A Record Calculus Based on Symmetric Concatenation

Robert Harper Benjamin Pierce

Revised July 2, 1991
CMU-CS-90-157R

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Abstract

Type systems for operations on extensible records form a foundation for statically typed languages addressing some aspects of object oriented programming and database applications. A number of primitive operations have been proposed: extending a record with a new field, overwriting an existing field, removing a field, and various kinds of concatenation. We show here that a record calculus based on a symmetric concatenation operator, where two records may be concatenated only if they have no overlapping fields, also captures the types of many other useful primitive record operations. "Mergeability constraints" are expressed directly using explicit annotations on type variables and constrained second-order type quantification instead of a rule of subsumption; we argue that the resulting system is more straightforward than subsumption-based alternatives.

This research was supported in part by the Office of Naval Research and in part by the Defense Advanced Research Projects Agency (DOD), monitored by the Office of Naval Research under Contract N00014-84-K-0415, ARPA Order No. 5404.

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of ONR, DARPA or the U.S. government.

Keywords: Lambda calculus and related systems, Language theory, Programming, Type structure, Data types and structures, Records.

1 Introduction

Cardelli [2, 3] observed that certain aspects of *inheritance* in object-oriented languages can be understood in terms of inclusion relations among record types in a typed λ-calculus. These inclusions are defined formally as a *subtype* relation: a type $\mathtt{t}$ is a subtype of $\mathtt{t}'$, written $\mathtt{t} \leq \mathtt{t}'$, if any member of $\mathtt{t}$ may safely be used in a context where a member of $\mathtt{t}'$ is expected. The fact that the type of an expression may always be promoted to a supertype is captured by the rule of *subsumption*:

$$\frac{\mathtt{G} \vdash \mathtt{e} \in \mathtt{t} \qquad \mathtt{G} \vdash \mathtt{t} \leq \mathtt{t}'}{\mathtt{G} \vdash \mathtt{e} \in \mathtt{t}'} \qquad \text{(SUBSUMPTION)}$$

Cardelli and Wegner [6] extended this idea to a powerful second-order type system combining Cardelli's ordering on record types with type quantification [9, 23] using techniques developed by Mitchell [17]. Wand [25, 26] analyzed the concept of record polymorphism in the context of ML type inference and introduced the notion of "row variables," which allow types to be given to terms involving a natural *record extension* operator. This work was refined by Jategaonkar and Mitchell [12, 13] and Stansifer [24].

Rémy [20] introduced the notion of *positive and negative information* about record fields and the intuition that increasing either positive or negative information — specifying that fields are either definitely present or definitely absent — gives more refined types. This intuition, formalized as an appropriate extension to the kind system, plus the restriction that the set of field labels is finite, enabled him to use ordinary unification as in ML [8] to do type inference for programs involving extensible records. Both Wand [28] and Rémy [21, 22] later extended this system to infinite label sets.

More recently, Cardelli and Mitchell [4, 5] discovered an elegant calculus of primitive record operations combining bounded quantification with positive and negative information about fields and generalizing Cardelli's original subtype ordering on fixed-length records. In this system, the preorder on types is used to encode both positive and negative information. For example, record extensions like $\mathtt{e}|\mathtt{l}{=}\mathtt{e}'$ ("$\mathtt{e}$ extended with value $\mathtt{e}'$ at label $\mathtt{l}$") are only well formed when the field being added is not already present; to prevent run time type errors, the typing rule for extension must ensure that this is the case. Cardelli and Mitchell express this constraint in terms of the preorder by requiring that "$\mathtt{e}$ has some type $\mathtt{r}$ that is a subtype of a type lacking $\mathtt{l}$." The *restriction* operator $\backslash$ is used to increase negative information; for example, if $\mathtt{r}$ is the record type $\{\mathtt{l}_1{:}\mathtt{t}_1\}$, then $\mathtt{r}\backslash\mathtt{l}_2$ is a subtype of $\mathtt{r}$.

In an earlier report [10], we set out to represent positive and negative information as directly as possible, using explicit constraints on record type variables rather than encoding constraints in a preorder structure on types. For example, this system expresses the well-typedness constraint on $\mathtt{e}|\mathtt{l}{=}\mathtt{e}'$ as "$\mathtt{e}$ has type $\mathtt{r}$ and $\mathtt{r}$ lacks $\mathtt{l}$," where the judgement form "$\mathtt{r}$ lacks $\mathtt{l}$" is axiomatized explicitly. The result is a somewhat simpler but more verbose system with no rule of subsumption, where genericity over record types arises solely from *constrained quantification* of type variables: a quantified type "$\forall\mathtt{a}$ lacks $\mathtt{L}^-$ has $\mathtt{L}^+{:}\mathtt{T}^+.\,\mathtt{t}$" can be instantiated with any record type $\mathtt{r}$ such that $\mathtt{r}$'s set of fields is disjoint from $\mathtt{L}^-$ and includes each $\mathtt{l}_i{:}\mathtt{t}_i$ in $\mathtt{L}^+{:}\mathtt{T}^+$. This line of development essentially amounts to reverse-engineering Cardelli and Mitchell's system back toward Rémy's. In fact, during the early stages of their work Cardelli and Mitchell independently developed a similar system by extending the kind system of the polymorphic λ-calculus along the lines suggested by Rémy.

Other useful ways of manipulating records are provided by the *merge* or *concatenate* operator $||$, which combines the fields of two existing records. There are several alternative forms of the merge operator, distinguished by what happens when the records $\mathtt{e}_1$ and $\mathtt{e}_2$ in a merge expression $\mathtt{e}_1||\mathtt{e}_2$ have one or more fields in common. The *asymmetric merge* operator gives preference to the values from $\mathtt{e}_2$. The *symmetric merge* operator disallows merge expressions where the fields of $\mathtt{e}_1$ and $\mathtt{e}_2$ are not guaranteed to be disjoint. The *recursive merge* computes the values of common fields by recursively merging their values in $\mathtt{e}_1$ and $\mathtt{e}_2$. Of these, the symmetric variant seems to us to be the most useful, since it makes the finest distinctions. This is the version we assume in the present paper, except where explicitly indicated.

A restricted form of merging can be defined directly. For example, $\{\mathtt{l}_1{:}\mathtt{t}_1, \mathtt{l}_2{:}\mathtt{t}_2\} \,||\, \{\mathtt{l}_3{:}\mathtt{t}_3, \mathtt{l}_4{:}\mathtt{t}_4\}$ can be rewritten simply as $\{\mathtt{l}_1{:}\mathtt{t}_1, \mathtt{l}_2{:}\mathtt{t}_2, \mathtt{l}_3{:}\mathtt{t}_3, \mathtt{l}_4{:}\mathtt{t}_4\}$. But in general — when the types of $\mathtt{e}_1$ and $\mathtt{e}_2$ may involve variables — typechecking with $||$ requires a substantial increase in the complexity of the type system. To

ensure that λx:a. λy:b. (x||y) is well typed, we need to guarantee that the type variables a and b are never instantiated to types with overlapping fields. This condition cannot be stated in terms of the previous forms of positive and negative information ("has" and "lacks" constraints), but must be provided explicitly by annotating type variables and quantifiers with *compatibility constraints*. Once this information is provided for type variables, we can define what it means for two arbitrary types r_1 and r_2 to be compatible, written $r_1 \# r_2$. The merge expression $e_1||e_2$ is then well typed when $e_1 \in r_1$, $e_2 \in r_2$, and $r_1 \# r_2$. The type of this expression is the *merge type* $r_1||r_2$.

Wand [28] studied type inference for an extension of ML with an asymmetric merge operator and showed how to encode class definitions similar to those found in object-oriented programming languages in this calculus. The asymmetric merge operation has the advantage that compatibility constraints are not necessary: any two records may be merged, with the rightmost one overriding. On the other hand, the use of symmetric merge allows the type checker to detect inadvertent clashes of labels, which can be useful in practice. Both systems have the property that the type checker must keep track of which component of a merge has a given field, leading to problems in type reconstruction.

Ohori and Buneman studied type inference for object-oriented programming [18] and for database programming languages [19] — another promising application area for record type systems. In their work on database programming languages they consider a type system including records and sets, with operations such as "relational join" chosen to support database applications. To perform ML-like type inference for this language, they introduce the notion of a *conditional type scheme*, in which a type variable may be constrained to range over records possessing certain components. These constraints are similar to the "has" constraints discussed above. (They also used another form of constraint pertinant to the relational join and projection operations.) In their work on object-oriented programming, they consider a form of record update operation in which a value of a given field may be overridden. Once again, their notion of conditional type scheme plays a central role. They also consider extensions to support object-oriented programming constructs similar to those suggested by Wand. In order to support inheritance, they introduce an *ad hoc* form of subsumption in connection with "self" and an additional form of condition on conditional type schemes.

Cardelli and Mitchell sketched several increasingly ambitious formulations of recursive record concatenation as extensions to their calculus of operations on records [5]. The most powerful of these requires the notion of "constrained, multiply-bounded quantification," where a finite set of type variables is bound simultaneously, with each constrained to be a subtype of some given type and certain subsets constrained to be compatible. For example, a function that takes two compatible records x_1 and x_2, where x_1 has at least a field l_1 of type Int and x_2 has at least a field l_2 of type Int, and returns the result of merging x_1 and x_2, can be written

$$\Lambda(a_1 \le \{l_1 : \mathtt{Int}\}, a_2 \le \{l_2 : \mathtt{Int}\}, a_1 \# a_2).\ \ \lambda x_1{:}a_1.\ \lambda x_2{:}a_2.\ x_1||x_2.$$

(altering their concrete syntax slightly).

In the present paper, we study a record calculus $\lambda^{||}$ based on a more straightforward formulation of constrained quantification. In $\lambda^{||}$, each record type variable in a context G has a list of *compatibility assumptions* R, where the elements of R are record types and a#R asserts that $a \# r_i$ for each $r_i \in R$. The constrained type abstraction operator Λa#R. e adds the assumption a#R to the context used to typecheck e. A type application e[r] must check that r satisfies all of the constraints on the quantifier. For example, the function mentioned above can be defined in $\lambda^{||}$ as follows:

$$\Lambda a_1 \# l_1{:}\mathtt{Int}, l_2{:}\mathtt{Int}.\ \ \Lambda a_2 \# a_1, l_1{:}\mathtt{Int}, l_2{:}\mathtt{Int}.$$
$$\lambda x_1{:}a_1||l_1{:}\mathtt{Int}.\ \lambda x_2{:}a_2||l_2{:}\mathtt{Int}.\ x_1\ ||\ x_2.$$

This example underscores an important point: the form of constraint used in $\lambda^{||}$ can only be used to express *negative* information about record type variables. The function above takes two type variables, each of which *lacks* the appropriate field. To form the types expected for the records x_1 and x_2 on the two λ-abstractions, the missing fields are merged back into a_1 and a_2. This kind of transformation from mixed positive and negative constraints on quantifiers to pure negative constraints can be carried out mechanically.

The use of constrained type variables here has a very similar flavor to Wand's treatment of merging with row variables [28]. In fact, we adopt the same point of view as Wand with regard to subsumption: rather than introduce a preorder on types that includes record extension as a special case, we prefer to use a form of quantification to capture the possible extensions of a record type and use type application to

choose the appropriate extension for a given context. However, in contrast to Wand, we are dealing with an explicitly-typed, second-order calculus with a symmetric, rather than asymmetric, merge operator. This leads to a somewhat different overall flavor, as we shall illustrate below.

Our central claim is that the straightforward formulation of constrained quantification embodied in $\lambda^{||}$ may be viewed as *primary*, in the sense that most of the examples motivating row variables, bounded quantification, and Cardelli and Mitchell's bounded quantification with positive and negative information can be expressed in a calculus based on this form of constrained quantifier, with no need for additional mechanisms like subsumption.

In Section 2 we define the syntax and typing rules of $\lambda^{||}$ and sketch a proof of the decidability of typechecking. Section 3 illustrates the expressiveness of the system through a number of examples. Section 4 describes some promising avenues for further research. Section 5 offers concluding remarks. A complete listing of the typing rules for $\lambda^{||}$ appears in Appendix A; complete rules for the algorithmic formulation used to prove decidability are given in Appendix B.

2 Definition and Properties of $\lambda^{||}$

2.1 Syntax

This section introduces some notational conventions and defines the concrete syntax of $\lambda^{||}$.

The metavariable $\mathtt{t}$ and $\mathtt{u}$ range over types; $\mathtt{r}$, and $\mathtt{s}$ range over record types; $\mathtt{p}$ ranges over primitive types; $\mathtt{a}$ and $\mathtt{b}$ range over record type variables; $\mathtt{R}$ and $\mathtt{S}$ range over finite sequences of record types; $\mathtt{e}$ and $\mathtt{f}$ range over terms; $\mathtt{x}$ ranges over variables; $\mathtt{l}$ ranges over field labels.

Types:

$\mathtt{t}$	::=	$\mathtt{p}$	primitive
	|	$\mathtt{t}_1 \to \mathtt{t}_2$	function space
	|	$\forall \mathtt{a} \# \mathtt{R}.\ \mathtt{t}$	constrained quantification
	|	$\mathtt{r}$	record type

Record types:

$\mathtt{r}$	::=	$\mathtt{a}$	record type variable
	|	$\mathtt{Empty}$	empty record
	|	$\mathtt{l}{:}\mathtt{t}$	single-field record
	|	$\mathtt{r} \backslash \mathtt{l}$	restriction
	|	$\mathtt{r}_1 \,||\, \mathtt{r}_2$	merge

The record types are those built up from record type variables, $\mathtt{Empty}$, and single-field records by applications of merge and restriction. Ordinary type quantification is omitted from this presentation, but could be added by considering general type variables and an associated quantifier.

Constraint lists:

$\mathtt{R}$	::=	$\diamond$	empty constraint list
	|	$\mathtt{r}, \mathtt{R}$	nonempty constraint list

Note that we make no provision here for including "bare labels" in constraint lists. Formally, expressions like $\forall \mathtt{a} \# \mathtt{l}.\ \mathtt{t}$ are taken as abbreviations for $\forall \mathtt{a} \# (\mathtt{l}{:}\mathtt{s}).\ \mathtt{t}$, where $\mathtt{s}$ is some dummy type. (See Section 3 for examples of this idiom.)

It is sometimes convenient to consider a list as a finite set and write, for example, $\mathtt{r} \in \mathtt{R}$.

Terms:

e	::=	x	variable
		λx:t. e	abstraction
		$e_1 e_2$	application
		empty	empty record
		l=e	single-field record
		e\l	restriction
		$e_1 \,||\, e_2$	merge
		e.l	selection
		Λa#R. e	constrained type abstraction
		e[r]	constrained type application

Free and bound variables are defined in the usual way; in the case of type quantification and abstraction, the variable a is not considered bound in the constraint list R. Terms and types are identified up to renaming of bound variables. The notation [t/a]t′ denotes capture-avoiding substitution of t for free occurrences of a in t′; similarly, [e/x]e′ denotes capture-avoiding substitution of e for free occurrences of x in e′.

The metavariable T ranges over type contexts — finite sequences of declarations of the form a#R with no type variable declared twice. The metavariable G ranges over term contexts — finite sequences of declarations of the form x:t with no variable mentioned twice.

If l is a label and r is a well-formed record type, then r_l is defined to be the type associated with label l in r, if any. More precisely, the partial function r_l is defined by induction on the structure of r as follows. (We write r_l ↑ for "r_l is undefined" and r_l ↓ for "r_l is defined.")

(l:t)_l	=	t	
(r\l′)_l	=	r_l	when $l \neq l'$
$(r_1 \,||\, r_2)$_l	=	r_1_l	if r_1_l ↓ and r_2_l ↑
$(r_1 \,||\, r_2)$_l	=	r_2_l	if r_2_l ↓ and r_1_l ↑
r_l ↑			otherwise.

2.2 Typing Rules

$\lambda^{||}$ is a formal system for deriving judgements of the following forms:

Well-formed type context:	T ok
Well-formed term context:	T ⊢ G ok
Well-formed type:	T ⊢ t type
Well-formed record type:	T ⊢ r record
Well-formed constraint list:	T ⊢ R ok
Constraint list satisfaction:	T ⊢ r # R
Compatible types:	T ⊢ r_1 # r_2
Equivalent types:	$t_1 \sim t_2$
Equivalent constraint sets:	$R_1 \sim R_2$
Well-formed term:	T ; G ⊢ e ∈ t

The complete set of rules for $\lambda^{||}$ appears in Appendix A. We summarize these rules in the remainder of this section.

The rules for context formation are the expected ones (rules WFTC-* and WFC-*; see Appendix A). A type context T, a#R is well-formed if a is not already declared in T and R is well-formed in T. A term context G, x:t is well-formed in T if x is not already declared in G and if t is a well-formed type in T.

A constraint list R is well formed in T iff each component type expression r in R is a well-formed record type in T (rule WFCL).

The rules for formation of primitive types (WFT-PRIM) and function types (WFT-ARROW) are as usual. A quantified type ∀a#R. t is well-formed in T if R is a well-formed constraint list in T, and t is a well-formed type in T, r#R (rule WFT-ALL). Every record type is a type(rule WFT-REC).

The formation rules for record types are summarized in Figure 1. A record type variable is a record type in T provided that it is declared in T (rule WFR-VAR). The empty record is always well-formed (rule WFR-EMPTY). The single-field record l:t is well-formed in T if t is a well-formed type in T (rule WFR-BASE).

$$\frac{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \text{ ok}}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{a} \text{ record}} \quad \text{(WFR-VAR)}$$

$$\frac{\mathtt{T} \vdash \mathtt{t} \text{ type}}{\mathtt{T} \vdash \mathtt{l}{:}\mathtt{t} \text{ record}} \quad \text{(WFR-BASE)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \text{ record} \qquad \mathtt{r_l}\downarrow}{\mathtt{T} \vdash \mathtt{r}\backslash\mathtt{l} \text{ record}} \quad \text{(WFR-RESTR)}$$

$$\frac{\mathtt{T} \text{ ok}}{\mathtt{T} \vdash \mathtt{Empty} \text{ record}} \quad \text{(WFR-EMPTY)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r}_1 \# \mathtt{r}_2}{\mathtt{T} \vdash \mathtt{r}_1 \,||\, \mathtt{r}_2 \text{ record}} \quad \text{(WFR-MERGE)}$$

Figure 1: Selected formation rules for record types

$$\frac{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e} \in \mathtt{t}}{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{l}{=}\mathtt{e} \in \mathtt{l}{:}\mathtt{t}} \quad \text{(WTT-BASE)}$$

$$\frac{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e} \in \mathtt{r} \qquad \mathtt{r_l}\downarrow}{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}\backslash\mathtt{l} \in \mathtt{r}\backslash\mathtt{l}} \quad \text{(WTT-RESTR)}$$

$$\frac{\mathtt{T} \vdash \mathtt{G} \text{ ok}}{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{empty} \in \mathtt{Empty}} \quad \text{(WTT-EMPTY)}$$

$$\frac{\begin{array}{c}\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}_1 \in \mathtt{r}_1 \\ \mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}_2 \in \mathtt{r}_2 \\ \mathtt{T} \vdash \mathtt{r}_1 \# \mathtt{r}_2\end{array}}{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}_1||\mathtt{e}_2 \in \mathtt{r}_1||\mathtt{r}_2} \quad \text{(WTT-MERGE)}$$

$$\frac{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e} \in \mathtt{r} \qquad \mathtt{r_l}\downarrow}{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e.l} \in \mathtt{r_l}} \quad \text{(WTT-SELECT)}$$

$$\frac{\mathtt{T}, \mathtt{a}\#\mathtt{R}\,;\mathtt{G} \vdash \mathtt{e} \in \mathtt{t}}{\mathtt{T}\,;\mathtt{G} \vdash \Lambda\mathtt{a}\#\mathtt{R}.\mathtt{e} \in \forall\mathtt{a}\#\mathtt{R}.\,\mathtt{t}} \quad \text{(WTT-ALL-I)}$$

$$\frac{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e} \in \forall\mathtt{a}\#\mathtt{R}.\,\mathtt{t} \qquad \mathtt{T} \vdash \mathtt{r} \# \mathtt{R}}{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}[\mathtt{r}] \in [\mathtt{r}/\mathtt{a}]\mathtt{t}} \quad \text{(WTT-ALL-E)}$$

Figure 2: Selected typing rules

$$\frac{\mathtt{T} \vdash \mathtt{r} \# \mathtt{s} \qquad \mathtt{r} \sim \mathtt{r}' \qquad \mathtt{s} \sim \mathtt{s}'}{\mathtt{T} \vdash \mathtt{r}' \# \mathtt{s}'} \quad \text{(Cmp-Eq)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \# \mathtt{s}}{\mathtt{T} \vdash \mathtt{s} \# \mathtt{r}} \quad \text{(Cmp-Symm)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \# \mathtt{l}{:}\mathtt{t} \qquad \mathtt{T} \vdash \mathtt{t}' \text{ type}}{\mathtt{T} \vdash \mathtt{r} \# \mathtt{l}{:}\mathtt{t}'} \quad \text{(Cmp-Base)}$$

$$\frac{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \text{ ok} \qquad \mathtt{r}_i \in \mathtt{R}}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{a} \# \mathtt{r}_i} \quad \text{(Cmp-Tvar)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \# (\mathtt{s}_1 || \mathtt{s}_2)}{\mathtt{T} \vdash \mathtt{r} \# \mathtt{s}_i} \quad \text{(Cmp-Merge-E)}$$

$$\frac{\mathtt{T} \vdash \mathtt{s}_1 \# \mathtt{s}_2 \qquad \mathtt{T} \vdash \mathtt{r} \# \mathtt{s}_1 \qquad \mathtt{T} \vdash \mathtt{r} \# \mathtt{s}_2}{\mathtt{T} \vdash \mathtt{r} \# (\mathtt{s}_1 || \mathtt{s}_2)} \quad \text{(Cmp-Merge-I)}$$

$$\frac{\mathtt{l} \neq \mathtt{l}' \qquad \mathtt{T} \vdash \mathtt{l}{:}\mathtt{t} \text{ record} \qquad \mathtt{T} \vdash \mathtt{l}'{:}\mathtt{t}' \text{ record}}{\mathtt{T} \vdash \mathtt{l}{:}\mathtt{t} \# \mathtt{l}'{:}\mathtt{t}'} \quad \text{(Cmp-Base/Base)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \text{ record}}{\mathtt{T} \vdash \mathtt{r} \# \mathtt{Empty}} \quad \text{(Cmp-Empty)}$$

Figure 3: Selected compatibility rules

$$\mathtt{r} || \mathtt{Empty} \sim \mathtt{r} \quad \text{(Eq-Merge-Unit)}$$

$$\mathtt{r}_1 \,||\, (\mathtt{r}_2 || \mathtt{r}_3) \sim (\mathtt{r}_1 || \mathtt{r}_2) \,||\, \mathtt{r}_3 \quad \text{(Eq-Merge-Assoc)}$$

$$\mathtt{r}_1 \,||\, \mathtt{r}_2 \sim \mathtt{r}_2 \,||\, \mathtt{r}_1 \quad \text{(Eq-Merge-Comm)}$$

$$\mathtt{r}\backslash\mathtt{l}\backslash\mathtt{l}' \sim \mathtt{r}\backslash\mathtt{l}'\backslash\mathtt{l} \quad \text{(Eq-Restr/Restr')}$$

$$(\mathtt{l}{:}\mathtt{t})\backslash\mathtt{l} \sim \mathtt{Empty} \quad \text{(Eq-Base/Restr)}$$

$$\frac{\mathtt{r}_1 _ \mathtt{l} \downarrow}{(\mathtt{r}_1 || \mathtt{r}_2)\backslash\mathtt{l} \sim (\mathtt{r}_1\backslash\mathtt{l} || \mathtt{r}_2)} \quad \text{(Eq-Merge/Restr)}$$

$$\frac{\mathtt{R} \sim \mathtt{R}' \qquad \mathtt{t} \sim \mathtt{t}'}{\forall \mathtt{a}\#\mathtt{R}.\ \mathtt{t} \sim \forall \mathtt{a}\#\mathtt{R}'.\ \mathtt{t}'} \quad \text{(Eq-Cong-All)}$$

Figure 4: Selected type equivalence rules

$$\mathtt{r}, (\mathtt{r}', \mathtt{R}) \sim \mathtt{r}', (\mathtt{r}, \mathtt{R}) \qquad \text{(CEQ-SWAP)}$$

$$\mathtt{Empty}, \mathtt{R} \sim \mathtt{R} \qquad \text{(CEQ-EMPTY)}$$

$$(\mathtt{r}_1 || \mathtt{r}_2), \mathtt{R} \sim \mathtt{r}_1, (\mathtt{r}_2, \mathtt{R}) \qquad \text{(CEQ-MERGE)}$$

$$\mathtt{r}, (\mathtt{r}, \mathtt{R}) \sim \mathtt{r}, \mathtt{R} \qquad \text{(CEQ-DUPL)}$$

$$\mathtt{l}{:}\mathtt{t}, \mathtt{R} \sim \mathtt{l}{:}\mathtt{t}', \mathtt{R} \qquad \text{(CEQ-BASE)}$$

Figure 5: Selected constraint list equivalence rules

The restriction $\mathtt{r}\backslash\mathtt{l}$ is well formed in $\mathtt{T}$ if $\mathtt{r}$ is well formed in $\mathtt{T}$ and $\mathtt{r_l}$ is defined (rule WFR-RESTR). In particular, no expression of the form $\mathtt{a}\backslash\mathtt{l}$, where $\mathtt{a}$ is a variable, is ever well formed, since $\mathtt{a_l}$ is never defined. This reflects the fact that compatibility constraints on a variable $\mathtt{a}$ are negative in character and cannot be used to postulate that all instances of $\mathtt{a}$ *have* any particular fields, only that they *lack* certain fields. It also implies that if $\mathtt{r}\backslash\mathtt{l}$ is a well-formed record expression, then the restriction may be eliminated (see the discussion of type equivalence below). A merge $\mathtt{r}_1||\mathtt{r}_2$ is well-formed in $\mathtt{T}$ if $\mathtt{r}_1$ and $\mathtt{r}_2$ are well-formed in $\mathtt{T}$, and, morover, $\mathtt{r}_1$ and $\mathtt{r}_2$ are compatible in $\mathtt{T}$ (see below).

The typing rules for $\lambda^{||}$ terms are organized along standard lines. Typing is invariant under type equality (rule WTT-EQ). The rules for variables, lambda abstractions, and application are standard (rules WTT-VAR, WTT-ARROW-I, WTT-ARROW-E).

The abstraction $\Lambda\mathtt{a}\#\mathtt{R}.\ \mathtt{e}$ has type $\forall\mathtt{a}\#\mathtt{R}.\ \mathtt{t}$ provided that $\mathtt{e}$ has type $\mathtt{t}$ in $\mathtt{T}, \mathtt{a}\#\mathtt{R}$, which also entails that $\mathtt{R}$ is a well-formed constraint set in $\mathtt{T}$ (rule WTT-ALL-I). It is important to realize that the constraint list $\mathtt{R}$ cannot be replaced by a single record type $\mathtt{r}$, for two related reasons. First, it is necessary to postulate that a variable be compatible with a number of different record types. For example, if we are to merge a variable $\mathtt{a}$ with the base records $\mathtt{l}{:}\mathtt{t}$ and $\mathtt{l}'{:}\mathtt{t}'$, then $\mathtt{a}$ must be constrained to be compatible with both of these records, which is to say that all instances of $\mathtt{a}$ must not contain $\mathtt{l}$ or $\mathtt{l}'$ fields. Second, the constraint list $\mathtt{R}$ cannot be collapsed into a single record type consisting of the merge of the component record types $\mathtt{r}_i$ of $\mathtt{R}$ because the records in $\mathtt{R}$ need not themselves be mutually compatible. In particular, we may wish to postulate that a variable $\mathtt{a}$ is compatible with two other variables $\mathtt{b}$ and $\mathtt{c}$ so that the merges $\mathtt{a}||\mathtt{b}$ and $\mathtt{a}||\mathtt{c}$ are both well-formed. This in no way entails that $\mathtt{b}$ and $\mathtt{c}$ must be compatible, and it would be a serious restriction to require that they be so.

The type application $\mathtt{e}[\mathtt{r}]$ is well formed in $\mathtt{T}$ if $\mathtt{e}$ has type $\forall\mathtt{a}\#\mathtt{R}.\ \mathtt{t}$ in $\mathtt{T}$, $\mathtt{r}$ is a record in $\mathtt{T}$, and $\mathtt{r}$ is compatible with each element of $\mathtt{R}$ (relative to $\mathtt{T}$). In other words, $\mathtt{r}$ must satisfy the constraints associated with the quantifier in order for the type application to be sensible. When this is the case, the type of $\mathtt{e}[\mathtt{r}]$ is $[\mathtt{r}/\mathtt{a}]\mathtt{t}$, as usual (rule WTT-ALL-E). It will turn out that the formulation of the system ensures that if $\mathtt{r}$ satisfies the constraints in $\mathtt{R}$ relative to $\mathtt{T}$, then $\mathtt{r}$ is a record type in $\mathtt{T}$. To support general parametric polymorphism, we would have to extend the system with a separate form of quantifier that quantifies over all types. We omit this extension for the sake of simplicity.

The compatibility relation plays a central role in $\lambda^{||}$. Informally, $\mathtt{T} \vdash \mathtt{r} \# \mathtt{s}$ holds iff $\mathtt{r}$ and $\mathtt{s}$ are mergeable, that is, iff $\mathtt{r}$ lacks every field possessed by $\mathtt{s}$ and $\mathtt{s}$ lacks every field possessed by $\mathtt{r}$. The definition is made relative to a context $\mathtt{T}$ since the compatibility for a type variable $\mathtt{a}$ is determined by the constraint set associated with $\mathtt{a}$ in $\mathtt{T}$. It follows from this informal description that compatibility is symmetric, respects type equivalence, and is insensitive to the types ascribed to fields of a record. In particular, $\mathtt{l}{:}\mathtt{t}$ is compatible with $\mathtt{l}'{:}\mathtt{t}'$ iff $\mathtt{l}$ is different from $\mathtt{l}'$.

A selection of the rules defining the compatiblity relation appear in Figure 3. Compatibility is symmetric (rule CMP-SYMM) and respects type equivalence (rule CMP-EQ). If a record is compatible with a single-field record $\mathtt{l}{:}\mathtt{t}$, then it is compatible with every single-field record $\mathtt{l}{:}\mathtt{t}'$ (rule CMP-BASE). A type variable is

compatible with the records in its constraint list (rule CMP-TVAR). A record is compatible with a merge iff it is compatible with each of the components of the merge (rules CMP-MERGE-I and CMP-MERGE-E). Two single-field records are compatible if they have different labels (rule CMP-BASE/BASE). Every record is compatible with the empty record (rule CMP-EMPTY). It is worth noting that there are no rules for compatibility of records of the form $\mathtt{r}\backslash\mathtt{l}$. It will be possible to prove that every well-formed record is equivalent to a unique restriction-free record; hence compatibility of restrictions is covered by the general rule of invariance of compatibility under equivalence.

A selection of the rules defining equivalence of types and constraint sets appears in Figures 4 and 5). The relation $\mathtt{t} \sim \mathtt{t}'$ is an equivalence relation (rules EQ-REFL, EQ-SYMM, and EQ-TRANS) and is a congruence with respect to the type-forming operations (rules EQ-CONG-*). The axioms for record type equivalence are as follows. Restrictions commute with one another (rule EQ-RESTR/RESTR') (in a well-formed expression $\mathtt{l}$ will be distinct from $\mathtt{l}'$, but there is no reason to insist on that in the rule.) Restriction of a singleton $\mathtt{l}$:$\mathtt{t}$ on $\mathtt{l}$ results in the empty record type (rule EQ-BASE-RESTR). Restriction distributes to the appropriate (given EQ-SYMM and EQ-CONG-RESTR) component of a merge (rule EQ-MERGE-RESTR). Merge is associative (rule EQ-MERGE-ASSOC), `Empty` is a unit of merge (rule EQ-MERGE-UNIT), and merge is commutative (rule EQ-MERGE-COMM).

Since the quantifier of $\lambda^{||}$ is constrained, the equivalence on constraint lists effects type equivalence, and hence the collection of well-typed terms. There is some flexibility in the choice of equivalence for constraint sets; the guiding principle is that equivalent constraint sets should be satisfied by the same record types. Order and multiplicity of constraints are irrelevant (rules CEQ-SWAP and CEQ-DUPL); constraint lists are essentially finite sets. Merge types in a constraint list may be "flattened", occurrences of `Empty` may be eliminated, and the types of single-field records are ignored (rules CEQ-MERGE, CEQ-EMPTY, and CEQ-BASE). As we will see below, these equivalences are sufficient to ensure that constraint sets may be normalized into the form $\mathtt{l}_1, ..., \mathtt{l}_n, \mathtt{a}_1, ..., \mathtt{a}_k$ where the $\mathtt{l}'_i$s are labels and the $\mathtt{a}_i$'s are record type variables. This is consistent with the intuition that the relevant properties of a record, for the purposes of consistency checking, are its atomic components. Note that it will not do to simply *define* constraint sets this way due to the possibility of substituting record types for type variables.

2.3 Properties

In this section we establish the decidability of type checking for $\lambda^{||}$.

The proof proceeds largely along standard lines: type checking is reduced to checking equivalence and compatibility of types by way of a syntax-directed set of type synthesis rules. Equivalence of well-formed types is established using Huet's method of confluence modulo an equivalence relation [11]. The main idea is to handle the associative and commutative rules for merge types and the permutation and idempotency equations for constraints lists by segregating the "proper reductions" from the "pure equations," so that the equivalence problem is reduced to checking a simple form of equivalence of normal forms. Compatiblity checking is based on a simple characterization of normal forms of record types and constraint lists, with the main complications stemming from the need to take account of all of the consequences of assuming that a variable is compatible with a complex record type.

2.3.1 Technical Lemmas

Lemma 2.3.1.1: A derivation of the well-formedness of a type, record type, or constraint list includes subderivations of the well-formedness of all of its subphrases.

Lemma 2.3.1.2:

1. $\mathtt{a}\backslash\mathtt{l}$ is never well formed for any variable $\mathtt{a}$, regardless of context.
2. $\mathtt{Empty}\backslash\mathtt{l}$ is never well-formed.
3. $\mathtt{r}\backslash\mathtt{l}\backslash\mathtt{l}'$ is well-formed only if $\mathtt{l} \neq \mathtt{l}'$ and $\mathtt{r}$ is not a single-field record.
4. $\mathtt{l}$:$\mathtt{t}\backslash\mathtt{l}'$ is well-formed only if $\mathtt{l} = \mathtt{l}'$.

Lemma 2.3.1.3: If $\mathtt{r_l}$ is defined and $\mathtt{r} \sim \mathtt{s}$, then $\mathtt{s_l}$ is defined and $\mathtt{r_l} \sim \mathtt{s_l}$.

Lemma 2.3.1.4: Assume that $\mathtt{T} \vdash \mathtt{r} \# \mathtt{s}$. Then it is not the case that both $\mathtt{r_l}$ and $\mathtt{s_l}$ are defined.

Corollary 2.3.1.5: If $\mathtt{r}||\mathtt{s}$ is well formed, then $\mathtt{r_l}$ defined implies $\mathtt{s_l}$ undefined, and vice versa.

Lemma 2.3.1.6: $\vdash \mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2$ ok implies $\mathtt{T}_1 \vdash \mathtt{R}$ ok as a subderivation.

Lemma 2.3.1.7: $\mathtt{T} \vdash \mathtt{r} \# \mathtt{s}$ implies $\mathtt{T} \vdash \mathtt{r}$ record and $\mathtt{T} \vdash \mathtt{s}$ record.

Lemma 2.3.1.8: If $\mathtt{T} \vdash \mathtt{r} \# \mathtt{R}$ and $\mathtt{r} \sim \mathtt{r}'$ and $\mathtt{R} \sim \mathtt{R}'$, then $\mathtt{T} \vdash \mathtt{r}' \# \mathtt{R}'$.

Lemma 2.3.1.9: Let $\mathtt{J}$ stand for an arbitrary judgement. If $\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{J}$, and $\mathtt{T}_1 \vdash \mathtt{r}\#\mathtt{R}$, then $\mathtt{T}_1, [\mathtt{r}/\mathtt{a}]\mathtt{T}_2 \vdash [\mathtt{r}/\mathtt{a}]\mathtt{J}$.

2.3.2 Confluence of reduction modulo an equivalence relation

Our proof of the confluence of type and constraint list normalization uses a technique due to Huet [11]. In this section we briefly recapitulate Huet's main theorem.

Definition 2.3.2.1: The metavariables $\mathtt{M}$, $\mathtt{N}$, $\mathtt{P}$, $\mathtt{Q}$, and $\mathtt{U}$ here range over an unspecified set of phrases (in the next section they will be either types or constraint lists).

Definition 2.3.2.2: $\mathcal{V}(\mathtt{M})$ is the set of variables appearing free in a phrase $\mathtt{M}$.

Definition 2.3.2.3: A phrase $\mathtt{M}$ is linear iff all of its variable occurrences are distinct.

Definition 2.3.2.4: A rewrite rule is a pair of terms.

Definition 2.3.2.5: A critical pair $\langle \mathtt{P}, \mathtt{Q} \rangle$ for two rewriting rules $\langle \mathtt{M}_1, \mathtt{N}_1 \rangle$ and $\langle \mathtt{M}_2, \mathtt{N}_2 \rangle$ is a most general common instance of the two rules, found by superposing $\mathtt{M}_2$ on a non-variable subphrase $\mathtt{U}$ of $\mathtt{M}_1$. $\mathtt{P}$ is the result of rewriting the subphrase $\mathtt{U}$ of the common instance according to the rule $\langle \mathtt{M}_2, \mathtt{N}_2 \rangle$. $\mathtt{Q}$ is the result of rewriting the whole common instance according to the rule $\langle \mathtt{M}_1, \mathtt{N}_1 \rangle$.

Definition 2.3.2.6: An equational theory $\langle \mathcal{R}, \mathcal{E} \rangle$ consists of two sets of rewriting rules: a "reduction part" $\mathcal{R}$ and an "equivalence part" $\mathcal{E}$.

Definition 2.3.2.7: Let $\langle \mathcal{R}, \mathcal{E} \rangle$ be an equational theory. The one-step reduction relation induced by $\mathcal{R}$ is denoted by $\twoheadrightarrow^1_{\mathcal{R}}$, and the one-step reduction relation induced by $\mathcal{E}$ is denoted by $\approx^1_{\mathcal{E}}$. The reflexive, transitive closure of $\twoheadrightarrow^1_{\mathcal{R}}$ is denoted by $\twoheadrightarrow_{\mathcal{R}}$, and the reflexive, symmetric, and transitive closure of $\approx^1_{\mathcal{E}}$ is denoted by $\approx_{\mathcal{E}}$.

The subscripts are omitted when they are clear from context.

Definition 2.3.2.8: The set of critical pairs of a reduction relation $\mathcal{R}$ is

$$\{\langle \mathtt{P}, \mathtt{Q} \rangle \mid \langle \mathtt{P}, \mathtt{Q} \rangle \text{ is a critical pair for } \langle \mathtt{M}_1, \mathtt{M}_2 \rangle, \langle \mathtt{N}_1, \mathtt{N}_2 \rangle \in \mathcal{R}\}.$$

Definition 2.3.2.9: Let $\langle \mathcal{R}, \mathcal{E} \rangle$ be an equational theory. The set of critical pairs of $\mathcal{E}/\mathcal{R}$ is

$$\begin{array}{rl} & \{\langle \mathtt{P}, \mathtt{Q} \rangle \mid \langle \mathtt{P}, \mathtt{Q} \rangle \text{ is a critical pair for } \langle \mathtt{M}_1, \mathtt{M}_2 \rangle \in \mathcal{R} \text{ and } \langle \mathtt{N}_1, \mathtt{N}_2 \rangle \in (\mathcal{E} \cup \mathcal{E}^{-1})\} \\ \cup & \{\langle \mathtt{P}, \mathtt{Q} \rangle \mid \langle \mathtt{P}, \mathtt{Q} \rangle \text{ is a critical pair for } \langle \mathtt{M}_1, \mathtt{M}_2 \rangle \in (\mathcal{E} \cup \mathcal{E}^{-1}) \text{ and } \langle \mathtt{N}_1, \mathtt{N}_2 \rangle \in \mathcal{R}\}, \end{array}$$

where

$$\mathcal{E}^{-1} = \{\langle \mathtt{N}, \mathtt{M} \rangle \mid \langle \mathtt{M}, \mathtt{N} \rangle \in \mathcal{E}\}.$$

Definition 2.3.2.10: The set of critical pairs of a theory $\langle \mathcal{R}, \mathcal{E} \rangle$ is the union of the set of critical pairs of $\mathcal{R}$ and the set of critical pairs of $\mathcal{E}/\mathcal{R}$.

Definition 2.3.2.11: $\mathtt{M}^*$ denotes an arbitrary $\mathcal{R}$-normal form of $\mathtt{M}$.

Proposition 2.3.2.12: (Huet's Theorem 3.3) Let $\langle \mathcal{R}, \mathcal{E} \rangle$ be an equational theory such that

1. for all $\langle \mathtt{M}\ ,\ \mathtt{N} \rangle \in \mathcal{R}$, $\mathcal{V}(\mathtt{N}) \subseteq \mathcal{V}(\mathtt{M})$ and $\mathtt{M}$ is linear;
2. for all $\langle \mathtt{M}\ ,\ \mathtt{N} \rangle \in \mathcal{E}$, $\mathcal{V}(\mathtt{M}) = \mathcal{V}(\mathtt{N})$;
3. $\mathcal{R} \circ \approx$ is noetherian, where $\approx$ is the reflexive, symmetric, transitive closure of $\mathcal{E}$.

The theory $\langle \mathcal{R}, \mathcal{E} \rangle$ is confluent iff for all its critical pairs $\langle \mathtt{P}, \mathtt{Q} \rangle$ we have $\mathtt{P}^* \approx \mathtt{Q}^*$. When $\langle \mathcal{R}, \mathcal{E} \rangle$ is confluent, we say that "$\mathcal{R}$ is confluent modulo $\mathcal{E}$." Then $\mathtt{M} =_{\mathcal{R} \cup \mathcal{E}} \mathtt{N}$ iff $\mathtt{M}^* \approx \mathtt{N}^*$, where $=_{\mathcal{R} \cup \mathcal{E}}$ is the equivalence relation induced by $\mathcal{R}$ and $\mathcal{E}$.

2.3.3 Type and Constraint List Equivalence

We now apply Huet's theory to the confluence of a type normalization procedure for $\lambda^{||}$.

Definition 2.3.3.1: For the algorithmic version of the system, constraint lists are extended with "bare labels":

$\mathtt{R}$	::=	$\diamond$	empty constraint list
		$\mathtt{r}, \mathtt{R}$	constraint list beginning with a type
		$\mathtt{l}, \mathtt{R}$	constraint list beginning with a bare label

We extend the relation $\mathtt{T} \vdash \mathtt{r} \# \mathtt{R}$ to constraint lists by defining $\mathtt{T} \vdash \mathtt{r} \# \mathtt{l}, \mathtt{R}$ to mean $\mathtt{T} \vdash \mathtt{r} \# \mathtt{R}$ and $\mathtt{T} \vdash \mathtt{r} \# \mathtt{l}{:}\mathtt{t}$ for any well-formed type $\mathtt{t}$.

Definition 2.3.3.2: In this section, it is convenient to be able to refer to phrases from certain related syntactic categories uniformly:

1. The metavariable α ranges over atoms: variables, base records, and bare labels.
2. The metavariables ρ, σ, and τ range over types and bare labels.
3. The metavariable ϕ ranges over type variables and bare labels.
4. The metavariable $\mathtt{C}$ ranges over types and constraint lists.

Definition 2.3.3.3: Let $\twoheadrightarrow^1$ denote the compatible extension to types and constraint lists of the reduction relation given in Figure 8.

Definition 2.3.3.4: Let $\approx^1$ denote the compatible extension to types and constraint lists of the relation given in Figure 9.

Let $\approx$ denote the equivalence relation generated by $\approx^1$. Let $\equiv$ denote the equivalence relation generated by $\twoheadrightarrow^1$ and $\approx^1$.

Theorem 2.3.3.5:

1. If $\mathtt{T} \vdash \mathtt{r}$ record and $\mathtt{r} \twoheadrightarrow^1 \mathtt{r}'$, then $\mathtt{T} \vdash \mathtt{r}'$ record.
2. If $\mathtt{T} \vdash \mathtt{t}$ type and $\mathtt{t} \twoheadrightarrow^1 \mathtt{t}'$, then $\mathtt{T} \vdash \mathtt{t}'$ type.
3. If $\mathtt{T} \vdash \mathtt{R}$ ok, and $\mathtt{R} \twoheadrightarrow^1 \mathtt{R}'$, then $\mathtt{T} \vdash \mathtt{R}'$ ok.

Proof: By induction on derivations, making use of the technical lemmas in Section 2.3.1. □

Definition 2.3.3.6: The "outer size" of a type r is defined as follows:

$$\begin{array}{lcl}
\text{outer-size}(\mathtt{a}) & = & 1 \\
\text{outer-size}(\mathtt{Empty}) & = & 1 \\
\text{outer-size}(\mathtt{l{:}t}) & = & 1 \\
\text{outer-size}(\mathtt{r\backslash l}) & = & \text{outer-size}(\mathtt{r}) + 1 \\
\text{outer-size}(\mathtt{r}_1 || \mathtt{r}_2) & = & \text{outer-size}(\mathtt{r}_1) + \text{outer-size}(\mathtt{r}_2) + 1 \\
\text{outer-size}(\mathtt{p}) & = & 0 \\
\text{outer-size}(\mathtt{t}_1 \rightarrow \mathtt{t}_2) & = & 0 \\
\text{outer-size}(\forall \mathtt{a} \# \mathtt{R}.\ \mathtt{t}) & = & 0.
\end{array}$$

Definition 2.3.3.7: The rank of a constraint list is defined as follows:

$$\begin{array}{lcl}
\text{rank}(\diamond) & = & 0 \\
\text{rank}(\mathtt{l}, \mathtt{R}) & = & \text{rank}(\mathtt{R}) \\
\text{rank}(\mathtt{r}, \mathtt{R}) & = & \text{rank}(\mathtt{r}) + \text{rank}(\mathtt{R}).
\end{array}$$

The rank of a type is the sum

$$\text{rank}(\mathtt{t}) = \text{restr-count}(\mathtt{t}) + \text{base-count}(\mathtt{t}) + \text{empty-count}(\mathtt{t}) + \text{merge-count}(\mathtt{t}),$$

where

- restr-count($\mathtt{t}$) is the sum, over all occurrences of the form $\mathtt{s\backslash l}$ in $\mathtt{t}$, of outer-size($\mathtt{s}$),
- base-count($\mathtt{t}$) is the number of base record phrases $\mathtt{l{:}t'}$ in $\mathtt{t}$,
- empty-count($\mathtt{t}$) is the number of occurrences of $\mathtt{Empty}$ in $\mathtt{t}$, and
- merge-count($\mathtt{t}$) is the number of occurrences of $||$ in $\mathtt{t}$.

Lemma 2.3.3.8: The relation $\twoheadrightarrow^1 \circ \approx$ is Noetherian when restricted to well-formed expressions. That is, there are no infinite reduction sequences of the form

$$\cdot \twoheadrightarrow^1 \cdot \approx \cdot \twoheadrightarrow^1 \cdot \approx \cdot \twoheadrightarrow^1 \cdots$$

where each of the terms in the sequence is well-formed.

Proof: Applying any of the $\twoheadrightarrow^1$ rules to a type or constraint list strictly reduces its rank, while applying any of the $\approx^1$ rules in either direction leaves the rank unchanged. □

Lemma 2.3.3.9:

1. If $\mathtt{T} \vdash (\mathtt{r\backslash l} \,||\, \mathtt{s})\mathtt{\backslash l'}$ record and $\mathtt{T} \vdash (\mathtt{r}||\mathtt{s})\mathtt{\backslash l\backslash l'}$ record, then $((\mathtt{r\backslash l} \,||\, \mathtt{s})\mathtt{\backslash l'})^* \approx ((\mathtt{r}||\mathtt{s})\mathtt{\backslash l'\backslash l})^*$.
2. If $\mathtt{T} \vdash \mathtt{a}, \mathtt{b}, (\mathtt{a}||\mathtt{b}), \mathtt{R}$ ok and $\mathtt{T} \vdash (\mathtt{a}||\mathtt{b}), \mathtt{R}$ ok, then $(\mathtt{a}, \mathtt{b}, (\mathtt{a}||\mathtt{b}), \mathtt{R})^* \approx ((\mathtt{a}||\mathtt{b}), \mathtt{R})^*$.
3. If $\mathtt{T} \vdash \mathtt{a}, \mathtt{b}, \mathtt{R}$ ok and $\mathtt{T} \vdash (\mathtt{a}||\mathtt{b}), (\mathtt{a}||\mathtt{b}), \mathtt{R}$ ok, then $(\mathtt{a}, \mathtt{b}, \mathtt{R})^* \approx ((\mathtt{a}||\mathtt{b}), (\mathtt{a}||\mathtt{b}), \mathtt{R})^*$.
4. If $\mathtt{T} \vdash \tau, \rho, \sigma, \mathtt{R}$ ok and $\mathtt{T} \vdash (\rho||\sigma), \tau, \mathtt{R}$ ok, then $(\tau, \rho, \sigma, \mathtt{R})^* \approx ((\rho||\sigma), \tau, \mathtt{R})^*$.

Lemma 2.3.3.10: For every critical pair $\langle \mathtt{C}_1, \mathtt{C}_2 \rangle$ of $\langle \twoheadrightarrow^1, \approx^1 \rangle$, we have ${\mathtt{C}_1}^* \approx {\mathtt{C}_2}^*$.

Proof: By a tedious verification, using Lemma 2.3.3.9 for the interesting cases. □

Theorem 2.3.3.11: The restriction of $\twoheadrightarrow^1$ to well-typed terms is confluent modulo $\approx$.

Corollary 2.3.3.12:

1. If $\mathtt{r}$ and $\mathtt{s}$ are well-formed records, then $\mathtt{r} \equiv \mathtt{s}$ iff there exist $\mathtt{r}'$ and $\mathtt{s}'$ in normal form such that $\mathtt{r} \twoheadrightarrow \mathtt{r}'$ and $\mathtt{s} \twoheadrightarrow \mathtt{s}'$ and $\mathtt{r}' \approx \mathtt{s}'$.

2. If $\mathtt{t}$ and $\mathtt{u}$ are well-formed types, then $\mathtt{t} \equiv \mathtt{u}$ iff there exist $\mathtt{t}'$ and $\mathtt{u}'$ such that $\mathtt{t} \twoheadrightarrow \mathtt{t}'$ and $\mathtt{u} \twoheadrightarrow \mathtt{u}'$ and $\mathtt{t}' \approx \mathtt{u}'$.

3. If $\mathtt{R}$ and $\mathtt{S}$ are well-formed constraint lists, then $\mathtt{R} \approx \mathtt{S}$ iff there exist $\mathtt{R}'$ and $\mathtt{S}'$ such that $\mathtt{R} \twoheadrightarrow \mathtt{R}'$ and $\mathtt{S} \twoheadrightarrow \mathtt{S}'$ and $\mathtt{R}' \approx \mathtt{S}'$.

Corollary 2.3.3.13: Normal forms are unique up to $\approx$.

If $\mathtt{r}$ is a well-formed record, let $\mathtt{r}^*$ denote one of its normal forms computed by applying the $\twoheadrightarrow$ rules in some canonical order; similarly for types and constraint lists.

Theorem 2.3.3.14:

1. Let $\mathtt{r}$ be a well-formed record type. Then $\mathtt{r}^*$ has the form

$$\mathtt{a}_1 \,||\, \mathtt{a}_2 \,||\, \ldots \,||\, \mathtt{a}_n \,||\, \mathtt{l}_1{:}\mathtt{t}_1 \,||\, \ldots \,||\, \mathtt{l}_k{:}\mathtt{t}_k$$

   up to associativity and commutativity of $||$, where the $\mathtt{a}_i$'s are distinct variables, the $\mathtt{l}_j$'s are distinct labels, the $\mathtt{t}_j$'s are in normal form, and n and k are greater than or equal to 0 (when both are 0, the normal form is `Empty`).

2. Let $\mathtt{R}$ be a well-formed constraint list. Then $\mathtt{R}^*$ has the form

$$\mathtt{a}_1, \ldots, \mathtt{a}_n, \mathtt{l}_1, \ldots, \mathtt{l}_k$$

   where the $\mathtt{a}_i$'s are all distinct, the $\mathtt{l}_j$'s are all distinct, and n and k are greater than or equal to 0. (That is, $\mathtt{R}^*$ is a list of variables and labels in some order.)

Note that as a consequence, a well-formed normal form is restriction-free. This implies that every well-formed record expression reduces to a well-formed restriction-free record expression.

Lemma 2.3.3.15: The rule

$$\mathtt{r}, \mathtt{r}, \mathtt{R} \;\equiv\; \mathtt{r}, \mathtt{R} \qquad \text{(A-CEQ-FULL-DUPL)}$$

is admissible when $\mathtt{r}, \mathtt{r}, \mathtt{R}$ and $\mathtt{r}, \mathtt{R}$ are well formed.

Proof sketch: By construction. Consider a reduction of $\mathtt{r}, \mathtt{R}$ to normal form. By Theorem 2.3.3.14, $(\mathtt{r}, \mathtt{R})^*$ consists only of type variables and labels. We may therefore use rules A-CEQ-DUPL and A-CEQ-MERGE to duplicate the sublist of type variables and labels that come from $\mathtt{r}$. By replaying the reduction from $\mathtt{r}, \mathtt{R}$ to $(\mathtt{r}, \mathtt{R})^*$ twice in reverse, we obtain $\mathtt{r}, \mathtt{r}, \mathtt{R} \equiv (\mathtt{r}, \mathtt{R})^*$. The result follows by transitivity of $\equiv$. □

Theorem 2.3.3.16: The relations $\sim$ and $\equiv$ coincide on well-typed terms.

Proof: It is easy to see that every $\twoheadrightarrow^1$ and $\approx^1$ axiom is a valid equivalence, and conversely (using Lemma 2.3.3.15 in the case of EQ-DUPL), that every equivalence axiom holds in $\equiv$. □

Corollary 2.3.3.17: The relation $\sim$ is decidable for well-formed expressions.

Proof: To decide whether or not $\mathtt{r} \sim \mathtt{s}$, given that $\mathtt{r}$ and $\mathtt{s}$ are well-formed, reduce each to their normal forms and test whether or not $\mathtt{r}^* \sim \mathtt{s}^*$. Given the characterization of normal forms given above, this reduces to re-grouping the atomic record types in some standard order. Similar methods apply to constraint sets and types. □

$$\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{Empty} \qquad \text{(A-Cmp-Empty-1)}$$

$$\mathtt{T} \vdash \mathtt{Empty} \#^{\Rightarrow} \mathtt{r} \qquad \text{(A-Cmp-Empty-2)}$$

$$\frac{\mathtt{T} \vdash \mathtt{s}_1 \#^{\Rightarrow} \mathtt{r} \qquad \mathtt{T} \vdash \mathtt{s}_2 \#^{\Rightarrow} \mathtt{r}}{\mathtt{T} \vdash (\mathtt{s}_1 \,||\, \mathtt{s}_2) \#^{\Rightarrow} \mathtt{r}} \qquad \text{(A-Cmp-Merge-I-1)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{s}_1 \qquad \mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{s}_2}{\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} (\mathtt{s}_1 \,||\, \mathtt{s}_2)} \qquad \text{(A-Cmp-Merge-I-2)}$$

$$\frac{\mathtt{l} \neq \mathtt{l}'}{\mathtt{T} \vdash \mathtt{l}{:}\mathtt{t} \#^{\Rightarrow} \mathtt{l}'{:}\mathtt{t}'} \qquad \text{(A-Cmp-Base/Base)}$$

$$\frac{\mathtt{a} \in \mathtt{S}^*}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2, \mathtt{b}\#\mathtt{S}, \mathtt{T}_3 \vdash \mathtt{a} \#^{\Rightarrow} \mathtt{b}} \qquad \text{(A-Cmp-Tvar/Tvar-1)}$$

$$\frac{\mathtt{a} \in \mathtt{S}^*}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2, \mathtt{b}\#\mathtt{S}, \mathtt{T}_3 \vdash \mathtt{b} \#^{\Rightarrow} \mathtt{a}} \qquad \text{(A-Cmp-Tvar/Tvar-2)}$$

$$\frac{\mathtt{l} \in \mathtt{R}^*}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{a} \#^{\Rightarrow} \mathtt{l}{:}\mathtt{t}} \qquad \text{(A-Cmp-Base/Tvar-1)}$$

$$\frac{\mathtt{l} \in \mathtt{R}^*}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{l}{:}\mathtt{t} \#^{\Rightarrow} \mathtt{a}} \qquad \text{(A-Cmp-Base/Tvar-2)}$$

Figure 6: Algorithmic compatibility rules

2.3.4 Compatibility Checking

The compatibility checking algorithm is presented as a collection of inference rules for deriving judgements of the form $\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{s}$ where $\mathtt{r}$ and $\mathtt{s}$ are restriction-free, well-formed record types. The rules appear in Figure 6. To prove that these rules define an algorithm for compatibility checking, we show that they are sound and complete with respect to the declarative formulation, and that we may effectively decide whether or not a derivation exists in accordance with these rules.

The soundness of the algorithm is stated by the following theorem:

Theorem 2.3.4.1:

1. If $\mathtt{T} \vdash \mathtt{r}$ record and $\mathtt{T} \vdash \mathtt{r}'$ record and $\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{r}'$, then $\mathtt{T} \vdash \mathtt{r} \# \mathtt{r}'$.
2. If $\mathtt{T} \vdash \mathtt{r}$ record and $\mathtt{T} \vdash \mathtt{R}$ ok and $\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{R}$, then $\mathtt{T} \vdash \mathtt{r} \# \mathtt{R}$.

The proof relies on the following facts:

Lemma 2.3.4.2: If $\mathtt{T} \vdash \mathtt{R}$ ok and $\mathtt{R} \twoheadrightarrow^1 \mathtt{R}'$ and $\mathtt{T} \vdash \mathtt{r} \# \mathtt{R}'$, then $\mathtt{T} \vdash \mathtt{r} \# \mathtt{R}$.

Lemma 2.3.4.3: If $\vdash \mathtt{T}$ ok and $\mathtt{T} = \mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2, \mathtt{b}\#\mathtt{S}, \mathtt{T}_3$ and $\mathtt{a} \in \mathtt{S}^*$, then $\mathtt{T} \vdash \mathtt{a} \# \mathtt{b}$.

Lemma 2.3.4.4: If $\vdash \mathtt{T}$ ok and $\mathtt{T} = \mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2$ and $\mathtt{l} \in \mathtt{R}^*$ and $\mathtt{T} \vdash \mathtt{l}{:}\mathtt{t}$ record, then $\mathtt{T} \vdash \mathtt{a} \# \mathtt{l}{:}\mathtt{t}$.

The completeness of the algorithm is stated by the following theorem:

Theorem 2.3.4.5:

1. If $\mathtt{T} \vdash \mathtt{r} \# \mathtt{s}$, then $\mathtt{T} \vdash \mathtt{r}^* \#^{\Rightarrow} \mathtt{s}^*$.
2. If $\mathtt{T} \vdash \mathtt{r} \# \mathtt{R}$, then $\mathtt{T} \vdash \mathtt{r}^* \#^{\Rightarrow} \mathtt{R}^*$.

The proof relies on a number of preliminary results.

Lemma 2.3.4.6: The relation computed by the algorithm is symmetric on normal forms:

1. Suppose that $\mathtt{r}$ and $\mathtt{s}$ are well-formed record types in normal form and that $\mathtt{r} \approx \mathtt{r}'$ and $\mathtt{s} \approx \mathtt{s}'$. Then $\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{s}$ iff $\mathtt{T} \vdash \mathtt{r}' \#^{\Rightarrow} \mathtt{s}'$.

2. Suppose that $\mathtt{r}$ and $\mathtt{s}$ are well-formed record types in normal form. If $\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{s}$, then $\mathtt{T} \vdash \mathtt{s} \#^{\Rightarrow} \mathtt{r}$.

Proof:

1. Since $\mathtt{r}$ and $\mathtt{s}$ are in normal form, $\mathtt{r}'$ and $\mathtt{s}'$ must also be, and $\mathtt{r}'$ and $\mathtt{s}'$ must be a commutative, associative re-grouping of $\mathtt{r}$ and $\mathtt{s}$.

2. A simple induction on derivations. Box

Lemma 2.3.4.7: Suppose that $\mathtt{r}$ and $\mathtt{t}$ are well-formed normal forms. Then $\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{l}{:}\mathtt{t}$ implies $\mathtt{T} \vdash \mathtt{r} \# \mathtt{l}{:}\mathtt{t}'$ for any well-formed type $\mathtt{t}'$.

Proof: Consider the form of $\mathtt{r}$, and note that the property holds for atomic record types. □

Lemma 2.3.4.8: If $\mathtt{T} \vdash \mathtt{s}_1||\mathtt{s}_2$ record and $\mathtt{T} \vdash \mathtt{r}^* \#^{\Rightarrow} \mathtt{s}_1^*$ and $\mathtt{T} \vdash \mathtt{r}^* \#^{\Rightarrow} \mathtt{s}_2^*$, then $\mathtt{T} \vdash \mathtt{r}^* \#^{\Rightarrow} (\mathtt{s}_1||\mathtt{s}_2)^*$.

Proof: By a straightforward induction on a reduction sequence from $\mathtt{s}_1||\mathtt{s}_2$ to $(\mathtt{s1}||\mathtt{s2})^*$. □

Definition 2.3.4.9: Let atoms($\mathtt{r}^*$) be

1. the empty set if $\mathtt{r}^*$ is $\mathtt{Empty}$,

2. otherwise, the result of replacing each atom of the form $\mathtt{l}{:}\mathtt{t}$ by the bare label $\mathtt{l}$ in the set of atoms of the normal form of $\mathtt{r}$.

Lemma 2.3.4.10: If $\mathtt{T} \vdash \mathtt{R}$ ok and $\mathtt{r} \in \mathtt{R}$, then atoms($\mathtt{r}^*$) $\subseteq \mathtt{R}^*$.

Proof: If $\mathtt{r}^*$ is $\mathtt{Empty}$, the result is immediate. So assume $\mathtt{r}^*$ is not $\mathtt{Empty}$. Since the relation $\twoheadrightarrow$ is confluent modulo $\approx$, we may focus on any reduction path from $\mathtt{R}$ to a $\twoheadrightarrow$-normal form $\mathtt{R}^{*\prime}$ such that $\mathtt{R}^{*\prime} \approx \mathtt{R}^*$. Begin by reducing $\mathtt{r}$ to $\mathtt{r}^*$ in $\mathtt{R}$, giving $\mathtt{R}'$. Then flatten $\mathtt{r}^*$ in $\mathtt{R}'$ to its constituent atoms, giving $\mathtt{R}''$, and perform all the base reductions $\mathtt{l}{:}\mathtt{t} \twoheadrightarrow \mathtt{l}$ in the residuals of $\mathtt{r}$ in $\mathtt{R}''$, giving $\mathtt{R}^{*\prime}$. Observe that atoms($\mathtt{r}^*$) $\subseteq \mathtt{R}^{*\prime}$. Finally, rewrite $\mathtt{R}^{*\prime}$ to $\mathtt{R}^*$ using the axioms for $\approx$, noting that no bare label or type variable is dropped from $\mathtt{R}^{*\prime}$ (considered as a set) during any of these reductions. □

Lemma 2.3.4.11: Let $\mathtt{T} = \mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2$, and suppose that $\vdash \mathtt{T}$ ok and $\mathtt{r} \in \mathtt{R}$ (so that $\mathtt{T} \vdash \mathtt{a} \# \mathtt{r}$.) Then $\mathtt{T} \vdash \mathtt{a} \#^{\Rightarrow} \mathtt{r}^*$.

Proof: By induction on the form of $\mathtt{r}^*$, using Lemma 2.3.4.10. □

It remains to show that the relation axiomatized by the rules of Figure 6 is decidable. This follows from two observations. First, the rules are "almost syntax-directed" in the sense that there is a pair of rules for each form of restriction-free record type, one the symmetric version of the other. Second, in the cases where two rules apply to a given pair of types, it is immaterial which rule is applied. To see this we have to consider four combinations. If both $\mathtt{r}$ and $\mathtt{s}$ are $\mathtt{Empty}$, either rule yields the same result (success). If one of $\mathtt{r}$ and $\mathtt{s}$ is $\mathtt{Empty}$ and the other is a merge, then no matter how we proceed the result is the same (success). In the case that both $\mathtt{r}$ and $\mathtt{s}$ are merges, we have no choice but to apply A-Cmp-Merge-I-1 and A-Cmp-Merge-I-2 to break down both merges into their components; the order in which we do this has no effect on the result. We may therefore check compatibility by decomposing merges in an arbitrary order until we reach atoms, then apply the appropriate rules. If any derivation exists, this procedure will construct it, and we can effectively decide whether any rule applies.

$$\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{a} \Rightarrow \text{record} \qquad \text{(A-WFR-VAR)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r}_1 \Rightarrow \text{record} \quad \mathtt{T} \vdash \mathtt{r}_2 \Rightarrow \text{record} \quad \mathtt{T} \vdash \mathtt{r}_1 \#^{\Rightarrow} \mathtt{r}_2}{\mathtt{T} \vdash \mathtt{r}_1 \,||\, \mathtt{r}_2 \Rightarrow \text{record}} \qquad \text{(A-WFR-MERGE)}$$

$$\frac{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}_1 \Rightarrow \mathtt{r}_1 \quad \mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}_2 \Rightarrow \mathtt{r}_2 \quad \mathtt{T} \vdash \mathtt{r}_1^* \#^{\Rightarrow} \mathtt{r}_2^*}{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}_1 \,||\, \mathtt{e}_2 \Rightarrow \mathtt{r}_1 \,||\, \mathtt{r}_2} \qquad \text{(A-WTT-MERGE)}$$

$$\frac{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e} \Rightarrow \forall \mathtt{a}\#\mathtt{R}.\,\mathtt{t} \quad \mathtt{T} \vdash \mathtt{r} \Rightarrow \text{record} \quad \mathtt{T} \vdash \mathtt{r}^* \#^{\Rightarrow} \mathtt{R}^*}{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}[\mathtt{r}] \Rightarrow [\mathtt{r}/\mathtt{a}]\mathtt{t}} \qquad \text{(A-WTT-ALL-E)}$$

Figure 7: Selected type synthesis rules

2.3.5 Type Synthesis

The type checking algorithm for $\lambda^{||}$ is given in terms of a type synthesis procedure that constructs a "canonical" type for a given expression in a given context. This procedure is described by a formal system for deriving judgements of the form $\mathtt{T}\,;\,\mathtt{G} \vdash \mathtt{e} \Rightarrow \mathtt{t}$, together with a number of auxiliary judgements of a similar form. As with the compatibility checker, we show that this formal system defines a type checking algorithm by proving that it is sound and complete with respect to the definition of $\lambda^{||}$ and that we may effectively decide whether or not a derivation exists. A representative set of rules from the definition of the type synthesis algorithm is given in Figure 7. The complete set of rules appears in Appendix B.

The judgements derived by the algorithm are:

$$\mathtt{T} \vdash \mathtt{R} \Rightarrow \text{ok} \qquad \mathtt{T} \vdash \mathtt{t} \Rightarrow \text{type} \qquad \mathtt{T} \vdash \mathtt{r} \Rightarrow \text{record} \qquad \mathtt{T}\,;\mathtt{G} \vdash \mathtt{e} \Rightarrow \mathtt{t}.$$

Note that in rules A-WTT-MERGE and A-WTT-ALL-E, the record types and constraint lists are normalized before checking compatibility.

The soundness and completness of the algorithm are stated by the following theorems:

Theorem 2.3.5.1: (Soundness)

1. If $\vdash \mathtt{T}$ ok and $\mathtt{T} \vdash \mathtt{r} \Rightarrow$ record, then $\mathtt{T} \vdash \mathtt{r}$ record.
2. If $\vdash \mathtt{T}$ ok and $\mathtt{T} \vdash \mathtt{t} \Rightarrow$ type, then $\mathtt{T} \vdash \mathtt{t}$ type.
3. If $\vdash \mathtt{T}$ ok and $\mathtt{T} \vdash \mathtt{R} \Rightarrow$ ok, then $\mathtt{T} \vdash \mathtt{R}$ ok.
4. If $\mathtt{T} \vdash \mathtt{G}$ ok and $\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e} \Rightarrow \mathtt{t}$, then $\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e} \in \mathtt{t}$.

Theorem 2.3.5.2: (Completeness)

1. If $\mathtt{T} \vdash \mathtt{r}$ record, then $\mathtt{T} \vdash \mathtt{r} \Rightarrow$ record.
2. If $\mathtt{T} \vdash \mathtt{t}$ type, then $\mathtt{T} \vdash \mathtt{t} \Rightarrow$ type.
3. If $\mathtt{T} \vdash \mathtt{R}$ ok, then $\mathtt{T} \vdash \mathtt{R} \Rightarrow$ ok.
4. If $\mathtt{T} \vdash \mathtt{e} \in \mathtt{t}$, then $\mathtt{T} \vdash \mathtt{e} \Rightarrow \mathtt{t}'$ for some $\mathtt{t}'$ such that $\mathtt{t}' \sim \mathtt{t}$.

Both may be proved by induction on derivations.

For decidability, we have only to note that the relevant instances of compatibility and conversion checking are decidable, and that the rules are syntax-directed.

3 Examples

In this section we develop some examples illustrating the expressiveness of $\lambda^{||}$. Section 3.1 presents some short examples and compares them to their formulations in related record calculi. Section 3.2 shows how Wand's model of a simple object-oriented programming language with method inheritance and a notion of `self` may be emulated in $\lambda^{||}$. Section 3.3 shows that in the presence of recursive types, quantifiers carrying negative constraints are sufficient to satisfactorily express the examples motivating the extension of bounded quantification to F-bounded quantification. Section 3.4 shows how some other primitive record operations may be added to the language.

3.1 Simple Record Manipulation

A function that accepts any record not already possessing an `l` field and adds the field `l`=5 can be written in $\lambda^{||}$ as:

Λa#l.
  λx:a.
    x || l=5
$\in \forall$a#l. a $\rightarrow$ (a || l:Int)

A similar function that accepts any record *with* an `l` field and overrides it with the field `l`=5 can also be expressed:

Λb. Λa#l.
  λx:(a||l:b).
    (x\l) || l=5
$\in \forall$b. $\forall$a#l. (a||l:b) $\rightarrow$ (a || l:Int)

(Strictly speaking, this function can only accept a record whose `l` field has some *record* type, because for simplicity we have omitted ordinary type quantification. The empty constraint list on the first quantifier is dropped, by convention, to reduce clutter, but it should not be confused with the usual unconstrained quantifier.)

Unlike the calculi of Rémy, Wand, and Cardelli and Mitchell, $\lambda^{||}$ is unable to express the function that takes any record whatsoever and gives it an `l` field with value 5.

Functions that perform "deep updates" of fields within fields of records, preserving all the type information about the unmodified fields, can be expressed in $\lambda^{||}$. For example:

Λa#l_a.
  Λb#l_b.
    λx:(b || l_b:(a||l_a:Bool)).
      (x\$l_b$) || l_b = (($x.l_b$)\$l_a$ || l_a = (not $x.l_b.l_a$))

Cardelli and Mitchell's formulation of this function, which relies on *extraction types* like `a.l`, is somewhat shorter.

3.2 Object-Oriented Programming

Wand [25, 26, 27, 28] has shown how a simple form of object-oriented programming may be modeled in an extension of ML [14, 16] with record concatenation and recursive types. An analogous construction can be made in an extension of $\lambda^{||}$ with polymorphism (quantification over arbitrary types), fixed point operators at the term level, base types such as `int` and `bool`, and recursive types. Recursive types are denoted μ a. t(a), where t(a) is an arbitrary type expression, possibly involving the variable a. Let $\lambda^{||\mu}$ stand for the extension of $\lambda^{||}$ with recursive types. Type equivalence for $\lambda^{||\mu}$ is defined by considering recursive types to denote

the infinite, regular tree obtained by unrolling all occurrences of $\mu\,\mathtt{a}.\ \mathtt{t}(\mathtt{a})$, and applying the equivalences on type expressions given in Appendix A. Although this description of type equivalence is sufficient for the examples to follow, it should be emphasized that we have not studied the decidability of type equivalence, and hence the decidability of type checking for $\lambda^{||\mu}$ remains open.

Following Wand, we consider first a very simple notion of class that does not include a notion of `self` or provide for inheritance. In this setting classes are functions from a parameter type, representing instance-specific values, to some record type, representing the methods. Specifically,

$\mathtt{class\ x{:}t\ methods\ l}_1\mathtt{=e}_1, \ldots, \mathtt{l}_n\mathtt{=e}_n$

stands for the expression

$\lambda\mathtt{x{:}t}.\ (\mathtt{l}_1\mathtt{=e}_1 \,||\, \ldots \,||\, \mathtt{l}_n = \mathtt{e}_n)$

which has type

$\mathtt{t} \to (\mathtt{l}_1\mathtt{:t}_1 \,||\, \ldots \,||\, \mathtt{l}_n\mathtt{:t}_n)$

provided that $\mathtt{t}$ is a type, $\mathtt{x{:}t} \vdash \mathtt{e}_i \in \mathtt{t}_i$, and all the $\mathtt{l}_i$'s are distinct. Let $\mathtt{C}$ be such a class. If $\mathtt{e}$ is a term of type $\mathtt{t}$, then $\mathtt{C(e)}$ is a record of type $\mathtt{l}_1\mathtt{:t}_1 \,||\, \ldots \,||\, \mathtt{l}_n\mathtt{:t}_n$, so that $\mathtt{C(e).l}_i$ selects the method associated with the instance of $\mathtt{C}$ determined by $\mathtt{e}$. Following Wand we write

`new C e`

for the application $\mathtt{C(e)}$.

Wand's list-processing example may be readily translated into this setting as follows. First, we introduce some abbreviations:

$$\begin{array}{lcl}
\mathtt{cellPlus[r,s,t]} & = & \mathtt{r} \,||\, \mathtt{null{:}Bool} \,||\, \mathtt{car{:}s} \,||\, \mathtt{cdr{:}t} \\
\mathtt{cell[s,t]} & = & \mathtt{cellPlus[Empty,s,t]} \\
\mathtt{listPlus[r,s]} & = & \mu\,\mathtt{a}.\ \mathtt{cellPlus[r,s,a]} \\
\mathtt{list[s]} & = & \mathtt{listPlus[Empty,s]}.
\end{array}$$

Note that

$$\begin{array}{lcl}
\mathtt{listPlus[r,s]} & \sim & \mathtt{cellPlus[r,s,listPlus[s]]} \\
& \sim & \mathtt{r} \,||\, \mathtt{null{:}Bool} \,||\, \mathtt{car{:}s} \,||\, \mathtt{cdr{:}listPlus[r,s]}
\end{array}$$

and that

$$\begin{array}{lcl}
\mathtt{list[s]} & \sim & \mathtt{cell[s,list[s]]} \\
& \sim & \mathtt{null{:}Bool} \,||\, \mathtt{car{:}s} \,||\, \mathtt{cdr{:}list[s]}.
\end{array}$$

These equations will be important for type checking the examples below.

Define

$$\begin{array}{lcl}
\mathtt{nil} & = & \Lambda\mathtt{s,t}.\ \lambda\mathtt{x}{:}1.\ (\mathtt{null{=}true} \,||\, \mathtt{car{=}error[s]} \,||\, \mathtt{cdr\ {=}error[t]}) \\
& \in & \forall\mathtt{s,t}.\ 1 \to \mathtt{cell[s,t]}.
\end{array}$$

Note that `nil` is parameterized by the types of the cells. We assume a special constant $\mathtt{error} \in \forall\mathtt{t}.\ \mathtt{t}$ assigning an "error element" to each type. (In a richer calculus one may wish to arrange that selecting the `car` or the `cdr` field raise an exception.)

Define

$$\begin{array}{lcl}
\mathtt{cons} & = & \Lambda\mathtt{s,t}.\ \lambda(\mathtt{h,t}){:}\mathtt{s}\times\mathtt{t}.\ (\mathtt{null{=}false} \,||\, \mathtt{car{=}h} \,||\, \mathtt{cdr{=}t}) \\
& \in & \forall\mathtt{s,t}.\ (\mathtt{s}\times\mathtt{t}) \to \mathtt{cell[s,t]}.
\end{array}$$

Now consider

$$\begin{array}{l}
\mathtt{map} \ = \ \Lambda\mathtt{s,t}.\ \Lambda\mathtt{r}\#\mathtt{null,car,cdr}.\ \lambda\mathtt{f{:}s}\to\mathtt{t}. \\
\qquad\qquad \mathtt{fix_u}\ \lambda\mathtt{map'{:}u}.\ \lambda\mathtt{l{:}listPlus[r,s]}. \\
\qquad\qquad\quad \mathtt{if\ l.null} \\
\qquad\qquad\qquad \mathtt{then\ new\ nil[t,list[t]]()} \\
\qquad\qquad\qquad \mathtt{else\ new\ cons[t][list[t]](f\ l.car)(map'\ l.cdr)}
\end{array}$$

where $\mathtt{u} \ = \ \mathtt{listPlus[r,s]}\to\mathtt{list[t]}$.

It is easy to see that map has type

$\forall\mathtt{s,t}.\ \forall\mathtt{r}\#\mathtt{null,car,cdr}.\ (\mathtt{s}\to\mathtt{t}) \to \mathtt{listPlus[r,s]} \to \mathtt{list[s]}$

under some obvious assumptions about typing conditionals and taking account of the equations between recursive types noted above.

Extending the example to a simple, self-less form of multiple inheritance presents no particular difficulties:

$\texttt{class x:t inherits } \mathtt{f}_1, \ldots, \mathtt{f}_k \texttt{ methods } \mathtt{l}_1 = \mathtt{e}_1, \ldots, \mathtt{l}_n = \mathtt{e}_n \texttt{ end}$

stands for

$\lambda \mathtt{x}{:}\mathtt{t}.\ (\mathtt{f}_1 \mid\mid \ldots \mid\mid \mathtt{f}_k \mid\mid \mathtt{l}_1 = \mathtt{e}_1 \mid\mid \ldots \mid\mid \mathtt{l}_n = \mathtt{e}_n)$

which has type

$\mathtt{t} \rightarrow (\mathtt{F}_1 \mid\mid \ldots \mid\mid \mathtt{F}_k \mid\mid \mathtt{l}_1{:}\mathtt{t}_1 \mid\mid \ldots \mid\mid \mathtt{l}_n{:}\mathtt{t}_n)$

provided that $\mathtt{t}$ is well formed, $\mathtt{x}{:}\mathtt{t} \vdash \mathtt{f}_j \in \mathtt{F}_j$, $\mathtt{x}{:}\mathtt{t} \vdash \mathtt{e}_i \in \mathtt{t}_i$, and the following compatibility conditions are satisfied:

1. all $\mathtt{l}_i$'s are distinct,
2. $\mathtt{F}_i \# \mathtt{F}_j$ whenever $i \neq j$,
3. $\mathtt{F}_i \# \mathtt{l}_j$ for each $\mathtt{F}_i$ and each label $\mathtt{l}_j$.

These conditions are not enforced in Wand's system since he prefers the asymmetric form of merge in which the rightmost occurrence of a field in a record type determines the value assigned to that field. We prefer instead that the type checker ensure that no clashes are possible, and insist that the programmer explicitly use the restriction operation to eliminate the field that he or she wishes to override.

The extension to model "`self`" presents some interesting problems for typing. We begin by considering a form of `self` that does not behave correctly in the presence of inheritance and then consider how to combine `self` and inheritance. The simple-minded approach to `self` proceeds by defining

$\texttt{class x:s methods } \mathtt{l}_1 = \mathtt{e}_1, \ldots, \mathtt{l}_n = \mathtt{e}_n \texttt{ end}$

to be

$\lambda \mathtt{x}{:}\mathtt{s}.\ \lambda \mathtt{self}{:}\mathtt{t}.\ (\mathtt{l}_1 = \mathtt{e}_1 \mid\mid \ldots \mid\mid \mathtt{l}_n = \mathtt{e}_n)$

which has type $\mathtt{s} \rightarrow \mathtt{t} \rightarrow \mathtt{t}$, where $\mathtt{t} = (\mathtt{l}_1{:}\mathtt{t}_1 \mid\mid \ldots \mid\mid \mathtt{l}_n{:}\mathtt{t}_n)$, provided that $\mathtt{t}$ is a type and $\mathtt{x}{:}\mathtt{t}, \mathtt{self}{:}\mathtt{t} \vdash \mathtt{e}_i : \mathtt{t}_i$.

Class instantiation is performed by taking a fixed point, as described in Wand's paper. If `C` is a class of the form just described, then

$\texttt{new C e}$

is defined to be

$\mathtt{fix}_{\mathtt{t}}\ (\mathtt{C}(\mathtt{e}))$,

where `C` has type $\mathtt{s} \rightarrow \mathtt{t} \rightarrow \mathtt{t}$ and `e` has type `s`.

This simple-minded approach interacts badly with inheritance in two ways. First, the type assigned to `self` is required to coincide with the type of the body of the class definition. This forces us to define at class definition time all methods that are used by any method of the class. This precludes the possibility of "mixing in" the missing methods at a later stage, a significant feature of object-oriented programming. Second, the type assigned to `self` does not take account of the fact that the class may occur as the superclass of some subclass which may define not only the "missing" methods, but also some additional methods not relevant to the definition of the superclass. In short, `self` should refer to the entire subclass, and not just the superclass or even just the subclass of the superclass required to achieve "closure."

This means that a class definition must have a "floating" notion of `self` that can be instantiated at any subclass consistent with the requirements imposed on `self` and with the methods that are given for `self` as part of the class definition. Following Wand, we take

$\texttt{class x:t inherits } \mathtt{f}_1, \ldots, \mathtt{f}_k \texttt{ methods } \mathtt{l}_1 = \mathtt{e}_1, \ldots, \mathtt{l}_n = \mathtt{e}_n \texttt{ end}$

to stand for (roughly)

$\lambda \mathtt{x}{:}\mathtt{t}.\ \mathtt{fix}_{\mathtt{v}}\ (\lambda \mathtt{s}{:}\mathtt{v}.\ (\mathtt{f}_1(\mathtt{s}) \mid\mid \ldots \mid\mid \mathtt{f}_2(\mathtt{s}) \mid\mid \mathtt{l}_1 = \mathtt{e}_1 \mid\mid \ldots \mid\mid \mathtt{l}_n = \mathtt{e}_n))$

where $\mathtt{v}$ is a suitable type expression. This ensures that the $\mathtt{f}_i$'s and the new class share a common sense of `self`.

Since our system is explicitly-typed, we must take explicit account of the variability of the type of `self` by introducing suitable constrained type abstractions. The main idea is to abstract with respect to a record type variable `a` representing an arbitrary "extension" to the type of record comprising the object, and to assign to `self` a type of the form $\mathtt{a} \,||\, \mathtt{l}_1{:}\mathtt{t}_1 \,||\, \ldots \,||\, \mathtt{l}_n{:}\mathtt{t}_n$, where the $\mathtt{l}_i{:}\mathtt{t}_i$'s include both the types of the methods actually defined by the class and the types of the methods assumed by the new methods. By choosing the type `a` appropriately we may instantiate `self` to be any superclass of the class, as required for inheritance.

A class definition of the form

$$\mathtt{class\ x{:}t\ methods\ l}_1{=}\mathtt{e}_1, \ldots, \mathtt{l}_n{=}\mathtt{e}_n\ \mathtt{end}$$

is represented by a λ-term of the form

$$\begin{array}{l}\lambda\mathtt{x}{:}\mathtt{t}.\\ \quad \Lambda\mathtt{a}\#\mathtt{l}_1, \ldots, \mathtt{l}_n.\\ \quad\quad \lambda\mathtt{s}{:}(\mathtt{a} \,||\, \mathtt{l}_1{:}\mathtt{t}_1 \,||\, \ldots \,||\, \mathtt{l}_n{:}\mathtt{t}_n).\\ \quad\quad\quad (\mathtt{l}_{i_1}{=}\mathtt{e}_{i_1} \,||\, \ldots \,||\, \mathtt{l}_{i_\mathtt{r}}{=}\mathtt{e}_{i_\mathtt{r}}),\end{array}$$

where $\{i_1, \ldots, i_\mathtt{r}\} \subseteq 1 \ldots n$. This expression has type

$$\begin{array}{l}\mathtt{t} \rightarrow \forall\mathtt{a}\#\mathtt{l}_1, \ldots, \mathtt{l}_n.\\ \quad (\mathtt{a} \,||\, \mathtt{l}_1{:}\mathtt{t}_1 \,||\, \ldots \,||\, \mathtt{l}_n{:}\mathtt{t}_n)\\ \quad\quad \rightarrow (\mathtt{l}_{i_1}{:}\mathtt{t}_{i_1} \,||\, \ldots \,||\, \mathtt{l}_{i_\mathtt{r}}{:}\mathtt{t}_{i_\mathtt{r}})\end{array}$$

provided that `t` type and $\mathtt{x}{:}\mathtt{t}$, $\mathtt{a}\#\mathtt{l}_1, \ldots, \mathtt{l}_n$ and $\mathtt{s}{:}\mathtt{a}||\mathtt{l}_1 : \mathtt{t}_1|| \ldots ||\mathtt{l}_n : \mathtt{t}_n \vdash\ \mathtt{e}_j \in \mathtt{t}_j$.

To build a subclass of such a class `C`, we proceed as follows. Let us suppose that we intend to build a class `D`, and instantiate it at some value `v`. Therefore we must at least define the methods assumed in the definition of `C`, and perhaps some additional methods particular to `D`. Thus we will want to use a definition of the form

$$\mathtt{class\ x{:}t\ inherits\ new\ C\ e\ methods\ l}_{j_1}{=}\mathtt{e}_{j_1} \,||\, \ldots \,||\, \mathtt{l}_{j_q}{=}\mathtt{e}_{j_q} \,||\, k_1{=}\mathtt{d}_1 \,||\, \ldots \,||\, k_p{=}\mathtt{d}_p\ \mathtt{end}$$

where $\mathtt{l}_{i_1}, \ldots, \mathtt{l}_{i_\mathtt{r}}, \mathtt{l}_{j_1}, \ldots, \mathtt{l}_{j_q} = \mathtt{l}_1 \ldots \mathtt{l}_n$ (so that the $\mathtt{l}_j$'s supply the missing methods and the k_i's are new methods associated with `D`). This corresponds to the following lambda term:

$$\begin{array}{l}\lambda\mathtt{x}{:}\mathtt{t}.\ \Lambda\mathtt{a}\#\mathtt{l}_1, \ldots, \mathtt{l}_n, k_1, \ldots, k_p.\\ \quad \lambda\mathtt{self}{:}(\mathtt{a}||\mathtt{l}_1{:}\mathtt{t}_1|| \ldots ||\mathtt{l}_n{:}\mathtt{t}_n||k_1{:}\mathtt{s}_1|| \ldots ||k_p{:}\mathtt{s}_p).\\ \quad\quad \mathtt{C(e)}[\mathtt{a}||k_1{:}\mathtt{s}_1|| \ldots ||k_p{:}\mathtt{s}_p](\mathtt{self})\\ \quad\quad\quad || \mathtt{l}_{j_1}{=}\mathtt{e}_{j_1} \,||\, \ldots \,||\, \mathtt{l}_{j_q}{=}\mathtt{e}_{j_q} \,||\, k_1{=}\mathtt{d}_1 \,||\, \ldots \,||\, k_p{=}\mathtt{d}_p\end{array}$$

which has type

$$\begin{array}{l}\mathtt{t} \rightarrow \forall\mathtt{a}\#\mathtt{l}_1, \ldots, \mathtt{l}_n, k_1, \ldots, k_p.\\ \quad\quad\quad (\mathtt{a}||\mathtt{l}_1{:}\mathtt{t}_1|| \ldots ||\mathtt{l}_n{:}\mathtt{t}_n||k_1{:}\mathtt{s}_1|| \ldots ||k_p{:}\mathtt{s}_p)\\ \quad\quad\quad \rightarrow (\mathtt{l}_1{:}\mathtt{t}_1|| \ldots ||\mathtt{l}_n{:}\mathtt{t}_n||k_1{:}\mathtt{s}_1|| \ldots ||k_p{:}\mathtt{s}_p)\end{array}$$

so that $\lambda\mathtt{x}{:}\mathtt{t}.\ \mathtt{fix(D(x)[Empty])} \ \in\ \mathtt{t} \rightarrow \mathtt{l}_1{:}\mathtt{t}_1 \,||\, \ldots \,||\, k_p{:}\mathtt{s}_p$ (assuming that the $\mathtt{l}_j$'s supplied the missing methods).

Here is a concrete example using `self`, taken from Wand.

Define the "class" `A` to be

$$\begin{array}{l}\lambda\mathtt{x}{:}\mathtt{int}.\\ \quad \Lambda\mathtt{a}\#\mathtt{sum},\mathtt{n}.\\ \quad\quad \lambda\mathtt{self}{:}(\mathtt{a}||\mathtt{sum}{:}\mathtt{int}||\mathtt{n}{:}\mathtt{int}).\\ \quad\quad\quad \mathtt{sum}{=}(\mathtt{x} + \mathtt{self.n})\end{array}$$

with type

$$\begin{array}{l}\mathtt{int} \rightarrow \forall\mathtt{a}\#\mathtt{sum},\mathtt{n}.\\ \quad\quad\quad (\mathtt{a}||\mathtt{sum}{:}\mathtt{int}||\mathtt{n}{:}\mathtt{int}) \rightarrow\ (\mathtt{sum}{:}\mathtt{int}).\end{array}$$

Here `x` is a parameter of the "class instantiation" operation: when `A` is instantiated, the value supplied for `x` becomes a hidden component of the new object. The row variable `a` is a placeholder for any fields that

may be added by subclasses of A. The parameter self provides a name within the new instance of A for the instance itself, which is supplied at instantiation time using the fixed point operator.

As it stands, the class A cannot actually be instantiated since it lacks a method for n. Define the class B to be a subclass of A with a method for n:

λy:int.
  Λa#sum,n.
    λself:(a||sum:int||n:int).
      A(5)[a](self) || n=y

with type

int $\rightarrow \forall$a#sum,n.
        (a||sum:int||n:int) $\rightarrow$ (sum:int||n:int).

We may now instantiate B by writing, for example, B(3)[Empty] $\in$ sum:int||n:int $\rightarrow$ sum:int||n:int, so that (fix(B(3)[Empty])).sum $= 8$.

We may also define a class C that extends A with a method for n and a method for m:

λy:int.
  Λa#sum,n,m.
    λself:(a||sum:int||n:int||m:int).
      A(5)[a||m:int](self) || n=y || m=10.

The instantiation expression fix(C(3)[Empty]) results in an object with sum and n fields agreeing with B and with an additional m field whose value is 10.

It is worth noting that the translations of the object-oriented programming idioms into our calculus are to be understood only informally since the target expression involves information not apparent in the source expression. Moreover, it seems reasonable to impose additional typing constraints on classes beyond those that would arise out of their representation in $\lambda^{||\mu}$. For example, it seems sensible to insist that the type ascribed to self be consistent with the type of the body of the class. This suggests that in a more complete development of these ideas, special syntax for class operations would be needed.

One major difference between this model of object-oriented programming and Wand's is that Wand's record concatenation operator is asymmetric while that of $\lambda^{||\mu}$ is symmetric. This difference represents an important methodological committment in the models of object oriented programming that arise from the two type systems.

Any language with multiple inheritance must address the issue of what happens when a class definition inherits the same method from two or more superclasses. One solution, adopted in many existing languages, is to choose one of the superclasses — say, the one mentioned furthest to the right in the subclass' definition — as the "principal superclass," resolving all conflicts in favor of this one. Wand's model implements this kind of conflict resolution scheme.

Another possibility, preferred by some designers of strongly typed object-oriented languages, is simply to disallow class definitions where the same method is inherited ambiguously from more than one superclass. When describing a class whose superclasses have overlapping sets of method names, the programmer must explicitly specify which superclass each ambigous method comes from. Our model can be used to implement this kind of conflict resolution strategy: the typing rules for the merge operator ensure that each method comes from exactly one superclass; the restriction operator is used to hide all but one of the inherited instances of a method.

3.3 F-Bounded Quantification

Members of the ABEL group have argued persuasively that "bounded quantification does not provide the same degree of flexibility in the presence of recursive types as it does for non-recursive types" [1, 7]. They consider two classes of situations in which problems arise, one when the recursion variable occurs negatively, the other when it occurs positively. To deal with these problems, they propose an extended notion, called F-bounded quantification, where the pure bounded quantifier of the form $\forall$a $\leq$ r. t is generalized to the

form $\forall \mathtt{a} \leq \mathtt{F}(\mathtt{a}).\ \mathtt{t}$, where $\mathtt{F}$ is a function from types to types. In this section we show that the motivating examples of F-bounded quantification may be encoded directly in $\lambda^{\cap\mu}$.

In the class of situations where the recursion variable appears in negative positions, Canning et al. show that the pure type system of Cardelli and Wegner [6] does not allow functions to be applied to a variety of values for which they make semantic sense. Consider the type

$$\mathtt{PartialOrder} = \mu \mathtt{po}.\ \{\mathtt{leq} : \mathtt{po} \to \mathtt{Bool}\}$$

and assume we are given a function for computing the minimum of two values of any "subclass" of `PartialOrder`:

$$\mathtt{min} \in \forall \mathtt{a} \leq \mathtt{PartialOrder}.\ \mathtt{a} \to \mathtt{a} \to \mathtt{a}.$$

One of the types that we would like to be able to pass to `min` is

$$\mathtt{Number} = \mu \mathtt{num}.\ \{\mathtt{leq} : \mathtt{num} \to \mathtt{Bool}, \mathtt{other} : \mathtt{t}\}.$$

But by the usual rule for subtyping on recursive types,

$$\frac{\mathtt{G}, \mathtt{a} \leq \mathtt{b} \vdash \mathtt{s} \leq \mathtt{t} \qquad \begin{array}{l}\mathtt{a} \text{ free only in } \mathtt{s} \\ \mathtt{b} \text{ free only in } \mathtt{t}\end{array}}{\mathtt{G} \vdash \mu \mathtt{a}.\ \mathtt{s} \ \leq \ \mu \mathtt{b}.\ \mathtt{t}} \qquad \text{(LEQ-REC)}$$

it is *not* the case that $\mathtt{Number} \leq \mathtt{PartialOrder}$.

F-bounded quantification can be used to redefine `min` so that it can be applied to elements of `Number` as well as `PartialOrder`. Define a type function

$$\mathtt{FPartialOrder}(\mathtt{t}) = \{\mathtt{leq} : \mathtt{t} \to \mathtt{Bool}\}$$

and check that $\mathtt{Number} \leq \mathtt{FPartialOrder}(\mathtt{Number})$. Now write

$$\begin{array}{lll} \mathtt{min} & = & \Lambda \mathtt{a} \leq \mathtt{FPartialOrder}(\mathtt{a}). \\ & & \quad \lambda \mathtt{x}{:}\mathtt{a}.\ \lambda \mathtt{y}{:}\mathtt{a}. \\ & & \quad\ \ \mathtt{if\ x.leq(y)\ then\ x\ else\ y} \\ & \in & \forall \mathtt{a} \leq \mathtt{FPartialOrder}(\mathtt{a}).\ \mathtt{a} \to \mathtt{a} \to \mathtt{a}. \end{array}$$

The same intention — to express `min` so that it can be applied generically to members of any class possessing at least an `leq` operation mapping another member of the same class to a truth value — can be realized directly in $\lambda^{\cap\mu}$. We write:

$$\begin{array}{l} \mathtt{min} \in \forall \mathtt{a}\#\mathtt{leq}.\ \mu \mathtt{b}.\ (\mathtt{a} \,||\, \mathtt{leq}{:}\mathtt{b} \to \mathtt{Bool}) \\ \qquad\qquad \to \mu \mathtt{b}.\ (\mathtt{a} \,||\, \mathtt{leq}{:}\mathtt{b} \to \mathtt{Bool}) \\ \qquad\qquad \to \mu \mathtt{b}.\ (\mathtt{a} \,||\, \mathtt{leq}{:}\mathtt{b} \to \mathtt{Bool}) \\ \mathtt{Number} = \mu \mathtt{num}.\ (\mathtt{leq}{:}\mathtt{num} \to \mathtt{Bool} \,||\, \mathtt{other}{:}\mathtt{t}) \\ \mathtt{five} \in \mathtt{Number}. \end{array}$$

To type the application

$$\mathtt{min\ five\ five}$$

we need to restrict away the `leq` field from `Number`:

$$\mathtt{min}\ [\mathtt{Number} \backslash \mathtt{leq}]\ \mathtt{five\ five}.$$

The type application is well formed because $\mathtt{Number} \backslash \mathtt{leq}$ lacks an `leq` field. To apply this term to `five`, we need to know that

$$\mathtt{Number} \sim \mu \mathtt{b}.\ (\mathtt{Number} \backslash \mathtt{leq}) \,||\, \mathtt{leq}{:}\mathtt{b} \to \mathtt{Bool}.$$

Unrolling the definition of `Number` and applying the rule for elimination of restriction operations, this reduces to showing

$$\begin{array}{l} \mathtt{Number} \sim \mu \mathtt{b}.\ (\mathtt{other}{:}[\mathtt{Number}/\mathtt{num}]\mathtt{t}) \\ \qquad\qquad\qquad\qquad \,||\, \mathtt{leq}{:}\mathtt{b} \to \mathtt{Bool}. \end{array}$$

But these type expressions have the same infinite unrolling and hence are equal under our interpretation of recursive types. This argument may be made precise by considering a definition of type equivalence similar to the definition of bisimulation equivalence in CCS [15]. To establish the above equivalence, it suffices to

show that it is consistent to assume that it holds, where the consistency constraints ensure, for example, that two records are equal only if they have the same fields and corresponding fields are equal.

The other class of situations where bounded quantification appears to be inadequate are those involving positive occurrences of the recursion variable in a recursively defined record type. Here again, pure bounded quantification prevents functions from being applied to a variety of values for which they make sense.

For example, define a recursive record type

$$\texttt{Movable} = \mu\texttt{mv}.\{\texttt{move} : \texttt{Real}\to\texttt{Real}\to\texttt{mv}\}$$

and a function

$$\texttt{translate} = \lambda\texttt{x}{:}\texttt{Movable}.\ \texttt{x.move}\ 1.0\ 1.0.$$

Since `translate` is intended to operate on values possessing any "subsclass" of "class" `Movable`, we want to show that it has type $\forall\texttt{a} \le \texttt{Movable}.\ \texttt{a}\to\texttt{a}$. But it does not; the best that can be said for it is that it has type $\forall\texttt{a} \le \texttt{Movable}.\ \texttt{a}\to\texttt{Movable}$, which is no better than $\texttt{Movable}\to\texttt{Movable}$. So if

$$\texttt{Point} = \mu\,\texttt{pnt}.\ \{\texttt{x}{:}\texttt{void}\to\texttt{Real},\ \texttt{y}{:}\texttt{void}\to\texttt{Real},\ \texttt{move}{:}\texttt{Real}\to\texttt{Real}\to\texttt{pnt}\}$$

and

$$\texttt{mypoint} \in \texttt{Point},$$

then the application

$$\texttt{translate mypoint}$$

will have type `Movable`, not `Point`.

Using F-bounded quantification, a `translate` function that will map elements of `Point` back into `Point` can be written as follows. Define the type function

$$\texttt{FMovable(t)} = \{\texttt{move} : \texttt{Real}\to\texttt{Real}\to\texttt{t}\}.$$

and write

$$\begin{aligned}\texttt{translate} \;=\; & \Lambda\texttt{a} \le \texttt{FMovable(a)}.\\ & \lambda\texttt{x}{:}\texttt{a}.\\ & \quad \texttt{x.move}\ 1.0\ 1.0.\end{aligned}$$

Then since $\texttt{Point} \le \texttt{FMovable(Point)}$, the application `translate [Point] mypoint` is well typed and has result type `Point`.

To express `translate` in $\lambda^{||}$ so that it can be applied to `mypoint`, we write:

$$\begin{aligned}\texttt{translate} \;=\; & \Lambda\texttt{a}\#\texttt{move}.\\ & \lambda\texttt{x}{:}(\mu\,\texttt{b}.\ \texttt{a}||(\texttt{move} : \texttt{Real}\to\texttt{Real}\to\texttt{b})).\\ & \quad \texttt{x.move}\ 1.01.0\\ \in\; & \forall\texttt{a}\#\texttt{move}.\ (\mu\,\texttt{b}.\ \texttt{a}||(\texttt{move} : \texttt{Real}\to\texttt{Real}\to\texttt{b}))\to(\mu\,\texttt{b}.\ \texttt{a}||(\texttt{move} : \texttt{Real}\to\texttt{Real}\to\texttt{b})).\end{aligned}$$

Again, we apply `translate` to `mypoint` by first restricting away the `move` field of its type:

$$\texttt{translate}\ [\texttt{Point}\backslash\texttt{move}]\ \texttt{mypoint}.$$

3.4 Language Extensions

This section shows how some other primitive record operations may be added to $\lambda^{||}$.

The "consistent update" operator $\texttt{e}$ upd $\texttt{l=e}'$ takes a record $\texttt{e}$ with an $\texttt{l}$ and replaces the value of this field with $\texttt{e}'$, which must have exactly the same type as the present contents of the field. This operation cannot be expressed directly in $\lambda^{||}$, but it can be provided easily by adding a new typing rule:

$$\frac{\texttt{T}\,;\texttt{G} \vdash \texttt{e} \in \texttt{r} \qquad \texttt{r_l}\downarrow \qquad \texttt{T}\,;\texttt{G} \vdash \texttt{e}' \in \texttt{t} \qquad \texttt{t} \sim \texttt{r_l}}{\texttt{T}\,;\texttt{G} \vdash \texttt{e upd l=e}' \in \texttt{r}} \qquad \text{(WTT-UPD)}$$

Similarly, field renaming can be provided by adding two new rules:

$$\frac{\texttt{T} \vdash \texttt{r record} \qquad \texttt{r_l}_1\downarrow \qquad \texttt{r_l}_2\uparrow}{\texttt{T}\,;\texttt{G} \vdash \texttt{r}[\texttt{l}_1\to\texttt{l}_2]\ \text{record}} \qquad \text{(WFT-RENAME)}$$

$$\frac{\mathtt{r_l}_1\downarrow \qquad \mathtt{r_l}_2\uparrow}{\mathtt{T\,;\,G} \vdash\ \mathtt{r}[\mathtt{l}_1{\rightarrow}\mathtt{l}_2] \sim (\mathtt{r}\backslash\mathtt{l}_1) \,||\, \mathtt{l}_2{:}\mathtt{r_l}} \qquad \text{(Eq-Rename)}$$

At the level of values, syntactic sugar suffices for the field renaming operation:

$$\mathtt{e}[\mathtt{l}_1{\rightarrow}\mathtt{l}_2] = \mathtt{e}\backslash\mathtt{l}_1 \,||\, \mathtt{l}_1{=}(\mathtt{e}.\mathtt{l}_1).$$

The identity function on all records with *only* an `l` field requires ordinary type quantification:

$$\Lambda\mathtt{a}.\ \Lambda\mathtt{b}\#(\mathtt{l}{:}\mathtt{a}).\ \lambda\mathtt{x}{:}\mathtt{b}.\ \mathtt{x}.\mathtt{l}.$$

4 Future Work

The research described here suggests a number of intriguing paths for future work. Among those that we would like to pursue are:

Record kinds: At one stage in the development of $\lambda^{||}$, we attempted to classify record types into *kinds* according to the record types with which they can safely be merged. Rather than "`r` # `R`," we wrote "`r` : rec#`R`," meaning "`r` has the kind describing records compatible with the types in `R`."

This reorganization has the advantage of allowing record type quantification to be unified cleanly with ordinary type quantification. Also, a form of subsumption — already implicit in $\lambda^{||}$ in the fact that a record type abstraction may be applied to a record type that happens to satisfy *more* constraints than those required by the quantifier — can be made explicit in this reformulation by introducing a "weaker than" ordering on record kinds.

In the end, the formulation used in this paper appeared to have a more more tractable proof theory, so we chose to stick with it for this stage of our investigation. But the elegance of the formulation in terms of kinds remains attractive.

Alternative primitives: The definition of $\lambda^{||}$ is strongly committed to a particular choice of primitives: symmetric merge and "checked" restriction, where a record can only be restricted at a field that it definitely possesses. Substituting a different formulation of either of these operators would require making some changes to the definition of the system, and probably major changes to the algorithms for typechecking. Nevertheless, we believe that the methodology used to develop $\lambda^{||}$ could be effectively applied to similar systems with different — perhaps more useful — sets of primitives.

Type reconstruction: The prenex fragment of $\lambda^{||}$, in which quantifiers are restricted to appear only outermost in type phrases, can be viewed as an explicitly typed version of Wand's calculus with row variables, with the difference that the merge operator is symmetric and the restriction operator is checked. From this analogy, we believe that the problem of finding a well-typed term whose erasure is the same as a given untyped term in this fragment (type reconstruction) may be decidable, though a type reconstruction algorithm would almost certainly have exponential complexity because, like Wand's, it would be inferring not principal types but finite sets of principal types.

Recursive types: In order to fully justify the examples inspired by F-bounded quantification in Section 3.3, the decidability of typechecking for $\lambda^{||\mu}$ needs to be established. Typechecking for polymorphic λ-calculi in the presence of μ-types is beginning to be understood, but the complex equivalence relation already defined on types appears to complicate matters substantially.

Notation for object-oriented programming: From the examples inspired by Wand in Section 3.2, it appears that a type system like this one could be used as the basis of a fairly expressive object-oriented programming language. It would be interesting to try to formalize the informal "class" notation used in these examples and describe a rigorous translation into $\lambda^{||\mu}$.

5 Conclusions

The decision to annotate quantifiers with purely positive information, with purely negative information, or with a mixture of positive and negative information is an important point of variation among calculi of record operations. Ordinary bounded quantification [6], F-bounded quantification [1], and the systems of Ohori and Buneman [18, 19] are positive-information systems. Cardelli and Mitchell's calculus [4, 5] and our earlier "symmetric system" [10] are mixed positive and negative. Wand's system of row variables [28] and $\lambda^{||}$ are pure negative-information systems.

The differences among these classes of systems are particularly clear in the presence of recursive types. In positive-information systems, something like F-bounded quantification seems to be required. In the negative setting we do not need an analogue of F-bounded quantification, since we can explicitly quantify over the "rest" of the fields in a record type. This leads to the observation that, in mixed systems like Cardelli and Mitchell's, the negative-information fragment can be used to directly express the examples motivating F-bounded quantification. Indeed, the construction given in Section 3.3 can be carried out almost verbatim in Cardelli and Mitchell's calculus.

6 Acknowledgements

We are grateful for productive discussions with Val Breazu-Tannen, Peter Buneman, Luca Cardelli, Carl Gunter, Frank Pfenning, Didier Rémy, and John Reynolds.

A Complete Typing Rules

A.1 Judgement Forms

Well-formed type context:	$\mathtt{T}$ ok
Well-formed term context:	$\mathtt{T} \vdash \mathtt{G}$ ok
Well-formed type:	$\mathtt{T} \vdash \mathtt{t}$ type
Well-formed record type:	$\mathtt{T} \vdash \mathtt{r}$ record
Well-formed constraint list:	$\mathtt{T} \vdash \mathtt{R}$ ok
Constraint list satisfaction:	$\mathtt{T} \vdash \mathtt{r} \# \mathtt{R}$
Compatible types:	$\mathtt{T} \vdash \mathtt{r}_1 \# \mathtt{r}_2$
Equivalent types:	$\mathtt{t}_1 \sim \mathtt{t}_2$
Equivalent constraint sets:	$\mathtt{R}_1 \sim \mathtt{R}_2$
Well-formed term:	$\mathtt{T} ; \mathtt{G} \vdash \mathtt{e} \in \mathtt{t}$

A.2 Well-formed type contexts

$$\diamond \text{ ok} \qquad \text{(WFTC-EMPTY)}$$

$$\frac{\mathtt{T} \vdash \mathtt{R} \text{ ok}}{\mathtt{T}, \mathtt{a}\#\mathtt{R} \text{ ok}} \qquad \text{(WFTC-TVAR)}$$

A.3 Well-formed constraint lists

$$\frac{\mathtt{T} \text{ ok}}{\mathtt{T} \vdash \diamond \text{ ok}} \qquad \text{(WFCL-NIL)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \text{ record} \qquad \mathtt{T} \vdash \mathtt{R} \text{ ok}}{\mathtt{T} \vdash \mathtt{r}, \mathtt{R} \text{ ok}} \qquad \text{(WFCL-CONS)}$$

A.4 Well-formed term contexts

$$\frac{\mathtt{T}\ \mathrm{ok}}{\mathtt{T} \vdash \diamond\ \mathrm{ok}} \qquad \text{(WFC-EMPTY)}$$

$$\frac{\mathtt{T} \vdash \mathtt{G}\ \mathrm{ok} \qquad \mathtt{T} \vdash \mathtt{t}\ \mathrm{type}}{\mathtt{T} \vdash \mathtt{G}, \mathtt{x}{:}\mathtt{t}\ \mathrm{ok}} \qquad \text{(WFC-VAR)}$$

A.5 Well-formed types

$$\frac{\mathtt{T}\ \mathrm{ok}}{\mathtt{T} \vdash \mathtt{p}\ \mathrm{type}} \qquad \text{(WFT-PRIM)}$$

$$\frac{\mathtt{T} \vdash \mathtt{t}_1\ \mathrm{type} \qquad \mathtt{T} \vdash \mathtt{t}_2\ \mathrm{type}}{\mathtt{T} \vdash \mathtt{t}_1 \rightarrow \mathtt{t}_2\ \mathrm{type}} \qquad \text{(WFT-ARROW)}$$

$$\frac{\mathtt{T}, \mathtt{a}\#\mathtt{R} \vdash \mathtt{t}\ \mathrm{type}}{\mathtt{T} \vdash \forall \mathtt{a}\#\mathtt{R}.\, \mathtt{t}\ \ \mathrm{type}} \qquad \text{(WFT-ALL)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r}\ \mathrm{record}}{\mathtt{T} \vdash \mathtt{r}\ \mathrm{type}} \qquad \text{(WFT-REC)}$$

A.6 Well-formed record types

$$\frac{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2\ \mathrm{ok}}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{a}\ \mathrm{record}} \qquad \text{(WFR-VAR)}$$

$$\frac{\mathtt{T} \vdash \mathtt{t}\ \mathrm{type}}{\mathtt{T} \vdash \mathtt{l}{:}\mathtt{t}\ \mathrm{record}} \qquad \text{(WFR-BASE)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r}\ \mathrm{record} \qquad \mathtt{r_l}\downarrow}{\mathtt{T} \vdash \mathtt{r} \backslash \mathtt{l}\ \mathrm{record}} \qquad \text{(WFR-RESTR)}$$

$$\frac{\mathtt{T}\ \mathrm{ok}}{\mathtt{T} \vdash \mathtt{Empty}\ \mathrm{record}} \qquad \text{(WFR-EMPTY)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r}_1 \# \mathtt{r}_2}{\mathtt{T} \vdash \mathtt{r}_1 \,||\, \mathtt{r}_2\ \mathrm{record}} \qquad \text{(WFR-MERGE)}$$

A.7 Constraint list satisfaction

$$\frac{\mathtt{T} \vdash \mathtt{r}\ \mathrm{record}}{\mathtt{T} \vdash \mathtt{r} \# \diamond} \qquad \text{(CMP-LIST-NIL)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \# \mathtt{r}_i \qquad \mathtt{T} \vdash \mathtt{r} \# \mathtt{R}}{\mathtt{T} \vdash \mathtt{r} \# \mathtt{r}_i, \mathtt{R}} \qquad \text{(CMP-LIST-CONS)}$$

A.8 Compatibility

$$\frac{\mathtt{T} \vdash \mathtt{r} \# \mathtt{s} \qquad \mathtt{r} \sim \mathtt{r}' \qquad \mathtt{s} \sim \mathtt{s}'}{\mathtt{T} \vdash \mathtt{r}' \# \mathtt{s}'} \quad \text{(Cmp-Eq)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \# \mathtt{s}}{\mathtt{T} \vdash \mathtt{s} \# \mathtt{r}} \quad \text{(Cmp-Symm)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \# \mathtt{l}{:}\mathtt{t} \qquad \mathtt{T} \vdash \mathtt{t}' \text{ type}}{\mathtt{T} \vdash \mathtt{r} \# \mathtt{l}{:}\mathtt{t}'} \quad \text{(Cmp-Base)}$$

$$\frac{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \text{ ok} \qquad \mathtt{r}_i \in \mathtt{R}}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{a} \# \mathtt{r}_i} \quad \text{(Cmp-Tvar)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \# (\mathtt{s}_1 || \mathtt{s}_2)}{\mathtt{T} \vdash \mathtt{r} \# \mathtt{s}_i} \quad \text{(Cmp-Merge-E)}$$

$$\frac{\mathtt{T} \vdash \mathtt{s}_1 \# \mathtt{s}_2 \qquad \mathtt{T} \vdash \mathtt{r} \# \mathtt{s}_1 \qquad \mathtt{T} \vdash \mathtt{r} \# \mathtt{s}_2}{\mathtt{T} \vdash \mathtt{r} \# (\mathtt{s}_1 || \mathtt{s}_2)} \quad \text{(Cmp-Merge-I)}$$

$$\frac{\mathtt{l} \neq \mathtt{l}' \qquad \mathtt{T} \vdash \mathtt{l}{:}\mathtt{t} \text{ record} \qquad \mathtt{T} \vdash \mathtt{l}'{:}\mathtt{t}' \text{ record}}{\mathtt{T} \vdash \mathtt{l}{:}\mathtt{t} \# \mathtt{l}'{:}\mathtt{t}'} \quad \text{(Cmp-Base/Base)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \text{ record}}{\mathtt{T} \vdash \mathtt{r} \# \mathtt{Empty}} \quad \text{(Cmp-Empty)}$$

A.9 Constraint list equivalence

$$\mathtt{R} \sim \mathtt{R} \quad \text{(Ceq-Refl)}$$

$$\frac{\mathtt{R} \sim \mathtt{R}'}{\mathtt{R}' \sim \mathtt{R}} \quad \text{(Ceq-Symm)}$$

$$\frac{\mathtt{R} \sim \mathtt{R}' \qquad \mathtt{R}' \sim \mathtt{R}''}{\mathtt{R} \sim \mathtt{R}''} \quad \text{(Ceq-Trans)}$$

$$\frac{\mathtt{R} \sim \mathtt{R}' \qquad \mathtt{r} \sim \mathtt{r}'}{\mathtt{r}, \mathtt{R} \sim \mathtt{r}', \mathtt{R}'} \quad \text{(Ceq-Inner)}$$

$$\mathtt{r}, (\mathtt{r}', \mathtt{R}) \sim \mathtt{r}', (\mathtt{r}, \mathtt{R}) \quad \text{(Ceq-Swap)}$$

$$\mathtt{Empty}, \mathtt{R} \sim \mathtt{R} \quad \text{(Ceq-Empty)}$$

$$(\mathtt{r}_1 || \mathtt{r}_2), \mathtt{R} \sim \mathtt{r}_1, (\mathtt{r}_2, \mathtt{R}) \quad \text{(Ceq-Merge)}$$

$$\mathtt{r}, (\mathtt{r}, \mathtt{R}) \sim \mathtt{r}, \mathtt{R} \quad \text{(Ceq-Dupl)}$$

$$\mathtt{l}{:}\mathtt{t}, \mathtt{R} \sim \mathtt{l}{:}\mathtt{t}', \mathtt{R} \quad \text{(Ceq-Base)}$$

A.10 Type equivalence

$$\mathtt{r}||\mathtt{Empty} \sim \mathtt{r} \qquad \text{(Eq-Merge-Unit)}$$

$$\mathtt{r}_1 \,||\, (\mathtt{r}_2||\mathtt{r}_3) \sim (\mathtt{r}_1||\mathtt{r}_2) \,||\, \mathtt{r}_3 \qquad \text{(Eq-Merge-Assoc)}$$

$$\mathtt{r}_1 \,||\, \mathtt{r}_2 \sim \mathtt{r}_2 \,||\, \mathtt{r}_1 \qquad \text{(Eq-Merge-Comm)}$$

$$\mathtt{r}\backslash\mathtt{l}\backslash\mathtt{l}' \sim \mathtt{r}\backslash\mathtt{l}'\backslash\mathtt{l} \qquad \text{(Eq-Restr/Restr')}$$

$$(\mathtt{l}{:}\mathtt{t})\backslash\mathtt{l} \sim \mathtt{Empty} \qquad \text{(Eq-Base/Restr)}$$

$$\frac{\mathtt{r}_1 _ \mathtt{l} \downarrow}{(\mathtt{r}_1||\mathtt{r}_2)\backslash\mathtt{l} \sim (\mathtt{r}_1\backslash\mathtt{l}||\mathtt{r}_2)} \qquad \text{(Eq-Merge/Restr)}$$

A.11 Type equivalence (congruence)

$$\mathtt{t} \sim \mathtt{t} \qquad \text{(Eq-Refl)}$$

$$\frac{\mathtt{t}' \sim \mathtt{t}}{\mathtt{t} \sim \mathtt{t}'} \qquad \text{(Eq-Symm)}$$

$$\frac{\mathtt{t} \sim \mathtt{t}' \qquad \mathtt{t}' \sim \mathtt{t}''}{\mathtt{t} \sim \mathtt{t}''} \qquad \text{(Eq-Trans)}$$

$$\frac{\mathtt{t}_1 \sim \mathtt{t}_1' \qquad \mathtt{t}_2 \sim \mathtt{t}_2'}{\mathtt{t}_1 \to \mathtt{t}_2 \sim \mathtt{t}_1' \to \mathtt{t}_2'} \qquad \text{(Eq-Cong-Arrow)}$$

$$\frac{\mathtt{R} \sim \mathtt{R}' \qquad \mathtt{t} \sim \mathtt{t}'}{\forall \mathtt{a}\#\mathtt{R}.\ \mathtt{t} \sim \forall \mathtt{a}\#\mathtt{R}'.\ \mathtt{t}'} \qquad \text{(Eq-Cong-All)}$$

$$\frac{\mathtt{t} \sim \mathtt{t}'}{\mathtt{l}{:}\mathtt{t} \sim \mathtt{l}{:}\mathtt{t}'} \qquad \text{(Eq-Cong-Base)}$$

$$\frac{\mathtt{r} \sim \mathtt{r}}{\mathtt{r}\backslash\mathtt{l} \sim \mathtt{r}'\backslash\mathtt{l}} \qquad \text{(Eq-Cong-Restr)}$$

$$\frac{\mathtt{r}_1 \sim \mathtt{r}_1' \qquad \mathtt{r}_2 \sim \mathtt{r}_2'}{\mathtt{r}_1 \,||\, \mathtt{r}_2 \sim \mathtt{r}_1' \,||\, \mathtt{r}_2'} \qquad \text{(Eq-Cong-Merge)}$$

A.12 Well-typed terms

$$\frac{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e} \in \mathtt{t} \qquad \mathtt{T} \vdash \mathtt{t}' \text{ type} \qquad \mathtt{t} \sim \mathtt{t}'}{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e} \in \mathtt{t}'} \qquad \text{(Wtt-Eq)}$$

$$\frac{\mathtt{T} \vdash \mathtt{G}_1, \mathtt{x}{:}\mathtt{t}, \mathtt{G}_2 \text{ ok}}{\mathtt{T}\,;\mathtt{G}_1, \mathtt{x}{:}\mathtt{t}, \mathtt{G}_2 \vdash \mathtt{x} \in \mathtt{t}} \qquad \text{(Wtt-Var)}$$

$$\frac{\mathtt{T}\,;\mathtt{G}, \mathtt{x}{:}\mathtt{t} \vdash \mathtt{e} \in \mathtt{t}'}{\mathtt{T}\,;\mathtt{G} \vdash \lambda\mathtt{x}{:}\mathtt{t}.\ \mathtt{e} \in \mathtt{t} \to \mathtt{t}'} \qquad \text{(Wtt-Arrow-I)}$$

$$\frac{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}_1 \in \mathtt{t} \to \mathtt{t}' \qquad \mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}_2 \in \mathtt{t}}{\mathtt{T}\,;\mathtt{G} \vdash \mathtt{e}_1\ \mathtt{e}_2 \in \mathtt{t}'} \qquad \text{(Wtt-Arrow-E)}$$

$$\frac{\mathtt{T\,;G} \vdash \mathtt{e} \in \mathtt{t}}{\mathtt{T\,;G} \vdash \mathtt{l{=}e} \in \mathtt{l{:}t}} \quad \text{(WTT-BASE)}$$

$$\frac{\mathtt{T\,;G} \vdash \mathtt{e} \in \mathtt{r} \qquad \mathtt{r_l}\downarrow}{\mathtt{T\,;G} \vdash \mathtt{e\backslash l} \in \mathtt{r\backslash l}} \quad \text{(WTT-RESTR)}$$

$$\frac{\mathtt{T} \vdash \mathtt{G\ ok}}{\mathtt{T\,;G} \vdash \mathtt{empty} \in \mathtt{Empty}} \quad \text{(WTT-EMPTY)}$$

$$\frac{\mathtt{T\,;G} \vdash \mathtt{e}_1 \in \mathtt{r}_1 \qquad \mathtt{T\,;G} \vdash \mathtt{e}_2 \in \mathtt{r}_2 \qquad \mathtt{T} \vdash \mathtt{r}_1 \,\#\, \mathtt{r}_2}{\mathtt{T\,;G} \vdash \mathtt{e}_1||\mathtt{e}_2 \in \mathtt{r}_1||\mathtt{r}_2} \quad \text{(WTT-MERGE)}$$

$$\frac{\mathtt{T\,;G} \vdash \mathtt{e} \in \mathtt{r} \qquad \mathtt{r_l}\downarrow}{\mathtt{T\,;G} \vdash \mathtt{e.l} \in \mathtt{r_l}} \quad \text{(WTT-SELECT)}$$

$$\frac{\mathtt{T,a\#R\,;G} \vdash \mathtt{e} \in \mathtt{t}}{\mathtt{T\,;G} \vdash \Lambda\mathtt{a\#R.e} \in \forall\mathtt{a\#R.\,t}} \quad \text{(WTT-ALL-I)}$$

$$\frac{\mathtt{T\,;G} \vdash \mathtt{e} \in \forall\mathtt{a\#R.\,t} \qquad \mathtt{T} \vdash \mathtt{r} \,\#\, \mathtt{R}}{\mathtt{T\,;G} \vdash \mathtt{e[r]} \in \mathtt{[r/a]t}} \quad \text{(WTT-ALL-E)}$$

B Complete Typechecking Rules (Algorithmic Version)

B.1 Judgement forms

Well-formed type:	$\mathtt{T} \vdash \mathtt{t} \Rightarrow \text{type}$
Well-formed record type:	$\mathtt{T} \vdash \mathtt{r} \Rightarrow \text{record}$
Well-formed constraint list:	$\mathtt{T} \vdash \mathtt{R} \Rightarrow \text{ok}$
Constraint list satisfaction:	$\mathtt{T} \vdash \mathtt{r} \,\#^{\Rightarrow}\, \mathtt{R}$
Compatible types:	$\mathtt{T} \vdash \mathtt{r}_1 \,\#^{\Rightarrow}\, \mathtt{r}_2$
Well-formed term:	$\mathtt{T\,;G} \vdash \mathtt{e} \Rightarrow \mathtt{t}$

B.2 Type and constraint list normalization

B.3 Well-formed constraint lists

$$\frac{\mathtt{T} \Rightarrow \text{ok}}{\mathtt{T} \vdash \diamond \Rightarrow \text{ok}} \quad \text{(A-WFCL-NIL)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \Rightarrow \text{record} \qquad \mathtt{T} \vdash \mathtt{R} \Rightarrow \text{ok}}{\mathtt{T} \vdash \mathtt{r,R} \Rightarrow \text{ok}} \quad \text{(A-WFCL-CONS)}$$

B.4 Well-formed types

$$\mathtt{T} \vdash \mathtt{p} \Rightarrow \text{type} \quad \text{(A-WFT-PRIM)}$$

$$\frac{\mathtt{T} \vdash \mathtt{t}_1 \Rightarrow \text{type} \qquad \mathtt{T} \vdash \mathtt{t}_2 \Rightarrow \text{type}}{\mathtt{T} \vdash \mathtt{t}_1 \rightarrow \mathtt{t}_2 \Rightarrow \text{type}} \quad \text{(A-WFT-ARROW)}$$

$$\frac{\mathtt{T,a\#R} \vdash \mathtt{t} \Rightarrow \text{type} \qquad \mathtt{T} \vdash \mathtt{R} \Rightarrow \text{ok}}{\mathtt{T} \vdash \forall\mathtt{a\#R.\,t} \Rightarrow \text{type}} \quad \text{(A-WFT-ALL)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \Rightarrow \text{record}}{\mathtt{T} \vdash \mathtt{r} \Rightarrow \text{type}} \quad \text{(A-WFT-REC)}$$

$$\texttt{Empty} \,||\, \texttt{r} \twoheadrightarrow^1 \texttt{r} \qquad \text{(A-Red-Empty-1)}$$

$$\texttt{r} \,||\, \texttt{Empty} \twoheadrightarrow^1 \texttt{r} \qquad \text{(A-Red-Empty-2)}$$

$$\texttt{l:t}\backslash\texttt{l} \twoheadrightarrow^1 \texttt{Empty} \qquad \text{(A-Red-Restr/Base)}$$

$$(\texttt{r} \,||\, \texttt{s})\backslash\texttt{l} \twoheadrightarrow^1 (\texttt{r}\backslash\texttt{l}) \,||\, \texttt{s} \quad \text{if } \texttt{r_l}\downarrow \qquad \text{(A-Red-Restr/Merge-1)}$$

$$(\texttt{r} \,||\, \texttt{s})\backslash\texttt{l} \twoheadrightarrow^1 \texttt{r} \,||\, (\texttt{s}\backslash\texttt{l}) \quad \text{if } \texttt{s_l}\downarrow \qquad \text{(A-Red-Restr/Merge-2)}$$

$$\rho||\sigma, \texttt{R} \twoheadrightarrow^1 \rho, \sigma, \texttt{R} \qquad \text{(A-Cred-Merge)}$$

$$\texttt{Empty}, \texttt{R} \twoheadrightarrow^1 \texttt{R} \qquad \text{(A-Cred-Empty)}$$

$$\texttt{l:t}, \texttt{R} \twoheadrightarrow^1 \texttt{l}, \texttt{R} \qquad \text{(A-Cred-Base)}$$

Figure 8: Proper reduction rules

$$\texttt{r}\backslash\texttt{l}\backslash\texttt{l}' \approx^1 \texttt{r}\backslash\texttt{l}'\backslash\texttt{l} \qquad \text{(A-Eq-Restr/Restr')}$$

$$\texttt{r} \,||\, \texttt{s} \approx^1 \texttt{s} \,||\, \texttt{r} \qquad \text{(A-Eq-Comm)}$$

$$\texttt{r} \,||\, (\texttt{s} \,||\, \texttt{t}) \approx^1 (\texttt{r} \,||\, \texttt{s}) \,||\, \texttt{t} \qquad \text{(A-Eq-Assoc)}$$

$$\phi, \phi, \texttt{R} \approx^1 \phi, \texttt{R} \qquad \text{(A-Ceq-Dupl)}$$

$$\rho, \sigma, \texttt{R} \approx^1 \sigma, \rho, \texttt{R} \qquad \text{(A-Ceq-Comm)}$$

Figure 9: Pure equivalences

B.5 Well-formed record types

$$\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{a} \Rightarrow \text{record} \qquad \text{(A-Wfr-Var)}$$

$$\frac{\mathtt{T} \vdash \mathtt{t} \Rightarrow \text{type}}{\mathtt{T} \vdash \mathtt{l{:}t} \Rightarrow \text{record}} \qquad \text{(A-Wfr-Base)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \Rightarrow \text{record} \qquad \mathtt{r_l}\downarrow}{\mathtt{T} \vdash \mathtt{r}\backslash\mathtt{l} \Rightarrow \text{record}} \qquad \text{(A-Wfr-Restr)}$$

$$\mathtt{T} \vdash \mathtt{Empty} \Rightarrow \text{record} \qquad \text{(A-Wfr-Empty)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r}_1 \Rightarrow \text{record} \qquad \mathtt{T} \vdash \mathtt{r}_2 \Rightarrow \text{record} \qquad \mathtt{T} \vdash \mathtt{r}_1 \#^{\Rightarrow} \mathtt{r}_2}{\mathtt{T} \vdash \mathtt{r}_1 \,||\, \mathtt{r}_2 \Rightarrow \text{record}} \qquad \text{(A-Wfr-Merge)}$$

B.6 Constraint list satisfaction

$$\frac{\mathtt{T} \vdash \mathtt{r} \Rightarrow \text{record}}{\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \diamond} \qquad \text{(A-Cmp-List-Nil)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{r}_i \qquad \mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{R}}{\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{r}_i, \mathtt{R}} \qquad \text{(A-Cmp-List-Cons)}$$

B.7 Compatibility

$$\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{Empty} \qquad \text{(A-Cmp-Empty-1)}$$

$$\mathtt{T} \vdash \mathtt{Empty} \#^{\Rightarrow} \mathtt{r} \qquad \text{(A-Cmp-Empty-2)}$$

$$\frac{\mathtt{T} \vdash \mathtt{s}_1 \#^{\Rightarrow} \mathtt{r} \qquad \mathtt{T} \vdash \mathtt{s}_2 \#^{\Rightarrow} \mathtt{r}}{\mathtt{T} \vdash (\mathtt{s}_1 \,||\, \mathtt{s}_2) \#^{\Rightarrow} \mathtt{r}} \qquad \text{(A-Cmp-Merge-I-1)}$$

$$\frac{\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{s}_1 \qquad \mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} \mathtt{s}_2}{\mathtt{T} \vdash \mathtt{r} \#^{\Rightarrow} (\mathtt{s}_1 \,||\, \mathtt{s}_2)} \qquad \text{(A-Cmp-Merge-I-2)}$$

$$\frac{\mathtt{l} \neq \mathtt{l}'}{\mathtt{T} \vdash \mathtt{l{:}t} \#^{\Rightarrow} \mathtt{l}'\mathtt{{:}t}'} \qquad \text{(A-Cmp-Base/Base)}$$

$$\frac{\mathtt{a} \in \mathtt{S}^*}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2, \mathtt{b}\#\mathtt{S}, \mathtt{T}_3 \vdash \mathtt{a} \#^{\Rightarrow} \mathtt{b}} \qquad \text{(A-Cmp-Tvar/Tvar-1)}$$

$$\frac{\mathtt{a} \in \mathtt{S}^*}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2, \mathtt{b}\#\mathtt{S}, \mathtt{T}_3 \vdash \mathtt{b} \#^{\Rightarrow} \mathtt{a}} \qquad \text{(A-Cmp-Tvar/Tvar-2)}$$

$$\frac{\mathtt{l} \in \mathtt{R}^*}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{a} \#^{\Rightarrow} \mathtt{l{:}t}} \qquad \text{(A-Cmp-Base/Tvar-1)}$$

$$\frac{\mathtt{l} \in \mathtt{R}^*}{\mathtt{T}_1, \mathtt{a}\#\mathtt{R}, \mathtt{T}_2 \vdash \mathtt{l{:}t} \#^{\Rightarrow} \mathtt{a}} \qquad \text{(A-Cmp-Base/Tvar-2)}$$

B.8 Well-typed terms

$$\mathtt{T\,;\,G_1, x{:}t, G_2 \vdash x \Rightarrow t} \qquad \text{(A-Wtt-Var)}$$

$$\frac{\mathtt{T \vdash t \Rightarrow}\ \text{type} \qquad \mathtt{T\,;\,G, x{:}t \vdash e \Rightarrow t'}}{\mathtt{T\,;\,G \vdash \lambda x{:}t.\ e \Rightarrow t \to t'}} \qquad \text{(A-Wtt-Arrow-I)}$$

$$\frac{\mathtt{T\,;\,G \vdash e_1 \Rightarrow t \to t'} \qquad \mathtt{T\,;\,G \vdash e_2 \Rightarrow t''} \qquad \mathtt{t'' \equiv t}}{\mathtt{T\,;\,G \vdash e_1\ e_2 \Rightarrow t'}} \qquad \text{(A-Wtt-Arrow-E)}$$

$$\frac{\mathtt{T\,;\,G \vdash e \Rightarrow t}}{\mathtt{T\,;\,G \vdash l{=}e \Rightarrow l{:}t}} \qquad \text{(A-Wtt-Base)}$$

$$\frac{\mathtt{T\,;\,G \vdash e \Rightarrow r} \qquad \mathtt{r_l}\downarrow}{\mathtt{T\,;\,G \vdash e \backslash l \Rightarrow r \backslash l}} \qquad \text{(A-Wtt-Restr)}$$

$$\mathtt{T\,;\,G \vdash empty \Rightarrow Empty} \qquad \text{(A-Wtt-Empty)}$$

$$\frac{\mathtt{T\,;\,G \vdash e_1 \Rightarrow r_1} \qquad \mathtt{T\,;\,G \vdash e_2 \Rightarrow r_2} \qquad \mathtt{T \vdash r_1^* \#^{\Rightarrow} r_2^*}}{\mathtt{T\,;\,G \vdash e_1 \,||\, e_2 \Rightarrow r_1 \,||\, r_2}} \qquad \text{(A-Wtt-Merge)}$$

$$\frac{\mathtt{T\,;\,G \vdash e \Rightarrow r} \qquad \mathtt{r_l}\downarrow}{\mathtt{T\,;\,G \vdash e.l \Rightarrow r_l}} \qquad \text{(A-Wtt-Select)}$$

$$\frac{\mathtt{T \vdash R\ ok} \qquad \mathtt{T, a\#R\,;\,G \vdash e \Rightarrow t}}{\mathtt{T\,;\,G \vdash \Lambda a\#R.\ e \Rightarrow \forall a\#R.\ t}} \qquad \text{(A-Wtt-All-I)}$$

$$\frac{\mathtt{T\,;\,G \vdash e \Rightarrow \forall a\#R.\ t} \qquad \mathtt{T \vdash r \Rightarrow}\ \text{record} \qquad \mathtt{T \vdash r^* \#^{\Rightarrow} R^*}}{\mathtt{T\,;\,G \vdash e[r] \Rightarrow [r/a]t}} \qquad \text{(A-Wtt-All-E)}$$

References

[1] 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.

[2] Luca Cardelli. A semantics of multiple inheritance. In G. Kahn, D. MacQueen, and G. Plotkin, editors, *Semantics of Data Types*, volume 173 of *Lecture Notes in Computer Science*, pages 51–67. Springer-Verlag, 1984.

[3] Luca Cardelli. A semantics of multiple inheritance. *Information and Computation*, 76:138–164, 1988.

[4] Luca Cardelli and John Mitchell. Operations on records (summary). In M. Main, A. Melton, M. Mislove, and D. Schmidt, editors, *Proceedings of Fifth International Conference on Mathematical Foundations of Programming Language Semantics*, volume 442 of *Lecture Notes in Computer Science*, pages 22–52, Tulane University, New Orleans, March 1989. Springer Verlag. To appear in Mathematical Structures in Computer Science.

[5] Luca Cardelli and John C. Mitchell. Operations on records. Research Report 48, Digital Equipment Corporation, Systems Research Center, August 1989.

[6] Luca Cardelli and Peter Wegner. On understanding types, data abstraction, and polymorphism. *Computing Surveys*, 17(4), December 1985.

[7] 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.

[8] Luis Damas and Robin Milner. Principal type schemes for functional programs. In *Proceedings of the 9th ACM Symposium on Principles of Programming Languages*, pages 207–212, 1982.

[9] Jean-Yves Girard. *Interprétation fonctionelle et élimination des coupures de l'arithmétique d'ordre supérieur*. PhD thesis, Université Paris VII, 1972.

[10] Robert W. Harper and Benjamin C. Pierce. Extensible records without subsumption. Technical Report CMU-CS-90-102, School of Computer Science, Carnegie Mellon University, Feburary 1990.

[11] Gérard Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *Journal of the Association for Computing Machinery*, 27(4):797–821, October 1980.

[12] Lalita A. Jategaonkar. ML with extended pattern matching and subtypes. Master's thesis, MIT, August 1989.

[13] Lalita A. Jategaonkar and John C. Mitchell. ML with extended pattern matching and subtypes (preliminary version). In *Proceedings of the ACM Conference on Lisp and Functional Programming*, pages 198–211, Snowbird, Utah, July 1988.

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

[15] Robin Milner. *A Calculus of Communicating Systems*. Springer-Verlag, LNCS 92, 1980.

[16] Robin Milner, Mads Tofte, and Robert Harper. *The Definition of Standard ML*. The MIT Press, 1990.

[17] John C. Mitchell. Coercion and type inference (summary). In *Proc. 11th ACM Symp. on Principles of Programming Languages*, pages 175–185, January 1984.

[18] Atsushi Ohori and Peter Buneman. Static type inference for parametric classes. In *OOPSLA '89: Object-Oriented Programming Systems, Languages, and Applications, Conference Proceedings*, pages 445–456, October 1989.

[19] Atsushi Ohori and Peter Buneman. Type inference in a database programming language. In *1988 ACM Conference on Lisp and Functional Programming*, pages 174–183, Snowbird, Utah, July 1989. Revised manuscript, September, 1988.

[20] Didier Rémy. Typechecking records and variants in a natural extension of ML. In *Proceedings of the Sixteenth Annual ACM Symposium on Principles of Programming Languages, Austin*, pages 242–249. ACM, January 1989.

[21] Didier Rémy. *Algèbres Touffues. Application au Typage Polymorphe des Objets Enregistrements dans les Langages Fonctionnels.* PhD thesis, Université Paris VII, 1990.

[22] Didier Rémy. Typechecking records in a natural extension of ML. Submitted to TOPLAS, June 1990.

[23] John Reynolds. Towards a theory of type structure. In *Proc. Colloque sur la Programmation*, pages 408–425, New York, 1974. Springer-Verlag LNCS 19.

[24] Ryan Stansifer. Type inference with subtypes. In *Proceedings of the Fifteenth ACM Symposium on Principles of Programming Languages*, pages 88–97, San Diego, CA, January 1988.

[25] Mitchell Wand. Complete type inference for simple objects. In *Proceedings of the IEEE Symposium on Logic in Computer Science*, Ithaca, NY, June 1987.

[26] Mitchell Wand. Corrigendum: Complete type inference for simple objects. In *Proceedings of the IEEE Symposium on Logic in Computer Science*, 1988.

[27] Mitchell Wand. Type inference for objects with instance variables and inheritance. Technical Report NU-CCS-89-2, College of Computer Science, Northeastern University, 1989.

[28] Mitchell Wand. Type inference for record concatenation and multiple inheritance. In *Fourth Annual IEEE Symposium on Logic in Computer Science*, pages 92–97, Pacific Grove, CA, June 1989.