On Context Semantics, Linear Logic and Computational Complexity

Ugo Dal Lago

Dipartimento di Scienze dell'Informazione
Università di Bologna

ICC Workshop, February 16th 2006

Outline

The Need for a Unifying Framework

- Many systems are sound and complete w.r.t. relevant complexity classes (polytime functions, elementary functions, etc.).
- Proof techniques for soundness results are ad-hoc and cannot be easily generalized.
- As a consequence:
  - There are many open problems. For example: the impact of linearity costraint on the expressive power of higher-order recursion [Hofmann97,BNS00] has not been analyzed precisely.
  - It is not known in general whether combining different systems characterizing the same class would break soundness.
- The above mentioned systems are all extensionally complete but definately not intensionally complete.

The Need for a Unifying Framework

- Many systems are sound and complete w.r.t. relevant complexity classes (polytime functions, elementary functions, etc.).
- Proof techniques for soundness results are ad-hoc and cannot be easily generalized.
- As a consequence:
  - There are many open problems. For example: the impact of linearity costraint on the expressive power of higher-order recursion [Hofmann97,BNS00] has not been analyzed precisely.
  - It is not known in general whether combining different systems characterizing the same class would break soundness.
- The above mentioned systems are all extensionally complete but definately not intensionally complete.

The Need for a Unifying Framework

- Many systems are sound and complete w.r.t. relevant complexity classes (polytime functions, elementary functions, etc.).
- Proof techniques for soundness results are ad-hoc and cannot be easily generalized.
- As a consequence:
  - There are many open problems. For example: the impact of linearity costraint on the expressive power of higher-order recursion [Hofmann97,BNS00] has not been analyzed precisely.
  - It is not known in general whether combining different systems characterizing the same class would break soundness.
- The above mentioned systems are all extensionally complete but definately not intensionally complete.

The Need for a Unifying Framework

- Many systems are sound and complete w.r.t. relevant complexity classes (polytime functions, elementary functions, etc.).
- Proof techniques for soundness results are ad-hoc and cannot be easily generalized.
- As a consequence:
  - There are many open problems. For example: the impact of linearity costraint on the expressive power of higher-order recursion [Hofmann97,BNS00] has not been analyzed precisely.
  - It is not known in general whether combining different systems characterizing the same class would break soundness.
- The above mentioned systems are all extensionally complete but definately not intensionally complete.

Context Semantics

- *Intensional* ways of giving semantics to logics and programming languages:
  - Game semantics [AJM92];
  - Geometry of interaction [Girard89];
  - Context semantics [GAL92a,GAL92b].
- Game semantics and geometry of interaction have been already used to study quantitative properties of programs and proofs [BaillotPedicini01,Ghica05].
- We chose context semantics because of its simplicity.
- We applied it to linear logic and its subsystems.
- Strong results can be obtained.

Context Semantics

- *Intensional* ways of giving semantics to logics and programming languages:
  - Game semantics [AJM92];
  - Geometry of interaction [Girard89];
  - Context semantics [GAL92a,GAL92b].
- Game semantics and geometry of interaction have been already used to study quantitative properties of programs and proofs [BaillotPedicini01,Ghica05].
- We chose context semantics because of its simplicity.
- We applied it to linear logic and its subsystems.
- Strong results can be obtained.

Context Semantics

- *Intensional* ways of giving semantics to logics and programming languages:
  - Game semantics [AJM92];
  - Geometry of interaction [Girard89];
  - Context semantics [GAL92a,GAL92b].
- Game semantics and geometry of interaction have been already used to study quantitative properties of programs and proofs [BaillotPedicini01,Ghica05].
- We chose context semantics because of its simplicity.
- We applied it to linear logic and its subsystems.
- Strong results can be obtained.

Context Semantics vs. Normalization Time

From the context semantics of any linear logic proof-net G, a *weight* $W_G \in \mathbb{N} \cup \{\omega\}$ can be defined in such a way that:

Theorem

There is a polynomial $p : \mathbb{N}^2 \to \mathbb{N}$ such that for every proof-net G, G normalizes in at most $p(W_G, |G|)$ steps and the size of any reduct H of G is at most $p(W_G, |G|)$.

Theorem

Let G be a proof-net. Then, there is H with $G \to^{W_G} H$.

Syntax

- Formulae:

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

- Rules:

$$\frac{}{A \vdash A}\ A \qquad \frac{\Gamma \vdash A \quad \Delta, A \vdash B}{\Gamma, \Delta \vdash B}\ U \qquad \frac{\Gamma \vdash B}{\Gamma, !A \vdash B}\ W \qquad \frac{\Gamma, !A, !A \vdash B}{\Gamma, !A \vdash B}\ X$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B}\ R_{\multimap} \qquad \frac{\Gamma \vdash A \quad \Delta, B \vdash C}{\Gamma, \Delta, A \multimap B \vdash C}\ L_{\multimap}$$

$$\frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B}\ R_{\otimes} \qquad \frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C}\ L_{\otimes}$$

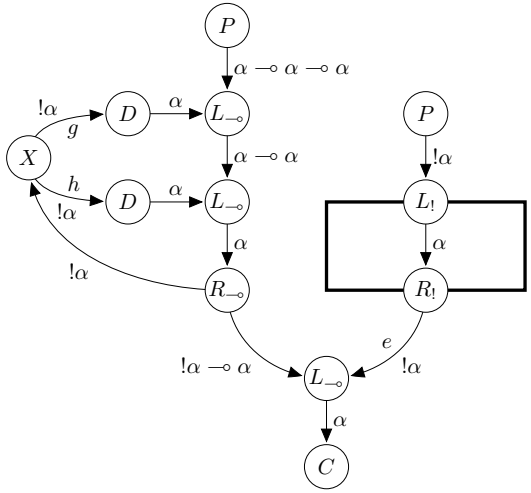
$$\frac{A_1, \ldots, A_n \vdash B}{!A_1, \ldots, !A_n \vdash !B}\ P_! \qquad \frac{A, \Gamma \vdash B}{!A, \Gamma \vdash B}\ D_! \qquad \frac{!!A, \Gamma \vdash B}{!A, \Gamma \vdash B}\ N_!$$

$$\frac{\Gamma \vdash A \quad \alpha \notin FV(\Gamma)}{\Gamma \vdash \forall \alpha.A}\ R_{\forall} \qquad \frac{\Gamma, A\{B/\alpha\} \vdash C}{\Gamma, \forall \alpha.A \vdash C}\ L_{\forall}$$

Proof-nets

- We adopt a system of intuitionistic proof-nets.
- Nodes for axioms and cuts are not needed.
- For example:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\alpha \vdash \alpha}\,A \quad \dfrac{}{\alpha \vdash \alpha}\,A}{\alpha, \alpha \multimap \alpha \vdash \alpha}\,L_! \quad \dfrac{}{\alpha \vdash \alpha}\,A}{\alpha, \alpha, \alpha \multimap \alpha \multimap \alpha \vdash \alpha}\,L_!}{!\alpha, \alpha, \alpha \multimap \alpha \multimap \alpha \vdash \alpha}\,D_!}{!\alpha, !\alpha, \alpha \multimap \alpha \multimap \alpha \vdash \alpha}\,D_!}{!\alpha, \alpha \multimap \alpha \multimap \alpha \vdash \alpha}\,X}{\alpha \multimap \alpha \multimap \alpha \vdash !\alpha \multimap \alpha}\,R_! \qquad \dfrac{\dfrac{}{\alpha \vdash \alpha}\,A \quad \dfrac{\dfrac{}{\alpha \vdash \alpha}\,A}{!\alpha \vdash !\alpha}\,P_!}{!\alpha \multimap \alpha, !\alpha \vdash \alpha}\,L_!}{\alpha \multimap \alpha \multimap \alpha, !\alpha \vdash \alpha}\,U$$



Copying - The Root of Complexity?

- Linear logic without exponentials and additives cannot express anything beyond polynomial time.
- Suppose we know the total number of times boxes in a proof-net G can *possibly* be duplicated. Call it W_G.
- How W_G relates to the complexity of normalizing G?
- Context semantics helps in giving strong results on this question.

Context Semantics - I

- The language $\mathscr{E}$ of *exponential trees* is defined by induction from the following sets of productions:

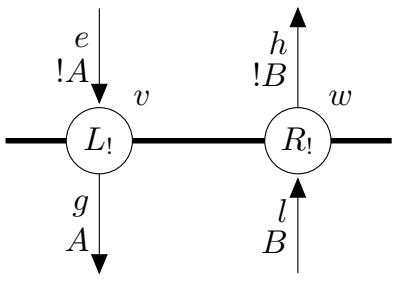
$$t ::= \mathsf{e} \mid \mathsf{r}(t) \mid \mathsf{l}(t) \mid \mathsf{p}(t) \mid \mathsf{n}(t, t).$$

- A *stack element* is either an exponential tree or one of the following characters: $\mathsf{a}, \mathsf{o}, \mathsf{s}, \mathsf{f}, \mathsf{x}$. $\mathscr{S}$ is the set of stack elements.
- Every proof-net G induces rewriting rules on

$$C_G = E_G \times \mathscr{E}^* \times \mathscr{S}^+ \times \{0, 1\}$$

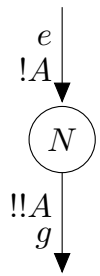
where E_G is the set of G edges,

Context Semantics - II



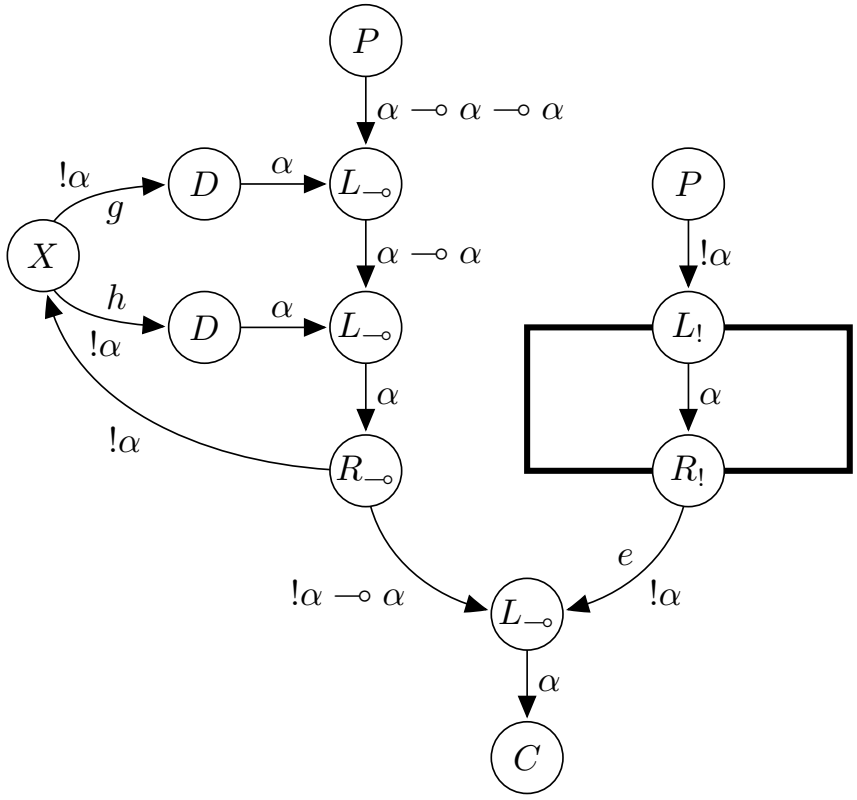
$$
\begin{aligned}
(e, U, V \cdot t, +) &\rightarrow_G (g, U \cdot t, V, +) \\
(g, U \cdot t, V, -) &\rightarrow_G (e, U, V \cdot t, -) \\
(l, U \cdot t, V, +) &\rightarrow_G (h, U, V \cdot t, +) \\
(h, U, V \cdot t, -) &\rightarrow_G (l, U \cdot t, V, -) \\
(e, U, t, +) &\rightarrow_G (h, U, t, +) \\
(h, U, t, -) &\rightarrow_G (e, U, t, -)
\end{aligned}
$$

Context Semantics - III

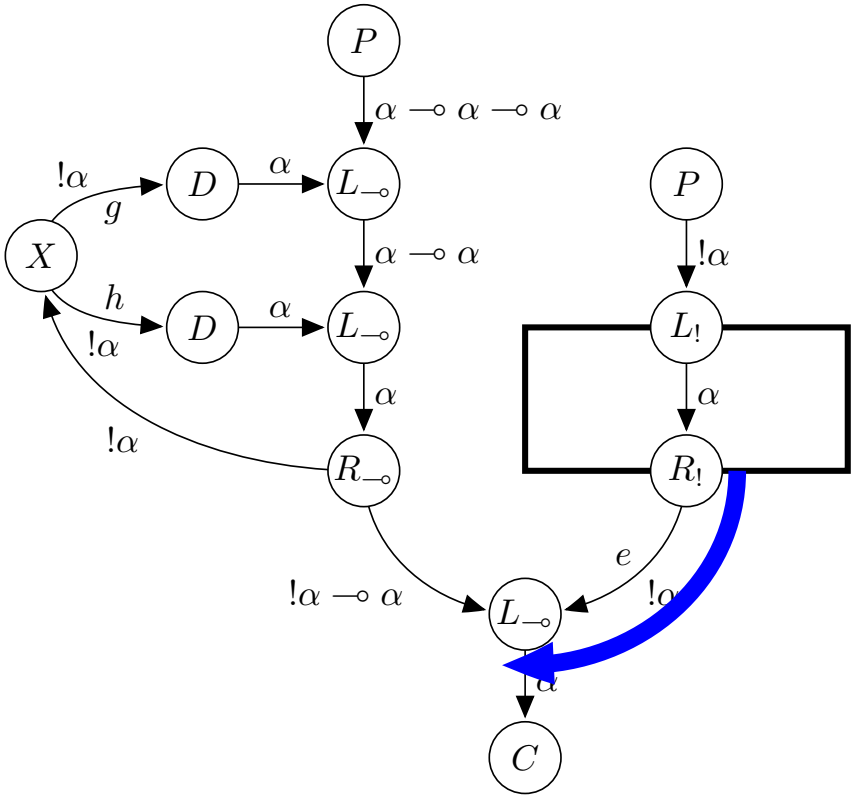


$$
\begin{aligned}
(e, U, V \cdot \mathsf{n}(t,u), +) &\rightarrow_G (g, U, V \cdot t \cdot u, +) \\
(g, U, V \cdot t \cdot u, -) &\rightarrow_G (e, U, V \cdot \mathsf{n}(t,u), -) \\
(e, U, \mathsf{p}(t), +) &\rightarrow_G (g, U, t, +) \\
(g, U, t, -) &\rightarrow_G (e, U, \mathsf{p}(t), -)
\end{aligned}
$$

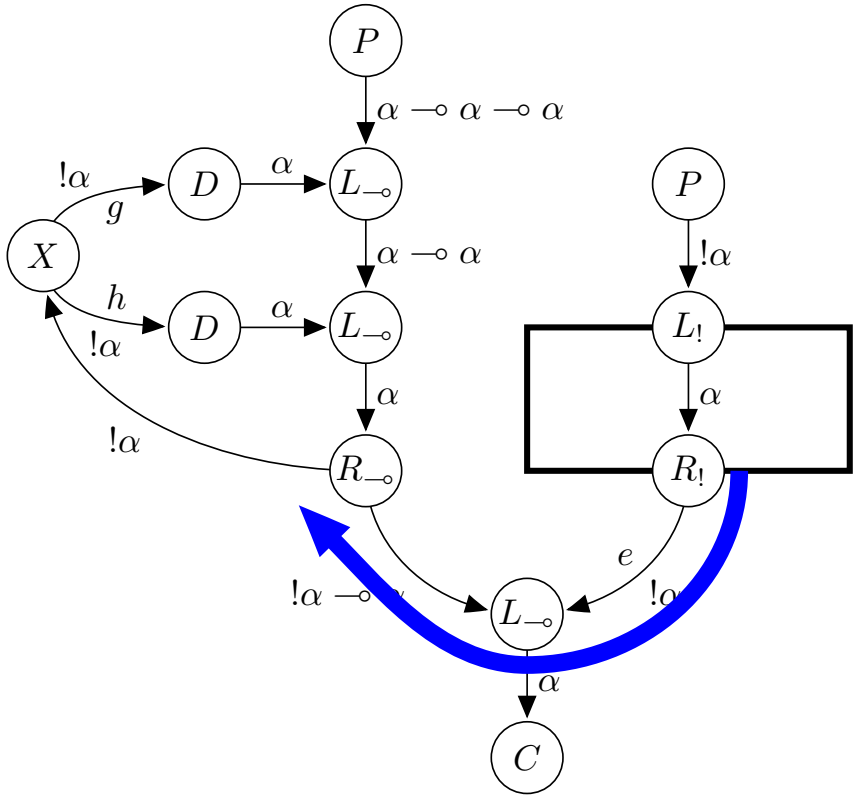
An Example



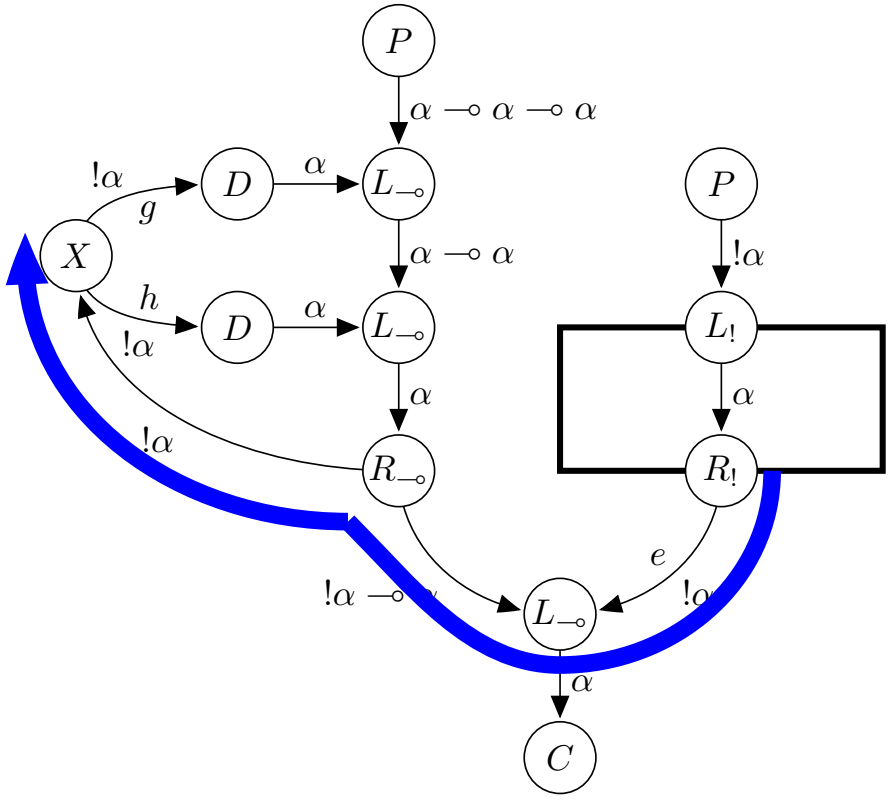
An Example



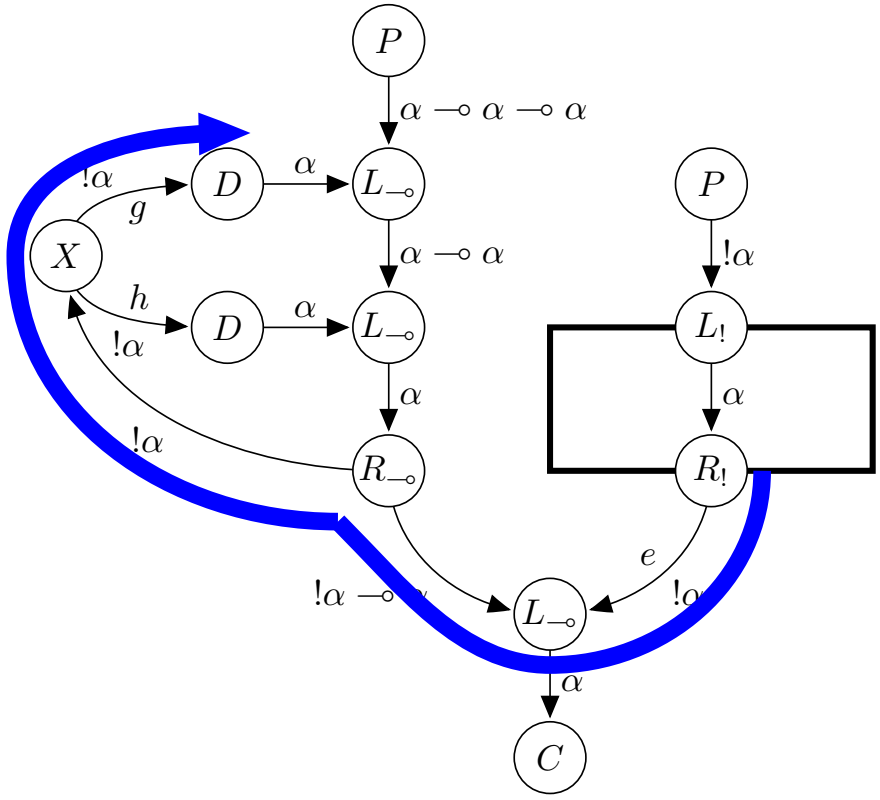
An Example



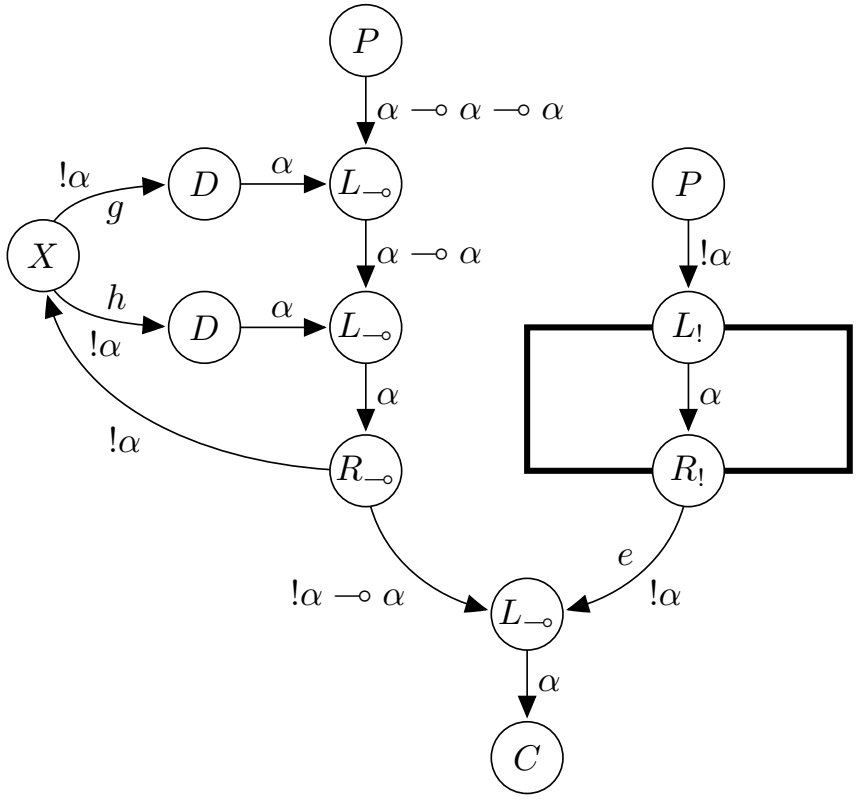
An Example



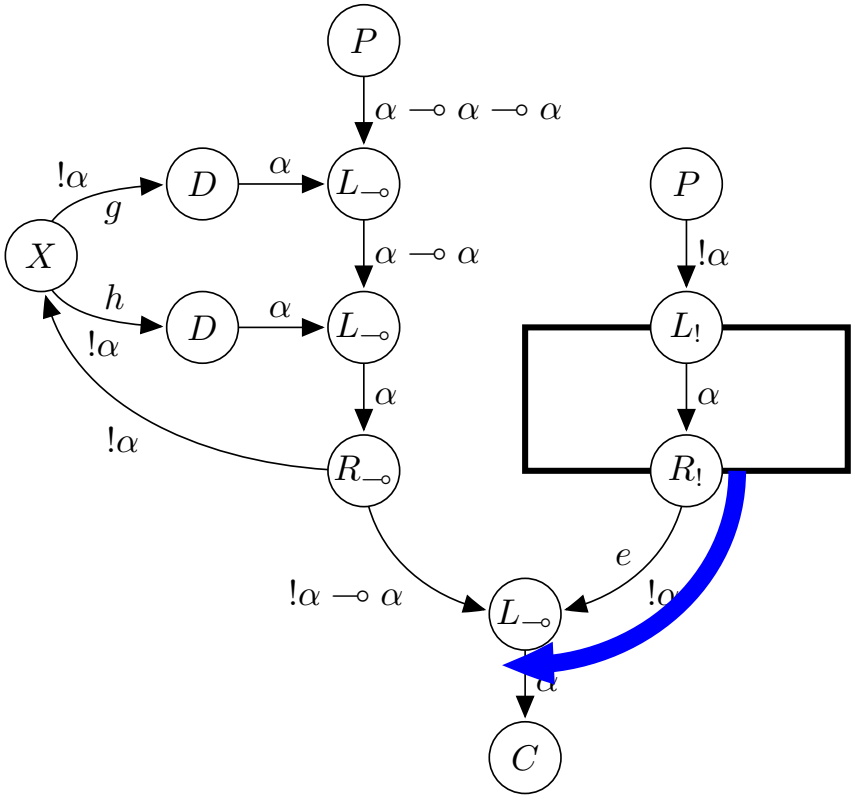
An Example



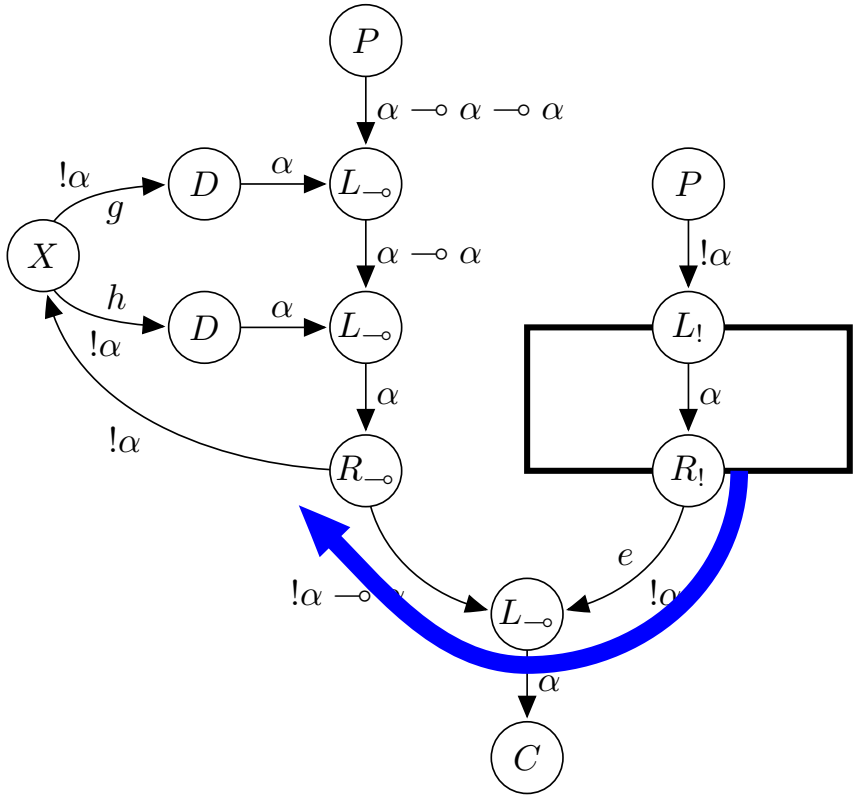
An Example



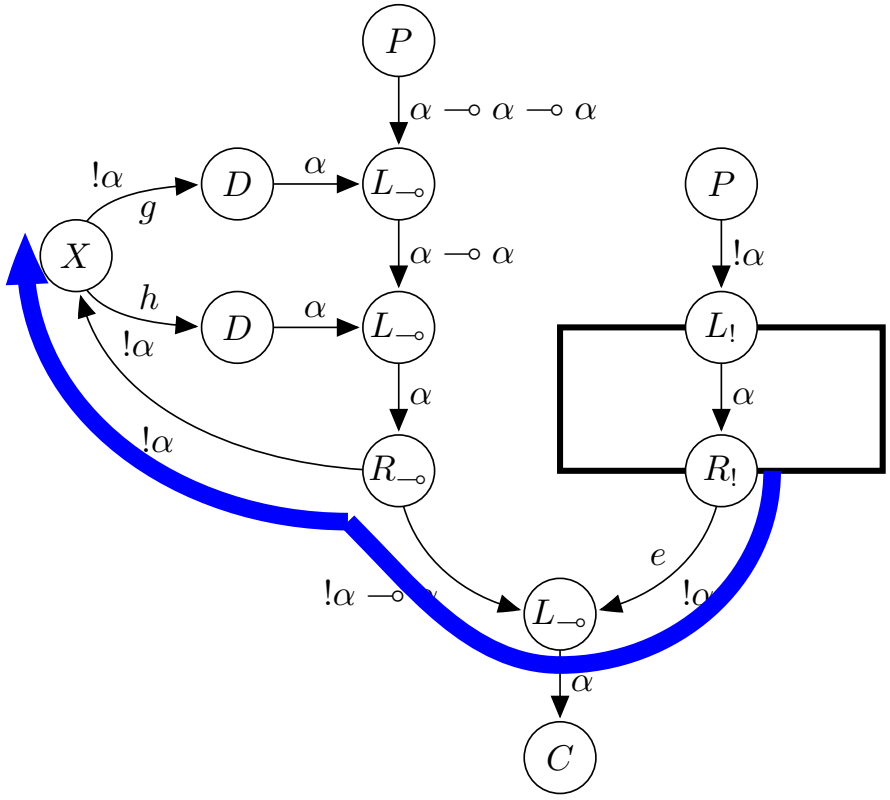
An Example



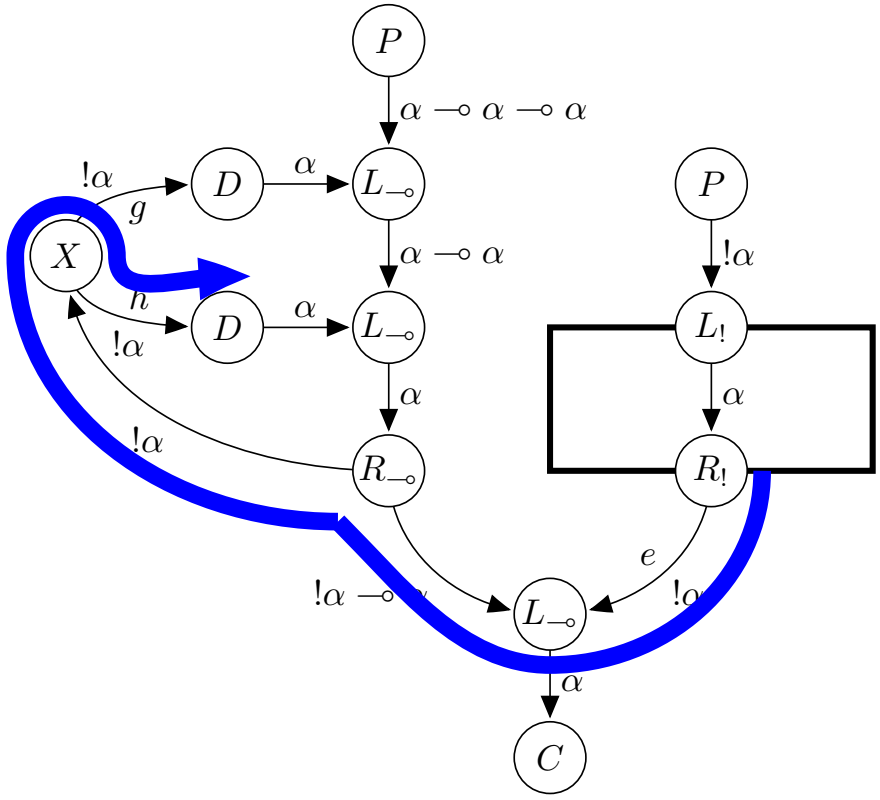
An Example



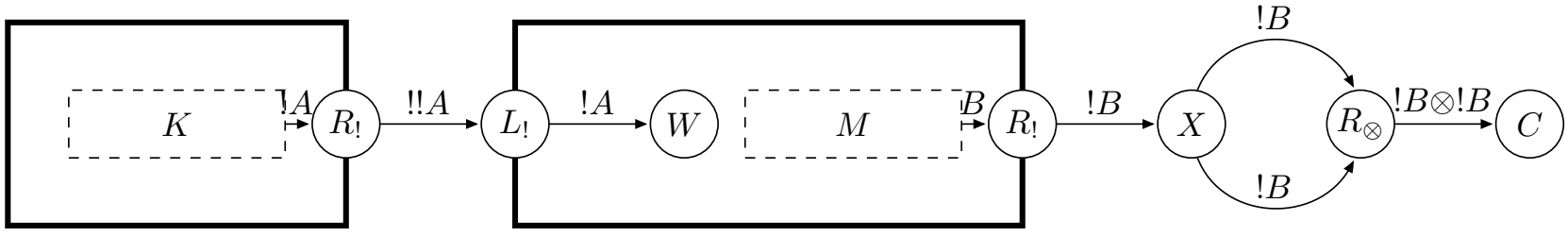
An Example



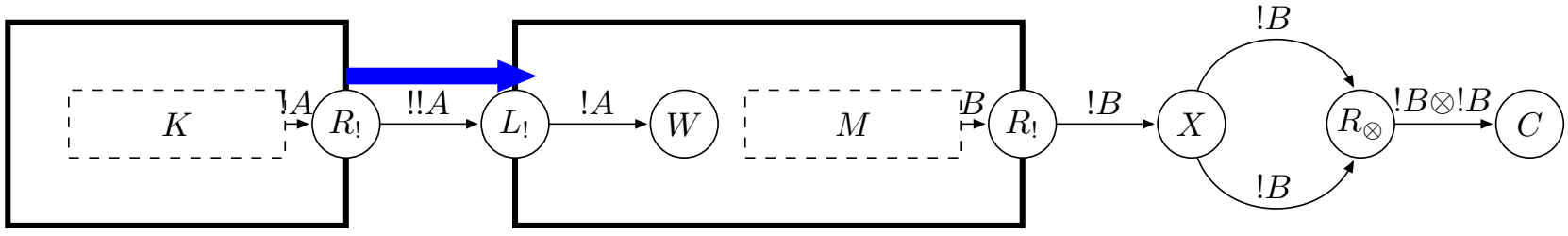
An Example



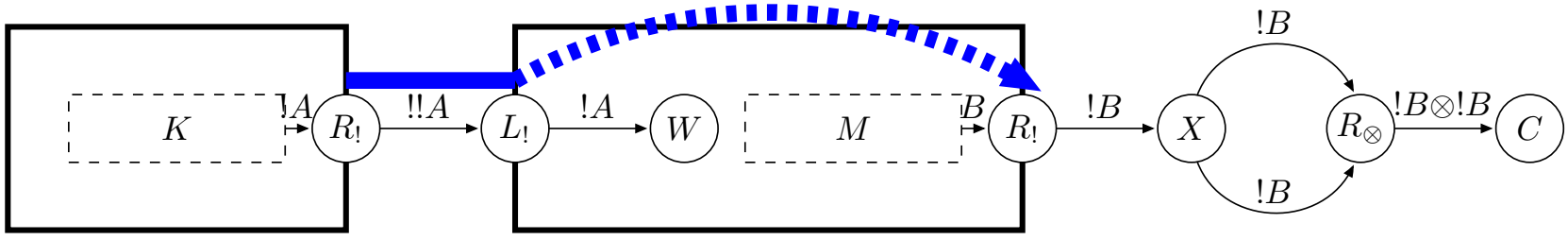
Another Example



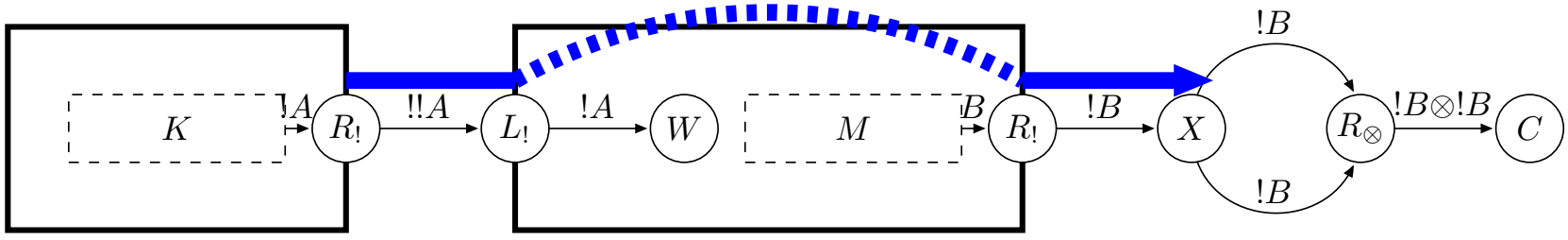
Another Example



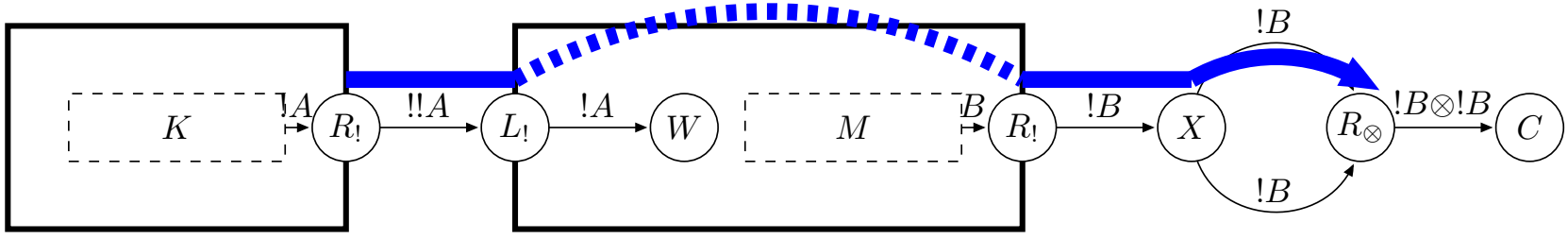
Another Example



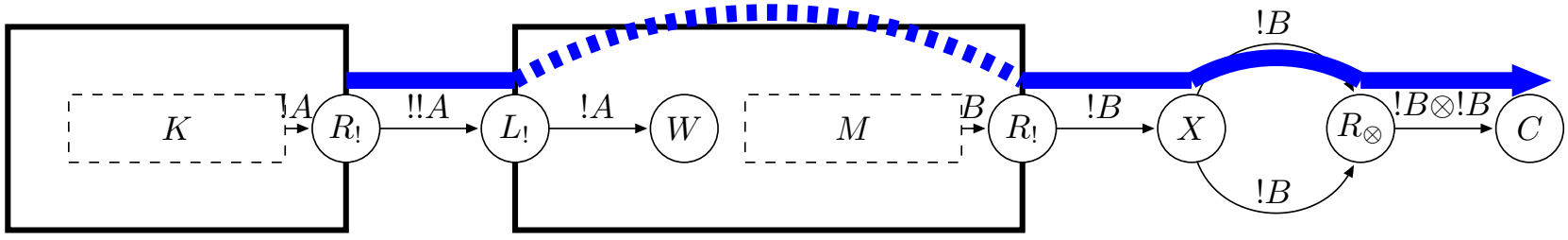
Another Example



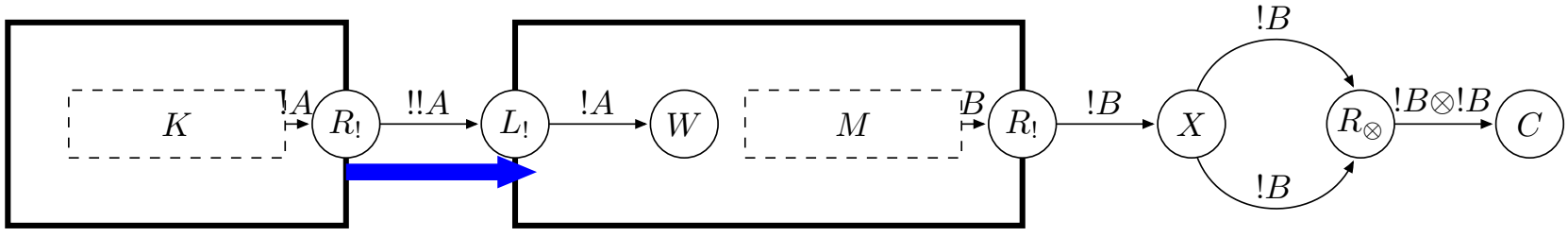
Another Example



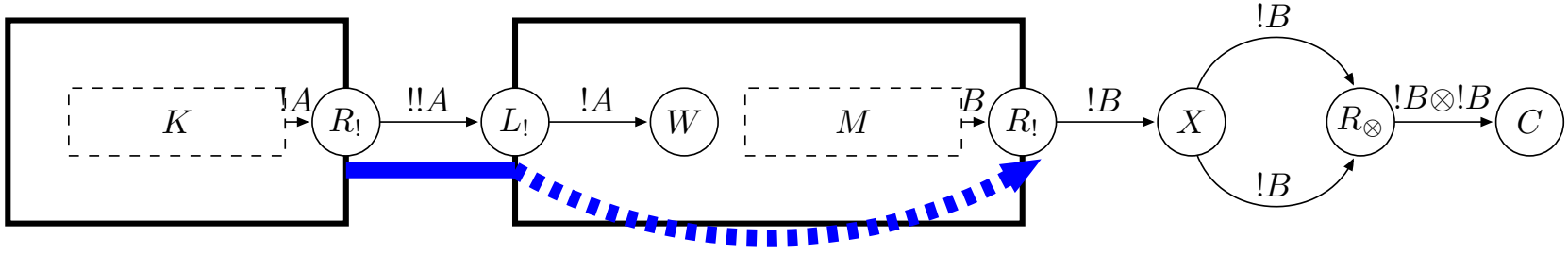
Another Example



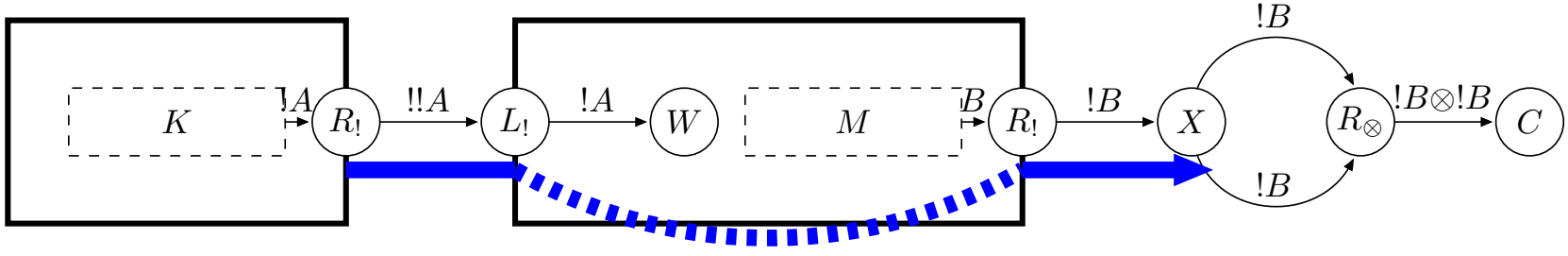
Another Example



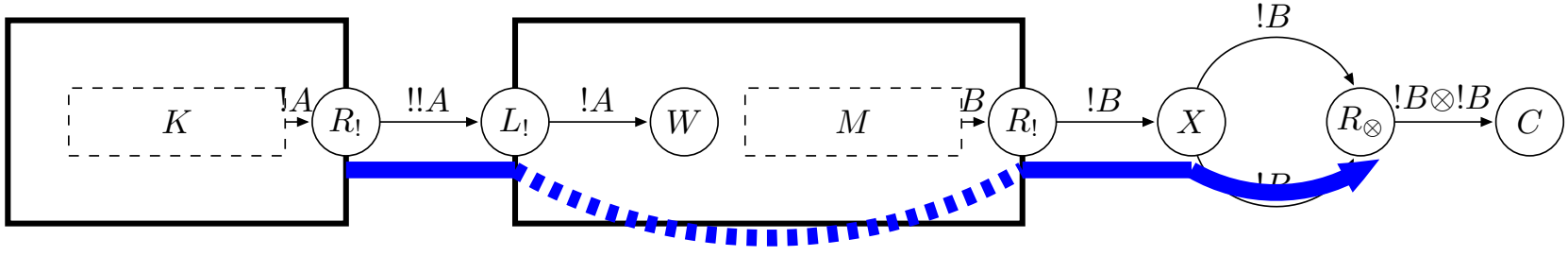
Another Example



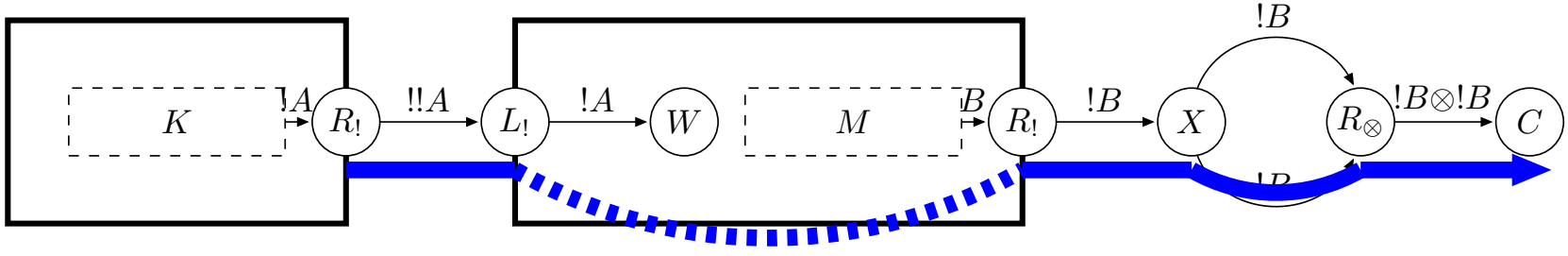
Another Example



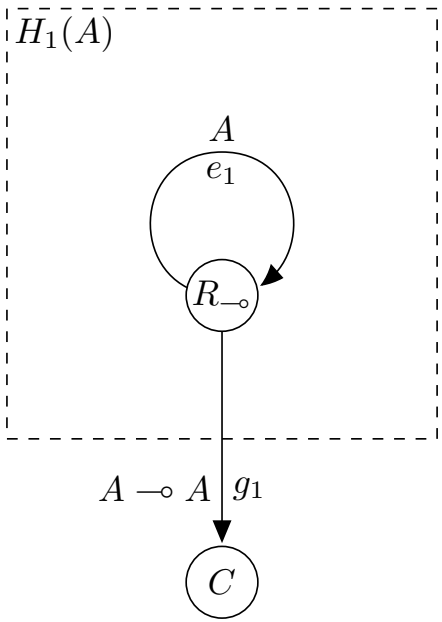
Another Example

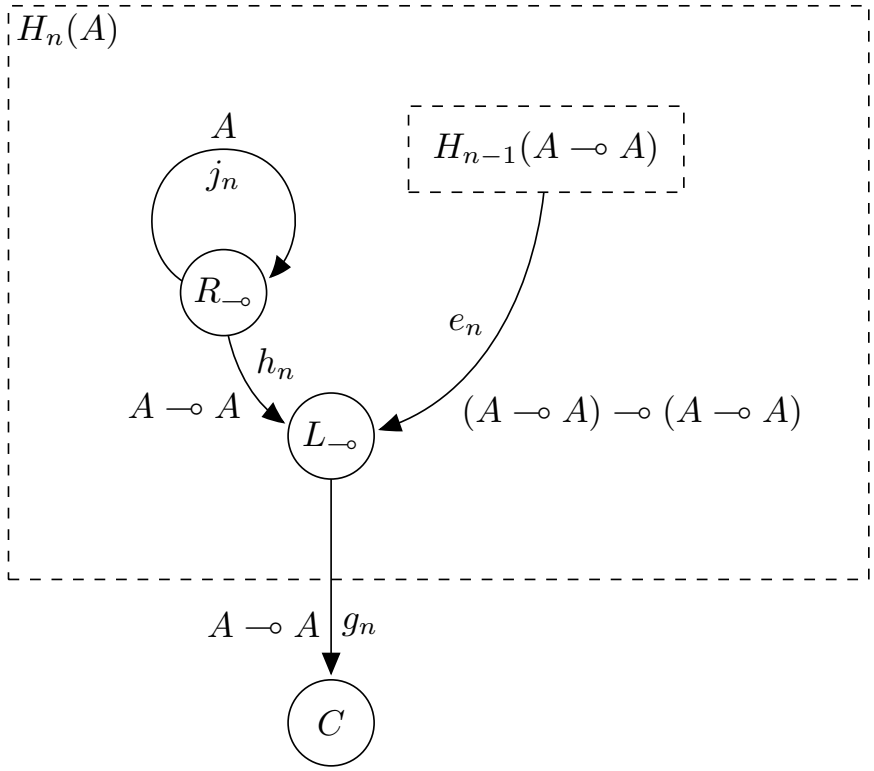


Another Example

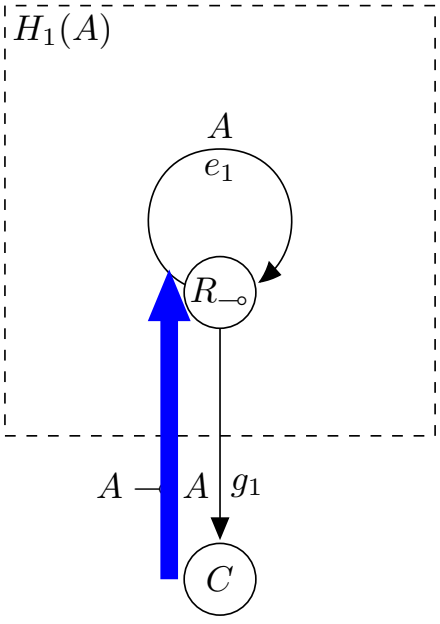


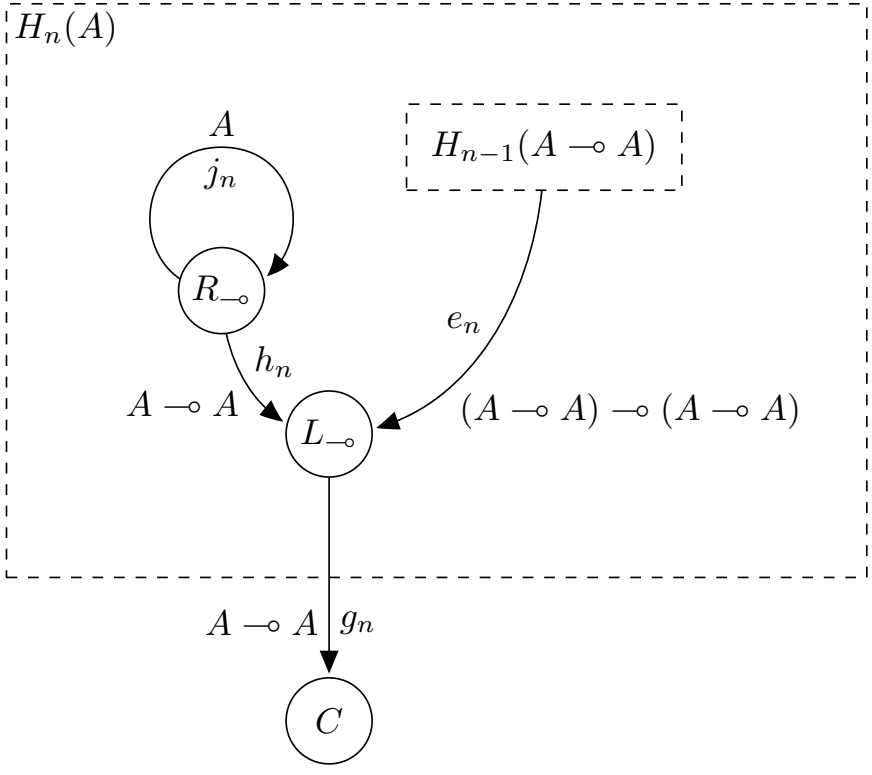
A Further Example



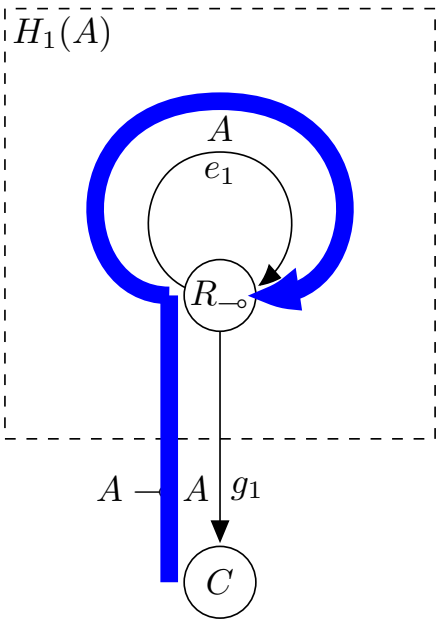


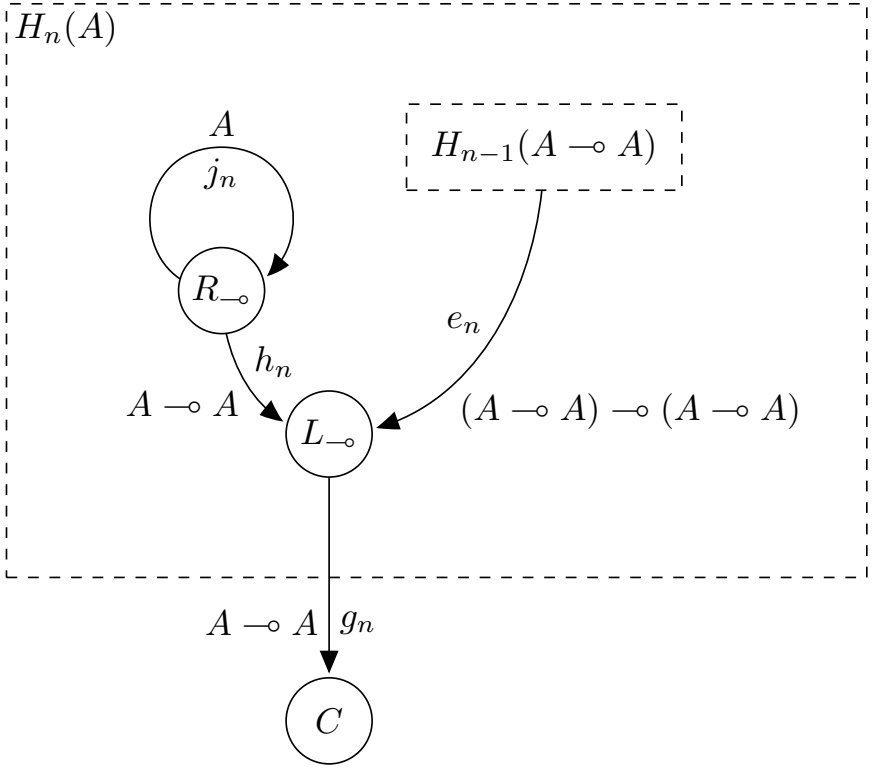
A Further Example



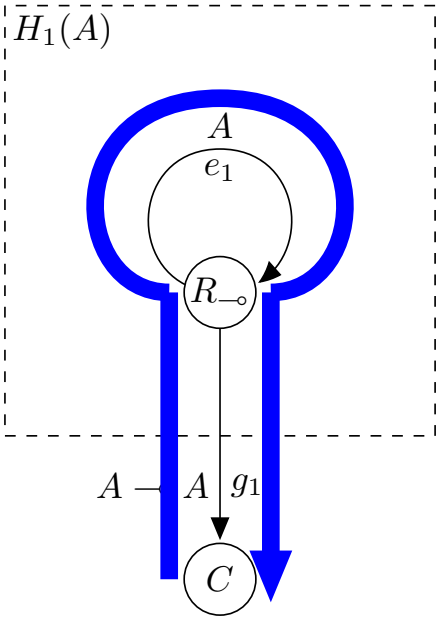


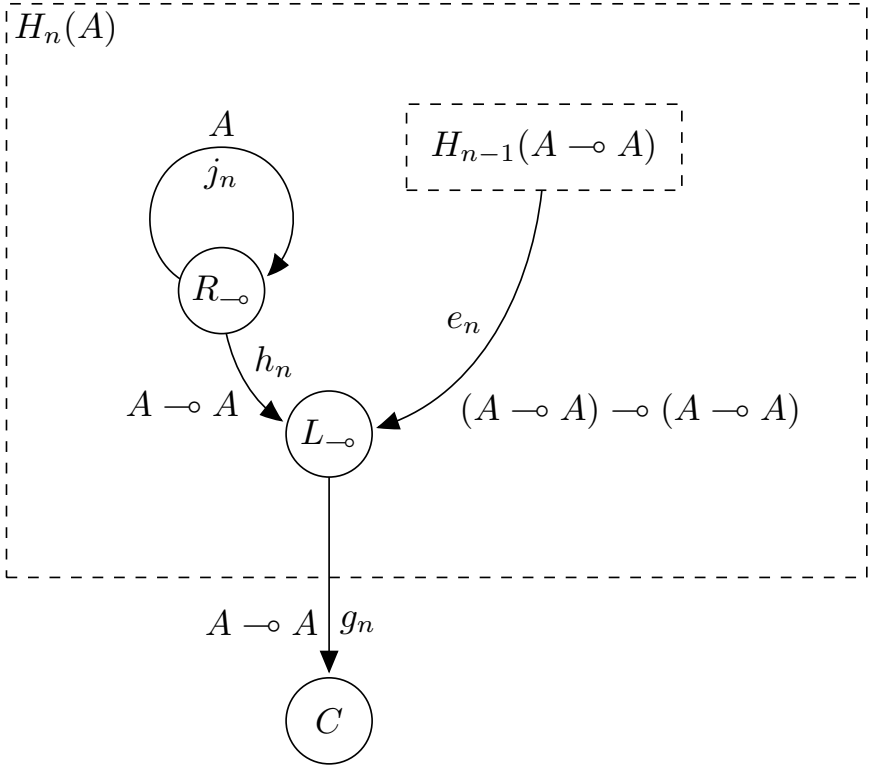
A Further Example



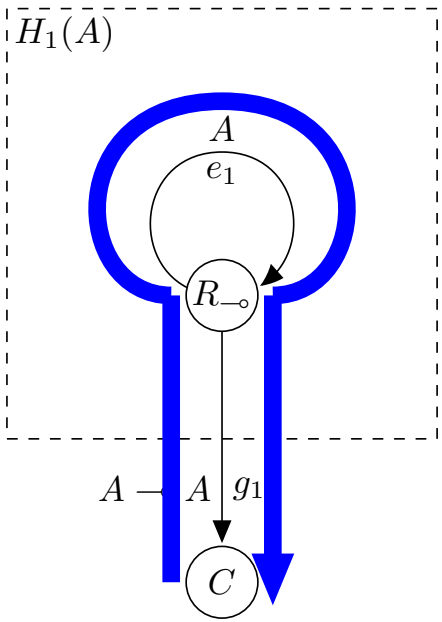


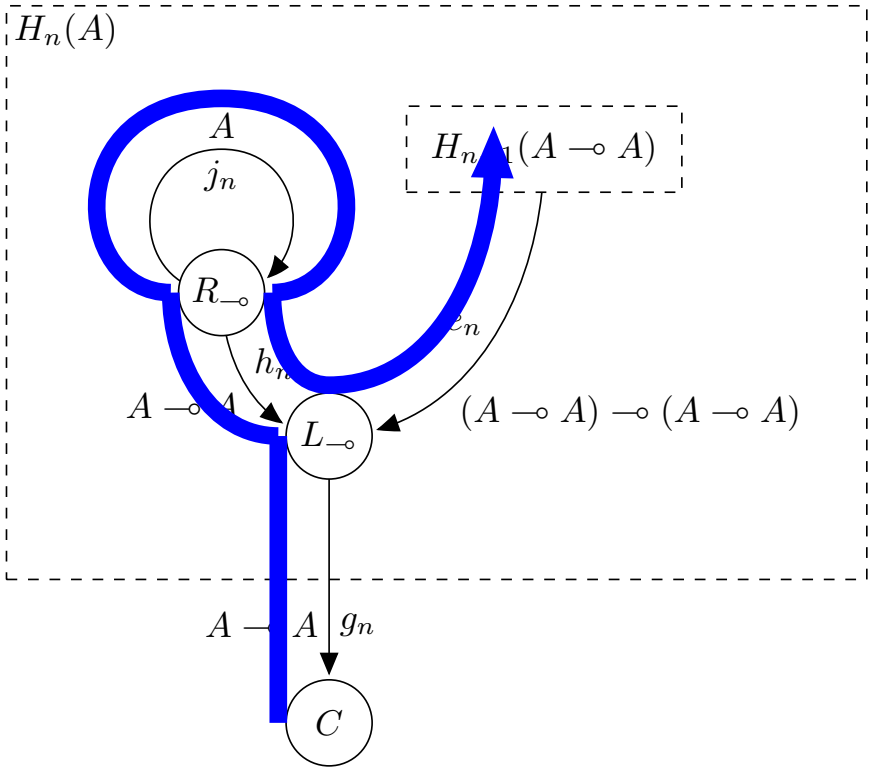
A Further Example



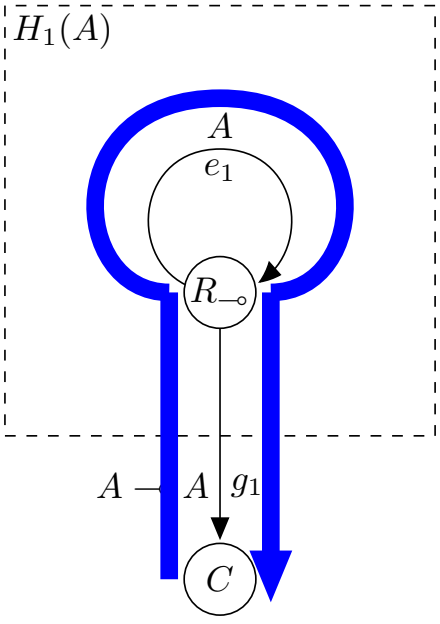


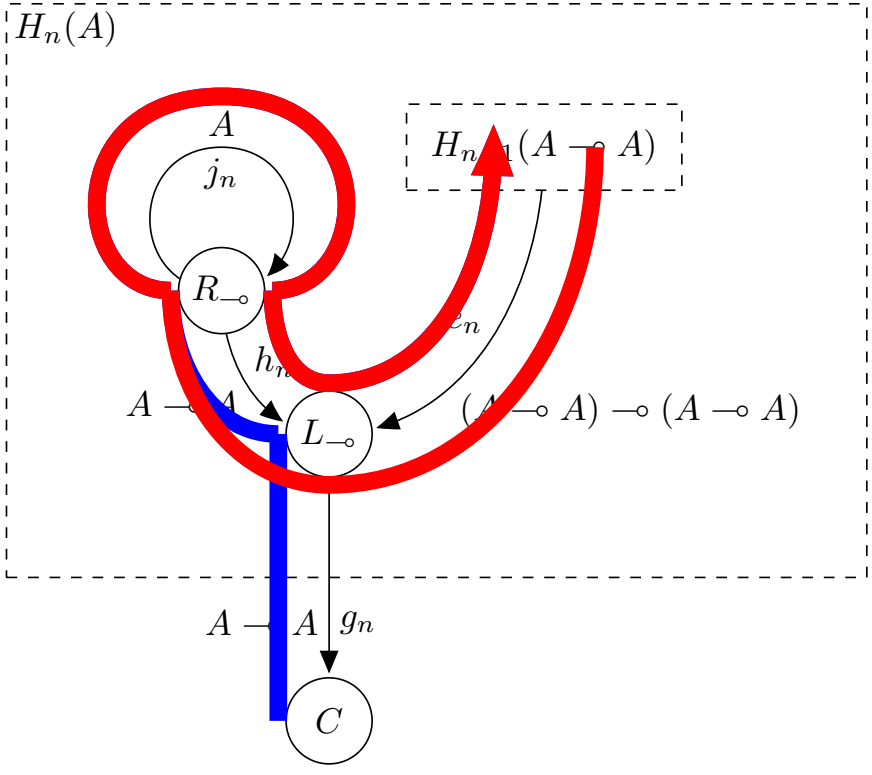
A Further Example



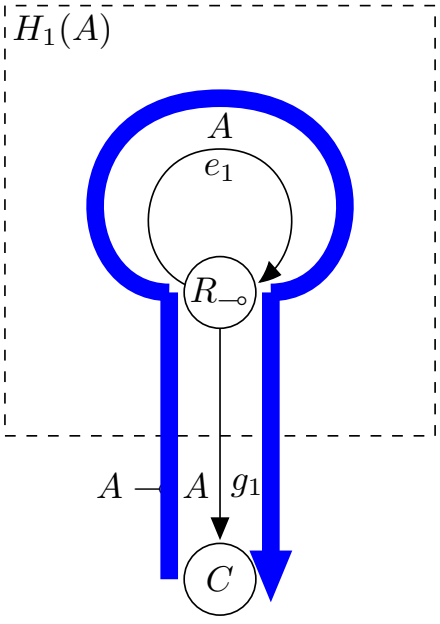


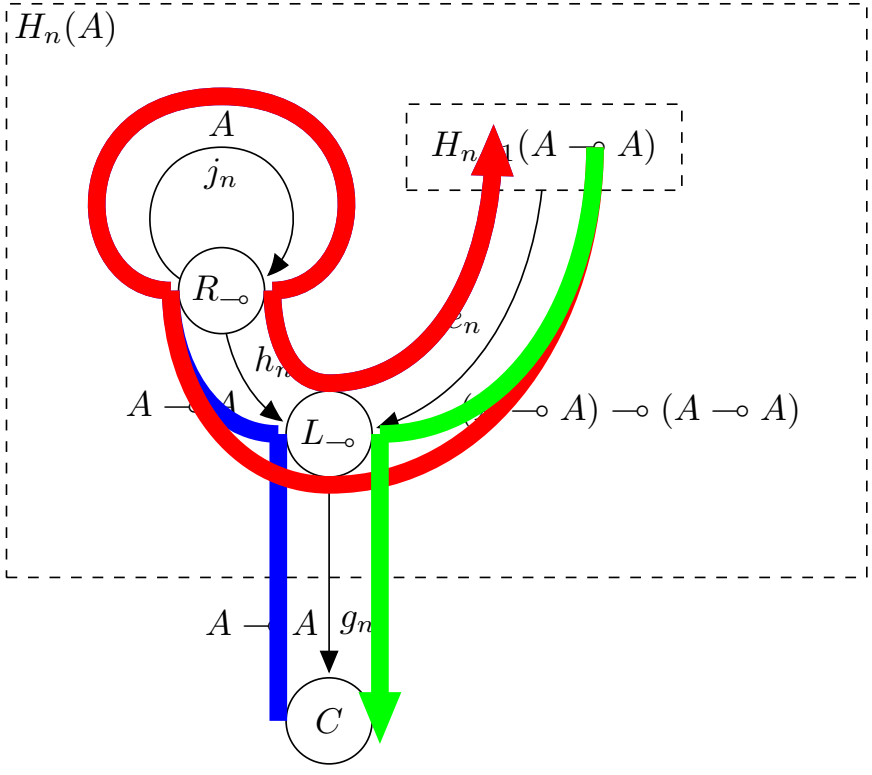
A Further Example





A Further Example





The Weight of a Proof-net

- If $e \in E_G$ is a box main premise, then every exponential tree t with $(e, U, t, +) \mapsto^* C$ (where C is final) corresponds to a different *copy* of the box *under* U.
- U is canonical for $e \in E_G$ if it is built up from copies of the boxes in which $e \in E_G$ is contained.
- The natural number $R_G(e, U)$ is the number of distinct copies of e under U.
- W_G is the sum of $R_G(e, U)$ over all box main premises and over all canonical sequences for them.

Key Property

- W_G is always positive, but is not guaranteed to strictly decrease at any normalization step.
- It is not clear whether the size of $|G|$ is related to W_G or not.
- However, we can define another quantity T_G which *both* decreases at every normalizatop step and majorizes $|G|$.
- As a consequence, we get:

Proposition (Monotonicity)

There are normalization strategies PW and LBL such that $W_G \geq W_H$ and $T_G > T_H$ whenever H is obtained from U using the PW strategy and, moreover, $W_G \leq W_H + 1$ whenever H is obtained from G using the LBL strategy.

One Direction

- T_G is polynomially related to W_G and $|G|$.
- The PW strategy is the worst one:
  - It takes as least as many steps as any other reduction strategy.
  - It maximizes the size of reducts.
- As a consequence, we get:

Theorem

There is a polynomial $p : \mathbb{N}^2 \to \mathbb{N}$ such that for every proof-net G, G normalizes in at most $p(W_G, |G|)$ steps and the size of any reduct H of G is at most $p(W_G, |G|)$.

The Other Direction

- Is W_G a gross overestimate on the time needed to normalize G?
- Consider the LBL strategy:
  - For every $n \in \mathbb{N}$, a cut at level $n+1$ is fired only if there are not cuts at levels from 1 to n.
  - For every $n \in \mathbb{N}$, a !-cut at level n is fired only if every cut at level n is either a W-cut or a !-cut.
  - A W-cut is fired only if every cut in the proof-net is a W-cut.
- W_G decreases by at most one at every step.
- As a consequence, we get:

Theorem

Let G be a proof-net. Then there is H with $G \rightarrow^{W_G} H$.

Consequences

- The two results can together be seen as a strengthening of the well-known correspondence between strongly normalizing nets and finiteness of regular paths.
- This has very interesting consequences: for example, a family $\mathscr{G}$ 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 $G \in \mathscr{G}$.
- This will greatly help when giving new proofs of soundness for various subsystems of linear logic.
- As a side-effect, we have succeeded in defining an invariant cost-model for MELL proof-nets. If we consider W_G as *the cost* of normalizing G, proof-nets and Turing machines can simulate each other with a polynomial overhead in time.

Elementary Linear Logic

- Rules $N_!$ and $D_!$ are no more part of the sequence calculus.
- As a consequence:

Lemma (Stratification)

Let G be an elementary linear logic proof-net. If $(e, U, V, b) \to^* (g, W, Z, c)$, then $\|U\| + \|V\| = \|W\| + \|Z\|$.

- The usual soundness theorem can be reproved:

Proposition (ELL Soundness)

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

Soft Linear Logic

- It can be defined from ELL by replacing rule X with M as follows:

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

- Exponential trees becomes simpler:

$$t ::= \mathrm{e} \mid \mathrm{m}(i)$$

where i ranges over natural numbers.

- We obtain:

Proposition (SLL Soundness)

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

Light Linear Logic - I

- (Multiplicative) Light linear logic can be obtained from ELL by enriching the language of formulae with a new modal operator § and splitting rule $P_!$ into two rules:

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

- At the proof-nets level, two box constructions, !-boxes and §-boxes, correspond to $S_!$ and $S_\S$.
- As for the underlying context semantics, !-boxes induce the usual rewriting rules on C_G, while the last two rules are not valid for §-boxes.

Light Linear Logic - II

- As an immediate consequence of the restrictions on rules for exponentials, we get

Lemma (Strong Determinacy)

For every context C there is at most one context D such that $C \to_G D$.

- So:

Proposition (LLL Soundness)

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

Contributions

- We have proved the existence of deep connections between W_G and the cost of normalizing G.
- Copying has been proved to be the real source of complexity in the realm of linear logic.
- We have reproved strong soundness results for fragments of multiplicative and exponential linear logic.
- Most work is factored over the various fragments and done just once.

Contributions

- We have proved the existence of deep connections between W_G and the cost of normalizing G.
- Copying has been proved to be the real source of complexity in the realm of linear logic.
- We have reproved strong soundness results for fragments of multiplicative and exponential linear logic.
- Most work is factored over the various fragments and done just once.

Contributions

- We have proved the existence of deep connections between W_G and the cost of normalizing G.
- Copying has been proved to be the real source of complexity in the realm of linear logic.
- We have reproved strong soundness results for fragments of multiplicative and exponential linear logic.
- Most work is factored over the various fragments and done just once.

Future Developments

- Is context semantics related to resource polynomials and weights in bounded linear logic?
- Extend the results to affine variants of the considered systems (easy).
- Extend the results to pure, untyped, nets.

Questions?