

Context Semantics, Linear Logic and Computational Complexity*

Ugo Dal Lago

Laboratoire d'Informatique de Paris-Nord

Université Paris 13, France

dallago@lipn.univ-paris13.fr

Abstract

We show that context semantics can be fruitfully applied to the quantitative analysis of proof normalization in linear logic. In particular, context semantics lets us define the weight of a proof-net as a measure of its inherent complexity: it is both an upper bound to normalization time (modulo a polynomial overhead, independently on the reduction strategy) and a lower bound to the number of steps to normal form (for certain reduction strategies). Weights are then exploited in proving strong soundness theorems for various subsystems of linear logic, namely elementary linear logic, soft linear logic and light linear logic.

1 Introduction

Linear logic has always been claimed to be resource-conscious: structural rules are applicable only when the involved formulas are modal, i.e. in the form $!A$. Indeed, while (multiplicative) linear logic embeds intuitionistic logic, restricting the rules governing the exponential operator $!$ leads to characterizations of interesting complexity classes [2, 12, 16]. On the other hand, completely forbidding duplication highlights strong relations between proofs and boolean circuits [20]. These results demonstrate the relevance of linear logic in implicit computational complexity, where the aim is obtaining machine-independent, logic-based characterization of complexity classes. Nevertheless, relations between copying and complexity are not fully understood yet. Is copying the real “root” of complexity? Can we give a complexity-theoretic interpretation of Girard’s embedding $A \rightarrow B \equiv !A \multimap B$? Bounds on normalization time for different fragments of linear logic are indeed obtained by ad-hoc techniques which cannot be easily generalized.

Context semantics [14] is a powerful framework for the analysis of proof and program dynamics. It can be considered as a model of Girard’s geometry of interaction [10, 9] where the underlying algebra consists of *contexts*. Context semantics and the geometry of interaction have been used to prove the correctness of optimal reduction algorithms [14] and in the design of sequential and parallel interpreters for the lambda calculus [17, 18]. There are evidences that these semantic frameworks are useful in capturing quantitative as well as qualitative properties of programs. The inherent computational difficulty of normalizing a proof has indeed direct counterpart in its interpretation. It is well known that strongly normalizing proofs are exactly the ones having finitely many so-called regular paths in the geometry of interaction [7]. A class of proof-nets which are not just strongly normalizing but normalizable in elementary time can still be captured in the geometry of interaction framework, as suggested by Baillot and Pedicini [3]. Until recently, it was not known whether this correspondence scales down to smaller complexity classes, such as the one of polynomial time computable functions. The usual measure based on the length of regular paths cannot be used, since there are proof-nets which can be normalized in polynomial time but whose regular paths have exponential length (as we are going to show in the following). Context semantics has been recently exploited by the author in the quantitative analysis of linear lambda calculi with higher-order recursion [4]. Noticeably, context semantics is powerful enough to induce bounds on the algebraic potential size of terms, a parameter which itself bounds normalization time (up to a polynomial overhead). From existing literature, it is not clear whether similar results can be achieved for linear logic, where exponentials take the place of recursion in providing the essential expressive power.

*The author is partially supported by PRIN project FOLLIA (2004) and ANR project NOCOST (2005).

In this paper, we show that context semantics reveals precise quantitative information on the dynamics of second order multiplicative and exponential linear logic. More specifically, a weight W_G is assigned to every proof-net G in such a way that:

- Both the number of steps to normal form *and* the size of any reduct of G are bounded by $p(W_G, |G|)$, where $p : \mathbb{N}^2 \rightarrow \mathbb{N}$ is a fixed polynomial and $|G|$ is the size of G .
- There is a reduction strategy which *realizes* W_G , i.e. there is a proof-net H such that $G \rightarrow^{W_G} H$.

In other words, we show that context semantics is somehow “fully-abstract” with respect to the operational theory equating all proofs having the same quantitative behaviour (modulo a fixed polynomial and considering all reduction strategies).

Moreover, studying W_G is easier than dealing directly with the underlying syntax. In particular, we here prove strong soundness theorems (any proof can be reduced in a bounded amount of time, independently on the underlying reduction strategy) for various subsystems of multiplicative linear logic by studying how restricting exponential rules reflect to W_G . These proofs are simpler than similar ones from the literature [12, 2, 19, 16], which in many cases refer to weak rather than strong soundness.

The weight W_G of a proof-net G will be defined from the context semantics of G following two ideas:

- The cost of a given box inside G is the number of times it can possibly be copied during normalization;
- The weight of G is the sum of costs of boxes inside G , where boxes that are inside other boxes are possibly counted more than once.

As a consequence, W_G only takes into account the exponential portion of G and is null whenever G does not contain any instance of the exponential rules.

We are going to define context semantics in a style which is very reminiscent of the one used by Danos and Regnier when defining their interaction abstract machine (IAM, see [8]). There are, however, some additional rules that makes the underlying machine not strictly bideterministic. As we will detail in the rest of the paper, the added transition rules are essential to capture the quantitative behaviour of proofs under every possible reduction strategy.

The rest of this paper is organized as follows. In Section 2, we will define linear logic as a sequent calculus and as a system of proof-nets. In Section 3, context semantics is defined and some examples of proof-nets are presented, together with their interpretation. Section 4 is devoted to relationships between context semantics and computational complexity and presents the two main results. Section 5 describe how context semantics can be useful in studying subsystems of linear logic, namely elementary linear logic, soft linear logic and light linear logic. This is the full version of a recently appeared extended-abstract [5].

2 Syntax

We here introduce multiplicative linear logic as a sequent calculus. Then, we will show how a proof-net can be associated to any sequent-calculus proof. The results described in the rest of this paper are formulated in terms of proof-nets.

The language of *formulae* is defined by the following productions:

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

where α ranges over a countable set of *atoms*. The rules in Figure 1 define a sequent calculus for (intuitionistic) multiplicative and exponential linear logic (with second order). We shall use $\text{MELL}_{\multimap \otimes \forall}$ as a shorthand for this system. In this way, we are able to easily identify interesting fragments, such as the propositional fragment $\text{MELL}_{\multimap \otimes}$ or the implicative fragment MELL_{\multimap} . Observe the Girard’s translation $A \rightarrow B \equiv !A \multimap B$ enforces the following embeddings:

- Simply-typed lambda calculus into MELL_{\multimap} .
- Intuitionistic propositional logic into $\text{MELL}_{\multimap \otimes}$.
- Intuitionistic second-order logic into $\text{MELL}_{\multimap \otimes \forall}$.

Proof-nets [11] are graph-like representations for proofs. We here adopt a system of intuitionistic proof-nets; in other words, we do not map derivations in $\text{MELL}_{\multimap \otimes \forall}$ to usual, classical, proof-nets.

Let \mathcal{L} be the set

$$\{R_{\multimap}, L_{\multimap}, R_{\otimes}, L_{\otimes}, R_{\forall}, L_{\forall}, R_{!}, L_{!}, W, X, D, N, P, C\}$$

A *proof-net* is a graph-like structure G . It can be defined inductively as follows: a proof-net is either the graph in Figure 2(a) or one of those in Figure 3 where G, H are themselves proof-nets as in Figure 2(b). If G is a proof-net, then V_G denotes the set of vertices of G , E_G denotes the set of direct edges of G , α_G is a labelling functions mapping every vertex in V_G to an

$$\begin{array}{c}
\frac{}{A \vdash A} A \quad \frac{\Gamma \vdash A \quad \Delta, A \vdash B}{\Gamma, \Delta \vdash B} U \quad \frac{\Gamma \vdash B}{\Gamma, !A \vdash B} W \quad \frac{\Gamma, !A, !A \vdash B}{\Gamma, !A \vdash B} X \\
\\
\frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B} R_{\multimap} \quad \frac{\Gamma \vdash A \quad \Delta, B \vdash C}{\Gamma, \Delta, A \multimap B \vdash C} L_{\multimap} \quad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B} R_{\otimes} \quad \frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C} L_{\otimes} \\
\\
\frac{A_1, \dots, A_n \vdash B}{!A_1, \dots, !A_n \vdash !B} P! \quad \frac{A, \Gamma \vdash B}{!A, \Gamma \vdash B} D! \quad \frac{!!A, \Gamma \vdash B}{!A, \Gamma \vdash B} N! \quad \frac{\Gamma \vdash A \quad \alpha \notin FV(\Gamma)}{\Gamma \vdash \forall \alpha. A} R_{\forall} \quad \frac{\Gamma, A\{B/\alpha\} \vdash C}{\Gamma, \forall \alpha. A \vdash C} L_{\forall}
\end{array}$$

Figure 1. A sequent calculus for MELL

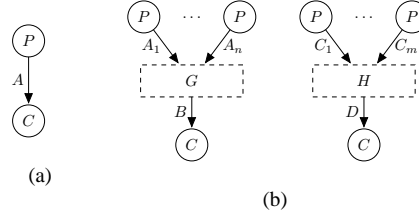


Figure 2. Base cases.

element of \mathcal{L} and β_G maps every edge in E_G to a formula. We do not need to explicitly denote axioms and cuts by vertices in V_G .

Note that each of the rules in figures 2(a) and 3 closely corresponds to a rule in the sequent calculus. Given a sequent calculus proof π , a proof-net G_π corresponding to π can be built. We should always be able to distinguish edges which are incident to a vertex v . In particular, we assume the existence of an order between them, which corresponds to the clockwise order in the graphical representation of v . Nodes labelled with C (respectively, P) mark the conclusion (respectively, the premises) of the proof-net. Notice that the rule corresponding to $P!$ (see Figure 3) allows seeing interaction graphs as nested structures, where nodes labelled with $R!$ and $L!$ delimit a *box*. If $e \in E_G$, $\theta_G(e)$ denotes the vertex labelled with $R!$ delimiting the box containing e (if such a box exists, otherwise $\theta_G(e)$ is undefined). If $v \in V_G$, $\theta_G(v)$ has the same meaning. If v is a vertex with $\alpha_G(v) = R!$, then $\rho_G(v)$ denotes the edge departing from v and going outside the box. Expressions $\sigma_G(e)$ and $\sigma_G(v)$ are shorthand for $\rho_G(\theta_G(e))$ and $\rho_G(\theta_G(v))$, respectively.

If $e = (u, v) \in E_G$, and $\alpha_G(u) = R!$, then e is said to be a *box-edge*. B_G is the set of all box-edges of G . Given a box-edge e , $P_G(e)$ is the number of premises of the box. I_G is the set of all vertices $v \in V_G$ with $\alpha_G(v) \notin \{R!, L!\}$. If $v \in V_G$, then $\partial(v)$ is the so-called box-depth of v , i.e. the number of boxes where v is included; similarly, $\partial(e)$ is the box-depth of $e \in E_G$, while $\partial(G)$ is the box-depth of the whole proof-net G . The size $|G|$ of a proof-net G is simply $|V_G|$.

Cut elimination is performed by graph rewriting in proof-nets. There are eight different rewriting rules \rightarrow_S , where $S \in \mathcal{C} = \{\multimap, \otimes, \forall, !, X, D, N, W\}$. We distinguish three linear rewriting rules (see figure 4) and five exponential rewriting rules (see figure 5). If $\mathcal{Q} \subseteq \mathcal{C}$, then $\rightarrow_{\mathcal{Q}}$ is the union of \rightarrow_S over $S \in \mathcal{Q}$. The relation \rightarrow is simply $\rightarrow_{\mathcal{C}}$. The notion of a normal form proof-net is the usual one. A *cut edge* is the edge linking two nodes interacting in a cut-elimination step. In figures 4 and 5, e is always a cut edge. If $S \in \mathcal{C}$, an edge linking two nodes that interact in \rightarrow_S is called an S -cut.

Given a proof-net G , the expression $\|G\|_{\rightarrow}$ denotes the natural number

$$\max_{G \rightarrow^* H} |H|.$$

The expression $[G]_{\rightarrow}$ denotes the natural number

$$\max_{G \rightarrow^n H} n.$$

These are well-defined concepts, since the calculus is strongly normalizing.

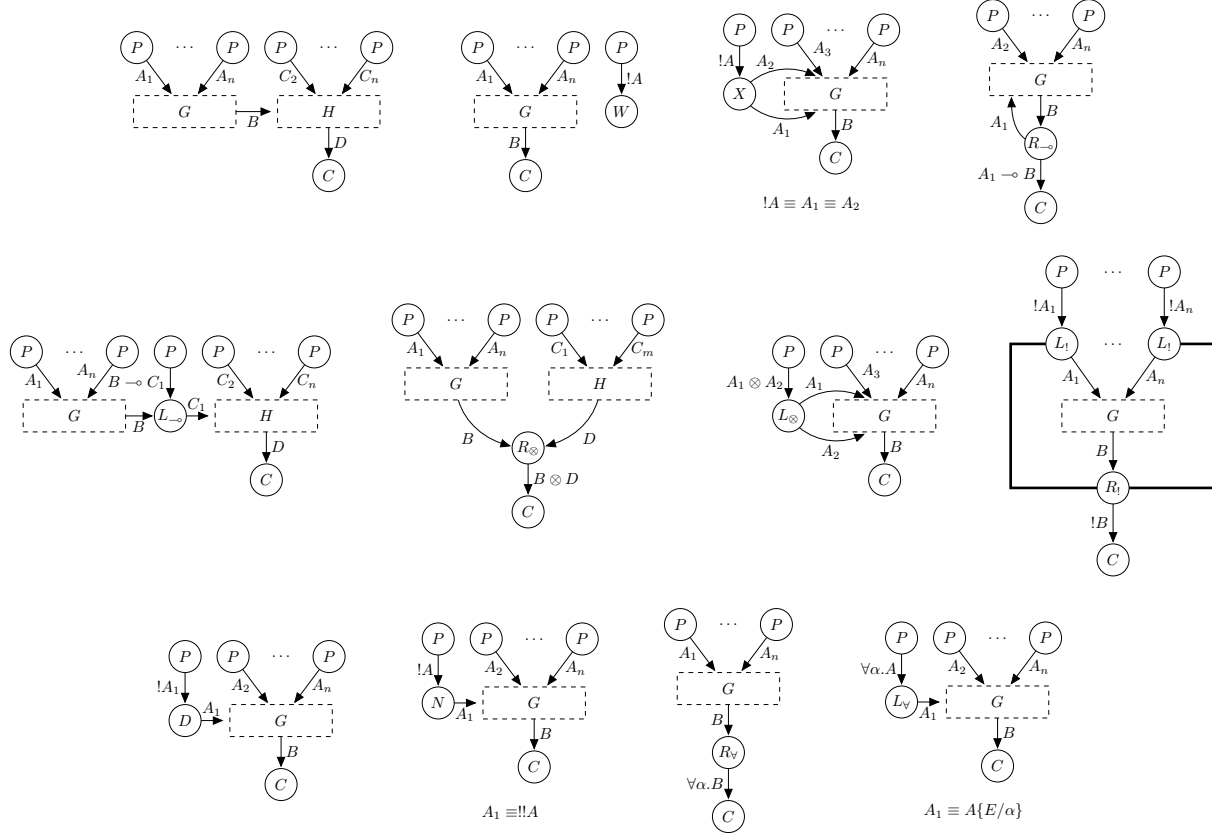


Figure 3. Inductive cases

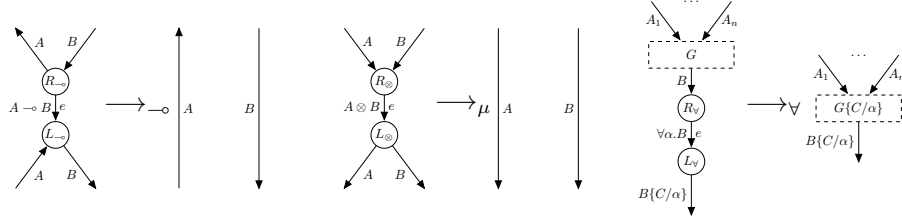


Figure 4. Linear graph rewriting rules.

The relation \Rightarrow is a restriction on \rightarrow defined as follows: $G \Rightarrow H$ iff $G \rightarrow_S H$ where $S = W$ only in case any cut in G is a W -cut. This is a reduction strategy, i.e. $G \Rightarrow^* H$ whenever H is the normal form of G . Indeed, firing a W -cut can only introduce other W -cuts. The expressions $\|G\|_{\Rightarrow}$ and $[G]_{\Rightarrow}$ are defined in the obvious way, similarly to $\|G\|_{\rightarrow}$ and $[G]_{\rightarrow}$. Studying \Rightarrow is easier than studying \rightarrow . From a complexity point of view, this is not problematic, since results about \Rightarrow can be easily transferred to \rightarrow :

Lemma 1 (Standardization) *For every proof-net G , both $[G]_{\Rightarrow} = [G]_{\rightarrow}$ and $\|G\|_{\Rightarrow} = \|G\|_{\rightarrow}$.*

Proof. Whenever $G \rightarrow_W H \rightarrow_S J$ and $S \neq W$, there are K and $n \in \{1, 2\}$ such that $G \rightarrow_S K \rightarrow_W^n J$, because the two cut-elimination steps do not overlap with each other. As a consequence, for any sequence $M_1 \rightarrow \dots \rightarrow M_n$ there is another sequence $L_1 \Rightarrow \dots \Rightarrow L_m$ such that $L_1 = M_1$, $L_m = M_n$ and $m \geq n$. This proves the first claim. Now, observe that for any $1 \leq i \leq n$ there is j such that $|L_j| \geq |M_i|$: at any step a proof-net, H , disappears from the sequence being replaced by another one, K , but clearly $|G| \geq |H|$. This concludes the proof. \square

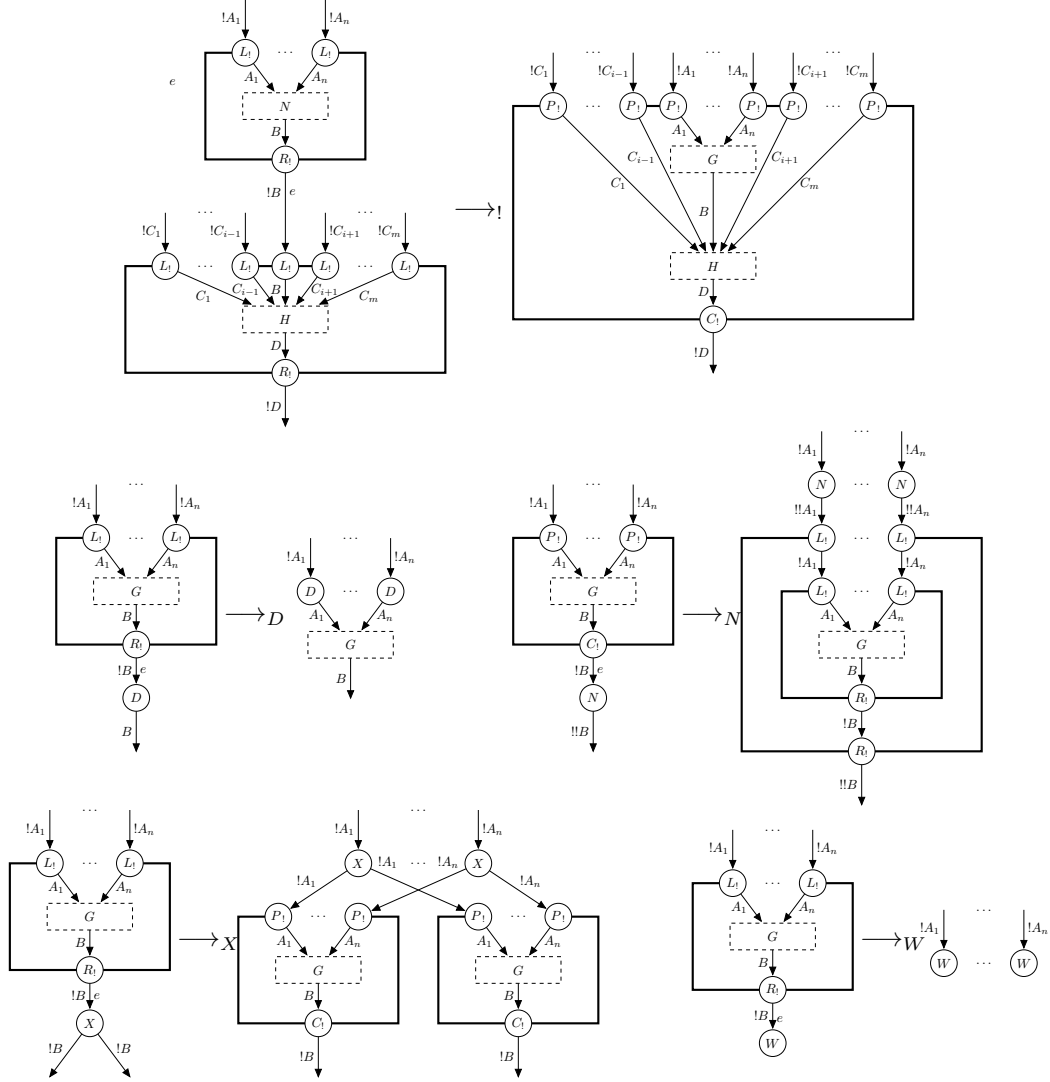


Figure 5. Exponential graph rewriting rules.

In the following, we will prove combinatorial properties of \Rightarrow that, by lemma 1, can be easily transferred to \longrightarrow . Consider the following further conditions on \Rightarrow :

1. For every $n \in \mathbb{N}$, a cut at level $n + 1$ is fired only when any cut at levels from 1 to n is a W -cut.
2. For every $n \in \mathbb{N}$, a $!$ -cut at level n is fired only when any cut at level n is either a W -cut or a $!$ -cut

These two conditions induce another relation \longrightarrow , which is itself a reduction strategy: note that firing a cut at level n does not introduce cuts at levels strictly smaller than n , while firing a $!$ -cut at level n only introduces cuts at level $n + 1$. As a consequence, \longrightarrow can be considered as a “level-by-level” strategy [2, 19].

3 Context Semantics

In this section, the context semantics of proof-nets is studied. The context semantics of a proof-net G allows to isolate certain paths among those in G , called *persistent* in the literature; studying the length and numerosity of persistent paths for a proof-net G helps inferring useful quantitative properties of G .

The first preliminary concept is that of an exponential signature. Exponential signatures are trees whose nodes are labelled with symbols e, r, l, p, n . They serve as contexts while constructing a path in a proof-net, similarly to what *context marks*

do in Gonthier, Abadi and Lévy's framework [15]. Label p has a special role and helps capturing the tricky combinatorial behavior of rule $N_!$ (see Figure 1). For similar reasons, a binary relation \sqsubseteq on exponential signatures is needed.

Definition 1 • The language \mathcal{E} of exponential signatures is defined by induction from the following sets of productions:

$$t, u, v, w ::= e \mid r(t) \mid l(t) \mid p(t) \mid n(t, t).$$

- A standard exponential signature is one that does not contain the constructor p . An exponential signature t is quasi-standard iff for every subtree $n(u, v)$ of t , the exponential signature v is standard.
- The binary relation \sqsubseteq on \mathcal{E} is defined as follows:

$$\begin{aligned} e &\sqsubseteq e; \\ r(t) &\sqsubseteq r(u) \Leftrightarrow t \sqsubseteq u; \\ l(t) &\sqsubseteq l(u) \Leftrightarrow t \sqsubseteq u; \\ p(t) &\sqsubseteq p(u) \Leftrightarrow t \sqsubseteq u; \\ p(t) &\sqsubseteq n(u, v) \Leftrightarrow t \sqsubseteq v; \\ n(t, u) &\sqsubseteq n(v, w) \Leftrightarrow t \sqsubseteq v \text{ and } u = w. \end{aligned}$$

If $u \sqsubseteq t$ then u is a simplification of t .

- A stack element is either an exponential signature or one of the following characters: a, o, s, f, x . \mathcal{S} is the set of stack elements. \mathcal{S} is ranged over by s, r .
- A polarity is either $+$ or $-$. \mathcal{B} is the set of polarities. The following notation is useful: $+\downarrow$ is $-$, while $-\downarrow$ is $+$. If n is a natural number $\text{parity}(n) = +$ if n is even, while $\text{parity}(n) = 0$ if n is odd.
- If $U \in \mathcal{S}^*$, then $\|U\|$ denotes the number of exponential signatures in U . If $s \in \{a, o, s, f, x\}$, then $|U|_s$ is the number of occurrences of s in U .

Please observe that if t is standard and $t \sqsubseteq u$, then $t = u$. Moreover, if t is quasi-standard and $u \sqsubseteq t$, then u is quasi-standard, too. The structure $(\mathcal{E}, \sqsubseteq)$ is a partial order:

Lemma 2 The relation \sqsubseteq is reflexive, transitive and antisymmetric.

Proof. The fact $t \sqsubseteq t$ can be proved by an induction on t . Similarly, if $t \sqsubseteq u$ and $u \sqsubseteq t$, then $t = u$ by induction on t . Finally, if $t \sqsubseteq u$ and $u \sqsubseteq v$, then $t \sqsubseteq v$ by induction on t . \square

We are finally ready to define the context semantics for a proof-net G . Given a proof-net G , the set of *contexts* for G is

$$C_G = E_G \times \mathcal{E}^* \times \mathcal{S}^+ \times \mathcal{B}.$$

Vertices of G with labels $R_{\multimap}, L_{\multimap}, R_{\otimes}, L_{\otimes}, R_{\forall}, L_{\forall}, R_!, L_!, X, D, N$ induce rewriting rules on C_G . These rules are detailed in Table 1 and Table 2. For any such rule

$$(e, U, V, b) \mapsto_G (g, W, Z, c),$$

the *dual* rule

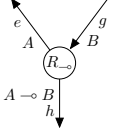
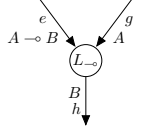
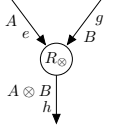
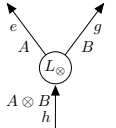
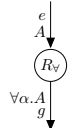
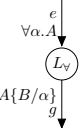
$$(g, W, Z, c\downarrow) \mapsto_G (e, U, V, b\downarrow).$$

holds as well. In other words, relation \mapsto_G is the smallest binary relation on C_G including every instance of rules in Table 1 and Table 2, together with every instance of their duals.

The role of the four components of a context can be intuitively explained as follows:

- The first component is an edge in the proof-net G . As a consequence, from every sequence $C_1 \mapsto_G C_2 \mapsto_G \dots \mapsto_G C_n$ we can extract a sequence e_1, e_2, \dots, e_n of edges. Rewriting rules in tables 1 and 2 enforce this sequence to be a path in G , i.e. e_i has a vertex in common with e_{i+1} . The only exception is caused by the last rule induced by boxes (see Table 2): in that case e and h do not share any vertex, but the two vertices v and w (which are adjacent to e and h , respectively) are part of the same box.
- The second component is a (possibly empty) sequence of exponential signatures which keeps track of which copies of boxes we are currently traveling into. More specifically, if e and U are the first and second components of a context, then the $\partial(e)$ rightmost exponential signatures in U correspond to copies of the $\partial(e)$ boxes where e is contained. Although the definition of a context does not prescribe this correspondence (U can be empty even if $\partial(e)$ is strictly positive), it is preserved by rewriting.

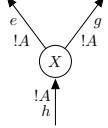


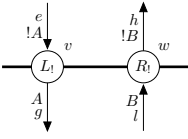
Table 1. Rewrite Rules for Vertices $R_{\multimap}, L_{\multimap}, R_{\otimes}, L_{\otimes}, R_{\forall}, L_{\forall}$

	$(e, U, V, -) \mapsto_G (h, U, V \cdot a, +)$ $(g, U, V, +) \mapsto_G (h, U, V \cdot o, +)$
	$(e, U, V \cdot a, +) \mapsto_G (g, U, V, -)$ $(e, U, V \cdot o, +) \mapsto_G (h, U, V, +)$
	$(e, U, V, +) \mapsto_G (h, U, V \cdot f, +)$ $(g, U, V, +) \mapsto_G (h, U, V \cdot x, +)$
	$(h, U, V \cdot f, +) \mapsto_G (e, U, V, +)$ $(h, U, V \cdot x, +) \mapsto_G (g, U, V, +)$
	$(e, U, V, +) \mapsto_G (g, U, V \cdot s, +)$
	$(e, U, V \cdot s, +) \mapsto_G (g, U, V, +)$

- The third component is a nonempty sequence of stack elements. It keeps track of the history of previously visited edges. In this way, the fundamental property called *path-persistence* is enforced: any path induced by the context semantics is preserved by normalization [15]. This property is fundamental for proving the correctness of optimal reduction algorithms [14], but it is not directly exploited in this paper. Notice that exponential signatures can float from the second component to the third component and vice versa (see the rules induced by vertices $R_!$ and $L_!$).
- The only purpose of the last component is forcing rewriting to be (almost) deterministic: for every C there is at most one context D such that $C \mapsto_G D$, except when $C = (e, U, t, -)$ and $e \in B_G$. In fact, $C \mapsto_G (g_i, U, t, -)$ for every i , where g_1, \dots, g_n are the premises of the box whose conclusion is e .

The way we have defined context semantics, namely by a set of contexts endowed with a rewrite relation, is fairly standard [14, 15]. In particular, our definition owes much to Danos and Regnier's Interaction Abstract Machine (IAM, see [8]). Both our machinery and the IAM are reversible, but while IAM can be considered as a bideterministic automaton, our context semantics cannot, due to the last rule induced by boxes. Noticeably, a fragment of MELL called light linear logic does enforce strong determinacy, as we will detail in Section 5. A property that holds for IAM as well as for our context semantics is reversibility: If $(e, U, V, b) \mapsto_G (g, W, Z, c)$, then $(g, W, Z, c \downarrow) \mapsto_G (e, U, V, b \downarrow)$.

Table 2. Rewrite Rules for Vertices X , D , N , L_l and R_l .

	$(h, U, V \cdot l(t), +) \mapsto_G (e, U, V \cdot t, +)$ $(h, U, V \cdot r(t), +) \mapsto_G (g, U, V \cdot t, +)$
	$(e, U, V \cdot e, +) \mapsto_G (g, U, V, +)$
	$(e, U, V \cdot n(t, u), +) \mapsto_G (g, U, V \cdot t \cdot u, +)$ $(e, U, p(t), +) \mapsto_G (g, U, t, +)$
	$(e, U, V \cdot t, +) \mapsto_G (g, U \cdot t, V, +)$ $(l, U \cdot t, V, +) \mapsto_G (h, U, V \cdot t, +)$ $(e, U, t, +) \mapsto_G (h, U, t, +)$

Although context semantics can be defined on sharing graphs as well, proof-nets have been considered here. Indeed, sharing graphs are more problematic from a complexity viewpoint, since a computationally expensive read-back procedure is necessary in order to retrieve the proof (or term) corresponding to a sharing graph in normal form (see [1]).

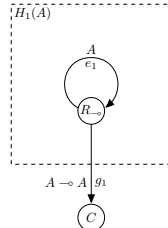
Observe that the semantic framework we have just introduced is *not* a model of geometry of interaction as described by Girard [10]. In particular, jumps between distinct conclusions of a box are not permitted in geometry of interaction, which is completely local in this sense. Moreover, algebraic equations induced by rule N are here slightly different. As we are going to see, this mismatch is somehow necessary in order to capture the combinatorial behavior of proofs independently on the underlying reduction strategy.

3.1 Motivating Examples

We now define some proof-nets together with observations about how context-semantics reflects the complexity of normalization.

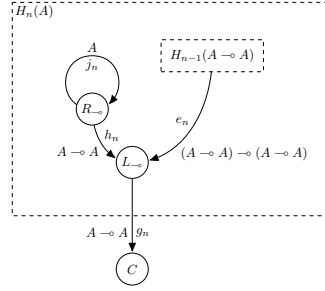
The first example (due to Danos and Regnier) is somehow discouraging: a family of proof-nets which normalize in polynomial time having paths of exponential lengths. For every positive natural number n and for every formula A , a proof-net $G_n(A)$ can be defined. We go by induction on n :

- The proof-net $G_1(A)$ is the following:



Notice we have implicitly defined a sub-graph $H_1(A)$ of $G_1(A)$.

- If $n > 1$, then $G_n(A)$ is the following proof-net:



Notice we have implicitly defined a sub-graph $H_n(A)$ of $G_n(A)$.

Although the size of $G_n(A)$ is $2n$ and, most important, $G_n(A)$ normalizes in $n - 1$ steps to $G_1(A)$, we can easily prove the following, surprising, fact: for every n , for every A and for every $V \in \mathcal{S}^*$,

$$\begin{aligned} (g_n, \varepsilon, V \cdot a, -) &\mapsto_{G_n(A)}^{f(n)} (g_n, \varepsilon, V \cdot o, +) \\ (g_n, \varepsilon, V \cdot o, -) &\mapsto_{G_n(A)}^{f(n)} (g_n, \varepsilon, V \cdot a, +) \end{aligned}$$

where $f(n) = O(2^n)$. Indeed, let $f(n) = 8 \cdot 2^{n-1} - 6$ for every $n \geq 1$ and proceed by an easy induction on n :

- If $n = 1$, then

$$\begin{aligned} (g_1, \varepsilon, V \cdot a, -) &\mapsto_{G_1(A)} (e_1, \varepsilon, V, +) \mapsto_{G_1(A)} (g_1, \varepsilon, V \cdot o, +) \\ (g_1, \varepsilon, V \cdot o, -) &\mapsto_{G_1(A)} (e_1, \varepsilon, V, -) \mapsto_{G_1(A)} (g_1, \varepsilon, V \cdot a, +) \end{aligned}$$

and $f(1) = 8 \cdot 2^0 - 6 = 2$.

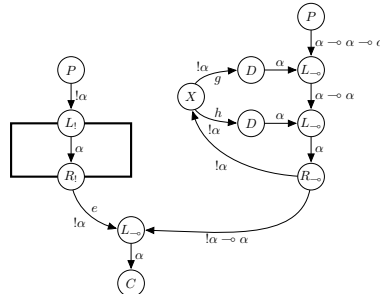
- If $n > 1$, then

$$\begin{aligned} (g_n, \varepsilon, V \cdot a, -) &\mapsto_{G_n(A)} (e_n, \varepsilon, V \cdot a \cdot o, -) \mapsto_{G_n(A)}^{f(n-1)} (e_n, \varepsilon, V \cdot a \cdot a, +) \\ &\mapsto_{G_n(A)} (h_n, \varepsilon, V \cdot a, -) \mapsto_{G_n(A)} (j_n, \varepsilon, V, +) \mapsto_{G_n(A)} (h_n, \varepsilon, V \cdot o, +) \\ &\mapsto_{G_n(A)} (e_n, \varepsilon, V \cdot o \cdot a, -) \mapsto_{G_n(A)}^{f(n-1)} (e_n, \varepsilon, V \cdot o \cdot o, +) \\ &\mapsto_{G_n(A)} (g_n, \varepsilon, V \cdot o, +) \\ (g_n, \varepsilon, V \cdot o, -) &\mapsto_{G_n(A)} (e_n, \varepsilon, V \cdot o \cdot o, -) \mapsto_{G_n(A)}^{f(n-1)} (e_n, \varepsilon, V \cdot o \cdot a, +) \\ &\mapsto_{G_n(A)} (h_n, \varepsilon, V \cdot o, -) \mapsto_{G_n(A)} (j_n, \varepsilon, V, -) \mapsto_{G_n(A)} (h_n, \varepsilon, V \cdot a, +) \\ &\mapsto_{G_n(A)} (e_n, \varepsilon, V \cdot a \cdot a, -) \mapsto_{G_n(A)}^{f(n-1)} (e_n, \varepsilon, V \cdot a \cdot o, +) \\ &\mapsto_{G_n(A)} (g_n, \varepsilon, V \cdot o, +) \end{aligned}$$

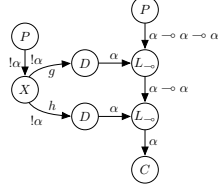
and $f(n) = 8 \cdot 2^{n-1} - 6 = 2 \cdot (8 \cdot 2^{n-2} - 6) + 6 = 2 \cdot f(n-1) + 6$.

In other words, proof-nets in the family $\{G_n(A)\}_{n \in \mathbb{N}}$ normalize in polynomial time but have exponentially long paths. The weights $W_{G_n(A)}$, as we are going to see, will be null. This is accomplished by focusing on paths starting from boxes, this in contrast to the execution formula [10], which takes into account conclusion-to-conclusion paths only.

The second example is a proof-net G :



Observe $G \longrightarrow^* H$ where H is the following cut-free proof:

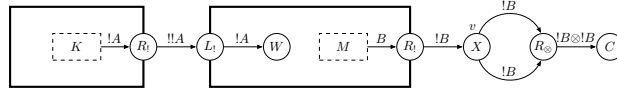


The proof-net G corresponds to a type derivation for the lambda-term $(\lambda x.yxx)z$, while H corresponds to a type derivation for yzx . There are finitely many paths in C_G , all of them having finite length. But the context semantics of G reflects the fact that G is strongly normalizing in another way, too: there are finitely many exponential signatures t such that $(e, \varepsilon, t, +) \mapsto_G^* (k, U, e, +)$, where $k \in E_G$ and $U \in \mathcal{E}^+$. We can concentrate on e since it is the only box-edge on G . In particular:

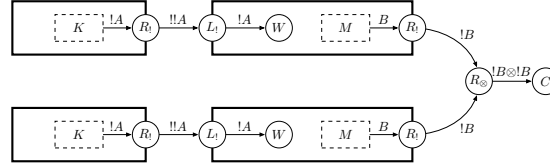
$$\begin{aligned} (e, \varepsilon, e, +) &\mapsto_G^* (e, \varepsilon, e, +) \\ (e, \varepsilon, r(e), +) &\mapsto_G^* (h, \varepsilon, e, +) \\ (e, \varepsilon, l(e), +) &\mapsto_G^* (g, \varepsilon, e, +) \end{aligned}$$

Intuitively, the exponential signature e corresponds to the initial status of the single box in G , while $l(e)$ and $r(e)$ correspond to the two copies of the same box appearing after some normalization steps. In the following section, we will formally investigate this new way of exploiting the context semantics as a method of studying the quantitative behavior of proofs.

Let us now present one last example. Consider the proof-net J :



The leftmost box (i.e. the box containing K) can interact with the vertex v and, as a consequence, can be copied:



However, there is not any persistent path (in the sense of [15]) between the box and v . The reason is simple: there is not any path between them. This mismatch shows why an extended notion of path encompassing jumps between box premises and conclusions is necessary in order to capture the quantitative behavior of proofs (at least if *every* reduction strategy is taken into account).

4 Context Semantics and Time Complexity

We are now in a position to define the weight W_G of a proof-net G . As already mentioned, W_G takes into account the number of times each box in G is copied during normalization. Suppose G contains a sub-net matching the left-hand side of the rule \longrightarrow_X . Then, there is a box-edge e in G such that the corresponding box will be duplicated at least once. In the context semantics, for every $t \in \{e, l(e), r(e)\}$ there are $g \in E_G$ and $V \in \mathcal{E}^*$ such that

$$(e, U, t, +) \mapsto_G^* (g, V, e, b). \quad (1)$$

As a consequence, we would be tempted to define the “weight” of any box-edge e as the number of “maximal” exponential signatures satisfying (1). What we need, in order to capture “maximality” is a notion of final contexts.

Definition 2 (Final Stacks, Final Contexts) *Let G be a proof-net. Then:*

- *First of all, we need to define what a final stack $U \in \mathcal{S}^+$ is. We distinguish positive and negative final stacks and define them mutually recursively:*

- A positive final stack is either e or $V \cdot a$ (where V is a negative final stack) or $V \cdot s$ (where $s \in \{o, f, x, s\}$ and V is a positive final stack) or $V \cdot e$ (where V is a positive final stack).
- A negative final stack is either $V \cdot a$ (where V is a positive final stack) or $V \cdot s$ (where $s \in \{o, f, x, s\}$ and V is a negative final stack) or $V \cdot t$ (where V is a negative final stack and t is an exponential signature).
- A context $C \in C_G$ is final iff one of the following four cases hold:
 - If $C = ((u, v), U, V, +)$, $\alpha_G(v) = W$ and V is a positive final stack;
 - If $C = ((u, v), U, V, +)$, $\alpha_G(v) = C$ and V is a positive final stack;
 - If $C = ((u, v), U, e, +)$ and $\alpha_G(v) = D$;
 - If $C = ((u, v), U, V, -)$, $\alpha_G(v) = P$ and V is a negative final stack;

Although the definition of a final stack is not trivial, the underlying idea is very simple: if we reach a final context C from $(e, U, t, +)$, then the exponential signature t must have been completely “consumed” along the path. Moreover, if C is final, then there are not any context D such that $C \mapsto_G D$. For example, the stack $e \cdot a \cdot n(e, e)$ is negative final, while $e \cdot a \cdot f \cdot a$ is positive final.

Now, consider exponential signatures t such that

$$(e, U, t, +) \mapsto_G^* C \quad (2)$$

where C is final. Apparently, (2) could take the place of (1) in defining what the weight of any box-edge should be. However, this does not work due to rewriting rule \rightarrow_N which, differently from \rightarrow_X , duplicates a *box* without duplicating its *content*. The binary relation \sqsubseteq will help us to manage this mismatch.

Definition 3 (Copies, Canonicity, Cardinalities) *Let G be a proof-net. Then:*

- A copy for $e \in B_G$ on $U \in \mathcal{E}^*$ (under G) is a standard exponential signature t such that for every $u \sqsubseteq t$ there is a final context C such that $(e, U, u, +) \mapsto_G^* C$.
 - A sequence $U \in \mathcal{E}^*$ is said to be canonical for $e \in E_G$ iff one of the following conditions holds:
 - $\theta_G(e)$ is undefined and U is the empty sequence;
 - $\theta_G(e) = v$, V is canonical for $\rho_G(v)$, t is a copy for $\rho_G(v)$ under V , and $U = V \cdot t$.
- $L_G(e)$ is the class of canonical sequences for e . If $v \in V_G$, then $L_G(v)$ is defined similarly.
- The cardinality $R_G(e, U)$ of $e \in B_G$ under $U \in \mathcal{E}^*$ is the number of different simplifications of copies of e under U . G has strictly positive weights iff $R_G(e, U) \geq 1$ whenever U is canonical for e .
 - A context $(e, U, t, +)$ is said to be cyclic for G iff $(e, U, t, +) \mapsto_G^+ (e, U, v, +)$.

Observe that $|U| = \partial(e)$ whenever U is a canonical sequence for e .

Consider a proof-net G , an edge $e \in B_G$ such that $\partial(e) = 0$ and let H be the box whose conclusion is e . Observe that the only canonical sequence for e is ε . Each copy of e under ε corresponds to a potential copy of the *content* of H . Indeed, if $g \in B_G$, $\partial(g) = 1$, and $\rho_G(g) = e$, canonical sequences for g are precisely the copies of e under ε . The cardinality $R_G(e, \varepsilon)$ will be the number of potential copies of H itself, which is not necessarily equal to the number of copies of e under ε : firing a N -cut causes a box to be copied, without its content (see Figure 5).

For every proof-net G , W_G is defined as follows:

$$W_G = \sum_{e \in B_G} \sum_{U \in L_G(e)} (R_G(e, U) - 1).$$

The quantity W_G is the *weight* of the proof-net G . As we will show later, W_G cannot increase during cut-elimination. However, it is not guaranteed to decrease at any cut-elimination step and, moreover, it is not necessarily a bound to the size $|G|$ of G . As a consequence, we need to define another quantity, called T_G :

$$T_G = \sum_{v \in I_G} |L_G(v)| + \sum_{e \in B_G} P_G(e) \sum_{U \in L_G(e)} (2R_G(e, U) - 1).$$

As we will show in the following, T_G is polynomially related to W_G . Since any box-edge $e \in B_G$ is charged for $P_G(e)$ in T_G , T_G is clearly greater or equal to $|G|$. Please notice that W_G and T_G can in principle be infinite.

We now analyze how W_G and T_G evolve during normalization. This will be carried out by carefully studying to which extent paths induced by contexts semantics are preserved during the process of cut-elimination. This task becomes easier once the notion of canonicity is extended to contexts:

Definition 4 (Cononical Contexts) A context $(e, U, V, \text{parity}(|V|_a)) \in C_G$ is said to be canonical iff U is canonical for e and whenever $V = W \cdot t \cdot Z$ the following two conditions hold:

1. Either $W = \varepsilon$ and t is quasi-standard or $W \neq \varepsilon$ and t is standard.
2. For every $u \sqsubseteq t$, it holds that $(e, U, u \cdot Z, \text{parity}(|Z|_a)) \mapsto_G^* C$, where $C \in C_G$ is a final context.

We denote with $A_G \subseteq C_G$ the set of canonical contexts.

Observe, in particular, that in any canonical context $(e, U, V, b) \in A_G$, U must be canonical for e . More importantly, please notice that if t is a copy for e on U and U is canonical for e , then $(e, U, t, +)$ as well as any context $(e, U, u, +)$ (where $u \sqsubseteq t$) are canonical. Canonicity of contexts is preserved by the relation \mapsto_G :

Lemma 3 If $C \in A_G$ and $C \mapsto_G D$, then $D \in A_G$.

Proof. A straightforward case-analysis suffices. We here consider some cases:

- Let $(e, U, V \cdot t, +) \mapsto_G (g, U \cdot t, V, +)$ and suppose $(e, U, V \cdot t, +)$ is canonical. Clearly, V must be different from ε and, as a consequence, t is standard. Moreover, $(e, U, u, +) \mapsto_G^* C$ whenever $u \sqsubseteq t$. This implies $U \cdot t$ is a canonical sequence for g . Now, suppose $V = W \cdot u \cdot Z$. Clearly, u is quasi-standard if $W = \varepsilon$ and standard if $W \neq \varepsilon$, because $(e, U, V \cdot t, +)$ is canonical. Moreover for every $v \sqsubseteq u$, either $(g, U \cdot t, v \cdot Z, c) \mapsto_G (e, U, v \cdot Z \cdot t, c)$ or $(e, U, v \cdot Z \cdot t, c) \mapsto_G (g, U \cdot t, v \cdot Z, c)$. This implies $(g, U \cdot t, v \cdot Z, c) \mapsto_G^* C$, where C is final.
- Let $(e, U, V, -) \mapsto_G (g, U, V \cdot a, +)$ and suppose $(e, U, V, -)$ is canonical. Clearly, $\theta_G(e) = \theta_G(g)$ and, as a consequence, U is canonical for g . Now, suppose $V = W \cdot t \cdot Z$. Clearly, t is quasi-standard if $W = \varepsilon$ and standard if $W \neq \varepsilon$, because $(e, U, V, -)$ is canonical. Moreover for every $u \sqsubseteq t$, either $(g, U, u \cdot Z \cdot a, c) \mapsto_G (e, U, u \cdot Z, c \downarrow)$ or $(e, U, v \cdot Z, c) \mapsto_G (g, U, u \cdot Z \cdot a, c \downarrow)$. This implies $(g, U, u \cdot Z \cdot a, c) \mapsto_G^* C$, where C is final.
- Let $(e, U, V \cdot n(t, u), +) \mapsto_G (g, U, V \cdot t \cdot u, +)$ and suppose $(e, U, n(t, u), +)$ is canonical. Clearly, $\theta_G(e) = \theta_G(g)$ and, as a consequence, U is canonical for g . First of all, u must be standard. Let $v \sqsubseteq u$. Then $p(v) \sqsubseteq n(t, u)$ and, as a consequence, $(e, U, p(v), +) \mapsto_G (g, U, v, +) \mapsto_G^* C$ where C is final. $n(t, u)$ is standard if $V \neq \varepsilon$ and quasi-standard if $V = \varepsilon$. As a consequence, t is standard if $V \neq \varepsilon$ and quasi-standard if $V = \varepsilon$. Let $v \sqsubseteq t$. Then $n(v, u) \sqsubseteq n(t, u)$ and, as a consequence, $(e, U, n(v, u), +) \mapsto_G (g, U, v \cdot u, +) \mapsto_G^* C$ where C is final. Now, suppose $V = W \cdot v \cdot Z$. Clearly, v is quasi-standard if $W = \varepsilon$ and standard if $W \neq \varepsilon$, because $(e, U, V \cdot n(t, u), -)$ is canonical. Moreover for every $w \sqsubseteq v$, either $(g, U, w \cdot Z \cdot t \cdot u, c) \mapsto_G (e, U, w \cdot Z \cdot n(t, u), c)$ or $(e, U, w \cdot Z \cdot n(t, u), c) \mapsto_G (g, U, w \cdot Z \cdot t \cdot u, c)$. This implies $(g, U, w \cdot Z \cdot t \cdot u, c) \mapsto_G^* C$, where C is final.

This concludes the proof. \square

As a consequence of Lemma 3, when analyzing how W_G and T_G evolve during cut-elimination we can only assume that all involved contexts are canonical. This will make the proofs simpler. A sequence of canonical contexts $C_1 \mapsto_G C_2 \mapsto_G \dots \mapsto_G C_n$ is called a *canonical path*.

We now analyze proof-nets only containing W -cuts at levels from 0 to n and $!$ -cuts at level n . Observe that, by definition, G must be in this form whenever $G \rightarrow H$.

Lemma 4 Let G be a proof-net, let $n \in \mathbb{N}$ and let $e \in B_G$ such that $\partial(e) \leq n$. Suppose any cut at levels 0 to $n - 1$ in G is a W -cut and any cut at level n in G is either a W -cut or a $!$ -cut. Then the only canonical context for e is

$$U_e = \underbrace{e \dots e}_{\partial(e) \text{ times}}$$

and the only copy of e on U_e is e .

Proof. We prove the lemma by induction on $n \in \mathbb{N}$. Let us first consider the case $n = 0$. We can proceed by an induction on the structure of a proof π such that $G = G_\pi$, here. The only interesting inductive case is the one for the rule corresponding to U . By hypothesis, it must be either a W -cut or a $!$ -cut. The case $n > 0$ can be treated in the same way. This concludes the proof. \square

As a consequence, any proof-net G satisfying the conditions of Lemma 4 has strictly positive weights, although $W_G = 0$. We can go even further, proving that A_G does not contain any cycle whenever G only contains W -cuts:

Lemma 5 Let G be a proof-net containing W -cuts only. Then A_G does not contain any cycle.

Proof. We can prove the following, stronger statement by a straightforward induction on G : if $(e, U, V, b) \mapsto_G^+ (e, W, Z, c)$ then $b \neq c$. \square

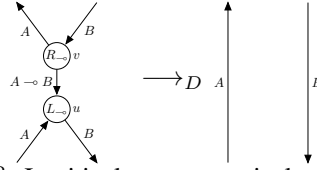
If $G \Rightarrow_S H$, the property of having strictly positive weights and not containing canonical cycles propagates from H to G . Moreover, it is possible to precisely evaluate the difference between W_G and W_H , depending on S . Independently on S , T_G is going to be strictly higher than T_H . Formally:

Lemma 6 *Suppose that $G \Rightarrow_S H$, H has strictly positive weights and A_H does not contain any cycle. Then:*

- G has strictly positive weights;
- A_G does not contain any cycle;
- $T_G > T_H$;
- If $S \in \{-\circ, \otimes, \forall, D, W\}$, then $W_G = W_H$;
- If $S = !$, then $W_G = W_H + \sum_{U \in L_G(e)} R_G(e, U)$, where e is the box edge involved in the cut-elimination step;
- If $S \in \{X, N\}$, then $W_G = W_H + |L_G(e)|$, where e is the box edge involved in the cut-elimination step.

Proof. We can distinguish some cases:

- Let now $G \Rightarrow_{-\circ} H$. Then we are in the following situation:

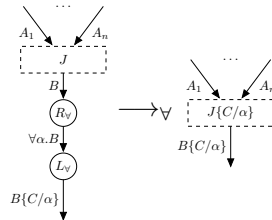


Observe that $B_G = B_H$ and $I_G = I_H \cup \{u, v\}$. Intuitively, any canonical path in G can be mimicked by a canonical path in H and viceversa. We can make this claim more precise: for every $e \in B_G = B_H$, $L_G(e) = L_H(e)$ and, moreover, for every $U \in L_G(e) = L_H(e)$ and for every $t \in \mathcal{E}$, t is a copy for e on U under G iff t is a copy for e on U under H . We can proceed by induction on $\partial(e)$:

- If $\partial(e)=0$, then by definition $L_G(e) = L_H(e) = \{\varepsilon\}$. Moreover, for every exponential signature u and every final context C (for G or for H), we have $(e, \varepsilon, u, +) \mapsto_G^* C$ iff $(e, \varepsilon, u, +) \mapsto_H^* C$. This implies the thesis.
- If $\partial(e) > 0$, then $\rho_G(e) = \rho_H(e)$ and $\partial(\rho_G(e)) = \partial(\rho_H(e)) < \partial(e)$. By the inductive hypothesis, $L_G(\rho_G(e)) = L_H(\rho_H(e))$. This implies $L_G(e) = L_H(e)$, because elements of $L_G(e)$ are defined by extending $U \in L_G(\rho_G(e))$ with a copy for $\rho_G(e)$ on U (and the same definition applies to H). Moreover, for every exponential signature u , every $U \in L_G(e) = L_H(e)$ and every final context C (for G or for H), we have $(e, U, u, +) \mapsto_G^* C$ iff $(e, U, u, +) \mapsto_H^* C$. This implies the thesis.

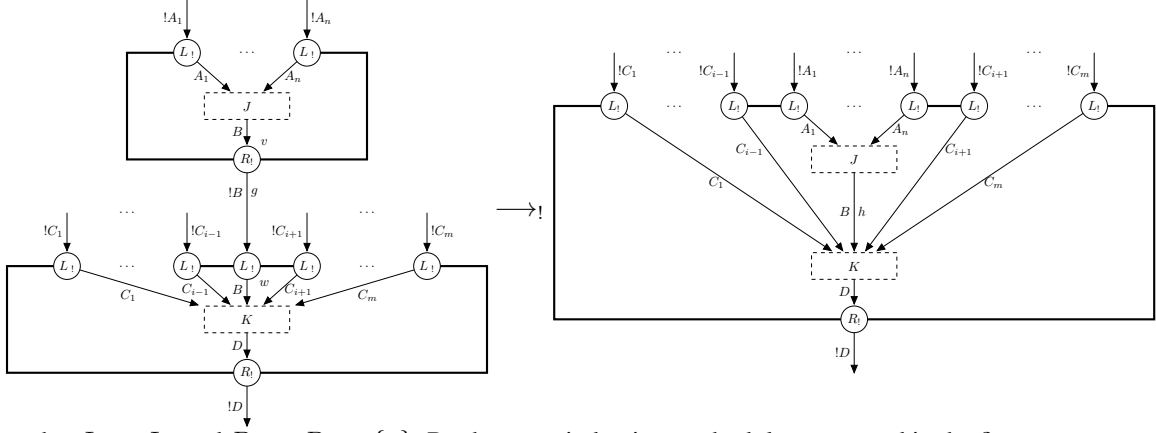
As a consequence, $R_G(e, U) = R_H(e, U)$, whenever e is a box edge and whenever U is canonical for e . This implies $W_G = W_H$. Moreover $L_G(w) = L_H(w)$ whenever $w \in V_G$. But since $|L_G(v)|, |L_G(u)| \geq 1$, we have $T_G > T_H$. If H is strictly positive then G is strictly positive, too. Finally, if A_G contains a cycle for G , then this same cycle is a cycle in A_H for H .

- Let $G \Rightarrow_{\forall} H$. Then we are in the following situation:



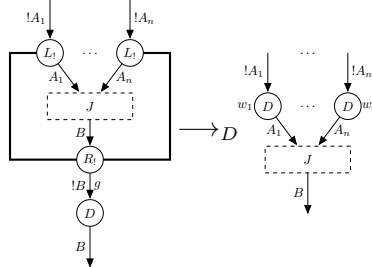
The argument used in the previous case applies here, too. Notice that $J\{C/\alpha\}$ is structurally identical to J (they only differ in the labelling functions β_J and $\beta_{J\{C/\alpha\}}$). We can conclude that $W_G = W_H$, $T_G > T_H$, G is strictly positive whenever H is and if A_G contains a cycle, then A_H contains a cycle, too.

- Let $G \Rightarrow_! H$. Then we are in the following situation:



Observe that $I_G = I_H$ and $B_G = B_H \cup \{g\}$. By the same induction methodology we used in the first case we can prove the following: for every $e \in B_H$, $L_G(e) = L_H(e)$ and, moreover, for every $e \in B_H$, for every $U \in L_H(e) = L_G(e)$ and for every $t \in \mathcal{E}$, t is a copy for e on U under G iff t is a copy for e on U under H . Observe that here proving the preservation of paths become a bit more delicate and, in particular, Lemma 3 is crucial. For example, suppose we want to mimick a canonical path in H going from K to J through h by a path in G going through g . This can be done only if any context $C = (r, U, V, c)$ is such that $U \neq \varepsilon$. But since we know that $C \in A_H$, we can conclude that, indeed, U is canonical for h , and is nonempty. This implies that $R_G(h, U)$ is always equal to $R_H(h, U)$ except when $h = e$. As a consequence, $T_G > T_H$ and $W_G = W_H + \sum_{U \in L_G(g)} R(g, U)$. Notice that $\sum_{U \in L_G(g)} R(g, U) = 1$ whenever $G \rightarrow H$. If A_G contains a cycle, then A_H contains a cycle, too.

- Let $G \Rightarrow_D H$. Then we are in the following situation:



Observe that $I_G \supseteq I_H - \{w_1, \dots, w_n\}$ and $B_G = B_H \cup \{g\}$. Furthermore, notice that $R_G(g, U) = 1$ for every U , since the only copy of g on any U is e . We can prove the following for every $e \in B_H$:

- If $e \in B_J$, then

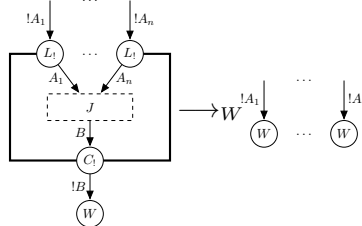
$$L_G(e) = \{U \cdot e \cdot V \mid U \cdot V \in L_H(e) \text{ and } |U| = \partial(e)\}$$

and, moreover, for every $U \cdot e \cdot V \in L_G(e)$ (where $|U| = \partial(e)$) and for every $t \in \mathcal{E}$, t is a copy for e on $U \cdot e \cdot V$ under G iff t is a copy for e on $U \cdot V$ under H .

- If $e \notin B_J$, then $L_G(e) = L_H(e)$ and, moreover, for every $U \in L_G(e)$ and for every $t \in \mathcal{E}$, t is a copy for e on U under G iff t is a copy for e on U under H .

As usual, we can proceed by induction. As a consequence, $W_G = W_H$. Notice that $n = P_G(g) - 1$. This implies $T_G > T_H$, since $|L_G(w_i)| = |L_H(g)|$. If A_G contains a cycle, a cycle can be found in A_H as well.

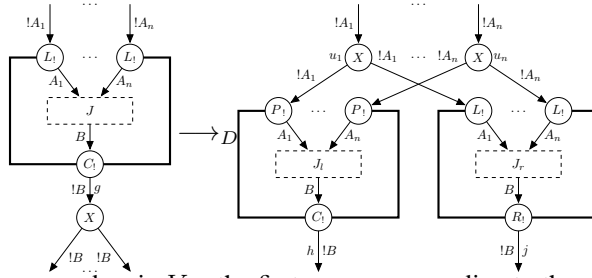
- Let $G \Rightarrow_W H$. Then G and H only contain W -cuts. By lemma 4, G and H satisfy claim 1. By lemma 5, G and H satisfy claim 2. Moreover, $W_G = W_H = 0$. We are in the following situation:



But

$$\begin{aligned}
T_G &= \sum_{v \in I_G} |L_G(v)| + \sum_{e \in B_G} P_G(e) \sum_{U \in L_G(e)} (2R_G(e, U) - 1) \\
&= \sum_{v \in I_G} 1 + \sum_{e \in B_G} P_G(e) \cdot 1 \\
&= |I_G| + \sum_{e \in B_G} P_G(e) \\
&\geq |I_H| - n + \sum_{e \in B_H} P_H(e) + P_G(g) \\
&= |I_H| - n + \sum_{e \in B_H} P_H(e) + n + 1 \\
&> |I_H| + \sum_{e \in B_H} P_H(e) \\
&= \sum_{v \in I_H} |L_H(v)| + \sum_{e \in B_H} P_H(e) \sum_{U \in L_H(e)} (2R_H(e, U) - 1) \\
&= T_H
\end{aligned}$$

- Suppose $G \Rightarrow_X H$. Then we are in the following situation:



For every edge $e \in V_J$, there are two edges e_l and e_r in V_H , the first one corresponding to the copy of e in J_l and the second one corresponding to the copy of e in J_r . We can prove the following for every $e \in B_G$:

- If $e \in B_J$, then

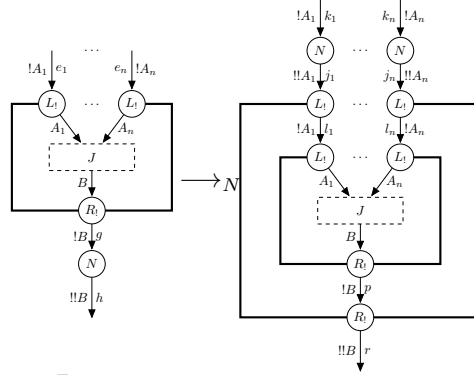
$$L_G(e) = \{U \cdot l(t) \cdot V \mid U \cdot t \cdot V \in L_H(e_l) \text{ and } |U| = \partial(e)\} \cup \{U \cdot r(t) \cdot V \mid U \cdot t \cdot V \in L_H(e_r) \text{ and } |U| = \partial(e)\}.$$

Moreover, for every $U \cdot l(u) \cdot V \in L_G(e)$ (where $|U| = \partial(e)$) and for every $t \in \mathcal{E}$, t is a copy for e on $U \cdot l(u) \cdot V$ under G iff t is a copy for e_l on $U \cdot u \cdot V$ under H . Furthermore, for every $U \cdot r(u) \cdot V \in L_G(e)$ (where $|U| = \partial(e)$) and for every $t \in \mathcal{E}$, t is a copy for e on $U \cdot r(u) \cdot V$ under G iff t is a copy for e_r on $U \cdot u \cdot V$ under H .

- If $e \notin B_J$ and $e \neq g$, then $L_G(e) = L_H(e)$ and, moreover, for every $U \in L_G(e)$ and for every $t \in \mathcal{E}$, t is a copy for e on U under G iff t is a copy for e on U under H .
- $L_G(g) = L_H(h) = L_H(j)$ and for every $U \in L_G(g)$ and for every $t \in \mathcal{E}$, t is a copy for e on U under G iff $t = l(u)$ and u is a copy for r on U under H or $t = r(u)$ and u is a copy for q on U under H .

As usual, we can proceed by induction on $\partial(e)$ and Lemma 3 is crucial. It follows that $R_G(g, U) = R_H(h, U) + R_H(j, U)$ and $W_G = W_H + |L_G(g)|$. Moreover, notice that for every vertex $w \in I_J$, there are two vertices $z \in I_{J_l}$ and $s \in I_{J_r}$ such that $|L_G(w)| = |L_H(z)| + |L_H(s)|$. Since $n = P_G(g) - 1$, we can conclude $T_G > T_H$. If A_G contains a cycle, a cycle can be found in A_H , too.

- Suppose $G \rightarrow_N H$. Then we are in the following situation:



We can prove the following for every $e \in B_G$:

- If $e \in B_J$, then

$$L_G(e) = \{U \cdot n(u, v) \cdot V \mid U \cdot v \cdot u \cdot V \in L_H(e) \text{ and } |U| = \partial(e)\}.$$

Moreover, for every $U \cdot n(u, v) \cdot V \in L_G(e)$ (where $|U| = \partial(e)$) and for every $t \in \mathcal{E}$, t is a copy for e on $U \cdot n(u, v) \cdot V$ under G iff t is a copy for e_1 on $U \cdot v \cdot u \cdot V$ under H .

- If $e \notin B_J$ and $e \neq g$, then $L_G(e) = L_H(e)$ and, moreover, for every $U \in L_G(e)$ and for every $t \in \mathcal{E}$, t is a copy for e on U under G iff t is a copy for e on U under H .
- $L_G(g) = L_H(j)$ and for every $U \in L_G(g)$ and for every $t \in \mathcal{E}$, t is a copy for e on U under G iff $t = n(u, v)$, v is a copy for j on U under H and u is a copy for h on $v \cdot U$ under H .

As usual, we can proceed by induction on $\partial(e)$ and Lemma 3 is crucial. But notice that a simplification of t is either $n(w, v)$, where w is a simplification of u or $p(z)$ where z is a simplification of v . It follows that

$$R_G(g, U) = R_H(j, U) + \sum_{t \cdot U \in L_H(j)} R_H(h, t \cdot U),$$

and, as a consequence, $W_G = W_H + |L_G(g)|$. Moreover, notice that for every vertex w in J , it holds that $|L_G(w)| = |L_H(w)|$. Since $n = P_G(g) - 1$, we can conclude $T_H \leq T_G + |L_G(g)|(P_G(g) - 1)$.

This concludes the proof. \square

Lemma 6 gives us enough information to establish strong correspondences between T_G , W_G and the number of steps necessary to rewrite G to normal form:

Proposition 1 (Positive Weights, Absense of Cycles and Monotonicity) *Let G be a proof-net. Then*

1. G has strictly positive weights;
2. A_G does not contain any cycle;
3. $W_G \geq W_H$ and $T_G > T_H$ whenever $G \Longrightarrow H$;
4. $W_G \leq W_H + 1$ whenever $G \longrightarrow H$,

Proof. We prove claims 1 to 3 by induction on $[G]_{\Longrightarrow}$ and claim 4 by induction on $[G]_{\longrightarrow}$. First of all, consider a proof-net G such that $[G]_{\Longrightarrow} = 0$. Clearly, G must be cut-free. By lemma 4, G satisfies claim 1. By lemma 5, G satisfies claim 2. Moreover, there cannot be any H such that $G \Longrightarrow H$. Now, suppose $[G]_{\Longrightarrow} \geq 1$ and suppose $G \Longrightarrow H$. Clearly $[H]_{\Longrightarrow} < [G]_{\Longrightarrow}$ and, as a consequence, we can assume H satisfies conditions 1 and 2. We can prove G satisfies conditions 1 to 3 by lemma 6.

Now, consider a proof-net G such that $[G]_{\longrightarrow} = 0$. Clearly, G must be cut-free. As a consequence, there cannot be any H such that $G \longrightarrow H$ and condition 4 is satisfied. Now, suppose $[G]_{\longrightarrow} \geq 1$ and let $G \longrightarrow_S H$. Clearly, we can assume G satisfies conditions 1 to 4. From lemma 6, we know that $W_G = W_H$ if $S \in \{\neg, \otimes, \forall, D, W\}$. Suppose $S \in \{!, X, N\}$ and let $e \in B_G$ be the cut-edge involved in the cut-elimination step. From lemma 4, we know that $L_G(e) = \{U_e\}$ and $R_G(e, U_e) = 1$. By lemma 6, this implies the thesis. \square

The following is a technical lemm that will be essential in proving T_G to be polynomially related to W_G :

Lemma 7 *Let G be a proof-net and let $e \in B_G$. Then, $\sum_{U \in L_G(e)} R_G(e, U) \leq W_G + 1$.*

Proof. Let $D_G(e) \subseteq B_G$ be defined as follows:

$$D_G(e) = \begin{cases} \{e\} \cup D_G(\sigma_G(e)) & \text{if } \sigma_G(e) \text{ is defined} \\ \{e\} & \text{otherwise} \end{cases}$$

We will prove the following statement

$$\sum_{U \in L_G(e)} R_G(e, U) \leq \left(\sum_{g \in D_G(e)} \sum_{U \in L_G(g)} (R_G(g, U) - 1) \right) + 1.$$

We go by induction on $\partial(e)$. If $\partial(e) = 0$, then $L_G(e) = \{\varepsilon\}$ and $D_G(e) = \{e\}$. Then

$$\sum_{U \in L_G(e)} R_G(e, U) = R_G(e, \varepsilon) = R_G(e, \varepsilon) - 1 + 1 = \left(\sum_{g \in D_G(e)} \sum_{U \in L_G(g)} (R_G(g, U) - 1) \right) + 1.$$

If $\partial(e) > 0$, then $\sigma_G(e)$ is defined and, moreover,

$$\begin{aligned} \sum_{U \in L_G(e)} R_G(e, U) &= \left(\sum_{U \in L_G(e)} (R_G(e, U) - 1) \right) + |L_G(e)| \\ &\leq \left(\sum_{U \in L_G(e)} (R_G(e, U) - 1) \right) + \sum_{U \in L_G(\sigma_G(e))} R_G(e, U) \\ &\leq \left(\sum_{U \in L_G(e)} (R_G(e, U) - 1) \right) + \left(\sum_{g \in D_G(\sigma_G(e))} \sum_{U \in L_G(g)} (R_G(g, U) - 1) \right) + 1 \\ &= \sum_{g \in D_G(e)} \sum_{U \in L_G(g)} (R_G(g, U) - 1) + 1. \end{aligned}$$

Now observe that for every $e \in B_G$, $D_G(e) \subseteq B_G$ and, as a consequence,

$$\left(\sum_{g \in D_G(e)} \sum_{U \in L_G(g)} (R_G(g, U) - 1) \right) + 1 \leq W_G + 1.$$

This concludes the proof. \square

As a consequence of Proposition 1, T_G bounds the number of cut-elimination steps necessary to rewrite G to its normal form. As it can be easily shown, T_G is also an upper bound on $|G|$. The following result can then be obtained by proving appropriate inequalities between W_G , $|G|$ and T_G :

Theorem 1 *There is a polynomial $p : \mathbb{N}^2 \rightarrow \mathbb{N}$ such that for every proof-net G , $[G] \rightarrow, ||G|| \rightarrow \leq p(W_G, |G|)$.*

Proof. By Proposition 1, we can conclude that $T_G > T_H$ whenever $G \Rightarrow H$. Moreover, by lemma 7,

$$\begin{aligned} T_G &= \sum_{e \in B_G} P_G(e) \sum_{U \in L_G(e)} (2R_G(e, U) - 1) + \sum_{v \in I_G} |L_G(v)| \\ &\leq \sum_{e \in B_G} 2|G| \sum_{U \in L_G(e)} R_G(e, U) + \sum_{v \in I_G} (W_G + 1) \\ &\leq \sum_{e \in B_G} 2|G|(W_G + 1) + |G|(W_G + 1) \\ &\leq 2|G|^2(W_G + 1) + |G|(W_G + 1) \\ &= (2|G|^2 + |G|)(W_G + 1) \end{aligned}$$

Finally:

$$T_G \geq \sum_{e \in B_G} P_G(e) + |I_G| = |V_G| = |G|$$

Since $T_G \geq 0$ for every G , it is clear that $[G] \Rightarrow, ||G|| \Rightarrow \leq p(W_G, |G|)$, where $p(x, y) = (2y^2 + y)(x + 1)$. This concludes the proof, since, by lemma 1, $[G] \rightarrow = [G] \Rightarrow$ and $||G|| \rightarrow = ||G|| \Rightarrow$. \square

The weight W_G can only decrease during cut-elimination. Moreover, it decreases by at most one at any normalization step when performing the level-by-level strategy. As a consequence, the following theorem holds:

Theorem 2 *Let G be a proof-net. There is H with $G \rightarrow^{W_G} H$.*

Proof. By Proposition 1, W_G decreases by at most one at any normalization step when performing the “level-by-level” strategy \rightarrow . Observe that $W_G = 0$ whenever G is cut-free. This concludes the proof. \square

Theorems 1 and 2 highlights the existence of strong relations between context semantics and computational complexity. The two results can together be seen as a strengthening of the well-known correspondence between strongly normalizing nets and finiteness of regular paths (see [7]). This has very interesting consequences: for example, a family \mathcal{G} of proof-nets can be normalized in polynomial (respectively, elementary) time iff there is a polynomial (respectively, an elementary function) p such that $W_G \leq p(|G|)$ for every $G \in \mathcal{G}$. This will greatly help in the following section, where we sketch new proofs of soundness for various subsystems of linear logic.

Now, suppose t is a copy of $e \in B_G$ under $U \in \mathcal{E}^*$. By definition, there is a finite (possibly empty) sequence C_1, \dots, C_n such that

$$(e, U, t, +) \mapsto_G C_1 \mapsto_G C_2 \mapsto_G \dots \mapsto_G C_n$$

and C_n is final. But what else can be said about this sequence? Let $C_i = (g_i, V_i, W_i, b_i)$ for every i . By induction on i , the leftmost component of W_i must be an exponential signature, i.e. $W_i = u_i \cdot Z_i$ for every i . Moreover, every u_i must be a subtree of t (another easy induction on i). This observation can in fact be slightly generalized into the following result:

Proposition 2 (Subtree Property) *Suppose t is a standard exponential signature. For every subtree u of t , there is $v \sqsubseteq t$ such that, whenever G is a proof-net, $U \in \mathcal{E}^*$ is canonical for $e \in B_G$ and t is a copy of e on U , there are $g \in E_G$ and $V \in \mathcal{E}^*$ with $(e, U, v, +) \mapsto_G^* (g, V, u, +)$.*

Proof. We prove the following, stronger statement: for every exponential signature t and for every subtree u of t , there is $v \sqsubseteq t$ such that whenever $(e, U, t, +) \in A_G$, there are $g \in E_G$ and $W \in \mathcal{E}^*$ with $(e, U, v, +) \mapsto_G^* (g, W, u, +)$. We proceed by induction on t :

- If $t = e$, then $g = e$ and $V = U$.
- If $t = r(w)$, then $u = t$ or u is a subtree of w . In the first case $g = e$ and $V = U$. In the second case, apply the induction hypothesis to w and u obtaining a term $z \sqsubseteq w$. Since $(e, U, r(w), +) \mapsto_G^* C$ and $(e, U, r(z), +) \mapsto_G^* D$ where C, D are final, we can conclude that

$$\begin{aligned} (e, U, r(w), +) &\mapsto_G^* (h, W, w, +) \\ (e, U, r(z), +) &\mapsto_G^* (h, W, z, +) \end{aligned}$$

for some h, W . By induction hypothesis, $(h, W, z, +) \mapsto_G^* (g, V, u, +)$ for some g, V and, as a consequence $(e, U, r(z), +) \mapsto_G^* (g, V, u, +)$.

- If $t = l(w)$ or $t = p(w)$ then we can proceed as in the preceeding case.
- If $t = n(w, z)$, then $u = t$ or t is a subtree of z or t is a subtree of w . In the first case, $g = e$ and $V = U$ as usual. In the second case, apply the induction hypothesis to z and u obtaining a term $x \sqsubseteq z$. Notice that $p(x) \sqsubseteq n(w, z)$ and $p(z) \sqsubseteq n(w, z)$. Since $(e, U, p(x), +) \mapsto_G^* C$ and $(e, U, p(z), +) \mapsto_G^* D$ where C, D are final, we can conclude that

$$\begin{aligned} (e, U, p(z), +) &\mapsto_G^* (h, W, z, +) \\ (e, U, p(x), +) &\mapsto_G^* (h, W, x, +) \end{aligned}$$

for some h, W . By induction hypothesis, $(h, W, x, +) \mapsto_G^* (g, V, u, +)$ for some g, V and, as a consequence $(e, U, p(x), +) \mapsto_G^* (g, V, u, +)$.

In the third case, we can assume $u \neq e$ and apply the induction hypothesis to w and u obtaining a term $y \sqsubseteq z$. Notice that $n(y, z) \sqsubseteq n(w, z)$. Since $(e, U, n(y, z), +) \mapsto_G^* C$ and $(e, U, n(w, z), +) \mapsto_G^* D$ where C, D are final and $y, w \neq e$, we can conclude that

$$\begin{aligned} (e, U, n(y, z), +) &\mapsto_G^* (h, W, y, +) \\ (e, U, n(w, z), +) &\mapsto_G^* (h, W, w, +) \end{aligned}$$

for some h, W . By induction hypothesis, $(h, W, y, +) \mapsto_G^* (g, V, u, +)$ for some g, V and, as a consequence $(e, U, n(y, z), +) \mapsto_G^* (g, V, u, +)$.

This concludes the proof. \square

The subtree property is extremely useful when proving bounds on $R_G(e, U)$ and W_G in subsystems of MELL. The intuitive idea behind the subtree property is the following: whenever t is a copy of e under U and U is canonical for e , the exponential signature t must be completely “consumed” along the canonical path leading from $(e, U, t, +)$ to a final context C .

5 Subsystems

In this section, we will give some arguments about the usefulness of context semantics by analyzing three subsystems of MELL from a complexity viewpoint.

5.1 Elementary Linear Logic

Elementary linear logic (ELL, [12]) is just MELL with a weaker modality: rules $D_!$ and $N_!$ are not part of the underlying sequent calculus. This restriction enforces the following property at the semantic level:

Lemma 8 (Stratification) *Let G be a ELL proof-net. If $(e, U, V, b) \mapsto_G^* (g, W, Z, c)$, then $\|U\| + \|V\| = \|W\| + \|Z\|$.*

Proof. Suppose $(e, U, V, b) \mapsto_G^n (g, W, Z, c)$, where $n \geq 0$. By induction on n , we can prove that $\|U\| + \|V\| = \|W\| + \|Z\|$. Notice that the only rewriting rules that can break the above equality in MELL are precisely those induced by D and N . \square

By exploiting stratification together with the subtree property, we can easily prove the following result:

Proposition 3 (ELL Soundness) *For every $n \in \mathbb{N}$ there is an elementary function $p_n : \mathbb{N} \rightarrow \mathbb{N}$ such that $W_G \leq p_{\partial(G)}(|G|)$ for every ELL proof-net G .*

Proof. For every $n \in \mathbb{N}$, define two elementary functions $r_n, q_n : \mathbb{N} \rightarrow \mathbb{N}$ as follows:

$$\begin{aligned} \forall x. r_0(x) &= 1; \\ \forall n. \forall x. q_n(x) &= 2^{x \cdot r_n(x) + 1}; \\ \forall n. \forall x. r_{n+1}(x) &= r_n(x) q_n(x). \end{aligned}$$

We can now prove that for every $e \in B_G$ and whenever U is canonical for e the following inequalities hold:

$$\begin{aligned} |L_G(e)| &\leq r_{\partial(e)}(|G|) \\ R_G(e, U) &\leq q_{\partial(e)}(|G|) \end{aligned}$$

We can proceed by induction on $\partial(e)$. If $\partial(e) = 0$, then the only canonical sequence for e is ε and the first inequality is satisfied. Moreover, any copy of e under ε is an exponential signature containing at most $|G|$ instances of r and l constructors: by way of contradiction, suppose t is a copy of e under ε containing $m > |G|$ constructors. Then, by the subtree property, there are m distinct subterms u_1, \dots, u_m of t and $g_1, \dots, g_m \in E_G$ such that $(e, \varepsilon, t, +) \mapsto_G^* (g_i, \varepsilon, u_i, +)$ for every i . Clearly, $g_i = g_j$ for some $i \neq j$ (since $m > |G|$) and the g_i can always be chosen as to be the only edge incident to a vertex labelled with X, C, W or the only edge leaving from a vertex labelled with P , but this contradicts acyclicity. As a consequence, the second inequality is satisfied, because there are at most $2^{|G|+1}$ exponential signatures with length at most

$|G|$. If $\partial(e) > 0$, we can observe that canonical sequences for $\partial(e)$ are in the form $V \cdot t$, where V is canonical for $\sigma_G(e)$ and t is a copy for $\sigma_G(e)$ under V . By the induction hypothesis we can conclude that:

$$\begin{aligned} |L_G(e)| &\leq \sum_{U \in L_G(\sigma_G(e))} R_G(\sigma_G(e), U) \leq \sum_{U \in L_G(\sigma_G(e))} q_{\partial(e)-1}(|G|) \\ &\leq r_{\partial(e)-1}(|G|) \cdot q_{\partial(e)-1}(|G|) = r_{\partial(e)}(|G|). \end{aligned}$$

As for the second inequality, we claim that any copy of e under U (where U is canonical for e) is an exponential signature containing at most $|G| r_{\partial(e)-1}(|G|)$ instances of r and l constructors. To prove that, we can proceed in the usual way (see the base case above). Now observe that:

$$\begin{aligned} W_G &= \sum_{e \in B_G} \sum_{U \in L_G(e)} (R_G(e, U) - 1) \leq \sum_{e \in B_G} \sum_{U \in L_G(e)} q_{\partial(e)}(|G|) \\ &\leq \sum_{e \in B_G} \sum_{U \in L_G(e)} q_{\partial(G)}(|G|) \leq \sum_{e \in B_G} r_{\partial(e)}(|G|) \cdot q_{\partial(G)}(|G|) \\ &\leq \sum_{e \in B_G} r_{\partial(G)}(|G|) \cdot q_{\partial(G)}(|G|) \leq |G| \cdot r_{\partial(G)}(|G|) \cdot q_{\partial(G)}(|G|). \end{aligned}$$

As a consequence, putting $p_n(x) = x \cdot r_n(x) \cdot q_n(x)$ suffices. \square

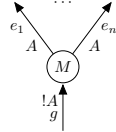
By Proposition 3 and Theorem 1, normalization of **ELL** proof-nets can be done in elementary time, provided $\partial(G)$ is fixed. To this respect, observe that ordinary encodings of data structures such as natural numbers, binary lists or trees have bounded box-depth.

5.2 Soft Linear Logic

Soft linear logic (SLL, [16]) can be defined from **ELL** by replacing rule X with M as follows:

$$\frac{\Gamma, A, \dots, A \vdash B}{\Gamma, !A \vdash B} M$$

In proof-nets for SLL, there are vertices labelled with M and equipped with an arbitrary number of outgoing edges:



Exponential signatures becomes simpler:

$$t ::= e \mid m(i)$$

where i ranges over natural numbers. The new vertex induce the following rewriting rules:

$$\begin{aligned} (h, U, V \cdot m(i), +) &\mapsto_G (e_i, U, V, +) \\ (e_i, U, V, -) &\mapsto_G (h, U, V \cdot m(i), -) \end{aligned}$$

It can be easily verified that for every $e \in B_G$ and for every $U \in \mathcal{E}^*$, it holds that $R_G(e, U) \leq |G|$. Indeed, if $(e, U, t \cdot V, b) \mapsto_G^* (g, W, Z, c)$, then $Z = t \cdot Y$. As a consequence:

Proposition 4 (SLL Soundness) *For every $n \in \mathbb{N}$ there is a polynomial $p_n : \mathbb{N} \rightarrow \mathbb{N}$ such that $W_G \leq p_{\partial(G)}(|G|)$ for every SLL proof-net G .*

Proof. Simply observe that $R_G(e, U) \leq |G|$ and $|L_G(e)| \leq |G|^{\partial(e)}$. As a consequence:

$$\begin{aligned} W_G &= \sum_{e \in B_G} \sum_{U \in L_G(e)} (R_G(e, U) - 1) \leq \sum_{e \in B_G} \sum_{U \in L_G(e)} |G| \\ &\leq \sum_{e \in B_G} |G|^{\partial(e)+1} \leq \sum_{e \in B_G} |G|^{\partial(G)+1} \leq |G|^{\partial(G)+2}. \end{aligned}$$

But this implies $p_n(x)$ is just x^{n+2} . \square

5.3 Light Linear Logic

Light linear logic (LLL, [12]) can be obtained from ELL by enriching the language of formulae with a new modal operator \S and splitting rule $P!$ into two rules:

$$\frac{\Gamma \vdash B \quad |\Gamma| \leq 1}{!\Gamma \vdash B} S! \quad \frac{\Gamma, \Delta \vdash A}{!\Gamma, \S\Delta \vdash \S A} S\S$$

At the level of proof-nets, two box constructions, $!$ -boxes and \S -boxes, correspond to $S!$ and $S\S$. As for the underlying context semantics, $!$ -boxes induce the usual rewriting rules on C_G (see Table 2), while the last rule and its dual are not valid for \S -boxes. This enforces *strong determinacy*, which does not hold for MELL or ELL: for every $C \in C_G$, there is at most one context $D \in C_G$ such that $C \mapsto_G D$. As a consequence, weights can be bounded by appropriate polynomials:

Proposition 5 (LLL soundness) *For every $n \in \mathbb{N}$ there is an polynomial $p_n : \mathbb{N} \rightarrow \mathbb{N}$ such that $W_G \leq p_{\partial(G)}(|G|)$ for every LLL proof-net G .*

Proof. Observe that, by the subterm property and by stratification, to every copy of $e \in B_G$ under $U \in \mathcal{E}^*$ (where U is canonical for e) it corresponds $g \in E_G$ and $V \in \mathcal{E}^*$ such that $|V| = |U|$ and

$$(e, U, t, +) \mapsto_G^* (g, V, e, +).$$

Contrarily to ELL, this correspondence is injective. If, by way of contradiction,

$$\begin{aligned} (e, U, t, +) &\mapsto_G^* (g, V, e, +) \\ (e, U, u, +) &\mapsto_G^* (g, V, e, +) \end{aligned}$$

where $t \neq u$, then, by duality

$$\begin{aligned} (g, V, e, -) &\mapsto_G^* (e, U, t, -) \\ (g, V, e, -) &\mapsto_G^* (e, U, u, -) \end{aligned}$$

But remember that now we have strong determinacy; this implies either $(e, U, t, +) \mapsto_G^* (e, U, u, +)$ or $(e, U, u, +) \mapsto_G^* (e, U, t, +)$. This cannot be, because of acyclicity. We can now proceed exactly as in Proposition 3. Functions $r_n, q_n : \mathbb{N} \rightarrow \mathbb{N}$ are the following ones:

$$\begin{aligned} \forall x. r_0(x) &= 1; \\ \forall n. \forall x. q_n(x) &= |G| \cdot r_n(x); \\ \forall n. \forall x. r_{n+1}(x) &= r_n(x) \cdot q_n(x). \end{aligned}$$

The inequalities:

$$\begin{aligned} |L_G(e)| &\leq r_{\partial(e)}(|G|); \\ R_G(e, U) &\leq q_{\partial(e)}(|G|); \end{aligned}$$

can be proved with the same technique used in Proposition 3. Letting $p_n(x) = x r_n(x) q_n(x)$ concludes the proof. \square

6 Conclusions

In this paper, we define a context semantics for linear logic proof-nets, showing it gives precise quantitative information on the dynamics of normalization. Theorems 1 and 2 are the main achievements of this work: they show that the weight W_G of a proof-net G is a *tight* estimate of the time needed to normalize G . Interestingly, proving bounds on W_G is in general easier than bounding normalization time by purely syntactic arguments. Section 5 presents some evidence supporting this claim. Results described in this paper can be transferred to affine logical systems, which offer some advantages over their linear counterparts (for example, additive connectives can be expressed in the logic).

An interesting problem (which we leave for future work) is characterizing the expressive power of other fragments of MELL, such as 4LL or TLL (see [6]), about which very few results are actually known. We believe that the semantic techniques described here could help dealing with them. Any sharp result would definitely help completing the picture.

Interestingly, the way bounded linear logic (BLL, [13]) is defined is very reminiscent to the way context semantics is used here. We are currently investigating relations between the two frameworks.

Acknowledgments

The author wishes to thank Patrick Baillot and Olivier Laurent for many interesting discussions about the topics of this paper

References

- [1] A. Asperti and S. Guerrini. *The optimal implementation of functional programming languages*. Cambridge University Press, 1998.
- [2] A. Asperti and L. Roversi. Intuitionistic light affine logic. *ACM Transactions on Computational Logic*, 3(1):137–175, 2002.
- [3] P. Baillot and M. Pedicini. Elementary complexity and geometry of interaction. *Fundamenta Informaticae*, 45(1-2):1–31, 2001.
- [4] U. Dal Lago. The geometry of linear higher-order recursion. In *Proc. 20th Annual Symposium on Logic in Computer Science*, pages 366–375. IEEE Computer Society, 2005.
- [5] U. Dal Lago. Context semantics, linear logic and computational complexity. In *Proc. 21st Annual Symposium on Logic in Computer Science*, pages 169–178. IEEE Computer Society, 2006.
- [6] V. Danos and J.-B. Joinet. Linear logic and elementary time. *Information and Computation*, 183(1):123–137, 2003.
- [7] V. Danos and L. Regnier. Proof-nets and Hilbert space. In J.-Y. Girard, Y. Lafont, and L. Regnier, editors, *Advances in Linear Logic*, pages 307–328. Cambridge University Press, 1995.
- [8] V. Danos and L. Regnier. Reversible, irreversible and optimal lambda-machines. *Theoretical Computer Science*, 227(1-2):79–97, 1999.
- [9] J.-Y. Girard. Geometry of interaction 2: deadlock-free algorithms. In *Proc. Conference on Computer Logic*, volume 417 of *LNCS*, pages 76–93, 1988.
- [10] J.-Y. Girard. Geometry of interaction 1: interpretation of system F. In *Proc. Logic Colloquium '88*, pages 221–260, 1989.
- [11] J.-Y. Girard. Proof-nets: the parallel syntax for proof-theory. In A. Ursini and P. Agliano, editors, *Logic and Algebra*, volume 180 of *Lecture Notes in Pure and Applied Mathematics*, pages 97–124. Marcel Dekker, New York, 1995.
- [12] J.-Y. Girard. Light linear logic. *Information and Computation*, 143(2):175–204, 1998.
- [13] J.-Y. Girard, A. Scedrov, and P. J. Scott. Bounded linear logic: A modular approach to polynomial-time computability. *Theoretical Computer Science*, 97(1):1–66, 1992.
- [14] G. Gonthier, M. Abadi, and J.-J. Lévy. The geometry of optimal lambda reduction. In *Proc. 12th ACM Symposium on Principles of Programming Languages*, pages 15–26, 1992.
- [15] G. Gonthier, M. Abadi, and J.-J. Lévy. Linear logic without boxes. In *Proc. 7th Annual Symposium on Logic in Computer Science*, pages 223–234, 1992.
- [16] Y. Lafont. Soft linear logic and polynomial time. *Theoretical Computer Science*, 318:163–180, 2004.
- [17] I. Mackie. The geometry of interaction machine. In *Proc. 22nd ACM Symposium on Principles of Programming Languages*, pages 198–208, 1995.
- [18] J. S. Pinto. Parallel implementation models for the lambda-calculus using the geometry of interaction. In *Proc. 5th International Conference on Typed Lambda Calculi and Applications*, pages 385–399, 2001.
- [19] K. Terui. Light affine lambda calculus and polytime strong normalization. In *Proc. of 16th Annual IEEE Symposium on Logic in Computer Science*, pages 209–220, 2001.
- [20] K. Terui. Proof nets and boolean circuits. In *Proc. 7th Annual Symposium on Logic in Computer Science*, pages 182–191, 2004.