Constructive Logic (15-317), Fall 2015
Recitation 10: G4ip in Prolog and review for midterm 2 (11/4/2015)

Vincent Huang (`vincenth@andrew`), Anna Gommerstadt (`hgommers@cs`), Michael Coblenz (`mcoblenz@cs`)

1 Continuations

What to remember: continuations give a computational interpretation to classical logic. Specifically, use of proof by contradiction corresponds to $\mathcal{C}$ or `callcc`, and producing a contradiction corresponds to `throw`.

2 Sequent calculus

What's wrong with this proof?

$$\dfrac{\dfrac{}{(A \lor B) \land C, A \lor B \implies A \lor B}\ \text{init}}{(A \lor B) \land C \implies A \lor B}\ \land L_1$$

How about this one?

$$\dfrac{\dfrac{}{A \implies A}\ \text{init} \qquad \dfrac{\dfrac{}{A, B \implies B}\ \text{init}}{A \implies B}\ \text{weak}}{A \implies A \land B}\ \land R$$

How about this one?

$$\dfrac{\dfrac{\dfrac{}{a : \tau; \exists x : \tau.\ C(x), C(a) \implies C(a)}\ \text{id}}{\cdot; \exists x : \tau.\ C(x) \implies C(a)}\ \exists L}{\cdot; \cdot \implies \exists x : \tau.\ C(x) \supset C(a)}\ \supset R$$

2.1 Unprovable stuff

1 Show that $\neg(A \supset B) \supset (A \land \neg B)$ is not provable in sequent calculus.
2 Show that $\neg(\neg A \land \neg B) \supset (A \lor B)$ is not provable in sequent calculus.
3 Show that $\neg \exists x : \tau.\ \neg A(x) \supset \forall x : \tau.\ A(x)$ is not provable in sequent calculus.

3 Cut elimination

- $\mathcal{D}$ is the proof of $\Gamma \implies A$.
- $\mathcal{E}$ is the proof of $\Gamma, A \implies C$.
- Cut is the theorem that if $\Gamma \implies A$ and $\Gamma, A \implies C$, then $\Gamma \implies C$.
- Cut elimination is proven by lexicographic induction over A, then $\mathcal{D}$, then $\mathcal{E}$.
- When we appeal to the IH in this proof, "smaller" means contains fewer connectives (when we say A grows smaller), or contains fewer proof steps (when we say $\mathcal{D}$ or $\mathcal{E}$ grows smaller).
- The "principal formula" is the thing that the last rule applied in the derivation operated on, i.e. decomposed or whatever.

4 Dependent types

You can use these to encode stronger invariants about your programs. They correspond to the universal and existential quantifiers in first-order logic.

5 Reduced sequent calculi

What to remember:

- the motivation behind reduced sequent calculus rules.
- the idea of reducing the "weight" when going bottom-up.

6 Inversion

We've discussed invertibility in the past, but to recap, how do we know if a rule is invertible?

A rule is invertible when the premises hold iff the conclusion holds. One way to show this is, given the conclusion, producing a derivation that reconstructs its premises. So,

- To show invertibility, start with the conclusion of the relevant rule, and apply other rules to get to the premises. As a simple example, to show that $\wedge I$ is invertible, $\dfrac{A \wedge B \; \mathit{true}}{A \; \mathit{true}} \wedge E_L \; \dfrac{A \wedge B \; \mathit{true}}{B \; \mathit{true}} \wedge E_R$ so, since (by using other rules in the system) we can get back both premises from the conclusion, it's invertible.
- To show non-invertibility, simply exhibit a counterexample! There's no need for convoluted arguments. For instance, to show that the $\vee I$ rules are not invertible, take $A = \top$ and $B = \bot$. Clearly $A \vee B \; \mathit{true}$ holds, but one can't conclude from that that $B \; \mathit{true}$ holds (and it doesn't). So $\vee I_R$ is non-invertible, and the same argument works for $\vee I_L$.

Proofs of invertibility may look somewhat reminiscent of local expansions, because you generally have a connective, and then you apply elimination rules to "get rid" of the connective and get back the connective-free premises. But

- A local completeness proof would involve reintroducing the connective after this, which is wholly unnecessary in this case!
- They only seem to be similar because all the things you've been trying to show are invertible have been introduction rules. This doesn't always have to be the case.

Another important thing to note is that invertibility depends heavily on the *presentation* of the rule. For instance, sequent calculus as presented in this class was entirely motivated by a correspondence to verifications and uses, and thereby natural deduction. Yet $\wedge E_L$ and $\wedge E_R$ are not invertible, but all the $\wedge L$ rules are invertible.

6.1 Problems

Recall: in the reduced sequent calculus we've seen, there are 5 invertible rules. $\wedge L, \wedge R, \top L, \vee L, \supset R$. Actually, $\forall R$ and $\exists L$ are also invertible.

$$\dfrac{\Sigma, c : \tau; \Gamma, A(c) \to C}{\Sigma; \Gamma, \exists x : \tau . A(x) \to C} \exists L \qquad \dfrac{\Sigma, c : \tau; \Gamma \to A(c)}{\Sigma; \Gamma \to \forall x : \tau . A(x)} \forall R$$

Prove that these last 2 rules are invertible. You may (and probably should) use any of the standard sequent calculus theorems/lemmas.

So, the remaining rules, namely $\vee R_1, \vee R_2, \supset L, \forall L$, and $\exists R$, are not invertible.

$$\dfrac{\Sigma \vdash t : \tau \qquad \Sigma; \Gamma, \forall x : \tau .\ A(x), A(t) \implies C}{\Sigma; \Gamma, \forall x : \tau .\ A(x) \implies C} \forall L \qquad \dfrac{\Sigma \vdash t : \tau \qquad \Sigma; \Gamma \to A(t)}{\Sigma; \Gamma \to \exists x : \tau .\ A(x)} \exists R$$

Prove that the last 2 are not invertible.