Curry Howard Correspondence

Presented by
Siddharth Srivastava
with material from Harper, Sorensen & Urzyczyn, Goubault-Larrecq & Mackie

May 15, 2007

Classical Propositional Logic

Given a set $\mathcal{P}$ of proposition variables (atoms) construct formulas as:

$$\varphi ::= p|\varphi \vee \varphi|\varphi \wedge \varphi|\varphi \subset \varphi|\neg\varphi$$

p represents an atomic proposition e.g. “apples are blue”

Classical Logic: Semantics

Interpretation: $\rho : \mathcal{P} \rightarrow \{0, 1\}$

- $[\![p]\!]^\rho = \rho(p)$
- $[\![\phi \wedge \phi']\!]^\rho = [\![\phi]\!]^\rho \bar{\wedge} [\![\phi']\!]^\rho$
- $[\![\phi \vee \phi']\!]^\rho = [\![\phi]\!]^\rho \bar{\vee} [\![\phi']\!]^\rho$
- $[\![\phi \subset \phi']\!]^\rho = \bar{\neg}[\![\phi]\!]^\rho \bar{\vee} [\![\phi']\!]^\rho$
- $[\![\neg\phi]\!]^\rho = \bar{\neg}[\![\phi]\!]^\rho$

$\bar{\wedge}, \bar{\vee}, \bar{\neg}$ are operations on $\{0, 1\}$.

Classical Logic: Semantics (ctd)

- A formula ϕ is *valid* if $[\![\phi]\!]^\rho = 1$ for all ρ.
- A formula ϕ is *unsatisfiable* if $[\![\phi]\!]^\rho = 0$ for all ρ.

Thus $\phi \vee \neg\phi$ is valid for any ϕ.
Proof Systems attempt to determine the validity of a formula.

Classical Logic: Proof Theory

$\Gamma \vdash \phi$: under any interpretation, if all of Γ is true, then so is ϕ.
$\neg\phi$ is an abbreviation for $\phi \subset \bot$.
$\bot$ is an abbreviation for any formula of the form $\phi \wedge \neg\phi$

Natural Deduction

$$\frac{}{\Gamma, \phi \vdash \phi} \qquad \frac{\Gamma \vdash \phi_i}{\Gamma \vdash \phi_1 \vee \phi_2}\ i = 1, 2$$

$$\frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi} \qquad \frac{\Gamma \vdash \phi_1 \vee \phi_2 \quad \Gamma, \phi_1 \vdash \phi \quad \Gamma, \phi_2 \vdash \phi}{\Gamma \vdash \phi}\ i = 1, 2$$

$$\frac{\Gamma \vdash \phi_1 \wedge \phi_2}{\Gamma \vdash \phi_i}\ i = 1, 2 \qquad \frac{\Gamma \vdash \phi \quad \Gamma \vdash \neg\phi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \subset \psi} \qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash \neg\neg\phi}$$

$$\frac{\Gamma \vdash \phi \subset \phi' \quad \Gamma \vdash \phi}{\Gamma \vdash \phi'} \qquad \frac{\Gamma \vdash \neg\neg\phi}{\Gamma \vdash \phi}$$

Law of Excluded Middle

- Possible to obtain a proof of $\vdash \phi \vee \neg\phi$.
- Reflects the semantics: either a proposition or its negation is true, under any interpretation.
- Conflicts with existence of explicit proofs: don't need to have a proof for ϕ or $\neg\phi$ to assert this.
- Use the equivalence of ϕ and $\neg\neg\phi$.

The proof system is for asserting truth (falsity): not the existence of direct proofs!

Intuitionistic Logic: Proof Theory

Throw out the negation elimination axioms.

Natural Deduction for Intuitionistic Logic

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

$$\frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}$$

$$\frac{\Gamma \vdash \phi_1 \wedge \phi_2}{\Gamma \vdash \phi_i} \; i = 1, 2$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \subset \psi}$$

$$\frac{\Gamma \vdash \phi \subset \phi' \quad \Gamma \vdash \phi}{\Gamma \vdash \phi'}$$

$$\frac{\Gamma \vdash \phi_i}{\Gamma \vdash \phi_1 \vee \phi_2} \; i = 1, 2$$

$$\frac{\Gamma \vdash \phi_1 \vee \phi_2 \quad \Gamma, \phi_1 \vdash \phi \quad \Gamma, \phi_2 \vdash \phi}{\Gamma \vdash \phi} \; i = 1, 2$$

$$\frac{\Gamma \vdash \phi \quad \Gamma \vdash \neg\phi}{\Gamma \vdash \psi}$$

Again, $\neg\phi$ is an abbreviation for $\phi \subset \bot$.
This gives a completely different semantics!

Intuitionistic Logic: Semantics

- Instead of classical truth, intuitionistic logic deals with explicit provability.
- $\vdash \phi$ could be understood as "there is a proof for ϕ"
- $\vdash \phi \subset \bot$: "there is a refutation for ϕ".
- $(\phi \subset \bot) \subset \bot$ only indicates the absence of a refutation.

Intuitionistic Logic: Semantics

Kripke Frames

A Kripke Frame $\mathcal{F}$ is a tuple $(X, \leq, D, \models)$ such that:

- $(X, \leq)$ is a poset,
- D is a domain function associating sets of atoms to nodes of X.
- If $p \in D(x)$ and $x \leq y$ then $p \in D(y)$.
- The forcing relation $\models$ is defined using D:

$$\begin{array}{rcl}
x \models \phi \wedge \phi' & \textit{iff} & x \models \phi \text{ and } x \models \phi' \\
x \models \phi \vee \phi' & \textit{iff} & x \models \phi \text{ or } x \models \phi \\
x \models \phi \subset \phi' & \textit{iff} & \text{for all } y, x \leq y, y \models \phi \text{ implies } y \models \phi' \\
x \models \neg\phi & \textit{iff} & \text{for all } y, x \leq y, y \not\models \phi \\
x \models p & \textit{iff} & p \in D(x)
\end{array}$$

Intuitionistic Logic: Semantics

- ϕ is forced in a frame if every $x \in X$ forces it.
- ϕ is intuitionistically valid if it is forced in every frame.

Nodes of X can be seen as points of evidence; ϕ is "valid" if it has a proof in every frame.

Intuitionistic Logic: Explicit Proofs

Γ is a set of qualified formulas $x_i : \phi_i$.

$$\frac{}{\Gamma \vdash \texttt{true-i} : \top}$$

$$\frac{\Gamma \vdash p : \phi \quad \Gamma \vdash q : \psi}{\Gamma \vdash \texttt{and-i}(p, q) : \phi \wedge \psi}$$

$$\frac{\Gamma \vdash p : \phi \wedge \psi}{\Gamma \vdash \texttt{and-e-l}(p) : \phi}$$

$$\frac{\Gamma \vdash p : \phi \wedge \psi}{\Gamma \vdash \texttt{and-e-r}(p) : \psi}$$

$$\frac{\Gamma, x : \phi \vdash p : \psi}{\Gamma \vdash \texttt{imp-i}[\phi](x.p) : \phi \supset \psi}$$

$$\frac{\Gamma \vdash p : \phi \supset \psi \quad \Gamma \vdash q : \phi}{\Gamma \vdash \texttt{imp-e}(p, q) : \psi}$$

$$\frac{\Gamma \vdash p : \bot}{\Gamma \vdash \texttt{false-e}[\phi](p) : \phi}$$

$$\frac{\Gamma \vdash p : \phi}{\Gamma \vdash \texttt{or-i-l}[\psi](p) : \phi \vee \psi}$$

$$\frac{\Gamma \vdash p : \psi}{\Gamma \vdash \texttt{or-i-r}[\phi](p) : \phi \vee \psi}$$

$$\frac{\Gamma \vdash p : \phi \vee \psi \quad \Gamma, x : \phi \vdash q : \theta \quad \Gamma, y : \psi \vdash r : \theta}{\Gamma \vdash \texttt{or-e}[\phi, \psi](p, x.q, y.r) : \theta}$$

Curry Howard Isomorphism

- Curry Howard isomorphism ≡ rules on previous slide are remarkably familiar!
- These rules correspond to constructor and destructor rules for the usual terms: function abstractions, sums, products, and case expressions.

CH: Details

Proposition	*Type*
$\top$	`unit`
$\bot$	`void`
$\phi \wedge \psi$	$\phi^* \times \psi^*$
$\phi \supset \psi$	$\phi^* \to \psi^*$
$\phi \vee \psi$	$\phi^* + \psi^*$

CH: Details

Proof	*Program*
`true-i`	`triv`
`false-e`$[\phi](p)$	`abort`$[\phi^*](p^*)$
`and-i`(p,q)	`pair`(p^*,q^*)
`and-e-l`(p)	`fst`(p^*)
`and-e-r`(p)	`snd`(p^*)
`imp-i`$[\phi](x.p)$	`lam`$[\phi^*](x.p^*)$
`imp-e`(p,q)	`ap`(p^*,q^*)
`or-i-l`$[\psi](p)$	`inl`$[\psi^*](p^*)$
`or-i-r`$[\phi](p)$	`inr`$[\phi^*](p^*)$
`or-e`$[\phi,\psi](p,x.q,y.r)$	`case`$[\phi^*,\psi^*](p^*,x.q^*,y.r^*)$

CH: Illustration

$$\frac{\Gamma \vdash e : \tau_1 \quad \tau = \mathtt{sum}(\tau_1, \tau_2)}{\Gamma \vdash \mathtt{inl}[\tau](e) : \tau}\ \lambda - \mathit{calc}$$

$$\frac{\Gamma \vdash p : \phi}{\Gamma \vdash \mathtt{or\text{-}i\text{-}l}[\psi](p) : \phi \vee \psi}\ \mathit{logic}$$

$$\frac{\Gamma \vdash e : \mathtt{sum}(\tau_1, \tau_2) \quad \Gamma, x_1 : \tau_1 \vdash e_1 : \tau \quad \Gamma, x_2 : \tau_2 \vdash e_2 : \tau}{\Gamma \vdash \mathtt{case}[\tau_1, \tau_2](e, x_1.e_1, x_2.e_2) : \tau}\ \lambda - \mathit{calc}$$

$$\frac{\Gamma \vdash x : \phi_1 \vee \phi_2 \quad \Gamma, x_1 : \phi_1 \vdash q_1 : \phi \quad \Gamma, x_2 : \phi_2 \vdash q_2 : \phi}{\Gamma \vdash \mathtt{or\text{-}e}[\phi_1, \phi_2](x, x_1.q_1, x_2.q_2) : \phi}\ \mathit{logic}$$

Curry Howard Isomorphism (ctd.)

The correspondence can be extended along various dimensions:

term variable	assumption
term	construction (proof)
type variable	propositional variable
type	formula
type constructor	connective
inhabitation	provability
typable term	construction for a proposition
redex	construction representing proof tree with redundancy
reduction	normalization
value	normal construction

Extension to Classical Logic

3 kinds of terms:

- $x : \phi$, x proves ϕ
- $u \div \phi$, u refutes ϕ.
- $u \# x$, u is in contradiction with x

Encoding Classical Logic Proofs

$$\frac{\Delta;\Gamma \vdash k \div \phi \quad \Delta;\Gamma \vdash p : \phi}{\Delta;\Gamma \vdash k \# p}$$

$$\frac{}{\Delta, u \div \phi;\Gamma \vdash u \div \phi}$$

$$\frac{}{\Delta;\Gamma, x : \phi \vdash x : \phi}$$

$$\frac{\Delta, u \div \phi;\Gamma \vdash k \# p}{\Delta;\Gamma \vdash \mathtt{ccr}(u \div \phi . k \# p) : \phi}$$

$$\frac{\Delta;\Gamma, x : \phi \vdash k \# p}{\Delta;\Gamma \vdash \mathtt{ccp}(x : \phi . k \# p) \div \phi}$$

Rest of the rules are extensions of this notation...

Classical Logic Proofs: ctd.

$$\frac{}{\Delta;\Gamma \vdash \langle\rangle : \top}$$

$$\frac{}{\Delta;\Gamma \vdash \mathtt{abort} \div \bot}$$

$$\frac{\Delta;\Gamma \vdash p : \phi \quad \Delta;\Gamma \vdash q : \psi}{\Delta;\Gamma \vdash \langle p, q\rangle : \phi \wedge \psi}$$

$$\frac{\Delta;\Gamma \vdash k \div \phi \wedge \psi}{\Delta;\Gamma \vdash \mathtt{fst}; k \div \phi}$$

$$\frac{\Delta;\Gamma \vdash k \div \phi \wedge \psi}{\Delta;\Gamma \vdash \mathtt{snd}; k \div \psi}$$

$$\frac{\Delta;\Gamma, x : \phi \vdash p : \psi}{\Delta;\Gamma \vdash \lambda(x : \phi . p) : \phi \supset \psi}$$

$$\frac{\Delta;\Gamma \vdash p : \phi \quad \Delta;\Gamma \vdash k \div \psi}{\Delta;\Gamma \vdash \mathtt{app}(p); k \div \phi \supset \psi}$$

$$\frac{\Delta;\Gamma \vdash p : \phi}{\Delta;\Gamma \vdash \mathtt{inl}_{\psi}(p) : \phi \vee \psi}$$

$$\frac{\Delta;\Gamma \vdash p : \psi}{\Delta;\Gamma \vdash \mathtt{inr}_{\phi}(p) : \phi \vee \psi}$$

$$\frac{\Delta;\Gamma \vdash k \div \phi \quad \Delta;\Gamma \vdash l \div \psi}{\Delta;\Gamma \vdash \mathtt{case}(k, l) \div \phi \vee \psi}$$

$$\frac{\Delta;\Gamma \vdash k \div \phi}{\Delta;\Gamma \vdash \mathtt{not}(k) : \neg\phi}$$

$$\frac{\Delta;\Gamma \vdash p : \phi}{\Delta;\Gamma \vdash \mathtt{not}(p) \div \neg\phi}$$

Applications..

- Programs with implicit proofs.
- Proofs with computational content: algorithm extraction.

Manifesting these ideas requires several enhancements to the type theory... *Ωmega*, *Twelf*