15-399 Supplementary Notes: Equivalence of Proofs

Robert Harper

February 17, 2005

1 Equivalence of Proofs

Simplification and reduction give rise to a notion of equivalence of proofs, providing a (minimal) answer to the question "when are two proofs the same proof?" Richer notions of equivalence can also be considered.

Proof Simplification

A basic principle of constructive logic is the *local soundness* of the introduction and elimination rules, which we also called the principle of *conservation of proof.* Roughly speaking, this principle states that the elimination rules are no stronger than the introduction rules in the sense that an elimination cannot obtain more information from a proof than was put into it by the introduction rule.

This principle is captured by the following *simplification rules* for proofs:

$$\begin{array}{rcl}
\mathbf{fst}(\langle M, N\rangle) & \leadsto & M \\
\mathbf{snd}(\langle M, N\rangle) & \leadsto & N \\
\\
(\lambda u{:}A.N)(M) & \leadsto & [M/u]N \\
\\
\multicolumn{3}{l}{\mathbf{case}\,\mathbf{inl}(M)\ \ \mathbf{of}\ \mathbf{inl}(u{:}A) \Rightarrow N_1 \mid \mathbf{inr}(v{:}B) \Rightarrow N_2} \\
 & \leadsto & [M/u]N_1 \\
\multicolumn{3}{l}{\mathbf{case}\,\mathbf{inr}(M)\ \ \mathbf{of}\ \mathbf{inl}(u{:}A) \Rightarrow N_1 \mid \mathbf{inr}(v{:}B) \Rightarrow N_2} \\
 & \leadsto & [M/v]N_2
\end{array}$$

Each simplification states that the elimination form for a connective is a *post-inverse* of the introduction form. That is, if you introduce a connective, and then eliminate it, what you get is (constructed from) what you already had.

The simplification lemma states that a simplified proof is a proof of the same result as the original, unsimplified proof.

Lemma 1.1 *If* $\Gamma \vdash M : A$ *and* $M \leadsto N$*, then* $\Gamma \vdash N : A$*.*

Proof Reduction

Proof simplification determines a notion of *proof reduction*, defined by the following rules:

$$\frac{M \rightsquigarrow N}{M \Rightarrow N}$$

$$\frac{M \Rightarrow M'}{\langle M, N \rangle \Rightarrow \langle M', N \rangle} \qquad \frac{N \Rightarrow N'}{\langle M, N \rangle \Rightarrow \langle M, N' \rangle}$$

$$\frac{M \Rightarrow M'}{\lambda u{:}A.M \Rightarrow \lambda u{:}A.M'}$$

$$\frac{M \Rightarrow M'}{\mathbf{inl}(M) \Rightarrow \mathbf{inl}(M')} \qquad \frac{M \Rightarrow M'}{\mathbf{inr}(M) \Rightarrow \mathbf{inr}(M')}$$

$$\frac{M \Rightarrow M'}{\mathbf{case}\, M \;\mathbf{of}\; \mathbf{inl}(u{:}A) {\Rightarrow} N_1 \mid \mathbf{inr}(v{:}B) {\Rightarrow} N_2 \Rightarrow \mathbf{case}\, M' \;\mathbf{of}\; \mathbf{inl}(u{:}A) {\Rightarrow} N_1 \mid \mathbf{inr}(v{:}B) {\Rightarrow} N_2}$$

$$\frac{N_1 \Rightarrow N_1'}{\mathbf{case}\, M \;\mathbf{of}\; \mathbf{inl}(u{:}A) {\Rightarrow} N_1 \mid \mathbf{inr}(v{:}B) {\Rightarrow} N_2 \Rightarrow \mathbf{case}\, M \;\mathbf{of}\; \mathbf{inl}(u{:}A) {\Rightarrow} N_1' \mid \mathbf{inr}(v{:}B) {\Rightarrow} N_2}$$

$$\frac{N_2 \Rightarrow N_2'}{\mathbf{case}\, M \;\mathbf{of}\; \mathbf{inl}(u{:}A) {\Rightarrow} N_1 \mid \mathbf{inr}(v{:}B) {\Rightarrow} N_2 \Rightarrow \mathbf{case}\, M \;\mathbf{of}\; \mathbf{inl}(u{:}A) {\Rightarrow} N_1 \mid \mathbf{inr}(v{:}B) {\Rightarrow} N_2'}$$

Simply put, $M \Rightarrow N$ iff N can be obtained by applying a simplification rule somewhere within M.

The *subject reduction theorem* states that reduction of a proof of a proposition yields another proof of the same proposition.

Theorem 1.1 *If* $\Gamma \vdash M : A$ *and* $M \Rightarrow N$, *then* $\Gamma \vdash M : A$.

Proof Equivalence

Proof reduction, in turn, determines a notion of *proof equivalence* defined by the following rules:

$$\frac{}{M \Leftrightarrow M} \qquad \frac{M \Rightarrow N}{M \Leftrightarrow N}$$

$$\frac{M \Leftrightarrow N}{N \Leftrightarrow M} \qquad \frac{M \Leftrightarrow N \quad N \Leftrightarrow P}{M \Leftrightarrow P}$$

Thus, $M \Leftrightarrow N$ iff M and N are related by some sequence of simplifications and expansions ("reverse" simplifications). This relation is sometimes called *definitional equality*, or *conversion*.

Richer Notions of Equivalence

The notion of proof equivalence presented in the preceding subsection is based entirely on the principle of local soundness of the inference rules for the logical connectives. A richer notion of proof equivalence may be obtained by taking account also of the *local completeness* of the rules. Local completeness is the converse of local soundness; it says that the introduction rules are no stronger than the elimination rules. This means that every proof of a proposition may be put into the form of an introduction rule.

Unlike local soundness, the local completeness principles are not easily stated in terms of a simplification relation. Instead we must state them only as equivalences that take account of the proposition that a proof proves, and not just the form of the proof. The local completeness principles for constructive propositional logic may be stated as follows:

$$\frac{\Gamma \vdash M : \top}{M \Leftrightarrow \langle\rangle}$$

$$\frac{\Gamma \vdash M : A \wedge B}{M \Leftrightarrow \langle \mathbf{fst}(M), \mathbf{snd}(M) \rangle}$$

$$\frac{\Gamma \vdash M : A \supset B \quad u\#M}{M \Leftrightarrow \lambda u{:}A.M(u)}$$

$$\frac{\Gamma \vdash M : A \vee B}{M \Leftrightarrow \mathbf{case}\, M\ \mathbf{of}\ \mathbf{inl}(u{:}A) \Rightarrow \mathbf{inl}(u) \mid \mathbf{inr}(v{:}B) \Rightarrow \mathbf{inr}(v)}$$

Each rule states that a proof of a proposition is, up to proof equivalence, of introductory form.