Constructive Logic (15-317), Fall 2016
Recitation 5: Cut Elimination and KeYmaera I (10/5/2016)

Evan Cavallo (`ecavallo@cs.cmu.edu`), Oliver Daids `ojd@andrew`, Giselle Reis `greis@andrew`

1 Cut Elimination

$$
\begin{array}{lcc}
 & \text{Sequent Calculus} & \text{Verifications and Uses} \\
\text{Identity} & \dfrac{}{\Gamma, A \Longrightarrow A} & \dfrac{A\downarrow}{A\uparrow} \\[2em]
\text{Cut} & \dfrac{\Gamma \Longrightarrow A \quad \Gamma, A \Longrightarrow C}{\Gamma \Longrightarrow C} & \dfrac{A\uparrow \quad \begin{array}{c} A\downarrow \\ \vdots \\ C\uparrow \end{array}}{C\uparrow}
\end{array}
$$

Identity and cut are *admissible* rules, not *derivable rules*.

Task 1. One instance of cut is

$$\dfrac{\Longrightarrow A \supset A \lor A \quad A \supset A \lor A \Longrightarrow A \land A \supset A}{\Longrightarrow A \land A \supset A}$$

(where A is atomic). Suppose we give cut these proofs:

$$\dfrac{\dfrac{\dfrac{}{A \Longrightarrow A}\,init}{A \Longrightarrow A \lor A}\,\lor R_1}{\Longrightarrow A \supset A \lor A}\,\supset R$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \supset A \lor A, A \land A, A \Longrightarrow A}\,init}{A \supset A \lor A, A \land A \Longrightarrow A}\,\land L_1 \quad \dfrac{\dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,init \quad \dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,init}{A \supset A \land A, A \land A, A \lor A \Longrightarrow A}\,\lor L}{A \supset A \lor A, A \land A \Longrightarrow A}\,\supset L}{A \supset A \lor A \Longrightarrow A \land A \supset A}\,\supset R$$

What is the resulting proof of $\Longrightarrow A \land A \supset A$? Can you see the relationship between cut and local soundness?

On your own time: try the analogous cut in verifications and uses.

Solution 1: We'll demonstrate how the cut proof is computed by reducing a use of the admissible *cut* rule down to smaller cuts, step-by-step. To start with, we have cut applied to the two proofs:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Longrightarrow A}\,\mathit{init}}{A \Longrightarrow A \lor A}\,\lor R_1}{\Longrightarrow A \supset A \lor A}\,\supset R \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A \supset A \lor A, A \land A, A \Longrightarrow A}\,\mathit{init}}{A \supset A \lor A, A \land A \Longrightarrow A}\,\land L_1 \quad \dfrac{\dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,\mathit{init} \quad \dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,\mathit{init}}{A \supset A \land A, A \land A, A \lor A \Longrightarrow A}\,\lor L}{A \supset A \lor A, A \land A \Longrightarrow A}\,\supset L}{A \supset A \lor A \Longrightarrow A \land A \supset A}\,\supset R}{\Longrightarrow A \land A \supset A}\,\mathit{cut}$$

This is a case where the last rule in the right-hand premise of cut ($\supset R$ applied to $A \land A \supset A$) is unrelated to the cut formula ($A \supset A \lor A$). In a case like this, we can just pull the rule out of the cut (weakening the left-hand premise with the assumption $\supset R$ introduces):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \land A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \Longrightarrow A \lor A}\,\lor R_1}{A \land A \Longrightarrow A \supset A \lor A}\,\supset R \qquad \dfrac{\dfrac{\dfrac{}{A \supset A \lor A, A \land A, A \Longrightarrow A}\,\mathit{init}}{A \supset A \lor A, A \land A \Longrightarrow A}\,\land L_1 \quad \dfrac{\dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,\mathit{init} \quad \dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,\mathit{init}}{A \supset A \land A, A \land A, A \lor A \Longrightarrow A}\,\lor L}{A \supset A \lor A, A \land A \Longrightarrow A}\,\supset L}{A \land A \Longrightarrow A}\,\mathit{cut}}{\Longrightarrow A \land A \supset A}\,\supset R$$

Now we come to a spot where the last rule in the right-hand proof ($\supset L$ applied on $A \supset A \lor A$) is actually applied to the cut formula (again, $A \supset A \lor A$). In such a case, we also need to look at the last rule in the left-hand proof. Here, the left-hand proof also ends in a rule involving the cut formula ($\supset R$). This kind of case, where the left-hand proof ends in a right rule on the cut formula and the right-hand proof ends in a left rule on the cut formula, is where the real work of cut happens. One characteristic of these cases is that the reduction introduces cuts on smaller formulas (A and $A \lor A$). Although it's hard to see here, the fact that we can reduce cuts in cases where a left and right rule combine is intimately related to local soundness.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \land A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \Longrightarrow A \lor A}\,\lor R_1}{A \land A \Longrightarrow A \supset A \lor A}\,\supset R \quad \dfrac{\dfrac{}{A \supset A \lor A, A \land A, A \Longrightarrow A}\,\mathit{init}}{A \supset A \lor A, A \land A \Longrightarrow A}\,\land L_1}{A \land A \Longrightarrow A}\,\mathit{cut} \quad \dfrac{\dfrac{}{A \land A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \Longrightarrow A \lor A}\,\lor R_1}{A \land A \Longrightarrow A \lor A}\,\mathit{cut} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{A \land A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \Longrightarrow A \lor A}\,\lor R_1}{A \land A \Longrightarrow A \supset A \lor A}\,\supset R \quad \dfrac{\dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,\mathit{init} \quad \dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,\mathit{init}}{A \supset A \land A, A \land A, A \lor A \Longrightarrow A}\,\lor L}{A \land A, A \lor A \Longrightarrow A}\,\mathit{cut}}{A \land A \Longrightarrow A}\,\mathit{cut}}{\Longrightarrow A \land A \supset A}\,\supset R$$

Let's proceed by first reducing the top-left cut:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \land A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \Longrightarrow A \lor A}\,\lor R_1}{A \land A \Longrightarrow A \supset A \lor A}\,\supset R \qquad \dfrac{\dfrac{}{A \supset A \lor A, A \land A, A \Longrightarrow A}\,\mathit{init}}{A \supset A \lor A, A \land A \Longrightarrow A}\,\land L_1}{A \land A \Longrightarrow A}\,\mathit{cut}$$

This is another case where the last rule in the right premise is unrelated to the cut formula, so we just move the cut up and weaken the left premise with the introduced assumption (A):

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \land A, A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A, A \Longrightarrow A \lor A}\,\lor R_1}{A \land A, A \Longrightarrow A \supset A \lor A}\,\supset R \qquad \dfrac{}{A \supset A \lor A, A \land A, A \Longrightarrow A}\,\mathit{init}}{\dfrac{A \land A, A \Longrightarrow A}{A \land A \Longrightarrow A}\,\land L_1}\,\mathit{cut}$$

At last we come to a case where the right premise ends in *init*. Since the init is on A and not the cut formula $A \supset A \lor A$, we can just replace the *cut* with an *init*:

$$\dfrac{\dfrac{}{A \land A, A \Longrightarrow A}\,\mathit{init}}{A \land A \Longrightarrow A}\,\land L_1$$

Now we've finished reducing the first cut of the four we introduced when $\supset R$ met $\supset L$. Next we'll look at the top right cut:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \land A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \Longrightarrow A \lor A}\,\lor R_1}{A \land A \Longrightarrow A \supset A \lor A}\,\supset R \qquad \dfrac{\dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,\mathit{init} \quad \dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,\mathit{init}}{A \supset A \land A, A \land A, A \lor A \Longrightarrow A}\,\lor L}{A \land A, A \lor A \Longrightarrow A}\,\mathit{cut}$$

This is another one of those cases where we just move the cut up, since the last rule in the right premise ($\lor L$ on $A \lor A$) is not applied to the cut formula ($A \supset A \lor A$). The only difference from previous cases like this is that $\lor L$ has two premises, so we have to apply a cut to each of them:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \land A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \Longrightarrow A \lor A}\,\lor R_1}{A \land A \Longrightarrow A \supset A \lor A}\,\supset R \quad \dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \lor A, A \Longrightarrow A}\,\mathit{cut} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{A \land A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \Longrightarrow A \lor A}\,\lor R_1}{A \land A \Longrightarrow A \supset A \lor A}\,\supset R \quad \dfrac{}{\ldots, A \lor A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \lor A, A \Longrightarrow A}\,\mathit{cut}}{A \land A, A \lor A \Longrightarrow A}\,\lor L$$

Each of the two new cuts has an *init* on the right side, applied to something other than the cut formula, so they both reduce to *init*:

$$\dfrac{\dfrac{}{A \land A, A \lor A, A \Longrightarrow A}\,\mathit{init} \quad \dfrac{}{A \land A, A \lor A, A \Longrightarrow A}\,\mathit{init}}{A \land A, A \lor A \Longrightarrow A}\,\lor L$$

Now that we've reduced two of four cuts, let's return to the main proof. After replacing the two upper cuts with their reduced forms, we're left with:

$$\begin{prooftree}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \Longrightarrow A$}
\RightLabel{$\wedge L_1$}
\UnaryInfC{$A \wedge A \Longrightarrow A$}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \Longrightarrow A$}
\RightLabel{$\vee R_1$}
\UnaryInfC{$A \wedge A, A \Longrightarrow A \vee A$}
\RightLabel{\textit{cut}}
\dottedLine
\BinaryInfC{$A \wedge A \Longrightarrow A \vee A$}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \vee A, A \Longrightarrow A$}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \vee A, A \Longrightarrow A$}
\RightLabel{$\vee L$}
\BinaryInfC{$A \wedge A, A \vee A \Longrightarrow A$}
\RightLabel{\textit{cut}}
\dottedLine
\BinaryInfC{$A \wedge A \Longrightarrow A$}
\RightLabel{$\supset R$}
\UnaryInfC{$\Longrightarrow A \wedge A \supset A$}
\end{prooftree}$$

First we have to take care of the upper cut:

$$\begin{prooftree}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \Longrightarrow A$}
\RightLabel{$\wedge L_1$}
\UnaryInfC{$A \wedge A \Longrightarrow A$}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \Longrightarrow A$}
\RightLabel{$\vee R_1$}
\UnaryInfC{$A \wedge A, A \Longrightarrow A \vee A$}
\RightLabel{\textit{cut}}
\dottedLine
\BinaryInfC{$A \wedge A \Longrightarrow A \vee A$}
\end{prooftree}$$

The first step is another one where we just push the cut up.

$$\begin{prooftree}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \Longrightarrow A$}
\RightLabel{$\wedge L_1$}
\UnaryInfC{$A \wedge A \Longrightarrow A$}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \Longrightarrow A$}
\RightLabel{\textit{cut}}
\dottedLine
\BinaryInfC{$A \wedge A \Longrightarrow A$}
\RightLabel{$\vee R_1$}
\UnaryInfC{$A \wedge A \Longrightarrow A \vee A$}
\end{prooftree}$$

Now we've come to an *init* in the right premise. For the first time, however, *init* is applied with the cut formula (A). In this case, we can't just reduce to an *init*, since we're cutting out the premise A. So instead, we use the proof of the left premise, which is exactly what we need:

$$\begin{prooftree}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \Longrightarrow A$}
\RightLabel{$\wedge L_1$}
\UnaryInfC{$A \wedge A \Longrightarrow A$}
\RightLabel{$\vee R_1$}
\UnaryInfC{$A \wedge A \Longrightarrow A \vee A$}
\end{prooftree}$$

Now we can return again to the main proof, replacing the upper cut with its reduced form:

$$\begin{prooftree}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \Longrightarrow A$}
\RightLabel{$\wedge L_1$}
\UnaryInfC{$A \wedge A \Longrightarrow A$}
\RightLabel{$\vee R_1$}
\UnaryInfC{$A \wedge A \Longrightarrow A \vee A$}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \vee A, A \Longrightarrow A$}
\AxiomC{}
\RightLabel{\textit{init}}
\UnaryInfC{$A \wedge A, A \vee A, A \Longrightarrow A$}
\RightLabel{$\vee L$}
\BinaryInfC{$A \wedge A, A \vee A \Longrightarrow A$}
\RightLabel{\textit{cut}}
\dottedLine
\BinaryInfC{$A \wedge A \Longrightarrow A$}
\RightLabel{$\supset R$}
\UnaryInfC{$\Longrightarrow A \wedge A \supset A$}
\end{prooftree}$$

For the second time, we have a case where the right premise has a left rule applied to the cut formula ($\vee L$) and the left premise has a right rule applied to the cut formula ($\vee R_1$). As in the implication case, this reduction introduces a cut at a smaller formula (A). Although we can't really tell the difference here, since the two branches above the $\vee L$ are the same, in general the fact that we have a $\vee R_1$ tells us to take the first branch (seen in the reduced proof as the right premise of the upper cut). Again, this matches how the local soundness reductions for $\vee$ each choose a branch.

$$\dfrac{\dfrac{\dfrac{}{A \wedge A, A \Longrightarrow A}\;\mathit{init}}{A \wedge A \Longrightarrow A}\;\wedge L_1 \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge A, A \Longrightarrow A}\;\mathit{init}}{A \wedge A \Longrightarrow A}\;\wedge L_1}{A \wedge A \Longrightarrow A \vee A}\;\vee R_1 \qquad \dfrac{}{A \wedge A, A \vee A, A \Longrightarrow A}\;\mathit{init}}{A \wedge A, A \Longrightarrow A}\;\mathit{cut}}{\dfrac{A \wedge A \Longrightarrow A}{\Longrightarrow A \wedge A \supset A}\;\supset R}\;\mathit{cut}$$

Now the upper cut is applied to an *init* on something other than the cut formula, so it reduces to an *init*.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge A, A \Longrightarrow A}\;\mathit{init}}{A \wedge A \Longrightarrow A}\;\wedge L_1 \qquad \dfrac{}{A \wedge A, A \Longrightarrow A}\;\mathit{init}}{A \wedge A \Longrightarrow A}\;\mathit{cut}}{\Longrightarrow A \wedge A \supset A}\;\supset R$$

Last of all, the remaining cut is an *init* on the cut formula, so it reduces to the left premise.

$$\dfrac{\dfrac{\dfrac{}{A \wedge A, A \Longrightarrow A}\;\mathit{init}}{A \wedge A \Longrightarrow A}\;\wedge L_1}{\Longrightarrow A \wedge A \supset A}\;\supset R$$

Finally, the proof is fully reduced to a cut-free form! In this case, the reduced proof is rather short. In general, though, cut can produce extremely large proofs. One way of thinking of cut reduction is as "inlining a lemma."

$$\dfrac{\overset{\mathcal{D}}{\Gamma \Longrightarrow A} \quad \overset{\mathcal{E}}{\Gamma, A \Longrightarrow C}}{\Gamma \Longrightarrow C}\;\mathit{cut}$$

Using the cut rule, we can use some lemma A we've proven to prove some other theorem C. The process of cut reduction essentially pulls everything that is necessary for the proof out of $\mathcal{D}$ and incorporates it into $\mathcal{E}$ to build a complete proof of C. Since we might use the lemma many times, the complete proof could be much larger than either $\mathcal{D}$ or $\mathcal{E}$.

2 KeYmaera I

`http://keymaerax.org/KeYmaeraI.jar`
Username: `guest`
Password: `guest`