Type Inference for Recursively Constrained Types and its Application to OOP

Jonathan Eifrig*† Scott Smith* Valery Trifonov*†

The Johns Hopkins University ‡

November 16, 1994

1 Introduction

This paper addresses the problem of designing an object-oriented programming language with an effective type inference mechanism. Recently developed programming languages including Standard ML and Haskell incorporate type inference as a core component of the language. However, type inference has yet to achieve practical application to object-oriented programming languages.

We strongly feel the core type features necessary to model object-oriented programming with type inference include a notion of subtyping [CW85], and a notion of "recursively constrained polymorphism," a generalization of F-bounded polymorphism [CHC90, CCH+89].

Recursively constrained types κ are types of the form $\tau \setminus C$, with " $\setminus$ " reading "where." C is a set of type constraints of the form $\tau_1 \leq \tau_2$, possibly containing free type variables. These constraints may be *recursive* in that a variable t could occur free in both τ_1 and τ_2. The recursive constraint set $\{t \rightarrow \mathsf{Nat} \leq t, t \leq t \rightarrow \mathsf{Nat}\}$ expresses $t = t \rightarrow \mathsf{Nat}$, so recursively constrained types subsume recursive types. We will use *rc type* to abbreviate recursively constrained type.

Polymorphic rc types are types $\forall t_1, \ldots, t_n. \tau \setminus C$ where constraints $\tau_1 \leq \tau_2$ in C may contain type variables $t_1, \ldots t_n$ free. Polymorphic rc types generalize the more well-known bounded types [CW85] $\forall t \leq \tau. \tau'$ in several ways. First, they are recursive, so t could occur free in τ; this is not allowed in bounded types. Types with t occurring free in τ are the so-called F-bounded types [CCH+89]. Polymorphic rc types generalize F-bounded types by allowing more than one upper bound on a type variable, as well as allowing multiple lower-bound constraints $\tau \leq t$. This generalized form of polymorphic type is very useful in typing object-oriented programs that are otherwise untypable, irrespective of the question of type inference. An example of such a program is given in Section 5 below.

It is not difficult to see how rc polymorphism is useful in typing classes and objects, for it is at least as useful as F-bounded polymorphism. Classes may have so-called binary methods that refer to the type of objects of their own class; for instance an object with an **equal** method takes as parameter another object of its own type. Thus, a self-type is needed. And, this self-type needs to be open-ended since a class may be extended; we wish the type of **self** to be "an object with all

*Partially supported by NSF grants CCR-9109070 and CCR-9301340

†Partially supported by AFOSR grant F49620-93-1-0169

‡Contact: Scott Smith, Department of Computer Science, The Johns Hopkins University, Baltimore, Maryland 21218. E-mail: scott@cs.jhu.edu. Fax: (410) 516-6134. Phone: (410) 516-5299

the methods currently defined, and possibly additional ones". Polymorphic rc types capture this notion by constraining the polymorphic "self-type" t to include the current methods, for instance

$$\forall t.\, \tau \setminus \{t \leq \ldots \mathsf{equal} : t \to \mathsf{Bool}, \ldots\}$$

Binary methods have proven very difficult to type in a general way; it has even been suggested that they be disallowed.

One way to understand the usefulness of lower bounds $\tau \leq t$ in rc types are as generalizations of recursive types. It is possible to write an rc type $\kappa = t \setminus \{\tau_1 \leq t \leq \tau_2\}$ where lower bound τ_1 differs from upper bound τ_2 (it is a recursive type if $\tau_1 = \tau_2$). These generalized forms are useful as intermediate results produced during the type inference process as "partial" forms of recursive types. During the type inference process, constraints are accumulated on types in a "bottom-up" fashion, and so types at the leaves of typing proofs have small constraint sets, and have fat constraint sets at the root. The lower bound τ_1 constrains the "output" of the type κ (what properties objects of type κ must have); if an object of type κ is used (*i.e.*, passed to a function of type $\tau' \to \ldots$), an additional upper-bound constraint $t \leq \tau'$ will be placed on the type by the type inference mechanism, and this could only be contradictory if $\tau_1 \leq \tau'$, which follows by transitivity, was contradictory. The upper bound is the dual of this, constraining the "input" of the type (what functions of type $t \to \ldots$ must do).

The presence of multiple upper-bound constraints or multiple lower-bound constraints can be understood as a restricted form of union and intersection type: $\{\tau \leq t, \tau' \leq t\}$ would be equivalent to $\{\tau \vee \tau' \leq t\}$ if there were union types $\tau \vee \tau'$ in the language; a dual relationship exists between intersections and upper bounds. We believe general union and intersection types cause too many problems to be worthwhile, but this implicit restricted form is quite natural.

In this paper we develop a type inference algorithm for the I-Soop language (Inference Semantics of OOP). I-Soop is not an object-oriented language; however, it has an expressive enough type system so that typed OOP may be effectively encoded within I-Soop. We take a translational approach because we find the factoring to help clarify ambiguities; however, there is also merit in studying languages where objects themselves are primitive [AC94], and the concepts herein should eventually be recast as primitive object typings. I-Soop's type system contains both subtyping and polymorphic rc types. We infer shallow polymorphic rc types at let-expressions as in the Hindley/Milner algorithm [Mil78]. In addition the underlying language includes records and a notion of state, for with these features it is possible to obtain an effective encoding of object-oriented programming. Records are needed so record subtyping can be used to model object subtyping [CW85]. Without state, the critical state-holding property of objects is lost [ESTZ94].

Our approach to establishing the soundness of constrained type inference differs from other work in the literature. In other approaches (e.g. [AW93, Kae92, SY94, PS94]), a method is given that either produces a satisfying assignment to the constraints and thus establishes their consistency, or establishes that no such solution exists and the constraints are thus inconsistent. In our approach, an rc type's constraint system is considered "consistent" if it does not contain any "obvious" contradictions such as $\mathsf{Nat} \leq \mathsf{Bool}$. We show this view is sound, *without* ever showing the "consistent" constraint systems have solutions. Instead we directly establish a subject-reduction property over a proof of typing with "consistent" rc types at each node [Tof90, WF91]. We believe the standard method of finding solutions to the constraint sets can be overly restrictive, for it forces one to have a rich enough type language or type model that can express the solutions as types or sets. In our language, for instance, we expect general union and intersection types would be required to express the solution of constraints as types, but we do not wish to pay the penalty of having these types in our language.

We also take a more primitive approach to establishing the completeness of type inference, i.e. that all typable programs will successfully have some type inferred by the type inference algorithm. We first define a restricted set of typing rules, the *inference rules*, for which typing derivations are deterministic. Then these rules are shown equivalent in strength to the general form of rules, without recourse to a "principal types" property.

1.1 Related Work

A number of type inference systems have been developed that bear on the type inference problem for OOP. Papers of Reynolds [Rey85], Cardelli [Car84], and Mitchell [Mit84] are foundational papers in the field that develop the basic concepts of constraints and subtyping. Many papers have been written since; we focus on the more recent work the most relevant to ours.

Kaes [Kae92] develops a type inference algorithm for a language containing polymorphic and recursive types and type constraints. This work incorporates subtyping constraints, recursive types, and polymorphism. Kaes writes so-called constrained types $\tau|C$ in close analogy to our rc types $\tau \setminus C$. This approach cannot solve general recursive constraints: $t \leq \tau$ generates a non-terminating unification problem in his system if t occurs free in τ, while our approach can handle such constraints without difficulty. He does allow a "fixing" of such a constraint by replacing it with a recursive type $\mu t.\tau$, but at the cost of an important loss of generality. Kaes takes the standard approach to constraint consistency, by producing a solution to the constraints. He also intends $\leq$ to model overloading, not record subtyping (his system has no record types). Sekiguchi and Yonezawa [SY94] take an approach similar to Kaes but interpret $\leq$ as subtyping on record types, making it more directly applicable to object-oriented programming.

Palsberg, Schwartzbach, *et. al.* have written a number of papers concerning type inference for objects [PS94, OPS92, PS92, KPS92]. The main feature of their work is they do not take the Hindley/Milner approach to type inference. Instead, their inference algorithm uses flow analysis to generate a set of constraints about a program, and then applies another algorithm to come up with a solution to these constraints if it exists. Their work represents the current state-of-the-art in having a practical type inference algorithm for object-oriented programming languages. Other advantages of their approach include asymptotically efficient inference algorithms, and named class types. Their system however has no polymorphism, and they take a code-expansion view of inheritance, requiring re-type-checking with each class extension. This lack of polymorphism has been partially addressed by Plevyak and Chien [PC94].

Our work is closest to that of Aiken and Wimmers [AW93]. They develop a type system with subtyping, union and intersection types, and a form of polymorphic type similar to polymorphic rc types. They prove soundness using the ideal model [MPS86]. As with the previously mentioned researchers, they have an algorithm that produces a satisfying assignment to the top-level constraints to establish consistency of a constraint set. The satisfying assignment they produce is an ideal in the ideal model. We have no union, intersection, or negation types. These types prove problematic in their system, and they are in fact unnecessary for type inference — if they are not used in the types of atomic constructs, they are not generated by the inference algorithm (provided multiple upper and lower bounds to the same variable are allowed, as we do). Aiken and Wimmers have not addressed the problem of using their system for typing object-oriented programs; their language lacks important features necessary for the encoding of objects. In particular their language is a functional language without records. The ideal model cannot model languages with state, so their approach would not extend to a language with state. Aiken has implemented the type inference algorithm [Aik94], and this implemented system has an optimized inference algorithm and an implementation of extensible records.

Encoding object-oriented features within a more basic language is one possible approach to how object-oriented programming should be done [Rémy94]. We could take a similar approach by programming in an object-oriented style via the encoding of objects in I-Soop that we give in Section 5. Rémy gives a collection of extensions to ML that allow OOP to be encoded. Rémy is the only author amongst of those previously discussed who has a proof of soundness of his system in the presence of reference cells. His encoding is missing a notion of subtyping and thus lacks the core feature of object lifting: allowing subclass objects to be implicitly coerced to be superclass objects. Instead, coercion functions must be explicitly supplied. Rémy's encoding is more efficient than the encoding we use; each object creation in our encoding entails forming closures for each method of the object. If our language were to be used as a primitive OOP language, some more efficient object representations would need to be developed. Rémy's system also has a notion of extensible record, which we expect will be useful for encoding delegation-style object-oriented programming.

1.2 Outline

In Section 2 we present I-Soop and its operational semantics. Section 3 presents the I-Soop type system. In Section 4 the proof of subject reduction and type inference are sketched; a more detailed proof of subject reduction is found in Appendix A. Then, to show how OOP can be faithfully encoded, an extended example is worked in Section 5. This example also serves to illustrate the power of the type inference system. We draw some final conclusions in Section 6.

2 The I-Soop Language

We begin by defining the I-Soop language, which is roughly call-by-value PCF with records, reference cells, and let-expressions.

$$\begin{array}{lcl}
\mathit{Var} & \ni & x \\
\mathit{Num} & \ni & n ::= \mathsf{0} \mid \mathsf{1} \mid \mathsf{2} \mid \ldots \\
\mathit{Val} & \ni & v ::= x \mid n \mid \lambda x.\, e \mid \{\overline{m = v}\} \\
\mathit{Exp} & \ni & e ::= v \mid e\ e \mid \mathsf{let}\ x = e\ \mathsf{in}\ e \mid \mathsf{if}\ e\ \mathsf{then}\ e\ \mathsf{else}\ e \mid \{\overline{m = e}\} \mid e.m
\end{array}$$

The "vector notation" $\overline{m = v}$ is shorthand for $m_1 = v_1, \ldots, m_k = v_k$ for some k; $\overline{m_i = v_i}$ is shorthand for the same and indicates i will range over the elements of the vector. The set $B = \{\mathsf{true}, \mathsf{false}, \mathsf{pred}, \mathsf{succ}, \mathsf{is\_zero}, \mathsf{ref}, !, \mathsf{set}\} \subset \mathit{Var}$ contains the built-in boolean constants as well as the primitive functions on numbers and reference cells.

A *store* (ranged over by s) is a finite mapping from variables to values. A *configuration* $\langle s, e\rangle$ is a pair of a store and an expression. Computation is defined via a single-step relation $\mapsto_1$ between configurations. A *reduction context* R is an expression with a "hole" $\circ$ in it, into which one may put a subexpression via $R[e]$. Reduction contexts serve to isolate the next step of computation to be performed—it is always in the hole.

Definition 2.1 A reduction context is defined as

$$\begin{array}{rl}
R ::= & \circ \mid R\ e \mid v\ R \mid \mathsf{let}\ x = R\ \mathsf{in}\ e \mid \mathsf{if}\ R\ \mathsf{then}\ e\ \mathsf{else}\ e \\
& \mid \{ m_1 = v_1, \ldots, m_{i-1} = v_{i-1}, m_i = R, m_{i+1} = e_{i+1}, \ldots, m_k = e_k \} \mid R.m
\end{array}$$

Definition 2.2 $\mapsto_1$ is the least relation on configurations such that

$$
\begin{array}{rcll}
\langle s,\, R[\textsf{if true then } e_1 \textsf{ else } e_2]\rangle & \mapsto_1 & \langle s,\, R[e_1]\rangle & \\
\langle s,\, R[\textsf{if false then } e_1 \textsf{ else } e_2]\rangle & \mapsto_1 & \langle s,\, R[e_2]\rangle & \\
\langle s,\, R[\textsf{let } x = v \textsf{ in } e]\rangle & \mapsto_1 & \langle s,\, R[e[v/x]]\rangle & \\
\langle s,\, R[(\lambda x.\, e)\ v]\rangle & \mapsto_1 & \langle s,\, R[e[v/x]]\rangle & \\
\langle s,\, R[\textsf{is\_zero } 0]\rangle & \mapsto_1 & \langle s,\, R[\textsf{true}]\rangle & \\
\langle s,\, R[\textsf{is\_zero } n]\rangle & \mapsto_1 & \langle s,\, R[\textsf{false}]\rangle & (\text{if } n \neq 0) \\
\langle s,\, R[\textsf{succ } n]\rangle & \mapsto_1 & \langle s,\, R[n']\rangle & (\text{if } n' = n + 1) \\
\langle s,\, R[\textsf{pred } n]\rangle & \mapsto_1 & \langle s,\, R[n']\rangle & (\text{if } n' = n \dot{-} 1) \\
\langle s,\, R[\{\, \ldots, m = v,\, \ldots \,\}.m]\rangle & \mapsto_1 & \langle s,\, R[v]\rangle & \\
\langle s,\, R[\textsf{ref } v]\rangle & \mapsto_1 & \langle s \| [\, x \mapsto v \,],\, R[a]\rangle & (x \notin \mathit{dom}(s) \cup B) \\
\langle s,\, R[!x]\rangle & \mapsto_1 & \langle s,\, R[s(x)]\rangle & (x \in \mathit{dom}(s)) \\
\langle s,\, R[\textsf{set } \{\, \textsf{cell} = x, \textsf{val} = v \,\}]\rangle & \mapsto_1 & \langle s \| [\, x \mapsto v \,],\, R[v]\rangle & (x \in \mathit{dom}(s))
\end{array}
$$

where

$e[e'/x]$ is the capture-free substitution of e' for x in e,
$[\, x \mapsto v \,]$ is the map defined only on x with result v,
$f \| g$ is the functional extension of f by g.

Here is a sample execution.

$$
\begin{array}{l}
\langle \emptyset,\, (\lambda \textsf{x}.\, \textsf{succ } (!(\textsf{x.field})))\ \{\, \textsf{field} = \textsf{ref } 5 \,\}\rangle \mapsto_1 \langle [\, \textsf{y} \mapsto 5 \,],\, (\lambda \textsf{x}.\, \textsf{succ } (!(\textsf{x.field})))\ \{\, \textsf{field} = \textsf{y} \,\}\rangle \mapsto_1 \\
\langle [\, \textsf{y} \mapsto 5 \,],\, \textsf{succ } (!(\{\, \textsf{field} = \textsf{y} \,\}.\textsf{field}))\rangle \mapsto_1 \langle [\, \textsf{y} \mapsto 5 \,],\, \textsf{succ } (!\textsf{y})\rangle \mapsto_1 \langle [\, \textsf{y} \mapsto 5 \,],\, \textsf{succ } 5\rangle \mapsto_1 \langle [\, \textsf{y} \mapsto 5 \,],\, 6\rangle
\end{array}
$$

Lemma 2.3

(i) $\mapsto_1$ is deterministic: if $\langle s,\, e\rangle \mapsto_1 \langle s',\, e'\rangle$ and $\langle s,\, e\rangle \mapsto_1 \langle s'',\, e''\rangle$, then there is a uniform renaming of variables in s' and e' to those in s'' and e'' respectively.

(ii) $\mapsto_1$ is compositional: if $\langle s,\, e\rangle \mapsto_1 \langle s',\, e'\rangle$, then $\langle s,\, R[e]\rangle \mapsto_1 \langle s',\, R[e']\rangle$ for every reduction context R.

3 I-Soop Types

The monomorphic types of the language are

$$
\begin{array}{lcl}
\mathit{TyVar} \ni \alpha & ::= & t \mid u \\
\mathit{Typ} \ni \tau & ::= & \alpha \mid \textsf{Nat} \mid \textsf{Bool} \mid \tau \to \tau' \mid \{\, \overline{m : \tau} \,\} \mid \tau \textsf{ ref}
\end{array}
$$

where t ranges over the *applicative* type variables $\mathit{AppTyVar} \stackrel{\text{def}}{=} \{\textsf{t}_1, \textsf{t}_2, \ldots\}$, and u ranges over the *imperative* ones: $\mathit{ImpTyVar} \stackrel{\text{def}}{=} \{\textsf{u}_1, \textsf{u}_2, \ldots\}$. This division of variables into two classes is similar to that of Standard ML. The set of free type variables in a type τ is $FTV(\tau)$; τ is *imperative* if $FTV(\tau) \subseteq \mathit{ImpTyVar}$.

A *type constraint* is a subtyping assertion between two (monomorphic) types, written $\tau_1 \leq \tau_2$. We will require all sets of constraints used in types and rules to be implicitly closed under obvious laws.

Definition 3.1 (Constraint System) A set of type constraints C is *closed* iff

(i) If $\tau_1 \leq \tau_2 \in C$ and $\tau_2 \leq \tau_3 \in C$, then $\tau_1 \leq \tau_3 \in C$.

(ii) If $\tau_1 \rightarrow \tau_1' \leq \tau_2 \rightarrow \tau_2' \in C$, then $\{\tau_2 \leq \tau_1,\ \tau_1' \leq \tau_2'\} \subseteq C$.

(iii) If $\{\overline{m_i : \tau_i}\} \leq \{\overline{m_j : \tau_j'}\} \in C$ and $\{\overline{m_i}\} \supseteq \{\overline{m_j}\}$, then $\{\overline{\tau_j \leq \tau_j'}\} \subseteq C$.

(iv) If $\tau_1\ \mathsf{ref} \leq \tau_2\ \mathsf{ref} \in C$, then $\{\tau_1 \leq \tau_2,\ \tau_2 \leq \tau_1\} \subseteq C$.

A closed set of constraints is a *constraint system.*

We let C range over (implicitly closed) constraint systems, and thus will be careful to make sure any new set of constraints we form is closed. The closed union of sets of constraints is denoted by $C_1 \uplus C_2$, an operation that by inspection can be seen to be associative.

Definition 3.2 (Constraint Consistency) A constraint $\tau_1 \leq \tau_2$ is *consistent* if

(i) $\tau_1 \in \mathit{TyVar}$ or $\tau_2 \in \mathit{TyVar}$;

(ii) $\tau_1 = c_t(\overline{\tau})$ and $\tau_2 = c_t(\overline{\tau'})$, where c_t is a type constructor other than a record; or

(iii) $\tau_1 = \{\overline{m : \tau}\}$, $\tau_2 = \{\overline{m' : \tau'}\}$, and $\{\overline{m}\} \supseteq \{\overline{m'}\}$.

Otherwise a constraint is *inconsistent.*

For example, $\mathsf{Nat} \leq \mathsf{t} \rightarrow \mathsf{Nat}$ and $\mathsf{t\ ref} \leq \{\mathsf{m} : \mathsf{Bool}\}$ are inconsistent constraints, while $\mathsf{t} \leq \mathsf{t}' \rightarrow \mathsf{Bool}$, $\mathsf{t} \leq \mathsf{u}$, and $\mathsf{u} \leq \mathsf{Bool}$ are each consistent. A constraint system is consistent if all the constraints in the system are consistent. The rules will require all constraint systems to implicitly be consistent.

The type system assigns I-Soop expressions *rc types* of the form

$$\kappa ::= \tau \setminus C$$

to indicate an expression of type τ which is constrained by the constraints in C. Since the rules implicitly require C to be consistent, it makes sense to view κ as a type and to write C on the right side of the turnstile as part of the type.

We define the following notion of subtyping on rc types.

Definition 3.3 (Subtyping rc Types) $\tau \setminus C \leq \tau' \setminus C'$ provided that C' is consistent and either $C \uplus \{\tau \leq \tau'\} \subseteq C'$, or $\tau = \tau'$ and $C \subseteq C'$.

Stronger notions of subtyping could be defined, but for our purposes this definition suffices. The type schemes σ are as follows.

$$\sigma ::= \tau \mid \forall \overline{\alpha}.\ \kappa$$

Note that since $\kappa = \tau \setminus C$ can contain an arbitrary collection of constraints C, shallow F-bounded polymorphic types are a special case of these polymorphic rc types.

3.1 I-Soop Typing Rules

Before giving the rules we describe notation used in the rules. Notation used in sequent judgements includes the following. A *type environment* A is a mapping from variables to type schemes; we use the more intuitive notation $[\,x : \sigma\,]$ instead of $[\,x \mapsto \sigma\,]$. Given a type environment A, the proof system assigns to an expression e a rc type $\tau \setminus C$, written as the *type judgement* $A \vdash e : \tau \setminus C$, under the condition that C is consistent (as mentioned previously, all constraint sets C appearing in the rules implicitly *must* be consistent); we occasionally may write $A \vdash e_1 : \tau_1 \setminus C_1,\ e_2 : \tau_2 \setminus C_2,\ \ldots$ to indicate several type judgements provable in the same environment. Programs are type-checked in the initial environment A_0 assigning the following type schemes to the built-ins:

$$\begin{aligned} A_0 = [\,&\mathsf{true} : \mathsf{Bool},\ \mathsf{false} : \mathsf{Bool},\ \mathsf{pred} : \mathsf{Nat} \rightarrow \mathsf{Nat},\ \mathsf{succ} : \mathsf{Nat} \rightarrow \mathsf{Nat},\ \mathsf{is\_zero} : \mathsf{Nat} \rightarrow \mathsf{Bool},\\ &\mathsf{ref} : \forall \mathsf{u}.\ \mathsf{u} \rightarrow \mathsf{u\ ref},\ ! : \forall \mathsf{t}.\ \mathsf{t\ ref} \rightarrow \mathsf{t},\ \mathsf{set} : \forall \mathsf{t}.\ \{\mathsf{cell} : \mathsf{t\ ref}, \mathsf{val} : \mathsf{t}\} \rightarrow \mathsf{t}\,] \end{aligned}$$

$$
(\mathsf{Sub})\quad \frac{A \vdash e : \kappa, \quad \kappa \leq \kappa'}{A \vdash e : \kappa'}
$$

$$
(\mathsf{App})\quad \frac{A \vdash e_1 : \tau \to \tau' \setminus C_1, \quad e_2 : \tau \setminus C_2}{A \vdash e_1\ e_2 : \tau' \setminus C_1 \uplus C_2}
\qquad
(\mathsf{Abs})\quad \frac{A || [x : \tau] \vdash e : \tau' \setminus C}{A \vdash \lambda x.\, e : \tau \to \tau' \setminus C}
$$

$$
(\mathsf{PVar})\quad \frac{A(x) = \forall \overline{\alpha}.\, \kappa, \quad \Psi \text{ is a substitution on } \{\overline{\alpha}\}}{A \vdash x : \Psi \kappa}
\qquad
(\mathsf{Var})\quad \frac{A(x) = \tau}{A \vdash x : \tau \setminus \emptyset}
$$

$$
(\mathsf{Record})\quad \frac{A \vdash \overline{e_i : \tau_i \setminus C_i}}{A \vdash \{\overline{m_i = e_i}\} : \{\overline{m_i : \tau_i}\} \setminus \biguplus_i C_i}
\qquad
(\mathsf{Sel})\quad \frac{A \vdash e : \{m : \tau\} \setminus C}{A \vdash e.m : \tau \setminus C}
$$

$$
(\mathsf{Cond})\quad \frac{A \vdash e_1 : \mathsf{Bool} \setminus C_1, \ e_2 : \tau \setminus C_2, \ e_3 : \tau \setminus C_3}{A \vdash \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 : \tau \setminus C_1 \uplus C_2 \uplus C_3}
\qquad
(\mathsf{Num})\quad \frac{}{A \vdash n : \mathsf{Nat} \setminus \emptyset}
$$

$$
(\mathsf{Let})\quad \frac{A \vdash e : \tau \setminus C, \quad A || [x : \forall \overline{\alpha}.\, \tau \setminus C] \vdash e' : \tau' \setminus C', \quad \Phi \text{ is a renaming of } \{\overline{\alpha}\}}{A \vdash \mathsf{let}\ x = e\ \mathsf{in}\ e' : \tau' \setminus \Phi C \uplus C'}
$$

$$
\text{where } \{\overline{\alpha}\} \subseteq \begin{cases} \text{if } e \text{ is expansive then } \mathit{AppClos}(\tau \setminus C, A) \\ \text{else } \mathit{Clos}(\tau \setminus C, A) \end{cases}
$$

Figure 1: Typing rules of I-Soop.

A *substitution* on $\{\overline{\alpha}\}$ is a map $\Psi \in \mathit{TyVar} \to \mathit{Typ}$ which is the identity on $\mathit{TyVar} \setminus \{\overline{\alpha}\}$ and maps $\mathit{ImpTyVar}$ to imperative types; a *renaming* Φ of $\{\overline{\alpha}\}$ is a substitution on $\{\overline{\alpha}\}$ with $\mathit{codom}(\Phi) \subseteq \mathit{TyVar}$. An expression is *expansive* if and only if it is not a value; following Tofte [Tof90] we form type schemes by making the sets of type variables we generalize over dependent on the expansiveness of the expression. The definitions of these sets are

$$
\begin{aligned}
\mathit{Clos}(\tau \setminus C, A) &= (\mathit{FTV}(\tau) \cup \mathit{FTV}(C)) \setminus \mathit{FTV}(A) \\
\mathit{AppClos}(\tau \setminus C, A) &= \mathit{Clos}(\tau \setminus C, A) \cap \mathit{AppTyVar}
\end{aligned}
$$

where the functionality of FTV is extended as usual to constraint systems, rc types, type schemes, and type environments.

The typing rules for I-Soop are given in Figure 1. Most of the rules have obvious relation to those of standard systems with subtyping and records; as in Tofte's system [Tof90], the typing of ref introduces imperative types. The main difference is the addition of constraints as part of types, the associated subsumption rule on these types, and the way consistent constraints accumulate from the leaves to the root of a typing proof. It is important to observe that consistency of constraints is implicitly enforced by each rule. Other presentations of constrained type systems [Mit84, AW93, Kae92] do not require local consistency, so the constraints in the rules have both a hypothetical and assertional component. They are hypothetical in that they may be inconsistent, and they are assertional in that they assert properties of the type if they are consistent. For this reason they write C on the left of the turnstile, and perform some top-level consistency check before a proved typing is "true." Since constraints are never inconsistent in our rules we have no hypothetical component and constraints are thus written on the right-hand side of the turnstile.

Some justification is required for the (Let) rule, in which the constraint system of the let expression contains not only the constraints in C', necessary for typing its body, but also those in C, accumulated for the type of the bound variable. Leaving the latter constraints out (as [AW93] do) results in a system unsound with respect to the standard call-by-value semantics of the let expression; C may contain constraints on type variables free in the environment, and their omission may lead to accepting programs which get stuck while evaluating the expression assigned to the bound variable. As an example, consider the expression

$$
(\lambda \mathsf{x}.\ \mathsf{let}\ \mathsf{y} = !\mathsf{x}\ \mathsf{in}\ \mathsf{succ}\ \mathsf{x})\ 5
$$

By rules (PVar), (Var), (Sub), and (App) the constraint system C of the rc type of $\mathsf{!x}$ contains $\tau \leq \tau'\ \mathsf{ref}$ for some type τ', where τ is the type associated with x by the rule (Abs). This constraint will lead to inconsistency when combined with the constraint $\mathsf{Nat} \leq \tau$ at the outermost rule of the typing proof, (App). If it were omitted from the constraint system of the let, the other constraint on τ, namely $\tau \leq \mathsf{Nat}$ from the body $\mathsf{succ\ x}$, would not cause an inconsistency, and the program would type-check; however its execution obviously leads to the stuck state $\langle \emptyset,\ \mathsf{let\ y = !5\ in\ succ\ 5} \rangle$.

While the type language does not have recursive types, $\lambda\mathsf{x}.\,\mathsf{x\ x}$ can be given the rc type $\mathsf{t}_1 \rightarrow \mathsf{t}_2 \setminus \{\mathsf{t}_1 \leq \mathsf{t}_1 \rightarrow \mathsf{t}_2\}$. We do not have a "bottom" type, but its positive occurrences may be simulated by an unconstrained type variable, e.g. $(\lambda\mathsf{x}.\,\mathsf{x\ x})\ \lambda\mathsf{x}.\,\mathsf{x\ x}$ has the rc type

$$\mathsf{t}_2 \setminus \{\mathsf{t}_1 \rightarrow \mathsf{t}_2 \leq \mathsf{t}_1,\ \mathsf{t}_1 \leq \mathsf{t}_1 \rightarrow \mathsf{t}_2\}$$

An unconstrained variable can also be used instead of a "top" type in negative positions. Positive occurrences of "top" may be simulated by overconstraining from below:

$$A_0 \vdash \mathsf{if\ true\ then\ true\ else}\ 5\ :\ \mathsf{t} \setminus \{\mathsf{Nat} \leq \mathsf{t},\ \mathsf{Bool} \leq \mathsf{t}\}$$

This constraint system is consistent. Note that not all typable programs are of this particular "top" type, but they are provably of type $t \setminus \{\mathsf{Nat} \leq t,\ \mathsf{Bool} \leq t\} \uplus C$ for some C and fresh t by a single use of (Sub). Similarly overconstraining from above achieves the effect of "bottom" in negative positions.

4 Subject Reduction, Soundness, and Type Inference

We prove soundness of the type system by demonstrating a subject reduction property. First extend the notion of typing to configurations:

DEFINITION 4.1 $A \vdash \langle s,\ e \rangle\ :\ \tau \setminus C$ if and only if

1. $A \vdash e\ :\ \tau \setminus C$;
2. $dom(A) = dom(A_0) \cup dom(s)$, $dom(A_0) \cap dom(s) = \emptyset$, and $A|_{dom(A_0)} = A_0$;
3. for each $x \in dom(s)$ we have $A(x) = \tau_x\ \mathsf{ref}$ and $A \vdash s(x)\ :\ \tau_x \setminus C_x$ for some τ_x and $C_x \subseteq C$.

THEOREM 4.2 (SUBJECT REDUCTION) If $A \vdash \langle s,\ e \rangle\ :\ \kappa$, then either $e \in \mathit{Val}$ or else $\langle s,\ e \rangle \mapsto_1 \langle s',\ e' \rangle$ and there exists an environment A' such that $A' \vdash \langle s',\ e' \rangle\ :\ \kappa$.

The full proof of subject reduction appears in Appendix A; here we provide an overview. The proof proceeds in the standard fashion: given a configuration and a proof of its typability, perform one step of computation and transform the original typing proof into a proof for the new configuration. The interaction between let-polymorphism and reference cells is known to cause significant difficulty [Tof90]; our approach to this problem derives from [WF91], avoiding Tofte's complex greatest fixed-point construction.

The differences between our proof and that of [WF91] result from the constraint systems of rc types and polymorphic rc types. Each step of computation is accompanied by a proof transformation that pushes constraints present near the top of the proof tree towards the leaves. The complications of the proof arise when these constraints are pushed through uses of the (Let) rule; demonstrating that the type generalizations performed in the initial application of the rule remain valid is non-trivial.

This pushing of constraints from the root of the typing proof towards the leaves during reduction can be considered a lazy approach to proof canonicalization. An alternative approach would be to

$$\text{(App)}\quad \frac{A \vdash_{\mathrm{inf}} e_1 : \tau_1 \setminus C_1, \quad e_2 : \tau_2 \setminus C_2}{A \vdash_{\mathrm{inf}} e_1\ e_2 : t \setminus C_1 \uplus C_2 \uplus \{\tau_1 \leq \tau_2 \rightarrow t\}} \qquad \text{(Abs)}\quad \frac{A \| [x : t] \vdash_{\mathrm{inf}} e : \tau \setminus C}{A \vdash_{\mathrm{inf}} \lambda x.\, e : t \rightarrow \tau \setminus C}$$

$$\text{(PVar)}\quad \frac{A(x) = \forall \overline{\alpha}.\ \kappa, \quad \Phi \text{ is a renaming of } \{\overline{\alpha}\}}{A \vdash_{\mathrm{inf}} x : \Phi\kappa} \qquad \text{(Var)}\quad \frac{A(x) = \tau}{A \vdash_{\mathrm{inf}} x : \tau \setminus \emptyset}$$

$$\text{(Record)}\quad \frac{A \vdash_{\mathrm{inf}} \overline{e_i : \tau_i \setminus C_i}}{A \vdash_{\mathrm{inf}} \{\,\overline{m_i = e_i}\,\} : \{\,\overline{m_i : \tau_i}\,\} \setminus \biguplus_i C_i} \qquad \text{(Sel)}\quad \frac{A \vdash_{\mathrm{inf}} e : \tau \setminus C}{A \vdash_{\mathrm{inf}} e.m : t \setminus C \uplus \{\tau \leq \{\, m : t \,\}\}}$$

$$\text{(Let)}\quad \frac{A \vdash_{\mathrm{inf}} e : \tau \setminus C, \quad A \| [x : \forall \overline{\alpha}.\ \tau \setminus C] \vdash_{\mathrm{inf}} e' : \tau' \setminus C'}{A \vdash_{\mathrm{inf}} \mathsf{let}\ x = e\ \mathsf{in}\ e' : \tau' \setminus C \uplus C'} \qquad \text{(Num)}\quad \frac{}{A \vdash_{\mathrm{inf}} n : \mathsf{Nat} \setminus \emptyset}$$

$$\text{where}\quad \{\overline{\alpha}\} = \begin{cases} \text{if } e \text{ is expansive then } \mathit{AppClos}(\tau \setminus C, A) \\ \text{else } \mathit{Clos}(\tau \setminus C, A) \end{cases}$$

$$\text{(Cond)}\quad \frac{A \vdash_{\mathrm{inf}} e_1 : \tau_1 \setminus C_1,\ e_2 : \tau_2 \setminus C_2,\ e_3 : \tau_3 \setminus C_3}{A \vdash_{\mathrm{inf}} \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3 : t \setminus C_1 \uplus C_2 \uplus C_3 \uplus \{\tau_1 \leq \mathsf{Bool},\ \tau_2 \leq t,\ \tau_3 \leq t\}}$$

Figure 2: Type inference rules of I-Soop.

regularize the initial typing proof of a program to canonical form by pushing all of the constraints present at the root to the leaves before performing any computation. This would result in a more straightforward subject reduction proof, at the expense of a more complicated proof canonicalization lemma.

The soundness of the type system is a corollary of the Subject Reduction theorem:

Theorem 4.3 (Soundness) If $A_0 \vdash e : \kappa$, then either e diverges, or e computes to a value.

Proof: By induction on the length of computation, using Theorem 4.2. □

Note we have thus proved soundness of the constrained type system without ever having shown the systems of constraints have a solution.

4.1 Type Inference

We now define the type inference algorithm and prove it is complete, i.e. if a program has a type derivation the inference algorithm will infer a type for it. The strategy we take to reach this desired outcome is the following.

1. Define a new set of rules (the *inference rules*) for which typing derivations are deterministic.
2. Prove the inference rules are equivalent in strength to the *general rules* we had been using previously.

The inference rules appear in Figure 2.

Theorem 4.4 For all terms e and environments A, it is decidable whether there exists a κ such that $A \vdash_{\mathrm{inf}} e : \kappa$.

Proof Sketch: By inspection of the rules, there is only one rule for typing each expression construct. By further inspection, the only nondeterminism that may be introduced in rule application is the choice of type variables used in rules (Abs) and (PVar). We thus choose *canonical* proofs that use fresh variables in every place possible. If a proof exists, there clearly must then be a corresponding canonical proof. For expression e the canonical proof is unique modulo α-conversion. Thus a decision procedure may be defined for constructing such a canonical proof. The algorithm fails when an inconsistent constraint system is obtained when combining the constraint systems inferred for subterms, and detection of such inconsistencies is trivially decidable. □

We now relate the inference rules to the general rules.

Theorem 4.5 (Completeness of Type Inference) Given an environment A and an expression e, the typing judgement $A \vdash e : \kappa$ is provable for some κ if and only if $A \vdash_{\text{inf}} e : \kappa'$ is provable for some κ'.

Proof Sketch: If $A \vdash_{\text{inf}} e : \kappa'$ is provable, $A \vdash e : \kappa$ is obviously provable as well; each inference rule is a special case of a combination of (Sub) and a general rule.

Conversely, a proof of $A \vdash e : \kappa$ can be transformed into a proof of $A \vdash_{\text{inf}} e : \kappa'$ in several stages. First, each assumption $x : \tau$ extending A by rule (Abs) is replaced with the assumption $x : t$ for some fresh t, and the constraint $\{t = \tau\}$ (shorthand for $\{t \leq \tau,\ \tau \leq t\}$) is added to the constraint system of each judgement. A use of the (Sub) rule is then used after each (Var) rule for x to lift $x : t$ to $x : \tau$; an application of (Sub) also follows (Abs) to reduce the domain t of the λ-abstraction back to τ. A similar transformation is then used to convert each substitution Ψ in the (PVar) rule into a renaming, replacing each type τ in the codomain of Ψ with fresh type variable t and adding the constraint $\{t = \tau\}$ as above. Finally, the proof is inductively transformed from the leaves to the root, replacing each general rule with its inference form. Uses of rule (Sub) are combined into the implicit subsumption present in each inference-style rule, whilst removing garbage constraints. $\square$

Thus from Theorems 4.5 and 4.4 we may conclude that every program typable under the general rules has a type inferred by the type inference algorithm. Note we establish no principal typing property. The typing produced by the inference algorithm is indeed "minimal" in an intuitive sense, but it is not formally minimal since our definition of $\kappa \leq \kappa'$ is weak: $t \rightarrow \mathsf{Nat} \setminus \{t \leq \mathsf{Nat}\}$ is not a subtype of $\mathsf{Nat} \rightarrow \mathsf{Nat} \setminus \emptyset$, even though any term that can be given the former type can also be given the latter. We leave the question of principal typings for future study, since completeness is ultimately all the programmer desires.

5 Applications to OOP

We now illustrate how this type inference algorithm is useful for typing object-oriented programs, the main motivation for our work. We show its utility in class-based OOP; we expect it also applies to delegation-style OOP but that topic is beyond the scope of this paper. The basic OOP concepts we wish to incorporate include standard notions of object, method, instance variable, class, inheritance, method/instance hiding, and object lifting[1]. The more advanced notions we wish to account for include polymorphism, multiple inheritance and binary methods. Without binary methods (in general, methods that take objects as parameters or return objects as values), the object typing problem is not overly difficult: objects may be interpreted as records of functions (methods) and cells (instance variables), inheritance is subtyping, and object lifting is accomplished by a subsumption rule. As we show, typing becomes considerably more difficult in the presence of binary methods [CHC90].

The ideal way to show applicability to OOP would be to define a complete OOP language, types, and inference algorithm; this is beyond the scope of this paper, however. Instead, we will show how a collection of simple macros allow OOP to be embedded into I-Soop.

The basic idea of the representation is to interpret classes as functions on records $\lambda s.\{\ \ldots\ \}$ where s is the "self"; **new** then takes the fixed point of a class to produce an object, in the form of a record (see [KR94]). We cannot quite use this encoding. First, it is difficult to take fixed points of records in a call-by-value language. Second, when taking a fixed point via a Y-combinator, the semantics entails re-evaluating the record with each recursive access, and thus erroneously re-initialize any instance variables. In previous work [ESTZ95] we avoided these problems by using a memory-based fixed point. Unfortunately this encoding will not work here as the use of reference

[1] Also called implicit object coercion or object subsumption.

cells to form the fixed point will infer imperative polymorphic types for objects. We thus opt for an encoding using a Y-combinator with an initial instance variable allocation phase. In a more complete treatment of this topic a limited form of memory-based fixed point such as the single-assignment reference (SAR) of [ESTZ93] could be used. We ignore the issue of information hiding in this presentation, though it is not difficult to incorporate.

DEFINITION 5.1 The object syntax is defined by the following macros.

$$
\begin{array}{lrcl}
\text{(class)} & \multicolumn{3}{l}{\mathsf{class}\ s\ \mathsf{super}\ \overline{u_i\ \mathsf{of}\ e_i}\ \mathsf{inst}\ \overline{x_j = e'_j}\ \mathsf{meth}\ \overline{m_k = e''_k}} \\
& \multicolumn{3}{c}{=} \\
& \multicolumn{3}{l}{\lambda\{\,\}.\ \mathsf{let}\ \overline{u_i^0 = e_i\ \{\,\}}\ \mathsf{in}\ \mathsf{let}\ \overline{u_i = u_i^0\ (\lambda x.\,\Omega)}\ \mathsf{in}\ \mathsf{let}\ y = \overline{\{\,x_j = \mathsf{ref}\ e'_j\,\}}\ \mathsf{in}} \\
& \multicolumn{3}{l}{\quad \lambda s.\ \mathsf{let}\ \overline{u_i = u_i^0\ (s)}\ \mathsf{in}\ \lambda\{\,\}.\ \{\,\mathsf{inst} = y,\ \mathsf{meth} = \{\,\overline{m_k = e''_k}\,\}\,\}} \\
\text{(new)} & \mathsf{new} & = & \lambda \mathsf{x}.\ \mathsf{Y}(\mathsf{x}\ \{\,\}) \\
\text{(message send)} & e \,\texttt{<-}\, m & = & (e\ \{\,\}).\mathsf{meth}.m \\
\text{(instance read)} & e{\cdot}x & = & !((e\ \{\,\}).\mathsf{inst}.x) \\
\text{(instance write)} & e_1{\cdot}x := e_2 & = & \mathsf{set}\ \{\,\mathsf{cell} = (e_1\ \{\,\}).\mathsf{inst}.x,\ \mathsf{val} = e_2\,\}
\end{array}
$$

where $\mathsf{Y} \stackrel{\text{def}}{=} \lambda \mathsf{y}.\,(\lambda \mathsf{x}.\,\mathsf{x}\ \mathsf{x})\ \lambda \mathsf{x}.\,\lambda \mathsf{z}.\,\mathsf{y}\ (\mathsf{x}\ \mathsf{x})\ \mathsf{z}$ is a call-by-value Y-combinator, $\Omega \stackrel{\text{def}}{=} \mathsf{Y}\ (\lambda \mathsf{x}.\,\mathsf{x})$, and $\lambda\{\,\}.\,e$ abbreviates $\lambda x.\,e$ for fresh x.

Note that the class macro binds occurrences of s free in the e''_k, and those of u_i free in e'_j and e''_k.

We illustrate the typing problems involved with binary methods through an example of a GcdNum class that has a binary method gcd that takes another GcdNum and recursively computes the GCD of itself and the other GcdNum. In order to keep the example very simple we assume the instance variable containing the actual number, val, is publicly accessible, and that GcdNum defines no other methods. ZGcdNum is a subclass of GcdNum with an additional unimportant method zero. Here mod is taken to be a function that computes the modulus of two numbers.

```
let GcdNum = class s super
    inst
        val = 0
    meth
        gcd = λnum. if is_zero (s·val) then s
                    else if is_zero (mod (num·val) (s·val)) then s
                    else s·val := mod (s·val) (num·val); num <- gcd s
```

The method gcd takes another GcdNum object, num, as argument. Because num is of the same type as the type of objects of the class we are currently defining, expressing the type of the gcd method will require some self-referentiality.

We first consider appropriate types for the inheritance-is-subtyping paradigm. This is known to have serious limitations [CHC90], but is nonetheless frequently found in commercial OOP languages. In this paradigm we give GcdNum the type

$$\mathsf{GcdNum} : \mathsf{GcdType} \to \mathsf{GcdType},\ \text{ where } \mathsf{GcdType} = \mu \mathsf{t}.\,(\{\,\} \to \{\,\mathsf{val} : \mathsf{Nat\ ref}, \mathsf{gcd} : \mathsf{t} \to \mathsf{t}\,\})$$

Note that μ is the usual recursive type constructor. We use it instead of the I-SOOP encoding of recursive types using recursive constraints. new GcdNum then returns an object of type GcdType. Without inheritance this type is perfectly adequate. We now look at the adequacy of this type with inheritance. We extend our example by defining ZGcdNum, a subclass of GcdNum that also includes a method that tests for zero.

```
let ZGcdNum = class s
      super
          u of GcdNum
     inst
          val = u·val
      meth
          gcd = u <- gcd,
          zero = λ{ }. is_zero (s·val)
```

In this case we did not override the gcd method; instead, we inherited it from GcdNum, denoted here by the superclass variable u (in this encoding we explicitly state the superclass of each inherited method). Using the inheritance-is-subtyping paradigm, the inherited instance variables and methods must have the same types as in the superclass since these types are fixed. Thus, the type of ZGcdNum must be

$$\mathsf{ZGcdNum} : \mathsf{ZGcdType} \rightarrow \mathsf{ZGcdType},$$

where $\mathsf{ZGcdType} = \mu \mathsf{t}.\,(\{\,\} \rightarrow \{\mathsf{val} : \mathsf{Nat\ ref}, \mathsf{gcd} : \mathsf{GcdType} \rightarrow \mathsf{GcdType}, \mathsf{zero} : \{\,\} \rightarrow \mathsf{Bool}\})$

Note the gcd method still operates on GcdType, not ZGcdType. Thus if gcd were overridden in ZGcdNum with a function that used num's zero method, this typing would fail, an undesirable fact. Another problem with this typing is illustrated in the following additional code.

```
let zgnum = new ZGcdNum in (zgnum <- gcd zgnum) <- zero { }
```

The gcd method type is not parametric in the type of the object given to it. Thus it will accept an object of ZGcdType as an argument since by subtyping $\mathsf{ZGcdType} \leq \mathsf{GcdType}$, but the result returned is only of GcdType, and thus is not known to have a zero method. The above code will thus not type-check, even though it executes without error.

An alternative typing is needed. Since we inherit from GcdNum, the ZGcdNum objects that eventually are created will have more methods than just gcd. To capture this, we must take a *parametric* or *open-ended* view of the self-type in GcdNum's type. The parametricity we desire in GcdNum is that t should be any subclass with at least gcd and val, and furthermore that gcd parametrically maps t to t. To express the open-ended view as a type, F-bounded quantification is used as follows.

$$\mathsf{GcdNum} : \forall \mathsf{t} \leq \mathsf{GcdTypeF}(\mathsf{t}).\ \mathsf{t} \rightarrow \mathsf{GcdTypeF}(\mathsf{t}),$$

where $\mathsf{GcdTypeF}(\mathsf{t}) = \{\,\} \rightarrow \{\mathsf{val} : \mathsf{Nat\ ref}, \mathsf{gcd} : \mathsf{t} \rightarrow \mathsf{t}\}$

ZGcdNum may then be typed as

$$\mathsf{ZGcdNum} : \forall \mathsf{t} \leq \mathsf{ZGcdTypeF}(\mathsf{t}).\ \mathsf{t} \rightarrow \mathsf{ZGcdTypeF}(\mathsf{t}),$$

where $\mathsf{ZGcdTypeF}(\mathsf{t}) = \{\,\} \rightarrow \{\mathsf{val} : \mathsf{Nat\ ref}, \mathsf{gcd} : \mathsf{t} \rightarrow \mathsf{t}, \mathsf{zero} : \{\,\} \rightarrow \mathsf{Bool}\}$,

giving zgnum the type $\mu \mathsf{t}.\,\mathsf{ZGcdTypeF}(\mathsf{t})$. Thus the above code type-checks. In addition, it would have been possible to override gcd in ZGcdNum, impossible in the simple recursive-types view.

The F-bounded typing has a drawback, however. ZGcdNum objects can no longer be lifted to be GcdNum objects (since their types are recursive types with t occurring negatively), and thus the following code will not type-check.

```
let gnum = new GcdNum in
   let zgnum = new ZGcdNum in
       gnum <- gcd zgnum
```

Note that the recursive typing *would* allow this code to type-check.

So, both the F-bounded interpretation of inheritance and the recursive types interpretation fail to typecheck certain typable programs. Our type inference algorithm, however, infers types that will allow both of the above varieties of message send to be typed in a single program.

5.1 Types inferred in I-SOOP

To simplify the presentation, we will ignore the instance variable val in the example. We will also simplify the translation scheme to reflect this, by eliminating the first line from the macro expansion of class and replacing u_i^0 by e, and defining new as Y.

First consider the types inferred for the classes GcdNum and ZGcdNum. The simplified translations are

```
let GcdNum =
          λs. λ{ }. { gcd = λnum.  if — then s
                                   else if — then s
                                   else (num { }).gcd s }
in let ZGcdNum =
          λs. let u = GcdNum (s) in
              λ{ }. { gcd = (u { }).gcd,
                      zero = λ{ }. is_zero — }
```

We first sketch how the inference system of rules, $\vdash_{\text{inf}}$, infers GcdNum's type. These rules are deterministic modulo α-variants so proof construction is mechanical. Starting from the leaves and using rules (Record), (App), and (Sel) in turn we obtain

$$A_0 || [\mathsf{s} : \mathsf{t}_1,\ \{\} : \mathsf{t_a},\ \mathsf{num} : \mathsf{t_b}] \vdash_{\text{inf}} (\mathsf{num}\ \{\}).\mathsf{gcd} : \mathsf{t_d} \setminus \{\mathsf{t_b} \le \{\} \rightarrow \mathsf{t_c},\ \mathsf{t_c} \le \{\mathsf{gcd} : \mathsf{t_d}\}\}$$

Next, using (App),

$$A_0 || [\mathsf{s} : \mathsf{t}_1,\ \{\} : \mathsf{t_a},\ \mathsf{num} : \mathsf{t_b}] \vdash_{\text{inf}} (\mathsf{num}\ \{\}).\mathsf{gcd}\ \mathsf{s} : \mathsf{t_e} \setminus C_1,$$

where $C_1 = \{\mathsf{t_b} \le \{\} \rightarrow \mathsf{t_c},\ \mathsf{t_c} \le \{\mathsf{gcd} : \mathsf{t_d}\},\ \mathsf{t_d} \le \mathsf{t}_1 \rightarrow \mathsf{t_e}\}$

Next, using (Cond) twice and (Abs),

$$A_0 || [\mathsf{s} : \mathsf{t}_1,\ \{\} : \mathsf{t_a}] \vdash_{\text{inf}} \lambda\mathsf{num}. \ldots : \mathsf{t_b} \rightarrow \mathsf{t}_2 \setminus C_1 \uplus \{\mathsf{t_e} \le \mathsf{t}_2,\ \mathsf{t}_1 \le \mathsf{t}_2\}$$

Finally, by (Record) and (Abs) twice,

$$A_0 \vdash_{\text{inf}} \mathsf{GcdNum} : \mathsf{t}_1 \rightarrow \mathsf{t_a} \rightarrow \{\mathsf{gcd} : \mathsf{t_b} \rightarrow \mathsf{t}_2\} \setminus C_1 \uplus \{\mathsf{t_e} \le \mathsf{t}_2,\ \mathsf{t}_1 \le \mathsf{t}_2\}$$

This is the type inferred by the inference rule system. An actual implemented type inference algorithm would automatically perform a number of simplifications on this type that do not change the meaning. Here we present these simplifications informally by giving typings deduced in the general rules that are simplified forms of the inferred types. For GcdNum, $\mathsf{t_a}$ is unconstrained so it may be replaced by $\{\}$ by subsumption. $\mathsf{t_b}$ has only one positive occurrence in the type, so it may be replaced with its upper bound. $\mathsf{t_c}$, $\mathsf{t_d}$ and $\mathsf{t_e}$ may also each be replaced. The following type may then be deduced for GcdNum in the general rules:

$$\mathsf{GcdNum} : \forall \mathsf{t}_1, \mathsf{t}_2.\ \mathsf{t}_1 \rightarrow \{\} \rightarrow \{\mathsf{gcd} : (\{\} \rightarrow \{\mathsf{gcd} : \mathsf{t}_1 \rightarrow \mathsf{t}_2\}) \rightarrow \mathsf{t}_2\} \setminus \{\mathsf{t}_1 \le \mathsf{t}_2\}$$

Hereafter we present the simplified forms of types only. An actual implemented type inference algorithm would automatically perform these simplifications. For $\mathsf{ZGcdNum}$, the (simplified) inferred type is

$$\mathsf{ZGcdNum} : \forall \mathsf{t}_1, \mathsf{t}_2.\, \mathsf{t}_1 \rightarrow \{\} \rightarrow \{\, \mathsf{gcd} : (\{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}_1 \rightarrow \mathsf{t}_2 \,\}) \rightarrow \mathsf{t}_2, \mathsf{zero} : \{\} \rightarrow \mathsf{Bool} \,\} \setminus \{\mathsf{t}_1 \leq \mathsf{t}_2\}$$

Contrast these types with the F-bounded type given GcdNum in the "open-self" encoding above. Observe that the parameter num is an object with a gcd method. Since that is the only method of num that is used, no more fields are required in the inferred type. Contrast that with the F-bounded case where num has all methods of GcdNum: the open-endedness here is more precise, each method that is passed the "self" requires that self to only have the methods actually used. Note also that this is not even an F-bounded type, the constraint $\mathsf{t}_1 \leq \mathsf{t}_2$ is not recursive. Recursive constraints may not arise in classes, since the knot has not been tied yet.

Consider now the object types. gnum and zgnum have the following (simplified) types inferred:

$$\mathsf{gnum} : \forall \mathsf{t}_1, \mathsf{t}_2.\, \mathsf{t}_1 \setminus \{\{\} \rightarrow \{\, \mathsf{gcd} : (\{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}_1 \rightarrow \mathsf{t}_2 \,\}) \rightarrow \mathsf{t}_2 \,\} \leq \mathsf{t}_1 \leq \mathsf{t}_2\},$$

$$\mathsf{zgnum} : \forall \mathsf{t}_1, \mathsf{t}_2.\, \mathsf{t}_1 \setminus \{\{\} \rightarrow \{\, \mathsf{gcd} : (\{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}_1 \rightarrow \mathsf{t}_2 \,\}) \rightarrow \mathsf{t}_2, \mathsf{zero} : \{\} \rightarrow \mathsf{Bool} \,\} \leq \mathsf{t}_1 \leq \mathsf{t}_2\}$$

It is difficult to explain precisely what these types denote, except to say they are definitely not the recursive types used in both encodings for objects above.

The message sends from the example have the following constrained types.

$$\begin{aligned}
&\mathsf{zgnum} \mathrel{<\!-} \mathsf{gcd}\ \mathsf{gnum} : \mathsf{t}_2 \setminus \{\\
&\quad \{\} \rightarrow \{\, \mathsf{gcd} : (\{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}_{1\mathsf{a}} \rightarrow \mathsf{t}_2 \,\}) \rightarrow \mathsf{t}_2, \mathsf{zero} : \{\} \rightarrow \mathsf{Bool} \,\} \leq \mathsf{t}_{1\mathsf{a}} \leq \{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}_{1\mathsf{b}} \rightarrow \mathsf{t}_2 \,\},\\
&\quad \{\} \rightarrow \{\, \mathsf{gcd} : (\{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}_{1\mathsf{b}} \rightarrow \mathsf{t}_2 \,\}) \rightarrow \mathsf{t}_2 \,\} \leq \mathsf{t}_{1\mathsf{b}} \leq \{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}_{1\mathsf{a}} \rightarrow \mathsf{t}_2 \,\},\\
&\quad \mathsf{t}_{1\mathsf{a}} \leq \mathsf{t}_2, \mathsf{t}_{1\mathsf{b}} \leq \mathsf{t}_2\},\\
&\mathsf{zgnum} \mathrel{<\!-} \mathsf{gcd}\ \mathsf{zgnum} : \mathsf{t}'_2 \setminus \{\\
&\quad \{\} \rightarrow \{\, \mathsf{gcd} : (\{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}'_{1\mathsf{a}} \rightarrow \mathsf{t}'_2 \,\}) \rightarrow \mathsf{t}'_2, \mathsf{zero} : \{\} \rightarrow \mathsf{Bool} \,\} \leq \mathsf{t}'_{1\mathsf{a}} \leq \{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}'_{1\mathsf{b}} \rightarrow \mathsf{t}'_2 \,\},\\
&\quad \{\} \rightarrow \{\, \mathsf{gcd} : (\{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}'_{1\mathsf{b}} \rightarrow \mathsf{t}'_2 \,\}) \rightarrow \mathsf{t}'_2, \mathsf{zero} : \{\} \rightarrow \mathsf{Bool} \,\} \leq \mathsf{t}'_{1\mathsf{b}} \leq \{\} \rightarrow \{\, \mathsf{gcd} : \mathsf{t}'_{1\mathsf{a}} \rightarrow \mathsf{t}'_2 \,\},\\
&\quad \mathsf{t}'_{1\mathsf{a}} \leq \mathsf{t}'_2, \mathsf{t}'_{1\mathsf{b}} \leq \mathsf{t}'_2\}
\end{aligned}$$

Note the function upper bounds of $\mathsf{t}_{1\mathsf{a}}$, $\mathsf{t}_{1\mathsf{b}}$, $\mathsf{t}'_{1\mathsf{a}}$ and $\mathsf{t}'_{1\mathsf{b}}$ can be proved to never be used; a more complete set of simplification transformations would justify their removal. Each use of gnum and zgnum gives rise to fresh variables by the (PVar) rule; if these objects were not let-polymorphic, the two message sends above would share type variables and generality would be lost. Observe there are no contradictions in the constraint systems of either of these message sends. Also note the result type t_2 is in effect the union of $\mathsf{t}_{1\mathsf{a}}$ and $\mathsf{t}_{1\mathsf{b}}$ since it is an upper bound of these two types. This corresponds to the fact that the result of gcd could be either a gnum or a zgnum. Consider sending a zero message to the result of the second message send, $(\mathsf{zgnum} \mathrel{<\!-} \mathsf{gcd}\ \mathsf{zgnum}) \mathrel{<\!-} \mathsf{zero}\ \{\}$. The rules force $\mathsf{t}'_2 \leq \{\} \rightarrow \{\, \mathsf{zero} : \{\} \rightarrow \mathsf{Bool} \,\}$ to be added to the constraints, but this is still consistent. On the other hand, consider $(\mathsf{zgnum} \mathrel{<\!-} \mathsf{gcd}\ \mathsf{gnum}) \mathrel{<\!-} \mathsf{zero}\ \{\}$. This may give a run-time error, so should not type-check. Indeed, $\mathsf{t}_2 \leq \{\} \rightarrow \{\, \mathsf{zero} : \{\} \rightarrow \mathsf{Bool} \,\}$ by transitive closure also requires a record without zero to be a subtype of a record with zero, but this is by definition an inconsistent constraint.

Compared to other work on rigorously sound class-based object languages, neither Bruce's TOOPLE or TOIL languages [Bru93, BvG93], nor our LOOP language [ESTZ95] allows the above program to type-check; in fact we know of no static type-system for object-oriented programming that successfully type-checks this example. So, not only do we obtain object type inference, we have a richer type language where it is not required to choose between "inheritance is subtyping" and the open-ended view of self.

6 Discussion

We have given a new, powerful method for type inference for object-oriented languages that is in many ways more powerful than previously existing methods. We have hopes that the core we present here will lead to development of a full-scale object-oriented programming language incorporating type inference. What we present here only shows this method is feasible, however. Further study is necessary to see if it can be implemented efficiently in practice. There also is the question of how well other language features will combine with this inference method. Modules in particular will be a challenge. There also should be separate syntax and types added for OOP features such as class definition and message send. This will provide a uniform notion of what OOP is to all programmers, and limit incompatibility of code. Lastly, even though this system is significantly stronger than the existing Hindley/Milner-style inference algorithms, the types it produces are larger and less easily readable by programmers. Thus it is important to address both the problem of simplification of these types, and the problem of how a better descriptions of what led to a type error can be given to programmers.

Acknowledgements

We would like to acknowledge Jens Palsberg for helpful discussions on related work, and Amy Zwarico for contributions in the early phases of this project.

References

[AC94] M. Abadi and L. Cardelli. A semantics of object types. In *Proceedings of the Ninth Annual IEEE Symposium on Logic in Computer Science*, pages 332–341, 1994.

[Aik94] A. Aiken. Illyria system. ftp://s2k-ftp.cs.berkeley.edu/pub/personal/aiken/, 1994.

[AW93] A. Aiken and E. L. Wimmers. Type inclusion constraints and type inference. In *Proceedings of the International Conference on Functional Programming Languages and Computer Architecture*, pages 31–41, 1993.

[Bru93] K. Bruce. Safe type checking in a statically-typed object-oriented programming language. In *Conference Record of the Twentieth Annual ACM Symposium on Principles of Programming Languages*, pages 285–298, 1993.

[BvG93] Kim B. Bruce and Robert van Gent. TOIL: A new type-safe object-oriented imperative language. Technical report, Williams College, 1993.

[Car84] L. Cardelli. A semantics of multiple inheritance. In *Semantics of Data Types*, volume 173 of *Lecture notes in Computer Science*, pages 51–67. Springer-Verlag, 1984.

[CCH+89] P. Canning, W. Cook, W. Hill, J. Mitchell, and W. Olthoff. F-bounded polymorphism for object-oriented programming. In *Proceedings of the Conference on Functional Programming Languages and Computer Architecture*, pages 273–280, 1989.

[CHC90] William R. Cook, Walter L. Hill, and Peter S. Canning. Inheritance is not subtyping. In *Conference Record of the Seventeenth Annual ACM Symposium on Principles of Programming Languages*. ACM Press, 1990.

[CW85] L. Cardelli and P. Wegner. On understanding types, data abstraction and polymorphism. *Computing Surveys*, 17(4):471–522, December 1985.

[ESTZ93] J. Eifrig, S. Smith, V. Trifonov, and A. Zwarico. A simple interpretation of OOP in a language with state. Technical Report YALEU/DCS/RR-968, Yale University, 1993.

[ESTZ94] J. Eifrig, S. Smith, V. Trifonov, and A. Zwarico. Application of OOP type theory: State, decidability, integration. In *Proceedings of the Conference on Object-Oriented Programming Systems, Languages, and Applications*, 1994.

[ESTZ95] J. Eifrig, S. Smith, V. Trifonov, and A. Zwarico. An interpretation of typed OOP in a language with state. *Lisp and Symbolic Computation*, 1995. To appear.

[Kae92] S. Kaes. Type inference in the presence of overloading, subtyping and recursive types. In *ACM Conference on Lisp and Functional Programming*, pages 193–204, 1992.

[KPS92] D. Kozen, J. Palsberg, and M. I. Schwartzbach. Efficient inference of partial types. In *Foundations of Computer Science*, 1992.

[KR94] Samuel N. Kamin and Uday S. Reddy. Two semantic models of object-oriented languages. In Carl A. Gunter and John C. Mitchell, editors, *Theoretical Aspects of Object-Oriented Programming*, chapter 13, pages 464–495. MIT Press, 1994.

[Mil78] R. Milner. A theory of type polymorphism in programming. *Journal of Computer and System Sciences*, 17:348–375, 1978.

[Mit84] J. Mitchell. Coercion and type inference (summary). In *Conference Record of the Eleventh Annual ACM Symposium on Principles of Programming Languages*, 1984.

[MPS86] D. B. MacQueen, G. Plotkin, and R. Sethi. An ideal model for recursive polymorphic types. *Information and Control*, 71:95–130, 1986.

[OPS92] N. Oxhøj, J. Palsberg, and M. I. Schwartzbach. Type inference with subtypes. In *ECOOP'92 European Conference on Object-Oriented Programming*, volume 615 of *Lecture notes in Computer Science*, pages 329–349. Springer-Verlag, 1992.

[PC94] J. Plevyak and A. Chien. Precise concrete type inference for object-oriented languages. In *Proceedings of the Ninth Annual ACM Conference on Object-Oriented Programming Systems, Languages, and Applications*, pages 324–340, 1994.

[PS92] Jens Palsberg and Michael I. Schwartzbach. Safety analysis versus type inference for partial types. *Information Processing Letters*, pages 175–180, 1992.

[PS94] J. Palsberg and M. Schwartzbach. *Object-Oriented Type Systems*. Wiley, 1994.

[Rémy94] Didier Rémy. Programming objects with ML-ART: An extension to ML with abstract and record types. In Masami Hagiya and John C. Mitchell, editors, *International Symposium on Theoretical Aspects of Computer Software*, pages 321–346, Sendai, Japan, April 1994. Springer-Verlag.

[Rey85] J. C. Reynolds. Three approaches to type structure. In *TAPSOFT proceedings*, volume 185 of *Lecture notes in Computer Science*, pages 97–138, 1985.

[SY94] T. Sekiguchi and A. Yonezawa. A complete type inference system for subtyped recursive types. In *Proc. Theoretical Aspects of Computer Software*, volume 789 of *Lecture Notes in Computer Science*, pages 667–686. Springer-Verlag, 1994.

[Tof90] M. Tofte. Type inference for polymorphic references. *Information and Computation*, 89:1–34, 1990.

[WF91] A. Wright and M. Felleisen. A syntactic approach to type soundness. Technical Report TR91-160, Rice University Department of Computer Science, 1991. To appear in *Information and Computation*.

A Proof of Subject Reduction

Definition A.1 A *canonical proof* is a proof in which no instance of (Sub) has another instance of (Sub) as an antecedent.

Lemma A.2 If $A \vdash e : \tau \setminus C$ has a proof, it has a canonical proof.

Proof: By induction on the original proof. There are essentially two cases:

(i) The final rule in the proof of $A \vdash e : \tau \setminus C$ is not (Sub). Then by induction this rule's antecedents have canonical proofs, and from these proofs a canonical proof of $A \vdash e : \tau \setminus C$ can be formed using the original rule.

(ii) The final rule in the proof is (Sub). Its antecedent is therefore some proof of $A \vdash e : \tau' \setminus C'$, with $C' \uplus \{\tau' \leq \tau\} \subseteq C$, and by induction it has a canonical proof. Again, there are two cases:

  (a) The canonical proof of $A \vdash e : \tau' \setminus C'$ does not end in (Sub). Then a proof of $A \vdash e : \tau \setminus C$ can be formed from this proof via rule (Sub), and this proof will be canonical.

(b) The canonical proof of $A \vdash e : \tau' \setminus C'$ ends in (Sub). Thus it has a proof of $A \vdash e : \tau'' \setminus C''$ as an antecedent, and this proof does not end in (Sub); also, $C'' \uplus \{\tau'' \leq \tau'\} \subseteq C'$. Therefore, $C'' \uplus \{\tau'' \leq \tau\} \subseteq C$, and from this proof a canonical proof of $A \vdash e : \tau \setminus C$ can be constructed via rule (Sub).

□

LEMMA A.3 (CONSTRAINT SYSTEM EXTENSION) If $A||[\, x : \forall\overline{\alpha}.\ \tau \setminus C\,] \vdash e : \tau' \setminus C'$ and C_1 is consistent with both C and C', with $FTV(C_1) \cap \{\overline{\alpha}\} = \emptyset$, then $A||[\, x : \forall\overline{\alpha}.\ \tau \setminus C \uplus C_3\,] \vdash e : \tau' \setminus C' \uplus C_1$.

PROOF: By induction on the structure of e. □

LEMMA A.4 (SUBSTITUTION)

(i) If $A||[\, x : \forall\overline{\alpha}.\ \tau \setminus C\,] \vdash e' : \tau' \setminus C'$ and $A \vdash e : \tau \setminus C$ and $\{\overline{\alpha}\} \subseteq \mathit{Clos}(\tau \setminus C, A)$, then $A \vdash e'[e/x] : \tau' \setminus C'$.

(ii) If $A||[\, x : \tau\,] \vdash e' : \tau' \setminus C'$, $A \vdash e : \tau \setminus C$, and $C' \uplus C$ is consistent, then $A \vdash e'[e/x] : \tau' \setminus C' \uplus C$.

PROOF: By induction on the structure of e'. □

LEMMA A.5 (TYPING OF VALUES) If $v \in \mathit{Val}$ and $A \vdash \langle s, v \rangle : \tau \setminus C$, then

(i) if $\tau = \mathsf{Nat}$, then $v \in \mathit{Num}$;

(ii) if $\tau = \mathsf{Bool}$, then $v \in \{\mathsf{true}, \mathsf{false}\}$;

(iii) if $\tau = \{\, \overline{m_i : \tau_i}\,\}$, then $v = \{\, \overline{m_i = v_i},\ \ldots\,\}$ for some $\overline{v_i}$;

(iv) if $\tau = \tau' \rightarrow \tau''$, then either $v = \lambda x.\, e$ for some x and e, or $v \in \{\mathsf{pred}, \mathsf{succ}, \mathsf{is\_zero}, \mathsf{ref}, !, \mathsf{set}\}$;

(v) if $\tau = \tau'\ \mathsf{ref}$, then $v \in \mathit{Var} - B$.

PROOF: Observe that any value is in exactly one of these five disjoint subsets of Val; therefore it suffices to show that any value in one of these subsets cannot have a type with a top level constructor associated with another subset. Suppose for instance that $A \vdash n : \mathsf{Bool} \setminus C$, where $n \in \mathit{Num}$. A canonical proof of this judgement must end in (Sub) and (Num); since the conclusion of the latter is $A \vdash n : \mathsf{Nat} \setminus \emptyset$, it follows that (Sub) can only be applied if $\mathsf{Nat} \setminus \emptyset \leq \mathsf{Bool} \setminus C$, which implies $\mathsf{Nat} \leq \mathsf{Bool} \in C$. But this constraint is inconsistent, hence the judgement is not provable for any C. The other cases are similar. □

THEOREM A.6 (SUBJECT REDUCTION) If $A \vdash \langle s, e \rangle : \kappa$, then either $e \in \mathit{Val}$ or else $\langle s, e \rangle \mapsto_1 \langle s', e' \rangle$ and there exists an environment A' such that $A'|_{dom(A)} = A$ and $A' \vdash \langle s', e' \rangle : \kappa$.

PROOF: By induction on the structure of e. If $A \vdash \langle s, e \rangle : \tau \setminus C$, then by the definition of typability of configurations $A \vdash e : \tau \setminus C$ must be provable, and thus have a canonical proof. We have the following cases to consider.

(i) e is a value. The theorem is then trivial.

(ii) $e = \{\overline{m_i = e_i}\}$ where at least one of $\overline{e_i}$ is not a value (otherwise e is a value and case (i) applies); let k be the smallest index for which e_k is not a value. A canonical proof of $A \vdash \{\overline{m_i = e_i}\} : \tau \setminus C$ must end in rules (Sub) and (Record), and so $\overline{A \vdash e_i : \tau_i \setminus C_i}$ must be provable for some $\overline{\tau_i}$ and $\overline{C_i}$ such that $\{\{\overline{m_i : \tau_i}\} \leq \tau\} \uplus \biguplus_i C_i \subseteq C$. Therefore $A \vdash \langle s, e_k \rangle : \tau_k \setminus C$; hence by induction $\langle s, e_k \rangle \mapsto_1 \langle s', e'_k \rangle$, and there exists an environment A' such that $A' \vdash \langle s', e'_k \rangle : \tau_k \setminus C$, meaning $A' \vdash e'_k : \tau_k \setminus C$ is provable. Since reduction is compositional, we have $\langle s, e \rangle \mapsto_1 \langle s', e' \rangle$, where $e' = \{m_1 = e_1, \ldots, m_{k-1} = e_{k-1}, m_k = e'_k, m_{k+1} = e_{k+1}, \ldots\}$, and $A' \vdash \langle s', e' \rangle : \tau \setminus C$ (since A' extends A).

(iii) $e = \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3$. The case of $e_1 \notin \mathit{Val}$ is analogous to case (ii); suppose now that $e_1 \in \mathit{Val}$. A canonical proof of $A \vdash e : \tau \setminus C$ must end in (Sub) and (Cond); therefore a proof of $A \vdash e_1 : \mathsf{Bool} \setminus C_1$ is available, and hence (by Lemma A.5) $e_1 \in \{\mathsf{true}, \mathsf{false}\}$. Consider $e_1 = \mathsf{true}$; then $\langle s, e \rangle \mapsto_1 \langle s, e_2 \rangle$, and we also have a proof of $A \vdash e_2 : \tau \setminus C_2$ (which is a premise of (Cond)), with $C_2 \subseteq C$. Hence by (Sub) we may obtain $A \vdash e_2 : \tau \setminus C$, which implies $A \vdash \langle s, e_2 \rangle : \tau \setminus C$.

Similar reasoning proves the theorem in the case of $e = e_1.m$.

(iv) $e = e_1\ e_2$. A canonical proof of $A \vdash e_1\ e_2 : \tau \setminus C$ must then end in rules (Sub) and (App); therefore $A \vdash e_1 : \tau_2 \to \tau_1 \setminus C_1$ and $A \vdash e_2 : \tau_2 \setminus C_2$ are both provable for some τ_2, τ_1, C_1, and C_2 with $C_1 \uplus C_2 \uplus \{\tau_1 \leq \tau\} \subseteq C$. The cases when e_1 and e_2 are not both values are similar to case (ii). Suppose now that both e_1 and $e_2 = v$ are values. By Lemma A.5 there are the following possibilities for e_1:

(a) e_1 is an abstraction $\lambda x.\, e'_1$. A canonical proof of $A \vdash \lambda x.\, e'_1 : \tau_2 \to \tau_1 \setminus C_1$ must end in rules (Sub) and (Abs), so $A || [\, x : \tau'_2\,] \vdash e'_1 : \tau'_1 \setminus C'_1$ is provable for some τ'_1, τ'_2, and C'_1 with $C'_1 \uplus \{\tau'_2 \to \tau'_1 \leq \tau_2 \to \tau_1\} \subseteq C_1$. Since C_1 is closed, this means $\{\tau_2 \leq \tau'_2\} \subseteq C_1 \subseteq C$, and thus $A \vdash v : \tau'_2 \setminus C$ by rule (Sub). By the Substitution Lemma A.4, this means $A \vdash e'_1[v/x] : \tau'_1 \setminus C$, as $C'_1 \uplus C = C$. Furthermore, C contains $\{\tau'_1 \leq \tau\}$ by transitivity, and thus $A \vdash e'_1[v/x] : \tau \setminus C$ is provable by rule (Sub).
Therefore, $\langle s, (\lambda x.\, e'_1)\ v \rangle \mapsto_1 \langle s, e'_1[v/x] \rangle$ and $A \vdash \langle s, e'_1[v/x] \rangle : \tau \setminus C$.

(b) $e_1 \in \mathit{Var}$, i.e. e_1 is a primitive function. This includes the following cases.

i. $e_1 = \mathsf{is\_zero}$. Since $A_0(\mathsf{is\_zero}) = \mathsf{Nat} \to \mathsf{Bool}$, it must be the case that $\{\tau_2 \leq \mathsf{Nat}, \mathsf{Bool} \leq \tau_1\} \subseteq C$, and therefore by Lemma A.5 the value v must be a numeral n; thus $\langle s, \mathsf{is\_zero}\ n \rangle \mapsto_1 \langle s, b \rangle$ for some $b \in \{\mathsf{true}, \mathsf{false}\}$. By rule (Var) it follows that $A \vdash b : \mathsf{Bool} \setminus \emptyset$, and since $\{\mathsf{Bool} \leq \tau_1, \tau_1 \leq \tau\} \subseteq C$ and C is closed under transitivity, by (Sub) we have $A \vdash b : \tau \setminus C$; thus $A \vdash \langle s, b \rangle : \tau \setminus C$.
The cases when $e_1 \in \{\mathsf{pred}, \mathsf{succ}\}$ follow in similar fashion.

ii. $e_1 = !$. A canonical proof of $A \vdash\ ! : \tau_2 \to \tau_1 \setminus C_1$ must end in (Sub) and (PVar); since $A(!) = A_0(!) = \forall \mathsf{t}.\ \mathsf{t\ ref} \to \mathsf{t}$, we have $\{\tau_2 \leq \tau_{\mathsf{t}}\ \mathsf{ref},\ \tau_{\mathsf{t}} \leq \tau_1\} \subseteq C_1$, where τ_{t} is the type substituted for t in (PVar). Recall that $A \vdash e_2 : \tau_2 \setminus C_2$ and e_2 is a value v; therefore v must be a variable x, and the canonical proof of its typing ends in rules (Var) and (Sub). Since the configuration $\langle s, e \rangle$ is typable under C, we have $x \in \mathit{dom}(s)$, $A(x) = \tau_x\ \mathsf{ref}$ for some τ_x such that $\tau_x\ \mathsf{ref} \leq \tau_2 \in C$, and $A \vdash s(x) : \tau_x \setminus C_x$ is provable for some $C_x \subseteq C$. Thus via rule (Sub) $A \vdash s(x) : \tau \setminus C$ is also provable, and therefore $A \vdash \langle s, s(x) \rangle : \tau \setminus C$ is provable as well; observe that $\langle s, !x \rangle \mapsto_1 \langle s, s(x) \rangle$.

iii. $e_1 = \mathsf{ref}$. Similarly to the previous case we have $A_0(\mathsf{ref}) = \forall \mathsf{u}.\ \mathsf{u} \to \mathsf{u\ ref}$, and so $\{\tau_2 \leq \tau_{\mathsf{u}},\ \tau_{\mathsf{u}}\ \mathsf{ref} \leq \tau_1\} \subseteq C_1$, where τ_{u} is the type substituted for u in (PVar). The reduction step is $\langle s, \mathsf{ref}\ v \rangle \mapsto_1 \langle s || [\, x \mapsto v\,], x \rangle$, for some new variable $x \notin \mathit{dom}(s)$. Let $A' = A || [\, x : \tau_{\mathsf{u}}\,]$. Now $A' \vdash v : \tau_{\mathsf{u}} \setminus C_1$ is provable by subsumption, and

$A' \vdash x : \tau \setminus C$ follows by rules (Var) and (Sub) from $\tau_{\mathsf{u}}\ \mathsf{ref} \leq \tau \in C$. Thus $A' \vdash \langle s||[\,x \mapsto v\,],\, x\rangle : \tau \setminus C$.

iv. $e_1 = \mathsf{set}$. Since $A_0(\mathsf{set}) = \forall \mathsf{t}.\ \{\mathsf{cell} : \mathsf{t}\ \mathsf{ref}, \mathsf{val} : \mathsf{t}\} \rightarrow \mathsf{t}$, the canonical proof of $A \vdash e_1 : \tau_2 \rightarrow \tau_1 \setminus C_1$ ends in (Sub) and (PVar), and assume that some τ_{t} is substituted in the latter for t. Then we have $\{\tau_2 \leq \{\mathsf{cell} : \tau_{\mathsf{t}}\ \mathsf{ref}, \mathsf{val} : \tau_{\mathsf{t}}\},\ \tau_{\mathsf{t}} \leq \tau_1\} \subseteq C_1$. The value $v = e_2$ is hence a record with (at least) fields cell and val; let their values be v' and v'' respectively. From the canonical proof of typing of v we obtain proofs of $A \vdash v' : \tau' \setminus C'$ and $A \vdash v'' : \tau'' \setminus C''$ such that $C' \uplus C'' \uplus \{\tau' \leq \tau_{\mathsf{t}}\ \mathsf{ref},\ \tau'' \leq \tau_{\mathsf{t}}\} \subseteq C$; hence v' must be a variable x, and by the typability of $\langle s,\, e\rangle$ in C it follows that $x \in dom(A)$ and $\tau' = A(x) = \tau_x\ \mathsf{ref}$ for some τ_x. Since C is closed, $\{\tau_{\mathsf{t}} \leq \tau_x,\ \tau'' \leq \tau_x\} \subseteq C$, and hence $A \vdash v'' : \tau_x \setminus C$ by (Sub); also $\tau'' \leq \tau \in C$. Thus $\langle s,\, e\rangle \mapsto_1 \langle s||[\,x \mapsto v''\,],\, v''\rangle$, and $A \vdash \langle s||[\,x \mapsto v''\,],\, v''\rangle : \tau \setminus C$.

(v) $e = \mathsf{let}\ x = e_1\ \mathsf{in}\ e_2$. A canonical proof of $A \vdash \mathsf{let}\ x = e_1\ \mathsf{in}\ e_2 : \tau \setminus C$ must then end in rules (Sub) and (Let). Therefore, $A \vdash e_1 : \tau_1 \setminus C_1$ and $A||[\,x : \forall\overline{\alpha}.\ \tau_1 \setminus C_1\,] \vdash e_2 : \tau_2 \setminus C_2$ are both provable judgements, for some constraint systems C_1 and C_2 and set of type variables $\{\overline{\alpha}\}$, where $\Phi C_1 \uplus C_2 \uplus \{\tau_2 \leq \tau\} \subseteq C$ and Φ is some renaming of $\{\overline{\alpha}\}$. There are then two subcases:

(a) e_1 is a value v. Then $\langle s,\, \mathsf{let}\ x = v\ \mathsf{in}\ e_2\rangle \mapsto_1 \langle s,\, e_2[v/x]\rangle$. By the Substitution Lemma A.4 we know that $A \vdash e_2[v/x] : \tau_2 \setminus C_2$ is provable, and since $C_2 \uplus \{\tau_2 \leq \tau\} \subseteq C$, by rule (Sub) $A \vdash e_2[v/x] : \tau \setminus C$ is provable as well.

(b) e_1 is not a value. Then e_1 is expansive, and hence $\{\overline{\alpha}\}$ contains only applicative type variables. First, choose a one-to-one renaming Φ_1 that maps $\{\overline{\alpha}\}$ to variables not occurring in C, and apply it uniformly to the proof of $A \vdash e_1 : \tau_1 \setminus C_1$. This results in a proof of $A \vdash e_1 : \Phi_1\tau_1 \setminus \Phi_1 C_1$ (observe that $\Phi_1 A = A$ since by definition $\{\overline{\alpha}\} = \mathit{AppClos}(\tau_1 \setminus C_1,\, A)$ is disjoint with $\mathit{FTV}(A)$). Consider the renaming $\Phi_2 = \Phi \circ \Phi_1^{-1}$, which by construction maps only variables not occurring in C. Then $\Phi_2(\Phi_1 C_1 \uplus C) \subseteq \Phi_2(\Phi_1 C_1) \uplus \Phi_2 C = \Phi C_1 \uplus C = C$, which is consistent. Therefore $\Phi_1 C_1 \uplus C$ is consistent as well, and thus $A \vdash \langle s,\, e_1\rangle : \Phi_1\tau_1 \setminus \Phi_1 C_1 \uplus C$ is provable. By induction, $\langle s,\, e_1\rangle \mapsto_1 \langle s',\, e_1'\rangle$ and there exists a new environment A' such that $A' \vdash \langle s',\, e_1'\rangle : \Phi_1\tau_1 \setminus \Phi_1 C_1 \uplus C$.

Now, consider the proof of $A||[\,x : \forall\overline{\alpha}.\ \tau_1 \setminus C_1\,] \vdash e_2 : \tau_2 \setminus C_2$. Since $A'|_{dom(A)} = A$, this proof can be converted to a proof of $A'||[\,x : \forall\overline{\alpha}.\ \tau_1 \setminus C_1\,] \vdash e_2 : \tau_2 \setminus C_2$ by merely substituting A' for A. Because the type variables $\{\overline{\alpha}\}$ are bound, this proof can be renamed to a proof of $A'||[\,x : \forall\overline{\Phi_1\alpha}.\ \Phi_1\tau_1 \setminus \Phi_1 C_1\,] \vdash e_2 : \tau_2 \setminus C_2$. By construction C does not contain any of the variables in $\{\overline{\Phi_1\alpha}\}$. Thus, by Lemma A.3, this proof can be transformed into a proof of $A'||[\,x : \forall\overline{\Phi_1\alpha}.\ \Phi_1\tau_1 \setminus \Phi_1 C_1 \uplus C\,] \vdash e_2 : \tau_2 \setminus C_2 \uplus C$, and by rule (Let) we have a proof of $A' \vdash \mathsf{let}\ x = e_1'\ \mathsf{in}\ e_2 : \tau_2 \setminus \Phi_2(\Phi_1 C_1 \uplus C) \uplus (C_2 \uplus C)$. But $\Phi_2(\Phi_1 C_1 \uplus C) \uplus (C_2 \uplus C) \subseteq \Phi_2(\Phi_1 C_1) \uplus \Phi_2 C \uplus C_2 \uplus C = \Phi C_1 \uplus C_2 \uplus C = C$, since both ΦC_1 and C_2 are contained in C by hypothesis. The desired judgement then follows directly via rule (Sub).

$\square$