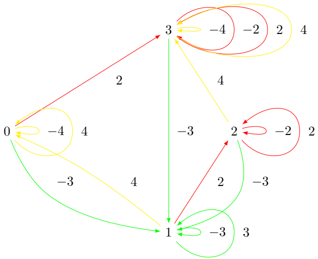
Computational representation theory of finite monoids & applications to Markov chains

Nicolas M. Thiéry

Laboratoire de Recherche en Informatique
Université Paris Sud 11

Combin'à Tour, July 4th 2013



Abstract

La théorie des représentations des groupes finis est un sujet classique. Dans le cadre plus général des monoïdes finis, la théorie est plus récente et a priori plus complexe. Cependant il existe des classes de monoïdes où, comme pour les groupes, la théorie se simplifie et fait surgir de la combinatoire, ce qui ouvre la porte à des applications.

Dans cet exposé, nous présentons brièvement les éléments de la théorie en mentionnant quelques développements algorithmiques récents (calcul de la matrice de Cartan), et décrirons une application typique à l'étude d'une chaîne de Markov sur des tas de sable à écoulement orienté (travail en commun avec Arvind Ayyer, Benjamin Steinberg, Anne Schilling). La démarche exploratoire sera illustrée par quelques calculs typiques avec le logiciel Sage.

Highlight of the talk

- Motivation : Markov chains and monoids
- Anatomy of monoids
- (Computational) representation theory of monoids
  In progress : Clifford, Munn, Ponizovskiĭ, Mc Alister, Putcha, Saliola, Steinberg, Margolis, Bergeron, Denton, Hivert, Schilling, T., . . .
- Algorithm for the Cartan invariants matrix

A first example : the Tsetlin library

Configuration : n books on a shelf
Operation T_i : move the i-th book to the right

A typical self-optimizing model for :

- Cache handling
- Prioritizing

Problem

- *Average behavior ?*
- *Convergence speed ?*

Controlling the behavior of the Tsetlin library ?

Markov chain description

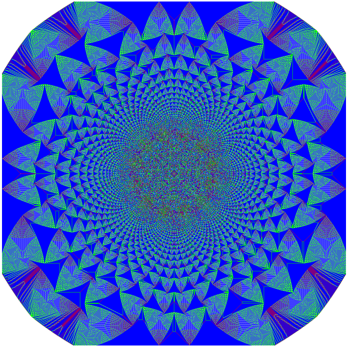
- Configuration space Ω : all permutations of the books
- Transition T_i : taking book i with probability x_i
- Stationary distribution ?
- Spectrum of the transition operator $x_1 T_1 + \cdots + x_n T_n$?

Theorem (Brown, Bidigare '99)

Each $S \subseteq \{1, \ldots, n\}$ contributes the eigenvalue $\sum_{i \in S} x_i$ with multiplicity the number of **derangements** *of S.*

Abelian sandpile models / chip-firing games

- A graph G
- Configuration : distribution of grains of sand at each site
- Grains fall in at random
- Grains topple to the neighbor sites
- Grains fall off at sinks

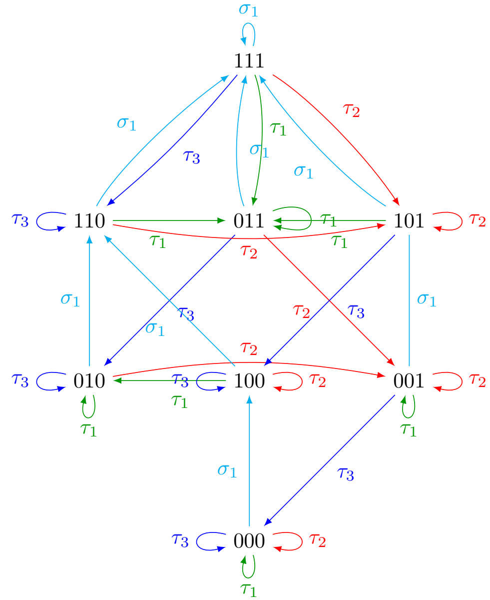


- Prototypical model for the phenomenon of self-organized criticality, like a heap of sand

Directed sandpile Models

- A tree, with edges pointing toward its root
- Configuration : distribution of grains of sand at each site
- Grains fall in at random (leaves only or everywhere)
- Grains topple down at random (one by one or all at once)
- Grains fall off at the sink (=root)
- System with reservoirs in nonequilibrium statistical physics

Directed sandpile model on a line with thresholds 1



Directed sandpile models are very nicely behaved

Proposition (Ayyer, Schilling, Steinberg, T. '13)

The transition graph is strongly connected
Equivalently the Markov chain is ergodic

Theorem (ASST'13)

Characteristic polynomial of the transition matrix :

$$\det(M_\tau - \lambda 1) = \prod_{S \subseteq V} (\lambda - (y_S + x_S))^{T_{S^c}},$$

where $S^c = V \setminus S$ *and* $T_S = \prod_{v \in S} T_v$

Theorem (ASST'13)

Mixing time : at most $\frac{2(n_T + c - 1)}{p}$

Punchline

Our models have exceptionally nice eigenvalues.

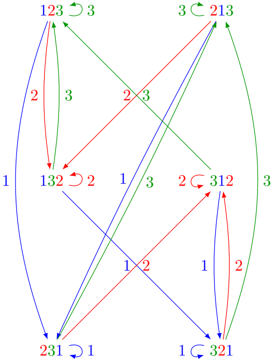
In fact many examples of Markov chains have similar behaviors :

- Promotion Markov chain
- Nonabelian directed sandpile models
- Toom models
- Walks on longest words of finite Coxeter groups
- Half-regular bands

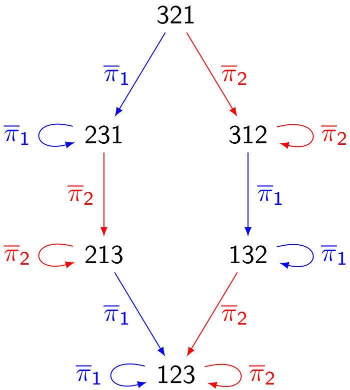
Is there some uniform explanation ?

Yes :representation theory !

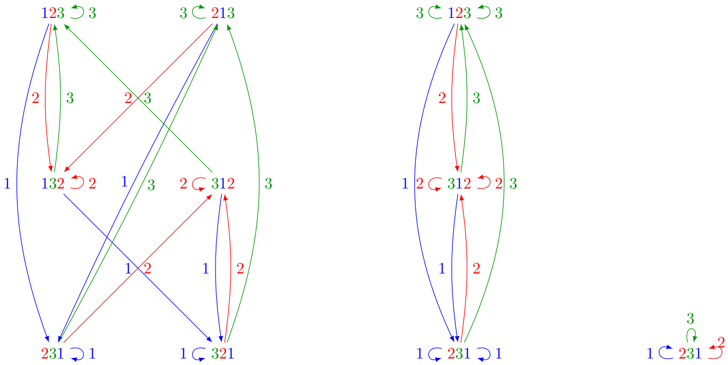
Approach 1 : decomposition of the configuration space (lumping)



Let's train on a simpler example



Approach 1 : decomposition of the configuration space (lumping)



Approach 2 : monoids and representation theory

Definition (Transition monoid of a Markov chain / automaton)

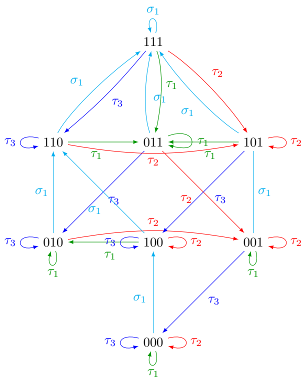
$m_i : \Omega \mapsto \Omega$ *transition operators* of the Markov chain

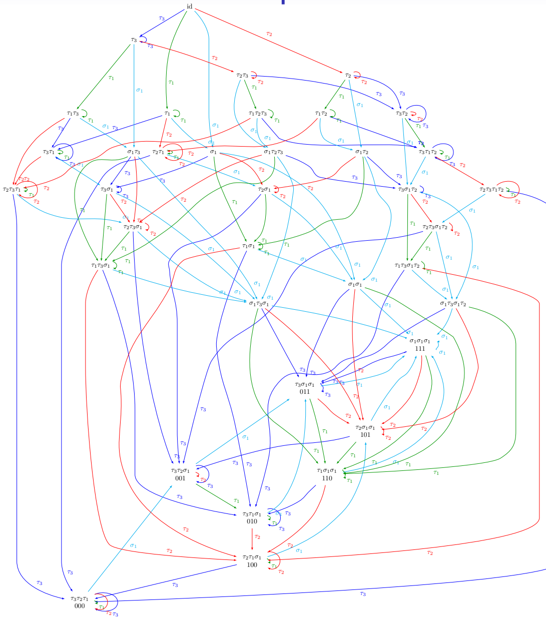
Monoid : $(\mathcal{M}, \circ) = \langle m_i \rangle$

a finite monoid of functions

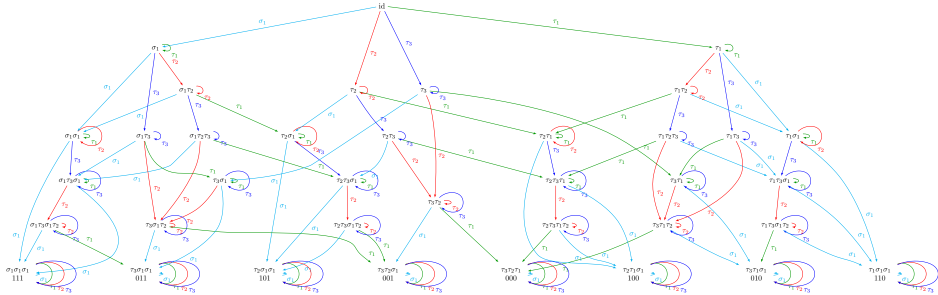
almost a permutation group

The left Cayley graph for the 1D sandpile model





The right Cayley graph for the 1D sandpile model



- This graph is acyclic : $\mathcal{R}$-triviality $\Longrightarrow$ Eigenvalues
- Not too deep

  $\Longrightarrow$ Bound on the rates of convergence / mixing time

Strategy

Method

- Show that $\mathcal{M}$ is *$\mathcal{R}$-trivial*
  $\Rightarrow$ the representation matrix are simultaneously triangularizable
- Eigenvalues indexed by a lattice of subsets of the generators
- Multiplicities from Möbius inversion on the lattice

Representation theory point of view

- Simple modules are of dimension 1
- Compute the character of a transformation module
  (counting fixed points)
- Recover the composition factors using the character table

Markov chains and Representation Theory

The idea of decomposing the configuration space is not new !

Using representation theory of groups

- Diaconis et al.
- Nice combinatorics (symmetric functions, ...)

Using representation theory of right regular bands

- Tsetlin library, Hyperplane arrangements, ...
- Bidigare, Hanlon, Rockmore '99, Brown '00, Saliola, ...
- Revived the interest for representation theory of monoids

Using representation of $\mathcal{R}$-trivial monoids ?

- Steinberg '06, ...
- Not semi-simple. But simple modules of dimension 1 !
- Nice combinatorics

Representation Theory

Algebraic structure A under study :

- A finite *monoid* $(M, *)$
- A finite *group* $(G, *)$
- A finite dimensional *algebra* $(A, +, ., *)$

Key questions

- How does A relate with other algebraic structures (morphisms) ?
- How to *represent* A using well known objects ? (transformations, permutations, matrices, ...)

Representation Theory

Search for “all” *representations* :

- $A \mapsto M_n(\mathbb{K})$ (linear action on a module V)

In practice

- Simple modules (no submodules)
- Indecomposable projective modules
- Morphisms between indecomposable projective modules (Cartan matrix)

Computational Representation Theory

Finite groups (characteristic zero)

- Simple modules $\Leftrightarrow$ conjugacy classes
- Complexity : $O(\log(|G|))$
- Main tool : strong generating sets, character theory

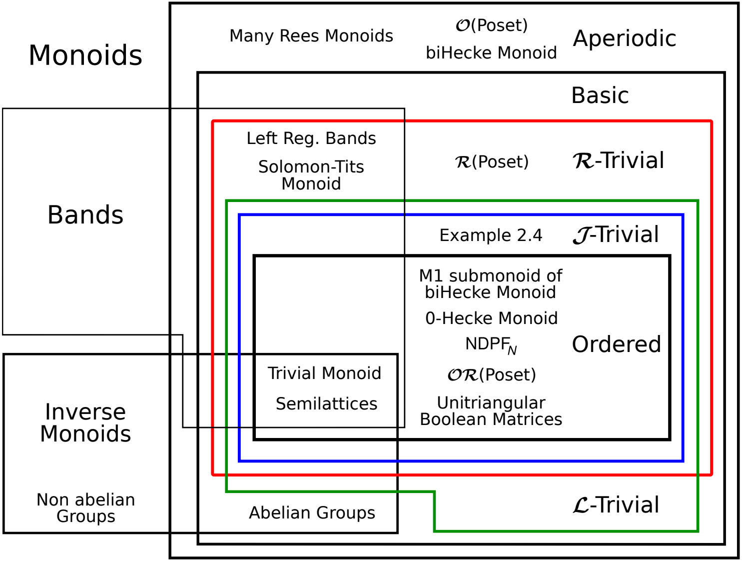
Finite dimensional algebras

- Complexity : $O(\dim A^3)$ (in practice : $\dim \leq 1000$)
- Main tools : linear algebra, minimal polynomial, ...

Finite dimensional commutative algebras

- Simple modules $\Leftrightarrow$ solutions of the polynomial system
- Main tools : Gröbner basis, RUR, ...

And for monoids ?



Another motivation

Many examples in algebraic combinatorics are monoid algebras

- 0-Hecke algebras (Norton, Carter, Krob-Thibon, Duchamp-Hivert-Thibon, Fayers, Denton)
- Non-decreasing parking function (Denton-Hivert-Schilling-T)
- Solomon-Tits algebras (Schocker, Saliola)
- Left Regular Bands (Brown, Saliola)
- . . .

Question

Can we take advantage of this fact ?

Running example : order preserving functions on the chain

Definition

$f : \{1, \ldots, n\} \longmapsto \{1, \ldots, n\}$ is *order preserving* if :

$$i \leq j \implies f(i) \leq f(j)$$

Example

The order preserving functions on $\{1 < 2 < 3\}$:

$$\{111, 112, 113, 122, 123, 133, 222, 223, 233, 333\}$$

Remark

If f, g are order preserving, then so is fg
Hence, the set $\mathcal{O}_n$ of such functions is a monoid !

This still works if $\leq$ is replaced by a partial order

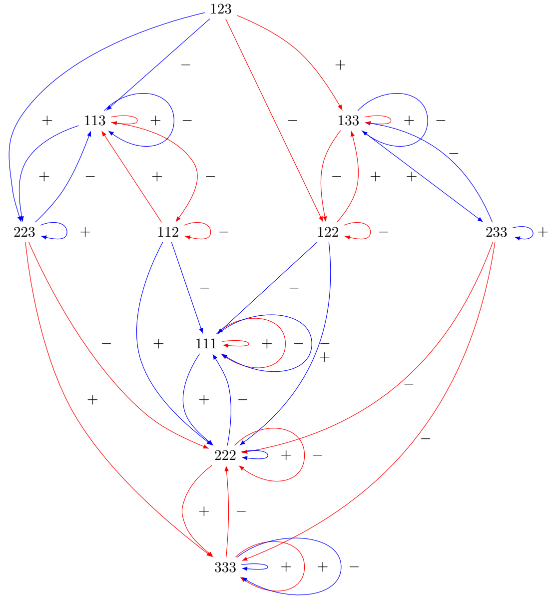
Understanding the multiplication ?

First approach : the multiplication table :

$*$	111	112	113	122	123	133	222	223	233	333
111	111	111	111	111	111	111	222	222	222	333
112	111	111	111	112	112	113	222	222	223	333
113	111	112	113	112	113	113	222	223	223	333
122	111	111	111	122	122	133	222	222	233	333
123	111	112	113	122	123	133	222	223	233	333
133	111	122	133	122	133	133	222	233	233	333
222	111	111	111	222	222	333	222	222	333	333
223	111	112	113	222	223	333	222	223	333	333
233	111	122	133	222	233	333	222	233	333	333
333	111	222	333	222	333	333	222	333	333	333

Complexity : $O(|M|^2)$

The right Cayley graph of $\mathcal{O}_3$



$\mathcal{R}$-preorder (Green 50)

Definition ($\mathcal{R}$-preorder)

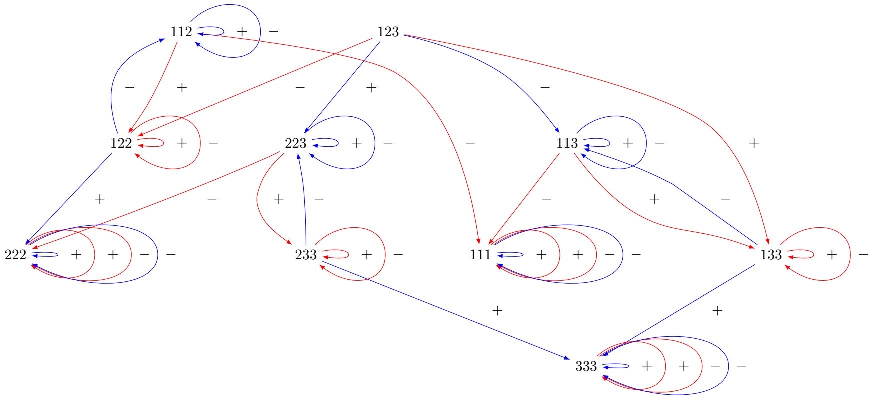
$$x \leq_R y \quad \text{if} \quad x \in yM$$

- *$\mathcal{R}$-class $\mathcal{R}(x)$* : strongly connected component
- *$\mathcal{R}$-order* on $\mathcal{R}$-classes
- *$\mathcal{R}$-trivial monoid* : all $\mathcal{R}$-classes are trivial

Algorithms

- Naive : $O(|M||G|)$ (strongly connected components in a graph)
- `Semigroupe` : roughly $O(|M|)$ (ideas similar to F5)
- `GAP+Monoid` : $\leq O(|M|)$ using group theory, when possible

The left Cayley graph of $\mathcal{O}_3$



$\mathcal{L}$-preorder, $\mathcal{L}$-classes, ...

Left-right Cayley graph, $\mathcal{J}$-preorder

Problem

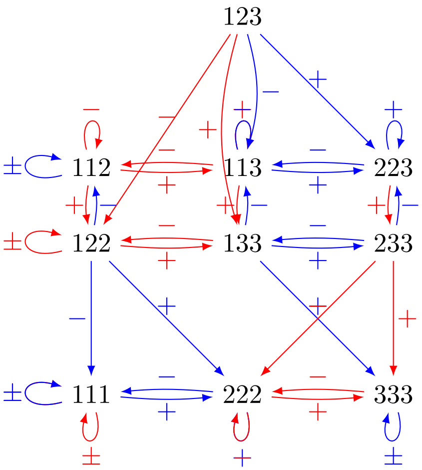
- *Why do we get several times the same module ?*
- *Can we exploit associativity ?*

Definition ($\mathcal{J}$-preorder)

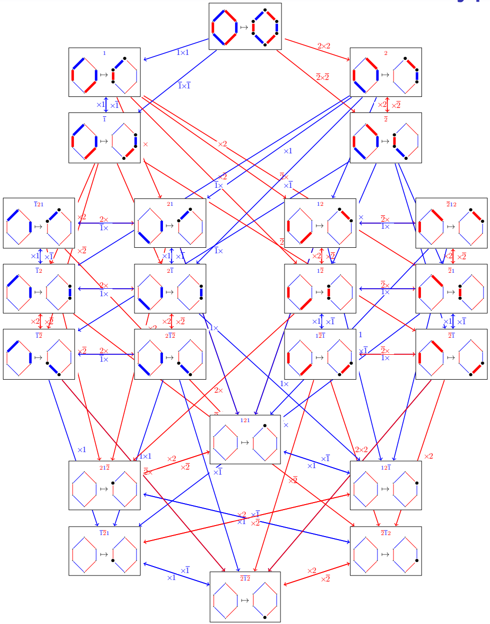
$$x \leq_J y \quad \text{if} \quad x \in MyM$$

- *Left-right Cayley graph*
- *$\mathcal{J}$-class*
- *$\mathcal{J}$-preorder*
- *$\mathcal{J}$-trivial*

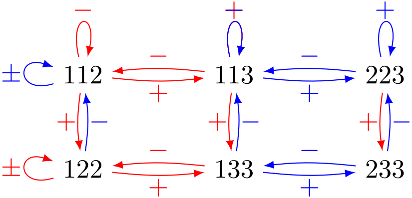
Example : the left-right Cayley graph for $\mathcal{O}3$



Example : the biHecke monoid for type A_2



The eggbox picture



Proposition

Let J be a $\mathcal{J}$-class. Then,

$$J \quad \approx_{M-\text{mod}-M} \quad L \times R$$

Definition (Eggbox matrix)

	$*$	$*$
$*$	$*$	

* : positions of idempotents ; completely encodes the product

Err, but groups are monoids, aren't they ?

- A group has a single $\mathcal{J}$-class !
- So far we have been only speaking about *aperiodic monoids*
- Example : the transformation monoid

$123^*, 132, 213$ $231, 312, 321$

$122^*, 211$	$121^*, 212$	$112, 221$
$133^*, 311$	$131, 313$	$113^*, 331$
$233, 322$	$232, 323^*$	$223^*, 332$

111^*	222^*	333^*

Zoology of monoids

- $\mathcal{L}$-trivial :

*	*	*	*	*	*

- $\mathcal{R}$-trivial :

*
*
*

- DA :

*	*	*	*	*	*
*	*	*	*	*	*
*	*	*	*	*	*

- $\mathcal{H}$-trivial / aperiodic :

*		*		*	
	*	*		*	*
*			*		*

Simple modules, Clifford, Munn, Ponizovskiĭ

Theorem (Aperiodic case)

Each regular $\mathcal{J}$-class contributes a simple module :

$$S_i := \operatorname{Top} \mathbb{K}R_i = \mathbb{K}R_i / \operatorname{rad}\mathbb{K}R_i$$

$\operatorname{rad}\mathbb{K}R_i$ *: kernel of the eggbox matrix*

Theorem (General case)

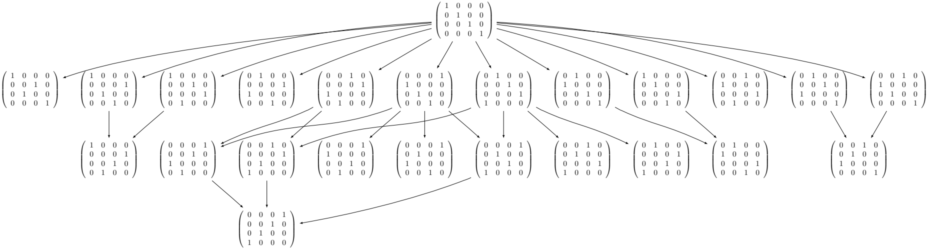
- *Take a $\mathcal{J}$-class and G_i its group*
- *Take a simple module $S^{G_i}_{i,j}$ of G_i*
- *Define $S_{i,j} := \operatorname{Top} S^{G_i}_{i,j} \uparrow^{M}_{G_i}$*
- *This construction gives each simple module of M exactly once*
- *In practice : decompose $\operatorname{Top} \mathbb{K}R_i$ as G_i-mod*

Simple modules for the biHecke Monoid

First non trivial aperiodic monoid admitting a combinatorial description of the (dimension) of the simple modules [Hivert, Schilling, T. '09]

Combinatorial ingredients

- Intervals in right order (for right classes)
- Möbius inversion along the cutting poset (for moding out the radical)



Monoids are not semi-simple !

- Groups (in char 0) are semi-simple
  (i.e. any module is a direct sum of simple modules)
- Monoids are not !
- Commutative algebras : are the roots simple ?

New players in the game

- Composition series : $\{0\} = V_0 \subset \cdots \subset V_\ell = V$
- Composition factors : V_{k+1}/V_k
  Refinement of strongly connected component
  Jordan Holder theorem
- Projective modules

Characters for monoids, Mc Alister 1972

Definition

- Character $\chi_V(x)$ of an element x acting on a module V : trace of the matrix of x acting on V
- Choose one element $g_{i,j}$ in each conjugacy class of each G_i.
- Character table : characters of the simple modules $S_{i,j}$

$$\left(\chi_{S_{i,j}}(g_{i',j'})\right)_{(i,j),(i',j')}$$

Theorem (Mc Alister 1972, T'11)

The character table is invertible and upper block triangular
Blocks : character tables of the groups G_i

Corollary

Characters can be used to compute composition factors!

Even over $\mathbb{Z}$ for aperiodic monoids!

The Cartan (invariant) matrix

Definition

Cartan (invariant) matrix of an algebra A

- Combinatorial invariant :

$$\dim Hom(P_I, P_J)$$

- Composition factors of the projective modules

Typical algorithm

- Compute orthogonal idempotents e_J (hard to describe !)
- Compute $\dim e_I A e_J$

Alternative definition

The composition factors of A as A-mod-A !

The Cartan matrix for a monoid using characters

Proposition (T'11)

Cartan matrix from a combinatorial statistic and the character table :

$$\sum_{i,j \in I} c_{i,j}\ s_i \otimes s_j^* \ = \ \chi_{\mathbb{K}M} \ = \ \sum_{i,j \in I} \overline{c}_{i,j}\ p_i \otimes p_j^*$$

For a group in char 0 : $\chi_{\mathbb{K}M} = \sum_I s_I \otimes s_I^*$ (Cauchy kernel for $\mathfrak{S}_n$!)

Algorithm

complexity roughly $O(|M|)^3$

Special case : aperiodic monoids

Algorithm [T'11]

Input : an aperiodic monoid

1. Construct representatives of left and right class modules
2. Construct the simple modules as quotients thereof
3. Compute the character table
4. Compute the character of each left and right class module
5. Compute the decomposition matrices $M_{\mathcal{L}}$ and $M_{\mathcal{R}}$

Output : The cartan matrix $C = M_{\mathcal{L}}^t M_{\mathcal{R}}$

Remarks

$M_{\mathcal{L}}$ and $M_{\mathcal{R}}$ are upper unitriangular on regular $\mathcal{J}$-classes
A regular monoid has Cartan matrix with det 1 !

Advantages of this algorithm

- Splits the linear algebra in small chunks
- Take advantage of the redundancy
- Rough complexity : $O(\sum_{i \in I} |R_i|^3)$
- Cartan matrix of a monoid of size 31103 in one hour
- Potential for parallelism !

Implementation

- Short algorithms
- Quite a few prerequisites
- Currently only fully implemented for aperiodic monoids
- Beta publicly available
- Send me examples !

Theoretical consequences (aperiodic case)

Aperiodic case

- Mostly characteristic free
- No algebraic extension needed (no surprise)
- Generalization to PIDs ($\mathbb{Z}$, ...)

$\mathcal{J}$-trivial case [Denton, Hivert, Schilling, T'2010]

- Completely combinatorial
- Quiver, ...

Going further ?

- Use Brauer characters for general monoids/characteristic
- Quiver, socle / radical filtration, projective resolution, ...
- Construction of projective modules ?
- More interesting examples in combinatorics ?

Summary

- Many Markov chains have very nice behaviorthat can be explained by representation theory of monoids
- Nice combinatorics comes out of representation theory of monoids
- Algebraic combinatorics is a good source of examples.

- Progress from studying examples and simple ideas
- Tool : computer exploration