

Logarithmic Space and Permutations

(Joint work with Clément Aubert)

Thomas Seiller



DICE, Rome, March 17th 2013

Introduction

- ▶ Linear Logic and Geometry of Interaction (GoI) have lead to a number of work on computational complexity.
- ▶ This work develops a new approach for the study of complexity classes proposed by Girard (2012):
 - ▶ It uses operator theory, and it is in particular constructed around the construction of the *crossed product algebra*;
 - ▶ It comes from Girard's latest GoI construction;
 - ▶ We use it to characterize the classes **co-NL** and **L** by sets of operators.

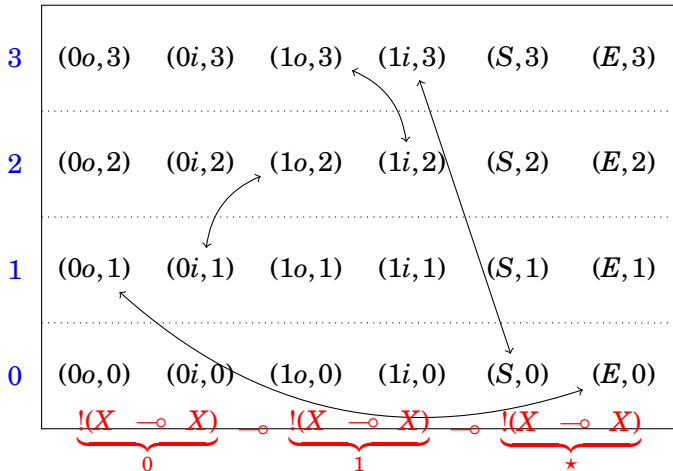
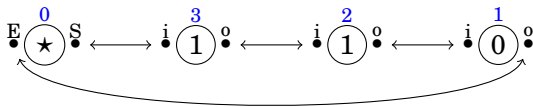
Representation of Integers

- ▶ Principle: an integer n is represented as a binary list, i.e. as a proof of

$$\underbrace{!(X \multimap X)}_0 \multimap \underbrace{!(X \multimap X)}_1 \multimap \underbrace{!(X \multimap X)}_{\star}$$

- ▶ The list can be read from the contraction rules.
- ▶ The GoI interpretation of these proofs are matrices (M_n) representing the sets of axiom links: we obtain a 6×6 matrix whose coefficients are $k \times k$ matrices ($k = \log_2(n)$ is the length of the list).

Representation of Integers: Example



Uniform Representation: The Hyperfinite Factor

The last GoI construction takes place in the hyperfinite factor $\mathfrak{R}$ of type II_1 . The property we are interested in is that every matrix algebra embeds in the hyperfinite factor.

Definition

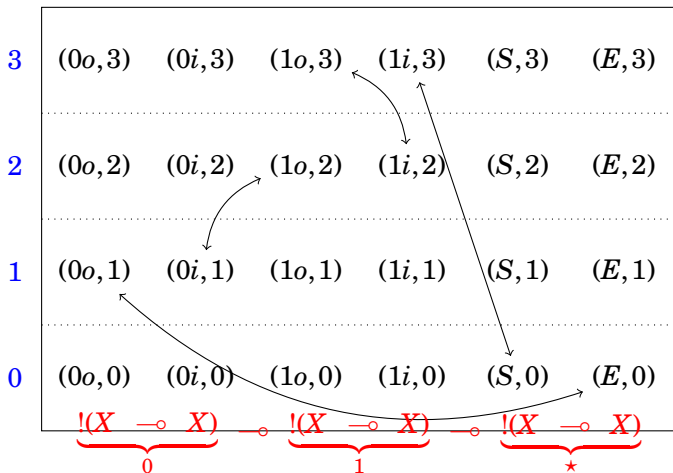
A representation N_n of n is the image of the matrix M_n by a trace-preserving injective $*$ -morphism $\phi : \mathfrak{M}_{\log_2(n)}(\mathbf{C}) \rightarrow \mathfrak{R}$:

$$N_n = \text{Id}_{\mathfrak{M}_6} \otimes \phi(M_n)$$

- ▶ We now have a uniform representation of integers (all representations live in the same algebra $\mathfrak{M}_6(\mathfrak{R})$).

Integers

Integers still look like that:



Inner/Outer Automorphisms

Consider a group G and an element $a \in G$. Then:

$$\phi_a : g \mapsto a^{-1}ga$$

is an automorphism. Such automorphisms are called *inner*.

- ▶ If G is now an algebra, then we need to pick up an $a \in G$ which is invertible. If G is an involutive algebra (i.e. endowed with an involution $(\cdot)^*$), then $a \in G$ must also satisfy $a^{-1} = a^*$. Such an element is called *unitary*.
- ▶ If an automorphism is not inner, we say it is *outer*.

Uniform Representation: The Hyperfinite Factor

Definition

A representation of n is the image of the matrix M_n by a trace-preserving injective $*$ -morphism $\mathfrak{M}_{\log_2(n)}(\mathbf{C}) \rightarrow \mathfrak{K}$.

Remark

This is in no way unique!

Proposition

Let N_n be a representation of the integer n . Then N'_n is a representation of n if and only if there exists a unitary $u \in \mathfrak{K}$ such that:

$$N_n = (Id \otimes u)^* N'_n (Id \otimes u)$$

Crossed Product

Let A be an algebra acting on a Hilbert space $\mathbb{H}$, and G a group of (outer) automorphisms of A . We can construct $\mathbb{K} = L^2(G, \mathbb{H})$, i.e. the space of maps $f : G \rightarrow \mathbb{H}$ such that $\sum_G \|f(g)\|_{\mathbb{H}}^2 < \infty$ and then:

- ▶ represent elements $a \in A$ as operators $\pi(a)$ acting on $\mathbb{K}$;
- ▶ represent elements $g \in G$ as unitary operators $\lambda(g)$ acting on $\mathbb{K}$ that *internalize* g , i.e. such that:

$$\pi(g(a)) = \lambda(g)^* \pi(a) \lambda(g)$$

These two sets of operators generate the *crossed product algebra*, denoted $A \rtimes G$.

The Basic Picture

$$\mathfrak{E} = \mathfrak{M}_6((\bigotimes_{n \in \mathbf{N}} \mathfrak{R}) \rtimes \mathfrak{S})$$

where:

- ▶ $\mathfrak{R}$ is the hyperfinite type II_1 factor;
- ▶ $\mathfrak{S}$ is the group of finite permutations of $\mathbf{N}$ acting on $\bigotimes_{n \in \mathbf{N}} \mathfrak{R}$:

$$\sigma.(x_0 \otimes x_1 \otimes \cdots \otimes x_n \otimes \cdots) = x_{\sigma^{-1}(0)} \otimes x_{\sigma^{-1}(1)} \otimes \cdots \otimes x_{\sigma^{-1}(n)} \otimes \cdots$$

The Basic Picture

$$\mathfrak{E} = \mathfrak{M}_6((\underbrace{\mathfrak{R}}_{\text{integers}} \otimes \mathfrak{R} \otimes \mathfrak{R} \otimes \dots) \rtimes \underbrace{\mathfrak{S}}_{\text{machines}})$$

where:

- ▶ $\mathfrak{R}$ contains representations of integers;
- ▶ $\mathfrak{S}$ generates an algebra $\mathfrak{M}$ in $\mathfrak{E}$ containing the "machines", i.e. the algebra generated by the unitaries $\lambda(g)$ ($g \in G$).

The Algebra of Machines

Recall $\mathfrak{M}$ is the algebra of machines.

Proposition

Let N_n and N'_n be two representations of the same integer and $\phi \in \mathfrak{M}_6(\mathfrak{M})$. Then:

$$\phi N_n \text{ is nilpotent iff } \phi N'_n \text{ is nilpotent}$$

Definition

For $\phi \in \mathfrak{M}$, one can define:

$$[\phi] = \{n \in \mathbf{N} \mid \phi N_n \text{ is nilpotent}\}$$

- ▶ We will now define two sets P_+ and $P_{+,1}$ of elements[†] of $\mathfrak{M}_6(\mathfrak{M})$ and show that $[P_+] = \mathbf{co-NL}$ and $[P_{+,1}] = \mathbf{L}$.

Pointer Machines

- ▶ Pointers: move back and forth on the input tape, but never write.
- ▶ The input tape is cyclic.

Definition

A non-deterministic pointer machine with $p \in \mathbf{N}^*$ pointers is a couple $M = \{Q, \rightarrow\}$ where:

- ▶ Q is the set of *states*;
- ▶ $\rightarrow$ is the *transition relation*.

Pointer Machines and Logarithmic Space

Pointer machines are equivalent to *Multi-Head Two-Way Finite Automata*. Since the latter characterize **NL** (non-deterministic automata) and **L** (deterministic automata), we obtain:

Theorem

$$DPM = L \quad \text{and} \quad NDPM = \mathbf{co-NL}$$

Pointer Machines and Operators

We can encode the pointer machines as operators:

- ▶ We encode the basic instructions (move forward/backward and change the state) as partial isometries in ${}^\dagger \mathfrak{M}_6(\mathfrak{M})$;
- ▶ We define $\rightarrow^*$ as the sum of these atomic transitions.
- ▶ We obtain an encoding M^* of M as an operator in ${}^\dagger \mathfrak{M}_6(\mathfrak{M})$.

We then obtain:

Theorem

Let M be a non-deterministic pointer machine, $n \in \mathbf{N}$ and N_n a representation of n . Then M accepts $n \in \mathbf{N}$ if and only if M^*N_n is nilpotent.

Operators and Logarithmic Space: Non-deterministic case

The encoding of pointer machines are *boolean operators*:

Definition

A boolean operator is an element of $\mathfrak{M}_{6 \times q}(\mathfrak{M})$ such that each coefficient is a finite sum of unitaries $\lambda(g)$ ($g \in \mathfrak{S}$).

Proposition

If P_+ denotes the set of boolean operators.

$$\mathbf{co-NL} \subset [P_+]$$

Operators and Logarithmic Space: deterministic case

Proposition

If M is deterministic pointer machine, then M^* satisfies $\|M^*\|_1 \leq 1$.

Proposition

If $P_{+,1}$ denotes the set of boolean operators ϕ such that $\|\phi\|_1 \leq 1$.

$$L \subset [P_{+,1}]$$

Converse Inclusions

To get the converse inclusion, we prove a technical lemma:

Lemma

Let ϕ be a boolean operator and N_n the representation of an integer. Then there exists matrices $\bar{\phi}$ and $\bar{N}_n$ such that:

$$\phi N_n \text{ is nilpotent iff } \bar{\phi} \bar{N}_n \text{ is nilpotent}$$

- ▶ To check nilpotency of ϕN_n , one can check the nilpotency of $\bar{\phi} \bar{N}_n$ which can be done by a Turing machine using only logarithmic space (only positive coefficients).
- ▶ This Turing machine can be chosen deterministic if we restrict to boolean operators ϕ such that $\|\phi\|_1 \leq 1$.

Theorem

$$\mathbf{co}\text{-}\mathbf{NL} = \mathbf{NDPM} = [P_+]$$

Theorem

$$\mathbf{L} = \mathbf{DPM} = [P_{+,1}]$$

Perspectives

- ▶ Extend to other classes (other groups, supersets of P_+);
- ▶ Obtain a real connection with GoI (construct **co-NL** and **L** types);
- ▶ Obtain new proofs of classical results such as **co-NL** = **NL**;
- ▶ Separation ?