Homework 3: Double Negation, Gödel's T and Co-data

15-814: Types and Programming Languages
TA: Bernardo Toninho (btoninho@cs.cmu.edu)

Out: 11/10/11
Due: 25/10/11

This assignment is due before class on 25/10/11.
Edit 14/10/11: Minor typos.
Edit 17/10/11: Added extra assumption to the smerge problem.

1 Double Negation Translation

As was discussed in class, intuitionistic logic takes a fine-grained view of the notion of truth when compared to classical logic. In intuitionistic logic, in general, the law of excluded middle does not hold. In classical logic, the law of excluded middle is considered to be an axiom, hence for any particular proposition it is the case that we can always case analyze on whether it is true or false. This distinction arises because in intuitionistic logic, truth is tied to justification and the preservation of justification throughout the rules, hence it is natural that the proposition $A \vee \neg A$ is not true, since there is (in general) no justification of A, nor a justification $\neg A$.

However, we can understand classical truth in intuitionistic logic through what is known as the double-negation translation of classical logic, that roughly maps each classical proposition A to the intuitionistic proposition $\neg\neg A$. Formally, the translation of A, written $A^{\perp\perp}$ is defined inductively on the structure of A as follows:

$$
\begin{array}{lcl}
A^{\perp\perp} & \triangleq & \neg\neg A^{\perp} \\
\\
(A \vee B)^{\perp} & \triangleq & A^{\perp\perp} \vee B^{\perp\perp} \\
(A \supset B)^{\perp} & \triangleq & A^{\perp\perp} \supset B^{\perp\perp} \\
(\neg A)^{\perp} & \triangleq & \neg A^{\perp\perp} \\
(\perp)^{\perp} & \triangleq & \perp
\end{array}
$$

This is not exactly the translation presented in class. In fact, there are many translations that work, but with different operational meanings.

We define classical logic as the extension of intuitionistic logic with the law of excluded middle axiom ($\Gamma \vdash A \vee \neg A$) and we will refer to classical derivations using $\vdash_C$. Note that this adding this axiom is safe (in terms of soundness) because intuitionistic logic does not refute the law of the excluded middle. The fragment of intuitionistic logic we will consider for this exercise is:

$$
\frac{}{\Gamma, A \vdash A}\ (hyp) \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee I_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee I_2
$$

$$
\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee E \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}\ \supset I \qquad \frac{\Gamma \vdash A \supset B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \supset E
$$

$$
\frac{\Gamma \vdash \perp}{\Gamma \vdash C}\ \perp E
$$

You may use the following derived rules of inference for negation (since negation is defined in terms of implication and falsehood, you don't need to show the cases for these derived rules):

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg I \qquad \frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash C}\ \neg E$$

Task 1 (From Classical to Intuitionistic Logic) *Show that if* $\Gamma \vdash_C A$ *then* $\Gamma^\perp \vdash A^{\perp\perp}$, *where* $\Gamma^\perp$ *denotes that all assumptions* $B \in \Gamma$ *become* $B^\perp \in \Gamma^\perp$. *You may use weakening without proving it again.*

2 Gödel's T

Recall the statics for Gödel's T (assume the dynamics presented in class):

$$\frac{}{\Gamma, x : \tau \vdash x : \tau} \qquad \frac{\Gamma, x : \tau_1 \vdash M : \tau_2}{\Gamma \vdash \lambda x : \tau_1 . M : \tau_1 \to \tau_2} \qquad \frac{\Gamma \vdash M : \tau_1 \to \tau_2 \quad \Gamma \vdash N : \tau_1}{\Gamma \vdash M\, N : \tau_2}$$

$$\frac{}{\Gamma \vdash \mathbf{z} : \omega} \qquad \frac{\Gamma \vdash M : \omega}{\Gamma \vdash \mathbf{s}(M) : \omega} \qquad \frac{\Gamma \vdash M : \omega \quad \Gamma \vdash M_o : \tau \quad \Gamma, x : \tau \vdash M_1 : \tau}{\Gamma \vdash \mathbf{rec}(M; M_o; x.M_1) : \tau}$$

Task 2 (Preservation) *Show that if* $\cdot \vdash M : \tau$ *and* $M \mapsto M'$ *then* $\Gamma \vdash M' : \tau$. *You may assume substitution holds.*

Task 3 (Progress) *Show that if* $\cdot \vdash M : \tau$ *then either* $M\ \mathsf{val}$ *or* $M \mapsto M'$, *for some* M'.

We will now show that all well-typed terms in Gödel's T terminate. We will use a slightly different definition of hereditary termination at a given type τ, written $\mathbf{HT}_\tau(M)$, as follows:

Definition 1 (Hereditary Termination)

1. $\mathbf{HT}_\omega(M)$ *is defined to be the strongest closed predicate* $\mathcal{P}$ *such that:*
   - *If* $M \mapsto^* \mathbf{z}$ *then* $\mathcal{P}(M)$
   - *If* $M \mapsto^* \mathbf{s}(M')$ *and* $\mathcal{P}(M')$ *then* $\mathcal{P}(M)$.
2. $HT_{\tau_1 \to \tau_2}(M)$ *iff:*
   - $M \mapsto^* \lambda x : \tau_1 . M'$ *and* $\mathbf{HT}_{\tau_1}(M_1)$ *then* $\mathbf{HT}_{\tau_2}([M_1/x]M')$

Task 4 *Show that* $\mathbf{HT}_\omega(M)$ *iff* $M \mapsto^* \mathbf{z}$ *or* ($M \mapsto^* \mathbf{s}(M')$ *and* $\mathbf{HT}_\omega(M')$). *Recall that by definition,* $\mathbf{HT}_\omega$ *is the strongest predicate closed under the rules given above, therefore,* $\mathbf{HT}_\omega$ *implies any predicate that is closed under the rules. It might help to think of* $\mathbf{HT}_\omega$ *as the intersection of all such predicates.*

Suppose Γ is a well-defined context and γ is a mapping from variables in Γ to closed terms such that, for all $x : \tau \in \Gamma$, $\gamma(x) : \tau$. We state $\mathbf{HT}_\Gamma(\gamma)$ iff for all $x : \tau \in \Gamma$ we have $\mathbf{HT}_\tau(\gamma(x))$. We define $\hat{\gamma}(M)$ to be the result of simultaneous substitution as determined by the mapping γ. We need the following lemma:

Task 5 (Head Expansion) *Show that if* $\mathbf{HT}_\tau(M)$, $M' : \tau$ *and* $M' \mapsto M$ *then* $\mathbf{HT}_\tau(M')$.

We can now prove our main result:

Task 6 *Show that if* $\Gamma \vdash M : \tau$ *and* $\mathbf{HT}_\Gamma(\gamma)$ *then* $\mathbf{HT}_\tau(\hat{\gamma}(M))$.

(Hint) Use induction on the typing derivation. Recall the setup from class. You will need to use a double induction for the case for the recursor.

Task 7 (Termination) *Show that if* $\mathbf{HT}_\tau(M)$ *then* M *terminates.*

3 Streams and coinductive data

In this exercise we will develop some simple programming examples using streams. Recall the statics and dynamics for streams (where σ is the type of streams of natural numbers – assume the typical statics and dynamics for functions and natural numbers):

$$\frac{\Gamma \vdash M : \sigma}{\Gamma \vdash \mathsf{tl}(M) : \sigma}\ \sigma E_1 \quad \frac{\Gamma \vdash M : \sigma}{\Gamma \vdash \mathsf{hd}(M) : \omega}\ \sigma E_2 \quad \frac{\Gamma \vdash M : \tau \quad \Gamma, x : \tau \vdash M_0 : \omega \quad \Gamma, x : \tau \vdash M_1 : \tau}{\Gamma \vdash \mathbf{corec}(M; x.M_0; x.M_1) : \sigma}\ \sigma I$$

$$\frac{}{\mathbf{corec}(M; x.M_0; x.M_1)\ \mathsf{val}}$$

$$\frac{M \mapsto M'}{\mathsf{hd}(M) \mapsto \mathsf{hd}(M')} \qquad \frac{M \mapsto M'}{\mathsf{tl}(M) \mapsto \mathsf{tl}(M')}$$

$$\frac{}{\mathsf{hd}(\mathbf{corec}(M; x.M_0; x.M_1)) \mapsto [M/x]M_0}$$

$$\frac{}{\mathsf{tl}(\mathbf{corec}(M; x.M_0; x.M_1)) \mapsto \mathbf{corec}([M/x]M_1; x.M_0; x.M_1)}$$

For the following three tasks, remember that you can't case analyze the "structure" of a stream, you can only obtain its head and tail. For instance, in Task 7, you want a function that given a stream s computes a stream s' such that $\mathsf{hd}(s') = f(\mathsf{hd}(s))$, $\mathsf{hd}(\mathsf{tl}(s')) = f(\mathsf{hd}(\mathsf{tl}(s)))$, and so on. The programs you will write can make use of booleans, streams, pairs, functions and natural numbers (you may use boolean comparisons between natural numbers $==$ and $<$ and conditional branching, since these are all definable).

Task 8 (Warm up) *Define a function* $\mathsf{smap} : \sigma \to (\omega \to \omega) \to \sigma$ *that given a stream s and a function on natural numbers f computes the stream obtained by applying f to each element of s.*

Task 9 (The Fibonacci Stream) *Define the stream of all Fibonacci numbers. You may assume the language has pairs.*

Task 10 (Merging Streams) *Define a function* $\mathsf{smerge} : \sigma \to \sigma \to \sigma$ *that given two streams s_1 and s_2 produces the stream obtained by merging s_1 and s_2 in ascending order (assume s_1 and s_2 are sorted in the appropriate order).*

Termination

We will now prove that all terms in the extension of Gödel's T with streams terminate. We extend the definition of hereditary termination as follows:

Definition 2 (Hereditary Termination for σ) $\mathbf{HT}_\sigma$ *is the weakest consistent predicate $\mathcal{P}$ such that the following conditions hold:*

- $\mathcal{P}(M)$ *implies* $\mathbf{HT}_\omega(\mathsf{hd}(M))$
- $\mathcal{P}(M)$ *implies* $\mathcal{P}(\mathsf{tl}(M))$

Recall that hereditary termination for streams defines a coinduction principle. To show $\mathbf{HT}_\sigma(M)$ for some term M, it suffices to exhibit some predicate $\mathcal{P}(M)$ such that $\mathcal{P}$ satisfies the two conditions above (it might help to understand weakest as the union of all such predicates).

Task 11 *Show that* $\mathbf{HT}_\sigma(M)$ *iff* $\mathbf{HT}_\omega(\mathsf{hd}(M))$ *and* $\mathbf{HT}_\sigma(\mathsf{tl}(M))$.

Task 12 (Head Expansion for streams) *Show the new cases in the head expansion lemma.* **(Hint)** *Suppose $M \mapsto N$ and $\mathbf{HT}_\sigma(N)$, to show $\mathbf{HT}_\sigma(M)$ consider $\mathcal{P}(M) = \exists N.(M \mapsto N \wedge \mathbf{HT}_\sigma(N))$.*

We can now extend our termination result.

Task 13 (Hereditary Termination) *Show that if $\Gamma \vdash M : \tau$ and $\mathbf{HT}_\Gamma(\gamma)$ then $\mathbf{HT}_\tau(\hat{\gamma}(M))$. You only need to show the new cases.*