Stuctural Proof-Theory and Complexity

Luca Roversi

Dipartimento di Informatica – Università di Torino

Light Linear Logic (LLL)

- Introduced by Girard 1998
- Characterizes **DTIME**$[n^k]$ under the paradigm "derivations-as-programs and normalization-as-evaluation"
- *Systems without contraction* $\subset$ **LLL** $\subset$ **LL** $\simeq$ System F
- Limits two dynamical aspects:
  - the duplication of terms;
  - the freedom of arbitrary and independent manipulation of the duplicated terms

LLL and DTIME[n^k]

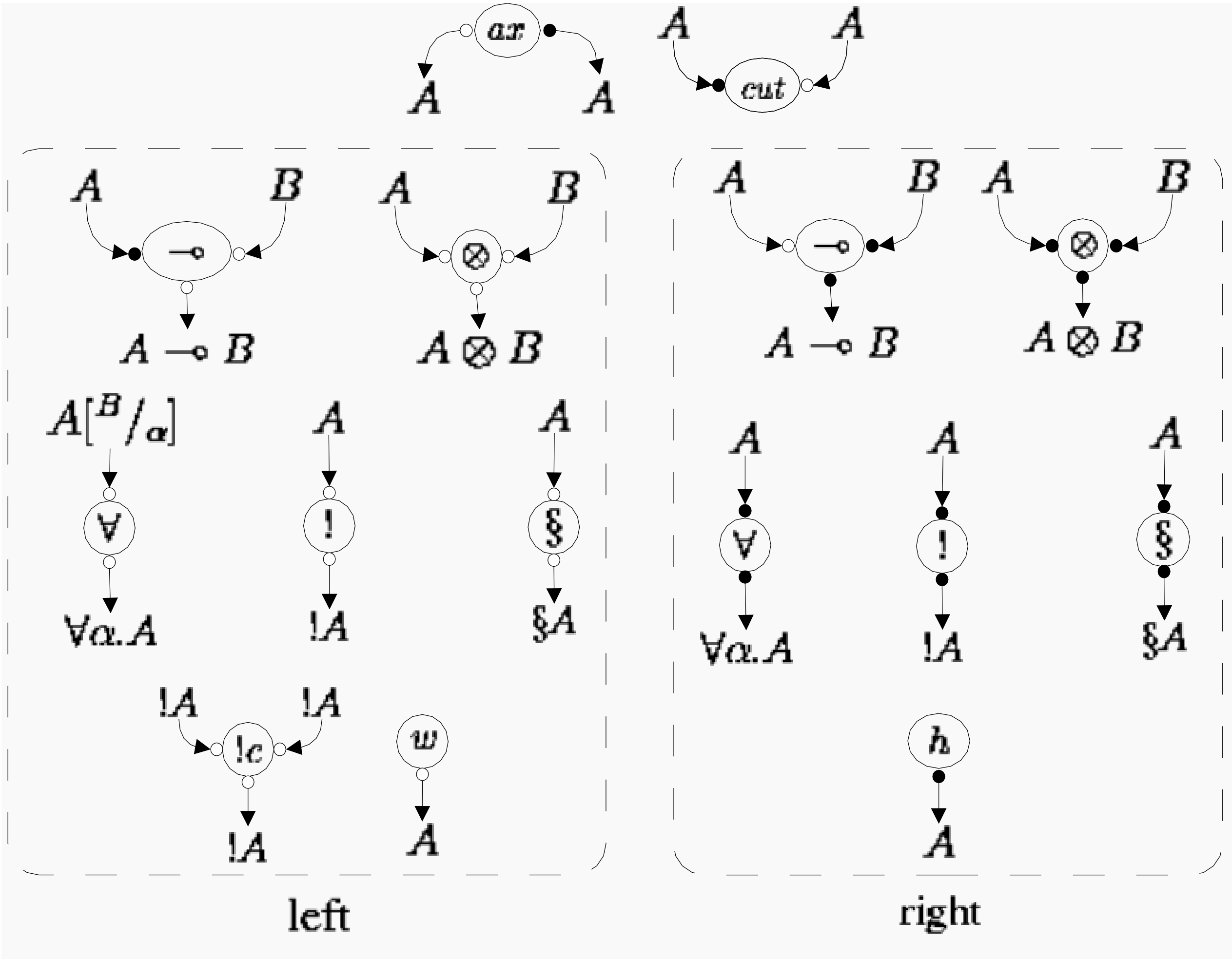
- **LLL** is *sound* with respect to **DTIME**[n^k]:
  - Any $\Pi \in$ **LLL** can be normalized, in polynomial time with respect to $|\Pi|$
- **LLL** is *complete* with respect to **DTIME**[n^k]:
  - There exists $\widehat{(\ )}$:**DTIME**[n^k]$\rightarrow$**LLL** such that, for every function $f \in$ **DTIME**[n^k], if $f(a) = b$, then $\widehat{f}(\widehat{a})$ normalizes to $\widehat{b}$

LLL vs. LAL

- "*The abuse of contraction may have damaging complexity effects*" (Girard)
- "*... , but the abstinence from weakening leads to inessential syntactical complications*" (Asperti)

LAL = **LLL** + unconstrained weakening

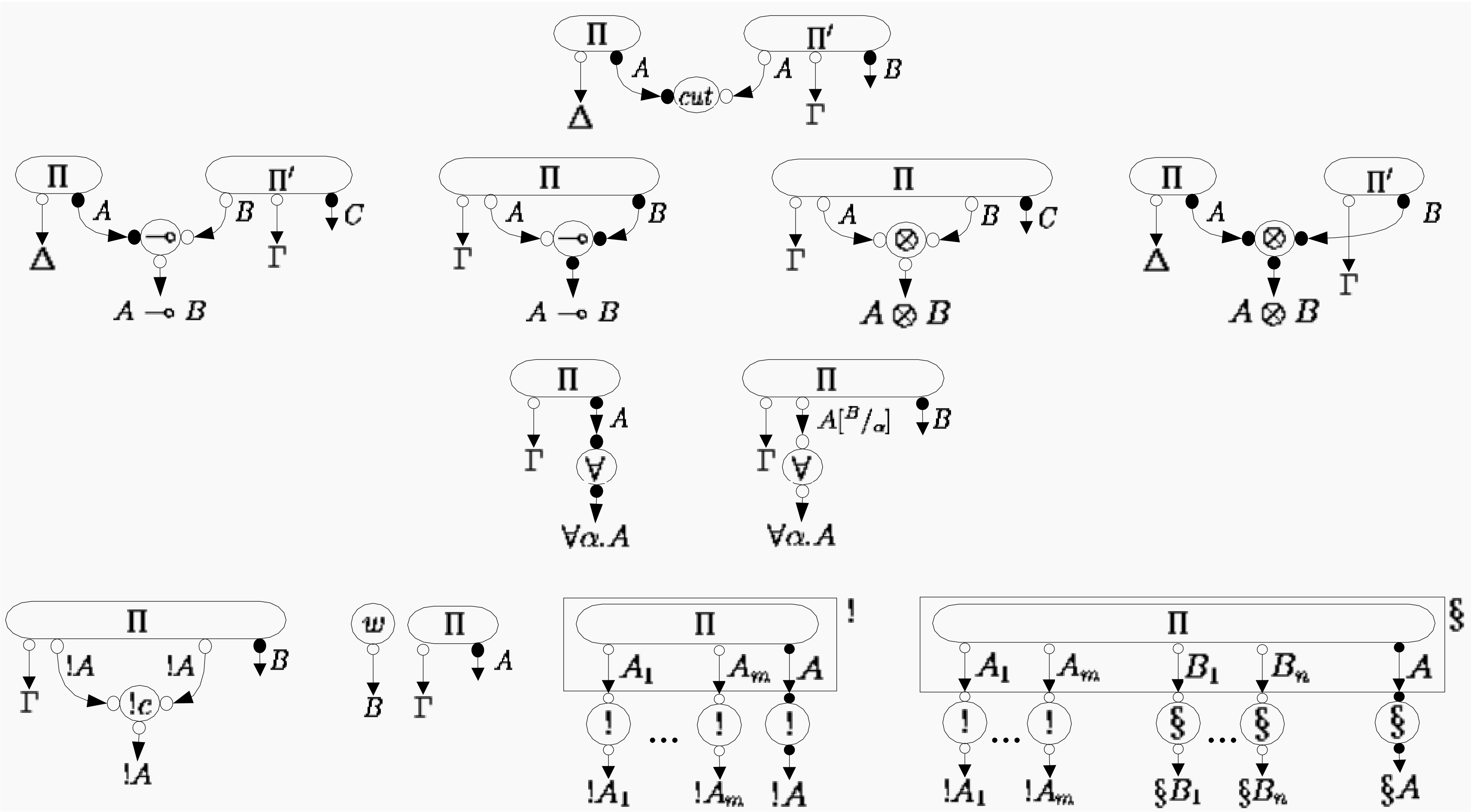
Intuitionistic LAL(ILAL): nodes



$$A ::= A \otimes A \mid A \multimap A \mid \forall\alpha.A \mid !A \mid \S A \mid \alpha \ \ldots$$

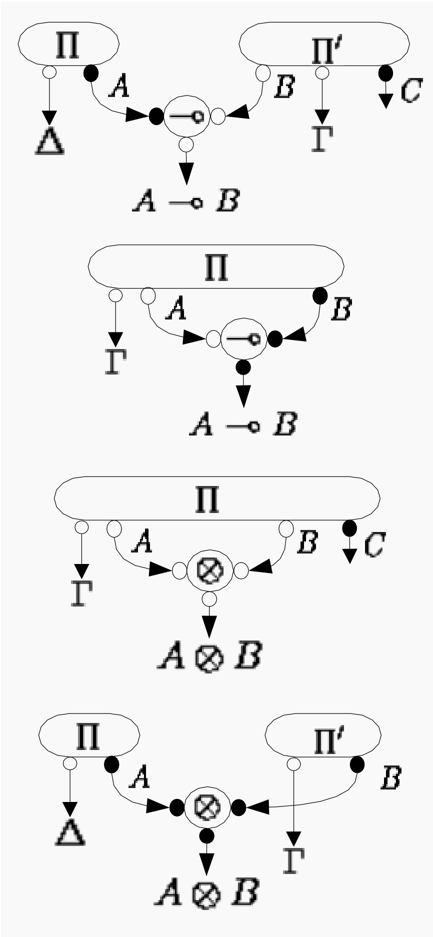
ILAL: proof-nets

ax and h-nodes are proof-nets



unconstrained weakening and $m \leq 1$

ILAL: Proof-nets vs. sequent calculus ...



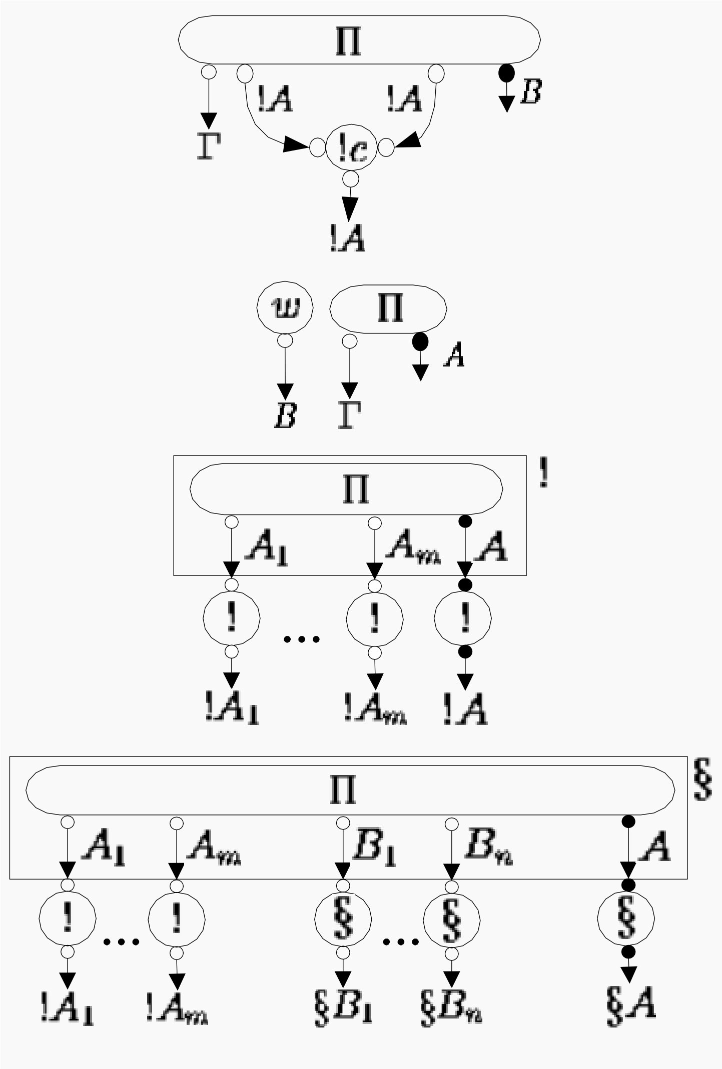
$$(\multimap_l)\ \frac{\Delta, \vdash A \qquad B, \Gamma \vdash C}{\Delta, A \multimap B, \Gamma \vdash C}$$

$$(\multimap_r)\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B}$$

$$(\otimes_l)\ \frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C}$$

$$(\otimes_r)\ \frac{\Delta \vdash A \quad \Gamma \vdash B}{\Delta, \Gamma \vdash A \otimes B}$$

... Proof-nets vs. sequent calculus



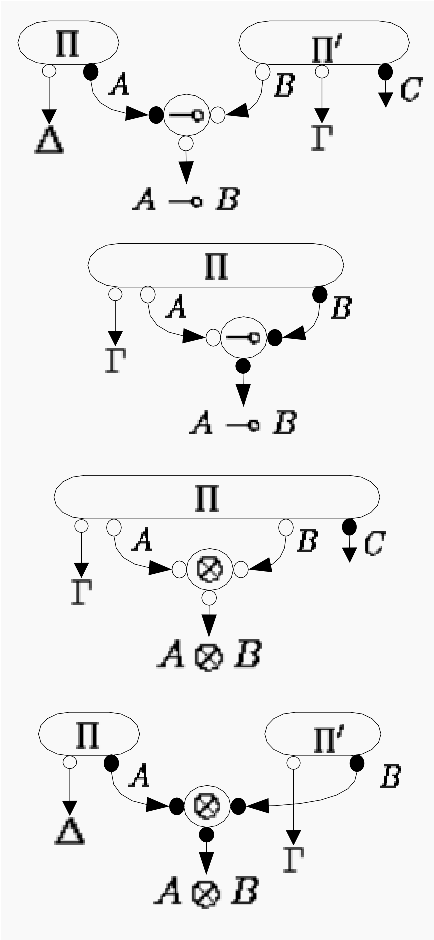
$$(c)\ \frac{\Gamma, !A, !A \vdash B}{\Gamma, !A \vdash B}$$

$$(w)\ \frac{\Gamma \vdash A}{B, \Gamma \vdash A}$$

$$(!)\ \frac{A_1 \ldots A_m \vdash A \qquad 0 \leq m \leq 1}{!A_1 \ldots !A_m \vdash !A}$$

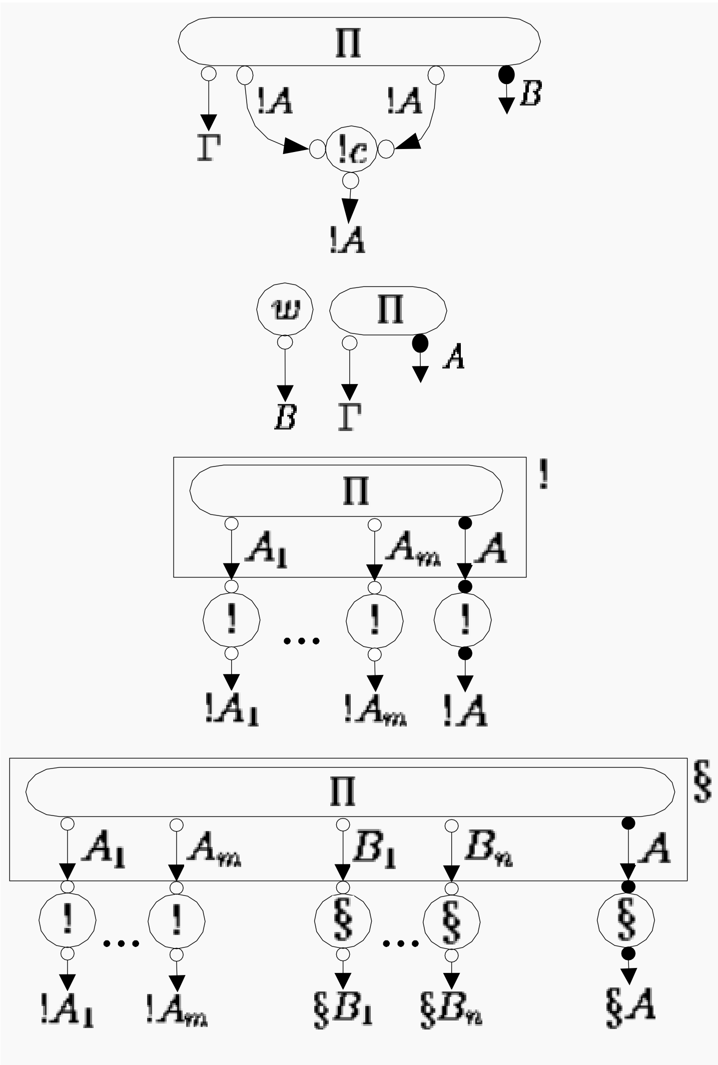
$$(\S)\ \frac{A_1 \ldots A_m, B_1 \ldots B_n \vdash B \qquad \begin{array}{c} 0 \leq i \leq m \\ 0 \leq j \leq n \end{array}}{!A_1 \ldots !A_m, \S B_1 \ldots \S B_n \vdash \S B}$$

ILAL: Proof-nets vs. models ...



$$\frac{\dfrac{A \otimes B \multimap C}{}}{A \multimap B \multimap C}$$

... Proof-nets vs. models



$$!A \multimap !A \otimes !A$$

$$\mathbb{I} \multimap A$$

$$\mathbb{I} \multimap !B$$

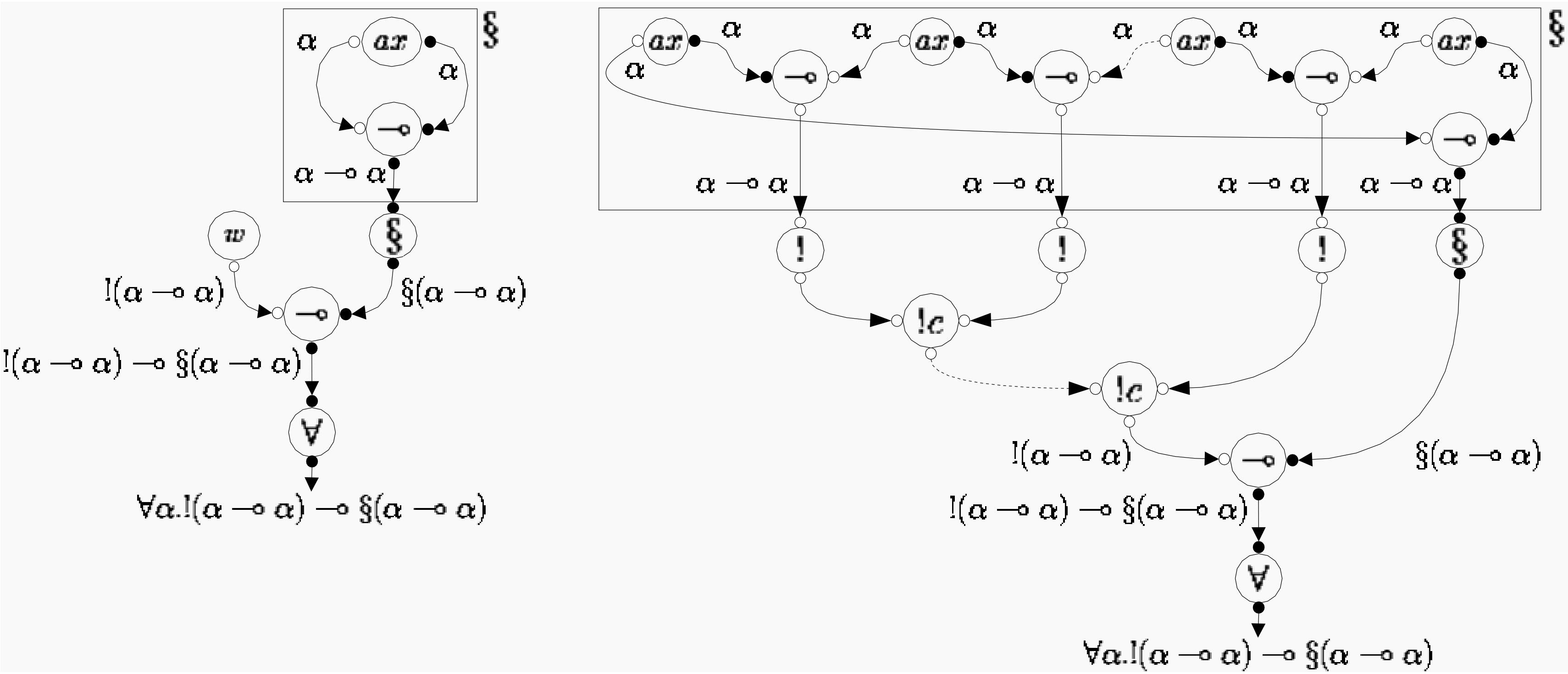
$$!A \multimap !B$$

$$!A \multimap \S B$$

A bottom-up approach to complexity

ILAL axioms	**LL** axioms
$!A \multimap !A \otimes !A$	$!A \multimap !A \otimes !A$
$\mathbb{I} \multimap !B$ $!A \multimap !B$	$!A_1 \otimes \cdots \otimes !A_n \multimap !A$ $!A \otimes !B \multimap !(A \otimes B)$
$!A \multimap \S B$	$!A \multimap A$
	$!A \multimap !!A$
$\mathbb{I} \multimap A$	$\mathbb{I} \multimap !A$

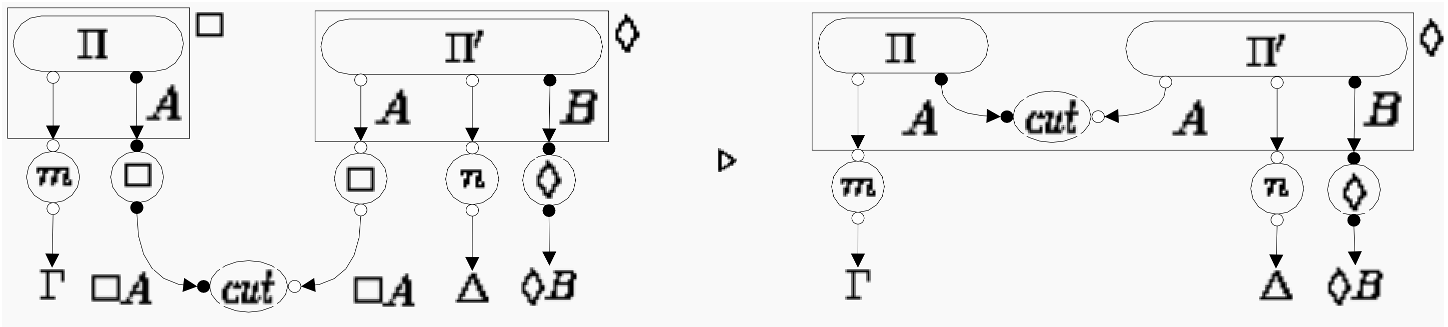
ILAL: $\overline{0}, \overline{1}, \ldots$



$\forall\alpha.!(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha)$ type of the Church numerals

$\overline{n}$ has $n-1$ occurrences of $!c$, for every $n \geq 1$

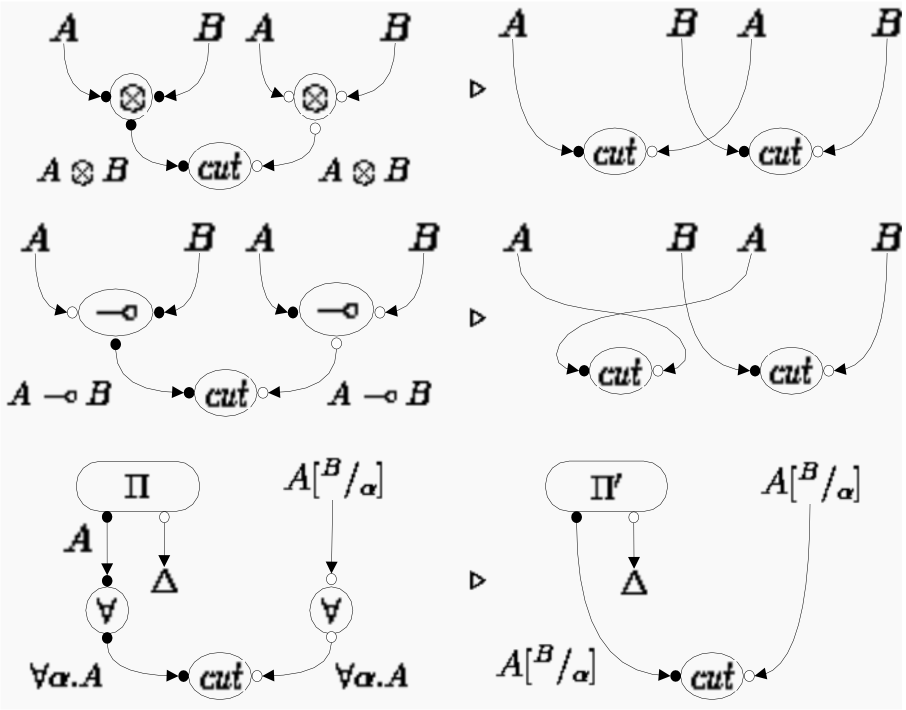
ILAL: shifting ers



Preserve the *depth* of the nodes

- *Depth* of a node n: number of boxes around n
- *Maximal* depth δ of Π: maximal number of nested boxes

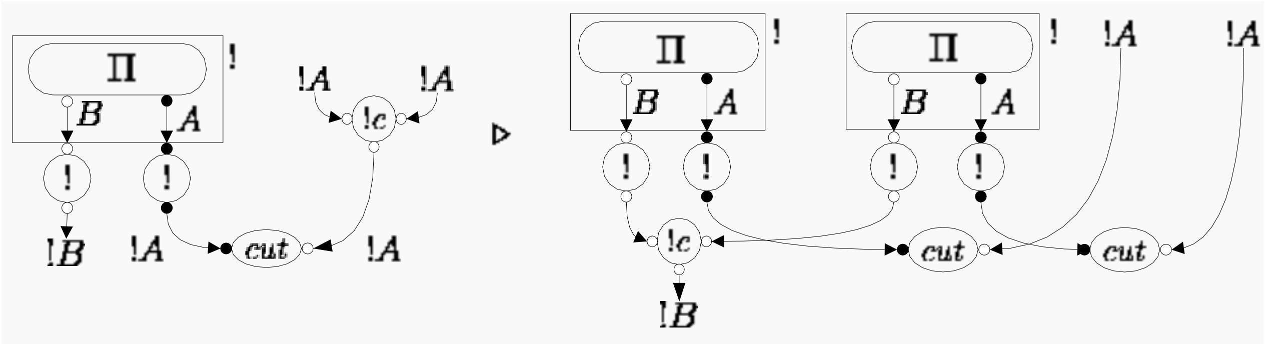
ILAL: linear ers



Strictly shrink the *dimension* $|\Pi|$ of a proof-net Π

- $|\Pi| = \sum_{l=1}^{\delta} |l|$
- $|l|$ = number of nodes of Π at depth l

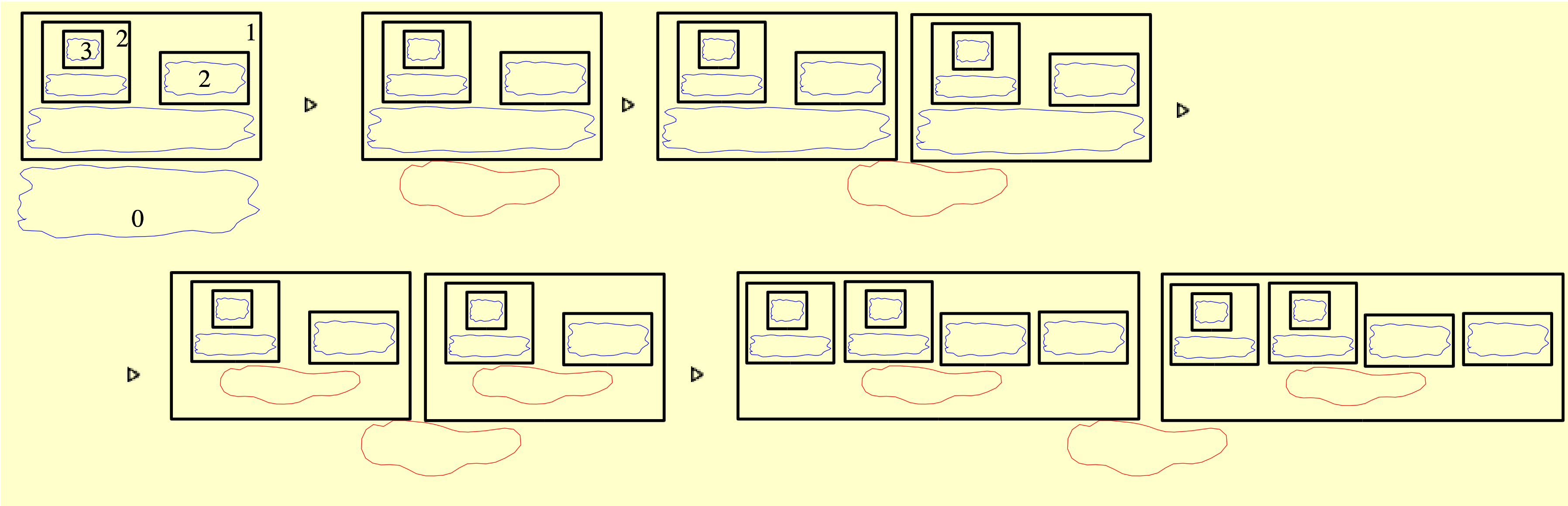
ILAL: polynomial ers



Encreases the *dimension* $|\Pi|$ of a proof-net Π

A redex at depth l replicates nodes at depth $l+1, l+2, \ldots, \delta$

RBR-strategy: intuition



1. shrinks depth 0, expands depth $1, 2, \ldots, \delta$
2. shrinks depth 1, expands depth $2, \ldots, \delta$
3. shrinks depth 2, expands depth $3, \ldots, \delta$
4. $\ldots\ldots$

ILAL: RBR-strategy

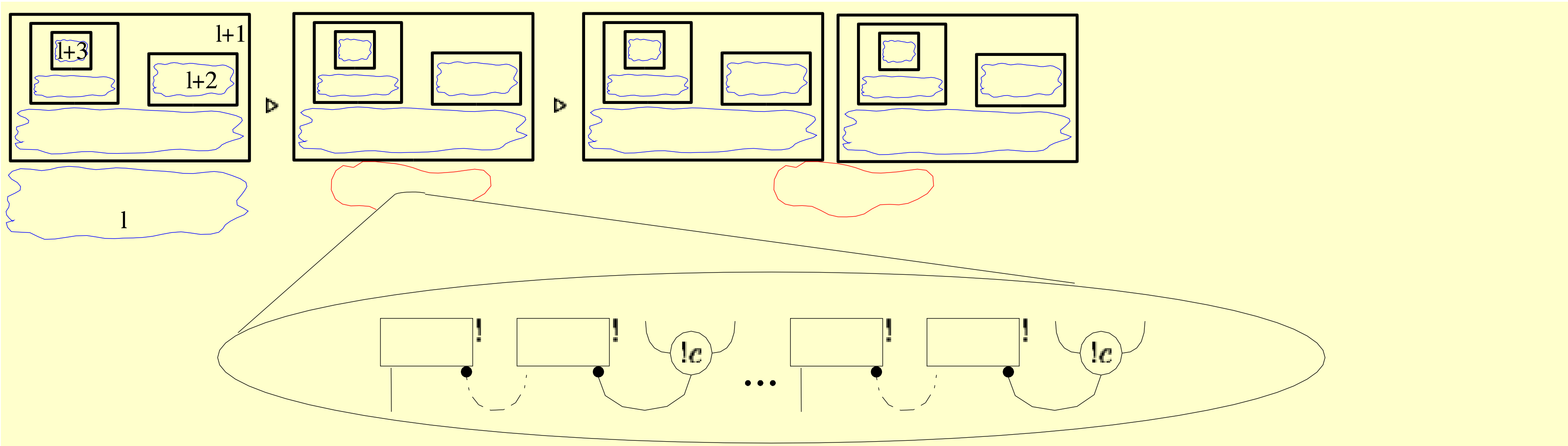
- For every proof-net Π, **RBR-strategy** at depth l:
  - applies the *elementary rewriting steps* as far as possible
  - applies, in any order, both *shifting and polynomial rewriting steps*

Theorem 1

Let Π *be free of redexes at depths* $0, 1, 2, l-1$

If Π *rewrites to* Π' *by* ***RBR-strategy*** *at* $0, 1, 2, l-1, l$*, then* Π' *is free of redexes at depth* l *as well*

RBR-strategy: the cost of reducing at l



- shrinking depth l, costs $O(|l|)$
- expanding depth $l+1, l+2, \ldots$ means:
  - reducing *at most* $|l|$ polynomial ers at depth l
  - for *at most* $|l|$ $!c$-nodes at depth l

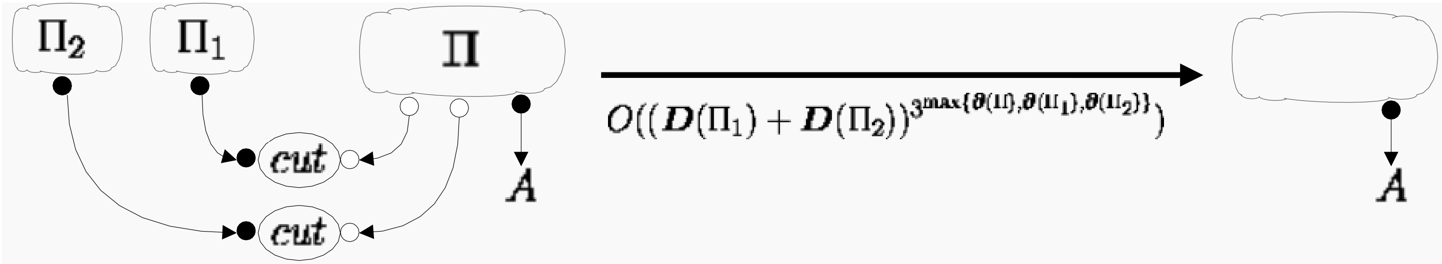
- Depths $l+1, \ldots$ pass from $|l+1|, \ldots$ to $|l|^2|l+1|, \ldots$

RBR-strategy: the cost

$$
\begin{array}{llllllll}
|0| & & |\Pi| & & |\Pi| & & |\Pi| & & |\Pi| \\
|1| & & |\Pi| & & O(|\Pi^3|) & & O(|\Pi^3|) & & O(|\Pi^3|) \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
|l| & \leq & |\Pi| & \triangleright & O(|\Pi^3|) & \triangleright \cdots \triangleright & O(|\Pi^{3^{l-1}}|) & \cdots & O(|\Pi^{3^{l-1}}|) \\
|l+1| & & |\Pi| & & O(|\Pi^3|) & & O(|\Pi^{3^l}|) & & O(|\Pi^{3^l}|) \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
|\delta| & & |\Pi| & & O(|\Pi^3|) & & O(|\Pi^{3^l}|) & & O(|\Pi^{3^{\delta-1}})|
\end{array}
$$

$O(|\Pi^{3^{\delta-1}})|$ bounds the cut-elimination length

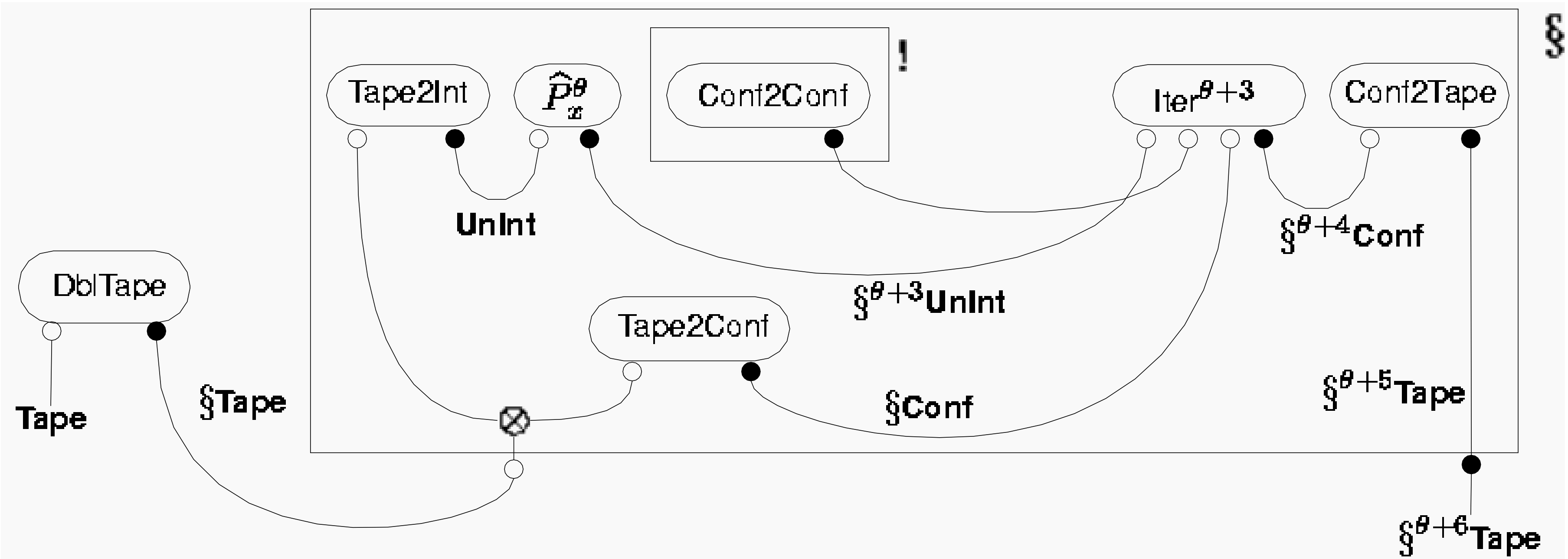
The bound can be a polynomial



- Π is a program
- Π_1, Π_2 are arguments such that:
  - their maximal depth is constant
  - their dimension represents the value of a measure

"The length of the cut-elimination grows as a polynomial in the dimensions of Π_1 and Π_2"

ILAL: DTIME[n^k] completeness



- $\widehat{P}_x^\theta =$ polynomial in x with maximal not null degree θ
- A tape "is" $\lambda 01.\lambda x.\chi_1(\cdots(\chi_n\ x)\cdots)$ with $\chi_i \in \{0, 1\}$
- A configuration represents the portions of the used tape, with the state

Future work

- "Play with **LLL**" and preserve the characterization of sub-recursive classes
- Relate systems à la **LLL** to systems with the same goal, but developed under other principles
- Typing inference on systems à la **LLL**