An extended framework for specifying and reasoning about proof systems

Giselle Reis

TUWien

June, 2012

Joint work with Vivek Nigam and Elaine Pimentel
An extended framework for specifying and reasoning about proof systems
There are several logics: classical logic, intuitionistic logic (and fragments), modal logics, paraconsistent logics...
Developed for the most varied applications: theorem provers, knowledge representation, proof carrying code...

These logics need proof systems for reasoning.

These proof systems should have nice properties, such as:

- cut-elimination
- admissibility of non-atomic axioms
- invertibility of rules

But proving each property for each system by hand can be very time-consuming and error-prone...
Our approach

Provide a framework that can prove these properties in a uniform and automatic way to various proof systems.

Sequent Calculus Proof System $\Rightarrow$ Logical Framework

- Are cuts admissible?
- Are non-atomic axioms admissible?
- Which are the invertible rules?

Logical Framework $\equiv$ Linear Logic with Subexponentials
Linear Logic

Resource-aware logic:

- **Classical** formulas: “marked” with the exponential operators (! and ?)
- **Linear** formulas: are consumed when used

Refinement of classical logic:

<table>
<thead>
<tr>
<th></th>
<th>Additive</th>
<th>Multiplicative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conjunction ((\land))</td>
<td>&amp;</td>
<td>(\otimes)</td>
</tr>
<tr>
<td>Disjunction ((\lor))</td>
<td>(\oplus)</td>
<td>(\otimes)</td>
</tr>
</tbody>
</table>

\[
\frac{\vdash \Theta : \Gamma, P \quad \vdash \Theta : \Gamma, Q}{\vdash \Theta : \Gamma, P \& Q} \quad [\&]
\]

\[
\frac{\vdash \Theta : \Gamma, P \quad \vdash \Theta : \Delta, Q}{\vdash \Theta : \Gamma, \Delta, P \otimes Q} \quad [\otimes]
\]

Operators can be **canonical**:

\[
A \&^a B \equiv A \&^b B
\]

Exponentials are not canonical (all others are):

\[
!^a F \neq !^b F \quad \text{and} \quad ?^a F \neq ?^b F
\]

\(^a\) and \(^b\) are different operators in linear logic, they are called **subexponentials**.

\[
\vdash \Theta_a : \Theta_b : \Gamma \equiv \vdash \mathcal{K} : \Gamma
\]
One may declare as many subexponentials as needed, organized in a pre-order.

\[
i \text{ allows contraction and weakening} \quad \Rightarrow \quad \Theta_i \text{ is a set}
\]

\[
i \text{ does not allow contraction and weakening} \quad \Rightarrow \quad \Theta_i \text{ is a multi-set}
\]

**Note:** The logics specified may have contexts that behave as set or multi-set. Interesting... :)

---

**Subexponentials** [Danos, et al 1993, Nigam and Dale, 2009]

\[
\frac{\vdash \mathcal{K} \leq_l \vdash A}{\vdash \mathcal{K} \vdash \downarrow ! A} \quad [!'], \text{ s.t. } \mathcal{K}[[x | l \not\in x \land x \not\in \mathcal{U}]] = \emptyset
\]

\[
\vdash \mathcal{K} : ! A \vdash \mathcal{K} : \Gamma \uparrow L, ?' A \quad [?']
\]

Rule ?': stores a formula in a context.
Rule !': very useful for the restrictions on the context.

- smaller or not related “linear” subexponentials must be empty
- smaller or not related “classical” subexponentials are made empty
Focused proofs are the normal form of proofs for proof search

- **Sound** and **complete** proof search strategy for linear logic
- Based on the division of linear logic’s connectives:
  - **Asynchronous** (negative): $\otimes, \&, ?^i, \top, \bot, \forall$
  - **Synchronous** (positive): $\otimes, \oplus, !^i, 1, 0, \exists$

  Asynchronous $\Rightarrow$ invertible rules $\Rightarrow$ apply eagerly

  Synchronous $\Rightarrow$ non-invertible rules $\Rightarrow$ apply when no negative formula is left
Focused proofs are composed by the alternation of **negative** and **positive** phases.

Each *phase* is a collection of rules of the same polarity that can compose one or more **macro-rule**:

\[ \vdash \mathcal{K} : \Gamma \downarrow A_i \quad \vdash \mathcal{K} : \Gamma \downarrow A_1 \oplus A_2 \quad \vdash \mathcal{K} : \Gamma \downarrow A_1 \quad \vdash \mathcal{K} : \Gamma \downarrow A_2 \quad \vdash \mathcal{K} : \Gamma \uparrow N \quad \vdash \mathcal{K} : \Gamma \downarrow \neg \]

\[ N_1 \oplus (N_2 \otimes N_3) \Rightarrow \]

\[ \vdash \mathcal{K} : \Gamma \uparrow N_1 \quad \vdash \mathcal{K} : \Gamma \downarrow N_1 \oplus (N_2 \otimes N_3) \quad \text{or} \quad \vdash \mathcal{K} : \Gamma \uparrow N_2 \quad \vdash \mathcal{K} : \Delta \uparrow N_3 \quad \vdash \mathcal{K} : \Gamma, \Delta \downarrow N_1 \oplus (N_2 \otimes N_3) \]
Encoding Sequent Calculus Systems in LL

Types:

<table>
<thead>
<tr>
<th></th>
<th>Linear-Logic Formulas</th>
</tr>
</thead>
<tbody>
<tr>
<td>o</td>
<td>Linear-Logic Formulas</td>
</tr>
<tr>
<td>form</td>
<td>Object-Logic Formulas</td>
</tr>
<tr>
<td>term</td>
<td>Object-Logic Terms</td>
</tr>
</tbody>
</table>

Propositions:

\[
\frac{\llbracket B_1 \rrbracket, \ldots, \llbracket B_n \rrbracket, \llbracket C_1 \rrbracket, \ldots, \llbracket C_m \rrbracket}{\llbracket B_1, \ldots, B_n \rrbracket \vdash C_1, \ldots, C_m}
\]

Object-Logic

Meta-Logic (SELLF)
Bipoles

Monopole: atoms and negative connectives.

Bipole: negated atoms, monopoles and positive connectives.

A bipole derivation contains a single alternation of phases:
**Adequacy of encoding**

Bipole-derivation $\equiv$ **object-logic rule**

\[
\begin{align*}
\Gamma, A &\rightarrow B \\
\Gamma &\rightarrow A \supset B, \Delta \overset{r}{\supset}
\end{align*}
\]

$(\supset r) : \lceil A \supset B \rceil \perp \otimes !^l (\lceil ?^l [A] \otimes r^l [B] \rceil)$

\[
\begin{align*}
\vdash \Theta \otimes [\Gamma] \downarrow i [\Delta, A \supset B] \downarrow \uparrow [A \supset B] \perp & \quad \Theta \otimes [\Gamma] \downarrow i [\Delta, A \supset B] \downarrow \uparrow !^l (\lceil ?^l [A] \otimes r^l [B] \rceil) & \Theta \otimes [\Gamma] \downarrow i [\Delta, A \supset B] \downarrow \uparrow !^l (\lceil ?^l [A] \otimes r^l [B] \rceil) & D_{\infty}, 2 \times \exists
\end{align*}
\]

**Adequacy on the level of derivations**
Another example

**System G3K**

\[
\frac{y : A, x : \Box A, xRy, \Gamma \Rightarrow \Delta}{x : \Box A, xRy, \Gamma \Rightarrow \Delta} \quad (\Box I) \quad [x : \Box A] \bot \otimes \exists y. (R^\top R(x, y) \bot \otimes ?^\top [y : A])
\]

\[
\begin{align*}
\Gamma & \vdash \infty R \quad \hat{R} \quad \hat{i} \quad \hat{r} \quad \uparrow \quad R(a, b) \bot \\
\Gamma & \vdash \mathcal{L}_{G3K} \otimes \hat{R} \quad \hat{i} \quad \hat{r} \quad \downarrow \quad (R^\top R(a, b) \bot \otimes ?^\top [b : A]) \quad \otimes, \exists \\
\Gamma & \vdash \mathcal{L}_{G3K} \otimes \hat{R} \quad \hat{i} \quad \hat{r} \quad \downarrow \quad [a : \Box A] \bot \otimes \exists y. (R^\top R(a, y) \bot \otimes ?^\top [y : A]) \quad D_{\infty}, \exists \\
\Gamma & \vdash \mathcal{L}_{G3K} \otimes \hat{R} \quad \hat{i} \quad \hat{r} \quad \downarrow \quad [a : \Box A, \Gamma] \bot \otimes \exists y. (R^\top R(a, y) \bot \otimes ?^\top [y : A]) \quad \otimes, \exists
\end{align*}
\]

Where Ξ is a derivation containing only the initial rule.

This system + a subset of the labels’ relations captures different modal logics, such as T, 4, B, S4, TB, S5.
Proof Systems Theories

1. Identity rules (cut and initial)

\[ \text{Cut} = \exists A. !^a ?^b [A] \otimes !^c ?^d [A] \]
\[ \text{Init} = \exists A. [A] \perp \otimes [A] \perp \]

2. Structural rules

\[ \exists A. [A] \perp \otimes (?!^i [A] \otimes \ldots \otimes ?^i [A]) ] \]
\[ \exists A. [A] \perp \otimes (?!^j [A] \otimes \ldots \otimes ?^j [A]) ] \]

3. Introduction rules

\[ \exists x_1 \ldots \exists x_n ([\diamond (x_1, \ldots, x_n)] \perp \otimes B] \]
\[ \exists x_1 \ldots \exists x_n ([\diamond (x_1, \ldots, x_n)] \perp \otimes B] \]
Systems encoded and the subexponentials used

- G1m (minimal logic): $l, r$ both linear
- mLJ (multi-conclusion LJ): $l, r$ both classical
- LJQ* (focused sequent calculus for LJ): $f$ linear, $l, r$ classical
- S4 (modal logic):
  - $l, r$: classical
  - $\Box_L, \Diamond_R$: classical (holds formulas marked with $\Box$ or $\Diamond$ on the left or right)
  - $e$: classical (“dummy” subexponential to specify structural properties)
- Lax Logic (intuitionistic modal logic):
  - $l$ classical, $r$ linear
  - $\triangleright_r$ linear
- G3K + relation rules (modal logics T, 4, B, S4, TB, S5): $l, r, R$ classical
Proving cut-elimination

1. Reduction to principal cuts
   - Permute cut rules upwards
   - Permute introduction rules downwards
   - Transform one cut into another (no general procedure was found yet)

2. Reduction to atomic cuts

3. Elimination of atomic cuts
Proving cut-elimination

**Step 1:** Reduction to principal cuts

- Permute cut rules upwards

\[
\begin{align*}
\Gamma, \Gamma' & \rightarrow \ell \\
\Gamma & \rightarrow A & \Gamma', A & \rightarrow F \supset G \\
\Gamma & \rightarrow \ell & \Gamma, \Gamma' & \rightarrow F \supset G
\end{align*}
\]

- Permute introduction rules downwards

\[
\begin{align*}
\phi & \Gamma, A \land B & \rightarrow F \supset G, \Delta \\
\ensuremath{\varphi} & \Gamma, A, B & \rightarrow F \supset G, \Delta \\
\Gamma & \rightarrow \ell & \Gamma & \rightarrow \ell
\end{align*}
\]

**Permutations:**
Depend on the subexponentials and their relations.
Proving cut-elimination

**Step 1:** Reduction to principal cuts
Proof by static analysis of subexponentials.
Example: Cut $= \exists A.!^a?^b[A] \otimes !^c?^d[A]$

\[
\begin{align*}
& \vdash K_1 \leq_a +_b[A] : \cdot \uparrow . \quad !^a, ?^b \\
& \vdash K_1 : \cdot \downarrow !^a?^b[A] & \Xi_1 \\
& \vdash K_2 \leq_c +_d[A] : \cdot \uparrow . \quad B : \cdot \uparrow . \quad !^s, ?^t \\
& \vdash K_2 \leq_c +_d[A] : \cdot \uparrow . \quad C \vdash K_2 : \cdot \downarrow !^c?^d[A] & \Xi_2' \\
& \vdash K_1 \otimes K_2 : \cdot \downarrow !^a?^b[A] \otimes !^c?^d[A] \quad D_\infty \otimes \\
& \vdash K_1 \otimes K_2 : \cdot \uparrow D_\infty, \exists
\end{align*}
\]

Case: $s \not\preceq d$ impossible (otherwise rule $!^s$ could not be applied).
**Proving cut-elimination**

**Step 1:** Reduction to principal cuts

Case: \( s \preceq d \)

\[
\begin{align*}
\Xi_1 & \quad \dfrac{\vdash \mathcal{K}_1 \leq_{s,a + b} A : \uparrow \cdot}{\vdash \mathcal{K}_1 \leq_s : \downarrow^a \downarrow^b [A]} \\
\Xi_2 & \quad \dfrac{\vdash \mathcal{K}_2 \leq_{s,c + t} B + d \ [A] : \uparrow \cdot}{\vdash \mathcal{K}_2 \leq_{s + t} : \downarrow^c \downarrow^d [A]} \\
\times & \quad \dfrac{\vdash \mathcal{K}_1 \otimes \mathcal{K}_2 \leq_{s + t} B : \downarrow^a \downarrow^b [A] \otimes \downarrow^c \downarrow^d [A]}{D_\infty, \exists} \\
\Rightarrow & \quad \dfrac{\vdash \mathcal{K}_1 \otimes \mathcal{K}_2 \leq_{s + t} \uparrow \cdot}{\vdash \mathcal{K}_1 \otimes \mathcal{K}_2 : \downarrow^s \downarrow^t B} \\
\Rightarrow & \quad \dfrac{\vdash \mathcal{K}_1 \otimes \mathcal{K}_2 : \uparrow \cdot}{D_\infty}
\end{align*}
\]

This permutation is possible given:

- \( s \preceq a \Rightarrow \mathcal{K}_1 \leq_{s,a} \mathcal{K}_1 \leq_a \)
- \( c \preceq t \Rightarrow \downarrow^c \) is allowed
Proving cut-elimination

**Step 2:** Reduction to atomic cuts [Miller and Pimentel, 2012]

Left and right introduction rules must be **dual**.

Introduction rules for a connective $\diamond$:

$$\exists \bar{x}(\downarrow \diamond(\bar{x}) \downarrow \otimes B_l) \quad \text{and} \quad \exists \bar{x}(\uparrow \diamond(\bar{x}) \uparrow \otimes B_r)$$

They are called **dual** the following can be proved in sellf:

$$\vdash \text{Cut} : \cdot \vdash \forall \bar{x}(B_l \uparrow \otimes B_r)$$
Proving cut-elimination

**Step 2:** Reduction to atomic cuts [Miller and Pimentel, 2012]

Proof:

\[
\vdash \Psi; \Delta_1 \Downarrow B_l \quad \vdash \Psi; \Delta_2 \Downarrow B_r \\
\vdash \Psi; \Delta_1, \Delta_2 \uparrow \cdot \quad D_2 \quad \Rightarrow \quad \text{Cut on object logic}
\]
Proving cut-elimination

**Step 2**: Reduction to atomic cuts [Miller and Pimentel, 2012]

Since $B_l$ and $B_r$ are dual:

\[
\begin{align*}
\tilde{\Pi}_2 & \vdash \exists \chi, \exists \text{Cut}, \exists \psi, \Delta_2, B_r \\
\tilde{\Pi}_1 & \vdash \exists \chi, \exists \text{Cut}, \exists \psi, \Delta_1, B_l \\
\Pi' & \vdash \exists \chi, \exists \text{Cut}, \exists \psi, \Delta_1, B_r \vdash \exists \chi, \exists \text{Cut}, \exists \psi, \Sigma, B_l \vdash \exists \chi, \exists \text{Cut}, \exists \psi, \Delta_1, \Delta_2
\end{align*}
\]

$	ilde{\Pi}_1$ and $	ilde{\Pi}_2$ are the proofs $\Pi_1$ and $\Pi_2$ transformed to unfocused proofs.

**Cut-elimination on meta-level**: decides on object level cuts may still exist, but on simpler formulas than $B_l$ and $B_r$.  

Giselle Reis | An extended framework for specifying and reasoning about proof systems
Step 3: Elimination of atomic cuts

Further restrictions needed on the subexponentials used for the cut rule:

\[ \vdash \mathcal{K}_1 \leq a + b [A] : \uparrow \cdot \]
\[ \vdash \mathcal{K}_1 : \downarrow !a ?b [A] \]
\[ \vdash \mathcal{K}_2 \leq c + d : \downarrow [A] \uparrow \cdot \]
\[ \vdash \mathcal{K}_2 \leq c + d [A] : \uparrow \cdot \]
\[ \vdash \mathcal{K}_2 : \downarrow !c ?d [A] \]
\[ \vdash \mathcal{K}_1 \otimes \mathcal{K}_2 : \downarrow !a ?b [A] \otimes !c ?d [A] \]
\[ \vdash \mathcal{K} : \uparrow \cdot \]

\[ \mathcal{K}_1 \subset \mathcal{K} \text{ and } [A] \in \mathcal{K} \Rightarrow [A] \text{ must be in } s \text{ such that } b \preceq s \]

Note: A formula may be moved to an upper subexponential without affecting provability.
Theorem: Given a proof system’s specification in SELLF, all conditions for the admissibility of cuts described are decidable.

- Permutation of rules and elimination of atomic cuts: static check of the subexponentials used.
- Duality of introduction rules: proved in $\nu + 2$ steps, where $\nu$ is the maximum number of premisse atoms in the body of the introduction clauses.

Note: Some cut-elimination cases cannot yet be identified, such as the transformation of one cut into another.
Proving admissibility of non-atomic identities

[Miller and Pimentel, 2012]

Introduction rules for a connective \( \diamond \):

\[
\exists \bar{x}(\lceil \diamond (\bar{x}) \rceil \perp \otimes B_l) \quad \text{and} \quad \exists \bar{x}(\lceil \diamond (\bar{x}) \rceil \perp \otimes B_r)
\]

They are called initial-coherent the following can be proved in sellf:

\[
\vdash \text{Init} : \cdot \uparrow \forall \bar{x}(\exists^\infty B_l \otimes \exists^\infty B_r)
\]

In a system with initial coherent introduction rules, the initial rule can be restricted to its atomic version.
Proving the invertibility of rules

Follows from the facts:

- object-logic rules $\Rightarrow$ bipoles in SELLF
- bipoles in SELLF $\Rightarrow$ bodies are (purely) negative formulas
- negative formulas $\Rightarrow$ negative rules are invertible in SELLF
- invertible rules $\Rightarrow$ permutable rules
- permutable rules in meta-logic + adequacy on the level of derivations $\Rightarrow$ permutable rules in the object-logic
- object-logic rules are invertible
Conclusion

Given a sequent calculus system’s specification in SELLF, we can:

- Prove cut-elimination (if the proof is not very involved)
- Prove admissibility of non-atomic initial rules
- Check the invertibility of rules

Implemented and online at http://www.logic.at/people/giselle/tatu.
Thank you for your attention!

Questions?