Lecture Notes on
Proof Search in Authorization Logic

15-316: Software Foundations of Security & Privacy
Frank Pfenning

Lecture 16
October 31, 2024

1 Introduction

In Boolean logic, the sequent calculus was a good basis for proof search (at least on the small scale) because all rules were sound and invertible. This is no longer the case for intuitionistic logic, whether extended with affirmation or not. In fact, Boolean propositional logic is just about the only logic where we can arrange for all rules to be invertible. Our task then is to find out which rules *are* invertible and which are not. This gives rise to a classification of logical connectives based on the invertibility of their right and left rules. This can be done generally for logics that admit a sequent calculus formulation. It was first discovered for *linear logic* [Girard, 1987] by Andreoli [1992] but since been applied to many other ones, including those with a lax modality [Liang and Miller, 2009, Watkins et al., 2002].

Our first order of business, then, is to identify invertibility properties, followed by proof strategies based on them.

2 Inversion

Since it is a pervasively used connective, we start with implication.

$$\frac{\Gamma, P \vdash Q}{\Gamma \vdash P \to Q}\ {\to}R \qquad\qquad \frac{\Gamma \vdash P \quad \Gamma, Q \vdash \delta}{\Gamma, P \to Q \vdash \delta}\ {\to}L$$

invertible not invertible

It turns out the right rule is invertible, while the left rule is not. To see that the left rule is *not* invertible, we only need a counterexample. Consider

$$p \to q, q \to r \vdash p \to r$$

Trying to apply the left rule for implication to the first antecedent results in a sequent that cannot be derived.

$$\dfrac{\dfrac{\mathsf{XXX}\quad \cdot \vdash q \qquad \mathsf{XXX}\quad r \vdash p}{q \to r \vdash p}\,{\to}L \qquad \vdots}{p \to q, q \to r \vdash p \to r}\,{\to}L \qquad q, q \to r \vdash p \to r$$

We suspect that the right rule for implication is invertible, but how do we prove it? Previously, we used a *semantic argument*, using the validity of a sequent. Here, such a direct argument is not available—we would have to introduce a semantics which is not straightforward. But there is also a syntactic technique, using the *admissibility of cut*. So we make a brief detour to introduce it.

When presented as a rule

$$\dfrac{\Gamma \vdash P \quad \Gamma, P \vdash \delta}{\Gamma \vdash \delta}\ \mathsf{cut}$$

its meaning is clear: if we can prove P we are allowed to assume it in further reasoning. For bottom-up proof search it is somewhat problematic because we have to determine a useful P, which could be *any* formula. So we use it only under controlled circumstances.

Gentzen [1935] showed that the rule of cut is redundant for both classical (Boolean) and intuitionistic logic. What do we mean by "redundant"? More technically, we call a rule *admissible* if it is both sound and whenever the premises can be derived, so can the conclusion *without using the rule*. We write an admissible rule with a dashed line:

$$\dfrac{\Gamma \vdash P \quad \Gamma, P \vdash \delta}{\Gamma \vdash \delta}\ \mathsf{cut}$$

We won't go into detail how to show that cut is admissible. This is covered in many articles (including Gentzen's original one) and also in *15-317 Constructive Logic* in somewhat more modern notation (see Lecture 8).

Here we concentrate on how to use the admissibility of cut to obtain other properties. First, it is convenient to have an alternative version that is also admissible and more suitable to top-down reasoning.

$$\dfrac{\Gamma_1 \vdash P \quad \Gamma_2, P \vdash \delta}{\Gamma_1, \Gamma_2 \vdash \delta}\ \mathsf{cut}'$$

We want to prove that $\to R$ is invertible. That is, we want to show that

$$\dfrac{\Gamma \vdash P \to Q}{\Gamma, P \vdash Q}\ {\to}R^{-1}$$

is admissible. Step-by-step: first, we have a succedent $P \to Q$ in the premise, so we should try to cut it with a sequent with antecedent $P \to Q$ with some Γ' and δ.

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \vdash P \to Q \quad \Gamma', P \to Q \vdash \delta\end{array}}{\Gamma, P \vdash Q}\ \mathsf{cut}'$$

What could we choose for Γ' and δ? It is pretty obvious from the conclusion: $\Gamma' = P$ and $\delta = Q$. We can then complete the derivation of the second premise.

$$\dfrac{\Gamma \vdash P \to Q \qquad \dfrac{\dfrac{}{P \vdash P}\ \mathsf{id} \quad \dfrac{}{Q \vdash Q}\ \mathsf{id}}{P, P \to Q \vdash Q}\ {\to}L}{\Gamma, P \vdash Q}\ \mathsf{cut}'$$

We see in the second premise everything is proved, so this derivation shows that ${\to}R^{-1}$ is admissible.

We can prove other rules invertible as well, with clever uses of cut′. On our fragment (excluding affirmation for now), the invertible rules are $\wedge R$, $\wedge L$, $\vee L$, $\forall R$. The noninvertible rules are ${\to}L$, $\vee R_1$, $\vee R_2$, and $\forall L$.

A first simple strategy emerges: apply all the invertible rules in some arbitrary, unspecified order until we reach a sequent where either identity applies, or we have to make a choice between noninvertible rules. This choice typically then requires backtracking, in case we make a wrong choice.

We can express such a strategy with three judgment forms, two that force only invertible rules to be used on the left or right, and one that requires a choice. Since it is not our ultimate destination, we elide this here and refer the interest reader to Lecture 15 of the course on constructive logic.

3 Inversion for Affirmation

An empirical observation is that if the right rule for a connective is invertible then the left rule is not and vice versa. This is apparently violated by conjunction which is invertible on both sides. This is because there are actually two forms of conjunction hiding under the symbol "$\wedge$" that are indistinguishable with respect to provability.

We call connectives whose right rule is invertible *negative connectives* and the ones whole left rule is invertible are *positive connectives*. The inversion phase of proof search then applies negative right rules and positive left rules.

But what about affirmation? There is something rather strange going on because in the right rule we go from $(A\ \mathbf{says}\ P)\ \mathsf{true}$ to $A\ \mathbf{aff}\ P$ and in the left rule we jump directly from $A\ \mathbf{says}\ P$ to P. It turns out that the affirmation modality

signifies a change in polarity. One way to state that is that A **says** P is negative, but the judgment underneath, A **aff** P is positive. That means, the right rule is invertible, but the rule of affirmation is not.

$$\frac{\Gamma \vdash A \text{ aff } P}{\Gamma \vdash (A \text{ says } P) \text{ true}}\ \text{says}R \qquad \frac{\Gamma \vdash P \text{ true}}{\Gamma \vdash A \text{ aff } P}\ \text{aff}$$

invertible not invertible

As for the left rules, because A **says** P is negative, it's left rules is not invertible. However, if the succedent has the form A **aff** Q we can always apply the rule since P is a stronger assumption than A **says** P. So we put "invertible" in quotation: we can apply the rule when possible, but we cannot always apply it when A **says** P is an antecedent.

$$\frac{\Gamma, P \vdash A \text{ aff } Q}{\Gamma, A \text{ says } P \vdash A \text{ aff } Q}\ \text{says}L$$

"invertible"

Now we also see why A **aff** P does not appear as a judgment among the antecedents: it is positive, and therefore the corresponding rule can be applied immediately and the stepping stone be omitted.

$$\frac{\dfrac{\Gamma, P \vdash A \text{ aff } Q}{\Gamma, \text{“}A \text{ aff } P\text{”} \vdash A \text{ aff } Q}}{\Gamma, A \text{ says } P \vdash A \text{ aff } Q}\ \text{says}L$$

4 Focusing

If we look at the example from the last lecture we see that the only invertible step is the right rule for **says**, followed by stripping the "$admin$ **says** " prefix from (1), (2), and (3) using **says**L.

$(1) : admin$ **says** $(\forall A.\, \forall R.\, \mathsf{owns}(A, R) \rightarrow \mathsf{mayOpen}(A, R))$,
$(2) : admin$ **says** $(\forall A.\, \forall B.\, \forall R.\, \mathsf{owns}(A, R) \wedge fp$ **says** $\mathsf{studentOf}(B, A) \rightarrow \mathsf{mayOpen}(B, R))$,

$(3) : admin$ **says** $\mathsf{owns}(fp, ghc6017)$,
$(4) : fp$ **says** $\mathsf{studentOf}(hemant, fp)$

$\vdash$

$admin$ **says** $\mathsf{mayOpen}(hemant, ghc6017)$

The resulting sequent below has no invertible rule we can blindly apply.

$(1)' : \forall A.\, \forall R.\, \mathsf{owns}(A, R) \to \mathsf{mayOpen}(A, R)$,
$(2)' : \forall A.\, \forall B.\, \forall R.\, \mathsf{owns}(A, R) \wedge \mathit{fp}\ \mathbf{says}\ \mathsf{studentOf}(B, A) \to \mathsf{mayOpen}(B, R)$,
$(3)' : \mathsf{owns}(\mathit{fp}, \mathit{ghc6017})$,
$(4) : \mathit{fp}\ \mathbf{says}\ \mathsf{studentOf}(\mathit{hemant}, \mathit{fp})$
$\vdash$
$\mathit{admin}\ \mathbf{aff}\ \mathsf{mayOpen}(\mathit{hemant}, \mathit{ghc6017})$

For example, we could instantiate the quantifier $\forall A$ in $(1)'$. But still, everything remains negative and we could instantiate either the $\forall R$ we have uncovered or the $\forall A$ quantifier in (2). We see that at every step we have to choose between a number of alternatives. This can lead to a lot of backtracking if the choices are incorrect.

Focusing [Andreoli, 1992] is the idea that we can pick a negative antecedent or a positive succedent and continue to apply noninvertible rules to this particular formula until we reach either an atomic formula or the polarity switches. For example, if we guess $(2)'$ we would apply $\forall L$ three times, followed by $\to L$. Let's treat conjunction as positive, which we continue with that as well and succeed when we find the needed assumptions.[1] All that reasoning adds $\mathsf{mayOpen}(\mathit{hemant}, \mathit{ghc6017})$ to the assumptions and we have to make another choice. At this point we want to choose the rule of affirmation followed by the identity to complete the proof.

We don't write out the sequent calculus for focusing in its most general form, but you may refer to Lecture 17 of the constructive logic course notes for details. We write $\Gamma, [P] \vdash \delta$ for a formula P in left focus and $\Gamma \vdash [Q]$ for a formula in right focus. In this kind of sequent just one formula can be in focus, and rules can be applied only to the formula in focus. The rules with no focus are the invertible rules.

This gives us the following rules. We work with following polarities below. Except for atoms and conjunction (which we choose to be positive), they are determined by the inversion properties of the connectives.

$$\begin{array}{lllll} \text{Negative} & P^-, Q^- & ::= & P \to Q \mid \forall x.\, P(x) \mid A\ \mathbf{says}\ P \\ \text{Positive} & P^+, Q^+ & ::= & p \mid P \wedge Q \mid P \vee Q \end{array}$$

First the rules to *initiate* a phase of focusing.

$$\frac{\Gamma \vdash [Q^+]}{\Gamma \vdash Q^+}\ \mathbf{focus}R \qquad \frac{P^- \in \Gamma \quad \Gamma, [P^-] \vdash \delta}{\Gamma \vdash \delta}\ \mathbf{focus}L$$

In the left rule we focus on a *copy* of P^- because we may need this formula again. In the examples we sometimes drop the extra copy if we anticipate (or know) it will not be needed again.

[1] Actually, not quite. The affirmation "*fp* **says**" forces us to stop and make another explicit choice.

The rule for affirmation is an additional transition rule. Next, the logical rules. For brevity, we mostly omit "true" in the succedent if it is just a formula. The judgment $\Gamma \vdash \delta$, $\Gamma, [P] \vdash \delta$ and $\Gamma \vdash [Q]$ are mutually exclusive, that is, there may be no focused formula in Γ or δ.

$$\frac{}{\Gamma, p \vdash [p]}\ \mathsf{id}$$

$$\frac{\Gamma, P \vdash Q}{\Gamma \vdash P \to Q}\ {\to}R \qquad \frac{\Gamma \vdash [P] \quad \Gamma, [Q] \vdash \delta}{\Gamma, [P \to Q] \vdash \delta}\ {\to}L$$

$$\frac{\Gamma \vdash [P] \quad \Gamma \vdash [Q]}{\Gamma \vdash [P \wedge Q]}\ {\wedge}R \qquad \frac{\Gamma, P, Q \vdash \delta}{\Gamma, P \wedge Q \vdash \delta}\ {\wedge}L$$

$$\frac{\Gamma \vdash P(y) \quad y \notin \Gamma, P(x)}{\Gamma \vdash \forall x.\, P(x)}\ {\forall}R^y \qquad \frac{\Gamma, [P(c)] \vdash \delta}{\Gamma, [\forall x.\, P(x)] \vdash \delta}\ {\forall}L$$

$$\frac{\Gamma \vdash [P]}{\Gamma \vdash [P \vee Q]}\ {\vee}R_1 \quad \frac{\Gamma \vdash [Q]}{\Gamma \vdash [P \vee Q]}\ {\vee}R_2 \qquad \frac{\Gamma, P \vdash \delta \quad \Gamma, Q \vdash \delta}{\Gamma, P \vee Q \vdash \delta}\ {\vee}L$$

Next, the rules to complete a focusing phase (still postponing affirmations). We say that we *blur the focus*.

$$\frac{\Gamma, P^+ \vdash \delta}{\Gamma, [P^+] \vdash \delta}\ \mathsf{blur}L \qquad \frac{\Gamma \vdash Q^-}{\Gamma \vdash [Q^-]}\ \mathsf{blur}R$$

Finally, the rules for affirmation. They incorporate some phase transitions because of the polarity shift intrinsic to the modality.

$$\frac{\Gamma \vdash A\ \mathbf{aff}\ P}{\Gamma \vdash (A\ \mathbf{says}\ P)\ \mathsf{true}}\ \mathbf{says}R \qquad \frac{\Gamma, P \vdash A\ \mathbf{aff}\ Q}{\Gamma, [A\ \mathbf{says}\ P] \vdash A\ \mathbf{aff}\ Q}\ \mathbf{says}L$$

$$\frac{\Gamma \vdash [P]\ \mathsf{true}}{\Gamma \vdash A\ \mathbf{aff}\ P}\ \mathbf{aff}$$

Our motivating example is too lengthy to write out formally with these rules for focusing, but we can try a small example and see how focusing reduces nondeterminism. Consider

$$p \to q, p \to (q \to r) \vdash p \to r$$

After the obligatory right inversion, we arrive at

$$p, p \to q, p \to (q \to r) \vdash r$$

In this situation, we could in principle try to focus on $p \to q$, on $p \to (q \to r)$ or r. Let's try right focus first. We immediately fail because r is not among the antecedents.

$$\dfrac{\overset{\mathsf{XXX}}{p, p \to q, p \to (q \to r) \vdash [r]}}{p, p \to q, p \to (q \to r) \vdash r}\ \mathbf{focus}R$$

Next we try to focus on $p \to (q \to r)$.

$$\dfrac{\dfrac{}{p, p \to q \vdash [p]}\ \mathsf{id} \quad \dfrac{\overset{\mathsf{XXX}}{p, p \to q \vdash [q]} \quad \overset{\vdots}{p, p \to q, [r] \vdash r}}{p, p \to q, [q \to r] \vdash r}\ {\to}L}{\dfrac{p, p \to q, [p \to (q \to r)] \vdash r}{p, p \to q, p \to (q \to r) \vdash r}\ \mathbf{focus}L}\ {\to}L$$

Note that after we decided which antecedent to focus on, everything was determined. We fail, because q is not among the antecedents.

We cannot focus on p on the left because it is positive, but we can try one final option, namely to focus on $p \to q$.

$$\dfrac{\dfrac{}{p, p \to (q \to r) \vdash [p]}\ \mathsf{id} \quad \dfrac{\overset{\vdots}{p, q, p \to (q \to r) \vdash r}}{p, [q], p \to (q \to r) \vdash r}\ \mathbf{blur}L}{\dfrac{p, [p \to q], p \to (q \to r) \vdash r}{p, p \to q, p \to (q \to r) \vdash r}\ \mathbf{focus}L}\ {\to}L$$

Now it is possible to focus on $p \to (q \to r)$ because both p and q are among the antecedents. This will add r to the antecedents and we can finally successfully focus on the succedent.

Remarkably, with focusing there is just a single proof (assuming we don't copy the formula in focus).

Using inversion and focusing is sound and complete with respect to the sequent calculus. Soundness is important

Theorem 1 (Soundness and Completeness of Inversion and Focusing) *$\Gamma \vdash \delta$ in the sequent calculus if and only if $\Gamma \vdash \delta$ in the calculus with inversion and focusing.*

Proof: Soundness is straightforward, since we only restrict the application of certain rules.

The proof of completeness is quite complex, and not just because of affirmations. See Liang and Miller [2009] for a blueprint that can be adapted to this authorization logic. □

In the architecture of proof-carrying authorization we have to contend with the fact that more complex policies engender more difficult theorem proving problems. In the next lecture we will identify a fragment of authorization logic that represents a reasonable compromise between expressiveness and difficulty of proving. It is inspired by Horn clauses, but goes beyond it due the presence of affirmations.

References

Jean-Marc Andreoli. Logic programming with focusing proofs in linear logic. *Journal of Logic and Computation*, 2(3):197–347, 1992.

Gerhard Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1935. English translation in M. E. Szabo, editor, *The Collected Papers of Gerhard Gentzen*, pages 68–131, North-Holland, 1969.

Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.

Chuck Liang and Dale Miller. Focusing and polarization in linear, intuitionistic, and classical logics. *Theoretical Computer Science*, 410(46):4747–4768, November 2009.

Kevin Watkins, Iliano Cervesato, Frank Pfenning, and David Walker. A concurrent logical framework I: Judgments and properties. Technical Report CMU-CS-02-101, Department of Computer Science, Carnegie Mellon University, 2002. Revised May 2003.