1 Natural Deduction

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

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

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

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

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

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

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

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

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

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

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

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

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: $\mathcal{D} = \dfrac{\dfrac{\mathcal{D}'}{\Gamma, x : A, \Gamma' \vdash M : C \wedge D}}{\Gamma, x : A, \Gamma' \vdash fst\ M : C}\wedge E_l$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Completeness:

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

Implication: Soundness

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

Completeness

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

Disjunction: Soundness

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

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

Soundness: quantifiers

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

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

Completeness:

$\dfrac{\mathcal{D}}{\forall x : \tau.A(x)} \implies \dfrac{\dfrac{\mathcal{D}}{\forall x : \tau.A(x)} \qquad \dfrac{}{a : \tau}}{A(a)}\forall E$

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

4 Translating Systems

Translate $\dfrac{\dfrac{\dfrac{}{u : A}u}{\vdots} \qquad }{}$ $\dfrac{N : A \qquad M : C}{let\ u = N\ in\ M : C}let^u$ 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 if no new connectives, same target lang)

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

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: $\dfrac{\dfrac{\mathcal{D}'}{\Gamma \vdash E : A \wedge B}}{\Gamma \vdash fst\ E : A}$

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

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

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

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

$M = x$ is a variable. $\mathcal{E} :: \Gamma \vdash x : B$ by assumption. Inversion on $\mathcal{E}$:

$\mathcal{E} = \dfrac{\dfrac{\mathcal{E}'}{x : B \in \Gamma}}{\Gamma \vdash x : B}u$

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

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

$M = \lambda x : A'.M'$ and $A = A' \supset B_1$. $\mathcal{E} :: \Gamma \vdash \lambda x : A'.M' : B$ by assumption. Inversion gives:

$\mathcal{E} = \dfrac{\dfrac{\mathcal{E}'}{\Gamma, x : A' \vdash M' : B_2}}{\Gamma \vdash \lambda x : A'.M' : A' \supset B_2}$

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

$M = M'\ N$ and $A = B_1$. Inversion:

$\mathcal{E} = \dfrac{\dfrac{\mathcal{E}_1}{\Gamma \vdash M' : A_2 \supset B_2} \qquad \dfrac{\mathcal{E}_2}{\Gamma \vdash N : A_2}}{\Gamma \vdash M'\ N : B_2}$

$B = B_2$. 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: $\mathcal{D} = \dfrac{\dfrac{\mathcal{D}'}{\Gamma \vdash M' : A_1}}{\Gamma \vdash inl^{B'}M' : A_1 \vee B'}$

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

$B = A_2 \vee B'$. 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 Induction

Nats: $\dfrac{}{z : nat}nat\ I_z \quad \dfrac{n : nat}{s\ n : nat}nat\ I_s$

Encode relations to form signature $\mathcal{Y}$: $le\_z : \forall n : nat.z \leq n$

$le\_s : \forall n : nat.\forall m.nat.n \leq m \supset s\ n \leq s\ m$

$ref : \forall x : nat.x = x$

$\dfrac{\Gamma \vdash t : nat \qquad \Gamma \vdash A(z)\text{ true} \qquad \Gamma, n : nat, ih : A(n)\text{ true} \vdash A(s\ n)\text{ true}}{\Gamma \vdash A(t)\text{ true}}nat\ E^{n,ih}$

Example proof:

$\dfrac{\dfrac{\dfrac{}{\mathcal{Y}, a : nat \vdash a : nat} \qquad \dfrac{\mathcal{D}_1}{\mathcal{Y}, a : nat \vdash z \leq z\text{ true}} \qquad \dfrac{\mathcal{D}_2}{\mathcal{Y}, a : nat, n : nat, ih : n \leq n \vdash s\ n \leq s\ n}}{\mathcal{Y}, a : nat \vdash a \leq a\text{ true}}nat\ E^{n,ih}}{\mathcal{Y} \vdash \forall x : nat.x \leq x}\forall I^a$

$\mathcal{D}_1 = \dfrac{\dfrac{}{\mathcal{Y}, n : nat \vdash z \leq n}le\_z \qquad \dfrac{}{\mathcal{Y} \vdash z : nat}nat\ I_z}{\mathcal{Y} \vdash z \leq z}$

Let $\mathcal{Y}' = \mathcal{Y}, a : nat, n : nat, ih : n \leq n$

$\mathcal{D}_2 = \dfrac{\dfrac{}{\mathcal{Y} \vdash n \leq n}ih \qquad \dfrac{\dfrac{}{\mathcal{Y}' \vdash \forall n : nat.\forall m : nat.n \leq m \supset s\ n \leq s\ m}le\_s \qquad \dfrac{}{\mathcal{Y}' \vdash n : nat}}{\mathcal{Y}' \vdash n \leq n \supset s\ n \leq s\ n}\forall E(2}{\mathcal{Y}' \vdash s\ n \leq s\ n}\supset E$

Proof terms:

$\dfrac{t : nat \qquad M_z : A(z)\text{ true} \qquad \dfrac{\dfrac{}{n : nat} \quad \dfrac{}{f\ n : A(n)\text{ true}}ih}{\ddots \quad \vdots}\ \ M_s : A(s\ n)\text{ true}}{rec(t, M_z, n, ih, M_s) : A(t)\text{ true}}nat\ E^{n,ih}$

Write rec term as $rec\ t$ with $f\ z \to M_z \mid f(s\ n) \to M_s$. Program for our ex: $\lambda a : nat.rec\ a$ with $f\ z \to le\_z\ z \mid f\ s\ n \to$

$(le\_s\ n\ n)(f\ n)$

$\dfrac{\dfrac{}{\mathcal{Y}\vdash \forall x:nat.x=x}\text{refl}}{\mathcal{Y}\vdash z=z}\forall E$ $\dfrac{\dfrac{}{\mathcal{Y}'\vdash \forall x:nat.x=x}\text{refl}\quad \dfrac{\mathcal{Y}'\vdash n:nat}{\mathcal{Y}'\vdash s\ n:nat}}{\mathcal{Y}',u:\neg(s\ n=z):s\ n=s\ n}\forall E$

The program
$\mathcal{Y}\vdash\forall x:nat.\neg(x=z)\supset\exists y:nat.\ s\ y=x$ can be written as:
$\lambda a:nat.rec\ a$ with $f\ z\to\lambda u:\neg(z=z).abort(u\ (refl\ z))\mid f\ (s\ n)\to\lambda u:\neg(s\ n=z).\langle ref\ (s\ n),n\rangle$.
If we erase proofs for equality, we get:
$\lambda a:nat.rec\ a$ with $f\ z\to\_\mid f(s\ n)\to n$, predecessor function!
Reduction rules: $(rec\ z$ with $f\ z\to M_z\mid f\ (s\ n)\to M_s)\implies M_z$
$(rec\ (s\ m)$ with $f\ z\to M_z\mid f\ (s\ n)\to M_s)\implies[m/n,f_m/f_n]M_s$, where $f_m=rec\ m$ with $f\ z\to M_z\mid f\ (s\ n)\to M_s$
Cong rules are just $N_z\implies N_z'$ and corresponding change for rec. Similarly for N_s.
Proving subject red. $M\implies M'$ and $\Gamma\vdash M:C$ then $\Gamma\vdash M':C$. Pf on structural ind $M\implies M'$
Case: $\ldots\implies[m/n,f_m/f_n]M_s$
$\Gamma\vdash rec\ (s\ m)$ with $f\ z\to M_z\mid f\ (s\ n)\to M_s:C$ by ass
$\Gamma\vdash s\ m:nat,\Gamma\vdash M_z:A(z)$
$\Gamma,n:nat,f\ n:A(n)\vdash M_s:A(s\ n)$ by inv on natE
$\Gamma\vdash m:nat$ nat I_s
$\Gamma\vdash rec\ m$ with $f\ z\to M_z\mid f\ (s\ n)\to M_s:A(m)$ natE
$[m/n,f_m/f_n]M_s:A(s\ m)$ by subs lemma 2x
Case: $N_z\implies N_z'\ldots$
$\Gamma\vdash rec\ m$ with $f\ z\to N_z\mid f\ (s\ n)\to N_s:C$ by ass
$\Gamma\vdash m:nat$
$\Gamma,n:nat,f\ n:A(n)\vdash N_s:A(s\ n)$
$\Gamma\vdash N_Z:A(z)$ by inv natE
$\Gamma\vdash N_z':A(z)$ by IH
$\Gamma\vdash rec\ m$ with $f\ z\to N_z'\mid f\ (s\ n)\to N_s:C$

7 Normal Proofs

Normal terms: $M:=\lambda x:A.M\mid\langle M,N\rangle\mid inl^A\ M\mid inl^B\ M\mid R$
Neutral terms: $R:=fst\ R\mid snd\ R\mid x\mid R\ M$
Normal term cannot be reduced further
$\Gamma^\downarrow\vdash M:A\uparrow$, there is normal deriv
$\Gamma^\downarrow\vdash R:A\downarrow$, there is neutral deriv
$\uparrow$ means apply intro-rules bottom up, saying we have a proof for this, $\downarrow$ means synthesizing info top down from ass. Elim rules usually $\downarrow$, intro rules usually $\uparrow$

Rules: $\dfrac{x:A\downarrow}{\Gamma^\downarrow\vdash x:A\downarrow}$ $\dfrac{\Gamma^\downarrow,x:A\downarrow\vdash M:B\uparrow}{\Gamma^\downarrow\vdash\lambda x.M:A\supset B\uparrow}\supset I^x$

$\dfrac{\Gamma^\downarrow\vdash M:A\uparrow\quad\Gamma^\downarrow\vdash N:B\uparrow}{\Gamma^\downarrow\vdash\langle M,n\rangle:A\wedge B\uparrow}\wedge I$ $\dfrac{\Gamma^\downarrow\vdash R:A\wedge B\downarrow}{\Gamma^\downarrow\vdash fst\ R:A\downarrow}$ $\dfrac{\Gamma^\downarrow\vdash R:A\wedge B\downarrow}{\Gamma^\downarrow\vdash snd\ R:B\downarrow}$

$\dfrac{\Gamma^\downarrow\vdash R:A\supset B\downarrow\quad\Gamma^\downarrow\vdash M:A\uparrow}{\Gamma^\downarrow\vdash R\ M:B\downarrow}$ $\dfrac{\Gamma^\downarrow\vdash M:A\uparrow}{\Gamma^\downarrow\vdash inl\ M:A\vee B\uparrow}$

$\dfrac{\Gamma^\downarrow\vdash R:A\vee B\downarrow\quad\Gamma^\downarrow,x:A\downarrow\vdash N_1:C\uparrow\quad\Gamma^\downarrow,x:B\downarrow\vdash N_2:C\uparrow}{\Gamma^\downarrow\vdash case\ R\ of\ inl\ x\to N_1\mid inr\ x\to N_2:C\uparrow}$

$\dfrac{\Gamma^\downarrow\vdash R:A\downarrow}{\Gamma^\downarrow\vdash R:A\uparrow}\uparrow\downarrow$ System is sound. If $\Gamma^\downarrow\vdash M:A\uparrow$ then $\Gamma\vdash M:A$. If $\Gamma^\downarrow\vdash R:A\downarrow$ then $\Gamma\vdash R:A$. Prove by mutual structural induction on 1st deriv (two IHs).
To make this complete, need to add other direction: $\dfrac{\Gamma^\downarrow\vdash M:A\uparrow}{\Gamma^\downarrow\vdash(M:A):A\downarrow}$
This will make proofs non-normal but allows us to prove completeness. If $\Gamma\vdash M:A$ then $\Gamma^\downarrow\vdash M:A\uparrow$ and $\Gamma^\downarrow\vdash M:A\downarrow$.
Proof by ind on $\Gamma\vdash M:A$.

8 Sequent Calculus

Rules: $\dfrac{u:A\in\Gamma}{\Gamma\implies A}\text{init}$ $\dfrac{\Gamma\implies A\quad\Gamma\implies B}{\Gamma\implies A\wedge B}\wedge R$

$\dfrac{\Gamma,u:A\wedge B,w:A\implies C}{\Gamma,u:A\wedge B\implies C}\wedge L_1$ $\dfrac{\Gamma,u:A\wedge B,w:B\implies C}{\Gamma,u:A\wedge B\implies C}\wedge L_2$

$\dfrac{\Gamma,u:A\implies B}{\Gamma\implies A\supset B}\supset R^u$ $\dfrac{\Gamma,u:A\supset B,w:B\implies C\quad\Gamma,u:A\supset B\implies A}{\Gamma,u:A\supset B\implies C}\supset L$

$\dfrac{}{\Gamma\implies T}TR$ $\dfrac{}{\Gamma,u:\bot\implies C}\bot L$ $\dfrac{\Gamma\implies A}{\Gamma\implies A\vee B}\vee R_1$ $\dfrac{\Gamma\implies B}{\Gamma\implies A\vee B}\vee R_2$

$\dfrac{\Gamma,u:A\vee B,v:A\implies C\quad\Gamma,u:A\vee B,w:B\implies C}{\Gamma,u:A\vee B\implies C}\vee L^{v,w}$

$\dfrac{\Gamma\implies A(a)}{\Gamma\implies\forall x:\tau.A(x)}\forall^a R$ $\dfrac{\Gamma\vdash t:\tau\quad\Gamma,u:\forall x:\tau.A(x),w:A(t)\implies C}{\Gamma,u:\forall x:\tau.A(x)\implies C}\forall L$

$\dfrac{\Gamma\vdash t:\tau\quad\Gamma\implies A(t)}{\Gamma\implies\exists x:\tau.A(x)}\exists R$ $\dfrac{\Gamma,u:\exists x:\tau.A(x),w:A(a)\implies C}{\Gamma,u:\exists x:\tau.A(x)\implies C}\exists L$

Sound: If $\Gamma\implies A$ then $\Gamma^\downarrow\vdash A\uparrow$.
Induction on $\Gamma\implies A$
Completeness: If $\Gamma^\uparrow\vdash A\uparrow$ then $\Gamma\implies A$. To prove, show if $\Gamma^\downarrow\vdash A\downarrow$ and $\Gamma,A\implies C$ then $\Gamma\implies C$. $\uparrow\downarrow$ rule corresponds to cut rule.
Also have weakening and contraction for seq calc.

Cut: $\dfrac{\Gamma\implies A\qquad\Gamma,A\implies C}{\Gamma\implies C}$

Cut is admissible. If $\Gamma\overset{\mathcal{D}}{\implies}A$ and $\Gamma,\underline{A}\overset{\mathcal{E}}{\implies}C$ then $\Gamma\implies C$, where A is the principle formula/cut formula.
Case: A is principal formula of final inf for both (R) $\mathcal{D}$ and (L) $\mathcal{E}$.
Subcase: $A=A\wedge B$

$\mathcal{D}=\dfrac{\overset{\mathcal{D}_1}{\Gamma\implies A}\quad\overset{\mathcal{D}_2}{\Gamma\implies B}}{\Gamma\implies A\wedge B}$, $\mathcal{E}=\dfrac{\overset{\mathcal{E}'}{\Gamma,A\wedge B,A\implies C}}{\Gamma,A\wedge B\implies C}$

$\Gamma,A\implies A\wedge B$ by weak $\mathcal{D}$
$\mathcal{F}:\Gamma,A\implies C$ by IH $(A\wedge B,\mathcal{D},\mathcal{E}')$
$\Gamma\implies C$ by IH because $A<A\wedge B$ $(A,\mathcal{D}_1,\mathcal{F})$
One of the formulas has to be getting smaller.
Case: A not princ form of final inf in $\mathcal{D}$. So $\mathcal{D}$ must end in a left rule.

$\mathcal{D}=\dfrac{\overset{\mathcal{D}_1}{\Gamma',B_1\wedge B_2,B_1\implies A}}{\Gamma',B_1\wedge B_2\implies A}\wedge L_1$

$\Gamma=\Gamma',B_1\wedge B_2$ by ass
$\Gamma',B_1\wedge B_2,B_1\implies C$ IH $(A,\mathcal{D}_1,\mathcal{E})$
$\Gamma',B_1\wedge B_2\implies C\wedge L_1$
Case: A not princ form of final inf in $\mathcal{E}$. Can be R or L

Sub: $\mathcal{E}=\dfrac{\overset{\mathcal{E}_1}{\Gamma,A\implies C_1}\quad\overset{\mathcal{E}_2}{\Gamma,A\implies C_2}}{\Gamma,A\implies C_1\wedge C_2}\wedge R$

$\Gamma\implies C_1$, IH$(A,\mathcal{D},\mathcal{E}_1)$
$\Gamma\implies C_2$, IH$(A,\mathcal{D},\mathcal{E}_2)$
$\Gamma\implies C_1\wedge C_2$ by $\wedge$ R

Sub: $\mathcal{E}=\dfrac{\overset{\mathcal{E}_1}{\Gamma',B_1\wedge B_2,B_1,A\implies C}}{\Gamma',B_1\wedge B_2,A\implies C}\wedge L_1$

$\Gamma',B_1\wedge B_2,B_1\implies C$, IH $(A,\mathcal{D},\mathcal{E}_1)$
$\Gamma',B_1\wedge B_2\implies C$ by $\wedge L_1$
With cut elim, we show $\Gamma\vdash A\iff\Gamma\implies A$ (without cut)
$\implies$ no ND deriv for $\bot$, since no seq calc for $\bot$. If $\bot$ $A\vee B$ then A or B. There is no $\vdash A\vee\neg A$ for arbitrary A, because we'd need $\cdot\implies A$ or $\cdot\implies\neg A$, which means $A\implies\bot$. No rules for either.
For proof search, we sometimes have a choice of several rules to apply.
do-care non-determinism ($\vee R_1$, $\vee R_2$, $\supset$L, $\forall$ L, $\exists$ R)
don't-care non-determinism ($\wedge$ R, $\wedge L_1$, $\wedge L_2$, $\forall$ R, $\exists$ L), order we apply these in doesn't matter. For these rules we can prove inversion, i.e. If $\Gamma\implies A\wedge B$ then $\Gamma\implies A$ and $\Gamma\implies B$, etc.

9 Proof Search

Horn clause: $D:=P\mid G\supset P\mid\forall x:\tau.D$
Horn goal: $G:=P\mid G_1\wedge G_2$
Example theories: $e\_z:even\ z$, $e\_ab:edge\ a\ b$
To search: start with goal, apply inf rules backwards. If no more rules whose conclusion matches the goal at a step, fail. Because of non-determinism when choosing rules, we introduce uniform and focusing phases:
$\Delta\overset{u}{\implies}G$, with horn theory Δ we can prove G uniformly
$\Delta>D\overset{u}{\implies}G$, can prove G by focusing/backchaining on D
Alg is as follows: Apply init and $\wedge$ R until $\Delta\implies P$. Pick a clause from Δ and focus on it.

$\dfrac{\Delta\overset{u}{\implies}G_1\quad\Delta\overset{u}{\implies}G_2}{\Delta\overset{u}{\implies}G_1\wedge G_2}$ $\dfrac{\Delta>D\implies P\quad D\in\Delta}{\Delta\overset{u}{\implies}P}$

$\dfrac{P\in\Delta}{\Delta>P\implies P}$ $\dfrac{\Delta>[t/x]\mathcal{D}\implies P}{\Delta>\forall x:\tau.D\implies P}$

$\dfrac{\Delta,G\supset P\implies G\quad\Delta>G\supset P,P\implies P'}{\Delta>G\supset P\implies P'}$

Soundness: If $\Delta\overset{u}{\implies}G$ then $\Delta\implies G$. If $\Delta>D\implies P$ then $\Delta,D\implies P$.
Completeness: If $\Delta\implies G$ then $\Delta\overset{u}{\implies}G$. If $\Delta\implies P$ then $\Delta>D\implies P$ for $D\in\Delta$. Completeness requires the postponement lemma:
Postponement lemma: If $\Delta,G_1\supset P_1\overset{u}{\implies}G_1$ and $\Delta,G_1\supset P_1,P_1\overset{u}{\implies}G$ then $\Delta,G_1\supset P_1\overset{u}{\implies}G$. If $\Delta,G\supset Q,Q>D'\implies P$ and $\Delta,G\supset Q\overset{u}{\implies}G$ then $\Delta,G\supset Q>D'\implies P$.
HHF allows all formulas to be goals (not only atomic).
$F:=P\mid F_1\supset F_2\mid\forall x:\tau.F$

$\dfrac{\Delta\overset{u}{\implies}[a/x]F}{\Delta\overset{u}{\implies}\forall x:\tau.F}\forall R^a$ $\dfrac{\Delta,u:F_1\overset{u}{\implies}F_2}{\Delta\overset{u}{\implies}F_1\supset F_2}$ $\dfrac{\Delta>F\implies P}{\Delta\overset{u}{\implies}P}F\in\Delta$

$\dfrac{}{\Delta>P\implies P}$ $\dfrac{\Delta>[t/x]F\implies P}{\Delta>\forall x:\tau.F\implies P}$ $\dfrac{\Delta\overset{u}{\implies}F_1\quad\Delta>F_2\implies P}{\Delta>F_1\supset F_2\implies P}$

ND to HHF:
nd_topI: nd top.
nd_andI: $\forall A:prop.\forall B:prop.nd\ A\supset nd\ B\supset nd(and\ A\ B)$
nd_impI: $\forall A:prop.\forall B:prop.(nd\ A\supset nd\ B)\supset nd\ (imp\ A\ B)$
nd_orE: $\forall A:prop.\forall B:prop.\forall C:prop.nd\ (or\ A\ B)\supset(nd\ A\supset nd\ C)\supset(nd\ B\supset nd\ C)\supset nd\ C$

10 Modal Logic(S4)

Logic in a world. Have reflexivity + transitivity.
Validity: If $\cdot\vdash A$ true then $\vdash A$ valid. If $\vdash A$ valid then $\vdash A$ true.

$\dfrac{x:A\text{ true}\in\Gamma}{\Delta;\Gamma\vdash x:A\text{ true}}$ $\dfrac{u:A\text{ valid}\in\Delta}{\Delta;\Gamma\vdash u:A\text{ true}}$ $\dfrac{\Delta;\cdot\vdash M:A\text{ true}}{\Delta;\Gamma\vdash box\ M:\Box A\text{ true}}\Box I$

$\dfrac{\Delta;\Gamma\vdash M:\Box A\text{ true}\qquad\Delta,u:A\text{ valid};\Gamma\vdash N:C\text{ true}}{\Delta;\Gamma\vdash let\ box\ u=M\ in\ N:C\text{ true}}\Box E$

Substitution: If $\Delta;\Gamma\vdash A$ true and $\Delta;\Gamma,A$ true$,\Gamma'\vdash C$ true then $\Delta;\Gamma,\Gamma'\vdash C$ true. If $\Delta;\cdot\vdash B$ true and Δ,B valid$,\Delta';\Gamma\vdash C$ true then $(\Delta,\Delta');\Gamma\vdash C$ true
Contextual: $[\psi]A$ means A is true in every world where we have assumptions ψ or $\Box(\psi\supset A)$.

$\dfrac{x:A\in\Gamma}{\Delta;\Gamma\vdash x:A}$ $\dfrac{u:[\psi]A\in\Delta\qquad\Delta;\Gamma\vdash\sigma:\psi}{\Delta;\Gamma\vdash\text{clo}(u,\sigma):A}\text{hyp}^*$

$\dfrac{\Delta;\Gamma\vdash M_1:A_1\quad\ldots\quad\Delta;\Gamma\vdash M_n:A_n}{\Delta;\Gamma\vdash\underbrace{M_1/x_1\ldots M_n/x_n}_{\sigma}:\underbrace{\psi}_{x_1:A_1\ldots x_n:A_n}}$ $\dfrac{\Delta;\psi\vdash M:A}{\Delta;\Gamma\vdash\text{box}(\psi.M):[\psi]A}\Box I$

$\dfrac{\Delta;\Gamma\vdash M:[\psi]A\qquad\Delta,u:[\psi]A;\Gamma\vdash N:C}{\Delta;\Gamma\vdash\text{let box }u=M\ in\ N:C}\Box E$

Example proof and term:

$$\dfrac{\dfrac{}{\Gamma_x\vdash[C]A\text{ true}}\qquad\dfrac{\dfrac{\dfrac{\dfrac{}{\Delta_u;\Gamma_x,y_1:D\text{ true},y_2:C\text{ true}\vdash C\text{ true}}\text{hyp}^*}{\Delta_u;\Gamma_x,y_1:D\text{ true},y_2:C\text{ true}\vdash A\text{ true}}\Box I}{\Delta_u;\Gamma_x,y_1:D\text{ true}\vdash[C]A\text{ true}}\Box I}{\overbrace{u:[C]A\ valid}^{\Delta_u};\Gamma_x\vdash[D][C]A\text{ true}}}{\dfrac{\overbrace{x:[C]A\ true}^{\Gamma_x}\vdash[D][C]A\text{ true}}{\vdash[x_2:C]A\supset[y_1:D][y_2:C]A\text{ true}}\supset I^x}\Box E^u$$

$\lambda x:[x_2:C]A.let\ box\ u=x\ in\ box(y_1.box(y_2.clo(u,[y_2/x_2])))$
From bottom up, do $\supset$ I and then all let boxes ($\Box$ E) before you introduce box, as you'll lose the vars.
$let\ box\ u=box(\psi.M)\ in\ N\implies[\![\psi.M/u]\!]N$
Note that we define substitution: $[M/x](box(\psi.N))=box(\psi.N),[M/x](let\ box\ u=N_1\ in\ N_2)=let\ box\ u=[M/x]N_1\ in\ [M/x]N_2,u\notin FMV(M),[M/x](clo(u,\sigma))=clo(u,[M/x]\sigma)$. $[\![\psi.M/u]\!](\lambda y.N)=\lambda y.[\![\psi.M/u]\!]N,[\![\psi.M/u]\!](box(\phi.N))=box(\phi.[\![\psi.M/u]\!]N),[\![\psi.M/u]\!](let\ box\ v=N_1\ in\ N_2)=let\ box\ v=[\![\psi.M/u]\!]N_1\ in[\![\psi.M/u]\!]N_2,v\notin FMV(M),[\![\psi.M/u]\!]clo(v,\sigma)=clo(v,[\![\psi.M/u]\!]\sigma)$
$\supset$ L, $\supset$ R and $\dfrac{\Delta;\psi\implies A}{\Delta;\Gamma\implies[\psi]A}\Box R$ $\dfrac{}{\Delta;\Gamma,A\implies A}\text{init}$

$\dfrac{\Delta,u:[\psi]A;\Gamma,x:[\psi]A\implies C}{\Delta;\Gamma,x:[\psi]A\implies C}\Box L$

$\dfrac{(\Delta,u:[\psi]A);\Gamma\implies\psi\qquad\Delta,u:[\psi]A;\Gamma,A\implies C}{\Delta,u:[\psi]A;\Gamma\implies C}\text{reflect}$

Implicit box: $\dfrac{x:A\in\Gamma}{\Psi;\Gamma\vdash x:A}$ $\dfrac{\Psi;\Gamma;\cdot\vdash M:A}{\Psi;\Gamma\vdash box\ M:\Box A}$

$\dfrac{\Psi;\Gamma\vdash M:\Box A}{\Psi;\Gamma;\Gamma_1;\ldots;\Gamma_n\vdash unbox_n\ M:A}$ $\dfrac{\Psi;\Gamma\vdash M:\Box A}{\Psi;\Gamma\vdash unbox_0\ M:A}$

Context fusion/modal fusion: If $\Psi;\Gamma;\Gamma';\Psi'\vdash C$ true then $\Psi;(\Gamma,\Gamma');\Psi'\vdash C$ true
Possibility: A true, then A possible. If A possible and if ass A then C possible, then C poss.

$\dfrac{\Delta;\Gamma\vdash M:\diamond A\qquad\Delta;x:A\vdash E\div C\text{ poss}}{\Delta;\Gamma\vdash let\ dia\ x=M\ in\ E\div C\text{ poss}}$ $\dfrac{\Delta;\Gamma\vdash E\div A\text{ poss}}{\Delta;\Gamma\vdash dia\ E:\diamond A}$ $\dfrac{\Delta;\Gamma\vdash M:A}{\Delta;\Gamma\vdash M\div A\text{ poss}}$

$let\ dia\ x=dia\ E\ in\ F\implies\langle E/x\rangle F$
Linear logic, no weak or contrac.
If $\Delta\vdash A$ true and Δ',A true $\vdash C$ true then $\Delta,\Delta'\vdash C$ true.

$\dfrac{\Delta_1\vdash A\text{ true}\qquad\Delta_2\vdash B\text{ true}}{\Delta_1,\Delta_2\vdash A\otimes B\text{ true}}$ $\dfrac{\Delta_1\vdash A\otimes B\text{ true}\qquad\Delta_2,A\text{ true},B\text{ true}\vdash C\text{ true}}{\Delta_1,\Delta_2\vdash C\text{ true}}$

$\dfrac{\Delta\vdash A\text{ true}\qquad\Delta\vdash B\text{ true}}{\Delta\vdash A\&B\text{ true}}$ $\dfrac{\Delta\vdash A\&B\text{ true}}{\Delta\vdash A\text{ true}}$ $\dfrac{\Delta\vdash A\&B\text{ true}}{\Delta\vdash B\text{ true}}$

$\dfrac{\Delta,A\text{ true}\vdash B\text{ true}}{\Delta\vdash A\multimap B\text{ true}}$ $\dfrac{\Delta_1\vdash A\multimap B\text{ true}\qquad\Delta_2\vdash A\text{ true}}{\Delta_1,\Delta_2\vdash B\text{ true}}$

$\dfrac{\Delta\vdash A\text{ true}}{\Delta\vdash A\oplus B\text{ true}}$ $\dfrac{\Delta\vdash B\text{ true}}{\Delta\vdash A\oplus B\text{ true}}$

$\dfrac{\Delta'\vdash A\oplus B\text{ true}\qquad\Delta,A\text{ true}\vdash C\text{ true}\qquad\Delta,B\text{ true}\vdash C\text{ true}}{\Delta,\Delta'\vdash C\text{ true}}$

$\dfrac{\Gamma;\cdot\vdash A\text{ true}}{\Gamma;\cdot\vdash!A\text{ true}}$ $\dfrac{\Gamma;\Delta\vdash!A\text{ true}\qquad\Gamma,A\text{ valid};\Delta'\vdash C\text{ true}}{\Gamma;(\Delta,\Delta')\vdash C\text{ true}}$

$\dfrac{}{\Delta\vdash\mathrm{T}\text{ true}}$ $\dfrac{}{\cdot\vdash1\text{ true}}$ $\dfrac{\Delta\vdash1\text{ true}\qquad\Delta'\vdash C\text{ true}}{\Delta,\Delta'\vdash C\text{ true}}$

T consumes all resources, 1 requires none, optional. &, internal choice, we choose. $\oplus$, external choice, something else chooses.