Notes on proof-nets II

Daniel Murfet

Most of these notes are copied from the following paper:

[BM] = Baillot, Mazza "Linear logic by levels and bounded time complexity", 2009.

15/4/2016

therisingsea.org/post/seminar-proofnets/

Curry-Howard correspondence

logic	programming	categories
formula	type	objects
sequent	input/output spec	—
proof	program	morphisms
cut-elimination	execution	—
contraction	copying	coproducts
stratification	complexity	**?**

Curry-Howard correspondence

(modulo many details)

logic	programming
$\begin{array}{c} \pi \\ \vdots \\ \mathbf{bint} \vdash \mathbf{bint} \end{array}$	Computable $f : \mathbb{N} \longrightarrow \mathbb{N}$
π admits a stratification	f is elementary time
... and only promotes on ≤ 1 premise	f is polynomial time

Recall: **Theorem** (Girard)

A function $\{0,1\}^* \longrightarrow \{0,1\}^*$ is "polytime"
if and only if it can be typed as a proof
π of $\mathbf{bint} \vdash \mathbf{bint}$ which admits a stratification.

$f : \{0,1\}^* \longrightarrow \{0,1\}^*$ computed by a Turing machine T with polyclock P

$$
\dfrac{
\dfrac{
\dfrac{
\begin{matrix}\text{copy}\\ \vdots \\ \mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{bint}\end{matrix}
\qquad
\dfrac{
\dfrac{}{\mathbf{bint} \vdash \mathbf{bint}}
\quad
\dfrac{\begin{matrix}\text{length}\\ \vdots \\ \mathbf{bint} \vdash \mathbf{int}\end{matrix} \quad \begin{matrix}\text{P}\\ \vdots \\ \mathbf{int} \vdash \mathbf{int}\end{matrix}}{\mathbf{bint} \vdash \mathbf{int}}\,\text{cut}
}{\mathbf{bint} \otimes \mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{int}}\,\otimes R, \otimes L
}{\mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{int}}\,\text{cut}
\qquad
\dfrac{\begin{matrix}\text{iterate T}\\ \vdots \\ \mathbf{bint}, \mathbf{int} \vdash \mathbf{Tur}\end{matrix}}{\mathbf{bint} \otimes \mathbf{int} \vdash \mathbf{Tur}}
}{\mathbf{bint} \vdash \mathbf{Tur}}
\qquad
\begin{matrix}\text{read off output}\\ \vdots \\ \mathbf{Tur} \vdash \mathbf{bint}\end{matrix}
}{\mathbf{bint} \vdash \mathbf{bint}}
\qquad \pi
$$

Upshot: π computes f

The formulas of second order unit-free multiplicative exponential linear logic (**meLL**) are generated by the following grammar, where $X, X^\perp$ range over a denumerable set of propositional variables:

$$A, B ::= X \mid X^\perp \mid A \otimes B \mid A \parr B \mid !A \mid ?A \mid \exists X.A \mid \forall X.A \mid \S A.$$

Linear negation is defined through De Morgan laws:

$$\begin{array}{rclcrcl}
(X)^\perp & = & X^\perp & \qquad & (X^\perp)^\perp & = & X \\
(A \otimes B)^\perp & = & B^\perp \parr A^\perp & & (A \parr B)^\perp & = & B^\perp \otimes A^\perp \\
(!A)^\perp & = & ?A^\perp & & (?A)^\perp & = & !A^\perp \\
(\exists X.A)^\perp & = & \forall X.A^\perp & & (\forall X.A)^\perp & = & \exists X.A^\perp
\end{array}$$

$$(\S A)^\perp = \S A^\perp$$

Two connectives exchanged by negation are said to be *dual*. Note that the self-dual paragraph modality is not present in the standard definition of **meLL** [Girard, 1987]; we include it here for convenience. Also observe that full linear logic has a further pair of dual binary connectives, called *additive* (denoted by & and $\oplus$), which we shall briefly discuss in Sect. 5. They are not strictly needed for our purposes, hence we restrict to **meLL** in the paper.

Linear implication is defined as $A \multimap B = A^\perp \parr B$. Multisets of formulas will be ranged over by $\Gamma, \Delta, \ldots$

For technical reasons, it is also useful to consider *discharged formulas*, which will be denoted by $\flat A$, where A is a formula.

Sequent calculus

$$\frac{}{\vdash A^\perp, A}\ \text{Axiom}$$

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}\ \text{Cut}$$

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ \text{Tensor}$$

$$\frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ \text{Par}$$

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, \forall X.A}\ \text{For all } (X \text{ not free in } \Gamma)$$

$$\frac{\vdash \Gamma, A[B/X]}{\vdash \Gamma, \exists X.A}\ \text{Exists}$$

$$\frac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A}\ \text{Promotion}$$

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, ?A}\ \text{Dereliction}$$

$$\frac{\vdash \Gamma}{\vdash \Gamma, ?A}\ \text{Weakening}$$

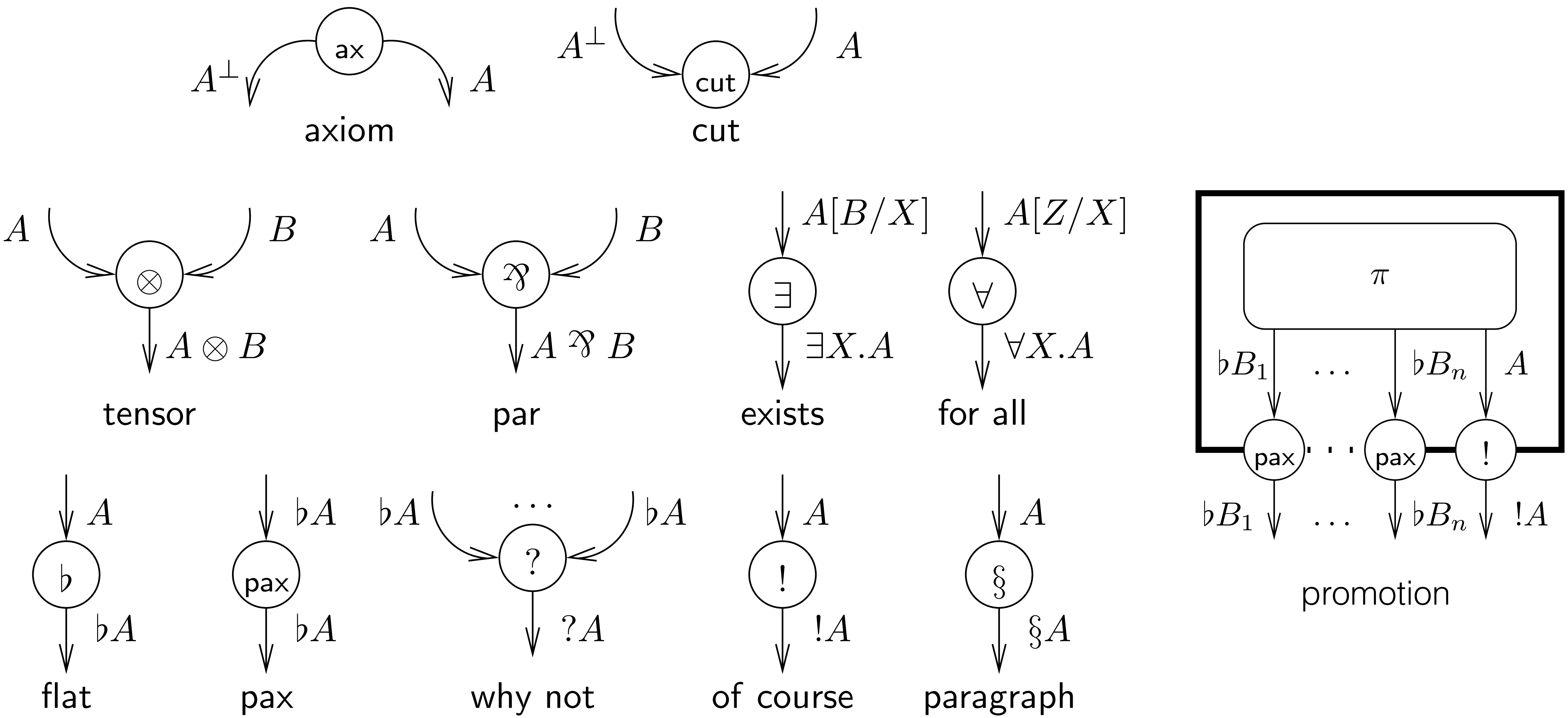
$$\frac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A}\ \text{Contraction}$$

$$\frac{}{\vdash}\ \text{Daimon}$$

$$\frac{\vdash \Gamma \quad \vdash \Delta}{\vdash \Gamma, \Delta}\ \text{Mix}$$

$$\boxed{\frac{\vdash \Gamma, A}{\vdash \Gamma, \S A}\ \text{Paragraph}}$$

Proof-net links



Note: paragraph is used for polytime, not needed to encode elementary time functions.

Baillot, Mazza "Linear logic by levels and bounded time complexity", 2009.

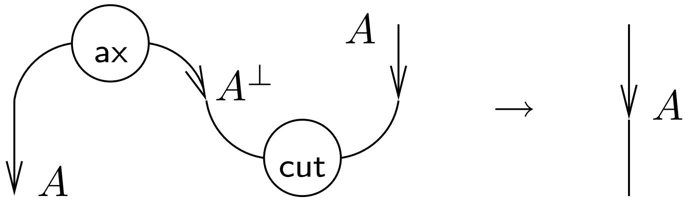


Figure 4: Axiom step.

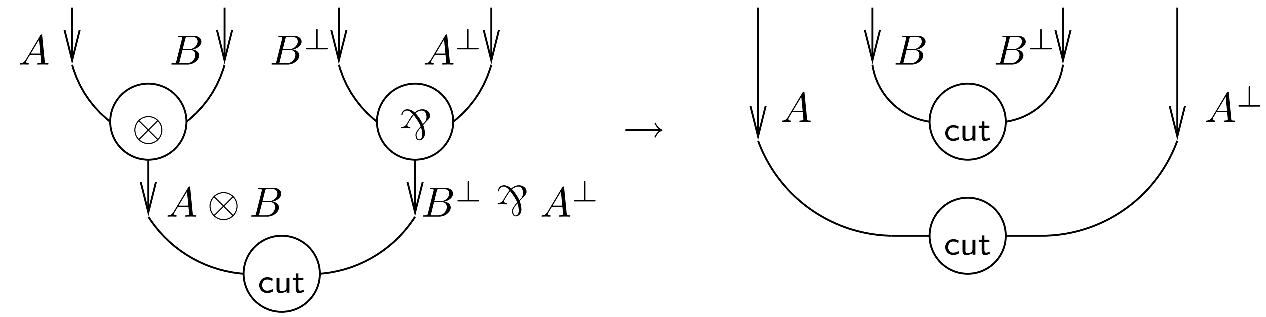


Figure 5: Multiplicative step.

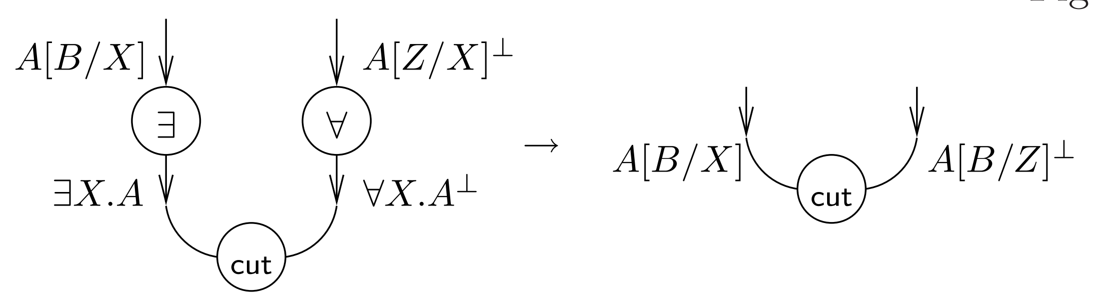


Figure 6: Quantifier step; the substitution is performed on the whole net.

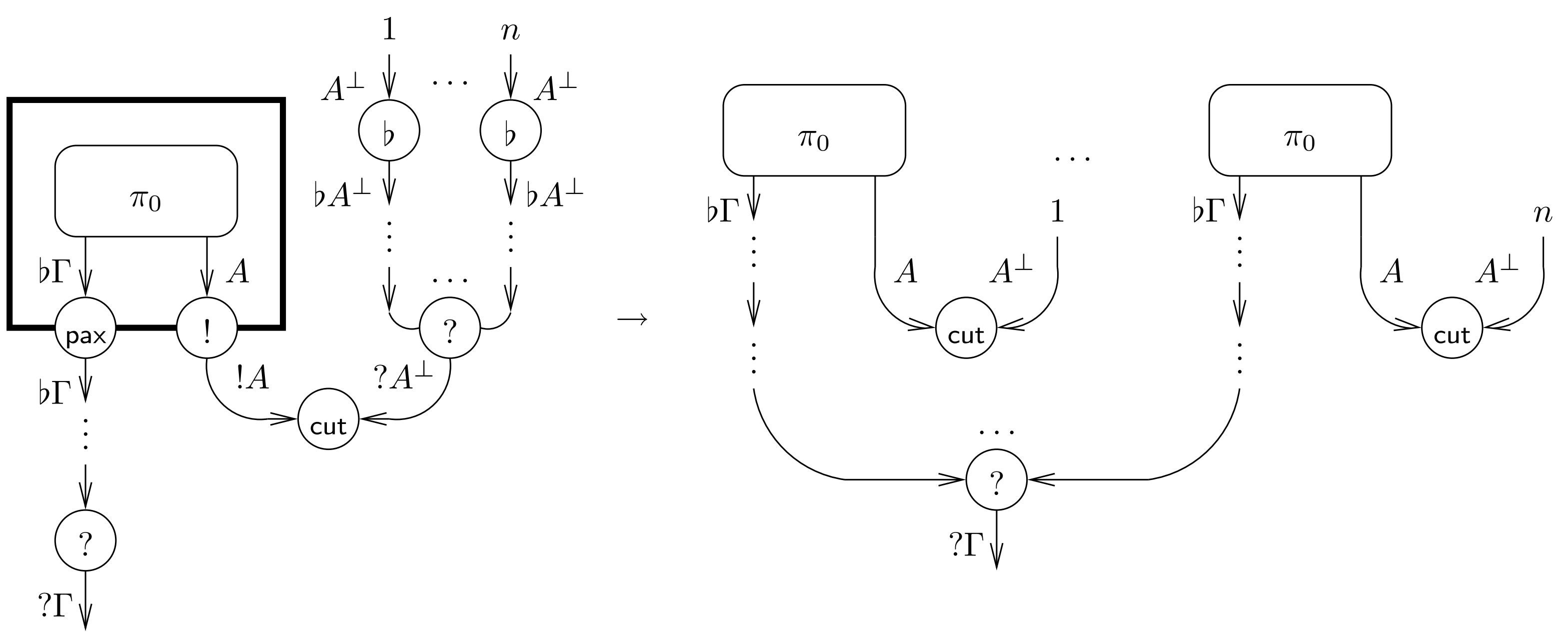


Figure 7: Exponential step; $\flat\Gamma$ is a multiset of discharged formulas, so one pax link, why not link, or wire in the picture may in some case stand for several (including zero) pax links, why not links, or wires.

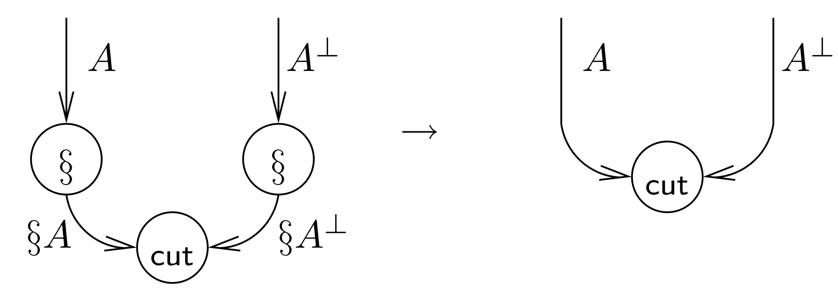


Figure 8: Paragraph step.

Indexing of proof-nets

Definition 12 (Indexing) *Let π be a* **meLL** *net. An indexing for π is a function I from the edges of π to $\mathbb{Z}$ satisfying the constraints given in Fig. 11 and such that, for all conclusions e, e' of π, $I(e) = I(e')$.*

[BM] Prop 5, 6

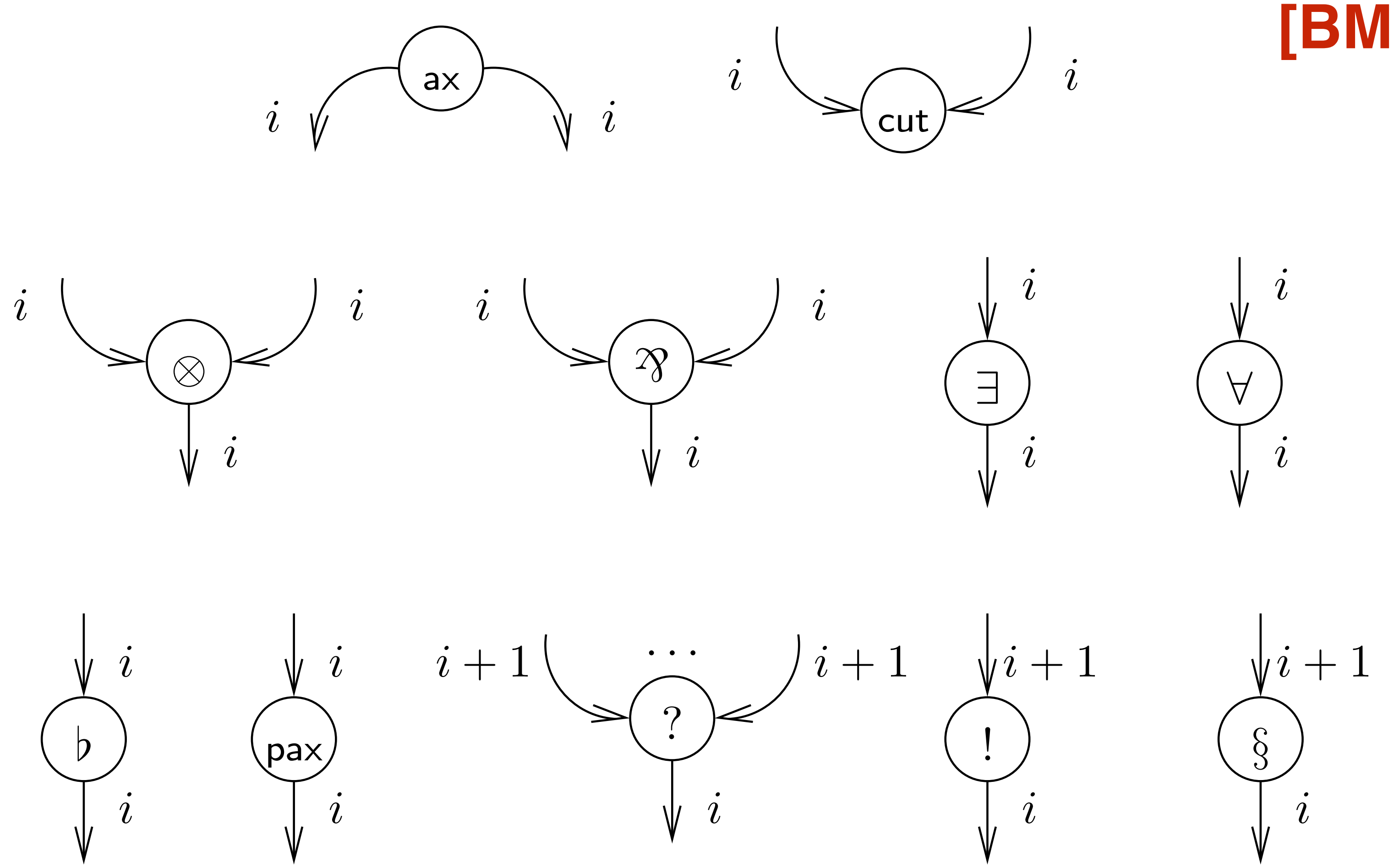


Figure 11: Constraints for indexing **meLL** proof nets. Next to each edge we represent the integer assigned by the indexing; formulas are omitted, because irrelevant to the indexing.

Definition 13 (Multiplicative linear logic by levels) *Multiplicative linear logic by levels* (**mL³**) *is the logical system defined by taking all* **meLL** *proof nets admitting an indexing.*

Theorem to be proven

Below, we use the notation 2^n_k with the following meaning: for all n, $2^n_0 = n$, and $2^n_{k+1} = 2^{2^n_k}$.

Definition 2 (Depth, size) *Let σ be a pre-net.*

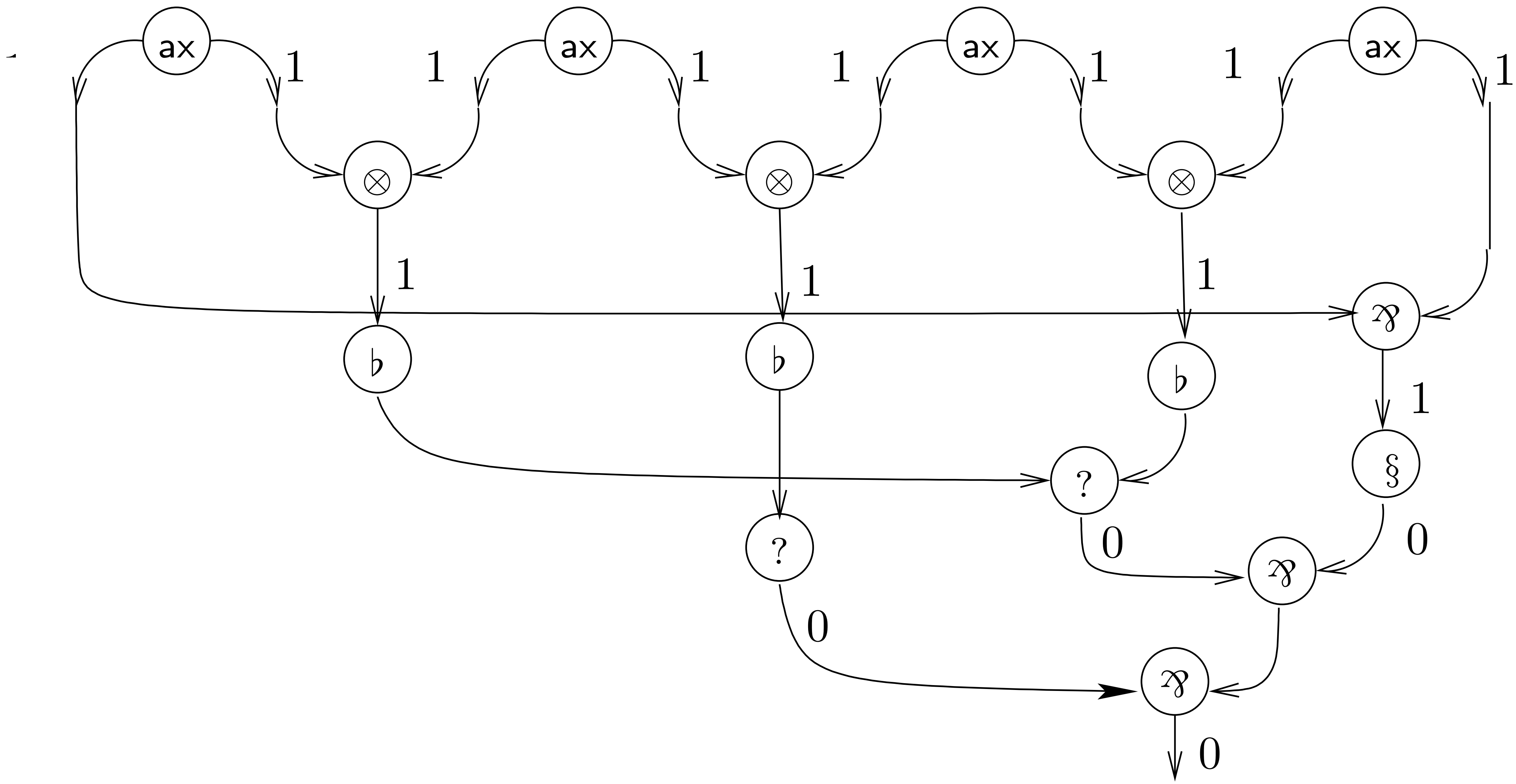
- *A link (or edge) of σ is said to have* depth *d if it is contained in d (necessarily nested) boxes. The depth of a box of σ is the depth of the links forming its border. The depth of a link l, edge e, or box $\mathcal{B}$ are denoted resp. by $\mathrm{d}(l)$, $\mathrm{d}(e)$ and $\mathrm{d}(\mathcal{B})$. The depth of σ, denoted by $\mathrm{d}(\sigma)$, is the maximum depth of its links.*

- *The* size *of σ, denoted by $|\sigma|$, is the number of links contained in σ, excluding auxiliary ports.*

Definition 15 (Level) *Let π be an $\mathbf{mL^3}$ proof net, and let I_0 be its canonical indexing. The* level *of π, denoted by $\ell(\pi)$, is the maximum integer assigned by I_0 to the edges of π. If l is a link of π of conclusion e (or of conclusions e_1, e_2 in the case of an* axiom *link), and if $\mathcal{B}$ is a box of π whose principal port has conclusion e', we say that the level of l, denoted by $\ell(l)$, is $I_0(e)$ (or $I_0(e_1) = I_0(e_2)$ in the case of an axiom), and that the level of $\mathcal{B}$, denoted by $\ell(\mathcal{B})$, is $I_0(e')$.*

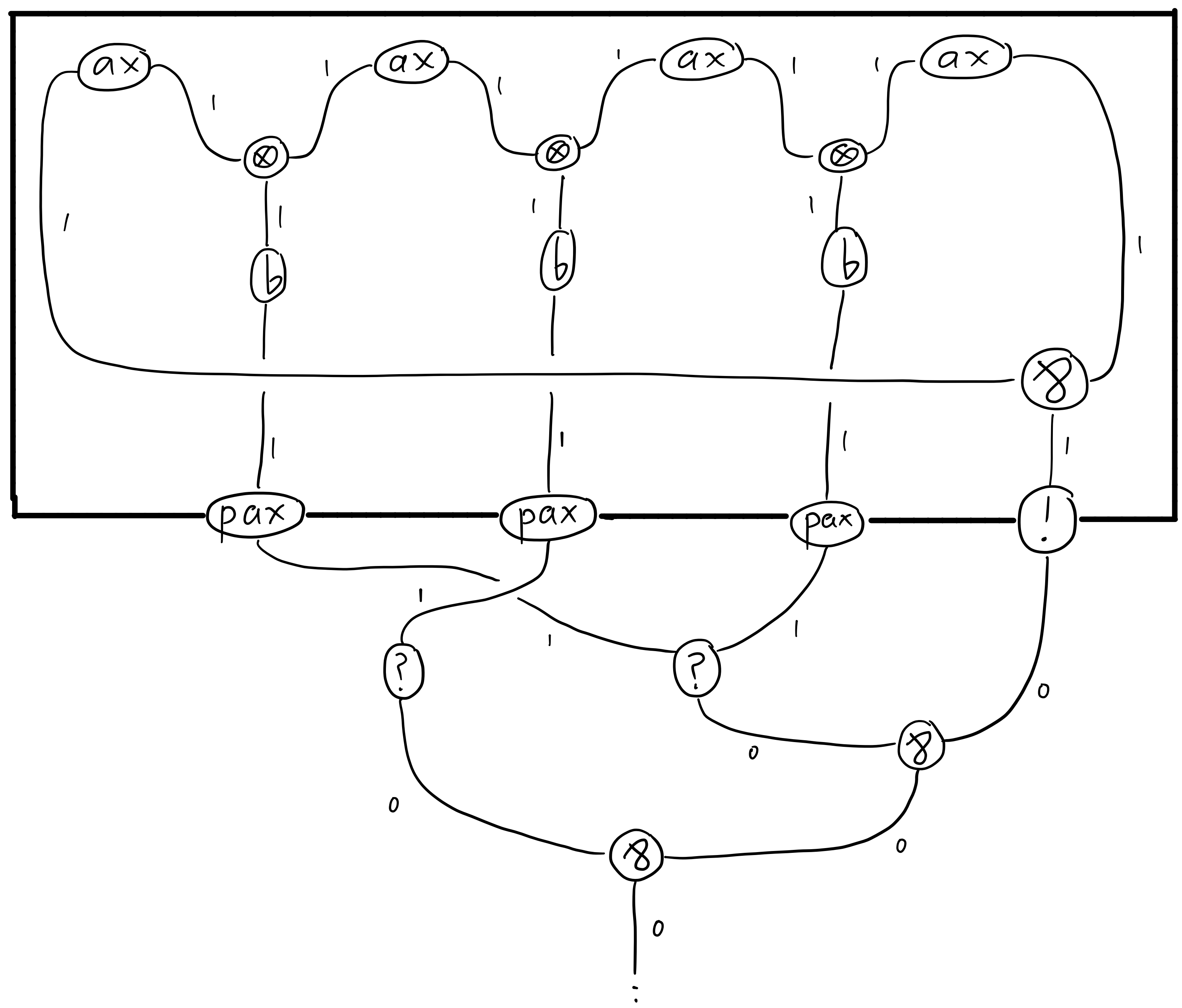
Theorem 16 (Elementary bound for $\mathbf{mL^3}$) *Let π be an $\mathbf{mL^3}$ proof net of size s and level l. Then, the round-by-round procedure reaches a normal form in at most $(l+1)2^s_{2l}$ steps.*

First encoding of 101 in mL3



$$\mathbf{bint}^{\S} = \forall\alpha\ !(\alpha \multimap \alpha) \multimap \big(!(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha)\big)$$

Second encoding of 101 in mL3



$$\mathbf{bint}^! = \forall\alpha\ !(\alpha \multimap \alpha) \multimap \big(!(\alpha \multimap \alpha) \multimap !(\alpha \multimap \alpha)\big)$$

Level $\neq$ depth

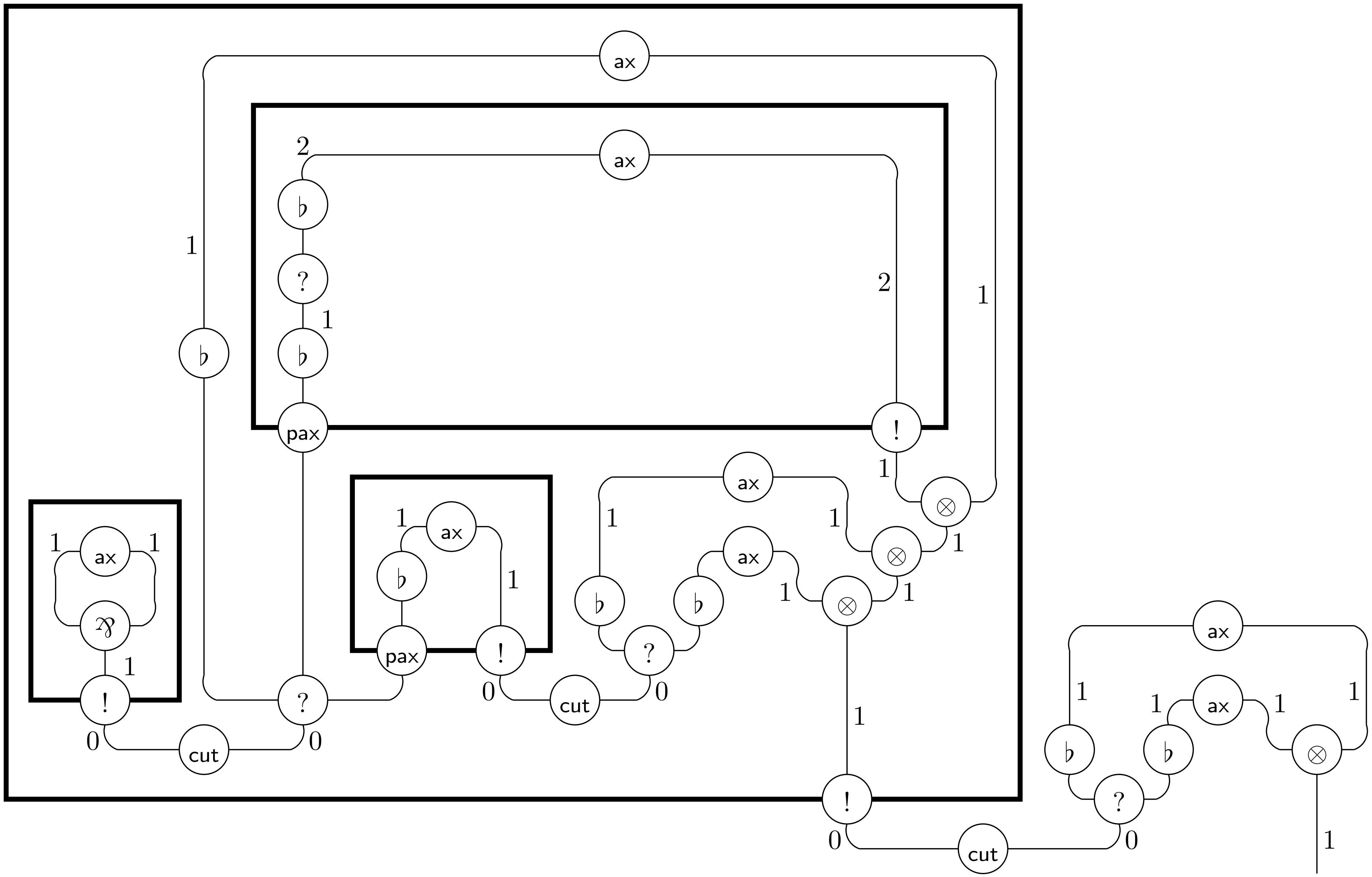


Figure 15: An example of nested boxes of identical level (much smaller examples exist; we gave this one because we shall re-use it later on for different purposes).

Round by round procedure for reduction

(Here proof net = untyped proof net)

Definition 17 (Isolevel tree) *Let π be a* **meLL** *proof net, and let e be an edge of π which is the conclusion of a link l different from* flat *or* pax*. The* isolevel tree *of e is defined by induction as follows:*

- *if l is an* axiom, why not, of course, *or* paragraph *link, then the isolevel tree of e consists of the link l alone;*
- *otherwise, let $e_1, \ldots, e_k$ (with $k \in \{1, 2\}$) be the premises of l; then, the isolevel tree of e is the tree whose root is l and whose immediate subtrees are the isolevel trees of $e_1, \ldots, e_k$.*

Definition 18 (Complexity of reducible cuts) *Let π be a* **meLL** *proof net, and let c be a reducible* cut *link of π, whose premises are e_1, e_2. The* complexity *of c, denoted by $\sharp c$, is the sum of the number of nodes contained in the isolevel trees of e_1 and e_2. (Note that the isolevel trees of e_1, e_2 are always defined because the premises of a* cut *can never be conclusions of* flat *or* pax *links).*

Definition 19 (Weight of an $\mathbf{mL^3}$ proof net) *Let π be an* $\mathbf{mL^3}$ *proof net of level l. If $k \in \mathbb{Z}$, we denote by $\mathsf{cuts}_k(\pi)$ the set of reducible* cut *links of π at level k. The* weight *of π, denoted by α_π, is the function from $\mathbb{N}$ to $\mathbb{N}$ defined as follows:*

$$\alpha_\pi(i) = \sum_{c \in \mathsf{cuts}_{l-i}(\pi)} \sharp c.$$

[BM] Contractive order

Round by round procedure for reduction

Definition 21 (Cut order) *Let π be an $\mathbf{mL^3}$ proof net, and let* $\mathsf{cuts}(\pi)$ *be the set of reducible* cut *links of π. We turn* $\mathsf{cuts}(\pi)$ *into a partially ordered set by posing, for $c, c' \in \mathsf{cuts}(\pi)$, $c \leq c'$ iff one of the following holds:*

- $\ell(c) < \ell(c')$;

Or $\ell(c) = \ell(c')$ and

- *c is non-contractive and c' is contractive;*
- *c and c' are both contractive, involving resp. the boxes $\mathcal{B}$ and $\mathcal{B}'$, and $\mathcal{B} \preceq \mathcal{B}'$.*

From now on, we shall only consider the cut-elimination procedure given by the proof of Lemma 12, i.e., the one reducing only minimal cuts in the cut order. More concretely, given an $\mathbf{mL^3}$ proof net π, this procedure chooses a cut to be reduced in the following way:

1. find the lowest level at which reducible cuts are present in π, say i;
2. if non-contractive cuts are present at level i, choose any of them and reduce it;
3. if only contractive cuts are left, chose one involving a minimal box in the contractive order.

Proofs

Lemma 12 *Let π be an* $\mathbf{mL^3}$ *proof net which is not normal. Then, there exists π' such that $\pi \to \pi'$ and $\alpha_{\pi'} < \alpha_\pi$.*

Proposition 13 (Untyped weak normalization) *Untyped* $\mathbf{mL^3}$ *proof nets are weakly normalizable.*

Definition 22 *Let π be an* $\mathbf{mL^3}$ *proof net.*

1. *The* size of level i *of π, denoted by $|\pi|_i$, is the number of links at level i of π different from auxiliary ports.*
2. *π is* i-normal *iff it contains no reducible* cut *link at all levels $j \leq i$.*
3. *π is* i-contractive *iff it is $(i-1)$-normal and contains only contractive* cut *links at level i.*

Lemma 14 *Let π be an $(i-1)$-normal proof net. Then, the round-by-round procedure reaches an i-normal proof net in at most $|\pi|_i$ steps.*

Lemma 15 *Let π be an i-contractive proof net, such that $\pi \to^* \pi'$ under the round-by-round procedure, with π' i-normal. Then, $|\pi'| \leq 2_2^{|\pi|}$.*

Theorem 16 (Elementary bound for $\mathbf{mL^3}$) *Let π be an* $\mathbf{mL^3}$ *proof net of size s and level l. Then, the round-by-round procedure reaches a normal form in at most $(l+1)2_{2l}^{s}$ steps.*

Admits stratification = elementary time

$$\mathbf{bint}^! = \forall \alpha \ !(\alpha \multimap \alpha) \multimap \big(!(\alpha \multimap \alpha) \multimap !(\alpha \multimap \alpha)\big)$$

Theorem (Girard, Baillot-Mazza, Danos-Joinet, Mairson-Terui)

A function $f : \{0,1\}^* \longrightarrow \{0,1\}^*$ is elementary time if and only if it can be typed as a proof in $\mathbf{mL}^3$ of level d with conclusion $(\mathbf{bint}^!)^\perp, !^d\mathbf{bint}^!$.

Admits stratification + restricted promotion = polytime

$$\mathbf{bint}^{\S} = \forall\alpha\ !(\alpha \multimap \alpha) \multimap \big(!(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha)\big)$$

Definition 16 (Multiplicative light linear logic by levels) *Multiplicative light linear logic by levels* ($\mathbf{mL^4}$) *is the logical system composed of all* $\mathbf{mL^3}$ *proof nets* π *satisfying the following conditions:*

(Weak) Depth-stratification: *Each exponential branch (Definition 8) of* π *crosses at most one auxiliary port.*

Lightness: *Each box of* π *has at most one auxiliary port.*

Theorem 23 (Polynomial bound for $\mathbf{mL^4}$) *Let* π *be an* $\mathbf{mL^4}$ *proof net of size* s, *level* l, *and relative depth* r. *Then, the round-by-round procedure reaches a normal form in at most* $(l+1)s^{(r+2)^l}$ *steps.*

Theorem (Girard, Baillot-Mazza, Danos-Joinet, Mairson-Terui)

A function $f : \{0,1\}^* \longrightarrow \{0,1\}^*$ is polytime if and only if it can be typed as a proof in $\mathbf{mL}^4$ of level d with conclusion $(\mathbf{bint}^{\S})^{\perp}, \S^d\mathbf{bint}^{\S}$.