Modular control-flow analysis with rank 2 intersection types

ANINDYA BANERJEE and THOMAS JENSEN

Mathematical Structures in Computer Science / Volume 13 / Issue 01 / February 2003, pp 87 - 124
DOI: 10.1017/S0960129502003845, Published online: 06 March 2003

Math. Struct. in Comp. Science (2003), *vol.* 13, *pp.* 87–124.
DOI: 10.1017/S0960129502003845 Printed in the United Kingdom

Modular control-flow analysis with rank 2 intersection types

ANINDYA BANERJEE[†] and THOMAS JENSEN[‡]

[†]*Department of Computing and Information Sciences, Kansas State University, Manhattan KS 66506, U.S.A.*
Email: ab@cis.ksu.edu

[‡]*IRISA/CNRS, Campus de Beaulieu, F-35042 Rennes, France*
Email: jensen@irisa.fr

Received 22 January 2001; revised 18 April 2002

We show how the principal typing property of the rank 2 intersection type system enables the specification of a modular and polyvariant control-flow analysis.

1. Introduction

The performance of optimising compilers crucially depends on the availability of control-flow information at compile time. For any first-order imperative program, such information is available *via* a flowchart constructed from the program text. Consequently, traditional dataflow analyses can be used to perform a series of compile-time program optimisations (Aho *et al.* 1986). For higher-order programs, however, a control-flow graph is often not evident from the program text. In these programs, even simple control structures like while loops are implemented using functions and computation is hidden under a single operation: function application. Hence, a number of *control-flow analyses* have been proposed (Jones 1981; Sestoft 1988; Shivers 1991; Jagannathan and Weeks 1995) for higher-order programs, all of which seek to answer the fundamental question: given a program point, what functions can be the result of evaluation there? Given this information, the call-graph of a program can be constructed and a suite of compiler optimisations, for example, closure conversion (Steckler and Wand 1997; Dimock *et al.* 2001), useless variable elimination (Wand and Siveroni 1999), constant propagation, induction variable elimination (Shivers 1991), and so on, can be enabled.

The classical technique for control-flow analysis is abstract interpretation (Cousot and Cousot 1977) of either the denotational semantics of the underlying language (Shivers 1991) or of its operational semantics (Nielson and Nielson 1997). An equivalent

[†] Partially supported by postdoctoral fellowships at the Laboratoire d'Informatique, École Polytechnique, Palaiseau, France (thanks to Radhia Cousot) and at DAIMI, University of Aarhus, Denmark (thanks to Flemming Nielson); and by NSF grant EIA-9806835.
[‡] Partially supported by the European IST Future and Emerging Technologies scheme (project IST-1999-29075 'Secsafe').

technique uses a system of constraints to specify control-flow analysis so that flow information is obtained as the minimal solution of the constraint system (Palsberg 1995). Both techniques require whole-program analysis. For control-flow analysis of program fragments containing free variables, the above techniques usually assume an environment that associates a property with each free variable or assume that only trivial properties hold for the free variables. Neither assumption is satisfactory: the former requires re-analysis whenever the environment changes; the latter leads to poor analysis results and the rejection of program fragments that require functions as inputs.

We describe an algorithm for modular and polyvariant control-flow analysis of simply typed program fragments. The result of analysing a program fragment P is a pair containing a property *and* an environment: the pair describes a *relation* between the properties of the free variables of P and the property of the entire program fragment P. The environment provides a summary of the minimum set of constraints that must be satisfied by any other program fragment that may link to P. Our algorithm computes a 'principal solution': the environment and property of any other program fragment that links to P can be obtained as an instance of the environment and property computed for P (see Theorem 6.4 for the precise statement). Thus, no re-analysis of P is required.

Recently, there has been much interest in using annotated type systems for program analysis. The intuition is that types and expressions can be annotated with the properties of interest, for example, control-flows (Tang 1994; Heintze 1995; Banerjee 1997), binding times (Nielson and Nielson 1992; Hatcliff and Danvy 1997; Nielson and Nielson 1998), strictness (Kuo and Mishra 1989; Jensen 1991; Benton 1992; Jensen 1998) effects (Talpin and Jouvelot 1994), regions (Tofte and Talpin 1994; Tofte and Talpin 1997), concurrent behaviours (Amtoft *et al.* 1997), dead-code (Damiani 1996; Damiani and Prost 1996; Coppo *et al.* 1998; Kobayashi 2000), and so on, so that if an expression e has the annotated type τ, then evaluation of the expression exhibits the properties described by the annotation of τ. Static analysis of the expression e is then synonymous with the calculation, *via* an annotated-type inference algorithm, of its property annotations. For control-flow analysis, we annotate every function in an expression with a label, and associate a set of function labels φ with every function type τ. The intuition is that if e evaluates to a closure, then the text of the closure is a function whose label is in φ. The static determination of the set of function labels that e can possibly evaluate to is thus synonymous with the calculation, *via* an inference algorithm, of its flow annotations.

An advantage of the type-based approach is that it provides a method for performing *compositional* and *modular* program analysis. 'Compositional' means that the analysis of an expression is derived through the composition of the analyses of its proper subparts. We say that an analysis is 'modular' if it can analyse program fragments containing free variables in isolation, and if the linking of fragments does not require their re-analysis. A modular program analysis thus seems indispensable for *separate compilation*; however, the extent to which modular analyses can be used in practice for efficient separate compilation, remains to be seen. The effective use of the information obtained from a modular analysis depends on link-time optimisations; but such optimisations are rarely done in industrial-strength compilers at present.

1.1. *Goals and methods*

The goal of this article is to provide an algorithm for modular control-flow analysis of simply typed functional programs. For precision, we also demand that our analysis be *polyvariant*, that is, it must annotate a function with different properties at its different application sites.

How can we achieve a modular analysis? We make the following observation due to Damas (Damas 1985, Chapter 1): the simply typed lambda calculus satisfies the *principal typing property*. This means, given a typable program fragment e, possibly containing free variables, there is a pair $\langle \Gamma, \tau \rangle$ such that $\Gamma \vdash e : \tau$ represents all valid typings (that is, type-derivation trees) of e. Furthermore, there is an algorithm that calculates such a pair for e. The significance is first that the user does *not* have to supply the types of the free variables of e (they can be inferred automatically, which means that one can type all *uses* of a free variable independently of its *definitions*) a feature crucial for analysing program fragments. Second, when fragments are linked, the typing of e might possibly change, though principality guarantees that the new typing is always a substitution instance of $\Gamma \vdash e : \tau$. Thus we can avoid a re-inference of e upon linking. Principal typing is thus a simple way of achieving a modular analysis. In the rest of the paper, we apply this idea to obtain a modular closure analysis.

How can we achieve a polyvariant analysis? Since a function may be applied to different arguments and may return different results at each of its application sites, we can represent the different behaviours as an intersection type (Sallé 1978; Coppo *et al.* 1980a; Coppo *et al.* 1980b). This idea has been used in other contexts, for example, strictness analysis. In such analyses, the ability to form intersections of types has proved essential since they allow us to express several properties of a function in one formula. Jensen (1991; 1995) proved that by adding intersections to a language of strictness types, we obtain an analysis in the style of intersection types that is equivalent in power to the abstract interpretation-based strictness analysis of Burn *et al.* (1986).

The intersection types we will consider are the 'rank 2 intersection types'. Intuitively, the rank of a type describes the nesting of functions in argument position. The notion of rank has been used to identify restricted versions of intersection type systems for which type inference is decidable. In particular, type inference in the rank 2 intersection type system yields principal typings (Jim 1996). Thus, we can achieve our goal of providing a modular and polyvariant analysis. Furthermore, the rank 2 intersection type system types significantly more terms than core ML, and, moreover, can assign more general principal types to some core ML terms than the ML type system (van Bakel 1993). While recent results by Kfoury and Wells indicate the existence of principal typings and show decidability of type inference in systems of finite-rank intersection types (Kfoury and Wells 1999), we have not pursued this direction. Rather, we restrict ourselves to rank 2 intersection types because the constraints resulting from an analysis based on such types are simple to solve. In technical terms, we avoid having to solve constraints of the form $\varphi_1 \wedge \varphi_2 \leqslant \psi$ over function domains; this is also the reason why we have not considered the full intersection type discipline.

The inference algorithm that implements the control-flow analysis deals with the subtyping that naturally arises from the fact that one program property implies other properties. We follow the standard approach to type inference in the presence of subtyping by letting the result of typing a term e be a *triple* (Γ, φ, C), where φ is a property of e, Γ is a set of assumptions on the free variables of e, and C is a set of constraints. Property variables are used to describe the dependencies between the property φ and the properties in the environment. The constraint set C limits the way in which the property variables in Γ and φ can be instantiated.

1.2. *A small typed functional language*

We choose a language with simple types as our base language. The language, called vPCF (Riecke 1991), is essentially call-by-value PCF (Plotkin 1977) with recursion, conditionals and basic arithmetic. The types and terms of the language are given by following grammar, where op abbreviates either the succ or the pred operations.

$$\begin{aligned} \sigma, \tau &::= \mathsf{int} \mid \sigma \to \sigma \\ v &::= n \mid \lambda x^{\sigma} \cdot e \mid \mathsf{fun}\, f^{\sigma \to \tau}(x^{\sigma}) = e \\ e &::= v \mid x \mid e_1 e_2 \mid \mathsf{op}\ e \mid \mathsf{if}\ e\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 \end{aligned}$$

Values v in vPCF are integers, lambda abstractions and recursive function definitions. Since we have anonymous functions in the language *via* lambda abstractions, we insist that in a recursive function declaration $\mathsf{fun}\, f^{\sigma \to \tau}(x^{\sigma}) = e$, the function name f and the parameter x both appear in e. The type system for vPCF is the standard one and is omitted except for the rule for recursion:

$$\frac{\Gamma \oplus \{f : \sigma \to \tau\} \oplus \{x : \sigma\} \vdash e : \tau}{\Gamma \vdash \mathsf{fun}\, f^{\sigma \to \tau}(x^{\sigma}) = e : \sigma \to \tau}$$

where Γ denotes the type environment, in which identifiers are associated with simple types. The notation $\Gamma \oplus \{x : \sigma\}$ means 'extend the environment Γ with the binding $\{x : \sigma\}$, where $x \notin \mathit{Dom}(\Gamma)$'.

1.3. *Organisation*

The rest of this paper is structured as follows. Section 2 gives a brief review of control-flow analysis by means of an example. Section 3 introduces the language of properties, defines the rank 2 intersection properties and shows how to define a 'generic' control-flow property for each type. Section 4 introduces the language ℓPCF and specifies, *via* inference rules, a property system for polyvariant control-flow analysis for ℓPCF. Orderings on ranked properties, needed in the inference rules, are introduced and several properties of the ranked types and of the inference rules are shown in this section. Section 5 provides the small-step operational semantics and type soundness results for ℓPCF. Section 6 provides the type inference algorithm for inferring control-flow information, and proves soundness (Section 6.2) and completeness (Section 6.3) of the algorithm. The soundness

of the inference algorithm, in conjunction with type soundness, shows correctness of the analysis: this is explained at the end of Section 6.2. Section 7 surveys related work and Section 8 concludes with a discussion.

This article grew out of two papers: Banerjee (1997) developed a modular and polyvariant control-flow analysis for untyped programs that infers control flow information and types at the same time; Jensen (1998) proposed a modular strictness analysis for typed programs based on intersection types and parametric polymorphism. Working with a typed language means that the analysis can use powerful induction principles (akin to polymorphic recursion) and still guarantee that the analysis terminates. In this article, we show how a control-flow analysis for a typed, higher-order functional language can be designed based on the techniques developed in these previous works.

2. Control-flow analysis

Consider an expression in vPCF such that all lambda abstractions and recursive function definitions in this expression are labelled uniquely. Let λ^{ℓ} and $\mathsf{fun}^{\ell'}$ refer to the lambda abstraction labelled ℓ and the recursive function labelled ℓ'. A node in the abstract syntax tree of an expression is called a 'program point'. Then, given a closed expression, control-flow analysis (CFA) seeks to answer the following question:

What set of function labels (that is, labelled lambda abstractions or recursive function definitions) can each program point possibly evaluate to?

In particular, if the program point is an application site, the question is the same as:

What set of function labels (that is, labelled lambda abstractions or recursive function definitions) can be called from the application site?

We give an example of CFA below. For precise details of the usual abstract interpretation-based analysis, we refer the reader to the Sestoft (1991) and Shivers (1991), which provide two distinct control-flow analyses using abstract interpretation; see Mossin (1997b) for a comparison of the two analyses.

Example. The term

$$T = (\lambda^1 g^{(\mathsf{int}\to\mathsf{int})\to(\mathsf{int}\to\mathsf{int})} \cdot g(g(\lambda^2 v^{\mathsf{int}} \cdot v)))\ \ (\lambda^3 x^{(\mathsf{int}\to\mathsf{int})} \cdot \lambda^4 y^{\mathsf{int}} \cdot y)$$

with type $\mathsf{int} \to \mathsf{int}$, will serve as a running example throughout the article. Control-flow analysis of T yields the following results:

1 The function part of the application, $\lambda^1 g \cdot g(g(\lambda^2 v \cdot v))$, yields $\{1\}$.
  The variable g yields $\{3\}$.
  $\lambda^2 v \cdot v$ yields $\{2\}$.
  The application $g(\lambda^2 v \cdot v)$ yields $\{4\}$.
  The application $g(g(\lambda^2 v \cdot v))$ yields $\{4\}$.
2 The argument part of the application $\lambda^3 x \cdot \lambda^4 y \cdot y$ yields $\{3\}$.
  y yields $\varnothing$.
  $\lambda^4 y \cdot y$, yields $\{4\}$.
3 The entire expression T yields $\{4\}$.

Table 1. *Rank 2 properties.*

$\mathsf{t}^{\mathsf{int}} \in Prop_0(\mathsf{int})$	$\dfrac{\varphi_1 \in Prop_0(\sigma) \quad \varphi_2 \in Prop_0(\tau) \quad \kappa \in Labels(\sigma \to \tau)}{(\varphi_1 \to \varphi_2, \kappa) \in Prop_0(\sigma \to \tau)}$
$\dfrac{\varphi \in Prop_0(\sigma)}{\varphi \in Prop_1(\sigma)}$	$\dfrac{\varphi_i \in Prop_0(\sigma), i \in I}{\bigwedge_{i \in I} \varphi_i \in Prop_1(\sigma)}$
$\dfrac{\varphi \in Prop_0(\sigma)}{\varphi \in Prop_2(\sigma)}$	$\dfrac{\varphi_1 \in Prop_1(\sigma) \quad \varphi_2 \in Prop_2(\tau), \quad \kappa \in Labels(\sigma \to \tau)}{(\varphi_1 \to \varphi_2, \kappa) \in Prop_2(\sigma \to \tau)}$

The interesting case is that of the function, λ^3: it gets applied once to λ^2, and again to the result of this application, that is, to λ^4. Shivers's abstract interpretation-based 0CFA analysis would report that at each of its application sites, λ^3 is possibly applied to the set $\{2, 4\}$. For a polyvariant analysis, however, we expect the analysis to report: at the application site $g(\lambda^2 v \cdot v)$, λ^3 is applied to λ^2, and at the application site $g(g(\ldots))$, λ^3 is applied to λ^4. In the following, we will capture this polyvariance using intersection types.

3. A property system for polyvariant control-flow analysis

Here and in the following sections, we are motivated by the general framework for type inference in the presence of subtypes as defined in Mitchell (1991), and extended to control-flow analysis by Heintze (1995), and to behaviour analysis by Amtoft *et al.* (1997) and Amtoft *et al.* (1999) We show that the rank 2 fragment of the intersection type discipline can be instrumented to perform a polyvariant control-flow analysis. We first define the instrumented rank 2 intersection types (called rank 2 control-flow properties). The definition follows that of Jim (Jim 1995; 1996), who built on earlier work (Leivant 1983; van Bakel 1993; van Bakel 1996).

Let L be a countably infinite set of labels. For each type σ, we have an infinite set of *label variables* ranged over by ξ. The BNF of labels at a given type σ is specified below:

$$Labels(\sigma) \ni \kappa ::= \xi \mid L \mid \kappa_1 \cup \kappa_2.$$

For each type σ, define the *properties at* σ, $Prop(\sigma)$, to be the smallest set satisfying

$$\mathsf{t}^{\mathsf{int}} \in Prop(\mathsf{int}) \qquad \frac{\varphi_i \in Prop(\sigma) \quad i \in I}{\bigwedge_{i \in I} \varphi_i \in Prop(\sigma)}$$

$$\frac{\varphi_1 \in Prop(\sigma) \quad \varphi_2 \in Prop(\tau) \quad \kappa \in Labels(\sigma \to \tau)}{(\varphi_1 \to \varphi_2, \kappa) \in Prop(\sigma \to \tau)}$$

For each type σ, we also have *ranked properties at* σ, denoted by $Prop_k(\sigma)$. A property has rank k provided all intersection constructors are to the left of at most $k-1$ arrow constructors. A property at rank 0 has no intersection constructors. In this paper, we will only be interested in properties at ranks 0, 1, 2. Such properties are amenable to automatic inference and are defined in Table 1. Furthermore, we assume that the intersection operator $\wedge$ is associative, commutative and idempotent.

We can define a 'generic' property for a given type σ, written σ^*, by decorating the type with fresh property variables. Formally, the translation $(.)^*$ from types to properties is defined by induction on the structure of types as shown below:

$$\mathsf{int}^* = \mathtt{t}^{\mathsf{int}}$$
$$(\sigma \to \tau)^* = (\sigma^* \to \tau^*, \xi),\ \xi \text{ is fresh and } \xi \in \mathit{Labels}(\sigma \to \tau)$$

Clearly, $\sigma^* \in \mathit{Prop}_0(\sigma)$, and labels, if any, in σ^* are all label variables. The translation extends to environments in the obvious manner. Note how the shape of σ^* is the same as that of σ: if σ has n arrows, so has σ^*. We will exploit this property in the inference algorithm in Section 6 when generating fresh properties for variables.

Example. The control flow properties of the term $\lambda^3 x^{(\mathsf{int}\to\mathsf{int})} \cdot \lambda^4 y^{\mathsf{int}} \cdot y$ are described by the property

$$((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\}), \{3\}),$$

which states that the value of the expression is the lambda abstraction labelled 3 and that no matter what function it receives as argument, it will return the lambda expression labelled 4 as result.

4. Inference rules for control flow

4.1. ℓPCF

The language of study, ℓPCF(labelled call-by-value PCF), is an instrumented version of vPCF, with lambda abstractions and recursive functions annotated by labels. Such labelled functions are the control-flow properties of interest. Values in ℓPCF are integers and labelled functions.

$$v ::= n \mid \lambda^{\ell} x^{\sigma} \cdot e \mid \mathsf{fun}^{\ell}\, f^{\sigma\to\tau}(x^{\sigma}) = e$$
$$e ::= v \mid x \mid e_1 e_2 \mid \mathsf{op}\ e \mid \mathsf{if}\ e\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2.$$

We will assume that labels in the expression to be analysed are disjoint from the set of variables. Also, we assume the variable convention of Barendregt (1984), that is, for any expression, the set of its free variables is disjoint from the set of its bound variables.

Just as an ordinary environment Γ in the specification of vPCF maps variables to types, a property environment maps variables to properties. The sum of two property environments π_1 and π_2, denoted $\pi_1 + \pi_2$, is defined to be the property environment π, where $\mathit{Dom}(\pi) = \mathit{Dom}(\pi_1) \cup \mathit{Dom}(\pi_2)$, and

$$\pi(x) = \begin{cases} \pi_1(x) \wedge \pi_2(x), & \text{if } x \in \mathit{Dom}(\pi_1) \cap \mathit{Dom}(\pi_2) \\ \pi_1(x), & \text{if } x \in \mathit{Dom}(\pi_1) \text{ and } x \notin \mathit{Dom}(\pi_2) \\ \pi_2(x), & \text{if } x \in \mathit{Dom}(\pi_2) \text{ and } x \notin \mathit{Dom}(\pi_1). \end{cases}$$

The disjoint sum of two property environments π_1 and π_2, denoted $\pi_1 \oplus \pi_2$, is defined provided $\mathit{Dom}(\pi_1)$ and $\mathit{Dom}(\pi_2)$ are disjoint, in which case it is $\pi_1 + \pi_2$ (with the first case absent since $\mathit{Dom}(\pi_1)$ and $\mathit{Dom}(\pi_2)$ are disjoint).

Before giving the inference rules for polyvariant control-flow analysis, we give an axiomatisation of an inclusion relation between properties. Intuitively, the inclusion relation expresses when one control flow property is more approximate than another. The situation arises, for example, in a conditional expression, where the analysis for each branch of the conditional may yield different sets of functions, but each set must be coerced to a common superset. A similar situation arises in applications.

4.2. *Property orderings*

Formally, we axiomatise propositions of the form $\varphi_1 \leqslant \varphi_2$, where φ_1 and φ_2 are control flow properties.

Ordering on properties

$$\varphi \leqslant \varphi \qquad \frac{\varphi_1 \leqslant \varphi_2 \quad \varphi_2 \leqslant \varphi_3}{\varphi_1 \leqslant \varphi_3} \qquad \frac{\psi_1 \leqslant \varphi_1 \quad \varphi_2 \leqslant \psi_2 \quad \kappa_1 \subseteq \kappa_2}{(\varphi_1 \to \varphi_2, \kappa_1) \leqslant (\psi_1 \to \psi_2, \kappa_2)}$$

$$\frac{\forall \varphi \in \{\varphi_j \mid j \in J\}.\ \exists \psi \in \{\psi_i \mid i \in I\}.\ \ \psi \leqslant \varphi}{(\bigwedge_{i\in I} \psi_i) \leqslant (\bigwedge_{j\in J} \varphi_j)} \quad \varphi_j \in Prop_0(\sigma), \quad \psi_i \in Prop_0(\sigma)$$

Note that the following can be derived easily from the above ordering on properties:

$$\varphi_1 \wedge \varphi_2 \leqslant \varphi_1$$

$$\varphi_1 \wedge \varphi_2 \leqslant \varphi_2$$

$$\frac{\varphi \leqslant \varphi_i \quad i \in I}{\varphi \leqslant \bigwedge_{i\in I} \varphi_i}$$

We now show several properties of the $\leqslant$ ordering. First, we define the notion of substitution germane to this paper.

Definition 4.1. A *substitution* is a map from label variables to finite sets of labels.

We write [ ] for the empty substitution. A substitution S is lifted to properties as follows: $S(\mathsf{t}^{\mathsf{int}}) = \mathsf{t}^{\mathsf{int}}$; and, for any property φ in which all occurrences of labels are label variables, $S(\varphi)$ is defined in the obvious manner. We say that property φ is *ground* if it does not contain any occurrences of property variables. A property environment π is ground if $\pi(x)$ is ground for all $x \in Dom(\pi)$. The next three propositions relate ground properties φ at rank i, for $i = 0, 1, 2$, to their underlying types.

Proposition 4.2. Let $\varphi \in Prop_0(\sigma)$. Then there exists a substitution S with $S(\sigma^*) = \varphi$.

Proof. We use induction on the structure of properties at rank 0:

— $\mathsf{t}^{\mathsf{int}}$:
We need substitution S such that $S(\mathsf{int}^*) = \mathsf{t}^{\mathsf{int}}$. Choose S to be [ ].

— $(\varphi_1 \to \varphi_2, \kappa)$:
Then, $\varphi_1 \in Prop_0(\sigma)$ and $\varphi_2 \in Prop_0(\tau)$ and $\kappa \in Labels(\sigma \to \tau)$. Therefore, by the induction hypothesis on φ_1 and on φ_2, there exist substitutions S_1 and S_2 such that $S_1(\sigma^*) = \varphi_1$ and $S_2(\tau^*) = \varphi_2$. We need substitution S such that $S(\sigma \to \tau)^* = (\varphi_1 \to$

$\varphi_2, \kappa)$. That is, $S(\sigma^* \to \tau^*, \xi) = (\varphi_1 \to \varphi_2, \kappa)$, where ξ is the label variable, chosen fresh for $(\sigma \to \tau)^*$. Let S_3 be the substitution $[\xi \mapsto \kappa]$. Then choose the required substitution S to be $S_3 \circ S_2 \circ S_1$. □

Proposition 4.3. Let $\varphi \in Prop_1(\sigma)$. Then there exists substitution S with $\varphi \leqslant S(\sigma^*)$.

Proof. There are two cases. If $\varphi \in Prop_0(\sigma)$, then, by Proposition 4.2, there exists a substitution S such that $S(\sigma^*) = \varphi$, hence $\varphi \leqslant S(\sigma^*)$. Otherwise, $\varphi = (\bigwedge_{i \in I} \varphi_i)$. Now, for every $i \in I$, $\varphi_i \in Prop_0(\sigma)$. Hence, for any i, by Proposition 4.2, there exists substitution S such that $S(\sigma^*) = \varphi_i$; thus, for any i, we have $\varphi_i \leqslant S(\sigma^*)$, hence, by the ordering on properties, $(\bigwedge_{i \in I} \varphi_i) \leqslant S(\sigma^*)$. □

Proposition 4.4. Let $\varphi \in Prop_2(\sigma)$. Then there exists substitution S with $S(\sigma^*) \leqslant \varphi$.

Proof. There are two cases. If $\varphi \in Prop_0(\sigma)$, then, by Proposition 4.2, there exists substitution S such that $S(\sigma^*) = \varphi$, hence $S(\sigma^*) \leqslant \varphi$. Otherwise, $\varphi = (\varphi_1 \to \varphi_2, \kappa)$, where $\varphi_1 \in Prop_1(\sigma)$, $\varphi_2 \in Prop_2(\tau)$ and $\kappa \in Labels(\sigma \to \tau)$. By Proposition 4.3, there exists substitution S_1 such that $\varphi_1 \leqslant S_1(\sigma^*)$. By the induction hypothesis on φ_2, there exists substitution S_2 such that $S_2(\tau^*) \leqslant \varphi_2$. Let S_3 be the substitution $[\xi \mapsto \kappa]$. Choose the required substitution $S = S_3 \circ S_2 \circ S_1$. Then, by, the ordering on properties, $S(\sigma^* \to \tau^*, \xi) \leqslant (\varphi_1 \to \varphi_2, \kappa)$. □

Ordering on environments

The ordering on properties is extended to environments in a pointwise manner.

Definition 4.5. Let π, η be rank 1 property environments. Then, we say that $\eta \leqslant \pi$, provided for all $x \in Dom(\pi)$, it is the case that $x \in Dom(\eta)$ and $\eta(x) \leqslant \pi(x)$.

Definition 4.6. Let π, η be rank 1 property environments and φ, ψ be rank 2 properties. Then, we say that $\langle \pi, \varphi \rangle \leqslant \langle \eta, \psi \rangle$ provided $\eta \leqslant \pi$, and $\varphi \leqslant \psi$.

Proposition 4.7. Let η, π_1, π_2 be rank 1 property environments. Suppose $\eta \leqslant \pi_i$, for $i = 1, 2$. Then, $\eta \leqslant \pi_1 + \pi_2$.

Proof. Suppose $x \in Dom(\pi_1 + \pi_2)$. Then, clearly, $x \in Dom(\eta)$. We need to show $\eta(x) \leqslant (\pi_1 + \pi_2)(x)$, given $\eta(x) \leqslant \pi_1(x)$ and $\eta(x) \leqslant \pi_2(x)$. Suppose $\pi_1(x) = \varphi_1$ and $\pi_2(x) = \varphi_2$. Then $\eta(x) \leqslant \varphi_1 \wedge \varphi_2$ follows by the ordering on properties. □

4.3. *A property system for polyvariant closure analysis*

Now we are in a position to explain the property system for polyvariant control-flow analysis, which is given in Table 2. Judgements in the system have the form $\pi \vdash e^{\sigma} : \varphi$, that is, in rank 1 property environment π, expression e of type σ has rank 2 property φ. An invariant that the property system must satisfy is that the erasure of the property annotations from π and φ must yield a judgement typable in the underlying type system; in particular, the erasure of φ must yield σ. This can be easily formalised, but we choose not to do so in this paper.

Table 2. *Property system for polyvariant control-flow analysis.*

$$\textbf{Var}\ \ \pi \oplus \left\{ x : \bigwedge_{i\in I} \varphi_i \right\} \vdash x^{\sigma} : \varphi_j \quad j \in I$$

$$\textbf{Int}\ \ \pi \vdash n^{\mathsf{int}} : \mathtt{t}^{\mathsf{int}}$$

$$\textbf{Lam}\ \ \frac{\pi \oplus \{x : \bigwedge_{i\in I} \varphi_i\} \vdash e^{\tau} : \varphi \quad \ell \in L}{\pi \vdash \lambda^{\ell} x^{\sigma} \cdot e^{\tau} : ((\bigwedge_{i\in I} \varphi_i) \to \varphi, L)}$$

$$\textbf{App}\ \ \frac{\pi \vdash e_1^{\sigma\to\tau} : ((\bigwedge_{i\in I} \varphi_i) \to \varphi, \kappa) \quad \forall i \in I : \pi \vdash e_2^{\sigma} : \varphi_i' \quad \forall i \in I : \varphi_i' \leqslant \varphi_i}{\pi \vdash e_1^{\sigma\to\tau} e_2^{\sigma} : \varphi}$$

$$\textbf{If}\ \ \frac{\pi \vdash e_1^{\mathsf{int}} : \mathtt{t}^{\mathsf{int}} \quad \pi \vdash e_2^{\sigma} : \varphi_2 \quad \pi \vdash e_3^{\sigma} : \varphi_3 \quad \varphi_2 \leqslant \varphi \quad \varphi_3 \leqslant \varphi}{\pi \vdash \mathsf{if}\ e_1^{\mathsf{int}}\ \mathsf{then}\ e_2^{\sigma}\ \mathsf{else}\ e_3^{\sigma} : \varphi}$$

$$\textbf{Fun}\ \ \frac{\pi \oplus \{f : \bigwedge_{i\in I}(\varphi_i \to \varphi_i', L_i), x : \bigwedge_{j\in J} \theta_j\} \vdash e^{\tau} : \theta \quad \forall i \in I : ((\bigwedge_{j\in J} \theta_j) \to \theta, L) \leqslant (\varphi_i \to \varphi_i', L_i) \quad \ell \in L}{\pi \vdash \mathsf{fun}^{\ell} f^{\sigma\to\tau}(x^{\sigma}) = e^{\tau} : ((\bigwedge_{j\in J} \theta_j) \to \theta, L)}$$

$$\textbf{Op}\ \ \frac{\pi \vdash e^{\mathsf{int}} : \mathtt{t}^{\mathsf{int}}}{\pi \vdash \mathsf{op}\ e^{\mathsf{int}} : \mathtt{t}^{\mathsf{int}}}$$

Rule **Var** is applied at the leaves of the derivation tree. Since property environments are rank 1, that is, the property associated with each variable in the environment is a conjunction of rank 0 properties, we can (non-deterministically) choose an appropriate conjunct as property of the variable. In rule **Lam**, the bound variable x may have multiple occurrences in the body e of the lambda abstraction labelled ℓ. Therefore, since we are interested in polyvariance, in order to represent all the hypotheses made on x, we choose to give it an intersection property. In particular, if there is no occurrence of x in the body, x can be given any property as long as the erasure of x's property annotation yields its underlying type σ. Note that ℓ must be contained in the set of possible functions that the lambda abstraction can evaluate to. In rule **App**, if the function part returns a rank 2 type of the form $((\bigwedge_{i\in I} \varphi_i) \to \varphi, \kappa)$, the argument part must have properties φ_i' for each $i \in I$, such that φ_i' is a 'sub-property' of φ_i, according to the ordering on properties in Section 4. In rule **If**, the branches of the conditional may yield different properties $\varphi_2 and \varphi_3$. But since we are interested in specifying a *static* analysis, both φ_2 and φ_3 must be a sub-property of a common property φ according to the ordering on properties. In Rule **Fun**, each recursive function invocation can assign different properties to a recursive function f with label ℓ. Hence f is given the intersection type $\bigwedge_{i\in I}(\varphi_i \to \varphi_i', L_i)$ in the

antecedent. As in rule **Lam**, we require that ℓ be contained in the set of possible functions the recursive function can evaluate to (and also in each L_i).

Note how the property system is syntax-directed; there is no explicit rule for subsumption – instead subsumption is inlined in the rules in which it can occur, namely, rules **App**, **If** and **Fun**. This is done for technical convenience, namely, to facilitate proofs by structural induction. One can show the following propositions for the property system.

Proposition 4.8 (Weakening). Let $\pi \vdash e : \varphi$ be derivable. Then, for any property environment π'

$$\pi + \pi' \vdash e : \varphi.$$

Proposition 4.9 (Subproperty). Let $\pi \vdash e : \varphi$ be derivable. Then $\pi' \vdash e : \varphi'$ is derivable provided $\pi' \leqslant \pi$ and $\varphi \leqslant \varphi'$.

The proofs for both propositions are easy inductions on the height of the derivation tree of e.

Example. Consider our running example from Section 2:

$$T = (\lambda^1 g^{(\mathsf{int}\to\mathsf{int})\to(\mathsf{int}\to\mathsf{int})} \cdot g\ (g\ (\lambda^2 v^{\mathsf{int}} \cdot v)))\ \ (\lambda^3 x^{(\mathsf{int}\to\mathsf{int})} \cdot \lambda^4 y^{\mathsf{int}} \cdot y).$$

Let

$$\varphi = ((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\}) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\}), \{3\})$$

and

$$\varphi' = ((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{2\}) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\}), \{3\}).$$

We first show a typing derivation of the function part

$$\lambda^1 g^{(\mathsf{int}\to\mathsf{int})\to(\mathsf{int}\to\mathsf{int})} \cdot g\ (g\ (\lambda^2 v^{\mathsf{int}} \cdot v))$$

in stages:

$$\frac{\{g : \varphi \wedge \varphi'\} \vdash g : \varphi' \qquad \dfrac{\{g:\varphi\wedge\varphi', v:\mathtt{t}^{\mathsf{int}}\} \vdash v : \mathtt{t}^{\mathsf{int}}}{\{g:\varphi\wedge\varphi'\} \vdash \lambda^2 v \cdot v : (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{2\})}}{\{g : \varphi \wedge \varphi'\} \vdash g(\lambda^2 v \cdot v) : (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\})}. \tag{A}$$

From (**A**) using rule **App**,

$$\frac{\{g : \varphi \wedge \varphi'\} \vdash g : \varphi \qquad \{g : \varphi \wedge \varphi'\} \vdash g(\lambda^2 v \cdot v) : (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\})}{\{g : \varphi \wedge \varphi'\} \vdash g(g(\lambda^2 v \cdot v)) : (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\})}. \tag{B}$$

From (**B**) using rule **Lam**,

$$\frac{\{g : \varphi \wedge \varphi'\} \vdash g(g(\lambda^2 v \cdot v)) : (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\})}{\varnothing \vdash \lambda^1 g(g(\lambda^2 v \cdot v)) \cdot\ : (\varphi \wedge \varphi' \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\}), \{1\})}. \tag{C}$$

For the argument part $\lambda^3 x \cdot \lambda^4 y \cdot y$, note that using rule **Lam**,

$$\frac{\{x : (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{2\})\} \vdash \lambda^4 y \cdot y : (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\})}{\varnothing \vdash \lambda^3 x \cdot \lambda^4 y \cdot y : \varphi'} \tag{D}$$

and

$$\frac{\{x : (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\})\} \vdash \lambda^4 y \cdot y : (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\})}{\varnothing \vdash \lambda^3 x \cdot \lambda^4 y \cdot y : \varphi}. \tag{E}$$

Table 3. *Small-step operational semantics.*

$(\lambda^{\ell} x \cdot e)\ v$	$\rightarrow e[x \mapsto v]$
$(\mathsf{fun}^{\ell}\ f\ (x) = e)\ v$	$\rightarrow e[f \mapsto (\mathsf{fun}^{\ell}\ f\ (x) = e)][x \mapsto v]$
$(\mathsf{succ}\ n)$	$\rightarrow (n+1)$
$(\mathsf{pred}\ 0)$	$\rightarrow 0$
$(\mathsf{pred}\ (n+1))$	$\rightarrow n$
$(\mathsf{if}\ 0\ \mathsf{then}\ e\ \mathsf{else}\ e')$	$\rightarrow e$
$(\mathsf{if}\ (n+1)\ \mathsf{then}\ e\ \mathsf{else}\ e')$	$\rightarrow e'$

Hence from (**D**), (**E**) and (**C**), using rule **App**,

$$\varnothing \vdash T : (\mathtt{t}^{\mathsf{int}} \rightarrow \mathtt{t}^{\mathsf{int}}, \{4\}).$$

5. Operational semantics and correctness

Table 3 gives the small-step operational semantics of our language. In the operational semantics, the notation $e[x \mapsto v]$ denotes the capture-avoiding substitution of all free occurrences of the variable x by the value v in expression e. The operational semantics show reductions of simple redexes. They lift to arbitrary terms *via*

$$\frac{e \rightarrow e'}{E[e] \rightarrow E[e']}$$

where E denotes evaluation contexts (Wright and Felleisen 1991) specified by the BNF

$$E ::= [\,] \mid (E\ e) \mid (v\ E) \mid \mathsf{if}\ E\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 \mid \mathsf{succ}\ E \mid \mathsf{pred}\ E$$

Using the operational semantics, we can show type soundness. This requires us to prove a substitution lemma.

5.1. *Substitution lemma*

Lemma 5.1. Suppose that $\pi \oplus \{x : \bigwedge_{i \in I} \varphi_i\} \vdash e : \varphi$ and for all $i \in I$, $\pi \vdash v : \varphi'_i$ where $\varphi'_i \leqslant \varphi_i$. Then, there exists φ' such that $\pi \vdash e[x \mapsto v] : \varphi'$ and $\varphi' \leqslant \varphi$.

Proof. We use induction on the height of the derivation tree of e and by case analysis on the final step. The following are the interesting cases, the rest being routine. In fact, the case for recursive functions mirrors the case for lambda abstraction.

— $\pi \oplus \{x : \bigwedge_{i \in I} \varphi_i\} \vdash x' : \varphi$:
We have two cases:

- $x' = x$:
  Then $\pi \oplus \{x : \bigwedge_{i \in I} \varphi_i\} \vdash x : \varphi_j$, where $j \in I$. Assume that for all $i \in I$, $\pi \vdash v : \varphi'_i$, where $\varphi'_i \leqslant \varphi_i$. In particular, since $j \in I$, we obtain $\pi \vdash v : \varphi'_j$, where $\varphi'_j \leqslant \varphi_j$. That is, $\pi \vdash x[x \mapsto v] : \varphi'_j$ and $\varphi'_j \leqslant \varphi_j$.
- $x' \neq x$:
  Then $x' \in Dom(\pi)$ and $\pi \vdash x' : \varphi$. Thus, $\pi \vdash x'[x \mapsto v] : \varphi$ and $\varphi \leqslant \varphi$.

— $\pi \oplus \{x : \bigwedge_{i\in I} \varphi_i\} \vdash \lambda^{\ell} x' \cdot e : ((\bigwedge_{j\in J} \varphi'_j) \to \varphi', L)$:
Assume that $x' \neq x$. (If $x' = x$, rename the bound variable x' to x''.) For all $i \in I$, let $\pi \vdash v : \varphi'_i$ such that $\varphi'_i \leqslant \varphi_i$. We must show that there exists θ such that $\pi \vdash (\lambda^{\ell} x' \cdot e)[x \mapsto v] : \theta$ and $\theta \leqslant ((\bigwedge_{j\in J} \varphi'_j) \to \varphi', L)$. From the derivation tree of $\lambda^{\ell} x' \cdot e$, it must be the case that

$$\pi \oplus \left\{ x : \bigwedge_{i\in I} \varphi_i \right\} \oplus \left\{ x' : \bigwedge_{j\in J} \varphi'_j \right\} \vdash e : \varphi' \text{ and } \ell \in L. \tag{i}$$

By the induction hypothesis on the derivation tree for e, there exists θ' such that

$$\pi \oplus \left\{ x' : \bigwedge_{j\in J} \varphi'_j \right\} \vdash e[x \mapsto v] : \theta' \tag{ii}$$

and

$$\theta' \leqslant \varphi'. \tag{iii}$$

Hence, from (**ii**), using the fact that $\ell \in L$, $\pi \vdash \lambda^{\ell} x' \cdot e[x \mapsto v] : ((\bigwedge_j \varphi'_j) \to \theta', L)$, that is, $\pi \vdash (\lambda^{\ell} x' \cdot e)[x \mapsto v] : ((\bigwedge_j \varphi'_j) \to \theta', L)$. Now choose $\theta = ((\bigwedge_j \varphi'_j) \to \theta', L)$. Clearly, using (**iii**), we have $\theta \leqslant ((\bigwedge_j \varphi'_j) \to \varphi', L)$.

— $\pi \oplus \{x : \bigwedge_{i\in I} \varphi_i\} \vdash e_1 e_2 : \varphi'$:
Assume for all $i \in I$, $\pi \vdash v : \varphi'_i$ where $\varphi'_i \leqslant \varphi_i$. We must show there exists θ' such that $\pi \vdash (e_1 e_2)[x \mapsto v] : \theta'$ and $\theta' \leqslant \varphi'$. From the derivation tree of $e_1 e_2$, it must be the case that:

$$\pi \oplus \left\{ x : \bigwedge_{i\in I} \varphi_i \right\} \vdash e_1 : \left(\left(\bigwedge_{j\in J} \varphi'_j \right) \to \varphi', \kappa \right) \tag{i}$$

$$\pi \oplus \left\{ x : \bigwedge_{i\in I} \varphi_i \right\} \vdash e_2 : \varphi''_j, \text{ for each } j \in J \tag{ii}$$

$$\varphi''_j \leqslant \varphi'_j, \text{ for each } j \in J. \tag{iii}$$

By the induction hypothesis on derivation tree of e_1, there exists θ with shape $((\bigwedge_{k\in K} \theta'_k) \to \theta', \mu)$, such that

$$\pi \vdash e_1[x \mapsto v] : \left(\left(\bigwedge_{k\in K} \theta'_k \right) \to \theta', \mu \right) \tag{iv}$$

with

$$\left(\left(\bigwedge_{k\in K} \theta'_k \right) \to \theta', \mu \right) \leqslant \left(\left(\bigwedge_{j\in J} \varphi'_j \right) \to \varphi', \kappa \right). \tag{v}$$

From (**v**), by contravariance, $(\bigwedge_{j\in J} \varphi'_j) \leqslant (\bigwedge_{k\in K} \theta'_k)$. Hence, by the ordering on properties, for all $k \in K$, there exists $j_k \in J$, such that

$$\varphi'_{j_k} \leqslant \theta'_k. \tag{vi}$$

From (**v**), by covariance,

$$\theta' \leqslant \varphi'. \tag{vii}$$

By the induction hypothesis on derivation tree of e_2, for all $j \in J$,

$$\pi \vdash e_2[x \mapsto v] : \theta''_j, \tag{viii}$$

such that

$$\theta''_j \leqslant \varphi''_j. \tag{ix}$$

To show the result, we need to demonstrate using (**iv**) and (**viii**) that for all $k \in K$, $\theta''_{j_k} \leqslant \theta'_k$. Accordingly, consider any pair (k, j_k) as in (**vi**) where $k \in K$. Then, using (**ix**), (**iii**) and (**vi**), we have $\theta''_{j_k} \leqslant \varphi''_{j_k} \leqslant \varphi'_{j_k} \leqslant \theta'_k$. Hence by the ordering on properties,

$$\theta''_{j_k} \leqslant \theta'_k \tag{x}$$

for all $k \in K$. Now using (**iv**), (**viii**) and (**x**), and using the idempotence of $\wedge$, we have $\pi \vdash e_1[x \mapsto v]e_2[x \mapsto v] : \theta'$, that is, $\pi \vdash (e_1 e_2)[x \mapsto v] : \theta'$. Now the lemma holds by appealing to (**vii**). □

5.2. *Type soundness*

To prove type soundness, we proceed in two steps: first we prove a type soundness result for simple redexes defined by the operational semantics in Table 3; then we lift this result to arbitrary terms.

Lemma 5.2. Let $\pi \vdash e_1 : \varphi$ and $e_1 \to e_2$, where e_1 and e_2 are the left- and right-hand sides, respectively, of the operational semantics in Table 3. Then there exists φ' such that $\pi \vdash e_2 : \varphi'$ and $\varphi' \leqslant \varphi$.

Proof. We analyse cases on the reduction $e_1 \to e_2$ in Table 3. The interesting cases are the ones for application – the other cases being routine.

— $(\lambda^\ell x \cdot e)v \to e[x \mapsto v]$g:

For this case the derivation is $\pi \vdash (\lambda^\ell x \cdot e)v : \varphi$. Hence:

$$\pi \vdash \lambda^\ell x \cdot e : \left(\left(\bigwedge_{i \in I} \varphi_i \right) \to \varphi, L \right) \tag{i}$$

$$\pi \vdash v : \varphi'_i, \text{ for each } i \in I \tag{ii}$$

$$\varphi'_i \leqslant \varphi_i, \text{ for each } i \in I. \tag{iii}$$

From (**i**), it must be the case that

$$\pi \oplus \left\{ x : \bigwedge_{i \in I} \varphi_i \right\} \vdash e : \varphi. \tag{iv}$$

Hence from (**iv**), (**ii**) and (**iii**), using Lemma 5.1, there exists φ' such that $\pi \vdash e[x \mapsto v] : \varphi'$ and $\varphi' \leqslant \varphi$.

— $(\mathsf{fun}^{\ell}\, f\,(x) = e)v \to e[f \mapsto (\mathsf{fun}^{\ell}\, f\,(x) = e)][x \mapsto v]$:
For this case the derivation is $\pi \vdash (\mathsf{fun}^{\ell}\, f\,(x) = e)v : \varphi$. Hence

$$\pi \vdash \mathsf{fun}^{\ell}\, f\,(x) = e : \left(\left(\bigwedge_{j\in J} \theta_j\right) \to \varphi, L\right) \tag{i}$$

$$\pi \vdash v : \theta'_j, \text{ for each } j \in J \tag{ii}$$

$$\theta'_j \leqslant \theta_j, \text{ for each } j \in J \tag{iii}$$

From (**i**), it must be the case that

$$\pi \oplus \left\{ f : \bigwedge_{i\in I}(\varphi_i \to \varphi'_i, L_i), x : \left(\bigwedge_{j\in J} \theta_j\right)\right\} \vdash e : \varphi \tag{iv}$$

and

$$\left(\left(\bigwedge_{j\in J} \theta_j\right) \to \varphi, L\right) \leqslant (\varphi_i \to \varphi'_i, L_i), \text{ for each } i \in I \tag{v}$$

Hence from (**iv**), (**i**) and (**v**), applying Lemma 5.1, there exists φ' such that

$$\pi \oplus \left\{ x : \left(\bigwedge_{j\in J} \theta_j\right)\right\} \vdash e[f \mapsto \mathsf{fun}^{\ell}\, f\,(x) = e] : \varphi' \tag{vi}$$

and

$$\varphi' \leqslant \varphi. \tag{vii}$$

Now from (**vi**), (**ii**) and (**iii**), applying Lemma 5.1 again, there exists φ'' such that

$$\pi \vdash e[f \mapsto \mathsf{fun}^{\ell}\, f\,(x) = e][x \mapsto v] : \varphi'' \tag{viii}$$

and

$$\varphi'' \leqslant \varphi'. \tag{ix}$$

Hence from (**ix**) and (**vii**), we get $\varphi'' \leqslant \varphi$. □

Theorem 5.3 (Type Soundness Theorem). Let $\pi \vdash e : \varphi$ and $e \to e'$. Then there exists φ' such that $\pi \vdash e' : \varphi'$ and $\varphi' \leqslant \varphi$.

Proof. By a simple induction on the structure of evaluation contexts, $e = E[e_1]$, where $e_1 \to e_2$ *via* one of the rules in Table 3, and $e' = E[e_2]$. Now an induction on the structure of evaluation contexts using Lemma 5.2 completes the proof. □

6. An inference algorithm based on ranked properties

In this section we present an inference algorithm for the property system in Table 2. For an expression e^{σ}, algorithm $\mathscr{I}$ computes a triple $\langle \pi, \varphi, C\rangle$, where π is the inferred rank 1 property environment for the free variables of e^{σ}, φ is the inferred rank 2 property, and C is a set of constraints where each constraint in C has the form, $\xi \subseteq \xi'$ or $L \subseteq \xi$ for some label variables ξ, ξ' and label set L. The algorithm $\mathscr{I}$ is specified in Table 4 in a

Table 4. *The inference algorithm, $\mathscr{I}$.*

Variables ξ, ξ_i used in the inference algorithm are required to be fresh.

$$\mathscr{I}(x^\sigma) = \textbf{let } \varphi = \sigma^* \textbf{ in } \langle \{x^\sigma : \varphi\}, \varphi, \varnothing \rangle$$

$$\mathscr{I}(n^{\mathsf{int}}) = \langle \varnothing, \mathtt{t}^{\mathsf{int}}, \varnothing \rangle$$

$$\mathscr{I}(\lambda^\ell x^\sigma \cdot e^\tau) = \textbf{let } \langle \pi, \varphi, C \rangle = \mathscr{I}(e^\tau) \textbf{ in } \begin{array}{ll} \langle \pi', \left(\left(\bigwedge_{i \in I} \varphi_i \right) \to \varphi, \xi \right), C \cup \{\{\ell\} \subseteq \xi\} \rangle & \textbf{if } \pi = \pi' \oplus \{x^\sigma : \bigwedge_{i \in I} \varphi_i\} \\ \langle \pi, (\psi \to \varphi, \xi), C \cup \{\{\ell\} \subseteq \xi\} \rangle & \textbf{if } \psi = \sigma^* \textbf{ and } x^\sigma \notin \mathit{Dom}(\pi) \end{array}$$

$$\begin{array}{l} \mathscr{I}\left(e_1^{\sigma \to \tau} e_2^\sigma\right) = \textbf{let } \langle \pi_1, \varphi_1, C_1 \rangle = \mathscr{I}\left(e_1^{\sigma \to \tau}\right) \\ \qquad \langle \pi_2, \varphi_2, C_2 \rangle = \mathscr{I}\left(e_2^\sigma\right) \\ \qquad \textbf{in case } \varphi_1 \textbf{ of} \\ \qquad \left(\left(\bigwedge_{i \in I} \varphi_{1i} \right) \to \varphi_{12}, \xi \right) : \\ \qquad\qquad \textbf{let } \langle \widetilde{\pi}_i, \widetilde{\varphi}_i, \widetilde{C}_i \rangle = \mathit{Rename}(\pi_2, \varphi_2, C_2) \\ \qquad\qquad\quad \{\widetilde{\varphi}_i \leqslant \varphi_{1i} \mid i \in I\} \overset{+}{\rightsquigarrow} C' \\ \qquad\qquad\quad C = C_1 \cup (\bigcup_{i \in I} \widetilde{C}_i) \cup C' \\ \qquad\qquad \textbf{in } \left\langle \pi_1 + \sum_{i \in I} \widetilde{\pi}_i, \varphi_{12}, C \right\rangle \end{array}$$

$$\begin{array}{l} \mathscr{I}(\textsf{if } e_1^{\mathsf{int}} \textsf{ then } e_2^\sigma \textsf{ else } e_3^\sigma) = \textbf{let} \\ \qquad\qquad \langle \pi_1, \mathtt{t}^{\mathsf{int}}, C_1 \rangle = \mathscr{I}\left(e_1^{\mathsf{int}}\right) \\ \qquad\qquad \langle \pi_2, \varphi_2, C_2 \rangle = \mathscr{I}\left(e_2^\sigma\right) \\ \qquad\qquad \langle \pi_3, \varphi_3, C_3 \rangle = \mathscr{I}\left(e_3^\sigma\right) \\ \qquad\qquad \varphi = \sigma^* \\ \qquad\qquad \{\varphi_2 \leqslant \varphi, \varphi_3 \leqslant \varphi\} \overset{+}{\rightsquigarrow} C_4 \\ \qquad\qquad C = C_1 \cup C_2 \cup C_3 \cup C_4 \\ \qquad \textbf{in } \langle \pi_1 + \pi_2 + \pi_3, \varphi, C \rangle \end{array}$$

$$\mathscr{I}(\textsf{fun}^\ell f^{\sigma \to \tau}(x^\sigma) = e^\tau) = \begin{cases} \textbf{if } x \notin FV(e) \textbf{ then} \\ \textbf{let} \\ \langle \pi \oplus \{f : \bigwedge_{i \in I} (\varphi_i \to \varphi_i', \xi_i)\}, \delta, C \rangle = \mathscr{I}(e^\tau) \\ \{(\sigma^* \to \delta, \xi) \leqslant \bigwedge_{i \in I} (\varphi_i \to \varphi_i', \xi_i)\} \overset{+}{\rightsquigarrow} C_1 \\ \textbf{in } \langle \pi, (\sigma^* \to \delta, \xi), C \cup C_1 \cup \{\{\ell\} \subseteq \xi\} \rangle \\ \textbf{else let} \\ \langle \pi \oplus \{f : \bigwedge_{i \in I} (\varphi_i \to \varphi_i', \xi_i), x : (\bigwedge_{j \in J} \delta_j)\}, \delta, C \rangle = \mathscr{I}(e^\tau) \\ \{((\bigwedge_{j \in J} \delta_j) \to \delta, \xi) \leqslant \bigwedge_{i \in I} (\varphi_i \to \varphi_i', \xi_i)\} \overset{+}{\rightsquigarrow} C_1 \\ \textbf{in } \langle \pi, ((\bigwedge_{j \in J} \delta_j) \to \delta, \xi), C \cup C_1 \cup \{\{\ell\} \subseteq \xi\} \rangle \end{cases}$$

$$\mathscr{I}(\textsf{op } e^{\mathsf{int}}) = \mathscr{I}(e^{\mathsf{int}})$$

bottom-up manner, reminiscent of Damas's Algorithm T (Damas 1985). We explain the cases for variables, lambda abstractions and applications below.

For a variable x^σ, the algorithm returns a property $\varphi = \sigma^*$, since the flow must have the same shape as the type σ. For example, if σ is the type $\mathsf{int} \to \mathsf{int}$, we know that x can only be bound to functions of type $\mathsf{int} \to \mathsf{int}$. Therefore, x's property must have the shape $(\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi)$ where fresh ξ is the placeholder for the set of possible functions that can be bound to x.

For a lambda abstraction $\lambda^\ell x^\sigma \cdot e^\tau$, the algorithm first analyses the body e. Suppose the inferred property for e is φ. Let $FV(e)$ denote the set of free variables in e. If $x \in FV(e)$, the

property φ_i of each occurrence is collected together in the inferred property environment π, so that $\pi(x) = \bigwedge_{i\in I} \varphi_i$. Moreover, each $\varphi_i = \sigma^*$. The property inferred for the entire lambda abstraction is $((\bigwedge_{i\in I} \varphi_i) \to \varphi, \xi)$ where ξ is fresh and $\{\ell\} \subseteq \xi$. If $x \notin FV(e)$, then $x \notin Dom(\pi)$. Then the inferred property for the entire lambda abstraction is $(\psi \to \varphi, \xi)$, where ξ is fresh and $\psi = \sigma^*$ and $\{\ell\} \subseteq \xi$.

For the application $e_1^{\sigma\to\tau} e_2^{\sigma}$, the algorithm first analyses e_1. Suppose the inferred environment is π_1. The inferred property for e_1 must have the shape $((\bigwedge_{i\in I} \varphi_{1i}) \to \varphi_{12}, \xi)$. Next e_2 is analysed. Suppose the inferred environment is π_2 and the inferred property is φ_2. From the inference rule for application in Table 2, we need to make i copies of φ_2 and, for every $i \in I$, 'satisfy the ordering' $\widetilde{\varphi}_i \leqslant \varphi_{1i}$, where $\widetilde{\varphi}_i$ is the i-th copy of φ_2. Once the ordering is satisfied, the algorithm returns the environment $\pi_1 + \sum_{i\in I} \pi_i$ and the property φ_{12} for the entire application.

Consider properties φ, φ' in which all labels (if any) are label variables; then we say that substitution S *satisfies* $\varphi \leqslant \varphi'$ provided applying the substitution to φ, φ' maintains the ordering; that is, $S(\varphi) \leqslant S(\varphi')$. (This is lifted to a set of orderings in the obvious manner.) How can we satisfy $\widetilde{\varphi}_i \leqslant \varphi_{1i}$, for every $i \in I$? By inspection of the inference algorithm, first note that if $\mathscr{I}(e^{\sigma\to\tau}) = \langle \pi, \varphi, C\rangle$, then $\varphi \in Prop_2(\sigma \to \tau)$ and all labels in φ are label variables. Note too the shapes of orderings on properties: these can only be

$$\begin{aligned} \mathtt{t}^{\mathsf{int}} &\leqslant \mathtt{t}^{\mathsf{int}} \\ \varphi &\leqslant \bigwedge_{i\in I} \varphi_i \\ (\varphi_1 \to \varphi_2, \xi_1) &\leqslant (\varphi_3 \to \varphi_4, \xi_2). \end{aligned}$$

Now the specification of $\leqslant$ in Section 4 gives an algorithm for satisfying the set $\{\widetilde{\varphi}_i \leqslant \varphi_{1i} \mid i \in I\}$: we just 'run the rules backwards'. We formalise this using the $\rightsquigarrow$ relation below; the main idea is to decompose the set K of ordering on properties, into a set C of constraints between label variables, that is, $\langle K, C\rangle \overset{+}{\rightsquigarrow} \langle K', C'\rangle$.

$$\begin{aligned} \langle \{\mathtt{t}^{\mathsf{int}} \leqslant \mathtt{t}^{\mathsf{int}}\} \cup K, C\rangle &\rightsquigarrow \langle K, C\rangle \\ \langle \{\varphi \leqslant (\textstyle\bigwedge_{i\in I} \varphi_i)\} \cup K, C\rangle &\rightsquigarrow \langle \{\varphi \leqslant \varphi_i \mid i \in I\} \cup K, C\rangle \\ \langle \{(\varphi_1 \to \varphi_2, \xi_1) \leqslant (\varphi_3 \to \varphi_4, \xi_2)\} \cup K, C\rangle &\rightsquigarrow \langle \{\varphi_3 \leqslant \varphi_1, \varphi_2 \leqslant \varphi_4\} \cup K, C \cup \{\xi_1 \subseteq \xi_2\}\rangle \end{aligned}$$

Note that the $\rightsquigarrow$ relation as defined above is indeed an *algorithm*, since at every rewrite step either the number of arrows, or the number of intersections, or the size of the constraint set on the left-hand side decreases. More formally, we can prove the termination of rewriting by a lexicographic induction on (a, i, s), where a is the number of arrows in K, i is the number of intersections in K, and s is the size of K. Upon termination, we obtain a set of constraints, where each constraint has the form $\xi \subseteq \xi'$.

We say that a substitution S is a *solution* of a constraint $\kappa \subseteq \kappa'$ if $S(\kappa) \subseteq S(\kappa')$ holds. (This is lifted to a set of constraints in the obvious manner.)

Lemma 6.1. Let $\langle K, C\rangle \rightsquigarrow \langle K', C'\rangle$. For any substitution S, S satisfies K and S is a solution to C iff S satisfies K' and S is a solution to C'.

Proof. We analyse cases in the reduction $\langle K, C\rangle \rightsquigarrow \langle K', C'\rangle$.

— $\langle \{\mathtt{t}^{\mathsf{int}} \leqslant \mathtt{t}^{\mathsf{int}}\} \cup K, C\rangle \rightsquigarrow \langle K, C\rangle$:
Let S satisfy $\{\mathtt{t}^{\mathsf{int}} \leqslant \mathtt{t}^{\mathsf{int}}\} \cup K$ and let S be a solution to C. Then S satisfies K.
Conversely, let S satisfy K and let S be a solution to C. Then S satisfies $\{\mathtt{t}^{\mathsf{int}} \leqslant \mathtt{t}^{\mathsf{int}}\} \cup K$.

— $\langle \{\varphi \leqslant (\bigwedge_{i\in I} \varphi_i)\} \cup K, C\rangle \rightsquigarrow \langle \{\varphi \leqslant \varphi_i \mid i \in I\} \cup K, C\rangle$:
Let S satisfy $\{\varphi \leqslant (\bigwedge_{i\in I} \varphi_i)\} \cup K$ and let S also be a solution to C. Then $S(\varphi) \leqslant S(\bigwedge_{i\in I} \varphi_i)$ holds. Hence, by the ordering on properties, we have $S(\varphi) \leqslant S(\varphi_i)$, for every $i \in I$. Hence S satisfies $\{\varphi \leqslant (\bigwedge_{i\in I} \varphi_i)\} \cup K$.
Conversely, let S satisfy $\{\varphi \leqslant \varphi_i \mid i \in I\} \cup K$ and let S also be a solution to C. That is, S satisfies K, and $S(\varphi) \leqslant S(\varphi_i)$ for every $i \in I$. But then by the ordering on properties, $S(\varphi) \leqslant (\bigwedge_{i\in I} S(\varphi_i))$, that is, $S(\varphi) \leqslant S(\bigwedge_{i\in I}(\varphi_i))$. Hence S satisfies $\{\varphi \leqslant (\bigwedge_{i\in I}(\varphi_i))\} \cup K$.

— $\langle \{(\varphi_1 \to \varphi_2, \xi_1) \leqslant (\varphi_3 \to \varphi_4, \xi_2)\} \cup K, C\rangle \rightsquigarrow \langle \{\varphi_3 \leqslant \varphi_1, \varphi_2 \leqslant \varphi_4\} \cup K, C \cup \{\xi_1 \subseteq \xi_2\}\rangle$:
Let S satisfy $\{(\varphi_1 \to \varphi_2, \xi_1) \leqslant (\varphi_3 \to \varphi_4, \xi_2)\} \cup K$ and let S also be a solution to C. Then $S(\varphi_1 \to \varphi_2, \xi_1) \leqslant S(\varphi_3 \to \varphi_4, \xi_2)$. Hence, by the ordering on properties, we have $S(\varphi_3) \leqslant S(\varphi_1)$, $S(\varphi_2) \leqslant S(\varphi_4)$ and $S(\xi_1) \subseteq S(\xi_2)$. Hence S satisfies $\{\varphi_3 \leqslant \varphi_1, \varphi_2 \leqslant \varphi_4\} \cup K$ and S is a solution to $C \cup \{\xi_1 \subseteq \xi_2\}$.
Conversely, let S satisfy $\{\varphi_3 \leqslant \varphi_1, \varphi_2 \leqslant \varphi_4\} \cup K$ and let S also be a solution to $C \cup \{\xi_1 \subseteq \xi_2\}$. That is, S satisfies K and $S(\varphi_3) \leqslant S(\varphi_1)$ and $S(\varphi_2) \leqslant S(\varphi_4)$. Moreover, $S(\xi_1) \subseteq S(\xi_2)$. Hence by the ordering on properties, $S(\varphi_1 \to \varphi_2, \xi_1) \leqslant S(\varphi_3 \to \varphi_4, \xi_2)$, that is, S satisfies $\{(\varphi_1 \to \varphi_2, \xi_1) \leqslant (\varphi_3 \to \varphi_4, \xi_2)\} \cup K$ and S is a solution to C. □

A consequence of Lemma 6.1 is that it holds when $\rightsquigarrow$ is replaced by $\overset{+}{\rightsquigarrow}$, where $\overset{+}{\rightsquigarrow}$ denotes repeated rewriting using $\rightsquigarrow$. More specifically, an initial set K of orderings on properties can be rewritten to a set of constraints C on label variables; substitution S satisfies K iff S is a solution to C.

Lemma 6.2. Let $\langle K, \varnothing\rangle \overset{+}{\rightsquigarrow} \langle \varnothing, C\rangle$. Then S satisfies K iff S is a solution to C.

Proof. The proof follows directly from Lemma 6.1, noting that any S that satisfies K is a solution to the empty set of constraints and satisfies the empty set of orderings between properties. □

In the following we will abbreviate $\langle K, \varnothing\rangle \overset{+}{\rightsquigarrow} \langle \varnothing, C\rangle$ as $K \overset{+}{\rightsquigarrow} C$. Note that by inspection of algorithm $\mathscr{I}$, for any expression e, if $\mathscr{I}(e) = \langle \pi, \varphi, C\rangle$, then all constraints in C have the form $\kappa \subseteq \xi$. Such a set of constraints always admits a solution computed by the usual transitive closure algorithm.

6.1. *Example*

Consider our example from Section 2:

$$T = (\lambda^1 g^{(\mathsf{int}\to\mathsf{int})\to(\mathsf{int}\to\mathsf{int})} \cdot g(g(\lambda^2 v^{\mathsf{int}} \cdot v)))(\lambda^3 x^{(\mathsf{int}\to\mathsf{int})} \cdot \lambda^4 y^{\mathsf{int}} \cdot y).$$

We show the result of the inference algorithm of Table 4 applied to T. First, consider the argument part, $\lambda^3 x^{(\mathsf{int}\to\mathsf{int})} \cdot \lambda^4 y^{\mathsf{int}} \cdot y$. We have

$$\begin{array}{ll}
\mathscr{I}(y) & = \langle \{y : \mathtt{t}^{\mathsf{int}}\}, \mathtt{t}^{\mathsf{int}}, \varnothing \rangle \\
\mathscr{I}(\lambda^4 y \cdot y) & = \langle \varnothing, (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_1), \{\{4\} \subseteq \xi_1\} \rangle \\
\mathscr{I}(\lambda^3 x \cdot \lambda^4 y \cdot y) & = \langle \varnothing, ((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_2) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_1), \xi_3), \{\{3\} \subseteq \xi_3, \{4\} \subseteq \xi_1\} \rangle \\
 & \quad \text{where } (\mathsf{int} \to \mathsf{int})^* = (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_2).
\end{array}$$

Next, consider the function part, $\lambda^1 g^{(\mathsf{int}\to\mathsf{int})\to(\mathsf{int}\to\mathsf{int})} \cdot g\ (g\ (\lambda^2 v^{\mathsf{int}} \cdot v))$. We have

$$\begin{array}{ll}
\mathscr{I}(v) & = \langle \{v : \mathtt{t}^{\mathsf{int}}\}, \mathtt{t}^{\mathsf{int}}, \varnothing \rangle \\
\mathscr{I}(\lambda^2 v \cdot v) & = \langle \varnothing, (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_4), \{\{2\} \subseteq \xi_4\} \rangle \\
\mathscr{I}(g) & = \langle \{g : \varphi'\}, \varphi', \varnothing \rangle \text{where} \\
 & \quad \varphi' = ((\mathsf{int} \to \mathsf{int}) \to (\mathsf{int} \to \mathsf{int}))^* \\
 & \quad\quad = ((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_5) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_6), \xi_7) \\
\mathscr{I}(g\ (\lambda^2 v \cdot v)) & = \langle g : \varphi', (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_6), \{\{2\} \subseteq \xi_4, \xi_4 \subseteq \xi_5\} \rangle \\
 & \quad \text{since } \{(\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_4) \leqslant (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_5)\} \rightsquigarrow \{\xi_4 \subseteq \xi_5\} \\
\mathscr{I}(g) & = \langle \{g : \varphi\}, \varphi, \varnothing \rangle \text{where} \\
 & \quad \varphi = ((\mathsf{int} \to \mathsf{int}) \to (\mathsf{int} \to \mathsf{int}))^* \\
 & \quad\quad = ((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_8) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_9), \xi_{10}) \\
\mathscr{I}(g\ (g\ (\lambda^2 v \cdot v))) & = \langle g : (\varphi \wedge \varphi'), (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_9), \{\{2\} \subseteq \xi_4,\ \xi_4 \subseteq \xi_5,\ \xi_6 \subseteq \xi_8\} \rangle \\
 & \quad \text{since } \{(\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_6) \leqslant (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_8)\} \rightsquigarrow \{\xi_6 \subseteq \xi_8\}.
\end{array}$$

Hence

$$\mathscr{I}(\lambda^1 g \cdot g\ (g\ (\lambda^2 v \cdot v))) = \langle \varnothing, ((\varphi \wedge \varphi') \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_9), \xi_{11}), C_1 \rangle$$

where $C_1 = \{\{2\} \subseteq \xi_4,\ \xi_4 \subseteq \xi_5,\ \xi_6 \subseteq \xi_8,\ \{1\} \subseteq \xi_{11}\}$.

Now to obtain the result for the entire expression T, we first rename the flow variables in the flow property for the argument twice (once for φ and once for φ') and obtain

$$\{((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_2') \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_1'), \xi_3') \leqslant ((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_8) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_9), \xi_{10})\} \rightsquigarrow C_2$$

and

$$\{((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_2'') \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_1''), \xi_3'') \leqslant ((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_5) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_6), \xi_7)\} \rightsquigarrow C_3$$

where

$$C_2 = \{\xi_8 \subseteq \xi_2',\ \xi_1' \subseteq \xi_9,\ \xi_3' \subseteq \xi_{10}\} \text{ and } C_3 = \{\xi_5 \subseteq \xi_2'',\ \xi_1'' \subseteq \xi_6,\ \xi_3' \subseteq \xi_7\}.$$

Finally,

$$\mathscr{I}(T) = \langle \varnothing, (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi_9), C \rangle$$

where $C = \{\{3\} \subseteq \xi_3', \{4\} \subseteq \xi_1', \{3\} \subseteq \xi_3'', \{4\} \subseteq \xi_1''\} \cup C_1 \cup C_2 \cup C_3$. The minimal solution for C, obtained by the transitive closure algorithm, is given by

$$[(\xi_{10}, \xi_3') \mapsto \{3\},\ (\xi_2'', \xi_5, \xi_4) \mapsto \{2\},\ (\xi_1', \xi_9) \mapsto \{4\},\ (\xi_2', \xi_8, \xi_6, \xi_1'') \mapsto \{4\},\ (\xi_7, \xi_3'') \mapsto \{3\}],$$

where $[(\xi, \xi') \mapsto L]$ abbreviates $[\xi \mapsto L,\ \xi' \mapsto L]$.

We can therefore conclude that the entire expression evaluates to λ^4 as we expect. Moreover, note that the type of g in the body of λ^1 is $\varphi \wedge \varphi'$, where

$$\varphi = ((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\}) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\}), \{3\})$$

and

$$\varphi' = ((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{2\}) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\}), \{3\}).$$

Thus λ^1 is applied to λ^3 and λ^3 exhibits the following behaviours: at one application site it obtains λ^2 as argument, yielding λ^4 as result; at another application site it obtains λ^4 as argument, yielding λ^4 as result. This conforms to our expectations in Section 2.

6.2. *Soundness of the inference algorithm*

Theorem 6.3 (Soundness). Let $\mathscr{I}(e^\sigma) = \langle \pi, \varphi, C \rangle$. If S is a solution to C, then $S(\pi) \vdash e : S(\varphi)$ is derivable in the property system.

Proof. We use induction on the structure of e^σ.

— x^σ:
Let $\varphi = \sigma^*$. Then we have $\mathscr{I}(x^\sigma) = \langle \{x : \varphi\}, \varphi, \emptyset \rangle$. Let S be any solution chosen for $\emptyset$. By rule **Var** in Table 2, $\{x : S(\varphi)\} \vdash x : S(\varphi)$.

— n^{int}:
We have $\mathscr{I}(n^{\mathsf{int}}) = \langle \emptyset, \mathtt{t}^{\mathsf{int}}, \emptyset \rangle$. Let S be any solution chosen for $\emptyset$. By rule **Int** in Table 2, and since $S(\mathtt{t}^{\mathsf{int}}) = \mathtt{t}^{\mathsf{int}}$ for any S, we have, $\emptyset \vdash n^{\mathsf{int}} : \mathtt{t}^{\mathsf{int}}$.

— $\lambda^\ell x^\sigma \cdot e^\tau$:
We have two cases:

– $x \in Dom(\pi)$:
Then

$$\mathscr{I}(\lambda^\ell x^\sigma \cdot e^\tau) = \left\langle \pi', \left(\left(\bigwedge_{i \in I} \varphi_i \right) \to \varphi, \xi \right), C \cup \{\{\ell\} \subseteq \xi\} \right\rangle,$$

where $\mathscr{I}(e^\tau) = \langle \pi, \varphi, C \rangle$, and $\pi = \pi' \oplus \{x : \bigwedge_{i \in I} \varphi_i\}$. Let S be a solution to $C \cup \{\{\ell\} \subseteq \xi\}$. Then S is a solution to C, and, $\ell \in S(\xi)$; hence, by the induction hypothesis on e^τ, we have, $S(\pi) \vdash e : S(\varphi)$. Thus $S(\pi') \oplus \{x : \bigwedge_{i \in I} S(\varphi_i)\} \vdash e^\tau : S(\varphi)$. Therefore, by rule **Lam** in Table 2, $S(\pi') \vdash \lambda^\ell x^\sigma \cdot e^\tau : S((\bigwedge_{i \in I} \varphi_i) \to \varphi, \xi)$.

– $x \notin Dom(\pi)$:
Then

$$\mathscr{I}(\lambda^\ell x^\sigma \cdot e^\tau) = \langle \pi, (\psi \to \varphi, \xi), C \cup \{\{\ell\} \subseteq \xi\} \rangle,$$

where $\psi = \sigma^*$ and $\mathscr{I}(e^\tau) = \langle \pi, \varphi, C \rangle$. Let S be a solution to $C \cup \{\{\ell\} \subseteq \xi\}$. Then S is a solution to C, and $\ell \in S(\xi)$. Hence, by the induction hypothesis on e^τ, we have $S(\pi) \vdash e^\tau : S(\varphi)$. By weakening the property environment π, we have, by Proposition 4.8, $S(\pi) \oplus \{x : \psi\} \vdash e^\tau : S(\varphi)$. Therefore, by rule **Lam** in Table 2, $S(\pi) \vdash \lambda^\ell x^\sigma \cdot e^\tau : (\psi \to S(\varphi), S(\xi))$. Now, since $Dom(S)$ is disjoint from set of label variables occurring in ψ, we get, $S(\pi) \vdash \lambda^\ell x^\sigma \cdot e^\tau : S(\psi \to \varphi, \xi)$.

— $e_1^{\sigma\to\tau} e_2^{\sigma}$:
We have $\mathscr{I}(e_1^{\sigma\to\tau} e_2^{\sigma}) = \langle \pi + \sum_{i\in I} \widetilde{\pi}_i, \varphi_{12}, C\rangle$, where $C = C_1 \cup (\bigcup_{i\in I} \widetilde{C}_i) \cup C'$. Let S be a solution to C. Then S is a solution to C_1, to $\widetilde{C}_i$, for $i \in I$ and to C'. Since $\mathscr{I}(e_1^{\sigma\to\tau}) = \langle \pi_1, \varphi_1, C_1\rangle$, by the induction hypothesis on $e_1^{\sigma\to\tau}$, we have $S(\pi_1) \vdash e_1^{\sigma\to\tau} : ((\bigwedge_{i\in I} S(\varphi_{1i})) \to S(\varphi_{12}), S(\kappa))$. Furthermore, since $\mathscr{I}(e_2^{\sigma}) = \langle \pi_2, \varphi_2, C_2\rangle$, by the induction hypothesis on e_2^{σ}, we have $S(\pi_2) \vdash e_2^{\sigma} : S(\varphi_2)$, and renaming for each $i \in I$ yields i disjoint triples $\langle \widetilde{\pi}_i, \widetilde{\varphi}_i, \widetilde{C}_i\rangle$ such that $S(\widetilde{\pi}_i) \vdash e_2^{\sigma} : S(\widetilde{\varphi}_i)$. Now, since $\{\widetilde{\varphi}_i \leqslant \varphi_{1i} \mid i \in I\} \overset{+}{\rightsquigarrow} C'$, and since S is a solution to C', by Lemma 6.2, we have $S(\widetilde{\varphi}_i) \leqslant S(\varphi_{1i})$ for $i \in I$. By weakening of the property environment $S(\pi_1)$, we obtain

$$S(\pi_1) + \sum_{i\in I} S(\widetilde{\pi}_i) \vdash e_1^{\sigma\to\tau} : \left(\left(\bigwedge_{i\in I} S(\varphi_{1i})\right)\right) \to S(\varphi_{12}), S(\kappa)).$$

Similarly, by weakening of the property environment $S(\widetilde{\pi}_i)$, for each $i \in I$, we obtain

$$S(\pi_1) + \sum_{i\in I} S(\widetilde{\pi}_i) \vdash e_2^{\sigma} : S(\widetilde{\varphi}_i).$$

Hence, by rule **App** in Table 2, we obtain

$$S\left(\pi_1 + \sum_{i\in I} \widetilde{\pi}_i\right) \vdash e_1^{\sigma\to\tau} e_2^{\sigma} : S(\varphi_{12}).$$

— $\mathsf{if}\ e_1^{\mathsf{int}}\ \mathsf{then}\ e_2^{\sigma}\ \mathsf{else}\ e_3^{\sigma}$:
We have

$$\mathscr{I}\left(\mathsf{if}\ e_1^{\mathsf{int}}\ \mathsf{then}\ e_2^{\sigma}\ \mathsf{else}\ e_3^{\sigma}\right) = \langle \pi_1 + \pi_2 + \pi_3, \varphi, C\rangle,$$

where $C = C_1 \cup C_2 \cup C_3 \cup C_4$. Let S be a solution to C. Then S is a solution to C_1, C_2, C_3 and C_4. Since $\mathscr{I}(e_1^{\mathsf{int}}) = \langle \pi_1, \mathtt{t}^{\mathsf{int}}, C_1\rangle$, by the induction hypothesis on e_1^{int}, we have $S(\pi_1) \vdash e_1^{\mathsf{int}} : \mathtt{t}^{\mathsf{int}}$. Since $\mathscr{I}(e_2^{\sigma}) = \langle \pi_2, \varphi_2, C_2\rangle$, by the induction hypothesis on e_2^{σ}, we have $S(\pi_2) \vdash e_2^{\sigma} : S(\varphi_2)$. Finally, since $\mathscr{I}(e_3^{\sigma}) = \langle \pi_3, \varphi_3, C_3\rangle$, by the induction hypothesis on e_3^{σ}, we have $S(\pi_3) \vdash e_3^{\sigma} : S(\varphi_3)$. Let $\sigma^* = \varphi$. Since S is a solution to C_4, and $\{\varphi_2 \leqslant \varphi, \varphi_3 \leqslant \varphi\} \overset{+}{\rightsquigarrow} C_4$, by Lemma 6.2, $S(\varphi_2) \leqslant S(\varphi)$ and $S(\varphi_3) \leqslant S(\varphi)$. Thus, by the weakening of property environments and rule **If** in Table 2,

$$S(\pi_1 + \pi_2 + \pi_3) \vdash \mathsf{if}\ e_1^{\mathsf{int}}\ \mathsf{then}\ e_2^{\sigma}\ \mathsf{else}\ e_3^{\sigma} : S(\varphi).$$

— $\mathsf{fun}^{\ell}\, f^{\sigma\to\tau}(x^{\sigma}) = e^{\tau}$:
We have two cases:

– $x \notin FV(e)$:
We have

$$\mathscr{I}(\mathsf{fun}^{\ell}\, f^{\sigma\to\tau}(x^{\sigma}) = e^{\tau}) = \langle \pi, (\sigma^* \to \delta, \xi), C \cup C_1 \cup \{\{\ell\} \subseteq \xi\}\rangle.$$

Let S be a solution to $C \cup C_1 \cup \{\{\ell\} \subseteq \xi\}$. Then S is a solution to C, C_1, and $\ell \in S(\xi)$. Let

$$\left\{(\sigma^* \to \delta, \xi) \leqslant \bigwedge_{i\in I} (\varphi_i \to \varphi_i', \xi_i)\right\} \overset{+}{\rightsquigarrow} C_1.$$

Since S is a solution to C_1, by Lemma 6.2,

$$S(\sigma^* \to \delta, \xi) \leqslant \bigwedge_{i \in I} S(\varphi_i \to \varphi_i', \xi_i).$$

Since

$$\mathscr{I}(e^\tau) = \left\langle \pi \oplus \left\{ f : \bigwedge_{i \in I} (\varphi_i \to \varphi_i', \xi_i) \right\}, \delta, C \right\rangle,$$

by the induction hypothesis on e^τ, we have

$$S(\pi) \oplus \left\{ f : \bigwedge_{i \in I} S(\varphi_i \to \varphi_i', \xi_i) \right\} \vdash e^\tau : S(\delta).$$

By weakening (Proposition 4.8), we obtain,

$$S(\pi) \oplus \left\{ f : \bigwedge_{i \in I} S(\varphi_i \to \varphi_i', \xi_i), x : S(\sigma^*) \right\} \vdash e^\tau : S(\delta).$$

Hence, by rule **Fun** in Table 2,

$$S(\pi) \vdash \mathsf{fun}^\ell \, f^{\sigma \to \tau} \, (x^\sigma) = e^\tau : S\left(\left(\bigwedge_{j \in J} \delta_j \right) \to \delta, \xi \right).$$

– $x \in FV(e)$:
We have

$$\mathscr{I}(\mathsf{fun}^\ell \, f^{\sigma \to \tau} \, (x^\sigma) = e^\tau) = \left\langle \pi, \left(\left(\bigwedge_{j \in J} \delta_j \right) \to \delta, \xi \right), C \cup C_1 \cup \{\{\ell\} \subseteq \xi\} \right\rangle.$$

Let S be a solution to $C \cup C_1 \cup \{\{\ell\} \subseteq \xi\}$. Then S is a solution to C, C_1 and $\ell \in S(\xi)$. Since

$$\mathscr{I}(e^\tau) = \left\langle \pi \oplus \left\{ f : \bigwedge_{i \in I} (\varphi_i \to \varphi_i', \xi_i), x : \bigwedge_{j \in J} \delta_j \right\}, \delta, C \right\rangle,$$

by the induction hypothesis on e^τ, we have

$$S(\pi) \oplus \left\{ f : \bigwedge_{i \in I} S(\varphi_i \to \varphi_i', \xi_i), x : \bigwedge_{j \in J} S(\delta_j) \right\} \vdash e^\tau : S(\delta).$$

Let

$$\left\{ \left(\left(\bigwedge_{j \in J} \delta_j \right) \to \delta, \xi \right) \leqslant \bigwedge_{i \in I} (\varphi_i \to \varphi_i', \xi_i) \right\} \overset{+}{\rightsquigarrow} C_1.$$

Since S is a solution to C_1, by Lemma 6.2, we have

$$S\left(\left(\bigwedge_{j \in J} \delta_j \right) \to \delta, \xi \right) \leqslant \bigwedge_{i \in I} S(\varphi_i \to \varphi_i', \xi_i).$$

Hence, by rule **Fun** in Table 2,

$$S(\pi) \vdash \mathsf{fun}^{\ell}\, f^{\sigma\to\tau}\,(x^{\sigma}) = e^{\tau} : S\left(\left(\bigwedge_{j\in J}\delta_j\right)\to\delta, \xi\right).$$

— $\mathsf{op}\ e^{\mathsf{int}}$:
We have $\mathscr{I}(\mathsf{op}\ e^{\mathsf{int}}) = \langle \pi, \mathtt{t}^{\mathsf{int}}, C\rangle$. Let S be a solution to C. Therefore, by the induction hypothesis on e^{int}, we have $S(\pi) \vdash e^{\mathsf{int}} : \mathtt{t}^{\mathsf{int}}$. Thus, using rule **Op** in Table 2, we have $S(\pi) \vdash \mathsf{op}\ e^{\mathsf{int}} : \mathtt{t}^{\mathsf{int}}$. □

Now we can revisit the type soundness theorem, Theorem 5.3. The main import of the theorem is in conjunction with the soundness theorem for $\mathscr{I}$: suppose $S(\pi) \vdash e : S(\varphi)$ as in Theorem 6.3. Let $e \to e'$ as in Theorem 5.3. Then there exists φ' such that $S(\pi) \vdash e' : \varphi'$ and $\varphi' \leqslant S(\varphi)$. In particular, if e is of function type, by the ordering on properties, the outermost set of labels associated with φ' will be contained in the outermost set of labels associated with $S(\varphi)$. That is, the evaluation of e yields a function that is predicted by the analysis. Hence the analysis is sound.

6.3. *Completeness of the inference algorithm*

The inference algorithm $\mathscr{I}$ defined in Table 4 is complete. This means that for any expression e, if $\mathscr{I}(e) = \langle \pi, \varphi, C\rangle$, then $\pi \vdash e : \varphi$ is a principal typing for e. Any other typing for e can be obtained as an instance of the above typing. This is formalised in the following completeness theorem.

Theorem 6.4 (Completeness). Let $\mathscr{I}(e) = \langle \pi, \varphi, C\rangle$. Suppose $\eta \vdash e^{\sigma} : \psi$ is derivable and that η is a rank 1 property environment, ψ is a rank 2 property and η, ψ are ground. Then there exists a substitution S, such that:

(i) S is a solution to C.
(ii) $S\langle \pi,\ \varphi\rangle \leqslant \langle \eta,\ \psi\rangle$, that is, $\eta \leqslant S(\pi)$ and $S(\varphi) \leqslant \psi$.

Proof. We use induction on the structure of e^{σ}.

— x^{σ}:
The derivation is: $\eta \oplus \{x : \bigwedge_{i\in I}\psi_i\} \vdash x^{\sigma} : \psi_j$, where $j \in I$. By the inference algorithm, $\mathscr{I}(x^{\sigma}) = \langle \{x : \varphi\}, \varphi, \varnothing\rangle$, where $\varphi = \sigma^{*}$. We need a substitution S such that S is a solution to $\varnothing$ (holds trivially for any S) and $S(\langle \{x : \varphi\},\ \varphi\rangle) \leqslant \langle \eta \oplus \{x : \bigwedge_{i\in I}\psi_i\},\ \psi_j\rangle$. That is:

$$\eta \oplus \left\{x : \bigwedge_{i\in I}\psi_i\right\} \leqslant S(\{x : \varphi\}) \qquad \textbf{(Ai)}$$

$$S(\varphi) \leqslant \psi_j. \qquad \textbf{(Aii)}$$

To prove (**Aii**), note that $\psi_j \in \mathit{Prop}_0(\sigma)$. Hence, by Proposition 4.2, there exists a substitution S' such that $S'(\sigma^{*}) = \psi_j$. But $\varphi = \sigma^{*}$. Therefore, choose S to be S' so that $S'(\varphi) = S'(\sigma^{*}) = \psi_j$. Thus $S'(\varphi) \leqslant \psi_j$.

To prove (**Ai**), we need only show that for all $x \in Dom(\{x : \varphi\})$, it is the case that $x \in Dom(\eta \oplus \{x : \bigwedge_{i\in I} \psi_i\})$, and $\bigwedge_{i\in I} \psi_i \leqslant S'(\varphi)$, that is, $\bigwedge_{i\in I} \psi_i \leqslant \psi_j$. But this holds by the ordering on properties (Section 4) since $j \in I$.

— n^{int}:

The derivation is $\eta \vdash n^{\mathsf{int}} : \mathtt{t}^{\mathsf{int}}$. By the inference algorithm, $\mathscr{I}(n^{\mathsf{int}}) = \langle \varnothing, \mathtt{t}^{\mathsf{int}}, \varnothing \rangle$. Case (i) of the theorem holds trivially for any substitution S. For case (ii), we need a substitution S such that $S(\mathtt{t}^{\mathsf{int}}) \leqslant \mathtt{t}^{\mathsf{int}}$. Choose S to be empty, that is, [ ].

— $\lambda^{\ell} x^{\sigma} \cdot e^{\tau}$:

The derivation is

$$\frac{\eta' \oplus \{x : \bigwedge_{j\in J} \psi_j\} \vdash e^{\tau} : \psi \quad \ell \in L}{\eta' \vdash \lambda^{\ell} x^{\sigma} \cdot e^{\tau} : ((\bigwedge_{j\in J} \psi_j) \to \psi, L)} \; \eta = \eta' \oplus \left\{ x : \bigwedge_{j\in J} \psi_j \right\}$$

By the inference algorithm, we have two cases.

– $\mathscr{I}(\lambda^{\ell} x^{\sigma} \cdot e^{\tau}) = \textbf{let } \langle \pi, \varphi, C \rangle = \mathscr{I}(e^{\tau}) \textbf{ in } \langle \pi', ((\bigwedge_{i\in I} \varphi_i) \to \varphi, \xi), C \cup \{\{\ell\} \subseteq \xi\} \rangle$
where $\pi = \pi' \oplus \{x^{\sigma} : \bigwedge_{i\in I} \varphi_i\}$.
By the induction hypothesis on e^{τ}, there exists a substitution, S, such that

$$S \text{ is a solution for } C \tag{Ai}$$
$$\eta \leqslant S(\pi) \tag{Aii}$$
$$S(\varphi) \leqslant \psi. \tag{Aiii}$$

From (**Aii**), we obtain, in particular,

$$\textstyle\bigwedge_{j\in J}(\psi_j) \leqslant \bigwedge_{i\in I} S(\varphi_i) \tag{Bi}$$
$$\eta' \leqslant S(\pi'). \tag{Bii}$$

To prove the theorem, we need a substitution S' such that

$$S' \text{ is a solution for } C \cup \{\{\ell\} \subseteq \xi\} \tag{Ci}$$
$$\eta' \leqslant S'(\pi') \tag{Cii}$$
$$S'((\textstyle\bigwedge_{i\in I} \varphi_i) \to \varphi, \xi) \leqslant ((\bigwedge_{j\in J} \psi_j) \to \psi, L). \tag{Ciii}$$

Since fresh ξ, and S is a solution for C, and $\ell \in L$, choose the solution for (**Ci**) as $S' = [\xi \mapsto \{\ell\}] \circ S$. Then (**Cii**) follows from (**Bii**), and (**Ciii**) follows from (**Bi**), (**Aiii**) and $\ell \in L$.

– $\mathscr{I}(\lambda^{\ell} x^{\sigma} \cdot e^{\tau}) = \textbf{let } \langle \pi, \varphi, C \rangle = \mathscr{I}(e^{\tau}) \textbf{ in } \langle \pi, (\varphi' \to \varphi, \xi), C \cup \{\{\ell\} \subseteq \xi\} \rangle$
where $\varphi' = \sigma^*$ *and* $x \notin Dom(\pi)$.
By the induction hypothesis on e^{τ}, there exists a substitution S such that:

$$S \text{ is a solution for } C \tag{Ai}$$
$$\eta \leqslant S(\pi) \tag{Aii}$$
$$S(\varphi) \leqslant \psi. \tag{Aiii}$$

To prove the theorem, we need a substitution, S', such that

$$S' \text{ is a solution for } (C \cup \{\{\ell\} \subseteq \xi\}) \tag{Ci}$$

$$\eta' \leqslant S'(\pi'), \tag{Cii}$$

$$S'(\varphi' \to \varphi, \xi) \leqslant ((\textstyle\bigwedge_{j\in J} \psi_j) \to \psi, L). \tag{Ciii}$$

From (**Ciii**), this means we need S' such that

$$\textstyle\bigwedge_{j\in J}(\psi_j) \leqslant S'(\varphi') \tag{Civ}$$

$$S'(\varphi) \leqslant \psi \tag{Cv}$$

$$S'(\xi) \subseteq L. \tag{Cvi}$$

To prove (**Civ**), note that each $\psi_j \in Prop_0(\sigma)$. Since $\varphi' = \sigma^*$, there exists $\widehat{j} \in J$ and substitution $\widehat{S}$ such that, by Proposition 4.2, $\widehat{S}(\sigma^*) = \psi_{\widehat{j}}$. Thus, $\widehat{S}(\varphi') = \psi_{\widehat{j}}$. Therefore, by the ordering on properties, $\bigwedge_{j\in J}(\psi_j) \leqslant \widehat{S}(\varphi')$. Since fresh ξ, and S is a solution to C, choose the solution to (**Ci**) as $S' = [\xi \mapsto \{\ell\}] \circ \widehat{S} \circ S$. Then it is easy to see that (**Cii**) follows from (**Aii**), (**Cv**) follows from (**Aiii**), and (**Cvi**) follows since $\ell \in L$.

— $e_1^{\sigma\to\tau} e_2^{\sigma}$:
The derivation is

$$\frac{\eta \vdash e_1^{\sigma\to\tau} : ((\textstyle\bigwedge_{i\in I} \psi_i) \to \psi, \kappa) \quad \forall i \in I \,:\, \eta \vdash e_2^{\sigma} : \psi_i' \quad \forall i \in I \,:\, \psi_i' \leqslant \psi_i}{\eta \vdash e_1^{\sigma\to\tau} e_2^{\sigma} : \psi}$$

By the inference algorithm, we have

$$\begin{aligned}
\mathscr{I}\left(e_1^{\sigma\to\tau} e_2^{\sigma}\right) \;=\; & \textbf{let } \langle \pi_1, \varphi_1, C_1\rangle = \mathscr{I}\left(e_1^{\sigma\to\tau}\right) \\
& \quad \langle \pi_2, \varphi_2, C_2\rangle = \mathscr{I}\left(e_2^{\sigma}\right) \\
& \textbf{in case } \varphi_1 \textbf{ of} \\
& \left(\left(\bigwedge_{j\in J} \varphi_{1j}\right) \to \varphi_{12}, \mu\right) : \\
& \quad \textbf{let } \langle \widetilde{\pi}_j, \widetilde{\varphi_j}, \widetilde{C_j}\rangle = \mathit{Rename}(\pi_2, \varphi_2, C_2) \\
& \quad \{\widetilde{\varphi_j} \leqslant \varphi_{1j} \mid j \in J\} \overset{+}{\rightsquigarrow} \widehat{C} \\
& \quad C' = C_1 \cup (\textstyle\bigcup_{j\in J} \widetilde{C_j}) \cup \widehat{C} \\
& \quad \textbf{in } \left\langle \pi_1 + \textstyle\sum_{j\in J}, \widetilde{\pi}_j, \varphi_{12}, C'\right\rangle
\end{aligned}$$

By the induction hypothesis on $e_1^{\sigma\to\tau}$, there exists substitution S_1 such that

$$S_1 \text{ is a solution for } C_1 \tag{Ai}$$

$$\eta \leqslant S_1(\pi_1) \tag{Aii}$$

$$S_1((\textstyle\bigwedge_{j\in J} \varphi_{1j}) \to \varphi_{12}, \mu) \leqslant ((\textstyle\bigwedge_{i\in I} \psi_i) \to \psi, \kappa). \tag{Aiii}$$

From (**Aiii**), we know that:

$$\textstyle\bigwedge_{i\in I}(\psi_i) \leqslant \bigwedge_{j\in J} S_1(\varphi_{1j}) \tag{Aiv}$$

$$S_1(\varphi_{12}) \leqslant \psi \tag{Av}$$

$$S_1(\mu) \subseteq \kappa. \tag{Avi}$$

From (**Aiv**), it must be the case that, for all $j \in J$, there exists $i_j \in I$, such that

$$\psi_{i_j} \leqslant S_1(\varphi_{1j}). \tag{**Avii**}$$

By the induction hypothesis on e_2^σ, for all $j \in J$, there exists substitution $\widetilde{S}_j$, and there exists $i \in I$ such that

$$S_j \text{ is a solution for } \widetilde{C_j} \tag{**Bi**}$$
$$\eta \leqslant \widetilde{S}_j(\widetilde{\pi}_j) \tag{**Bii**}$$
$$\widetilde{S}_j(\widetilde{\varphi_j}) \leqslant \psi'_{i_j}. \tag{**Biii**}$$

To prove the theorem, we need a substitution S' such that

$$S' \text{ is a solution for } C' \tag{**Ci**}$$
$$\eta \leqslant S'\big(\pi_1 + \textstyle\sum_{j\in J} \widetilde{\pi}_j\big) \tag{**Cii**}$$
$$S'(\varphi_{12}) \leqslant \psi. \tag{**Ciii**}$$

Choose $S' = S_1 \circ \bigcirc_{j\in J}\widetilde{S}_j$. Then (**Cii**) holds by (**Aii**), (**Bii**) and Proposition 4.7, and, (**Ciii**) holds by (**Av**). To show (**Ci**), we need to establish that S' is a solution for $\widehat{C}$; for this, the crucial bit is to show that $S'(\widetilde{\varphi_j}) \leqslant S'(\varphi_{1j})$, for every $j \in J$; this we obtain as follows:

$S'(\widetilde{\varphi_j}) \leqslant \psi'_{i_j}$ (by **Biii**); $\psi'_{i_j} \leqslant \psi_{i_j}$ (by the hypothesis in the derivation);
$\psi_{i_j} \leqslant S'(\varphi_{1j})$ (by **Avii**)

Therefore, $S'(\widetilde{\varphi_j}) \leqslant S'(\varphi_{1j})$ for every $j \in J$; hence S' is a solution for $\widehat{C}$ by Lemma 6.2. By (**Ai**), S' is a solution for C_1, and by (**Bi**), S' is a solution for $\widetilde{C_j}$, for all $j \in J$.

— $\mathsf{if}\ e_1^{\mathsf{int}}\ \mathsf{then}\ e_2^\sigma\ \mathsf{else}\ e_3^\sigma$:
The derivation is

$$\frac{\eta \vdash e_1^{\mathsf{int}} : \mathtt{t}^{\mathsf{int}} \quad \eta \vdash e_2^\sigma : \psi_2 \quad \eta \vdash e_3^\sigma : \psi_3 \quad \psi_2 \leqslant \psi \quad \psi_3 \leqslant \psi}{\eta \vdash \mathsf{if}\ e_1^{\mathsf{int}}\ \mathsf{then}\ e_2^\sigma\ \mathsf{else}\ e_3^\sigma : \psi}$$

By the inference algorithm,

$$\begin{array}{l}\mathscr{I}\big(\mathsf{if}\ e_1^{\mathsf{int}}\ \mathsf{then}\ e_2^\sigma\ \mathsf{else}\ e_3^\sigma\big) = \\ \quad \textbf{let } \big\langle \pi_1, \mathtt{t}^{\mathsf{int}}, C_1\big\rangle = \mathscr{I}(e_1^{\mathsf{int}}) \\ \qquad \langle \pi_2, \varphi_2, C_2\rangle = \mathscr{I}\big(e_2^\sigma\big) \\ \qquad \langle \pi_3, \varphi_3, C_3\rangle = \mathscr{I}\big(e_3^\sigma\big) \\ \qquad \varphi = \sigma^* \\ \qquad \{\varphi_2 \leqslant \varphi, \varphi_3 \leqslant \varphi\} \overset{+}{\rightsquigarrow} C_4 \\ \qquad C = C_1 \cup C_2 \cup C_3 \cup C_4 \\ \quad \textbf{in } \langle \pi_1 + \pi_2 + \pi_3, \varphi, C\rangle\end{array}$$

By the induction hypothesis on e_1^{int}, e_2^σ, e_3^σ, there exist substitutions S_1, S_2, S_3 such that

S_1 is a solution for C_1 (**Ai**) $\quad \eta \leqslant S_1(\pi_1)$ (**Aii**) $\quad S_1(\mathtt{t}^{\mathsf{int}}) \leqslant \mathtt{t}^{\mathsf{int}}$ (**Aiii**)
S_2 is a solution for C_2 (**Bi**) $\quad \eta \leqslant S_2(\pi_2)$ (**Bii**) $\quad S_2(\varphi_2) \leqslant \psi_2$ (**Biii**)
S_3 is a solution for C_3 (**Ci**) $\quad \eta \leqslant S_3(\pi_3)$ (**Cii**) $\quad S_3(\varphi_3) \leqslant \psi_3$ (**Ciii**)

Let $\pi = \pi_1 + \pi_2 + \pi_3$. To prove the theorem, we need substitution S such that

$$S \text{ is a solution for } C \quad \textbf{(Di)}$$
$$\eta \leqslant S(\pi) \quad \textbf{(Dii)}$$
$$S(\varphi) \leqslant \psi. \quad \textbf{(Diii)}$$

By Proposition 4.4, there exists a substitution S_4 such that $S_4(\sigma^*) \leqslant \psi$. Since $\varphi = \sigma^*$, we obtain $S_4(\varphi) \leqslant \psi$. Now choose the substitution S to be $S_4 \circ S_3 \circ S_2 \circ S_1$. Hence, (**Diii**) holds. Clearly, (**Di**) holds by (**Ai**), (**Bi**), and (**Ci**), and (**Dii**) holds by (**Aii**), (**Bii**), and (**Cii**) and Proposition 4.7.

— $\mathsf{fun}^{\ell}\, f^{\sigma\to\tau}(x^{\sigma}) = e^{\tau}$:

The derivation is

$$\frac{\begin{array}{l}\eta \oplus \{f : \bigwedge_{i\in I}(\psi_i \to \psi_i', L_i), x : \bigwedge_{j\in J}\theta_j\} \vdash e^{\tau} : \theta \\ \forall i \in I : ((\bigwedge_{j\in J}\theta_j) \to \theta, L) \leqslant (\psi_i \to \psi_i', L_i) \\ \ell \in L\end{array}}{\eta \vdash \mathsf{fun}^{\ell}\, f^{\sigma\to\tau}(x^{\sigma}) = e^{\tau} : ((\bigwedge_{j\in J}\theta_j) \to \theta, L)}$$

By the inference algorithm, we have two cases, of which we will just prove the case when $x \in FV(e)$. The other case is similar. Let $\eta' = \eta \oplus \{f : \bigwedge_{i\in I}(\psi_i \to \psi_i', L_i), x : \bigwedge_{j\in J}\theta_j\}$.

$$\begin{array}{rl}\mathscr{I}(\mathsf{fun}^{\ell}\, f^{\sigma\to\tau}(x^{\sigma}) = e^{\tau}) \;=\; & \textbf{let} \\ & \quad \langle \pi', \delta, C\rangle = \mathscr{I}(e^{\tau}) \\ & \quad \{((\bigwedge_{m\in M}\delta_m) \to \delta, \xi) \leqslant \bigwedge_{k\in K}(\varphi_k \to \varphi_k', \xi_k)\} \overset{+}{\rightsquigarrow} C_1 \\ & \textbf{in } \langle \pi, ((\bigwedge_{m\in M}\delta_m) \to \delta,\ \xi),\ C \cup C_1 \cup \{\{\ell\} \subseteq \xi\}\rangle\end{array}$$

where $\pi' = \pi \oplus \{f : \bigwedge_{k\in K}(\varphi_k \to \varphi_k', \xi_k), x : \bigwedge_{m\in M}\delta_m\}$. By the induction hypothesis on e^{τ}, there exists substitution, S, such that

$$S \text{ is a solution for } C \quad \textbf{(Ai)}$$
$$\eta' \leqslant S(\pi') \quad \textbf{(Aii)}$$
$$S(\delta) \leqslant \theta. \quad \textbf{(Aiii)}$$

From (**Aii**) we obtain:

$$\eta \leqslant S(\pi) \quad \textbf{(Bi)}$$
$$\bigwedge_{i\in I}(\psi_i \to \psi_i', L_i) \leqslant \bigwedge_{k\in K} S(\varphi_k \to \varphi_k', \xi_k) \quad \textbf{(Bii)}$$
$$\bigwedge_{j\in J}\theta_j \leqslant S(\bigwedge_{m\in M}\delta_m). \quad \textbf{(Biii)}$$

From (**Bii**), for all $k \in K$, there exists $i_k \in I$, such that,

$$(\psi_{i_k} \to \psi_{i_k}', L_{i_k}) \leqslant S(\varphi_k \to \varphi_k', \xi_k). \quad \textbf{(Biv)}$$

From (**Biv**), we obtain, for all $k \in K$ and $i_k \in I$,

$$S(\varphi_k) \leqslant \psi_{i_k} \quad \textbf{(Bv)}$$
$$\psi_{i_k}' \leqslant S(\varphi_k') \quad \textbf{(Bvi)}$$
$$L_{i_k} \subseteq S(\xi_k). \quad \textbf{(Bvii)}$$

To prove the theorem, we need substitution S' such that

$$S' \text{ is a solution for } C \cup C_1 \cup \{\{\ell\} \subseteq \xi\}), \tag{Ci}$$

$$\eta \leqslant S'(\pi) \tag{Cii}$$

$$S'((\textstyle\bigwedge_{m\in M} \delta_m) \to \delta, \xi) \leqslant ((\bigwedge_{j\in J} \theta_j) \to \theta, L). \tag{Ciii}$$

Note that ξ is fresh and choose substitution $S' = [\xi \mapsto \{\ell\}] \circ S$. (Hence $\xi \notin Dom(S)$). Now (**Cii**) holds by (**Bi**). To show (**Ciii**), we need to show:

$$\textstyle\bigwedge_{j\in J} \theta_j \leqslant S'(\bigwedge_{m\in M} \delta_m) \tag{Di}$$

$$S'(\delta) \leqslant \theta \tag{Dii}$$

$$S'(\xi) \subseteq L. \tag{Diii}$$

But now (**Di**) follows from (**Biii**), (**Dii**) follows from (**Aiii**), and (**Diii**) follows since $\ell \in L$.

To show (**Ci**), the crucial bit is to show that S' is a solution for C_1 since (**Ai**) shows that S' is a solution for C and since $S'(\xi) = \{\ell\} \subseteq L$ by the derivation. It is enough to show, for all $k \in K$, that S' satisfies $((\bigwedge_{m\in M} \delta_m) \to \delta,\ \xi) \leqslant (\varphi_k \to \varphi'_k,\ \xi_k)$. Then, by Lemma 6.2, assert that S' is a solution to C_1. Thus we need to show, for all $k \in K$,

$$S'(\varphi_k) \leqslant \textstyle\bigwedge_{m\in M} S'(\delta_m) \tag{Ei}$$

$$S'(\delta) \leqslant S'(\varphi'_k) \tag{Eii}$$

$$S'(\xi) \subseteq S'(\xi_k). \tag{Eiii}$$

To show (**Ei**), first note that by (**Bv**), $S'(\varphi_k) \leqslant \psi_{i_k}$. By the derivation, we know, for all $i \in I$, that $((\bigwedge_{j\in J} \theta_j) \to \theta, L) \leqslant (\psi_i \to \psi'_i, L_i)$. That is, by contravariance, $\psi_{i_k} \leqslant \bigwedge_{j\in J} \theta_j$. But, by (**Di**), $\bigwedge_{j\in J} \theta_j \leqslant \bigwedge_{m\in M} S'(\delta_m)$. Hence, it follows that $S'(\varphi_k) \leqslant \bigwedge_{m\in M} S'(\delta_m)$.

To show (**Eii**), note that by (**Aiii**), $S'(\delta) \leqslant \theta$. By the derivation, we know, for all $i \in I$, that $((\bigwedge_{j\in J} \theta_j) \to \theta, L) \leqslant (\psi_i \to \psi'_i, L_i)$. That is, by covariance, $\theta \leqslant \psi'_{i_k}$. But, by (**Bvi**), $\psi'_{i_k} \leqslant S'(\varphi'_k)$. Hence, it follows that $S'(\delta) \leqslant S'(\varphi'_k)$.

To show (**Eiii**), we know by the derivation that for all $i \in I$:$((\bigwedge_{j\in J} \theta_j) \to \theta, L) \leqslant (\psi_i \to \psi'_i, L_i)$. Hence for all $i \in I$ we have $L \subseteq L_i$, so, in particular, $L \subseteq L_{i_k}$. Now, by (**Bviii**), $L \subseteq S'(\xi_k)$. But $S'(\xi) = \ell \in L$, therefore, $\{\ell\} \subseteq S'(\xi_k)$.

— $\mathsf{op}\ e^{\mathsf{int}}$:

This case is easy and omitted. □

7. Related work

Jim (Jim 1995; Jim 1996) advocates the use of rank 2 intersection types for typing the lambda calculus with a recursion operator, building on earlier work on intersection type systems in, among other papers, Leivant (1983), van Bakel (1992), and Coppo and Giannini (1992). Rank 2 intersection types only allow conjunctions to appear to the left of a single arrow in a functional type (for example, $((\sigma_1 \wedge \sigma_2) \to \tau) \to \rho$ is rejected). The restriction to rank 2 makes type inference in the system decidable (which is not the case with general intersection types) while retaining the property of principal typing:given a typable term e there exists a pair (A, τ) such that $A \vdash e : \tau$ is derivable and any other

pair (A', τ') constituting a typing of e is a substitution instance of (A, τ). The language considered by Jim does not include arithmetic or logical operations, and a main feature of his inference algorithm is that all inequalities can be reduced to equalities solvable by unification. This is not the case for the constraints generated by our control flow analysis.

7.1. *Type-based program analysis*

Kuo and Mishra (1989) proposes a type inference for strictness analysis without conjunctions. This is extended to conjunctions in Benton (1992) and Jensen (1991) and to conjunctive and disjunctive strictness types in Jensen (1997). None of them propose inference algorithms for the systems. Hankin and Le Métayer (1994; 1995) present a framework for implementing conjunctive program analyses by deriving an abstract machine for proof search from the logics, following the work in Hannan and Miller (1992) For a given term *e and* property φ, this abstract machine will search for a proof of $\vdash_\wedge e : \varphi$. It is thus a method for checking that a program has a particular property rather than a method that infers a property for the program.

Jensen has proposed a strictness analysis for higher-order functional languages based on intersection types and parametric polymorphism (Jensen 1998). This combination allows the writing of certain strictness types in a very compact way. For example, a binary function that is strict in each argument (for example, addition) is given the type

$$\forall \alpha_1, \alpha_2 \,.\, \alpha_1 \to \alpha_2 \to \alpha_1 \wedge \alpha_2.$$

By instantiating the α's appropriately, all strictness properties of such a function can be obtained. These types are used to define a modular inference algorithm in the style of this paper. For each expression, the algorithm infers a property and an environment of hypotheses on the free variables. The inference algorithm follows the same structure as in this paper. However, the constraints that result from inference are over a different set of properties that are axiomatised differently, and hence require another constraint resolution technique.

Henglein and Mossin (1994) and Dussart *et al.* (1995) present a polymorphic binding-time analysis for an extension of the simply typed lambda calculus. They do not include conjunctions or conditional types but introduce instead 'qualified types' of the form $b_1 \leqslant b_2 \Rightarrow b$ where $b_1 \leqslant b_2$ is a constraint that applies to b. Judgments in their logic are of the form

$$C, A \vdash e : \forall \overline{\alpha}.b$$

where A is a set of conjunctions and C is a set of constraints that must be satisfied for the deduction to be valid. Polymorphic recursion is used to analyse fixed points and mutually recursive definitions are handled by applying an improvement of Mycroft's iterative calculation of fixed points in a lattice of type schemes. The absence of conjunctions seems to be of less importance in binding-time analysis than it would be for strictness analysis since there are fewer 'bi-static' functions than bi-strict ones. For example, $e_1 + e_2$ is undefined as soon as one of e_1 and e_2 is undefined, whereas it is static only if both e_1 and e_2 are static.

7.2. *Type-based control flow analysis*

Control flow analysis for higher-order functional languages (also called closure analysis) originated with the work by Jones (Jones 1981; 1987), Sestoft (Sestoft 1988; 1991) and Shivers (Shivers 1991). Several authors have extended this work to frameworks for control-flow analysis that can be instantiated to yield different mono- or polyvariant whole-program analyses (Jagannathan and Weeks 1995; Schmidt 1995; Jagannathan *et al.* 1997; Nielson and Nielson 1997; Amtoft and Turbak 2000; Palsberg and Pavloupoulou 2001; Schmidt 1995). These frameworks are derived from an operational semantics of the language and thus provide the semantic foundations for control flow analysis, though they do not address the problem of modularising the analysis.

The algorithmic aspects of control flow analysis is addressed in Palsberg (1995), which shows how a control flow analysis can be reduced to solving set constraints. Palsberg and O'Keefe show that Amadio and Cardelli's type system for the untyped lambda calculus with recursive types and subtyping (Amadio and Cardelli 1993) is equivalent to *safety analysis* (Palsberg and O'Keefe 1995; Palsberg and Schwartzbach 1995). Safety analysis for the untyped lambda calculus is a global program analysis that detects run-time errors due to illegal use of operators, for example, when a constant is applied to a function. The equivalence says that a term is declared safe by the analysis if and only if it is typable in Amadio and Cardelli's type system. Heintze (1995) shows that, given a variety of type systems instrumented by control-flow information, there exist corresponding control-flow analyses augmented by type information such that each type system is equivalent to its corresponding control-flow analysis. Equivalence here means that each system calculates the same flow and type information. Both of the above papers use type systems for control-flow analysis, but their methods of computing the flow information differ: in Palsberg and O'Keefe's work, the information is indirectly obtained *via* a safety analysis, while for an expression in Heintze's system, it is obtained by enumerating all of the possible control-flow types of the expression, and then systematically removing the (structural) type information. The upshot is that both methods lead to *global analyses* of expressions in a (type-based) setting where most analyses usually rely on compositional inference algorithms to calculate program properties.

In her Ph.D. thesis, Tang provides a *type and effect discipline* for a call-tracking analysis of the simply typed lambda calculus with a recursion operator (Tang 1994). The analysis computes what functions may be called at a program point. Types are annotated with *control-flow effects* that statically approximate the set of functions called during the evaluation of an expression. *Subtyping* is used to obtain greater precision for this analysis by disambiguating call contexts. Tang's framework is attractive because it is *local*: given an expression e and an annotated-type environment Γ containing the annotations of the free variables in e, the (ML-style) type inference algorithm can *locally analyse* proper subexpressions of e, independently of the rest of the program; subsequently, it can compose the local analyses to obtain an analysis for the entire expression. Tang's analysis *is* modular: though she only proves that the analysis has principal types, it is easy to show that it also has principal typings.

This article extends the results of an earlier paper (Banerjee 1997), which developed a modular and polyvariant control-flow analysis for untyped programs. In that paper, the properties inferred were rank 2 intersection properties, and type inference and control-flow analysis were carried out in a single pass. The paper did not address control-flow analysis for recursive function definitions, which the current paper does. The control-flow analysis proposed by Banerjee in the earlier paper has been used extensively by the Church Project[†] in the implementation of a flow-based compiler for Standard ML of New Jersey (Dimock *et al.* 1997; Dimock *et al.* 2001).

The control flow analysis most closely related to ours is that of Mossin, who presents an intersection type-based control-flow analysis (Mossin 1997a; 1997b, Chapter 6). A reduced version of Mossin's analysis (product types are not considered) is shown in Table 5. Mossin is mainly interested in the theoretical aspects and proves that the analysis is 'exact' in the sense that if it calculates the control flow under *all* reduction strategies (and not just, for example, innermost or outermost reduction). He does not consider the algorithmic aspects of implementing the analysis but mentions in passing that the problem it solves is non-elementary recursive. The difference between our system and that of Mossin is that we have imposed a restriction that the function properties appearing in the inference rules must be of rank 2. This is done so that the constraints in the inference algorithm have a simple form.

Finally, as discussed in Amtoft and Turbak (2000) and Palsberg and Pavloupoulou (2001), a more general system of polyvariant control-flow analysis may include both intersection and union types.

8. Discussion

We have developed a modular and polyvariant control-flow analysis for simply typed program fragments. The inherent polymorphism of intersection types is exploited to provide a polyvariant analysis. The analysis is performed by a sound and complete inference algorithm that infers rank 2 intersection properties. The algorithm is compositional and works in a bottom-up manner inferring property environments as well as control-flow properties of program fragments. The completeness result shows that the algorithm computes principal typings: this facilitates linking of program fragments without reanalysis.

The inference algorithm for the application $e_1 e_2$ in Table 4 reveals that the merging of the type environments in the result does *not* unify the possibly different types of a free variable occurring in both e_1 and e_2: rather, the variable is given an intersection type. This is of crucial importance in providing polyvariance.

The assumption of a simply typed base language is exploited in the inference algorithm in computing properties of variables. If a variable has type σ, its control-flow property must have the same shape. For instance, if $\sigma = \mathsf{int} \to \mathsf{int}$, then any function that flows to x must have the property $\sigma^* = (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \xi)$, where ξ is a placeholder for the set that

[†] For details, see `http://types.bu.edu/comp-flow-types.html`.

Table 5. *Mossin's control-flow logic (without products).*

Properties: For each type σ define the set of properties $L_{CF}(\sigma)$ as follows. Here, $Labels(\sigma)$ denotes the set of labels of terms of type σ.

$$\frac{M \subseteq Labels(\texttt{Bool})}{\mathrm{Bool}^M \in L_{CF}(\mathsf{Bool})}$$

$$\frac{\varphi_1 \in L_{CF}(\sigma_1) \quad \varphi_2 \in L_{CF}(\sigma_2) \quad M \subseteq Labels(\sigma_1 \to \sigma_2)}{\varphi_1 \xrightarrow{M} \varphi_2 \in L_{CF}(\sigma_1 \to \sigma_2)}$$

$$\frac{\varphi_i \in L_{CF}(\sigma) \quad i \in I}{\bigwedge_{i\in I} \varphi_i \in L_{CF}(\sigma)}$$

Axiomatisation: (I denotes a finite, non-empty set).

- $\dfrac{\varphi \leqslant \psi_i, \quad i \in I}{\varphi \leqslant \bigwedge_{i\in I} \psi_i}$
- $\bigwedge_{i\in I} \varphi_i \leqslant \varphi_i, \quad \forall i \in I$
- $\dfrac{\psi_1 \leqslant \varphi_1, \varphi_2 \leqslant \psi_2 \quad M \subseteq N}{\varphi_1 \xrightarrow{M} \varphi_2 \leqslant \psi_1 \xrightarrow{N} \psi_2}$
- $\varphi \xrightarrow{M} \psi_1 \wedge \varphi \xrightarrow{M} \psi_2 = \varphi \xrightarrow{M} \psi_1 \wedge \psi_2$

Inference rules:

$$\textbf{Var} \quad \Delta[x \mapsto \varphi] \vdash_{CF} x : \varphi$$

$$\textbf{Const} \quad \frac{c^l \in \{\texttt{true}, \texttt{false}\}}{\Delta \vdash_{CF} c : \mathrm{Bool}^{\{l\}}}$$

$$\textbf{Abs} \quad \frac{\Delta[x \mapsto \varphi] \vdash_{CF} e : \psi}{\Delta \vdash_{CF} \lambda x^l.e : \varphi \xrightarrow{\{l\}} \psi}$$

$$\textbf{Fix} \quad \frac{\forall i \in I.\Delta[x : \psi] \vdash_{CF} e : \psi_i \quad \bigwedge_{i\in I} \psi_i \leqslant \psi}{\Delta \vdash_{CF} (\mathsf{fix}^l x.e) : \psi_j} \text{for any } j \in I$$

$$\textbf{App} \quad \frac{\Delta \vdash_{CF} e_1 : (\varphi_1 \xrightarrow{M} \varphi_2) \quad \forall i \in I.\Delta \vdash_{CF} e_2 : \psi_i \quad \bigwedge_{i\in I} \psi_i \leqslant \varphi_1}{\Delta \vdash_{CF} e_1 e_2 : \varphi_2}$$

$$\textbf{If} \quad \frac{\Delta \vdash_{CF} b : \mathrm{Bool}^M \quad \Delta \vdash_{CF} e_1 : \varphi_1 \quad \Delta \vdash_{CF} e_2 : \varphi_2 \quad \varphi_1 \leqslant \varphi \quad \varphi_2 \leqslant \varphi}{\Delta \vdash_{CF} \mathsf{if}\ b\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 : \varphi}$$

contains the function. We need not have restricted the base language to be simply typed: we could have chosen a rank 2 intersection type system instead. For instance, given the term $M = (\lambda f : \sigma \cdot (\lambda x : \mathsf{int} \cdot fI)(f0))I$ (from Palsberg and O'Keefe (1995)) where I is the identity combinator and $\sigma = (\mathsf{int} \to \mathsf{int}) \to (\mathsf{int} \to \mathsf{int}) \wedge (\mathsf{int} \to \mathsf{int})$, we can show that M has the rank 2 intersection type $\sigma \to (\mathsf{int} \to \mathsf{int})$. Let us annotate the term in ℓPCF (writing out the identity combinator), as follows: $(\lambda^1 f \cdot (\lambda^2 x \cdot (f(\lambda^3 u \cdot u))(f0)))(\lambda^4 v \cdot v)$. Then, executing the inference algorithm $\mathscr{I}$ and solving the set of flow constraints shows that the property of M is $(\mathsf{t}^{\mathsf{int}} \to \mathsf{t}^{\mathsf{int}}, \{3\})$. This means that M evaluates to λ^3. The type of the function part of M is $(\varphi \to (\mathsf{t}^{\mathsf{int}} \to \mathsf{t}^{\mathsf{int}}, \{3\}), \{1\})$, where $\varphi = ((\mathsf{t}^{\mathsf{int}} \to \mathsf{t}^{\mathsf{int}}, \{3\}) \to (\mathsf{t}^{\mathsf{int}} \to$

$\mathtt{t}^{\mathsf{int}}, \{3\}), \{4\}) \wedge (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\})$. This shows the expected polyvariance: the two uses of f expect the identity λ^4; at one application site λ^4 calls λ^3 and returns λ^3; at the other application site it expects an integer and returns an integer.

By focusing on what set of functions every program point can possibly evaluate to, our analysis automatically performs Tang and Jouvelot's call-tracking analysis (Tang 1995). For example, suppose an expression has the property

$$((\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{2\}) \to (\mathtt{t}^{\mathsf{int}} \to \mathtt{t}^{\mathsf{int}}, \{4\}), \{1\}).$$

Then the property signifies that it evaluates to the function labelled 1. This function, when applied, may call the function labelled 2 and may yield the function labelled 4 as result. Moreover, functions labelled 2 and 4 never call any functions and are applied to integer values.

Several issues of a fundamental nature have not been treated in this article and merit further investigations:

— The expressiveness of ranked intersection types for control-flow analysis needs a precise characterisation, especially with respect to properties in the style of parametric polymorphism. The work by Mossin on Exact Flow Analysis mentioned in Section 7.2 and by Kfoury and Wells on finite-rank intersection type inference mentioned in the Introduction seem to be good starting points for such an investigation.

— The complexity (both theoretical and practical) of the analysis should be further investigated, notably with respect to the size of the constraint sets produced by the analysis. Because of the rewriting relation $\overset{+}{\rightsquigarrow}$ (Section 6) on function properties, it is possible that the number of constraints generated due to the corresponding step in the application, conditional and recursive function cases in algorithm $\mathscr{I}$ will be exponential in the rank of function properties. However, we have not investigated optimisations, for example, on-line cycle elimination (Fähndrich *et al.* 1998), to cut down the size of the constraint set generated. This is a topic of future research.

— While there has been much work on control-flow analysis for functional programs in the past decade, not much attention has been paid to the use of control-flow analysis for transformations of functional programs, and, more importantly, for proofs of correctness of the transformations. The main work in the area is due to Wand and his co-authors (Steckler and Wand 1997; Wand and Siveroni 1999), who have formalised the use of control-flow analysis for implementing program transformations such as lightweight closure conversion, useless variable elimination, destructive array updates. Cejtin *et al.* have also used flow-directed closure conversion (Tolmach and Oliva 1998; Dimock *et al.* 2001) in the MLton compiler (Cejtin *et al.* 2000). In recent work, Banerjee *et al.* have considered a uniform method for proving the correctness of control-flow analysis-based program transformations in functional languages (Banerjee *et al.* 2001). The method relies on 'defunctionalisation', which is a mapping from a higher-order language to a first-order language. They give methods for proving defunctionalisation correct. Using this proof and common semantic techniques, they show how two program transformations (flow-based inlining and lightweight defunctionalisation) can be proved correct. However, all the techniques developed above have been for whole-program transformations. It remains a challenge to provide and formalise techniques

for program transformations for program fragments and for program transformations at link time.

Acknowledgements

We should like to thanks the members of the Church Project, especially, Torben Amtoft, Allyn Dimock, Bob Muller, Franklyn Turbak and Joe Wells for discussions. We should also like to thank the anonymous referees for their suggestions, and Jens Palsberg for his interest. Special thanks are due to Franklyn Turbak for making copious comments on the paper in a short time.

References

Aho, A. V., Sethi, R. and Ullman, J. D. (1986) *Compilers: Principles, Techniques and Tools*, Addison-Wesley.

Amadio, R. and Cardelli, L. (1993) Subtyping recursive types. *ACM Transactions on Programming Languages and Systems* **15** (4) 575–631.

Amtoft, T., Nielson, F. and Nielson, H. R. (1997) Type and behaviour reconstruction for higher-order concurrent programs. *Journal of Functional Programming* **7** (3) 321–347.

Amtoft, T., Nielson, F. and Nielson, H. R. (1999) *Type and Effect Systems: Behaviours for Concurrency*, Imperial College Press.

Amtoft, T. and Turbak, F. (2000) Faithful translations between polyvariant flows and polymorphic types. In: Smolka, G. (ed.) Proc. of European Symp. on Programming (ESOP2000). *Springer-Verlag Lecture Notes in Computer Science* **1782**.

Banerjee, A. (1997) A modular, polyvariant and type-based closure analysis. In: *Proceedings of International Conference on Functional Programming (ICFP'97)*, Amsterdam, The Netherlands, ACM Press 1–10.

Banerjee, A., Heintze, N. and Riecke, J. G. (2001) Design and correctness of program transformations based on control-flow analysis. In: Proceedings of International Symposium on Theoretical Aspects of Computer Software (TACS'01). *Springer-Verlag Lecture Notes in Computer Science* **2215**.

Barendregt, H. (1984) *The Lambda Calculus: its Syntax and Semantics*, North-Holland.

Benton, N. (1992) Strictness logic and polymorphic invariance. In: Proceedings of the Second International Symposium on Logical Foundations of Computer Science. *Springer-Verlag Lecture Notes in Computer Science* **620**.

Burn, G., Hankin, C. and Abramsky, S. (1986) Strictness analysis for higher-order functions. *Science of Computer Programming* **7** 249–278.

Cejtin, H., Jagannathan, S. and Weeks, S. (2000) Flow-directed closure conversion for typed languages. In: Smolka, G. (ed.) Proc. of European Symp. on Programming (ESOP2000). *Springer-Verlag Lecture Notes in Computer Science* **1782**.

Coppo, M., Dezani-Ciancaglini, M. and Venneri, B. (1980a) Functional characters of solvable terms. *Zeitschrifft f. Mathematische Logik* **27** 45–58.

Coppo, M., Dezani-Ciancaglini, M. and Venneri, B. (1980b) Principal type schemes and lambda calculus semantics. In: Seldin, J. P. and Hindley, J. R. (eds.) *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, Academic Press 535–560.

Coppo, M. and Giannini, P. (1992) A complete type inference algorithm for simple intersection types. In: Raoult, J.-C. (ed.) Proceedings of 17th Colloquium on Trees in Algebra and Programming (CAAP'92). *Springer-Verlag Lecture Notes in Computer Science* **581** 102–123.

Coppo, M., Damiani, F. and Giannini, P. (1998) Inference based analysis of functional programs: dead-code and strictness. In: *MSI-Memoir Volume 2, 'Theories of Types and Proofs'*, Mathematical Society of Japan 143–176.

Cousot, P. and Cousot, R. (1977) Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fix-points. In: *Proceedings of the Fourth Annual ACM Symposium on Principles of Programming Languages (POPL'77)*.

Damas, L. M. M. (1985) *Type assignment in programming languages*, Ph.D. thesis, University of Edinburgh, Scotland.

Damiani, F. (1996) Refinement types for program analysis. In: Cousot, R. and Schmidt, D. (eds.) Proceedings of 3rd International Static Analysis Symposium (SAS'96). *Springer-Verlag Lecture Notes in Computer Science* **1145** 285–300.

Damiani, F. and Prost, F. (1996) Detecting and removing dead code using rank 2 intersection types. In: Proceedings of TYPES'96 Selected Papers. *Springer-Verlag Lecture Notes in Computer Science* **1512** 66–87.

Dimock, A., Muller, R., Turbak, F. and Wells, J. B. (1997) Strongly typed flow-directed representation transformations. In: *Proceedings of International Conference on Functional Programming (ICFP'97)*, Amsterdam, The Netherlands, ACM Press 11–24.

Dimock, A., Westmacott, I., Muller, R., Turbak, F., Wells, J. and Considine, J. (2000) Program representation size in an intermediate language with intersection and union types. In: Harper, R. (ed.) Proceedings of the Third Workshop on Types in Compilation, (TIC'00). *Springer-Verlag Lecture Notes in Computer Science* **2071**.

Dimock, A., Westmacott, I., Muller, R., Turbak, F. and Wells, J. (2001) Functioning without closure: type-safe customized function representations for Standard ML. In: *Proceedings of the International Conference on Functional Programming (ICFP'01)*, ACM Press.

Dussart, D., Henglein, F. and Mossin, C. (1995) Polymorphic recursion and subtype qualifications: Polymorphic binding-time analysis in polynomial time. In: Mycroft, A. (ed.) Proceedings of the Static Analysis Symposium (SAS'95). *Springer-Verlag Lecture Notes in Computer Science* **983**.

Fähndrich, M., Foster, J. S., Su, Z. and Aiken, A. (1998) Partial online cycle elimination in inclusion constraint graphs. In: *Proceedings of the SIGPLAN Conference on Programming Language Design and Implementation (PLDI'98)*, ACM Press 85–96.

Hankin, C. and Le Métayer, D. (1994) Deriving algorithms from type inference systems: Applications to strictness analysis. In: *Proceedings of Twenty-first ACM Symposium on Principles of Programming Languages (POPL'94)*, ACM Press 202–212.

Hankin, C. and Le Métayer, D. (1995) Lazy type inference and program analysis. *Science of Computer Programming* **25** 219–249.

Hannan, J. and Miller, D. (1992) From operational semantics to abstract machines. *Mathematical Structures in Computer Science* **2** (4) 415–459.

Hatcliff, J. and Danvy, O. (1997) A computational formalization for partial evaluation. *Mathematical Structures in Computer Science* **7** 507–541. (Special issue containing selected papers presented at the 1995 Workshop on Logic, Domains, and Programming Languages, Darmstadt, Germany.)

Heintze, and N, N. (1995) Control-flow analysis and type systems. In: Mycroft, A. (ed.) Proceedings of Static Analysis Symposium. *Springer-Verlag Lecture Notes in Computer Science* **983** 189–206.

Henglein, F. and Mossin, C. (1994) Polymorphic binding-time analysis. In: Proceedings of the Fifth European Symposium on Programming (ESOP'94). *Springer-Verlag Lecture Notes in Computer Science*.

Jagannathan, S. and Weeks, S. (1995) A unified treatment of flow analysis in higher-order languages. In: *Proceedings of the Twenty-second Annual ACM Symposium on Principles of Programming Languages (POPL'95)*, San Francisco, California.

Jagannathan, S., Weeks, S. and Wright, A. (1997) Type-directed flow analysis for typed intermediate languages. In: Hentenryck, P.V. (ed.) Proceedings of the Static Analysis Symposium (SAS'97). *Springer-Verlag Lecture Notes in Computer Science* **1302** 232–249.

Jensen, T. (1991) Strictness analysis in logical form. In: Hughes, J. (ed.) Proceedings of 5th ACM Conference on Functional Programming Languages and Computer Architecture. *Springer-Verlag Lecture Notes in Computer Science* **523** 352–366.

Jensen, T. (1995) Conjunctive type systems and abstract interpretation of higher-order functional programs. *Journal of Logic and Computation* **5** (4) 397–421.

Jensen, T. (1997) Disjunctive program analysis for algebraic data types. *ACM Transactions on Programming Languages and Systems* **19** (5) 752–804.

Jensen, T. (1998) Inference of polymorphic and conditional strictness properties. In: *Proc. of 25th ACM Symposium on Principles of Programming Languages*, ACM Press 209–221.

Jim, T. (1995) Rank 2 type systems and recursive definitions. Technical Memorandum MIT/LCS/TM-531, Laboratory for Computer Science, Massachussetts Institute of Technology.

Jim, T. (1996) What are principal typings and what are they good for? In: *Proceedings of the Twenty-third Annual ACM Symposium on Principles of Programming Languages (POPL'96)*, St. Petersburg, Florida.

Jones, N.D. (1981) Flow analysis of lambda expressions. In: Proceedings of Eighth Colloquium on Automata, Languages, and Programming. *Springer-Verlag Lecture Notes in Computer Science* **115**.

Jones, N.D. (1987) Flow analysis of lazy, higher order functional programs. In: Abramsky, S. and Hankin, C. (eds.) *Abstract Interpretation of Declarative Languages*, Ellis Horwood.

Kfoury, A. J. and Wells, J. B. (1999) Principality and decidable type inference for finite-rank intersection types. In: *Proceedings of the Twentysixth Annual ACM Symposium on Principles of Programming Languages (POPL'99)*, San Antonio, Texas.

Kobayashi, N. (2000) Type-based useless variable elimination. In: Lawall, J.L. (ed.) *Workshop on Partial Evaluation and Semantics-Based Program Manipulation*, Boston, Massachusetts, ACM Press 84–93.

Kuo, T.-M. and Mishra, P. (1989) Strictness analysis: A new perspective based on type inference. In: *Proceedings of 4th. International Conference on Functional Programming and Computer Architecture*, ACM Press.

Leivant, D. (1983) Polymorphic type inference. In: *Proceedings of the Tenth Annual ACM Symposium on Principles of Programming Languages (POPL'83)* 88–98.

Mitchell, J.C. (1991) Type inference with simple subtypes. *Journal of Functional Programming* **1** (3) 245–285.

Mossin, C. (1997a) Exact flow analysis. In: *Proceedings of the Fourth International Static Analysis Symposium*, Paris, France.

Mossin, C. (1997b) *Flow analysis of typed higher-order programs*, Ph.D. thesis, DIKU, University of Copenhagen.

Nielson, F. and Nielson, H.R. (1992) *Two-Level Functional Languages*, Cambridge Tracts in Theoretical Computer Science **34**, Cambridge University Press.

Nielson, F. and Nielson, H.R. (1997) Infinitary control flow analysis: a collecting semantics for closure analysis. In: *Proceedings of the Twenty-fourth Annual ACM Symposium on Principles of Programming Languages (POPL'97)*, Paris, France.

Nielson, H. R. and Nielson, F. (1998) Automatic binding time analysis for a typed λ-calculus. In: *Proceedings of the Fifteenth Annual ACM Symposium on Principles of Programming Languages (POPL'88)* 98–106.

Palsberg, J. (1995) Closure analysis in constraint form. *ACM Transactions on Programming Languages and Systems* **17** (1) 47–62.

Palsberg, J. and O'Keefe, P. (1995) A type system equivalent to flow analysis. *ACM Transactions on Programming Languages and Systems* **17** (4) 576–599.

Palsberg, J. and Pavlopoulou, C. (2001) From polyvariant flow information to intersection and union types. *Journal of Functional Programming* **11** (3) 263–317.

Palsberg, J. and Schwartzbach, M. (1995) Safety analysis versus type inference. *Information and Computation* **118** (1) 128–141.

Plotkin, G. D. (1977) LCF considered as a programming language. *Theoretical Computer Science* **5** 223–255.

Riecke, J. G. (1991) *The Logic and Expressibility of Simply Typed Call-by-Value and Lazy Languages*, Ph.D. thesis, Massachusetts Institute of Technology. (Available as technical report MIT/LCS/TR-523 (MIT Laboratory for Computer Science).)

Sallé, P. (1978) Une extension de la théorie des types en λ-calcul. In: Ausiello, G. and Böhm, C. (eds.) *Fifth International Conference on Automata, Languages and Programming*, Springer-Verlag 398–410.

Schmidt, D. A. (1995) Natural semantics-based abstract interpretation. In: Mycroft, A. (ed.) Proceedings of the Static Analysis Symposium. *Springer-Verlag Lecture Notes in Computer Science* **983** 1–18.

Sestoft, P. (1988) Replacing function parameters by global variables. Master's thesis, University of Copenhagen.

Sestoft, P. (1991) *Analysis and Efficient Implementation of Functional Programs*, Ph.D. thesis, DIKU, Copenhagen, Denmark. (Rapport Nr. 92/6.)

Shivers, O. (1991) *Control-Flow Analysis of Higher-Order Languages or Taming Lambda*, Ph.D. thesis, Carnegie-Mellon University. (Technical Report CMU-CS-91-145.)

Steckler, P. A. and Wand, M. (1997) Lightweight closure conversion. *ACM Transactions on Programming Languages and Systems* **19** (1) 48–86.

Talpin, J.-P. and Jouvelot, P. (1994) The type and effect discipline. *Information and Computation* **111** (2) 245–296.

Tang, Y.-M. (1994) *Systèmes d'effet et interprétation abstraite pour l'analyse de flot de contrôle*, Ph.D. thesis, Ecole Nationale Supérieure des Mines de Paris. (Rapport A/258/CRI.)

Tang, Y.-M. and Jouvelot, P. (1995) Effect systems with subtyping. In: Scherlis, W. L. (ed.) *Symposium on Partial Evaluation and Semantics-Based Program Manipulation*, La Jolla, California, ACM SIGPLAN, ACM Press.

Tofte, M. and Talpin, J.-P. (1994) Implementation of the typed call-by-value λ-calculus using a stack of regions. In: *Proc. of 21st Symposium on Principles of Programming Languages (POPL'94)*, ACM Press.

Tofte, M. and Talpin, J.-P. (1997) Region-based memory management. *Information and Computation* **132** (2) 109–176.

Tolmach, A. and Oliva, D. (1998) From ML to Ada: strongly-typed language interoperability via source translation. *Journal of Functional Programming* **8** (4) 367–412.

van Bakel, S. (1992) Complete restrictions of the intersection type discipline. *Theoretical Computer Science* **102** 135–163.

van Bakel, S. (1993) Intersection type disciplines in lambda calculus and applicative term rewriting systems, Ph.D. thesis, Mathematisch Centrum, Amsterdam.

van Bakel, S. (1996) Rank 2 intersection type assignment in term rewriting systems. *Fundamenta Informaticae* **26** (2).

Wand, M. and Siveroni, I. (1999) Constraint systems for useless variable elimination. In: *Proceedings of the Twenty-sixth Annual ACM Symposium on Principles of Programming Languages* 291–302.

Wright, A. and Felleisen, M. (1991) A syntactic approach to type soundness. *Information and Computation* **115** (1) 38–94.