15-317 Lecture 12: Theorem proving

- Proof search (and related problems)
- Reduced sequent calculus
- Contraction-free sequent calculus

Proof Search

- Given A, find a proof of $\Longrightarrow A$
  - Or justify that $\Longrightarrow A$ is not provable
- Second idea: Given $\Gamma, A, \ldots$,
  prove $\Gamma \Longrightarrow A$ or justify $\Gamma \not\Longrightarrow A$

Similar problems:

- Given a proof, find prop / sequent
- Given a proof *and* a sequent: Do they match?

Proof	Sequent
Find	Given
Given	Given
Given	Find

Proof search / Program synthesis

Proof checking / Type checking

Type inference

Reduced Sequent Calculus

- Ideally we never apply the same rule to the same prop

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, A, A, A, A \wedge B \Rightarrow C}}{\Gamma, A \wedge B, A, A \Rightarrow C}\wedge L_1}{\Gamma, A \wedge B, A \Rightarrow C}\wedge L_1}{\Gamma, A \wedge B \Rightarrow C}\wedge L_1$$

$$\dfrac{\Gamma \to A \qquad \Gamma \to B}{\Gamma \longrightarrow A \wedge B}\wedge R$$

$$\dfrac{\Gamma, A, B \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C}\wedge L$$

Ensure $\Gamma \Rightarrow A$ iff $\Gamma \longrightarrow A$

Soundness of $\longrightarrow$ w.r.t. $\Rightarrow$

$$\dfrac{\dfrac{\Gamma, A, B \Rightarrow C}{\Gamma, A \wedge B, A, B \Rightarrow C}\,\text{weakening}\Rightarrow}{\Gamma, A \wedge B, A \Rightarrow C}\wedge L_2$$

$$\dfrac{\Gamma, A \wedge B, A \Rightarrow C}{\Gamma, A \wedge B \Rightarrow C}\wedge L_1$$

Completeness of $\longrightarrow$ w.r.t. $\Rightarrow$

If $\mathcal{D} = \dfrac{\mathcal{D}_1}{\Gamma, A \wedge B, A \Rightarrow C}\wedge L_1$,

$$\dfrac{\dfrac{\dfrac{}{\Gamma, A, B \longrightarrow A}\,id_A}{\Gamma, A \wedge B \longrightarrow A}\wedge L \qquad \text{i.h.}(\mathcal{D}_1)\ \ \Gamma, A \wedge B, A \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C}\,cut_A$$

$$\frac{}{T/F}$$

$$\frac{}{\Gamma, F \longrightarrow C}\,FL$$

$$\frac{}{\Gamma \longrightarrow T}\,TR \qquad \frac{\Gamma \longrightarrow C}{\Gamma, T \longrightarrow C}\,TL$$

Disjunction

$$\frac{\Gamma \to A}{\Gamma \to A \vee B} \vee R_1 \qquad \frac{\Gamma \to B}{\Gamma \to A \vee B} \vee R_2$$

$$\frac{\Gamma, A \to C \qquad \Gamma, B \to C}{\Gamma, A \vee B \to C} \vee L$$

$$\dfrac{\dfrac{\Gamma, A \to C \qquad \Gamma, B \to C}{\Gamma, A \vee B \to C}\vee L \qquad\qquad}{}$$

$\mathcal{D}_1$ $\qquad$ $\mathcal{D}_2$

$$\mathcal{D} = \dfrac{\Gamma, A \vee B, A \Rightarrow C \qquad \Gamma, A \vee B, B \Rightarrow C}{\Gamma, A \vee B \Rightarrow C}\vee L$$

$$\dfrac{\dfrac{\dfrac{}{\Gamma, A \to A}\, id_A}{\Gamma, A \to A \vee B}\vee R_1 \qquad \dfrac{\text{i.h.}(\mathcal{D}_1)}{\Gamma, A \vee B, A \to C} \qquad \dfrac{\vdots}{\Gamma, B \to C}}{\Gamma, A \to C}\, cut_A}{\Gamma, A \vee B \to C}\vee L$$

Implication

$$\frac{\Gamma, A \to B}{\Gamma \to A \supset B} \supset R \qquad \frac{\Gamma, A \supset B \to A \quad \Gamma, B \to C}{\Gamma, A \supset B \to C} \supset L$$

Properties of $\to$

- Weakening: If $\Gamma \to C$, then $\Gamma, A \to C$
- Contraction: If $\Gamma, A, A \to$ then $\Gamma, A \Rightarrow C$
- Identity: $\Gamma, A \to A$
- Cut: If $\Gamma \to A$ and $\Gamma, A \to C$, then $\Gamma \to C$

- Soundness If $\Gamma \to A$ then $\Gamma \Rightarrow A$
- Completeness If $\Gamma \Rightarrow A$ then $\Gamma \to A$

$$\frac{\Gamma, A \supset B \to A \quad \Gamma, B \to C}{\Gamma, A \supset B \to C} \supset L$$

Consider cases of what A can be

$A = \top$

$$\frac{\left[\Gamma, \top \supset B \to \top\right)^{\overline{\top R}} \quad \Gamma, B \to C}{\Gamma, \top \supset B \to C} \top \supset L$$

$$\frac{\Gamma, B \to C}{\Gamma, \top \supset B \to C} \top \supset L$$

$A = F$

$$\frac{\Gamma, F \supset B \to F \qquad \Gamma, B \to C}{\Gamma, F \supset B \to C}\ F \supset L \cdot \qquad \frac{\Gamma, B \to C}{\Gamma, F \supset B \to C}\ F \supset L$$

$\Gamma, F \supset B \to F \rightsquigarrow \Gamma, T \to F$

$$\frac{\Gamma \to C}{\Gamma, \underbrace{F \supset B}_{T} \to C}\ F \supset L$$

$A = A_1 \vee A_2$

$$\frac{\Gamma, (A_1 \vee A_2) \supset B \to A_1 \vee A_2 \qquad \Gamma, B \to C}{\Gamma, (A_1 \vee A_2) \supset B \to C} \vee \supset L$$

$$\frac{\Gamma, A_1 \supset B, A_2 \supset B \to C}{\Gamma, (A_1 \vee A_2) \supset B \to C} \vee \supset L$$

$\downarrow$

$(A_1 \vee A_2) \supset B \equiv (A_1 \supset B) \wedge (A_2 \supset B)$

$\downarrow$

$$\frac{\Gamma, A_1 \supset B, A_2 \supset B \to A_1 \vee A_2 \qquad \Gamma, B \to C}{\Gamma, (A_1 \vee A_2) \supset B \to C} \vee \supset L$$

$A = P$

$$\frac{\Gamma, P \supset B \to P \qquad \Gamma, B \to C}{\Gamma, P \supset B \to C} \longrightarrow \frac{P \in \Gamma \qquad \Gamma, B \to C}{\Gamma, P \supset B \to C} \; P \supset L$$

$A = A_1 \wedge A_2$

$$\frac{\Gamma, A_1 \supset (A_2 \supset B) \longrightarrow C}{\Gamma, (A_1 \wedge A_2) \supset B \longrightarrow C}$$

- Justified by letting
  $\wedge$ have higher weight than $\supset$
  in the induction.

$A = A_1 \supset A_2$

$A_1 \wedge \big((A_1 \supset A_2) \supset B \big)$

$\Vert$

$A_1 \wedge (A_2 \supset B)$

$$\dfrac{\dfrac{}{\Gamma, A_2 \supset B, A_1 \to A_2} \quad \Gamma, B \to C}{\Gamma, (A_1 \supset A_2) \supset B \to C} \supset L$$

$$\dfrac{\dfrac{}{\Gamma, (A_1 \supset A_2) \supset B, A_1 \to A_2}}{\Gamma, (A_1 \supset A_2) \supset B \to A_1 \supset A_2} \supset R \qquad \dfrac{\Gamma, B \to C}{\Gamma, (A_1 \supset A_2) \supset B \to C} \supset L$$

Induction notes

- Multiset ordering:

Given a set A with an order $\leq$.

Suppose M_1, M_2 are multisets of elements of A.

We say $M_1 \leq M_2$ if

- $M_1 \subseteq M_2$
- $M_2 = M_2', a$ and $M_1 = M_1' \cup \{b_1, \ldots, b_n\}$, where each $b_i < a$ and $M_1' \leq M_2'$