Recursive types and the subject reduction theorem

Richard Statman
Carnegie Mellon University

Follow this and additional works at: http://repository.cmu.edu/math
NOTICE WARNING CONCERNING COPYRIGHT RESTRICTIONS:
The copyright law of the United States (title 17, U.S. Code) governs the making of photocopies or other reproductions of copyrighted material. Any copying of this document without permission of its author may be prohibited by law.
INTRODUCTION

Dana Scott began talking about type algebras before 1975 ([9]) and his ideas have been pursued by Albert Meyer and Val Breazu-Tannen ([3]) among others. It is clear that in this framework the notion of recursive type ([8]) can be developed and principal properties proved. The notion of type algebra provides an alternative environment to the mu calculus([4]). In this setting it is clear that the regular tree semantics ([4]) is just one possible semantics for recursive types. This semantics identifies

\[ p = p \rightarrow p \]

and

\[ p = (p \rightarrow p) \rightarrow p \]

but the latter fails to syntactically type \( \lambda x. xx \). In other words syntactic typing makes more distinctions. There is even a very interesting result concerning syntactic typing due to Mendler ([8]). Here we shall pursue the syntactic approach.

In this note we shall prove that the type algebras which satisfy Curry's subject reduction theorem are precisely the recursive types. Here lambda calculus and type theory are in remarkable harmony. Along the way we shall solve the type inference problem for recursive types. This problem has not been adequately considered in the literature.

PRELIMINARIES
Type expressions are built up from atoms p, q, r, ... by \rightarrow. \ A, B, C, ...
... are type expressions. A type algebra T is a congruence on the type
expressions. Instead of T(A, B) we write T \vdash A = B. T can be
presented by sets of identities. If S is such a set we will often abuse
notation and write S \vdash A = B instead of T \vdash A = B.

A simultaneous recursion R is a set of identities of the form
p = A

such that
(1) for each p there is at most one A such that p = A: R
(2) each A is a non-atom.
The set of atoms p such that there exists an A with p = A: R is de-
noted def(R) and the map p \mapsto A such that p = A: R with domain
def(R) is denoted R(.). When R is finite we can write it as the
simultaneous system
p_1 = A_1(p_1, ..., p_n)

\vdots

p_n = A_n(p_1, ..., p_n).

This can be solved in the mu calculus ([\mu]) by
q_1 \leftarrow \mu x_1 A_1(x_1, ..., x_n)

\vdots

q_n \leftarrow \mu x_n A_n(q_{n-1}/x_{n-1})(...((q_2/x_2)q_1)...), ..., q_{n-1}, x_n)
p_n \leftarrow q_n

\vdots

p_1 \leftarrow [p_2/x_2, ..., p_n/x_n]q_1.
More generally it is easy to see that for finite recursions our formalization and the mu calculus are equivalent.

INVERTIBILITY

With each simultaneous recursion R we associate a rewrite system \( R^+ = \{ R(p) \rightarrow p \mid p: \text{def}(R) \} \). Since the rules of \( R^+ \) are length decreasing if there are no critical pairs then \( R^+ \) is Church-Rosser. In particular, we can pass to what amounts to the Knuth-Bendix completion to insure Church-Rosser as follows.

Suppose that \( s: \text{Natural Numbers} \rightarrow \text{Atoms} \times \text{Atoms} \) such that

(a) \( s(t) \) has distinct coordinates
(b) if \( p \) and \( q \) are distinct then \( \{ t \mid s(t) = \langle p, q \rangle \} \) is infinite.

Here \( s \) is to be thought of as a fair schedule of pairs. Define two sequences \( R_n, S_n \) of sets of identities as follows. \( R_0 = R \) and \( S_0 = \emptyset \). If \( R_n \) and \( S_n \) are defined and \( s(n+1) = \langle p_0, p_1 \rangle \) then

(1) If \( p_0 = A_0 \) and \( p_1 = A_1 \) belong to \( R_n \), \( A_1 \) is a proper subexpression of \( A_0 \) and \( A_0^* \) is the result of replacing each occurrence of \( A_1 \) by \( p_1 \) in \( A_0 \) then \( R_{n+1} = R_n - \{ p_0 = A_0 \} + \{ p_0 = A_0^* \} \) and \( S_{n+1} = S_n \).

(2) If \( p_0 = A \) and \( p_1 = A \) belong to \( R_n \) and \( p_i < p(1-i) \), where we here assume that the atoms have somehow been encoded as natural numbers, then \( R_{n+1} = [p_i/p(1-i)]R_n \) and \( S_{n+1} = S_n + \{ p(1-i) = p_i \} \) and otherwise we set \( R_{n+1} = R_n \) and \( S_{n+1} = S_n \). Now we let \( S^\uparrow = \bigcup \{ S_n \mid n = 0, 1, \ldots \} \) and \( R^\uparrow = \{ p = A \mid p = A: R_n \text{ for all but finitely many } n \} \).

The principal fact about the above construction is that \( R \) is logically equivalent to \( R^\uparrow \cup S^\uparrow \). To see this we trace a given member of \( R \) through the construction of the \( R_n \) and \( S_n \) as a finite set \( F_n \) such that \( F_{n+1} \models F_n \). We begin with \( p = A: R \) and set \( F_0 = \{ p = A \} \).

To go from \( F_n \) to \( F_{n+1} \) in case

(1) we replace \( p_0 = A_0 \) by \( p_1 = A_1 \) and \( p_0 = A_0^* \).
(2) we replace each identity E by \([\pi/p(1-i)]E\) and add \(p(1-i)=p1\). Note that only finitely many changes can be made in the \(Fn\) by (1) since each such operation reduces the number of nested (non-outermost) \(\rightarrow\)'s. In addition, the atoms in the last such \(Fn\) resulting from operation (1) can be changed and augmented by (2) at most finitely often since the operation (2) decreases their numerical value. Thus there exists a \(t\) such that for all \(n>t\) \(Ft\) is contained in \(Fn\). Thus \( Ft\) is contained in \(R^+ U S^+\) and \(R^+ U S^+ \models p=A\).

Now it is easily seen that \(R^+\) is a simultaneous recursion and \(R^+\) has no critical pairs. The structure of \(S^+\) is similar. The members of \(S^+\) have the form \(p=q\) where \(p>q\). For each \(p\) there is at most one \(q\) such that \(p=q;S^+\) and if such a \(q\) exists \(p\) does not occur in a member of \(R^+.\) Let \(S^+ = \{ p\rightarrow q \mid p=q;S^+ \};\) then \(R^+ U S^+\) has no critical pairs and is terminating. Finally, if \(R \models A=B\) then there exist \(A+,B+\) and \(C\) such that \(A\rightarrow A+\) and \(B\rightarrow B+\) in \(S^+\) and \(A+\rightarrow C\rightleftharpoons B+\) in \(R^+.\) Because \(S^+\) is logically trivial we shall assume that all of our recursions are presented in the form of \(R^+\), i.e. no critical pairs.

A type algebra \(T\) is said to be invertible if whenever we have \(T \models A\rightarrow B=C\rightarrow D\) then \(T \models A=C\) and \(T \models B=D\.\) We can now see that every simultaneous recursion \(R\) is invertible for if \(R \models A\rightarrow B=C\rightarrow D\) then by the Church-Rosser theorem there exists a type expression \(E\) such that \(A\rightarrow B \rightarrow \rightarrow E \rightleftharpoons C \rightleftharpoons D\). If \(E\) is an atom then the last step in each of the two reductions is the only step which uses the entire expression as a redex. Since \(R\) is a recursion it must be of the from \(R(E)\rightleftharpoons E\). In particular, \(R(E)= E0\rightleftharpoons E1\) and \(A\rightarrow E0\rightleftharpoons C\) and \(B\rightarrow E1\rightleftharpoons D\) so \(R \models A=C\) and \(R \models B=D\). If \(E\) is not an atom it has the form \(E0\rightarrow E1\) and no reductions use the entire expression as a redex. Thus \(A\rightleftharpoons E0\rightleftharpoons C\) and \(B\rightleftharpoons E1\)
Conversely every invertible type algebra can be presented as a simultaneous recursion together with a logically trivial set of identities between atoms. This will be seen below.

**Solvability of Equations**

The type algebra $T$ is said to solve the equation $A = B$ if there is a homomorphism (substitution) $h$ such that $T \vdash h(A) = h(B)$. Here we wish to determine all solutions to a system $S$ in a simultaneous recursion $R$. Note that for any homomorphism $h$, $h(S)$ has the invertibility property. Let $\vdash^*$ refer to a congruence generated by using the invertibility rule in addition to the laws of logic. For each sub-congruence class $S[p] = \{q \mid q \text{ an atom and } S \vdash^* q = p \}$ pick a canonical member $p^*$ and let $A[p^*]$ be any shortest type expression such that:

1. $S \vdash^* p^* = A[p^*]$

Put $S^* = \{p^* = A[p^*] \mid A[p^*] \text{ a non-atom} \}$ and let $T = \{ p = p^* \mid p \text{ an atom} \}$. We claim that $S^* \cup T$ logically implies $S$. To see this we prove by induction that if $B$ is built up only from *'ed atoms and $S \vdash^* p^* = B$ then $S^* \vdash^* p^* = B$. This is trivial if $B$ is $p^*$ itself. Otherwise $B = C \rightarrow D$ and $A[p^*] = A_0 \rightarrow A_1$, and $S \vdash^* C = A_0 \& D = A_1$. Now, by induction hypothesis $S^* \vdash^* C = A_0 \& D = A_1$, thus $S^* \vdash^* p^* = B$. The claim now follows easily. Since $S \vdash^* S^* \cup T$ we now see that that $S$ and $S^* \cup T$ have the same solutions in any simultaneous recursion $R$. Since $T$ is logically trivial we now consider only the problem of solving simultaneous recursions $S$ in simultaneous recursions $R$. This show the claim above that invertibility $\Rightarrow$ recursiveness.

Note also that if $p^*$ does not appear in $A[p^*]$ then $p^*$ can be eliminated by substitution, so we shall assume that $S$ is a simultaneous recursion such that $p = A : S \Rightarrow p$ appears in $A$. 
Given a homomorphism \( h \) we may think of \( h \) as a substitution of expressions for atoms. Since \( R^+ \) is terminating & Church-Rosser we may assume that the expression substituted for an atom is in normal form. Thus we have \( h(A) \gg h(p) \) for each \( p=A:S \). Now any occurrence of \( h(p) \) in \( h(A) \) can have no residual in \( h(p) \) so, since \( h(p) \) is itself normal, \( h(p) \) must be a subexpression of an \( R^+ \) redex. This bounds all solutions of \( S \) in \( R \).

These remarks imply that solvability of \( S \) in \( R \) is an NP time problem. Indeed we have the

**PROPOSITION** The solvability of \( S \) in \( R \) is NP complete even for a fixed \( R \).

**PROOF:** For each \( k \) define \( R_k \) as follows. \( R_k \) has the \( k \) atoms \( c_1, c_2, \ldots, c_k \), and \( d\langle i,j\rangle \) for \( 0<i<j<k+1 \). It consists of the identities

\[
d\langle i,j\rangle = c_i \rightarrow (c_j \rightarrow d\langle i,j\rangle)
\]

for \( 0<i<j<k+1 \).

The fixed \( R \) mentioned above will be \( R_3 \). We shall encode graph colorability into solvability in the \( R_k \) above. Suppose the graph \( G=(V,E) \) is given. Define the simultaneous recursion \( S(G) \) as follows.

The atoms of \( S(G) \) are \( v_1, \ldots, v_n \) for \( V=\{v_1, \ldots, v_n\} \), and \( e_{\langle i,j\rangle} \) for each \( \langle i,j\rangle \in E \). The identities of \( S(G) \) are the following

\[
e_{\langle i,j\rangle} = v_i \rightarrow (v_j \rightarrow e_{\langle i,j\rangle})
\]

for \( \langle i,j\rangle \in E \).

Now suppose that \( F \) is a \( k \) coloring of \( G \) in the colors \( \{c_1, \ldots, c_k\} \). We define a homomorphism \( h \) by

\[
h(vi) = F(vi)
\]

\[
h(e_{\langle i,j\rangle}) = d\langle F(i), F(j)\rangle
\]

where we assume \( F(i) < F(j) \).

Clearly \( h \) solves \( S(G) \) in \( R_k \). Now suppose that \( h \) is a solution of \( S(G) \) in \( R_k \). By invertibility and Church-Rosser there exists a \( k \) coloring \( F \) in \( \{c_1, \ldots, c_k\} \) such that \( h(vi) = F(vi) \). Thus \( S(G) \) is solvable in \( R_k \) \( \iff \) \( G \) is \( k \) colorable.

Let \( \sim \) be the equivalence relation on atoms generated
by the relation $p[q$ if $VA (p=A:S \& q \text{ appears in } A)$. Let $[-$ be the corresponding poset of equivalence classes. We have the following

COROLLARY When $[-$ is a flat ordering the problem of determining if $S$ is solvable in $R$ is $P$-time.

PROOF: We need only try each subexpression in $R$ for any particular atom of $S$, for each equivalence class of $][-$, independently.

TYPING LAMBDA TERMS

Given a type algebra $T$ we can type lambda terms a’la Church or a’la Curry ([2] but see [3]). If $H$ is a basis then we write $H |- M:A$ for the typing judgement that $M:A$ is derivable from the basis $H$. The two notions of typing are equivalent for any type algebra $T$.

The subject reduction theorem for $T$ is the statement $H |- M:A \& M \rightarrow N \Rightarrow H |- N:A$ for $\rightarrow$ taken as beta reduction.

A type algebra $T_0$ is said to be an expansion of the type algebra $T_1$ if the atoms of $T_1$ are a subset of the atoms of $T_0$ and the identities of $T_0$ are logically equivalent to those of $T_1$ plus a set of identities $p=q$ for $p$ an atom of $T_1$ and $q$ an atom of $T_0$, and each $q$ occurring at most once. We shall prove the

THEOREM The following are equivalent

(1) $T$ is an expansion of a simultaneous recursion
(2) $T$ is invertible
(3) $T$ satisfies the subject reduction theorem

PROOF: We have in essence already proved that (1) and (2) are equivalent. For the proof that (2)$\Rightarrow$(3) we need only copy the proof in [a] observing that all that is used about $T$ is the invertibility property. Now suppose $\neg$(2), we shall show $\neg$(3). Suppose that $T |- A \rightarrow B = C \rightarrow D$ but either $\neg T |- A = C \lor \neg T |- T$
B=D for A->B shortest with this property and A=B if possible within these constraints. We distinguish two cases

(1) $\sim T \vdash B=D$

We have $y:B, z:C \vdash (\lambda x.y)z:D$ but not $y:B, z:C \vdash y:D$ by the generation lemma for $\lambda \to -$ Curry ([2]). Thus subject reduction fails.

(2) $T \vdash B=D \land \sim T \vdash A=C$

Let $A=A_1 \to (\ldots (A_s \to p) \ldots)$. We have the following

$u:p \to B, v:A \to p, y:C \vdash (\lambda x.u(vx))y:D$

Suppose that

$u:p \to B, v:A \to p, y:C \vdash u(vy):D$

By the generation lemma there exists a type expression $E$ s.t. $T \vdash p \to B=E \to D \land A \to p=C \to E$. We argue by cases

(i) $s>0$

In this case $p \to B$ is shorter than $A \to B$ so by choice of $A \to B$ we have $T \vdash p=E$. We have

$x_1:A_1, \ldots, x_s:A_s, y:C \vdash (\lambda x. xx_1 \ldots x_s)y:p$

Suppose that

$x_1:A_1, \ldots, x_s:A_s, y:C \vdash yx_1 \ldots x_s:p$.

Then by the generation lemma

$x_1:A_1, \ldots, x_s:A_s, y:C \vdash y:A$

hence $T \vdash A=C$ contradicting the choice of case. Thus the subject reduction theorem fails.

(ii) $s=0$

In this case we have $T \vdash p \to B=E \to D \land p \to p=C \to E$. By the special choice of $A \to B$, since $p=A$ and $\sim T \vdash A=C$ we have $p=B$. Thus we have

$y:E \vdash (\lambda x.y)p$

and

$z:C \vdash (\lambda x.z):E$. 

If subject reduction holds in both cases we have
\[
y : E \vdash y : p \\
z : C \vdash z : E
\]
and by the generation lemma \( T \vdash C = E = p = A \). This contradicts
the choice of case and subject reduction must fail.

Thus in all cases subject reduction fails. This completes
the proof.

REFERENCES

[1] Barendregt The Lambda Calculus
North Holland 1984

[2] Lambda calculi with types
in Handbook of Logic in Computer Science
Abramsky, Gabbay, & Maibaum eds.
North Holland 1992

[3] Breazu-Tannen & Meyer Lambda calculus with constrained
    types
in LNCS 193: Logics of Programs
    Parikh ed
    Springer-Verlag 1985

[4] Coppo & Cardone Type inference with recursive types
    Information and Computation
    1992

[5] Kozen Finitely presented algebras and the polynomial
time hierarchy
Dept of Comp. Sci. Tech. Report 77-303
Cornell Univ. 1977

[6] Complexity of finitely presented algebras
Dept. of Comp. Sci. Tech. Report 76-294
Cornell Univ. 1976

[7] Le Chenadec Cannonical Forms in Finitely Presented
[8] Mendler, Recursive types and type constraints...
in Proceedings LICS 1987
IEEE 1987

[9] Scott, Some philosophical issues concerning theories of combiners
in LNCS 37: Lambda Calculus and Computer Science Theory
Bohm ed
Springer-Verlag 1975