Efficient recursive subtyping

Dexter Kozen, Jens Palsberg and Michael I. Schwartzbach

Mathematical Structures in Computer Science / Volume 5 / Issue 01 / March 1995, pp 113 - 125
DOI: 10.1017/S0960129500000657, Published online: 04 March 2009

Math. Struct. in Comp. Science (1995), *vol.* 5, *pp.* 113–125 Copyright © Cambridge University Press

Efficient recursive subtyping

DEXTER KOZEN[†], JENS PALSBERG[‡]
and MICHAEL I. SCHWARTZBACH[‡]

[†]*Computer Science Department, Cornell University, Ithaca, New York 14853, USA*
[‡]*Computer Science Department, Aarhus University, 8000 Aarhus C, Denmark*

Received 16 April 1993; revised 20 September 1994

Subtyping in the presence of recursive types for the λ-calculus was studied by Amadio and Cardelli in 1991 (Amadio and Cardelli 1991). In that paper they showed that the problem of deciding whether one recursive type is a subtype of another is decidable in exponential time. In this paper we give an $O(n^2)$ algorithm. Our algorithm is based on a simplification of the definition of the subtype relation, which allows us to reduce the problem to the emptiness problem for a certain finite automaton with quadratically many states.
It is known that equality of recursive types and the covariant Böhm order can be decided efficiently by means of finite automata, since they are just language equality and language inclusion, respectively. Our results extend the automata-theoretic approach to handle orderings based on contravariance.

1. Introduction

Recursive types are present in most programming languages, since they provide a means of typing recursive functions and data structures. Subtyping is also present in many languages and is especially important in object-oriented languages as a means of typing functions in the presence of inheritance and late binding.

The unrestricted combination of recursion and subtyping, found for example in Amber (Cardelli 1985) and Quest (Cardelli and Wegner 1985; Cardelli 1989), is of substantial pragmatic value. Because it does not depend on programmer-defined names, it allows the flexible typing of such constructs as data persistence and data migration.

The combination of recursive types and subtyping at an abstract level was studied by Amadio and Cardelli in 1991 (Amadio and Cardelli 1991). They considered types for the λ-calculus generated by the following grammar, where v is a type variable:

$$t ::= v \mid \bot \mid \top \mid t_1 \rightarrow t_2 \mid \mu v.t \ .$$

Intuitively, $\bot$ is a minimal type containing only the divergent computation; $\top$ is a maximal or universal type containing all values; $t_1 \rightarrow t_2$ is the usual function space; and $\mu v.t$ is a recursive type that satisfies the equation

$$\mu v.t \quad = \quad t[v/\mu v.t] \ ,$$

where $t[v/s]$ denotes the term t with s substituted for free occurrences of v (after renaming bound variables if necessary).

In Amadio and Cardelli's approach, types are understood as collections of values, and subtypes are subcollections. Thus, types are partially ordered by an inclusion relation $\leq$. It is postulated that $\bot \leq t \leq \top$ for any type t, and function spaces are ordered by the usual rule

$$s \to t \leq s' \to t' \quad \text{if and only if} \quad s' \leq s \text{ and } t \leq t' ,$$

i.e., $\to$ is covariant in the range and contravariant in the domain. This defines a partial order inductively on finite types, but not on recursive types.

Amadio and Cardelli showed how to extend the ordering to recursive types. Their definition involves a rule of the form

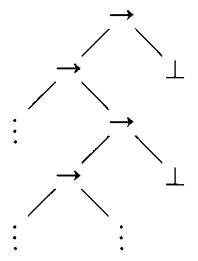
$$(v \leq v' \Rightarrow t \leq t') \quad \Rightarrow \quad (\mu v.t \leq \mu v'.t') ,$$

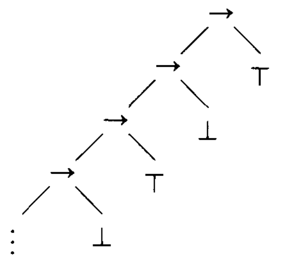
where v occurs only in t, and v' occurs only in t'. In other words, if by assuming the inclusion of the recursion variables we can verify the inclusion of the bodies, we can deduce the inclusion of the recursive types.

They also considered the standard representation of types as labeled trees, defined a partial order on infinite trees, and showed that it agrees with the type inclusion order. Their definition of the order on trees involves infinite sequences of finite approximations, where the approximations are obtained by truncating the trees at some finite level. The relation $\leq$ holds between two trees iff it holds between all their finite truncations.

For an illustration of the type and tree orderings, consider the following two types and their tree representations.

$\mu u.((u \to u) \to \bot)$ $\qquad\qquad\qquad$ $\mu v.((v \to \bot) \to \top)$





It can be shown using Amadio and Cardelli's type rules that the left type is included in the right. It is somewhat easier to see this for the corresponding trees: all level-k truncations are clearly ordered from left to right.

In order to automate type checking in the presence of subtypes and recursive types, the problem of deciding type inclusion is of paramount importance:

Given two types s and t, is $s \leq t$?

Amadio and Cardelli showed that this problem is decidable, but gave no complexity analysis. However, their algorithm involves the explicit construction of a binary tree of polynomial depth, thus it is exponential in some cases. Their algorithm is based on a concrete representation of recursive types involving back-pointers to represent recursion.

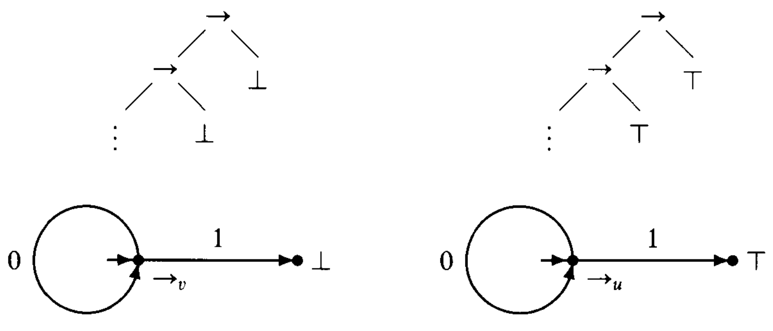
In this paper we show that the type inclusion problem is solvable in time $O(n^2)$. Our algorithm is based on a simplification of Amadio and Cardelli's definition of the subtype relation on trees; we show that the two definitions are equivalent. Our definition, which is a generalization of an order introduced by us in (Kozen, Palsberg and Schwartzbach 1992), intuitively says:

Two trees are ordered if no common path detects a counterexample.

This allows us to reduce the problem to the emptiness problem for a certain finite automaton that accepts a language of counterexamples.

Our algorithm represents recursive types as so-called *term automata.* The automaton that detects counterexamples is then defined as a certain product of two term automata. For an illustration of this, consider the following two types, their tree representations, and the term automata for these trees.

$$\mu v.(v \to \bot) \;\not\leq\; \mu u.(u \to \top)$$



These two types are *not* in the subtype relation: consider for example their level-3 truncations. This can be detected by the following product automaton (we show only the reachable states):

$$\begin{tikzcd}
& {} \arrow[d] & \\
& (\to_v, \to_u, 0) \arrow[dl, bend left, "0"] \arrow[dr, "1"] & \\
(\to_v, \to_u, 1) \arrow[ur, bend left, "0"] \arrow[dr, "1"'] & & (\bot, \top, 0) \\
& ((\bot, \top, 1)) &
\end{tikzcd}$$

The idea is that the accept states (marked with double parentheses) are those where the first component is *not* less than the second component in the ordering $\bot \leq \to \leq \top$. Because of contravariance, however, we use the third component to signal if the ordering should be reversed: 0 means 'no' and 1 means 'yes'. The automaton above accepts the word 01, thus the level-3 truncations of the trees are not ordered.

The test for emptiness takes linear time in the size of the product automaton using depth first search. The size of the product automaton is the product of the sizes of the two term automata. Thus, our algorithm runs in $O(n^2)$ time.

It may be surprising that the inclusion of recursive types can be decided efficiently using finite automata. To quote Amadio and Cardelli (Amadio and Cardelli 1991):

> The problem of equating recursive types ... can be related to well-known solvable problems, such as the equivalence of finite-state automata. However, the similar problem for subtyping has no well-known parallel.

Our results establish that the automata-theoretic approach is fruitful even in the presence of subtyping and contravariance. Further evidence is provided by the results of Kozen, Palsberg and Schwartzbach (1992), which establish the first known polynomial time algorithm for a type inference problem studied by Thatte (Thatte 1988) and O'Keefe and Wand (O'Keefe and Wand 1992).

In the remainder of this paper we provide the definitions of term automata and labeled trees, prove that Amadio and Cardelli's tree ordering and ours agree, and give the details of our algorithm. We introduce term automata and labeled trees in a more general form than needed here; they may be useful in other contexts.

2. Terms

Here we give a general definition of (possibly infinite) terms over an arbitrary finite ranked alphabet Σ. Such terms are essentially labeled trees, which we represent as partial functions labeling strings over ω (the natural numbers) with elements of Σ. In our application, types are terms over the ranked alphabet $\{\bot, \rightarrow, \top\}$; finite types are finite terms and recursive types are regular terms.

Let Σ_n denote the set of elements of Σ of arity n. Let ω denote the set of natural numbers and let ω^* denote the set of finite-length strings over ω.

Definition 2.1. A *term* over Σ is a partial function

$$t : \omega^* \rightarrow \Sigma$$

with domain $\mathscr{D}(t)$ satisfying the following properties:

— $\mathscr{D}(t)$ is nonempty and prefix-closed;
— if $t(\alpha) \in \Sigma_n$, then $\{i \mid \alpha i \in \mathscr{D}(t)\} = \{0, 1, \ldots, n-1\}$.

The set of all terms is denoted T_Σ.
An element $\alpha \in \omega^*$ is a *leaf* of t if $\alpha \in \mathscr{D}(t)$ and α is not a proper prefix of any other element of $\mathscr{D}(t)$; equivalently, if $t(\alpha) \in \Sigma_0$.

A term t is *finite* if its domain $\mathscr{D}(t)$ is a finite set. We denote the set of finite terms over Σ by F_Σ. A *path* in a term t is a maximal subset of $\mathscr{D}(t)$ linearly ordered by the prefix relation. By König's Lemma, a term is finite iff it has no infinite paths.

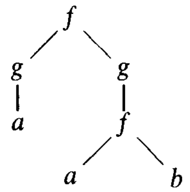
Definition 2.2. Let t be a term and $\alpha \in \omega^*$. Define the partial function $t\downarrow\alpha : \omega^* \to \Sigma$ by

$$t\downarrow\alpha(\beta) \quad = \quad t(\alpha\beta)\,.$$

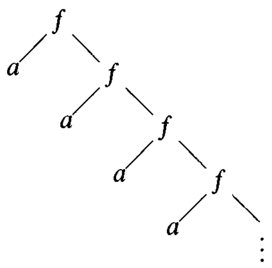
If $t\downarrow\alpha$ has nonempty domain, then it is a term, and is called the *subterm of t at position α.*

Definition 2.3. A term t is said to be *regular* if it has only finitely many distinct subterms; *i.e.*, if $\{t\downarrow\alpha \mid \alpha \in \omega^*\}$ is a finite set. The set of regular terms is denoted R_Σ.

Example 2.4. Let $\Sigma = \{f,g,a,b\}$, where f,g,a,b have arities 2,1,0,0 respectively. The following picture represents a typical finite term t:



The leaves of t are the strings $00, 100, 101$ with $t(00) = t(100) = a$ and $t(101) = b$. The domain $\mathscr{D}(t)$ of t is the set of all prefixes of these strings, namely $\epsilon, 0, 1, 10$ in addition to those already mentioned, with $t(\epsilon) = t(10) = f$ and $t(0) = t(1) = g$.
The following picture represents a typical infinite regular term s:



The domain of s is the infinite regular set $1^* + 1^*0$, with $s(1^n0) = a$ and $s(1^n) = f$ for all $n \geq 0$. The leaves are the elements of the regular subset 1^*0. The term is regular because it has only two subterms, namely s itself and the singleton term a.

The sets T_Σ, F_Σ, and R_Σ become algebraic structures of signature Σ under the natural syntactic definition of the operators

$$f^{T_\Sigma} : T_\Sigma^n \quad \to \quad T_\Sigma$$

for each $f \in \Sigma_n$ given by

$$\begin{aligned} f^{T_\Sigma}(t_0,\ldots,t_{n-1})(i\alpha) &= t_i(\alpha), \quad 0 \leq i < n \\ f^{T_\Sigma}(t_0,\ldots,t_{n-1})(\epsilon) &= f\,. \end{aligned}$$

Then

$$\mathscr{D}(f^{T_\Sigma}(t_0,\ldots,t_{n-1})) \quad = \quad \{\epsilon\} \cup \bigcup_{i=0}^{n-1}\{i\alpha \mid \alpha \in \mathscr{D}(t_i)\}\,.$$

In particular, for $c \in \Sigma_0$, we have $c^{T_\Sigma}(\epsilon) = c$ and c^{T_Σ} undefined otherwise.

The following lemma establishes some elementary properties of these operators.

Lemma 2.5.

(i) If $f \in \Sigma_n$ and $0 \leq i < n$, then $f^{T_\Sigma}(t_0, \ldots, t_{n-1}) \downarrow i = t_i$.

(ii) If $t(\epsilon) = f \in \Sigma_n$, then $t = f^{T_\Sigma}(t \downarrow 0, \ldots, t \downarrow (n-1))$.

(iii) $(t \downarrow \alpha) \downarrow \beta = t \downarrow \alpha\beta$.

(iv) The string α is a leaf of t iff $\mathscr{D}(t \downarrow \alpha) = \{\epsilon\}$.

Proof. All properties are immediate consequences of the definitions. □

3. Term automata

Every regular term over a finite ranked alphabet Σ has a finite representation in terms of a special type of automaton called a *term automaton*.

Definition 3.1. Let Σ be a finite ranked alphabet. A *term automaton* over Σ is a tuple

$$\mathscr{M} \quad = \quad (Q,\ \Sigma,\ q_0,\ \delta,\ \ell)$$

where:

— Q is a finite set of *states*,

— $q_0 \in Q$ is the *start state*,

— $\delta : Q \times \omega \to Q$ is a partial function called the *transition function*, and

— $\ell : Q \to \Sigma$ is a (total) *labeling function*,

such that for any state $q \in Q$, if $\ell(q) \in \Sigma_n$, then

$$\{i \mid \delta(q,i) \text{ is defined}\} \quad = \quad \{0, 1, \ldots, n-1\} .$$

We decorate Q, δ, *etc.* with the superscript $\mathscr{M}$ where necessary.

Let $\mathscr{M}$ be a term automaton as in Definition 3.1. The partial function δ extends naturally to a partial function

$$\widehat{\delta} : Q \times \omega^* \to Q ,$$

defined inductively as follows:

$$\begin{aligned} \widehat{\delta}(q,\epsilon) &= q \\ \widehat{\delta}(q,\alpha i) &= \delta(\widehat{\delta}(q,\alpha), i) . \end{aligned}$$

For any $q \in Q$, the domain of the partial function $\lambda\alpha.\widehat{\delta}(q,\alpha)$ is nonempty (it always contains ϵ) and prefix-closed. Moreover, because of the condition on the existence of i-successors in Definition 3.1, the partial function

$$\lambda\alpha.\ell(\widehat{\delta}(q,\alpha))$$

is a term.

Definition 3.2. Let $\mathscr{M}$ be a term automaton. The term *represented by* $\mathscr{M}$ is the term

$$t_{\mathscr{M}} \quad = \quad \lambda\alpha.\ell(\widehat{\delta}(q_0,\alpha)) .$$

A term t is said to be *representable* if $t = t_{\mathscr{M}}$ for some $\mathscr{M}$.

Intuitively, $t_{\mathcal{M}}(\alpha)$ is determined by starting in the start state q_0 and scanning the input α, following transitions of $\mathcal{M}$ as far as possible. If it is not possible to scan all of α because some i-transition along the way does not exist, then $t_{\mathcal{M}}(\alpha)$ is undefined. If, on the other hand, $\mathcal{M}$ scans the entire input α and ends up in state q, then $t_{\mathcal{M}}(\alpha) = \ell(q)$.

Lemma 3.3. Let $t \in T_\Sigma$. The following are equivalent:

(i) t is regular;
(ii) t is representable;
(iii) t is described by a finite set of equations involving the μ operator.

Proof. (i) $\Longrightarrow$ (ii) Suppose t has only finitely many subterms. Define

$$\begin{array}{rcl} Q &=& \{t\downarrow\alpha \mid \alpha \in \omega^*,\ \mathcal{D}(t\downarrow\alpha) \neq \emptyset\} \\ q_0 &=& t \ = \ t\downarrow\epsilon \\ \ell(s) &=& s(\epsilon) \\ \delta(s,i) &=& \begin{cases} s\downarrow i\,, & \text{if } 0 \le i \le \text{arity}(\ell(s)) \\ \text{undefined}\,, & \text{otherwise} \end{cases} \end{array}$$

and let $\mathcal{M}$ be the automaton with these data. A straightforward inductive argument using Lemma 2.5 shows that

$$\widehat{\delta}(t,\alpha) = \begin{cases} t\downarrow\alpha\,, & \text{if } \mathcal{D}(t\downarrow\alpha) \neq \emptyset \\ \text{undefined}\,, & \text{otherwise}\,. \end{cases}$$

Thus

$$\begin{array}{rcl} \ell(\widehat{\delta}(q_0,\alpha)) &=& \ell(\widehat{\delta}(t,\alpha)) \\ &=& \widehat{\delta}(t,\alpha)(\epsilon) \\ &=& t\downarrow\alpha(\epsilon) \\ &=& t(\alpha)\,. \end{array}$$

Therefore $t = t_{\mathcal{M}}$.

(ii) $\Longrightarrow$ (i) For any term automaton $\mathcal{M}$ and α, $\beta \in \omega^*$, a straightforward inductive argument shows that

$$\widehat{\delta}(q_0,\alpha\beta) = \widehat{\delta}(\widehat{\delta}(q_0,\alpha),\beta)\,,$$

thus

$$\begin{array}{rcl} t_{\mathcal{M}}\downarrow\alpha &=& \lambda\beta.t_{\mathcal{M}}(\alpha\beta) \\ &=& \lambda\beta.\ell(\widehat{\delta}(q_0,\alpha\beta)) \\ &=& \lambda\beta.\ell(\widehat{\delta}(\widehat{\delta}(q_0,\alpha),\beta)) \\ &=& t_{\mathcal{M}_\alpha}\,, \end{array}$$

where $\mathcal{M}_\alpha$ is $\mathcal{M}$ with start state $\widehat{\delta}(q_0,\alpha)$ (if it exists) instead of q_0. If $\widehat{\delta}(q_0,\alpha)$ does not exist, then $t_{\mathcal{M}}\downarrow\alpha$ has empty domain. Thus $t_{\mathcal{M}}$ has no more subterms than there are states of $\mathcal{M}$. The equivalence of (i) and (iii) is proved in Courcelle (1983). □

4. Types

Types are terms over the ranked alphabet $\Sigma = \{\bot, \rightarrow, \top\}$, where $\rightarrow$ is binary and $\bot$ and $\top$ are nullary. Over this signature, every $\mathscr{D}(t) \subseteq \{0,1\}^*$. At the risk of some ambiguity, we omit the superscript T_Σ on the derived operators $\rightarrow^{T_\Sigma}$, $\bot^{T_\Sigma}$, $\top^{T_\Sigma}$, and use infix notation for $\rightarrow$; thus we write $s \rightarrow t$ for the term with left subterm s and right subterm t, and $\bot$ and $\top$ for the singleton terms with the corresponding labels.

The finite types F_Σ are ordered naturally by the following inductively defined binary relation $\leq_{\mathrm{FIN}}$. This relation captures the natural type inclusion or coercion order, in that it is covariant in the range and contravariant in the domain of a function type.

Definition 4.1. The order $\leq_{\mathrm{FIN}}$ is the smallest binary relation on F_Σ such that

(i) $\bot \leq_{\mathrm{FIN}} t \leq_{\mathrm{FIN}} \top$ for all finite t;
(ii) if $s' \leq_{\mathrm{FIN}} s$ and $t \leq_{\mathrm{FIN}} t'$, then $s \rightarrow t \leq_{\mathrm{FIN}} s' \rightarrow t'$.

We remark that the converse of Definition 4.1(ii) holds as well, since F_Σ is a free algebra.

In order to handle recursive types, we need to extend the ordering $\leq_{\mathrm{FIN}}$ to infinite types in a natural way. Much of the effort in Amadio and Cardelli's paper (Amadio and Cardelli 1991) is devoted to this task. Their definition, which involves infinite sequences of finite approximations, is given later (Definition 4.7). Here we give a simplified definition that does not involve approximations (Definition 4.3). We will eventually show (Theorem 4.8) that the two definitions are equivalent.

Definition 4.2. The *parity* of $\alpha \in \{0,1\}^*$ is the number mod 2 of 0's in α. The parity of α is denoted $\pi\alpha$. A string α is said to be *even* if $\pi\alpha = 0$ and *odd* if $\pi\alpha = 1$.

Definition 4.3. Let $\leq_0$ be the linear order

$$\bot \leq_0 \rightarrow \leq_0 \top$$

on Σ, and let $\leq_1$ be its reverse

$$\top \leq_1 \rightarrow \leq_1 \bot .$$

For $s, t \in T_\Sigma$, define $s \leq t$ if $s(\alpha) \leq_{\pi\alpha} t(\alpha)$ for all $\alpha \in \mathscr{D}(s) \cap \mathscr{D}(t)$.

Lemma 4.4. The relation $\leq$ is a partial order on T_Σ, and agrees with $\leq_{\mathrm{FIN}}$ on F_Σ. In particular, for any s, t, s', t',

(i) $\bot \leq t \leq \top$
(ii) $t \leq \bot$ if and only if $t = \bot$
(iii) $\top \leq t$ if and only if $t = \top$
(iv) $s \rightarrow t \leq s' \rightarrow t'$ if and only if $s' \leq s$ and $t \leq t'$.

Proof. First we show that $\leq$ is a partial order. Reflexivity is trivial, since $\leq_{\pi\alpha}$ is a partial order.

For transitivity, suppose $s \leq t \leq u$. Let $\alpha \in \mathscr{D}(s) \cap \mathscr{D}(u)$. Surely $\epsilon \in \mathscr{D}(t)$; and if β is a proper prefix of α in $\mathscr{D}(t)$, then

$$\rightarrow \;=\; s(\beta) \;\leq_{\pi\beta}\; t(\beta) \;\leq_{\pi\beta}\; u(\beta) \;=\; \rightarrow ,$$

so $t(\beta) = \rightarrow$, therefore, β is not a leaf of $\mathscr{D}(t)$. Since $\epsilon \in \mathscr{D}(t)$ and no proper prefix of α is a leaf of $\mathscr{D}(t)$, we must have $\alpha \in \mathscr{D}(t)$. But then

$$s(\alpha) \quad \leq_{\pi\alpha} \quad t(\alpha) \quad \leq_{\pi\alpha} \quad u(\alpha) \ ,$$

thus $s(\alpha) \leq_{\pi\alpha} u(\alpha)$ by the transitivity of $\leq_{\pi\alpha}$. Since α was arbitrary, $s \leq u$.
For antisymmetry, assume $s \leq t \leq s$. Let $\alpha \in \mathscr{D}(s)$. Arguing as above, we must have $\alpha \in \mathscr{D}(t)$, thus $\mathscr{D}(s) \subseteq \mathscr{D}(t)$, and by symmetry, $\mathscr{D}(t) \subseteq \mathscr{D}(s)$. For any $\alpha \in \mathscr{D}(s) \cap \mathscr{D}(t)$, we have

$$s(\alpha) \quad \leq_{\pi\alpha} \quad t(\alpha) \quad \leq_{\pi\alpha} \quad s(\alpha) \ ,$$

thus $s(\alpha) = t(\alpha)$. Since s and t have the same domain and agree on the intersection of their domains, they are equal.
We next establish the properties (i)–(iv) in turn.
(i) For any t, we have $\epsilon \in \mathscr{D}(t)$ and $\bot(\epsilon) \leq_0 t(\epsilon) \leq_0 \top(\epsilon)$.
(ii), (iii) follow immediately from (i) and antisymmetry.
(iv) For *if*, suppose $s' \leq s$ and $t \leq t'$ and let $\alpha \in \mathscr{D}(s \to t) \cap \mathscr{D}(s' \to t')$. If $\alpha = \epsilon$, we have

$$(s \to t)(\epsilon) \quad = \quad (s' \to t')(\epsilon) \quad = \quad \to \ ,$$

so

$$(s \to t)(\epsilon) \quad \leq_{\pi\epsilon} \quad (s' \to t')(\epsilon) \ .$$

If $\alpha = 0\beta$, then $\beta \in \mathscr{D}(s) \cap \mathscr{D}(s')$ and

$$\begin{aligned} (s' \to t')(\alpha) &= (s' \to t')(0\beta) \\ &= s'(\beta) \\ &\leq_{\pi\beta} s(\beta) \\ &= (s \to t)(0\beta) \\ &= (s \to t)(\alpha) \ , \end{aligned}$$

therefore

$$(s \to t)(\alpha) \quad \leq_{\pi\alpha} \quad (s' \to t')(\alpha) \ .$$

If $\alpha = 1\beta$, then $\beta \in \mathscr{D}(t) \cap \mathscr{D}(t')$ and

$$(s \to t)(\alpha) \quad \leq_{\pi\alpha} \quad (s' \to t')(\alpha) \ ,$$

by a similar argument.
For *only if*, assume that $s \to t \leq s' \to t'$. Let $\alpha \in \mathscr{D}(s) \cap \mathscr{D}(s')$. Then $0\alpha \in \mathscr{D}(s \to t) \cap \mathscr{D}(s' \to t')$, so

$$\begin{aligned} s(\alpha) &= (s \to t)(0\alpha) \\ &\leq_{\pi(0\alpha)} (s' \to t')(0\alpha) \\ &= s'(\alpha) \ , \end{aligned}$$

thus $s'(\alpha) \leq_{\pi\alpha} s(\alpha)$. Since α was arbitrary, $s' \leq s$. A similar argument shows that for arbitrary $\alpha \in \mathscr{D}(t) \cap \mathscr{D}(t')$, we have $t(\alpha) \leq_{\pi\alpha} t'(\alpha)$, thus $t \leq t'$.
Finally, we show that the orders $\leq_{\text{FIN}}$ and $\leq$ agree on finite types, *i.e.*, $s \leq t$ if and only

if $s \leq_{\mathrm{FIN}} t$. We proceed by induction on the structure of s and t. If $s = \bot$ or $t = \top$, the result follows from (i). If $t = \bot$, the result is immediate from (ii), and if $s = \top$, the result is immediate from (iii). The remaining case

$$s \to t \leq s' \to t' \iff s \to t \leq_{\mathrm{FIN}} s' \to t'$$

follows immediately from (iv) and the induction hypothesis on the subterms. □

In order to define Amadio and Cardelli's order, we have to consider finite approximations to infinite terms. This is done using a *truncation operator.*

Definition 4.5. Let $g : \omega^* \to \{\bot, \top\}$. For any term t, we define a finite term $t|_k^g$, the *level-k truncation of t with respect to g*, as follows:

$$\begin{aligned}\mathcal{D}(t|_k^g) &= \{\alpha \in \mathcal{D}(t) \mid |\alpha| \leq k\} \\ t|_k^g(\alpha) &= \begin{cases} t(\alpha), & \text{if } |\alpha| < k, \\ g(\alpha), & \text{if } |\alpha| = k. \end{cases}\end{aligned}$$

In other words, $t|_k^g$ is obtained by truncating the term t at depth k and relabeling the leaves according to g.

For example, let

$$\mathrm{AC}(\alpha) = \begin{cases} \bot, & \text{if } \alpha \text{ even}, \\ \top, & \text{if } \alpha \text{ odd}. \end{cases}$$

The truncation operator $|_k^{\mathrm{AC}}$ is the one employed by Amadio and Cardelli (Amadio and Cardelli 1991). It has the nice property that $t|_k^{\mathrm{AC}} \leq_{\mathrm{FIN}} t|_{k+1}^{\mathrm{AC}}$, although this property turns out not to be essential. The following lemma shows that the particular function g chosen in the definition of the truncation operator is irrelevant for our purposes.

Define $s \leq^k t$ if $s(\alpha) \leq_{\pi\alpha} t(\alpha)$ for all $\alpha \in \mathcal{D}(s) \cap \mathcal{D}(t)$ such that $|\alpha| < k$. Note that g is not mentioned in this condition.

Lemma 4.6. For any function $g : \omega^* \to \{\bot, \top\}$, terms s and t, and $k \geq 0$,

$$s|_k^g \leq t|_k^g \quad \text{iff} \quad s \leq^k t\,.$$

Proof. Suppose $s|_k^g \leq t|_k^g$. If $\alpha \in \mathcal{D}(s) \cap \mathcal{D}(t)$ and $|\alpha| < k$, then $\alpha \in \mathcal{D}(s|_k^g) \cap \mathcal{D}(t|_k^g)$ and

$$s(\alpha) = s|_k^g(\alpha) \leq_{\pi\alpha} t|_k^g(\alpha) = t(\alpha)\,.$$

Conversely, suppose $s \leq^k t$. If $\alpha \in \mathcal{D}(s|_k^g) \cap \mathcal{D}(t|_k^g)$ and $|\alpha| < k$, then $\alpha \in \mathcal{D}(s) \cap \mathcal{D}(t)$ and

$$s|_k^g(\alpha) = s(\alpha) \leq_{\pi\alpha} t(\alpha) = t|_k^g(\alpha)\,,$$

and if $\alpha \in \mathcal{D}(s|_k^g) \cap \mathcal{D}(t|_k^g)$ and $|\alpha| = k$, then $s|_k^g(\alpha) = t|_k^g(\alpha) = g(\alpha)$. □

Definition 4.7. Amadio-Cardelli's order $\leq_{\mathrm{AC}}$ is defined as

$$s \leq_{\mathrm{AC}} t \iff s|_k^{\mathrm{AC}} \leq_{\mathrm{FIN}} t|_k^{\mathrm{AC}} \text{ for all } k \geq 0.$$

By Lemmas 4.4 and 4.6, this definition is independent of the choice of truncation operator.

Theorem 4.8. The relations $\leq$ and $\leq_{\mathrm{AC}}$ agree.

Proof. For any terms s and t,

$$\begin{aligned} s \le t &\iff s \le^k t \text{ for all } k \ge 0 \\ &\iff s|_k^{\mathrm{AC}} \le t|_k^{\mathrm{AC}} \text{ for all } k \ge 0, \text{ by Lemma 4.6} \\ &\iff s|_k^{\mathrm{AC}} \le_{\mathrm{FIN}} t|_k^{\mathrm{AC}} \text{ for all } k \ge 0, \text{ by Lemma 4.4} \\ &\iff s \le_{\mathrm{AC}} t\,. \end{aligned}$$

□

5. An algorithm

In this section we give an algorithm to decide whether $s \le t$ for two given regular types s and t. Assume s and t are given by term automata $\mathscr{M}$ and $\mathscr{N}$ respectively over the ranked alphabet $\Sigma = \{\bot, \rightarrow, \top\}$. If s and t are given by other means, say by simultaneous equations as in Amadio and Cardelli (1991), then results of Courcelle (1983) can be used to obtain the automata in linear time, as described in Lemma 3.3 of Section 3.

Recall from Definition 4.3 that $s \le t$ iff $s(\alpha) \le_{\pi\alpha} t(\alpha)$ for all $\alpha \in \mathscr{D}(s) \cap \mathscr{D}(t)$. Equivalently, $s \not\le t$ iff the set

$$\{\alpha \in \mathscr{D}(s) \cap \mathscr{D}(t) \mid s(\alpha) \not\le_{\pi\alpha} t(\alpha)\} \tag{1}$$

is nonempty. We show that the set (1) is a regular subset of $\{0,1\}^*$, and describe a conventional finite automaton $\mathscr{A}$ (in the sense of Hofcroft and Ullman (1979)) over the input alphabet $\{0,1\}$ that accepts exactly this set.

Define

$$\mathscr{A} \quad = \quad (Q^{\mathscr{A}},\ \{0,1\},\ q_0^{\mathscr{A}},\ \delta^{\mathscr{A}},\ F^{\mathscr{A}})$$

where:

— $Q^{\mathscr{A}} = Q^{\mathscr{M}} \times Q^{\mathscr{N}} \times \{0,1\}$ are the states of $\mathscr{A}$;
— $q_0^{\mathscr{A}} = (q_0^{\mathscr{M}}, q_0^{\mathscr{N}}, 0)$ is the start state of $\mathscr{A}$;
— $\delta^{\mathscr{A}} : Q^{\mathscr{A}} \times \{0,1\} \rightarrow Q^{\mathscr{A}}$ is the partial function that for $b, i \in \{0,1\}$, $p \in Q^{\mathscr{M}}$ and $q \in Q^{\mathscr{N}}$ gives

$$\delta^{\mathscr{A}}((p,q,b),i) \quad = \quad (\delta^{\mathscr{M}}(p,i), \delta^{\mathscr{N}}(q,i), b \oplus \pi i)\,,$$

where $\oplus$ denotes mod 2 sum;
— the set of accept states of $\mathscr{A}$ is

$$F^{\mathscr{A}} \quad = \quad \{(p,q,b) \mid \ell^{\mathscr{M}}(p) \not\le_b \ell^{\mathscr{N}}(q)\}\,.$$

According to this definition, $\delta^{\mathscr{A}}((p,q,b),i)$ is defined if and only if $\ell^{\mathscr{M}}(p) = \ell^{\mathscr{N}}(q) = \rightarrow$. The automaton $\mathscr{A}$ is nondeterministic only in the sense that the state (p,q,b) has no i-successors if either $\ell^{\mathscr{M}}(p)$ or $\ell^{\mathscr{N}}(q) \in \{\bot, \top\}$. If $\ell^{\mathscr{M}}(p) = \ell^{\mathscr{N}}(q) = \rightarrow$, the i-successor of (p,q,b) is defined and unique.

Theorem 5.1. The automaton $\mathscr{A}$ accepts the set (1).

Proof. Extend the partial function $\delta^{\mathscr{A}}$ to a partial function

$$\widehat{\delta}^{\mathscr{A}} : Q^{\mathscr{A}} \times \{0,1\}^* \quad \rightarrow \quad Q^{\mathscr{A}}$$

inductively as usual:

$$\begin{aligned}\widehat{\delta}^{\mathscr{A}}(p,\epsilon) &= p\\ \widehat{\delta}^{\mathscr{A}}(p,\alpha i) &= \delta^{\mathscr{A}}(\widehat{\delta}^{\mathscr{A}}(p,\alpha),i)\ .\end{aligned}$$

By definition, α is accepted by $\mathscr{A}$ iff $\widehat{\delta}^{\mathscr{A}}(q_0^{\mathscr{A}},\alpha)$ exists and is in $F^{\mathscr{A}}$.
We show by induction that for any $\alpha \in \{0,1\}^*$, $p \in Q^{\mathscr{M}}$, $q \in Q^{\mathscr{N}}$, and $b \in \{0,1\}$,

$$\widehat{\delta}^{\mathscr{A}}((p,q,b),\alpha) = (\widehat{\delta}^{\mathscr{M}}(p,\alpha),\widehat{\delta}^{\mathscr{N}}(q,\alpha),b\oplus\pi\alpha)\ . \tag{2}$$

(Of course, the use of the equality symbol $=$ to compare expressions involving partial functions bears the extra semantic condition that the left hand side is defined if and only if the right hand side is. This is an implicit but important part of our equational arguments.)
For the basis $\alpha = \epsilon$, we have

$$\begin{aligned}\widehat{\delta}^{\mathscr{A}}((p,q,b),\epsilon) &= (p,q,b)\\ &= (\widehat{\delta}^{\mathscr{M}}(p,\epsilon),\widehat{\delta}^{\mathscr{N}}(q,\epsilon),b\oplus\pi\epsilon)\ .\end{aligned}$$

For the induction step,

$$\begin{aligned}\widehat{\delta}^{\mathscr{A}}((p,q,b),\alpha i) &= \delta^{\mathscr{A}}(\widehat{\delta}^{\mathscr{A}}((p,q,b),\alpha),i)\\ &= \delta^{\mathscr{A}}((\widehat{\delta}^{\mathscr{M}}(p,\alpha),\widehat{\delta}^{\mathscr{N}}(q,\alpha),b\oplus\pi\alpha),i)\\ &= (\delta^{\mathscr{M}}(\widehat{\delta}^{\mathscr{M}}(p,\alpha),i),\delta^{\mathscr{N}}(\widehat{\delta}^{\mathscr{N}}(q,\alpha),i),b\oplus\pi\alpha\oplus\pi i)\\ &= (\widehat{\delta}^{\mathscr{M}}(p,\alpha i),\widehat{\delta}^{\mathscr{N}}(q,\alpha i),b\oplus\pi(\alpha i))\ .\end{aligned}$$

From (2) we have that the domain of the partial function

$$\lambda\alpha.\widehat{\delta}^{\mathscr{A}}((p,q,b),\alpha)$$

is the intersection of the domains of $\lambda\alpha.\widehat{\delta}^{\mathscr{M}}(p,\alpha)$ and $\lambda\alpha.\widehat{\delta}^{\mathscr{N}}(q,\alpha)$. This says that any string α accepted by $\mathscr{A}$ must lie in the set

$$\begin{aligned}\mathscr{D}(\lambda\alpha.\widehat{\delta}^{\mathscr{A}}(q_0^{\mathscr{A}},\alpha)) &= \mathscr{D}(\lambda\alpha.\widehat{\delta}^{\mathscr{M}}(q_0^{\mathscr{M}},\alpha))\cap\mathscr{D}(\lambda\alpha.\widehat{\delta}^{\mathscr{N}}(q_0^{\mathscr{N}},\alpha))\\ &= \mathscr{D}(s)\cap\mathscr{D}(t)\ .\end{aligned}$$

For such strings α,

$$\begin{aligned}\alpha \text{ is accepted by } \mathscr{A} &\iff \widehat{\delta}^{\mathscr{A}}(q_0^{\mathscr{A}},\alpha)\in F^{\mathscr{A}}\\ &\iff \widehat{\delta}^{\mathscr{A}}((q_0^{\mathscr{M}},q_0^{\mathscr{N}},0),\alpha)\in F^{\mathscr{A}}\\ &\iff (\widehat{\delta}^{\mathscr{M}}(q_0^{\mathscr{M}},\alpha),\widehat{\delta}^{\mathscr{N}}(q_0^{\mathscr{N}},\alpha),0\oplus\pi\alpha)\in F^{\mathscr{A}}\\ &\iff (\widehat{\delta}^{\mathscr{M}}(q_0^{\mathscr{M}},\alpha),\widehat{\delta}^{\mathscr{N}}(q_0^{\mathscr{N}},\alpha),\pi\alpha)\in F^{\mathscr{A}}\\ &\iff \ell^{\mathscr{M}}(\widehat{\delta}^{\mathscr{M}}(q_0^{\mathscr{M}},\alpha))\not\leq_{\pi\alpha}\ell^{\mathscr{N}}(\widehat{\delta}^{\mathscr{N}}(q_0^{\mathscr{N}},\alpha))\\ &\iff s(\alpha)\not\leq_{\pi\alpha}t(\alpha)\ .\end{aligned}$$

Thus $\mathscr{A}$ accepts the set (1). □

To decide whether $s \leq t$, we construct the automaton $\mathscr{A}$ and ask whether it accepts a nonempty set, *i.e.*, whether there exists a path from the start state to some final state. This can be determined in linear time in the size of $\mathscr{A}$ using depth first search.

The automaton $\mathscr{A}$ has $2 \cdot |Q^{\mathscr{M}}| \cdot |Q^{\mathscr{N}}|$ states and at most two transition edges from each state. Thus the entire algorithm takes no more than $O(|s| \cdot |t|)$ time, where $|s|$ and $|t|$ are the sizes of the representations of the regular terms s and t. We have shown.

Theorem 5.2. The subtype relation for recursive types can be decided in time $O(n^2)$.

This result generalizes to an arbitrary signature of type constructors, each having for every argument a given polarity.

Acknowledgements

This work was supported by the Danish Research Academy, the National Science Foundation, the John Simon Guggenheim Foundation, the U.S. Army Research Office through the ACSyAM branch of the Mathematical Sciences Institute of Cornell University under contract DAAL03-91-C-0027, and the Danish Research Council under the DART Project (5.21.08.03). An earlier version of this paper appeared as (Kozen, Palsberg and Schwartzbach 1993).

References

Amadio, R. M. and Cardelli, L. (1991) Subtyping recursive types. In: *Proc. 18th Symp. Princip. Programming Lang.*, ACM 104–118.

Cardelli, L. (1985) Amber. In: Combinators and Functional Programming Languages, Proc. 13th Summer School School of the LITP. *Springer-Verlag Lecture Notes in Computer Science* **242**.

Cardelli, L. (1989) Typeful programming. In: *Lect. Notes for the IFIP Advanced Seminar on Formal Methods in Programming Language Semantics.*

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

Courcelle, B. (1983) Fundamental properties of infinite trees. *Theor. Comput. Sci.* **25** 95–169.

Hopcroft, J. E. and Ullman, J. D. (1979) *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley.

Kozen, D., Palsberg, J. and Schwartzbach, M. I. (1992) Efficient inference of partial types. In: *Proc. 33rd IEEE Symp. Found. Comput. Sci.* 363–371.

Kozen, D., Palsberg, J. and Schwartzbach, M. I. (1993) Efficient recursive subtyping. In: *Proc. 20th ACM Symp. Princip. Programming Lang.*, ACM 419–428.

O'Keefe, P. M. and Wand, M. (1992) Type inference for partial types is decidable. In: Proc. ESOP'92, European Symposium on Programming. *Springer-Verlag Lecture Notes in Computer Science* **582**.

Thatte, S. (1988) Type inference with partial types. In: Proc. International Colloquium on Automata, Languages, and Programming 1988. *Springer-Verlag Lecture Notes in Computer Science* **317**.