

Homework 2

15-814: Type Systems for Programming Languages

TA: Kumar Avijit (kavijit@cs.cmu.edu)

Out: September 25, 2009

Due: October 2, 2009 (11:59 PM)

The homework should be submitted electronically as a single PDF file named `solution.pdf`. Submit the homework by copying the file(s) to the directory

`/afs/cs.cmu.edu/academic/class/15814/handin/⟨user-id⟩/hw2`

1 Constructive Logic

In this question, the judgment $A \text{ true}$ refers to the truth judgment of constructive logic, summarized in Figure 1 in the appendix.

Recall the definition of negation from the class:

$$\neg A = A \supset \perp$$

A doubly negated proposition $\neg\neg A$ is *weaker* than A because $A \supset \neg\neg A$. The converse does not hold, in general. However the converse is true when A is a negated proposition.

Task 1 Give a formal derivation for $\vdash \neg\neg\neg A \supset \neg A \text{ true}$.

An important difference between classical logic and constructive logic is the treatment of disjunction. While the Law of Excluded Middle $A \vee \neg A$ is a tautology for all propositions A in classical logic, it is not affirmed in constructive logic. However, it is also not refutable in constructive logic.

Task 2 Give a formal derivation for $\vdash \neg\neg(A \vee \neg A) \text{ true}$.

2 Weak-head reduction

In this part, we shall characterize normal forms for weak-head reduction for the $\lambda^{\rightarrow 1 \times}$. Figure 2 recaps the calculus and weak-head reduction for this calculus is defined in Figure 3 in the appendix.

We recall that a term m is called *normal* if there does not exist an m' such that $m \rightarrow_{\text{wh}} m'$.

Note that if one considers only closed terms, the only possible normal terms would be the ones that are introduction forms, i.e. $\lambda x:A.m$, $\langle m_1; m_2 \rangle$, and $\langle \rangle$. This is because a closed elimination form always has a β -redex!

In this task, we would like to characterize normal forms that may be *open*. We begin by considering intro- and elim- forms separately:

1. If m is an intro form then it is always normal (regardless of whether it is open or closed) because \rightarrow_{wh} does not reduce inside intro forms.
2. If m is an elimination form, then its normality depends solely on the term at the head position:
 - (a) If $m = x$, then it is normal.
 - (b) If the head is an intro form, then m is reducible.
 - (c) If the head is not an intro form and is normal, then m is normal.

For example $\text{ap}(n_1; n_2)$ is normal only if n_1 is normal and is not an abstraction.

Let us call normal terms that are intro-forms as *canonical*, and denote them by w , and call the elim-normal forms as *paths* and denote them by p . Let us denote arbitrary terms (which may not be normal) as m .

Task 3 Based on the above discussion, give an inductive definition of canonical terms w , and paths p for $\lambda^{1 \times \rightarrow}$. i.e. fill in the following:

$$\begin{aligned} \text{Canonical forms } w & ::= \dots \\ \text{Paths } p & ::= x \mid \dots \end{aligned}$$

Remark: Note that the notion of values defined in the class is actually *closed*, *canonical* terms.

3 Type Safety

In this part, we shall prove type safety for $\lambda^{1 \times \rightarrow +}$. This calculus is defined by adding the intro- and elim- rules for the type $A_1 + A_2$ to the calculus in Figure 2.

$$\text{(all rules for } \lambda^{1 \times \rightarrow}) \quad \frac{\Gamma \vdash m : A_1}{\Gamma \vdash \text{inl}_{A_1, A_2}(m) : A_1 + A_2} (+\text{-I}_1)$$

$$\frac{\Gamma \vdash m : A_2}{\Gamma \vdash \text{inr}_{A_1, A_2}(m) : A_1 + A_2} (+\text{-I}_2)$$

$$\frac{\Gamma \vdash m : A_1 + A_2 \quad \Gamma, x:A_1 \vdash m_1 : A \quad \Gamma, y:A_2 \vdash m_2 : A}{\Gamma \vdash \text{case } m \{ \text{inl } x \Rightarrow m_1 \mid \text{inr } y \Rightarrow m_2 \} : A} (+\text{-E})$$

The reduction rules (in addition to those in Figure 3) are given below. We have “lazy” sums because we do not evaluate under an `inl` or an `inr`:

$$\frac{}{\text{case } \text{inl}_{A,B}(m)\{\text{inl } x \Rightarrow m_1 \mid \text{inr } y \Rightarrow m_2\} \rightsquigarrow [m/x]m_1} (+ \rightsquigarrow_1)$$

$$\frac{}{\text{case } \text{inr}_{A,B}(m)\{\text{inl } x \Rightarrow m_1 \mid \text{inr } y \Rightarrow m_2\} \rightsquigarrow [m/y]m_2} (+ \rightsquigarrow_2)$$

$$\frac{m \rightarrow_{\text{wh}} m'}{\text{case } m\{\text{inl } x \Rightarrow m_1 \mid \text{inr } y \Rightarrow m_2\} \rightarrow_{\text{wh}} \text{case } m'\{\text{inl } x \Rightarrow m_1 \mid \text{inr } y \Rightarrow m_2\}} \text{case } \rightarrow_{\text{wh}}$$

Task 4 (Canonical forms) Augment the definition of canonical terms w for $\lambda^{1 \times \rightarrow +}$.

Task 5 (Inversion Lemma) Recall the Inversion Lemma from the class. State (without proof) the inversion lemma for $\lambda^{1 \times \rightarrow +}$. You need to state only the clauses corresponding to the new rules for $+$.

Task 6 (Canonical forms lemma) State (without proof) the clauses corresponding to canonical terms of type $A_1 + A_2$ in the canonical forms lemma for $\lambda^{1 \times \rightarrow +}$. That is, complete the following:

If m is a value of type $A_1 + A_2$, i.e. if $\cdot \vdash m : A_1 + A_2$ and m is a canonical term, then

Task 7 (Preservation) Prove that if $\cdot \vdash m : A$, and $m \rightarrow_{\text{wh}} n$, then $\cdot \vdash n : A$. We did preservation only for $1 \times \rightarrow$ fragment in the class. We proceeded by induction on definition of $m \rightarrow_{\text{wh}} n$. We needed an auxiliary lemma stating that if $\cdot \vdash m : A$ and $m \rightsquigarrow n$, then $\cdot \vdash n : A$. For this task, you need only show the cases corresponding to Rule (`case` \rightarrow_{wh}) (in proof of Preservation), and Rules $(+ \rightsquigarrow_1)$, $(+ \rightsquigarrow_2)$ (in proof of the auxiliary lemma).

Task 8 (Progress) Prove that if $\cdot \vdash m : A$, then m is either a canonical term, or there exists n such that $m \rightarrow_{\text{wh}} n$. This is proved by induction on the derivation $\cdot \vdash m : A$. You need only show the cases corresponding to Rules $(+I_1)$, $(+I_2)$, and $(+E)$.

4 Confluence of full reduction

Head reduction cuts down on choices about what β -redex to contract in a term by always choosing the outermost redex. In contrast, in full reduction, one can contract a β -redex anywhere in the term. A crucial property about full reduction for the calculus we have been working with, is that the choice of β -reductions does not matter. In other words, full reduction is a *confluent* relation, where the confluence is defined as follows:

Definition 1 (Confluence) An abstract relation \rightarrow satisfies diamond property iff whenever $m \rightarrow n_1$ and $m \rightarrow n_2$, then there exists n such that $n_1 \rightarrow n$ and $n_2 \rightarrow n$.

A relation \rightarrow is confluent iff \rightarrow^* satisfies diamond property.

Theorem 1 (Reduction relation is confluent) *If $m \rightarrow^* m_1$, and $m \rightarrow^* m_2$, then there exists n such that $m_1 \rightarrow^* n$, and $m_2 \rightarrow^* n$.*

As a corollary to this theorem, we get:

Corollary 1 (Conversion is an equivalence) *The conversion relation conv defined by:*

$$m \text{ conv } n \text{ iff there exists } p \text{ such that } m \rightarrow^* p, \text{ and } n \rightarrow^* p.$$

is an equivalence relation.

In this part of the homework, we will prove Theorem 1 for the calculus λ^\rightarrow , i.e. only the implication fragment. The full reduction relation for λ^\rightarrow is defined in Figure 4. To prove the theorem, we define *parallel* reduction (\Rightarrow) that contracts several (even overlapping) redexes simultaneously in a term.

$$\frac{}{x \Rightarrow x} \quad \frac{m \Rightarrow m'}{\lambda x:A.m \Rightarrow \lambda x:A.m'} \quad \frac{m_1 \Rightarrow m'_1 \quad m_2 \Rightarrow m'_2}{\text{ap}(m_1; m_2) \Rightarrow \text{ap}(m'_1; m'_2)}$$

$$\frac{m_1 \Rightarrow m'_1 \quad m_2 \Rightarrow m'_2}{\text{ap}(\lambda x:A.m_1; m_2) \Rightarrow [m'_2/x]m'_1}$$

The proof proceeds in two parts:

1. We show that $\Rightarrow^* = \rightarrow^*$. This reduces the problem to showing that \Rightarrow is confluent.
2. We then show that \Rightarrow has the diamond property. Since diamond property implies confluence (although we shall not prove this here), we are done.

Task 9 *In order to show that $m \Rightarrow^* n$ iff $m \rightarrow^* n$, one proceeds by induction while proving both directions. In this task, you do not need to give the full proof. The main cases that you have to show are:*

1. *If $m \rightarrow n$, then $m \Rightarrow^* n$. You may use reflexivity of \Rightarrow without proving.*
2. *If $m \Rightarrow n$, then $m \rightarrow^* n$. You may use the following without proving:*
 - \rightarrow^* is a congruence.
 - \rightarrow^* is transitive.

We now wish to show that \Rightarrow has diamond property. It is here that the power of parallel reductions is used. For every m , let m^\sharp denote the result of applying all β -reductions simultaneously. Then it turns out that if $m \Rightarrow n$ then $n \Rightarrow m^\sharp$. Note that this implies the diamond property for \Rightarrow since m^\sharp is determined solely by m .

We define m^\sharp as

$$\begin{aligned} x^\sharp &= x \\ \lambda x:A.m^\sharp &= \lambda x:A.m^\sharp \\ \text{ap}(m_1; m_2)^\sharp &= \text{ap}(m_1^\sharp; m_2^\sharp) \quad \text{if } m_1 \text{ is not an abstraction} \\ \text{ap}(\lambda x:A.m_1; m_2)^\sharp &= [m_2^\sharp/x]m_1^\sharp \end{aligned}$$

Task 10 Show that if $m \Rightarrow n$, then $n \Rightarrow m^\sharp$. You can use the following lemma without proof:

Lemma 1 If $m \Rightarrow m'$ and $n \Rightarrow n'$, then $[m'/x]n' \Rightarrow [m^\sharp/x]n^\sharp$.

$$\begin{array}{c}
\frac{}{\Gamma, A \text{ true} \vdash A \text{ true}} \text{(hypo)} \qquad \frac{\Gamma, A \text{ true} \vdash B \text{ true}}{\Gamma \vdash A \supset B \text{ true}} (\supset\text{-I}) \\
\frac{\Gamma \vdash A \supset B \text{ true} \quad \Gamma \vdash A \text{ true}}{\Gamma \vdash B \text{ true}} (\supset\text{-E}) \qquad \frac{\Gamma \vdash A \text{ true}}{\Gamma \vdash A \vee B \text{ true}} (\vee\text{-I}_1) \\
\frac{\Gamma \vdash B \text{ true}}{\Gamma \vdash A \vee B \text{ true}} (\vee\text{-I}_2) \\
\frac{\Gamma \vdash A \vee B \text{ true} \quad \Gamma, A \text{ true} \vdash C \text{ true} \quad \Gamma, B \text{ true} \vdash C \text{ true}}{\Gamma \vdash C \text{ true}} (\vee\text{-E})
\end{array}$$

Figure 1: Natural deduction for intuitionistic logic

$$\begin{array}{c}
\frac{}{\Gamma, x:A \vdash x : A} \text{(hyp)} \qquad \frac{\Gamma, x:A \vdash m : A'}{\Gamma \vdash \lambda x:A. m : A \rightarrow A'} (\rightarrow\text{-I}) \\
\frac{\Gamma \vdash m_2 : A_1 \rightarrow A_2 \quad \Gamma \vdash m_1 : A_1}{\Gamma \vdash \text{ap}(m_2; m_1) : A_2} (\rightarrow\text{-E}) \qquad \frac{\Gamma \vdash m_1 : A_1 \quad \Gamma \vdash m_2 : A_2}{\Gamma \vdash \langle m_1; m_2 \rangle : A_1 \times A_2} (\times\text{-I}) \\
\frac{\Gamma \vdash m : A_1 \times A_2}{\Gamma \vdash \text{fst}(m) : A_1} (\times\text{-E}_1) \qquad \frac{\Gamma \vdash m : A_1 \times A_2}{\Gamma \vdash \text{snd}(m) : A_2} (\times\text{-E}_2) \qquad \frac{}{\Gamma \vdash \langle \rangle : \mathbf{1}} (\mathbf{1}\text{-I})
\end{array}$$

Figure 2: λ -calculus with $\mathbf{1}$, \times , \rightarrow .

$$\begin{array}{c}
\frac{}{\text{ap}(\lambda x:A. m; n) \rightsquigarrow [n/x]m} (\rightarrow\rightsquigarrow) \qquad \frac{}{\text{fst}(\langle m_1; m_2 \rangle) \rightsquigarrow m_1} (\times \rightsquigarrow_1) \\
\frac{}{\text{snd}(\langle m_1; m_2 \rangle) \rightsquigarrow m_2} (\times \rightsquigarrow_2)
\end{array}$$

$$\begin{array}{c}
\frac{m \rightsquigarrow n}{m \rightarrow_{\text{wh}} n} \text{(step)} \qquad \frac{m \rightarrow_{\text{wh}} m'}{\text{ap}(m; n) \rightarrow_{\text{wh}} \text{ap}(m'; n)} \text{(app } \rightarrow_{\text{wh}}) \\
\frac{m \rightarrow_{\text{wh}} m'}{\text{fst}(m) \rightarrow_{\text{wh}} \text{fst}(m')} \text{(fst } \rightarrow_{\text{wh}}) \qquad \frac{m \rightarrow_{\text{wh}} m'}{\text{snd}(m) \rightarrow_{\text{wh}} \text{snd}(m')} \text{(snd } \rightarrow_{\text{wh}})
\end{array}$$

Figure 3: Weak-head reduction for $\lambda^{1 \times \rightarrow}$ -calculus

$$\frac{}{\mathbf{ap}(\lambda x:A.m; n) \rightsquigarrow [n/x]m} (\rightarrow \rightsquigarrow)$$

$$\frac{m \rightsquigarrow n}{m \rightarrow n} (\mathbf{step}_{\rightsquigarrow})$$

$$\frac{m \rightarrow m'}{\lambda x:A.m \rightarrow \lambda x:A.m'} (\mathbf{lam} \rightarrow)$$

$$\frac{m \rightarrow m'}{\mathbf{ap}(m; n) \rightarrow \mathbf{ap}(m'; n)} (\mathbf{app} \rightarrow_1)$$

$$\frac{n \rightarrow n'}{\mathbf{ap}(m; n) \rightarrow \mathbf{ap}(m; n')} (\mathbf{app} \rightarrow_2)$$

Figure 4: Full reduction relation for $\lambda^{\rightsquigarrow}$.