Record concatenation with intersection types

Citation for published version (APA):

Document status and date:
Published: 01/01/1995

Document Version:
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:
• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher’s website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:
www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.
Record concatenation with intersection types

by

Jan Zwanenburg

95/34

ISSN 0926-4515

All rights reserved
editors: prof.dr. R.C. Backhouse
         prof.dr. J.C.M. Baeten

Reports are available at:
http://www.win.tue.nl/win/cs

Computing Science Report 95/34
Eindhoven, December 1995
Record concatenation with intersection types

Jan Zwanenburg
Department of Mathematics and Computing Science
Eindhoven University of Technology
P.O.Box 513, 5600 MB Eindhoven, The Netherlands
e-mail janz@win.tue.nl

December 20, 1995

Abstract

We define an extension of a second-order type system with records and operations on them, including record concatenation. Our aim is to model the most important concepts in object-oriented languages in a type system with subtyping. Such a model needs a form of record concatenation. The novelty in our approach is that intersection types are used for record concatenation. We give examples of how object-oriented concepts can be modelled and show how the system can be translated to a type system without subtyping.
1 Introduction

Object-oriented programming (OOP) is concerned with objects, classes and methods. Objects are grouped into classes. Every class has a set of methods that operate on the objects in that class. A class can be extended in such a way that the objects in the new class (the subclass) still can be handled by the methods of the original class (the superclass). This defining property of OOP is called inheritance. It permits easily extensible software systems which is very important for programming in the real.

Our goal is to model the most important concepts of OOP in the framework of the typed lambda-calculus, because it has well known semantics, proof-rules and typing rules, which are all (largely) missing in object-oriented languages. By such a model we hope to gain insight in these issues.

But pure lambda calculus is not rich enough to model OOP. To implement objects, records are needed, and to implement some aspects of inheritance, subtyping is needed. A type is a subtype of another type if there is a natural coercion from the former type to the latter type. Even in a calculus with records and subtyping, two problems remain.

One is a consequence of our framework being functional and not imperative. It is not possible to make a function that returns a copy of a record with a certain field changed, working on all records with that field. This is called the polymorphic record update problem.

An example is a function that increases the x-field of a record by one. We need to write it as a polymorphic function with some demand on the type variable:

\[ \text{up} = \lambda P \text{ "with x-field of type Int". } \lambda p : P \text{ "p with x-increased by one" } \]

\[ \text{up} : \forall P \text{ "with x-field of type Int". } P \rightarrow P \]

\[ \text{up} \{ x : \text{Int}, y : \text{Int} \} \{ z = 3, y = 5 \} = \{ z = 4, y = 5 \} \]

The demand "with x-field of type Int" cannot be expressed by subtyping laws for records.

The other problem is that in order to model inheritance, a form of record concatenation or extension is needed.

Record extension is the extension of a record with one field. By doing this repeatedly, a record can be extended with a certain number of fields. The record concatenation of two records is a new record, that has all the fields that any of the constituents have. This is more flexible than record extension, and is necessary for multiple inheritance (where a class may have more than one superclass).

Wand [Wan 87] gave a system of extensible records in an implicitly typed language. This was later extended to include concatenation and the type-inference problem was solved [Wan 89]. Cardelli and Wegner [CW 85] defined a full second-order, explicitly typed language with records, subtyping and bounded quantification, i.e. an abstraction over a type variable that has to be a subtype of some type.

To solve the polymorphic record update problem, more powerful explicitly typed calculi were defined. Most introduced a form of disjoint concatenation (only new fields may be added), and a way of restricting records (removing a field). Together these operations can provide a polymorphic update. But the ones that include subtyping [CM 91, Car 92] have no full record concatenation, just extension. Alternatives that do have record concatenation [HP 90], do not have subtyping, which is necessary for a natural model of inheritance. Most problems are caused by type variables that represent records.

In this paper, we model concatenation by intersection types, developed by Coppo and Dezani-Ciancaglini [CD 78]. This choice is based on the fact that, given two record types \( R \) and \( S \), the concatenation of \( R \) and \( S \) should be a subtype of \( R \) and a subtype of \( S \). This is one of the defining property of the intersection of \( R \) and \( S \). More formally, the intersection is defined as the greatest lower bound in the subtype hierarchy:

\[ R \land S \leq R \quad R \land S \leq S \quad T \leq R \text{ and } T \leq S \Rightarrow T \leq R \land S \]

All three rules are also valid if one reads record concatenation for \( \land \), so the interpretation of intersection types for concatenation is correct.

If we permit concatenation of arbitrary record values, the system becomes unsound. Therefore we permit the concatenation of two record values only if the record types have the same type on common fields. This relation between types \( R \) and \( S \) is denoted by \( R \# S \) (\( R \) compatible with \( S \)). The meaning of a concatenation on values is that for common fields preference
is given to the right value. In this way the polymorphic record update problem is solved in presence of both full record concatenation and subtyping.

Our concatenation doesn't require both records to be disjoint, therefore eliminating the need for record restriction. But it is more stringent than a concatenation without any demands on its arguments, which leads to inconsistencies, when coupled with subtyping in an explicitly typed calculus.

In section 2 we will, starting with a pure second-order lambda calculus, gradually extend the system with records, subtyping, intersection types and compatibility. Section 3 will show how the most important concepts of OOP can be modelled in our language. Again, we will do this in a gradual fashion. The more complex models will need some constructions not formally described in this paper (type constructors, existential types and the fixpoint combinator, all well known). The semantics of our system are described in section 4. This is based on a translation to the second-order lambda calculus with cartesian products.

2 Development

In this section we will present the second-order lambda calculus, and extend it with records, subtyping, the $\text{Top}$ type, intersection types and compatibility. From section 2.6 onwards we will only extend the compatibility rules so as to make the record concatenation more flexible.

In each subsection we will only give the new rules, and designate which old rules are redundant. In appendix A the total system is given.

2.1 Second-order lambda calculus

The starting point is $F$, the second-order lambda calculus [Gir 72]. In this calculus it is possible to make polymorphic functions, i.e. functions that work on several types.

Rules:

Types:

$T ::= X$ \hspace{1cm} type variable

$T \rightarrow T$ \hspace{1cm} function type

$\forall X: *. T$ \hspace{1cm} quantification

Terms:

$e ::= x$ \hspace{1cm} variable

$\lambda x: T. e$ \hspace{1cm} abstraction

$e \ e$ \hspace{1cm} application

$\lambda X: *. e$ \hspace{1cm} type abstraction

$e \ T$ \hspace{1cm} type application

Contexts:

$\Gamma ::= \emptyset$ \hspace{1cm} empty context

$\Gamma, x: T$ \hspace{1cm} term variable declaration

$\Gamma, X: *$ \hspace{1cm} type variable declaration

Judgments:

$\Gamma \vdash ok$ \hspace{1cm} well-formed context

$\Gamma \vdash T : *$ \hspace{1cm} well-formed type

$\Gamma \vdash e : T$ \hspace{1cm} well-typed term

Meta-variables:

$\Gamma$ \hspace{1cm} for contexts

$X$ \hspace{1cm} for type variables

$R, S, T, U, V$ \hspace{1cm} for types

$x$ \hspace{1cm} for term variables

$e, f$ \hspace{1cm} for terms

Derivation rules:
Context formation:

\[ \emptyset \vdash ok \quad (\text{C-Empty}) \]
\[ \Gamma \vdash T : * \quad x \notin \text{dom}(\Gamma) \quad (\text{C-Var}) \]
\[ \Gamma, x : T \vdash ok \]
\[ \Gamma \vdash ok \quad X \notin \text{dom}(\Gamma) \quad (\text{C-TVar}) \]
\[ \Gamma, X : * \vdash ok \]

Type formation:

\[ \Gamma_{1}, X : *, \Gamma_{2} \vdash ok \quad (\text{K-TVar}) \]
\[ \Gamma_{1}, X : *, \Gamma_{2} \vdash X : * \]
\[ \Gamma \vdash T_{1} : * \quad \Gamma \vdash T_{2} : * \quad (\text{K-Arrow}) \]
\[ \Gamma \vdash T_{1} \rightarrow T_{2} : * \]
\[ \Gamma, X : * \vdash T : * \quad (\text{K-All}) \]
\[ \Gamma \vdash (\forall X : *, T) : * \]

Term formation:

\[ \Gamma_{1}, x : T, \Gamma_{2} \vdash ok \quad (\text{T-Var}) \]
\[ \Gamma_{1}, x : T, \Gamma_{2} \vdash x : T \]
\[ \Gamma \vdash f : S \rightarrow T \quad \Gamma \vdash e : S \quad (\text{T-Abs}) \]
\[ \Gamma \vdash \lambda x : S. e : S \rightarrow T \]
\[ \Gamma \vdash f : T \quad (\text{T-App}) \]
\[ \Gamma \vdash f : S \rightarrow T \]
\[ \Gamma \vdash e : S \]
\[ \Gamma \vdash \lambda x : e : S \rightarrow T \quad (\text{T-TAbs}) \]
\[ \Gamma \vdash f : \forall X : *, T \quad (\text{T-TApp}) \]
\[ \Gamma \vdash U : * \]
\[ \Gamma \vdash U : T \]

Reduction rules:

\[ (\lambda x : e_{1}) e_{2} \triangleright_{\beta} e_{2}[x := e_{2}] \]
\[ (\lambda X : * e) T \triangleright_{\beta} e[T := X] \]

In examples we will assume there are types \text{Real}, \text{Int} and \text{Char}, and the usual terms of these types. More formally, we will consider \text{Real} : *, \text{Int} : *, \text{Char} : *, + : \text{Int} \rightarrow \text{Int} = \text{Int} \rightarrow \text{Int} \rightarrow \text{Int} \rightarrow \text{Int} \rightarrow \text{Int} etc. to be always part of the context.

Convention: We write \vdash e : T for \emptyset \vdash e : T etc.

Examples:
1. \vdash (\lambda X : * \lambda z : X. z) : \forall X : * X \rightarrow X
   the polymorphic identity
2. \vdash 7.00 : \text{Real}
3. \vdash 7 : \text{Int}
4. \vdash 'a' : \text{Char}

Limitations: There is no tuple datastructure.
2.2 Records

When objects and classes are modelled in a λ-calculus, records are used. Therefore we will first extend our system with basic record operations, i.e. the construction of a record and the selection of a field of a record.

We introduce a set of labels $\mathcal{L}$ (with meta-variables $l, m$) and add the following rules to the system:

Rules:

\begin{align*}
\text{(K-Rec)} & \quad \frac{\text{all } l_i \in \mathcal{L} \text{ distinct labels} \quad \text{for } i = 1..n \quad \Gamma \vdash T_i : * \quad n \geq 0}{\Gamma \vdash \{l_1:T_1, \ldots, l_n:T_n\} : *}
\text{(T-Rec)} & \quad \frac{\Gamma \vdash \{l_1=e_1, \ldots, l_n=e_n\} : \{l_1:T_1, \ldots, l_n:T_n\}}{\Gamma \vdash e : \{l_1:T_1, \ldots, l_n:T_n\}}
\text{(T-Sc1)} & \quad \frac{1 \leq i \leq n}{\Gamma \vdash e_i : T_i} \quad \Gamma \vdash e \{l_1:T_1, \ldots, l_n:T_n\}
\end{align*}

Reduction is extended by:

\begin{align*}
\{l_1=e_1, \ldots, l_n=e_n\} \Downarrow e_i
\end{align*}

We do not identify records that differ only in the order of the fields (unlike most other calculi do), because we will model them with unlabelled products.

Examples:

1. $\Gamma \vdash \lambda p:\{x:\text{Int}, y:\text{Int}\}. \ p.x + p.y : \{x:\text{Int}, y:\text{Int}\} \to \text{Int}$
2. $\Gamma \vdash \lambda p:\{x:\text{Int}, y:\text{Int}\}. \ \{x=p.x+1, y=p.y\} : \{x:\text{Int}, y:\text{Int}\} \to \{x:\text{Int}, y:\text{Int}\}$
3. $\Gamma \vdash \{l=\{p=7, q='a', m=3.14\} : \{l:\{p:\text{Int}, q:\text{Char}\}, m:\text{Real}\}\} \quad \text{(this is called a nested record)}$
4. $\{l=6\} \Downarrow 6$

Limitations: The typing is very rigid and there is no structure in the record types that can help to overcome this problem. E.g. we cannot apply the function of example 2 to $\{x=3, y=4, z=5\}$ or to $\{y=4, x=3\}$.

2.3 Subtyping

The standard way to alleviate the rigid typing is to introduce subtyping, see e.g. [Car 88] for subtyping on records. Subtyping is a relation between types, denoted by $\leq$. If $S$ is a subtype of $T$, it means that a term of type $S$ can be used at every place where a term of type $T$ can be used, because there is a natural way of coercing a value of type $S$ to type $T$.

Subtyping is used to model one crucial aspect of inheritance, viz. that an object of a subclass may be used in any place where an object of the superclass is used. As objects are modelled by records, and an object of a subclass has more fields than an object of a superclass, the subtyping relationship we need is that a recordtype with more fields is a subtype of a recordtype with less fields. Of course, there is a natural coercion from the first to the latter: forget some fields. This rule for subtyping is formalized by (S-Width) below.

Sometimes it is necessary to demand that a type variable in a polymorphic function is a subtype of some type $T$. This is called bounded quantification: The type variable is noted with its bound in the abstraction or polymorphic type.

Here we will present the extension of the rules to realize subtyping.

Rules:

Types:

\begin{align*}
T := \forall X \leq T. \ T \quad \text{bounded quantification}
\end{align*}

Terms:

\begin{align*}
e := \forall X \leq T. \ e \quad \text{type abstraction}
\end{align*}
Contexts:
\[ \Gamma ::= \Gamma, X \leq T \quad \text{type variable declaration} \]

Judgments:
\[ \Gamma \vdash S \leq T \quad \text{subtype} \]

Derivation rules:

**Context formation:**
\[
\frac{\Gamma_1, X \leq T, \Gamma_2 \vdash \text{ok}}{\Gamma_1, X \leq T, \Gamma_2, \Gamma \vdash X : \ast} \quad \text{(C-TVar)}
\]

**Type formation:**
\[
\frac{\Gamma_1, X \leq T, \Gamma_2 \vdash \text{ok}}{\Gamma_1, X \leq T, \Gamma_2, \Gamma \vdash X : \ast} \quad \text{(K-TVar)}
\]
\[
\frac{\Gamma, X \leq T \vdash U : \ast}{\Gamma \vdash \forall X \leq T. U : \ast} \quad \text{(K-All)}
\]

**Subtyping:**
\[
\frac{\Gamma \vdash T : \ast}{\Gamma \vdash T \leq T} \quad \text{(S-Refl)}
\]
\[
\frac{\Gamma \vdash S \leq T \quad \Gamma \vdash T \leq U}{\Gamma \vdash S \leq U} \quad \text{(S-Trans)}
\]
\[
\frac{\Gamma_1, X \leq T, \Gamma_2 \vdash \text{ok}}{\Gamma_1, X \leq T, \Gamma_2, \Gamma \vdash X \leq T} \quad \text{(S-Var)}
\]
\[
\frac{\Gamma \vdash S_1 \leq S_2 \quad \Gamma \vdash S \leq T_2}{\Gamma \vdash S_1 \rightarrow S_2 \leq T_1 \rightarrow T_2} \quad \text{(S-Arrow)}
\]
\[
\frac{\Gamma, X \leq U \vdash S \leq T}{\Gamma \vdash \forall X \leq U. S \leq \forall X \leq U. T} \quad \text{(S-All)}
\]
\[
\frac{\Gamma \vdash \{I_1: T_1, \ldots, I_m: T_m\} : \ast \quad n \geq m}{\Gamma \vdash \{I_1: T_1, \ldots, I_m: T_m\} \leq \{I_1: T_1, \ldots, I_m: T_m\}} \quad \text{(S-Width)}
\]
\[
\frac{\{\text{for } i = 1..n \Gamma \vdash S_i \leq T_i\}}{\Gamma \vdash \{I_1: T_1, \ldots, I_m: T_m\} \leq \{I_1: T_1, \ldots, I_m: T_m\}} \quad \text{(S-Depth)}
\]
\[
\frac{\text{for } f : 1..n \rightarrow 1..n \text{ bijection}}{\Gamma \vdash \{I_1: T_1, \ldots, I_m: T_m\} \leq \{I_1: T_1, \ldots, I_m: T_m\}} \quad \text{(S-Order)}
\]

**Term formation:**
\[
\frac{\Gamma, X \leq S \vdash e : T}{\Gamma \vdash \lambda X \leq S. e : \forall X \leq S. T} \quad \text{(T-TAbs)}
\]
\[
\frac{\Gamma \vdash f : \forall X \leq S. T \quad \Gamma \vdash U \leq S}{\Gamma \vdash f \cdot U : T[X := U]} \quad \text{(T-TApp)}
\]
\[
\frac{\Gamma \vdash e : S \quad \Gamma \vdash S \leq T}{\Gamma \vdash e : T} \quad \text{(T-Subsumption)}
\]
\[
\frac{\Gamma \vdash e : \{\text{for } I = \{I_1, \ldots, I_m\}\}}{\Gamma \vdash e : \{I = \{I_1, \ldots, I_m\}\}} \quad \text{(T-Sel)}
\]

**Equality:**
\[
(\lambda x : t. e_1) e_2 = e_1[x := e_2]
\]
\[
(\lambda x : t. e) T = e[x := T]
\]
\[
(\lambda X : t. e) T_2 = e[X := T_2]
\]
\[
\{I_1 = e_1, \ldots, I_m = e_m\}, I_i = e_i
\]
Notation:
\[ \Gamma \vdash S \sim T \] is an abbreviation for \[ \Gamma \vdash S \leq T \text{ and } \Gamma \vdash T \leq S. \]
This relation is called equivalence.

Discussion:
All rules except (S-All) and the ones for records, viz. (S-Width), (S-Depth), (S-Order) and (T-Sel) are standard.
There has been a long debate about the (S-All) rule (for a summary, see [SP 94]). The following is considered the most natural rule:

\[
\begin{align*}
\Gamma & \vdash V \leq U \\
\Gamma, X \leq V & \vdash S \leq T
\end{align*}
\]
\[ (S-All') \]

Unfortunately, the subtyping problem of the system with this rule is undecidable [Pie 94], so we stick to the (S-All) rule.
Rule (T-Sel) is a short rule for the selection of a field of a record in a calculus of subtyping and makes the old (T-Sel) rule redundant. Rule (S-Width) expresses that a record with more fields is a subtype of a record with less fields, and (S-Depth) expresses that a record can be subtyped field-wise. Normally these two rules are presented as one, but we won’t do this to make the different aspects of subtyping for records clear. In other calculi rule (S-Order) is not present: records are considered modulo permutation of the fields. Here records with fields in a different order are equivalent, but not the same. From an implementational point of view, where records are modelled as unlabelled tuples this is the most natural. The computer has to apply a coercion, i.e. a permutation of the fields, but we don’t want the programmer having to write this coercion explicitly.

In examples we will consider the declaration of the integers in the context to be Int \leq Real.

Examples:
1. \( \vdash [k:\text{Int}, l:\text{Int}, m:\text{Int}] \leq [l:\text{Int}] \) (use S-order and S-width)
2. \( \vdash \text{Real} \rightarrow \text{Int} \leq \text{Int} \rightarrow \text{Real} \)
3. \( \vdash (\lambda r:\{l:\text{Int}\}, r.l) \{k=4, l=5, m=6\} : \text{Int} \) (use subtyping derivation from example 1)
4. \( \vdash (\lambda r:\{x:\text{Int}, y:\text{Int}\}, p.x + p.y)\{x=4, y=5, z=6\} : \text{Int} \)
5. \( \vdash (\lambda r:\{x:\text{Int}\}, \{x=p.x + 1\})\{x=4, y=5\} : \{x:\text{Int}\} \)
6. \( \vdash \lambda P \leq [x:\text{Int}] \cdot \lambda P : \{z=p.x + 1\} : \forall P \leq [x:\text{Int}] \cdot P \rightarrow [x:\text{Int}] \)
   As is clearly visible from the typing, this function always delivers a one-field record.
   Effectively, this function is the same as the one of example 5.
7. \( \vdash \{l:\{p:\text{Int}, q:\text{Char}\}, m:\text{Real}\} \leq \{l:\{p:\text{Int}\}\} \)

Discussion:
A major consequence of the introduction of subtyping is that \( \beta \)-reduction doesn’t fully describe the operational meaning of a program anymore, since coercions are left implicit. E.g. we would like to have

\[
(\lambda x: \text{Real}. x)7 > 7.000
\]

One way to solve this is to place coercions explicitly in the terms (section 4). However, to give the reader an idea of the meaning of terms, we have given equality rules and we will give equality rules for records in the following sections. These rules do not compose a full equational system for our calculus, this is outside the scope of this article. A more indirect way of formally deriving equality is presented in section 4.

Limitations: We would like to make a polymorphic record update, a polymorphic function that changes one field of a record, and leaves all other fields untouched. Examples 5 and 6 try to do this, but don’t succeed. In [BL 90] is a semantic argument that such a function cannot be made in calculi like this one, and, more generally, a function of type \( \forall X \leq T. X \rightarrow X \) must be an identity function.
2.4 Top type for ≤

The type $\text{Top}$ is introduced to recover an $F$ polymorphic function as a special case of bounded quantification, viz. with bound $\text{Top}$. This is done to reduce the number of derivation rules, and make the system more uniform.

We add to our system the type $\text{Top}$ with derivation rules:

Rules:

\[ \frac{ \Gamma \vdash \text{ok} }{ \Gamma \vdash \text{Top} : \ast } \quad (\text{K-Top}) \]

\[ \frac{ \Gamma \vdash S : \ast }{ \Gamma \vdash S \leq \text{Top} } \quad (\text{S-Top}) \]

\[ \frac{ \Gamma \vdash \text{ok} }{ \Gamma \vdash \text{top} : \text{Top} } \quad (\text{T-Top}) \]

The rules (C-TVar), (K-All), (T-TAbs) and (T-TApp) of section 2.1 are redundant now as they can be replaced by their counterparts of section 2.3 with bound set to $\text{Top}$. $\text{Top}$ has one element: $\text{top}$, so a coercion of any value to type $\text{Top}$ will yield $\text{top}$. Categorically, $\text{Top}$ is the terminal element of the set of types.

Examples:

1. $\vdash \lambda x \leq \text{Top}. \; \lambda x : X. \; z : \forall x \leq \text{Top}. \; X \rightarrow X$
   the polymorphic identity

2.5 Record concatenation

An operation that occurs frequently in OOP is extending the methods of a superclass with some new methods to make a subclass. As the set of methods of a class is represented by a record, this operation has to be represented by record extension: adding fields to a record. When a subclass has more than one superclass, i.e. in the case of multiple inheritance, all records of the superclasses have to be concatenated.

Therefore we will introduce record concatenation operators, $\land$ for record types and $\with$ for record values. We denote the concatenation with intersection, because the first has the same subtyping properties as the latter: the concatenation of record types $S$ and $T$ is a subtype of both $S$ and $T$. To prevent confusion, concatenation is only permitted if there are no common fields. This notion is formalized by the relation $\#$ (pronounce: compatible).

Note: $R \# S$ expresses that $R$ and $S$ are record types and don't have any fields in common.

Just as we needed bounded quantification when we introduced the relation $\leq$, we need restricted quantification now. This is a quantification where there is a restriction that the type variable must be compatible to a certain type. This means we have compatibility relations in contexts as well.

If we have record concatenation, we don't need multi-fields record as a primitive anymore since they can be constructed by repeatedly concatenating single-field records. However, we do need the record with no fields as a primitive. Because of these new primitives, we need other reduction rules for records.

All this is formalized in the following rules, as extension of the previous system. After the rules we will give a discussion, where we show which rules of the previous system are redundant (but still valid).

Rules:

Types:

\[
T ::= \forall X \leq T ; X \# T . \; T \\
\emptyset \; \text{restricted quantification}
\{\} \; \text{empty record type}
\{L : T\} \; \text{one-field record type}
T \land T \; \text{record concatenation}
\]
Terms:
\[ e ::= \lambda X \leq T; X \not\in T. e \quad \text{type abstraction} \]
\[ \{ \} \quad \text{empty record} \]
\[ \{ L = e \} \quad \text{one-field record} \]
\[ e \cdot T \text{ with } T e \quad \text{concatenation} \]
\[ e . L \quad \text{field selection} \]

Contexts:
\[ \Gamma ::= \Gamma, X \leq T; X \not\in T \quad \text{type variable declaration} \]

Judgments:
\[ \Gamma \vdash S \not\in T \quad \text{compatible} \]

Derivation rules:

Context formation:
\[
\frac{\Gamma \vdash T : * \quad \Gamma \vdash U : * \quad X \not\in \text{dom}(\Gamma)}{\Gamma, X \leq T; X \not\in U \vdash \text{ok}} \quad \text{(C-Var)}
\]

Type formation:
\[
\frac{\Gamma_1, X \leq T; X \not\in U, \Gamma_2 \vdash \text{ok}}{\Gamma_1, X \leq T; X \not\in U, \Gamma_2 \vdash X : *} \quad \text{(K-Var)}
\]
\[
\frac{\Gamma, X \leq T; X \not\in U \vdash S : *}{\Gamma \vdash \exists Y \leq T; X \not\in U. S : *} \quad \text{(K-All)}
\]
\[
\frac{\Gamma \vdash \text{ok}}{\Gamma \vdash \{ \} : *} \quad \text{(K-Empty)}
\]
\[
\frac{\Gamma \vdash T : *}{\Gamma \vdash \{ T \} : *} \quad \text{(K-Single)}
\]
\[
\frac{\Gamma \vdash R : * \quad \Gamma \vdash S : *}{\Gamma \vdash R \land S : *} \quad \text{(K-And)}
\]

Subtyping:
\[
\frac{\Gamma_1, X \leq T; X \not\in U, \Gamma_2 \vdash \text{ok}}{\Gamma_1, X \leq T, X \not\in U, \Gamma_2 \vdash X : T} \quad \text{(S-Var)}
\]
\[
\frac{\Gamma, X \leq U; X \not\in V \vdash S \leq T}{\Gamma \vdash \exists Y \leq U; X \not\in V. S \leq \exists Y \leq U. T} \quad \text{(S-All)}
\]
\[
\frac{\Gamma \vdash \{ R \} : *}{\Gamma \vdash \{ R \} \leq \{ S \}} \quad \text{(S-Empty)}
\]
\[
\frac{\Gamma \vdash R \leq S}{\Gamma \vdash \{ R \} \leq \{ S \}} \quad \text{(S-Depth)}
\]
\[
\frac{\Gamma \vdash S_1 \land S_2 : * \quad i = 1, 2}{\Gamma \vdash S_1 \land S_2 \leq S_i} \quad \text{(S-Inter-LB)}
\]
\[
\frac{\Gamma \vdash R \leq S \quad \Gamma \vdash R \leq T}{\Gamma \vdash R \leq S \land T} \quad \text{(S-Inter-G)}
\]

Compatibility rules:
\[
\frac{\Gamma_1, X \leq T; X \not\in U, \Gamma_2 \vdash \text{ok}}{\Gamma_1, X \leq T; X \not\in U, \Gamma_2 \vdash X \not\in U} \quad \text{(#-Var)}
\]
\[
\frac{\Gamma \vdash R \leq \{ S \}}{\Gamma \vdash \{ S \} \not\in R} \quad \text{( #-Empty-L)}
\]
\[
\frac{\Gamma \vdash R \leq \{ S \}}{\Gamma \vdash R \not\in \{ S \}} \quad \text{( #-Empty-R)}
\]
Term formation:

\[
\Gamma, X \subseteq S; X \# T \vdash e : U \quad \text{(T-TAbs)}
\]

\[
\Gamma, X \subseteq S; X \# T \vdash f : \forall X \subseteq S; X \# T. U \quad \Gamma \vdash V \subseteq S \quad \Gamma \vdash V \# T \quad \text{\text{T-App)}}
\]

\[
\Gamma \vdash f : \forall X \subseteq S; X \# T. U \quad \Gamma \vdash V \subseteq S \quad \Gamma \vdash V \# T \\
\Gamma \vdash f V : U[X := V]
\]

\[
\Gamma \vdash \text{ok} : \{\} \quad \text{(T-Empty)}
\]

\[
\Gamma \vdash e : T \\
\Gamma \vdash \{l = e\} : \{l: T\} \quad \text{(T-Single)}
\]

\[
\Gamma \vdash \tau : R \quad \Gamma \vdash \tau : S \quad \Gamma \vdash R \# S \\
\Gamma \vdash \tau R \text{ with } S : S \quad \text{(T-With)}
\]

Equations:

\[
(\lambda X \subseteq U; X \# V. e) T = e[X := T]
\]

\[
\{l = e\}.1 = e
\]

\[
r R \text{ with } \{\} s = r
\]

\[
[r R \text{ with } \{l: T\} s].l = s.l
\]

\[
[r R \text{ with } \{m: T\} s].l = r.l , \text{ if } l \neq m
\]

\[
[r R \text{ with } (S \& T) (s S \text{ with } T t)] = (r R \text{ with } S s) (R S) \text{ with } T t
\]

Discussion: We will discuss the new derivation rules sort by sort, in the context of records and record-operations.

The type formation rule (K-With) permits the intersection of any two types. In examples we will use it only for record-types; maybe the restriction of (K-With) to record-types has better theoretical properties, and should be preferred.

The subtyping rule (S-Inter-LB) expresses that a concatenation of two records is always a subtype of each of the records, since it has all fields that the constituents have, with the corresponding types. Together with rule (S-Empty) it replaces the rule (S-Width) of section 3. Rule (S-Inter-G) means that a record that is a subtype of two other records, must be a subtype of the concatenation of these two records, since it has all of the fields of the two records, with appropriate types. This rule can be used together with (S-Inter-LB) to derive that records with their fields in a different order are equivalent, and make rule (S-Order) of section 3 redundant in this way. Rule (S-Depth) together with rules (S-Inter-LB) and (S-Inter-G) can be used to derive the field-wise subtyping rule for records, and replace the previous (S-Depth) rule.

A record may always be extended with the empty record, since they have trivially no field in common. This is expressed by rules (♯-Empty-L) and (♯-Empty-R). Two single-field records are compatible if their field-names (labels) are different, this is rule (♯-Diff). Finally, a concatenation of two records has no fields in common with a third record if both of the first two are disjoint with the third (♯-Inter-L and -R). This completes the formalization of the predicate "no fields in common" into #. Note that we don't have a symmetry rule. The reasons for this will be given in section 2.7 and in section 4.

Finally, rule (T-With) permits the concatenation of record values. Note that we decorate the with-operator with the types of the arguments. The values will be coerced to the corresponding types before they are concatenated. The type decorations are necessary because of the subtyping. If we didn't have them every concatenation of records would be permitted because every record is of type \{\} , and \{\} \# \{\} , . This introduction rule for intersection types
seems rather unusual. However, we can see it as the combination of the standard introduction rule and a typing rule for the \texttt{with} -construction.

\[
\begin{align*}
\Gamma \vdash r_1 : R_1 & \quad \Gamma \vdash r_2 : R_2 \\
\Gamma \vdash r_1 \text{ with } R_2 r_2 : R_i & \quad i = 1, 2 \\
\therefore \quad \Gamma \vdash r_1 R_1 \text{ with } R_2 &
\end{align*}
\]

(Hint 

\[
\begin{align*}
\Gamma \vdash e : R & \quad \Gamma \vdash e : S \\
\therefore \quad \Gamma \vdash e : RS &
\end{align*}
\]

However, for practical purposes, the given rule suits us better. The equations we give here seem rather complex, compared to the previous reduction rule for records, but remember that formally these rules are not relevant and serve only to give the reader an intuition about the meaning of concatenation. The rules depend on information in the types concerning presence or absence of fields. If a field is selected, the right-most field of the record is examined (later on the reasons for this will become clear). We will start our explanation of the equations with the third one. A record \( r \) concatenated with a record of the empty type stays the same record \( r \). A record extended with one field, of which a field is selected, can be equal to two things. If the selected field is in the extension, we can forget the rest of the record. Otherwise, we can forget the extension. The last equation says \text{with} is associative, so brackets may be moved to the left. This will eventually lead to the case that the last object of concatenation is a single field record, so that the selection of a field of a record will be the value of the field, irrespective of the way the record was constructed.

Examples:

1. \( \vdash \{l: \text{Int}\} \neq \{m: \text{Char}\} \)
   \( \vdash \{l=3\} \{l: \text{Int}\} \text{ with } \{m: \text{Char}\} \{m='a'\} : \{l: \text{Int}\} \land \{m: \text{Char}\} \)
   We have constructed a record with two fields from two single-field records.

2. \( \vdash \{l: \text{Int}\} \land \{m: \text{Char}\} \neq \{n: \text{Real}\} \)
   \( \vdash \{l=3\} \{l: \text{Int}\} \text{ with } \{m: \text{Char}\} \{m='a'\} : \{l: \text{Int}\} \land \{m: \text{Char}\} \text{ with } \{n: \text{Int}\} \{n=5\} \)
   \( : \{l: \text{Int}\} \land \{m: \text{Char}\} \land \{n: \text{Int}\} \)
   This is a record with 3 fields.

3. \( \vdash \{l: \text{Int}\} \land \{m: \text{Char}\} \neq \{n: \text{Real}\} \land \{y: \text{Int}\} \)
   So it is possible to concatenate two records of two fields each.

4. \( \vdash \{l: \text{Int}\} \neq \{m: \text{Char}\} \)
   \( \vdash \{l\} \text{ with } \{m: \text{Char}\} \{m='a'\} : \{l\} \land \{m: \text{Char}\} \)
   A concatenation with the empty record.

5. \( \vdash \{l: \text{Int}\} \land \{m: \text{Char}\} \leq \{l: \text{Int}\} \land \{m: \text{Char}\} \) and vice versa, so
   \( \vdash \{l: \text{Int}\} \land \{m: \text{Char}\} \sim \{l: \text{Int}\} \land \{m: \text{Char}\} \)
   Changing the order of the fields results in an equivalent type.

6. \( R \leq \{l\} \vdash R \sim R \land \{l\} \)
   Any record type \( R \) is equivalent with \( R \) extended by the empty record.

7. \( \vdash \{l: \text{Int}\} \land \{m: \text{Char}\} \leq \{l: \text{Real}\} \land \{m: \text{Char}\} \)
   Depth subtyping of a multifield record.

8. \( \vdash \lambda R \leq \text{Topp}; R \neq \{y: \text{Int}\} \). \( \lambda r: R \). \( r \) with \( \{y=\text{Int}\} \{y=0\} \)
   \( \vdash \forall R \leq \text{Topp}; R \neq \{y: \text{Int}\} \). \( R \rightarrow (R \land \{y: \text{Int}\}) \)
   This function accepts any record type \( R \) without \( y \)-field, a record of this type, and append a \( y \)-field with value 0 to this record.

9. \( \vdash \lambda R \leq \{x: \text{Int}\}; R \neq \{y: \text{Int}\} \). \( \lambda x: R \). \( r \) with \( \{x=\text{Int}\} \{y=r.x\} \)
   \( \vdash \forall R \leq \{x: \text{Int}\}; R \neq \{y: \text{Int}\} \). \( R \rightarrow (R \land \{y: \text{Int}\}) \)
   Here the possible use of two demands on the type variable is shown.

10. We have the following equalities
    \[
    (\{l=3\} \{l: \text{Int}\} \text{ with } \{n: \text{Int}\} \land \{y: \text{Int}\} \{y=r.x\}) \quad = \quad (\{l=3\} \{l: \text{Int}\} \text{ with } \{n=5\} \{n: \text{Int}\} \text{ with } \{p=7\} \{p=7\}) \quad .
    \]
    \[
    = \quad (\{l=3\} \{l: \text{Int}\} \text{ with } \{n=5\} \{n: \text{Int}\} \text{ with } \{p=7\} \{p=7\}) \quad .
    \]
    \[
    = \quad \{l=3\} \{l: \text{Int}\} \text{ with } \{n=5\} \{n: \text{Int}\} \text{ with } \{p=7\} \{p=7\} \quad .
    \]
Now it is easy to see this system is a conservative extension of the previous system since each record can be built up from one-field records with the record concatenation. To reduce the clutter of types in big records, we introduce the following abbreviation:

**Abbreviation:**

Let all \( i \) be different labels and let \( e_i \) have type \( T_i \), then

\[
\begin{align*}
\{i_1:T_1, i_2:T_2, \ldots, i_n:T_n\} & := \\
(\{i_1:T_1\} \wedge \{i_2:T_2\} \ldots \wedge \{i_n:T_n\}) \\
\{i_1=e_1, i_2=e_2, \ldots, i_n=e_n\} & := \\
\{(i_1=e_1) \ {\mid} \ (i_2=e_2) \} \ \{(i_1:T_1,i_2:T_2)\} \ldots \ {\mid} \ \{i_n:T_n\} \ \{i_n=e_n\}
\end{align*}
\]

**Examples:**

1. \( \{i=3, m='a', n=3.5\} : \{i:\text{Int}, m:\text{Char}, n:\text{Real}\} \)
   This is the abbreviation for the term of example 2 above.

2. \( \{i=5\} \ {\mid} \ {\mid} \ {\mid} \ {\mid} \ {\mid} \ \{i:\text{Int}\} \ \{i=m:\text{Char}\} \ \{i=6, m='a'\} \).
   \( \{i=5\}.1 = \{i=5\}.1 \)

   The right record value is coerced to type \( \{m:\text{Char}\} \), so there is no conflict.

   Note that derivation rules (K-Rec), (T-Rec) and (T-Sel) and the reduction rule for records of section 2 are derivable now.

   In the following sections we will extend the compatibility rules so \( \{\} \) becomes a more powerful operation.

**Limitations:** We still have no polymorphic record update

### 2.6 Top type for #

Just as we could see ordinary quantification as a special case of bounded quantification, we can see bounded quantification as a special case of restricted quantification. In this way we can reduce the number of derivation rules again.

We add the derivation rules:

**Rules:**

\[
\begin{align*}
\Gamma \vdash R : * & \quad (\#-Top-R) \\
\Gamma \vdash R \ # \ Top & \quad (\#-Top-L)
\end{align*}
\]

**Equations:**

\[
e T \ with \ Top f = e f \ Top \ with \ T e = e
\]

**Discussion:** Now every bounded quantification can be written as restricted quantification with the restriction set to top, e.g. \( \lambda X \leq \text{Real}. e \) will be written now as \( \lambda X \leq \text{Real}; X \ # \ Top. e \). The rules (C-TVar), (K-All), (T-TAbs) and (T-TApp) of section 3 are redundant now as they can be replaced by their counterparts of section 5 with restriction set to Top. This has as a consequence that it is permitted to concatenate an arbitrary value \( x \) with a value of type Top, but this will be the same as \( x \).

The attentive reader has remarked that the rules for \( \{\} \) and Top are very similar. Indeed, Top can be seen as the intersection of zero types, which is the same as the concatenation of zero fields, i.e. the empty record. There is no need to keep them separated in this calculus, so we will define the empty record as an abbreviation.
Abbreviation:
\[ \emptyset := Top \]
\[ \{ \} := top \]

Examples:
1. \( f - (\lambda x: X. x : \forall X \leq Top; X \# Top. X \to X ) \) is the polymorphic identity
2. \( 3 \text{ Int with Top top} : \text{Int}\&\text{Top} \)
   this term is equal to 3

From now on we will add only compatibility rules. The complete system is given in appendix A.

2.7 Record updating

The polymorphic record update problem is the problem of writing a polymorphic function that has a record as argument and returns the same record with one field changed. The polymorphism means here that the function can handle different types of records, e.g. with a different number of fields. As we have seen in section 2.3, subtyping is not sufficient for such a function. This problem is a consequence of our framework being functional and not imperative.

The solution we present is to allow the concatenation operator to work as well on two records with common fields, and give then preference to the right argument. So it is possible to update a field \( f \) of a record with value \( e \), by concatenating it with the single-field record \( \{ l = e \} \). Such a concatenation is only permitted when the common fields have the same type, so the intuition for changes.

Note: \( A \# B \) means: \( A \) and \( B \) agree on common fields.

To implement this extension, we have to add a compatibility rule:

Rules:
\[
\Gamma \vdash [T] : A \quad \Gamma \vdash [\{l:T\}] \quad (\#-\text{Equal})
\]

The equality rules of section 2.5 are chosen in such a way that the right-most occurrence of the selected field is chosen.

Note: The demands \( X \leq [A] \) and \( X \# [A] \) together mean that \( X \) has an \( l \)-field of type \( A \) (and not a subtype of \( A \)). In this way, the polymorphic update can be expressed, so this pair of demands will be used a lot. More generally, \( X \leq R \) and \( X \# R \) can be interpreted as: \( X \) has all the fields of \( R \), with the same type.

Abbreviation: We write
\[
\lambda X : \# T. e \quad := \quad \lambda X \leq T; X \# T. e
\]
\[
\forall X : \# T. U \quad := \quad \forall X \leq T; X \# T. U
\]

Examples:
1. \( \vdash \{x=3\} \{x: Int\} \text{ with } \{x: Int\} \{x=6\} : \{x: Int\} \land \{x: Int\} \)
   The \( x \)-field of the \( \{x=3\} \) record is updated with 6.
2. \( \vdash \{x: Int\} \land \{x: Int\} \sim \{x: Int\} \)
   \( \vdash \{x=3\} \{x: Int\} \text{ with } \{x: Int\} \{x=6\} : \{x: Int\} \)
   In most examples we will simplify typing as much as possible.
3. \( \{x=3\} \{x: Int\} \text{ with } \{x: Int\} \{x=6\} \).
   The right value has preference above the left value.
4. \( \{x=3\} \{x: Int\} \text{ with } \{\} \{x=6\} \).
   The right record is coerced to the empty record, so the \( x \)-field has to be the left one. Note that the value of the expression \( \{x=3\} \{x: Int\} \text{ with } T \{x=6\} \) depends on the type \( T \).
5. \( \vdash \{ x=3, y='a' \} \ (x:\Int, y:\Char) \) with \( \{ x=6 \} : (x:\Int, y:\Char) \)
Here a two-field record is updated.

6. \( \vdash \{ x=3 \} \ (x:\Int) \) with \( \{ x=6, y='b' \} : (x:\Int, y:\Char) \)

7. \( \vdash \{ x=3, y='a' \} \ (x:\Int, y:\Char) \) with \( \{ x=5, z=3.4 \} \)
\( : (x:\Int, y:\Char, z:\Real) \)

8. \( \vdash \{ x=3, y='a', z=8.2 \} \ (x:\Int, y:\Char, z:\Real) \) with \( \{ x=5, z=3.4 \} \)
\( : (x:\Int, y:\Char, z:\Real) \)

9. \( \vdash \lambda p : (x:\Int). \ p \ (x:\Int) \) with \( \{ x=p.x + 1 \} \)
\( \{ x=4, y='a' \} : (x:\Int) \)
The function throws all other fields away, as it is not polymorphic.

10. \( \vdash \lambda P : (x:\Int). \ p \ (x:\Int) \) with \( \{ x=p.x + 1 \} \)
\( : (\forall P : (x:\Int). \ P \# (x:\Int) \).
\( P \to P \land (x:\Int) \)
This function performs a polymorphic record update: it increases the \( x \)-field of an arbitrary record by one. We need the demand \( P \leq (x:\Int) \) to select the \( x \)-field, and \( P \# (x:\Int) \) to change it. All other fields are preserved.

Using the abbreviation above we write
\( \vdash \lambda P : (x:\Int). \ p \ (x:\Int) \) with \( \{ x=p.x + 1 \} \)
\( : (\forall P : (x:\Int). \ P \# (x:\Int) \).
\( P \to P \land (x:\Int) \)

11. \( (x=4, y='a') = (x=5, y='a') \)
With \( ex \) we mean the term of example \( n \). Of course the \( = \) is extensional for records.

12. \( \vdash \forall P \leq (x:\Int). \ P \to P \land (x:\Int) \) where \( \forall P \leq (x:\Int). \ P \to P \)
The typing of the polymorphic update is simplified by this equivalence. As we have said in section 2.3, a function of type \( \forall X \leq T. \ X \to X \) must be an identity function, but we see here that there are interesting functions of type \( \forall X \leq \# T. \ X \to X \).

13. This extension of \( \# \) implies that the functions \( ex8 \) and \( ex9 \) of section 2.5, that were intended to extend a record with a field, also can be applied to records already having this field (with the same type). In such a case, this field will be overwritten by the function.

Discussion:

There seem to be two approaches of making record update possible. One way is to have a record concatenation operator that works for disjoint records, and a restriction operator, that deletes fields from a record. These systems are powerful, but also complex, since there are two operators that can interact in various ways. This complexity reveals itself especially in the subtyping rules. Furthermore, we don’t need this power, because there is no need for record restriction in its own right.

Another approach, the one we have chosen here, is a record concatenation that gives precedence to the right argument for common fields, and a restriction operator, that deletes fields from a record. These systems are powerful, but also complex, since there are two operators that can interact in various ways. This complexity reveals itself especially in the subtyping rules. Furthermore, we don’t need this power, because there is no need for record restriction in its own right.

2.8 Specialized record updating

For certain uses, it is desirable to update not only with the same type, but also with a subtype. E.g. a record with an \( x \)-field of type \( \Real \) can be updated by an \( \Int \), because an integer can be converted to a real. This demands a generalisation of the \( (\#-\Equal) \) rule, so we have \( R \# S \) if on common fields \( S \) is a subtype of \( R \).

Rules:

\[
\Gamma \vdash U \leq T \\
\Gamma \vdash \{ U \} \# \{ U \} \quad (\#-\Equal)
\]
(this rule makes the old rule (#-Equal) redundant)

Examples:
1. \{x=5.4, y='a'\} \{x:Real, y:Char\} with \{x:Int, y:Char\} \{x=3\}
2. \{x=5.4, y='a'\} \{x:Real, y:Char\} with \{x:Int\} \{x=3\}, x = 3
3. Again functions ex8 and ex9 of section 2.5 can be applied to a wider class of records.

Discussion:
The types in the premise cannot be swapped, because this would violate the typing rules or the 'preference to right' meaning of with. This can be clarified by giving an example. Suppose we have the rule
\[ \Gamma, T \leq U \vdash \{x: Int\} \# \{y: Int\} \] (\#-?)
Then the following term would be permitted:
\[ \Gamma \vdash \{x: Int\} \{x=3\} \{x: Real\} \{x=5.4\} \] with
The 'preference to right' rule, the x-field of this term is equal to 5.4 (a real). However, this is in contradiction with rule (S-Inter-LB), that says the term should be convertible to \{x: Int\}, which is clearly not the case any more. So we can't admit rule (\#-?).

Note: The two demands \(X \leq \{x: Int\}\) and \(X \# \{y: Int\}\) can now be summarized by "X has an l-field with type equivalent to Int"

2.9 Transitivity
Suppose we have two functions updating a different field of a record:
\[ \text{changeX} = \lambda R \leq \# \{x: Int\}, r: R \rightarrow R \text{ with } \{x: Int\} \{x=r.x + 1\} \]
\[ \text{changeY} = \lambda R \leq \# \{y: Int\}, r: R \rightarrow R \text{ with } \{y: Int\} \{y=r.y - 1\} \]
We might want to define the function that performs both updates on a record that has both an x and a y-field like this:
\[ \text{changeXY} = \lambda R \leq \# \{x: Int, y: Int\}, r: R \rightarrow R \text{ with } \{x: Int\} \{x=r.x + 1\} \]
\[ \{y: Int\} \{y=r.y - 1\} \]
In OOP, functions would be frequently defined in such a way. Unfortunately, this function is not permitted (typable) with the current rules, because we can't derive:
\[ R \# \{x: Int, y: Int\} \vdash R \# \{x: Int\} \]
We remedy this situation by adding the rule:

Rules:
\[
\frac{\Gamma \vdash R \leq S \quad \Gamma \vdash S \leq T}{\Gamma \vdash R \# T} \quad (\#-\text{Trans})
\]

Discussion:
To understand this we have to remember what it means that types R and S are compatible and in the subtype relationship: recordtype R has all of the fields of S with the same type. If the same holds for S and T, then we clearly have that R has all of the fields of T with the same type, so R must be compatible with T.

With this rule it is permitted to define function changeXY as we did above. The rule (\#-\text{Trans}) is used twice for typing it: once to derive \(R \# \{x: Int\}\), and once to derive \(R \# \{y: Int\}\).

Examples:
1. \(R \leq \text{Top}; R \# \{x: Int, y: Int\} \vdash R \# \{x: Int\}\)
2.10 Recursive record update

A special form of the update problem is the so-called deep or recursive update. This is an update that takes place "deep" in a nested record, e.g. the update of the \( m \)-field of the \( l \)-field of a record of type \( \llbracket \{ l: \text{Int} \} \rrbracket \). We don't need this update in our model of OOP, so this section is not important for that goal. With the operations defined it is possible to perform such a deep update, but only in a very clumsy way:

\[
\lambda S \leq \# \{ m: \text{Int} \}. \quad \lambda R \leq \# \{ l: S \}. \quad \lambda r: R.
\]

\[
\{ l= r. I \} S \text{ with } \{ m: \text{Int} \} \{ m=1 + r.l.m \}
\]

We will generalize our compatibility rules and add a subtyping rule to make such an update easier:

Rules:

\[
\Gamma \vdash U \leq T \quad (\# \text{-Sub})
\]

\[
\Gamma \vdash T \neq U \quad (\# \text{-Equal})
\]

\[
\Gamma \vdash U \llbracket \{ l: (T \wedge U) \} \rrbracket \wedge U \leq \llbracket U : (T \wedge U) \rrbracket \quad (\text{S-Label-Distr})
\]

(If it is easy to see that the old rule (\#-Equal) is redundant now.)

Discussion:

The equality rules given in section 2.5 do not suffice any longer; the equality can depend on subtyping judgments. Only a full equational calculus can help here. All examples of the previous sections will remain valid, so the intuition gained there can be used here. The concatenation we have here is called recursive, because we have for compatible record types \( R \) and \( S \):

\[
\{ l=r \} \{ l: R \} \text{ with } \{ l: S \} \{ l=s \} = \{ l=(r \text{ with } s) \}
\]

This is to say: Suppose we have two records \( a \) and \( b \) that have a field \( I \) in common that contains in both cases another record, \( r \) and \( s \) respectively. Then the contents of the \( l \)-field of \( a \) and \( b \) concatenated will be the concatenation of \( r \) and \( s \). This corresponds to rule (\#-Equal). Rule (\#-Sub) covers the base case, where two types are (almost) the same, and permits the overwriting of the left value by the right value.

Already derivable in our system is

\[
\llbracket U: (R \wedge S) \rrbracket \leq \llbracket U: R \rrbracket \wedge \llbracket U: S \rrbracket
\]

so together with (S-Label-Distr) we have

\[
\llbracket U: (R \wedge S) \rrbracket \sim \llbracket U: R \rrbracket \wedge \llbracket U: S \rrbracket
\]

We need this equivalence for instance when typing the equation above or the selection of a field of a concatenated record (example 5 below).

Examples:

1. \( \vdash \{ l=\{ m=4, n='a' \} \} \{ l: \llbracket m: \text{Int}, n: \text{Char} \rrbracket \} \text{ with } \{ l: \llbracket m: \text{Int} \rrbracket \} \{ l=\{ m=5 \} \}
   
   \begin{align*}
   & : \llbracket l: \llbracket m: \text{Int}, n: \text{Char} \rrbracket \rrbracket \wedge \llbracket l: \llbracket m: \text{Int} \rrbracket \rrbracket \\
   & \text{This is a deep update.}
   \end{align*}

2. ex1.1. \( m = 5 \)

3. \( \vdash \{ l=\{ n='a' \} \} \{ l: \llbracket n: \text{Char} \rrbracket \} \text{ with } \{ l: \llbracket m: \text{Int}, p: \text{Real} \rrbracket \} \{ l=\{ m=4, p=3.14 \} \}
   
   \begin{align*}
   & : \llbracket l: \llbracket n: \text{Char} \rrbracket \rrbracket \wedge \llbracket l: \llbracket m: \text{Int}, p: \text{Real} \rrbracket \rrbracket \\
   & \text{A recursive concatenation.}
   \end{align*}

4. \( \vdash \{ l: \llbracket n: \text{Char} \rrbracket \} \wedge \{ l: \llbracket m: \text{Int}, p: \text{Real} \rrbracket \} \sim \{ l: \llbracket m: \text{Int}, n: \text{Char}, p: \text{Real} \rrbracket \rrbracket \)
   
   \begin{align*}
   & \text{using (S-Inter-\ With)}
   \end{align*}

5. \( \vdash \text{ex3.1} : \{ l: \llbracket m: \text{Int}, n: \text{Char}, p: \text{Real} \rrbracket \rrbracket
   
   \begin{align*}
   & \text{this uses the previous equivalence}
   \end{align*}
6. \( \vdash \lambda R \leq \# \{l:\{m: Int\}\} \). \( \lambda R. r \in R \) with \( \{l:\{m: Int\}\} \) \{l=m=r.l.m+1\} \)
   \( VR \leq \# \{l:\{m: Int\}\} \). \( R \rightarrow R \)
   this function increases the \( m \)-field of the \( l \)-field and preserves all other fields. This example is adopted from [CM 91].

7. \( \vdash \text{ex6} \{l:\{m: Int, n: Char\}, p: Real\} \{l=m=4, n='a', p=3.14\} \)
   \( \{l:\{m: Int, n: Char\}, p: Real\} \)

8. \( \text{ex7} \cdot \cdot \cdot = 5 \)

9. \( \vdash \text{Int with Int} 5 : \text{Int} \land \text{Int} \)
   this is an unintended but harmless consequence of the new compatibility rules: records, however deep, can be updated. Specifically, records of depth zero, i.e. no records at all, can be updated.

10. \( \text{Int with Int} 5 = 5 \)
    still preference to right.

2.11 Conclusion
We have presented the syntax and derivation rules of \( \mathcal{F}_\# \), by, starting with \( \mathcal{F} \), extending the set of rules in each section. Since many rules have become redundant, the final rules are put together in Appendix A. We have shown that the system elegantly solves the problem of record update, with a quite general concatenation operator.

There are variations of \( \mathcal{F}_\# \), where not all rules presented in sections 2.7-2.10 are used, e.g. the system with only the rules of sections 2.7 and 2.9 added to the basic rules is strong enough to model OOP as we do in section 3. There are also variations that include a rule for symmetry of \( \# \) (we then have to dispose specialised record updating, as discussed there).

3 Object Oriented Programming
In this chapter we will show how certain concepts of object oriented programming (OOP) can be modelled in \( \mathcal{F}_\# \). First we will give a quick introduction to some ideas of OOP, and give an example program. Then we will show briefly how these ideas can be modelled, some in \( \mathcal{F}_\# \), and some in extensions of \( \mathcal{F}_\# \). From section 3.1 onwards we will show how the example program will be translated to increasingly faithful and complex models.

The most important concepts of object-oriented programming are object, class, method and inheritance. Every object has a state and a collection of methods that are transformations on the state. Objects are grouped into classes. All objects in one class have the same methods and the same type of state. So a class describes the methods and the type of the state, and an object is defined by its class and the state. The state consists of a number of instance variables, that have some value. Instance variables of an object are comparable to fields of a record in more traditional languages.

A class may be defined independently, but also as an extension of an existing class. The new class is called a subclass of the old class, the superclass. A subclass may have more instance variables or more methods, and typically has both. The subclass only has to specify what it has more than the superclass, the rest of both state and methods is inherited. Methods can be inherited because objects of a subclass have all instance variables of objects of the superclass, so methods that work for objects of a superclass will also work for objects of the subclass. Sometimes a subclass redefines existing methods. A subclass may also have more superclasses, this idea is called multiple inheritance. In this way a whole class-hierarchy can be defined.

Another important concept is encapsulation: The state of an object can be reached only through its methods. OOP has this feature in common with the practice of abstract datatypes. The last major concept is that of self-reference: A method applied to an object may invoke other methods that are defined on this object. This encourages separation of tasks. There are different possibilities to determine which method is actually invoked, as we will see later on.

We have in figure 1 a small object oriented program in a functional OO language, derived from [PT 93]. Normally object-oriented languages are imperative, but a functional variant suits our purposes better. We will clarify the concepts introduced above with this example.
class Point is
  vars x:Int=0
with
  getx = state<>x,
  setx = fun i:Int. state<>x=i,
  bump = self.setx state (i+ (self.getx state))
end

class 2DPoint from Point is
  vars y:Int=0
with
  gety = state<>y,
  sety = fun i:Int. state<>y=i,
  bump = let state' = super.bump state in
    self.sety state' (i+ (self.gety state))
end

class Colour is
  vars c:String="red"
with
  getc = state<>c,
  setc = fun col:String. state<>c=col
end

class CPoint from Point, Colour is
with
  setx = fun i:Int. let state' = superi.setx state i in
    self.setc state' "blue"
end

Figure 1: An example of object oriented programming
The first lines define the class `Point`. An object in this class will represent a point on the line, that can be moved or bumped. The second line declares that there is just one instance variable, `x`, with initial value 0.

The rest of the class describes the methods of `Point`. The first method delivers the x-component of the state of a point, a method does not need to deliver an object. The abstraction over the point is implicit here, in contrast to pure functional languages. However, we are explicit in which state has to be examined, in contrary to imperative OO languages. This is a consequence of the absence of side-effects. The second method has the intention of moving the point to another place. Here is abstracted from the place, and a new point is returned. It is a copy of the old state, but with the x-component changed to 1. Again, in an imperative language we would just change an instance variable. The third method bumps a point. For this class it means that the x-coordinate is increased by one. It does so by invoking the other methods defined on points. This self-reference is denoted by prefixing the method’s name by “self.”, and is applied to a state.

Now a simple example of the use of this class can be given. We will assume that the program text of figure 1 is already read in by the interpreter. The expressions given to the interpreter are preceded by #; the output is given right under each expression.

```plaintext
# getX (bump point 'new)
1 : Int
```

The only remarkable thing is the function `point 'new`, which is implicitly defined when the class `Point` was declared, and delivers a new `Point` object with initial state as specified in the class.

```plaintext
The class 2DPoint will consists of movable points in the plane. We define it as a subclass of `Point`, so it has an instance variable x in the state, and all the methods of `Point`. It adds an instance variable y, and two new methods. The bump method is redefined, but it still makes use of the old version by calling super.bump. In this definition we also see why we have to specify on which state methods must act.

The bump method applied to a point in the plane will change both coordinates:
```
```
```plaintext
# getY (bump 2dpoint 'new)
1 : Int
```

Still the methods of `Point` can be applied, without disturbing any other information:

```plaintext
# getY (setX (setY 2dpoint 'new 7) 5)
7 : Int
```

Next we will demonstrate multiple inheritance. First we define another base class, `Colour` (a base class is a class without superclasses). The class `CPoint` has all the instance variables and methods of both `Point` and `Colour`, and adds nothing. It only redefines the `setX` method so that the colour is changed to blue every time a point is moved.

Now a question arises around the self-reference in the definition of bump. When this method is applied to a `CPoint`, will `self.setX` refer to the `setX` of class `Point` (and not change the colour), or to the `setX` of `CPoint` (and change the colour to blue)? In every object-oriented language this question appears. Most languages (e.g. Smalltalk) have chosen the last option as this is the most flexible. Our more advanced models will also model this so-called late-binding, and give the result:

```plaintext
# getC (bump cpoint 'new)
"blue" : String
```

We give one by one the concepts of OOP that we will model in the following sections, and for each concept the extension of the model to incorporate the new concept is given.

1. Objects and methods (without inheritance)
   - An object is modelled by a record, with a field for every instance variable. So we represent an object by just the state. A method is a global function that returns a new state.

2. The inheritance of instance variables. As a consequence, methods of a superclass K can read and modify an object of a subclass L.
The recordtype $B$ of objects of a subclass $L$ is an extension of the recordtype $A$ of objects of the superclass $K$. Consequently, we have $B<A$ and $B#A$, so functions that can read and modify $A$’s (these functions represent methods of the superclass $K$), can read and modify $B$’s (i.e. objects of $L$).

3. The inheritance of methods. When not explicitly redefined, a method is copied from its superclass. A method can refer to the methods of the superclass (super-reference).

$\Rightarrow$ The functions that represent the methods are packed in one record. The functions of the superclass are copied to the subclass by the with-construction. We will need type operators as in $F^\omega$.

4. Encapsulation. An object can be reached only through its methods.

$\Rightarrow$ The state and the methods are packed together in an object and the abstract datatype mechanism prevents the state from direct access. Existential types are needed.


$\Rightarrow$ The set of methods gets as extra parameter self. When an instance of the class is created, the record of functions representing the own methods is substituted for self. To implement this, we need a fixpoint combinator.

In the following sections we will further explain the modelling of the concepts above with the translation of the example OO program to a programming language based on $F^\omega$. The language is extended with transparent definitions (global and local) and some standard types. Furthermore, the notation is a little different: $\lambda$ and $\forall$ are written instead of $\text{fun}$ and $\text{all}$. The conventions about the program text are the same as before.

In the first section, we give an extremely poor translation of the program, as we only model concept 1. In each section we will model one more concept of the list above, so the model of OOP in section 3.5 is fairly complete.

### 3.1 Objects and methods

In this section we will give a very poor model of OOP; Objects and methods are modelled, but inheritance is not. We represent an object by a record with one field for each instance variable. So an object is solely represented by its state, not its methods. The state of a Point is a record with an $x$-field containing an integer:

```
# PointR = {lx: Int}
PointR : *
```

We have as convention that a state type ends with $R$ (for representation type). The methods are translated as global functions:

```
# getX = fun s:PointR. s.x
getX : PointR -> Int

# setX = fun s:PointR. fun i: Int. (x=i)
setX : PointR -> Int -> PointR

# bump = fun s:PointR. setX s (1+ getX s)
bump : PointR -> PointR
```

The functions get an extra parameter representing the state. This parameter is implicit in figure 1. Note that we resolved the self-references of the example program by giving the definitions in a specific order. In general, this doesn’t work (cross-dependencies), and we need the fixpoint combinator to resolve the mutual recursive definitions. To complete the class, we give the start object, so we can use our functions$^1$.

```
# point'new = {x=0}
point'new : PointR

# p1 = bump point'new
p1 : PointR
# getX p1
1
```

$^1$The ‘ has no special meaning; it is considered to be a letter.
We cannot extend the definitions we have given before to make a class of two dimensional points. We have to start all over again, and give for each method again a definition.

```fsharp
# 2DPointR = {x: Int, y: Int}
2DPointR : *
# 2dgetX = fun s:2DPointR. s.x
2dgetX : 2DPointR -> Int
# 2dsetX = fun s:2DPointR. fun i: Int. {x = i, y = s.y}
2dsetX : 2DPointR -> Int -> 2DPointR
# 2dgetY = fun s:2DPointR. s.y
2dgetY : 2DPointR -> Int
# 2dbump = fun s:2DPointR. let s' = 2dsetX s (1 + 2dgetX s) in
# 2dsetY s' (1 + 2dgetY s')
2dbump : 2DPointR -> 2DPointR
# 2dpoint'new = {x = 0, y = 0}
2dpoint'new : 2DPointR
```

Functions that work on points can be used for 2dpoints, but that results in loss of information.

```fsharp
# p2 = 2dgetY (2dbump 2dpoint'new)
Type error
```

Since inheritance is not yet implemented, it isn't particularly interesting to give the translation of the classes Colour and CPoint here, so we will not do so. For this model only the simply typed calculus extended with records is needed.

### 3.2 Inheritance of instance variables

In this section, we will give a model implementing the most crucial aspect of OOP: An object of a subclass may be used in any place where an object of the superclass is used.

This is possible because instance variables are inherited, i.e. a subclass always has all the instance variables the superclass has. A subclass doesn't have to name all instance variables it inherits, but name only the variables it *adds*. We can model this in F# by record concatenation.

```fsharp
# PointR = {x: Int}
PointR : *
# 2DPointR = PointR \ {y: Int}
2DPointR : *
```

Now we are justified in demanding that a function that works on Points, also works on 2DPoints, since "everything you do with a point can also be done with a 2dpoint". The functions given in section 3.1 do not satisfy this demand. We have to make them *polymorphic*. We might try to make a polymorphic `getX` function by

```fsharp
# try-getX = fun FinalR*: fun s:FinalR. s.x
Type Error
```

Obviously, this doesn't work because it isn't ensured that `s` has an `x`-field. By allowing only types `FinalR` that are a subtype of `PointR` we can type the body of the function (in programs we write `<` for `⊆`):

```fsharp
# try2-getX = fun FinalR<PointR. fun s:FinalR. s.x
try2-getX : all FinalR<PointR. FinalR->Int
```

We have `PointR<PointR`, so `try2-getX` accepts points, but also `2DPointR<PointR`, so it accepts 2dpoints as well. Now we move to the `setX` method.

```fsharp
# try-setX = fun FinalR<PointR. fun s:FinalR. fun i: Int. {x = i}
try-setX : all FinalR<PointR. FinalR->Int->PointR
```
This is not the desired typing, since it returns a PointR instead of a FinalR. We now have the update problem (see section 2.7). This is solved with the with-construction, yielding 2

```plaintext
# try2-setX = fun FinalR<#PointR. fun s:FinalR. fun i:Int.
  s FinalR with {Ix:Int} {x=i}
try2-setX : all FinalR<#PointR. FinalR->Int->FinalR
```

Here we demand that the state type of the object is compatible with PointR, so that it is permitted to update the object with a value of type PointR. We have PointR<#PointR, so try2-setX can be applied to points, and 2DPointR<#PointR, so the function can be applied to 2dpoints as well.

Thus we demand FinalR<#PointR to ensure we can read the object as if it were a point, and FinalR<#PointR to ensure we can update the object as if it were a point (update in the functional sense of course).

Now we give the uniform representation of all methods.

```plaintext
# getX = fun FinalR<#PointR. fun s:FinalR. s.x
getX : all FinalR<#PointR. FinalR -> Int

# setX = fun FinalR<#PointR. fun s:FinalR. fun i:Int.
  s FinalR with {Ix:Int} {x=i}
setX : all FinalR<#PointR. FinalR -> Int -> FinalR

# bump = fun FinalR<#PointR. fun s:FinalR.
  setX FinalR s (1+(getX FinalR s))
bump : all FinalR<#PointR. FinalR -> FinalR
```

To complete the class, we give start objects, so we can use our functions. Again, we use the record concatenation, this time to inherit the initial value of an object.

```plaintext
# point 'new : PointR
point 'new : PointR

# 2dpoint 'new : 2DPointR
2dpoint 'new : 2DPointR

# p1 = bump PointR point 'new
p1 : PointR

# p2 = bump 2DPointR 2dpoint 'new
p2 : 2DPointR
```

Now we have successfully modelled inheritance of instance variables and the use of methods of a superclass for objects of a subclass. To complete the class 2DPoint, we give its methods.

```plaintext
# getY = fun FinalR<#2DPointR. fun s:FinalR. s.y
getY : all FinalR<#2DPointR. FinalR -> Int

# setY = fun FinalR<#2DPointR. fun s:FinalR. fun i:Int.
  s FinalR with {y:Int} {y=i}
setY : all FinalR<#2DPointR. FinalR -> Int -> FinalR

# bump2 = fun FinalR<#2DPointR. fun s:FinalR.
  let s' = bump FinalR s in
  setY FinalR s' (1+(getY FinalR s))
bump2 : all FinalR<#2DPointR. FinalR -> FinalR
```

To type the body of the function `getY`, FinalR<#Int has to be derived. This is done by using transitivity of subtyping and 2DPointR<#Int. In the same way we use the transitivity law for #, to type the `setY` function. In typing `bump2`, both laws are used.

We have to give the `bump` method for two-dimensional points another name than the `bump` method for one-dimensional points, since the methods are global functions, and not

---

2We have an "intelligent" interpreter, that always gives the shortest minimal type.
packed with the instance variables in the object. This is clearly a disadvantage of this simple model of objects and classes.

Some examples that illustrate the difference between the various bump functions:

```fsharp
# getY 2DPointR (bump 2DPointR 2dpoint'new)
0 : Int
# getY 2DPointR (bump2 2DPointR 2dpoint'new)
1 : Int
```

Now we will show how multiple inheritance is modelled. First we define the other base class: Colour.

```fsharp
# ColourR = {lc: String!}
ColourR : =
# getC = fun FinalIR<#ColourR. fun s:FinalIR. s.c
getc : all FinalIR<#ColourR. FinalIR -> ColourR
# setC = fun FinalIR<#ColourR. fun s:FinalIR. fun col:String.
# s FinalIR with {lc: String!} {c=col}
setc : all FinalIR<#ColourR. FinalIR -> ColourR -> FinalIR
# colour'new = {c="red"}
colour'new : ColourR

Now we combine the class Point and Colour in one class of coloured points, to which all methods of both classes are applicable.

```fsharp
# CPointR = PointR \ ColourR
CPointR : =
# cpoint'new = point'new PointR with ColourR colour'new
cpoint'new : CPointR
```

Observe that we have that CPointR is a subtype of and compatible with both PointR and ColourR, so the elements of CPointR can be used everywhere where an element of PointR or ColourR can be used.

We define a bump method for coloured points, that bumps it as a point, and sets the colour to blue:

```fsharp
# setX2 = fun FinalIR<#CPointR. fun s:FinalIR. fun i: Int.
# setC FinalIR (setX FinalIR s i) "blue")
setX2 : all FinalIR<#CPointR. FinalIR -> FinalIR

# p1 = setX2 CPointR cpoint'new 3
p1 : CPointR
# getX CPointR p1
3
# getC CPointR p1
"blue"

But the bump function always uses setX, and not setX2 as is desirable for coloured points:

```fsharp
# getC CPointR (bump CPointR cpoint'new)
"red"
```

In this section we have shown that it is possible to give a simple model of classes and inheritance in F#.

This model has some important shortcomings. The most important one is that methods are not packed in the objects, but are separate functions. This has as a consequence that every time a class redefines a method a new name has to be chosen, and programs have to be explicit about which version of a method is used. This can result in undesired behaviour, as we see with the bump method of the class 2DPoint.

### 3.3 Inheritance of methods

Inheritance of methods is the mechanism that defines all methods of a subclass that are not redefined, to be equal to the corresponding methods of the superclass. We model this by first packing all methods together in a record. Now the combination of the methods of the
superclass and the methods of the subclass, is done with the \textit{with}-construction. An added advantage of packing the methods together is that later on, the state and the methods can easily be put together.

Extension of language

To implement this aspect of inheritance, type operators are very convenient, if not necessary. Type operators are functions from types to types, and are admitted in higher order type systems [Gir 72]. These operators are used here to indicate which methods a class has, i.e. to give the \textit{interface} of a class. So we assume we have a higher order type system instead of second-order. The resulting system is very close to Compagnoni’s $P^+_A$[Com 95], to which compatibility is added.

The subtyping and compatibility rules are extended point-wise for type operators:

\[
\frac{\Gamma, \forall X : * . S \leq T}{\Gamma \vdash \lambda X : * . S \leq \lambda X : * . T} \quad \text{(S-Oper)}
\]

\[
\frac{\Gamma \vdash S \leq T \quad \Gamma \vdash S U : *}{\Gamma \vdash S U \leq T U} \quad \text{(S-App)}
\]

\[
\frac{\Gamma, \forall X : * . S \# T}{\Gamma \vdash \lambda X : * . S \# \lambda X : * . T} \quad \text{(#-Oper)}
\]

\[
\frac{\Gamma \vdash S \# T \quad \Gamma \vdash S U : *}{\Gamma \vdash S U \# T U} \quad \text{(#-App)}
\]

That is, a type operator $S: \rightarrow *$ is a subtype of type operator $T$ iff for all types $U$ we have $S U \leq T U$, and likewise for compatibility of type operators. The intersection of type operators is also defined pointwise:

\[(\lambda X : * . S) \wedge (\lambda X : * . T) := (\lambda X : * . S \wedge T)\]

The model

We put all methods in a record, where the field name corresponds to the name of the method. As all functions are polymorphic, we push the type abstraction outside the record.

\[
\text{# PointR} = \{l: \text{Int}\}
\]

PointR : *

\[
\text{# pointclass} =
\text{# fun FinalR<#PointR.}
\]

\[
\text{# getX = fun s:FinalR. s.x,}
\]

\[
\text{# setX = fun s:FinalR. fun i:Int. s FinalR with \{l: \text{Int}\} \{x=i\},}
\]

\[
\text{# bump = fun s:FinalR. s FinalR with \{l: \text{Int}\} \{x=s.x+1\}}
\]

pointclass : all FinalR<#PointR. \{getX: FinalR->Int, setX: FinalR -> Int->FinalR, bump: FinalR->FinalR\}

We have the naming convention that the collection of methods of class C is called Cclass. Remarkable is the change in the body of bump: The previous definition used functions getX and setX, but since all functions are put in one record, we can’t do this anymore. Therefore the definitions of these two methods have to be substituted, which is bad programming practice. This will be recovered in section 3.5 by introducing self-reference.

This set of methods is used in the following way:

\[
\text{# point'new : PointR}
\]

point'new : PointR

\[
\text{# p1 = (pointclass PointR).setX point'new 5}
\]

p1 : PointR

\[
\text{# (pointclass PointR).getX p1}
\]

5 : Int

We can still get direct access to the object:
We can give pointclass a much shorter type if we define the interface of Points, that is, the set of methods abstracted from the representation.

```haskell
PointM : *->*
```

The typechecker responds with saying that PointM is a function from types to types. We use the name CM for the interface of class C. Now we have:

```haskell
# check pointclass : all FinalR<#PointR. PointM FinalR
Yes
```

This construction with an interface is useful below.

Abstracting from the interface and the representation, we get a general class constructor:

```haskell
# Class = fun M:*-->*. fun R:* . all FinalR<#R. M R
Class : (*/-->*)-->*/
# check pointclass : Class PointM PointR
Yes
```

We start the treatment of 2DPoint by giving the interface for the subclass:

```haskell
# 2DPointM = PointM \/
2DPointM : *->*
```

The type operator 2DPointM is the extension of PointM with another type operator. We have that 2DPointM is equivalent to:

```haskell
fun Rep:* . {getX: Rep->Int, setX: Rep->Int->Rep,
```

Now the methods of class 2DPoint are defined in terms of the methods of its superclass: some methods use in their body the methods of the superclass, whilst methods that are not named are copied from pointclass.

```haskell
# 2DPointR = PointR \/
{ly:Int!}
2DPointR : *
# 2dpointclass =
# fun FinalR<#2DPointR.
# 2dpointclass =
# fun FinalR<#2DPointR.
# let super = pointclass FinalR in
# super (PointM FinalR) with
# {getField: FinalR->Int, setField: FinalR->Int->FinalR, bump: FinalR->FinalR!}
# {getField: fun s:FinalR. s.*,
# setField: fun s:FinalR. fun i:Int. s FinalR with {ly:Int!} {x=i},
# bump: fun s:FinalR. let s' = super.bump s in
# s' FinalR with {ly:Int!} {y=s'.y+i}}
```

```haskell
2Dpointclass : Class 2DPointM 2DPointR
```

The record concatenation operator with is used to extend the record with the fields getField and setField, and to overwrite the field bump. Here the full power of with is used, whereas in the bodies of methods it is only used to perform an update. Note that we need the type operator PointM to type super in this concatenation.

We now have only one name for the bump method, but we have to select the right class:

```haskell
# 2dpointnew = pointnew PointR with {ly:Int!} {y=0}
2dpointnew : 2DPointR
```

```haskell
# p1 = (2dpointclass 2DPointR).bump 2dpointnew
p1 : 2DPointR
# (2dpointclass 2DPointR).getY p1
1
# p2 = (pointclass 2DPointR).bump 2dpointnew
p2 : 2DPointR
# (2dpointclass 2DPointR).getY p2
0
```

---

3 This is an example of a type operator that accepts a type operator as argument.
For reasons of brevity, we will not give the code for multiple inheritance.

In this section we have shown our system is powerful enough to implement the concept of inheritance of methods, if it is extended with type operators. We model this form of inheritance by interpreting the set of methods by a record and inheritance by record concatenation. So we use `with` here in two different situations: In methods to provide a polymorphic record update, and in classes, to provide inheritance of methods.

### 3.4 Encapsulation

The feature added to the model of the previous section is encapsulation. Encapsulation is the idea that an object can only be accessed through its methods. To implement this, we need to pack the state and methods together and apply a mechanism that hides the state.

In the literature two mechanisms for encapsulation have appeared: *procedural abstraction* (using recursive records, see e.g. [Car 88]) and *type abstraction*. Following [PT 93], we choose for type abstraction, which is formalized in the context of lambda-calculi by *existential types* [MP 88]. The rules for forming, introducing and eliminating an existential type are

\[
\begin{align*}
\Gamma, X: \tau & \vdash U : \sigma \\
\Gamma & \vdash \exists X: \tau. U : \exists \sigma \\
\end{align*}
\]

where we have written \(\exists\) for existential types. It is possible to define existential types in terms of universal (or polymorphic) types, so this is a very harmless extension of the system.

With the interface constructor, we can now pack state and methods together in a record, and encapsulate this to form the type of point objects (writing `some` for \(\exists\)):

```lisp
PointM : *->*
```

Abstracting from the interface, we get the following higher order type operator:

```lisp
# Object = fun M:*->*. some Rep:*. { lstate:Rep, methods:M Rep }
Object : (*->*)->*
```

When supplied with some interface, `Object` yields the types of objects with that interface. Now the type `Point` can be expressed more concisely as:

```lisp
# check Point = Object PointM

Yes
```

We are now in a position to define the class `Point` in this model. The interface and object-type are already given, so we will go to the methods. Because of the encapsulation, the implementation of an application of a method can be quite verbose. Therefore we introduce for every method a function that applies this method to an object. This function has to remove the encapsulation, select the right method, apply that to the state, and encapsulate the result with the unchanged methods. A naive implementation of the invocation of the `bump` method might be:

```lisp
# try-bump = fun p:Point. open p as Rand r in
    pack R and {state=r.methods.bump r.state, methods=r.methods} to Point
try-bump : Point -> Point
```

This is perfectly all right for points, but doesn't take subtyping into account: `try-bump` applied to a value of a subtype of `Point` always returns a `Point`, effectively throwing away the rest of the state and the methods. The correct solution for this problem is again using bounded quantification (method `m` of class `A` is denoted by `A'm`).
Point'bump = fun M:PointM. fun p:Object M. open p as R and r in pack R and {state=r.methods.bump r.state, methods=r.methods} to Object M

Point'bump : all M:PointM. Object M -> Object M

The higher order bounded quantification guarantees that the object has an interface at least as refined as PointM, so the bump method is present in an object with that interface. The code for the invocation of the setX method is similar, getX doesn't return an object and is even simpler.

point'setX = fun M:PointM. fun p:Object M. fun i:Int. open p as R and r in pack R and {state=r.methods.setX r.state, methods=r.methods} to Object M

point'setX : all M:PointM. Object M -> Int -> Object M

# point'getX = fun M:PointM. fun p:Object M. open p as R and r in r.methods.getX r.state

point'getX : all M:PointM. Object M -> Int

Noteworthy is that we don't have to demand M#PointK as we did for the state of an object, where we had FinalR#PointR; FinalR#PointR. This means we can actually have method specialisation, e.g. a subclass has a method that delivers an Int where the same method of the superclass delivers a Real. We cannot have "instance variable specialisation", i.e. a subclass has an instance variable with as type a proper subtype of the type of the same variable in the superclass, which would be unsound. Here we see a big difference between the state of an object and the methods of an object, in contrary to models of OOP with recursive records, where there is not such a big distinction between both concepts.

Up to now, we haven't said anything about the actual representation of a point, but only which interface a point has. Let's turn towards one possible representation of points:

# PointR = {Ix:lntl}
PointR : •

pointrep'new = {x=0}
pointrep'new : PointR

There is no change in the definitions of Class and pointclass, but the code for making a new object is new. The initial value and the methods are wrapped up to an existential type.

# Class = "The same as in the previous section"
Class : (->*)->*->.

pointclass = "The same as in the previous section"
pointclass : Class PointM PointR

# point'new = pack PointR and
# {state = pointrep'new, # methods = pointclass PointR}
# to Point
point'new : Point

We can make an abstracted version of new:

# new = fun M:*->*. fun R:*. # fun cl:Class M R:. # pack R and # {state = init, # methods = c1 R} # to Object M
new : all M:*->*. all R:*. Class M R -> R -> Object M

new applied to an interface, a representation type, the set of methods and an initial value delivers an object.

Now it is easy to use this machinery, and not possible to abuse objects:

# Point'getX PointM (Point'bump PointM point'new)
1 : Int
# point'new.x
Type error
The introduction of the subclass of two-dimensional points is straightforward:

\[
\begin{align*}
\textbf{2DPointM} &= \textbf{PointM} \setminus \{\text{fun } \text{Rep} : \text{Rep} \to \text{Int} \}, \text{setY} : \text{Rep} \to \text{Int} \to \text{Rep}! \}
\end{align*}
\]

\[
\begin{align*}
\textbf{2DPoint} &= \textbf{Object} \textbf{2DPointM} \\
\textbf{2DPoint} &= \ast
\end{align*}
\]

\[
\begin{align*}
\text{2dpoint}'\text{getY} &= \text{fun } \text{M<2DPointM}. \text{fun } \text{Object } \text{M}. \text{open } \text{p as R and r in } r.\text{methods}.\text{GetY } r.\text{state} \\
\text{2dpoint}'\text{setY} &= \text{fun } \text{M<2DPointM}. \text{fun } \text{i:Int}. \text{open } \text{p as R and r in } \text{pack } \text{R and } \{\text{state}=r.\text{methods}.\text{setY } r.\text{state } i, \text{methods}=r.\text{methods}\} \to \text{Object } \text{M} \\
\text{2dpoint}'\text{getY} &= \text{all } \text{M<2DPointM}. \text{Object } \text{M} \to \text{Int} \\
\text{2dpoint}'\text{setY} &= \text{all } \text{M<2DPointM}. \text{Object } \text{M} \to \text{Int} \to \text{Object } \text{M} \\
\end{align*}
\]

Observe that we have \textbf{2DPointM}<\textbf{PointM}, so indeed we can use the method invocation mechanisms of Point, like \textit{point}'\textit{setX}. For this reason, we didn't define \textit{2dpoint}'\textit{setX}, because it would be exactly the same as \textit{point}'\textit{setX} (apart from demanding an interface more refined than \textbf{2DPointM} instead of \textbf{PointM}).

Again, the representation of a \textit{2dpoint} is the same as section 3.3.

\[
\begin{align*}
\textbf{2DPointR} &= \textbf{PointR} \setminus \{\text{y:Int}\} \\
\textbf{2DPointR} &= \ast \\
\end{align*}
\]

\[
\begin{align*}
\text{2dpoint}'\text{rep}'\text{new} &= \text{point}'\text{rep}'\text{new } \textbf{PointR} \text{ with } \{\text{y:Int}\} \{y=0\} \\
\text{2dpoint}'\text{new} &= \textbf{2DPointR} \\
\text{2dpoint}'\text{class} &= "The same as in the previous section" \\
\text{2dpoint}'\text{new} &= \text{new } \textbf{2DPointM} \textbf{2DPointR} \textbf{2dpoint}'\text{new} \\
\text{2dpoint}'\text{new} &= \textbf{2DPoint} \\
\text{2dpoint}'\text{getY} &= \textbf{2DPointM} (\textit{point}'\textit{bump } \textbf{2DPointM} \textbf{2dpoint}'\text{new}) \\
1
\end{align*}
\]

The \textit{bump} method which is packed in a \textit{2DPoint} is used, not the one given in \textit{pointclass}.

In some OO languages, there is an even stricter sense of encapsulation. Methods of subclasses may not touch the instance variables of superclasses. This can also be modelled in our calculus, but falls outside the scope of this article. See [PT 93].

### 3.5 Self-reference

In this section we will add self-reference to our model of OOP, so it will be fairly complete. This model is based on [PT 93, CP 93], but it is simpler because of the extended underlying calculus.

Self-reference is the idea that a method can use the own methods of an object. In particular, a method can use itself, i.e. be recursive. To model this, we certainly need the fixpoint combinator \textit{Y} : all \textit{T} : \ast. (\textit{T} -> \textit{T}) -> \textit{T}.

After some definitions are reintroduced, we present a simple way to resolve the self-references.

\[
\begin{align*}
\textbf{Object}, \textbf{PointM}, \textbf{Point}, \textbf{point}'\text{iGetX}, \textbf{point}'\text{iSetX}, \textbf{point}'\text{iBump}, \\
\textbf{PointR}, \textbf{point}'\text{rep}'\text{new} &= "The same as in the previous section" \\
\textbf{Object} : (\ast \to \ast) \to \ast \\
\textbf{Point} : \ast \\
\textbf{point}'\text{iGetX} &= \text{all } \textbf{M<PointM}. \text{Object } \text{M} \to \text{Int} \\
\textbf{point}'\text{iSetX} &= \text{all } \textbf{M<PointM}. \text{Object } \text{M} \to \text{Int} \to \text{Object } \text{M} \\
\textbf{point}'\text{iBump} &= \text{all } \textbf{M<PointM}. \text{Object } \text{M} \to \text{Object } \text{M} \\
\textbf{PointR} : \ast \\
\textbf{point}'\text{rep}'\text{new} &= \textbf{PointR} \\
\text{try-pointclass} &= \\
\text{fun } \textbf{FinalR<#PointR}. \\
\text{Y } (\textbf{PointM} \textbf{FinalR})
\end{align*}
\]
Here self refers to the definitions given in the same record; self-references are immediately short-circuited. This is exactly what happens in some OO languages. However, this is considered to be rather rigid. Maybe subclasses of Point have another, more appropriate way of setting the x-coordinate, so we want self to refer to the final set of methods. This idea, called *late binding*, is present in SmallTalk, for example. Late binding means we cannot fix the references inside the definition of the class; the parameter self is left open.

```
# pointclass =
#  fun FinalR<#PointR.
#  fun self: PointM FinalR.
#    {getX = fun s:FinalR. s.x,
#     setX = fun s:FinalR. fun i:Int. s FinalR with {{x:Int} {x=i}},
#      bump = fun s:FinalR. self.setX (plus 1 (self.getX s))}
pointclass : all FinalR<#PointR. PointM FinalR
```

When we make a new object, we may fill in the final set of methods for self, by "short-circuiting" the class by Y.

```
# new = fun M:-->*. fun R:*.
#  fun cl:Class M R. fun init:R.
#    pack R and
#    {state = init,
#     methods = Y (M R) (cl R)}
#  to Object M
new : all M:-->*. all R:*. Class M R -> R -> Object M
# point'new = new PointM PointR pointclass pointrep'new
point'new : Point
# Point'getX PointM (Point'bump PointM point'new)
1
```

For objects of base class pointclass there is no difference in behaviour between late binding and not. So we introduce the subclass 2dpointclass. Most definitions stay the same:

```
# 2DPointM, 2DPoint, 2dpoint'getY, 2dpoint'setY, 2DPointR, 2dpoint'repnew
# = "The same as in the previous section"
2DPointM : *->*
2DPoint : *
2dpoint'getY : all M<2DPointM. Object M -> Int
2dpoint'setY : all M<2DPointM. Object M -> Int -> Object M
2DPointR : *
2dpoint'repnew : 2DPointR
```

Only the class definition changes:

```
# 2DPointR = PointR /\ {ly:Int!}
# 2dpointclass =
#  fun FinalR<#2DPointR.
#  fun self: 2DPointM FinalR.
#  let super = pointclass FinalR self in
#  super (PointM FinalR) with
#    {getX: FinalR->Int, setX: FinalR->Int->FinalR, bump: FinalR->FinalR}
#  {getY = fun s:FinalR. s.y,
#   setY = fun s:FinalR. fun i:Int. s FinalR with {{y:Int} {y=i}},
#   bump = fun s:FinalR. fun i:Int. let s' = super.bump s in
```
We define super as pointclass applied to the final set of methods, self. This is allowed, because 2DPointM FinalR < PointM FinalR. It means that self in the superclass refers to the same methods as self in this subclass.

The circle of references is closed in the definition of a new 2DPoint:

``` razor
# 2dpoint'new = new 2DPointM 2DPointR 2dpointclass 2dpointrep'new
2dpoint'new : 2DPoint
```

Unfortunately our example class 2DPoint cannot illustrate late binding. However the class CPoint can, so we will first show how multiple inheritance can be modelled. The base class Colour will be defined without any comments:

``` razor
# ColourM = fun Rep:* {lgetC : Rep->String, setC : Rep->String->Rep!}
ColourM : +++
# Colour = Object ColourM
Colour : *
# colour'getC = fun M<ColourM. fun p:Object M. open p as R and r in
# colour'getC : all M<ColourM. Object M -> String
# colour'setC fun M<ColourM.fun p:Object M. fun c:String. open p as R and r in
# colour'setC : all M<ColourM. Object M -> String -> Object M
```

Now we will combine the interfaces of both superclasses and the new (empty) part of the interface. Here the power of a full concatenation operation is needed, the operation of adding one field is not enough here.

``` razor
# CPointM = PointM /\ ColourM
CPointM : ++*
# CPoint = Object CPointM
CPoint : *
```

Observe that we have both CPointM<PointM and CPointM<ColourM, so the method invocation mechanisms of Point and Colour can be used.

The definition of cpointclass in terms of pointclass and colourclass also relies heavily on a full concatenation operator, on the level of values, and the level of types. Since we need to concatenate three record values a couple of times, we introduce a special operation.

``` razor
# with3 = fun C:* fun B&C. fun A#(B\C).
# with3 : all C:* all B&C. all A#(B\C). A -> B -> C -> A\(B\C)
```

Observe that we have both CPointM<PointM and CPointM<ColourM, so the method invocation mechanisms of Point and Colour can be used.
### 3.6 Conclusion

The final model is based on Pierce & Turner [PT 93]. A class is just an object with enough of the packaging left off, and enough decisions about representation and recursive self-reference postponed, that it can still be extended. When the class is instantiated to form an object, the representation and references to self are fixed and the methods all become concrete functions.

However, the encoding in F# is much simpler and more natural, than in F<, since it allows polymorphic record updates and concatenation of records of methods, both using the with-construction. Still it is desirable to design high-level syntax for OO programs, since the translated code can be rather verbose. The translation from high-level syntax to F# is relatively straightforward, because of the powerful new primitives.

Let us give a short inventoryisation what we used of our calculus in the model of 3.5. The concatenation with is used in three places:

1. For the polymorphic record update in the body of methods; the concatenation is used to overwrite some fields.
2. For the inheritance of methods. Here the full power of with is used to overwrite old methods and add some new ones.
3. For the inheritance of the initial state. Again the full power of with is used. (Overwriting occurs in the case of multiple inheritance, where the superclasses have a common instance variable.)

We used bounded quantification in two places:

1. For the polymorphic record update, where we demand that the final representation type is ≤ and # to the current representation, so subtyping on fields of the state is not possible.
2. For making polymorphic method calls, to ensure an object has the appropriate functions defined. Here we need only the ≤ demand.

Of the compatibility laws we used overwriting (section 2.7) and transitivity (2.9), but not specialized record updating (2.8) or recursive concatenation (2.10). These are needed for method specialisation (page 27) and for instance variables that are extendible records themselves respectively. There are concepts of OOP that we didn't model, such as private instance variables, binary methods and template classes. Because of the simplicity of our model we expect that these concepts can also be implemented without major changes in the system.
4 Translation semantics

We adopt the so-called Penn interpretation of $F\#$, which views subtyping as implicit coercion. This leads to a translation of $F\#$, where the coercions are implicit, to $F_x$, with explicit coercions. $F_x$ is the second-order lambda calculus with cartesian products and labelled types. This translation was given first for $F\#$ by Breazu-Tannen, Coquand, Gunter, Scedrov [BCGS 91], and for $F_x$ by Pierce [Pie 91h]. Our translation is an extension of the latter.

Such a translation is sometimes called a semantics because any semantics for the target system can be composed with this translation to yield a translation for the source system.

The idea is that well-typed terms are translated by induction on the typing derivation. So for each typing rule, we have to state how terms typed with that rule should be translated, given the translation of the terms occurring in the premises of the typing rule. Effectively, we have to give a translation for each typing rule.

Since there are typically several typing derivations possible for one term, we will also get several translations. We have to show that all derivations result in essentially the same translation. This demand is called coherence and will be formulated more formally in section 4.4. This will place a very important restraint on the translation, i.e. we cannot take just anything for a coercion.

4.1 Introduction

In a system with subtyping each occurrence of the subsumption rule, say

\[ \Gamma \vdash e : S \quad \Gamma \vdash S \subseteq T \]

(introduces a coercion from $S$ to $T$ that is applied to $e$, so each subtyping judgment $S \subseteq T$ delivers a coercion function $c$ of type $S \rightarrow T$, so the rule above will be translated as

\[ \Gamma \vdash e : S \quad \Gamma \vdash c : S \rightarrow T \]

(Translation)

Just as terms are translated by induction on the typing derivation, coercions are defined by induction on the subtyping derivation. Thus each subtyping rule determines a coercion, typically based on coercions in the premises of the rule.

To what type should an intersection $SAT$ be translated, in order to have coercions to $S$ and $T$? There has to be a simple function from the translation of $S$ to $S$ and, to $T$. Clearly, the cartesian product $S \times T$ satisfies this requirement: The coercions are just the projections (here we follow [Pie 91h]). So the type $[[\text{Int}, m : \text{Char}]]$, which is an abbreviation for $[[\text{Int}]] \times [[m : \text{Char}]]$, will be translated as $[[\text{Int}]] \times [[m : \text{Char}]]$. Suppose $e$ is an $F\#$-term of this type. Type $\llbracket e \rrbracket$, $e$ has to be coerced to $[[\text{Int}]]$ (remember the (T-Sel) rule). So the translation of $e.L$ will be $(\pi e.L)$.

Now consider the term $\{i=7, m='a'\} \{i: \text{Int}, m: \text{Char}\}$ with $[[\text{Int}]] \{i=5\}$. The type of this term is $[[\text{Int}]] \land [[m : \text{Char}]]$. Again, when the $l$-field of this term is selected, the term has to be coerced to $[[\text{Int}]]$. But this time it can be done in two different ways: via $[[\text{Int}]] \land [[m : \text{Char}]]$ or directly. Those two ways give rise to different coercions:

\[
\lambda x : ([[\text{Int}]] \times [[m : \text{Char}]] \times [[\text{Int}]], \pi_1 (\pi_1 x) \text{ and}
\lambda x : ([[\text{Int}]] \times [[m : \text{Char}]] \times [[\text{Int}]], \pi_2 x
\]

Of course, we want both coercions to give the same result when applied to the term. This is the coherence property.

In order to translate the value $\{i=7, m='a'\} \{i: \text{Int}, m: \text{Char}\}$ with $[[\text{Int}]] \{i=5\}$, we cannot just pair both records and be done with it, but we have to make all common fields equal, to ensure coherence. We chose the right record to have preference above the left record, so all common fields have to be overwritten in the left record. We will call the function that makes the common fields equal the overwriter. Just as the coercions are generated by subtyping derivations, overwriters will be generated by compatibility derivations. A function that overwrites parts of a value of type $A$ by a value of type $B$, has type $A \rightarrow B \rightarrow A$. Each occurrence of the and-introduction rule,

\[ \Gamma \vdash e : T \quad \Gamma \vdash f : U \quad \Gamma \vdash T \neq U \]

(T-With)
is translated with
\[
\Gamma \vdash e : T \quad \Gamma \vdash f : U \quad \Gamma \vdash p : T \to U \\
\Gamma \vdash (p \in e, f) : T \times U
\]  
(Translation)

where \( p \) is the overwriter, that will be defined by induction on the compatibility judgment.

First we will give a formal definition of the target calculus, then we will show how terms are translated

4.2 The target calculus

Our target calculus is \( F \) extended with cartesian products, a one-element type and labelled types. Formally, the syntax and the derivation rules are those of section 2.1 extended by:

Rules:

Types:

\[T ::= T \times T \] cartesian product

\[One\] one-element type

\[\{|l:T\}\] labelled type

Terms:

\[e ::= (e, e)\] pairing

\[\pi_1 e\] first projection

\[\pi_2 e\] second projection

\[one\] unique element

\[\{l=e\}\] labelled value

\[e.l\] selection

Reduction rules: \( \{l=e\}.l \beta \sim e \)

Derivation rules:

![Derivation rules for target calculus]

Examples:

1. \( \vdash \{|l:Int\} \times \{|m:Char\}\} : * \)
   This will be the translation of the \( F \# \) type \( \{|l:Int, m:Char\}\} \).

2. \( \vdash \{|l=7\}, \{m='a'\}\} : \{|l:Int\} \times \{|m:Char\}\) 
   This term will be the translation of the \( F \# \) term \( \{l=7, m='a'\}\). 

3. \( \vdash (\pi_1 \{|l=7\}, \{m='a'\}).l : Int \)
   This term will be the translation of \( \{|l=7, m='a'\}.l \)
4. \( \vdash \pi_1 (T, a') : \text{Int} \)

The labels in this calculus are silly: they are not necessary. Terms and types of this calculus can be converted directly to a calculus without labels, by deleting all label constructions (example 4 is the conversion of example 3). Then records with labels are translated to cartesian products, and field selection to projection, which is all very natural. Another nice effect is that this translation automatically delivers coercions (here: permutations) to convert between records that differ only in the order of their fields.

However, terms from \( F_\# \) translated to \( F_\text{x} \) retain their structure better, so it is easier to see what happens in the translation.

4.3 The translation

For each \( F_\# \) item \( i \), we will denote its \( F_\text{x} \) translation by \( i^0 \).

**Definition 4.1** The translation of types:

\[
X^0 = X \\
(S \land T)^0 = S^0 \times T^0 \\
[[X]]^0 = [[T]]^0 \\
\forall X \leq T, X \neq U. S)^0 = \forall X : X \rightarrow (X \rightarrow U^0 \rightarrow X) \rightarrow S^0
\]

**Definition 4.2** The translation of contexts:

\[
\emptyset^0 = \emptyset \\
\Gamma, x : T^0 = \Gamma^0, x : T^0 \\
\Gamma, X \leq T, X \neq U)^0 = \Gamma^0, X : X \rightarrow T^0, pX : X \rightarrow U^0 \rightarrow X
\]

**Lemma 4.3** If \( \Gamma \vdash \text{ok} \) then \( \Gamma^0 \vdash \text{ok} \).

**Lemma 4.4** If \( \Gamma \vdash T : * \) then \( \Gamma^0 \vdash \text{c} : T^0 : * \).

The translation of the other sorts of judgments depends on the derivation of the judgment: for each derivation rule a translation is given, i.e. a (derived) rule in \( F_\text{x} \). The translation of a derivation of a judgment is defined inductively on the structure of the derivation, by replacing occurrences of the derivation rules by their translations.

**Definition 4.5** The translation of derivation \( \Delta \) is of the following form:

If \( \Delta \) derives \( \Gamma \vdash T \), then \( \Delta^0 \) derives \( \Gamma^0 \vdash c : T^0 \) for some \( F_\text{x} \) term \( c' \)

If \( \Delta \) derives \( \Gamma \vdash T \leq U \), then \( \Delta^0 \) derives \( \Gamma^0 \vdash c : T^0 \rightarrow U^0 \) for some term \( c \)

If \( \Delta \) derives \( \Gamma \vdash T \neq U \), then \( \Delta^0 \) derives \( \Gamma^0 \vdash p : T^0 U^0 \rightarrow T^0 \) for some term \( p \)

where \( c \) stands for a coercion, and \( p \) for an overwriter.

First we give the translation of some rules already present in \( F_\text{x} \), then we will give some typical \( F_\# \) rules. We will use the meta-variables \( c \) and \( d \) for coercions, and \( p \) and \( q \) for overwriters. We assume that the new variables, introduced by the translation, are always fresh. For the rest of the rules we refer to appendix B.

A coercion is made explicit in the translation of the subsumption rule:

\[
\frac{\Gamma^0 \vdash e : S^0}{\Gamma^0 \vdash c : S^0 \rightarrow T^0} \quad (T - \text{Subsumption})^0
\]

Of course the coercion from a type to itself is the identity:

\[
\frac{\Gamma^0 \vdash T^0 : *}{\Gamma^0 \vdash \lambda x : T^0, x : T^0 \rightarrow T^0} \quad (S - \text{Ref})^0
\]

And we already gave the coercions for intersection types:

\[
\frac{\Gamma^0 \vdash S_1^0 \mathbf{\land} S_2^0 : *}{\Gamma^0 \vdash \lambda x : S_1^0 \times S_2^0, \pi : S_1^0 \times S_2^0 \rightarrow S_0^0} \quad (S - \text{Inter - LB})^0
\]

Now the rules that are specific for \( F_\# \). We discussed the (T-With) rule:

\[
\frac{\Gamma^0 \vdash r : R^0, \Gamma^0 \vdash s : S^0, \Gamma^0 \vdash p : R^0 \rightarrow S^0 \rightarrow R^0}{\Gamma^0 \vdash (p \ r \ s, s) : R^0 \times S^0} \quad (T - \text{With})^0
\]

34
The premise of the (#-Sub) rule says that \( T \) has more fields than \( S \), so all fields of \( S \) have to be overwritten. The translation accordingly:

\[
\frac{\Gamma^0 \vdash c : T^0 \to S^0}{\Gamma^1 \vdash \lambda x : [l : T^0], \lambda y : [m : U^0] : * \ x : [l : T^0] \to [m : U^0] \to [l : T^0]} \quad (\# \text{- Sub})^0
\]

The records in the conclusion of the (#-Diff) rule have no common fields, so nothing has to change in the left record:

\[
\frac{l \neq m \quad \Gamma^0 \vdash \forall x : [l : T^0] : * \quad \Gamma^0 \vdash \forall x : [m : U^0] : * \ x : [l : T^0] \to [m : U^0] \to [l : T^0]}{\quad (\# \text{- Diff})^0}
\]

The (#-Inter-L) is fairly straightforward, both parts of the left type have to be updated:

\[
\frac{\Gamma^0 \vdash c : R^0 \to R^0 \quad \Gamma^0 \vdash q : S^0 \to S^0 \quad \Gamma^0 \vdash R^0 \times S^0}{\Gamma^0 \vdash \lambda x : [l : T^0], \lambda y : [m : U^0] \ x : [l : T^0] \to [m : U^0] \to [l : T^0]} \quad (\# \text{- Inter \text{-} L})^0
\]

but the (#-Inter-R) rule is more tricky. The left value has to be updated by two values. This can happen in two orders, that won’t make any difference if the translation is coherent:

\[
\frac{\Gamma^0 \vdash c : R^0 \to R^0 \quad \Gamma^0 \vdash q : R^0 \to R^0 \quad \Gamma^0 \vdash S^0 \times T^0}{\Gamma^0 \vdash \lambda x : R^0, \lambda y : (S^0 \times T^0), \quad p : (\tau_1 \tau) \quad q : (\tau_2 \tau) \quad t : (R^0 \times S^0) \to (R^0 \times T^0) \to R^0}{\quad (\# \text{- Inter \text{-} R})^0}
\]

This concludes the explanation of the translation of # rules. It is interesting to see now how the (T-TApp) rule is translated. In a system with subtyping, each type application gets a coercion in the translation, in this system with compatibility, there is an additional function, the overwriter.

\[
\frac{\Gamma^0 \vdash c : V^0 \to S^0}{\Gamma^0 \vdash c \ : \ V^0 \to T^0 \to V^0}
\]

\[
(T \text{- TApp})^0
\]

Lemma 4.6 All translated rules are derivable in \( F_x \).

Examples:

1. A translation of
\[
\vdash \left( \llbracket l : \text{Int} \rrbracket, \llbracket m : \text{Char} \rrbracket \right) \leq \left( \llbracket l : \text{Int} \rrbracket \right)
\]
\[
\vdash c : \forall x : \left( \llbracket l : \text{Int} \rrbracket \right) \times \left( \llbracket m : \text{Char} \rrbracket \right) \to \left( \llbracket l : \text{Int} \rrbracket \right)
\]

2. A translation of
\[
\vdash \left( \llbracket l : \text{Int} \rrbracket \right) \neq \left( \llbracket m : \text{Char} \rrbracket \right)
\]
\[
\vdash c : \forall x : \left( \llbracket l : \text{Int} \rrbracket \right) \times \left( \llbracket m : \text{Char} \rrbracket \right) \to \left( \llbracket l : \text{Int} \rrbracket \right)
\]

3. A translation of
\[
\vdash \left( \llbracket l : \text{Int} \rrbracket \right) \neq \left( \llbracket l : \text{Int} \rrbracket \right)
\]
\[
\vdash c : \forall x : \left( \llbracket l : \text{Int} \rrbracket \right) \times \left( \llbracket m : \text{Char} \rrbracket \right) \to \left( \llbracket l : \text{Int} \rrbracket \right)
\]

The identity function is generated by the subtyping judgment \( \llbracket l : \text{Int} \rrbracket \leq \llbracket l : \text{Int} \rrbracket \) in the premise of the (#-Sub) rule. This makes the overwrite function less readable. Therefore we will sometimes apply some reduction steps in the terms.

4. A translation of
\[
\vdash \left( \llbracket l : \text{Int} \rrbracket \right) \text{ with } \left[ \llbracket m : \text{Char} \rrbracket \right] \{m = 'a'\} : \left[ \llbracket l : \text{Int} \rrbracket \right] \times \left[ \llbracket m : \text{Char} \rrbracket \right]
\]
\[
\vdash c : \forall x : \left( \llbracket l : \text{Int} \rrbracket \right) \times \left( \llbracket m : \text{Char} \rrbracket \right) \to \left( \llbracket l : \text{Int} \rrbracket \right) \times \left( \llbracket m : \text{Char} \rrbracket \right)
\]

With the convention of example 3 we say the translation is:
\[
\vdash c : \left[ \llbracket l : \text{Int} \rrbracket \right] \times \left[ \llbracket m : \text{Char} \rrbracket \right]
\]

5. A translation of
\[
\vdash \left( \llbracket l : \text{Int} \rrbracket, \llbracket m : \text{Char} \rrbracket \right) \neq \left( \llbracket l : \text{Int} \rrbracket \right)
\]
\[
\vdash c : \forall x : \left( \llbracket l : \text{Int} \rrbracket \right) \times \left( \llbracket m : \text{Char} \rrbracket \right) \to \left( \llbracket l : \text{Int} \rrbracket \right) \times \left( \llbracket m : \text{Char} \rrbracket \right)
\]

---

*In our explanation we will assume \( S \) and \( T \) are record types.

*In a context where the type of an argument is clear, we will sometimes replace the type by _._
6. A translation of
\( \vdash \{l=7, m=a\} \{l: \text{Int}, m: \text{Char} \} \) with \( \{l: \text{Int} \} \) is
\( \{l: \text{Int} \} \times \{l: \text{Char} \} \). (\( l=7, \{m='a'\} \)) \( \{l=5\} \), so whatever coercion is applied to this term, the \( l \)-field will always be 5.

7. A translation of
\( \vdash \lambda R \leq \{l: \text{Int}\} : R \# \{l: \text{Int}\} \), \( \lambda R : R \# R \) with \( \{l: \text{Int}\} \) \( \{z=r, z+1\} \)
\( \forall R \leq \{l: \text{Int}\} : R \# \{l: \text{Int}\} \), \( R \# R \) is
\( \forall R : R \# R \) \( \lambda R : R \# \{l: \text{Int}\} \), \( \lambda R : R \# \{l: \text{Int}\} \) \( \lambda R : R \# \{l: \text{Int}\} \)
\( \forall R : (R \leq \{l: \text{Int}\}) \rightarrow (R \# \{l: \text{Int}\}) \rightarrow R \rightarrow R \)
The polymorphic update is translated to this simple function.

Discussion: We give here the reasons for not having a symmetry rule for \( \# \). First of all, such a rule is inconsistent with specialized updating (section 2.8), so we lose some generality of the system. Suppose we don’t allow specialized updating and have a symmetry rule for \( \# \). This symmetry has a complicating effect on the semantics, because the semantics (as described above) is not symmetric: If \( S \# T \), we have an overwriter that overwrites an \( S \) (of type \( S-T-S \)), but not the dual one that overwrites a \( T \). For a symmetric \( \# \) both are needed, so the translation of \( S \# T \) will be a pair of overwriters, with type \( (S-T-S) \times (T-S-T) \), which is symmetric.

Definition 4.7 Let \( e \) and \( e' \) be \( F_\# \)-terms, with type \( T \) and translations \( f, f' \) respectively. Then \( e =_F f \) iff \( f =_F f' \).
Here a formal meaning to equality in \( F_\# \) is given via the translation.

4.4 Coherence

Coherence is the property that all translations of some \( F_\# \) judgment are equal with respect to the equational theory of \( F_\# \) (i.e. \( \beta_\eta \)-convertible). In specific:

Conjecture 4.8 Coherence of subtyping: Suppose \( \Gamma \vdash S \leq T \) has derivations \( \Delta_1 \) and \( \Delta_2 \), giving rise to translations \( \Gamma^0 \vdash c_1 : S \rightarrow \exists T_0 \) and \( \Gamma^0 \vdash c_2 : S \rightarrow \exists T_0 \) respectively. Then \( c_1 \) and \( c_2 \) are equal in \( F_\# \).

Conjecture 4.9 Coherence of compatibility: Suppose \( \Gamma \vdash S \# T \) has derivations \( \Delta_1 \) and \( \Delta_2 \), giving rise to translations \( \Gamma^0 \vdash p_1 : S \rightarrow \exists T_0 \rightarrow S_0 \) and \( \Gamma^0 \vdash p_2 : S \rightarrow \exists T_0 \rightarrow S_0 \) respectively. Then \( p_1 \) and \( p_2 \) are equal in \( F_\# \).

Conjecture 4.10 Coherence of typing: Suppose \( \Gamma \vdash e : T \) has derivations \( \Delta_1 \) and \( \Delta_2 \), giving rise to translations \( \Gamma^0 \vdash e_1 : T_0 \) and \( \Gamma^0 \vdash e_2 : T_0 \) respectively. Then \( e_1 \) and \( e_2 \) are equal in \( F_\# \).

As even for \( F_\# \) coherence is not yet proved, the proofs of these conjectures are outside the scope of this article.

5 Conclusions

5.1 Related work

Record concatenation

First we will compare \( F_\# \) with other explicitly typed second-order record calculi, viz. Cardelli [Car 92], Cardelli and Mitchell [CM 91] and Harper and Pierce [HP 90]. All of these calculi have a restriction operator, denoted by \( \backslash \), that removes a field from a record, and a way of extending a record with one new field. A polymorphic record update is performed by removing the field, and extending the record with the one-field record containing the new value.

In principle the combination of extension and restriction is in some respects more powerful than our calculus without a way of removing a field. However, such power is not needed for
a fairly extensive model of OOP, as section 3 suggests. Only for renaming of methods — not a very important feature of some OO languages — restrictions are necessary.

In the presence of a restriction operator, the combination of subtyping and a full concatenation (extend with a possibly unknown number of fields) is problematic; none of the systems has both. Subtyping is needed for a natural encoding of OO programs, concatenation for multiple inheritance. We dropped record restriction in favour of both other properties. The possibility of a polymorphic record update was retained by permitting concatenation of record with some common fields, as long as they are of the same type\(^6\).

Now we will compare these calculi to \(F\#\) in some more detail. For each calculus we will show how a polymorphic record update is implemented. In \(F\#\) this function is:

\[
\lambda R \leq \llbracket x : \text{Int} \rrbracket ; R \# \llbracket x : \text{Int} \rrbracket ; \lambda x : R. \ r \ R \text{ with } \llbracket x : \text{Int} \rrbracket \{x = r.x + 1\}
\]

\[
\forall R \leq \llbracket x : \text{Int} \rrbracket ; R \# \llbracket x : \text{Int} \rrbracket . \ R \rightarrow R
\]

The examples that we will give are largely adapted to our syntax.

- In [Car 92] Cardelli gives a record calculus based on row-variables. Just as in our system, Cardelli provides a translation of the system with records to a system with only cartesian products. There are two differences. First, his target system includes subtyping whereas ours does not. More importantly, there is some order fixed on the fields, say \(P, I^1, I^2\) etc.

The translation of a record type depends on this order. E.g. the type \(\llbracket x : \text{Int}, I : \text{Real} \rrbracket\) will be translated to \(\text{Int} \times (\text{Top} \times (\text{Real} \times \text{Top}))\). This interpretation of records makes it very difficult to make a concatenation.

Each extensible record has a row variable representing the unknown fields of the record. In this example of a polymorphic update:

\[
\lambda X[x. \ x.r : \llbracket x : \text{Int}, X \rrbracket \{z = r.x + 1, \ r \backslash x\}
\]

\[
\forall X[x. \ x.r : \llbracket x : \text{Int}, X \rrbracket \rightarrow \llbracket x : \text{Int}, X \rrbracket
\]

\(X\) is the row-variable representing all fields other than \(x\).

- In [CM 91] Cardelli and Mitchell give a record calculus where both positive (a record has a field) and negative information (a record doesn’t have a field) is determined by the record type. All record values that comply with this information belong to this record type.

E.g. \(\llbracket x : \text{Int} \rrbracket\) is the type of all records that have an \(x\)-field of type integer, such as \(\{x=3\}\) and \(\{x=3, y='a'\}\). This means that the identity \((\lambda r : \llbracket x : \text{Int} \rrbracket. \ x)\) applied to the term reduces to \(\{x=3, y='a'\}\). This is quite in contrast to \(F\#\) where the emphasis is on coercions and applying the identity above can have an effect, in this case it would remove the \(y\)-field. An example of a type with negative information is \(\llbracket x : \text{Int} \rrbracket \# y\), which is the type of all records with an \(x\)-field, but without a \(y\)-field. The example of the polymorphic update can be written simply as

\[
\lambda R \# \llbracket x : \text{Int} \rrbracket . \ n \ r : R \ x \ | x = r.x + 1
\]

\[
\forall R \# \llbracket x : \text{Int} \rrbracket . \ R \rightarrow R \ x | \llbracket x : \text{Int} \rrbracket
\]

where \(|\) is the extension with a field.

The very different philosophy makes it impossible to define a disjoint record concatenation, because two records, of whatever type, can always have a field in common. Furthermore this view complicates the semantics of the system.

- Harper and Pierce give in [HP 90] a calculus with only negative information and with a full concatenation operator on disjoint records. For negative information the same symbol as in \(F\#\) for compatibility is used, viz. \(#\). This relation expresses that two records are disjoint, so may be concatenated with \(||\).

The polymorphic update is implemented by

\[
\lambda R \# \llbracket x : \text{Int} \rrbracket . \ n \ r : R \ || \ \llbracket x : \text{Int} \rrbracket . \ r \ \ llbracket x = r.x + 1\}
\]

\[
\forall R \# \llbracket x : \text{Int} \rrbracket . \ R \ || \ \llbracket x : \text{Int} \rrbracket \rightarrow R \ || \ \llbracket x : \text{Int} \rrbracket
\]

\(^6\)Actually our concatenation is a little more liberal, but that is not relevant now.
In fact the presence of fields is forced by the typing in value-abstractions, whereas the absence of fields is forced by type abstractions.

The most important drawback of this calculus is that it does not have subtyping, which seems to be necessary to make a natural encoding of object-oriented features.

Our update is easier to use than the others because the type that has to be supplied to the polymorphic update is just the type of the record, not the type of a part of the record.

The idea of using intersection types for record concatenation already appeared in Reynolds imperative language Forsythe [Rey 88]. In Forsythe there is also a construction to make a value of an intersection type, called merge. Because Reynolds permits only merging with one field, there is no need for a compatibility relation. The restrictions for merge can be expressed directly by the derivation rules. Remarkable is that some totally different values may be combined. Translated to our framework, there are rules like

\[
\Gamma \vdash A \rightarrow B : * \quad \Gamma \vdash \left[\!\left[ t : C \right] \right] : *
\]

This means a function and a record may be combined. This is justified by the fact that in any context only one of the two can be used, so there is no danger of losing coherence.

A difference with our system is that it is possible to replace a field in a record with a value of some different type.

Modelling OOP concepts in a type system

There are different styles of OO programming languages. First there are class based and delegation based languages. In class based languages, the implementation of an object is specified by its class, and a class can be extended to form a new class. In delegation based languages an object can be extended to form a new object. We will only study class based languages in this paper.

The class based languages have two categories: single-dispatch and multiple dispatch. In multiple-dispatch languages, such as Common Lisp [Ste 84], the method is determined by any number of arguments instead of just one for single-dispatch languages. For a model of this more symmetrical notion of method invocation, run-time type information is needed. We concentrate on the single-dispatch variants, such as SmallTalk [GR 83] and C++.

There appeared two ways to model the concept of encapsulation of single-dispatch OO languages in a type-theoretic setting. The first is procedural abstraction, objects are encoded as elements of recursive record types. The second is type abstraction, which hides the type of the state, but permits the invocation of methods that can work on the state. A comparison of both methods can be found in [FM 94], a more theoretic treatment of the similarities and differences in [HP 95].

Our model is the same as the model of Pierce and Turner [PT 93] and Compagnoni and Pierce [CP 93], who chose for the second way, since the combination of subtyping with recursive types is still problematic for modelling inheritance. Because our type system is more powerful, the encoding is simpler. The differences are:

1. In both models, the state of a subclass (designated by B) is a longer record than the state of the corresponding superclass (designated by A). The methods of the superclass should not only work for A, but also for B. In their system, this is solved by introducing an extractor get to convert a B to an A, and an overwriter put that overwrites the A-part in a B. get is used whenever a method reads the state, and put whenever a method changes the state. The put is always used in conjunction with a non-polymorphic update, which can be implemented more elegantly using record concatenation.

In our system, the problem is solved by demanding that B is a subtype of and compatible with A. The first thing means that the state of the subclass can always be converted to a state of the superclass. This makes the extractor get redundant. The compatibility means that the state of the subclass may be concatenated with (a part of) the state of the superclass, so a field of the state of a subclass can be overwritten. In this way put becomes redundant.

In fact the translation we gave in section 4 translates the subtyping and compatibility demands in coercions (= extractors) and overwriters, so one could consider their model
to be a (partial) translation of our model. The extractors and overwriters are explicit in their system and implicit in ours.

2. The encoding of inheritance of methods is also facilitated by the concatenation: the record of old methods is concatenated with the record of new methods. A similar construction is used for inheritance of the initial state. Concretely, the code for inheritance does not depend on definitions of superclasses etc. This suggests that other concepts of OOP, such as template classes, probably can be modelled more easily.

So $F_\#$ gives rise to a more direct and natural model of OOP than $F_{\leq}$.

**Haskell type classes**

A subtyping judgment $A \leq B$ is translated to a function of type $A \rightarrow B$. A compatibility judgment $A \# B$ is translated to a function of type $A \rightarrow B \rightarrow A$. This asks for a generalisation. Subtyping and compatibility are predicates on two types. Their translation depends on the two types. In general, there will not always be two types involved, in other useful cases it will be just one. We can have the unary predicate "has equality defined on it", let's denote that with $Eq_A$, with an translation $A \rightarrow A \rightarrow Bool$. We could have a derivation rule that says that $Int$ has equality defined on it, and a derivation rule that says that if $Eq_A$, then also $Eq (List_A)$, where $List_A$ is the type of lists of $A$. The equality on type $A$, can be invoked by $is\ A$, provided that $Eq\ A$ is valid. Polymorphic functions can demand that a type variable has an equality, this is comparable to bounded quantification.

$Eq$ is an example of a so-called type class, as described by Wadler and Blott [WB 89] (the word type class has nothing to do with an object-oriented class). The derivation rules for type classes may be extended, but a few restrictions apply, that prevent the loss of coherence and make type checking for the type classes feasible. Even new type classes can be introduced. This type-class prevents the programmer having to make a boring definition of equality for every type that he uses. So the definition of equality is implicit, just like the definitions of coercions.

One could see both subtyping and compatibility as binary type classes, because they are translated to normal functions, just as ordinary type classes. But in other respects there are some differences. The most important one is that for $\leq$ the place where to use a coercion is implicit, in contrary to $\#$ or $Eq$ where the place to use the corresponding function is always explicit. Furthermore, type-checking the subtype or compatibility predicate is more complicated than unary predicates, because the former are binary and have some sort of transitivity law. The unification of type classes on one hand, and subtyping and compatibility on the other hand is an interesting point for future work.

**5.2 Future work**

**Proving coherence** As we pointed out in section 4.4, of $F_A$ is not yet proved. A major problem is caused by rule (T-Inter') on page 11, maybe the variant of the rules that we propose is easier proved coherent.

**Typing algorithm** For implementation, a typing algorithm is very important. Such a typing algorithm relies on a subtyping and a compatibility algorithm. For the subtyping and typing of similar systems algorithms have been proposed [Pie 91b, Com 95], and adaption seems straightforward, but for compatibility a new algorithm has to be constructed.

Just as with subtyping, the rule for transitivity poses the most problems. However the subtyping premises present in the ($\#$-Trans) rule can help with determining the unknown intermediate type, and compatibility seems decidable.

**Equational semantics for $F_\#$** An equational semantics is a derivation system, in which judgments state that two terms are equal as seen from some type. In systems with subtyping, this is a very important clause, since terms that are not equal on some type, may be equal on other types (e.g. all records are equal when seen from the empty record type).

Equational semantics gives a direct way of reasoning about equality of terms if there are no reduction rules (as in $F_\#$). It can also be used to guide the design of axioms for
proof rules of the system. The design of the equational semantics itself can be guided by the translation to $F_x$.

**Higher order types** As we have seen in section 3, we need to extend $F#$ to use it for a satisfying model of OOP. The higher-order aspect is the most involving: It complicates all points above.

**More demands for type variables** The sort of demands that one can place on a type variable in a system is a balance between pragmatics and feasibility (e.g. decidable typechecking). We have shown that we can come a long way towards OOP, by having type variables compatible to one type. We can also define a system where it is possible to demand from a variable that a certain type is compatible with the variable (the other way around). It turns out that with (the higher order version of) this system, we can define template classes relatively simple.

**Variant types** A record is seen as an intersection of labeled fields. The dual notion of intersection types are union types [Pie 91a]. So it is tempting to see a variant type as the union of labeled fields. We will see however, that this cannot be done in a coherent way.

Consider the judgment $\Gamma \vdash [[\text{Int}]\land [m:\text{Char}]] \leq [[\text{Int}]] \lor [m:\text{Char}]$. There are two simple derivations of it, one via type $[[\text{Int}]]$, and one via type $[[m:\text{Char}]]$. The coercions differ accordingly, the former always delivers the $l$-choice and the latter delivers the $m$-choice, so coherence is lost unfortunately.

A solution for this is to have two kinds of labeled types. However, for one thing there doesn’t seem to be such a big need for flexible variants, and for another there is still less known about union types than about intersection types. The combination of $F#$ with normal (not extendable) labeled variants seems unproblematic, however.

**Alternative for $\leq$** The coupled use of $\leq$ and $#$ in polymorphic update functions suggests a system where only the coupled use of subtyping and compatibility is permitted. This new relation, denoted by $\subseteq$, is a variant of subtyping that allows updating. So the translation of $S \subseteq T$ is $S \rightarrow T \times S \rightarrow S$, both a coercion and an overwriter. There are two uses for $\subseteq$, the subsumption rule and an update rule:

\[
\frac{\Gamma \vdash c : S \quad \Gamma \vdash S \subseteq T}{\Gamma \vdash c : T} \quad \text{(T-Subsum)}
\]

\[
\frac{\Gamma \vdash e : S \quad \Gamma \vdash f : T \quad \Gamma \vdash S \subseteq T}{\Gamma \vdash \text{update } S \rightarrow T e f : S} \quad \text{(T-Update)}
\]

Clearly, not all subtyping rules admissible for $\leq$ are admissible for $\subseteq$, e.g. $\text{Int} \leq \text{Real}$ or contravariant arrow subtyping, but reflexivity, transitivity and record subtyping do transfer.

Such a system can be very interesting if only polymorphic updates are needed (but no record concatenation), since the syntax is almost as simple as the standard subtyping syntax. This approach has been taken in [HP 94].

**Acknowledgments**

Thanks to Kees Hemerik, Benjamin Pierce and Erik Poll for reading drafts of this article.

**References**


[Car 88] Luca Cardelli. A Semantics of Multiple Inheritance. Information and Computation 76.


[Pie 94] Benjamin C. Pierce. *Bounded Quantification is Undecidable.* Information & Computation 112. Also in [Pie 91b] and [GM 94].


A Rules of F#

Labels:
\[ \mathcal{L} ::= \text{the set of labels} \]

Types:
\[
\begin{align*}
T ::= & \quad X & \text{type variable} \\
& T \rightarrow T & \text{function type} \\
& \forall X \leq T; X \neq T. T & \text{restricted quantification} \\
& \text{Top} & \text{top-type} \\
& \{ \mathcal{L} : T \} & \text{one-field record type} \\
& T \wedge T & \text{record concatenation} \\
\end{align*}
\]

Terms:
\[
\begin{align*}
e ::= & \quad x & \text{variable} \\
& \lambda x : T. e & \text{abstraction} \\
& e \, e & \text{application} \\
& \forall X \leq T; X \neq T. e & \text{type abstraction} \\
& e \, T & \text{type application} \\
& \text{top} & \text{top-value} \\
& \{ \mathcal{L} = e \} & \text{one-field record} \\
& e \, T \, \text{with} \, T \, e & \text{concatenation} \\
& e \cdot \mathcal{L} & \text{field selection}
\end{align*}
\]

Contexts:
\[ \Gamma ::= \emptyset \quad \text{empty context} \]
\[ \Gamma, x : T \quad \text{term variable declaration} \]
\[ \Gamma, X \leq T; X \neq T \quad \text{type variable declaration} \]

Judgments:
\[ \Gamma \vdash \text{ok} \quad \text{well-formed context} \]
\[ \Gamma \vdash T : * \quad \text{well-formed type} \]
\[ \Gamma \vdash S \leq T \quad \text{subtype} \]
\[ \Gamma \vdash S \neq T \quad \text{compatible} \]
\[ \Gamma \vdash e : T \quad \text{well-typed term} \]

Meta-variables:
\[ \Gamma \quad \text{for contexts} \]
\[ X \quad \text{for type variables} \]
\[ R, S, T, U, V \quad \text{for types} \]
\[ x \quad \text{for term variables} \]
\[ e, f \quad \text{for terms} \]
\[ l, m \quad \text{for labels} \]

Derivation rules:

Context formation:
\[
\begin{align*}
\emptyset & \vdash \text{ok} \quad \text{(C-Empty)} \\
\Gamma & \vdash T : * \quad x \notin \text{dom}(\Gamma) \\
\Gamma, x : T & \vdash \text{ok} \quad \text{(C-Var)} \\
\Gamma & \vdash T : * \quad \Gamma \vdash U : * \quad X \notin \text{dom}(\Gamma) \\
\Gamma, X \leq T; X \neq U & \vdash \text{ok} \quad \text{(C-TVar)}
\end{align*}
\]

Type formation:
\[
\begin{align*}
\Gamma_1, X \leq T; X \neq U & \vdash \text{ok} \quad \Gamma_2 & \vdash \text{ok} \\
\Gamma_1, X \leq T; X \neq U, \Gamma_2 & \vdash X : * \quad \text{(K-TVar)} \\
\Gamma & \vdash T_1 : * \quad \Gamma & \vdash T_2 : * \\
\Gamma & \vdash T_1 \rightarrow T_2 : * \quad \text{(K-Arrow)}
\end{align*}
\]

42
Subtyping:

\[
\Gamma, X \vdash T; X \# U \vdash S : * \\
\frac{\Gamma \vdash T : *}{\Gamma \vdash \llbracket [\Gamma : T] \rrbracket : *} \quad \text{(K-All)}
\]

\[
\Gamma \vdash R : * \\
\frac{\Gamma \vdash S : *}{\Gamma \vdash R \llbracket [\Gamma : S] \rrbracket : *} \quad \text{(K-Single)}
\]

\[
\frac{\Gamma \vdash R \llbracket [\Gamma : R] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : R] \rrbracket \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(K-With)}
\]

\[
\frac{\Gamma, X \vdash T; X \# U \vdash S : *}{\Gamma \vdash nums : *} \quad \text{(K-Top)}
\]

Compatibility rules:

\[
\frac{\Gamma \vdash T : *}{\Gamma \vdash T \leq T} \quad \text{(S-Refl)}
\]

\[
\frac{\Gamma \vdash T : *}{\Gamma \vdash T \leq U} \quad \text{(S-Sym)}
\]

\[
\frac{\Gamma, X \vdash T; X \# U, \Gamma \vdash ok}{\Gamma \vdash T \leq U} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma, X \vdash T; X \# U, \Gamma \vdash ok}{\Gamma \vdash T \leq U} \quad \text{(S-TVar)}
\]

\[
\frac{\Gamma \vdash T_1 \leq S_1 \quad \Gamma \vdash S_2 \leq T_2}{\Gamma \vdash T_1 \llbracket [\Gamma : S_1 \llbracket [\Gamma : T_1 \llbracket [\Gamma : S_1] \rrbracket \rrbracket \rrbracket \rrbracket \rrbracket \llbracket [\Gamma : T_2] \rrbracket : *} \quad \text{(S-Arrow)}
\]

\[
\frac{\Gamma, X \vdash U; X \# V \vdash S \leq T}{\Gamma \vdash \forall X \llbracket \forall X \leq U; X \# V \vdash T \rrbracket \rrbracket \rrbracket : *} \quad \text{(S-All)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]

\[
\frac{\Gamma \vdash T \llbracket [\Gamma : T] \rrbracket \llbracket [\Gamma : S] \rrbracket : * \quad \Gamma \vdash S \llbracket [\Gamma : S] \rrbracket : *}{\Gamma \vdash R \llbracket [\Gamma : R \llbracket [\Gamma : S] \rrbracket \rrbracket : *} \quad \text{(S-Trans)}
\]
Term formation:

\[
\frac{\Gamma_1, x : T, \Gamma_2 \vdash o} {\Gamma_1, x : T, \Gamma_2 \vdash x : T} \quad \text{(T-Var)}
\]

\[
\frac{\Gamma, x : S \vdash e : T} {\Gamma \vdash \lambda x : S. e : S \rightarrow T} \quad \text{(T-Abs)}
\]

\[
\frac{\Gamma \vdash f : S \rightarrow T \quad \Gamma \vdash e : S} {\Gamma \vdash f \cdot e : T} \quad \text{(T-App)}
\]

\[
\frac{\Gamma, X \triangleleft S; X \# T \vdash e : U} {\Gamma \vdash \lambda X \triangleleft S; X \# T . e : \forall X \triangleleft S; X \# T . U} \quad \text{(T-TAbs)}
\]

\[
\frac{\Gamma \vdash f : \forall X \triangleleft S; X \# T . U \quad \Gamma \vdash V \triangleleft S} {\Gamma \vdash f \cdot V : U[\{X \triangleright V\}]} \quad \text{(T-TApp)}
\]

\[
\frac{\Gamma \vdash o} {\Gamma \vdash \text{top} : \text{Top}} \quad \text{(T-Top)}
\]

\[
\frac{\Gamma \vdash e : T} {\Gamma \vdash \{l=e\} : \{l\} : T} \quad \text{(T-Single)}
\]

\[
\frac{\Gamma \vdash R \quad \Gamma \vdash s : S \quad \Gamma \vdash \# S} {\Gamma \vdash R \text{ with } S \vdash R \wedge S} \quad \text{(T-With)}
\]

\[
\frac{\Gamma \vdash e : \{l\} : T} {\Gamma \vdash e \cdot l : T} \quad \text{(T-Sel)}
\]

\[
\frac{\Gamma \vdash e : S \quad \Gamma \vdash S \triangleleft T} {\Gamma \vdash e : T} \quad \text{(T-Subsumption)}
\]

44
B Translation of $F#$ to $F_x$

Notes:

- Translations of rules not presented here are straightforward.
- We will use the meta-variables $c$ and $d$ for coercions, and $p$ and $q$ for overwriters. We assume that the new variables, introduced by the translation, are always fresh.

Subtyping:

$$
\begin{array}{c}
\Gamma^0 \vdash x : T^0 : * \\
\Gamma^0 \vdash \lambda x : T^0. x : T^0 \to T^0 \quad (S - \text{Refl})^0 \\
\Gamma^0 \vdash c : S^0 \to T^0 \quad \Gamma^0 \vdash d : T^0 \to U^0 \\
\Gamma^0 \vdash \lambda x : S^0. d \ (c \ x) : S^0 \to U^0 \\
\Gamma^0 \vdash X : *, c x : X \to T^0, p x : X \to U^0 \to X, \Gamma^0 \vdash ok \\
\Gamma^0 \vdash X : *, c x : X \to T^0, p x : X \to U^0 \to X, \Gamma^0 \vdash c x : X \to T^0 \\
\Gamma^0 \vdash c : S^0 \to S^0 \quad \Gamma^0 \vdash d : S^0 \to T^0 \\
\Gamma^0 \vdash \lambda f : S^0 \to S^0, \lambda : T^0 \to d \ (f (c \ t) ) : (S^0 \to S^0) \to (T^0 \to T^0) \\
\Gamma^0 \vdash X : *, c x : X \to U^0, p x : X \to V^0 \to X \vdash c : S^0 \to T^0 \\
\Gamma^0 \vdash X : *, (X \to U^0) \to (X \to V^0 \to X) \vdash S^0 \to T^0 \\
\Gamma^0 \vdash X : *, (X \to U^0) \to (X \to V^0 \to X) \vdash T^0 \\
\Gamma^0 \vdash c : R^0 \to S^0 \\
\Gamma^0 \vdash \lambda x : S^0 \times S^0. * \quad \Gamma^0 \vdash \pi_1 x \times \pi_2 x : S^0 \times S^0 \\
\Gamma^0 \vdash \lambda c : S^0 \times S^0, \pi_1 x \times \pi_2 x : S^0 \times S^0 \\
\Gamma^0 \vdash \lambda c : S^0 \times S^0, \pi_1 x \times \pi_2 x : S^0 \times S^0 \\
\end{array}
$$

(S - Subtyping)\(^0\)

Compatibility rules:

$$
\begin{array}{c}
\Gamma^0 \vdash x \vdash R^0 \quad * \\
\Gamma^0 \vdash \lambda o : \text{One}. \lambda r : R^0. \ r : \text{One} \to R^0 \to \text{One} \\
\Gamma^0 \vdash c : R^0 \to \text{One} \\
\Gamma^0 \vdash \lambda r : R^0. \ o : \text{One} \to R^0 \to \text{One} \\
\Gamma^0 \vdash c : R^0 \to \text{One} \\
\end{array}
$$

(S - Top)\(^0\)

$$
\begin{array}{c}
\Gamma^0 \vdash \lambda c : S^0 \times S^0, \pi_1 x \times \pi_2 x : S^0 \times S^0 \\
\Gamma^0 \vdash \lambda c : S^0 \times S^0, \pi_1 x \times \pi_2 x : S^0 \times S^0 \\
\Gamma^0 \vdash \lambda c : S^0 \times S^0, \pi_1 x \times \pi_2 x : S^0 \times S^0 \\
\end{array}
$$

(S - Diff)\(^0\)

$$
\begin{array}{c}
\Gamma^0 \vdash p : R^0 \to T^0 \quad \Gamma^0 \vdash q : S^0 \to T^0 \\
\Gamma^0 \vdash (p \ (\pi_1 r) \ q \ (\pi_2 s)) : (R^0 \times S^0) \to T^0 \to (R^0 \times S^0) \\
\Gamma^0 \vdash p : R^0 \to S^0 \quad \Gamma^0 \vdash q : R^0 \to S^0 \\
\Gamma^0 \vdash (p \ (\pi_1 r) \ q \ (\pi_2 s)) : R^0 \to (S^0 \times S^0) \\
\Gamma^0 \vdash c : B^0 \to A^0 \\
\end{array}
$$

(\# - Sub)^0

$$
\begin{array}{c}
\Gamma^0 \vdash p : A^0 \to B^0 \to A^0 \\
\Gamma^0 \vdash \lambda c : \ A^0, \ ab : A^0. \ c \ b : A^0 \to B^0 \to A^0 \\
\end{array}
$$

(\# - Equal)^0

$$
\begin{array}{c}
\Gamma^0 \vdash c : R^0 \to S^0 \quad \Gamma^0 \vdash d : S^0 \to T^0 \\
\end{array}
$$

(\# - Trans)^0
Term formation (selection):

\[ \Gamma^0 \vdash f : \forall X. (X \to S^0) \to (X \to T^0 \to X) \to U^0 \]
\[ \Gamma^0 \vdash c : V^0 \to S^0 \]
\[ \Gamma^0 \vdash p : V^0 \to T^0 \to V^0 \]
\[ (T - \text{TApp})^0 \]
\[ \Gamma^0 \vdash f \quad V^0 \quad c \quad p : U^0[X := V^0] \]

\[ \Gamma^0 \vdash r : R^0 \quad \Gamma^0 \vdash s : S^0 \quad \Gamma^0 \vdash p : R^0 \to S^0 \to R^0 \]
\[ (T - \text{With})^9 \]

\[ \frac{\Gamma^0 \vdash r \quad \Gamma^0 \vdash s : S^0 \quad \Gamma^0 \vdash p : R^0 \to S^0 \to R^0}{\Gamma^0 \vdash (p \ r \ s, s) : R^0 \times S^0} \]

\[ \Gamma^0 \vdash e : S^0 \quad \Gamma^0 \vdash c : S^0 \to T^0 \]
\[ (T - \text{Subsumption})^9 \]
Computing Science Reports

In this series appeared:

93/01 R. van Geldrop
93/02 T. Verhoef
93/03 T. Verhoef
93/04 B.H.L. Aarts
J.H.M. Korst
P.J. Zwistering
93/05 J.C.M. Baeten
C. Verhoef
93/06 J.P. Velikamp
93/07 P.D. Moerland
93/08 J. Verhoosel
93/09 K.M. van Hee
93/10 K.M. van Hee
93/11 K.M. van Hee
93/12 K.M. van Hee
93/13 K.M. van Hee
93/14 J.C.M. Baeten
J.A. Bergstra
93/15 J.C.M. Baeten
J.A. Bergstra
R.N. Bol
93/16 H. Schepers
J. Hooman
93/17 D. Alstein
P. van der Stok
93/18 C. Verhoef
93/19 G.J. Houben
93/20 F.S. de Boer
93/21 M. Codish
D. Dams
G. Fiat
M. Bruynooghe
93/22 E. Poll
93/23 E. de Kogel
93/24 E. Poll and Paula Severi
93/25 H. Schepers and R. Gerth
93/26 W.M.P. van der Aalst
93/27 T. Klops and D. Kratsch
93/28 F. Kamareddine and
R. Nederpelt
93/29 R. Post and P. De Bra
93/30 J. Deogun
T. Klops
D. Kratsch
H. Müller

Deriving the Aho-Corasick algorithms: a case study into the synergy of programming methods, p. 36.

A continuous version of the Prisoner's Dilemma, p. 17

Quick sort for linked lists, p. 8

Deterministic and randomized local search, p. 78.

A congruence theorem for structured operational semantics with predicates, p. 18.

On the unavoidability of metastable behaviour, p. 29

Exercises in Multiprogramming, p. 97

A Formal Deterministic Scheduling Model for Hard Real-Time Executions in DEDOS, p. 32.


Systems Engineering: a Formal Approach Part II: Frameworks, p. 44.


A Trace-Based Compositional Proof Theory for Fault Tolerant Distributed Systems, p. 27

Hard Real-Time Reliable Multicast in the DEDOS system, p. 19.

A congruence theorem for structured operational semantics with predicates and negative premises, p. 22.

The Design of an Online Help Facility for ExSpect, p.21.


Freeness Analysis for Logic Programs - And Correctness, p. 24

A Typochecker for Bijective Pure Type Systems, p. 28.

Relational Algebra and Equational Proofs, p. 23.

Pure Type Systems with Definitions, p. 38.


Multi-dimensional Petri nets, p. 25.

Finding all minimal separators of a graph, p. 11.

A Semantics for a fine λ-calculus with de Bruin indices, p. 49.

GOLD, a Graph Oriented Language for Databases, p. 42.

On Vertex Ranking for Permutation and Other Graphs, p. 11.
<table>
<thead>
<tr>
<th>Page</th>
<th>Authors</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>93/31</td>
<td>W. Körver</td>
<td>Derivation of delay insensitive and speed independent CMOS circuits, using directed commands and production rule sets, p. 40.</td>
</tr>
<tr>
<td>93/33</td>
<td>L. Loyens and J. Moonen</td>
<td>ILIAS, a sequential language for parallel matrix computations, p. 20.</td>
</tr>
<tr>
<td>93/34</td>
<td>J.C.M. Baeten and J.A. Bergstra</td>
<td>Real Time Process Algebra with Infinitesimals, p. 39.</td>
</tr>
<tr>
<td>93/36</td>
<td>J.C.M. Baeten and J.A. Bergstra</td>
<td>Non Interleaving Process Algebra, p. 17.</td>
</tr>
<tr>
<td>93/38</td>
<td>C. Verhoef</td>
<td>A general conservative extension theorem in process algebra, p. 17.</td>
</tr>
<tr>
<td>93/41</td>
<td>A. Bijlsma</td>
<td>Temporal operators viewed as predicate transformers, p. 11.</td>
</tr>
<tr>
<td>93/42</td>
<td>P.M.P. Rambags</td>
<td>Automatic Verification of Regular Protocols in P/T Nets, p. 23.</td>
</tr>
<tr>
<td>93/43</td>
<td>B.W. Watson</td>
<td>A taxonomy of finite automata construction algorithms, p. 87.</td>
</tr>
<tr>
<td>93/44</td>
<td>B.W. Watson</td>
<td>A taxonomy of finite automata minimization algorithms, p. 23.</td>
</tr>
<tr>
<td>93/48</td>
<td>R. Gerth</td>
<td>Verifying Sequentially Consistent Memory using Interface Refinement, p. 20.</td>
</tr>
<tr>
<td>94/01</td>
<td>P. America, M. van der Kammen, R.P. Nederpelt, O.S. van Roosmalen, H.C.M. de Swart</td>
<td>The object-oriented paradigm, p. 28.</td>
</tr>
<tr>
<td>94/02</td>
<td>F. Kameleekine, R.P. Nederpelt</td>
<td>Canonical typing and IT-conversion, p. 51.</td>
</tr>
<tr>
<td>94/04</td>
<td>J.C.M. Baeten, J.A. Bergstra</td>
<td>Graph Isomorphism Models for Non Interleaving Process Algebra, p. 18.</td>
</tr>
<tr>
<td>94/06</td>
<td>T. Basten, T. Kunz, J. Black, M. Coffin, D. Taylor</td>
<td>Time and the Order of Abstract Events in Distributed Computations, p. 29.</td>
</tr>
<tr>
<td>94/08</td>
<td>O.S. van Roosmalen</td>
<td>A Hierarchical Diagrammatic Representation of Class Structure, p. 22.</td>
</tr>
<tr>
<td>94/09</td>
<td>J.C.M. Baeten, J.A. Bergstra</td>
<td>Process Algebra with Partial Choice, p. 16.</td>
</tr>
</tbody>
</table>
94/10 T. Verheijen

94/11 J. Peleska
C. Huizing
C. Petersohn

94/12 T. Kloks
D. Kratsch
H. Müller

94/13 R. Seljé

94/14 W. Peremans

94/15 R.J.M. Vaessens
E.H.L. Aarts
J.K. Lenstra

94/16 R.C. Backhouse
H. Doornbos

94/17 S. Mauw
M.A. Reniers

94/18 F. Kamareddine
R. Nederpelt

94/19 B.W. Watson

94/20 R. Bloo
F. Kamareddine
R. Nederpelt

94/21 B.W. Watson

94/22 B.W. Watson

94/23 S. Mauw and M.A. Reniers

94/24 D. Dams
O. Grumberg
R. Gerth

94/25 T. Kloks

94/26 R.R. Hoogerwoord

94/27 S. Mauw and H. Mulder

94/28 C.W.A.M. van Overveld
M. Verhoefen

94/29 J. Hooman

94/30 J.C.M. Baeten
J.A. Bergstra
Gh. Stefanescu

94/31 B.W. Watson
R.E. Watson

94/32 J.J. Vereijken

94/33 T. Laan

94/34 R. Bloo
F. Kamareddine
R. Nederpelt

94/35 J.C.M. Baeten
S. Mauw

94/36 F. Kamareddine
R. Nederpelt

94/37 T. Basten
R. Bol
M. Voorhoeve

94/38 A. Bijlsma
C.S. Scholten

The testing Paradigm Applied to Network Structure. p. 31.


A New Method for Integrity Constraint checking in Deductive Databases, p. 34.

Ups and Downs of Type Theory, p. 9.

Job Shop Scheduling by Local Search, p. 21.

Mathematical Induction Made Calculational, p. 36.

An Algebraic Semantics of Basic Message Sequence Charts, p. 9.

Refining Reduction in the Lambda Calculus, p. 15.

The performance of single-keyword and multiple-keyword pattern matching algorithms, p. 46.

Beyond β-Reduction in Church's λ→, p. 22.


The design and implementation of the FIRE engine: A C++ toolkit for Finite automata and regular Expressions.

An algebraic semantics of Message Sequence Charts, p. 43.

Abstract Interpretation of Reactive Systems: Abstractions Preserving ∀CTL*, ∃CTL* and CTL*, p. 28.

K_4-free and W_6-free graphs, p. 10.

On the foundations of functional programming: a programmer's point of view, p. 54.


Correctness of Real Time Systems by Construction, p. 22.

Process Algebra with Feedback, p. 22.

A Boyer-Moore type algorithm for regular expression pattern matching, p. 22.


A formalization of the Ramified Type Theory, p. 40.

The Barendregt Cube with Definitions and Generalised Reduction, p. 37.

Delayed choice: an operator for joining Message Sequence Charts, p. 15.

Canonical typing and II-conversion in the Barendregt Cube, p. 19.

Simulating and Analyzing Railway Interlockings in ExSpect, p. 30.

Point-free substitution, p. 10.
<table>
<thead>
<tr>
<th>Year</th>
<th>Authors</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>94/39</td>
<td>A. Blokhuis, T. Kloks</td>
<td>On the equivalence covering number of splitgraphs, p. 4.</td>
</tr>
<tr>
<td>94/40</td>
<td>D. Alstein</td>
<td>Distributed Consensus and Hard Real-Time Systems, p. 34.</td>
</tr>
<tr>
<td>94/41</td>
<td>T. Kloks, D. Kratsch</td>
<td>Computing a perfect edge without vertex elimination ordering of a chordal bipartite graph, p. 6.</td>
</tr>
<tr>
<td>94/43</td>
<td>R.C. Backhouse, M. Bijnertveld</td>
<td>Category Theory as Coherently Constructive Lattice Theory: An Illustration, p. 35.</td>
</tr>
<tr>
<td>94/45</td>
<td>G.J. Houben</td>
<td>Tutorial voor de ExSpect-bibliotheek voor &quot;Administratieve Logistiek&quot;, p. 43.</td>
</tr>
<tr>
<td>94/46</td>
<td>R. Bloo, F. Kamareddine, R. Nederpelt</td>
<td>The A-cube with classes of terms modulo conversion, p. 16.</td>
</tr>
<tr>
<td>94/47</td>
<td>R. Bloo, F. Kamareddine, R. Nederpelt</td>
<td>On Π-conversion in Type Theory, p. 12.</td>
</tr>
<tr>
<td>94/48</td>
<td>Mathematics of Program Construction Group</td>
<td>Fixed-Point Calculus, p. 11.</td>
</tr>
<tr>
<td>94/50</td>
<td>H. Geuvers</td>
<td>A short and flexible proof of Strong Normalization for the Calculus of Constructions, p. 27.</td>
</tr>
<tr>
<td>94/52</td>
<td>W. Penczek, R. Kuiper</td>
<td>Traces and Logic, p. 81</td>
</tr>
<tr>
<td>95/01</td>
<td>J.J. Lukkien</td>
<td>The Construction of a small Communication Library, p. 16.</td>
</tr>
<tr>
<td>95/02</td>
<td>M. Bezem, R. Bol, J.F. Groote</td>
<td>Formalizing Process Algebraic Verifications in the Calculus of Constructions, p. 49.</td>
</tr>
<tr>
<td>95/03</td>
<td>J.C.M. Baeten, C. Verhoef</td>
<td>Concrete process algebra, p. 134.</td>
</tr>
<tr>
<td>95/04</td>
<td>J. Hidders</td>
<td>An Isotopic Invariant for Planar Drawings of Connected Planar Graphs, p. 9.</td>
</tr>
<tr>
<td>95/05</td>
<td>P. Severi</td>
<td>A Type Inference Algorithm for Pure Type Systems, p. 20.</td>
</tr>
<tr>
<td>95/07</td>
<td>G.A.M. de Bruyn, O.S. van Roosmalen</td>
<td>Drawing Execution Graphs by Parsing, p. 10.</td>
</tr>
<tr>
<td>95/08</td>
<td>R. Bloo</td>
<td>Preservation of Strong Normalisation for Explicit Substitution, p. 12.</td>
</tr>
<tr>
<td>95/09</td>
<td>J.C.M. Baeten, J.A. Bergstra</td>
<td>Discrete Time Process Algebra, p. 20</td>
</tr>
<tr>
<td>95/10</td>
<td>R.C. Backhouse, R. Verhoeven, O. Weber</td>
<td>Mathpad: A System for On-Line Preparation of Mathematical Documents, p. 15</td>
</tr>
<tr>
<td>95/11</td>
<td>R. Seljée</td>
<td>Deductive Database Systems and integrity constraint checking, p. 36.</td>
</tr>
<tr>
<td>95/12</td>
<td>S. Mauw and M. Reniers</td>
<td>Empty Interworkings and Refinement Semantics of Interworkings Revised, p. 19.</td>
</tr>
<tr>
<td>95/14</td>
<td>A. Posee, C. Verhoef, S.F.M. Vlijmen (eds.)</td>
<td>De proceedings: ACP95, p.</td>
</tr>
<tr>
<td>95/16</td>
<td>D. Dams, O. Grumberg, R. Gerth</td>
<td>Abstract Interpretation of Reactive Systems: Preservation of CTL*, p. 27.</td>
</tr>
<tr>
<td>95/17</td>
<td>S. Mauw and E.A. van der Meulen</td>
<td>Specification of tools for Message Sequence Charts, p. 36.</td>
</tr>
<tr>
<td>95/19</td>
<td>J.C.M. Baeten and J.A. Bergstra</td>
<td>Discrete Time Process Algebra with Abstraction, p. 15.</td>
</tr>
<tr>
<td>95/20</td>
<td>F. van Raamsdonk and P. Severi</td>
<td>On Normalisation, p. 33.</td>
</tr>
<tr>
<td>95/21</td>
<td>A. van Deursen</td>
<td>Axiomatizing Early and Late Input by Variable Elimination, p. 44.</td>
</tr>
<tr>
<td>95/23</td>
<td>W.M.P. van der Aalst</td>
<td>Petri net based scheduling, p. 20.</td>
</tr>
<tr>
<td>95/25</td>
<td>L. Feijs</td>
<td>Synchronous Sequence Charts In Action, p. 36.</td>
</tr>
<tr>
<td>95/26</td>
<td>W.M.P. van der Aalst</td>
<td>A Class of Petri nets for modeling and analyzing business processes, p. 24.</td>
</tr>
<tr>
<td>95/29</td>
<td>H. Jurjus</td>
<td>On Nesting of a Nonmonotonic Conditional, p. 14</td>
</tr>
<tr>
<td>95/31</td>
<td>P. Kelb, D. Dams and R. Gerth</td>
<td>Practical Symbolic Model Checking of the full $\mu$-calculus using Compositional Abstractions, p. 17.</td>
</tr>
<tr>
<td>95/32</td>
<td>W.M.P. van der Aalst</td>
<td>Handboek simulatie, p. 51.</td>
</tr>
<tr>
<td>95/33</td>
<td>J. Engelfriet and JJ. Vereijken</td>
<td>Context-Free Graph Grammars and Concatenation of Graphs, p. 35.</td>
</tr>
</tbody>
</table>