Lecture Notes on Linear Logic

15-816: Modal Logic
Frank Pfenning

Lecture 23
April 20, 2010

1 Introduction

In this lecture we will introduce *linear logic* [**?**] in its judgmental formulation [**?**, **?**]. Linear logic is a logic of state, and used to describe system and situations involving changes of state. As such, it seems amenable to a form of Kripke semantics where worlds corresponds to states and logical formulas describe transitions between the states. As we will see, things are not quite as simple, although using the technique of *tethering* from Lecture 17 we can achieve a kind of multiple world semantics.

We will not use this lecture to give an introduction to linear logic from the application point of view. The interested reader is referred to notes in a dedicated course on linear logic (for example, its introduction).

2 Multiplicative Linear Logic

The quintessence of the formalization of linear logic is the repudiation of the usual structural rules of weakening and contraction for hypotheses. Instead of the ordinary hypothetical judgment we therefore have a *linear hypothetical judgment* where hypotheses must be used exactly once in a proof. When they are used, they are thereby consumed and are no longer available in the remainder of the proof. This very small change in our view on hypothetical judgments has dramatic consequences for the nature of the connectives and reasoning. On the other hand, there are many constants. Logical connectives are still explained via their introduction and elimination rules which satisfy local soundness and completeness properties. The notions of verification and uses still work the same way, as do the principles of cut and identity.

We forego here a natural deduction presentation of linear logic and directly give a sequent calculus. Instead of verifying local soundness and completeness, we verify the local properties relating to identity and cut, followed at the end by global proofs of identity and cut. We begin with the so-called *multiplicative fragment*. A linear sequent as the form

$$A_1\ \mathit{left}, \ldots, A_n\ \mathit{left} \longrightarrow C\ \mathit{right}$$

which we abbreviate as

$$\Gamma \longrightarrow C$$

omitting the judgments that can be inferred from position. The linear hypothetical judgment means that every linear hypothesis in Γ must be used exactly once. We therefore read it as: "*With resources* Γ *we can achieve goal* C." We will use this reading to define the logical connectives.

First, initial sequents have the form

$$\frac{}{P \longrightarrow P}\ \mathsf{init}$$

where no additional assumptions are permitted, so that $\Gamma, P \longrightarrow P$ is only an initial sequent if $\Gamma = (\cdot)$ is empty. From this we see that the identity principle must have the form

Identity: $A \longrightarrow A$ for any A.

Similarly, the cut principle has a slightly different form than for intuitionistic (or modal) logic.

Cut: If $\Gamma \longrightarrow A$ and $\Gamma', A \longrightarrow C$ then $\Gamma', \Gamma \longrightarrow C$.

We can read this as follows

If we have resources Γ *and* Γ'*, we can achieve goal* C *by devoting the resources* Γ *to achieve* A *and then use* A *together with* Γ' *to achieve* C.

Recall that in our sequents, order of the hypotheses never matters: we can silently reorder them. This means that in the conclusion of cut, the hypotheses from both premises can appear in any order.

Simultaneous Conjunction. To achieve a goal $A \otimes B$ with the current resources means that we must be able to achieve both A and B simultaneously. That means we must split the available resources, devoting some to achieving A and other to achieving B.

$$\frac{\Gamma_1 \longrightarrow A \quad \Gamma_2 \longrightarrow B}{\Gamma_1, \Gamma_2 \longrightarrow A \otimes B} \otimes R$$

Conversely, if we have resource $A \otimes B$ we can use both A and B.

$$\frac{\Gamma, A, B \longrightarrow C}{\Gamma, A \otimes B \longrightarrow C} \otimes L$$

These two rules are in harmony. For identity, we see that the identity principle for $A \otimes B$ follows from the identity principles for A and B.

$$\dfrac{\dfrac{A \longrightarrow A \quad B \longrightarrow B}{A, B \longrightarrow A \otimes B} \otimes R}{A \otimes B \longrightarrow A \otimes B} \otimes L$$

For the principal case of cut, we see that we can reduce a cut of $A \otimes B$ to cuts of A and B:

$\Gamma_1 \longrightarrow A$ and $\Gamma_2 \longrightarrow B$	Given ($\mathcal{D}_1$ and $\mathcal{D}_2$)
$\Gamma_1, \Gamma_2 \longrightarrow A \otimes B$	By $\otimes R$
$\Gamma', A, B \longrightarrow C$	Given ($\mathcal{E}'$)
$\Gamma', A \otimes B \longrightarrow C$	By $\otimes L$
$\Gamma', \Gamma_1, B \longrightarrow C$	By cut on A, $\mathcal{D}_1$ and $\mathcal{E}'$
$\Gamma', \Gamma_1, \Gamma_2 \longrightarrow C$	By cut on B, $\mathcal{D}_2$ and above

Linear Implication. To achieve goal $A \multimap B$ means to show that we can achieve goal B with resources A (together with any other resources we may have at our disposal already.

$$\frac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \multimap B} \multimap R$$

If we have $A \multimap B$ as a resource, this means that if solve A as a subgoal we can then obtain resource B. This requires us to split our resources, devoting some to achieving A, and some to (finally) achieving C.

$$\frac{\Gamma_1 \longrightarrow A \quad \Gamma_2, B \longrightarrow C}{\Gamma_1, \Gamma_2, A \multimap B \longrightarrow C} \multimap L$$

We show the identity:

$$\dfrac{\dfrac{A \longrightarrow A \quad B \longrightarrow B}{A \multimap B, A \longrightarrow B} \multimap L}{A \multimap B \longrightarrow A \multimap B} \multimap R$$

and leave cut as an exercise.

As a simple example we can show that simultaneous conjunction is commutative (assuming here A and B are atomic, for simplicity):

$$\dfrac{\dfrac{\dfrac{\dfrac{}{B \longrightarrow B}\,\mathsf{init} \quad \dfrac{}{A \longrightarrow A}\,\mathsf{init}}{A, B \longrightarrow B \otimes A} \otimes R}{A \otimes B \longrightarrow B \otimes A} \otimes L}{\longrightarrow A \otimes B \multimap B \otimes A} \multimap R$$

Unit. We also have the unit for multiplicative conjunction, which corresponds to the empty resource. Since all linear hypothesis must be used exactly once, this can only be proved if there are no resources.

$$\dfrac{}{\bullet \longrightarrow \mathbf{1}}\,\mathbf{1}R$$

Consequently, a resource $\mathbf{1}$ is of no help and can be discarded.

$$\dfrac{\Gamma \longrightarrow C}{\Gamma, \mathbf{1} \longrightarrow C}\,\mathbf{1}L$$

Again, we check only identity:

$$\dfrac{\dfrac{}{\cdot \longrightarrow \mathbf{1}}\,\mathbf{1}R}{\mathbf{1} \longrightarrow \mathbf{1}}\,\mathbf{1}L$$

3 A Resource Semantics

In order to give a Kripke-like resource semantics we label all the resources with unique labels representing that resource. In the succedent we record all the resources that may be used, which may be a subset of the resources listed in the antecedent. So a sequent has the form

$$A_1@\alpha_1, \ldots, A_n@\alpha_n \longrightarrow C \mathbin{@} p$$

where p is formed from $\alpha_1, \ldots, \alpha_n$ with a binary resource combination $*$. In addition we have the empty resource label ϵ, which is the unit of $*$. Resource combination is associative and commutative, so we have the laws

$$\begin{array}{rcl} p * \epsilon & = & p \\ \epsilon * q & = & q \\ (p * q) * r & = & p * (q * r) \\ p * q & = & q * p \end{array}$$

We will apply these equations silently, just as we, for example, silently reorder hypotheses.

By labeling resources we recover the property of weakening.

> **Weakening:** If $\Gamma \longrightarrow C \mathbin{@} p$ then $\Gamma, A@\alpha \longrightarrow C \mathbin{@} p$. Here α must be new in order to maintain the invariant on seqents that all antecedents are labeled with distinct resource parameters.

Contraction cannot be quite formulated, since we cannot contract $A@\alpha, A@\beta$ to $A@\alpha * \beta$ because at least for the moment, hypotheses can only be labeled with resource parameters and not combinations of them.

We do, however, have a simple identity:

> **Identity**: $P@\alpha \longrightarrow P \mathbin{@} \alpha$.

From this, the initial sequent follows:

$$\frac{}{\Gamma, P@\alpha \longrightarrow P \mathbin{@} \alpha}\ \mathsf{init}$$

Cut is a bit more complicated, because resource labels in succedents are more general then in antecedents. But we have already seen this in substitution principles with proof terms, so we imitate this solution, substitution resources p for resource parameter α:

> **Cut**: If $\Gamma \longrightarrow A \mathbin{@} p$ and $\Gamma, A@\alpha \longrightarrow C \mathbin{@} \alpha * q$ then $\Gamma \longrightarrow C \mathbin{@} p * q$.

We now revisit each of the connectives so far in turn, deriving the appropriate rules. The goal is to achieve an exact isomorphism between the linear logic inference rules based on hypothetical judgments and the inference rules based on resources. Hidden behind the isomorphism is the equational reasoning in the resource algebra.

Simultaneous Conjunction. The resources available to achieve the goals are split between the two premises. Previously, this was achieved by splitting the context itself. Note that we use Γ here to stand for a context in which all assumptions are labeled with unique resource parameters.

$$\frac{\Gamma \longrightarrow A \mathbin{@} p \quad \Gamma \longrightarrow B \mathbin{@} q}{\Gamma \longrightarrow A \otimes B \mathbin{@} p * q} \otimes R$$

The left rule reveals the close analogy with the tethered semantics for JS4 presented before. In order to apply a left rule to a given assumption $A@\alpha$, the resource α must actually be available, which is recorded in the succedent. Upon application of the rule the resource is no longer available, but new resources may now be available (depending on the connective).

$$\frac{\Gamma, A \otimes B@\alpha, A@\beta, B@\gamma \longrightarrow C \mathbin{@} p * \beta * \gamma}{\Gamma, A \otimes B@\alpha \longrightarrow C \mathbin{@} p * \alpha} \otimes L^{\beta,\gamma}$$

In this rule, α is consumed and new resources β and γ are introduced.

Linear Implication. The intuitions above give us enough information to write out these rules directly, modeling the linear sequent calculus.

$$\frac{\Gamma, A@\alpha \longrightarrow B \mathbin{@} p * \alpha}{\Gamma \longrightarrow A \multimap B \mathbin{@} p} \multimap R^{\alpha}$$

In the elimination rule we see again how a split between the antecedents is represented as a split between the resources.

$$\frac{\Gamma, A \multimap B@\alpha \longrightarrow A \mathbin{@} q \quad \Gamma, A \multimap B@\alpha, B@\beta \longrightarrow C \mathbin{@} p * \beta}{\Gamma, A \multimap B@\alpha \longrightarrow C \mathbin{@} p * q * \alpha} \multimap L^{\beta}$$

By strengthening, we can see that the antecedent $A \multimap B@\alpha$ can not be used in either premise.

Unit. Here, we just have to enforce the emptiness of the resources.

$$\frac{}{\Gamma \longrightarrow \mathbf{1} \mathbin{@} \epsilon} \mathbf{1}R \qquad \frac{\Gamma, \mathbf{1}@\alpha \longrightarrow C \mathbin{@} p}{\Gamma, \mathbf{1}@\alpha \longrightarrow C \mathbin{@} p * \alpha} \mathbf{1}L$$

In the $\mathbf{1}L$ rule we replace α by ϵ and then use its unit property to obtain p.

Exponentials

In linear logic, we add a judgment of validity in order to regain the full expressive power of intuitionistic logic. From the perspective of resources, A *valid* means that the truth of A does not depend on any resources. This in turn means that we can use as many copies of A as we like in a proof, including none. The extended judgment then has the form

$$\Delta; \Gamma \longrightarrow C$$

where the antecedents in Δ are unrestricted and the antecedents in Γ are linear.

We internalize validity as a modality, written $!A$ instead of the usual $\Box A$ of modal logic. We have a right and a left rule, as well as a judgmental rule to relate validity to truth.

$$\frac{\Delta; \bullet \longrightarrow A}{\Delta; \bullet \longrightarrow !A}\ !R \qquad \frac{\Delta, A; \Gamma \longrightarrow C}{\Delta; \Gamma, !A \longrightarrow C}\ !L$$

$$\frac{\Delta, A; \Gamma, A \longrightarrow C}{\Delta, A; \Gamma \longrightarrow C}\ \mathsf{copy}$$

Unlike in ordinary modal logic, in the $!R$ rule, the linear context must already be empty so that no resources are dropped (recall that all linear hypotheses must be used exactly once). Similarly, in the $!L$ rule, the principal formula $!A$ is consumed and no longer available in the premise. In contrast, the copy rule is the same, because valid hypotheses are subject to weakening and contraction.

We now need to revisit all the previous rules, systematically adding unrestricted assumptions everywhere. The resulting system is summarized in Figure 1.

Fortunately, our representation technique for the sequent calculus using explicit resources is already rich enough to handle validity. We just allow assumptions $A@\epsilon$ to indicate A *valid*. Since resource-annotated hypothesis already allow weakening and contraction, no additional structural rules are required. In $!R$, both premise and conclusion may not use any resources, so they are at ϵ. In $!L$, the resource α labeling $!A$ is consumed (that is, replaced by ϵ, which is eliminated by the unit property of '$*$').

$$\frac{\Gamma \longrightarrow A \ @\ \epsilon}{\Gamma \longrightarrow !A \ @\ \epsilon}\ !R \qquad \frac{\Gamma, !A@\alpha, A@\epsilon \Longrightarrow C \ @\ p}{\Gamma, !A@\alpha \Longrightarrow C \ @\ p * \alpha}\ !L$$

$$\frac{}{\Delta; P \longrightarrow P}\ \mathsf{init}$$

$$\frac{\Delta; \Gamma_1 \longrightarrow A \quad \Delta; \Gamma_2 \longrightarrow B}{\Delta; \Gamma_1, \Gamma_2 \longrightarrow A \otimes B}\ \otimes R \qquad \frac{\Delta; \Gamma, A, B \longrightarrow C}{\Delta; \Gamma, A \otimes B \longrightarrow C}\ \otimes L$$

$$\frac{}{\Delta; \bullet \longrightarrow \mathbf{1}}\ \mathbf{1}R \qquad \frac{\Delta; \Gamma \longrightarrow C}{\Delta; \Gamma, \mathbf{1} \longrightarrow C}\ \mathbf{1}L$$

$$\frac{\Delta; \bullet \longrightarrow A}{\Delta; \bullet \longrightarrow\ !A}\ !R \qquad \frac{\Delta, A; \Gamma \longrightarrow C}{\Delta; \Gamma, !A \longrightarrow C}\ !L$$

$$\frac{\Delta, A; \Gamma, A \longrightarrow C}{\Delta, A; \Gamma \longrightarrow C}\ \mathsf{copy}$$

Figure 1: Sequent Calculus for Multiplicative Exponential Linear Logic

If we want to maintain a bijection between sequent proofs in the two systems, we also need a special judgmental rule which creates a fresh resource α and $A@\alpha$ from $A@\epsilon$. This is justified by the resource semantics, but nevertheless somewhat unexpected. A different solution will be presented in the next lectures.

$$\frac{\Gamma, A@\epsilon, A@\alpha \longrightarrow C \ @\ p * \alpha}{\Gamma, A@\epsilon \longrightarrow C \ @\ p}\ \mathsf{copy}^{\alpha}$$

The resulting system is summarized in Figure 2.

An interesting aspect of this system is that we did not need to generalize the available judgments when we added the exponentials; the empty resource and the hypothetical judgment was sufficient. We do, however, need a new form of cut because the previous version allowed only to cut a hypothesis $A@\alpha$ for a resource parameter α.

Cut!: If $\Gamma \longrightarrow A \ @\ \epsilon$ and $\Gamma, A@\epsilon \longrightarrow C \ @\ p$ then $\Gamma \longrightarrow C \ @\ p$.

4 Correspondence

It is now easy to establish that the resource calculus is in bijective correspondence with the linear sequent calculus. Moroever, it satisfies the ex-

$$\frac{}{\Gamma, P@\alpha \longrightarrow P\ @\ \alpha}\ \mathsf{init}$$

$$\frac{\Gamma \longrightarrow A\ @\ p \quad \Gamma \longrightarrow B\ @\ q}{\Gamma \longrightarrow A \otimes B\ @\ p * q}\ \otimes R$$

$$\frac{\Gamma, A \otimes B@\alpha, A@\beta, B@\gamma \longrightarrow @\ p * \beta * \gamma}{\Gamma, A \otimes B@\alpha \longrightarrow C\ @\ p * \alpha}\ \otimes L^{\beta,\gamma}$$

$$\frac{\Gamma, A@\alpha \longrightarrow B\ @\ p * \alpha}{\Gamma \longrightarrow A \multimap B\ @\ p}\ \multimap R^{\alpha}$$

$$\frac{\Gamma, A \multimap B@\alpha \longrightarrow A\ @\ q \quad \Gamma, A \multimap B@\alpha, B@\beta \longrightarrow C\ @\ p * \beta}{\Gamma, A \multimap B@\alpha \longrightarrow C\ @\ p * q * \alpha}\ \multimap L^{\beta}$$

$$\frac{}{\Gamma \longrightarrow \mathbf{1}\ @\ \epsilon}\ \mathbf{1}R \qquad \frac{\Gamma, \mathbf{1}@\alpha \longrightarrow C\ @\ p}{\Gamma, \mathbf{1}@\alpha \longrightarrow C\ @\ p * \alpha}\ \mathbf{1}L$$

$$\frac{\Gamma \longrightarrow A\ @\ \epsilon}{\Gamma \longrightarrow !A\ @\ \epsilon}\ !R \qquad \frac{\Gamma, !A@\alpha, A@\epsilon \Longrightarrow C\ @\ p}{\Gamma, !A@\alpha \Longrightarrow C\ @\ p * \alpha}\ !L$$

$$\frac{\Gamma, A@\epsilon, A@\alpha \longrightarrow C\ @\ p * \alpha}{\Gamma, A@\epsilon \longrightarrow C\ @\ p}\ \mathsf{copy}^{\alpha}$$

Figure 2: Resource Semantics for Multiplicative Exponential Linear Logic

pected properties of cut and identity. Key is the crucial strengthening property.

For the remainder of this lecture we assume that a resource context has hypotheses of the form $A@\epsilon$ and $A@\alpha$, where all resource parameters α are distinct, and the succedent has the form $C\ @\ p$, where p is a product of distinct resource parameters. We write $\alpha \notin p$ if α does not occur in p. The equational theory for resources remains associativity and commutatitivity for '$*$' with unit ϵ.

Theorem 1 (Strengthening for Resource Semantics) *If* $\Gamma, A@\alpha \longrightarrow C\ @\ p$ *and* $\alpha \notin p$ *then* $\Gamma \longrightarrow C\ @\ p$ *with the same proof.*

Proof: By induction on the structure of the given proof. □

Theorem 2 (Identity) $A@\alpha \longrightarrow A\ @\ \alpha$.

Proof: By induction on the structure of A. □

Theorem 3 (Cut)

(i) *If* $\Gamma \longrightarrow A\ @\ q$ *and* $\Gamma, A@\alpha \longrightarrow C\ @\ p * \alpha$ *then* $\Gamma \longrightarrow C\ @\ p * q$.

(ii) *If* $\Gamma \longrightarrow A\ @\ \epsilon$ *and* $\Gamma, A@\epsilon \longrightarrow C\ @\ p$ *then* $\Gamma \longrightarrow C\ @\ p$.

Proof: By nested induction, first on the cut formula A, then on the form of cut where $(i) < (ii)$, then on the structure of the proofs in the two premises (one must become smaller while the other remains the same). □

In order to formulate a correspondence theorem, we need to express relationships between assumptions. We write $(A_1, \ldots, A_n)@\epsilon = A_1@\epsilon, \ldots, A_n@\epsilon$ and $(A_1, \ldots, A_n)@\vec{\alpha} = A_1@\alpha_1, \ldots, A_n@\alpha_n$. Furthermore, we need to construct a pair of contexts $\Delta; \Gamma$ from given a resource context. For ease of definition, we do not require a separation of zones but write Ψ for a mixed context with assumptions A *valid* and A *left* (expressing a truth antecedent which is linear).

$$\begin{array}{lcl} (\cdot)|_\epsilon & = & (\cdot) \\ (\Gamma, \Gamma')|_{p*q} & = & \Gamma|_p, \Gamma'|_q \\ (A@\alpha)|_\alpha & = & A\ \mathit{left} \\ (A@\alpha)|_\epsilon & = & (\cdot) \\ (A@\epsilon)|_\epsilon & = & A\ \mathit{valid} \end{array}$$

Because of the equational theory, this definition has some nondeterminism. Under the general assumptions of this section, $\Gamma|_p$ will be defined and unique.

Theorem 4 (Correspondence)

(i) *If* $\Delta; \Gamma \longrightarrow C$ *then* $\Delta@\epsilon, \Gamma@\vec{\alpha} \longrightarrow C \mathbin{@} \alpha_1 * \cdots * \alpha_n$.

(ii) *If* $\Gamma \longrightarrow C \mathbin{@} p$ *then* $\Gamma|_p \longrightarrow C$.

Moreover, the correspondence between linear and resource proofs is a bijection.

Proof: By straightforward inductions, exploiting strengthening. □

Exercises