Lecture 15: The Curry-Howard Correspondance

Polyvios Pratikakis

Computer Science Department, University of Crete

Type Systems and Static Analysis

Curry-Howard Correspondance

- Another use of λ-calculus
- Roughly:
  - Types correspond to theorems
  - Programs correspond to proofs
  - Typed languages correspond to logics
  - A typechecker is a proof verifier

Classical propositional logic

- Formulas of the form

$$\phi ::= p \mid \bot \mid \phi \vee \phi \mid \phi \wedge \phi \mid \phi \rightarrow \phi$$

- Where $p \in \mathcal{P}$ is an atomic proposition, e.g. "Socrates is a man"
- Convenient abbreviations:
  - $\neg\phi$ means $\phi \rightarrow \bot$
  - $\phi \longleftrightarrow \phi'$ means $(\phi \rightarrow \phi') \wedge (\phi' \rightarrow \phi)$

Semantics of classical logic

- Interpretation $\mathfrak{m} : \mathcal{P} \to \{\text{true}, \text{false}\}$

$$
\begin{array}{rcl}
\mathrm{J}p\mathrm{K}^{\mathfrak{m}} & = & \mathfrak{m}(p) \\
\mathrm{J}\bot\mathrm{K}^{\mathfrak{m}} & = & \text{false} \\
\mathrm{J}\phi \wedge \phi'\mathrm{K}^{\mathfrak{m}} & = & \mathrm{J}\phi\mathrm{K}^{\mathfrak{m}} \bar{\wedge} \mathrm{J}\phi'\mathrm{K}^{\mathfrak{m}} \\
\mathrm{J}\phi \vee \phi'\mathrm{K}^{\mathfrak{m}} & = & \mathrm{J}\phi\mathrm{K}^{\mathfrak{m}} \bar{\vee} \mathrm{J}\phi'\mathrm{K}^{\mathfrak{m}} \\
\mathrm{J}\phi \to \phi'\mathrm{K}^{\mathfrak{m}} & = & \bar{\neg}\mathrm{J}\phi\mathrm{K}^{\mathfrak{m}} \bar{\vee} \mathrm{J}\phi'\mathrm{K}^{\mathfrak{m}}
\end{array}
$$

- Where $\bar{\wedge}, \bar{\vee}, \bar{\neg}$ are the standard boolean operations on $\{\text{true}, \text{false}\}$

Terminology

- A formula ϕ is *valid* if $\mathrm{J}\phi\mathrm{K}^{\mathfrak{m}} =$ true for all $\mathfrak{m}$
- A formula ϕ is *unsatisfiable* if $\mathrm{J}\phi\mathrm{K}^{\mathfrak{m}} =$ false for all $\mathfrak{m}$
- *Law of excluded middle*:
- Formula $\phi \vee \neg\phi$ is valid for any ϕ
- A *proof system* attempts to determine the validity of a formula

Proof theory for classical logic

- Proves judgements of the form $\Gamma \vdash \phi$:
  - For any interpretation, under assumption Γ, ϕ is true
- Syntactic deduction rules that produce "proof trees" of $\Gamma \vdash \phi$: *Natural deduction*
- Problem: classical proofs only address truth value, not constructive
- Example: "There are two irrational numbers x and y, such that x^y is rational"
  - Proof does not include much information

Intuitionistic logic

- Get rid of the law of excluded middle
- Notion of "truth" is not the same
  - A proposition is true, if we can construct a proof
  - Cannot assume predefined truth values without constructed proofs (no "either true or false")
- Judgements are not expression of "truth", they are constructions
  - $\vdash \phi$ means "there is a proof for ϕ"
  - $\vdash \phi \rightarrow \bot$ means "there is a refutation for ϕ", not "there is no proof"
  - $\vdash (\phi \rightarrow \bot) \rightarrow \bot$ only means the absense of a refutation for ϕ, does not imply ϕ as in classical logic

Proofs in intuitionistic logic

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

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

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi} \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi} \qquad \frac{\Gamma, \phi \vdash \rho \qquad \Gamma, \psi \vdash \rho \qquad \Gamma \vdash \phi \vee \psi}{\Gamma \vdash \rho}$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi} \qquad \frac{\Gamma \vdash \phi \to \psi \qquad \Gamma \vdash \phi}{\Gamma \vdash \psi}$$

Does that resemble anything?

Curry-Howard correspondence

- We can mechanically translate formulas ϕ into type τ for every ϕ and the reverse
  - E.g. replace $\wedge$ with $\times$, $\vee$ with $+$, ...
- *If* $\Gamma \vdash e : \tau$ *in simply-typed lambda calculus, and* τ *translates to* ϕ*, then* $\text{range}(\Gamma) \vdash \phi$ *in intuistionistic logic*
- *If* $\Gamma \vdash \phi$ *in intuitionistic logic, and* ϕ *translates to* τ*, then there exists* e *and* Γ' *such that* $\text{range}(\Gamma') = \Gamma$ *and* $\Gamma' \vdash e : \tau$
- Proof by induction on the derivation $\Gamma \vdash \phi$
  - Can be simplified by fixing the logic and type languages to match

Consequences

- Lambda terms encode proof trees
- Evaluation of lambda terms is proof simplification
- Automated proving by trying to construct a lambda term with the wanted type
- Verifying a proof is typechecking
  - Increased trust in complicated proofs when machine-verifiable
- Proof-carrying code
- Certifying compilers