 381 401	1 117 914 965 031	?	?	?	?	?	?
25	6 817 846 303 141	3 367 595 543 685	?	?	?	?	?	?
26	20 685 162 738 521	9 899 367 122 108	?	?	?	?	?	?
27	61 344 769 628 932	28 419 503 469 233	?	?	?	?	?	?
28	177 957 673 667 963	79 744 067 043 342	?	?	?	?	?	?
29	505 353 870 932 825	218 878 652 050 646	?	?	?	?	?	?
30	1 405 829 417 329 895	588 133 719 494 113	?	?	?	?	?	?

TAB. A.9 – Statistiques sur l'algèbre des invariants sur les graphes à 11 sommets

			produit usuel			produit de chaînes		
arêtes	graphes	multigraphes	sec.	sec. irréd.	gén. min.	sec.	sec. irréd.	gén. min.
0	1	1	1	0	0	1	0	0
1	1	0	0	0	1	0	0	1
2	3	0	?	?	?	?	?	?
3	8	3	?	?	?	?	?	?
4	23	10	?	?	?	?	?	?
5	66	31	?	?	?	?	?	?
6	212	107	?	?	?	?	?	?
7	684	359	?	?	?	?	?	?
8	2 374	1 316	?	?	?	?	?	?
9	8 574	4 974	?	?	?	?	?	?
10	32 380	19 491	?	?	?	?	?	?
11	126 643	78 503	?	?	?	?	?	?
12	510 517	323 761	?	?	?	?	?	?
13	2 100 956	1 353 587	?	?	?	?	?	?
14	8 759 231	5 697 927	?	?	?	?	?	?
15	36 687 382	23 959 461	?	?	?	?	?	?
16	153 270 352	99 990 897	?	?	?	?	?	?
17	634 767 848	411 896 689	?	?	?	?	?	?
18	2 593 453 320	1 667 779 522	?	?	?	?	?	?
19	10 414 568 349	6 616 909 244	?	?	?	?	?	?
20	40 996 981 328	25 668 723 237	?	?	?	?	?	?
21	157 916 042 319	97 225 986 492	?	?	?	?	?	?
22	594 531 003 482	359 292 327 439	?	?	?	?	?	?
23	2 186 405 971 716	1 294 957 466 080	?	?	?	?	?	?
24	7 852 313 265 055	4 552 028 340 356	?	?	?	?	?	?
25	27 542 317 199 300	15 609 918 200 602	?	?	?	?	?	?
26	94 374 228 014 298	52 242 083 344 872	?	?	?	?	?	?
27	316 033 022 744 176	170 723 242 755 156	?	?	?	?	?	?
28	1 034 798 774 393 935	545 102 332 009 525	?	?	?	?	?	?
29	3 314 892 808 309 447	1 701 600 248 317 375	?	?	?	?	?	?
30	10 395 266 115 901 992	5 196 640 442 534 973	?	?	?	?	?	?

TAB. A.10 – Statistiques sur l'algèbre des invariants sur les graphes à 12 sommets

	$m_{n,d}$: Dimension de la composante homogène de degré d de l'algèbre des invariants sur n sommets (*i.e.* nombre de multigraphes non étiquetés à n sommets et d arêtes)																				
$n\backslash d$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	1	1	2	3																	
4	1	1	3	6	11	18	32														
5	1	1	3	7	17	35	76	149	291	539	974										
6	1	1	3	8	21	52	132	313	741	1684	3711	7895	16310	32604	63363	119745					
7	1	1	3	8	22	60	173	471	1303	3510	9234	23574	58464	140340	326792	738090	1619321	3455129	7180856	14555856	28819926
8	1	1	3	8	23	64	197	588	1806	5509	16677	49505	143761	406091	1114890	2970964	7685972	19311709	47170674	112123118	259662333
9	1	1	3	8	23	65	206	645	2121	7042	23615	78845	260526	844911	2679422	8280672	24900625	72797692	206906004	571913238	1538467541
10	1	1	3	8	23	66	210	671	2283	7964	28494	103220	375543	1358128	4851060	17015285	58389489	195533148	638081578	2027677587	6273874644
11	1	1	3	8	23	66	211	680	2347	8392	31153	118662	460621	1802421	7053679	27396123	104991688	395243518	1457002920	5248431818	18451338205
12	1	1	3	8	23	66	212	684	2374	8574	32380	126643	510517	2100956	8759231	36687382	153270352	634767848	2593453320	10414568349	40996981328
13	1	1	3	8	23	66	212	685	2383	8640	32862	130101	534585	2262738	9806336	43185448	191866801	854072028	3786041295	16628259281	72061201563
14	1	1	3	8	23	66	212	686	2387	8667	33051	131475	544733	2336972	10337474	46870463	216513479	1012472046	4762923216	22408475683	104895265170
15	1	1	3	8	23	66	212	686	2388	8676	33118	131977	548592	2366896	10568563	48625631	229504968	1105569954	5406307498	26687837080	132271197561
16	1	1	3	8	23	66	212	686	2389	8680	33145	132168	550025	2378128	10658921	49356177	235357470	1151511724	5757021559	29279157755	150754030065
17	1	1	3	8	23	66	212	686	2389	8681	33154	132235	550534	2382146	10691797	49631881	237690821	1171163995	5919927877	30597607768	161117575784
18	1	1	3	8	23	66	212	686	2389	8682	33158	132262	550726	2383599	10703477	49730320	238546300	1178706266	5986424739	31177136505	166067982291

	$f_{n,d}$: Majoration de la dimension de la composante homogène de degré d de la sous-algèbre des invariants algébriquement reconstructibles sur n sommets																				
3	1	1	1	1																	
4	1	1	3	6	13	24	49														
5	1	1	3	9	23	53	132	300	693	1556	3465										
6	1	1	3	8	25	66	184	473	1235	3125	7903	19665	48747	119488	291220	703873					
7	1	1	3	8	23	68	211	615	1793	5063	14094	38637	105192	284235	765170	2050791	5476151	14559495	38542503	101559848	266405628
8	1	1	3	8	23	64	208	659	2148	6820	21232	64418	191905	562195	1630385	4696321	13487841	38692508	110988456	318280722	911931816
9	1	1	3	8	23	66	208	672	2315	8043	27831	94388	313094	1013988	3216692	10027536	30857639	94146149	285995951	867982046	2638229159
10	1	1	3	8	23	66	212	679	2354	8481	31435	116773	429319	1546471	5445058	18727305	63029485	208146983	676870619	2176071351	6945618108
11	1	1	3	8	23	66	212	689	2389	8646	32786	128040	506713	1997445	7765830	29592619	110250886	401399245	1429561645	4989855949	17114930289
12	1	1	3	8	23	66	212	686	2398	8707	33157	131544	539854	2255709	9465419	39419043	161690096	650264482	2558505972	9842337554	37035819086
13	1	1	3	8	23	66	212	686	2387	8694	33220	132341	549168	2354652	10328023	45761910	202573892	888194378	3834762409	16244231053	67381727478
14	1	1	3	8	23	66	212	686	2389	8674	33162	132368	550960	2380063	10626275	48634982	225968278	1055116567	4908542291	22599804299	102499043791
15	1	1	3	8	23	66	212	686	2389	8682	33137	132213	550808	2384200	10697216	49542845	235520124	1140480638	5578060030	27332664416	133254612592
16	1	1	3	8	23	66	212	686	2389	8682	33166	132244	550668	2384126	10708860	49748733	238314598	1172198421	5886565136	29974758188	153663976288
17	1	1	3	8	23	66	212	686	2389	8682	33160	132299	550831	2384138	10709060	49779911	238909723	1180817144	5991610494	31079831538	163937847447
18	1	1	3	8	23	66	212	686	2389	8682	33160	132275	550897	2384582	10709842	49782124	238995702	1182549517	6018292920	31427227266	167867172493

	Majoration $f_{n,d}/m_{n,d}$ du rapport de ces deux dimensions																				
3	1	1	0,5	0,33																	
4	1	1	1	1	1,18	1,33	1,53														
5	1	1	1	1,29	1,35	1,51	1,74	2,01	2,38	2,89	3,56										
6	1	1	1	1	1,19	1,27	1,39	1,51	1,67	1,86	2,13	2,49	2,99	3,66	4,60	5,88					
7	1	1	1	1	1,05	1,13	1,22	1,31	1,38	1,44	1,53	1,64	1,80	2,03	2,34	2,78	3,38	4,21	5,37	6,98	9,24
8	1	1	1	1	1	1	1,06	1,12	1,19	1,24	1,27	1,30	1,33	1,38	1,46	1,58	1,75	2,00	2,35	2,84	3,51
9	1	1	1	1	1	1,02	1,01	1,04	1,09	1,14	1,18	1,20	1,20	1,20	1,20	1,21	1,24	1,29	1,38	1,52	1,71
10	1	1	1	1	1	1	1,01	1,01	1,03	1,06	1,10	1,13	1,14	1,14	1,12	1,10	1,08	1,06	1,06	1,07	1,11
11	1	1	1	1	1	1	1,00	1,01	1,02	1,03	1,05	1,08	1,10	1,11	1,10	1,08	1,05	1,02	0,98	0,95	0,93
12	1	1	1	1	1	1	1	1,00	1,01	1,02	1,02	1,04	1,06	1,07	1,08	1,07	1,05	1,02	0,99	0,95	0,90
13	1	1	1	1	1	1	1	1,00	1,00	1,01	1,01	1,02	1,03	1,04	1,05	1,06	1,06	1,04	1,01	0,98	0,94
14	1	1	1	1	1	1	1	1	1,00	1,00	1,00	1,01	1,01	1,02	1,03	1,04	1,04	1,04	1,03	1,01	0,98
15	1	1	1	1	1	1	1	1	1,00	1,00	1,00	1,00	1,00	1,01	1,01	1,02	1,03	1,03	1,03	1,02	1,01
16	1	1	1	1	1	1	1	1	1	1,00	1,00	1,00	1,00	1,00	1,00	1,01	1,01	1,02	1,02	1,02	1,02
17	1	1	1	1	1	1	1	1	1	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,01	1,01	1,01	1,02	1,02
18	1	1	1	1	1	1	1	1	1	1	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,01	1,01	1,01

TAB. A.11 – Comparaison de la dimension de l'algèbre des invariants et de sa sous-algèbre des polynômes alg. reconstructibles
Voir § 18.1. Noter que pour $n = 11$ et $d = 18$, le rapport est < 1.

	$g_{n,d}$: Dimension de la composante homogène de degré d de l'algèbre des graphes simples sur n sommets (*i.e.* nombre de graphes simples non étiquetés à n sommets et d arêtes)																				
$n\backslash d$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	1	1	1	1																	
4	1	1	2	3	2	1	1														
5	1	1	2	4	6	6	6	4	2												
6	1	1	2	5	9	15	21	24	24	21	15										
7	1	1	2	5	10	21	41	65	97	131	148	148									
8	1	1	2	5	11	24	56	115	221	402	663	980	1312	1557	1646						
9	1	1	2	5	11	25	63	148	345	771	1637	3252	5995	10120	15615	21933	27987				
10	1	1	2	5	11	26	66	165	428	1103	2769	6759	15772	34663	71318	136433	241577	395166	596191	828728	1061159
11	1	1	2	5	11	26	67	172	467	1305	3664	10250	28259	75415	192788	467807	1069890	2295898	4609179	8640134	15108047
12	1	1	2	5	11	26	68	175	485	1405	4191	12763	39243	119890	359307	1043774	2911086	7739601	19515361	46505609	104504341
13	1	1	2	5	11	26	68	176	492	1446	4435	14140	46415	154658	517121	1711908	5546619	17422984	52664857	152339952	420048805
14	1	1	2	5	11	26	68	177	495	1464	4541	14775	50159	175652	628635	2271860	8191607	29148848	101403945	342260293	1114246152
15	1	1	2	5	11	26	68	177	496	1471	4583	15036	51814	185987	691001	2632420	10176660	39500169	152374465	578891716	2149523582
16	1	1	2	5	11	26	68	177	497	1474	4601	15144	52496	190443	720298	2821116	11353457	46541024	192525021	796277250	3264731685
17	1	1	2	5	11	26	68	177	497	1475	4608	15186	52763	192218	732472	2905512	11932174	50411413	217511951	950868860	4177279665
18	1	1	2	5	11	26	68	177	497	1476	4611	15204	52872	192917	737248	2939612	12180208	52211412	230341716	1039651295	4769060224

	$f_{n,d}$: Majoration de la dimension de la composante homogène de degré d de la sous-algèbre des vecteurs algébriquement reconstructibles sur n sommets																				
3	1	1	1	1																	
4	1	1	2	3	4	5	7														
5	1	1	2	5	8	12	22	32	48												
6	1	1	2	5	11	20	38	66	119	206	353										
7	1	1	2	5	11	26	57	110	216	417	810	1552									
8	1	1	2	5	11	26	68	154	338	712	1469	3020	6294	13045	26938						
9	1	1	2	5	11	26	68	177	450	1083	2484	5490	12006	26200	57731	128180	285539				
10	1	1	2	5	11	26	68	177	497	1370	3615	9077	21887	51096	117558	269807	624552	1463813	3469611	8266510	19669186
11	1	1	2	5	11	26	68	177	497	1476	4378	12624	34957	92401	234840	578676	1398606	3357345	8100764	19807651	49245358
12	1	1	2	5	11	26	68	177	497	1476	4613	14665	46066	139872	407816	1140033	3065223	7974400	20250790	50737162	126912623
13	1	1	2	5	11	26	68	177	497	1476	4613	15216	51643	174908	579896	1859293	5734635	16991357	48433623	133315702	356495391
14	1	1	2	5	11	26	68	177	497	1476	4613	15216	52944	190208	690066	2476752	8675415	29416529	96142004	302337363	915070878
15	1	1	2	5	11	26	68	177	497	1476	4613	15216	52944	193367	732485	2823078	10870178	41229959	152553841	547156786	1895074029
16	1	1	2	5	11	26	68	177	497	1476	4613	15216	52944	193367	740226	2941200	11955415	48948506	199148817	796750703	3110820921
17	1	1	2	5	11	26	68	177	497	1476	4613	15216	52944	193367	740226	2960520	12286200	52341419	226029620	977410299	4188458391
18	1	1	2	5	11	26	68	177	497	1476	4613	15216	52944	193367	740226	2960520	12334829	53270888	236605397	1070147278	4877797578

	Majoration $f_{n,d}/g_{n,d}$ du rapport de ces deux dimensions																				
3	1	1	1	1																	
4	1	1	1	1	2,00	5,00	7,00														
5	1	1	1	1,25	1,33	2,00	3,67	8,00	24,00												
6	1	1	1	1	1,22	1,33	1,81	2,75	4,96	9,81	23,53										
7	1	1	1	1	1,10	1,24	1,39	1,69	2,23	3,18	5,47	10,49									
8	1	1	1	1	1	1,08	1,21	1,34	1,53	1,77	2,22	3,08	4,80	8,38	16,37						
9	1	1	1	1	1	1,04	1,08	1,20	1,30	1,40	1,52	1,69	2,00	2,59	3,70	5,84	10,20				
10	1	1	1	1	1	1	1,03	1,07	1,16	1,24	1,31	1,34	1,39	1,47	1,65	1,98	2,59	3,70	5,82	9,97	18,54
11	1	1	1	1	1	1	1,01	1,03	1,06	1,13	1,19	1,23	1,24	1,23	1,22	1,24	1,31	1,46	1,76	2,29	3,26
12	1	1	1	1	1	1	1	1,01	1,02	1,05	1,10	1,15	1,17	1,17	1,14	1,09	1,05	1,03	1,04	1,09	1,21
13	1	1	1	1	1	1	1	1,01	1,01	1,02	1,04	1,08	1,11	1,13	1,12	1,09	1,03	0,98	0,92	0,88	0,85
14	1	1	1	1	1	1	1	1	1,00	1,01	1,02	1,03	1,06	1,08	1,10	1,09	1,06	1,01	0,95	0,88	0,82
15	1	1	1	1	1	1	1	1	1,00	1,00	1,01	1,01	1,02	1,04	1,06	1,07	1,07	1,04	1,00	0,95	0,88
16	1	1	1	1	1	1	1	1	1	1,00	1,00	1,00	1,01	1,02	1,03	1,04	1,05	1,05	1,03	1,00	0,95
17	1	1	1	1	1	1	1	1	1	1,00	1,00	1,00	1,00	1,01	1,01	1,02	1,03	1,04	1,04	1,03	1,00
18	1	1	1	1	1	1	1	1	1	1	1,00	1,00	1,00	1,00	1,00	1,01	1,01	1,02	1,03	1,03	1,02

TAB. A.12 – Comparaison de la dimension de l'algèbre des graphes simples et de sa sous-algèbre des vecteurs alg. reconstructibles
Voir § 18.2. Noter que pour $n = 13$ et $d = 17$, le rapport est < 1.

A.2.1 Arbres et forêts

arêtes	nombre d'arbres	nombre de forêts
0	1	1
1	1	1
2	1	2
3	2	4
4	3	8
5	6	16
6	11	34
7	23	71
8	47	154
9	106	341
10	235	768
11	551	1 765
12	1 301	4 134
13	3 159	9 838
14	7 741	23 766
15	19 320	58 226
16	48 629	144 353
17	123 867	361 899
18	317 955	916 152
19	823 065	2 339 912
20	2 144 505	6 023 447
21	5 623 756	15 617 254
22	14 828 074	40 752 401
23	39 299 897	106 967 331
24	104 636 890	282 267 774
25	279 793 450	748 500 921
26	751 065 460	1 993 727 506
27	2 023 443 032	5 332 497 586
28	5 469 566 585	14 316 894 271
29	14 830 871 802	38 574 473 086
30	40 330 829 030	104 273 776 038
31	109 972 410 221	282 733 466 684
32	300 628 862 480	768 809 041 078
33	823 779 631 721	2 096 137 922 913
34	2 262 366 343 746	5 729 403 824 857
35	6 226 306 037 178	15 697 191 330 365
36	17 169 677 490 714	43 102 035 058 770
37	47 436 313 524 262	118 599 374 289 394
38	131 290 543 779 126	326 983 459 233 040
39	363 990 257 783 343	903 195 870 237 963
40	1 010 748 076 717 151	2 499 242 925 004 047
41	2 810 986 483 493 475	6 927 335 230 052 545
42	7 828 986 221 515 605	19 231 753 576 007 353
43	21 835 027 912 963 086	53 472 795 340 610 602
44	60 978 390 985 918 906	148 893 919 901 693 396
45	170 508 699 155 987 862	415 166 235 705 396 109
46	477 355 090 753 926 460	1 159 153 508 234 805 894
47	1 337 946 100 045 842 285	3 240 473 073 102 744 397
48	3 754 194 185 716 399 992	9 069 862 918 722 020 474
49	10 545 233 702 911 509 534	25 415 325 709 128 110 892
50	29 650 945 107 763 261 531	71 297 199 131 570 944 647
51	83 453 838 443 384 019 701	200 221 881 516 280 122 786
52	235 105 687 101 888 719 584	562 852 367 663 655 847 577
53	662 938 933 002 209 627 441	1 583 813 463 472 884 696 992
54	1 870 953 015 095 482 429 652	4 460 913 611 897 659 396 844
55	5 284 664 207 525 664 213 829	12 575 881 532 608 402 667 109
56	14 939 085 337 180 746 355 566	35 484 063 424 740 148 197 460
57	42 263 974 955 306 727 781 419	100 206 241 242 125 399 259 317
58	119 658 805 094 937 105 691 820	283 210 712 652 312 375 949 285
59	339 028 211 512 423 891 688 777	801 061 218 867 168 150 017 270
60	961 243 233 639 785 344 919 176	2 267 520 089 293 057 725 881 695
61	2 727 262 741 095 797 582 221 596	6 423 250 491 755 112 708 054 538
62	7 742 965 484 889 942 077 995 284	18 208 169 157 713 063 193 533 728
63	21 997 089 323 359 313 345 245 965	51 650 597 339 336 303 414 196 027
64	62 530 511 740 700 762 556 497 214	146 613 004 364 397 005 716 783 499
65	177 860 429 663 307 725 889 568 506	416 436 314 802 886 535 615 823 190
66	506 196 780 047 997 923 896 917 090	1 183 572 752 091 431 862 808 326 740
67	1 441 466 514 390 993 079 627 089 660	3 365 916 128 500 877 245 524 953 305
68	4 107 027 983 726 675 748 574 105 451	9 577 797 933 035 566 348 202 804 136
69	11 707 975 085 109 065 447 981 840 723	27 269 334 090 518 047 927 212 445 373
70	33 393 376 702 424 236 289 672 201 975	77 682 401 555 972 460 263 199 272 753

TAB. A.13 – Nombre de forêts, nombre d'arbres et rapport entre ces deux nombres, par nombre d d'arêtes, indépendamment du nombre de sommets

$n\backslash c$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0	0	0	0	0	0	0
3	1	1	1	0	0	0	0	0	0	0	0	0	0	0
4	2	2	1	1	0	0	0	0	0	0	0	0	0	0
5	3	3	2	1	1	0	0	0	0	0	0	0	0	0
6	6	6	4	2	1	1	0	0	0	0	0	0	0	0
7	11	11	7	4	2	1	1	0	0	0	0	0	0	0
8	23	23	14	8	4	2	1	1	0	0	0	0	0	0
9	47	46	29	15	8	4	2	1	1	0	0	0	0	0
10	106	99	60	32	16	8	4	2	1	1	0	0	0	0
11	235	216	128	66	33	16	8	4	2	1	1	0	0	0
12	551	488	284	143	69	34	16	8	4	2	1	1	0	0
13	1 301	1 121	636	315	149	70	34	16	8	4	2	1	1	0
14	3 159	2 644	1 467	710	330	152	71	34	16	8	4	2	1	1
15	7 741	6 334	3 440	1 631	742	336	153	71	34	16	8	4	2	1
16	19 320	15 437	8 225	3 829	1 707	757	339	154	71	34	16	8	4	2
17	48 629	38 132	19 944	9 126	3 999	1 739	763	340	154	71	34	16	8	4
18	123 867	95 368	49 102	22 103	9 531	4 076	1 754	766	341	154	71	34	16	8
19	317 955	241 029	122 253	54 275	23 047	9 703	4 108	1 760	767	341	154	71	34	16
20	823 065	614 968	307 880	134 896	56 545	23 458	9 780	4 123	1 763	768	341	154	71	34
21	2 144 505	1 582 030	782 560	338 950	140 352	57 505	23 631	9 812	4 129	1 764	768	341	154	71
22	5 623 756	4 100 157	2 006 552	859 963	352 313	142 665	57 918	23 708	9 827	4 132	1 765	768	341	154
23	$1,482 \cdot 10^7$	$1,069 \cdot 10^7$	5 183 685	2 200 799	892 863	357 880	143 631	58 091	23 740	9 833	4 133	1 765	768	341
24	$3,929 \cdot 10^7$	$2,807 \cdot 10^7$	$1,348 \cdot 10^7$	5 675 996	2 282 856	906 516	360 209	144 045	58 168	23 755	9 836	4 134	1 765	768
25	$1,046 \cdot 10^8$	$7,408 \cdot 10^7$	$3,529 \cdot 10^7$	$1,474 \cdot 10^7$	5 882 098	2 316 494	912 126	361 177	144 218	58 200	23 761	9 837	4 134	1 765
26	$2,797 \cdot 10^8$	$1,964 \cdot 10^8$	$9,290 \cdot 10^7$	$3,852 \cdot 10^7$	$1,526 \cdot 10^7$	5 966 051	2 330 258	914 461	361 591	144 295	58 215	23 764	9 838	4 134
27	$7,510 \cdot 10^8$	$5,233 \cdot 10^8$	$2,457 \cdot 10^8$	$1,012 \cdot 10^8$	$3,986 \cdot 10^7$	$1,547 \cdot 10^7$	5 999 979	2 335 884	915 430	361 764	144 327	58 221	23 765	9 838
28	$2,023 \cdot 10^9$	$1,400 \cdot 10^9$	$6,533 \cdot 10^8$	$2,675 \cdot 10^8$	$1,047 \cdot 10^8$	$4,039 \cdot 10^7$	$1,555 \cdot 10^7$	6 013 786	2 338 221	915 844	361 841	144 342	58 224	23 766
29	$5,469 \cdot 10^9$	$3,759 \cdot 10^9$	$1,744 \cdot 10^9$	$7,104 \cdot 10^8$	$2,764 \cdot 10^8$	$1,060 \cdot 10^8$	$4,060 \cdot 10^7$	$1,559 \cdot 10^7$	6 019 418	2 339 190	916 017	361 873	144 348	58 225
30	$1,483 \cdot 10^{10}$	$1,013 \cdot 10^{10}$	$4,674 \cdot 10^9$	$1,894 \cdot 10^9$	$7,335 \cdot 10^8$	$2,799 \cdot 10^8$	$1,066 \cdot 10^8$	$4,069 \cdot 10^7$	$1,560 \cdot 10^7$	6 021 756	2 339 604	916 094	361 888	144 351
31	$4,033 \cdot 10^{10}$	$2,739 \cdot 10^{10}$	$1,257 \cdot 10^{10}$	$5,071 \cdot 10^9$	$1,955 \cdot 10^9$	$7,426 \cdot 10^8$	$2,813 \cdot 10^8$	$1,068 \cdot 10^8$	$4,072 \cdot 10^7$	$1,561 \cdot 10^7$	6 022 725	2 339 777	916 126	361 894
32	$1,099 \cdot 10^{11}$	$7,428 \cdot 10^{10}$	$3,393 \cdot 10^{10}$	$1,363 \cdot 10^{10}$	$5,231 \cdot 10^9$	$1,978 \cdot 10^9$	$7,462 \cdot 10^8$	$2,819 \cdot 10^8$	$1,069 \cdot 10^8$	$4,074 \cdot 10^7$	$1,561 \cdot 10^7$	6 023 139	2 339 854	916 141
33	$3,006 \cdot 10^{11}$	$2,020 \cdot 10^{11}$	$9,189 \cdot 10^{10}$	$3,675 \cdot 10^{10}$	$1,405 \cdot 10^{10}$	$5,293 \cdot 10^9$	$1,987 \cdot 10^9$	$7,476 \cdot 10^8$	$2,821 \cdot 10^8$	$1,069 \cdot 10^8$	$4,074 \cdot 10^7$	$1,561 \cdot 10^7$	6 023 312	2 339 886
34	$8,237 \cdot 10^{11}$	$5,509 \cdot 10^{11}$	$2,495 \cdot 10^{11}$	$9,943 \cdot 10^{10}$	$3,787 \cdot 10^{10}$	$1,421 \cdot 10^{10}$	$5,317 \cdot 10^9$	$1,991 \cdot 10^9$	$7,481 \cdot 10^8$	$2,822 \cdot 10^8$	$1,069 \cdot 10^8$	$4,075 \cdot 10^7$	$1,561 \cdot 10^7$	6 023 389
35	$2,262 \cdot 10^{12}$	$1,506 \cdot 10^{12}$	$6,795 \cdot 10^{11}$	$2,698 \cdot 10^{11}$	$1,024 \cdot 10^{11}$	$3,830 \cdot 10^{10}$	$1,427 \cdot 10^{10}$	$5,326 \cdot 10^9$	$1,992 \cdot 10^9$	$7,483 \cdot 10^8$	$2,822 \cdot 10^8$	$1,069 \cdot 10^8$	$4,075 \cdot 10^7$	$1,561 \cdot 10^7$
36	$6,226 \cdot 10^{12}$	$4,127 \cdot 10^{12}$	$1,855 \cdot 10^{12}$	$7,342 \cdot 10^{11}$	$2,778 \cdot 10^{11}$	$1,035 \cdot 10^{11}$	$3,847 \cdot 10^{10}$	$1,430 \cdot 10^{10}$	$5,330 \cdot 10^9$	$1,993 \cdot 10^9$	$7,484 \cdot 10^8$	$2,822 \cdot 10^8$	$1,069 \cdot 10^8$	$4,075 \cdot 10^7$
37	$1,716 \cdot 10^{13}$	$1,133 \cdot 10^{13}$	$5,077 \cdot 10^{12}$	$2,003 \cdot 10^{12}$	$7,556 \cdot 10^{11}$	$2,808 \cdot 10^{11}$	$1,040 \cdot 10^{11}$	$3,853 \cdot 10^{10}$	$1,431 \cdot 10^{10}$	$5,331 \cdot 10^9$	$1,993 \cdot 10^9$	$7,484 \cdot 10^8$	$2,822 \cdot 10^8$	$1,069 \cdot 10^8$
38	$4,743 \cdot 10^{13}$	$3,119 \cdot 10^{13}$	$1,392 \cdot 10^{13}$	$5,478 \cdot 10^{12}$	$2,060 \cdot 10^{12}$	$7,638 \cdot 10^{11}$	$2,820 \cdot 10^{11}$	$1,041 \cdot 10^{11}$	$3,855 \cdot 10^{10}$	$1,431 \cdot 10^{10}$	$5,332 \cdot 10^9$	$1,993 \cdot 10^9$	$7,484 \cdot 10^8$	$2,822 \cdot 10^8$
39	$1,312 \cdot 10^{14}$	$8,602 \cdot 10^{13}$	$3,828 \cdot 10^{13}$	$1,501 \cdot 10^{13}$	$5,634 \cdot 10^{12}$	$2,082 \cdot 10^{12}$	$7,669 \cdot 10^{11}$	$2,824 \cdot 10^{11}$	$1,042 \cdot 10^{11}$	$3,856 \cdot 10^{10}$	$1,431 \cdot 10^{10}$	$5,332 \cdot 10^9$	$1,993 \cdot 10^9$	$7,484 \cdot 10^8$
40	$3,639 \cdot 10^{14}$	$2,376 \cdot 10^{14}$	$1,054 \cdot 10^{14}$	$4,125 \cdot 10^{13}$	$1,544 \cdot 10^{13}$	$5,694 \cdot 10^{12}$	$2,091 \cdot 10^{12}$	$7,681 \cdot 10^{11}$	$2,826 \cdot 10^{11}$	$1,042 \cdot 10^{11}$	$3,857 \cdot 10^{10}$	$1,431 \cdot 10^{10}$	$5,332 \cdot 10^9$	$1,993 \cdot 10^9$
41	$1,010 \cdot 10^{15}$	$6,577 \cdot 10^{14}$	$2,910 \cdot 10^{14}$	$1,135 \cdot 10^{14}$	$4,241 \cdot 10^{13}$	$1,560 \cdot 10^{13}$	$5,716 \cdot 10^{12}$	$2,094 \cdot 10^{12}$	$7,685 \cdot 10^{11}$	$2,826 \cdot 10^{11}$	$1,042 \cdot 10^{11}$	$3,857 \cdot 10^{10}$	$1,431 \cdot 10^{10}$	$5,332 \cdot 10^9$
42	$2,810 \cdot 10^{15}$	$1,823 \cdot 10^{15}$	$8,047 \cdot 10^{14}$	$3,133 \cdot 10^{14}$	$1,167 \cdot 10^{14}$	$4,284 \cdot 10^{13}$	$1,566 \cdot 10^{13}$	$5,724 \cdot 10^{12}$	$2,095 \cdot 10^{12}$	$7,687 \cdot 10^{11}$	$2,827 \cdot 10^{11}$	$1,042 \cdot 10^{11}$	$3,857 \cdot 10^{10}$	$1,431 \cdot 10^{10}$
43	$7,828 \cdot 10^{15}$	$5,062 \cdot 10^{15}$	$2,228 \cdot 10^{15}$	$8,658 \cdot 10^{14}$	$3,218 \cdot 10^{14}$	$1,179 \cdot 10^{14}$	$4,300 \cdot 10^{13}$	$1,568 \cdot 10^{13}$	$5,727 \cdot 10^{12}$	$2,095 \cdot 10^{12}$	$7,687 \cdot 10^{11}$	$2,827 \cdot 10^{11}$	$1,042 \cdot 10^{11}$	$3,857 \cdot 10^{10}$
44	$2,183 \cdot 10^{16}$	$1,407 \cdot 10^{16}$	$6,183 \cdot 10^{15}$	$2,396 \cdot 10^{15}$	$8,893 \cdot 10^{14}$	$3,250 \cdot 10^{14}$	$1,183 \cdot 10^{14}$	$4,306 \cdot 10^{13}$	$1,569 \cdot 10^{13}$	$5,728 \cdot 10^{12}$	$2,096 \cdot 10^{12}$	$7,687 \cdot 10^{11}$	$2,827 \cdot 10^{11}$	$1,042 \cdot 10^{11}$
45	$6,097 \cdot 10^{16}$	$3,920 \cdot 10^{16}$	$1,717 \cdot 10^{16}$	$6,646 \cdot 10^{15}$	$2,461 \cdot 10^{15}$	$8,980 \cdot 10^{14}$	$3,262 \cdot 10^{14}$	$1,185 \cdot 10^{14}$	$4,308 \cdot 10^{13}$	$1,569 \cdot 10^{13}$	$5,729 \cdot 10^{12}$	$2,096 \cdot 10^{12}$	$7,688 \cdot 10^{11}$	$2,827 \cdot 10^{11}$
46	$1,705 \cdot 10^{17}$	$1,093 \cdot 10^{17}$	$4,780 \cdot 10^{16}$	$1,845 \cdot 10^{16}$	$6,823 \cdot 10^{15}$	$2,485 \cdot 10^{15}$	$9,013 \cdot 10^{14}$	$3,267 \cdot 10^{14}$	$1,185 \cdot 10^{14}$	$4,309 \cdot 10^{13}$	$1,569 \cdot 10^{13}$	$5,729 \cdot 10^{12}$	$2,096 \cdot 10^{12}$	$7,688 \cdot 10^{11}$
47	$4,773 \cdot 10^{17}$	$3,053 \cdot 10^{17}$	$1,332 \cdot 10^{17}$	$5,133 \cdot 10^{16}$	$1,894 \cdot 10^{16}$	$6,889 \cdot 10^{15}$	$2,494 \cdot 10^{15}$	$9,024 \cdot 10^{14}$	$3,268 \cdot 10^{14}$	$1,185 \cdot 10^{14}$	$4,310 \cdot 10^{13}$	$1,569 \cdot 10^{13}$	$5,729 \cdot 10^{12}$	$2,096 \cdot 10^{12}$
48	$1,337 \cdot 10^{18}$	$8,537 \cdot 10^{17}$	$3,716 \cdot 10^{17}$	$1,430 \cdot 10^{17}$	$5,268 \cdot 10^{16}$	$1,912 \cdot 10^{16}$	$6,913 \cdot 10^{15}$	$2,497 \cdot 10^{15}$	$9,029 \cdot 10^{14}$	$3,269 \cdot 10^{14}$	$1,185 \cdot 10^{14}$	$4,310 \cdot 10^{13}$	$1,569 \cdot 10^{13}$	$5,729 \cdot 10^{12}$
49	$3,754 \cdot 10^{18}$	$2,389 \cdot 10^{18}$	$1,038 \cdot 10^{18}$	$3,988 \cdot 10^{17}$	$1,467 \cdot 10^{17}$	$5,318 \cdot 10^{16}$	$1,919 \cdot 10^{16}$	$6,922 \cdot 10^{15}$	$2,498 \cdot 10^{15}$	$9,031 \cdot 10^{14}$	$3,269 \cdot 10^{14}$	$1,185 \cdot 10^{14}$	$4,310 \cdot 10^{13}$	$1,569 \cdot 10^{13}$
50	$1,054 \cdot 10^{19}$	$6,697 \cdot 10^{18}$	$2,905 \cdot 10^{18}$	$1,113 \cdot 10^{18}$	$4,091 \cdot 10^{17}$	$1,481 \cdot 10^{17}$	$5,336 \cdot 10^{16}$	$1,921 \cdot 10^{16}$	$6,925 \cdot 10^{15}$	$2,498 \cdot 10^{15}$	$9,031 \cdot 10^{14}$	$3,269 \cdot 10^{14}$	$1,185 \cdot 10^{14}$	$4,310 \cdot 10^{13}$
51	$2,965 \cdot 10^{19}$	$1,879 \cdot 10^{19}$	$8,135 \cdot 10^{18}$	$3,115 \cdot 10^{18}$	$1,142 \cdot 10^{18}$	$4,129 \cdot 10^{17}$	$1,486 \cdot 10^{17}$	$5,343 \cdot 10^{16}$	$1,922 \cdot 10^{16}$	$6,926 \cdot 10^{15}$	$2,499 \cdot 10^{15}$	$9,031 \cdot 10^{14}$	$3,269 \cdot 10^{14}$	$1,185 \cdot 10^{14}$
52	$8,345 \cdot 10^{19}$	$5,277 \cdot 10^{19}$	$2,281 \cdot 10^{19}$	$8,721 \cdot 10^{18}$	$3,194 \cdot 10^{18}$	$1,153 \cdot 10^{18}$	$4,143 \cdot 10^{17}$	$1,487 \cdot 10^{17}$	$5,345 \cdot 10^{16}$	$1,922 \cdot 10^{16}$	$6,927 \cdot 10^{15}$	$2,499 \cdot 10^{15}$	$9,031 \cdot 10^{14}$	$3,269 \cdot 10^{14}$
53	$2,351 \cdot 10^{20}$	$1,483 \cdot 10^{20}$	$6,403 \cdot 10^{19}$	$2,444 \cdot 10^{19}$	$8,942 \cdot 10^{18}$	$3,223 \cdot 10^{18}$	$1,156 \cdot 10^{18}$	$4,148 \cdot 10^{17}$	$1,488 \cdot 10^{17}$	$5,346 \cdot 10^{16}$	$1,923 \cdot 10^{16}$	$6,927 \cdot 10^{15}$	$2,499 \cdot 10^{15}$	$9,031 \cdot 10^{14}$
54	$6,629 \cdot 10^{20}$	$4,175 \cdot 10^{20}$	$1,799 \cdot 10^{20}$	$6,859 \cdot 10^{19}$	$2,506 \cdot 10^{19}$	$9,023 \cdot 10^{18}$	$3,234 \cdot 10^{18}$	$1,158 \cdot 10^{18}$	$4,150 \cdot 10^{17}$	$1,488 \cdot 10^{17}$	$5,347 \cdot 10^{16}$	$1,923 \cdot 10^{16}$	$6,927 \cdot 10^{15}$	$2,499 \cdot 10^{15}$
55	$1,870 \cdot 10^{21}$	$1,176 \cdot 10^{21}$	$5,060 \cdot 10^{20}$	$1,926 \cdot 10^{20}$	$7,031 \cdot 10^{19}$	$2,528 \cdot 10^{19}$	$9,053 \cdot 10^{18}$	$3,238 \cdot 10^{18}$	$1,158 \cdot 10^{18}$	$4,151 \cdot 10^{17}$	$1,488 \cdot 10^{17}$	$5,347 \cdot 10^{16}$	$1,923 \cdot 10^{16}$	$6,927 \cdot 10^{15}$

TAB. A.14 – Nombre de forêts par nombre n de sommets et nombre c de composantes connexes

Annexe B

Liste des logiciels utilisés

Cette annexe liste les logiciels que nous avons essayé ou utilisé pour au cours de cette thèse. Elle donne pour chacun d'entre eux une description rapide, une adresse web, une référence, une indication sur le type de licence (libre : logiciel libre, sous licence GPL ou équivalente donnant accès aux sources ; gratuit : logiciel gratuit pour recherche et education ; payant : autres) et éventuellement quelques commentaires personnels (et donc parfaitement subjectifs). Nous avons essayé d'utiliser le plus possible de logiciel libres.

B.1 Calcul formel

`Maple` **[CGG+88]** Système de calcul formel généraliste (payant, `http://www.maplesoft.com/index.html`) jolie interface ; bien documenté ; bonne bibliothèque (combstruct, invar, ...). Mauvais support : les développeurs ne s'intéressent plus à l'utilisation par les chercheurs.

`MuPAD` **[The96]** Système de calcul formel généraliste (gratuit, `http://www.mupad.de`) : programmation orientée objet via le mechanisme de domaines, catégories et axiomes ; modules dynamiques en C++ ; très bon support de l'équipe des développeurs.

`Magma` **[CP96, BCP97]** Système de calcul formel généraliste (payant, `http://www.maths.usyd.edu.au:8000/u/magma/`) : efficace pour manipuler des polynômes (bases de gröbner, ...), bonne bibliothèque pour la géométrie algébrique (de résolutions libres, d'invariants).

`REDUCE` **[Hea95]** Système de calcul formel généraliste (payant, mais avec accès au sources, `http://www.rrz.uni-koeln.de/REDUCE/`).

`Singular` **[GPS98]** Système de calcul formel spécialisé en algèbre commutative, géométrie algébrique et théorie des singularités (libre, `http://www.mathematik.uni-kl.de/~zca/Singular/`) : il existe une interface avec `MuPAD`.

`GAP` **[GAP99]** Système de calcul formel specialisé en théorie des groupes et en algèbre discrète (GPL,`http://www-history.mcs.st-and.ac.uk/~gap/`) : seulement essayé.

`CoCoA` **[CNR]** Système de calcul formel spécialisé en algèbre commutative (gratuit, `http://cocoa.dima.unige.it/`) bibliothèque très efficace et abondante en

algèbre commutative.

`Macaulay` CAS spécialisé en géométrie algébrique et en algèbre commutative (`http://www-sop.inria.fr/safir/SAM/Macaulay/`) : seulement essayé. Mêmes qualités que `CoCoA`.

`GB` **[Fau99]** Logiciel de calcul de bases de Gröbner, avec entre autre une interface avec `MuPAD` (gratuit, `http://www-calfor.lip6.fr/~jcf/GB.html`) : il n'y a pas plus rapide, à part FGb[Fau99](`http://posso.lip6.fr/~jcf/FGb.html`). C'est vraiment dommage que ce ne soit pas du logiciel libre !

B.2 Théorie des invariants

`Invar` **[Kem93]** bibliothèque pour `Maple` de théorie des invariants (libre, fournie avec `Maple`) : Souffre de la lenteur et de certaines limitations de `Maple`.

`RngInvar` **[Kem96]** bibliothèque pour `Magma` de théorie des invariants (fournie avec `Magma`) : Très efficace. Dommage que `Magma` ne soit pas libre.

`FINVAR.LIB` **[Hey96]** bibliothèque pour `Singular` de théorie des invariants (libre, fournie avec `Singular`).

`FINVAR.LIB` **[Gat96]** bibliothèque pour `Maple` de théorie des invariants (libre, `http://www.zib.de/gatermann/symmetry.html#symmetry`) : non essayée. Inclus une réimplémentation efficace du calcul de bases de Gröbner en `Maple`.

B.3 Combinatoire

`ACE` **[Vei98]** Bibliothèque `Maple` de combinatoire algébrique (gratuit, `http://www-igm.univ-mlv.fr/~veigneau/HTML/ACE_PAGE.html`) : Incompatible avec la dernière version de `Maple`.

`muEC` **[Pro99]** Adaptation d'ACE pour `MuPAD`, utilisant la bibliothèque C `SYMMETRICA` [KKL] (`http://www.mathe2.uni-bayreuth.de/axel/symneu_engl.html`) pour les calculs intensifs (gratuit, `http://weyl.univ-mlv.fr/~muec/`).

`nauty` **[McK90]** Logiciel pour étudier les graphes à isomorphie près (génération, calcul de groupe d'automorphismes, etc.). (GPL, `http://cs.anu.edu.au/people/bdm/nauty/`) : inimaginablement rapide.

`combstruct` **[FZVC94, Zim94]** Bibliothèque `Maple` pour engendrer des structures combinatoires (GPL) : la seule raison pour laquelle nous continuons d'utiliser `Maple`.

B.4 Calcul numérique

`Scilab` Système de calcul numérique (GPL, `http://www-rocq.inria.fr/scilab/`). Utilisé pour le calcul du rang de quelques grosses matrices creuses.

`LiDIA` Bibliothèque `C++` de calcul en théorie des nombres (gratuit, `http://monkey.mcs.kent.edu/systems/LiDIA.html`) : Utilisation en projet pour le calcul de rang de nos grosses matrices creuses à coefficients entiers.

B.5 Rédaction du document

`graphlet` Logiciel de dessin de graphes (GPL/gratuit, `http://www.fmi.uni-passau.de/Graphlet/index.html`) : très complet, et les relations avec les développeurs sont agréables.

`VGJ` Logiciel de dessin de graphes (GPL, `http://www.eecs.tufts.edu/~mccreary/graph\_drawing.html`).

`xfig` Logiciel de dessin vectoriel (GPL, `http://www-epb.lbl.gov/xfig/`).

LaTeX, `pdfLaTeX`, `bibtex`, `xindy`, `metapost`, `xdvi`, `gs`, `gv` Système de production de documents (GPL, `http://www.loria.fr/cgi-bin/ctan-index`). Jugez vous-même du résultat.

`hevea` Convertisseur LaTeX → `HTML` (GPL, `http://para.inria.fr/~maranget/hevea/`).

B.6 Programmation

Perl Langage de programmation généraliste et de haut niveau. (GPL, http ://www.perl.org/) : très grande bibliothèque, programmation orienté objet, glanage de cellule, expressions rationnelles très puissantes, etc. Utilisé intensivement pour toutes les conversions de formats de fichiers, et plus généralement dès que `MuPAD` se révèle trop lent.

C/C++ Langage de programmation généraliste. Utilisé comme colle pour lier dynamiquement certains bouts de programmes externes avec `MuPAD`.

`CVS` Système de gestion de version de projets (GPL, `http://www.loria.fr/~molli/cvs-index.html`).

`emacs` Éditeur de texte et environnement de programmation (GPL, `http://www.emacs.org/`) : certainement mieux que vi :-)

`KDE` Environnement graphique (GPL, `http://www.kde.org`).

`Linux` Système d'exploitation (GPL, `http://www.linux.org/`).

Annexe C

The PerMuVAR library for MuPAD

C.1 Introduction

PerMuVAR is a set of libraries for computing inVARiants rings of PerMutations groups, using MuPAD and Perl. Here are some highlights of what this software can do: computations of Hilbert series, weighted Pólya enumeration, fast computation in the invariant ring, computation of secondary invariants and, up to some level, of minimal generating sets of polynomials; computations in the invariant ring using the chain product, and of the corresponding secondary invariants, etc. Those tools can be used, for example, to test if the ring of invariants is generated by some given set of invariants. Note that this software does not provide tools for computing primary invariants. By default it uses the elementary symmetric polynomials, but you can provide your own.

The part of PerMuVAR written in Perl is a tool for generating canonical representative of orbits of lists under the action of the group of permutation.

Why yet another invariant theory software ?

Softwares, written in Maple [Kem93], Magma [Kem96] or Singular already exists for computing invariants of finite groups. However, one of the drawback of those packages is that they use a preliminary Gröbner basis computation. This is really nice in small examples, since this allows a big speedup of the further computations. But, for bigger groups, if this preliminary stage fails (this happens quite often in my case) you don't get any information at all on your invariant ring. To be precise, the Invar package does not require this preliminary computation, but still fails because of some internal limitation of Maple. I needed some tool, maybe slower if not sluggish, but that would skip this preliminary stage and be at least able to give information on the homogeneous components of low degree of the invariant ring. This software only uses linear algebra methods, and its behavior is usually quite predictable. As a rule of thumb, it can compute a partial minimal generating set up to the degree d as long as the homogeneous components of degree less than d are of dimension less than one thousand. This can take some time and memory though. Quite often, this already shed interesting light on the structure of the invariant ring.

This software is also specialized in invariants rings on permutation groups. This is a critical property which, if well used, allows big speedups of computations, as

well as memory consumption shortage.

One other reason for this software is that `MuPAD`'s domains and categories mechanism allows object oriented programming. This makes it easy to split up the job in small parts, and to implement specialized versions of some of the routines for one's particular group of interest. Suppose for example that the sizes of the conjugacy classes of the group, as well as the cycle type of the permutations in those conjugacy classes, are known. One just have to redefine the `cycleType` method to have a much faster computation of the Hilbert series. This also allowed to put all the routines that are not particularly specialized for permutations groups in more general categories. Therefore, it should be possible to reuse part of this package for computations on other finite groups.

Finally, in the long term, `MuPAD`'s dynamic modules ability could allow to reimplement the critical parts of the algorithms in an external module in C or some other very fast language. One can expect a gain of an order of magnitude in both memory usage and time.

When to use this software

If you have a group action by permutation, that is too big for the other packages; if you still want information on the invariant ring even if you have to do some work for it, then this software is for you. If you can derive from the structure of your group, how to optimize time critical methods such as `canonic`, then this is even more for you.

C.2 Mathematical background

Let $x_1, \ldots, x_m$ be m variables, and $\mathbb{C}[x_1, \ldots, x_m]$ be the ring of polynomials in those variables. Let G be a subgroup of the symmetric group $\mathfrak{S}_m$, acting on the m variables by $\sigma.x_i := x_{\sigma(i)}$. This action extends naturally on all polynomials. We call a polynomial p *invariant* if for any permutation σ of the group $\sigma.p = p$. The set $\mathbb{C}[x_1, \ldots, x_m]^G$ of all the invariants polynomials is clearly stable by sum and product, and is called the *ring of invariants* of the group G. This ring is finitely generated, and one of the goal is to find systems of polynomials which generates it. Two kinds of such systems are of main interest: minimal systems of generators and generating systems composed of primary invariants and secondary invariants. There is a nice description of the algorithms for computing primary and secondary invariants in [Kem93] and [Kem98b]. See also the part II of this document.

Lets call *multivector* a vector $\mathbf{v} := (v_1, \ldots, v_m)$ of m non-negative integers. The group G acts on those vectors by permuting the v_i. The orbit $\overline{\mathbf{v}} := \{\sigma.\mathbf{v}, \sigma \in G\}$ of a multivector $\mathbf{v}$ is the set of multivectors obtained by letting G act on $\mathbf{v}$. Such a multivector can be identified with a monomial. Since the representation is by permutation, an invariant polynomial can be seen as a sum of orbits of such multivectors. The main originality of this software is to use this fact internally to store polynomials in an efficient manner. In my case, the size of the orbits can go up to a few thousands, so this really saves a lot to only store one canonical element for each orbit. This also saves time on the computation of the product of

two polynomials. Note that this relies heavily on the method canonic which returns a canonic representant of a multivector.

C.3 PerMuVAR's internals

C.3.1 Domains

`Dom::PermModule(Dimen, S, G)`
: This is the first domain you define. It contains methods to deal with vectors of Dimen elements of S under the action of the permutation group G. The group is described as a list of permutations. In a future release, it will be possible to only list generators of the group. Most of the time, you don't create a `Dom::PermModule` directly, but better define another domain which will inherit its method. Thus you can override time-critical methods by specialized versions.

`Dom::GraphModule` `Dom::DiGraphModule` `Dom::HyperGraphModule` `Dom::BipartiModule`
: Those are four such specializations of PermModule, for dealing respectively with graphs, digraphs, hypergraphs and bipartite graphs.

  There is a `Perl` interface with `Graphlet`, which allows to interactively input graphs into `MuPAD` by drawing them, and to view computed graphs. I did not use the `Network` library for this since it does not deal with labels on the edges, and stuff like this. Of course, I could have enhanced this library instead. But anyway, using `Graphlet` for input is great.

  One can work with subgroups of the group of permutations of the nodes of the graph. I used this for testing the i-reconstructibility of some polynomials (see the examples).

`Dom::InvariantAlgebra(R,S)`

  Here S is a permutation module as defined above. The resulting domain is the ring of invariants on the permutation module S. Its elements, which represent invariant polynomials are stored as described in 10.1.4.

  This domain has all the usual methods to deal with polynomials, which makes it a `Cat::FiniteMonoidRing`.

  It's possible to work in quotients of this algebra by defining an `iszero` method which decides if some orbit is in the ideal to be quotiented out. This was used for doing computations in the simple graph algebra and in the forest algebra (see § 12.2.1 and § 12.2.2).

  Note that this domain could have inherited a lot from `Dom::MonoidAlgebra`. However, for efficiency reasons, I had to use another internal structure. Indeed, elements are represented by tables instead of lists, which allows constant time access to the coefficient of a polynomial on some element of the basis.

C.3.2 Categories

`Cat::FiniteGroupModule`
: This is the very generic category of modules under the action of a finite group. It contains some default methods for computing canonical elements, computing Hilbert Series with Molien theorems, and such.

`Cat::PermutationGroupModule`
: The category of free modules under action of a finite permutation group. This provides methods for computing the Hilbert Series (basic or fine), the secondary invariants series (basic or fine), the cycle indicator polynomial, or for doing Pólya weighted enumeration. It provides default methods for the cycle types of the element of the group as well as primary invariants and their degrees. Finally it provides methods for exporting files for doing computations on the invariant ring with the other invariant packages (`Invar`, `FINVAR.LIB`, `RngInvar`).

C.3.3 Other libraries

`Secondary`
: Procedures for computing secondary invariants and minimal generating sets, either with usual or chain product are currently in external libraries. The reason for this is that it's really a pain to debug code in the modules, since you quite always have to do a complete reset of `MuPAD`'s kernel after any change.

`LinPol`
: This is a library for computations on homogeneous polynomials (or anything that looks like a homogeneous polynomial, see `Cat::FiniteMonoidRing`). Its main purpose is to check if some polynomial is in the algebra generated by some other list of polynomial, and if so to give the relationship. This is done using some kind of Gauss elimination.

`IsilPolynom`
: This library defines the domain `Dom::IsilPolynomial` which inherits from the usual `Dom::Polynomial`, but redefines the TEX generating method, for a nicer output.

C.4 Example

Here is a typical `MuPAD` session.

```
/* Load various libraries */
loadlib("DOMAIN/DiGrapheModule"):
loadlib("DOMAIN/InAlg"):
loadlib("IsilPolynom"):
loadlib("LinPol"):

/* The domain of digraphs on 3 nodes weighted in N */
```

```
G:=Dom::DiGrapheModule(Dom::Integer, 3):

/* The data base of graphs is in the graphdb/ subdirectory */
G::dataBase:="graphdb/":

/* Do quiet computations of canonical forms. */
setuserinfo(Any, 0);

/* The domain of invariant polynomial over G, with coefficients in Q */
In:=Dom::InvariantAlgebra(Dom::Rational, G):

/* Define a digraph, as a list representing the valuations of its
   edges. Here g is an arrow followed by a double arrow.
   It can also be drawn with graphlet by using g:=G::input(),
   and edited using g:=G::edit(g); */

g:=G([0, 1, 0, 0, 0, 2, 0, 0, 0]);

/* Put g in canonical form, and convert it into an invariant polynomial.
   Recall that this polynomial represents the sum of the monomials
   corresponding to g', where g' go through the orbit of g  */

p:=In(G::canonic(g));
/*      [0, 2, 0, 0, 0, 0, 1, 0, 0]                                    */

/* Just for fun, lets compute p^2 */

p^2;
/* [0, 4, 0, 0, 0, 0, 2, 0, 0] + 2·[0, 0, 2, 3, 0, 0, 0, 1, 0] +

   2·[0, 1, 2, 1, 0, 2, 0, 0, 0] + 2·[0, 2, 2, 1, 0, 0, 1, 0, 0] +

   2·[0, 2, 0, 2, 0, 0, 1, 1, 0]                                      */

/* Now we want to check if this polynomial is generated by simple
   digraphs. We first read from the database the list of all simple
   digraphs of degree less or equal to the degree of p, and convert
   them into polynomials. The graphs in my database are not
   necessarily in canonical form, so I have to put them in canonical
   form first.
*/

l:=_concat(map(G::allGraphs("digraphs.simple".(G::n)."-".(i)),In@G::canonic)
               $ hold(i)=1..degree(p)):

/* Construct a frozen copy of this list. */
```

```
lfreeze:=map(l,In::FreePoly):

/*  This allows to write the formal product of those polynomials,
    without expansion. This is a goody used for exporting the final
    result for LaTeX in a nice form. */

lfreeze[1]^2=l[1]^2;

/* Try to express p as sums and products of polynomials in l. */

res:=matrixLsolve(p, l);
/*                              FAIL                                  */

/* No, this is impossible */
```

C.5 Distribution

This software has been implemented for MuPAD 1.4. As the syntax for domains is going to change in MuPAD 1.5, it will need some translations. To avoid maintaining two parallel versions of this software, there will be no official release for MuPAD 1.4. Note that this is still experimental software. It works well for me, but the user interface is still minimal. Moreover, names of functions, domains and such are likely to change a lot, as well as the internal structure of the domains (see § C.7).

However, feel free to ask by e-mail (Nicolas.Thieryjonas.univ-lyon1.fr) a copy of it to the author. It will also be on my web page real soon ™:

http://www.lmd.univ-lyon1.fr/home/nthiery/

Finally, I will try to get this software included in the standard distribution of MuPAD 1.5. As usual, comments, bug reports, bug fixes and such are warmly welcomed.

C.6 Prerequisites

- Obviously you need MuPAD, version 1.4 right now, and 1.5 for the official release.
- One can speedup quite a lot PerMuVAR's computations of minimal generating sets by precomputing the orbits. I wrote a Perl package Math::GenGraph for this. It's specialized for the case of graphs, but a good part can be reused for other permutation groups.
- Graphlet is a graph drawing tool. It's only used for input and preview of graphs.
- LaTeXcan be used for viewing graphically the equations obtained with PerMuVAR.
- The Perl module Math::GML (same author) is used for the interface with Graphlet, and for drawing the little postscript pictures to be included by LaTeX.

C.7 To do

The computation of minimal generating set is a by-product of the computation of the secondary invariants. However, the result is currently not truly a minimal generating set, since `PerMuVAR` does not yet check if the primary invariants are really necessary or can be removed.

The documentation of all the methods is currently scattered through-out the code. I still have to extract it, and put it in the standard `MuPAD`'s help format.

The organization of the various module has to be cleaned up. For example a lot of code is shared between the various modules for graphs, digraphs or hypergraphs. They all should inherit from a common father.

As for now, `Perl` has to be called by hand for the precomputations of the orbits. `PerMuVAR` should call it automatically. I also have to define a basic generation procedure in `Perl` for the case where the group is only described as a list of permutations.

It would be great to have a `Perl` interpreter embedded as a dynamic module for `MuPAD`. This would make the calls to `Perl` really fast. I wrote a first hack in this direction, but it's still an unstable toy.

Some classical combinatorial functions are defined in an external library, called `isil-combinat`. Most of those are also defined in mu-EC, so it would be better to use the latter.

The use of an external fast sparse integer matrix library would probably speed up the computations by an order of magnitude.

The use of an external fast module in C/C++ for computing canonical forms of lists under the action of a permutation group would probably also speed up the computations by an order of magnitude, and save memory (no need to use remember table). `nauty` would be a good place to start writing this module.

Bibliographie

[AB95] Arnaudies et Bertin. – *Groupes, Algèbres et Géométrie, T. 2* . – ellipses, 1995.

[ACG96] Aslaksen (Helmer), Chan (Shih-Ping) et Gulliksen (Tor). – Invariants of S_4 and the shape of sets of vectors. *Appl. Algebra Engrg. Comm. Comput.*, vol. 7, n 1, 1996, pp. 53–57.

[And97] André (D.). – 1897.

[BCP97] Bosma (Wieb), Cannon (John) et Playoust (Catherine). – The Magma algebra system. I. The user language. *J. Symbolic Comput.*, vol. 24, n 3-4, 1997, pp. 235–265. – Computational algebra and number theory (London, 1993).

[Ber83] Berge (Claude). – *Graphes.* – Paris, Dunod, 1983, troisième édition, ix+400p.

[BGS82] Björner (A.), Garsia (A. M.) et Stanley (R. P.). – An introduction to Cohen-Macaulay partially ordered sets. *In : Ordered sets (Banff, Alta., 1981)*, pp. 583–615. – Dordrecht, Reidel, 1982.

[BH77] Bondy (J. A.) et Hemminger (R. L.). – Graph reconstruction—a survey. *J. Graph Theory*, vol. 1, n 3, 1977, pp. 227–268.

[BK92] Björner (Anders) et Karlander (Johan). – Invertibility of the base Radon transform of a matroid. *Discrete Math.*, vol. 108, n 1-3, 1992, pp. 139–147. – Topological, algebraical and combinatorial structures. Frolík's memorial volume.

[Bon91] Bondy (J. A.). – A graph reconstructor's manual. *In : Surveys in combinatorics, 1991 (Guildford, 1991)* , pp. 221–252. – Cambridge, Cambridge Univ. Press, 1991.

[Bri96] Brion (Michel). – Invariants et covariants des groupes réductifs. *In : École d'été de Théorie des Invariants, Monastir 1994* . CIMPA.

[Cam96] Cameron (Peter J.). – Stories from the age of reconstruction. *Congr. Numer.*, vol. 113, 1996, pp. 31–41. – Festschrift for C. St. J. A. Nash-Williams.

[CCRW85] Cameron (R. D.), Colbourn (C. J.), Read (R. C.) et Wormald (N. C.). – Cataloguing the graphs on 10 vertices. *J. Graph Theory*, vol. 9, n 4, 1985, pp. 551–562.

[CGG+88] Char (Bruce W.), Geddes (Keith O.), Gonnet (Gaston H.), Leong (Benton), Monagan (Michael B.) et Watt (Stephen M.). – *Maple Reference*

Manual. – 415 Philip St, Waterloo, Ontario N2L 3X2, Canada, WATCOM Publications Limited, 1988, fifth édition, xxvi + 403p.

[Che94] Chen (Dong Ling). – The linear point-arboricity of a graph. *Shandong Kuangye Xueyuan Xuebao*, vol. 13, n 1, 1994, pp. 92–95.

[CLO97] Cox (David), Little (John) et O'Shea (Donal). – *Ideals, varieties, and algorithms.* – New York, Springer-Verlag, 1997, second édition, xiv+536p. An introduction to computational algebraic geometry and commutative algebra.

[CNR] Capani (A.), Niesi (G.) et Robbiano (L.). – Cocoa, a system for doing computations in commutative algebra. Available via anonymous ftp from : cocoa.dima.unige.it.

[CP96] Cannon (John) et Playoust (Catherine). – MAGMA : a new computer algebra system. *Euromath Bull.*, vol. 2, n 1, 1996, pp. 113–144.

[Der99] Derksen (Harm). – Computation of invariants for reductive groups. *Adv. Math.*, vol. 141, n 2, 1999, pp. 366–384.

[Dix91] Dixmier (Jacques). – Sur les invariants du groupe symétrique dans certaines représentations. II. *In : Topics in invariant theory (Paris, 1989/1990)*, pp. 1–34. – Berlin, Springer, 1991.

[DK97] Derksen (Harm) et Kraft (Hanspeter). – Constructive invariant theory. *In : Algèbre non commutative, groupes quantiques et invariants (Reims, 1995)*, pp. 221–244. – Paris, Soc. Math. France, 1997.

[Eis95] Eisenbud (David). – *Commutative algebra*. – New York, Springer-Verlag, 1995, xvi+785p. With a view toward algebraic geometry.

[Esc97] Escofier (Jean-Pierre). – *Théorie de Galois*. – Paris, Masson, 1997, viii+248p. Cours avec exercices corrigés. [Course with exercises and solutions].

[Fau99] Faugère (Jean-Charles). – A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra*, vol. 139, n 1-3, 1999, pp. 61–88. – Effective methods in algebraic geometry (Saint-Malo, 1998).

[FH96] Fulton (William) et Harris (Joe). – *Representation theory*. – New York, Springer-Verlag, 1991 - 1996, *Graduate Texts in Mathematics*, volume 129, xvi+551p. A first course, Readings in Mathematics.

[FIKW94] Faradzev (I. A.), Ivanov (A. A.), Klin (M. H.) et Woldar (A. J.) (édité par). – *Investigations in algebraic theory of combinatorial objects* . – Dordrecht, Kluwer Academic Publishers Group, 1994, xii+510p.

[FR] Flajolet (Philippe) et Robert (Sedgewick). – Counting and generating functions. – In preparation.

[FZVC94] Flajolet (Philippe), Zimmermann (Paul) et Van Cutsem (Bernard). – A calculus for the random generation of labelled combinatorial structures. *Theoret. Comput. Sci.*, vol. 132, n 1-2, 1994, pp. 1–35.

[GAP99] The GAP Group, Aachen, St Andrews. – *GAP – Groups, Algorithms, and Programming, Version 4.1* , 1999.

[Gar80] Garsia (Adriano M.). – Combinatorial methods in the theory of Cohen-Macaulay rings. *Adv. in Math.*, vol. 38, n3, 1980, pp. 229–266.

[Gat96] Gatermann (Karin). – Semi-invariants, equivariants and algorithms. *Appl. Algebra Engrg. Comm. Comput.*, vol. 7, n2, 1996, pp. 105–124.

[GH94] Garsia (A. M.) et Hamain (M.). – *Orbit Harmonics and Graded Representations*. – Ucsd lecture notes, UCSD, 1994.

[GPS98] Greuel (G.-M.), Pfister (G.) et Schönemann (H.). – Singular version 1.2 User Manual . *In : Reports On Computer Algebra*. – Centre for Computer Algebra, University of Kaiserslautern, June 1998.

[Gri79] Grigoriev (D. Ju.). – Two reductions of the graph isomorphism to problems for polynomials. *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, vol. 88, 1979, pp. 56–61, 237–238. – Studies in constructive mathematics and mathematical logic, VIII.

[GS84] Garsia (A. M.) et Stanton (D.). – Group actions of Stanley - Reisner rings and invariants of permutation groups. *Adv. in Math.*, vol. 51, n2, 1984, pp. 107–201.

[Har83] Harary (Frank). – Maximum versus minimum invariants for graphs. *J. Graph Theory*, vol. 7, n3, 1983, pp. 275–284.

[Hea95] Hearn (Anthony C.). – *REDUCE User's Manual, Version 3.6*. – Report nCP 78, RAND, July 1995.

[Hey96] Heydtmann (A. E.). – *Generating Invariant Rings of Finite Groups* . – Thèse de PhD, Saabrücken, 1996.

[HP73] Harary (Frank) et Palmer (Edgar M.). – *Graphical enumeration*. – New York, Academic Press, 1973, xiv+271p.

[HR18] Hardy (G. H.) et Ramajuan (S.). – Asymptotic formulae in combinatory analysis. *Proc. London Math. Soc.*, vol. 17, n2, 1918, pp. 75–115.

[Kan72] Kantor (William M.). – On incidence matrices of finite projective and affine spaces. *Math. Z.*, vol. 124, 1972, pp. 315–318.

[Kel57] Kelly (Paul J.). – A congruence theorem for trees. *Pacific J. Math.*, vol. 7, 1957, pp. 961–968.

[Kem93] Kemper (Gregor). – *The* Invar *Package for Calculating Rings of Invariants*. – IWR Preprint n93-94, University of Heidelberg, 1993.

[Kem96] Kemper (Gregor). – Calculating invariant rings of finite groups over arbitrary fields. *J. Symbolic Comput.*, vol. 21, n3, 1996, pp. 351–366.

[Kem98a] Kemper (Gregor). – An algorithm to calculate optimal homogeneous systems of parameters. *J. Symbolic Comput.*, 1998.

[Kem98b] Kemper (Gregor). – Computational invariant theory. *Queen's Papers in Pure and Applied Math.*, février 1998.

[Ker91] Kerber (Adalbert). – *Algebraic combinatorics via finite group actions* . – Mannheim, Bibliographisches Institut, 1991, 436p.

[KKL] Kerber (Adalbert), Kohnert (Axel) et Lascoux (Alain). – SYMMETRICA, an object oriented computer-algebra system for the symmetric group.

[Knu69] Knuth (Donald E.). – *The art of computer programming. Vol. 1 : Fundamental algorithms*. – Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont, 1969, xxi+634p. Second printing.

[Koc82] Kocay (W. L.). – Some new methods in reconstruction theory. *In : Combinatorial mathematics, IX (Brisbane, 1981)* , pp. 89–114. – Berlin, Springer, 1982.

[Kun86] Kung (Joseph P. S.). – Radon transforms in combinatorics and lattice theory. *In : Combinatorics and ordered sets (Arcata, Calif., 1985)* , pp. 33–74. – Providence, R.I., Amer. Math. Soc., 1986.

[Lic76] Lick (Don R.). – The k-point-arboricity of a graph. *Colloq. Math.*, vol. 35, n 1, 1976, pp. 165–176.

[Lov72] Lovász (L.). – A note on the line reconstruction problem. *J. Combinatorial Theory Ser. B*, vol. 13, 1972, pp. 309–310.

[LW65] Livingstone (Donald) et Wagner (Ascher). – Transitivity of finite permutation groups on unordered sets. *Math. Z.*, vol. 90, 1965, pp. 393–403.

[LW74] Lick (Don R.) et White (Arthur T.). – Point partition numbers of complementary graphs. *Math. Japon.*, vol. 19, n 3, 1974, pp. 233–237.

[Mac91] Macdonald (I. G.). – Schubert polynomials. *In : Surveys in combinatorics, 1991 (Guildford, 1991)* , pp. 73–99. – Cambridge, Cambridge Univ. Press, 1991.

[McK90] McKay (Brendan D.). – *nauty User's Guide (version 1.5)* . – Rapport technique, Dept. Computer Science, Austral. Nat. Univ., 1990.

[McK97] McKay (Brendan D.). – Small graphs are reconstructible. *Australas. J. Combin.*, vol. 15, 1997, pp. 123–126.

[Mnu92] Mnukhin (V. B.). – The k-orbit reconstruction and the orbit algebra. *Acta Appl. Math.*, vol. 29, n 1-2, 1992, pp. 83–117. – Interactions between algebra and combinatorics.

[MS73] Mallows (C. L.) et Sloane (N. J. A.). – On the invariants of a linear group of order 336. *Proc. Cambridge Philos. Soc.*, vol. 74, 1973, pp. 435–440.

[Pou76] Pouzet (Maurice). – Application d'une propriété combinatoire des parties d'un ensemble aux groupes et aux relations. *Math. Z.*, vol. 150, n 2, 1976, pp. 117–134.

[Pou77] Pouzet (Maurice). – Quelques remarques sur les résultats de Tutte concernant le problème de Ulam. *Publ. Dép. Math. (Lyon)*, vol. 14, n 2, 1977, pp. 1–8.

[PR86] Pouzet (M.) et Rosenberg (I. G.). – Sperner properties for groups and relations. *European J. Combin.*, vol. 7, n 4, 1986, pp. 349–370.

[Pro99] Prosper (V.). – *Combinatoire des polynômes multivariés* . – Thèse de PhD, Université de Marne la Vallée, 1999.

[PT00] Pouzet (Maurice) et Thiéry (Nicolas M.). – Invariants algébriques de graphes. *Comptes Rendus de l'Académie des Sciences* , 2000. – In preparation.

[RC77] Read (Ronald C.) et Corneil (Derek G.). – The graph isomorphism disease. *J. Graph Theory*, vol. 1, n 4, 1977, pp. 339–363.

[Rea81] Read (Ronald C.). – A survey of graph generation techniques. *In : Combinatorial mathematics, VIII (Geelong, 1980)* , pp. 77–89. – Berlin, Springer, 1981.

[Rev84] Reverdy (F.). – *Représentation des graphes dans les espaces euclidiens et problèmes de représentation*. – Mémoire de dea, Université Claude Bernard, octobre 1984.

[Rob67] Robinson (G. de B.). – Note on a theorem of Livingstone and Wagner. *Math. Z.*, vol. 102, 1967, pp. 351–352.

[RS90] Robbiano (Lorenzo) et Sweedler (Moss). – Subalgebra bases. *In : Commutative algebra (Salvador, 1988)* , pp. 61–87. – Berlin, Springer, 1990.

[Sag91] Sagan (Bruce E.). – *The symmetric group*. – Pacific Grove, CA, Wadsworth & Brooks/Cole Advanced Books & Software, 1991, xviii+197p. Representations, combinatorial algorithms, and symmetric functions.

[Sch91] Schmid (Barbara J.). – Finite groups and invariant theory. *In : Topics in invariant theory (Paris, 1989/1990)* , pp. 35–66. – Berlin, Springer, 1991.

[Sch96] Schwarz (Gerald). – Topologie des quotients algébriques. *In : École d'été de Théorie des Invariants, Monastir 1994* . CIMPA.

[Smi97] Smith (Larry). – Polynomial invariants of finite groups. A survey of recent developments. *Bull. Amer. Math. Soc. (N.S.)* , vol. 34, n 3, 1997, pp. 211–250.

[Sou91] Soulié (Edgar). – Une permutation sur un ensemble dont le cardinal est un nombre triangulaire. *EDF Bull. Direction Études Rech. Sér. C Math. Inform.*, vol. 1991, n 2, 1991, pp. iii, 103–118.

[Sta79] Stanley (Richard P.). – Invariants of finite groups and their applications to combinatorics. *Bull. Amer. Math. Soc. (N.S.)* , vol. 1, n 3, 1979, pp. 475–511.

[Sta84] Stanley (Richard P.). – Quotients of Peck posets. *Order*, vol. 1, n 1, 1984, pp. 29–34.

[Stu93] Sturmfels (Bernd). – *Algorithms in invariant theory*. – Vienna, Springer-Verlag, 1993, vi+197p.

[Stu96] Sturmfels (Bernd). – *Gröbner bases and convex polytopes* . – Providence, RI, American Mathematical Society, 1996, xii+162p.

[SW86] Stanton (Dennis) et White (Dennis). – *Constructive combinatorics*. – New York, Springer-Verlag, 1986, *Undergraduate Texts in Mathematics* , x+183p.

[The96] The MuPAD Group, Benno Fuchssteiner et al. – *MuPAD User's Manual - MuPAD Version 1.2.2*. – John Wiley and sons, Chichester, New York, march 1996, first édition. includes a CD for Apple Macintosh and UNIX.

[Tut76] Tutte (W. T.). – *All the king's horse*. – Dept of Combinatorics and Optimization - Faculty of Math. University of Waterloo, Waterloo, Ontario, CANADA., preprint, 1976.

[Tut79] Tutte (W. T.). – All the king's horses. A guide to reconstruction. *In : Graph theory and related topics (Proc. Conf., Univ. Waterloo, Waterloo, Ont., 1977)*, pp. 15–33. – New York, Academic Press, 1979.

[Ula60] Ulam (S. M.). – *A collection of mathematical problems* . – Interscience Publishers, New York-London, 1960, xiii+150p. Interscience Tracts in Pure and Applied Mathematics, no. 8.

[VdW91] Van der Waerden (B. L.). – *Algebra. Vol. I*. – New York, Springer-Verlag, 1991, xiv+265p. Based in part on lectures by E. Artin and E. Noether, Translated from the seventh German edition by Fred Blum and John R. Schulenberger.

[Vei98] Veigneau (S.). – *ACE, an Algebraic Combinatorics Environment for the computer algebra system MAPLE : User's Reference Manual, Version 3.0*. – Report n 98–11, IGM, 1998.

[Wel76] Welsh (D. J. A.). – *Matroid theory*. – London, Academic Press [Harcourt Brace Jovanovich Publishers], 1976, xi+433p. L. M. S. Monographs, No. 8.

[Whi77] White (Neil L.). – The basis monomial ring of a matroid. *Advances in Math.*, vol. 24, n 3, 1977, pp. 292–297.

[Zim94] Zimmermann (Paul). – Gaia : A package for the random generation of combinatorial structures. *The Maple Technical Newsletter*, vol. 1, n 1, 1994.

[ZS75] Zariski (Oscar) et Samuel (Pierre). – *Commutative algebra. Vol. 1* . – New York, Springer-Verlag, 1975, xi+329p. With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28.

Index des notations

- $\mathbb{F}_q, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$: corps classiques ;
- $\mathbb{K}$: corps quelconque, de caractéristique 0 sauf mention explicite du contraire ;
- $\mathbf{K}, \mathbf{L}, \mathbf{N}$: corps, extension de ce corps, extension normale de ce corps ;
- $\oplus$, $\oplus^{\perp}$: Somme directe, somme directe orthogonale
- $S^{[n-1,1]}, [n-1,1]$: Représentation irréductible du groupe symétrique paramétrée par la partition $[n-1,1]$;
- S^{λ}, M^{λ} : Modules de Specht et de permutation paramétrés par la partition λ ;
- χ : Caractère d'une représentation ;
- $\mathbf{v} := (v_1, \ldots, v_n)$: vecteur ;
- $\mathrm{Etoile}^{i \to k}, \mathrm{Div}^{k \to i}$: Opérateurs étoile et dérivation ;
- $\mathbf{E}_i$: graphe simple en forme d'étoile centré sur i ;
- x_i : *variable* ;
- $\mathbf{x} := (x_1, \ldots, x_n)$: famille de variables ;
- $\langle \mathbf{v} | \mathbf{v}' \rangle$: Produit scalaire de $\mathbf{v}$ par $\mathbf{v}'$;
- $\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$, $\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle_{\mathbb{K}}$: Espace vectoriel ou module, $\mathbb{K}$-espace vectoriel engendré par les vecteurs $\mathbf{v}_i$;
- $\langle p_1, \ldots, p_n \rangle$, $\langle p_1, \ldots, p_n \rangle_{\mathbb{K}[\mathbf{x}]}$: Idéal, Idéal dans $\mathbb{K}[\mathbf{x}]$ engendré par les p_i ;
- $\mathbb{K}[p_1, \ldots, p_n]$: $\mathbb{K}$-Algèbre engendré par les p_i ;
- $\mathbb{K}[V]$: Algèbre des polynômes sur l'espace vectoriel V ;
- $\mathbb{K}[V]^G$: Algèbre des polynômes sur V invariants par le groupe G ;
- $\mathbb{K}[V]^G_{\chi}$: Composante isotypique dans $\mathbb{K}[V]$ d'un caractère irréductible χ de G ;
- $\mathbb{K}[\mathbf{x}_{\{i,j\}}]$: Algèbre des polynômes sur les graphes à n sommets ;
- $\mathcal{I}_n := \mathbb{K}[\mathbf{x}_{\{i,j\}}]^{\mathfrak{S}_n}$: Algèbre des invariants sur les graphes à n sommets ;
- $\mathcal{R}_n$: Algèbre des polynômes de $\mathcal{I}_n$ algébriquement reconstructibles ;
- $\mathbb{K}[\mathbf{x}_{(i,j)}]^{\mathfrak{S}_n}$: Algèbre des polynômes invariants sur les digraphes à n sommets ;
- $H(\mathcal{A}, z)$: Série de Hilbert de l'algèbre graduée $\mathcal{A}$;
- $\mathcal{A}_0, \mathcal{A}_1, \ldots$: Polynômes homogènes de degré 0, 1, ... de $\mathcal{A}$;
- $\mathcal{A}_+ := \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \ldots$: Polynômes sans constante de $\mathcal{A}$;
- $\mathcal{A}_{<d} := \sum_{d'<d} \mathcal{A}_{d'}$: Polynômes de degré strictement inférieur à d de $\mathcal{A}$;
- $\beta(\mathcal{A})$: Borne sur le degré des générateurs de l'algèbre graduée $\mathcal{A}$;
- $\beta(n)$: Borne sur le degré des générateurs de $\mathcal{I}_n$;
- $\theta_1, \ldots, \theta_m$: Invariants primaires ;
- $d_1, \ldots, d_m$: Degrés des invariants primaires ;
- $\eta_1, \ldots, \eta_t$: Invariants secondaires ;
- $\mathbf{e}_1, \ldots, \mathbf{e}_t$: Degrés des invariants secondaires ;
- μ : Plus petit degré d'un polynôme invariant relativement au caractère $\det^{-1}$.
- $o(x^2)$: négligeable devant x^2
- $O(x^2)$: d'ordre de grandeur au plus x^2

Index

Algebraic invariants of graphs and Reconstruction.
A study based on computer exploration.

Abstract :

This thesis presents a study of the ring $\mathcal{I}_n$ of algebraic invariants over weighted graphs on n vertices. This ring had only be completely described for $n \leq 4$, by Aslaksen et al.(1996). Using tools from invariant theory, and in particular effective methods, we obtain partial information on the structure of $\mathcal{I}_n$, for $n \geq 5$. To this end, we implemented `PerMuVAR`, a library of routines for `MuPAD`. Following Pouzet (1976), we use the ring $\mathcal{I}_n$ to define and study various algebraic versions of Ulam's reconstruction conjecture. We link our work with similar approaches (Kocay 1982, Cameron 1996). We look in detail at the algebraic reconstruction of trees, which is related to an unsolved problem raised by Kocay in 1982.

Keywords :

Graph Theory – Isomorphism of Graphs – Ulam's Reconstruction Conjecture – Invariant Theory – Representations of the Symmetric Group – Permutation Groups – Symbolic Computations – Computer Exploration.

Résumé :

Cette thèse présente une étude expérimentale de l'algèbre $\mathcal{I}_n$ des invariants polynômiaux sur les graphes valués à n sommets. Cette algèbre n'avait été entièrement décrite que pour $n \leq 4$ par Aslaksen et al.(1996). Nous utilisons les outils de la théorie des invariants, et en particulier de calculs effectifs, pour obtenir des informations partielles sur sa structure pour $n \geq 5$. À cet effet, nous avons conçu et implémenté une bibliothèque de fonctions, `PerMuVAR`. Comme résultats et conjectures issues de cette exploration, mentionnons un système générateur de $\mathcal{I}_5$ (formé d'un millier de polynômes de degré au plus 22), et un système générateur minimal partiel de $\mathcal{I}_5$ (formé de 57 polynômes de degré au plus 9) qui pourrait être générateur. Citons aussi une hypothèse sur un système de paramètres (vérifiée pour $n \leq 5$) et des contre-exemples à des hypothèses ou assertions sur la forme des générateurs.

L'algèbre $\mathcal{I}_n$ présente un intérêt en combinatoire. Pouzet (1976) avait introduit la sous-algèbre $\mathcal{R}_n$ des invariants de $\mathcal{I}_n$ algébriquement reconstructibles. L'égalité de $\mathcal{R}_n$ et de $\mathcal{I}_n$ entraîne la conjecture de reconstruction de Ulam pour les graphes valués à n sommets. Par un argument non constructif de dimension, nous montrons que $\mathcal{R}_n$ est une sous-algèbre stricte de $\mathcal{I}_n$, lorsque $11 \leq n \leq 18$ et vraisemblablement au delà. D'un autre côté, nous montrons que $\mathcal{R}_n$ est préservée par dérivation, fraction (sous certaines conditions) et passage au complémentaire, et contient de nombreux invariants classiques (nombre de cycles hamiltoniens, polynôme caractéristique, polynôme chromatique, « k-point partition numbers », etc.). Nous mettons en relation notre travail avec d'autres approches similaires (Kocay 1982, Cameron 1996). Enfin, nous étudions la reconstructibilité algébrique des arbres, variante d'un problème soulevé en 1982 par Kocay et toujours non résolu.

Discipline : Mathématiques et Informatique

Mots clefs :

Théorie des Graphes – Isomorphisme – Conjecture de Reconstruction de Ulam –
Théorie des Invariants – Représentations du Groupe Symétrique –
Groupes de Permutations – Calcul Formel – Recherche Expérimentale.

UFR de Mathématiques, Université Lyon I
Bâtiment 401 D / Bâtiment 101
43, boulevard du 11 Novembre 1918
69622 VILLEURBANNE Cedex