A Linear Logic Modulo

Olivier Hermant

June 29, 2007

- Linear Logic has much to say about connectors.
- Deduction Modulo has much to say about (first-order) quantifiers.

- Linear Logic has much to say about connectors.
- Deduction Modulo has much to say about (first-order) quantifiers.
- let’s combine them.

The language

- Usual first-order logic language.
- logical connectors

$$\overbrace{\otimes, \parr, \multimap}^{\text{multiplicatives}} \quad , \quad \overbrace{\&, \oplus}^{\text{additives}} \quad , \quad \overbrace{!, ?}^{\text{exponentials}}$$

- logical constants

$$\overbrace{\mathbf{1}, \bot}^{\text{multiplicatives}} \quad , \quad \overbrace{\top, \mathbf{0}}^{\text{additives}}$$

- first-order quantifiers $\forall, \exists$

The language

- Usual first-order logic language.
- logical connectors

$$\overbrace{\otimes, \parr, \multimap}^{\text{multiplicatives}}, \overbrace{\&, \oplus}^{\text{additives}}, \overbrace{!, ?}^{\text{exponentials}}$$

- logical constants

$$\overbrace{\mathbf{1}, \bot}^{\text{multiplicatives}}, \overbrace{\top, \mathbf{0}}^{\text{additives}}$$

- first-order quantifiers $\forall, \exists$
- the negation symbol $\bot$ is not a primitive symbol
- atoms A and negated atoms $A^\bot$
- we work with negation normal forms (classical LL, one sided sequent calculus)

Dualities in Linear Logic

$$A^{\perp\perp} = (A^{\perp})^{\perp} = A$$

Multiplicatives

$$\perp^{\perp} = \mathbf{1} \qquad \mathbf{1}^{\perp} = \perp$$

$$(A \otimes B)^{\perp} = A^{\perp} \parr B^{\perp} \qquad (A \parr B)^{\perp} = A^{\perp} \otimes B^{\perp}$$

$$A \multimap B = A^{\perp} \parr B$$

Additives

$$\top^{\perp} = \mathbf{0} \qquad \mathbf{0}^{\perp} = \top$$

$$(A \oplus B)^{\perp} = A^{\perp} \,\&\, B^{\perp} \qquad (A \,\&\, B)^{\perp} = A^{\perp} \oplus B^{\perp}$$

Exponentials

$$(!A)^{\perp} = ?(A^{\perp}) \qquad (?A)^{\perp} = !(A^{\perp})$$

Quantifiers

$$(\forall x A)^{\perp} = \exists x A^{\perp} \qquad (\exists x A)^{\perp} = \forall x A^{\perp}$$

Deduction rules

- sequent style
- one-sided (duality): $\Gamma \vdash \Delta$ is written $\vdash \Gamma^{\perp}, \Delta$ (negation NF)
- axiom looks like $\vdash A^{\perp}, A$

Deduction rules

- sequent style
- one-sided (duality): $\Gamma \vdash \Delta$ is written $\vdash \Gamma^{\perp}, \Delta$ (negation NF)
- axiom looks like $\vdash A^{\perp}, A$
- independent groups of connectors (substructural logics)
- multiplicatives separate the context (perfect world)
- additives do not (imperfect world)
- contexts: sets (no permutation needed)

Deduction rules of Linear Logic

Identities

$$\frac{}{\vdash A^\perp, A}\ \text{init} \qquad \frac{\vdash A^\perp, \Gamma \qquad \vdash A, \Delta}{\vdash \Gamma, \Delta}\ \text{cut}$$

Multiplicatives

$$\frac{}{\vdash \mathbf{1}}\ \mathbf{1}\text{-r} \qquad \frac{\vdash \Delta}{\vdash \perp, \Delta}\ \perp\text{-r}$$

$$\frac{\vdash A, \Gamma \qquad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta}\ \otimes\text{-r} \qquad \frac{\vdash A, B, \Delta}{\vdash A \parr B, \Delta}\ \parr\text{-r}$$

Additives

no **0**-r

$$\frac{}{\vdash \top, \Gamma}\ \top\text{-r}$$

$$\frac{\vdash A, \Delta \qquad \vdash B, \Delta}{\vdash A \,\&\, B, \Delta}\ \&\text{-r} \qquad \frac{\vdash A, \Delta}{\vdash A \oplus B, \Delta}\ \oplus\text{-r1} \qquad \frac{\vdash B, \Delta}{\vdash A \oplus B, \Delta}\ \oplus\text{-r2}$$

Quantifiers

$$\frac{\vdash A, \Delta}{\vdash \forall x A, \Delta}\ \forall\text{-r, } x \text{ fresh} \qquad \frac{\vdash (t/x)A, \Delta}{\vdash \exists x A, \Delta}\ \exists\text{-r, } t \text{ any term}$$

Exponentials

$$\frac{\vdash ?A, ?A, \Delta}{\vdash ?A, \Delta}\ \text{contraction} \qquad \frac{\vdash \Delta, A}{\vdash \Delta, ?A}\ \text{dereliction}$$

$$\frac{\vdash \Delta}{\vdash \Delta, ?A}\ \text{weakening} \qquad \frac{\vdash ?\Delta, A}{\vdash ?\Delta, !A}\ \text{promotion}$$

Adding rewrite rules

- rewrite rules are of the two following forms:
  - on terms

$$\begin{array}{rcl} x * 0 & \longrightarrow & 0 \\ x + 0 & \longrightarrow & 0 \end{array}$$

  - on propositions

$$P(0) \to \forall x P(x)$$

- a set of rewrite rules $\mathcal{R}$ defines a congruence $\equiv$

Adding rewrite rules

- rewrite rules are of the two following forms:
  - on terms

$$\begin{array}{rcl} x * 0 & \to & 0 \\ x + 0 & \to & 0 \end{array}$$

  - on propositions

$$P(0) \to \forall x P(x)$$

- a set of rewrite rules $\mathcal{R}$ defines a congruence $\equiv$
- it is taken into account in the rules (side condition):

$$\text{axiom}\ \frac{}{\vdash A^{\perp}, A} \quad \text{turns into} \quad \frac{}{\vdash B, A}\ \text{axiom},\ B \equiv A^{\perp}$$

Adding rewrite rules

- rewrite rules are of the two following forms:
  - on terms

$$\begin{array}{rcl} x * 0 & \to & 0 \\ x + 0 & \to & 0 \end{array}$$

  - on propositions

$$P(0) \to \forall x P(x)$$

- a set of rewrite rules $\mathcal{R}$ defines a congruence $\equiv$
- it is taken into account in the rules (side condition):

$$\text{axiom}\ \frac{}{\vdash A^{\perp}, A} \quad \text{turns into} \quad \frac{}{\vdash B, A}\ \text{axiom}, B \equiv A^{\perp}$$

- many interesting examples, e.g. Church's simple types theory: first-order encoding of higher-order LL by rewrite rules.

Rules of Linear Logic modulo

Identities

$$\frac{}{\vdash A, B}\ \text{init},\ A \equiv B^\perp \qquad \frac{\vdash A, \Gamma \qquad \vdash B, \Delta}{\vdash \Gamma, \Delta}\ \text{cut},\ A \equiv B^\perp$$

Multiplicatives

$$\frac{}{\vdash A}\ \mathbf{1}\text{-r},\ A \equiv \mathbf{1} \qquad \frac{\vdash \Delta}{\vdash A, \Delta}\ \perp\text{-r},\ A \equiv \perp$$

$$\frac{\vdash A, \Gamma \qquad \vdash B, \Delta}{\vdash C, \Gamma, \Delta}\ \otimes\text{-r},\ C \equiv A \otimes B \qquad \frac{\vdash A, B, \Delta}{\vdash C, \Delta}\ \parr\text{-r},\ C \equiv A \parr B$$

Additives

$$\frac{}{\vdash A, \Gamma}\ \top\text{-r},\ A \equiv \top$$

no $\mathbf{0}$-r

$$\frac{\vdash A, \Delta \qquad \vdash B, \Delta}{\vdash C, \Delta}\ \&\text{-r},\ C \equiv A \,\&\, B \qquad \frac{\vdash A, \Delta}{\vdash C, \Delta}\ \oplus\text{-r1},\ C \equiv A \oplus B \qquad \frac{\vdash B, \Delta}{\vdash C, \Delta}\ \oplus\text{-r2},\ C$$

Quantifiers

$$\frac{\vdash A, \Delta}{\vdash C, \Delta}\ \forall\text{-r},\ C \equiv \forall x A,\ x \text{ fresh} \qquad \frac{\vdash (t/x)A, \Delta}{\vdash C, \Delta}\ \exists\text{-r},\ C \equiv \exists x A,\ t \text{ term}$$

Exponentials

$$\frac{\vdash A, B, \Delta}{\vdash C, \Delta}\ \text{contr.},\ A \equiv B \equiv C \equiv ?D \qquad \frac{\vdash \Delta, A}{\vdash \Delta, B}\ \text{derel.},\ B \equiv ?A$$

$$\frac{\vdash \Delta}{\vdash \Delta, B}\ \text{weak.},\ B \equiv ?A \qquad \frac{\vdash \Delta, A}{\vdash \Delta, B}\ \text{promo.},\ B \equiv !A,\ \Delta \equiv ?\Gamma$$

A toy example

- Rewrite system:

$$
\begin{array}{rcl}
P(0) & \rightarrow & A \\
P(1) & \rightarrow & B
\end{array}
$$

- Proof of $\vdash ?\exists x(P(x)^{\perp}), A \otimes B$ (two sided: $!\forall x P(x) \vdash A \otimes B$)

A toy example

- Rewrite system:

$$\begin{array}{rcl} P(0) & \to & A \\ P(1) & \to & B \end{array}$$

- Proof of $\vdash ?\exists x(P(x)^{\perp}), A \otimes B$ (two sided: $!\forall x P(x) \vdash A \otimes B$)
-

$$\dfrac{\dfrac{\text{dereliction}\ \dfrac{\exists\text{-r}\ \dfrac{\overline{\vdash P(0)^{\perp}, A}}{\vdash \exists x(P(x)^{\perp}), A}}{\vdash ?\exists x(P(x)^{\perp}), A} \qquad \dfrac{\dfrac{\overline{\vdash P(1)^{\perp}, A}}{\vdash \exists x(P(x)^{\perp}), B}\ \exists\text{-r}}{\vdash ?\exists x(P(x)^{\perp}), B}\ \text{dereliction}}{\vdash ?\exists x(P(x)^{\perp}), ?\exists x(P(x)^{\perp}), A \otimes B}\ \otimes\text{-r}}{\vdash ?\exists x(P(x)^{\perp}), A \otimes B}\ \text{contraction}$$

Studying cut elimination

- theoretic power of DM: in some cases, no cut elimination.

Studying cut elimination

- theoretic power of DM: in some cases, no cut elimination.
- counterexample

$$A \to (!A) \multimap A$$

  can type every (untyped) λ-term (especially $\Omega = \lambda x.(xx)$)

Studying cut elimination

- theoretic power of DM: in some cases, no cut elimination.
- counterexample

$$A \to (!A) \multimap A$$

  can type every (untyped) λ-term (especially $\Omega = \lambda x.(xx)$)
- worse: this rule admits cuts but no normalization
- we give semantic ways to prove cut elimination (admissibility)

Phase spaces

- a topological interpretation
- idea behind: sets of contexts (i.e. $A^* = \{\Gamma \mid \Gamma \vdash A \text{ provable } \}$)
- like Boolean algebras, Heyting algebras (pseudo-complement: think about open sets !). “Natural” interpretation:

$$(A \wedge B)^* = A^* \cap B^*$$

intended meaning:

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

Phase spaces

- a topological interpretation
- idea behind: sets of contexts (i.e. $A^* = \{\Gamma \mid \Gamma \vdash A$ provable $\}$)
- like Boolean algebras, Heyting algebras (pseudo-complement: think about open sets !). "Natural" interpretation:

$$(A \wedge B)^* = A^* \cap B^*$$

  intended meaning:

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

- in LL: two conjunctions $\otimes$ and $\&$: which one is the intersection ?

Phase spaces

- a topological interpretation
- idea behind: sets of contexts (i.e. $A^* = \{\Gamma \mid \Gamma \vdash A \text{ provable }\}$)
- like Boolean algebras, Heyting algebras (pseudo-complement: think about open sets !). "Natural" interpretation:

$$(A \wedge B)^* = A^* \cap B^*$$

  intended meaning:

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

- in LL: two conjunctions $\otimes$ and $\&$: which one is the intersection ?
- Hint: look at the previous rule. But what for the other ?

Phase spaces

- $(M, .)$: a commutative monoid, 1: unit, $\perp$: a fixed subset of M (intended meaning: contexts with concatenation, empty context and some fixed subset – the pole)

Phase spaces

- $(M, .)$: a commutative monoid, 1: unit, $\perp$: a fixed subset of M (intended meaning: contexts with concatenation, empty context and some fixed subset – the pole)
- plus special treatment for exponentials (modalities): set J ...
- basic construct: orthogonal of subsets $\alpha \subseteq M$

$$\alpha^{\perp} = \{a \mid \alpha.a \subseteq \perp\}$$

- consider only sets closed by bi-orthogonality ($\alpha = \alpha^{\perp\perp}$): facts. (involutive closure operator: $(\_)^{\perp\perp}$)

Phase spaces

- $(M, .)$: a commutative monoid, 1: unit, $\perp$: a fixed subset of M (intended meaning: contexts with concatenation, empty context and some fixed subset – the pole)
- plus special treatment for exponentials (modalities): set J ...
- basic construct: orthogonal of subsets $\alpha \subseteq M$

$$\alpha^\perp = \{a \mid \alpha.a \subseteq \perp\}$$

- consider only sets closed by bi-orthogonality ($\alpha = \alpha^{\perp\perp}$): facts. (involutive closure operator: $(\_)^{\perp\perp}$)
- semantic operators
  - $\top = M$
  - $\mathbf{0} = \top^\perp = \{a \mid M.a \subseteq \perp\}$
  - $\alpha \,\&\, \beta = \alpha \cap \beta$
  - $\alpha \otimes \beta = (\alpha.\beta)^{\perp\perp}$

Phase models

- defining a model: usual business
  - base interpretation for terms and predicates
  - connectors as operators
  - quantifiers: $\forall$ infinite intersection (on domain), $\exists$ closure of infinite union
- specific condition on models. Rewrite rules valid:

$$A \equiv B \text{ should imply } A^* = B^*$$

Phase models

- defining a model: usual business
  - base interpretation for terms and predicates
  - connectors as operators
  - quantifiers: $\forall$ infinite intersection (on domain), $\exists$ closure of infinite union
- specific condition on models. Rewrite rules valid:

$$A \equiv B \text{ should imply } A^* = B^*$$

- soundness holds (well ... confluence of rewrite rules required)

$$\Gamma \vdash A \text{ implies } \Gamma^* \leq A^* \quad (\text{one sided version: } \Gamma^{*\perp} \subseteq A^*)$$

- completeness also ...

Phase models for cut elimination

- ... but we can do more !

Find a model such that $\Gamma^* \leq A^*$ implies $\vdash_{cf} A, \Delta$

- Okada's work extended to deduction modulo settings

Context phase spaces

- monoid M: set of finite contexts, composition law . : concatenation.
- define the

$$\text{(\textbf{outer value})} \quad [\![A]\!] = \{\Gamma \mid \vdash_{cf} \Gamma, A\}$$

- take $[\![\perp]\!]$ for (the semantical) $\perp$. Exercise: $\{A\}^{\perp} = [\![A]\!]$

Context phase spaces

- monoid M: set of finite contexts, composition law . : concatenation.
- define the

$$(\textbf{outer value}) \quad [\![A]\!] = \{\Gamma \mid \vdash_{cf} \Gamma, A\}$$

- take $[\![\bot]\!]$ for (the semantical) $\bot$. Exercise: $\{A\}^\bot = [\![A]\!]$
- interepret each atomic predicate symbol P by $[\![P]\!]$.
- this defines a phase space. (would also define Heyting or Boolean algebra)

Context phase spaces

- monoid M: set of finite contexts, composition law . : concatenation.
- define the

$$\textbf{(outer value)} \quad [\![A]\!] = \{\Gamma \mid \vdash_{cf} \Gamma, A\}$$

- take $[\![\bot]\!]$ for (the semantical) $\bot$. Exercise: $\{A\}^{\bot} = [\![A]\!]$
- interepret each atomic predicate symbol P by $[\![P]\!]$.
- this defines a phase space. (would also define Heyting or Boolean algebra)
- aim: $\Gamma \in [\![A]\!]$.

semantic cut elimination

- show $\Gamma \in [\![A]\!]$ in a few steps
- Main Lemma: for any A,

$$A^{\perp} \in A^{*} \subseteq [\![A]\!]$$

semantic cut elimination

- show $\Gamma \in [\![A]\!]$ in a few steps
- Main Lemma: for any A,

$$A^\perp \in A^* \subseteq [\![A]\!]$$

- consequence:
  - $\Gamma^* \subseteq [\![\Gamma]\!] = \{\Gamma\}^\perp$
  - $\{\Gamma\}^{\perp\perp} \subseteq \Gamma^{*\perp}$ (negating the previous)
  - $\Gamma \in \{\Gamma\}^{\perp\perp}$ (exercise)
  - $\Gamma^{*\perp} \subseteq A^*$ (soundness)
  - $A^* \subseteq [\![A]\!]$
  - Q.E.D: $\vdash_{cf} \Gamma, A$

semantic cut elimination

- show $\Gamma \in [\![A]\!]$ in a few steps
- Main Lemma: for any A,

$$A^{\perp} \in A^{*} \subseteq [\![A]\!]$$

- consequence:
  - $\Gamma^{*} \subseteq [\![\Gamma]\!] = \{\Gamma\}^{\perp}$
  - $\{\Gamma\}^{\perp\perp} \subseteq \Gamma^{*\perp}$ (negating the previous)
  - $\Gamma \in \{\Gamma\}^{\perp\perp}$ (exercise)
  - $\Gamma^{*\perp} \subseteq A^{*}$ (soundness)
  - $A^{*} \subseteq [\![A]\!]$
  - Q.E.D: $\vdash_{cf} \Gamma, A$
- Stop! Additional constraint: $A^{*} = B^{*}$ when $A \equiv B$
- dependent on $\equiv$
- we do that for two conditions on rewrite rules: order and positivity. Plus a combination of both.

The positivity condition in short

Core ideas

- define proof nets for linear logic modulo
- study the proof normalization algorithms
- define some pseudo-Phase spaces (as Truth values algebras)