Intersection Types and Bounded Polymorphism

Benjamin C. Pierce

Department of Computer Science
King's Buildings
Edinburgh, EH9 3JZ
United Kingdom
bcp@dcs.ed.ac.uk

August 24, 1993

Abstract

Intersection types and bounded quantification are complementary extensions of a first-order programming language with subtyping. We define a typed λ-calculus combining these extensions, illustrate its unusual properties, and develop basic proof-theoretic and semantic results leading to algorithms for subtyping and typechecking.

1 Introduction

Intersection types were developed in the late 1970s by Coppo and Dezani-Ciancaglini [29], and independently by Sallé [35, 73] and Pottinger [66]. Since then, they have been studied extensively by members of the group at Torino and many others [3, 23, 30, 31, 32, 33, 34, 41, 42, 50, 51, 69, 70, 71, 72, 75, 76]. Various extensions of the original intersection type discipline have also been explored, including the notion of infinite intersections [56], the dual notion of union types [1, 63], and the relationship between intersection types and models of polymorphism [55, 62, 77]. Some related extensions to ML-style type inference systems are the notions of refinement types [44, 49, 63] and soft typing [24, 43], as well as Coppo and Giannini's recent work on type inference for a decidable restriction of intersection types [36]. Reynolds provided the first demonstration that intersection types can be used as the basis for practical programming languages [68, 69].

Among the most intriguing properties of intersection types is their ability to express an essentially unbounded (though finite) amount of information about a program. For example, the addition function + can be given the type $Int \rightarrow Int \rightarrow Int \wedge Real \rightarrow Real \rightarrow Real$, capturing both the general fact that the sum of two real numbers is always real and the more specialized observation that the sum of two integers is an integer. A compiler for a language with intersection types might even provide two different object-code sequences for the different versions of +, one using a floating point addition instruction and one using integer addition. For each instance of + in a program, the compiler would check whether both arguments are integers and generate the more efficient code sequence in this case. This kind of *finitary polymorphism* or *coherent overloading* is so expressive, that the set of all valid typings for an untyped λ-term amounts to a complete characterization of its behavior (c.f. [23]).

Bounded quantification was introduced by Cardelli and Wegner [21] in the language Fun. Based on informal ideas by Cardelli and formalized using techniques developed by Mitchell [58], Fun integrated Girard-Reynolds polymorphism [47, 67] with Cardelli's first-order calculus of subtyping [13]. The original Fun was simplified and slightly generalized by Bruce and Longo [7], and again by Curien and Ghelli [38]. (Curien and Ghelli's formulation, called *minimal Bounded Fun* or $F_{\leq}$ ("F-sub"), has become standard and is the one considered here.) Cardelli and Wegner's survey paper [21] gives the first programming examples using bounded quantification; more are developed in Cardelli's study of power kinds [14]. Curien and Ghelli [38, 46] address a number of syntactic properties of $F_{\leq}$. Semantic aspects of closely related systems have been studied by Bruce and Longo [7], Martini [57], Breazu-Tannen, Coquand, Gunter, and Scedrov [4], Cardone [22], Cardelli and Longo [18], Cardelli, Martini, Mitchell, and Scedrov [19], Curien and Ghelli [38, 37], and Bruce and Mitchell [9]. $F_{\leq}$ has been extended to include record types and richer notions of inheritance by Cardelli and Mitchell [20], Bruce [5], Cardelli [16], and Canning, Cook, Hill, Olthoff, and Mitchell [11]. It forms the basis of some recent "full-scale" accounts of object-oriented programming [6, 65]. Bounded quantification also plays a key role in Cardelli's programming language Quest [15, 18] and in the Abel language developed at HP Labs [10, 11, 12, 28], in Mitchell's Rapide language [60], and in Bruce's TOOPL [6].

Cardelli and Wegner integrated impredicative polymorphism with the notion of subtyping by allowing a quantified type to give a *bound* for its parameter; for example, $\forall\alpha{\leq}Student.\ List(\alpha)\rightarrow List(\alpha)$ takes as its first parameter an arbitrary subtype of the type $Student$ and returns a function on lists of this type. This *universal* or *parametric polymorphism* is both broader (since the number of possible instantiations of a polymorphic type is infinite) and more rigid (since all instances must have the same basic shape) than the finitary polymorphism provided by intersection types. Its main practical advantages are brevity and compile-time efficiency: it allows polymorphic expressions to be written, typechecked, and compiled just once.

Intersection types and bounded quantification thus complement and, in a sense, complete each another: quantifiers can be used to compactly capture the common cases where all the desired types of a term are structurally similar, which lead to long and unwieldy typings when expressed only in terms of intersections, while intersections allow a degree of refinement that is impossible with pure polymorphism. Moreover, intersections can be used in the bounds of quantifiers to express a simple form of "multiple inheritance"; for example, the type $\forall\alpha{\leq}Student{\wedge}Employee.\ List(\alpha)\rightarrow List(\alpha)$ describes polymorphic functions applicable only to the common subtypes of $Student$ and $Employee$. Indeed, a higher-order extension of the system described in this paper has recently been used in a type-theoretic model of object-oriented multiple inheritance [27].

Following a more detailed discussion of the pure systems of intersections and bounded quantification (Section 2), we describe, in Section 3, a typed λ-calculus called $F_{\wedge}$ ("F-meet"), a "core type system" integrating the features of both. Section 4 some gives examples illustrating this system's expressive power. Section 5 presents the main results of the paper, a proof-theoretic analysis of $F_{\wedge}$'s subtyping and typechecking relations leading to algorithms for checking subtyping and for synthesizing minimal types for terms. Section 6 discusses semantic aspects of the calculus, obtaining a simple soundess proof for the typing rules by interpreting types as partial equivalence relations; however, another proof-theoretic result, the nonexistence of least upper bounds for arbitrary pairs of types, implies that typed models may be more difficult to construct. Section 7 offers concluding remarks.

2 Background

We set the stage for the $F_\wedge$ calculus in this section by establishing notational conventions and reviewing its two immediate ancestors. We begin with a common core calculus, a simply typed λ-calculus with subtyping, and then discuss two extensions, a first-order calculus with intersection types and a second-order calculus with bounded quantification.

2.1 Notational Preliminaries

The metavariables α and β range over type variables; σ, τ, θ, ϕ, and ψ range over types; e and f range over terms; and x and y range over term variables. A finite sequence with elements x_1 through x_n is written $[x_1..x_n]$. Concatenation of finite sequences is written $X_1 * X_2$. Single elements are adjoined to the right or left of sequences with a comma: $[x_a, X_b]$ or $[X_a, x_b]$. Sequences are sometimes written using "comprehension" notation: $[x \mid \ldots]$; for example, if $T \equiv [\sigma{\rightarrow}\tau,\ \psi{\rightarrow}\psi,\ \sigma{\rightarrow}\theta]$, then the comprehension $[\zeta_2 \mid \zeta_1{\rightarrow}\zeta_2 \in T \text{ and } \zeta_1{\equiv}\sigma]$ stands for the sequence $[\tau,\ \theta]$. A *context* Γ is a finite sequence of typing assumptions $x{:}\tau$ and subtyping assumptions $\alpha{\leq}\tau$, with no variable or type variable appearing twice on the left. It is convenient to view a context Γ as a finite function and write $dom(\Gamma)$ for its domain.

A type τ is *closed* with respect to a context Γ if its free (type) variables are all in $dom(\Gamma)$. A term e is closed with respect to Γ if its free (term and type) variables are all in $dom(\Gamma)$. A context Γ is closed if $\Gamma \equiv \{\}$, or if $\Gamma \equiv \Gamma_1,\ \alpha{\leq}\tau$ with Γ_1 closed and τ closed with respect to Γ_1, or if $\Gamma \equiv \Gamma_1,\ x{:}\tau$ with Γ_1 closed and τ closed with respect to Γ_1. A subtyping statement $\Gamma \vdash \sigma \leq \tau$ is closed if Γ is closed and σ and τ are closed with respect to Γ; a typing statement $\Gamma \vdash e \in \tau$ is closed if Γ is closed and e and τ are closed with respect to Γ. In the following, we assume that all statements under discussion are closed; in particular, we allow only closed statements in instances of inference rules.

Types, terms, contexts, and statements that differ only in the names of bound variables are considered identical. (That is., we think of variables not as names but as pointers into the surrounding context, as suggested by deBruijn [40].)

Examples are set in a typewriter font; λ-calculus notation is transliterated as follows: $\top$ is written as `T`, λ as `\`, Λ as `\\`, $\forall$ as `All`, and $\leq$ as `<`. Lines of input to the typechecker are prefixed with `>` and followed by the system's response. The type constructors $\rightarrow$ and $\forall$ bind more tightly than $\wedge$. Also, $\rightarrow$ associates to the right and $\forall$ obeys the usual "dot rule" where the body τ of a quantified type $\forall\alpha{\leq}\sigma.\ \tau$ is taken to extend to the right as far as possible.

2.2 Simply Typed λ-Calculus with Subtyping

The $F_\wedge$ calculus may be viewed as a "least upper bound" of two calculi: a first-order λ-calculus with intersection types ($\lambda_\wedge$) and a second-order λ-calculus with bounded quantification ($F_\leq$). These, in turn, are both extensions of the simply typed λ-calculus enriched with a subtyping relation ($\lambda_\leq$). The latter system was proposed by Cardelli [13] as a "core calculus of subtyping" in a foundational framework for object-oriented programming languages. We briefly review its definition.

2.2.1. Definition: The types of $\lambda_\leq$ consist of a set of *primitive types* (ranged over by the metavariable ρ) closed under the *function space* type constructor $\rightarrow$:

$$\tau \quad ::= \quad \rho \quad | \quad \tau_1{\rightarrow}\tau_2$$

The terms of $\lambda_\leq$ consist of a countable set of variables (ranged over by x), together with all the phrases that can be built from these by functional abstraction and application:

$$e \quad ::= \quad x \quad | \quad \lambda x{:}\tau.\ e \quad | \quad e_1\ e_2$$

The presence of the *domain-type annotation* τ in the syntax of λ-abstractions marks a fundamental design choice, which we shall maintain throughout the paper: all of the calculi we consider are *explicitly typed* systems (as opposed to *type assignment* systems). This requires that a programmer exert firm control over the typechecker's behavior, making programs more verbose but rendering typechecking decidable in many cases where type inference would be undecidable.

2.2.2. Definition: A $\lambda_\leq$ context is a sequence of typing assumptions

$$\Gamma \quad ::= \quad \{\} \quad | \quad \Gamma, x{:}\tau$$

with no variable mentioned twice. The function $dom(\Gamma)$ denotes the set of variables defined by Γ; the *range* of Γ is the collection of right-hand sides of bindings in Γ. $\Gamma(x)$ denotes the type of x in Γ, if it has one. The set of free variables of a term e is written $FV(e)$. A term e is *closed* with respect to a context Γ if $FV(e) \subseteq dom(\Gamma)$. A typing statement $\Gamma \vdash e \in \tau$ is closed if e is closed with respect to Γ. In the following, we assume that all statements under discussion are closed. In particular, we allow only closed statements in instances of inference rules.

The typing relation of $\lambda_\leq$ is formalized as a collection of inference rules for deriving typing statements of the form $\Gamma \vdash e \in \tau$ ("under assumptions Γ, expression e has type τ"), where Γ contains a typing assumption for each of the free variables of e. The rules for variables, abstractions, and applications are exactly the same as in the ordinary simply typed λ-calculus [26]. In addition, we introduce a rule of *subsumption* stating that whenever a term e has a type σ and σ is a subtype of another type τ, the type of e may be promoted to τ.

2.2.3. Definition: The $\lambda_\leq$ typing relation $\Gamma \vdash e \in \tau$ is the least three-place relation closed under the following rules:

$$\Gamma \vdash x \in \Gamma(x) \tag{Var}$$

$$\frac{\Gamma, x{:}\tau_1 \vdash e \in \tau_2}{\Gamma \vdash \lambda x{:}\tau_1.\ e \in \tau_1 \rightarrow \tau_2} \tag{Arrow-I}$$

$$\frac{\Gamma \vdash e_1 \in \tau_1 \rightarrow \tau_2 \qquad \Gamma \vdash e_2 \in \tau_1}{\Gamma \vdash e_1\ e_2 \in \tau_2} \tag{Arrow-E}$$

$$\frac{\Gamma \vdash e \in \tau_1 \qquad \Gamma \vdash \tau_1 \leq \tau_2}{\Gamma \vdash e \in \tau_2} \tag{Sub}$$

This definition may be viewed in two different ways:

1. as a three-place relation constructed as the limit of a sequence beginning with the empty relation and successively enriching it according to the rules Var, Arrow-I, Arrow-E, and Sub, or
2. as a simple logic whose derivable judgements are those appearing as conclusions of valid derivation trees built from these rules.

We adopt both views, interchangeably, in what follows.

By analogy with types, we might expect the definition of $\lambda_\leq$ terms to include a collection of constants. These can be added to the calculus, but they are not strictly necessary: we can write programs involving "built-in values" like numbers and arithmetic operators simply by considering these as variables and providing a *pervasive context* — call it Γ_P — assigning them appropriate types. When contexts are extended in Section 2.4 to allow assumptions for type variables, primitive types can also be dropped, although not every conceivable ordering on the primitive types can be encoded as a pervasive context c.f. 3.3.2.4).

It remains to define the subtype relation. Intuitively, a subtyping statement $\Gamma \vdash \sigma \leq \tau$ corresponds to the assertion that σ is a *refinement* of τ, in the sense that every element of σ contains enough information to meaningfully be regarded as an element of τ. In some models this means simply that σ is a subset of τ; more generally, it implies the existence of a distinguished *coercion function* from σ to τ.

These considerations immediately entail that the subtype relation should be both reflexive and transitive — i.e., that it should be a preorder. We assume that the subtype relation on primitive types is given in advance by some preorder $\leq_P$. This relation is extended to the smallest preorder closed under the following subtyping rule for function types: $\sigma_1 \rightarrow \sigma_2$ is a subtype of $\tau_1 \rightarrow \tau_2$ iff τ_1 is a subtype of σ_1 and σ_2 is a subtype of τ_2. Notice that, as usual, this relation is *covariant* in the right-hand side and *contravariant* in the left-hand side of the $\rightarrow$ constructor: a collection of functions can be refined either by narrowing the range into which their results must fall or by enlarging the domain over which they must behave properly.

A key feature of this notion of subtyping is that it is *structural*: the ordering of two arrow types is completely determined by their left- and right-hand sides. In logical terms, the only extended theories we consider are those whose non-logical rules are restricted to statements about primitive types. This feature is retained in the other calculi we consider in the paper.

In fact, the subtype relation of $\lambda_\leq$ is not only structural, but *compositional*: the ordering on arrow types may be computed as a function of the ordering of their left- and right-hand sides. The introduction of intersection types in the next section will invalidate this stronger property.

2.2.4. Definition: The $\lambda_\leq$ subtyping relation $\Gamma \vdash \sigma \leq \tau$ is the least three-place relation closed under the following rules:

$$\Gamma \vdash \tau \leq \tau \qquad \text{(S{\small UB}-R{\small EFL})}$$

$$\frac{\Gamma \vdash \tau_1 \leq \tau_2 \qquad \Gamma \vdash \tau_2 \leq \tau_3}{\Gamma \vdash \tau_1 \leq \tau_3} \qquad \text{(S{\small UB}-T{\small RANS})}$$

$$\frac{\Gamma \vdash \rho_1 \leq_P \rho_2}{\Gamma \vdash \rho_1 \leq \rho_2} \qquad \text{(S{\small UB}-P{\small RIM})}$$

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \sigma_1 \rightarrow \sigma_2 \leq \tau_1 \rightarrow \tau_2} \qquad \text{(S{\small UB}-A{\small RROW})}$$

Of course, the context Γ plays no part in these rules and could be dropped without changing the system. We include it here for notational compatibility with later systems, in which contexts will also contain subtyping assumptions about type variables.

When $\Gamma \vdash \sigma \leq \tau$, we call τ a *supertype* of σ. When $\Gamma \vdash \sigma \leq \tau$ and $\Gamma \vdash \tau \leq \sigma$, we say that σ and τ are *equivalent* under Γ, written $\Gamma \vdash \sigma \sim \tau$. We write $\Gamma \nvdash \sigma \leq \tau$ to *deny* the derivability of the statement $\Gamma \vdash \sigma \leq \tau$.

When necessary to prevent confusion with other calculi, turnstiles in $\lambda_\leq$ derivations are written $\vdash^{\lambda_\leq}$.

2.3 Intersection Types

The original motivation for the introduction of intersection types was the desire for a type-assignment system in the spirit of Curry [39], but with two additional properties:

1. The typing of a term should be invariant under β-conversion. (Under Curry's system, β-reduction preserves types but β-expansion, in general, does not.)
2. Every term possessing a normal form should be given a meaningful typing.

2.3.1. Definition: The first-order calculus of intersection types, $\lambda_\wedge$, is formed from $\lambda_\leq$ by adding intersections to the language of types:

$$\tau \quad ::= \quad \rho \quad | \quad \tau_1 \to \tau_2 \quad | \quad \bigwedge[\tau_1..\tau_n]$$

For presenting examples, we introduce the following abbreviations:

$$\begin{array}{lcl} \sigma \wedge \tau & \stackrel{\text{def}}{=} & \bigwedge[\sigma, \tau] \\ \top & \stackrel{\text{def}}{=} & \bigwedge[\,]. \end{array}$$

(Of course, the whole system could equally well be formulated in terms of a binary constructor $\wedge$ and a nullary constructor $\top$.)

The notations $\sigma \cap \tau$, $\sigma \& \tau$, and $\sigma \wedge \tau$ have all been used to denote the intersection of σ and τ; the universal type (usually corresponding to a nullary intersection) has been written as both ω and ns ("nonsense"). The phrase $\sigma \wedge \tau$ (or $\bigwedge[\sigma, \tau]$) is pronounced "σ meet τ," "σ intersect τ," or "σ and τ." For the nullary intersection, we use the symbol $\top$ ("top") by analogy with the binary case.

Two new subtyping rules capture the order-theoretic properties of the $\wedge$ operator:

$$\frac{\text{for all } i,\ \Gamma \vdash \sigma \leq \tau_i}{\Gamma \vdash \sigma \leq \bigwedge[\tau_1..\tau_n]} \qquad (\text{SUB-INTER-G})$$

$$\Gamma \vdash \bigwedge[\tau_1..\tau_n] \leq \tau_i \qquad (\text{SUB-INTER-LB})$$

(Complete sets of inference rules for $\lambda_\wedge$ and the other major systems introduced in this paper appear in Appendix A.)

One additional subtyping rule captures the relation between intersections and function spaces, allowing the two constructors to "distribute" when an intersection appears on the right-hand side of an arrow:

$$\Gamma \vdash \bigwedge[\sigma \to \tau_1 .. \sigma \to \tau_n] \leq \sigma \to \bigwedge[\tau_1..\tau_n] \qquad (\text{SUB-DIST-IA})$$

(This inclusion is actually an equivalence, since the other direction may be proved from the rules for meets and arrows.)

This rule, though intuitively reasonable, will have a strong effect on both syntactic and semantic properties of the language. For example, it implies that $\top \leq \sigma \to \top$ for any σ.

The typing rules must also be extended slightly. As for any type constructor, we expect to find a pair of an introduction rule, by which terms can be shown to possess intersection types, and an elimination rule, by which this fact may later be exploited. The introduction rule allows an intersection type to be derived for a term whenever each of the elements of the intersection can be derived for it separately:

$$\frac{\text{for all } i,\ \Gamma \vdash e \in \tau_i}{\Gamma \vdash e \in \bigwedge[\tau_1..\tau_n]} \qquad (\text{INTER-I})$$

The corresponding elimination rule would allow us to infer, on the basis of a derivation of a statement like $\Gamma \vdash e \in \bigwedge[\tau_1..\tau_n]$, that e possesses every τ_i individually. But this follows already from the rule SUB-INTER-LB and the rule of subsumption; we need not add the elimination rule explicitly to the calculus.

The nullary case of this rule is worth particular notice, since it allows the type $\top$ to be derived for *every* term of the calculus, including terms whose evaluation intuitively encounters a run time error or fails to terminate:

The system as we have described it so far supports the use of intersection types in programming only to a limited degree. Suppose, for example, that the primitive subtype relation has $Int \leq Real$ and the addition function in the pervasive context is overloaded to operate on both integers and reals:

$$\Gamma_P(+) = Int \to Int \to Int \wedge Real \to Real \to Real.$$

Expressions involving addition of integers and reals will be given type *Int* if possible, otherwise type *Real*:

```
> x = plus 0 0;
x : Int

> x = plus pi pi;
x : Real

> x = plus 0 pi;
x : Real
```

(Note that the typechecker attempts to simplify the type it derives for each term, so that, for example, the type of `plus 0 0` is printed as `Int` instead of as `Int/\Real`.)

But using just the constructs introduced so far, there is no way of writing our own functions that behave in this way. For example, the doubling function $\lambda x{:}?.\ x + x$ cannot be given the type $Int \to Int \wedge Real \to Real$, since replacing the ? with either *Int* or *Real* (or even $Int \wedge Real$) gives a typing that is too restrictive:

```
> double1 = \x:Int. plus x x;
double1 : Int -> Int

> double2 = \x:Real. plus x x;
double2 : Real -> Real

> double3 = \x:Int/\Real. plus x x;
double3 : Int -> Int
```

This led Reynolds [69] to introduce a generalized form of λ-abstraction allowing explicit programmer-controlled generation of alternative typings for terms:

$$e \quad ::= \quad \ldots \quad | \quad \lambda x{:}\tau_1..\tau_n.\ e$$

The typing rule for this form allows the typechecker to make a choice of any of the σ's as the type of x in the body:

$$\frac{\Gamma,\ x{:}\sigma_i \ \vdash\ e \ \in\ \tau_i}{\Gamma \ \vdash\ \lambda x{:}\sigma_1..\sigma_n.\ e \ \in\ \sigma_i \to \tau_i} \qquad \text{(ARROW-I')}$$

This rule can be used together with INTER-I to generate a set of up to n alternative typings for the body and then form their intersection as the type of the whole λ-abstraction:

```
> double = \x:Int,Real. plus x x;
double : Real->Real /\ Int->Int
```

One peculiar property of the generalized λ is that adding extra alternatives to the set of possible domain types for x can only improve the typing of the whole expression. If some alternative results in a "typechecking failure," the best type for the body under this assumption will be equivalent to $\top$ (typically via the SUB-DIST-IA rule), and may therefore be dropped from the final type of the expression without changing its equivalence class in the subtype ordering:

```
> double = \x:Int,Real,Char. plus x x;
double : Int->(Real/\Int) /\ Real->/\[Real] /\ Char->T
    i.e. Real->Real /\ Int->Int
```

When necessary to prevent confusion with other calculi, turnstiles in $\lambda_\wedge$ derivations are written $\vdash^{\lambda\wedge}$.

2.4 Bounded Polymorphism

Like other second-order λ-calculi, the terms of $F_\leq$ include the variables, abstractions, and applications of $\lambda_\leq$, plus the type abstractions and type applications of the second-order λ-calculus — slightly refined to take account of the subtype relation: each type abstraction gives a *bound* for the type variable it introduces and each type application must satisfy the constraint that the argument type is a subtype of the bound of the polymorphic function being applied. Also, like that of $\lambda_\wedge$, the $F_\leq$ subtype ordering includes a maximal element. (Since the two are not exactly the same (c.f. 3.3.1), the maximal $F_\leq$ type is called here by its conventional name, *Top*, instead of $\top$.)

$$\begin{array}{lcl} \tau & ::= & \mathit{Top} \quad | \quad \alpha \quad | \quad \tau_1 \to \tau_2 \quad | \quad \forall\alpha{\leq}\tau_1.\ \tau_2 \\ e & ::= & x \quad | \quad \lambda x{:}\tau.\ e \quad | \quad e_1\ e_2 \quad | \quad \Lambda\alpha{\leq}\tau.\ e \quad | \quad e[\tau] \end{array}$$

To accomodate the subtyping assumptions introduced by type abstractions, we enrich the notion of "context" to include bindings for both term variables and type variables:

Type abstractions have almost the same typing rule as in other second-order λ-calculi; they are checked by moving their stated bound for the type variable they introduce into the context and checking the body of the abstraction under the enriched set of assumptions:

$$\frac{\Gamma,\ \alpha{\leq}\tau_1\ \vdash\ e\ \in\ \tau_2}{\Gamma\ \vdash\ \Lambda\alpha{\leq}\tau_1.\ e\ \in\ \forall\alpha{\leq}\tau_1.\ \tau_2} \qquad \text{(ALL-I)}$$

Type applications check that the type being passed as a parameter is indeed a subtype of the bound of the corresponding quantifier:

$$\frac{\Gamma\ \vdash\ e\ \in\ \forall\alpha{\leq}\tau_1.\ \tau_2 \qquad \Gamma\ \vdash\ \tau\ \leq\ \tau_1}{\Gamma\ \vdash\ e[\tau]\ \in\ \{\tau/\alpha\}\tau_2} \qquad \text{(ALL-E)}$$

The subtype relation of $\lambda_\leq$ is also extended with several rules. First, we stipulate that *Top* is a maximal element of the subtype order:

$$\Gamma\ \vdash\ \sigma\ \leq\ \mathit{Top} \qquad \text{(SUB-TOP)}$$

(One of the main uses of *Top* — in fact, the original reason it was introduced by Cardelli and Wegner — is to recover ordinary unbounded quantification as a special case of bounded quantification: $\forall\alpha.\ \tau$ becomes $\forall\alpha{\leq}\mathit{Top}.\ \tau$.)

Type variables are subtypes of the bounds given for them in the prevailing context:

$$\Gamma\ \vdash\ \alpha\ \leq\ \Gamma(\alpha) \qquad \text{(SUB-TVAR)}$$

Like arrow types, subtyping of quantified types is contravariant in their bounds and covariant in their bodies:

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma, \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \forall\alpha{\leq}\sigma_1.\ \sigma_2 \leq \forall\alpha{\leq}\tau_1.\ \tau_2} \tag{Sub-All}$$

This rule deserves a closer look, since it causes considerable difficulties (c.f. Section 6.2 and [64]). Intuitively, it reads as follows:

> A type $\tau \equiv \forall\alpha{\leq}\tau_1.\ \tau_2$ describes a collection of polymorphic values (functions from types to values), each mapping subtypes of τ_1 to instances of τ_2. If τ_1 is a subtype of σ_1, then the domain of τ is smaller than that of $\sigma \equiv \forall\alpha{\leq}\sigma_1.\ \sigma_2$, so σ is a stronger constraint and describes a smaller collection of polymorphic values. Moreover, if, for each type θ that is an acceptable argument to the functions in both collections (i.e., one that satisfies the more stringent requirement $\theta \leq \tau_1$), the θ-instance of σ_2 is a subtype of the θ-instance of τ_2, then σ is a "pointwise stronger" constraint and again describes a smaller collection of polymorphic values.

Thus, quantified types may be thought of as a kind of function spaces. We sometimes abuse this analogy and speak of the bound and body of a quantified type as its "left-hand" and "right-hand" sides.

When necessary to prevent confusion, turnstiles in $F_{\leq}$ derivations are written $\overset{\leq}{\vdash}$.

The rules defining $F_{\leq}$ do not directly constitute an algorithm for checking the subtype relation, since they are not syntax-directed. In particular, the rule Trans cannot effectively be applied backwards, since this would involve "guessing" an appropriate value for the intermediate type τ_2. Curien and Ghelli (as well as Cardelli and others) use the following reformulation:

2.4.1. Definition: $F_{\leq}^{N}$ ("N" for "normal form") is the least relation closed under the following rules:

$$\Gamma \vdash \sigma \leq \mathit{Top} \tag{NTop}$$

$$\Gamma \vdash \alpha \leq \alpha \tag{NRefl}$$

$$\frac{\Gamma \vdash \Gamma(\alpha) \leq \tau}{\Gamma \vdash \alpha \leq \tau} \tag{NVar}$$

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \sigma_1{\rightarrow}\sigma_2 \leq \tau_1{\rightarrow}\tau_2} \tag{NArrow}$$

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma, \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \forall\alpha{\leq}\sigma_1.\ \sigma_2 \leq \forall\alpha{\leq}\tau_1.\ \tau_2} \tag{NAll}$$

The reflexivity rule here is restricted to type variables. Transitivity is eliminated, except for instances of the form

$$\frac{\Gamma \vdash \alpha \leq \Gamma(\alpha) \qquad \Gamma \vdash \Gamma(\alpha) \leq \tau}{\Gamma \vdash \alpha \leq \tau,}$$

which are packaged together as instances of the new rule NVar.

These rules may be read as an algorithm (i.e., a recursively defined procedure) for checking the subtype relation:

$check(\Gamma \vdash \sigma \leq \tau) =$

1. *if* $\tau \equiv Top$
   then true
2. *else if* $\sigma \equiv \sigma_1 \rightarrow \sigma_2$ *and* $\tau \equiv \tau_1 \rightarrow \tau_2$
   then $\quad check(\Gamma \vdash \tau_1 \leq \sigma_1)$
   and $check(\Gamma \vdash \sigma_2 \leq \tau_2)$
3. *else if* $\sigma \equiv \forall\alpha{\leq}\sigma_1.\ \sigma_2$ *and* $\tau \equiv \forall\alpha{\leq}\tau_1.\ \tau_2$
   then $\quad check(\Gamma \vdash \tau_1 \leq \sigma_1)$
   and $check(\Gamma,\ \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2)$
4. *else if* $\sigma \equiv \alpha$ *and* $\tau \equiv \alpha$
   then true
5. *else if* $\sigma \equiv \alpha$
   then $check(\Gamma \vdash \Gamma(\alpha) \leq \tau)$

n. *else*
   false.

We write $F_{\leq}^{N}$ to refer either to the algorithm or to the inference system, depending on context.

2.4.2. Lemma: [Curien and Ghelli] The relations $F_{\leq}$ and $F_{\leq}^{N}$ coincide: $\Gamma \vdash \sigma \leq \tau$ is derivable in $F_{\leq}$ iff it is derivable in $F_{\leq}^{N}$.

The algorithm $F_{\leq}^{N}$ may be thought of as incrementally attempting to build a normal form derivation of a statement J, starting from the root and recursively building subderivations for the premises. By Lemma 2.4.2, if there is any derivation whatsoever of a statement J, there is one in normal form; the algorithm is guaranteed to recapitulate this derivation and halt in finite time.

2.4.3. Fact: [Curien and Ghelli] $\Gamma \vdash \sigma \leq \tau$ is derivable in $F_{\leq}^{N}$ iff the algorithm $F_{\leq}^{N}$ halts and returns *true* when given this statement as input.

Unfortunately, the algorithm is *not* a decision procedure for the subtype relation. Indeed, this relation can be shown to be undecidable [64].

3 The $\mathbf{F}_\wedge$ Calculus

This section introduces $F_\wedge$, an explicitly typed second-order lambda calculus with bounded quantification and intersection types. $F_\wedge$ can roughly be characterized as the union of the concrete syntax and typing rules for the systems $\lambda_\wedge$ and $F_{\leq}$:

$$\begin{tikzcd}
 & F_\wedge & \\
\lambda_\wedge \arrow[ur] & & F_{\leq} \arrow[ul] \\
 & \lambda_{\leq} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

To achieve a compact and symmetric calculus, however, a few small modifications and extensions are needed:

- Since $F_{\leq}$ allows primitive types to be encoded as elements of the pervasive context, we drop the primitive types of $\lambda_{\leq}$ and $\lambda_\wedge$ and the rule Sub-Prim.

- Since $\top$ and *Top* both function as maximal elements of their respective subtype orderings, we drop *Top* and let $\top$ take over its job. Section 3.3 discusses this design decision in more detail.
- Since $\forall$ behaves like a kind of function space constructor, we add a new law SUB-DIST-IQ, analogous to SUB-DIST-IA, which allows intersections to be distributed over quantifiers on the right-hand side.
- We use the ordinary form of λ-abstraction from $F_\leq$ rather than the generalized one introduced by Reynolds for $\lambda_\wedge$. The notion of deriving alternative typings for subphrases under different sets of assumptions is captured by a new syntactic form, *for*.

The *for* construct is described in detail in Section 3.1. Section 3.2 then summarizes the concrete syntax, subtyping rules, and typing rules of $F_\wedge$. Section 3.3 discusses some major design choices in the formulation of $F_\wedge$.

3.1 Explicit Alternation: The *for* Construct

The notions of type variables and type substitution inherited from $F_\leq$ can be used to define an elegant generalization of the alternation inherent in $\lambda_\wedge$'s λ-abstractions with multiple type annotations. We extend the concrete syntax of terms with a *for* form

$$e \quad ::= \quad \ldots \quad | \quad \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e$$

whose typing rule allows a choice of any of the σ's as a replacement for α in the body:

$$\frac{\Gamma \vdash \{\sigma_i/\alpha\}e \in \tau_i}{\Gamma \vdash \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e \in \tau_i} \qquad \text{(FOR)}$$

This rule, like the generalized arrow introduction rule ARROW-I' of $\lambda_\wedge$, can be used together with INTER-I to generate a set of up to n alternative typings for the body and then form their intersection as the type of the whole *for* expression:

```
> double = for A in Int,Real. \x:A. plus x x;
double : Real->Real /\ Int->Int
```

Indeed, $\lambda_\wedge$'s λ-abstraction may be reintroduced as a syntactic abbreviation:

$$\lambda x{:}\sigma_1..\sigma_n.\ e \stackrel{\text{def}}{=} \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ \lambda x{:}\alpha.\ e,$$

where α is fresh.

Besides separating the mechanisms of functional abstraction and alternation, the *for* construct extends the expressive power of the language by providing a *name* for the "current choice" being made by the type checker:

```
> for A in Int,Real.
>   \\B<A. \f:A->B. \x:A.
>     f (double x);
it : All B<Real. (Real->B)->Real->B /\ All B<Int. (Int->B)->Int->B
```

Indeed, the finer control over alternation allowed by the explicit *for* construct may be used to improve the efficiency of typechecking even for first-order languages with intersections, like Forsythe. For example, Forsythe's generalized λ-abstraction allows the definition of polynomial functions like the following:

```
> poly =
>   \w:Int,Real. \x:Int,Real. \y:Int,Real. \z:Int,Real.
>       plus (double x) (plus (plus w y) z);
poly : Real->Real->Real->Real->Real /\ Int->Int->Int->Int->Int
```

But the behavior of the typechecker on this program is unnecessarily inefficient. It is easy to see, from the types of `plus` and `double`, that when all the arguments to `poly` have type `Int`, the result type will be `Int`, and that otherwise the result type will be `Real`. So if we choose `Real` for the type of any of the four parameters, we might as well choose `Real` for the others too. We can realize a substantial gain in typechecking efficiency by making this observation explicit with a *for* expression:

```
> poly =
>   for A in Int,Real.
>      \w:A. \x:A. \y:A. \z:A.
>          plus (double x) (plus (plus w y) z);
poly : Real->Real->Real->Real->Real /\ Int->Int->Int->Int->Int
```

The second version of `poly` requires that the body be checked only twice, as compared to sixteen times for the first version.

3.2 Syntax, Subtyping, and Typing

We now give a precise definition of the $F_\wedge$ calculus, which forms the main object of study for the remainder of the paper. Since all of its components have already been discussed in detail, we present just the bare facts here. (These definitions are also summarized in Appendix A for quick reference.)

3.2.1. Definition: The set of $F_\wedge$ types is defined by the following grammar:

$$
\begin{array}{lll}
\tau & ::= & \alpha \\
 & | & \tau_1 \rightarrow \tau_2 \\
 & | & \forall\alpha{\leq}\tau_1.\ \tau_2 \\
 & | & \bigwedge[\tau_1..\tau_n]
\end{array}
$$

The set of $F_\wedge$ terms is defined by the following grammar:

$$
\begin{array}{lll}
e & ::= & x \\
 & | & \lambda x{:}\tau.\ e \\
 & | & e_1\ e_2 \\
 & | & \Lambda\alpha{\leq}\tau.\ e \\
 & | & e[\tau] \\
 & | & \mathit{for}\ \alpha\ \mathit{in}\ \tau_1..\tau_n.\ e
\end{array}
$$

3.2.2. Definition: The three-place $F_\wedge$ *subtype relation* $\Gamma \vdash \sigma \leq \tau$ is the least relation closed under the following rules:

$$\Gamma \vdash \tau \leq \tau \qquad \text{(SUB-REFL)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \tau_2 \qquad \Gamma \vdash \tau_2 \leq \tau_3}{\Gamma \vdash \tau_1 \leq \tau_3} \qquad \text{(SUB-TRANS)}$$

$$\Gamma \vdash \alpha \leq \Gamma(\alpha) \qquad \text{(SUB-TVAR)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \sigma_1 \rightarrow \sigma_2 \leq \tau_1 \rightarrow \tau_2} \qquad \text{(SUB-ARROW)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma, \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \forall\alpha{\leq}\sigma_1.\ \sigma_2 \leq \forall\alpha{\leq}\tau_1.\ \tau_2} \tag{Sub-All}$$

$$\frac{\text{for all } i,\ \Gamma \vdash \sigma \leq \tau_i}{\Gamma \vdash \sigma \leq \bigwedge[\tau_1..\tau_n]} \tag{Sub-Inter-G}$$

$$\Gamma \vdash \bigwedge[\tau_1..\tau_n] \leq \tau_i \tag{Sub-Inter-LB}$$

$$\Gamma \vdash \bigwedge[\sigma{\to}\tau_1 \,..\, \sigma{\to}\tau_n] \leq \sigma \to \bigwedge[\tau_1..\tau_n] \tag{Sub-Dist-IA}$$

$$\Gamma \vdash \bigwedge[\forall\alpha{\leq}\sigma.\ \tau_1 \,..\, \forall\alpha{\leq}\sigma.\ \tau_n] \leq \forall\alpha{\leq}\sigma.\ \bigwedge[\tau_1..\tau_n] \tag{Sub-Dist-IQ}$$

3.2.3. Definition: The three-place $F_\wedge$ *typing relation* $\Gamma \vdash e \in \tau$ is the least relation closed under the following rules:

$$\Gamma \vdash x \in \Gamma(x) \tag{Var}$$

$$\frac{\Gamma, x{:}\tau_1 \vdash e \in \tau_2}{\Gamma \vdash \lambda x{:}\tau_1.\ e \in \tau_1{\to}\tau_2} \tag{Arrow-I}$$

$$\frac{\Gamma \vdash e_1 \in \tau_1{\to}\tau_2 \qquad \Gamma \vdash e_2 \in \tau_1}{\Gamma \vdash e_1\, e_2 \in \tau_2} \tag{Arrow-E}$$

$$\frac{\Gamma, \alpha{\leq}\tau_1 \vdash e \in \tau_2}{\Gamma \vdash \Lambda\alpha{\leq}\tau_1.\ e \in \forall\alpha{\leq}\tau_1.\ \tau_2} \tag{All-I}$$

$$\frac{\Gamma \vdash e \in \forall\alpha{\leq}\tau_1.\ \tau_2 \qquad \Gamma \vdash \tau \leq \tau_1}{\Gamma \vdash e[\tau] \in \{\tau/\alpha\}\tau_2} \tag{All-E}$$

$$\frac{\Gamma \vdash \{\sigma_i/\alpha\}e \in \tau_i}{\Gamma \vdash \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e \in \tau_i} \tag{For}$$

$$\frac{\text{for all } i,\ \Gamma \vdash e \in \tau_i}{\Gamma \vdash e \in \bigwedge[\tau_1..\tau_n]} \tag{Inter-I}$$

$$\frac{\Gamma \vdash e \in \tau_1 \qquad \Gamma \vdash \tau_1 \leq \tau_2}{\Gamma \vdash e \in \tau_2} \tag{Sub}$$

When necessary to prevent confusion, turnstiles in $F_\wedge$ derivations are written $\overset{\wedge}{\vdash}$.

3.3 Discussion

We pause now to discuss some design choices that arise in the formulation of $F_\wedge$ and explore some of its properties.

3.3.1 *Top* vs. $\top$

In forming $F_\wedge$ from $\lambda_\wedge$ and $F_\leq$, we find, pleasantly, that most of their features are quite orthogonal: for a given feature, either it is found already in $\lambda_\leq$ or else it exists in either $\lambda_\wedge$ or $F_\leq$ in a form that interacts smoothly with all the features of the other. The one exception is the maximal types $\top$ and *Top*. In the best case, we might hope that these would coincide in $F_\wedge$, but this, unfortunately, is not the case.

The difference arises from the Inter-I rule of $\lambda_\wedge$, which, in its nullary form, states that any term whatsoever has type $\top$. $F_\leq$ has no such rule: the only way a term e can be assigned type *Top* is by the rules Sub and Sub-Top, which require that the term already have some type σ with $\sigma \leq \tau$. In other words,

- *Top* is the type of all *well-typed* terms;
- $\top$ is the type of *all* terms.

Order-theoretically, the two types are equivalent (each is a subtype of the other), since each is explicitly axiomatized as a maximal type.

For the sake of conceptual parsimony, we drop *Top* here and retain $\top$, since $\top$ can perform the same jobs as *Top* (in particular, it allows unbounded quantification to be recovered from bounded quantification), while requiring no extra typing or subtyping rules beyond those defining the behavior of general n-ary intersections.

The alternative system with both $\top$ and *Top*, though messier and probably not much more expressive than $F_\wedge$, makes reasonable syntactic sense and does not seem much harder to typecheck. More interesting, though, would be the system with *Top* instead of $\top$, where intersections are restricted to two or more elements: this language would have much of the practical expressiveness of $F_\wedge$ while avoiding the unfamiliar notion of a "type of all terms, even ill-behaved ones": this system supports the notion of *typechecking failure*, which in $F_\wedge$ is simply identified with $\top$.

3.3.2 Encoding Primitive Subtyping

As in $F_\leq$, both term and type constants are absent from $F_\wedge$, and programs involving them are expressed as terms with free variables whose typing and subtyping behavior are declared in a pervasive context Γ_P.

The presence of intersection types allows a greater variety of primitive subtype relations to be encoded in this way than was possible in $F_\leq$. For example, the relation

$$\begin{tikzcd}
 & Value & \\
Int \arrow[ur] & & Bool \arrow[ul] \\
 & Bit \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

is represented by the pervasive context

$\Gamma_P \equiv Value{\leq}\top,\ Int{\leq}Value,\ Bool{\leq}Value,\ Bit{\leq}Int{\wedge}Bool.$

Primitive subtype order structures that are not partially ordered, such as

$$PolarComplex \rightleftarrows RectComplex$$

are still not expressible, though.

The encodability of primitive subtype relations can be stated formally as follows:

3.3.2.1. Definition: A *topological sort* of a finite collection of primitive types P is a bijective mapping $index_P \in P \to \{1\,..\,|P|\}$ such that $\alpha \leq_P \beta$ implies $index_P(\alpha) \geq index_P(\beta)$.

3.3.2.2. Definition: Let P be a collection of primitive types topologically sorted by $index_P$. Let $\alpha_i \equiv index_P^{-1}(i)$. Then P is *encoded* by the following $F_\wedge$ context:

$\Gamma_P = \ldots,\ \alpha_i\ \leq\ \bigwedge[\gamma \in P \mid \alpha_i{\leq_P}\gamma],\ \ldots$

Note that every finite partial order can be topologically sorted.

3.3.2.3. Lemma: Let Γ be an $\lambda_\wedge$ context and assume that the primitive subtype relation $\leq_P$ can be topologically sorted by some function $index_P$. If $\Gamma \vdash^{\lambda\wedge} \sigma \leq \tau$, then $\Gamma_P, \Gamma \vdash^{\wedge} \sigma \leq \tau$.

Proof: By induction on the structure of the given derivation. All of the $\lambda_\wedge$ rules translate directly into $F_\wedge$ rules, except for SUB-PRIM; an instance of this rule with conclusion $\Gamma \vdash \alpha \leq \beta$ is translated into the following $F_\wedge$ derivation:

$$\dfrac{\dfrac{}{\Gamma_P, \Gamma \overset{\wedge}{\vdash} \alpha \leq \bigwedge[\gamma \in P \mid \alpha \leq_P \gamma]}\;(\text{SUB-TVAR}) \qquad \dfrac{}{\Gamma_P, \Gamma \overset{\wedge}{\vdash} \bigwedge[\gamma \in P \mid \alpha \leq_P \gamma] \leq \beta}\;(\text{SUB-INTER-LB})}{\Gamma_P, \Gamma \overset{\wedge}{\vdash} \alpha \leq \beta.}\;(\text{SUB-TRANS})$$

□

3.3.2.4. Lemma: Let Γ by a $\lambda_\wedge$ context and assume that the primitive subtype relation $\leq_P$ can be topologically sorted by some function $index_P$. Then $\Gamma \overset{\lambda\wedge}{\vdash} e \in \tau$ only if $\Gamma_P, \Gamma \overset{\wedge}{\vdash} e \in \tau$.

(In fact, the derivation-normalization results of the following section can be used to show the converse, so $\Gamma \overset{\lambda\wedge}{\vdash} e \in \tau$ iff $\Gamma_P, \Gamma \overset{\wedge}{\vdash} e \in \tau$.)

4 Examples

Intersection types allow very refined types to be assigned to expressions — much more refined than is possible in conventional polymorphic languages. Instead of a single description, each expression may be assigned any finite collection of descriptions, each capturing some aspect of its behavior. Since we are working in an explicitly typed calculus, this requires effort from the programmer in the form of type assumptions or annotations; in general, as more effort is expended, better typings are obtained.

Many functional languages provide a primitive type `Bool` with two elements, `true` and `false`. Here we can introduce two subtypes of `Bool`, called `True` and `False` and give more exact types for the constants `true` and `false` in terms of these refinements:

```
> Bool < T,
> True < Bool,
> False < Bool;
```

```
> true : True,
> false : False;
```

The polymorphic `if` primitive can also be given a more refined type: if we know whether the value of the test lies in the type `True` or the type `False`, we can tell in advance which of the branches will be chosen. An optimizing compiler might use this information to generate more efficient code.

```
> if : All A.    (True -> A -> T -> A)
>             /\ (False -> T -> A -> A)
>             /\ (Bool -> A -> A -> A);
```

(The third typing is needed here because $F_\wedge$'s types cannot express the idea that every element of `Bool` is an element of either `True` or `False`. This shortcoming, while not serious in practice, has motivated the investigation of a dual notion of *union types* [1, 49, 63].) The refinement in the types of `true`, `false`, and `if` can now be exploited in typing new functions:

```
> or =
>    \x:True,False,Bool. \y:True,False,Bool.
>       for R in True,False,Bool.
>          if [R] x true y;
or : Bool->(Bool->Bool/\True->True)
```

```
  /\ False->False->False
  /\ True->Bool->True
```

In fact, we can carry out the same construction in the *pure* $F_\wedge$ calculus with no assumptions about predefined types or constants, using a generalization of the familiar Church encoding of booleans in the λ-calculus.

```
> True  == All B. All TT<B. All FF<B. TT -> T  -> TT,
> False == All B. All TT<B. All FF<B. T  -> FF -> FF,
> Bool  == All B. All TT<B. All FF<B. TT -> FF -> B;
```

```
> true = \\B. \\TT<B. \\FF<B. \x:TT. \y:T. x,
> false = \\B. \\TT<B. \\FF<B. \x:T. \y:FF. y;
true : True
false : False
```

```
> or = for M in True,False,Bool.
>        for N in True,False,Bool.
>          \m:M. \n:N.
>             m [Bool] [True] [N] true n;
or : Bool->Bool->Bool
  /\ False->(False->False/\True->True)
  /\ True->Bool->True
```

5 Typechecking

This section develops the proof theory of the $F_\wedge$ calculus, leading up to the definition and correctness proof of an algorithm for synthesizing minimal types of $F_\wedge$ terms. The major results we establish are as follows:

- We give an alternative formulation of the subtype relation in terms of "canonical types," where intersections appear only on the left of arrows and quantifiers. This formulation is equivalent to the original, in the sense that there is some canonical type in the equivalence class of each ordinary type. More formally, the "flattening" map from ordinary to canonical types both preserves and reflects derivability of subtyping statements.
- A proof-normalization argument based on the one used by Curien and Ghelli [38] shows that every derivable canonical subtyping statement has a "normal form" derivation with a particular, restricted shape.
- The existence of normal-form canonical derivations is used to prove the semi-completeness of a syntax-directed algorithm for checking the subtype relation.
- The soundness of a syntax-directed type synthesis algorithm for $F_\wedge$ terms is established by showing that there exist finite bases for the collections of arrow types and quantified types lying above a given type. This argument also shows that the subroutine for checking the subtype relation is the only source of possible nontermination in the typechecking algorithm.
- The shapes of the typing derivations discovered by this algorithm are used to prove that $F_\wedge$ is a conservative extension of the first-order intersection calculus $\lambda_\wedge$. (Because of the different behavior of *Top* and $\top$, however, $F_\leq$ cannot similarly be embedded in $F_\wedge$.)

5.1 Linear Notation for Derivations

It will often be convenient to have a linear notation for typing and subtyping derivations, so that operations on proofs such as cut-elimination transformations can be expressed as textual rules rather than as pictures. Our notation is a modified version of Curien and Ghelli's [38].

5.1.1. Definition: The sets of *subtyping derivation abbreviations* c and *typing derivation abbreviations* s are defined by the following abstract grammar:

$$
\begin{array}{lcl}
c & ::= & id \\
 & \mid & c_1 \,;\, c_2 \\
 & \mid & V_\alpha \\
 & \mid & c_1 {\rightarrow} c_2 \\
 & \mid & \forall\alpha{\leq}c_1.\ c_2 \\
 & \mid & \langle c_1 \,..\, c_n \rangle \\
 & \mid & proj_i \\
 & \mid & dist\text{-}ia \\
 & \mid & dist\text{-}iq
\end{array}
$$

$$
\begin{array}{lcl}
s & ::= & V_x \\
 & \mid & \lambda x{:}\sigma.\ s \\
 & \mid & s_1\ s_2 \\
 & \mid & \Lambda\alpha{\leq}\sigma.\ s \\
 & \mid & s\ [c] \\
 & \mid & for\ \alpha\ in\ \sigma_1..\sigma_n.\ s_i \\
 & \mid & \langle s_1 \,..\, s_n \rangle \\
 & \mid & c \upharpoonright s
\end{array}
$$

5.1.2. Definition: The translation function $(\text{—})^\dagger$, which maps derivation trees to their abbreviated forms, is defined as follows. (Recall that $c :: J$ is read as "c is a derivation whose conclusion is the judgement J.")

$$\left(\frac{\scriptstyle\text{(SUB-REFL)}}{\Gamma \vdash \tau \leq \tau}\right)^\dagger \quad = \quad id$$

$$\left(\frac{c_1 :: \Gamma \vdash \tau_1 \leq \tau_2 \qquad c_2 :: \Gamma \vdash \tau_2 \leq \tau_3}{\Gamma \vdash \tau_1 \leq \tau_3}\ \scriptstyle\text{(SUB-TRANS)}\right)^\dagger \quad = \quad c_1^\dagger \,;\, c_2^\dagger$$

$$\left(\frac{\scriptstyle\text{(SUB-TVAR)}}{\Gamma \vdash \alpha \leq \Gamma(\alpha)}\right)^\dagger \quad = \quad V_\alpha$$

$$\left(\frac{c_1 :: \Gamma \vdash \tau_1 \leq \sigma_1 \qquad c_2 :: \Gamma \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \sigma_1{\rightarrow}\sigma_2 \leq \tau_1{\rightarrow}\tau_2}\ \scriptstyle\text{(SUB-ARROW)}\right)^\dagger \quad = \quad c_1^\dagger{\rightarrow}c_2^\dagger$$

$$\left(\frac{c_1 :: \Gamma \vdash \tau_1 \leq \sigma_1 \qquad c_2 :: \Gamma,\, \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \forall\alpha{\leq}\sigma_1.\ \sigma_2 \leq \forall\alpha{\leq}\tau_1.\ \tau_2}\ \scriptstyle\text{(SUB-ALL)}\right)^\dagger \quad = \quad \forall\alpha{\leq}c_1^\dagger.\ c_2^\dagger$$

$$\left(\frac{\text{for all } i,\ c_i :: \Gamma \vdash \sigma \leq \tau_i}{\Gamma \vdash \sigma \leq \bigwedge[\tau_1..\tau_n]}\ \scriptstyle\text{(SUB-INTER-G)}\right)^\dagger \quad = \quad \langle c_1^\dagger..c_n^\dagger \rangle$$

$$\left(\frac{\scriptstyle\text{(SUB-INTER-LB)}}{\Gamma \vdash \bigwedge[\tau_1..\tau_n] \leq \tau_i}\right)^\dagger \quad = \quad proj_i$$

$$\left(\frac{\text{(SUB-DIST-IA)}}{\Gamma \vdash \bigwedge[\sigma{\rightarrow}\tau_1 \mathinner{..} \sigma{\rightarrow}\tau_n] \leq \sigma \rightarrow \bigwedge[\tau_1..\tau_n]}\right)^\dagger \quad = \quad \mathit{dist\text{-}ia}$$

$$\left(\frac{\text{(SUB-DIST-IQ)}}{\Gamma \vdash \bigwedge[\forall\alpha{\leq}\sigma.\ \tau_1 \mathinner{..} \forall\alpha{\leq}\sigma.\ \tau_n] \leq \forall\alpha{\leq}\sigma.\ \bigwedge[\tau_1..\tau_n]}\right)^\dagger \quad = \quad \mathit{dist\text{-}iq}$$

$$\left(\frac{\text{(VAR)}}{\Gamma \vdash x \in \Gamma(x)}\right)^\dagger \quad = \quad V_x$$

$$\left(\frac{s :: \Gamma,\, x{:}\tau_1 \vdash e \in \tau_2}{\Gamma \vdash \lambda x{:}\tau_1.\ e \in \tau_1{\rightarrow}\tau_2}\ \text{(ARROW-I)}\right)^\dagger \quad = \quad \lambda x{:}\tau_1.\ s^\dagger$$

$$\left(\frac{s_1 :: \Gamma \vdash e_1 \in \tau_1{\rightarrow}\tau_2 \qquad s_2 :: \Gamma \vdash e_2 \in \tau_1}{\Gamma \vdash e_1\ e_2 \in \tau_2}\ \text{(ARROW-E)}\right)^\dagger \quad = \quad s_1^\dagger\ s_2^\dagger$$

$$\left(\frac{s :: \Gamma,\, \alpha{\leq}\tau_1 \vdash e \in \tau_2}{\Gamma \vdash \Lambda\alpha{\leq}\tau_1.\ e \in \forall\tau_1.\ \tau_2}\ \text{(ALL-I)}\right)^\dagger \quad = \quad \Lambda\alpha{\leq}\tau_1.\ s^\dagger$$

$$\left(\frac{s :: \Gamma \vdash e \in \forall\alpha{\leq}\tau_1.\ \tau_2 \qquad c :: \Gamma \vdash \tau \leq \tau_1}{\Gamma \vdash e\ [\tau] \in \{\tau/\alpha\}\tau_2}\ \text{(ALL-E)}\right)^\dagger \quad = \quad s^\dagger\ [c^\dagger]$$

$$\left(\frac{s_i :: \Gamma \vdash \{\sigma_i/\alpha\}e \in \tau_i}{\Gamma \vdash \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e \in \tau_i}\ \text{(FOR)}\right)^\dagger \quad = \quad \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ s_i^\dagger$$

$$\left(\frac{\text{for all } i,\ s_i :: \Gamma \vdash e \in \tau_i}{\Gamma \vdash e \in \bigwedge[\tau_1..\tau_n]}\ \text{(INTER-I)}\right)^\dagger \quad = \quad \langle s_i^\dagger..s_n^\dagger\rangle$$

$$\left(\frac{s :: \Gamma \vdash e \in \sigma \qquad c :: \Gamma \vdash \sigma \leq \tau}{\Gamma \vdash e \in \tau}\ \text{(SUB)}\right)^\dagger \quad = \quad s^\dagger \uparrow c^\dagger$$

For example, the subtyping derivation

$$\frac{\dfrac{\text{(SUB-TVAR)}}{\Gamma_P \ \vdash\ \mathit{Int}\ \leq\ \mathit{Real}} \qquad \dfrac{\dfrac{\text{(SUB-REFL)}}{\Gamma_P,\, \alpha{\leq}\mathit{Int}\ \vdash\ \alpha\ \leq\ \alpha} \qquad \dfrac{\text{(SUB-INTER-G)}}{\Gamma_P,\, \alpha{\leq}\mathit{Int}\ \vdash\ \mathit{Int}\ \leq\ \top}}{\Gamma_P,\, \alpha{\leq}\mathit{Int}\ \vdash\ \alpha{\rightarrow}\mathit{Int}\ \leq\ \alpha{\rightarrow}\top}\ \text{(SUB-ARROW)}}{\Gamma_P\ \vdash\ \forall\alpha{\leq}\mathit{Real}.\ \alpha{\rightarrow}\mathit{Int}\ \leq\ \forall\alpha{\leq}\mathit{Int}.\ \alpha{\rightarrow}\top}\ \text{(SUB-ALL)}$$

is abbreviated as

$\forall\alpha{\leq}V_{Int}.\ id{\rightarrow}\langle\rangle.$

Strictly speaking, our linear abbreviations should contain sufficient information that they uniquely determine proof trees; in other words, $(\text{—})^\dagger$ should be injective. Clearly, we could decorate our linear abbreviations with additional information and extend $(\text{—})^\dagger$ to a bijection. For example, each abbreviation could include an explicit indication of the judgement it derives. However, this would make the abbreviations much larger and less readable, eliminating most of the benefit of introducing them in the first place. We therefore use the present abbreviatory forms *as if* they contained sufficient information to unique determine derivation trees, relying on the reader to supply the necessary annotations.

When we need to be explicit about the conclusion of a derivation written in linear form, we use the notation $c :: J$.

5.2 Basic Properties

We begin by establishing some basic proof-theoretic properties of the subtype relation $\Gamma \vdash \sigma \leq \tau$ and the typing relation $\Gamma \vdash e \in \tau$. First, we state some useful derived rules of inference.

5.2.1. Lemma:

$$\Gamma \vdash \bigwedge[\sigma{\rightarrow}\tau_1 \mathinner{..} \sigma{\rightarrow}\tau_n] \sim \sigma \rightarrow \bigwedge[\tau_1 \mathinner{..} \tau_n] \qquad \text{(D-DIST-IA)}$$

$$\Gamma \vdash \bigwedge[\forall\alpha{\leq}\sigma.\ \tau_1 \mathinner{..} \forall\alpha{\leq}\sigma.\ \tau_n] \sim \forall\alpha{\leq}\sigma.\ \bigwedge[\tau_1 \mathinner{..} \tau_n] \qquad \text{(D-DIST-IQ)}$$

Proof: Straightforward. □

5.2.2. Lemma:

$$\Gamma \vdash \bigwedge[\bigwedge T_1 \mathinner{..} \bigwedge T_n] \sim \bigwedge(T_1 * \cdots * T_n) \qquad \text{(D-ABSORB)}$$

$$\frac{T \text{ and } T' \text{ enumerate the same finite set}}{\Gamma \vdash \bigwedge T \sim \bigwedge T'} \qquad \text{(D-REINDEX)}$$

$$\frac{\text{for all } \tau_j \text{ there is some } \sigma_i \text{ such that } \Gamma \vdash \sigma_i \leq \tau_j}{\Gamma \vdash \bigwedge[\sigma_1 \mathinner{..} \sigma_m] \leq \bigwedge[\tau_1 \mathinner{..} \tau_n]} \qquad \text{(D-ALL-SOME)}$$

Proof: Straightforward. □

5.2.3. Lemma: [Permutation] If Γ' is a permutation of Γ and both Γ and Γ' are closed, then

1. $\Gamma \vdash \sigma \leq \tau$ iff $\Gamma' \vdash \sigma \leq \tau$
2. $\Gamma \vdash e \in \tau$ iff $\Gamma' \vdash e \in \tau$.

Proof: By induction on derivations. (Note, furthermore, that the antecedent and consequent derivations are isomorphic.) □

Lemma 5.2.3 justifies a notational simplification: two closed contexts Γ and Γ' that differ only in the order of their bindings will be considered *identical* from now on.

5.2.4. Lemma: [Weakening] If Γ_1, Γ_2 is closed and $\Gamma_1 \vdash \sigma \leq \tau$, then $\Gamma_1, \Gamma_2 \vdash \sigma \leq \tau$.

Proof: By induction on the structure of a derivation of $\Gamma_1 \vdash \sigma \leq \tau$. At each stage of the induction, we proceed by a case analysis on the rule used in the last step of the derivation. The most interesting case is SUB-ALL:

Case Sub-All: $\sigma \equiv \forall\alpha{\leq}\sigma_1.\ \sigma_2 \qquad \tau \equiv \forall\alpha{\leq}\tau_1.\ \tau_2$

By assumption, $\Gamma_1 \vdash \tau_1 \leq \sigma_1$ and $\Gamma_1, \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2$. We may also assume that $\alpha \notin dom(\Gamma_1, \Gamma_2)$. Then $\Gamma_1, \Gamma_2, \alpha{\leq}\tau_1$ is closed, and, by the induction hypothesis, $\Gamma_1, \Gamma_2 \vdash \tau_1 \leq \sigma_1$ and $\Gamma_1, \Gamma_2, \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2$. By SUB-ALL, $\Gamma_1, \Gamma_2 \vdash \forall\alpha{\leq}\sigma_1.\ \sigma_2 \leq \forall\alpha{\leq}\tau_1.\ \tau_2$. □

A different kind of weakening lemma will also be needed. Rather than adding a new variable to the context, this one states that a derivable subtyping statement remains derivable when the bounds of some of the existing type variables are replaced by "narrower" bounds.

5.2.5. Lemma: [Narrowing] Let Γ and Γ' be closed contexts such that, for each $\alpha_i \in dom(\Gamma)$, $\Gamma' \vdash \Gamma'(\alpha_i) \leq \Gamma(\alpha_i)$. Then $\Gamma \vdash \sigma \leq \tau$ implies $\Gamma' \vdash \sigma \leq \tau$.

Proof: See Appendix B. □

Using narrowing, we can show that the equivalence relation induced by the subtype relation is a congruence:

5.2.6. Lemma:

$$\frac{\Gamma \vdash \tau_1 \sim \tau_1' \qquad \Gamma \vdash \tau_2 \sim \tau_2'}{\Gamma \vdash \tau_1 \rightarrow \tau_2 \sim \tau_1' \rightarrow \tau_2'} \qquad \text{(D-Cong-Arrow)}$$

$$\frac{\Gamma \vdash \tau_1 \sim \tau_1' \qquad \Gamma, \alpha \leq \tau_1' \vdash \tau_2 \sim \tau_2'}{\Gamma \vdash \forall \alpha \leq \tau_1.\ \tau_2 \sim \forall \alpha \leq \tau_1'.\ \tau_2'} \qquad \text{(D-Cong-All)}$$

$$\frac{\text{for all } i,\ \Gamma \vdash \tau_i \sim \tau_i'}{\Gamma \vdash \bigwedge[\tau_1..\tau_n] \sim \bigwedge[\tau_1'..\tau_n']} \qquad \text{(D-Cong-Inter)}$$

Proof: Easy except for D-Cong-All, which requires narrowing. □

5.2.7. Lemma: [Subtyping Substitution] If $\Gamma_1,\ \alpha \leq \psi,\ \Gamma_2 \vdash \sigma \leq \tau$ and $\Gamma_1 \vdash \phi \leq \psi$, then $\Gamma_1, \{\phi/\alpha\}\Gamma_2 \vdash \{\phi/\alpha\}\sigma \leq \{\phi/\alpha\}\tau$.

Proof: See Appendix B. □

We would also like to show that whenever a variable α or x in $dom(\Gamma)$ is unused in a statement $\Gamma \vdash \sigma \leq \tau$ or $\Gamma \vdash e \in \tau$, we may drop it from Γ without affecting derivability. Because the rule Sub-Trans allows subtyping derivations that can contain internal uses of arbitrary types, we cannot prove this property for type variables with the machinery we have developed so far (it will be an easy corollary of Theorem 5.3.8.10). But for term variables it is straightforward:

5.2.8. Lemma: [Term variable strengthening]

1. If $\Gamma, x{:}\theta \vdash \sigma \leq \tau$, then $\Gamma \vdash \sigma \leq \tau$.
2. If $\Gamma, x{:}\theta \vdash e \in \tau$ and $x \notin FV(e)$, then $\Gamma \vdash e \in \tau$.

Proof: By induction on derivations. □

5.2.9. Lemma: [Term substitution] If $\Gamma, x{:}\sigma \vdash f \in \tau$ and $\Gamma \vdash v \in \sigma$, then $\Gamma \vdash \{v/x\}f \in \tau$.

Proof: By induction on a derivation of $\Gamma,\ x{:}\sigma \vdash f \in \tau$, using weakening for the Arrow-I and All-I cases and term strengthening for the All-E and Sub cases. □

5.2.10. Lemma: [Type substitution in terms] If $\Gamma_1,\ \alpha \leq \sigma,\ \Gamma_2 \vdash f \in \tau$, then $\Gamma_1,\ \{\sigma/\alpha\}\Gamma_2 \vdash \{\sigma/\alpha\}f \in \{\sigma/\alpha\}\tau$.

Proof: By induction on a derivation of $\Gamma_1,\ \alpha \leq \sigma,\ \Gamma_2 \vdash f \in \tau$, using the subtyping substitution lemma for the All-E and Sub cases. □

5.3 Subtyping

In this section, we give a straightforward semi-decision procedure for the $F_\wedge$ subtype relation. This relation can be shown to be undecidable [64], so a semi-decision procedure is the best we can hope for; however, the same algorithm forms a decision procedure for some useful fragments of $F_\wedge$ (see Section 7).

We present the algorithm as a collection of syntax-directed rules and then show that the relation defined by these rules coincides with $F_\wedge$. It is technically convenient to make this argument using an intermediate representation called *canonical types*, roughly analogous to conjunctive-normal-form formulas in logic:

- We identify the set of canonical types (Section 5.3.1) and define a canonical subtyping relation (marked $\overset{\flat}{\vdash}$) over this set (Section 5.3.2).
- We show (Sections 5.3.3 and 5.3.4) that derivations of canonical subtyping statements can be transformed into *normal form* derivations of a certain restricted shape (Section 5.3.6).

- We give a *flattening transformation* $\flat$ mapping $F_\wedge$ types into canonical types (Section 5.3.7) and show that

$$\Gamma \vdash \sigma \leq \tau \quad \text{iff} \quad \Gamma^\flat \vdash^\flat \sigma^\flat \leq \tau^\flat.$$

- Finally, we define a syntax-directed subtyping relation on ordinary types (marked $\dot\vdash$) and show (Section 5.3.8) that it coincides with canonical subtyping after flattening:

$$\Gamma^\flat \vdash^\flat \sigma^\flat \leq \tau^\flat \quad \text{iff} \quad \Gamma \dot\vdash \sigma \leq \tau$$

5.3.1 Canonical Types

We might naively hope to develop an algorithm for checking $F_\wedge$ subtyping simply by extending the $F_\leq$ subtyping algorithm $F_\leq^N$ to include a case for intersections. Keeping cases *1* to *5* as before, the complete algorithm would then be:

check$(\Gamma \vdash \sigma \leq \tau)$ =
1. *if* $\tau \equiv$ *Top*
 then true
2. *else if* $\sigma \equiv \sigma_1 \rightarrow \sigma_2$ *and* $\tau \equiv \tau_1 \rightarrow \tau_2$
 then *check*$(\Gamma \vdash \tau_1 \leq \sigma_1)$
 and check$(\Gamma \vdash \sigma_2 \leq \tau_2)$
3. *else if* $\sigma \equiv \forall\alpha{\leq}\sigma_1.\ \sigma_2$ *and* $\tau \equiv \forall\alpha{\leq}\tau_1.\ \tau_2$
 then *check*$(\Gamma \vdash \tau_1 \leq \sigma_1)$
 and check$(\Gamma, \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2)$
4. *else if* $\sigma \equiv \alpha$ *and* $\tau \equiv \alpha$
 then true
5. *else if* $\sigma \equiv \alpha$
 then check$(\Gamma \vdash \Gamma(\alpha) \leq \tau)$
6. *else if* $\sigma \equiv \bigwedge[\sigma_1..\sigma_m]$ *and* $\tau \equiv \bigwedge[\tau_1..\tau_n]$
 then for each τ_i
 choose some σ_j
 such that check$(\Gamma \vdash \sigma_j \leq \tau_i)$
n. *else*
 false.

That is, to check whether $\bigwedge[\sigma_1..\sigma_m]$ is a subtype of $\bigwedge[\tau_1..\tau_n]$, check that for each τ_i there is some σ_j such that $\sigma_j \leq \tau_i$. The selection of the σ_j is expressed here as a nondeterministic choice; in practice, this is implemented using backtracking.

But case 6, though clearly sound (Lemma 5.2.2), is not complete, since there are many cases where a meet lies above or below a type that does not have the form of a meet. For example,

$$\alpha{\leq}\top \vdash \alpha \leq \bigwedge[\alpha]$$
$$\alpha{\leq}\top \vdash \bigwedge[\alpha] \leq \alpha.$$

These two cases can be handled by splitting the proposed rule into two,

6a. *else if* $\tau \equiv \bigwedge[\tau_1..\tau_n]$
 then for each τ_i
 check$(\Gamma \vdash \sigma \leq \tau_i)$
6b. *else if* $\sigma \equiv \bigwedge[\sigma_1..\sigma_m]$
 then choose some σ_j
 such that check$(\Gamma \vdash \sigma_j \leq \tau)$,

but we must be careful to apply *6a* before *6b* in order to respond correctly to the input

$$\alpha{\leq}\top,\, \beta{\leq}\top \;\vdash\; \bigwedge[\alpha, \beta] \;\leq\; \bigwedge[\alpha, \beta].$$

Unfortunately, the real problem is more subtle than this: in the presence of the distributivity axioms Sub-Dist-IA and Sub-Dist-IQ, steps *2* and *3* of the $F^{N}_{\leq}$ algorithm are also incomplete. For example, the judgement

$$\alpha{\leq}\top,\, \beta{\leq}\top \;\vdash\; \alpha{\to}\alpha \;\leq\; \beta{\to}\top,$$

is derivable (using Sub-Dist-IA and Sub-Trans, with intermediate type $\top$), although

$$\alpha{\leq}\top,\, \beta{\leq}\top \;\nvdash\; \beta \;\leq\; \alpha.$$

To get matters under control, we need to deal with the distributivity laws before doing anything else. We take the inverses of these laws (i.e., the other half of the equivalences D-Dist-IA and D-Dist-IQ given in 5.2.1) as rewrite rules,

$$\begin{array}{lcl} \sigma \;\to\; \bigwedge[\tau_1..\tau_n] & \longrightarrow & \bigwedge[\sigma{\to}\tau_1\,..\,\sigma{\to}\tau_n] \\ \forall\alpha{\leq}\sigma.\ \bigwedge[\tau_1..\tau_n] & \longrightarrow & \bigwedge[\forall\alpha{\leq}\sigma.\ \tau_1\,..\,\forall\alpha{\leq}\sigma.\ \tau_n], \end{array}$$

and apply them to a given $F_\wedge$ type as many times as possible to obtain an equivalent type with no intersections on the right-hand sides of arrows or quantifiers. For example, the type

$$\bigwedge[\alpha_1,\, \alpha_2] \;\to\; \bigwedge[\alpha_3,\, (\forall\beta{\leq}\alpha_4.\ \bigwedge[\alpha_5,\, \alpha_6])]$$

becomes

$$\begin{array}{l} \bigwedge[\bigwedge[\alpha_1,\, \alpha_2] \;\to\; \alpha_3, \\ \quad \bigwedge[\bigwedge[\alpha_1,\, \alpha_2] \;\to\; \forall\beta{\leq}\alpha_4.\ \alpha_5, \\ \quad\quad \bigwedge[\alpha_1,\, \alpha_2] \;\to\; \forall\beta{\leq}\alpha_4.\ \alpha_6]]. \end{array}$$

Since this type contains no meets on the right-hand sides of arrows or quantifiers, there is no way to use it (or any subphrase) in an instance of either of the distributivity rules.

Once the distributivity rules are eliminated, there remain just four subtyping rules in Definition 3.2.2 that can be used to prove subtyping statements involving meets: Sub-Refl, Sub-Trans, Sub-Inter-G, and Sub-Inter-LB. The reflexivity and transitivity rules can be eliminated by a normalization argument that shows how to transform any derivation into one that applies transitivity and reflexivity only to variables (c.f. Sections 5.3.4–5.3.6). This leaves just Sub-Inter-G and Sub-Inter-LB, which are accurately captured by our rules *6a* and *6b*.

In fact, it is convenient to work with types in an even more restricted form, in which every type has a single $\bigwedge$ as its outermost constructor and as the outermost constructor on the left-hand sides of arrows and quantifiers, and where no immediate component of a $\bigwedge$ is another $\bigwedge$. In this form, our example becomes:

$$\begin{array}{l} \bigwedge[\bigwedge[\alpha_1,\, \alpha_2] \;\to\; \alpha_3, \\ \quad \bigwedge[\alpha_1,\, \alpha_2] \;\to\; \forall\beta{\leq}\bigwedge[\alpha_4].\ \alpha_5, \\ \quad \bigwedge[\alpha_1,\, \alpha_2] \;\to\; \forall\beta{\leq}\bigwedge[\alpha_4].\ \alpha_6]. \end{array}$$

This transformation effectively separates the set of types into two syntactic classes: those whose outermost constructor is $\bigwedge$ (called "composite canonical types") and those whose outermost constructor is $\to$, $\forall$, or a variable (called "individual canonical types"). This separation is useful because our proposed rule *6* now captures *all* of the valid subtyping statements involving pairs of composite canonical types, while the original rules *2*–*5* are valid and complete for pairs of individual canonical types.

5.3.1.1. Definition: The sets of *composite canonical types* K and *individual canonical types* κ are defined by the following grammar:

$$
\begin{array}{lll}
K & ::= & \bigwedge[\kappa_1..\kappa_n] \\
\kappa & ::= & \alpha \;\;|\;\; K \rightarrow \kappa \;\;|\;\; \forall\alpha{\le}K.\ \kappa
\end{array}
$$

The metavariables K and I range over composite canonical types; κ and ι range over individual canonical types; k and i range over both sorts of canonical types. It will often be convenient to treat a composite canonical type $\bigwedge[\kappa_1..\kappa_n]$ as a finite set whose elements are the individual canonical types κ_1 through κ_n. The following conventions support this point of view:

$$
\begin{array}{lll}
\iota \in K & \stackrel{\text{def}}{=} & K \equiv \bigwedge[\kappa_1..\kappa_n] \text{ and } \iota{\equiv}\kappa_i \text{ for some } i \\
\bigwedge[F(\iota) \mid \iota \in K] & \stackrel{\text{def}}{=} & \bigwedge[F(\kappa_1)\,..\,F(\kappa_n)], \text{ where } K \equiv \bigwedge[\kappa_1..\kappa_n] \\
K \cup I & \stackrel{\text{def}}{=} & \bigwedge[\kappa_1\,..\,\kappa_m, \iota_1\,..\,\iota_n], \text{ where } K \equiv \bigwedge[\kappa_1..\kappa_m] \text{ and } I \equiv \bigwedge[\iota_1..\iota_n].
\end{array}
$$

Our canonical types are not as sparse as one could imagine. For example, we could imagine a notion of "fully canonical types" such that each $\sim$-equivalence class of types contains exactly one fully canonical type. But for present purposes, the canonical types we have defined are refined enough.

The idea of canonical types comes from a proof by Reynolds [personal communication, 1988] of the soundness and completeness of a decision procedure for the subtype relation of Forsythe [69]. (Related formulations of intersection types are studied in [30, 32, 33, 72, 75, 76].)

5.3.2 Canonical Subtyping

We now define the canonical subtype relation formally.

5.3.2.1. Definition: A *canonical context* Δ is a context whose range contains only canonical types.

5.3.2.2. Definition: The subtype relation on canonical types is defined as follows:

$$\frac{\forall i.\ \exists j.\quad \Delta \vdash \kappa_j \le \iota_i}{\Delta \vdash \bigwedge[\kappa_1..\kappa_m] \le \bigwedge[\iota_1..\iota_n]} \tag{CSub-AE}$$

$$\Delta \vdash k \le k \tag{CSub-Refl}$$

$$\frac{\Delta \vdash k_1 \le k_2 \qquad \Delta \vdash k_2 \le k_3}{\Delta \vdash k_1 \le k_3} \tag{CSub-Trans}$$

$$\frac{\Delta \vdash \Delta(\alpha) \le \bigwedge[\iota]}{\Delta \vdash \alpha \le \iota} \tag{CSub-TVar}$$

$$\frac{\Delta \vdash I_1 \le K_1 \qquad \Delta \vdash \kappa_2 \le \iota_2}{\Delta \vdash K_1{\rightarrow}\kappa_2 \le I_1{\rightarrow}\iota_2} \tag{CSub-Arrow}$$

$$\frac{\Delta \vdash I_1 \le K_1 \qquad \Delta, \alpha{\le}I_1 \vdash \kappa_2 \le \iota_2}{\Delta \vdash \forall\alpha{\le}K_1.\ \kappa_2 \le \forall\alpha{\le}I_1.\ \iota_2} \tag{CSub-All}$$

Note that individual and composite canonical types cannot be mixed in canonical subtyping statements: we have statements of the form $\Delta \vdash K \le I$ and $\Delta \vdash \kappa \le \iota$, but never $\Delta \vdash \kappa \le I$ or $\Delta \vdash K \le \iota$. Also, anticipating the requirements of the normal-form derivations to be defined in the following section, we have slightly generalized the type variable rule, in effect embedding an instance of CSub-Trans and an instance of CSub-AE in each instance of CSub-TVar. The turnstile symbol is sometimes decorated $\overset{\flat}{\vdash}$ to distinguish canonical subtyping derivations from derivations in other calculi.

Again, it is convenient to use a linear notation for canonical subtyping derivations:

5.3.2.3. Definition: The set of *canonical subtyping derivation abbreviations* is defined as follows:

$$
\begin{array}{lll}
C & ::= & AE[\xi_1..\xi_n] \\
 & | & id \\
 & | & C \,;\, C \\
 & & \\
\xi & ::= & id \\
 & | & \xi_1 \,;\, \xi_2 \\
 & | & V_\alpha(C) \\
 & | & C \rightarrow \xi \\
 & | & \forall\alpha{\leq}C.\ \xi
\end{array}
$$

The metavariables C and D range over derivations of subtyping statements between composite canonical types; ξ and δ range over derivations of subtyping statements between individual canonical types; c and d range over both sorts of derivations.

As in Section 5.1, we can define a mapping from canonical derivation trees to linear abbreviations, which, though not injective, could easily be extended to an injective map at some cost in readability. Again, we will prefer readability over rigor and impose on the reader's imagination to supply the evident annotations on linear abbreviations.

5.3.2.4. Definition: The translation function $(\text{—})^\dagger$ from canonical derivation trees to their abbreviated forms is defined as follows.

$$\left(\frac{\forall i.\ \exists j.\quad \xi_i :: \Delta \vdash \kappa_j \leq \iota_i}{\Delta \vdash \bigwedge[\kappa_1..\kappa_m] \leq \bigwedge[\iota_1..\iota_n]}\ \text{(CSUB-AE)}\right)^\dagger \quad = \quad AE[\xi_1^\dagger..\xi_n^\dagger]$$

$$\left(\frac{\text{(CSUB-REFL)}}{\Delta \vdash k \leq k}\right)^\dagger \quad = \quad id$$

$$\left(\frac{c_1 :: \Delta \vdash k_1 \leq k_2 \qquad c_2 :: \Delta \vdash k_2 \leq k_3}{\Delta \vdash k_1 \leq k_3}\ \text{(CSUB-TRANS)}\right)^\dagger \quad = \quad c_1^\dagger \,;\, c_2^\dagger$$

$$\left(\frac{C :: \Delta \vdash \Delta(\alpha) \leq \bigwedge[\iota]}{\Delta \vdash \alpha \leq \iota}\ \text{(CSUB-TVAR)}\right)^\dagger \quad = \quad V_\alpha(C^\dagger)$$

$$\left(\frac{C_1 :: \Delta \vdash I_1 \leq K_1 \qquad \xi_2 :: \Delta \vdash \kappa_2 \leq \iota_2}{\Delta \vdash K_1 \rightarrow \kappa_2 \leq I_1 \rightarrow \iota_2}\ \text{(CSUB-ARROW)}\right)^\dagger \quad = \quad C_1^\dagger \rightarrow \xi_2^\dagger$$

$$\left(\frac{C_1 :: \Delta \vdash I_1 \leq K_1 \qquad \xi_2 :: \Delta, \alpha \leq I_1 \vdash \kappa_2 \leq \iota_2}{\Delta \vdash \forall\alpha{\leq}K_1.\ \kappa_2 \leq \forall\alpha{\leq}I_1.\ \iota_2}\ \text{(CSUB-ALL)}\right)^\dagger \quad = \quad \forall\alpha{\leq}C_1^\dagger.\ \xi_2^\dagger$$

5.3.2.5. Lemma: [Canonical context permutation] If Δ' is a permutation of Δ and both Δ' and Δ are closed, and if $c :: \Delta \vdash k \leq i$, then there is a subtyping derivation c', identical to c except for the ordering of contexts, such that $c' :: \Delta \vdash k \leq i$.

If $\alpha \notin FTV(I)$ and $c :: \Delta_1,\ \alpha{\leq}K,\ \beta{\leq}I,\ \Delta_2 \vdash k \leq i$, then there is a subtyping derivation c', identical to c except for the ordering of contexts, such that $c' :: \Delta_1, \beta{\leq}I, \alpha{\leq}K, \Delta_2 \vdash k \leq i$.

Proof: By induction on the structure of c. □

As for ordinary subtyping this lemma justifies the convention that closed canonical contexts differing only in the ordering of their bindings are regarded as identical.

5.3.3 Weakening and Narrowing

The proof transformations used to normalize canonical subtyping derivations rely on analogues of the weakening and narrowing lemmas from Section 5.2. Because they will be used below in a proof normalization procedure whose termination requires a slightly delicate argument, we formulate them here as explicit operations on subtyping derivations.

By analogy with extending a context, our linear notation for weakening is "$c,\, \alpha{\le}K$." If c is a derivation term whose conclusion is $\Delta \vdash k \le i$, then $c,\, \alpha{\le}K$ is a derivation with conclusion $\Delta,\, \alpha{\le}K \vdash k \le i$.

5.3.3.1. Definition: The *weakening* of a derivation c with a new binding $\alpha{\le}K$, written $c,\, \alpha{\le}K$, is:

$$
\begin{array}{lcl}
(AE[\xi_1..\xi_n]),\, \alpha{\le}K & = & AE[(\xi_1,\, \alpha{\le}K) \,..\, (\xi_n,\, \alpha{\le}K)] \\
id,\, \alpha{\le}K & = & id \\
(c_1 \,;\, c_2),\, \alpha{\le}K & = & (c_1,\, \alpha{\le}K) \,;\, (c_2,\, \alpha{\le}K) \\
(V_\beta(C)),\, \alpha{\le}K & = & V_\beta(C,\, \alpha{\le}K) \\
(C_1{\to}\xi_2),\, \alpha{\le}K & = & (C_1,\, \alpha{\le}K){\to}(\xi_2,\, \alpha{\le}K) \\
(\forall\beta{\le}C_1.\ \xi_2),\, \alpha{\le}K & = & \forall\beta{\le}(C_1,\, \alpha{\le}K).\ (\xi_2,\, \alpha{\le}K).
\end{array}
$$

Note that, since weakening only changes contexts, this operation is an identity on our abbreviated linear forms, where contexts are always elided.

5.3.3.2. Lemma: [Weakening for canonical subtyping] If

$$c :: \Delta \vdash k \le i,$$

then

$$c,\, \alpha{\le}K \ :: \Delta,\, \alpha{\le}K \vdash k \le i.$$

Proof: See Appendix B. □

As was the case for ordinary types, the *narrowing* transformation allows the context in the conclusion of a derivation to be modified by replacing the bound of a variable with a subtype. For example,

$$\alpha_1{\le}\top,\, \alpha_2{\le}\bigwedge[\alpha_1],\, \alpha_3{\le}\bigwedge[\alpha_1] \vdash \bigwedge[\alpha_1]{\to}\alpha_3 \le \bigwedge[\alpha_1]{\to}\alpha_1$$

can be narrowed to

$$\alpha_1{\le}\top,\, \alpha_2{\le}\bigwedge[\alpha_1],\, \alpha_3{\le}\bigwedge[\alpha_2] \vdash \bigwedge[\alpha_1]{\to}\alpha_3 \le \bigwedge[\alpha_1]{\to}\alpha_1.$$

Note, however, that the structure of the original derivation must be altered in order for the result of narrowing to be valid: wherever the assumption $\alpha_3{\le}\alpha_1$ was used in the original, we must use the new assumption $\alpha_3{\le}\bigwedge[\alpha_2]$ plus the fact that $\alpha_2{\le}\bigwedge[\alpha_1]$. To take this into account, we use the linear notation $c[D@\alpha{\le}K]$, where c is a subtyping derivation, α is a variable in $dom(\Delta)$, K is α'a new bound, and D is a derivation establishing that the new bound K is a subtype of the existing one.

5.3.3.3. Definition: Let c and D be subtyping derivations such that

$$
\begin{array}{l}
c :: \Delta,\, \alpha{\le}I \ \vdash\ k \ \le\ i \\
D :: \Delta \ \vdash\ K \ \le\ I.
\end{array}
$$

The *narrowing* of c with the binding $\alpha{\leq}K$ (justified by D) is written $c[D@\alpha{\leq}K]$ and defined as follows:

$$\begin{array}{lcl}
(AE[\xi_1..\xi_n])[D@\alpha{\leq}K] & = & AE[(\xi_1[D@\alpha{\leq}K])\,..\,(\xi_n[D@\alpha{\leq}K])] \\
id[D@\alpha{\leq}K] & = & id \\
(c_1\,;\,c_2)[D@\alpha{\leq}K] & = & (c_1[D@\alpha{\leq}K])\,;\,(c_2[D@\alpha{\leq}K]) \\
(V_\beta(C))[D@\alpha{\leq}K] \quad \text{where } \beta{\not\equiv}\alpha & = & V_\beta(C[D@\alpha{\leq}K]) \\
(V_\alpha(C))[D@\alpha{\leq}K] & = & V_\alpha((D,\,\alpha{\leq}K)\,;\,(C[D@\alpha{\leq}K])) \\
(C_1{\rightarrow}\xi_2)[D@\alpha{\leq}K] & = & (C_1[D@\alpha{\leq}K]){\rightarrow}(\xi_2[D@\alpha{\leq}K]) \\
(\forall\beta{\leq}C_1.\ \xi_2)[D@\alpha{\leq}K] & = & \forall\beta{\leq}(C_1[D@\alpha{\leq}K]).\ (\xi_2[(D,\,\beta{\leq}I_1)@\alpha{\leq}K]) \\
 & & \text{where } C_1,\,\alpha{\leq}I :: \Delta \vdash I_1 \leq K_1.
\end{array}$$

5.3.3.4. Lemma: [Narrowing for canonical subtyping] If

$$c :: \Delta,\, \alpha{\leq}I \vdash k \leq i$$
$$D :: \Delta \vdash K \leq I,$$

then

$$(c[D@\alpha{\leq}K]) :: \Delta,\, \alpha{\leq}K \vdash k \leq i.$$

Proof: See Appendix B. □

5.3.4 Subtyping Derivation Normalization Rules

To construct an algorithm for checking the canonical subtype relation, we need a notion of *normal form*, and an effective procedure for transforming arbitrary derivations into this form. The main task of the normalization procedure is to push instances of CSub-Trans toward the leaves of the derivation, until they eventually disappear into instances of the CSub-TVar rule. For example, if $\Delta \equiv \alpha_1{\leq}\top,\, \alpha_2{\leq}\bigwedge[\alpha_1],\, \alpha_3{\leq}\bigwedge[\alpha_2]$, then the derivation

$$\dfrac{\Delta \vdash \alpha_3 \leq \alpha_2 \qquad \Delta \vdash \alpha_2 \leq \alpha_1}{\Delta \vdash \alpha_3 \leq \alpha_1}\ \text{(CSUB-TRANS)}$$

becomes the normal-form derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Delta \vdash \alpha_1 \leq \alpha_1}\ \text{(CSUB-REFL)}}{\Delta \vdash \bigwedge[\alpha_1] \leq \bigwedge[\alpha_1]}\ \text{(CSUB-AE)}}{\Delta \vdash \alpha_2 \leq \alpha_1}\ \text{(CSUB-TVAR)}}{\Delta \vdash \bigwedge[\alpha_2] \leq \bigwedge[\alpha_1]}\ \text{(CSUB-AE)}}{\Delta \vdash \alpha_3 \leq \alpha_1.}\ \text{(CSUB-TVAR)}$$

The normalization procedure is presented as a collection of rewrite rules on subtyping derivations. These rules are separated into two groups to simplify the presentation of a *rewriting strategy* later on (Section 5.3.5) and the proof that this strategy always terminates. We first list the abbreviated linear forms of the rules and then justify them by discussing how they operate on proof trees.

5.3.4.1. Definition: The *one-step, outermost simplification relation* on subtyping derivations, $\longrightarrow^t_1$, is defined by the following rewrite rules:

I. Reflexivity simplification

1. $id \;::\; \Delta \vdash K_1{\rightarrow}\kappa_2 \;\leq\; K_1{\rightarrow}\kappa_2$
   $\longrightarrow^t_1 \;\; id{\rightarrow}id$
2. $id \;::\; \Delta \vdash \forall\alpha{\leq}K_1.\ \kappa_2 \;\leq\; \forall\alpha{\leq}K_1.\ \kappa_2$
   $\longrightarrow^t_1 \;\; \forall\alpha{\leq}id.\ id$
3. $id \;::\; \Delta \vdash \bigwedge[\kappa_1..\kappa_n] \;\leq\; \bigwedge[\kappa_1..\kappa_n]$
   $\longrightarrow^t_1 \;\; AE[id\ ..\ id]$

II. Cut simplification

1. $id\ ;\ c$
   $\longrightarrow^t_1 \;\; c$
2. $c\ ;\ id$
   $\longrightarrow^t_1 \;\; c$
3. $AE[\xi_1..\xi_m]\ ;\ AE[\delta_1..\delta_n]$ where each $\delta_i :: \Delta \vdash \kappa_{j_i} \;\leq\; \iota_i$
   $\longrightarrow^t_1 \;\; AE[(\xi_{j_1}\ ;\ \delta_1)\ ..\ (\xi_{j_n}\ ;\ \delta_n)]$
4. $V_\alpha(AE[\xi])\ ;\ \delta$
   $\longrightarrow^t_1 \;\; V_\alpha(AE[\xi\ ;\ \delta])$
5. $V_\alpha(id)\ ;\ \delta$
   $\longrightarrow^t_1 \;\; V_\alpha(AE[\delta])$
6. $C{\rightarrow}\xi\ ;\ D{\rightarrow}\delta$
   $\longrightarrow^t_1 \;\; (D\ ;\ C){\rightarrow}(\xi\ ;\ \delta)$
7. $(\forall\alpha{\leq}C.\ \xi)\ ;\ (\forall\alpha{\leq}D.\ \delta)$ where $D :: \Delta \vdash K_3 \;\leq\; K_2$
   $\longrightarrow^t_1 \;\; \forall\alpha{\leq}(D\ ;\ C).\ (\xi[D@\alpha{\leq}K_3]\ ;\ \delta)$

Rules I.1, I.2, and I.3 together restrict the form of instances of reflexivity in normal form derivations to reflexivity between variables.

Rules II.1 and II.2 eliminate instances of transitivity with an instance of reflexivity as one of their immediate subderivations.

Rule II.3 simplifies instances of transitivity whose subderivations are both instances of CSub-AE by pushing the application of transitivity toward the leaves of the derivation. Similarly, rule II.4 simplifies instances of transitivity whose left-hand subderivations end with the rule CSub-TVar by pushing the application of transitivity toward the leaves of the derivation. Rule II.5 handles the simpler situation where the premise of CSub-TVar is an instance of CSub-Id, in which case no new instance of transitivity need be created. Rule II.6 simplifies instances of transitivity whose subderivations are both instances of CSub-Arrow by pushing the applications of transitivity toward the leaves.

Rule II.7 — the keystone of the definition — simplifies instances of transitivity whose subderivations are both instances of CSub-All. Pictorially, it rewrites the derivation

$$\dfrac{\dfrac{\dfrac{C}{\Delta \vdash K_2 \leq K_1} \qquad \dfrac{\xi}{\Delta, \alpha{\leq}K_2 \vdash \kappa_1 \leq \kappa_2}}{\Delta \vdash \forall\alpha{\leq}K_1.\ \kappa_1 \leq \forall\alpha{\leq}K_2.\ \kappa_2} \qquad \dfrac{\dfrac{D}{\Delta \vdash K_3 \leq K_2} \qquad \dfrac{\delta}{\Delta, \alpha{\leq}K_3 \vdash \kappa_2 \leq \kappa_3}}{\Delta \vdash \forall\alpha{\leq}K_2.\ \kappa_2 \leq \forall\alpha{\leq}K_3.\ \kappa_3}}{\Delta \vdash \forall\alpha{\leq}K_1.\ \kappa_1 \leq \forall\alpha{\leq}K_3.\ \kappa_3}$$

as

$$\dfrac{\dfrac{\dfrac{D}{\Delta \vdash K_3 \leq K_2} \qquad \dfrac{C}{\Delta \vdash K_2 \leq K_1}}{\Delta \vdash K_3 \leq K_1} \qquad \dfrac{\dfrac{\xi[D@\alpha{\leq}K_3]}{\Delta, \alpha{\leq}K_3 \vdash \kappa_1 \leq \kappa_2} \qquad \dfrac{\delta}{\Delta, \alpha{\leq}K_3 \vdash \kappa_2 \leq \kappa_3}}{\Delta, \alpha{\leq}K_3 \vdash \kappa_1 \leq \kappa_3}}{\Delta \vdash \forall\alpha{\leq}K_1.\ \kappa_1 \leq \forall\alpha{\leq}K_3.\ \kappa_3.}$$

5.3.4.2. Definition: $\longrightarrow_1$ is the compatible closure of $\longrightarrow_1^t$; that is:

if $c \longrightarrow_1^t c'$, then $c \longrightarrow_1 c'$
if $\xi_i \longrightarrow_1 \xi_i'$, then $AE[\xi_1..\xi_i..\xi_n] \longrightarrow_1 AE[\xi_1..\xi_i'..\xi_n]$
if $c \longrightarrow_1 c'$, then $(c\ ;d) \longrightarrow_1 (c'\ ;d)$
if $d \longrightarrow_1 d'$, then $(c\ ;d) \longrightarrow_1 (c\ ;d')$
if $C \longrightarrow_1 C'$, then $V_\alpha(C) \longrightarrow_1 V_\alpha(C')$
if $C \longrightarrow_1 C'$, then $(\forall\alpha{\leq}C.\ \delta) \longrightarrow_1 (\forall\alpha{\leq}C'.\ \delta)$
if $\delta \longrightarrow_1 \delta'$, then $(\forall\alpha{\leq}C.\ \delta) \longrightarrow_1 (\forall\alpha{\leq}C.\ \delta')$
if $C \longrightarrow_1 C'$, then $(C{\rightarrow}\delta) \longrightarrow_1 (C'{\rightarrow}\delta)$
if $\delta \longrightarrow_1 \delta'$, then $(C{\rightarrow}\delta) \longrightarrow_1 (C{\rightarrow}\delta')$.

The simplification relation $\longrightarrow^*$ is the reflexive and transitive closure of $\longrightarrow_1$. A *redex* in a subtyping derivation c is a subderivation d that matches the left-hand side of one of the simplification rules. The corresponding right-hand side, d', is the *contractum* of d. When $c \longrightarrow_1 c'$ by replacing d with d', we say that c *reduces* to c' in one step. A *normal-form* subtyping derivation is one that contains no redices. Similarly, a *I-normal-form* subtyping derivation is one that contains no I-redices (instances of the left hand sides of any of the rules in group I).

Having shown already that weakening and narrowing preserve validity, it is a simple matter to check that the rewriting rules do so as well.

5.3.4.3. Lemma: [Replacement] If c is a valid subtyping derivation and c' is formed from c by replacing some subderivation d by a valid derivation d' with the same conclusion as d, then c' is valid and has the same conclusion as c.

Proof: Immediate, since none of the CSub rules place any requirements on the shape of the derivations of their hypotheses. □

In type assignment systems, a typing statement $\Gamma \vdash e \in \tau$ is often thought of as a kind of sentence, where e is the *subject* and τ is the *predicate*. When $e \longrightarrow^* e'$ according to some system of rewrite rules (usually read "e evaluates to e'") we speak of "reducing the subject." If the type assignment system in question has the property that whenever $\Gamma \vdash e \in \tau$ is derivable and $e \longrightarrow^* e'$ the statement $\Gamma \vdash e' \in \tau$ is also derivable, we say that the typing relation is closed under subject reduction, or that the system in question has the *subject reduction property.* The same terminology can conveniently be applied to statements of the form $c :: \Delta \vdash k \leq i$ if we think of $\Delta \vdash k \leq i$ as a kind of predicate — true of valid subtyping derivations with this conclusion — and derivation simplification as a kind of evaluation.

5.3.4.4. Lemma: [Subject reduction for the simplification rules] If c is a valid subtyping derivation such that $c :: \Delta \vdash k \leq i$ and $c \longrightarrow^* d$, then $d :: \Delta \vdash k \leq i$.

Proof: First, note that all of the rewrite rules map valid subtyping derivations to valid derivations with the same conclusions (the argument is straightforward except for rule II.7, which follows from the narrowing lemma for canonical types (5.3.3.4)). This observation extends to $\longrightarrow_1$ by the replacement lemma (5.3.4.3) and to $\longrightarrow^*$ by induction. □

5.3.5 Termination of the Normalization Rules

Now we must show that every canonical subtyping derivation can be rewritten into one in normal form. The crux of the argument will be that whenever an instance of transitivity is reduced, the size of the intermediate type, or *cut type*, is decreased in any new instances of transitivity in the result. The argument is slightly delicate, since both rule II.3 and the narrowing operation in rule II.7 can create copies of subderivations that may themselves contain redices; this is handled by reducing redices with the largest cut types first.

The argument is further complicated by the fact that rule II.4 creates a new instance of transitivity whose intermediate type is exactly the same as that of the original. In this case, we argue that the resulting derivation is simpler because an instance of transitivity has been pushed toward the leaves of the derivation.

A subtyping derivation of the form c ; d is called a *compound derivation.* The *cut type* of a compound derivation $(c :: \Delta \vdash k_1 \leq k_2)$; $(d :: \Delta \vdash k_2 \leq k_3)$, written $\mathit{cut\text{-}type}(c ; d)$, is k_2. The *cut size* of a compound derivation c ; d is

$$\mathit{cut\text{-}size}(c ; d) = \mathit{size}(\mathit{cut\text{-}type}(c ; d)).$$

The *complexity* of a compound derivation c, written $\mathit{complexity}(c)$, is the pair $\langle \mathit{cut\text{-}size}(c),\ \mathit{size}(c)\rangle$, ordered lexicographically. A II-redex c is an *innermost* redex of complexity m if no proper subderivation of c is a II-redex of complexity m.

5.3.5.1. Definition: The *rewriting strategy* for normalizing subtyping derivations comprises the following steps:

1. *Perform I-reductions in any order until a I-normal form is reached.*
2. *If there are any remaining II-redexes, let m be the largest complexity of any remaining II-redex. Choose an innermost redex of complexity m, reduce it, and return to step 2.*

Since each I-reduction decreases the size of the types in the conclusions of any new I-redices it creates, the I-rules are clearly strongly normalizing. Moreover, none of the II-rules can create new I-redices when applied to I-normal forms, so we need worry no further about the I-rules.

Progress in normalizing the II-redices of a derivation c is measured as follows:

5.3.5.2. Definition: The *total complexity* of a derivation c, written $\mathit{total}(c)$, is the pair $\langle m, n\rangle$, where m is the maximum complexity of any compound subderivation of c and n is the number of compound subderivations of this size, ordered lexicographically.

5.3.5.3. Lemma: For any derivation c, the weakening $(c, \alpha{\leq}K)$ contains no II-redices not already present in c.

Proof: Immediate from the definition of weakening (5.3.3.1). □

5.3.5.4. Lemma: Let $c :: \Delta, \alpha{\leq}I \vdash k \leq k'$ and $D :: \Delta \vdash K \leq I$. Then the cut type of every new II-redex in the narrowing $c[D@\alpha{\leq}K]$ is I.

Proof: By induction on the structure of c.

Case: $c \equiv AE[\xi_1..\xi_n]$

By the induction hypothesis and CSub-AE.

Case: $c \equiv \mathit{id}$

Immediate.

Case: $c \equiv c_1 ; c_2$

Can't happen.

Case: $c \equiv V_\beta(C)$

Subcase: $\beta \neq \alpha$

By the induction hypothesis and CSub-TVar.

Subcase: $\beta = \alpha$

By the definition of narrowing (5.3.3.3),

$$(V_\alpha(C))[D@\alpha{\leq}K] = V_\alpha((D,\, \alpha{\leq}K)\ ;\ (C[D@\alpha{\leq}K])).$$

By the induction hypothesis, the cut type of every new II-redex in $C[D@\alpha{\leq}K]$ is I. By Lemma 5.3.5.3, there are no new redices in $(D,\, \alpha{\leq}K)$. The cut type of the new redex $((D,\, \alpha{\leq}K)\ ;\ (C[D@\alpha{\leq}K]))$ is I.

Case: $c \equiv C{\to}\xi$

By the induction hypothesis and CSub-Arrow.

Case: $c \equiv \forall\beta{\leq}C.\ \xi$

By the definition of narrowing (5.3.3.3),

$$(\forall\beta{\leq}C.\ \xi)[D@\alpha{\leq}K] = \forall\beta{\leq}(C[D@\alpha{\leq}K]).\ (\xi[(D,\, \beta{\leq}I_1)@\alpha{\leq}K]),$$

where $C :: \Delta,\, \alpha{\leq}I \vdash I_1 \leq K_1$. By the induction hypothesis, every new II-redex in $C[D@\alpha{\leq}K]$ has cut type I. By Lemma 5.3.5.3, $(D,\, \beta{\leq}I_1) :: \Delta,\, \beta{\leq}I_1 \vdash K \leq I$ has no new redices. By the induction hypothesis, every new II-redex in $\xi_2[(D,\, \beta{\leq}I_1)@\alpha{\leq}K]$ has cut type I. □

5.3.5.5. Lemma: Let o be a derivation and $(c\ ;\ d)$ an innermost II-redex of maximum complexity in o. Then $total(o) > total(o')$, where o' is the result of replacing $(c\ ;\ d)$ by its contractum, e.

Proof: By cases on the rule used to reduce $c\ ;\ d$ to e.

Case II.1: $c \equiv id \qquad e \equiv d$

This reduction removes one II-redex of maximum complexity from o.

Case II.2: $d \equiv id \qquad e \equiv c$

Similar.

Case II.3:
$c \equiv AE[\xi_1..\xi_m] \qquad d \equiv AE[\delta_1..\delta_n] \qquad \delta_i :: \Delta \vdash \kappa_{j_i} \leq \iota_i \qquad e \equiv AE[(\xi_{j_1}\ ;\ \delta_1)\ ..\ (\xi_{j_n}\ ;\ \delta_n)]$

This reduction removes one redex of maximum complexity with $cut\text{-}size = size(\bigwedge[\kappa_1..\kappa_n])$ and creates n new redices of cut sizes $size(\kappa_{j_1}),\ \ldots,\ size(\kappa_{j_n})$, all of which are strictly smaller. In addition, some redices in the ξ_i's may be copied, but these must also have smaller cut size because $c\ ;\ d$ is an innermost redex of maximal complexity.

Case II.4: $c \equiv V_\alpha(AE[\xi]) \qquad d \equiv \delta \qquad e \equiv V_\alpha(AE[\xi\ ;\ \delta])$

This reduction removes one redex of maximum complexity and creates one new one with exactly the same cut type. However, the size of the new redex is $size(\xi\ ;\ \delta) < size(c\ ;\ d)$, so its complexity is smaller. The complexities of other redices in o are unchanged.

Case II.5: $c \equiv V_\alpha(id) \qquad d \equiv \delta \qquad e \equiv V_\alpha(AE[\delta])$

This reduction removes one redex of maximum complexity and creates no new redices.

Case II.6:

$$\begin{array}{lll} c\ ;\ d & \equiv & (C{\to}\xi)\ ;\ (D{\to}\delta) \\ e & \equiv & (D\ ;\ C){\to}(\xi\ ;\ \delta) \\ \text{where} & & C{::}\Delta \vdash K_2 \leq K_1 \\ & & D{::}\Delta \vdash K_3 \leq K_2 \\ & & \xi\ {::}\Delta \vdash \kappa_1 \leq \kappa_2 \\ & & \delta\ {::}\Delta \vdash \kappa_2 \leq \kappa_3. \end{array}$$

This reduction removes one redex of maximal complexity with cut type $K_2{\to}\kappa_2$ and creates two new redices, one with cut type K_2 and one with cut type κ_2.

Case II.7: $c\ ;\ d \equiv (\forall\alpha{\leq}C.\ \xi)\ ;\ (\forall\alpha{\leq}D.\ \delta)$
$e \quad \equiv \forall\alpha{\leq}(D\ ;\ C).\ ((\xi[D@\alpha{\leq}K_3])\ ;\ \delta)$
where $C{::}\Delta \vdash K_2 \leq K_1$
$D{::}\Delta \vdash K_3 \leq K_2$
$\xi\ {::}\Delta,\ \alpha{\leq}K_2 \vdash \kappa_1 \leq \kappa_2$
$\delta\ {::}\Delta,\ \alpha{\leq}K_3 \vdash \kappa_2 \leq \kappa_3$.

The cut type of $(c\ ;\ d)$ is $\forall\alpha{\leq}K_2.\ \kappa_2$. The new II-redices in e are:

- $(D\ ;\ C)$, with cut type K_2;
- $(\xi[D_1@\alpha{\leq}K_3]\ ;\ \delta)$, with cut type κ_2; and
- new redices in $\xi[D@\alpha{\leq}K_3]$, with cut type K_2 (by Lemma 5.3.5.4).

Thus, rewriting $(c\ ;\ d)$ as e removes one redex of maximal complexity with cut type $\forall\alpha{\leq}K_2.\ \kappa_2$ and creates some new redices with strictly smaller cut types K_2 and κ_2. □

Since steps 1 and 2 of our rewriting stretegy each terminate, and since step 2 introduces no new I-redices, we are assured that every derivation is eventually rewritten by this strategy to one in I/II-normal form:

5.3.5.6. Theorem: This rewriting strategy is normalizing.

5.3.5.7. Corollary: If there is any derivation of a canonical subtyping statement $\Delta \vdash k \leq i$, then there is one in normal form.

5.3.6 Shapes of Normal-Form Subtyping Derivations

5.3.6.1. Lemma: If $id :: \Delta \vdash k \leq i$ is a normal-form subtyping derivation, then $k \equiv i \equiv \alpha$ for some variable α.

Proof: By the form of the I-rules (5.3.4.1). □

5.3.6.2. Lemma: If e is a normal-form subtyping derivation, then $e \not\equiv (c\ ;\ d)$.

Proof: See Appendix B. □

5.3.6.3. Lemma: [Syntax-directedness of canonical subtyping]

1. If $\Delta \vdash K \leq I$, then for every $\iota \in I$ there is some $\kappa \in K$ such that $\Delta \vdash \kappa \leq \iota$.
2. If $\Delta \vdash K_1 {\rightarrow} \kappa_2 \leq \iota$, then $\iota \equiv I_1 {\rightarrow} \iota_2$ with $\Delta \vdash I_1 \leq K_1$ and $\Delta \vdash \kappa_2 \leq \iota_2$.
3. If $\Delta \vdash \forall\alpha{\leq}K_1.\ \kappa_2 \leq \iota$, then $\iota \equiv \forall\alpha{\leq}I_1.\ \iota_2$ with $\Delta \vdash I_1 \leq K_1$ and $\Delta,\ \alpha{\leq}I_1 \vdash \kappa_2 \leq \iota_2$.
4. If $\Delta \vdash \alpha \leq \kappa$, then either $\kappa \equiv \alpha$ or else $\Delta \vdash \Delta(\alpha) \leq \bigwedge[\kappa]$.

Moreover, when the given derivation is in normal form, the derivations promised in each clause are proper subderivations of the original.

Proof: In each case, we are given a derivation of $\Delta \vdash k \leq i$. By Corollary 5.3.5.7, there exists a normal-form derivation of the same statement. By Lemmas 5.3.6.1 and 5.3.6.2, this normal derivation does not end with an instance of CSub-Refl (except CSub-Refl applied to variables) or CSub-Trans. The result follows by inspection of the remainder of the CSub rules. □

5.3.6.4. Corollary: If $\Delta \vdash \kappa \leq \alpha$, then either $\kappa \equiv \alpha$ or else $\kappa \equiv \beta$ for some β with $\Delta \vdash \Delta(\beta) \leq \bigwedge[\alpha]$.

5.3.7 Equivalence of Ordinary and Canonical Subtyping

Our next task is to establish that the subtyping relations on ordinary types and on the corresponding canonical types are equivalent in an appropriate sense. We accomplish this by defining a *flattening mapping* $\flat$ from ordinary types to canonical types with the following properties:

1. Flattening preserves subtyping: if $\Gamma \vdash^{\wedge} \sigma \leq \tau$, then $\Gamma^\flat \vdash^{\flat} \sigma^\flat \leq \tau^\flat$.
2. Flattening yields a type equivalent to the original: $\Gamma \vdash^{\wedge} \tau^\flat \sim \tau$.

The second observation (plus narrowing and the fact that the identity injection from the set of canonical types into the set of ordinary types preserves subtyping — if $\Delta \vdash^{\flat} \kappa \leq \iota$, then $\Delta \vdash^{\wedge} \kappa \leq \iota$) implies the converse of the first: if the translation of a statement is provable in the canonical system then the original statement is also provable. Thus, the flattening mapping also *reflects* subtyping.

5.3.7.1. Definition: The *flattening mapping* $\flat$ from ordinary types to composite canonical types is defined as follows:

$$\begin{array}{lcl}
\alpha^\flat & = & \bigwedge[\alpha] \\
(\sigma{\rightarrow}\tau)^\flat & = & \bigwedge[\sigma^\flat{\rightarrow}\kappa \mid \kappa \in \tau^\flat] \\
(\forall\alpha{\leq}\sigma.\ \tau)^\flat & = & \bigwedge[\forall\alpha{\leq}\sigma^\flat.\ \kappa \mid \kappa \in \tau^\flat] \\
\bigwedge[\tau_1..\tau_n]^\flat & = & \bigcup_i \tau_i{}^\flat
\end{array}$$

This mapping is extended pointwise to contexts:

$$\begin{array}{lcl}
\{\}^\flat & = & \{\} \\
(\Gamma,\, \alpha{\leq}\tau)^\flat & = & \Gamma^\flat,\, \alpha{\leq}\tau^\flat \\
(\Gamma,\, x{:}\tau)^\flat & = & \Gamma^\flat,\, x{:}\tau^\flat
\end{array}$$

5.3.7.2. Lemma: [$\flat$ preserves subtyping] If $\Gamma \vdash^{\wedge} \sigma \leq \tau$ then $\Gamma^\flat \vdash^{\flat} \sigma^\flat \leq \tau^\flat$.

Proof: See Appendix refapp:proofs. □

Next, we remark that subtyping on canonical types is preserved when canonical types are read as ordinary types.

5.3.7.3. Lemma: If $\Delta \vdash^{\flat} k \leq i$, then $\Delta \vdash^{\wedge} k \leq i$.

Proof: By induction on the structure of a canonical subtyping derivation. □

The last fact needed to establish the equivalence of subtyping on ordinary and canonical types is that the flattening transformation always yields a type equivalent to the original.

5.3.7.4. Lemma: $\Gamma \vdash^{\wedge} \tau^\flat \sim \tau$ for all $F_\wedge$ types τ and contexts Γ.

Proof: See Appendix B. □

Combining this with the previous lemma, we can show that the translation from ordinary to canonical types reflects subtyping in $F_\wedge$.

5.3.7.5. Lemma: [$\flat$ reflects subtyping] If $\Gamma^\flat \vdash^{\flat} \sigma^\flat \leq \tau^\flat$, then $\Gamma \vdash^{\wedge} \sigma \leq \tau$.

Proof: By Lemma 5.3.7.3, $\Gamma^\flat \vdash^{\wedge} \sigma^\flat \leq \tau^\flat$. By Lemma 5.3.7.4, $\Gamma \vdash^{\wedge} \Gamma(\alpha) \leq \Gamma^\flat(\alpha)$ for each $\alpha \in dom(\Gamma^\flat)$. By narrowing (5.3.3.4), $\Gamma \vdash^{\wedge} \sigma^\flat \leq \tau^\flat$. By Lemma 5.3.7.4 again, $\Gamma \vdash^{\wedge} \sigma \leq \sigma^\flat$ and $\Gamma \vdash^{\wedge} \tau^\flat \leq \tau$. By two applications of Sub-Trans, $\Gamma \vdash^{\wedge} \sigma \leq \tau$. □

Lemmas 5.3.7.2 and 5.3.7.5 together show that the subtype relations on ordinary and canonical types correspond appropriately:

5.3.7.6. Theorem: [Equivalence of ordinary and canonical subtyping]

$$\Gamma \vdash^{\wedge} \sigma \leq \tau \quad \text{iff} \quad \Gamma^\flat \vdash^{\flat} \sigma^\flat \leq \tau^\flat.$$

5.3.8 Subtyping Algorithm

The definition of canonical subtyping leads directly to an algorithm for deciding the subtype relation on $F_\wedge$ types: to check whether $\Gamma \vdash \sigma \leq \tau$, flatten Γ, σ, and τ and then check whether $\Gamma^\flat \vdash^\flat \sigma^\flat \leq \tau^\flat$. In this section we describe a more efficient algorithm that operates directly on $F_\wedge$ types, effectively performing the flattening translation on the fly. The algorithm presented here generalizes one described by Reynolds for deciding the subtype relation of Forsythe [personal communication, 1988].

Given Γ, σ, and τ, this algorithm first performs a complete analysis of the structure of τ. Whenever τ has the form $\tau_1 \rightarrow \tau_2$ or $\forall\alpha{\leq}\tau_1.\ \tau_2$, it pushes the left-hand side — τ_1 or $\alpha{\leq}\tau_1$ — onto a queue of pending left-hand sides and proceeds recursively with the analysis of τ_2. When τ has the form of an intersection, it calls itself recursively on each of the elements. When τ has finally been reduced to a type variable, the algorithm begins analyzing σ, matching left-hand sides of arrow and polymorphic types against the queue of pending left-hand sides from τ. In the base case, when both σ and τ have been reduced to variables, the algorithm first checks whether they are identical; if so, and if the queue of pending left-hand sides is empty, the algorithm immediately returns *true*. Otherwise, the variable σ is replaced by its upper bound from Γ and the analysis continues as before.

5.3.8.1. Definition: Let X be a finite sequence of elements of the set

$$\{\tau \mid \tau \text{ a type}\} \cup \{\alpha{\leq}\tau \mid \alpha \text{ a type variable and } \tau \text{ a type}\}.$$

Define the type $X{\Rightarrow}\tau$ as follows:

$$\begin{array}{lcl} [\,]{\Rightarrow}\tau & = & \tau \\ [\sigma, X]{\Rightarrow}\tau & = & \sigma \rightarrow (X{\Rightarrow}\tau) \\ [\alpha{\leq}\sigma, X]{\Rightarrow}\tau & = & \forall\alpha{\leq}\sigma.\ (X{\Rightarrow}\tau). \end{array}$$

From the definitions of $\flat$ and $X{\Rightarrow}\tau$, the following facts are immediate:

5.3.8.2. Lemma:

1. $(X{\Rightarrow}(\bigwedge[\tau_1..\tau_n]))^\flat = \bigcup_i (X{\Rightarrow}\tau_i)^\flat$.
2. $(X{\Rightarrow}(\tau_1{\rightarrow}\tau_2))^\flat = ([X, \tau_1] \Rightarrow \tau_2))^\flat$.
3. $(X{\Rightarrow}(\forall\alpha{\leq}\tau_1.\ \tau_2))^\flat = ([X, \alpha{\leq}\tau_1] \Rightarrow \tau_2)^\flat$.

Note that every type τ has either the form $X{\Rightarrow}\alpha$ or the form $X{\Rightarrow}\bigwedge[\tau_1..\tau_n]$ for a unique X.

5.3.8.3. Definition: The four-place algorithmic subtyping relation $\Gamma \vdash\!\!\!\!\cdot\ \sigma \leq X{\Rightarrow}\tau$ is the least relation closed under the following rules:

$$\frac{\text{for all } i,\ \Gamma \vdash \sigma \leq X \Rightarrow \tau_i}{\Gamma \vdash \sigma \leq X \Rightarrow \bigwedge[\tau_1..\tau_n]} \qquad \text{(ASubR-Inter)}$$

$$\frac{\text{for some } i,\ \Gamma \vdash \sigma_i \leq X \Rightarrow \alpha}{\Gamma \vdash \bigwedge[\sigma_1..\sigma_n] \leq X \Rightarrow \alpha} \qquad \text{(ASubL-Inter)}$$

$$\frac{\Gamma \vdash \tau_1 \leq [\,] \Rightarrow \sigma_1 \qquad \Gamma \vdash \sigma_2 \leq X_2 \Rightarrow \alpha}{\Gamma \vdash \sigma_1{\rightarrow}\sigma_2 \leq [\tau_1, X_2] \Rightarrow \alpha} \qquad \text{(ASubL-Arrow)}$$

$$\frac{\Gamma \vdash \tau_1 \leq [\,] \Rightarrow \sigma_1 \qquad \Gamma, \beta{\leq}\tau_1 \vdash \sigma_2 \leq X_2 \Rightarrow \alpha}{\Gamma \vdash \forall\beta{\leq}\sigma_1.\ \sigma_2 \leq [\beta{\leq}\tau_1, X_2] \Rightarrow \alpha} \qquad \text{(ASubL-All)}$$

$$\Gamma \vdash \alpha \leq [\,] \Rightarrow \alpha \qquad \text{(ASubL-Refl)}$$

$$\frac{\Gamma \vdash \Gamma(\beta) \leq X \Rightarrow \alpha}{\Gamma \vdash \beta \leq X \Rightarrow \alpha} \qquad \text{(ASubL-TVar)}$$

We sometimes decorate the turnstile symbol $\stackrel{.}{\vdash}$ to distinguish algorithmic derivations from derivations in other calculi.

5.3.8.4. Definition: We write $\textsc{Dist}^*_{\Gamma,\bigwedge[X\Rightarrow\tau_1..X\Rightarrow\tau_n]}$ (or just $\textsc{Dist}^*$ when the appropriate subscript is clear) for the following compound derivation:

$$\textsc{Dist}^*_{\Gamma,\bigwedge[[\,]\Rightarrow\tau_1..[\,]\Rightarrow\tau_n]} \quad = \quad \frac{\text{(sub-refl)}}{\Gamma \stackrel{\wedge}{\vdash} \bigwedge[[\,]\Rightarrow\tau_1 \;..\; [\,]\Rightarrow\tau_n] \leq [\,]\Rightarrow\bigwedge[\tau_1..\tau_n]}$$

$$\textsc{Dist}^*_{\Gamma,\bigwedge[\sigma\to(X'\Rightarrow\tau_1)..\sigma\to(X'\Rightarrow\tau_n)]} \quad =$$

$$\dfrac{\dfrac{\text{(sub-dist-ia)}}{\begin{array}{l}\Gamma \;\stackrel{\wedge}{\vdash}\; \bigwedge[\sigma\to(X'\Rightarrow\tau_1) \;..\; \sigma\to(X'\Rightarrow\tau_n)] \\ \quad\leq\; \sigma\to\bigwedge[X'\Rightarrow\tau_1 \;..\; X'\Rightarrow\tau_n]\end{array}} \qquad \dfrac{\overline{\Gamma \vdash \sigma \leq \sigma} \qquad \textsc{Dist}^*_{\Gamma,\bigwedge[X'\Rightarrow\tau_1..X'\Rightarrow\tau_n]}}{\begin{array}{l}\Gamma \;\stackrel{\wedge}{\vdash}\; \sigma\to\bigwedge[X'\Rightarrow\tau_1 \;..\; X'\Rightarrow\tau_n] \\ \quad\leq\; \sigma\to(X'\Rightarrow\bigwedge[\tau_1..\tau_n])\end{array}}\text{(sub-arrow)}}{\Gamma \stackrel{\wedge}{\vdash} \bigwedge[\sigma\to(X'\Rightarrow\tau_1) \;..\; \sigma\to(X'\Rightarrow\tau_n)] \leq \sigma\to(X'\Rightarrow\bigwedge[\tau_1..\tau_n])}\text{(sub-trans)}$$

$$\textsc{Dist}^*_{\Gamma,\bigwedge[\forall\alpha\leq\sigma.\ (X'\Rightarrow\tau_1)..\forall\alpha\leq\sigma.\ (X'\Rightarrow\tau_n)]} \quad =$$

$$\dfrac{\dfrac{\text{(sub-dist-iq)}}{\begin{array}{l}\Gamma \;\stackrel{\wedge}{\vdash}\; \bigwedge[\forall\alpha\leq\sigma.\ (X'\Rightarrow\tau_1) \;..\; \forall\alpha\leq\sigma.\ (X'\Rightarrow\tau_n)] \\ \quad\leq\; \forall\alpha\leq\sigma.\ \bigwedge[X'\Rightarrow\tau_1 \;..\; X'\Rightarrow\tau_n]\end{array}} \qquad \dfrac{\overline{\Gamma \vdash \sigma \leq \sigma} \qquad \textsc{Dist}^*_{(\Gamma,\alpha\leq\sigma),\bigwedge[X'\Rightarrow\tau_1..X'\Rightarrow\tau_n]}}{\begin{array}{l}\Gamma \;\stackrel{\wedge}{\vdash}\; \forall\alpha\leq\sigma.\ \bigwedge[X'\Rightarrow\tau_1 \;..\; X'\Rightarrow\tau_n] \\ \quad\leq\; \forall\alpha\leq\sigma.\ (X'\Rightarrow\bigwedge[\tau_1..\tau_n])\end{array}}\text{(sub-all)}}{\Gamma \stackrel{\wedge}{\vdash} \bigwedge[\forall\alpha\leq\sigma.\ (X'\Rightarrow\tau_1) \;..\; \forall\alpha\leq\sigma.\ (X'\Rightarrow\tau_n)] \leq \forall\alpha\leq\sigma.\ (X'\Rightarrow\bigwedge[\tau_1..\tau_n])}\text{(sub-trans)}$$

5.3.8.5. Definition: Let $c :: \Gamma \stackrel{.}{\vdash} \sigma \leq \tau$ be an algorithmic subtyping derivation. Then $c^\wedge :: \Gamma \stackrel{\wedge}{\vdash} \sigma \leq \tau$ is the following ordinary derivation:

$$\left(\frac{\text{for all } i,\ c_i :: \Gamma \stackrel{.}{\vdash} \sigma \leq X\Rightarrow\tau_i}{\Gamma \stackrel{.}{\vdash} \sigma \leq X\Rightarrow\bigwedge[\tau_1..\tau_n]}\text{(asubr-inter)}\right)^\wedge \quad =$$

$$\dfrac{\dfrac{c_1^\wedge \cdots c_n^\wedge}{\Gamma \stackrel{\wedge}{\vdash} \sigma \leq \bigwedge[X\Rightarrow\tau_1 \;..\; X\Rightarrow\tau_n]}\text{(sub-inter-g)} \qquad \begin{array}{l}\textsc{Dist}^* :: \Gamma\stackrel{\wedge}{\vdash}\bigwedge[X\Rightarrow\tau_1 \;..\; X\Rightarrow\tau_n] \\ \qquad\qquad \leq X\Rightarrow\bigwedge[\tau_1..\tau_n]\end{array}}{\Gamma \stackrel{\wedge}{\vdash} \sigma \leq X\Rightarrow\bigwedge[\tau_1..\tau_n]}$$

$$\left(\frac{\text{for some } i,\ c_i :: \Gamma \stackrel{.}{\vdash} \sigma_i \leq X\Rightarrow\alpha}{\Gamma \stackrel{.}{\vdash} \bigwedge[\sigma_1..\sigma_n] \leq X\Rightarrow\alpha}\text{(asubl-inter)}\right)^\wedge \quad =$$

$$\dfrac{\dfrac{}{\Gamma \stackrel{\wedge}{\vdash} \bigwedge[\sigma_1..\sigma_n] \leq \sigma_i}\text{(sub-inter-lb)} \qquad c_i^\wedge}{\Gamma \stackrel{\wedge}{\vdash} \bigwedge[\sigma_1..\sigma_n] \leq X\Rightarrow\alpha}$$

$$\left(\frac{c_1 :: \Gamma \stackrel{.}{\vdash} \tau_1 \leq [\,]\Rightarrow\sigma_1 \qquad c_2 :: \Gamma \stackrel{.}{\vdash} \sigma_2 \leq X\Rightarrow\alpha}{\Gamma \stackrel{.}{\vdash} \sigma_1\to\sigma_2 \leq [\tau_1, X]\Rightarrow\alpha}\text{(asubl-arrow)}\right)^\wedge \quad =$$

$$\frac{c_1^\wedge \qquad c_2^\wedge}{\Gamma \stackrel{\wedge}{\vdash} \sigma_1\to\sigma_2 \leq [\tau_1, X]\Rightarrow\alpha}\text{(sub-arrow)}$$

$$\left(\frac{c_1 :: \Gamma \overset{\cdot}{\vdash} \tau_1 \leq [\,]{\Rightarrow}\sigma_1 \qquad c_2 :: \Gamma, \beta{\leq}\tau_1 \overset{\cdot}{\vdash} \sigma_2 \leq X{\Rightarrow}\alpha}{\Gamma \overset{\cdot}{\vdash} \forall\beta{\leq}\sigma_1.\ \sigma_2 \leq [\beta{\leq}\tau_1, X]{\Rightarrow}\alpha}\ \text{(ASUBL-ALL)}\right)^{\wedge} =$$

$$\frac{c_1^{\wedge} \qquad c_2^{\wedge}}{\Gamma \overset{\wedge}{\vdash} \forall\beta{\leq}\sigma_1.\ \sigma_2 \leq [\beta{\leq}\tau_1, X]{\Rightarrow}\alpha}\ \text{(SUB-ALL)}$$

$$\left(\frac{}{\Gamma \overset{\cdot}{\vdash} \alpha \leq [\,]{\Rightarrow}\alpha}\ \text{(ASUBL-REFL)}\right)^{\wedge} = \frac{}{\Gamma \overset{\wedge}{\vdash} \alpha \leq [\,]{\Rightarrow}\alpha}\ \text{(SUB-REFL)}$$

$$\left(\frac{c_1 :: \Gamma \overset{\cdot}{\vdash} \Gamma(\beta) \leq X{\Rightarrow}\alpha}{\Gamma \overset{\cdot}{\vdash} \beta \leq X{\Rightarrow}\alpha}\ \text{(ASUBL-TVAR)}\right)^{\wedge} = \frac{\dfrac{}{\Gamma \overset{\wedge}{\vdash} \beta \leq \Gamma(\beta)}\ \text{(SUB-TVAR)} \qquad c_1^{\wedge}}{\Gamma \overset{\wedge}{\vdash} \beta \leq X{\Rightarrow}\alpha}\ \text{(SUB-TRANS)}$$

5.3.8.6. Theorem: [Soundness of the algorithm] If $\Gamma \overset{\cdot}{\vdash} \sigma \leq X{\Rightarrow}\tau$ then $\Gamma \overset{\wedge}{\vdash} \sigma \leq X{\Rightarrow}\tau$.

Proof: By the well-formedness of the translation in Definition 5.3.8.5. □

We must now check that the relation defined by these rules coincides with the subtype relation on canonical types, from which it follows, by Theorem 5.3.7.6, that the algorithm gives a semi-decision procedure for the $F_\wedge$ subtype relation.

5.3.8.7. Lemma: [Completeness of the algorithm with respect to canonical subtyping] If $\Gamma^\flat \overset{\flat}{\vdash} \sigma^\flat \leq (X{\Rightarrow}\tau)^\flat$, then $\Gamma \overset{\cdot}{\vdash} \sigma \leq X{\Rightarrow}\tau$.

Proof: By induction on the size of a normal-form derivation of $\Gamma^\flat \overset{\flat}{\vdash} \sigma^\flat \leq (X{\Rightarrow}\tau)^\flat$, with a sub-induction on the form of τ and, when $\tau \equiv \alpha$, a sub-sub-induction on the form of σ. Proceed by cases on the form of τ and σ.

Case: $\tau \equiv \bigwedge[\tau_1..\tau_n] \qquad \Gamma^\flat \overset{\flat}{\vdash} \sigma^\flat \leq (X{\Rightarrow}\bigwedge[\tau_1..\tau_n])^\flat$

By Lemma 5.3.8.2(1), $\Gamma^\flat \overset{\flat}{\vdash} \sigma^\flat \leq \bigcup_i (X{\Rightarrow}\tau_i)^\flat$. By the syntax-directedness of canonical subtyping (5.3.6.3(1)), for every $\iota \in \bigcup_i (X{\Rightarrow}\tau_i)^\flat$ there is some $\kappa \in \sigma^\flat$ and a subderivation of the original whose conclusion is $\Gamma^\flat \overset{\flat}{\vdash} \kappa \leq \iota$. In particular, for each i and every $\iota \in (X{\Rightarrow}\tau_i)^\flat$ there is some $\kappa \in \sigma^\flat$ such that $\Gamma^\flat \overset{\flat}{\vdash} \kappa \leq \iota$. By CSub-AE, $\Gamma^\flat \overset{\flat}{\vdash} \sigma^\flat \leq (X{\Rightarrow}\tau_i)^\flat$. This derivation is no larger than the original and τ_i is smaller than τ, so, by the main or sub-induction hypothesis, $\Gamma \overset{\cdot}{\vdash} \sigma \leq X{\Rightarrow}\tau_i$. Then by rule ASubR-Inter, $\Gamma \overset{\cdot}{\vdash} \sigma \leq \bigwedge[\tau_1..\tau_n]$.

Case: $\tau \equiv \alpha \qquad \sigma \equiv \bigwedge[\sigma_1..\sigma_m] \qquad \Gamma^\flat \overset{\flat}{\vdash} \bigwedge[\sigma_1..\sigma_n]^\flat \leq (X{\Rightarrow}\alpha)^\flat$

Since $(X{\Rightarrow}\alpha)^\flat \equiv \bigwedge[\iota]$ is a singleton, the syntax-directedness of canonical subtyping (5.3.6.3(1)) implies that for some $\kappa \in \sigma^\flat$ we have $\Gamma^\flat \overset{\flat}{\vdash} \kappa \leq \iota$ as a subderivation of the original. Since $\sigma^\flat \equiv \bigcup_i \sigma_i^\flat$, there is some σ_i such that $\kappa \in \sigma_i^\flat$. CSub-AE then gives $\Gamma^\flat \overset{\flat}{\vdash} \sigma_i^\flat \leq (X{\Rightarrow}\alpha)^\flat$. This derivation is no larger than the original and σ_i is strictly smaller than σ, so by either the main or the sub-sub-induction hypothesis, $\Gamma \overset{\cdot}{\vdash} \sigma_i \leq X{\Rightarrow}\alpha$. By rule ASubL-Inter, $\Gamma \overset{\cdot}{\vdash} \sigma \leq X{\Rightarrow}\alpha$.

Case: $\tau \equiv \alpha \qquad \sigma \equiv \sigma_1{\rightarrow}\sigma_2 \qquad \Gamma^\flat \overset{\flat}{\vdash} (\sigma_1{\rightarrow}\sigma_2)^\flat \leq (X{\Rightarrow}\alpha)^\flat$

Since $(X{\Rightarrow}\alpha)^\flat \equiv \bigwedge[\iota]$ is a singleton, the syntax-directedness of canonical subtyping (5.3.6.3(1)) implies that for some $K_1{\rightarrow}\kappa_2 \in \sigma^\flat$ we have $\Gamma^\flat \overset{\flat}{\vdash} K_1{\rightarrow}\kappa_2 \leq \iota$ as a subderivation. By syntax-directedness again (5.3.6.3(2)), ι must have the form $I_1{\rightarrow}\iota_2$, with $\Gamma^\flat \overset{\flat}{\vdash} I_1 \leq K_1$ and $\Gamma^\flat \overset{\flat}{\vdash} \kappa_2 \leq \iota_2$ as subderivations. By Definition 5.3.8.1, $X \equiv [\tau_1, X_2]$, where $I_1 \equiv \tau_1^\flat$ and $\bigwedge[\iota_2] \equiv (X_2{\Rightarrow}\alpha)^\flat$. Since $\kappa_2 \in {\sigma_2}^\flat$, we have $\Gamma^\flat \overset{\flat}{\vdash} {\sigma_2}^\flat \leq (X_2{\Rightarrow}\alpha)^\flat$ by CSub-AE. This derivation is no larger than the original, and σ is strictly smaller, so by either the main or the sub-sub-induction hypothesis, $\Gamma \overset{\cdot}{\vdash} \sigma_2 \leq X_2{\Rightarrow}\alpha$. Also, by the main induction hypothesis, $\Gamma \overset{\cdot}{\vdash} \tau_1 \leq [\,]{\Rightarrow}\sigma_1$. By rule ASubL-Arrow, $\Gamma \overset{\cdot}{\vdash} \sigma_1{\rightarrow}\sigma_2 \leq \tau_1{\rightarrow}(X_2{\Rightarrow}\tau_2)$, i.e., $\Gamma \overset{\cdot}{\vdash} \sigma_1{\rightarrow}\sigma_2 \leq [\tau_1, X_2]{\Rightarrow}\tau_2$.

Case: $\tau \equiv \alpha \qquad \sigma \equiv \forall\alpha{\leq}\sigma_1.\ \sigma_2$

Similar.

Case: $\tau \equiv \alpha \qquad \sigma \equiv \beta \qquad \Gamma^\flat \overset{\flat}{\vdash} \beta^\flat \leq (X{\Rightarrow}\alpha)^\flat$

Since $\beta^\flat \equiv \bigwedge[\beta]$ and $(X{\Rightarrow}\alpha)^\flat \equiv \bigwedge[\iota]$ are both singletons, the syntax-directedness of canonical subtyping (5.3.6.3(1)) gives $\Gamma^\flat \overset{\flat}{\vdash} \beta \leq \iota$ as a subderivation. By syntax-directedness again (5.3.6.3(4)), either $\iota \equiv \beta$ or $\Gamma^\flat \overset{\flat}{\vdash} \Gamma^\flat(\beta) \leq \bigwedge[\iota]$. In the first case, rule ASubL-Refl gives the desired result immediately. In the second case, the main induction hypothesis gives $\Gamma \overset{!}{\vdash} \Gamma(\beta) \leq X{\Rightarrow}\alpha$, from which rule ASubL-TVar again yields $\Gamma \overset{!}{\vdash} \beta \leq X{\Rightarrow}\alpha$. □

5.3.8.8. Theorem: [Completeness of the algorithm with respect to ordinary subtyping] If $\Gamma \overset{\wedge}{\vdash} \sigma \leq X{\Rightarrow}\tau$ then $\Gamma \overset{!}{\vdash} \sigma \leq X{\Rightarrow}\tau$.

Proof: By the equivalence of ordinary and canonical subtyping (Theorem 5.3.7.6) and the completeness of the algorithm with respect to canonical subtyping (Lemma 5.3.8.7). □

5.3.8.9. Definition: The more convenient three-place relation $\Gamma \overset{!}{\vdash} \sigma \leq \tau$ may be defined as

$$\Gamma \overset{!}{\vdash} \sigma \leq \tau \quad \text{iff} \quad \Gamma \overset{!}{\vdash} \sigma \leq X{\Rightarrow}\phi,$$

where $\tau \equiv X{\Rightarrow}\phi$ and either $\phi \equiv \bigwedge[\phi_1..\phi_n]$ or $\phi \equiv \alpha$.

5.3.8.10. Theorem: [Equivalence of ordinary and syntax-directed subtyping]

$$\Gamma \overset{\wedge}{\vdash} \sigma \leq \tau \quad \text{iff} \quad \Gamma \overset{!}{\vdash} \sigma \leq \tau.$$

5.4 Typechecking

We now present an algorithm for synthesizing types for $F_\wedge$ terms. Given a term e and a context Γ (where e is closed in Γ), the algorithm constructs a minimal type σ for e under Γ — that is, a type σ such that $\Gamma \vdash e \in \sigma$, and such that any other type that can be derived for e from these rules is a supertype of σ.

The algorithm can be explained by separating the typing rules of Definition 3.2.2 into two sets: the *structural* or *syntax-directed* rules Var, Arrow-E, All-I, All-E, and For, whose applicability depends on the form of e, and the non-structural rules Inter-I and Sub, which can be applied without regard to the form of e. The non-structural rules are then removed from the system and their possible effects accounted for by modifying the structural rules Var, Arrow-E, All-E, and For appropriately.

The main novel source of difficulty here is the application rules Arrow-E and All-E. An application $(e_1\ e_2)$ in the original system has *every* type τ_2 such that e_1 can be shown to have some type $\tau_1{\rightarrow}\tau_2$ and e_2 can be shown to have type τ_1, where the rule Sub may be used on both sides to promote the types of e_1 and e_2 to supertypes with appropriate shapes. For example, if

$$e_1 \in (\sigma_1{\rightarrow}\sigma_2) \wedge (\forall\alpha{\leq}\sigma_3.\ \sigma_4) \wedge (\sigma_5{\rightarrow}\sigma_6) \wedge (\sigma_7{\rightarrow}\sigma_8)$$
$$e_2 \in \sigma_1 \wedge (\forall\alpha{\leq}\sigma_3.\ \sigma_4) \wedge \sigma_5,$$

then

$$(e_1\ e_2)$$

has both types σ_2 and σ_6, and hence (by Inter-I) also type $\sigma_2{\wedge}\sigma_6$.

To deal with this flexibility deterministically, we observe that the set of supertypes of $(\sigma_1{\rightarrow}\sigma_2) \wedge (\forall\alpha{\leq}\sigma_3.\ \sigma_4) \wedge (\sigma_5{\rightarrow}\sigma_6) \wedge (\sigma_7{\rightarrow}\sigma_8)$ that have the appropriate shape to appear as the type of e_1 in an instance of Arrow-E can be characterized finitely:

$$\begin{aligned}&\mathit{arrowbasis}((\sigma_1{\rightarrow}\sigma_2) \wedge (\forall\alpha{\leq}\sigma_3.\ \sigma_4) \wedge (\sigma_5{\rightarrow}\sigma_6) \wedge (\sigma_7{\rightarrow}\sigma_8))\\ &\quad = [\sigma_1{\rightarrow}\sigma_2,\ \sigma_5{\rightarrow}\sigma_6,\ \sigma_7{\rightarrow}\sigma_8].\end{aligned}$$

It is then a simple matter to characterize the possible types for $(e_1\ e_2)$ by checking whether the minimal type of e_2 is a subtype of each domain type in the finite arrow basis of the minimal type of e_1. Type applications are handled similarly.

5.4.1 Finite Bases for Applications

5.4.1.1. Definition: The functions $arrowbasis_\Gamma$ and $allbasis_\Gamma$ are defined as follows:

$$\begin{array}{lcl}
arrowbasis_\Gamma(\alpha) & = & arrowbasis_\Gamma(\Gamma(\alpha)) \\
arrowbasis_\Gamma(\tau_1 \rightarrow \tau_2) & = & [\tau_1 \rightarrow \tau_2] \\
arrowbasis_\Gamma(\forall\alpha{\leq}\tau_1.\ \tau_2) & = & [\,] \\
arrowbasis_\Gamma(\bigwedge[\tau_1..\tau_n]) & = & arrowbasis_\Gamma(\tau_1) * \cdots * arrowbasis_\Gamma(\tau_n) \\
\\
allbasis_\Gamma(\alpha) & = & allbasis_\Gamma(\Gamma(\alpha)) \\
allbasis_\Gamma(\tau_1 \rightarrow \tau_2) & = & [\,] \\
allbasis_\Gamma(\forall\alpha{\leq}\tau_1.\ \tau_2) & = & [\forall\alpha{\leq}\tau_1.\ \tau_2] \\
allbasis_\Gamma(\bigwedge[\tau_1..\tau_n]) & = & allbasis_\Gamma(\tau_1) * \cdots * allbasis_\Gamma(\tau_n).
\end{array}$$

To check that these definitions are proper, note that a closed context cannot contain cyclic chains of variable references where $\alpha_0 \in FTV(\Gamma(\alpha_1))$, $\alpha_1 \in FTV(\Gamma(\alpha_2))$, ..., $\alpha_n \in FTV(\Gamma(\alpha_0))$.

The next two lemmas verify that $arrowbasis_\Gamma$ and $allbasis_\Gamma$ compute finite bases for the sets of arrow types and polymorphic types above a given type.

5.4.1.2. Lemma: [Finite $\rightarrow$ basis computed by $arrowbasis_\Gamma$]

1. $\Gamma \overset{\wedge}{\vdash} \sigma \leq \bigwedge(arrowbasis_\Gamma(\sigma))$.
2. If $\Gamma \overset{\wedge}{\vdash} \sigma \leq \tau_1 \rightarrow \tau_2$, then $\Gamma \overset{\wedge}{\vdash} \bigwedge(arrowbasis_\Gamma(\sigma)) \leq \tau_1 \rightarrow \tau_2$.

Proof: See Appendix B. □

5.4.1.3. Lemma: [Finite $\forall$ basis computed by $allbasis_\Gamma$]

1. $\Gamma \vdash \sigma \leq \bigwedge(allbasis_\Gamma(\sigma))$.
2. If $\Gamma \vdash \sigma \leq (\forall\alpha{\leq}\tau_1.\ \tau_2)$, then $\Gamma \vdash \bigwedge(allbasis_\Gamma(\sigma)) \leq (\forall\alpha{\leq}\tau_1.\ \tau_2)$.

Proof: Similar. □

The crucial step in the correctness proof for the type synthesis algorithm is showing that application and type application are correctly characterized by the sets computed by *arrowbasis* and *allbasis*.

5.4.1.4. Lemma: [Application]
If

$$\begin{array}{l}
M \equiv [\phi_1 \rightarrow \psi_1 \mathrel{..} \phi_n \rightarrow \psi_n] \\
V \equiv [\psi_i \mid \Gamma \vdash \sigma \leq \phi_i] \\
\Gamma \vdash \bigwedge M \leq \tau_1 \rightarrow \tau_2 \\
\Gamma \vdash \sigma \leq \tau_1,
\end{array}$$

then

$$\Gamma \vdash \bigwedge V \leq \tau_2.$$

Proof: See Appendix B. □

5.4.1.5. Lemma: [Type application]

If

$M \equiv [(\forall\alpha{\leq}\phi_1.\ \psi_1)\,..\,(\forall\alpha{\leq}\phi_n.\ \psi_n)]$
$V \equiv [\{\sigma/\alpha\}\psi_i \mid \Gamma \vdash \sigma \leq \phi_i]$
$\Gamma \vdash \bigwedge M \leq (\forall\alpha{\leq}\tau_1.\ \tau_2)$
$\Gamma \vdash \sigma \leq \tau_1,$

then

$\Gamma \vdash \bigwedge V \leq \{\sigma/\alpha\}\tau_2.$

Proof: See Appendix B. □

5.4.2 Type Synthesis

5.4.2.1. Definition: The three-place *type synthesis relation* $\Gamma \overset{.}{\vdash} e \in \tau$ is the least relation closed under the following rules:

$$\Gamma \vdash x \in \Gamma(x) \qquad \text{(A-VAR)}$$

$$\frac{\Gamma,\, x{:}\tau_1 \vdash e \in \tau_2}{\Gamma \vdash \lambda x{:}\tau_1.\ e \in \tau_1{\rightarrow}\tau_2} \qquad \text{(A-ARROW-I)}$$

$$\frac{\Gamma \vdash e_1 \in \sigma_1 \qquad \Gamma \vdash e_2 \in \sigma_2}{\Gamma \vdash e_1\ e_2 \in \bigwedge[\psi_i \mid (\phi_i{\rightarrow}\psi_i) \in \mathit{arrowbasis}_\Gamma(\sigma_1) \text{ and } \Gamma \vdash \sigma_2 \leq \phi_i]} \qquad \text{(A-ARROW-E)}$$

$$\frac{\Gamma,\, \alpha{\leq}\tau_1 \vdash e \in \tau_2}{\Gamma \vdash \Lambda\alpha{\leq}\tau_1.\ e \in \forall\alpha{\leq}\tau_1.\ \tau_2} \qquad \text{(A-ALL-I)}$$

$$\frac{\Gamma \vdash e \in \sigma}{\Gamma \vdash e[\tau] \in \bigwedge[\{\tau/\alpha\}\psi_i \mid (\forall\alpha{\leq}\phi_i.\ \psi_i) \in \mathit{allbasis}_\Gamma(\sigma) \text{ and } \Gamma \vdash \tau \leq \phi_i]} \qquad \text{(A-ALL-E)}$$

$$\frac{\text{for all } i,\ \Gamma \vdash \{\sigma_i/\alpha\}e \in \tau_i}{\Gamma \vdash \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e \in \bigwedge[\tau_1..\tau_n]} \qquad \text{(A-FOR)}$$

Again, turnstiles in type synthesis derivations are sometimes marked $\overset{.}{\vdash}$ to distinguish them from derivations in other calculi.

5.4.2.2. Lemma: [Syntax-directedness of the type synthesis rules] For given Γ and e, there is at most one rule that can be used to establish $\Gamma \overset{.}{\vdash} e \in \tau$ for some τ. Moreover, the existence of such a derivation can be established from the form of e and the results of applying the type synthesis procedure to proper subphrases of e plus a finite number of applications of the subroutine for checking the subtyping relation. In particular:

1. If $\Gamma \overset{.}{\vdash} x \in \theta$, then $\theta \equiv \Gamma(x)$.
2. If $\Gamma \overset{.}{\vdash} \lambda x{:}\tau_1.\ e \in \theta$, then $\theta \equiv \tau_1{\rightarrow}\tau_2$, where $\Gamma,\, x{:}\tau_1 \overset{.}{\vdash} e \in \tau_2$ as a subderivation.
3. If $\Gamma \overset{.}{\vdash} e_1 e_2 \in \theta$, then $\theta \equiv \bigwedge[\psi_i \mid (\phi_i{\rightarrow}\psi_i) \in \mathit{arrowbasis}_\Gamma(\sigma_1) \text{ and } \Gamma \vdash \sigma_2 \leq \phi_i]$, where $\Gamma \overset{.}{\vdash} e_1 \in \sigma_1$ and $\Gamma \overset{.}{\vdash} e_2 \in \sigma_2$ as subderivations.
4. If $\Gamma \overset{.}{\vdash} \Lambda\alpha{\leq}\tau_1.\ e \in \theta$, then $\theta \equiv \forall\alpha{\leq}\tau_1.\ \tau_2$, where $\Gamma,\, \alpha{\leq}\tau_1 \overset{.}{\vdash} e \in \tau_2$ as a subderivation.
5. If $\Gamma \overset{.}{\vdash} e[\tau] \in \theta$, then $\theta \equiv \bigwedge[\{\tau/\alpha\}\psi_i \mid (\forall\alpha{\leq}\phi_i.\ \psi_i) \in \mathit{allbasis}_\Gamma(\sigma_1) \text{ and } \Gamma \vdash \tau \leq \phi_i]$, where $\Gamma \overset{.}{\vdash} e \in \sigma_1$ as a subderivation.
6. If $\Gamma \overset{.}{\vdash} \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e \in \theta$, then $\theta \equiv \bigwedge[\tau_1..\tau_n]$, where $\Gamma \overset{.}{\vdash} \{\sigma_i/\alpha\}e \in \tau_i$, for each i, as a subderivation.

Proof: By inspection. □

5.4.2.3. Remark: The syntax-directedness of algorithmic derivations permits us to skip introducing a linear shorthand, as we did for ordinary and canonical derivations, since terms themselves are essentially the shorthand we need.

5.4.2.4. Definition: Let $c :: \Gamma \mathrel{\dot{\vdash}} e \in \tau$ be a typing derivation from the algorithmic rules (5.4.2.1). Then $c^{\wedge} :: \Gamma \vdash^{\wedge} e \in \tau$ is the following derivation from the ordinary typing rules:

$$\left(\frac{}{\Gamma \mathrel{\dot{\vdash}} x \in \Gamma(x)}\;{\scriptstyle(\text{A-VAR})}\right)^{\wedge} \quad = \quad \frac{}{\Gamma \vdash^{\wedge} x \in \Gamma(x)}\;{\scriptstyle(\text{VAR})}$$

$$\left(\frac{c_1 :: \Gamma,\, x{:}\tau_1 \mathrel{\dot{\vdash}} e \in \tau_2}{\Gamma \mathrel{\dot{\vdash}} (\lambda x{:}\tau_1.\ e) \in \tau_1 \rightarrow \tau_2}\;{\scriptstyle(\text{A-ARROW-I})}\right)^{\wedge} \quad = \quad \frac{c_1^{\wedge}}{\Gamma \vdash^{\wedge} (\lambda x{:}\tau_1.\ e) \in \tau_1 \rightarrow \tau_2}\;{\scriptstyle(\text{ARROW-I})}$$

$$\left(\frac{c_1 :: \Gamma \mathrel{\dot{\vdash}} e_1 \in \sigma_1 \qquad c_2 :: \Gamma \mathrel{\dot{\vdash}} e_2 \in \sigma_2}{\Gamma \mathrel{\dot{\vdash}} (e_1\ e_2) \in \bigwedge[\psi_i \mid (\phi_i \rightarrow \psi_i) \in \mathit{arrowbasis}_{\Gamma}(\sigma_1) \text{ and } d_i :: \Gamma \vdash \sigma_2 \leq \phi_i]}\;{\scriptstyle(\text{A-ARROW-E})}\right)^{\wedge} \quad =$$

$$\frac{\cdots \quad \dfrac{\dfrac{c_1^{\wedge} \qquad 5.4.1.2 :: \Gamma \vdash^{\wedge} \sigma_1 \leq \phi_i \rightarrow \psi_i}{\Gamma \vdash^{\wedge} e_1 \in \phi_i \rightarrow \psi_i}\;{\scriptstyle(\text{SUB})} \qquad \dfrac{c_2^{\wedge} \qquad d_i^{\wedge}}{\Gamma \vdash^{\wedge} e_2 \in \phi_i}\;{\scriptstyle(\text{SUB})}}{\Gamma \vdash^{\wedge} (e_1\ e_2) \in \psi_i}\;{\scriptstyle(\text{ARROW-E})} \quad \cdots}{\Gamma \vdash^{\wedge} (e_1\ e_2) \in \bigwedge[\psi_i \mid (\phi_i \rightarrow \psi_i) \in \mathit{arrowbasis}_{\Gamma}(\sigma_1) \text{ and } \Gamma \vdash \sigma_2 \leq \phi_i]}\;{\scriptstyle(\text{INTER-I})}$$

$$\left(\frac{c_1 :: \Gamma,\, \alpha{\leq}\tau_1 \mathrel{\dot{\vdash}} e \in \tau_2}{\Gamma \mathrel{\dot{\vdash}} (\Lambda\alpha{\leq}\tau_1.\ e) \in \forall\alpha{\leq}\tau_1.\ \tau_2}\;{\scriptstyle(\text{A-ALL-I})}\right)^{\wedge} \quad = \quad \frac{c_1^{\wedge}}{\Gamma \vdash^{\wedge} (\Lambda\alpha{\leq}\tau_1.\ e) \in \forall\alpha{\leq}\tau_1.\ \tau_2}\;{\scriptstyle(\text{ALL-I})}$$

$$\left(\frac{c_1 :: \Gamma \mathrel{\dot{\vdash}} e \in \sigma_1}{\Gamma \mathrel{\dot{\vdash}} e\,[\tau] \in \bigwedge[\{\tau/\alpha\}\psi_i \mid (\forall\alpha{\leq}\phi_i.\ \psi_i) \in \mathit{allbasis}_{\Gamma}(\sigma_1) \text{ and } d_i :: \Gamma \vdash \tau \leq \phi_i]}\;{\scriptstyle(\text{A-ALL-E})}\right)^{\wedge} \quad =$$

$$\frac{\cdots \quad \dfrac{\dfrac{c_1^{\wedge} \qquad 5.4.1.3 :: \Gamma \vdash^{\wedge} \sigma_1 \leq \forall\alpha{\leq}\phi_i.\ \psi_i}{\Gamma \vdash^{\wedge} e \in \forall\alpha{\leq}\phi_i.\ \psi_i}\;{\scriptstyle(\text{SUB})} \qquad d_i^{\wedge}}{\Gamma \vdash^{\wedge} e\,[\tau] \in \{\tau/\alpha\}\psi_i}\;{\scriptstyle(\text{ALL-E})} \quad \cdots}{\Gamma \vdash^{\wedge} e\,[\tau] \in \bigwedge[\{\tau/\alpha\}\psi_i \mid (\forall\alpha{\leq}\phi_i.\ \psi_i) \in \mathit{allbasis}_{\Gamma}(\sigma_1) \text{ and } \Gamma \vdash \tau \leq \phi_i]}\;{\scriptstyle(\text{INTER-I})}$$

$$\left(\frac{\text{for all } i,\ c_i :: \Gamma \mathrel{\dot{\vdash}} \{\sigma_i/\alpha\}e \in \tau_i}{\Gamma \mathrel{\dot{\vdash}} (\mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e) \in \bigwedge[\tau_1..\tau_n]}\;{\scriptstyle(\text{A-FOR})}\right)^{\wedge} \quad =$$

$$\frac{\cdots \quad \dfrac{c_i^{\wedge} :: \Gamma \vdash^{\wedge} \{\sigma_i/\alpha\}e \in \tau_i}{\Gamma \vdash^{\wedge} (\mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e) \in \tau_i}\;{\scriptstyle(\text{FOR})} \quad \cdots}{\Gamma \vdash^{\wedge} (\mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e) \in \bigwedge[\tau_1..\tau_n]}\;{\scriptstyle(\text{INTER-I})}$$

5.4.2.5. Theorem: If $s :: \Gamma \mathrel{\dot{\vdash}} e \in \tau$, then $s^{\wedge} :: \Gamma \vdash^{\wedge} e \in \tau$.

Proof: By induction on the structure of s. □

5.4.2.6. Theorem: [Minimal typing] If $\Gamma \mathrel{\dot{\vdash}} e \in \sigma$ and $\Gamma \vdash^{\wedge} e \in \tau$, then $\Gamma \vdash \sigma \leq \tau$.

Proof: By induction on a derivation of $\Gamma \vdash^{\wedge} e \in \tau$. Proceed by cases on the final rule.

Case Var: $e \equiv x \qquad \tau \equiv \Gamma(x)$

Immediate by A-Var.

Case Arrow-I: $e \equiv \lambda x{:}\tau_1.\ e' \qquad \Gamma,\ x{:}\tau_1 \ \hat{\vdash}\ e' \in \tau_2 \qquad \tau \equiv \tau_1 \rightarrow \tau_2$

By the syntax-directedness of the type synthesis rules (5.4.2.2), the last rule in the derivation of $\Gamma \dot{\vdash} e \in \sigma$ must be A-ARROW-I, so

$\Gamma,\ x{:}\tau_1 \vdash e' \in \sigma_2$

$\sigma \equiv \tau_1 \rightarrow \sigma_2.$

By the induction hypothesis, $\Gamma \ \hat{\vdash}\ \sigma_2 \leq \tau_2$. By SUB-REFL and SUB-ARROW,

$\Gamma \ \hat{\vdash}\ \tau_1 \rightarrow \sigma_2 \leq \tau_1 \rightarrow \tau_2.$

Case Arrow-E: $e \equiv e_1\ e_2 \qquad \Gamma \ \hat{\vdash}\ e_1 \in \tau_1 \rightarrow \tau_2 \qquad \Gamma \ \hat{\vdash}\ e_2 \in \tau_1 \qquad \tau \equiv \tau_2$

By the syntax-directedness of the type synthesis rules (5.4.2.2),

$\Gamma \dot{\vdash} e_1 \in \sigma_1$

$\Gamma \dot{\vdash} e_2 \in \sigma_2$

$\sigma \equiv \bigwedge[\psi_i \mid (\phi_i \rightarrow \psi_i) \in \mathit{arrowbasis}_\Gamma(\sigma_1) \text{ and } \Gamma \dot{\vdash} \sigma_2 \leq \phi_i].$

By the equivalence of ordinary and syntax-directed subtyping (5.3.8.10),

$\sigma \equiv \bigwedge[\psi_i \mid (\phi_i \rightarrow \psi_i) \in \mathit{arrowbasis}_\Gamma(\sigma_1) \text{ and } \Gamma \ \hat{\vdash}\ \sigma_2 \leq \phi_i].$

By the induction hypothesis,

$\Gamma \ \hat{\vdash}\ \sigma_1 \leq \tau_1 \rightarrow \tau_2$

$\Gamma \ \hat{\vdash}\ \sigma_2 \leq \tau_1.$

Since $\mathit{arrowbasis}_\Gamma(\sigma_1)$ is a finite basis for the arrow types above σ_1 (5.4.1.2),

$\Gamma \ \hat{\vdash}\ \bigwedge(\mathit{arrowbasis}_\Gamma(\sigma_1)) \leq \tau_1 \rightarrow \tau_2.$

By the application lemma (5.4.1.4),

$\Gamma \ \hat{\vdash}\ \bigwedge[\psi_i \mid (\phi_i \rightarrow \psi_i) \in \mathit{arrowbasis}_\Gamma(\sigma_1) \text{ and } \Gamma \ \hat{\vdash}\ \sigma_2 \leq \phi_i] \leq \tau_2.$

Case All-I: $e \equiv \Lambda\alpha{\leq}\tau_1.\ e' \qquad \Gamma,\ \alpha{\leq}\tau_1 \ \hat{\vdash}\ e' \in \tau_2 \qquad \tau \equiv \forall\alpha{\leq}\tau_1.\ \tau_2$

By the syntax-directedness of the type synthesis rules (5.4.2.2),

$\Gamma,\ \alpha{\leq}\tau_1 \dot{\vdash} e' \in \sigma_2$

$\sigma \equiv \forall\alpha{\leq}\tau_1.\ \sigma_2.$

By the induction hypothesis,

$\Gamma,\ \alpha{\leq}\tau_1 \ \hat{\vdash}\ \sigma_2 \leq \tau_2.$

By SUB-REFL and SUB-ALL,

$\Gamma \ \hat{\vdash}\ (\forall\alpha{\leq}\tau_1.\ \sigma_2) \leq (\forall\alpha{\leq}\tau_1.\ \tau_2).$

Case All-E: $e \equiv e'[\tau'] \qquad \Gamma \ \hat{\vdash}\ e' \in \forall\alpha{\leq}\tau_1.\ \tau_2 \qquad \Gamma \ \hat{\vdash}\ \tau' \leq \tau_1 \qquad \tau \equiv \{\tau'/\alpha\}\tau_2$

By the syntax-directedness of the type synthesis rules (5.4.2.2),

$\Gamma \dot{\vdash} e' \in \sigma_1$

$\sigma \equiv \bigwedge[\{\tau'/\alpha\}\psi_i \mid (\forall\alpha{\leq}\phi_i.\ \psi_i) \in \mathit{allbasis}_\Gamma(\sigma_1) \text{ and } \Gamma \dot{\vdash} \tau' \leq \phi_i].$

By the equivalence of ordinary and syntax-directed subtyping (5.3.8.10),

$\sigma \equiv \bigwedge[\{\tau'/\alpha\}\psi_i \mid (\forall\alpha{\leq}\phi_i.\ \psi_i) \in \mathit{allbasis}_\Gamma(\sigma_1) \text{ and } \Gamma \ \hat{\vdash}\ \tau' \leq \phi_i].$

By the induction hypothesis,

$\Gamma \ \hat{\vdash}\ \sigma_1 \leq \forall\alpha{\leq}\tau_1.\ \tau_2.$

Since $\mathit{allbasis}_\Gamma(\sigma_1)$ is a finite basis for the polymorphic types above σ_1 (5.4.1.3),

$\Gamma \ \hat{\vdash}\ \bigwedge(\mathit{allbasis}_\Gamma(\sigma_1)) \leq \forall\alpha{\leq}\tau_1.\ \tau_2.$

By the type application lemma (5.4.1.5),

$\Gamma \ \hat{\vdash}\ \bigwedge[\{\tau'/\alpha\}\psi_i \mid (\forall\alpha{\leq}\phi_i.\ \psi_i) \in \mathit{allbasis}_\Gamma(\sigma_1) \text{ and } \Gamma \vdash \tau' \leq \phi_i] \leq \{\tau'/\alpha\}\tau_2.$

Case For: $e \equiv \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e'$ $\quad \Gamma \overset{\wedge}{\vdash} \{\sigma_i/\alpha\}e \in \tau_i \quad \tau \equiv \tau_i$

By the syntax-directedness of the type synthesis rules (5.4.2.2),

for all j, $\Gamma \overset{\cdot}{\vdash} \{\sigma_j/\alpha\}e \in \phi_j$

$\sigma \equiv \bigwedge[\phi_1..\phi_n]$.

By the induction hypothesis,

$\Gamma \overset{\wedge}{\vdash} \phi_i \leq \tau_i$.

By SUB-INTER-LB and SUB-TRANS,

$\Gamma \overset{\wedge}{\vdash} \bigwedge[\phi_1..\phi_n] \leq \tau_i$.

Case Inter-I: for all i, $\Gamma \overset{\wedge}{\vdash} e \in \tau_i \quad \tau \equiv \bigwedge[\tau_1..\tau_n]$

By the induction hypothesis,

for all i, $\Gamma \overset{\wedge}{\vdash} \sigma \leq \tau_i$.

By SUB-INTER-G,

$\Gamma \overset{\wedge}{\vdash} \sigma \leq \bigwedge[\tau_1..\tau_n]$.

Case Sub: $\Gamma \overset{\wedge}{\vdash} e \in \tau_1 \quad \Gamma \overset{\wedge}{\vdash} \tau_1 \leq \tau_2 \quad \tau \equiv \tau_2$

By the induction hypothesis,

$\Gamma \overset{\wedge}{\vdash} \sigma \leq \tau_1$.

By SUB-TRANS,

$\Gamma \overset{\wedge}{\vdash} \sigma \leq \tau_2$.

□

5.4.3 Conservativity

$F_\wedge$ was described as essentially the union of the two simpler calculi $\lambda_\wedge$ and $F_\leq$. We can gauge the accuracy of this characterization by checking whether the features of the component calculi operate "orthogonally," so that each component system can be thought of as a restriction of $F_\wedge$— i.e., by asking whether $F_\wedge$ is a conservative extension of $\lambda_\wedge$ and of $F_\leq$.

5.4.3.1. Definition: Let C and E be two calculi and $E(—) \in C \rightarrow E$ an injective mapping from C statements to E statements. $E(—)$ is said to be an *embedding* of C into E if, for every C statement J, J is derivable in C iff $E(J)$ is derivable in E.

Typically, $E(—)$ is just an identity injection. For instance, this is the case for the embedding of $\lambda_\wedge$ into $F_\wedge$.

5.4.3.2. Definition: If the identity injection is an embedding of C into E, then E is said to be a *conservative extension* of C.

5.4.3.3. Theorem: Let σ and τ be $\lambda_\wedge$ types, Γ an $\lambda_\wedge$ context, and e an $\lambda_\wedge$ expression. Assume that the primitive subtype relation of $\lambda_\wedge$ is encoded as a context Γ_P (c.f. 3.3.2.2). Then:

1. $\Gamma_P, \Gamma \overset{\wedge}{\vdash} \sigma \leq \tau$ iff $\Gamma \overset{\lambda\wedge}{\vdash} \sigma \leq \tau$.
2. $\Gamma_P, \Gamma \overset{\wedge}{\vdash} e \in \tau$ iff $\Gamma \overset{\lambda\wedge}{\vdash} e \in \tau$.

Proof: See Appendix B. □

The mapping from the other subsystem, $F_\leq$, into $F_\wedge$ must take the type *Top* into $\top$, and it is here that it fails to be an embedding (as we might expect from the discussion in Section 3.3). For example, the subtyping statement

$\vdash\ \mathit{Top} \leq \forall\alpha{\leq}\mathit{Top}.\ \mathit{Top}$

is derivable in $F_\wedge$(reading *Top* as $\top$), but not in $F_\leq$.

5.4.3.4. Conjecture: Since *Top* must be mapped to a maximal type by any embedding function from $F_\leq$ to $F_\wedge$ and $\top$ is the only such type (up to equivalence), there is probably *no* embedding of $F_\leq$ into $F_\wedge$.

5.4.3.5. Conjecture: By replacing *Top* with $\top$ in $F_\leq$ and adding appropriate distributivity laws to the subtyping relation and a $\top$-introduction rule to the typing relation, we can construct a system that can be embedded into $F_\wedge$ (indeed, such that $F_\wedge$ extends it conservatively), but this system is only a technical curiosity: it has most of the problematic features of $F_\wedge$ (the distributivity laws in particular) but is much less expressive.

6 Semantics

This section presents two results about the semantics of $F_\wedge$. Section 6.1 gives a simple untyped semantics for $F_\wedge$ based on Bruce and Longo's partial equivalence relation model for $F_\leq$ [7]. Section 6.2 discusses a negative technical result — the nonexistence of syntactic least upper bounds — with some serious implications for the difficulty of constructing a typed model for $F_\wedge$ in which the subtype relation is interpreted by semantic coercion functions.

6.1 Untyped Semantics

One of the simplest styles of semantics for typed λ-calculi is based on partial equivalence relations (PERs). A model in this style is essentially untyped: terms are interpreted by erasing all type information and interpreting the resulting pure λ-term as an element of the model. A type in this setting is just a subset of the model along with an appropriate notion of equivalence of elements. Coercions between types are interpreted as inclusion of PERs.

The PER model given here for $F_\wedge$ is based on Bruce and Longo's model for $F_\leq$ [7]. However, the full generality of Bruce and Longo's construction, involving the category of ω-sets, is not required.

The usual interpretation of a quantified type $\forall\alpha.\ \tau$ in a second-order PER model is the PER-indexed intersection of all instances of τ. Bruce and Longo showed how to extend this definition to interpret a bounded quantifier $\forall\alpha{\leq}\sigma.\ \tau$ as the intersection of all the instances of τ where α is interpreted as a sub-PER of the interpretation of σ. This intuition also serves for intersection types: $\bigwedge[\tau_1..\tau_n]$ is interpreted as the intersection of the PERs interpreting each of the τ_i's.

We need to make one significant departure here from PER models of $F_\leq$: instead of allowing the elements of our PERs to be drawn from the carrier of an arbitrary partial combinatory algebra $\mathcal{D}$, we require that $\mathcal{D}$ be a *total* combinatory algebra. This restriction is needed to validate nullary instances of the distributive law SUB-DIST-IA, which have the form $\Gamma \vdash \top \leq \sigma{\rightarrow}\top$. To see why, let $\sigma \equiv \top$. The empty intersection $\top$ is interpreted by the everywhere-defined PER, i.e., $[\![\top]\!]$ relates every m to itself. To validate the distributivity law, it must therefore be the case that $[\![\top{\rightarrow}\top]\!]$ relates every element to itself. But this will only be true if the application of any element to any other element is defined. This observation is due to QingMing Ma [personal communication, 1991].

The notation and fundamental definitions used in this section are based on papers of Bruce and Longo [7], Freyd, Mulry, Rosolini, and Scott [45], and others. A good basic reference for PER models of second-order λ-calculi is [59]; also see [8] for more general discussion of second-order models and [2, 52] for general discussion of combinatory models.

6.1.1 Background

6.1.1.1. Definition: A *total combinatory algebra* is a tuple $\mathcal{D} = \langle D, \cdot, k, s\rangle$ comprising

- a set D of *elements*,
- an *application function* $\cdot$ with type $D \rightarrow (D \rightarrow D)$,
- distinguished elements k, $s \in D$,

such that, for all d_1, d_2, $d_3 \in D$,

$$\begin{aligned} &k \cdot d_1 \cdot d_2 = d_1 \\ &s \cdot d_1 \cdot d_2 \cdot d_3 = (d_1 \cdot d_3) \cdot (d_2 \cdot d_3). \end{aligned}$$

Throughout this section, we work with a fixed, but unspecified, total combinatory algebra $\mathcal{D}$. For example, think of Scott's D_∞ or P_ω [74] model.)

The set of *pure λ-terms* is:

$$M \quad ::= \quad x \quad | \quad \lambda x.\ M \quad | \quad M_1\ M_2$$

The set of *combinator terms* is:

$$C \quad ::= \quad x \quad | \quad C_1\ C_2 \quad | \quad K \quad | \quad S$$

The *bracket abstraction* of a combinator term C with respect to a variable x, written $\lambda^\star x.\ C$, is:

$$\begin{array}{lll} \lambda^\star x.\ C & = K\ C & \text{when } x \notin FV(C) \\ \lambda^\star x.\ x & = S\ K\ K & \\ \lambda^\star x.\ C_1\ C_2 & = S\ (\lambda^\star x.\ C_1)\ (\lambda^\star x.\ C_2) & \text{when } x \in FV(C_1\ C_2) \end{array}$$

The *combinator translation* of a pure λ-term M, written $|M|$, is defined as follows:

$$\begin{array}{ll} |x| & = x \\ |\lambda x.\ M| & = \lambda^\star x.\ |M| \\ |M_1\ M_2| & = |M_1|\ |M_2| \end{array}$$

An *environment* η is a finite function from type variables to PERs (defined below) and term variables to elements of D. When $x \notin dom(\eta)$, we write $\eta[x \leftarrow d]$ for the environment that maps x to d and agrees with η everywhere else; $\eta[\alpha \leftarrow A]$ is defined similarly. We write $\eta \backslash x$ for the environment like η except that $\eta(x)$ is undefined; $\eta \backslash \alpha$ similarly. We say that η' *extends* η when $dom(\eta) \subseteq dom(\eta')$ and η and η' agree on $dom(\eta)$.

Let C be a combinator term and η an environment such that $FV(C) \subseteq dom(\eta)$. Then the *interpretation* of C under η, written $[\![C]\!]_\eta$, is defined as follows:

$$\begin{array}{ll} [\![x]\!]_\eta & = \eta(x) \\ [\![C_1\ C_2]\!]_\eta & = [\![C_1]\!]_\eta \cdot [\![C_2]\!]_\eta \\ [\![K]\!]_\eta & = k \\ [\![S]\!]_\eta & = s \end{array}$$

6.1.1.2. Lemma: If η' extends η and $FV(C) \subseteq dom(\eta)$, then $[\![C]\!]_\eta = [\![C]\!]_{\eta'}$.

Proof: Straightforward induction on C. □

6.1.1.3. Lemma: $[\![\lambda^\star x.\ C]\!]_\eta \cdot m = [\![C]\!]_{\eta[x \leftarrow m]}$.

Proof: See Appendix B. □

6.1.1.4. Definition: A *partial equivalence relation* (PER) on $\mathcal{D}$ is a symmetric and transitive relation A on D. We write $m\ \{A\}\ n$ when A relates m and n. The *domain* of A, written $dom(A)$, is the set $\{n \mid n\ \{A\}\ n\}$. Note that $m\ \{A\}\ n$ implies $m \in dom(A)$.

Let A and B be relations. Then $A \rightarrow B$ is the relation defined by

$m\ \{A \rightarrow B\}\ n$ iff for all $p, q \in D$, $p\ \{A\}\ q$ implies $m \cdot p\ \{B\}\ n \cdot q$.

6.1.1.5. Lemma: $A \rightarrow B$ is a PER when A and B are PERs.

Proof: Standard. $\square$

6.1.1.6. Definition: A is a *subrelation* of B, written $A \subseteq B$, iff $m\ \{A\}\ n$ implies $m\ \{B\}\ n$ for all $m, n \in D$.

6.1.1.7. Definition: Let $\{A_i\}_{i \in I}$ be a set of relations indexed by a set I. Then $\bigcap_{i \in I} A_i$ is the relation defined by

$m\ \{\bigcap_{i \in I} A_i\}\ n$ iff for every i, $m\ \{A_i\}\ n$.

6.1.1.8. Lemma: $\bigcap_{i \in I} A_i$ is a PER when all the A_i's are PERs.

Proof: Straightforward. $\square$

6.1.2 PER Interpretation of $F_\wedge$

6.1.2.1. Definition: The *erasure* of an $F_\wedge$ term e, written $erase(e)$, is the pure λ-term defined as follows:

$$
\begin{array}{lcl}
erase(x) & = & x \\
erase(\lambda x{:}\tau.\ e) & = & \lambda x.\ erase(e) \\
erase(e_1\ e_2) & = & erase(e_1)\ erase(e_2) \\
erase(\Lambda \alpha \leq \tau.\ e) & = & erase(e) \\
erase(e\ [\tau]) & = & erase(e) \\
erase(for\ \alpha\ in\ \sigma_1..\sigma_n.\ e) & = & erase(e)
\end{array}
$$

6.1.2.2. Definition: Let η be an environment and e an expression such that $FV(e) \subseteq dom(\eta)$. Then the *interpretation* of e under η, written $[\![e]\!]_\eta$, is $[\![|erase(e)|]\!]_\eta$.

6.1.2.3. Lemma: $[\![\lambda x{:}\tau.\ e]\!]_\eta = [\![\lambda^\star x.\ |erase(e)|]\!]_\eta$.

Proof: Straightforward. $\square$

6.1.2.4. Definition: Let η be an environment and τ a type expression such that $FTV(\tau) \subseteq dom(\eta)$. The *interpretation* of τ under η, written $[\![\tau]\!]_\eta$, is the PER defined as follows:

$$
\begin{array}{lcl}
[\![\alpha]\!]_\eta & = & \eta(\alpha) \\
[\![\tau_1 \rightarrow \tau_2]\!]_\eta & = & [\![\tau_1]\!]_\eta \rightarrow [\![\tau_2]\!]_\eta \\
[\![\forall \alpha \leq \tau_1.\ \tau_2]\!]_\eta & = & \bigcap_{A \subseteq [\![\tau_1]\!]_\eta} [\![\tau_2]\!]_{\eta[\alpha \leftarrow A]} \quad \text{where } A \text{ is a PER} \\
[\![\bigwedge[\tau_1..\tau_n]]\!]_\eta & = & \bigcap_{1 \leq i \leq n} [\![\tau_i]\!]_\eta
\end{array}
$$

6.1.2.5. Definition: An environment η *satisfies* a context Γ, written $\eta \models \Gamma$, if $dom(\eta) = dom(\Gamma)$ and

1. $\Gamma \equiv \{\}$, or
2. $\Gamma \equiv \Gamma_1, x : \tau$, where $\eta \backslash x$ satisfies Γ_1 and $\eta(x) \in dom([\![\tau]\!]_{\eta \backslash x})$, or
3. $\Gamma \equiv \Gamma_1, \alpha \leq \tau$, where $\eta \backslash \alpha$ satisfies Γ_1 and $\eta(\alpha) \subseteq [\![\tau]\!]_{\eta \backslash \alpha}$.

6.1.2.6. Lemma: If η' extends η and $FTV(\tau) \subseteq dom(\eta)$, then $[\![\tau]\!]_\eta = [\![\tau]\!]_{\eta'}$.

Proof: Straightforward. $\square$

6.1.2.7. Lemma: (Soundness of subtyping) If $\Gamma \vdash \sigma \leq \tau$ and $\eta \models \Gamma$, then $[\![\sigma]\!]_\eta \subseteq [\![\tau]\!]_\eta$.

Proof: See Appendix B. $\square$

6.1.2.8. Lemma:

1. $[\![e_1\, e_2]\!]_\eta = [\![e_1]\!]_\eta \cdot [\![e_2]\!]_\eta$.
2. $erase(\{\sigma/\alpha\}e) = erase(e)$.
3. $[\![\tau]\!]_{\eta[\alpha \leftarrow [\![\sigma]\!]_\eta]} = [\![\{\sigma/\alpha\}\tau]\!]_\eta$.
4. $[\![C]\!]_{\eta[x \leftarrow [\![C']\!]_\eta]} = [\![\{C'/x\}C]\!]_\eta$.
5. $\{|erase(v)|/x\}|erase(f)| = |erase(\{v/x\}f)|$.

Proof: Straightforward. $\square$

6.1.2.9. Lemma: If

$$
\begin{array}{l}
\eta_1 \models \Gamma \\
\eta_2 \models \Gamma \\
\forall \alpha \in dom(\Gamma).\ \eta_1(\alpha) = \eta_2(\alpha) = \eta(\alpha) \\
\forall x \in dom(\Gamma).\ \eta_1(x)\, \{[\![\Gamma(x)]\!]_\eta\}\, \eta_2(x) \\
\Gamma \ \vdash \ e \ \in \ \tau,
\end{array}
$$

then

$$[\![e]\!]_{\eta_1}\ \{[\![\tau]\!]_\eta\}\ [\![e]\!]_{\eta_2}.$$

(Here η is just a convenient name for the portions of η_1 and η_2 dealing with type variables, which must be identical.)

Proof: See Appendix B. $\square$

6.1.2.10. Corollary: (Soundness of typing) If $\Gamma \vdash e \in \tau$ and $\eta \models \Gamma$, then $[\![e]\!]_\eta \in dom([\![\tau]\!]_\eta)$.

Proof: Take $\eta_1 = \eta_2 = \eta$. $\square$

6.2 Nonexistence of Least Upper Bounds

One important question about the order-theoretic properties of any calculus with subtyping is the existence or nonexistence of *least upper bounds* (lubs) for finite sets of types. When they are present, lubs often greatly simplify the presentations of both semantic and proof-theoretic arguments; for example, Reynolds' model construction for Forsythe depends on the existence and special properties of lubs. Unfortunately, like its component system $F_\leq$ (though not for exactly the same reason), $F_\wedge$ does *not* have a lub for every finite set of types.

To simplify the discussion, we consider only lubs of pairs of types. The fact that a calculus of intersection types may be formulated in terms of an n-ary meet constructor, as we have done here, or, equivalently, in terms of $\top$ and binary meets, implies that we may make this simplification without loss of generality.

6.2.1. Definition: Let σ and τ be types, both closed under a context Γ. Then a *least upper bound* of σ and τ under Γ is a supertype of both σ and τ and a subtype of every common supertype of σ and τ — that is, a type θ such that:

$$
\begin{array}{l}
\Gamma \ \vdash \ \sigma \ \leq \ \theta \\
\Gamma \ \vdash \ \tau \ \leq \ \theta \\
\Gamma \ \vdash \ \sigma \ \leq \ \phi \quad \text{and} \quad \Gamma \ \vdash \ \tau \ \leq \ \phi \quad \text{imply} \quad \Gamma \ \vdash \ \theta \ \leq \ \phi.
\end{array}
$$

In systems with intersection types, it is simplest to define least upper bounds for canonical types (c.f. Section 5.3.1) and then transfer the definition to ordinary types. Here is Reynolds' definition of lubs for the canonical formulation of first-order intersection types:

6.2.2. Definition: Assume that we are given a partial function $\sqcup_P$ that yielding a least upper bound for every pair of primitive types with any upper bound. That is:

$$\begin{array}{llll} \text{if} & (\rho_1 \sqcup_P \rho_2)\downarrow & \text{then} & \rho_1 \leq_P (\rho_1 \sqcup_P \rho_2) \\ & & & \rho_2 \leq_P (\rho_1 \sqcup_P \rho_2) \\ & & & \rho_1 \leq_P \rho' \ \text{ and } \ \rho_2 \leq_P \rho' \ \text{ imply } \ (\rho_1 \sqcup_P \rho_2) \leq_P \rho' \\ \text{if} & (\rho_1 \sqcup_P \rho_2)\uparrow & \text{then} & \text{there is no } \rho' \text{ such that } \rho_1 \leq_P \rho' \text{ and } \rho_2 \leq_P \rho'. \end{array}$$

6.2.3. Definition: Let k and i be canonical $\lambda_\wedge$ types. Then the distinguished least upper bound of k and i, written $k \sqcup i$, is defined by the following function (partial on individual canonical types and total on composite canonical types):

$$\begin{array}{lll} K \sqcup I & = & \bigwedge[\kappa \sqcup \iota \mid \kappa \in K \text{ and } \iota \in I \text{ and } (\kappa \sqcup \iota)\downarrow] \\ \rho_1 \sqcup \rho_2 & = & \rho_1 \sqcup_P \rho_2 \\ (K{\rightarrow}\kappa) \sqcup (I{\rightarrow}\iota) & = & (K \cup I){\rightarrow}(\iota \sqcup \kappa) \\ (K{\rightarrow}\kappa) \sqcup \rho & = & \uparrow \\ \rho \sqcup (I{\rightarrow}\iota) & = & \uparrow . \end{array}$$

(Recall that $K \cup I$ is shorthand for the intersection of all the elements of K and I.)

6.2.4. Fact: [Reynolds]

1. If $\kappa \sqcup \iota$ is defined, then it is a least upper bound of κ and ι. If $\kappa \sqcup \iota$ is undefined, then κ and ι have no common upper bounds.
2. $K \sqcup I$ is a least upper bound of K and I.

The existence of lubs for canonical types is easily shown to be equivalent to the existence of lubs for ordinary types, using the first-order analog of Theorem 5.3.7.6.

In his Ph.D. thesis [46], Ghelli observed that $F_{\leq}$ possesses neither least upper bounds nor greatest lower bounds.

6.2.5. Definition: A pair of types σ and τ is *downward compatible* if there is some type that is a subtype of both σ and τ.

6.2.6. Fact: [46, p. 92] There exists a pair of downward-compatible $F_{\leq}$ types σ and τ with no greatest lower bound.

Proof: Consider the context

$$\Gamma{=}\alpha{\leq}\, Top,\ \beta{\leq}\, Top,\ \alpha'{\leq}\alpha,\ \beta'{\leq}\beta$$

and the types

$$\begin{array}{lll} \sigma & = & \forall\gamma{\leq}\alpha{\rightarrow}\beta.\ \alpha{\rightarrow}\beta \\ \tau & = & \forall\gamma{\leq}\alpha'{\rightarrow}\beta'.\ \alpha'{\rightarrow}\beta'. \end{array}$$

Then both

$$\forall\gamma{\leq}\alpha'{\rightarrow}\beta.\ \alpha{\rightarrow}\beta'$$

and

$$\forall\gamma{\leq}\alpha'{\rightarrow}\beta.\ \gamma$$

are lower bounds for σ and τ, but these two types have no common supertype that is also a subtype of σ and τ. $\square$

6.2.7. Fact: [Ghelli] There is a pair of $F_{\leq}$ types with no least upper bound.

Proof: Consider $\sigma \rightarrow Top$ and $\tau \rightarrow Top$. $\square$

Since $F_{\wedge}$, by definition, possesses greatest lower bounds for every pair of types, we might hope that lubs would also be recovered in $F_{\wedge}$. Unfortunately, this is not the case.

For example, consider the individual canonical types

$$\begin{array}{lcl} \kappa & \equiv & \forall\alpha{\leq}\bigwedge[].\ \forall\beta{\leq}\bigwedge[].\ \alpha \\ \iota & \equiv & \forall\alpha{\leq}\bigwedge[].\ \forall\beta{\leq}\bigwedge[].\ \beta \\ \mu_1 & \equiv & \forall\alpha{\leq}\bigwedge[].\ \forall\beta{\leq}\bigwedge[\alpha].\ \alpha \\ \mu_2 & \equiv & \forall\alpha{\leq}\bigwedge[\nu].\ \forall\beta{\leq}\bigwedge[\nu].\ \nu, \end{array}$$

where ν is any closed individual canonical type with the property that $\alpha{\leq}\nu \not\vdash \nu \leq \alpha$. (For example, take $\nu \equiv \forall\gamma{\leq}\bigwedge[].\ \gamma$.) Then it is easy to check that the following subtype relations hold in the empty context:

$$\begin{tikzcd} \mu_1 & \mu_2 \\ \kappa \arrow[u] \arrow[ur] & \iota \arrow[u] \arrow[ul] \end{tikzcd}$$

Note, however, that $\not\vdash \mu_1 \leq \mu_2$.

Now, assume that κ and ι have some least upper bound; call it λ. Then by the syntax-directedness of canonical subtyping (5.3.6.3) and the fact that λ is a supertype of κ, λ must have the form

$$\lambda \equiv \forall\alpha{\leq}L_1.\ \forall\beta{\leq}L_2.\ \lambda_3.$$

By syntax-directedness again and the fact that $\vdash \lambda \leq \mu_1$ (since μ_1 is a common upper bound of κ and ι),

$$\begin{array}{l} \vdash\ \bigwedge[]\ \leq\ L_1 \\ \text{i.e. } L_1 \equiv \bigwedge[] \\ \\ \alpha{\leq}\bigwedge[]\ \vdash\ \bigwedge[\alpha]\ \leq\ L_2 \\ \text{i.e. } \lambda_2 \in L_2 \text{ implies } \alpha{\leq}\bigwedge[]\ \vdash\ \alpha\ \leq\ \lambda_2 \\ \text{i.e. } \lambda_2 \in L_2 \text{ implies } \lambda_2 \equiv \alpha \\ \text{i.e. } L_2 \equiv \bigwedge[] \text{ or } L_2 \equiv \bigwedge[\alpha] \text{ (up to equivalence) ,} \end{array}$$

and if $L_2 \equiv \bigwedge[\alpha]$ then

$$\begin{array}{l} \alpha{\leq}\bigwedge[], \beta{\leq}\bigwedge[\alpha]\ \vdash\ \lambda_3\ \leq\ \alpha \\ \text{i.e. } \lambda_3 \equiv \alpha \text{ or } \lambda_3 \equiv \beta, \end{array}$$

while if $L_2 \equiv \bigwedge[]$, then $\lambda_3 \equiv \alpha$.

Using the assumption that $\vdash \kappa \leq \lambda$, we may eliminate the case $\lambda_3 \equiv \beta$. Then, using $\vdash \iota \leq \lambda$, we may eliminate the case $L_2 \equiv \bigwedge[]$. In short, if κ and ι have any lub then it is equivalent to μ_1, which must therefore also be a lub. But μ_1 is not a subtype of μ_2, which is a the common upper bound of κ and ι; so μ_1 is *not* a lub of κ and ι. This contradicts our assumption.

To show that composite canonical types lack lubs, we actually need to show something stronger about individual canonical types: that they do not even possess complete finite sets of upper bounds.

6.2.8. Definition: Let σ and τ be types, both closed under Γ. Then a complete finite set of upper bounds for σ and τ under Γ is a finite set $T \equiv \{\theta_1..\theta_n\}$ such that:

1. $\Gamma \vdash \sigma \leq \theta_i$ and $\Gamma \vdash \tau \leq \theta_i$ for each θ_i;
2. if ϕ is a type such that $\Gamma \vdash \sigma \leq \phi$ and $\Gamma \vdash \tau \leq \phi$, then there is some θ_i such that $\Gamma \vdash \theta_i \leq \phi$.

6.2.9. Definition: Define the following infinite series of types:

$$\begin{array}{lcl} \nu_0 & \equiv & \forall\alpha{\leq}\bigwedge[].\ \alpha \\ \nu_{n+1} & \equiv & \forall\alpha{\leq}\bigwedge[].\ \nu_n. \end{array}$$

6.2.10. Lemma: If $\Delta \vdash \nu_i \sim \iota$ for some Δ and ι, then $\iota \equiv \nu_i$.

Proof: By induction on i.

Case: $i = 0$

Since $\Delta \vdash \nu_0 \leq \iota$, syntax-directedness (5.3.6.3) gives $\iota \equiv \forall\alpha{\leq}I_1.\ \iota_2$ and $\Delta,\ \alpha{\leq}I_1 \vdash \alpha \leq \iota_2$. From $\Delta \vdash \iota \leq \nu_0$, syntax-directedness gives $\Delta \vdash \bigwedge[] \leq I_1$, hence $I_1 \equiv \bigwedge[]$. Performing this substitution, we have $\Delta,\ \alpha{\leq}\bigwedge[] \vdash \alpha \leq \iota_2$, hence (by syntax-directedness again) $\iota_2 \equiv \alpha$.

Case: $i = n + 1$

By syntax-directedness, $\Delta \vdash \nu_{n+1} \leq \iota$ gives

$$\begin{array}{l} \iota \equiv \forall\alpha{\leq}I_1.\ \iota_2 \\ \Delta,\ \alpha{\leq}I_1 \ \vdash\ \nu_n \ \leq\ \iota_2. \end{array}$$

Using syntax-directedness on $\Delta \vdash \iota \leq \nu_{n+1}$, we also have

$$\begin{array}{l} \Delta \ \vdash\ \bigwedge[] \ \leq\ I \\ \text{i.e. } I \equiv \bigwedge[] \\ \Delta,\ \alpha{\leq}\bigwedge[] \ \vdash\ \iota_2 \ \leq\ \nu_n. \end{array}$$

By the induction hypothesis, $\iota_2 \equiv \nu_n$, so $\iota \equiv \forall\alpha{\leq}\bigwedge[].\ \nu_n$, which is just ν_{n+1}. □

6.2.11. Lemma: There exists a pair of individual canonical types in $F_\wedge$ with no complete finite set of upper bounds.

Proof: Assume, for a contradiction, that $B \equiv \{\lambda_1..\lambda_n\}$ is a complete finite set of upper bounds for the types

$$\begin{array}{lcl} \kappa & \equiv & \forall\alpha{\leq}\bigwedge[].\ \forall\beta{\leq}\bigwedge[].\ \alpha \\ \iota & \equiv & \forall\alpha{\leq}\bigwedge[].\ \forall\beta{\leq}\bigwedge[].\ \beta \end{array}$$

and let

$$\mu_i \equiv \forall\alpha{\leq}\bigwedge[\nu_i].\ \forall\beta{\leq}\bigwedge[\nu_i].\ \nu_i$$

for every i. Note that each μ_i is a common supertype of κ and ι. Also, since there are more μ's than λ's, we can choose some $\lambda \in B$ and some μ_i and μ_j (with $i \neq j$) such that $\vdash \lambda \leq \mu_i$ and $\vdash \lambda \leq \mu_j$.

From $\vdash \kappa \leq \lambda$ and $\vdash \iota \leq \lambda$, syntax-directedness gives

$$\begin{array}{l} \lambda \equiv \forall\alpha{\leq}L_1.\ \forall\beta{\leq}L_2.\ \lambda_3 \\ \alpha{\leq}L_1, \beta{\leq}L_2 \ \vdash\ \alpha \ \leq\ \lambda_3 \\ \alpha{\leq}L_1, \beta{\leq}L_2 \ \vdash\ \beta \ \leq\ \lambda_3. \end{array}$$

Since $\vdash \lambda \leq \mu_i$, syntax-directedness again yields

$$\begin{array}{l} \vdash\ \bigwedge[\nu_i] \ \leq\ L_1 \\ \alpha{\leq}\bigwedge[\nu_i] \ \vdash\ \bigwedge[\nu_i] \ \leq\ L_2 \\ \alpha{\leq}\bigwedge[\nu_i], \beta{\leq}\bigwedge[\nu_i] \ \vdash\ \lambda_3 \ \leq\ \nu_i. \end{array}$$

By canonical narrowing (5.3.3.4),

$$\alpha{\leq}\bigwedge[\nu_i], \beta{\leq}L_2 \vdash \alpha \leq \lambda_3$$
$$\alpha{\leq}\bigwedge[\nu_i], \beta{\leq}L_2 \vdash \beta \leq \lambda_3,$$

and again

$$\alpha{\leq}\bigwedge[\nu_i], \beta{\leq}\bigwedge[\nu_i] \vdash \alpha \leq \lambda_3$$
$$\alpha{\leq}\bigwedge[\nu_i], \beta{\leq}\bigwedge[\nu_i] \vdash \beta \leq \lambda_3.$$

Now by syntax-directedness,

$$\lambda_3 \equiv \alpha \quad \text{or} \quad \alpha{\leq}\bigwedge[\nu_i], \beta{\leq}\bigwedge[\nu_i] \vdash \bigwedge[\nu_i] \leq \bigwedge[\lambda_3]$$
$$\lambda_3 \equiv \beta \quad \text{or} \quad \alpha{\leq}\bigwedge[\nu_i], \beta{\leq}\bigwedge[\nu_i] \vdash \bigwedge[\nu_i] \leq \bigwedge[\lambda_3].$$

Since $\lambda \equiv \alpha$ and $\lambda \equiv \beta$ cannot both be true, we have $\alpha{\leq}\bigwedge[\nu_i], \beta{\leq}\bigwedge[\nu_i] \vdash \bigwedge[\nu_i] \leq \bigwedge[\lambda_3]$, i.e. (by syntax-directedness),

$$\alpha{\leq}\bigwedge[\nu_i], \beta{\leq}\bigwedge[\nu_i] \vdash \nu_i \leq \lambda_3.$$

Combining this with the type inclusion in the opposite direction (which we derived above), we get

$$\alpha{\leq}\bigwedge[\nu_i], \beta{\leq}\bigwedge[\nu_i] \vdash \nu_i \sim \lambda_3.$$

So, by Lemma 6.2.10, $\lambda_3 \equiv \nu_i$.

But starting from $\vdash \lambda \leq \mu_j$ and reasoning analogously, we can also obtain $\lambda_3 \equiv \nu_j$. Since $\nu_i \not\equiv \nu_j$, this is a contradiction. Our assumption that B is a complete finite set of upper bounds for κ and ι must therefore be false. □

Clearly, if κ and ι have no complete finite set of upper bounds, then the composite canonical types $\bigwedge[\kappa]$ and $\bigwedge[\iota]$ have no lub. As in the first-order case, by Theorem 5.3.7.6, $F_\wedge$ has lubs iff its canonical formulation does, so this counterexample for the canonical system amounts to a proof of the nonexistence of lubs for the original formulation of $F_\wedge$. (Also, in ordinary $F_\wedge$ a complete finite set of upper bounds can always be conjoined to form a single least upper bound, so the nonexistence of lubs is equivalent to the nonexistence of complete finite sets of upper bounds for ordinary types.)

The most immediate implication of the nonexistence of least upper bounds is that standard techniques developed by Reynolds [70] for constructing and analyzing models of first-order intersection types will not generalize straightforwardly to $F_\wedge$.

Reynolds' model construction proceeds as follows. First, the set of canonical type expressions is defined as the limit of a series formed by beginning with the primitives and, at each stage, first closing under the $\rightarrow$ constructor and then forming all finite meets of the resulting set. The semantics of types is defined by induction on the same series of sets of types: the interpretation of a type τ at stage $n+1$ is defined in terms of the interpretations of the components of τ at stage n.

The intended interpretation of an intersection $\sigma{\wedge}\tau$ in a typed semantics is the limit of a diagram containing the interpretations of σ and τ and all their common supertypes (c.f. [69]). But even if σ and τ both exist at level n, there might be many common supertypes that will not appear until some later stage, so the limit with respect to only those supertypes that exist at level n might be too large. At each level, then, it appears that we would need to recalculate the interpretations of all the intersection types from previous levels. It is not obvious that this process would converge.

Fortunately, in $\lambda_\wedge$, every σ and τ possess a least upper bound $\sigma \sqcup \tau$, which, furthermore, always appears at the first stage containing both σ and τ. So $\sigma{\wedge}\tau$ may be interpreted as the limit of a very tidy diagram

$$\begin{tikzcd}
 & {[\![\sigma \sqcup \tau]\!]} & \\
{[\![\sigma]\!]} \arrow[ur] & & {[\![\tau]\!]} \arrow[ul]
\end{tikzcd}$$

with no fear that this interpretation will ever need to be revised.

The nonexistence of least upper bounds in $F_\wedge$ renders this important simplification useless. It is not clear whether a model could be constructed by "incrementally revising" the interpretations of intersections at each level, as described above. This kind of construction, if it worked at all, would almost certainly be much more complex than the known models of $\lambda_\wedge$.

7 Future Work

A primary practical concern for programming notations based on intersection types is the efficiency of typechecking for large programs. Naive implementations of the algorithms given here exhibit exponential behavior — in practice — in both type synthesis (because of the *for* construct) and subtyping (because of rules ASubR-Inter and ASubL-Inter). Fortunately, this behavior normally occurs as a result of explicit programmer directives — requests, in effect, for an exponential amount of analysis of the program during typechecking. Still, a serious implementation must find ways to economize; for example, by cacheing the partial results of previous analysis.

Another consideration for any language based on second-order polymorphism is the problem of verbosity. Without some means of abbreviation or partial type inference, even modest programs quickly become overburdened with type annotations. Cardelli's partial type inference method for $F_\leq$ [17] offers one promising direction of investigation. Another possibility is to use a ω-order extension of $F_\wedge$, in which type operators could be used to express type information more succinctly.

Larger examples are needed to establish the practical need for intersection types and bounded quantification in their most general forms. It may be possible to obtain most of the practical power of $F_\wedge$ while remaining within a simpler, more tractable fragment.

Indeed, Castagna has recently observed [25] that all of the known examples of bounded quantification and its variants and extensions can be treated within a system in which the troublesome Sub-All rule is replaced by a much more tractable "pointwise" rule:

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma, \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \forall\alpha{\leq}\sigma_1.\ \sigma_2 \leq \forall\alpha{\leq}\tau_1.\ \tau_2} \qquad \text{(Sub-All-Pointwise)}$$

In particular, it can be shown that this variant of $F_\wedge$ does possess least upper bounds for finite sets of types. All the techniques developed in this paper can be applied (often in simplified form) to this variant.

Acknowledgements

The Ph.D. thesis on which this paper is based was written under the expert supervision of John Reynolds and Bob Harper. The other members of the thesis committee, Luca Cardelli and Nico Habermann, also contributed significantly to its final shape, and discussions with Peter Lee, Frank Pfenning, David Garlan, Nevin Heintze, Spiro Michaylov, QingMing Ma, and Tim Freeman led to the refinement of many of the ideas. Adriana Compagnoni made many useful comments on a later draft.

This research was sponsored in part by the Avionics Laboratory, Wright Research and Development Center, Aeronautical Systems Division (AFSC), U. S. Air Force, Wright-Patterson AFB, OH 45433-6543 under Contract F33615-90-C-1465, Arpa Order No. 7597; in part by the Office of Naval Research under Contract N00013-84-K-0415; in part by the National Science Foundation under Contract CCR-8922109; and in part by Siemens. The views and conclusions contained in this paper are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government.

A Summary of Major Definitions

A.1 $\mathbf{F}_\wedge$

A.1.1 Subtyping

$$\Gamma \vdash \tau \leq \tau \qquad \text{(Sub-Refl)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \tau_2 \qquad \Gamma \vdash \tau_2 \leq \tau_3}{\Gamma \vdash \tau_1 \leq \tau_3} \qquad \text{(Sub-Trans)}$$

$$\Gamma \vdash \alpha \leq \Gamma(\alpha) \qquad \text{(Sub-TVar)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \sigma_1 \rightarrow \sigma_2 \leq \tau_1 \rightarrow \tau_2} \qquad \text{(Sub-Arrow)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma, \alpha \leq \tau_1 \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \forall \alpha \leq \sigma_1.\ \sigma_2 \leq \forall \alpha \leq \tau_1.\ \tau_2} \qquad \text{(Sub-All)}$$

$$\frac{\text{for all } i,\ \Gamma \vdash \sigma \leq \tau_i}{\Gamma \vdash \sigma \leq \bigwedge[\tau_1..\tau_n]} \qquad \text{(Sub-Inter-G)}$$

$$\Gamma \vdash \bigwedge[\tau_1..\tau_n] \leq \tau_i \qquad \text{(Sub-Inter-LB)}$$

$$\Gamma \vdash \bigwedge[\sigma \rightarrow \tau_1 \mathinner{..} \sigma \rightarrow \tau_n] \leq \sigma \rightarrow \bigwedge[\tau_1..\tau_n] \qquad \text{(Sub-Dist-IA)}$$

$$\Gamma \vdash \bigwedge[\forall \alpha \leq \sigma.\ \tau_1 \mathinner{..} \forall \alpha \leq \sigma.\ \tau_n] \leq \forall \alpha \leq \sigma.\ \bigwedge[\tau_1..\tau_n] \qquad \text{(Sub-Dist-IQ)}$$

A.1.2 Typing

$$\Gamma \vdash x \in \Gamma(x) \qquad \text{(Var)}$$

$$\frac{\Gamma, x{:}\tau_1 \vdash e \in \tau_2}{\Gamma \vdash \lambda x{:}\tau_1.\ e \in \tau_1 \rightarrow \tau_2} \qquad \text{(Arrow-I)}$$

$$\frac{\Gamma \vdash e_1 \in \tau_1 \rightarrow \tau_2 \qquad \Gamma \vdash e_2 \in \tau_1}{\Gamma \vdash e_1\ e_2 \in \tau_2} \qquad \text{(Arrow-E)}$$

$$\frac{\Gamma, \alpha \leq \tau_1 \vdash e \in \tau_2}{\Gamma \vdash \Lambda \alpha \leq \tau_1.\ e \in \forall \alpha \leq \tau_1.\ \tau_2} \qquad \text{(All-I)}$$

$$\frac{\Gamma \vdash e \in \forall \alpha \leq \tau_1.\ \tau_2 \qquad \Gamma \vdash \tau \leq \tau_1}{\Gamma \vdash e[\tau] \in \{\tau/\alpha\}\tau_2} \qquad \text{(All-E)}$$

$$\frac{\Gamma \vdash \{\sigma_i/\alpha\}e \in \tau_i}{\Gamma \vdash \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e \in \tau_i} \qquad \text{(For)}$$

$$\frac{\text{for all } i,\ \Gamma \vdash e \in \tau_i}{\Gamma \vdash e \in \bigwedge[\tau_1..\tau_n]} \qquad \text{(Inter-I)}$$

$$\frac{\Gamma \vdash e \in \tau_1 \qquad \Gamma \vdash \tau_1 \leq \tau_2}{\Gamma \vdash e \in \tau_2} \qquad \text{(Sub)}$$

A.1.3 Syntax-Directed Subtyping

$$\frac{\text{for all } i,\ \Gamma \vdash \sigma \leq X \Rightarrow \tau_i}{\Gamma \vdash \sigma \leq X \Rightarrow \bigwedge[\tau_1..\tau_n]} \qquad \text{(ASubR-Inter)}$$

$$\frac{\text{for some } i,\ \Gamma \vdash \sigma_i \leq X \Rightarrow \alpha}{\Gamma \vdash \bigwedge[\sigma_1..\sigma_n] \leq X \Rightarrow \alpha} \qquad \text{(ASubL-Inter)}$$

$$\frac{\Gamma \vdash \tau_1 \leq [\,] \Rightarrow \sigma_1 \qquad \Gamma \vdash \sigma_2 \leq X_2 \Rightarrow \alpha}{\Gamma \vdash \sigma_1 \to \sigma_2 \leq [\tau_1, X_2] \Rightarrow \alpha} \qquad \text{(ASubL-Arrow)}$$

$$\frac{\Gamma \vdash \tau_1 \leq [\,] \Rightarrow \sigma_1 \qquad \Gamma, \beta \leq \tau_1 \vdash \sigma_2 \leq X_2 \Rightarrow \alpha}{\Gamma \vdash \forall \beta \leq \sigma_1.\ \sigma_2 \leq [\beta \leq \tau_1, X_2] \Rightarrow \alpha} \qquad \text{(ASubL-All)}$$

$$\Gamma \vdash \alpha \leq [\,] \Rightarrow \alpha \qquad \text{(ASubL-Refl)}$$

$$\frac{\Gamma \vdash \Gamma(\beta) \leq X \Rightarrow \alpha}{\Gamma \vdash \beta \leq X \Rightarrow \alpha} \qquad \text{(ASubL-TVar)}$$

A.1.4 Type Synthesis

$$\Gamma \vdash x \in \Gamma(x) \qquad \text{(A-Var)}$$

$$\frac{\Gamma, x{:}\tau_1 \vdash e \in \tau_2}{\Gamma \vdash \lambda x{:}\tau_1.\ e \in \tau_1 \to \tau_2} \qquad \text{(A-Arrow-I)}$$

$$\frac{\Gamma \vdash e_1 \in \sigma_1 \qquad \Gamma \vdash e_2 \in \sigma_2}{\Gamma \vdash e_1\ e_2 \in \bigwedge[\psi_i \mid (\phi_i \to \psi_i) \in \mathit{arrowbasis}_\Gamma(\sigma_1) \text{ and } \Gamma \vdash \sigma_2 \leq \phi_i]} \qquad \text{(A-Arrow-E)}$$

$$\frac{\Gamma, \alpha \leq \tau_1 \vdash e \in \tau_2}{\Gamma \vdash \Lambda \alpha \leq \tau_1.\ e \in \forall \alpha \leq \tau_1.\ \tau_2} \qquad \text{(A-All-I)}$$

$$\frac{\Gamma \vdash e \in \sigma}{\Gamma \vdash e[\tau] \in \bigwedge[\{\tau/\alpha\}\psi_i \mid (\forall \alpha \leq \phi_i.\ \psi_i) \in \mathit{allbasis}_\Gamma(\sigma) \text{ and } \Gamma \vdash \tau \leq \phi_i]} \qquad \text{(A-All-E)}$$

$$\frac{\text{for all } i,\ \Gamma \vdash \{\sigma_i/\alpha\}e \in \tau_i}{\Gamma \vdash \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ e \in \bigwedge[\tau_1..\tau_n]} \qquad \text{(A-For)}$$

A.2 $\mathbf{F}_{\leq}$

A.2.1 Subtyping

$$\Gamma \vdash \sigma \leq \mathit{Top} \qquad \text{(Sub-Top)}$$

$$\Gamma \vdash \tau \leq \tau \qquad \text{(Sub-Refl)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \tau_2 \qquad \Gamma \vdash \tau_2 \leq \tau_3}{\Gamma \vdash \tau_1 \leq \tau_3} \qquad \text{(Sub-Trans)}$$

$$\Gamma \vdash \alpha \leq \Gamma(\alpha) \qquad \text{(Sub-TVar)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \sigma_1 \to \sigma_2 \leq \tau_1 \to \tau_2} \qquad \text{(Sub-Arrow)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma, \alpha \leq \tau_1 \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \forall \alpha \leq \sigma_1.\ \sigma_2 \leq \forall \alpha \leq \tau_1.\ \tau_2} \qquad \text{(Sub-All)}$$

A.2.2 Typing

$$\Gamma \vdash x \in \Gamma(x) \qquad \text{(Var)}$$

$$\frac{\Gamma, x{:}\tau_1 \vdash e \in \tau_2}{\Gamma \vdash \lambda x{:}\tau_1.\ e \in \tau_1 \rightarrow \tau_2} \qquad \text{(Arrow-I)}$$

$$\frac{\Gamma \vdash e_1 \in \tau_1 \rightarrow \tau_2 \qquad \Gamma \vdash e_2 \in \tau_1}{\Gamma \vdash e_1\, e_2 \in \tau_2} \qquad \text{(Arrow-E)}$$

$$\frac{\Gamma, \alpha \leq \tau_1 \vdash e \in \tau_2}{\Gamma \vdash \Lambda \alpha \leq \tau_1.\ e \in \forall \alpha \leq \tau_1.\ \tau_2} \qquad \text{(All-I)}$$

$$\frac{\Gamma \vdash e \in \forall \alpha \leq \tau_1.\ \tau_2 \qquad \Gamma \vdash \tau \leq \tau_1}{\Gamma \vdash e[\tau] \in \{\tau/\alpha\}\tau_2} \qquad \text{(All-E)}$$

$$\frac{\Gamma \vdash e \in \tau_1 \qquad \Gamma \vdash \tau_1 \leq \tau_2}{\Gamma \vdash e \in \tau_2} \qquad \text{(Sub)}$$

A.3 $\lambda_\wedge$

A.3.1 Subtyping

$$\frac{\Gamma \vdash \rho_1 \leq_P \rho_2}{\Gamma \vdash \rho_1 \leq \rho_2} \qquad \text{(Sub-Prim)}$$

$$\Gamma \vdash \tau \leq \tau \qquad \text{(Sub-Refl)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \tau_2 \qquad \Gamma \vdash \tau_2 \leq \tau_3}{\Gamma \vdash \tau_1 \leq \tau_3} \qquad \text{(Sub-Trans)}$$

$$\frac{\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma \vdash \sigma_2 \leq \tau_2}{\Gamma \vdash \sigma_1 \rightarrow \sigma_2 \leq \tau_1 \rightarrow \tau_2} \qquad \text{(Sub-Arrow)}$$

$$\frac{\text{for all } i,\ \Gamma \vdash \sigma \leq \tau_i}{\Gamma \vdash \sigma \leq \bigwedge[\tau_1..\tau_n]} \qquad \text{(Sub-Inter-G)}$$

$$\Gamma \vdash \bigwedge[\tau_1..\tau_n] \leq \tau_i \qquad \text{(Sub-Inter-LB)}$$

$$\Gamma \vdash \bigwedge[\sigma \rightarrow \tau_1 \,..\, \sigma \rightarrow \tau_n] \leq \sigma \rightarrow \bigwedge[\tau_1..\tau_n] \qquad \text{(Sub-Dist-IA)}$$

A.3.2 Typing

$$\Gamma \vdash x \in \Gamma(x) \qquad \text{(Var)}$$

$$\frac{\Gamma, x{:}\sigma_i \vdash e \in \tau_i}{\Gamma \vdash \lambda x{:}\sigma_1..\sigma_n.\ e \in \sigma_i \rightarrow \tau_i} \qquad \text{(Arrow-I')}$$

$$\frac{\Gamma \vdash e_1 \in \tau_1 \rightarrow \tau_2 \qquad \Gamma \vdash e_2 \in \tau_1}{\Gamma \vdash e_1\, e_2 \in \tau_2} \qquad \text{(Arrow-E)}$$

$$\frac{\text{for all } i,\ \Gamma \vdash e \in \tau_i}{\Gamma \vdash e \in \bigwedge[\tau_1..\tau_n]} \qquad \text{(Inter-I)}$$

$$\frac{\Gamma \vdash e \in \tau_1 \qquad \Gamma \vdash \tau_1 \leq \tau_2}{\Gamma \vdash e \in \tau_2} \qquad \text{(Sub)}$$

B Proofs of Technical Lemmas

Proof of Lemma 5.2.5: By induction on a derivation of $\Gamma \vdash \sigma \leq \tau$. Proceed by cases on the final rule.

Cases Sub-Refl, Sub-Trans, Sub-Arrow, Sub-Inter-G, Sub-Inter-LB, Sub-Dist-IA, and Sub-Dist-IQ:

Either immediate or by straightforward use of the induction hypothesis.

Case Sub-TVar: $\sigma \equiv \alpha \qquad \tau \equiv \Gamma(\alpha)$

By SUB-TVAR, $\Gamma' \vdash \alpha \leq \Gamma'(\alpha)$. By assumption, $\Gamma' \vdash \Gamma'(\alpha) \leq \Gamma(\alpha)$. By SUB-TRANS, $\Gamma' \vdash \alpha \leq \Gamma(\alpha)$.

Case Sub-All: $\sigma \equiv \forall\alpha{\leq}\sigma_1.\ \sigma_2 \qquad \tau \equiv \forall\alpha{\leq}\tau_1.\ \tau_2$

By assumption, $\Gamma \vdash \tau_1 \leq \sigma_1$ and $\Gamma,\ \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2$. By the induction hypothesis, $\Gamma' \vdash \tau_1 \leq \sigma_1$. By assumption and weakening (Lemma 5.2.4), $\Gamma',\ \alpha{\leq}\tau_1 \vdash \Gamma'(\alpha_i) \leq \Gamma(\alpha_i)$ for each $\alpha_i \in dom(\Gamma)$. By SUB-REFL, $\Gamma',\ \alpha{\leq}\tau_1 \vdash (\Gamma',\ \alpha{\leq}\tau_1)(\alpha) \leq (\Gamma,\ \alpha{\leq}\tau_1)(\alpha)$. The induction hypothesis then gives $\Gamma',\ \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2$. By SUB-ALL, $\Gamma' \vdash \forall\alpha{\leq}\sigma_1.\ \sigma_2 \leq \forall\alpha{\leq}\tau_1.\ \tau_2$. □

Proof of Lemma 5.2.7: By induction on a derivation of $\Gamma_1,\ \alpha{\leq}\psi,\ \Gamma_2 \vdash \sigma \leq \tau$.

Cases Sub-Refl, Sub-Trans, Sub-Arrow, Sub-Inter-G, Sub-Inter-LB, Sub-Dist-IA, and Sub-Dist-IQ:

Either immediate or by straightforward use of the induction hypothesis.

Case Sub-TVar: $\sigma \equiv \beta \qquad \tau \equiv (\Gamma_1,\ \alpha{\leq}\psi,\ \Gamma_2)(\beta)$

Subcase: $\alpha \equiv \beta$

By assumption,

$$\Gamma_1 \vdash \phi \leq \psi.$$

By weakening (5.2.4),

$$\Gamma_1,\ \{\phi/\alpha\}\Gamma_2 \vdash \phi \leq \psi,$$

that is,

$$\Gamma_1,\ \{\phi/\alpha\}\Gamma_2 \vdash \{\phi/\alpha\}\alpha \leq \{\phi/\alpha\}\psi,$$

as required.

Subcase: $\alpha \not\equiv \beta$

By SUB-TVAR,

$$\Gamma_1,\ \{\phi/\alpha\}\Gamma_2 \vdash \beta \leq (\Gamma_1,\ \{\phi/\alpha\}\Gamma_2)(\beta),$$

that is,

$$\Gamma_1,\ \{\phi/\alpha\}\Gamma_2 \vdash \{\phi/\alpha\}\beta \leq \{\phi/\alpha\}(\Gamma_1,\ \alpha{\leq}\psi,\ \Gamma_2)(\beta).$$

Case Sub-All: $\sigma \equiv \forall\beta{\leq}\sigma_1.\ \sigma_2 \qquad \tau \equiv \forall\beta{\leq}\tau_1.\ \tau_2$

By assumption,

$$\Gamma_1,\ \alpha{\leq}\psi,\ \Gamma_2 \vdash \tau_1 \leq \sigma_1$$
$$\Gamma_1,\ \alpha{\leq}\psi,\ \Gamma_2,\ \beta \leq \tau_1 \vdash \sigma_2{\leq}\tau_2.$$

By the induction hypothesis,

$$\Gamma_1,\ \{\phi/\alpha\}\Gamma_2 \vdash \{\phi/\alpha\}\tau_1 \leq \{\phi/\alpha\}\sigma_1$$
$$\Gamma_1,\ \{\phi/\alpha\}\Gamma_2,\ \beta{\leq}\{\phi/\alpha\}\tau_1 \vdash \{\phi/\alpha\}\sigma_2 \leq \{\phi/\alpha\}\tau_2.$$

By SUB-ALL and the definition of substitution,

$$\Gamma_1,\ \{\phi/\alpha\}\Gamma_2 \ \vdash\ \{\phi/\alpha\}(\forall\beta{\leq}\sigma_1.\ \sigma_2)\ \leq\ \{\phi/\alpha\}(\forall\beta{\leq}\tau_1.\ \tau_2).$$

□

Proof of Lemma 5.3.3.2: By induction on the structure of c.

Cases CSub-AE, CSub-Trans, CSub-Refl, CSub-Arrow:

Either immediate or by straightforward use of the induction hypothesis.

Case CSub-TVar: $k \equiv \beta \quad (\beta \not\equiv \alpha) \qquad i \equiv \iota$
$c \equiv V_\beta(C) \qquad C :: \Delta \vdash \Delta(\beta) \leq \bigwedge[\iota]$

By the induction hypothesis,

$$C, \alpha{\leq}K :: \Delta, \alpha{\leq}K \;\vdash\; \Delta(\beta) \;\leq\; \bigwedge[\iota],$$

that is,

$$C, \alpha{\leq}K :: \Delta, \alpha{\leq}K \;\vdash\; (\Delta, \alpha{\leq}K)(\beta) \;\leq\; \bigwedge[\iota].$$

By CSub-TVar,

$$V_\beta(C, \alpha{\leq}K) :: \Delta, \alpha{\leq}K \;\vdash\; \beta \;\leq\; \iota,$$

that is,

$$(V_\beta(C)), \alpha{\leq}K :: \Delta, \alpha{\leq}K \;\vdash\; \beta \;\leq\; \iota.$$

Case CSub-All: $k \equiv \forall\beta{\leq}K_1.\ \kappa_2 \qquad i \equiv \forall\beta{\leq}I_1.\ \iota_2$
$c \equiv \forall\beta{\leq}C_1.\ \xi_2 \qquad C_1 :: \Delta \vdash I_1 \leq K_1 \qquad \xi_2 :: \Delta, \beta{\leq}I_1 \vdash \kappa_2 \leq \iota_2$

(Also, since β is bound, we may assume that $\alpha \not\equiv \beta$.) By the induction hypothesis,

$$C_1, \alpha{\leq}K :: \Delta, \alpha{\leq}K \;\vdash\; I_1 \;\leq\; K_1$$

and

$$\xi_2, \alpha{\leq}K :: \Delta, \alpha{\leq}K, \beta{\leq}I_1 \;\vdash\; \kappa_2 \;\leq\; \iota_2.$$

By CSub-All,

$$(\forall\beta{\leq}(C_1, \alpha{\leq}K).\ (\xi_2, \alpha{\leq}K)) :: \Delta, \alpha{\leq}K \;\vdash\; \forall\beta{\leq}K_1.\ \kappa_2 \;\leq\; \forall\beta{\leq}I_1.\ \iota_2,$$

that is,

$$((\forall\beta{\leq}C_1.\ \xi_2), \alpha{\leq}K) :: \Delta, \alpha{\leq}K \;\vdash\; \forall\beta{\leq}K_1.\ \kappa_2 \;\leq\; \forall\beta{\leq}I_1.\ \iota_2.$$

□

Proof of Lemma 5.3.3.4: By induction on c.

Cases CSub-AE, CSub-Refl, CSub-Trans, CSub-Arrow:

Either immediate or by straightforward induction.

Case CSub-TVar: $k \equiv \beta \quad (\beta \not\equiv \alpha) \qquad i \equiv \iota$

By the induction hypothesis and CSub-TVar.

Case CSub-TVar: $k \equiv \alpha \qquad i \equiv \iota$
$c \equiv V_\alpha(C) \qquad C :: \Delta, \alpha{\leq}I \vdash I \leq \bigwedge[\iota]$

By the induction hypothesis,

$$(C[D@\alpha{\leq}K]) :: \Delta, \alpha{\leq}K \;\vdash\; I \;\leq\; \bigwedge[\iota].$$

By weakening (5.3.3.2),

$$(D, \alpha{\leq}K) :: \Delta, \alpha{\leq}K \;\vdash\; K \;\leq\; I.$$

By CSub-Trans,

$$((D, \alpha{\leq}K)\,;(C[D@\alpha{\leq}K])) :: \Delta, \alpha{\leq}K \;\vdash\; K \;\leq\; \bigwedge[\iota].$$

By CSub-TVar,

$$V_\alpha((D,\, \alpha{\leq}K)\ ;\ (C[D@\alpha{\leq}K])) :: \Delta,\, \alpha{\leq}K \ \vdash\ \alpha\ \leq\ \iota,$$

that is,

$$(V_\alpha(C))[D@\alpha{\leq}K] :: \Delta,\, \alpha{\leq}K \ \vdash\ \alpha\ \leq\ \iota.$$

Case CSub-All: $k \equiv \forall\beta{\leq}K_1.\ \kappa_2 \qquad i \equiv \forall\beta{\leq}I_1.\ \iota_2$

$c \equiv \forall\beta{\leq}C_1.\ \xi_2$

$C_1 :: \Delta,\, \alpha{\leq}I \vdash I_1 \leq K_1 \qquad \xi_2 :: \Delta,\, \alpha{\leq}I,\, \beta{\leq}I_1 \vdash \kappa_2 \leq \iota_2$

By the induction hypothesis on the first subderivation,

$$(C_1[D@\alpha{\leq}K]) :: \Delta,\, \alpha{\leq}K \ \vdash\ I_1\ \leq\ K_1.$$

By weakening (5.3.3.2) on the second main hypothesis,

$$(D,\, \beta{\leq}I_1) :: \Delta,\, \beta{\leq}I_1 \ \vdash\ K\ \leq\ I.$$

By the induction hypothesis on the second subderivation,

$$\xi_2[(D,\, \beta{\leq}I_1)@\alpha{\leq}K] :: \Delta,\, \beta{\leq}I_1,\, \alpha{\leq}K \ \vdash\ \kappa_2\ \leq\ \iota_2.$$

By CSub-All,

$$(\forall\beta{\leq}(C_1[D@\alpha{\leq}K]).\ (\xi_2[(D,\, \beta{\leq}I_1)@\alpha{\leq}K])) :: \Delta,\, \alpha{\leq}K \ \vdash\ \forall\beta{\leq}K_1.\ \kappa_2\ \leq\ \forall\beta{\leq}I_1.\ \iota_2,$$

that is,

$$(\forall\beta{\leq}C_1.\ \xi_2)[D@\alpha{\leq}K] :: \Delta,\, \alpha{\leq}K \ \vdash\ \forall\beta{\leq}K_1.\ \kappa_2\ \leq\ \forall\beta{\leq}I_1.\ \iota_2.$$

□

Proof of Lemma 5.3.6.2: By induction on the size of e, with a case analysis on the possible forms of c and d. In each case, either the induction hypothesis or one of the II-rules guarantees that a well-formed derivation of the form $c\ ;\ d$ is not in normal form:

c	d	Reason
id	any	II.1
$c_1\ ;\ c_2$	any	induction hypothesis
any	id	II.2
any	$d_1\ ;\ d_2$	induction hypothesis
$AE[\xi_1..\xi_m]$	$AE[\delta_1..\delta_n]$	II.3
$V_\alpha(c_1\ ;\ c_2)$	δ	induction hypothesis
$V_\alpha(AE[\xi])$	δ	II.4
$V_\alpha(id)$	δ	II.5
$C{\rightarrow}\xi$	$V_\beta(D)$	ill formed
$C{\rightarrow}\xi$	$D{\rightarrow}\delta$	II.6
$C{\rightarrow}\xi$	$\forall\beta{\leq}D.\ \delta$	ill formed
$\forall\alpha{\leq}C.\ \xi$	$V_\beta(D)$	ill formed
$\forall\alpha{\leq}C.\ \xi$	$D{\rightarrow}\delta$	ill formed
$\forall\alpha{\leq}C.\ \xi$	$\forall\alpha{\leq}D.\ \delta$	II.7

□

Proof of Lemma 5.3.7.2: By induction on a derivation of $\Gamma \overset{\wedge}{\vdash} \sigma \leq \tau$. Proceed by cases on the final step of the derivation.

Case Sub-Refl: $\sigma \equiv \tau$

By CSub-Refl.

Case Sub-Trans:

By the induction hypothesis and CSub-Trans.

Case Sub-TVar: $\sigma \equiv \alpha \qquad \tau \equiv \Gamma(\alpha)$

By the definition of canonical subtyping, $(\Gamma(\alpha))^\flat \equiv \Gamma^\flat(\alpha) \equiv \bigwedge[\kappa_1..\kappa_n]$. The desired result is checked by constructing the following derivation:

$$\dfrac{\dfrac{\dfrac{\Gamma^\flat \overset{\flat}{\vdash} \kappa_1 \leq \kappa_1}{\Gamma^\flat \overset{\flat}{\vdash} \Gamma^\flat(\alpha) \leq \bigwedge[\kappa_1]}\,\scriptstyle(\text{CSUB-AE})}{\Gamma^\flat \overset{\flat}{\vdash} \alpha \leq \kappa_1}\,\scriptstyle(\text{CSUB-TVAR}) \qquad \cdots \qquad \dfrac{\dfrac{\Gamma^\flat \overset{\flat}{\vdash} \kappa_n \leq \kappa_n}{\Gamma^\flat \overset{\flat}{\vdash} \Gamma^\flat(\alpha) \leq \bigwedge[\kappa_n]}\,\scriptstyle(\text{CSUB-AE})}{\Gamma^\flat \overset{\flat}{\vdash} \alpha \leq \kappa_n}\,\scriptstyle(\text{CSUB-TVAR})}{\Gamma^\flat \overset{\flat}{\vdash} \bigwedge[\alpha] \leq \bigwedge[\kappa_1..\kappa_n]}\,\scriptstyle(\text{CSUB-AE})$$

Case Sub-Arrow: $\sigma \equiv \sigma_1 \rightarrow \sigma_2 \qquad \tau \equiv \tau_1 \rightarrow \tau_2$
$\Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma \vdash \sigma_2 \leq \tau_2$

By the induction hypothesis, $\Gamma^\flat \overset{\flat}{\vdash} \tau_1^\flat \leq \sigma_1^\flat$ and $\Gamma^\flat \overset{\flat}{\vdash} \sigma_2^\flat \leq \tau_2^\flat$. By the syntax-directedness of canonical subtyping (5.3.6.3(2)), for every $\iota_j \in \tau_2^\flat$ there is some $\kappa_j \in \sigma_2^\flat$ such that $\Gamma^\flat \overset{\flat}{\vdash} \kappa_j \leq \iota_j$; in each case, CSub-Arrow gives $\Gamma^\flat \overset{\flat}{\vdash} \sigma_1^\flat \rightarrow \kappa_j \leq \tau_1^\flat \rightarrow \iota_j$. By CSub-AE, $\Gamma^\flat \overset{\flat}{\vdash} \bigwedge[\sigma_1^\flat \rightarrow \kappa \mid \kappa \in \sigma_2^\flat] \leq \bigwedge[\tau_1^\flat \rightarrow \iota \mid \iota \in \tau_2^\flat]$, as required.

Case Sub-All: $\sigma \equiv \forall\alpha{\leq}\sigma_1.\ \sigma_2 \qquad \tau \equiv \forall\alpha{\leq}\tau_1.\ \tau_2$

Similar.

Case Sub-Inter-G: $\tau \equiv \bigwedge[\tau_1..\tau_n] \qquad \Gamma \vdash \sigma \leq \tau_i$ for each τ_i

For each τ_i, the induction hypothesis gives $\Gamma^\flat \overset{\flat}{\vdash} \sigma^\flat \leq \tau_i^\flat$. By the syntax-directedness of canonical subtyping, for each $\iota_{ij} \in \tau_i^\flat$ there is some $\kappa_{ij} \in \sigma^\flat$ such that $\Gamma^\flat \overset{\flat}{\vdash} \kappa_{ij} \leq \iota_{ij}$. Combining these derivations for all the τ_i's, we have $\Gamma^\flat \overset{\flat}{\vdash} \sigma^\flat \leq \bigcup_i \tau_i^\flat$ by CSub-AE.

Case Sub-Inter-LB: $\tau \equiv \sigma_i \qquad \sigma \equiv \bigwedge[\sigma_1..\sigma_n]$

Let ${\sigma_i}^\flat \equiv \bigwedge[\sigma_{i1} .. \sigma_{im}]$. Then the derivation

$$\dfrac{\Gamma^\flat \overset{\flat}{\vdash} \sigma_{i1}^\flat \leq \sigma_{i1}^\flat \qquad \cdots \qquad \Gamma^\flat \overset{\flat}{\vdash} \sigma_{im}^\flat \leq \sigma_{im}^\flat}{\Gamma^\flat \overset{\flat}{\vdash} \bigcup_i \sigma_i^\flat \leq \sigma_i^\flat}\,\scriptstyle(\text{CSUB-AE})$$

establishes the desired result.

Case Sub-Dist-IA: $\sigma \equiv \bigwedge[\sigma' \rightarrow \tau_1 .. \sigma' \rightarrow \tau_n] \qquad \tau \equiv \sigma' \rightarrow \bigwedge[\tau_1..\tau_n]$

By the definition of flattening, $\sigma^\flat \equiv \tau^\flat$. The result follows by CSub-Refl.

Case Sub-Dist-IQ: $\sigma \equiv \bigwedge[\forall\alpha{\leq}\sigma'.\ \tau_1 .. \forall\alpha{\leq}\sigma'.\ \tau_n] \qquad \tau \equiv \forall\alpha{\leq}\sigma'.\ \bigwedge[\tau_1..\tau_n]$

Similar. □

Proof of Lemma 5.3.7.4: By induction on the structure of τ.

Case: $\tau \equiv \alpha$

By SUB-INTER-LB and SUB-INTER-G.

Case: $\tau \equiv \tau_1 \rightarrow \tau_2$

By the definition of flattening (5.3.7.1), $\tau^\flat \equiv \bigwedge[\tau_1^\flat \rightarrow \kappa \mid \kappa \in \tau_2^\flat]$. By derived rule D-DIST-IA (5.2.1), $\Gamma \vdash \tau^\flat \sim (\tau_1^\flat \rightarrow \bigwedge[\kappa \mid \kappa \in \tau_2^\flat])$, i.e., $\Gamma \vdash \tau^\flat \sim \tau_1^\flat \rightarrow \tau_2^\flat$. By the induction hypothesis, $\Gamma \vdash \tau_1^\flat \sim \tau_1$ and $\Gamma \vdash \tau_2^\flat \sim \tau_2$. The desired result follows by D-CONG-ARROW (5.2.6) and SUB-TRANS.

Case: $\tau \equiv \forall\alpha{\leq}\tau_1.\ \tau_2$

Similar.

Case: $\tau \equiv \bigwedge[\tau_1..\tau_n]$

By the induction hypothesis, $\Gamma \vdash \tau_i^\flat \sim \tau_i$ for each i. By D-CONG-INTER (5.2.6), $\Gamma \vdash \bigwedge[\tau_1^\flat ..\ \tau_n^\flat] \sim \bigwedge[\tau_1..\tau_n]$. The result then follows by D-ABSORB (5.2.2) and SUB-TRANS. □

Proof of Lemma 5.4.1.2:

1. By induction on the definition of $arrowbasis_\Gamma$.
2. By the completeness of the subtyping algorithm (5.3.8.8), $\Gamma \overset{\wedge}{\vdash} \sigma \leq \tau_1 \rightarrow \tau_2$ implies $\Gamma \overset{\cdot}{\vdash} \sigma \leq [\tau_1, [\,]] \Rightarrow \tau_2$. We show, by induction on derivations, that $\Gamma \overset{\cdot}{\vdash} \sigma \leq [\tau_1, X_a] \Rightarrow \tau_b$ implies $\Gamma \overset{\wedge}{\vdash} \bigwedge(arrowbasis_\Gamma(\sigma)) \leq [\tau_1, X_a] \Rightarrow \tau_b$, from which the desired result follows as a special case, since $\tau_1 \rightarrow \tau_2$ can always be written in the form $[\tau_1, X_a] \Rightarrow \tau_b$, where the outermost constructor of τ_b is $\wedge$ or a variable.

   Proceed by cases on the final step of a derivation of $\Gamma \overset{\cdot}{\vdash} \sigma \leq [\tau_1, X_a] \Rightarrow \tau_b$.

   Case ASubR-Inter: $\tau_b \equiv \bigwedge[\tau_{b1}..\tau_{bn}]$

   By assumption,

   $$\Gamma \overset{\cdot}{\vdash} \sigma \leq [\tau_1, X_a] \Rightarrow \tau_{bi}$$

   for each i; by the induction hypothesis,

   $$\Gamma \overset{\wedge}{\vdash} \bigwedge(arrowbasis_\Gamma(\sigma)) \leq [\tau_1, X_a] \Rightarrow \tau_{bi}.$$

   By derived rule D-CONG-INTER (5.2.6),

   $$\Gamma \overset{\wedge}{\vdash} \bigwedge[\bigwedge(arrowbasis_\Gamma(\sigma)) .. \bigwedge(arrowbasis_\Gamma(\sigma))] \leq \bigwedge[([\tau_1, X_a] \Rightarrow \tau_{b1}) .. ([\tau_1, X_a] \Rightarrow \tau_{bn})].$$

   By D-ABSORB and D-REINDEX (5.2.2) and SUB-TRANS,

   $$\Gamma \overset{\wedge}{\vdash} \bigwedge(arrowbasis_\Gamma(\sigma)) \leq \bigwedge[([\tau_1, X_a] \Rightarrow \tau_{b1}) .. ([\tau_1, X_a] \Rightarrow \tau_{bn})].$$

   By $len([\tau_1, X_a])$ applications of SUB-DIST-IA and SUB-DIST-IQ (as appropriate) and SUB-TRANS,

   $$\Gamma \overset{\wedge}{\vdash} \bigwedge(arrowbasis_\Gamma(\sigma)) \leq [\tau_1, X_a] \Rightarrow \bigwedge[\tau_{b1}..\tau_{bn}].$$

   Case ASubL-Inter: $\sigma \equiv \bigwedge[\sigma_1..\sigma_n] \qquad \tau_b \equiv \alpha$

   By assumption, $\Gamma \overset{\cdot}{\vdash} \sigma_i \leq [\tau_1, X_a] \Rightarrow \alpha$ for some i. By the induction hypothesis,

   $$\Gamma \overset{\wedge}{\vdash} \bigwedge(arrowbasis_\Gamma(\sigma_i)) \leq [\tau_1, X_a] \Rightarrow \alpha.$$

   Since $arrowbasis_\Gamma(\sigma_i) \subseteq arrowbasis_\Gamma(\sigma)$, SUB-REFL, D-ALL-SOME (5.2.2), and SUB-TRANS give

   $$\Gamma \overset{\wedge}{\vdash} \bigwedge(arrowbasis_\Gamma(\sigma)) \leq [\tau_1, X_a] \Rightarrow \alpha.$$

   Case ASubL-Arrow: $\sigma \equiv \sigma_1 \rightarrow \sigma_2 \qquad \tau_b \equiv \alpha$

   By the definition of $arrowbasis_\Gamma$ and the equivalence of ordinary and syntax-directed subtyping (5.3.8.10).

Case ASubL-All: $\sigma \equiv \forall\alpha{\leq}\sigma_1.\ \sigma_2 \qquad \tau_b \equiv \alpha$

Can't happen ($[\tau_1, X_b]$ has the wrong form).

Case ASubL-Refl: $\sigma \equiv \beta \qquad \tau_b \equiv \beta \qquad [\tau_1, X_a] \equiv [\,]$

Can't happen.

Case ASubL-TVar: $\sigma \equiv \beta \qquad \tau_b \equiv \alpha \qquad \Gamma \vdash^{!} \Gamma(\beta) \leq [\tau_1, X_a] \Rightarrow \alpha$

By the induction hypothesis,

$$\Gamma \vdash^{\wedge} \bigwedge(\mathit{arrowbasis}(\Gamma(\beta))) \leq [\tau_1, X_a] \Rightarrow \alpha.$$

By the definition of $\mathit{arrowbasis}_\Gamma$,

$$\Gamma \vdash^{\wedge} \bigwedge(\mathit{arrowbasis}(\beta)) \leq [\tau_1, X_a] \Rightarrow \alpha.$$

□

Proof of Lemma 5.4.1.4: By the equivalence of ordinary and canonical subtyping (5.3.7.6),

$$\Gamma^\flat \vdash^\flat (\bigwedge M)^\flat \leq (\tau_1 \to \tau_2)^\flat$$
$$\Gamma^\flat \vdash^\flat \sigma^\flat \leq \tau_1^\flat$$
$$V \equiv [\psi_i \mid \Gamma^\flat \vdash^\flat \sigma^\flat \leq {\phi_i}^\flat].$$

By the definition of $\flat$ (5.3.7.1),

$$\Gamma^\flat \vdash^\flat \bigcup_i(\bigwedge[{\phi_i}^\flat \to \kappa \mid \kappa \in {\psi_i}^\flat]) \leq \bigwedge[\tau_1^\flat \to \iota \mid \iota \in \tau_2^\flat].$$

By the syntax-directedness of canonical subtyping (5.3.6.3(1)),

for all $\iota \in \tau_2^\flat$
  there is some i and some $\kappa \in {\psi_i}^\flat$ such that
    $\Gamma^\flat \vdash^\flat {\phi_i}^\flat \to \kappa \leq \tau_1^\flat \to \iota$.

By syntax-directedness again (5.3.6.3(2)),

for all $\iota \in \tau_2^\flat$
  there is some i and some $\kappa \in {\psi_i}^\flat$ such that
    $\Gamma^\flat \vdash^\flat \tau_1^\flat \leq {\phi_i}^\flat$ and
    $\Gamma^\flat \vdash^\flat \kappa \leq \iota$,

that is,

for all $\iota \in \tau_2^\flat$
  there is some i such that
    $\Gamma^\flat \vdash^\flat \tau_1^\flat \leq {\phi_i}^\flat$ and
    there is some $\kappa \in {\psi_\iota}^\flat$ such that
      $\Gamma^\flat \vdash^\flat \kappa \leq \iota$.

By CSub-Trans,

for all $\iota \in \tau_2^\flat$
  there is some i such that
    $\Gamma^\flat \vdash^\flat \sigma^\flat \leq {\phi_i}^\flat$ and
    there is some $\kappa \in {\psi_\iota}^\flat$ such that
      $\Gamma^\flat \vdash^\flat \kappa \leq \iota$.

By CSub-AE,

$$\Gamma^\flat \vdash^\flat \bigcup_i(\bigwedge[\kappa \mid \kappa \in {\psi_i}^\flat \text{ and } \Gamma^\flat \vdash^\flat \sigma^\flat \leq {\phi_i}^\flat]) \leq \tau_2^\flat,$$

that is,

$$\Gamma^\flat \vdash^\flat (\bigwedge V)^\flat \leq \tau_2^\flat.$$

By the equivalence of ordinary and canonical subtyping (5.3.7.6),

$$\Gamma \vdash^\wedge \bigwedge V \leq \tau_2.$$

□

Proof of Lemma 5.4.1.5: By the equivalence of ordinary and canonical subtyping (Theorem 5.3.7.6),

$$\Gamma^\flat \vdash^\flat (\bigwedge M)^\flat \leq (\forall\alpha{\leq}\tau_1.\ \tau_2)^\flat$$
$$\Gamma^\flat \vdash^\flat \sigma^\flat \leq \tau_1^\flat$$
$$V \equiv [\{\sigma/\alpha\}\psi_i \mid \Gamma^\flat \vdash^\flat \sigma^\flat \leq {\phi_i}^\flat].$$

By the definition of $\flat$,

$$\Gamma^\flat \vdash^\flat \bigcup_i(\bigwedge[\forall\alpha{\leq}{\phi_i}^\flat.\ \kappa \mid \kappa \in {\psi_i}^\flat]) \leq \bigwedge[\forall\alpha{\leq}\tau_1^\flat.\ \iota \mid \iota \in \tau_2^\flat].$$

By the syntax-directedness of canonical subtyping (5.3.6.3(1)),

for all $\iota \in \tau_2^\flat$
  there is some i and some $\kappa \in {\psi_i}^\flat$ such that
    $\Gamma^\flat \vdash^\flat (\forall\alpha{\leq}{\phi_i}^\flat.\ \kappa) \leq (\forall\alpha{\leq}\tau_1^\flat.\ \iota)$.

By syntax-directedness again (5.3.6.3(3)),

for all $\iota \in \tau_2^\flat$
  there is some i and some $\kappa \in {\psi_i}^\flat$ such that
    $\Gamma^\flat \vdash^\flat \tau_1^\flat \leq {\phi_i}^\flat$ and
    $\Gamma^\flat, \alpha{\leq}\tau_1^\flat \vdash \kappa \leq \iota$,

that is,

for all $\iota \in \tau_2^\flat$
  there is some i such that
    $\Gamma^\flat \vdash^\flat \tau_1^\flat \leq {\phi_i}^\flat$ and
    there is some $\kappa \in {\psi_i}^\flat$ such that
      $\Gamma^\flat, \alpha{\leq}\tau_1^\flat \vdash \kappa \leq \iota$.

By CSub-Trans,

for all $\iota \in \tau_2^\flat$
  there is some i such that
    $\Gamma^\flat \vdash^\flat \sigma^\flat \leq {\phi_i}^\flat$ and
    there is some $\kappa \in {\psi_i}^\flat$ such that
      $\Gamma^\flat, \alpha{\leq}\tau_1^\flat \vdash \kappa \leq \iota$.

By CSub-AE,

$$\Gamma^\flat,\ \alpha{\le}\tau_1^\flat \vdash^\flat \textstyle\bigcup_i(\bigwedge[\kappa \mid \kappa \in \psi_i \text{ and } \Gamma^\flat \vdash^\flat \sigma^\flat \le {\phi_i}^\flat]) \le \tau_2^\flat,$$

that is,

$$\Gamma^\flat,\ \alpha{\le}\tau_1^\flat \vdash^\flat (\textstyle\bigwedge[\psi_i \mid \Gamma^\flat \vdash^\flat \sigma^\flat \le {\phi_i}^\flat])^\flat \le \tau_2^\flat.$$

By the equivalence of ordinary and canonical subtyping (5.3.7.6),

$$\Gamma,\ \alpha{\le}\tau_1 \vdash^{\wedge} \textstyle\bigwedge[\psi_i \mid \Gamma \vdash \sigma \le \phi_i] \le \tau_2.$$

Then by the substitution property (5.2.7),

$$\Gamma \vdash^{\wedge} \{\sigma/\alpha\}(\textstyle\bigwedge[\psi_i \mid \Gamma \vdash \sigma \le \phi_i]) \le \{\sigma/\alpha\}\tau_2,$$

that is,

$$\Gamma \vdash^{\wedge} \textstyle\bigwedge V \ \le\ \{\sigma/\alpha\}\tau_2.$$

$\square$

Proof of Theorem 5.4.3.3:

1. ($\Longleftarrow$) Lemma 3.3.2.3.

   ($\Longrightarrow$) If $\Gamma_P, \Gamma \vdash^{\wedge} \sigma \le \tau$, then by the completeness of the subtyping algorithm, $\Gamma_P, \Gamma \dot{\vdash} \sigma \le \tau$. By the syntax-directedness of the subtyping algorithm and the fact that σ, τ, and Γ contain no quantified types, this derivation will not contain any instances of ASubL-All, the rule that deals with quantified types. It may be therefore be rewritten as a derivation from the $\lambda_\wedge$ rules by a translation similar to the one in the proof of Theorem 5.3.8.6, dropping the bindings Γ_P and translating instances of ASubL-Refl as instances of Sub-Refl and instances of ASubL-TVar as derivations of the following form:

$$\text{(SUB-TRANS)}\dfrac{\text{(SUB-INTER-G)}\dfrac{\forall\gamma \in P \text{ with } \beta{\le_P}\gamma.\quad \dfrac{\beta \le_P \gamma}{\Gamma \vdash^{\lambda\wedge} \beta \le \gamma}\,\text{(SUB-PRIM)}}{\Gamma \vdash^{\lambda\wedge} \beta \le \bigwedge[\gamma \in P \mid \beta{\le_P}\gamma]} \qquad \dfrac{\text{(induction hypothesis)}}{\Gamma \vdash^{\lambda\wedge} \bigwedge[\gamma \in P \mid \beta{\le_P}\gamma] \le X{\Rightarrow}\alpha}}{\Gamma \vdash^{\lambda\wedge} \beta \le X{\Rightarrow}\alpha.}$$

2. ($\Longleftarrow$) Lemma 3.3.2.4.

   ($\Longrightarrow$) If $\Gamma, \Gamma_P \vdash^{\wedge} e \in \tau$, then by the completeness of the subtyping algorithm, $\Gamma, \Gamma_P \dot{\vdash} e \in \tau$. By the syntax-directedness of the subtyping algorithm and the fact that e, τ, and Γ contain no type abstractions, type applications, or quantified types, this derivation will not contain any instances of A-All-I or A-All-E. It may be therefore be rewritten straightforwardly as a derivation from the $\lambda_\wedge$ rules, using the previous case to handle the translation of subtyping derivations. $\square$

Proof of Lemma 6.1.1.3: By induction on the form of C.

Case: $x \notin FV(C)$

$$\begin{array}{rcll} [\![\lambda^\star x.\ C]\!]_\eta \cdot m & = & [\![K\,C]\!]_\eta \cdot m & \\ & = & k \cdot [\![C]\!]_\eta \cdot m & \\ & = & [\![C]\!]_\eta & \\ & = & [\![C]\!]_{\eta[x\leftarrow m]} & \text{by Lemma 6.1.1.2.} \end{array}$$

Case: $C \equiv x$

$$\begin{array}{rcl} [\![\lambda^\star x.\ C]\!]_\eta \cdot m & = & [\![S\,K\,K]\!]_\eta \cdot m \\ & = & s \cdot k \cdot k \cdot m \\ & = & m \\ & = & (\eta[x\leftarrow m])(x) \\ & = & [\![C]\!]_{\eta[x\leftarrow m]}. \end{array}$$

Case: $C \equiv C_1\,C_2 \qquad x \in FV(C_1\,C_2)$

$$\begin{array}{rcll} [\![\lambda^\star x.\ C]\!]_\eta \cdot m & = & [\![S\,(\lambda^\star x.\ C_1)\,(\lambda^\star x.\ C_2)]\!]_\eta \cdot m & \\ & = & s \cdot [\![\lambda^\star x.\ C_1]\!]_\eta \cdot [\![\lambda^\star x.\ C_2]\!]_\eta \cdot m & \\ & = & ([\![\lambda^\star x.\ C_1]\!]_\eta \cdot m) \cdot ([\![\lambda^\star x.\ C_2]\!]_\eta \cdot m) & \\ & = & ([\![C_1]\!]_{\eta[x\leftarrow m]}) \cdot ([\![C_2]\!]_{\eta[x\leftarrow m]}) & \text{by the induction hypothesis} \\ & = & ([\![C_1\,C_2]\!]_{\eta[x\leftarrow m]}). & \end{array}$$

$\square$

Proof of Lemma 6.1.2.7: By induction on the structure of a derivation of $\Gamma \vdash \sigma \leq \tau$.

Case Sub-Refl: $\sigma \equiv \tau$

Immediate.

Case Sub-Trans: $\Gamma \vdash \sigma \leq \theta \qquad \Gamma \vdash \theta \leq \tau$

By the induction hypothesis.

Case Sub-TVar: $\sigma \equiv \alpha \qquad \tau \equiv \Gamma(\alpha)$

Immediate from 6.1.2.5.

Case Sub-Arrow: $\sigma \equiv \sigma_1 \rightarrow \sigma_2 \qquad \tau \equiv \tau_1 \rightarrow \tau_2 \qquad \Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma \vdash \sigma_2 \leq \tau_2$

$$\begin{array}{ll} & m\ \{[\![\sigma_1\rightarrow\sigma_2]\!]_\eta\}\ n \\ \Leftrightarrow & m\ \{[\![\sigma_1]\!]_\eta \rightarrow [\![\sigma_2]\!]_\eta\}\ n \\ \Leftrightarrow & \forall p, q.\quad p\ \{[\![\sigma_1]\!]_\eta\}\ q \text{ implies } m{\cdot}p\ \{[\![\sigma_2]\!]_\eta\}\ n{\cdot}q \\ \Rightarrow & \forall p, q.\quad p\ \{[\![\tau_1]\!]_\eta\}\ q \text{ implies } m{\cdot}p\ \{[\![\tau_2]\!]_\eta\}\ n{\cdot}q \quad \text{by the induction hypothesis} \\ \Leftrightarrow & m\ \{[\![\tau_1\rightarrow\tau_2]\!]_\eta\}\ n. \end{array}$$

Case Sub-All: $\sigma \equiv \forall\alpha{\leq}\sigma_1.\ \sigma_2 \qquad \tau \equiv \forall\alpha{\leq}\tau_1.\ \tau_2 \qquad \Gamma \vdash \tau_1 \leq \sigma_1 \qquad \Gamma, \alpha{\leq}\tau_1 \vdash \sigma_2 \leq \tau_2$

$$\begin{array}{ll} & m\ \{[\![\forall\alpha{\leq}\sigma_1.\ \sigma_2]\!]_\eta\}\ n \\ \Leftrightarrow & m\ \{\bigcap_{A\subseteq[\![\sigma_1]\!]_\eta} [\![\sigma_2]\!]_{\eta[\alpha\leftarrow A]}\}\ n \\ \Leftrightarrow & \forall A{\subseteq}[\![\sigma_1]\!]_\eta.\quad m\ \{[\![\sigma_2]\!]_{\eta[\alpha\leftarrow A]}\}\ n \\ \Rightarrow & \forall A{\subseteq}[\![\tau_1]\!]_\eta.\quad m\ \{[\![\tau_2]\!]_{\eta[\alpha\leftarrow A]}\}\ n \quad \text{by the induction hypothesis} \\ \Leftrightarrow & m\ \{[\![\forall\alpha{\leq}\tau_1.\ \tau_2]\!]_\eta\}\ n. \end{array}$$

Case Sub-Inter-G: $\tau \equiv \bigwedge[\tau_1..\tau_n] \qquad$ for all i, $\Gamma \vdash \sigma \leq \tau_i$

By the induction hypothesis, $[\![\sigma]\!]_\eta \subseteq [\![\tau_i]\!]_\eta$ for each i; so $[\![\sigma]\!]_\eta \subseteq \bigcap_{1\leq i\leq n} [\![\tau_i]\!]_\eta = [\![\bigwedge[\tau_1..\tau_n]]\!]_\eta$.

Case Sub-Inter-LB: $\sigma \equiv \bigwedge[\tau_1..\tau_n] \qquad \tau \equiv \tau_i$

Immediate from the definition of $\bigwedge$.

Case Sub-Dist-IA: $\sigma \equiv \bigwedge[\sigma'\!\rightarrow\!\tau_1 \,..\, \sigma'\!\rightarrow\!\tau_n] \qquad \tau \equiv \sigma'\!\rightarrow\!\bigwedge[\tau_1..\tau_n]$

$$
\begin{array}{ll}
 & m\;\{[\![\bigwedge[\sigma'\!\rightarrow\!\tau_1 \,..\, \sigma'\!\rightarrow\!\tau_n]]\!]_\eta\}\;m' \\
\Leftrightarrow & m\;\{\bigcap_{1\leq i\leq n}[\![\sigma'\!\rightarrow\!\tau_i]\!]_\eta\}\;m' \\
\Leftrightarrow & \forall i.\quad m\;\{[\![\sigma']\!]_\eta\rightarrow[\![\tau_i]\!]_\eta\}\;m' \\
\Leftrightarrow & \forall i.\quad \forall p,q.\quad p\;\{[\![\sigma']\!]_\eta\}\;q \text{ implies } m\cdot p\;\{[\![\tau_i]\!]_\eta\}\;m'\cdot q \\
\Leftrightarrow & \forall p,q.\quad p\;\{[\![\sigma']\!]_\eta\}\;q \text{ implies } (\forall i.\; m\cdot p\;\{[\![\tau_i]\!]_\eta\}\;m'\cdot q) \\
\Leftrightarrow & \forall p,q.\quad p\;\{[\![\sigma']\!]_\eta\}\;q \text{ implies } m\cdot p\;\{[\![\bigwedge[\tau_1..\tau_n]]\!]_\eta\}\;m'\cdot q \\
\Leftrightarrow & m\;\{[\![\sigma'\!\rightarrow\!\bigwedge[\tau_1..\tau_n]]\!]_\eta\}\;m'.
\end{array}
$$

Case Sub-Dist-IQ: $\sigma \equiv \bigwedge[\forall\alpha\!\leq\!\sigma'.\ \tau_1 \,..\, \forall\alpha\!\leq\!\sigma'.\ \tau_n] \qquad \tau \equiv \forall\alpha\!\leq\!\sigma'.\ \bigwedge[\tau_1..\tau_n]$

$$
\begin{array}{ll}
 & [\![\bigwedge[\forall\alpha\!\leq\!\sigma'.\ \tau_1 \,..\, \forall\alpha\!\leq\!\sigma'.\ \tau_n]]\!]_\eta \\
= & \bigcap_{1\leq i\leq n}\bigcap_{A\,\subseteq\,[\![\sigma']\!]_\eta}\tau_i \\
= & \bigcap_{A\,\subseteq\,[\![\sigma']\!]_\eta}\bigcap_{1\leq i\leq n}\tau_i \\
= & [\![\forall\alpha\!\leq\!\sigma.\ \bigwedge[\tau_1..\tau_n]]\!]_\eta.
\end{array}
$$

□

Proof of Lemma 6.1.2.9: By induction on a derivation of $\Gamma \vdash e \in \tau$.

Case Var: $e \equiv x \qquad \tau \equiv \Gamma(x)$

Immediate.

Case Arrow-I: $e \equiv \lambda x{:}\tau_1.\ e' \qquad \Gamma,\, x{:}\tau_1 \vdash e' \in \tau_2 \qquad \tau \equiv \tau_1\!\rightarrow\!\tau_2$

Choose m and n such that $m\;\{[\![\tau_1]\!]_\eta\}\;n$. Then $m\;\{[\![\tau_1]\!]_\eta\}\;m$ and $n\;\{[\![\tau_1]\!]_\eta\}\;n$, so $\eta_1[x\!\leftarrow\!m] \models \Gamma,\, x{:}\tau_1$ and $\eta_2[x\!\leftarrow\!n] \models \Gamma,\, x{:}\tau_1$. The induction hypothesis gives

$$[\![e']\!]_{\eta_1[x\leftarrow m]}\;\{[\![\tau_2]\!]_\eta\}\;[\![e']\!]_{\eta_2[x\leftarrow n]}.$$

But

$$
\begin{array}{rcll}
[\![e]\!]_{\eta_1}\cdot m & = & [\![\lambda^\star x.\ |erase(e')|]\!]_{\eta_1}\cdot m & \text{by definition} \\
 & = & [\![|erase(e')|]\!]_{\eta_1[x\leftarrow m]} & \text{by Lemma 6.1.1.3} \\
 & = & [\![e']\!]_{\eta_1[x\leftarrow m]} & \text{by definition,}
\end{array}
$$

and similarly $[\![e]\!]_{\eta_2}\cdot n = [\![e']\!]_{\eta_2[x\leftarrow n]}$. So

$$[\![e]\!]_{\eta_1}\cdot m\;\{[\![\tau_2]\!]_\eta\}\;[\![e]\!]_{\eta_2}\cdot n.$$

Since this holds for all m and n such that $m\;\{[\![\tau_1]\!]_\eta\}\;n$, the definition of $\rightarrow$ gives

$$[\![e]\!]_{\eta_1}\;\{[\![\tau_1]\!]_\eta\rightarrow[\![\tau_2]\!]_\eta\}\;[\![e]\!]_{\eta_2},$$

i.e.,

$$[\![e]\!]_{\eta_1}\;\{[\![\tau_1\!\rightarrow\!\tau_2]\!]_\eta\}\;[\![e]\!]_{\eta_2}.$$

Case Arrow-E: $e \equiv e_1\,e_2 \qquad \Gamma \vdash e_1 \in \tau_1\!\rightarrow\!\tau_2 \qquad \Gamma \vdash e_2 \in \tau_1 \qquad \tau \equiv \tau_2$

By the induction hypothesis,

$$[\![e_1]\!]_{\eta_1}\;\{[\![\tau_1\!\rightarrow\!\tau_2]\!]_\eta\}\;[\![e_1]\!]_{\eta_2},$$

i.e.

$$[\![e_1]\!]_{\eta_1}\;\{[\![\tau_1]\!]_\eta\rightarrow[\![\tau_2]\!]_\eta\}\;[\![e_1]\!]_{\eta_2},$$

and

$$[\![e_2]\!]_{\eta_1}\;\{[\![\tau_1]\!]_\eta\}\;[\![e_2]\!]_{\eta_2}.$$

So, by the definition of $\rightarrow$,

$$[\![e_1]\!]_{\eta_1} \cdot [\![e_2]\!]_{\eta_1} \ \{[\![\tau_2]\!]_\eta\} \ [\![e_1]\!]_{\eta_2} \cdot [\![e_2]\!]_{\eta_2},$$

i.e. (by Lemma 6.1.2.8(1)),

$$[\![e_1\ e_2]\!]_{\eta_1} \ \{[\![\tau_2]\!]_\eta\} \ [\![e_1\ e_2]\!]_{\eta_2}.$$

Case All-I: $e \equiv \Lambda\alpha{\leq}\tau.\ e' \qquad \Gamma,\ \alpha{\leq}\tau_1 \vdash e' \in \tau_2 \qquad \tau \equiv \forall\alpha{\leq}\tau_1.\ \tau_2$

Choose an arbitrary PER $A \subseteq [\![\tau_1]\!]_\eta$. By the induction hypothesis,

$$[\![e']\!]_{\eta_1[\alpha\leftarrow A]} \ \{[\![\tau_2]\!]_{\eta[\alpha\leftarrow A]}\} \ [\![e']\!]_{\eta_2[\alpha\leftarrow A]}.$$

By Lemma 6.1.1.2,

$$[\![e']\!]_{\eta_1} \ \{[\![\tau_2]\!]_{\eta[\alpha\leftarrow A]}\} \ [\![e']\!]_{\eta_2}.$$

Since this holds for every $A \subseteq [\![\tau_1]\!]_\eta$, the definition of $\bigcap$ yields,

$$[\![e']\!]_{\eta_1} \ \{\textstyle\bigcap_{A\subseteq[\![\tau_1]\!]_\eta} [\![\tau_2]\!]_{\eta[\alpha\leftarrow A]}\} \ [\![e']\!]_{\eta_2},$$

i.e.,

$$[\![e']\!]_{\eta_1} \ \{[\![\forall\alpha{\leq}\tau_1.\ \tau_2]\!]_\eta\} \ [\![e']\!]_{\eta_2},$$

i.e. (by the definition of *erase*),

$$[\![e]\!]_{\eta_1} \ \{[\![\forall\alpha{\leq}\tau_1.\ \tau_2]\!]_\eta\} \ [\![e]\!]_{\eta_2}.$$

Case All-E: $e \equiv e'\,[\sigma] \qquad \Gamma \vdash e' \in \forall\alpha{\leq}\tau_1.\ \tau_2 \qquad \Gamma \vdash \sigma \leq \tau_1 \qquad \tau \equiv \tau_2$

By the induction hypothesis,

$$[\![e']\!]_{\eta_1} \ \{[\![\forall\alpha{\leq}\tau_1.\ \tau_2]\!]_\eta\} \ [\![e']\!]_{\eta_2},$$

i.e.,

$$[\![e']\!]_{\eta_1} \ \{\textstyle\bigcap_{A\subseteq[\![\tau_1]\!]_\eta} [\![\tau_2]\!]_{\eta[\alpha\leftarrow A]}\} \ [\![e']\!]_{\eta_2}.$$

Since, by Lemma 6.1.2.7, $[\![\sigma]\!]_\eta \subseteq [\![\tau_1]\!]_\eta$,

$$[\![e']\!]_{\eta_1} \ \{[\![\tau_2]\!]_{\eta[\alpha\leftarrow[\![\sigma]\!]_\eta]}\} \ [\![e']\!]_{\eta_2},$$

i.e. (by the definition of *erase*),

$$[\![e]\!]_{\eta_1} \ \{[\![\tau_2]\!]_{\eta[\alpha\leftarrow[\![\sigma]\!]_\eta]}\} \ [\![e]\!]_{\eta_2},$$

i.e. (by Lemma 6.1.2.8(3)

$$[\![e]\!]_{\eta_1} \ \{[\![\{\sigma/\alpha\}\tau_2]\!]_\eta\} \ [\![e]\!]_{\eta_2}.$$

Case For: $e \equiv \mathit{for}\ \alpha\ \mathit{in}\ \sigma_1..\sigma_n.\ .e' \qquad \Gamma \vdash \{\sigma_i/\alpha\}e' \in \tau_i \qquad \tau \equiv \tau_i$

By the induction hypothesis,

$$[\![\{\sigma_i/\alpha\}e']\!]_{\eta_1} \ \{[\![\tau_i]\!]_\eta\} \ [\![\{\sigma_i/\alpha\}e']\!]_{\eta_2}.$$

By Lemma 6.1.2.8(2),

$$[\![e']\!]_{\eta_1} \ \{[\![\tau_i]\!]_\eta\} \ [\![e']\!]_{\eta_2}.$$

By the definition of *erase*,

$$[\![e]\!]_{\eta_1} \ \{[\![\tau_i]\!]_\eta\} \ [\![e]\!]_{\eta_2}.$$

Case Inter-I: $\Gamma \vdash e \in \tau_i$ for each $i \qquad \tau \equiv \bigwedge[\tau_1..\tau_n]$

By the induction hypothesis,

$$[\![e]\!]_{\eta_1} \ \{[\![\tau_i]\!]_\eta\} \ [\![e]\!]_{\eta_2}$$

for each i; hence,

$$[\![e]\!]_{\eta_1} \ \{\textstyle\bigcap_{1\leq i\leq n} [\![\tau_i]\!]_\eta\} \ [\![e]\!]_{\eta_2},$$

i.e.,

$$[\![e]\!]_{\eta_1} \ \{[\![\textstyle\bigwedge[\tau_1..\tau_n]]\!]_\eta\} \ [\![e]\!]_{\eta_2}.$$

Case Sub: $\Gamma \vdash e \in \sigma \qquad \Gamma \vdash \sigma \leq \tau$

By the induction hypothesis,

$$[\![e]\!]_{\eta_1} \; \{[\![\sigma]\!]_\eta\} \; [\![e]\!]_{\eta_2},$$

hence (by Lemma 6.1.2.7)

$$[\![e]\!]_{\eta_1} \; \{[\![\tau]\!]_\eta\} \; [\![e]\!]_{\eta_2}.$$

$\square$

References

[1] Franco Barbanera and Mariangiola Dezani-Ciancaglini. Intersection and union types. In Ito and Meyer [54], pages 651–674.

[2] H. P. Barendregt. *The Lambda Calculus*. North Holland, revised edition, 1984.

[3] H. Barendregt, M. Coppo, and M. Dezani-Ciancaglini. A filter lambda model and the completeness of type assignment. *Journal of Symbolic Logic*, 48(4):931–940, 1983.

[4] Val Breazu-Tannen, Thierry Coquand, Carl Gunter, and Andre Scedrov. Inheritance as implicit coercion. *Information and Computation*, 93:172–221, 1991.

[5] Kim B. Bruce. The equivalence of two semantic definitions for inheritance in object-oriented languages. In *Proceedings of Mathematical Foundations of Programming Semantics*, Pittsburgh, PA, March 1991.

[6] Kim B. Bruce. Safe type checking in a statically typed object-oriented programming language. In *Proceedings of the Twentieth ACM Symposium on Principles of Programming Languages*, January 1993.

[7] Kim B. Bruce and Giuseppe Longo. A modest model of records, inheritance, and bounded quantification. *Information and Computation*, 87:196–240, 1990. To appear in [48]. An earlier version appeared in the proceedings of the IEEE Symposium on Logic in Computer Science, 1988.

[8] Kim B. Bruce, Albert R. Meyer, and John C. Mitchell. The semantics of second-order lambda calculus. In Huet [53], pages 213–272. Also appeared in Information and Computation 84, 1 (January 1990).

[9] Kim Bruce and John Mitchell. PER models of subtyping, recursive types and higher-order polymorphism. In *Proceedings of the Nineteenth ACM Symposium on Principles of Programming Languages*, Albequerque, NM, January 1992.

[10] Peter Canning, William Cook, Walt Hill, and Walter Olthoff. Interfaces for strongly-typed object-oriented programming. In *Object Oriented Programing: Systems, Languages, and Applications (OOPSLA)*, pages 457–467, 1989.

[11] Peter Canning, William Cook, Walter Hill, Walter Olthoff, and John Mitchell. F-bounded quantification for object-oriented programming. In *Fourth International Conference on Functional Programming Languages and Computer Architecture*, pages 273–280, September 1989.

[12] Peter Canning, Walt Hill, and Walter Olthoff. A kernel language for object-oriented programming. Technical Report STL-88-21, Hewlett-Packard Labs, 1988.

[13] Luca Cardelli. A semantics of multiple inheritance. *Information and Computation*, 76:138–164, 1988. Preliminary version in *Semantics of Data Types*, Kahn, MacQueen, and Plotkin, eds., Springer-Verlag LNCS 173, 1984.

[14] Luca Cardelli. Structural subtyping and the notion of power type. In *Proceedings of the 15th ACM Symposium on Principles of Programming Languages*, pages 70–79, San Diego, CA, January 1988.

[15] Luca Cardelli. Typeful programming. In E. J. Neuhold and M. Paul, editors, *Formal Description of Programming Concepts*. Springer-Verlag, 1991. An earlier version appeared as DEC Systems Research Center Research Report #45, February 1989.

[16] Luca Cardelli. Extensible records in a pure calculus of subtyping. Research report 81, DEC Systems Research Center, January 1992. To appear in [48].

[17] Luca Cardelli. An implementation of $F_{<:}$. Research report 97, DEC Systems Research Center, Februart 1993.

[18] Luca Cardelli and Giuseppe Longo. A semantic basis for Quest. *Journal of Functional Programming*, 1(4):417–458, October 1991. Preliminary version in ACM Conference on Lisp and Functional Programming, June 1990. Also available as DEC SRC Research Report 55, Feb. 1990.

[19] Luca Cardelli, Simone Martini, John C. Mitchell, and Andre Scedrov. An extension of system F with subtyping. In Ito and Meyer [54], pages 750–770.

[20] Luca Cardelli and John Mitchell. Operations on records. *Mathematical Structures in Computer Science*, 1:3–48, 1991. To appear in [48]; also available as DEC Systems Research Center Research Report #48, August, 1989, and in the proceedings of MFPS '89, Springer LNCS volume 442.

[21] Luca Cardelli and Peter Wegner. On understanding types, data abstraction, and polymorphism. *Computing Surveys*, 17(4), December 1985.

[22] Felice Cardone. Relational semantics for recursive types and bounded quantification. In *Proceedings of the Sixteenth International Colloquium on Automata, Languages, and Programming*, volume 372 of *Lecture Notes in Computer Science*, pages 164–178, Stresa, Italy, July 1989. Springer-Verlag.

[23] Felice Cardone and Mario Coppo. Two extensions of Curry's type inference system. In Odifreddi [61], pages 19–76.

[24] Robert Cartwright and Mike Fagan. Soft typing. Submitted to PLDI '91, November 1990.

[25] Giuseppe Castagna and Benjamin Pierce. Decidable bounded quantification. Submitted for publication, July 1993.

[26] Alonzo Church. A formulation of the simple theory of types. *Journal of Symbolic Logic*, 5:56–68, 1940.

[27] Adriana B. Compagnoni and Benjamin C. Pierce. Multiple inheritance via intersection types. Submitted for publication, July 1993.

[28] William R. Cook, Walter L. Hill, and Peter S. Canning. Inheritance is not subtyping. In *Seventeenth Annual ACM Symposium on Principles of Programming Languages*, pages 125–135, San Francisco, CA, January 1990. To appear in [48].

[29] M. Coppo and M. Dezani-Ciancaglini. A new type-assignment for λ-terms. *Archiv. Math. Logik*, 19:139–156, 1978.

[30] M. Coppo and M. Dezani-Ciancaglini. An extension of the basic functionality theory for the λ-calculus. *Notre-Dame Journal of Formal Logic*, 21(4):685–693, October 1980.

[31] M. Coppo, M. Dezani-Ciancaglini, F. Honsell, and G. Longo. Extended type structures and filter lambda models. In G. Lolli, G. Longo, and A. Marja, editors, *Logic Colloquium 82*, pages 241–262, Amsterdam, 1983. North-Holland.

[32] M. Coppo, M. Dezani-Ciancaglini, and B. Venneri. Principal type schemes and lambda calculus semantics. In *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus, and Formalism*, pages 535–560, New York, 1980. Academic Press.

[33] M. Coppo, M. Dezani-Ciancaglini, and B. Venneri. Functional characters of solvable terms. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 27:45–58, 1981.

[34] M. Coppo, M. Dezani-Ciancaglini, and M. Zacchi. Type theories, normal forms and D_∞-lambda-models. *Information and Computation*, 72:85–116, 1987.

[35] M. Coppo, M. Dezani, and P. Sallé. Functional characterization of some semantic equalities inside λ-calculus. Number 81 in Lecture Notes in Computer Science, pages 133–146. Springer-Verlag, 1979.

[36] M. Coppo and P. Giannini. A complete type inference algorithm for simple intersection types. In *ESOP '92?*, 1992.

[37] Pierre-Louis Curien and Giorgio Ghelli. Subtyping + extensionality: Confluence of $\beta\eta$-reductions in $F_\leq$. In Ito and Meyer [54], pages 731–749.

[38] Pierre-Louis Curien and Giorgio Ghelli. Coherence of subsumption: Minimum typing and type-checking in $\mathrm{F}_\leq$. *Mathematical Structures in Computer Science*, 2:55–91, 1992. To appear in [48].

[39] H. B. Curry and R. Feys. *Combinatory Logic*, volume 1. North Holland, 1958.

[40] Nicolas G. de Bruijn. Lambda-calculus notation with nameless dummies: a tool for automatic formula manipulation with application to the Church-Rosser theorem. *Indag. Math.*, 34(5):381–392, 1972.

[41] M. Dezani-Ciancaglini and I. Margaria. F-semantics for intersection type discipline. In G. Kahn, D. B. MacQueen, and G. Plotkin, editors, *Semantics of Data Types*, volume 173 of *Lecture Notes in Computer Science*, pages 279–300. Springer-Verlag, 1984.

[42] Mariangiola Dezani-Ciancaglini and Ines Margaria. A characterisation of F-complete type assignments. *Theoretical Computer Science*, 45:121–157, 1986.

[43] Mike Fagan. *Soft Typing: An Approach to Type Checking for Dynamically Typed Languages.* PhD thesis, Rice University, December 1990.

[44] Tim Freeman and Frank Pfenning. Refinement types for ML. In *Proceedings of the SIGPLAN '91 Symposium on Language Design and Implementation, Toronto, Ontario.* ACM Press, June 1991.

[45] P. Freyd, P. Mulry, G. Rosolini, and D. Scott. Extensional PERs. In *Fifth Annual Symposium on Logic in Computer Science (Philadelphia, PA)*, pages 346–354. IEEE Computer Society Press, June 1990.

[46] Giorgio Ghelli. *Proof Theoretic Studies about a Minimal Type System Integrating Inclusion and Parametric Polymorphism.* PhD thesis, Università di Pisa, March 1990. Technical report TD–6/90, Dipartimento di Informatica, Università di Pisa.

[47] Jean-Yves Girard. *Interprétation fonctionelle et élimination des coupures de l'arithmétique d'ordre supérieur.* PhD thesis, Université Paris VII, 1972.

[48] Carl A. Gunter and John C. Mitchell. *Theoretical Aspects of Object-Oriented Programming: Types, Semantics, and Language Design.* The MIT Press, 1993. To appear.

[49] Susumu Hayashi. Singleton, union and intersection types for program extraction. In Ito and Meyer [54], pages 701–730. To appear in Information and Computation.

[50] J. R. Hindley. The simple semantics for Coppo-Dezani-Sallé types. In Dezani-Ciancaglini and Montanari, editors, *Proceedings of the International Symposium on Programming*, pages 212–226. Springer-Verlag, 1982. Lecture Notes in Computer Science No. 137.

[51] J. Roger Hindley. Coppo-Dezani-Sallé types in lambda-calculus, an introduction. Draft manuscript, February 1989.

[52] J. Roger Hindley and Jonathan P. Seldin. *Introduction to Combinators and λ-Calculus*, volume 1 of *London Mathematical Society Student Texts*. Cambridge University Press, 1986.

[53] Gérard Huet, editor. *Logical Foundations of Functional Programming.* University of Texas at Austin Year of Programming Series. Addison-Wesley, 1990.

[54] T. Ito and A. R. Meyer, editors. *Theoretical Aspects of Computer Software (Sendai, Japan)*, number 526 in Lecture Notes in Computer Science. Springer-Verlag, September 1991.

[55] Bart Jacobs, Ines Margaria, and Maddalena Zacchi. Expansion and conversion models in the lambda calculus from filters with polymorphic types. Manuscript, March 1989.

[56] Daniel Leivant. Discrete polymorphism (summary). In *Proceedings of the 1990 ACM Conference on Lisp and Functional Programming*, pages 288–297, 1990.

[57] Simone Martini. Bounded quantifiers have interval models. In *Proceedings of the ACM Conference on Lisp and Functional Programming*, pages 174–183, Snowbird, Utah, July 1988. ACM.

[58] John C. Mitchell. Polymorphic type inference and containment. *Information and Computation*, 76:211–249, 1988.

[59] John C. Mitchell. A type-inference approach to reduction properties and semantics of polymorphic expressions. In Huet [53], pages 195–212.

[60] John Mitchell, Sigurd Meldal, and Neel Madhav. An extension of Standard ML modules with subtyping and inheritance. In *Proceedings of the Eighteenth ACM Symposium on Principles of Programming Languages*, pages 270–278, Orlando, FL, January 1991.

[61] Piergiorgio Odifreddi, editor. *Logic and Computer Science.* Number 31 in APIC Studies in Data Processing. Academic Press, 1990.

[62] Benjamin Pierce. A decision procedure for the subtype relation on intersection types with bounded variables. Technical Report CMU-CS-89-169, School of Computer Science, Carnegie Mellon University, September 1989.

[63] Benjamin C. Pierce. Programming with intersection types, union types, and polymorphism. Technical Report CMU-CS-91-106, Carnegie Mellon University, February 1991.

[64] Benjamin C. Pierce. Bounded quantification is undecidable. *Information and Computation*, 1993. To appear; also to appear in [48]. Preliminary version in proceedings of POPL '91.

[65] Benjamin C. Pierce and David N. Turner. Simple type-theoretic foundations for object-oriented programming. *Journal of Functional Programming*, 1993. To appear; a preliminary version appeared in Principles of Programming Languages, 1993, and as University of Edinburgh technical report ECS-LFCS-92-225, under the title "Object-Oriented Programming Without Recursive Types".

[66] Garrell Pottinger. A type assignment for the strongly normalizable λ-terms. In *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus, and Formalism*, pages 561–577. Academic Press, New York, 1980.

[67] John Reynolds. Towards a theory of type structure. In *Proc. Colloque sur la Programmation*, pages 408–425, New York, 1974. Springer-Verlag LNCS 19.

[68] J. C. Reynolds. The essence of algol. In J. W. de Bakker and J. C. van Vliet, editors, *Algorithmic Languages*, pages 345–372, Amsterdam, 1981. North-Holland.

[69] John C. Reynolds. Preliminary design of the programming language Forsythe. Technical Report CMU-CS-88-159, Carnegie Mellon University, June 1988.

[70] John C. Reynolds. The coherence of languages with intersection types. In Ito and Meyer [54], pages 675–700.

[71] Simona Ronchi della Rocca. Principal type scheme and unification for intersection type discipline. *Theoretical Computer Science*, 59:181–209, 1988.

[72] S. Ronchi della Rocca and B. Venneri. Principal type schemes for an extended type theory. *Theoretical Computer Science*, 28:151–169, 1984.

[73] P. Sallé. Une extension de la theorie des types en λ-calcul. pages 398–410. Springer-Verlag, 1982. Lecture Notes in Computer Science No. 62.

[74] Dana Scott. Data types as lattices. *SIAM Journal on Computing*, 5(3):522–587, 1976.

[75] Steffen van Bakel. Principal type schemes for the strict type assignment system. Technical report 91-6, University of Nijmegen, 1991.

[76] Steffen van Bakel. Complete restrictions of the intersection type discipline. *Theoretical Computer Science*, 99, 1992. To appear.

[77] Hirofumi Yokouchi. Relationship between polymorphic types and intersection types (extended abstract). Unpublished manuscript, December 1990.