Type Systems as a Foundation for Reliable Computing

Robert Harper
Carnegie Mellon University

Summer School on Reliable Computing
University of Oregon
July, 2005

References

These lectures are based on the course *Constructive Logic* at Carnegie Mellon University. The course materials are available at the course web site:

`http://www.cs.cmu.edu/~rwh/courses/logic/www.`

The primary reference is Frank Pfenning's notes *Constructive Logic*, supplemented by the additional notes and references on the course readings page.

The following sources are especially relevant to these lectures:

1. J.-Y. Girard, *Proofs and Types*, Cambridge University Press, 1989.
2. P. Martin-Löf, *Intuitionistic Type Theory*, Bibliopolis Press, 1984.
3. B. C. Pierce, *Types and Programming Languages*, MIT Press, 2002.

Lecture 1: Intuitionistic Propositional Logic

1. Judgements and evidence.
   (a) Analytic = self-evident.
   (b) Synthetic = requires evidence.
2. Categorical judgements of IPL:
   (a) $P\ \mathsf{prop}$: analytic.
   (b) $P\ \mathsf{true}$: synthetic.
3. Hypothetical judgements: $J_1, \ldots, J_n \vdash J$.
   (a) Evidence consists of an "open" proof of J from hypotheses $J_1, \ldots, J_n$.

(b) Admissibility of the structural rules.

i. Reflexivity/assumption:

$$\frac{}{\Gamma, J \vdash J}$$

ii. Transitivity/substitution:

$$\frac{\Gamma \vdash J \quad \Gamma, J \vdash J'}{\Gamma \vdash J'}$$

iii. Weakening:

$$\frac{\Gamma \vdash J}{\Gamma, \Gamma' \vdash J}$$

iv. Contraction:

$$\frac{\Gamma, J, J \vdash J'}{\Gamma, J \vdash J'}$$

v. Permutation:

$$\frac{\Gamma, J', J, \Gamma' \vdash J''}{\Gamma, J, J', \Gamma' \vdash J''}$$

(c) Linear logic denies weakening and contraction; strict/relevance logic denies weakening; affine logic denies contraction; ordered logic denies permutation, weakening, and contraction.

4. Defining connectives:

(a) Introduction rules determine *canonical* evidence.

(b) Elimination rules exploit arbitrary evidence.

(c) Inversion principles: coherence of introduction and elimination.

5. Inference rules of IPL:

(a) The propositional connectives: $\top$, $\bot$, $P \wedge Q$, $P \supset Q$, $P \vee Q$, $\neg P$.

(b) Definability of connectives.

6. Algebraic structure of IPL.

(a) Entailment relation as a pre-order.

(b) Connectives specify algebraic structure called a *Heyting algebra*.

(c) IPL is sound and complete for interpretation into HA's.

Lecture 2: Proof Terms and Normal Proofs

1. IPL in analytic form.
   (a) Categorical judgements, revisited:
      i. $P\,\mathsf{prop}$: as before.
      ii. $M : P$: M is a proof of P.
   (b) Hypothetical judgements, revisited:
      i. $u_1{:}P_1, \ldots, u_n{:}P_n \vdash M : P$.
      ii. Structural rules.
   (c) Propositions as types principle:
      i. Propositions may be viewed as *types* of their proofs.
      ii. Proofs are λ-terms classified by propositions.
2. Normal and neutral proofs.
   (a) Idea: codify "direct" proofs.
      i. No digressions: no elimination of intro.
      ii. Sub-formula property.
   (b) Two relations (second is auxiliary):
      i. $\Gamma \vdash M \searrow P$: M is a normal proof of P.
      ii. $\Gamma \vdash M \nearrow P$: M is a neutral proof of P.
3. Independence results.
   (a) To show that P is not provable (from given assumptions Γ), show that there is no normal proof of P.
   (b) Examples
      i. LEM: $\neg\neg \mathit{LEM}\,\mathsf{true}$, so $\neg \mathit{LEM}\,\mathsf{true}$ is not provable. LEM is not provable either.
      ii. DNE: similar story.

Lecture 3: Normalization for the Multiplicative Fragment

1. Normalization and neutralization.
   (a) Show that every proof may be brought into normal form.
   (b) Head reduction and head normalization.
   (c) Two relations:
      i. $\Gamma \vdash M : P \searrow N$: N is the normal form of M.

ii. $\Gamma \vdash M \nearrow N : P$: N is the neutral form of M, where M is head-irreducible and of atomic type.

(d) Easy: if $\Gamma \vdash M : P \searrow N$, then $\Gamma \vdash N \searrow P$.

(e) Harder: if $\Gamma \vdash M : P$ then there exists N such that $\Gamma \vdash M : P \searrow N$.

2. Theorem: if $\Gamma M : P$, then there exits N such that $\Gamma \vdash M : P \searrow N$.

   (a) Obvious strategy: induction on derivation of antecedent.

      i. Need to make some assumption about hypotheses.

      ii. Need to ensure closure under typing rules.

   (b) Solution: strengthen the induction hypothesis. (Tait's Method aka logical relations).

      i. Show that well-formed proofs are *computable*.

      ii. Show that computable terms are normalizable.

3. Complications with additive fragment (summary):

   (a) Commuting conversions for case and abort.

   (b) Maintaining the sub-formula property for normal forms.

Lecture 4: Types and Programming Languages

1. Evaluation for PL's is a form of weak head reduction.

   (a) Restricted to closed terms; don't evaluate under binders.

   (b) Choice of whether to evaluate components of pairs, arguments to injections, arguments to applications.

   (c) Type safety: closed values have canonical form.

   (d) Transition system characterization of evaluation.

      i. SOS and its relation to ES.

      ii. Progress and preservation formulation of type safety.

2. Scaling up logical type theory.

   (a) Data types as domains of quantification.

      i. Judgements: τ type, $t \in \tau$.

      ii. Natural numbers, inductive types in general.

      iii. Streams, coinductive types in general.

      iv. Type of propositions, types of proofs.

      v. Closure properties for types: sums, products, functions.

   (b) Quantifier logic: $\forall, exists$ over a type.

      i. First-order arithmetic as quantification over the type nat.

ii. Second-order logic as quantification over the type prop.
iii. No traditional logic quantifies over proofs!
iv. Props-as-types, revisited. Status of existential quantification?

(c) Intuitionistic modal logics.
i. IS4: necessity and possiblity.
ii. Lax logic: weak notions of truth as possible necessity.

(d) Classical logic.
i. Two judgements: P true and P false.
ii. Symmetric axiomatization.
iii. Proof terms, tie-breaking.

3. Scaling up types for programming languages.

(a) General recursive types.
i. No positivity restrictions.
ii. Introduces non-termination.

(b) Second-order quantification:
i. Universal: polymorphism.
ii. Existential: data abstraction.

(c) Lax modality as a monad.
i. P lax means P is stably true after alteration of world.
ii. Expression / term distinction.

(d) Control via classical logic.
i. Classical logic adds call/cc and throw.
ii. Exposes computational content of classical logic.

Normal and Neutral Proofs

$$\frac{\Gamma \vdash V \nearrow \alpha}{\Gamma \vdash V \searrow \alpha}$$

$$\frac{}{\Gamma \vdash * \searrow \top} \qquad \frac{\Gamma \vdash V \nearrow \bot}{\Gamma \vdash V \searrow \bot}$$

$$\frac{\Gamma \vdash N_1 \searrow P_1 \quad \Gamma \vdash N_2 \searrow P_2}{\Gamma \vdash \langle N_1, N_2 \rangle \searrow P_1 \wedge P_2} \qquad \frac{\Gamma, x{:}P_1 \vdash N_2 \searrow P_2}{\Gamma \vdash \lambda x{:}P_1.N_2 \searrow P_1 \supset P_2}$$

$$\frac{\Gamma \vdash N_1 \searrow P_1}{\Gamma \vdash \mathsf{inl}(N_1) \searrow P_1 \vee P_2} \qquad \frac{\Gamma \vdash N_2 \searrow P_2}{\Gamma \vdash \mathsf{inr}(N_2) \searrow P_1 \vee P_2}$$

$$\frac{\Gamma \vdash V \nearrow P_1 \vee P_2 \quad \Gamma, x{:}P_1 \vdash N_1 \searrow Q \quad \Gamma, x{:}P_2 \vdash N_2 \searrow Q}{\Gamma \vdash \mathsf{case}\, V \,\{\, \mathsf{inl}(x) \Rightarrow N_1 \mid \mathsf{inr}(x) \Rightarrow N_2 \,\} \searrow Q}$$

$$\frac{}{\Gamma, x{:}P \vdash x \nearrow P}$$

$$\frac{\Gamma \vdash V \nearrow P_1 \wedge P_2}{\Gamma \vdash \mathsf{fst}(V) \nearrow P_1} \qquad \frac{\Gamma \vdash V \nearrow P_1 \wedge P_2}{\Gamma \vdash \mathsf{snd}(V) \nearrow P_2}$$

$$\frac{\Gamma \vdash V \nearrow P_1 \supset P_2 \quad \Gamma \vdash N \searrow P_2}{\Gamma \vdash V\, N \nearrow P_2} \qquad \frac{\Gamma \vdash V \nearrow \bot}{\Gamma \vdash \mathsf{abort}(V) \nearrow P}$$

Proof Normalization (Multiplicative Fragment)

Weak Head Reduction and Weak Head Normalization

$$\frac{}{\mathsf{fst}(\langle M_1, M_2 \rangle) \Rightarrow M_1} \qquad \frac{}{\mathsf{snd}(\langle M_1, M_2 \rangle) \Rightarrow M_2}$$

$$\frac{M \Rightarrow M'}{\mathsf{fst} M \Rightarrow \mathsf{fst} M'} \qquad \frac{M \Rightarrow M'}{\mathsf{snd} M \Rightarrow \mathsf{snd} M'}$$

$$\frac{}{(\lambda x{:}P.M_2)\, M_1 \Rightarrow [M_1/x]M_2} \qquad \frac{M_1 \Rightarrow M_1'}{M_1\, M_2 \Rightarrow M_1'\, M_2}$$

$$\text{whnf} \quad W \quad ::= \quad x \mid \mathsf{fst}(W) \mid \mathsf{snd}(W) \mid W\, M$$

$$\frac{}{W \Downarrow W} \qquad \frac{M \Rightarrow M' \quad M' \Downarrow W}{M \Downarrow W}$$

Lemma 1
If $M \Downarrow W_1$ and $M \Downarrow W_2$, then $W_1 = W_2$.

Normalization and Neutralization

$$\begin{array}{lrcl} \textit{normal} & N & ::= & V \mid * \mid \langle N_1, N_2 \rangle \mid \lambda x{:}P.N \\ \textit{neutral} & V & ::= & x \mid \mathsf{fst}(V) \mid \mathsf{snd}(V) \mid V\ N \end{array}$$

$$\frac{M \Downarrow W \quad \Gamma \vdash W \nearrow V : \alpha}{\Gamma \vdash M : \alpha \searrow V}$$

$$\frac{\Gamma \vdash \mathsf{fst}(M) : P \searrow N_1 \quad \Gamma \vdash \mathsf{snd}(M) : Q \searrow N_2}{\Gamma \vdash M : P \wedge Q \searrow \langle N_1, N_2 \rangle}$$

$$\frac{}{\Gamma \vdash M : \top \searrow *}$$

$$\frac{\Gamma, x{:}P \vdash M\ x : Q \searrow N}{\Gamma \vdash M : P \supset Q \searrow \lambda x{:}P.N}$$

$$\frac{\Gamma(x) = P}{\Gamma \vdash x \nearrow x : P}$$

$$\frac{\Gamma \vdash W \nearrow V : P \wedge Q}{\Gamma \vdash \mathsf{fst}(W) \nearrow \mathsf{fst}(V) : P}$$

$$\frac{\Gamma \vdash W_1 \nearrow V_1 : P \supset Q \quad \Gamma \vdash M_2 : P \searrow N_2}{\Gamma \vdash W_1\ M_2 \nearrow V_1\ N_2 : Q}$$

$$\frac{\Gamma \vdash W \nearrow V : P \wedge Q}{\Gamma \vdash \mathsf{snd}(W) \nearrow \mathsf{snd}(V) : P}$$

Lemma 2 (Determinacy)

1. *If* $\Gamma \vdash M : P \searrow N_1$ *and* $\Gamma \vdash M : P \searrow N_2$, *then* $N_1 = N_2$.
2. *If* $\Gamma \vdash W \nearrow V_1 : P_1$ *and* $\Gamma \vdash W \nearrow V_2 : P_2$, *then* $V_1 = V_2$ *and* $P_1 = P_2$.

Lemma 3 (Monotonicity)

1. *If* $\Gamma \vdash M : P \searrow N$ *and* $\Gamma' \supseteq \Gamma$, *then* $\Gamma' \vdash M : P \searrow N$.
2. *If* $\Gamma \vdash W \nearrow V : P$ *and* $\Gamma' \supseteq \Gamma$, *then* $\Gamma' \vdash W \nearrow V : P$.

Logical Relations for Normalization

$M\ \mathsf{norm}\ \alpha\ [\Delta]$	*if*	*there exists* N *s.t.* $\Delta \vdash M : \alpha \searrow N$
$M\ \mathsf{norm}\ \top\ [\Delta]$	*if*	*true*
$M\ \mathsf{norm}\ P \wedge Q\ [\Delta]$	*if*	$\mathsf{fst}(M)\ \mathsf{norm}\ P\ [\Delta]$ *and* $\mathsf{snd}(M)\ \mathsf{norm}\ Q\ [\Delta]$
$M\ \mathsf{norm}\ P \supset Q\ [\Delta]$	*if*	*for all* $\Delta' \supseteq \Delta$, $M'\ \mathsf{norm}\ P\ [\Delta']$ *implies* $M\ M'\ \mathsf{norm}\ Q\ [\Delta']$
$\gamma\ \mathsf{norm}\ \Gamma\ [\Delta]$	*if*	*for all* $x \in dom(\Gamma)$, $\gamma(x)\ \mathsf{norm}\ \Gamma(x)\ [\Delta]$

Lemma 4 (Monotonicity)
If $M\ \mathsf{norm}\ P\ [\Delta]$ *and* $\Delta' \supseteq \Delta$, *then* $M\ \mathsf{norm}\ P\ [\Delta']$.

Proof: By induction on the structure of P. ■

Lemma 5 (Normal Paths Normalize)

1. *If* $M \,\mathsf{norm}\, P\ [\Delta]$, *then* $\Delta \vdash M : P \searrow N$ *for some* N.
2. *If* $\Delta \vdash W \nearrow P$, *then* $W \,\mathsf{norm}\, P\ [\Delta]$.

Proof: Simultaneously, by induction on the structure of P.

$P = \alpha$ Immediate from the definition of the predicate.

$P = \top$ Trivial.

$P = P_1 \wedge Q_1$

1. If $M \,\mathsf{norm}\, P\ [\Delta]$, then $\mathsf{fst}(M) \,\mathsf{norm}\, P_1\ [\Delta]$ and $\mathsf{snd}(M) \,\mathsf{norm}\, P_2\ [\Delta]$. So by induction $\Delta \vdash \mathsf{fst}(M) : P_1 \searrow N_1$ and $\Delta \vdash \mathsf{snd}(M) : P_2 \searrow N_2$, and hence $\Delta \vdash M : P \searrow \langle N_1, N_2 \rangle$.
2. If $\Gamma \vdash W \nearrow V : P$, then $\Gamma \vdash \mathsf{fst}(W) \nearrow \mathsf{fst}(V) : P_1$ and $\Gamma \vdash \mathsf{snd}(W) \nearrow \mathsf{snd}(V) : P_2$. So by induction $\mathsf{fst}(W) \,\mathsf{norm}\, P_1\ [\Delta]$ and $\mathsf{snd}(W) \,\mathsf{norm}\, P_2\ [\Delta]$, and hence $W \,\mathsf{norm}\, P\ [\Delta]$.

$P = P_1 \supset P_2$

1. Suppose $M \,\mathsf{norm}\, P\ [\Delta]$. We are to show $\Delta \vdash M : P \searrow N$ for some N. Let $\Delta' = \Delta, x{:}P_1$. It suffices to show $\Delta' \vdash M\,x : P_2 \searrow N_2$, for then we may take $N = \lambda x{:}P_1.N_2$. By induction $x \,\mathsf{norm}\, P_1\ [\Delta']$. By monotonicity $M \,\mathsf{norm}\, P\ [\Delta']$, so $M\,x \,\mathsf{norm}\, P_2\ [\Delta']$, so by induction $\Delta' \vdash M\,x : P_2 \searrow N_2$, as required.
2. Suppose $\Delta \vdash W \nearrow V : P$. Let $\Delta' \supseteq \Delta$ and suppose $M_1 \,\mathsf{norm}\, P_1\ [\Delta']$. By monotonicity $\Delta' \vdash W \nearrow V : P$, and by induction $\Delta' \vdash M_1 : P_1 \searrow N_1$, so $\Delta' \vdash W\,M : P_2 \searrow N_2$, and hence by induction $W\,M \,\mathsf{norm}\, P_2\ [\Delta']$ as required.

■

Therefore $x \,\mathsf{norm}\, P\ [\Delta, x{:}P]$, and hence $id_\Gamma \,\mathsf{norm}\, \Gamma\ [\Gamma]$.

Lemma 6 (Weak Head Expansion)
If $M \,\mathsf{norm}\, P\ [\Delta]$ *and* $M' \Rightarrow M$, *then* $M' \,\mathsf{norm}\, P\ [\Delta]$.

Proof: By induction on the structure of P. For example, if $P = P_1 \supset P_2$, then to show that $M' \,\mathsf{norm}\, P\ [\Delta]$ it suffices to show that $M'\,M_1 \,\mathsf{norm}\, P_2\ [\Delta']$ for any $\Delta' \supseteq \Delta$ and $M_1 \,\mathsf{norm}\, P_1\ [\Delta']$. Now since $M' \Rightarrow M$, it follows by monotonicity and the definition of weak head reduction that $M'\,M_1 \Rightarrow M\,M_1$, from which the result follows by an application of the inductive hypothesis. ■

Lemma 7 (Fundamental Lemma)
If $\Gamma \vdash M : P$ *and* $\gamma\, \mathsf{norm}\, \Gamma\ [\Delta]$, *then* $\hat{\gamma}(M)\, \mathsf{norm}\, P\ [\Delta]$.

Proof: By induction on the definition of $\Gamma \vdash M : P$. The case of a variable is covered by the assumption on γ. The elimination rules are immediate consequences of the inductive hypothesis and the definition of the normalizability predicate. The introduction rules are handled by the inductive hypothesis, the definition of normalizability, and the weak head expansion lemma. ■

Theorem 8 (Normalization)
If $\Gamma \vdash M : P$, *then* $\Gamma \vdash M : P \searrow N$ *for some* N.

Proof: Take $\gamma = id_\Gamma$. ■