Constructive Logic (15-317), Fall 2015
Recitation 8: Invertibility, proof search, and being a computer (10/21/2015)
Vincent Huang (`vincenth@andrew`), Anna Gommerstadt (`hgommers@cs`), Michael Coblenz (`mcoblenz@cs`)

1 Invertibility

What does it mean to say a rule is *invertible*? It's a nice and simple concept — it simply means that the premises of the rule hold *if and only if* the conclusion of the rule holds. So when you look at the rule, you know that if one of the thingies in it is true, all of the thingies must be true.

Why do we like invertible rules? You've probably developed some intuition by this point in the course about how to go about proving things. What rules do you generally apply without worry? Probably not $\vee I$... you like nice rules like $\wedge I$ and $\supset I$. But this corresponds to liking to apply invertible rules first! In a sense, we lose no information by applying an invertible rule, so it always makes sense to apply them eagerly.

Spades (is inferior to bridge)

Consider the connective $\spadesuit$, with the following natural deduction-style introduction/elimination rules:

$$\frac{\begin{array}{c}\overline{A\ true}^{\,u}\\ \vdots\\ B\ true\end{array} \qquad \begin{array}{c}\overline{A\ true}^{\,u}\\ \vdots\\ C\ true\end{array}}{\spadesuit(A,B,C)\ true}\ \spadesuit I \qquad \frac{\spadesuit(A,B,C)\ true \qquad A\ true}{B\ true}\ \spadesuit E_1 \qquad \frac{\spadesuit(A,B,C)\ true \qquad A\ true}{C\ true}\ \spadesuit E_2$$

Which of these rules are invertible, and which are non-invertible?

It should be fairly clear that $\spadesuit I$ is invertible; given $\spadesuit(A,B,C)$, we can recover the premises of the rule by using $\spadesuit E_1$ and $\spadesuit E_2$. If this doesn't seem entirely obvious, make use of your newfound superpowers and re-express $\spadesuit I$ as

$$\frac{A\ true \vdash B\ true \qquad A\ true \vdash C\ true}{A\ true \vdash \spadesuit(A,B,C)\ true}\ \spadesuit I$$

and now it should be more obvious!

How about $\spadesuit E_1$ and $\spadesuit E_2$? Well, it certainly isn't true that the conclusions of those rules being true means that the premises are true. For a quick counterexample for $\spadesuit E_1$, consider $A = \bot$ and $B = \top$. Then the conclusion $B\ true$ is... true, but that certainly wouldn't license you to say $A\ true$. You can do something similar for $\spadesuit E_2$.

Clubbing (seals)

Consider the connective $\clubsuit$, with the following sequent-style right/left rules:

$$\frac{\Gamma \Longrightarrow A \qquad \Gamma \Longrightarrow B}{\Gamma \Longrightarrow \clubsuit(A,B,C)}\ \clubsuit R_1 \qquad \frac{\Gamma \Longrightarrow A \qquad \Gamma \Longrightarrow C}{\Gamma \Longrightarrow \clubsuit(A,B,C)}\ \clubsuit R_2 \qquad \frac{\Gamma, A, B \Longrightarrow D \qquad \Gamma, A, C \Longrightarrow D}{\Gamma, \clubsuit(A,B,C) \Longrightarrow D}\ \clubsuit L$$

Which are invertible, and which are non-invertible? Assume that nice theorems like cut and identity hold.

$\clubsuit L$ is invertible. It's slightly complicated, but

$$\frac{\dfrac{\overline{\Gamma, A, B \Longrightarrow A}\ \text{id} \qquad \overline{\Gamma, A, B \Longrightarrow B}\ \text{id}}{\Gamma, A, B \Longrightarrow \clubsuit(A,B,C)}\ \clubsuit R_1 \qquad \begin{array}{c}\text{conclusion of } \clubsuit L \text{ with weakening and stuff}\\ \Gamma, \clubsuit(A,B,C) \Longrightarrow D\end{array}}{\Gamma, A, B \Longrightarrow D}\ \text{cut}$$

and you can do similar things to get the second premise.

$\clubsuit R_1$ and $\clubsuit R_2$ are not invertible; we can have $\Gamma \Longrightarrow \clubsuit(A,B,C)$ without $\Gamma \Longrightarrow B$ or $\Gamma \Longrightarrow C$. Consider the counterexample with $A = C = \top$ and $B = \bot$.

2 Reduced sequent calculus

Recall the rules for the reduced sequent calculus.

$$\frac{\Gamma \longrightarrow A \qquad \Gamma \longrightarrow B}{\Gamma \longrightarrow A \wedge B} \wedge R \qquad \frac{\Gamma, A, B \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C} \wedge L \qquad \frac{}{\Gamma, P \longrightarrow P} \text{init}$$

(Why did we do this for $\wedge$? Well, we want to get rid of the original formula above the line so we can say our premises have grown smaller!)

$$\frac{}{\Gamma \longrightarrow \top} \top R \qquad \frac{\Gamma \longrightarrow C}{\Gamma, \top \longrightarrow C} \top L \qquad \frac{\Gamma \longrightarrow A}{\Gamma \longrightarrow A \vee B} \vee R_1 \qquad \frac{\Gamma \longrightarrow B}{\Gamma \longrightarrow A \vee B} \vee R_2 \qquad \frac{\Gamma, A \longrightarrow C \qquad \Gamma, B \longrightarrow C}{\Gamma, A \vee B \longrightarrow C} \vee L$$

(What did we do for $\vee$? Well, it makes sense that we can get rid of $A \vee B$ above the line, since A and B "tell you more" than $A \vee B$, and now you have those.

$$\frac{}{\Gamma, \bot \longrightarrow C} \bot L \qquad \frac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \supset B} \supset R \qquad \frac{\Gamma, A \supset B \longrightarrow A \qquad \Gamma, B \longrightarrow C}{\Gamma, A \supset B \longrightarrow C} \supset L$$

Notice how $\supset L$ is "annoying"; we weren't able to get rid of the original formula entirely above the line. This will bother us.

> "Pretend you're not a human, you're a parser, and all you know how to do is blindly apply rules."
> (An LTI professor)

Now we're going to pretend to be computers! Fun!

We know $\neg\neg(P \vee \neg P)$ is true, of course. So let's prove it!

Round and round we go

Try and prove $\longrightarrow ((P \vee (P \supset \bot)) \supset \bot) \supset \bot$. Act like you're a computer with no intelligence; pick out a rule from the ones above, in the order given, and apply it blindly.

... ok, that didn't go so well. Why? We can actually make this sort of procedure work using *loop checking.* Basically, you would use something like a hash table, and stick in sequents you'd seen before, so you would know it was unproductive if you set off to prove something that was already in your hash table.

Aside: what if we tried to "fix up" this reduced sequent calculus by changing $\supset L$ to look like

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

Is that a good rule? It's certainly making the sequents above the line smaller...

3 Inversion calculus

Remember the inversion calculus with an ordered context of assumptions, plus a separate context of "annoying" formulas (specifically, a context containing formulas whose left rules are not invertible)? In it, we can be in *right mode*, when we're trying to break things down on the right of the sequent arrow, or in *left mode*, when we're trying to break things down on the left of the sequent arrow. We switch from right mode to left mode if we encounter a formula whose right rule is not invertible. Basically, we're always trying to put off using non-invertible rules for as long as possible.

Confusing? Let's work an example!

$$
\dfrac{\dfrac{\dfrac{}{B \supset A; A \xrightarrow{L} A}\text{init} \qquad \dfrac{\dfrac{\dfrac{}{B \supset A, B; \cdot \xrightarrow{R} B}\text{init} \qquad \dfrac{}{B; A \xrightarrow{L} A}\text{init}}{B \supset A, B; \cdot \xrightarrow{L} A}\supset L}{B \supset A; B \xrightarrow{L} A}\text{shift}_P}{\dfrac{\dfrac{B \supset A; A \vee B \xrightarrow{L} A}{\cdot; A \vee B, B \supset A \xrightarrow{L} A}\text{shift}_\supset}{\cdot; (A \vee B) \wedge (B \supset A) \xrightarrow{L} A}\wedge L}\vee L}{\dfrac{\cdot; (A \vee B) \wedge (B \supset A) \xrightarrow{R} A}{\cdot; \cdot \xrightarrow{R} (A \vee B) \wedge (B \supset A) \supset A}\supset R}LR_P
$$

Nice! But does this fancy inversion calculus fix the problem we had with the $\neg\neg(P \vee \neg P)$ example we had earlier? Unfortunately, it doesn't :(

4 Left out

Yesterday in lecture we saw how to break down the $\supset L$ rule by cases on its antecedent. We used the equivalences

$$
\begin{aligned}
\top \supset B &\equiv B && (\top \text{ gives no information and can be discarded}) \\
(A \wedge B) \supset C &\equiv A \supset B \supset C && (\text{currying}) \\
\bot \supset B &\equiv \top && (\text{ex falso quodlibet\ldots\ kind of}) \\
(A \vee B) \supset C &\equiv (A \supset C) \wedge (B \supset C) && \\
((D \supset B) \supset C) \wedge D &\equiv (B \supset C) \wedge D &&
\end{aligned}
$$

That last equivalence, i.e. $\supset\supset L$ can be a little mysterious. Think of it this way. If we were trying to prove

$$\Gamma, (A \supset B) \supset C \longrightarrow D$$

using the normal $\supset L$ rule, our first premise would be

$$\Gamma, (A \supset B) \supset C \longrightarrow A \supset B$$

but since $\supset R$ is invertible, we can immediately say

$$\Gamma, (A \supset B) \supset C, A \longrightarrow B$$

But if we assume A, then $A \supset B \equiv B$! So we simplify the assumption to $B \supset C$.

Now we have no annoying rules left! Does this fix our problem with $\neg\neg(P \vee \neg P)$?

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\bot \longrightarrow \bot}\bot L}{P \supset \bot, P \longrightarrow \bot}P \supset L}{P \supset \bot, P, \bot \supset \bot \longrightarrow \bot}\bot \supset L \qquad \dfrac{}{P \supset \bot, \bot \longrightarrow \bot}\bot L}{P \supset \bot, (P \supset \bot) \supset \bot \longrightarrow \bot}\supset\supset L}{(P \vee (P \supset \bot)) \supset \bot \longrightarrow \bot}\vee \supset L}{\longrightarrow ((P \vee (P \supset \bot)) \supset \bot) \supset \bot}\supset R
$$

Your job for the next homework: to combine the ideas of the inversion calculus and G4ip to write a proof search procedure!