Terminating Untyped Hereditary Substitution

Jason Reed

January 28, 2007

Terms	M	$::=$	$x \cdot S \mid \lambda x.S$
Spines	S	$::=$	$() \mid (M; S)$
Positive Types	t	$::=$	$i \to \cdots \to i \to o$
Negative Type Sets	i	$::=$	$\{j_1, \dots, j_n\}$
Negative Types	j	$::=$	$t \to \cdots \to t \to o$

1 Syntactic Operations

$tp(M)$ computes the type of a (possibly open) term. It is a t.

$$\begin{aligned} tp(x \cdot S) &= o \\ tp(\lambda x.M) &= x \in M \to tp(M) \end{aligned}$$

$tp(S)$ computes the type of the head to go with a spine. It is a j.

$$\begin{aligned} tp() &= o \\ tp(M; S) &= tp(M) \to tp(S) \end{aligned}$$

$x \in M$ computes the set of types of a variable in a term. It is an i.

$$\begin{aligned} x \in x \cdot S &= \{tp(S)\} \cup x \in S \\ x \in y \cdot S &= x \in S \\ x \in \lambda y.M &= x \in M \\ x \in () &= \{\} \\ x \in (M; S) &= x \in M \cup x \in S \end{aligned}$$

We define relations $t \sqsubseteq t$ and $i \sqsubseteq i$ and $j \sqsubseteq j$, just to be very explicit about the intended subterm relation:

$$\frac{}{\{\} \sqsubseteq i}$$

$$\frac{i \sqsubseteq i'}{i \cup \{j\} \sqsubseteq i' \cup \{j\}}$$

$$\frac{i_1 \sqsubseteq i'_1 \qquad \cdots \qquad i_n \sqsubseteq i'_n}{i_1 \to \cdots \to i_n \to o \sqsubseteq i'_1 \to \cdots \to i'_n \to o}$$

$$\frac{t_1 \sqsubseteq t'_1 \qquad \cdots \qquad t_n \sqsubseteq t'_n}{t_1 \to \cdots \to t_n \to o \sqsubseteq t'_1 \to \cdots \to t'_n \to o}$$

Substitution and reduction are as follows, abbreviating $\sigma = [M/x]$:

$$\begin{aligned}
\sigma(\lambda y.N) &= \lambda y.\sigma N \\
\sigma(y \cdot S) &= y \cdot \sigma S \\
\sigma(x \cdot S) &= [M \mid \sigma S] \\
\sigma() &= () \\
\sigma(N; S) &= (\sigma N; \sigma S) \\
[\lambda x.N \mid (M; S)] &= [[M/x]N \mid S] \\
[x \cdot S \mid ()] &= x \cdot S \\
_ &= \mathbf{fail}
\end{aligned}$$

The critical thing is that $[\lambda x.M \mid ()]$ fails, for otherwise Lemma 1.1 part 2 below is certainly false. To say that $[M/y]V$ or $[M \mid S]$ 'exists' is to say that the substitution/reduction algorithm terminates, and does not fail.

In the induction measures, $+$ indicates a simultaneous ordering on two structures. That is, V and W are structures, then $V + W$ is considered the same size as $W + V$, and $V' + W' \leq V + W$ if both $V' \leq V$ and $W \leq W'$, and $V' + W' < V + W$ if at least one of the two individual inequalities is strict. Naturally, the subterm ordering on types means that $t < i \to t$ and $i < i \to t$. We incorporate the ordering $\sqsubseteq$ into $\leq$, so that if $i \sqsubseteq i'$, (resp. $j \sqsubseteq j'$, $t \sqsubseteq t'$) then $i \leq i'$ (resp. $j \leq j'$, $t \leq t'$).

1.1 Results

Lemma 1.1

1. *If $[M/y]V$ exists, then $x \in [M/y]V \sqsubseteq (x \in M) \cup (x \in V)$.*
2. *If $[M/y]V$ exists, then $tp([M/y]V) \sqsubseteq tp(V)$.*
3. *If $[M|S]$ exists, then $x \in [M|S] \sqsubseteq (x \in M) \cup (x \in S)$.*

Proof By lexicographic induction. The measure per case is

1. $tp(M) + y \in V$
2. $tp(M) + y \in V$
3. $tp(M) + tp(S)$

For equal values of this measure, case 3 is considered less than 1 and 2, and *ceteris paribus*, we may proceed with smaller V.

1. Split cases on V.

   Case: $V = ()$. In this case, we must merely observe $\{\} \sqsubseteq (x \in M) \cup \{\}$.

Case: $V = (N; S)$. Compute

$$\begin{array}{ll}
x \in [M/y](N;S) & \\
= x \in ([M/y]N; [M/y]S) & \\
= (x \in [M/y]N) \cup (x \in [M/y]S) & \\
\sqsubseteq ((x \in M) \cup (x \in N)) \cup ((x \in M) \cup (x \in S)) & \text{by i.h. 1 twice} \\
= (x \in M) \cup (x \in N) \cup (x \in S) & \text{properties of } \cup \\
= (x \in M) \cup (x \in (N;S)) &
\end{array}$$

Case: $V = \lambda z.N$. Compute

$$\begin{array}{ll}
x \in [M/y]\lambda z.N & \\
= x \in \lambda z.[M/y]N & \\
= x \in [M/y]N & \\
\sqsubseteq (x \in M) \cup (x \in N) & \text{by i.h. 1} \\
= (x \in M) \cup (x \in \lambda z.N) &
\end{array}$$

Case: $V = z \cdot S$ where $z \neq x$ and $z \neq y$. Compute

$$\begin{array}{ll}
x \in [M/y](z \cdot S) & \\
= x \in (z \cdot [M/y]S) & \\
= x \in [M/y]S & \\
\sqsubseteq (x \in M) \cup (x \in S) & \text{by i.h. 1} \\
= (x \in M) \cup (x \in (z \cdot S)) &
\end{array}$$

Case: $V = x \cdot S$. Compute

$$\begin{array}{ll}
x \in [M/y](x \cdot S) & \\
= x \in (x \cdot [M/y]S) & \\
= tp([M/y]S) \cup (x \in [M/y]S) & \\
\sqsubseteq tp([M/y]S) \cup ((x \in M) \cup (x \in S)) & \text{by i.h. 1} \\
\sqsubseteq tp(S) \cup ((x \in M) \cup (x \in S)) & \text{by i.h. 2} \\
= (x \in M) \cup (tp(S) \cup (x \in S)) & \text{properties of } \cup \\
= (x \in M) \cup (x \in (x \cdot S)) &
\end{array}$$

Case: $V = y \cdot S$. First observe that

$$\begin{array}{ll}
tp([M/y]S) \sqsubseteq tp(S) & \text{by i.h. 2} \\
tp(M) + tp([M/y]S) \leq tp(M) + (\{tp(S)\} \cup y \in S) & (*)
\end{array}$$

Now compute

$$\begin{array}{ll}
x \in [M/y](y \cdot S) & \\
= x \in [M \mid [M/y]S] & \\
\sqsubseteq (x \in M) \cup (x \in [M/y]S) & \text{by i.h. 3, licensed by } (*) \\
\sqsubseteq (x \in M) \cup (x \in M) \cup (x \in S) & \text{by i.h. 1} \\
= (x \in M) \cup (x \in S) & \text{properties of } \cup \\
= (x \in M) \cup (x \in y \cdot S) &
\end{array}$$

2. Split cases on V.

Case: $V = ()$. Immediate.

Case: $V = (N; S)$.

$$
\begin{array}{ll}
tp([M/y](N;S)) & \\
= tp(([M/y]N; [M/y]S)) & \\
= (tp([M/y]N), tp([M/y]S)) & \\
\sqsubseteq (tp(N), tp(S)) & \text{i.h. 2 twice} \\
= tp(N; S) &
\end{array}
$$

Case: $V = \lambda x.N$. Compute

$$
\begin{array}{ll}
tp([M/y]\lambda x.N) & \\
= tp(\lambda x.[M/y]N) & \\
= (x \in [M/y]N) \to tp([M/y]N) & \\
\sqsubseteq (x \in [M/y]N) \to tp(N) & \text{i.h. 2} \\
\sqsubseteq (x \in N) \to tp(N) & \text{i.h. 1} \\
= tp(\lambda x.N) &
\end{array}
$$

Case: $V = x \cdot S$. Immediate: $o \sqsubseteq o$.

3. Split cases on $tp(M)$.

Case: $tp(M) = o$. Then M is of the form $y \cdot S'$ for some variable y (which may in fact be x) and S must be $()$ for $[M|S]$ to be defined. All that remains to show is that

$$
\begin{array}{l}
x \in [M|S] \\
= x \in [y \cdot S' \mid ()] \\
= x \in (y \cdot S') \\
= x \in (y \cdot S') \cup \{\} \\
= x \in (y \cdot S') \cup x \in () \\
= (x \in M) \cup (x \in S)
\end{array}
$$

Case: $tp(M) = \tau_1 \to \tau_2$. Then M is of the form $\lambda y.N$ such that $y \in N = \tau_1$ and $tp(N) = \tau_2$. Moreoever S must be of the form $(M_0; S_0)$ for $[M|S]$ to be defined. Observe that

$$
\begin{array}{ll}
tp([M_0/y]N) \sqsubseteq tp(N) & \text{by i.h. 2} \\
tp([M_0/y]N) + tp(S_0) < tp(N) + tp(S_0) & \\
< (y \in N) \to tp(N) + tp(M_0) \to tp(S_0) & \\
= tp(\lambda y.N) + tp(M_0; S_0) & \\
\therefore tp([M_0/y]N) + tp(S_0) < tp(\lambda y.N) + tp(M_0; S_0) & (*)
\end{array}
$$

and also

$$
\begin{array}{ll}
(y \in N) + tp(M_0) & \\
< (y \in N) \to tp(N) + tp(M_0) \to tp(S_0) & \\
= tp(\lambda y.N) + tp(M_0; S_0) & \\
\therefore tp(M_0) + y \in N < tp(\lambda y.N) + tp(M_0; S_0) & (**)
\end{array}
$$

Now compute

$$
\begin{aligned}
& x \in [M|S] \\
& = x \in [\lambda y.N \mid (M_0; S_0)] \\
& = x \in [[M_0/y]N \mid S_0] \\
& \sqsubseteq (x \in [M_0/y]N) \cup (x \in S_0) && \text{i.h. 3, licensed by } (*) \\
& \sqsubseteq ((x \in M_0) \cup (x \in N)) \cup (x \in S_0) && \text{i.h. 1, licensed by } (**) \\
& = (x \in N) \cup ((x \in M_0) \cup (x \in S_0)) && \text{properties of } \cup \\
& = (x \in M) \cup (x \in S)
\end{aligned}
$$

■

Theorem 1.2

1. *$[M/x]V$ either exists, or finitely fails.*
2. *$[M|S]$ either exists, or finitely fails.*

Proof By induction on the measure

1. $tp(M) + y \in V$
2. $tp(M) + tp(S)$

Where case 2 is considered less for equal measure, and *ceteris paribus*, we may proceed with smaller V.

1. Split cases on V.

   Case: $V = ()$. Immediate.

   Case: $V = (N; S)$. Apply induction hypothesis to N and S, at the same (or possibly smaller) measure but smaller terms.

   Case: $V = \lambda y.N$. Apply induction hypothesis to N, at the same measure but a smaller term.

   Case: $V = y \cdot S$. Apply induction hypothesis to S, at the same measure but a smaller expression.

   Case: $V = x \cdot S$. Apply induction hypothesis part 1 to S, at the same (or possibly smaller) measure but a smaller expression. From this we find that $[M/x]S$ either exists or finitely fails. If it fails, we are already done, for $[M/x](x \cdot S) = [M \mid [M/x]S]$ has already failed. Otherwise, use Lemma 1.1 to see that $tp([M/x]S) \sqsubseteq tp(S)$, which implies that $tp(M) + tp([M/x]S) \leq tp(M) + tp(S) \leq tp(M) + \{x \in S\} \cup tp(S) = tp(M) + tp(x \in (x \cdot S))$. Thus we may appeal to the induction hypothesis part 2 to see that $[M \mid [M/x]S]$ either exists or finitely fails.

2. Split cases on $tp(M)$.

   Case: $tp(M) = o$. Then M is of the form $y \cdot S'$. If $S = ()$, then $[M \mid S] = M$. Otherwise, reduction immediately fails.

Case: $tp(M) = i \to t$. Then M is of the form $\lambda y.N$. Consider whether S is of the form $(M_0; S_0)$. If it is not, then reduction immediately fails. If it is, note that the induction measure coming in was $tp(\lambda y.N) + tp(M_0; S_0) = (y \in N) \to tp(N) + tp(M_0) \to tp(S_0)$, and we can show both of

$$tp([M_0/y]N) + tp(S_0) < (y \in N) \to tp(N) + tp(M_0) \to tp(S_0) \quad (*)$$

$$tp(y \in N) + tp(M_0) < (y \in N) \to tp(N) + tp(M_0) \to tp(S_0) \quad (**)$$

using Lemma 1.1 in $(*)$ to get that $tp([M_0/y]N) \sqsubseteq tp(N)$. By $(**)$, we can use the induction hypothesis part 1 to see that $[M_0/y]N$ either exists or finitely fails. If it fails, we are already done. If it succeeds, then $(*)$ licenses using the induction hypothesis part 2 to conclude that $[[M_0/y]N \mid S]$ either exists or finitely fails.

■