Logarithmic Space and Permutations

LCC'13, Torino

Clément Aubert
Joint work with Thomas Seiller

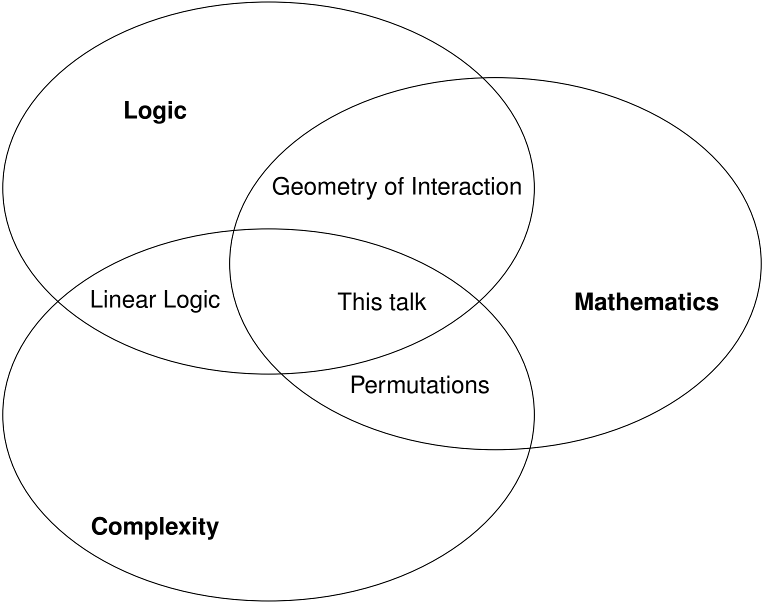
aubert@lipn.fr

5 September 2013

Clément Aubert and Thomas Seiller.
Characterizing co-NL by a group action.
CoRR, abs/1209.3422, 2012.

Clément Aubert and Thomas Seiller.
Logarithmic space and permutations.
CoRR, abs/1301.3189, 2013.

Jean-Yves Girard.
Normativity in logic.
In Peter Dybjer, Sten Lindström, Erik Palmgren, and Göran Sundholm, editors, *Epistemology versus Ontology*, volume 27 of *Logic, Epistemology, and the Unity of Science*, pages 243–263. Springer, 2012.


Logic
Geometry of Interaction
Linear Logic
This talk
Mathematics
Permutations
Complexity

Integers $\to$ Binary List $\to$ λ-term $\to$ proof $\to$ Proof-Net $\to$ Matrices

$0, 1, 2, 3, \dots$

$\hookrightarrow 001, 010, 011, 100, \dots$

$\hookrightarrow \lambda f_0 \lambda f_1 \lambda_x \cdot f_0(f_1(f_1(\dots(f_0 x)\dots)$

$\hookrightarrow \vdash \forall X(X \to X) \to ((X \to X) \to (X \to X))$

Integers $\rightarrow$ Binary List $\rightarrow$ λ-term $\rightarrow$ proof in L.L. $\rightarrow$ Proof-Net $\rightarrow$ Matrices

$0, 1, 2, 3, \ldots$

$\hookrightarrow 001, 010, 011, 100, \ldots$

$\hookrightarrow \lambda f_0 \lambda f_1 \lambda_x \cdot f_0(f_1(f_1(\ldots(f_0 x)\ldots)$

$\hookrightarrow \vdash \forall X ?(X \multimap X) \multimap (?(X \multimap X) \multimap !(X \multimap X))$

Integers $\rightarrow$ Binary List $\rightarrow$ λ-term $\rightarrow$ proof in L.L. $\rightarrow$ Proof-Net $\rightarrow$ Matrices

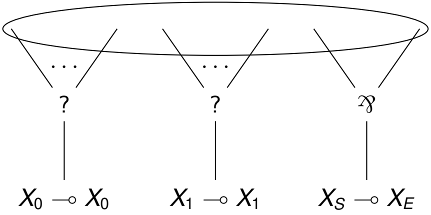
$0, 1, 2, 3, \ldots$

$\hookrightarrow 001, 010, 011, 100, \ldots$

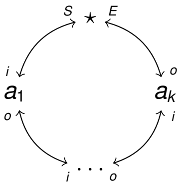
$\hookrightarrow \lambda f_0 \lambda f_1 \lambda_x \cdot f_0(f_1(f_1(\ldots(f_0 x)\ldots)$

$\hookrightarrow \ \vdash \forall X ?(X \multimap X) \multimap (?(X \multimap X) \multimap !(X \multimap X))$

$\hookrightarrow$



Integers $\rightarrow$ Binary List $\rightarrow$ λ-term $\rightarrow$ proof in L.L. $\rightarrow$ Proof-Net $\rightarrow$ Matrices

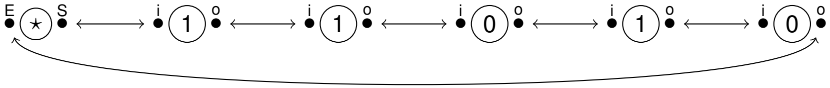


Integers $\rightarrow$ Binary List $\rightarrow$ λ-term $\rightarrow$ proof in L.L. $\rightarrow$ Proof-Net $\rightarrow$ Matrices

$$M_n = \begin{array}{c} \overbrace{\qquad\qquad}^{0} \; \overbrace{\qquad\qquad}^{1} \; \overbrace{\qquad\qquad}^{\star} \\ \begin{pmatrix} 0 & l_{00} & 0 & l_{10} & l_{S0} & 0 \\ {l_{00}}^t & 0 & {l_{01}}^t & 0 & 0 & {l_{0E}}^t \\ 0 & l_{01} & 0 & l_{11} & l_{S1} & 0 \\ {l_{10}}^t & 0 & {l_{11}}^t & 0 & 0 & {l_{1E}}^t \\ {l_{S0}}^t & 0 & {l_{S1}}^t & 0 & 0 & 0 \\ 0 & l_{0E} & 0 & l_{1E} & 0 & 0 \end{pmatrix} \end{array} \begin{array}{l} \left.\right\} 0 \\ \left.\right\} 1 \\ \left.\right\} \star \end{array}$$

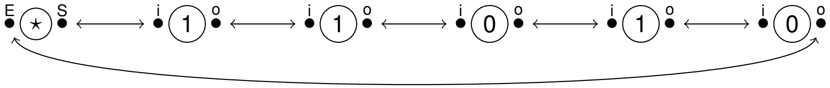
Definition (Binary representation of integers)

An operator $N_n \in \mathfrak{M}_6(\mathfrak{N}_0)$ is a *binary representation* of an integer n if ...



Definition (Binary representation of integers)

An operator $N_n \in \mathfrak{M}_6(\mathfrak{N}_0)$ is a *binary representation* of an integer n if ...



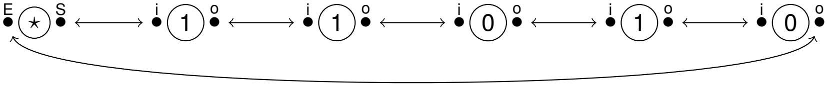
Definition (Observations)

An *observation* is an operator $\phi \in \mathfrak{M}_6(\mathfrak{S})$.

How to compute with integers as operators?

Definition (Binary representation of integers)

An operator $N_n \in \mathfrak{M}_6(\mathfrak{N}_0)$ is a *binary representation* of an integer n if . . .



Definition (Observations)

An *observation* is an operator $\phi \in \mathfrak{M}_6(\mathfrak{S})$.

Definition (Computing, accepting)

The computation ends if $\exists k \in \mathbb{N}$ such that

$$(\phi(N_n))^k = 0$$

Definition (Normative Pairs)

Let $\mathfrak{N}_0$ and $\mathfrak{S}$ be two subalgebras of a von Neumann algebra $\mathfrak{M}$. The pair $(\mathfrak{N}_0, \mathfrak{S})$ is a *normative pair (in $\mathfrak{M}$)* if:

- $\mathfrak{N}_0$ is isomorphic to $\mathfrak{R}$;
- For all $\Phi \in \mathfrak{M}_6(\mathfrak{S})$ and $N_n, N_n' \in \mathfrak{M}_6(\mathfrak{N}_0)$ two binary representations of n,

$$\Phi N_n \text{ is nilpotent} \Leftrightarrow \Phi N_n' \text{ is nilpotent}$$

Definition (Normative Pairs)

Let $\mathfrak{N}_0$ and $\mathfrak{S}$ be two subalgebras of a von Neumann algebra $\mathfrak{M}$. The pair $(\mathfrak{N}_0, \mathfrak{S})$ is a *normative pair (in $\mathfrak{M}$)* if:

- $\mathfrak{N}_0$ is isomorphic to $\mathfrak{R}$;
- For all $\Phi \in \mathfrak{M}_6(\mathfrak{S})$ and $N_n, N'_n \in \mathfrak{M}_6(\mathfrak{N}_0)$ two binary representations of n,

$$\Phi N_n \text{ is nilpotent} \Leftrightarrow \Phi N'_n \text{ is nilpotent}$$

Proposition

Let G be the group of finite permutations over $\mathbb{N}$, α an action of G and for all $n \in \mathbb{N}$, $\mathfrak{N}_n = \mathfrak{R}$. The algebra $(\otimes_{n\in\mathbb{N}}\mathfrak{N}_n) \rtimes_\alpha G$ contains a subalgebra generated by G that we will denote $\mathfrak{G}$.
$(\mathfrak{N}_0, \mathfrak{G})$ is a normative pair in $(\otimes_{n\in\mathbb{N}}\mathfrak{N}_n) \rtimes_\alpha G$.

Definition (P_+ and $P_{+,1}$)

Let $(\mathfrak{N}_0, \mathfrak{G})$ be a normative pair, $\phi \in \mathfrak{M}_6(\mathfrak{G})$ an observation, we define:

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

Definition (P_+ and $P_{+,1}$)

Let $(\mathfrak{N}_0, \mathfrak{G})$ be a normative pair, $\phi \in \mathfrak{M}_6(\mathfrak{G})$ an observation, we define:

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

An observation is said to be *positive* when all its coefficients are $\geqslant 0$.

Definition (P_+ and $P_{+,1}$)

Let $(\mathfrak{N}_0, \mathfrak{G})$ be a normative pair, $\phi \in \mathfrak{M}_6(\mathfrak{G})$ an observation, we define:

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

An observation is said to be *positive* when all its coefficients are $\geqslant 0$.
We then define:

$$\begin{aligned} P_+ &= \{\phi \mid \phi \text{ is a positive observation}\} \\ P_{+,1} &= \{\phi \mid \phi \in P_+ \text{ and } \|\phi\|_1 \leqslant 1\} \end{aligned}$$

$$\{P\} = \{[\phi] \mid \phi \in P\}$$

Definition (P_+ and $P_{+,1}$)

Let $(\mathfrak{N}_0, \mathfrak{G})$ be a normative pair, $\phi \in \mathfrak{M}_6(\mathfrak{G})$ an observation, we define:

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

An observation is said to be *positive* when all its coefficients are $\geqslant 0$.
We then define:

$$\begin{aligned} P_+ &= \{\phi \mid \phi \text{ is a positive observation}\} \\ P_{+,1} &= \{\phi \mid \phi \in P_+ \text{ and } \|\phi\|_1 \leqslant 1\} \end{aligned}$$

$$\{P\} = \{[\phi] \mid \phi \in P\}$$

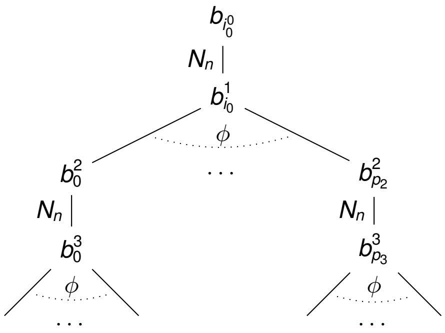
We will prove

$$\{P_+\} = \textbf{co-NL}$$
$$\{P_{+,1}\} = \textbf{L}$$

Checking the nilpotency in **co-NL**

If $\phi \in P_+$

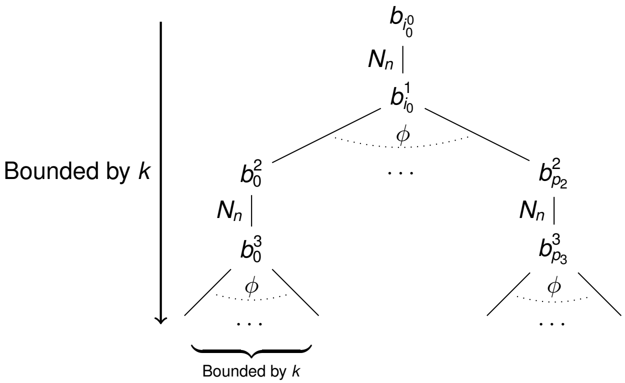
$$\phi(\pi, a_1, \ldots, a_p; \sigma; e) = \sum_{i=0}^{K} \alpha_i(\rho, a_{\tau_i(1)}, \ldots, a_{\tau_i(p)}; \tau_i\sigma; e_i)$$



With b_i^j the elements of the basis encountered.

If $\phi \in P_+$

$$\phi(\pi, a_1, \ldots, a_p; \sigma; e) = \sum_{i=0}^{K} \alpha_i(\rho, a_{\tau_i(1)}, \ldots, a_{\tau_i(p)}; \tau_i\sigma; e_i)$$



With b_i^j the elements of the basis encountered and k the dimensions of the underlying space.

Checking the nilpotency in **L**

If $\phi \in P_{+,1}$

$$\phi(\pi, a_1, \ldots, a_p; \sigma; e) = \qquad \alpha_i(\rho, a_{\tau_i(1)}, \ldots, a_{\tau_i(p)}; \tau_i\sigma; e_i)$$

Bounded by k $\downarrow$

$$\begin{array}{r} b_{i_0^0} \\ N_n \Big| \\ b_{i_0}^1 \\ \phi \Big| \\ b_0^2 \\ N_n \Big| \\ b_0^3 \\ \vdots \end{array}$$

With b_i^j the elements of the basis encountered and k the dimensions of the underlying space.

- Positive observations

  No interference between the “branches” of the computation.

  $\hookrightarrow$ Non-deterministic computation.

- **Positive observations**

  No interference between the “branches” of the computation.

  $\hookrightarrow$ Non-deterministic computation.

- **Nilpotency**

  All “branches” must reach 0 for the computation to stop.

  $\hookrightarrow$ “Universally non-deterministic”

Singularities of this framework

- **Positive observations**
  No interference between the “branches” of the computation.
  $\hookrightarrow$ Non-deterministic computation.

- **Nilpotency**
  All “branches” must reach 0 for the computation to stop.
  $\hookrightarrow$ “Universally non-deterministic”

- **Crossed product with the group of finite permutations**
  Permutations to chose where the bit currently read is stored.
  $\hookrightarrow$ Several registers / pointers.

- Positive observations

  No interference between the "branches" of the computation.

  $\hookrightarrow$ Non-deterministic computation.

- Nilpotency

  All "branches" must reach 0 for the computation to stop.

  $\hookrightarrow$ "Universally non-deterministic"

- Crossed product with the group of finite permutations

  Permutations to chose where the bit currently read is stored.

  $\hookrightarrow$ Several registers / pointers.

- Nilpotency as acceptation

  A "fresh copy" of the input and the program is provided at every step.

  $\hookrightarrow$ Not possible to modify the input.

Singularities of this framework

- **Positive observations**
  No interference between the “branches” of the computation.
  $\hookrightarrow$ Non-deterministic computation.

- **Nilpotency**
  All “branches” must reach 0 for the computation to stop.
  $\hookrightarrow$ “Universally non-deterministic”

- **Crossed product with the group of finite permutations**
  Permutations to chose where the bit currently read is stored.
  $\hookrightarrow$ Several registers / pointers.

- **Nilpotency as acceptation**
  A “fresh copy” of the input and the program is provided at every step.
  $\hookrightarrow$ Not possible to modify the input.

+ **Technical details** : circular input, specific kind of initialization, etc.

But which one?

- Purple
- JAG
- Knuth's Linking Automaton
- Tarjan's Reference Machine
- SMM, KUM,
- 2NDFA

Theorem

$$\boldsymbol{NL} = \cup_{k \geqslant 1} \mathcal{L}(2NDFA(k))$$
$$\boldsymbol{L} = \cup_{k \geqslant 1} \mathcal{L}(2DFA(k))$$

Theorem

$$\textbf{\textit{co-NL}} = \cup_{k \geqslant 1} \mathcal{L}(NDPM(k))$$
$$\textbf{\textit{L}} = \cup_{k \geqslant 1} \mathcal{L}(DPM(k))$$

Theorem

$$\textbf{\textit{co-NL}} = \cup_{k \geqslant 1} \mathcal{L}(NDPM(k))$$
$$\textbf{\textit{L}} = \cup_{k \geqslant 1} \mathcal{L}(DPM(k))$$

Theorem

For any NDPM M, there exists an observation $M^{\bullet} \in \mathfrak{M}_6(\mathfrak{G})$ such that for all $N_n \in \mathfrak{M}_6(\mathfrak{N}_0)$

$$M(n) \text{ accepts iff } M^{\bullet}(N_n) \text{ is nilpotent.}$$

Moreover, $M^{\bullet} \in P_{+}$, and if M was deterministic, $M^{\bullet} \in P_{+,1}$

Theorem

$$\textbf{co-NL} = \cup_{k \geqslant 1} \mathcal{L}(NDPM(k))$$
$$\textbf{L} = \cup_{k \geqslant 1} \mathcal{L}(DPM(k))$$

Theorem

For any NDPM M, there exists an observation $M^{\bullet} \in \mathfrak{M}_6(\mathfrak{G})$ such that for all $N_n \in \mathfrak{M}_6(\mathfrak{N}_0)$

$$M(n) \text{ accepts iff } M^{\bullet}(N_n) \text{ is nilpotent.}$$

Moreover, $M^{\bullet} \in P_{+}$, and if M was deterministic, $M^{\bullet} \in P_{+,1}$

Theorem

$$\{P_{+}\} = \textbf{co-NL}$$
$$\{P_{+,1}\} = \textbf{L}$$

- Defined a representation of integers as operators
- Defined “observations” *i.e.* programs as operators
- Took a specific sub-algebra
- Checked that nilpotency could be decided with logarithmic resources
- Defined an encoding from 2NDFA to operators

- Finite matrices?
- Different constrain on norm, coefficient, etc.
- Another group?