SNU 4541.310 Programming Languages (The Correspondence)

Prof. Kwangkeun Yi

The Correspondence

Between logic and programming

- Central organizing principle of
  - programming language design and programming
- Curry-Howard Correspondence
  - *Constructive Logic* $\leftrightarrow$ applicative programming
  - *Classical Logic* $\leftrightarrow$ imperative programming (goto, exception)

Constructive Logic

also called "Intuitionistic Logic"

- Logic of "positive" inference
- A is true exactly when we have a proof of A
  - $A \vee \neg A$ is not blindly true.
    - it's true only when either A has a proof or $\neg A$ has a proof.
  - that $\neg\neg A$ is true does not imply A is true.
  - $\neg A$ is true when we can prove $\bot$ assuming A.

Propositions

$$
\begin{array}{lcl}
f & ::= & \top \mid \bot \\
 & \mid & f \wedge f \\
 & \mid & f \vee f \\
 & \mid & f \supset f
\end{array}
$$

$$(\neg f \equiv f \supset \bot)$$

Proof Rules of Constructive Logic

Hypothesis Use

$$\frac{}{\Gamma \vdash f}\ f \in \Gamma$$

Introduction & Elimination

$$\frac{}{\Gamma \vdash \top} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash f}$$

$$\frac{\Gamma \vdash f_1 \quad \Gamma \vdash f_2}{\Gamma \vdash f_1 \wedge f_2} \qquad \frac{\Gamma \vdash f_1 \wedge f_2}{\Gamma \vdash f_i}$$

$$\frac{\Gamma \vdash f_1}{\Gamma \vdash f_1 \vee f_2}$$

$$\frac{\Gamma \vdash f_2}{\Gamma \vdash f_1 \vee f_2} \qquad \frac{\Gamma \vdash f_1 \vee f_2 \quad \Gamma \cup \{f_1\} \vdash f_3 \quad \Gamma \cup \{f_2\} \vdash f_3}{\Gamma \vdash f_3}$$

$$\frac{\Gamma \cup \{f_1\} \vdash f_2}{\Gamma \vdash f_1 \supset f_2} \qquad \frac{\Gamma \vdash f_1 \subset f_2 \quad \Gamma \vdash f_1}{\Gamma \vdash f_2}$$

Proof-Encoding Rules

- Rules for $\Gamma \vdash p : f$
- Encoded proof p for the proof of f
- Γ is the set of assumed propositions whose proofs are not known yet.
- Hence, we just name those assumed proofs by variables.

$$\Gamma = \{x : f_1, y : f_2, \cdots\}$$

Hypothesis Use

$$\frac{}{\Gamma \vdash x : f} \; x : f \in \Gamma$$

Introduction & Elimination

$$\frac{}{\Gamma \vdash \mathsf{trueI} : \top}$$

$$\frac{\Gamma \vdash p : \bot}{\Gamma \vdash \mathsf{falseE}(p) : f}$$

$$\frac{\Gamma \vdash p_1 : f_1 \quad \Gamma \vdash p_2 : f_2}{\Gamma \vdash \mathsf{andI}(p_1, p_2) : f_1 \wedge f_2}$$

$$\frac{\Gamma \vdash p : f_1 \wedge f_2}{\Gamma \vdash \mathsf{andE}_i(p) : f_i}$$

$$\frac{\Gamma \vdash p : f_1}{\Gamma \vdash \mathsf{orI}_l(p) : f_1 \vee f_2}$$

$$\frac{\Gamma \vdash p : f_2}{\Gamma \vdash \mathsf{orI}_r(p) : f_1 \vee f_2}$$

$$\frac{\begin{array}{c}\Gamma \vdash p : f_1 \vee f_2 \\ \Gamma \cup \{x : f_1\} \vdash p_1 : f_3 \\ \Gamma \cup \{y : f_2\} \vdash p_2 : f_3\end{array}}{\Gamma \vdash \mathsf{orE}(p, x.p_1, y.p_2) : f_3}$$

$$\frac{\Gamma \cup \{x : f_1\} \vdash p : f_2}{\Gamma \vdash \mathsf{impI}(x.p) : f_1 \supset f_2}$$

$$\frac{\Gamma \vdash p : f_1 \supset f_2 \quad \Gamma \vdash p_1 : f_1}{\Gamma \vdash \mathsf{impE}(p, p_1) : f_2}$$

Proof $\leftrightarrow$ Program

Correspondence of proof p with program $\underline{p}$:

$$
\begin{array}{rcl}
x & \leftrightarrow & \texttt{x} \\
\texttt{trueI} & \leftrightarrow & \textit{primitive constant} \\
\texttt{falseE}(p) & \leftrightarrow & \texttt{abort} \\
\texttt{andI}(p_1, p_2) & \leftrightarrow & \texttt{(}\underline{p_1}\texttt{, }\underline{p_2}\texttt{)} \\
\texttt{andE}_i(p) & \leftrightarrow & \underline{p}\,\texttt{.}\,i \\
\texttt{orI}_l(p) & \leftrightarrow & \texttt{inL}\,\underline{p} \\
\texttt{orI}_r(p) & \leftrightarrow & \texttt{inR}\,\underline{p} \\
\texttt{orE}(p, x.p_1, y.p2) & \leftrightarrow & \texttt{case }\underline{p}\texttt{ of inL x -> }\underline{p_1} \\
 & & \qquad\qquad\texttt{| inR y -> }\underline{p_2} \\
\texttt{impI}(x.p) & \leftrightarrow & \texttt{fun x -> }\underline{p} \\
\texttt{impE}(p_1, p_2) & \leftrightarrow & \underline{p_1}\,\underline{p_2}
\end{array}
$$

Proof Reduction $\leftrightarrow$ Computation

- $\mathsf{andE}_1(\mathsf{andI}(p, q)) \;\Rightarrow\; p$
- $\mathsf{andE}_2(\mathsf{andI}(p, q)) \;\Rightarrow\; q$
- $\mathsf{impE}(\mathsf{impI}(x.p), q) \;\Rightarrow\; \{q/x\}p$
- $\mathsf{orE}(\mathsf{orI}_l(p), x.q, y.r) \;\Rightarrow\; \{p/x\}q$
- $\mathsf{orE}(\mathsf{orI}_r(p), x.q, y.r) \;\Rightarrow\; \{p/y\}r$