COMP 527 Crib Sheet
by Julian Lore Side 1 of 1

1 Natural Deduction

Rules: $\dfrac{}{\Gamma \vdash () : \top}\ \top I$

$\dfrac{\Gamma \vdash M : A \qquad \Gamma \vdash N : B}{\Gamma \vdash \langle M, N\rangle : A \wedge B}\ \wedge I$

$\dfrac{\Gamma \vdash M : A \wedge B}{\Gamma \vdash fst\ M : A}\ \wedge E_l \qquad \dfrac{\Gamma \vdash M : A \wedge B}{\Gamma \vdash snd\ M : B}\ \wedge E_r$

$\dfrac{\Gamma, u : A \vdash M : B}{\Gamma \vdash \lambda u : A.M : A \supset B}\ \supset I^u$

$\dfrac{\Gamma \vdash M : A \supset B \qquad \Gamma \vdash N : A}{\Gamma \vdash M\ N : B}\ \supset E$

$\neg A \equiv A \supset \perp \qquad \dfrac{\Gamma \vdash M : \perp}{\Gamma \vdash abort^C\ M : C}\ \perp E$

$\dfrac{\Gamma \vdash M : A}{\Gamma \vdash inl^A\ M : A \vee B}\ \vee I_l \qquad \dfrac{\Gamma \vdash M : B}{\Gamma \vdash inr^B\ M : A \vee B}\ \vee I_r$

$\dfrac{\Gamma \vdash M : A \vee B \qquad \Gamma, u : A \vdash N_l : C \qquad \Gamma, v : B \vdash N_r : C}{\Gamma \vdash case\ M\ of\ inl^A\ u \to N_l \mid inr^B\ v \to N_r : C}\ \vee E^{u,v}$

$\dfrac{x : A \in \Gamma}{\Gamma \vdash x : A}\ u \qquad \dfrac{\Gamma, a : \tau \vdash M : A(a) \text{ true}}{\Gamma \vdash \lambda a : \tau.M : \forall x : \tau.A(x) \text{ true}}\ \forall I^a$

$\dfrac{\Gamma \vdash M : \forall x : \tau.A(x) \text{ true} \qquad \Gamma \vdash t : \tau}{\Gamma \vdash M\ t : A(t) \text{ true}}\ \forall E$

$\dfrac{\Gamma \vdash M : A(t) \text{ true} \qquad \Gamma \vdash t : \tau}{\Gamma \vdash \langle M, t\rangle : \exists x : \tau.A(x) \text{ true}}\ \exists I$

$\dfrac{\Gamma \vdash M : \exists x : \tau.A(x) \text{ true} \qquad \Gamma, a : \tau, w : A(a) \vdash N : C \text{ true}}{\Gamma \vdash let\ \langle u, a\rangle = M\ in\ N : C \text{ true}}\ \exists E^{w,a}$

Context $\Gamma ::= \cdot \mid \Gamma, u : A$

Structural props:

Weakening Extra assumps don't matter. If $\Gamma, \Gamma' \vdash A$ then $\Gamma, u : B, \Gamma' \vdash A$

Exchange Order of hypothetical assumps doesn't matter. If $\Gamma, x : B_1, y : B_2, \Gamma' \vdash A$ then $\Gamma, y : B_2, x : B_1, \Gamma' \vdash A$

Contraction Assump can be used as often as we like. If $\Gamma, x : B, y : B, \Gamma' \vdash A$ then $\Gamma, x : B, \Gamma' \vdash A$

Substitution: $[N/x]M = M', [N/x]x = N$. Replace the "free" occurence of x in M with N.

Substitution thm: If $\Gamma, x : A, \Gamma' \vdash M : B$ and $\Gamma \vdash N : A$ then $\Gamma, \Gamma' \vdash [N/x]M : B$.

Pf by structural induction on $\Gamma, x : A, \Gamma' \vdash M : B$

Case: $\dfrac{\begin{array}{c}\mathcal{D}'\\ \Gamma, x : A, \Gamma' \vdash M : C \wedge D\end{array}}{\Gamma, x : A, \Gamma' \vdash fst\ M : C}\ \wedge E_l$

$\Gamma, \Gamma' \vdash [N/x]M : C \wedge D$ by IH

$\Gamma, \Gamma' \vdash fst\ ([N/x]M) : C$ by $\wedge E_l$

$\Gamma, \Gamma' \vdash [N/x](fst\ M) : C$ by definition of substitution

Case: $\dfrac{x : A \in (\Gamma, x : A, \Gamma')}{\Gamma, x : A, \Gamma' \vdash x : A}$

$\Gamma \vdash N : A$ by assumption

$\Gamma, \Gamma' \vdash N : A$ by weakening

$\Gamma, \Gamma' \vdash [N/x]x : A$ by substitution definition

Case: $\dfrac{y : B \in (\Gamma, x : A, \Gamma') \qquad x \neq y}{\Gamma, x : A, \Gamma' \vdash y : B}$

$y : B \in (\Gamma, \Gamma')$

$\Gamma, \Gamma' \vdash y : B$ by variable

Substitution lemma on terms: Replace any occurrence of x with N

Substitution lemma on judgements: Replace assump $N : A$ with proof $\mathcal{E}$ establishing $N : A$

2 Reduction Rules

$M \implies M'$ means M reduces to M'

Get reduction rules from local soundness

$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}_1\\ M : A\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ N : B\end{array}}{\langle M, N\rangle : A \wedge B}\ \wedge I}{fst\ \langle M, N\rangle : A}\ \wedge E_l \implies \begin{array}{c}\mathcal{D}_1\\ M : A \text{ true}\end{array}$

$fst\langle M, N\rangle \implies M$

$snd\langle M, N\rangle \implies N$

$(\lambda x : A.M)N \implies [N/x]M$

$case\ (inl^A\ M)\ of\ inl^A\ x \to N_l \mid inr^B\ y \to N_r \implies [M/x]N_l$

$case\ (inr^B\ M)\ of\ inl^A\ x \to N_l \mid inr^B\ y \to N_r \implies [M/y]N_r$

$(\lambda a : \tau.M)t \implies [t/a]M$

$let\langle u, a\rangle = \langle M, t\rangle\ in\ N \implies [M/u][t/a]M$

Subject reduction If $M \implies M'$ and $\Gamma \vdash M : C$ then $\Gamma \vdash M' : C$

Pf by induction on $M \implies M'$ (have to prove for congruence rules too, just generalize)

Case: $fst\langle M, N\rangle \implies M$

$\Gamma \vdash fst\ \langle M, N\rangle : A$ by assumption

$\Gamma \vdash \langle M, N\rangle : A \wedge B$ inversion on $\wedge E_l$

$\Gamma \vdash M : A$ by inversion of $\wedge I$

Case: $(\lambda x : A.M)N \implies [N/x]M$

$\Gamma \vdash (\lambda x : A.M)N : B$ by assumption

$\Gamma \vdash \lambda x : A.M : A \supset B$, $\Gamma \vdash N : A$ by inversion on $\supset E$

$\Gamma, x : A \vdash M : B$ by inversion on $\supset I$

$\Gamma \vdash [N/x]M : B$ by substitution lemma (on above line and $\Gamma \vdash N : A$)

Case: $\dfrac{M \implies M'}{\lambda x : A.M \implies \lambda x : A.M'}$

$\Gamma \vdash \lambda x : A.M : A \supset B$ by assumption

$\Gamma, x : A \vdash M : B$ by inversion on $\supset I$

$\Gamma, x : A \vdash M' : B$ by IH

$\Gamma \vdash \lambda x : A.M' : A \supset B$ by $\supset I$

Congruence Rules

Get a congruence rule for every subterm of proof terms

$\dfrac{M \implies M'}{\langle M, N\rangle \implies \langle M', N\rangle} \qquad \dfrac{N \implies N'}{\langle M, N\rangle \implies \langle M, N'\rangle}$

$\dfrac{M \implies M'}{fst\ M \implies fst\ M'} \qquad \dfrac{M \implies M'}{snd\ M \implies snd\ M'}$

$\dfrac{M \implies M'}{\lambda x : A.M \implies \lambda x : A.M'} \qquad \dfrac{M \implies M'}{M\ N \implies M'\ N}$

$\dfrac{N \implies N'}{M\ N \implies M\ N'} \qquad \dfrac{M \implies M'}{inl^B\ M \implies inl^B\ M'}$

$\dfrac{M \implies M'}{inr^A\ M \implies inr^A\ M'}$

Case congruence rules omitted

3 Soundness and Completeness

Rules should not allow us to deduce new truths (soundness, introduce connective and immediately eliminate it, should be able to erase this detour, otherwise elim rules too strong) and should be strong enough to obtain all information contained in a connective (completeness, elim connective s.t. it retains enough info to reintroduce, otherwise elim rules too weak).

Examples

Conjunction: Soundness

$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A \text{ true}\end{array} \qquad \begin{array}{c}\mathcal{E}\\ B \text{ true}\end{array}}{A \wedge B \text{ true}}\ \wedge I}{A \text{ true}}\ \wedge E_l \implies \begin{array}{c}\mathcal{D}\\ A \text{ true}\end{array}$

$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A \text{ true}\end{array} \qquad \begin{array}{c}\mathcal{E}\\ B \text{ true}\end{array}}{A \wedge B \text{ true}}\ \wedge I}{B \text{ true}}\ \wedge E_r \implies \begin{array}{c}\mathcal{E}\\ B \text{ true}\end{array}$

Completeness:

$\begin{array}{c}\mathcal{D}\\ A \wedge B \text{ true}\end{array} \implies \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A \wedge B \text{ true}\end{array}}{A \text{ true}}\ \wedge E_l \qquad \dfrac{\begin{array}{c}\mathcal{D}\\ A \wedge B \text{ true}\end{array}}{B \text{ true}}\ \wedge E_r}{A \wedge B \text{ true}}\ \wedge I$

Implication: Soundness

$\dfrac{\dfrac{\begin{array}{c}\overline{A \text{ true}}\ u\\ \vdots\\ \mathcal{D}^u\\ B \text{ true}\end{array}}{A \supset B \text{ true}}\ \supset I^u \qquad \begin{array}{c}\mathcal{E}\\ A \text{ true}\end{array}}{B \text{ true}}\ \supset E \implies \begin{array}{c}\mathcal{E}\\ A \text{ true}\\ [\mathcal{E}/u](\mathcal{D})\\ B \text{ true}\end{array}$

Completeness

$\begin{array}{c}\alpha\\ A \supset B \text{ true}\end{array} \implies \dfrac{\dfrac{\begin{array}{c}\alpha\\ A \supset B \text{ true}\end{array} \qquad \dfrac{}{A \text{ true}}\ u}{B \text{ true}}\ \supset E}{A \supset B \text{ true}}\ \supset I^u$

Disjunction: Soundness

$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A\end{array}}{A \vee B}\ \vee I_l \qquad \begin{array}{c}\overline{A}\ u\\ \mathcal{E}\\ C\end{array} \qquad \begin{array}{c}\overline{B}\ v\\ \mathcal{F}\\ C\end{array}}{C}\ \vee E^{u,v} \implies \begin{array}{c}[\mathcal{D}/u]\mathcal{E}\\ C \text{ true}\end{array}$

$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ B\end{array}}{A \vee B}\ \vee I_r \qquad \begin{array}{c}\overline{A}\ u\\ \mathcal{E}\\ C\end{array} \qquad \begin{array}{c}\overline{B}\ v\\ \mathcal{F}\\ C\end{array}}{C}\ \vee E^{u,v} \implies \begin{array}{c}[\mathcal{D}/v]\mathcal{F}\\ C \text{ true}\end{array}$

Completeness

$\begin{array}{c}\mathcal{D}\\ A \vee B\end{array} \implies \dfrac{\begin{array}{c}\mathcal{D}\\ A \vee B\end{array} \qquad \dfrac{\dfrac{}{A \text{ true}}\ u}{A \vee B}\ \vee I_l \qquad \dfrac{\dfrac{}{B \text{ true}}\ v}{A \vee B}\ \vee I_r}{A \vee B}\ \vee E^{u,v}$

Soundness: quantifiers

$\dfrac{\dfrac{\begin{array}{c}\overline{a : \tau}\ a\\ \mathcal{D}\\ A(a)\end{array}}{\forall x : \tau.A(x)}\ \forall I^a \qquad \begin{array}{c}\mathcal{E}\\ t : \tau\end{array}}{A(t)}\ \forall E \implies \begin{array}{c}[t/a]\mathcal{D}\\ A(t)\end{array}$

$\dfrac{\dfrac{\begin{array}{c}\mathcal{E}_1\\ A(t)\end{array} \qquad \begin{array}{c}\mathcal{E}_2\\ t : \tau\end{array}}{\exists x : \tau.A(x)}\ \exists I \qquad \begin{array}{c}\overline{A(a)}\ u \quad \overline{a : \tau}\\ \mathcal{D}^{u,a}\\ C\end{array}}{C}\ \exists E^{u,a} \implies \begin{array}{c}[\mathcal{E}_1/u]([t/a]\mathcal{D})\\ C\end{array}$

Completeness:

$\begin{array}{c}\mathcal{D}\\ \forall x : \tau.A(x)\end{array} \implies \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ \forall x : \tau.A(x)\end{array} \qquad \overline{a : \tau}}{A(a)}\ \forall E}{\forall x : \tau.A(x)}\ \forall I^a$

$\begin{array}{c}\mathcal{D}\\ \exists x : \tau.A(x)\end{array} \implies \dfrac{\begin{array}{c}\mathcal{D}\\ \exists x : \tau.A(x)\end{array} \qquad \dfrac{\dfrac{}{A(a)}\ u \qquad \overline{a : \tau}}{\exists x : \tau.A(x)}\ \exists I}{\exists x : \tau.A(x)}\ \exists E^{u,a}$

4 Translating Systems

Translate $\dfrac{\begin{array}{c}\dfrac{}{u : A}\ u\\ \vdots\\ N : A \qquad M : C\end{array}}{\text{let } u = N \text{ in } M : C}\ \text{let}^u$ with normal ND.

For common part of lang, we just recursively translate subterms.

$x^- = x$

$\langle E_1, E_2\rangle^- = \langle E_1^-, E_2^-\rangle$

$(fst\ E_1)^- = fst\ E_1^-$

...

(No need to translate contexts!)

For let: $(\text{let } u = E_1 \text{ in } E_2)^- = [u/E_1^-]E_2^-$

Now we prove that translation preserves provability.

If $\mathcal{D} :: \Gamma \vdash E : A$ then there exists $\mathcal{D}' :: \Gamma \vdash M : A$ where $M = E^-$

Pf by structural induction on typing deriv $\mathcal{D}$

Case: $\mathcal{D} = \dfrac{x : A \in \Gamma}{\Gamma \vdash x : A}$

Show $\Gamma \vdash x^- : A$. But by definition of $\cdot^-$, all we need is $\Gamma \vdash x : A$. But that is just $\mathcal{D}$. (this is why not translating contexts here is good)

Case: $\dfrac{\begin{array}{c}\mathcal{D}'\\ \Gamma \vdash E : A \wedge B\end{array}}{\Gamma \vdash fst\ E : A}$

IH on $\mathcal{D}'$, get $\mathcal{E}' :: \Gamma \vdash M : A \wedge B$ where $M = E^-$. Then:

$\dfrac{\begin{array}{c}\mathcal{E}'\\ \Gamma \vdash M : A \wedge B\end{array}}{\Gamma \vdash fst\ M : A}$

Case: $\dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma \vdash E_1 : C\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ \Gamma, u : C \vdash E_2 : A\end{array}}{\Gamma \vdash let\ u = E_1\ in\ E_2 : A}$

IH on $\mathcal{D}_1$, get $\mathcal{E}_1 :: \Gamma \vdash M_1 : C$ and IH on $\mathcal{D}_2$, get $\mathcal{E}_2 :: \Gamma, u : C \vdash M_2 : A$ where $M_i = E_i^-$. Substitution lemma on $\mathcal{E}_1$ and $\mathcal{E}_2$, get $\mathcal{E} :: \Gamma \vdash [M_1/u]M_2 : A$.

5 Type Uniqueness

If $\mathcal{D} :: \Gamma \vdash M : A$ and $\mathcal{E} :: \Gamma \vdash M : B$ then $A = B$.

Pf by induction on typing derivation $\mathcal{D}$.

Case: $\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}'\\ x : A \in \Gamma\end{array}}{\Gamma \vdash x : A}\ u$

$M = x$ is a variable. $\mathcal{E} :: \Gamma \vdash x : B$ by assumption. Inversion on $\mathcal{E}$: $\mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}'\\ x : B \in \Gamma\end{array}}{\Gamma \vdash x : B}\ u$

Uniqueness of declarations in context Γ, so $A = B$.

Case: $\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}'\\ \Gamma, x : A' \vdash M' : B_1\end{array}}{\Gamma \vdash \lambda x : A'.M' : A' \supset B_1}$

$M = \lambda x : A'.M'$ and $A = A' \supset B_1$. $\mathcal{E} :: \Gamma \vdash \lambda x : A'.M' : B$ by assumption. Inversion gives: $\mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}'\\ \Gamma, x : A' \vdash M' : B_2\end{array}}{\Gamma \vdash \lambda x : A'.M' : A' \supset B_2}$

So $B = A' \supset B_2$. IH on $\mathcal{D}'$ and $\mathcal{E}'$, get $B_1 = B_2'$. So $A = A' \supset B_1 = A' \supset B_2 = B$

Case: $\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma \vdash M' : A_1 \supset B_1\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ \Gamma \vdash N : A_1\end{array}}{\Gamma \vdash M'\ N : B_1}$

$M = M'\ N$ and $A = B_1$. Inversion: $\mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}_1\\ \Gamma \vdash M' : A_2 \supset B_2\end{array} \qquad \begin{array}{c}\mathcal{E}_2\\ \Gamma \vdash N : A_2\end{array}}{\Gamma \vdash M'\ N : B_2}$

$B = B_2$. By IH on $\mathcal{D}_1$ and $\mathcal{E}_1$, get $A_1 \supset B_1 = A_2 \supset B_2$. By injectivity of $\supset$ constructor, get $A_1 = A_2$ and $A = B_1 = B_2 = B$.

Case: $\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}'\\ \Gamma \vdash M' : A_1\end{array}}{\Gamma \vdash inl^{B'} M' : A_1 \vee B'}$

$M = inl^{B'} N'$ and $A = A_1 \vee B'$. Inversion: $\mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}'\\ \Gamma \vdash M' : A_2\end{array}}{\Gamma \vdash inl^{B'} M' : A_2 \vee B'}$

$B = A_2 \vee B'$. By IH on $\mathcal{D}'$ and $\mathcal{E}'$, $A_1 = A_2$ so $A = A_1 \vee B' = A_2 \vee B' = B$

Case: for $\vee$ elim, only need to use IH on N_l or N_r to get equality of deduced term.

6 Misc

Defining proof terms for a new type: they should be *distinct* from other terms in the language so you can't distinguish which rules correspond to which terms.

When proving with many cases, show representative cases, i.e. all cases where something interesting happens and one of each kind of "boring" case.