# Higher-ranked Exception Types

Ruud Koot

March 2, 2016

# Contents


**1 Higher-ranked Exception Types** **7**

1.1 Motivation . . . 8

1.1.1 Overview . . . 11

1.1.2 Contributions . . . 11

1.2 The $\lambda^{\cup}$-calculus . . . 12

1.2.1 Syntax . . . 12

1.2.2 Typing relation . . . 12

1.2.3 Semantics . . . 13

1.2.4 Subsumption and observational equivalence . . . 13

1.2.5 Normalization . . . 14

1.2.6 Pattern unification . . . 16

1.2.7 Widening . . . 16

1.3 Source language . . . 17

1.3.1 Underlying type system . . . 19

1.3.2 Operational semantics . . . 19

1.4 Exception types . . . 25

1.4.1 Subtyping . . . 27

1.4.2 Conservative types . . . 28

1.4.3 Exception type completion . . . 30

1.4.4 Least exception types . . . 32

1.4.5 Exception typing and elaboration . . . 32

1.4.6 Presentation of exception types . . . 32

1.5 Type inference . . . 33

1.5.1 Polymorphic abstraction . . . 33

1.5.2 Polymorphic recursion . . . 34

1.5.3 Least upper bounds . . . 35
1.5.4 Complexity . . . 36
1.6 Metatheory . . . 36
1.6.1 $\lambda^{\cup}$-calculus . . . 36
1.6.2 Declarative type system . . . 37
1.6.3 Syntax-directed type elaboration . . . 42
1.6.4 Type inference algorithm . . . 42
1.7 Related work . . . 42
1.7.1 Higher-ranked polymorphism in type-and-effect systems 42
1.7.2 $\lambda^{\cup}$-calculus . . . 44
1.7.3 Exception analyses . . . 45
1.8 Further research . . . 45
1.9 Conclusion . . . 47

**A Old stuff** **51**
A.1 $\lambda^{\cup}$-calculus . . . 51
A.1.1 Reduction relation (wrong!) . . . 51
A.1.2 Semantics . . . 53
A.1.3 Normalization (with widening) . . . 54
A.2 Type inference . . . 55
A.3 Completion . . . 55
A.4 TODO . . . 56
A.4.1 Introduction . . . 57
A.4.2 The $\lambda^{\cup}$-calculus . . . 57
A.4.3 Source language . . . 58
A.4.4 Exception types . . . 58
A.4.5 Type inference . . . 60
A.4.6 Related work . . . 61
A.4.7 Future research . . . 61

# List of Figures


1.1 $\lambda^{\cup}$-calculus: syntax . . . . . 12
1.2 $\lambda^{\cup}$-calculus: type system . . . . . 13
1.3 $\lambda^{\cup}$-calculus: denotational semantics . . . . . 14
1.4 $\lambda^{\cup}$-calculus: reduction . . . . . 15
1.5 Source language: syntax . . . . . 18
1.6 Underlying type system ($\Gamma \vdash t : \tau$) . . . . . 20
1.7 Operational semantics ($t_1 \longrightarrow t_2$) . . . . . 21
1.8 Type completion ($\Delta \vdash \tau : \widehat{\tau} \,\&\, \xi \triangleright \Delta'$) . . . . . 22
1.9 Declarative type system ($\Gamma; \Delta \vdash t : \widehat{\tau} \,\&\, \xi$) . . . . . 23
1.10 Syntax-directed type elaboration system ($\Gamma; \Delta \vdash t \hookrightarrow t' : \widehat{\tau} \,\&\, \xi$) 24
1.11 Exception types: syntax . . . . . 25
1.12 Exception types: well-formedness ($\Delta \vdash \widehat{\tau}$ wff) . . . . . 27
1.13 Exception types: subtyping relation ($\Delta \vdash \widehat{\tau}_1 \leqslant \widehat{\tau}_2$) . . . . . 27
1.14 Source language: extended syntax . . . . . 33
1.15 Type inference algorithm ($\mathcal{R}$) . . . . . 48
1.16 Exception type matching ($\mathcal{M}$) . . . . . 49
1.17 Exception types: least upper bounds ($\sqcup$) . . . . . 49
1.18 Annotation substitution . . . . . 49
1.19 Term substitution . . . . . 50

A.1 To do.Normalization algorithm of $\lambda^{\cup}$-terms. . . . . 55

# Chapter 1

# Higher-ranked Exception Types

We present a type-and-effect system that derives an exception-annotated type signature for a given term of a simply typed non-strict functional language with general recursion and a list data type. This signature declares the set of exceptional values that may be present among the values of the term, or produced by terms of function type. Higher-ranked effect polymorphism and effect operators reminiscent of System $F_\omega$ help to achieve precision and clarity.

By restricting the use of higher-ranked polymorphism and operators to the effects, we conjecture the inference problem to remain decidable (in contrast to the type inference problem for System $F_\omega$). We give a type inference algorithm that builds on the techniques developed by Holdermans and Hage (2010).

The types in System $F_\omega$ form a simply typed $\lambda$-calculus. Similarly, the effects in our system form a simply typed algebraic $\lambda$-calculus embellished with the ACI1-structure of sets ($\lambda^{\cup}$). We briefly study this language in its own right.

## 1.1 Motivation

An often-heard selling point of non-strict functional languages is that they provide strong and expressive type systems that make side-effects explicit. This supposedly makes software more reliable by lessening the mental burden placed on programmers. Many programmers with a background in object-oriented languages are thus quite surprised, when making the transition to a functional language, that they lose a feature their type system formerly did provide: the tracking of uncaught exceptions.

There is an excuse for why this feature is missing from the type systems of contemporary non-strict functional languages: in a strict first-order language it is sufficient to annotate each function with a single set of uncaught exceptions the function may raise; in a non-strict higher-order language the situation becomes significantly more complicated. Let us first consider the two aspects 'higher-order' and 'non-strict' in isolation:

**Higher-order functions** The set of exceptions that may be raised by a higher-order function is not given by a fixed set of exceptions, but depends on the set of exceptions that may be raised by the function that is passed as its functional argument. Higher-order functions are thus *exception polymorphic*.

**Non-strict evaluation** In non-strictly evaluated languages, exceptions are not a form of control flow, but a kind of value. Typically the set of values of each type is extended with an *exceptional value* $\lightning$ (more commonly denoted $\bot$, but we shall not do so to avoid ambiguity), or family of exceptional values $\lightning^{\ell}$. This means we do not only need to give all functions an exception-annotated function type, but give every other expression an exception-annotated type as well.

Now let us consider these two aspects in combination. Take as an example the *map* function:

$$
\begin{aligned}
&\mathit{map} \;:\; \forall\alpha\beta.(\alpha \to \beta) \to [\alpha] \to [\beta] \\
&\mathit{map} = \lambda f.\lambda xs.\ \mathbf{case}\ xs\ \mathbf{of} \\
&\qquad\qquad [\,] \qquad\quad \mapsto [\,] \\
&\qquad\qquad (y :: ys) \mapsto f\ y :: \mathit{map}\ f\ ys
\end{aligned}
$$

We denote the exception-annotated type of a term by $\widehat{\tau}$ & $\xi$ or $\widehat{\tau}\langle\xi\rangle$. For function types we occasionally write $\widehat{\tau}_1\langle\xi_1\rangle \xrightarrow{\xi} \widehat{\tau}_2\langle\xi_2\rangle$ instead of $(\widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle)\langle\xi\rangle$. If $\xi$ is the empty exception set, then we sometimes omit this annotation completely.

The fully exception-polymorphic and exception-annotated type, or *exception type*, of *map* isTo do.cramped formatting

$$\begin{aligned} \mathit{map} : \forall\alpha\ \beta\ e_2\ e_3.(\forall e_1.\alpha\langle e_1\rangle &\xrightarrow{e_3} \beta\langle e_2\ e_1\rangle) \\ &\xrightarrow{\emptyset} (\forall e_4\ e_5.[\alpha\langle e_4\rangle]\langle e_5\rangle \xrightarrow{\emptyset} [\beta\langle e_2\ e_4 \cup e_3\rangle]\langle e_5\rangle) \end{aligned}$$

The exception type of the first argument $\forall e_1.\alpha\langle e_1\rangle \xrightarrow{e_3} \beta\langle e_2\ e_1\rangle$ states that it can be instantiated with a function that accepts any exceptional value as its argument (as the exception set $e_1$ is universally quantified) and returns a possibly exceptional value. In case the return value is exceptional, then it is one from the exception set $e_2\ e_1$. Here $e_2$ is an *exception set operator*—a function that takes a number of exception sets and exception set operators, and transforms them into another exception set, for example by adding a number of new elements to them, or discarding them and returning the empty set. Furthermore, the function (closure) itself may be an exceptional value from the exception set $e_3$.

The exception type of the second argument $[\alpha\langle e_4\rangle]\langle e_5\rangle$ states that it should be a list. Any of the exceptional elements in the list must be exceptional values from the exception set $e_4$. Any exceptional values among the constructors that form the spine of the list must be exceptional values from the exception set $e_5$.

The result of *map* is a list with the exception type $[\beta\langle e_2\ e_4 \cup e_3\rangle]\langle e_5\rangle$. Any exceptional constructors in the spine of this list must be exceptional values from the exception set $e_5$, the same exception set as where exceptional values in the spine of the list argument *xs* come from. By looking at the definition of *map* we can see why this is the case: *map* only produces non-exceptional constructors, but the pattern-match on the list argument *xs* propagates any exceptional values encountered there. The elements of the list are produced by the function application $f\ y$. Recall that $f$ has the exception type $\forall e_1.\alpha\langle e_1\rangle \xrightarrow{e_3} \beta\langle e_2\ e_1\rangle$. Now, one of two things can happen:

1. If $f$ is an exceptional function value, then it must be one from the exception set $e_3$. Applying the exceptional value to an argument causes the exceptional value to be propagated.

2. Otherwise, $f$ is a non-exceptional value. The argument $y$ has exception type $\alpha\langle e_4\rangle$—it is an element from the list argument *xs*—and so can only be applied to $f$ if we instantiate $e_1$ to $e_4$ first. If $f\ y$ produces an exceptional value, then it is thus one from the exception set $e_2\ e_4$.

To account for both cases we need to take the union of the two exception sets, giving us a value with the exception type $\beta\langle e_2\ e_4 \cup e_3\rangle$.

To get a better intuition for the behavior of these exception types and exception set operators, let us see what happens when we apply *map* to two different functions: the identity function *id* and the constant exception-valued function $const\ \lightning^{\mathbf{E}}$. These two functions can individually be given the exception types:

$$\begin{aligned} id &= \lambda x.x \ : \forall e_1.\alpha\langle e_1\rangle \xrightarrow{\emptyset} \alpha\langle e_1\rangle \\ const\ \lightning^{\mathbf{E}} &= \lambda x.\lightning^{\mathbf{E}} : \forall e_1.\alpha\langle e_1\rangle \xrightarrow{\emptyset} \beta\langle\{\mathbf{E}\}\rangle \end{aligned}$$

The term *id* merely propagates its argument to the result unchanged, so it also propagates any exceptional values unchanged. The term $const\ \lightning^{\mathbf{E}}$ discards its argument and always returns the exceptional value $\lightning^{\mathbf{E}}$. This behavior of *id* and $const\ \lightning^{\mathbf{E}}$ is also reflected in their exception types.

When we apply *map* to *id*, we need to unify the exception type of the formal parameter $\forall e_1.\alpha\langle e_1\rangle \xrightarrow{e_3} \beta\langle e_2\ e_1\rangle$ with the exception type of the actual parameter $\forall e_1.\alpha\langle e_1\rangle \xrightarrow{\emptyset} \alpha\langle e_1\rangle$. This can be accomplished by instantiating $e_3$ to $\emptyset$ and $e_2$ to $\lambda x.x$—as $(\lambda x.x)\ e_1$ evaluates to $e_1$—giving us the resulting exception type

$$map\ id : \forall\alpha\ e_4\ e_5.[\alpha\langle e_4\rangle]\langle e_5\rangle \xrightarrow{\emptyset} [\alpha\langle e_4\rangle]\langle e_5\rangle$$

In other words, mapping the identity function over a list propagates all exceptional values already present in the list and introduces no new exceptional values.

When we apply *map* to $const\ \lightning^{\mathbf{E}}$ we unify the exception type of the formal parameter with $\forall e_1.\alpha\langle e_1\rangle \xrightarrow{\emptyset} \beta\langle\{\mathbf{E}\}\rangle$, which can be accomplished by instantiating $e_3$ to $\emptyset$ and $e_2$ to $\lambda x.\{\mathbf{E}\}$—as $(\lambda x.\{\mathbf{E}\})\ e_1$ evaluates to $\{\mathbf{E}\}$—giving us the exception type

$$map\ (const\ \lightning^{\mathbf{E}}) : \forall\alpha\ \beta\ e_4\ e_5.[\alpha\langle e_4\rangle]\langle e_5\rangle \xrightarrow{\emptyset} [\beta\langle\{\mathbf{E}\}\rangle]\langle e_5\rangle$$

In other words, mapping the constant function with the exceptional value $\lightning^{\mathbf{E}}$ as its range over a list discards all existing exceptional values from the list and produces only non-exceptional values or the exceptional value $\lightning^{\mathbf{E}}$ as elements of the list.

### 1.1.1 Overview

In Section 1.2 we introduce the $\lambda^{\cup}$-calculus, a simply typed $\lambda$-calculus embellished with an associative, commutative, idempotent and unit (ACI1) structure. The $\lambda^{\cup}$-calculus forms the language of effects in the type-and-effect system. Section 1.3 describes the source language to which the analysis applies. In Section 1.4 we present the language of exception types and two type-and-effect systems for deriving exception types: a declarative type-and-effect system and a syntax-directed elaboration system that also produces an explicitly typed term. A type inference algorithm for this type-and-effect system is given in Section 1.5. Finally, we present related work in this area and discuss some directions for further research in Sections 1.7 and 1.8.

### 1.1.2 Contributions

This paper makes the following contributions:

- A *$\lambda$-calculus* extended with a union-operator that respect the associative, commutative, idempotent and unit structure of sets.
- A *type-and-effect system* with higher-ranked effect-polymorphic types and effect operators that precisely tracks exceptions.
- An *inference algorithm* for these higher-ranked exception types.

Some of the key insights used in the inference algorithm—in particular the facts that an underlying type can be completed to a most general exception type (Figure 1.8), and that the form of the types encountered in the inference algorithm makes it both easy to unify two types (Figure 1.16) and compute the least upper bound of two types (Figure 1.17)—were first noted by Holdermans and Hage (2010). Our inference algorithm differs in a number of aspects. Notably, by the use of reduction of $\lambda^{\cup}$-terms instead of constraint solving and in the manner in which recursive definitions in the source language are handled by the algorithm.

## 1.2 The $\lambda^{\cup}$-calculus

The $\lambda^{\cup}$-calculus is a simply typed $\lambda$-calculus extended at the term-level with empty set and singleton set constants, and a set union operator.

### 1.2.1 Syntax

We let $x \in \mathbf{Var}$ range over an infinite set of variables and $c \in \mathbf{Con}$ over a non-empty set of constants.

**Types**

$$\begin{array}{rcll} \tau \in \mathbf{Ty} & ::= & \star & \text{(base type)} \\ & \mid & \tau_1 \to \tau_2 & \text{(function type)} \end{array}$$

**Terms**

$$\begin{array}{rcll} t \in \mathbf{Tm} & ::= & x & \text{(variable)} \\ & \mid & \lambda x : \tau . t & \text{(abstraction)} \\ & \mid & t_1\ t_2 & \text{(application)} \\ & \mid & \emptyset & \text{(empty set)} \\ & \mid & \{c\} & \text{(singleton set)} \\ & \mid & t_1 \cup t_2 & \text{(union)} \end{array}$$

**Environments**

$$\Gamma \in \mathbf{Env} \ ::= \ \emptyset \mid \Gamma, x : \tau$$

Figure 1.1: $\lambda^{\cup}$-calculus: syntax

### 1.2.2 Typing relation

The typing relation of the $\lambda^{\cup}$-calculus is an extension of the typing relation of the simply typed $\lambda$-calculus.

$$\frac{}{\Gamma, x : \tau \vdash x : \tau}\ [\text{T-Var}] \qquad \frac{\Gamma, x : \tau_1 \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1 . t : \tau_1 \to \tau_2}\ [\text{T-Abs}]$$

$$\frac{\Gamma \vdash t_1 : \tau_1 \to \tau_2 \quad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ [\text{T-App}]$$

$$\frac{}{\Gamma \vdash \emptyset : \star}\ [\text{T-Empty}] \qquad \frac{}{\Gamma \vdash \{c\} : \star}\ [\text{T-Con}]$$

$$\frac{\Gamma \vdash t_1 : \tau \quad \Gamma \vdash t_2 : \tau}{\Gamma \vdash t_1 \cup t_2 : \tau}\ [\text{T-Union}]$$

Figure 1.2: $\lambda^{\cup}$-calculus: type system

The empty set and singleton set constants are of base type and the set union of two terms can only be taken if the involved terms have the same type.

### 1.2.3 Semantics

In the $\lambda^{\cup}$-calculus, terms are interpreted as sets and types as powersets.

### 1.2.4 Subsumption and observational equivalence

The set-structure of the $\lambda^{\cup}$-calculus induces a partial order on the terms.

**Definition 1.** Denote by $C[]$ a *context*—a $\lambda^{\cup}$-term with a single hole in it—and by $C[t]$ the term obtained by replacing the hole in $C[]$ with the term $t$.

**Definition 2.** Let $t_1$ and $t_2$ be terms such that $\Gamma \vdash t_1 : \tau$ and $\Gamma \vdash t_2 : \tau$. We say the term $t_2$ *subsumes* the term $t_1$, written $\Gamma \vdash t_1 \lesssim t_2$, if for any context $C[]$ such that $\vdash C[t_1] : \star$ and $\vdash C[t_2] : \star$ we have that $[\![C[t_1]]\!]_{\emptyset} \subseteq [\![C[t_2]]\!]_{\emptyset}$.

**Definition 3.** Let $t_1$ and $t_2$ be terms such that $\Gamma \vdash t_1 : \tau$ and $\Gamma \vdash t_2 : \tau$. We say that the terms $t_1$ and $t_2$ are *observationally equivalent*, denoted as $\Gamma \vdash t_1 \cong t_2$, if

1. $\Gamma \vdash t_1 \lesssim t_2$ and $\Gamma \vdash t_2 \lesssim t_1$, or equivalently that
2. for any context $C[]$ such that $\vdash C[t_1] : \star$ and $\vdash C[t_2] : \star$ we have that $[\![C[t_1]]\!]_{\emptyset} = [\![C[t_2]]\!]_{\emptyset}$.

**Types and values**

$$V_\star = \mathcal{P}(\mathbf{Con})$$
$$V_{\tau_1 \to \tau_2} = \mathcal{P}(V_{\tau_1} \to V_{\tau_2})$$

**Environments**

$$\rho : \mathbf{Var} \to \bigcup \{ V_\tau \mid \tau \text{ type} \}$$

**Terms**

$$\begin{aligned}
[\![x]\!]_\rho &= \rho(x) \\
[\![\lambda x : \tau . t]\!]_\rho &= \left\{ \lambda v \in V_\tau . [\![t]\!]_{\rho[x \mapsto v]} \right\} \\
[\![t_1\ t_2]\!]_\rho &= \bigcup \{ \varphi([\![t_2]\!]_\rho) \mid \varphi \in [\![t_1]\!]_\rho \} \\
[\![\varnothing]\!]_\rho &= \varnothing \\
[\![\{c\}]\!]_\rho &= \{c\} \\
[\![t_1 \cup t_2]\!]_\rho &= [\![t_1]\!]_\rho \cup [\![t_2]\!]_\rho
\end{aligned}$$

Figure 1.3: $\lambda^\cup$-calculus: denotational semantics

### 1.2.5 Normalization

To reduce $\lambda^\cup$-terms to a canonical normal form we combine the $\beta$-reduction rule of the simply typed $\lambda$-calculus with rewrite rules that deal with the associativity, commutativity, idempotence and identity (ACI1) properties of the set union operator.

#### $\beta$- and $\gamma$-reduction

If a term $t$ is $\eta$-long—i.e., it cannot be $\eta$-expanded without introducing additional $\beta$-redexes—it can be written in the form

$$t = \lambda x_1 \cdots x_n . f_1(t_{11}, ..., t_{1q_1}) \cup \cdots \cup f_p(t_{p1}, ..., t_{pq_p})$$

where $f_i$ can be a free or bound variable, a singleton-set constant, or another $\eta$-long term; and $q_i$ is equal to the arity of $f_i$ (for all $1 \leqslant i \leqslant p$). Here we have re-

moved any empty set constants (unit elements), duplicate terms $f_i(t_{i1}, ..., t_{iq_i})$ (idempotent elements), and 'forgotten' how the set union operator associates.

A *normal form* $v$ of a term $t$—obtained by repeatedly applying the reduction rules from Figure 1.4 and removing any empty set constants and duplicate terms—can be written as

$$v = \lambda x_1 \cdots x_n.k_1(v_{11}, ..., v_{1q_1}) \cup \cdots \cup k_p(v_{p1}, ..., v_{pq_p})$$

where $k_i$ can be a free or bound variable, or a singleton-set constant, but not a $\lambda$-abstraction (as this would form a $\beta$-redex), nor a union (as this would form a $\gamma_1$-redex).

$$\frac{}{(\lambda x.t_1)\ t_2 \longrightarrow t_1\,[t_2/x]}\ [\text{R-Beta}]$$

$$\frac{}{(t_1 \cup \cdots \cup t_n)\ t \longrightarrow t_1\ t \cup \cdots \cup t_n\ t}\ [\text{R-Gamma}_1]$$

$$\frac{}{(\lambda x.t_1) \cup \cdots \cup (\lambda x.t_n) \longrightarrow \lambda x.t_1 \cup \cdots \cup t_n}\ [\text{R-Gamma}_2]$$

Figure 1.4: $\lambda^{\cup}$-calculus: reduction

**Canonical ordering**

To be able to efficiently check two normalized terms for definitional equality up to ACI1, we also need to deal with the commutativity of the union operator. We can bring normalized terms into a fully canonical form by defining a total order on terms and use it to order unions of terms.

First, pick a strict total order $\prec$ on variables and constants. The order must be fixed and be invariant under $\alpha$-renaming of variables (for example, choose the De Bruijn index of a variable), but can otherwise be arbitrary. We extend this order to a total order on $\beta\gamma$-normal $\eta$-long terms in the following manner:

1. Given two fully applied terms $k(v_1, ..., v_n)$ and $k'(v'_1, ..., v'_m)$ we define:

$$\begin{aligned} k(v_1, ..., v_n) &\prec k'(v'_1, ..., v'_m) && \text{if } k \prec k' \\ k(v_1, ..., v_i, ..., v_n) &\prec k(v_1, ..., v_{i-1}, v'_i, ..., v'_n) && \text{if } v_i \prec v'_i \end{aligned}$$

2. Given two values $\lambda x_1 \cdots x_n.K_1 \cup \cdots \cup K_{i-1} \cup K_i \cup \cdots \cup K_p$ and $\lambda x_1 \cdots x_n.K_1 \cup \cdots \cup K_{i-1} \cup K'_i \cup \cdots \cup K'_q$ that have been ordered such that $K_1 \prec \cdots \prec K_{i-1} \prec K_i \prec \cdots \prec K_p$ and $K_1 \prec \cdots \prec K_{i-1} \prec K'_i \prec \cdots \prec K'_q$, we define:

$$\lambda x_1 \cdots x_n.K_1 \cup \cdots \cup K_{i-1} \cup K_i \cup \cdots \cup K_p \prec \lambda x_1 \cdots x_n.K_1 \cup \cdots \cup K_{i-1} \cup K'_i \cup \cdots \cup K'_q$$

if $K_i \prec K'_i$.

Given a term $t$ with the types of the free variables given by the environment $\Gamma$, we denote by $[\![t]\!]_\Gamma$ the $\beta\gamma$-normal $\eta$-long and canonically ordered derivation of the term $t$.

### 1.2.6 Pattern unification

**Definition 4.** A $\lambda^\cup$-term is called a *pattern* if it is of the form $f(e_1, ..., e_n)$ where $f$ is a free variable and $e_1, ..., e_n$ are distinct bound variables.

Note that this definition is a special case of what is usually called a *pattern* in higher-order unification theory Miller (1991); Dowek (2001).

If $f(e_1, ..., e_n)$ is a pattern and $t$ a term, then the equation

$$f : \tau_1 \to \cdots \to \tau_n \to \tau \vdash \forall e_1 : \tau_1, ..., e_n : \tau_n.f(e_1, ..., e_n) = t$$

has a unique solution given by the unifier

$$\theta = [f \mapsto \lambda e_1 : \tau_1, ..., e_n : \tau_n.t].$$

### 1.2.7 Widening

Typically we want the reduction rules of a $\lambda$-calculus to respect the (observational) equivalence of terms: if $t_1 \longrightarrow t_2$, then $t_1 \cong t_2$. As the $\lambda^\cup$-calculus does not only have the equivalence relation $\cong$ defined on its terms, but also a subsumption preorder $\lesssim$, it is also interesting to look at reduction rules $t_1 \longrightarrow t_2$ such that $t_1 \lesssim t_2$. We will call such reduction rules *widening rules*. Widening rules may rewrite a closed term $t_1$ of base type to a term $t_2$ that denotes a superset of the set denoted by $t_2$, but never to a subset or incomparable set.

A potential application of widening rules is to reduce the complexity of a $\lambda^\cup$-term. In some contexts it may be sound to extend the denotation of a term

with additional elements, as long as no elements are removed from it. Even if such a denotation is no longer a minimal sound denotation, the reduction in complexity of the term may be a worthwhile trade-off in some scenarios.

A reduction rule of the form $C[t_1] \longrightarrow C[t_2]$ is a widening rule if $t_1 \lesssim t_2$. Furthermore, it is the case that $t_1 \lesssim t_1 \cup t_2$ for any terms $t_1$ and $t_2$. An example of a widening rule that can be constructed using these observations is:

$$\frac{}{\cdots \cup k(t_1, ..., t_n) \cup \cdots \cup k(t'_1, ..., t'_n) \cup \cdots \longrightarrow \cdots \cup k(t_1 \cup t'_1, ..., t_n \cup t'_n) \cup \cdots} \text{[R-MERGE]}$$

This widening rule will merge any two terms together that have the same constant or variable at their heads.

**Example 1.** The widening rule R-MERGE can cause the denotation of a term to increase; it is a proper widening rule. Let $t_1$ and $t_2$ be the terms

$$t_1 = \lambda f.f\ (\lambda x.\emptyset)\ \{C\} \cup f\ (\lambda x.x)\ \emptyset$$
$$t_2 = \lambda f.f\ (\lambda x.x)\ \{C\}$$

where $C$ is an arbitrary constant. Then $t_1$ can be widened to $t_2$. However $t_1\ (\lambda g.\lambda y.g\ y)$ reduces (without using the widening rule) to $\emptyset$, while $t_2\ (\lambda g.\lambda y.g\ y)$ reduces to $\{C\}$.

Adding this widening rule to the normalization procedure can decrease the size of the normal forms. In a normal form $v$ belonging to a term $t$

$$v = \lambda x_1 \cdots x_n.k_1(v_{11}, ..., v_{1q_1}) \cup \cdots \cup k_p(v_{p1}, ..., v_{pq_p})$$

the number of subterms $p$ will now be bounded by the number of distinct free variables, bound variables and constants occurring in the term $t$, as each can occur at most once at the head of a subterm $k_i(v_{i1}, ..., v_{iq_i})$. It furthermore allows for a more efficient canonical ordering procedure. We no longer have to compare complete terms, but can order terms based on the atom occurring at the head of each term.

## 1.3 Source language

The type-and-effect system is applicable to a simple non-strict functional language that supports boolean, integer and list data types, as well as general

recursion.

**Terms**

$$
\begin{array}{rcll}
t \in \mathbf{Tm} & ::= & x & \text{(term variable)} \\
& | & c_\tau & \text{(term constant)} \\
& | & \lightning^\ell_\tau & \text{(exceptional constant)} \\
& | & \lambda x : \tau.t & \text{(term abstraction)} \\
& | & t_1\ t_2 & \text{(term application)} \\
& | & \mathbf{fix}\ x : \tau.t & \text{(general recursion)} \\
& | & t_1\ \mathbf{seq}\ t_2 & \text{(forcing)} \\
& | & t_1 \oplus t_2 & \text{(operator)} \\
& | & \mathbf{if}\ t_1\ \mathbf{then}\ t_2\ \mathbf{else}\ t_3 & \text{(conditional)} \\
& | & []_\tau & \text{(nil constructor)} \\
& | & t_1 :: t_2 & \text{(cons constructor)} \\
& | & \mathbf{case}\ t_1\ \mathbf{of}\ \{[] \mapsto t_2; x_1 :: x_2 \mapsto t_3\} & \text{(list eliminator)}
\end{array}
$$

**Values**

$$v \in \mathbf{Val} \ ::= \ c_\tau \mid \lambda x : \tau.t \mid \mathbf{fix}\ x : \tau.t \mid \ []_\tau \ \mid t_1 :: t_2$$

$$\widehat{v} \in \mathbf{ExnVal} \ ::= \ \lightning^\ell_\tau \mid v$$

Figure 1.5: Source language: syntax

Most constructs in Figure 1.5 should be familiar. The **seq**-construct evaluates the term on the left to a value and then continues evaluating the term on the right.

Missing from the language is a construct to 'catch' exceptional values. While this may be surprising to programmers familiar with strict languages, it is a common design decision to omit such a construct from the pure fragment of non-strict languages. The omission of such a construct allows for the introduction of a certain amount of non-determinism in the operational semantics of the language—giving more freedom to an optimizing compiler—without

breaking referential transparency.

The values of the source language are stratified into non-exceptional values $v$ and possibly exceptional values $\widehat{v}$.

### 1.3.1 Underlying type system

The type system of the source language is given for reference in Figure 1.6. This is the *underlying type system* with respect to the type-and-effect system that is presented in Section 1.4. We assume that any term we type in the type-and-effect system is already well-typed in the underlying type system.

### 1.3.2 Operational semantics

The operational semantics of the source language is given in Figure 1.7. Note that there is a small amount of non-determinism in the order of reduction. For example, in the derivation rules E-OpExn$_1$ and E-OpExn$_2$.[1]

The reduction rules E-AnnApp and E-AnnAbsApp apply to constructs that are introduced to the language in Section 1.4. This also holds for the additional annotations on the $\lambda$-abstraction and the **fix**-operator.

[1] We do not go so far as to have an *imprecise exception semantics* Peyton Jones et al. (1999). For example, when the guard of a conditional evaluates to an exceptional value (E-IfExn), we do not continue evaluation of the two branches in exception finding mode.

$$\frac{}{\Gamma, x : \tau \vdash x : \tau}\ \text{[U-Var]} \qquad \frac{}{\Gamma \vdash c_\tau : \tau}\ \text{[U-Con]} \qquad \frac{}{\Gamma \vdash \lightning^{\ell}_{\tau} : \tau}\ \text{[U-Crash]} \qquad \frac{\Gamma, x : \tau_1 \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1.t : \tau_1 \to \tau_2}$$

$$\frac{\Gamma \vdash t_1 : \tau_2 \to \tau \quad \Gamma \vdash t_2 : \tau_2}{\Gamma \vdash t_1\ t_2 : \tau}\ \text{[U-App]} \qquad \frac{\Gamma, x : \tau \vdash t : \tau}{\Gamma \vdash \mathbf{fix}\ x : \tau.t : \tau}\ \text{[U-Fix]} \qquad \frac{\Gamma \vdash t_1 : \mathbf{int} \quad \Gamma \vdash t_2 : \mathbf{int}}{\Gamma \vdash t_1 \oplus t_2 : \mathbf{bool}}\ \text{[U}$$

$$\frac{\Gamma \vdash t_1 : \tau_1 \quad \Gamma \vdash t_2 : \tau_2}{\Gamma \vdash t_1\ \mathbf{seq}\ t_2 : \tau_2}\ \text{[U-Seq]} \qquad \frac{\Gamma \vdash t_1 : \mathbf{bool} \quad \Gamma \vdash t_2 : \tau \quad \Gamma \vdash t_3 : \tau}{\Gamma \vdash \mathbf{if}\ t_1\ \mathbf{then}\ t_2\ \mathbf{else}\ t_3 : \tau}\ \text{[U-If]}$$

$$\frac{}{\Gamma \vdash []_\tau : [\tau]}\ \text{[U-Nil]} \qquad \frac{\Gamma \vdash t_1 : \tau \quad \Gamma \vdash t_2 : [\tau]}{\Gamma \vdash t_1 :: t_2 : [\tau]}\ \text{[U-Cons]} \qquad \frac{\Gamma \vdash t_1 : [\tau_1] \quad \Gamma \vdash t_2 : \tau \quad \Gamma, x_1 : \tau_1, x}{\Gamma \vdash \mathbf{case}\ t_1\ \mathbf{of}\ \{[] \mapsto t_2; x_1 :: x_2}$$

Figure 1.6: Underlying type system ($\Gamma \vdash t : \tau$)

$$\frac{t_1 \longrightarrow t_1'}{t_1\ t_2 \longrightarrow t_1'\ t_2}\ \text{[E-App]} \quad \frac{}{(\lambda x : \widehat{\tau}\ \&\ \xi.t_1)\ t_2 \longrightarrow t_1[t_2/x]}\ \text{[E-AppAbs]} \quad \frac{}{\lightning^{\ell}\ t_2 \longrightarrow \lightning^{\ell}}\ \text{[E-AppExn]}$$

$$\frac{t \longrightarrow t'}{t\ \langle\xi\rangle \longrightarrow t'\ \langle\xi\rangle}\ \text{[E-AnnApp]} \quad \frac{}{(\Lambda e :: \kappa.t)\ \langle\xi\rangle \longrightarrow t[\xi/e]}\ \text{[E-AnnAppAbs]}$$

$$\frac{t \longrightarrow t'}{\textbf{fix}\ x : \widehat{\tau}\ \&\ \xi.t \longrightarrow \textbf{fix}\ x : \widehat{\tau}\ \&\ \xi.t'}\ \text{[E-Fix}_1\text{]} \quad \frac{}{\textbf{fix}\ x : \widehat{\tau}\ \&\ \xi.t \longrightarrow t[\textbf{fix}\ x : \widehat{\tau}\ \&\ \xi.t/x]}\ \text{[E-Fix}_2\text{]}$$

$$\frac{t_1 \longrightarrow t_1'}{t_1 \oplus t_2 \longrightarrow t_1' \oplus t_2}\ \text{[E-Op}_1\text{]} \quad \frac{t_2 \longrightarrow t_2'}{t_1 \oplus t_2 \longrightarrow t_1 \oplus t_2'}\ \text{[E-Op}_2\text{]} \quad \frac{}{v_1 \oplus v_2 \longrightarrow [\![v_1 \oplus v_2]\!]}\ \text{[E-Op]}$$

$$\frac{}{\lightning^{\ell} \oplus t_2 \longrightarrow \lightning^{\ell}}\ \text{[E-OpExn}_1\text{]} \quad \frac{}{t_1 \oplus \lightning^{\ell} \longrightarrow \lightning^{\ell}}\ \text{[E-OpExn}_2\text{]}$$

$$\frac{t_1 \longrightarrow t_1'}{t_1\ \textbf{seq}\ t_2 \longrightarrow t_1'\ \textbf{seq}\ t_2}\ \text{[E-Seq}_1\text{]} \quad \frac{}{v_1\ \textbf{seq}\ t_2 \longrightarrow t_2}\ \text{[E-Seq}_2\text{]} \quad \frac{}{\lightning^{\ell}\ \textbf{seq}\ t_2 \longrightarrow \lightning^{\ell}}\ \text{[E-SeqExn]}$$

$$\frac{t_1 \longrightarrow t_1'}{\textbf{if}\ t_1\ \textbf{then}\ t_2\ \textbf{else}\ t_3 \longrightarrow \textbf{if}\ t_1'\ \textbf{then}\ t_2\ \textbf{else}\ t_3}\ \text{[E-If]} \quad \frac{}{\textbf{if true then}\ t_2\ \textbf{else}\ t_3 \longrightarrow t_2}\ \text{[E-IfTrue]}$$

$$\frac{}{\textbf{if false then}\ t_2\ \textbf{else}\ t_3 \longrightarrow t_3}\ \text{[E-IfFalse]} \quad \frac{}{\textbf{if}\ \lightning^{\ell}\ \textbf{then}\ t_2\ \textbf{else}\ t_3 \longrightarrow \lightning^{\ell}}\ \text{[E-IfExn]}$$

$$\frac{t_1 \longrightarrow t_1'}{\textbf{case}\ t_1\ \textbf{of}\ \{[] \mapsto t_2; x_1 :: x_2 \mapsto t_3\} \longrightarrow \textbf{case}\ t_1'\ \textbf{of}\ \{[] \mapsto t_2; x_1 :: x_2 \mapsto t_3\}}\ \text{[E-Case]}$$

$$\frac{}{\textbf{case}\ []\ \textbf{of}\ \{[] \mapsto t_2; x_1 :: x_2 \mapsto t_3\} \longrightarrow t_2}\ \text{[E-CaseNil]} \quad \frac{}{\textbf{case}\ t_1 :: t_1'\ \textbf{of}\ \{[] \mapsto t_2; x_1 :: x_2 \mapsto t_3\} \longrightarrow}$$

$$\frac{}{\textbf{case}\ \lightning^{\ell}\ \textbf{of}\ \{[] \mapsto t_2; x_1 :: x_2 \mapsto t_3\} \longrightarrow \lightning^{\ell}}\ \text{[E-CaseExn]}$$

Figure 1.7: Operational semantics ($t_1 \longrightarrow t_2$)

$$\frac{}{\overline{e_i :: \kappa_i} \vdash \mathbf{bool} : \widehat{\mathbf{bool}} \;\&\; e\ \overline{e_i} \triangleright e :: \overline{\kappa_i} \Rightarrow \mathbf{EXN}}\ [\text{C-Bool}] \qquad \frac{}{\overline{e_i :: \kappa_i} \vdash \mathbf{int} : \widehat{\mathbf{int}} \;\&\; e\ \overline{e_i} \triangleright e :: \overline{\kappa_i} \Rightarrow \mathbf{EXN}}\ [\text{C}$$

$$\frac{\overline{e_i :: \kappa_i} \vdash \tau : \widehat{\tau} \;\&\; \xi \triangleright \overline{e_j :: \kappa_j}}{\overline{e_i :: \kappa_i} \vdash [\tau] : [\widehat{\tau}\langle\xi\rangle] \;\&\; e\ \overline{e_i} \triangleright e :: \overline{\kappa_i} \Rightarrow \mathbf{EXN}, \overline{e_j :: \kappa_j}}\ [\text{C-List}]$$

$$\frac{\vdash \tau_1 : \widehat{\tau}_1 \;\&\; \xi_1 \triangleright \overline{e_j :: \kappa_j} \qquad \overline{e_i :: \kappa_i}, \overline{e_j :: \kappa_j} \vdash \tau_2 : \widehat{\tau}_2 \;\&\; \xi_2 \triangleright \overline{e_k :: \kappa_k}}{\overline{e_i :: \kappa_i} \vdash \tau_1 \to \tau_2 : \forall \overline{e_j :: \kappa_j}.\, (\widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle) \;\&\; e\ \overline{e_i} \triangleright e :: \overline{\kappa_i} \Rightarrow \mathbf{EXN}, \overline{e_k :: \kappa_k}}\ [\text{C-Arr}]$$

Figure 1.8: Type completion ($\Delta \vdash \tau : \widehat{\tau} \;\&\; \xi \triangleright \Delta'$)

$$\frac{}{\Gamma, x : \widehat{\tau} \;\&\; \xi; \Delta \vdash x : \widehat{\tau} \;\&\; \xi}\ [\text{T-Var}] \qquad \frac{}{\Gamma; \Delta \vdash c_\tau : \bot_\tau \;\&\; \emptyset}\ [\text{T-Con}] \qquad \frac{}{\Gamma; \Delta \vdash \lightning^{\ell}_{\tau} : \bot_\tau \;\&\; \{\ell\}}\ [\text{T-Crash}]$$

$$\frac{\Gamma, x : \widehat{\tau}_1 \;\&\; \xi_1; \Delta \vdash t : \widehat{\tau}_2 \;\&\; \xi_2}{\Gamma; \Delta \vdash \lambda x : \widehat{\tau}_1 \;\&\; \xi_1 . t : \widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle \;\&\; \emptyset}\ [\text{T-Abs}] \qquad \frac{\Gamma; \Delta, e :: \kappa \vdash t : \widehat{\tau} \;\&\; \xi \quad e \notin \text{fv}(\Gamma, \xi)}{\Gamma; \Delta \vdash \Lambda e :: \kappa . t : \forall e :: \kappa . \widehat{\tau} \;\&\; \xi}\ [\text{T-AnnAbs}$$

$$\frac{\Gamma; \Delta \vdash t_1 : \widehat{\tau}_2\langle\xi_2\rangle \to \widehat{\tau}\langle\xi\rangle \;\&\; \xi \quad \Gamma; \Delta \vdash t_2 : \widehat{\tau}_2 \;\&\; \xi_2}{\Gamma; \Delta \vdash t_1\ t_2 : \widehat{\tau} \;\&\; \xi}\ [\text{T-App}] \qquad \frac{\Gamma; \Delta \vdash t_1 : \forall e :: \kappa . \widehat{\tau} \;\&\; \xi \quad \Delta \vdash \xi_2 : \kappa}{\Gamma; \Delta \vdash t_1\ \langle\xi_2\rangle : \widehat{\tau}[\xi_2/e] \;\&\; \xi}\ [\text{T-A}$$

$$\frac{\Gamma, x : \widehat{\tau} \;\&\; \xi; \Delta \vdash t : \widehat{\tau} \;\&\; \xi}{\Gamma; \Delta \vdash \textbf{fix}\ x : \widehat{\tau} \;\&\; \xi . t : \widehat{\tau} \;\&\; \xi}\ [\text{T-Fix}]$$

$$\frac{\Gamma; \Delta \vdash t_1 : \widehat{\textbf{int}} \;\&\; \xi \quad \Gamma; \Delta \vdash t_2 : \widehat{\textbf{int}} \;\&\; \xi}{\Gamma; \Delta \vdash t_1 \oplus t_2 : \widehat{\textbf{bool}} \;\&\; \xi}\ [\text{T-Op}] \qquad \frac{\Gamma; \Delta \vdash t_1 : \widehat{\tau}_1 \;\&\; \xi \quad \Gamma; \Delta \vdash t_2 : \widehat{\tau}_2 \;\&\; \xi}{\Gamma; \Delta \vdash t_1\ \textbf{seq}\ t_2 : \widehat{\tau}_2 \;\&\; \xi}\ [\text{T-Seq}]$$

$$\frac{\Gamma; \Delta \vdash t_1 : \widehat{\textbf{bool}} \;\&\; \xi \quad \Gamma; \Delta \vdash t_2 : \widehat{\tau} \;\&\; \xi \quad \Gamma; \Delta \vdash t_3 : \widehat{\tau} \;\&\; \xi}{\Gamma; \Delta \vdash \textbf{if}\ t_1\ \textbf{then}\ t_2\ \textbf{else}\ t_3 : \widehat{\tau} \;\&\; \xi}\ [\text{T-If}]$$

$$\frac{}{\Gamma; \Delta \vdash []_\tau : [\bot_\tau\langle\emptyset\rangle] \;\&\; \emptyset}\ [\text{T-Nil}] \qquad \frac{\Gamma; \Delta \vdash t_1 : \widehat{\tau} \;\&\; \xi_1 \quad \Gamma; \Delta \vdash t_2 : [\widehat{\tau}\langle\xi_1\rangle] \;\&\; \xi_2}{\Gamma; \Delta \vdash t_1 :: t_2 : [\widehat{\tau}\langle\xi_1\rangle] \;\&\; \xi_2}\ [\text{T-Cons}]$$

$$\frac{\Gamma; \Delta \vdash t_1 : [\widehat{\tau}_1\langle\xi_1\rangle] \;\&\; \xi' \quad \Gamma; \Delta \vdash t_2 : \widehat{\tau} \;\&\; \xi \quad \Gamma, x_1 : \widehat{\tau}_1 \;\&\; \xi_1, x_2 : [\widehat{\tau}_1\langle\xi_1\rangle] \;\&\; \xi'; \Delta \vdash t_3 : \widehat{\tau} \;\&\; \xi \quad \Delta \vdash \xi' \leqslant}{\Gamma; \Delta \vdash \textbf{case}\ t_1\ \textbf{of}\ \{[] \mapsto t_2; x_1 :: x_2 \mapsto t_3\} : \widehat{\tau} \;\&\; \xi}$$

$$\frac{\Gamma; \Delta \vdash t : \widehat{\tau}' \;\&\; \xi' \quad \Delta \vdash \widehat{\tau}' \leqslant \widehat{\tau} \quad \Delta \vdash \xi' \leqslant \xi}{\Gamma; \Delta \vdash t : \widehat{\tau} \;\&\; \xi}\ [\text{T-Sub}]$$

Figure 1.9: Declarative type system ($\Gamma; \Delta \vdash t : \widehat{\tau} \;\&\; \xi$)

$$\frac{}{\Gamma, x : \widehat{\tau} \,\&\, \xi; \Delta \vdash x \hookrightarrow x : \widehat{\tau} \,\&\, \xi}\ \text{[L-Var]} \qquad \frac{}{\Gamma; \Delta \vdash c_\tau \hookrightarrow c_\tau : \bot_\tau \,\&\, \emptyset}\ \text{[L-Con]} \qquad \frac{}{\Gamma; \Delta \vdash \lightning^{\ell}_{\tau} \hookrightarrow \lightning^{\ell}_{\tau}$$

$$\frac{\Delta, \overline{e_i :: \kappa_i} \vdash \widehat{\tau}_1 \downarrow \tau_1 \quad \Delta, \overline{e_i :: \kappa_i} \vdash \xi_1 :: \textsc{exn} \quad \Gamma, x : \widehat{\tau}_1 \,\&\, \xi_1; \Delta, \overline{e_i :: \kappa_i} \vdash t \hookrightarrow t' : \widehat{\tau}_2 \,\&\, \xi_2}{\Gamma; \Delta \vdash \lambda x : \tau_1.t \hookrightarrow \Lambda \overline{e_i :: \kappa_i}.\lambda x : \widehat{\tau}_1 \,\&\, \xi_1.t' : \forall \overline{e_i :: \kappa_i}.\widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle \,\&\, \emptyset}\ \text{[L-Abs]}$$

$$\frac{\begin{array}{c}\Delta \vdash \widehat{\tau}_2 \leqslant \widehat{\tau}_1[\overline{\zeta_i}/\overline{e_i}] \quad \Delta \vdash \xi_2 \leqslant \xi_1[\overline{\zeta_i}/\overline{e_i}] \quad \overline{\Delta \vdash \zeta_i :: \kappa_i} \\ \Gamma; \Delta \vdash t_1 \hookrightarrow t_1' : \forall \overline{e_i :: \kappa_i}.\widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}\langle\xi\rangle \,\&\, \xi' \quad \Gamma; \Delta \vdash t_2 \hookrightarrow t_2' : \widehat{\tau}_2 \,\&\, \xi_2\end{array}}{\Gamma; \Delta \vdash t_1\ t_2 \hookrightarrow t_1'\ \langle\overline{\zeta_i}\rangle\ t_2' : \widehat{\tau}[\overline{\zeta_i}/\overline{e_i}] \,\&\, \xi[\overline{\zeta_i}/\overline{e_i}] \cup \xi'}\ \text{[L-App]}$$

$$\frac{\Delta \vdash \widehat{\tau} \downarrow \tau \quad \Delta \vdash \xi :: \textsc{exn} \quad \Gamma, x : \widehat{\tau} \,\&\, \xi; \Delta \vdash t \hookrightarrow t' : \widehat{\tau}' \,\&\, \xi' \quad \Delta \vdash \widehat{\tau}' \leqslant \widehat{\tau} \quad \Delta \vdash \xi' \leqslant \xi}{\Gamma; \Delta \vdash \textbf{fix}\ x : \tau.t \hookrightarrow \textbf{fix}\ x : \widehat{\tau} \,\&\, \xi.t' : \widehat{\tau} \,\&\, \xi}\ \text{[L-Fix]}$$

$$\frac{\Gamma; \Delta \vdash t_1 \hookrightarrow t_1' : \widehat{\textbf{int}} \,\&\, \xi_1 \quad \Gamma; \Delta \vdash t_2 \hookrightarrow t_2' : \widehat{\textbf{int}} \,\&\, \xi_2}{\Gamma; \Delta \vdash t_1 \oplus t_2 \hookrightarrow t_1' \oplus t_2' : \widehat{\textbf{bool}} \,\&\, \xi_1 \cup \xi_2}\ \text{[L-Op]} \qquad \frac{\Gamma; \Delta \vdash t_1 \hookrightarrow t_1' : \widehat{\tau}_1 \,\&\, \xi_1 \quad \Gamma; \Delta \vdash$$

$$\frac{\Gamma; \Delta \vdash t_1 \hookrightarrow t_1' : \widehat{\textbf{bool}} \,\&\, \xi_1 \quad \Gamma; \Delta \vdash t_2 \hookrightarrow t_2' : \widehat{\tau}_2 \,\&\, \xi_2 \quad \Gamma; \Delta \vdash t_3 \hookrightarrow t_3' : \widehat{\tau}_3 \,\&\, \xi_3}{\Gamma; \Delta \vdash \textbf{if}\ t_1\ \textbf{then}\ t_2\ \textbf{else}\ t_3 \hookrightarrow \textbf{if}\ t_1'\ \textbf{then}\ t_2'\ \textbf{else}\ t_3' : \widehat{\tau}_2 \sqcup \widehat{\tau}_3 \,\&\, \xi_1 \cup \xi_2 \cup \xi_3}\ \text{[L-If]}$$

$$\frac{}{\Gamma; \Delta \vdash []_\tau \hookrightarrow []_\tau : [\bot_\tau\langle\emptyset\rangle] \,\&\, \emptyset}\ \text{[L-Nil]} \qquad \frac{\Gamma; \Delta \vdash t_1 \hookrightarrow t_1' : \widehat{\tau}_1 \,\&\, \xi_1 \quad \Gamma; \Delta \vdash t_2 \hookrightarrow t_2' : [\widehat{\tau}_1'\langle\xi_1'\rangle] \,\&$$

$$\frac{\Gamma; \Delta \vdash t_1 \hookrightarrow t_1' : [\widehat{\tau}_1\langle\xi_1\rangle] \,\&\, \xi_1' \quad \Gamma; \Delta \vdash t_2 \hookrightarrow t_2' : \widehat{\tau}_2 \,\&\, \xi_2 \quad \Gamma, x_1 : \widehat{\tau}_1 \,\&\, \xi_1, x_2 : [\widehat{\tau}_1\langle\xi_1\rangle] \,\&\, \xi_1'; \Delta \vdash$$

$$\Gamma; \Delta \vdash \textbf{case}\ t_1\ \textbf{of}\ \{[] \mapsto t_2; x_1 :: x_2 \mapsto t_3\} \hookrightarrow \textbf{case}\ t_1'\ \textbf{of}\ \{[] \mapsto t_2'; x_1 :: x_2 \mapsto t_3'\} : \widehat{\tau}_2 \sqcup \widehat{\tau}_3 \,\&$$

Figure 1.10: Syntax-directed type elaboration system ($\Gamma; \Delta \vdash t \hookrightarrow t' : \widehat{\tau} \,\&\, \xi$)

## 1.4 Exception types

The syntax of well-formed exception types is given in Figures 1.11 and 1.12. We let $e$ range over an infinite set of exception set variables and $\ell$ over a finite set of exception labels. An exception type $\widehat{\tau}$ is formed out of base types (booleans and integers), compound types (lists), function types, and quantifiers (ranging over exception set variables[2]).

$$
\begin{array}{rcll}
\kappa \in \mathbf{ExnKi} & ::= & \textsc{exn} & \text{(exception set)} \\
& \mid & \kappa_1 \Rightarrow \kappa_2 & \text{(exception set operator)} \\
\\
\xi, \zeta \in \mathbf{Exn} & ::= & e & \text{(exception set variables)} \\
& \mid & \lambda e : \kappa.\xi & \text{(exception set abstraction)} \\
& \mid & \xi_1\ \xi_2 & \text{(exception set application)} \\
& \mid & \emptyset & \text{(empty exception set)} \\
& \mid & \{\ell\} & \text{(singleton exception set)} \\
& \mid & \xi_1 \cup \xi_2 & \text{(exception set union)} \\
\\
\widehat{\tau} \in \mathbf{ExnTy} & ::= & \forall e :: \kappa.\widehat{\tau} & \text{(exception set quantification)} \\
& \mid & \widehat{\mathbf{bool}} & \text{(boolean type)} \\
& \mid & \widehat{\mathbf{int}} & \text{(integer type)} \\
& \mid & [\widehat{\tau}\langle\xi\rangle] & \text{(list type)} \\
& \mid & \widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle & \text{(function type)}
\end{array}
$$

Figure 1.11: Exception types: syntax

For a list with exception type $[\widehat{\tau}\langle\xi\rangle]$ and effect $\zeta$, the type $\widehat{\tau}$ of the elements in the list is *annotated* with an exception set expression $\xi$ of kind EXN. This expression gives a set of exceptions, from which any one may be raised when an element of the list is forced. The effect $\zeta$ gives a set of exceptions, from

[2]To avoid complicating the presentation we do *not* allow quantification over type variables, i.e. polymorphism in the underlying type system.

which any one may be raised when a constructor forming the spine of the list is forced.

For a function with exception type $\widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle$ and effect $\zeta$, the argument of type $\widehat{\tau}_1$ is annotated with an exception set expression $\xi_1$ that gives a set of exceptions that may be raised if the argument is forced in the body of the function. The result of type $\widehat{\tau}_2$ is annotated with an exception set expression $\xi_2$ that gives the set of exceptions that may be raised when the result of the function is forced. The effect $\zeta$ gives the set of exceptions from which any one may be raised when the function closure is forced.

**Example 2.** The identity function

$$\begin{aligned} &id \;:\; \forall e.\widehat{\mathbf{bool}}\langle e\rangle \to \widehat{\mathbf{bool}}\langle e\rangle \;\&\; \emptyset \\ &id = \lambda x.x \end{aligned}$$

propagates any exceptional value passed to it as an argument to the result unchanged. As the identity function is constructed by a literal $\lambda$-abstraction, no exception is raised when the resulting closure is forced, hence the empty effect.

**Example 3.** The exceptional function value

$$\lightning^{\mathbf{E}}_{\mathbf{bool}\to\mathbf{bool}} : \forall e.\widehat{\mathbf{bool}}\langle e\rangle \to \widehat{\mathbf{bool}}\langle\emptyset\rangle \;\&\; \{\mathbf{E}\}$$

raises an exception when its closure is forced—as happens when it is applied to an argument, for example. As this function can never produce a result, it certainly cannot produce an exceptional value. So the result type is annotated with an empty exception set.

The exception set expressions $\xi$ and their kinds $\kappa$ are an instance of the $\lambda^{\cup}$-calculus, where exception set expressions are terms and kinds are the types. As the constants we takes the set of exception labels present in the program. Two exception set expressions are considered equivalent if they are convertible as $\lambda^{\cup}$-terms, which is to say that they reduce to the same normal form.

The type system resembles System $F_\omega$ Girard (1972) in that we have quantification, abstraction and application at the type level. A key difference is that abstraction and application are restricted to the effects (**Exn**) and cannot be used in the types (**ExnTy**) directly. Quantification, on the other hand, is restricted to the types, where it ranges over effects, and is not allowed to appear in the effect itself. The types thus remain predicative.

$$\frac{\Delta, e :: \kappa \vdash \widehat{\tau} \text{ wff}}{\Delta \vdash \forall e :: \kappa.\widehat{\tau} \text{ wff}} \text{ [W-FORALL]}$$

$$\frac{}{\Delta \vdash \widehat{\mathbf{bool}} \text{ wff}} \text{ [W-BOOL]} \quad \frac{}{\Delta \vdash \widehat{\mathbf{int}} \text{ wff}} \text{ [W-INT]}$$

$$\frac{\Delta \vdash \widehat{\tau} \text{ wff} \quad \Delta \vdash \xi :: \textsc{exn}}{\Delta \vdash [\widehat{\tau}\langle \xi \rangle] \text{ wff}} \text{ [W-LIST]}$$

$$\frac{\Delta \vdash \widehat{\tau}_1 \text{ wff } \Delta \vdash \xi_1 :: \textsc{exn } \Delta \vdash \widehat{\tau}_2 \text{ wff } \Delta \vdash \xi_2 :: \textsc{exn}}{\Delta \vdash \widehat{\tau}_1\langle \xi_1 \rangle \to \widehat{\tau}_2\langle \xi_2 \rangle \text{ wff}} \text{ [W-ARR]}$$

Figure 1.12: Exception types: well-formedness ($\Delta \vdash \widehat{\tau}$ wff)

### 1.4.1 Subtyping

Exception types are endowed with the usual subtyping relation for type-and-effect systems (Figure 1.13). The function type is contravariant in its first argument for both the type and the effect. The subeffecting relation $\Delta \vdash \xi_1 \leqslant \xi_2$ is the subsumption relation $\Gamma \vdash t_1 \lesssim t_2$ from the $\lambda^{\cup}$-calculus (Definition 2).

$$\frac{\Delta, e :: \kappa \vdash \widehat{\tau}_1 \leqslant \widehat{\tau}_2}{\Delta \vdash \forall e :: \kappa.\widehat{\tau}_1 \leqslant \forall e :: \kappa.\widehat{\tau}_2} \text{ [S-FORALL]}$$

$$\frac{}{\Delta \vdash \widehat{\tau} \leqslant \widehat{\tau}} \text{ [S-REFL]} \quad \frac{\Delta \vdash \widehat{\tau}_1 \leqslant \widehat{\tau}_2 \quad \Delta \vdash \widehat{\tau}_2 \leqslant \widehat{\tau}_3}{\Delta \vdash \widehat{\tau}_1 \leqslant \widehat{\tau}_3} \text{ [S-TRANS]}$$

$$\frac{\Delta \vdash \widehat{\tau} \leqslant \widehat{\tau}' \quad \Delta \vdash \xi \leqslant \xi'}{\Delta \vdash [\widehat{\tau}\langle \xi \rangle] \leqslant [\widehat{\tau}'\langle \xi' \rangle]} \text{ [S-LIST]}$$

$$\frac{\Delta \vdash \widehat{\tau}_1' \leqslant \widehat{\tau}_1 \;\; \Delta \vdash \xi_1' \leqslant \xi_1 \;\; \Delta \vdash \widehat{\tau}_2 \leqslant \widehat{\tau}_2' \;\; \Delta \vdash \xi_2 \leqslant \xi_2'}{\Delta \vdash \widehat{\tau}_1\langle \xi_1 \rangle \to \widehat{\tau}_2\langle \xi_2 \rangle \leqslant \widehat{\tau}_1'\langle \xi_1' \rangle \to \widehat{\tau}_2'\langle \xi_2' \rangle} \text{ [S-ARR]}$$

Figure 1.13: Exception types: subtyping relation ($\Delta \vdash \widehat{\tau}_1 \leqslant \widehat{\tau}_2$)

### 1.4.2 Conservative types

Any program that is typeable in the underlying type system should also have an exception type: the exception type system is a *conservative extension* of the underlying type system. Like type systems for strictness or control flow analysis—and unlike type systems for information flow security or dimensional analysis—we do not want to reject any program that is well-typed in the underlying type system, but merely provide more insight into its behavior.

If we furthermore want the type system to be modular—allowing type checking and inference to work on individual modules instead of whole programs—we cannot and need not make any assumptions about the exception types of the arguments that are applied to any function, as the function may be called from outside the module with an argument that also comes from outside the module and which we cannot know anything about.

For base and compound types that stand in an argument position their effect and any nested annotations must thus be able to be instantiated to any arbitrary exception set expression. They must therefore be exception set variables that have been universally quantified.

These observations lead to the following definition of *conservative exception types*:[3]

**Definition 5.** An exception set expression $\xi$ is *simple* if it is a single exception set variable $e$, an exception set expression is a *pattern* if it fits Definition 4, and any exception set expression is *conservative*.

We lift these three judgments to exception types $\widehat{\tau}$ in the following manner:

- If $\widehat{\tau} = \widehat{\mathbf{bool}}$ or $\widehat{\tau} = \widehat{\mathbf{int}}$, then $\widehat{\tau}$ is simple, a pattern and conservative.
- If $\widehat{\tau} = [\widehat{\tau}'\langle\xi\rangle]$, then $\widehat{\tau}$ is simple, a pattern or conservative if $\widehat{\tau}'$ and $\xi$ are respectively simple, patterns or conservative.
- If $\widehat{\tau} = \forall\overline{e_i :: \kappa_i}.\widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle$, then $\widehat{\tau}$ is both simple and a pattern if $\widehat{\tau}_1$ and $\xi_1$ are simple and $\widehat{\tau}_2$ and $\xi_2$ are patterns; and $\widehat{\tau}$ is conservative if $\widehat{\tau}_1$ and $\xi_1$ are simple and $\widehat{\tau}_2$ and $\xi_2$ are conservative.

**Example 4.** The function *tail* can be applied to any list, but may produce an additional exceptional value **E**, because it is partial:

[3] Holdermans and Hage (2010) call pattern types *fully parametric* and conservative types *fully flexible*.

$$\mathit{tail} : \forall e_1\ e_2.\ [\mathbf{b\widehat{oo}l}\langle e_1\rangle]\langle e_2\rangle \to [\mathbf{b\widehat{oo}l}\langle e_1\rangle]\langle e_2 \cup \{\mathbf{E}\}\rangle\ \&\ \emptyset$$

The type and effect of the argument are simple, while the type and effect of the result are conservative, making the whole type conservative.

The conjunction operator $\wedge$ can be applied to any two booleans, and—operators being strict in both arguments—will propagate any exceptional values:

$$\wedge\ : \forall e_1.\mathbf{b\widehat{oo}l}\langle e_1\rangle \to (\forall e_2.\mathbf{b\widehat{oo}l}\langle e_2\rangle \to \mathbf{b\widehat{oo}l}\langle e_1 \cup e_2\rangle)\langle\emptyset\rangle\ \&\ \emptyset$$

Here both arguments have simple types and effects.

For function types that stand in an argument position (the functional parameters of a higher-order function) the situation is slightly more complicated. For the argument of this function we can inductively assume that this is a universally quantified exception set variable. The result of this function, however, is some exception set expression that depends on the exception set variables that were quantified over in the argument. We cannot simply introduce a new exception set variable here, but must introduce a Skolem function that depends on each of the universally quantified exception set variables.

**Example 5.** Consider the higher-order function *apply* that applies its first argument to the second.

$$\begin{aligned}
\mathit{apply}\ :\ & \forall e_2 :: \textsc{exn}.\forall e_3 :: \textsc{exn} \Rightarrow \textsc{exn}.\\
& \quad (\forall e_1 :: \textsc{exn}.\mathbf{b\widehat{oo}l}\langle e_1\rangle \to \mathbf{b\widehat{oo}l}\langle e_3\ e_1\rangle)\langle e_2\rangle \to\\
& \quad\ (\forall e_4 :: \textsc{exn}.\mathbf{b\widehat{oo}l}\langle e_4\rangle \to \mathbf{b\widehat{oo}l}\langle e_2 \cup e_3\ e_4\rangle)\langle\emptyset\rangle\\
& \&\ \emptyset\\
\mathit{apply} = {} & \lambda f.\lambda x.f\ x
\end{aligned}$$

The first (functional) argument of *apply* has exception type $\forall e_1 :: \textsc{exn}.\mathbf{b\widehat{oo}l}\langle e_1\rangle \to \mathbf{b\widehat{oo}l}\langle e_3\ e_1\rangle$ and effect $e_2$. It can be instantiated with any function that accepts an argument annotated with any exception set effect, and produces a result annotated with some exception set effect depending on the exception set effect of the argument; the function closure itself may raise any exception. All functions of underlying type $\mathbf{bool} \to \mathbf{bool}$ satisfy these constraints, so we are not really constrained at all.

As $e_1$ has been quantified over, only the exception set operator $e_3$ and the effect $e_2$ are left free. We quantify over them outside the outer function space

constructor, allowing them to appear in the annotation $e_2 \cup e_3\ e_4$ on the result. The exception set operator $e_3$ is now applied to $e_4$, as the term-level application $f\ x$ instantiates the quantified exception set variable $e_1$ to $e_4$.

(Note that the exception annotation $e_2$ on the closure—unlike the exception set operator $e_3$ on the result—does not depend on the exception variable $e_1$, the annotation on the argument. As a closure is already a value, it being exceptional or not can never depend on the argument it is later applied to.)

**Example 6.** The semantics of terms in the source language is not invariant under $\eta$-conversion in the presence of exceptional values—thus neither are exception types. The term

$$\lambda x : \mathbf{bool}.\lightning^{\mathbf{E}}_{\mathbf{bool}\to\mathbf{bool}}\ x : \forall e :: \textsc{exn}.\mathbf{b\widehat{oo}l}\langle e\rangle \xrightarrow{\emptyset} \mathbf{b\widehat{oo}l}\langle\{\mathbf{E}\}\rangle$$

does not have the same exception type as the $\eta$-equivalent term

$$\lightning^{\mathbf{E}}_{\mathbf{bool}\to\mathbf{bool}} : \forall e :: \textsc{exn}.\mathbf{b\widehat{oo}l}\langle e\rangle \xrightarrow{\{\mathbf{E}\}} \mathbf{b\widehat{oo}l}\langle\emptyset\rangle$$

They cannot be distinguished by applying them to an argument

$$\begin{array}{ll}(\lambda x : \mathbf{bool}.\lightning^{\mathbf{E}}_{\mathbf{bool}\to\mathbf{bool}}\ x)\ \mathbf{true} & : \mathbf{b\widehat{oo}l}\ \&\ \{\mathbf{E}\}\\ \lightning^{\mathbf{E}}_{\mathbf{bool}\to\mathbf{bool}}\ \mathbf{true} & : \mathbf{b\widehat{oo}l}\ \&\ \{\mathbf{E}\}\end{array}$$

but they can be distinguished by forcing the closure

$$\begin{array}{ll}(\lambda x : \mathbf{bool}.\lightning^{\mathbf{E}}_{\mathbf{bool}\to\mathbf{bool}}\ x)\ \mathbf{seq}\ \mathbf{true} & : \mathbf{b\widehat{oo}l}\ \&\ \emptyset\\ \lightning^{\mathbf{E}}_{\mathbf{bool}\to\mathbf{bool}}\ \mathbf{seq}\ \mathbf{true} & : \mathbf{b\widehat{oo}l}\ \&\ \{\mathbf{E}\}\end{array}$$

### 1.4.3 Exception type completion

Given an underlying type $\tau$ we can compute the most general exception type $\widehat{\tau}$ that erases to $\tau$. This is done using the type completion system in Figure 1.8, that defines a type completion relation $\Delta \vdash \tau : \widehat{\tau}\ \&\ \xi \triangleright \Delta'$. A judgment $\overline{e_i :: \kappa_i} \vdash \tau : \widehat{\tau}\ \&\ \xi \triangleright \overline{e_j :: \kappa_j}$ is read: if the kinded exception set variables $\overline{e_i :: \kappa_i}$ are in scope, then the underlying type $\tau$ is completed to the exception type $\widehat{\tau}$ and effect $\xi$, while introducing the kinded free exception set variables $\overline{e_j :: \kappa_j}$. A completed exception type is always a pattern type.

**Example 7.** The higher-order underlying type

$$[\mathbf{bool} \to \mathbf{bool}] \to [\mathbf{bool}] \to [\mathbf{bool}]$$

is completed to the pattern type

$$\begin{aligned}
&\forall e_2 :: \textsc{exn}.\forall e_2' :: \textsc{exn}.\forall e_3 :: \textsc{exn} \Rightarrow \textsc{exn}.\\
&\quad [\forall e_1 :: \textsc{exn}.\widehat{\mathbf{bool}}\langle e_1\rangle \xrightarrow{e_2'} \widehat{\mathbf{bool}}\langle e_3\ e_1\rangle]\langle e_2\rangle \to\\
&\qquad (\forall e_5 :: \textsc{exn}.\forall e_5' :: \textsc{exn}.[\widehat{\mathbf{bool}}\langle e_5'\rangle]\langle e_5\rangle \xrightarrow{e_6\ e_2\ e_2'\ e_3}\\
&\qquad\qquad \left[\widehat{\mathbf{bool}}\langle e_7'\ e_2\ e_2'\ e_3\ e_5\ e_5'\rangle\right]\langle e_7\ e_2\ e_2'\ e_3\ e_5\ e_5'\rangle)
\end{aligned}$$

with effect $e_4$, and while introducing the free exception set variables

$$\begin{aligned}
e_4 &:: \textsc{exn},\\
e_6 &:: \textsc{exn} \Rightarrow \textsc{exn} \Rightarrow (\textsc{exn} \Rightarrow \textsc{exn}) \Rightarrow \textsc{exn},\\
e_7, e_7' &:: \textsc{exn} \Rightarrow \textsc{exn} \Rightarrow (\textsc{exn} \Rightarrow \textsc{exn}) \Rightarrow \textsc{exn} \Rightarrow \textsc{exn} \Rightarrow \textsc{exn}
\end{aligned}$$

Note that the types of both arguments are simple types with simple exception annotations. However, as the first argument is a functional argument, the result type of that function is still a pattern.

The exception annotation on the right-most function-space constructor is a pattern that depends on $e_2$, $e_2'$ and $e_3$. While we previously noted that the annotation on a function-space constructor cannot depend on the annotation belonging to the argument of that function, it is possible for a set of exceptional values that the closure may come to depend on any previous arguments of the whole function. This is more concretely demonstrated by the following function:

$$\begin{aligned}
&f :: \forall e_1, e_2 :: \textsc{exn}.\widehat{\mathbf{bool}}\langle e_1\rangle \xrightarrow{\emptyset} \widehat{\mathbf{bool}}\langle e_2\rangle \xrightarrow{e_1} \widehat{\mathbf{bool}}\langle e_2\rangle\\
&f = \lambda x : \mathbf{bool}.x\ \mathbf{seq}\ \lambda y : \mathbf{bool}.y
\end{aligned}$$

Whether the closure that is returned after partially applying $f$ to one argument is an exceptional value or not, depends on that argument $x$ being exceptional or not.

### 1.4.4 Least exception types

Besides completing an underlying type $\tau$ to a most general exception type, we also want to compute a least exception type $\bot_\tau$. Given an effect kind $\overline{\kappa_i \Rightarrow}\textsc{exn}$, denote by $\emptyset_{\overline{\kappa_i \Rightarrow}\textsc{exn}}$ the effect $\lambda\overline{e_i :: \kappa_i}.\emptyset$. We can construct a least exception type by first completing the type $\tau$ to the most general exception type, and then substituting $\emptyset_{\kappa_j}$ for all free freshly introduced exception set variables $\overline{e_j :: \kappa_j}$.

**Example 8.** The least exception type

$$\bot_{[\mathbf{bool}\to\mathbf{bool}]\to[\mathbf{bool}]\to[\mathbf{bool}]}$$

is the conservative type

$$\begin{aligned}&\forall e_2 :: \textsc{exn}.\forall e_2' :: \textsc{exn}.\forall e_3 :: \textsc{exn} \Rightarrow \textsc{exn}.\\ &\quad [\forall e_1 :: \textsc{exn}.\widehat{\mathbf{bool}}\langle e_1\rangle \xrightarrow{e_2'} \widehat{\mathbf{bool}}\langle e_3\ e_1\rangle]\langle e_2\rangle \to\\ &\qquad (\forall e_5 :: \textsc{exn}.\forall e_5' :: \textsc{exn}.[\widehat{\mathbf{bool}}\langle e_5'\rangle]\langle e_5\rangle \xrightarrow{\emptyset} [\widehat{\mathbf{bool}}\langle\emptyset\rangle]\langle\emptyset\rangle)\end{aligned}$$

### 1.4.5 Exception typing and elaboration

In Figure 1.9 we give a declarative system for deriving exception typing judgments $\Gamma;\Delta \vdash t : \widehat{\tau}\ \&\ \xi$.

These judgments work on an explicitly typed language and for this purpose we extend the terms of the source language with two new term-level constructs: effect abstraction and effect application.

As the source language is not explicitly typed, we also give a type elaboration system that given an implicitly typed term in the source language produces an explicitly typed term (Figure 1.10).

The auxiliary judgment $\Delta \vdash \widehat{\tau} \downarrow \tau$ holds for any exception type $\widehat{\tau}$ that erases to the underlying type $\tau$. The type $\widehat{\tau}_1 \sqcup \widehat{\tau}_2$ is an exception type such that $\Delta \vdash \widehat{\tau}_1 \leqslant \widehat{\tau}_1 \sqcup \widehat{\tau}_2$ and $\Delta \vdash \widehat{\tau}_2 \leqslant \widehat{\tau}_1 \sqcup \widehat{\tau}_2$.

### 1.4.6 Presentation of exception types

For most-general conservative exception types the location of the quantifiers is uniquely determined, we can therefore omit them from the type without introducing ambiguity. For example, the exception type of the *map* function from the introduction may be presented as:

**Terms**

$$
\begin{array}{rcll}
t \in \mathbf{ExnTm} & ::= & \ldots & \\
& | & \lambda x : \widehat{\tau} \;\&\; \xi.t & \text{(term abstraction)} \\
& | & \mathbf{fix}\ x : \widehat{\tau} \;\&\; \xi.t & \text{(general recursion)} \\
& | & \ldots & \\
& | & \Lambda e :: \kappa.t & \text{(effect abstraction)} \\
& | & t\ \langle \xi \rangle & \text{(effect application)}
\end{array}
$$

Figure 1.14: Source language: extended syntax

$$(\alpha\langle e_1\rangle \xrightarrow{e_3} \beta\langle e_2\ e_1\rangle) \to [\alpha\langle e_4\rangle]\langle e_5\rangle \to [\beta\langle e_2\ e_4 \cup e_3\rangle]\langle e_5\rangle$$

## 1.5 Type inference

A type inference algorithm is given in Figure 1.15.

### 1.5.1 Polymorphic abstraction

The cases for abstraction and application are handled similarly to the corresponding cases in Holdermans and Hage (2010).

In the case of abstractions, we first complete the type of the bound variable to a most general exception type using the procedure $\mathcal{C} : \mathbf{KiEnv} \times \mathbf{Ty} \to \mathbf{ExnTy} \times \mathbf{Exn} \times \mathbf{KiEnv}$. This procedure is a functional interpretation of the type completion relation $\Delta \vdash \tau : \widehat{\tau} \;\&\; \xi \triangleright \Delta'$, where the first two arguments $\Delta$ and $\tau$ are taken to be the domain and the last three arguments $\widehat{\tau}$, $\xi$ and $\Delta'$ are taken to be the range. Next, we infer the exception type of the body of the abstraction under the assumption that the bound variable has the just completed exception type-and-effect $\widehat{\tau}_1 \;\&\; e_1$. Finally we quantify over all free variables $\overline{e_i :: \kappa_i}$ introduced by completion.

In the case of applications, we instantiate ($\mathcal{I}$) all quantified variables of the exception type of $t_1$ with fresh exception variables. Next we use the auxiliary procedure $\mathcal{M}$ to find a matching substitution between the exception types of the formal and the actual parameters.

The interesting cases of exception type matching are the cases for list and function types, where we perform pattern unification on the exception annotations. The produced substitution $\theta$ covers all variables $\overline{e_i :: \kappa_i}$ freshly introduced by the instantiation procedure $\mathcal{I}$. Finally, we apply the substitution $\theta$ to the exception type $\widehat{\tau}'$ and effect $\xi'$ of the result of $t_1$.

### 1.5.2 Polymorphic recursion

The **fix**-construct abstracts over a variable that is of an exception polymorphic type. The algorithm handles this case with a Kleene–Mycroft iteration—which we conjecture to always converge.[4]

**Example 9** (Dussart–Henglein–Mossin)**.** Consider the term

$$\begin{aligned} f \;&:\; \mathbf{bool} \to \mathbf{bool} \to \mathbf{bool} \\ f &= \mathbf{fix}\, f' : \mathbf{bool} \to \mathbf{bool} \to \mathbf{bool}. \\ &\qquad \lambda x : \mathbf{bool}.\lambda y : \mathbf{bool}.\ \mathbf{if}\ x\ \mathbf{then\ true\ else}\ f'\ y\ x \end{aligned}$$

Algorithm $\mathcal{R}$ infers the exception type and elaborated term

$$\begin{aligned} f \;&:\; \forall e_1.\mathbf{b\widehat{oo}l}\langle e_1\rangle \xrightarrow{\emptyset} \forall e_2.\mathbf{b\widehat{oo}l}\langle e_2\rangle \xrightarrow{\emptyset} \mathbf{b\widehat{oo}l}\langle e_1 \cup e_2\rangle \\ f &= \mathbf{fix}\, f' : \forall e_1.\mathbf{b\widehat{oo}l}\langle e_1\rangle \xrightarrow{\emptyset} \forall e_2.\mathbf{b\widehat{oo}l}\langle e_2\rangle \xrightarrow{\emptyset} \mathbf{b\widehat{oo}l}\langle e_1 \cup e_2\rangle. \\ &\qquad \Lambda e_1 :: \textsc{exn}.\lambda x : \mathbf{b\widehat{oo}l}\ \&\ e_1.\Lambda e_2 :: \textsc{exn}.\lambda y : \mathbf{b\widehat{oo}l}\ \&\ e_2. \\ &\qquad\quad \mathbf{if}\ x\ \mathbf{then\ true\ else}\ f'\ \langle e_2\rangle\ y\ \langle e_1\rangle\ x \end{aligned}$$

Let us convince ourselves that the elaborated term is type-correct.

$$\begin{aligned} x &: \mathbf{b\widehat{oo}l}\ \&\ e_1 \\ \mathbf{true} &: \mathbf{b\widehat{oo}l}\ \&\ \emptyset \\ f\langle e_2\rangle\ y\ \langle e_1\rangle\ x &: \mathbf{b\widehat{oo}l}\ \&\ e_2 \cup e_1 \end{aligned}$$

Therefore,

$$\mathbf{if}\ x\ \mathbf{then\ true\ else}\ f\langle e_2\rangle\ y\ \langle e_1\rangle\ x : \mathbf{b\widehat{oo}l} \sqcup \mathbf{b\widehat{oo}l}\ \&\ e_1 \cup \emptyset \cup e_2 \cup e_1$$

[4] Holdermans and Hage (2010) note that $\lambda$-bound polymorpism gives us **fix**-bound polymorphism "for free." We believe this statement to be overly optimistic. While the highly polymorphic nature of these types do effectively force us to also handle polymorphic recursion, the inference step is arguably as complicated as the case for polymorphic abstraction.

By commutativity and idempotence of the union operator and the empty set being the unit, this reduces to

$$\textbf{if } x \textbf{ then true else } f\langle e_2\rangle\ y\ \langle e_1\rangle\ x : \widehat{\textbf{bool}} \,\&\, e_1 \cup e_2$$

Type checking is easier than type inference, however. To infer the type of the recursive definition $f$ we have to "guess" a type for it. How do we guess this type? We first try the least exception type $\bot_{\textbf{bool}\to\textbf{bool}\to\textbf{bool}}$:

$$\forall e_1.\widehat{\textbf{bool}}\langle e_1\rangle \xrightarrow{\emptyset} \forall e_2.\widehat{\textbf{bool}}\langle e_2\rangle \xrightarrow{\emptyset} \widehat{\textbf{bool}}\langle\emptyset\rangle$$

If we continue inferring the type with this guess, then we end up with a larger type than the guess:

$$\forall e_1.\widehat{\textbf{bool}}\langle e_1\rangle \xrightarrow{\emptyset} \forall e_2.\widehat{\textbf{bool}}\langle e_2\rangle \xrightarrow{\emptyset} \widehat{\textbf{bool}}\langle e_1\rangle$$

We try inferring the type again, but now start with this type as our guess instead of the least type. We end up with an even larger type:

$$\forall e_1.\widehat{\textbf{bool}}\langle e_1\rangle \xrightarrow{\emptyset} \forall e_2.\widehat{\textbf{bool}}\langle e_2\rangle \xrightarrow{\emptyset} \widehat{\textbf{bool}}\langle e_1 \cup e_2\rangle$$

Finally, if we take this type as our guess, we obtain the same type and conclude we have reached a fixed point.

TODOXExample: Glynn, Stuckey, Sulzman

### 1.5.3 Least upper bounds

The remaining cases of the algorithm are all relatively straightforward. Several of the cases (**if-then-else**, **case-of** and the list-consing constructor) require the least upper bound of two exception types to be computed. The fact that exception types and annotations occurring in argument positions of function types are always simple makes this easy, as they must be equal up to $\alpha$-renaming Holdermans and Hage (2010). This allows us to treat those arguments invariantly instead of contravariantly, obviating the need to also compute greatest lower bounds of exception types and annotations.

### 1.5.4 Complexity

There are three aspects that affect the run-time complexity of the algorithm: the complexity of the underlying type system, reduction of the effects, and the fixpoint-iteration in the inference step of the **fix**-construct. We have a simply typed underlying type system, but if we would extend this to full Hindley–Milner, then it is possible for types to become exponentially larger than terms Mairson (1990); Kfoury et al. (1990a). The effects are $\lambda^{\cup}$-terms, which contains the simply typed $\lambda$-calculus as a special case. Reduction of terms in the simply typed $\lambda$-calculus is non-elementary recursive Statman (1979). It is also easy to find an artificial family of terms that requires at least a linear number of iterations to converge to a fixpoint. For these reasons we do not believe the algorithm to have an attractive theoretical bound on time-complexity.

Anecdotal evidence suggests that the practical time-complexity is acceptable, however. Hindley–Milner has almost linear complexity in non-pathological cases. Types do not grow larger than the terms. The same seems to hold for the effects. Reduction of effects takes a small number of steps, as does the convergence of the fixpoint-iteration. In cases where the exception annotation does become too large, a widening rule could be applied.

## 1.6 Metatheory

### 1.6.1 $\lambda^{\cup}$-calculus

**Lemma 1.** *The terms $(t_1 \cup t_2)\ t$ and $t_1\ t \cup t_2\ t$ are equivalent.*

*Proof.*

$$
\begin{aligned}
&[\![(t_1 \cup t_2)\ t]\!]_\rho \\
&= \bigcup \{ \varphi([\![t]\!]_\rho) \mid \varphi \in [\![t_1 \cup t_2]\!]_\rho \} \\
&= \bigcup \{ \varphi([\![t]\!]_\rho) \mid \varphi \in [\![t_1]\!]_\rho \cup [\![t_2]\!]_\rho \} \\
&= \bigcup \{ \varphi([\![t]\!]_\rho) \mid \varphi \in [\![t_1]\!]_\rho \} \cup \bigcup \{ \varphi([\![t]\!]_\rho) \mid \varphi \in [\![t_2]\!]_\rho \} \\
&= [\![t_1\ t]\!]_\rho \cup [\![t_2\ t]\!]_\rho \\
&= [\![(t_1\ t) \cup (t_2\ t)]\!]_\rho
\end{aligned}
$$

□

**Lemma 2.** *The terms $(\lambda x : \tau . t_1) \cup (\lambda x : \tau . t_2)$ and $\lambda x : \tau . t_1 \cup t_2$ are extensionally equivalent.*

*Proof.* We show that

$$[\![((\lambda x : \tau.t_1) \cup (\lambda x : \tau.t_2))\ \ t_3]\!]_\rho = [\![(\lambda x : \tau.t_1 \cup t_2)\ \ t_3]\!]_\rho$$

for all suitable $\rho$ and $t_3$.

$$\begin{aligned}
&[\![((\lambda x : \tau.t_1) \cup (\lambda x : \tau.t_2))\ \ t_3]\!]_\rho \\
&= \bigcup \{\varphi([\![t_3]\!]_\rho) \mid \varphi \in [\![(\lambda x : \tau.t_1) \cup (\lambda x : \tau.t_2)]\!]_\rho\} \\
&= \bigcup \{\varphi([\![t_3]\!]_\rho) \mid \varphi \in [\![\lambda x : \tau.t_1]\!]_\rho \cup [\![\lambda x : \tau.t_2]\!]_\rho\} \\
&= \bigcup \left\{\varphi([\![t_3]\!]_\rho) \mid \varphi \in \left\{\lambda v \in V_\tau.[\![t_i]\!]_{\rho[x \mapsto v]} \mid i \in \{1,2\}\right\}\right\} \\
&= \bigcup \left\{[\![t_1]\!]_{\rho[x \mapsto [\![t_3]\!]_\rho]}, [\![t_2]\!]_{\rho[x \mapsto [\![t_3]\!]_\rho]}\right\} \\
&= [\![t_1]\!]_{\rho[x \mapsto [\![t_3]\!]_\rho]} \cup [\![t_2]\!]_{\rho[x \mapsto [\![t_3]\!]_\rho]} \\
&= \bigcup \left\{[\![t_1]\!]_{\rho[x \mapsto [\![t_3]\!]_\rho]} \cup [\![t_2]\!]_{\rho[x \mapsto [\![t_3]\!]_\rho]}\right\} \\
&= \bigcup \left\{[\![t_1 \cup t_2]\!]_{\rho[x \mapsto [\![t_3]\!]_\rho]}\right\} \\
&= \bigcup \left\{\varphi([\![t_3]\!]_\rho) \mid \varphi \in \left\{\lambda v \in V_\tau.[\![t_1 \cup t_2]\!]_{\rho[x \mapsto v]}\right\}\right\} \\
&= \bigcup \{\varphi([\![t_3]\!]_\rho) \mid \varphi \in [\![\lambda x : \tau.t_1 \cup t_2]\!]_\rho\} \\
&= [\![(\lambda x : \tau.t_1 \cup t_2)\ \ t_3]\!]_\rho
\end{aligned}$$

□

## 1.6.2 Declarative type system

**Lemma 3** (Canonical forms)**.**

1. *If $\widehat{v}$ is a possibly exceptional value of type $\widehat{\mathbf{bool}}$, then $\widehat{v}$ is either* **true**, **false**, *or $\lightning^\ell$.*
2. *If $\widehat{v}$ is a possibly exceptional value of type $\widehat{\mathbf{int}}$, then $\widehat{v}$ is either some integer $n$, or an exceptional value $\lightning^\ell$.*
3. *If $\widehat{v}$ is a possibly exceptional value of type $[\widehat{\tau}\langle\xi\rangle]$, then $\widehat{v}$ is either $[]$, $t :: t'$, or $\lightning^\ell$.*
4. *If $\widehat{v}$ is a possibly exceptional value of type $\widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle$, then $\widehat{v}$ is either $\lambda x : \widehat{\tau}_1 \,\&\, \xi_1.t'$ or $\lightning^\ell$.*
5. *If $\widehat{v}$ is a possibly exceptional value of type $\forall e :: \kappa.\widehat{\tau}$, then $\widehat{v}$ is $\Lambda e :: \kappa.t$*

*Proof.* For each part, inspect all forms of $\widehat{v}$ and discard the unwanted cases by inversion of the typing relation. Note that $\bot_\tau$ cannot give us a type of the form $\forall e :: \kappa.\widehat{\tau}$. □

To do.: Say something about T-Sub?

**Theorem 1** (Progress)**.** *If $\Gamma; \Delta \vdash t : \widehat{\tau}$ & $\xi$ with $t$ a closed term, then $t$ is either a possibly exceptional value $\widehat{v}$ or there is a closed term $t'$ such that $t \longrightarrow t'$.*

*Proof.* By induction on the typing derivation $\Gamma; \Delta \vdash t : \widehat{\tau}$ & $\xi$.

The case T-Var can be discarded, as a variable is not a closed term. The cases T-Con, T-Crash, T-Abs, T-AnnAbs, T-Nil and T-Cons are immediate as they are values.

Case T-App: We can immediately apply the induction hypothesis to $\Gamma; \Delta \vdash t_1 : \widehat{\tau}_2\langle\xi_2\rangle \to \widehat{\tau}\langle\xi\rangle$ & $\xi$, giving us either a $t_1'$ such that $t_1 \longrightarrow t_1'$ or that $t_1 = \widehat{v}$. In the former case we can make progress using E-App. In the latter case the canonical forms lemma tells us that either $t_1 = \lambda x : \widehat{\tau}_2$ & $\xi_2.t_1'$ or $t_1 = \lightning^\ell$, in which case we can make progress using E-AppAbs or E-AppExn, respectively.

The remaining cases follow by analogous reasoning. □

**Lemma 4** (Annotation substitution)**.**

1. *If $\Delta, e : \kappa' \vdash \xi : \kappa$ and $\Delta \vdash \xi' : \kappa'$ then $\Delta \vdash \xi[\xi'/e] : \kappa$.*
2. *If $\Delta, e : \kappa' \vdash \xi_1 \leqslant \xi_2$ and $\Delta \vdash \xi' :: \kappa'$ then $\Delta \vdash \xi_1[\xi'/e] \leqslant \xi_2[\xi'/e]$.*
3. *If $\Delta, e : \kappa' \vdash \widehat{\tau}_1 \leqslant \widehat{\tau}_2$ and $\Delta \vdash \xi' :: \kappa'$ then $\Delta \vdash \widehat{\tau}_1[\xi'/e] \leqslant \widehat{\tau}_2[\xi'/e]$.*
4. *If $\Gamma; \Delta, e : \kappa' \vdash t : \widehat{\tau}$ & $\xi$ and $\Delta \vdash \xi' : \kappa'$ then $\Gamma; \Delta \vdash t[\xi'/e] : \widehat{\tau}[\xi'/e]$ & $\xi$.*

To do.: In part 4, either we need the assumption $e \notin \mathrm{fv}(\xi)$ (which seems to be satisfied everywhere we want to apply this lemma), or we also need to apply the substitution to $\xi$ (is this expected or not in a type-and-effect system)? T-Fix seems to be to only rule where an exception variable can flow from $\widehat{\tau}$ to $\xi$....

*Proof.* 1. By induction on the derivation of $\Delta, e : \kappa' \vdash \xi : \kappa$. The cases A-Var, A-Abs and A-App are analogous to the respective cases in the proof of term substitution below. In the case A-Con one can strengthen the assumption

$\Delta, e : \kappa' \vdash \{\ell\} : \text{EXN}$ to $\Delta \vdash \{\ell\} : \text{EXN}$ as $e \notin \text{fv}(\{\ell\})$, the result is then immediate; similarly for A-EMPTY. The case A-UNION goes analogous to A-APP.

2. TO DO.

3. TO DO.

4. By induction on the derivation of $\Gamma; \Delta, e : \kappa' \vdash t : \widehat{\tau} \,\&\, \xi$. Most cases can be discarded by a straightforward application of the induction hypothesis; we show only the interesting case.

Case T-ANNAPP: TO DO.

TO DO.

□

**Lemma 5** (Term substitution). *If* $\Gamma, x : \widehat{\tau}' \,\&\, \xi'; \Delta \vdash t : \widehat{\tau} \,\&\, \xi$ *and* $\Gamma; \Delta \vdash t' : \widehat{\tau}' \,\&\, \xi'$ *then* $\Gamma; \Delta \vdash t[t'/x] : \widehat{\tau} \,\&\, \xi$.

*Proof.* By induction on the derivation of $\Gamma, x : \widehat{\tau}' \,\&\, \xi; \Delta \vdash t : \widehat{\tau} \,\&\, \xi$.

Case T-VAR: We either have $t = x$ or $t = x'$ with $x \neq x'$. In the first case we need to show that $\Gamma; \Delta \vdash x[t'/x] : \widehat{\tau} \,\&\, \xi$, which by definition of substitution is equal to $\Gamma; \Delta \vdash x : \widehat{\tau} \,\&\, \xi$, but this is one of our assumptions. In the second case we need to show that $\Gamma, x' : \widehat{\tau} \,\&\, \xi; \Delta \vdash x'[t/x] : \widehat{\tau} \,\&\, \xi$, which by definition of substitution is equal to $\Gamma, x' : \widehat{\tau} \,\&\, \xi; \Delta \vdash x' : \widehat{\tau} \,\&\, \xi$. This follows immediately from T-VAR.

Case T-ABS: Our assumptions are

$$\Gamma, x : \widehat{\tau}' \,\&\, \xi', y : \widehat{\tau}_1 \,\&\, \xi_1; \Delta \vdash t : \widehat{\tau}_2 \,\&\, \xi_2 \tag{1.1}$$

$$\Gamma; \Delta \vdash t' : \widehat{\tau}' \,\&\, \xi'. \tag{1.2}$$

By the Barendregt convention we may assume that $y \neq x$ and $y \notin \text{fv}(t')$. We need to show that $\Gamma; \Delta \vdash (\lambda y : \widehat{\tau}_1 \,\&\, \xi_1.t)[t'/x] : \widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle \,\&\, \emptyset$, which by definition of substitution is equal to

$$\Gamma; \Delta \vdash \lambda y : \widehat{\tau}_1 \,\&\, \xi_1.t[t'/x] : \widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle \,\&\, \emptyset. \tag{1.3}$$

We weaken (1.2) to $\Gamma, y : \widehat{\tau}_1 \,\&\, \xi_1; \Delta \vdash t' : \widehat{\tau}' \,\&\, \xi'$ and apply the induction hypothesis on this and (1.1) to obtain

$$\Gamma, y : \widehat{\tau}_1 \,\&\, \xi_1; \Delta \vdash t[t'/x] : \widehat{\tau}_2 \,\&\, \xi_2. \tag{1.4}$$

The desired result (1.3) can be constructed from (1.4) using T-ABS.

Case T-AnnAbs: Our assumptions are $\Gamma, x : \widehat{\tau}' \,\&\, \xi'; \Delta, e : \kappa \vdash t : \widehat{\tau} \,\&\, \xi$ and $\Gamma; \Delta \vdash t' : \widehat{\tau}' \,\&\, \xi'$. By the Barendregt convention we may assume that $e \notin \mathrm{fv}(t')$. We need to show that $\Gamma; \Delta \vdash (\Lambda e :: \kappa.t)\,[t'/x] : \widehat{\tau} \,\&\, \xi$, which is equal to $\Gamma; \Delta \vdash \Lambda e :: \kappa.t[t'/\kappa] : \widehat{\tau} \,\&\, \xi$ by definition of substitution. By applying the induction hypothesis we obtain $\Gamma; \Delta, e : \kappa \vdash t[t'/x] : \widehat{\tau} \,\&\, \xi$. The desired result can be constructed using T-AnnAbs.

Case T-App: Our assumptions are

$$\Gamma, x : \widehat{\tau}' \,\&\, \xi'; \Delta \vdash t_1 : \widehat{\tau}_2\langle\xi_2\rangle \to \widehat{\tau}\langle\xi\rangle \,\&\, \xi \tag{1.5}$$

$$\Gamma, x : \widehat{\tau}' \,\&\, \xi'; \Delta \vdash t_2 : \widehat{\tau}_2 \,\&\, \xi_2. \tag{1.6}$$

We need to show that $\Gamma; \Delta \vdash (t_1\ t_2)[t'/x] : \widehat{\tau} \,\&\, \xi$, which by definition of substitution is equal to

$$\Gamma; \Delta \vdash \big(t_1[t'/x]\big)\ \big(t_2[t'/x]\big) : \widehat{\tau} \,\&\, \xi. \tag{1.7}$$

By applying the induction hypothesis to (1.5) respectively (1.6) we obtain

$$\Gamma; \Delta \vdash t_1[t'/x] : \widehat{\tau}_2\langle\xi_2\rangle \to \widehat{\tau}\langle\xi\rangle \,\&\, \xi \tag{1.8}$$

$$\Gamma; \Delta \vdash t_2[t'/x] : \widehat{\tau}_2 \,\&\, \xi_2. \tag{1.9}$$

The desired result (1.7) can be constructed by applying T-App to (1.8) and (1.9).

All other cases are either immediate or analogous to the case of T-App. □

**Lemma 6** (Inversion)**.**

1. *If* $\Gamma; \Delta \vdash \lambda x : \widehat{\tau} \,\&\, \xi.t : \widehat{\tau}_1\langle\xi_1\rangle \to \widehat{\tau}_2\langle\xi_2\rangle \,\&\, \xi_3$, *then*
   - $\Gamma, x : \widehat{\tau} \,\&\, \xi; \Delta \vdash t : \widehat{\tau}' \,\&\, \xi'$,
   - $\Delta \vdash \widehat{\tau}_1 \leqslant \widehat{\tau}$ *and* $\Delta \vdash \xi_1 \leqslant \xi$,
   - $\Delta \vdash \widehat{\tau}' \leqslant \widehat{\tau}_2$ *and* $\Delta \vdash \xi' \leqslant \xi_2$.
2. *If* $\Gamma; \Delta \vdash \Lambda e :: \kappa.t : \forall e :: \kappa.\widehat{\tau} \,\&\, \xi$, *then*
   - $\Gamma; \Delta, e : \kappa \vdash t : \widehat{\tau}' \,\&\, \xi'$,
   - $\Delta, e : \kappa \vdash \widehat{\tau}' \leqslant \widehat{\tau}$,
   - $\Delta \vdash \xi' \leqslant \xi$.

– To do. $e \notin \mathrm{fv}(\xi)$ *and/or* $e \notin \mathrm{fv}(\xi')$.

*Proof.* 1. By induction on the typing derivation.

Case T-Abs: We have $\widehat{\tau} = \widehat{\tau}_1$, $\xi = \xi_1$ and take $\widehat{\tau}' = \widehat{\tau}_2$, $\xi' = \xi_2$, the result then follows immediately from the assumption $\Gamma, x : \widehat{\tau} \,\&\, \xi; \Delta \vdash t : \widehat{\tau}_2 \,\&\, \xi_2$ and reflexivity of the subtyping and subeffecting relations.

Case T-Sub: We are given the additional assumptions

$$\Gamma; \Delta \vdash \lambda x : \widehat{\tau} \,\&\, \xi.t : \widehat{\tau}'_1\langle \xi'_1 \rangle \to \widehat{\tau}'_2\langle \xi'_2 \rangle \,\&\, \xi'_3, \tag{1.10}$$

$$\Delta \vdash \widehat{\tau}'_1\langle \xi'_1 \rangle \to \widehat{\tau}'_2\langle \xi'_2 \rangle \leqslant \widehat{\tau}_1\langle \xi_1 \rangle \to \widehat{\tau}_2\langle \xi_2 \rangle, \tag{1.11}$$

$$\Delta \vdash \xi'_3 \leqslant \xi_3. \tag{1.12}$$

Applying the induction hypothesis to (1.10) gives us

$$\Gamma, x : \widehat{\tau} \,\&\, \xi; \Delta \vdash t : \widehat{\tau}''_2 \,\&\, \xi''_2, \tag{1.13}$$

$$\Delta \vdash \widehat{\tau}'_1 \leqslant \widehat{\tau}, \quad \Delta \vdash \xi'_1 \leqslant \xi, \tag{1.14}$$

$$\Delta \vdash \widehat{\tau}''_2 \leqslant \widehat{\tau}'_2, \quad \Delta \vdash \xi''_2 \leqslant \xi'_2. \tag{1.15}$$

Inversion of the subtyping relation on (1.11) gives us

$$\Delta \vdash \widehat{\tau}'_1 \leqslant \widehat{\tau}, \quad \Delta \vdash \xi'_1 \leqslant \xi, \tag{1.16}$$

$$\Delta \vdash \widehat{\tau}''_2 \leqslant \widehat{\tau}'_2, \quad \Delta \vdash \xi''_2 \leqslant \xi'_2. \tag{1.17}$$

The result follows from (1.13) and combining (1.16) with (1.14) and (1.15) with (1.17) using the transitivity of the subtyping and subeffecting relations.

2. By induction on the typing derivation.

Case T-AnnAbs: We need to show that $\Gamma; \Delta, e : \kappa \vdash t : \widehat{\tau} \,\&\, \xi$, which is one of our assumptions, and that $\Delta, e : \kappa \vdash \widehat{\tau} \leqslant \widehat{\tau}$ and $\Delta \vdash \xi \leqslant \xi$; this follows from the reflexivity of the subtyping, respectively subeffecting, relation (noting that $e \notin \mathrm{fv}(\xi)$).

Case T-Sub: Similar to the case T-Sub in part 1.

□

**Theorem 2** (Preservation). *If* $\Gamma; \Delta \vdash t : \widehat{\tau} \,\&\, \xi$ *and* $t \longrightarrow t'$, *then* $\Gamma; \Delta \vdash t' : \widehat{\tau} \,\&\, \xi$.

*Proof.* By induction on the typing derivation $\Gamma; \Delta \vdash t : \widehat{\tau} \,\&\, \xi$.

The cases for T-Var, T-Con, T-Crash, T-Abs, T-AnnAbs, T-Nil, and T-Cons can be discarded immediately, as they have no applicable evaluation rules.

To do. □

### 1.6.3 Syntax-directed type elaboration

### 1.6.4 Type inference algorithm

**Theorem 3** (Syntactic soundness)**.** *If* $\mathcal{R}\ \Gamma\ \Delta\ t = \langle \widehat{\tau}; \xi \rangle$*, then* $\Gamma; \Delta \vdash t : \widehat{\tau}\ \&\ \xi$*.*

*Proof.* By induction on the term $t$.
To do. □

**Theorem 4** (Termination)**.** $\mathcal{R}\ \Gamma\ \Delta\ t$ *terminates.*

*Proof.* By induction on the term $t$.
To do. □

## 1.7 Related work

### 1.7.1 Higher-ranked polymorphism in type-and-effect systems

**Effect polymorphism** For plain type systems, Hindley–Milner's **let**-bound polymorphism generally provides a good compromise between expressiveness of the type system and complexity of the inference algorithm Hindley (1969); Milner (1978); Damas and Milner (1982). Type systems were extended with effects—including **let**-bound effect-polymorphism—by Lucassen and Gifford (1988); Jouvelot and Gifford (1991); and Talpin and Jouvelot (1992, 1994). In type-and-effect systems it has long been recognized that **fix**-bound polymorphism (polymorphic recursion) *in the effects* is often beneficial or even necessary for achieving precise analysis results. For example, in type-and-effect systems for regions Tofte and Talpin (1994), dimensions Kennedy (1994); Rittri (1994, 1995), binding times Dussart et al. (1995), and exceptions Glynn et al. (2002); Koot and Hage (2015).

Inferring principal types in a type system with polymorphic recursion is equivalent to solving the undecidable semi-unification problem Mycroft (1984); Kfoury et al. (1990b, 1993); Henglein (1993). When restricted to polymorphic recursion in the effects, the problem often becomes decidable again. In Tofte and Talpin (1994) this is a conjecture based on empirical observation. Rittri (1995) gives a semi-unification procedure based on the general semi-unification semi-algorithm by Baaz (1993) and proves it terminates in the special case of semi-unification in Abelian groups. Dussart et al. (1995) use a

constraint-based algorithm. They show that all variables that do not occur free in the context or type can be eliminated from the constraint set by a constraint reduction step during each Kleene–Mycroft iteration. As at most $n^2$ subeffecting constraints can be formed over $n$ free variables, the whole procedure must terminate. By not restarting the Kleene–Mycroft iteration from bottom, their algorithm runs in polynomial time—even in the presence of nested fixpoints.

The extension to polymorphic effect-abstraction ($\lambda$-bound, higher-ranked effect polymorphism) remained less well-studied, possibly because it is of limited use without the simultaneous introduction of effect operators—in contrast to the situation of higher-ranked polymorphism in plain type systems.

**Effect operators** Kennedy (1996a) presents a type system that ensures the dimensional consistency of an ML-like language extended with units of measure ($\mathrm{ML}_\delta$). This language has predicative prenex dimension polymorphism. Kennedy gives an Algorithm $\mathcal{W}$-like type inference procedure that uses equational unification to deal with the Abelian group (AG) structure of dimension expressions. Also described are two explicitly typed variants of the language: a System F-like language with higher-ranked dimension polymorphism ($\Lambda_\delta$), and a System $\mathrm{F}_\omega$-like language that extends $\Lambda_\delta$ with dimension operators ($\Lambda_{\delta\omega}$). Kennedy notes that this language can type strictly more programs than the language without dimension operators:

$$
\begin{aligned}
\mathit{twice} \;&:\; \forall F :: \textsc{dim} \Rightarrow \textsc{dim}.\\
&\qquad (\forall d :: \textsc{dim}.\mathbf{real}\langle d\rangle \to \mathbf{real}\langle F\ d\rangle) \to\\
&\qquad\quad (\forall d :: \textsc{dim}.\mathbf{real}\langle d\rangle \to \mathbf{real}\langle F\ (F\ d)\rangle)\\
\mathit{twice} \;&= \Lambda F :: \textsc{dim} \Rightarrow \textsc{dim}.\\
&\qquad \lambda f : (\forall d :: \textsc{dim}.\mathbf{real}\langle d\rangle \to \mathbf{real}\langle F\ d\rangle).\\
&\qquad\quad \Lambda d :: \textsc{dim}.\lambda x : \mathbf{real}\langle d\rangle.f\ \langle F\ d\rangle\ (f\ \langle d\rangle\ x)\\
\mathit{square} \;&:\; \forall d :: \textsc{dim}.\mathbf{real}\langle d\rangle \to \mathbf{real}\langle d^2\rangle\\
\mathit{square} \;&= \Lambda d :: \textsc{dim}.\lambda x : \mathbf{real}\langle d\rangle.x^2\\
\mathit{fourth} \;&:\; \forall d :: \textsc{dim}.\mathbf{real}\langle d\rangle \to \mathbf{real}\langle d^4\rangle\\
\mathit{fourth} \;&= \mathit{twice}\ \langle \Lambda d :: \textsc{dim}.d^2\rangle\ \mathit{square}
\end{aligned}
$$

Without dimension operators the type of the higher-order function *twice* would not allow the application of the function *square* at the two distinct types $\forall d :: \textsc{dim}.\mathbf{real}\langle d\rangle \to \mathbf{real}\langle d^2\rangle$ and $\forall d :: \textsc{dim}.\mathbf{real}\langle d^2\rangle \to \mathbf{real}\langle d^4\rangle$ when invoked from the function *fourth*.

The language $\Lambda_{\delta\omega}$ bears a striking resemblance to the language in Figure 1.11: the empty and singleton exception sets constants, and the exception set union operator have been replaced with a unit dimension, and dimension product and inverse operators—as dimensions have an AG structure, whereas exception sets have an ACI1 structure; in the dimension type system the annotation is placed only on the real number base type instead of on the compound types, and there is no effect. No type inference algorithm is given for this language, however.

Faxén (1997) presents a type system for flow analysis that uses constrained type schemes in the style of Aiken and Wimmers (1993), and has $\lambda$-bound polymorphism (but no type operators) in the style of System F. To make the inference algorithm terminate for recursive programs the size of the name supply needs to be bounded, leading to imprecision. Smith and Wang (2000) present a similar framework, but one that can be instantiated with variants of either $k$-CFA Shivers (1991) or CPA Agesen (1995) to ensure termination.

Holdermans and Hage (2010) design a System $F_\omega$-like type system for flow analysis for a strict language that has both polymorphic abstraction and effect operators. Our type inference algorithm builds on their techniques. A key difference is that they work with a constraint-based type system and a constraint solver, while we replace these with reduction of terms in an algebraic $\lambda$-calculus. This difference expresses itself particularly in how the case of (polymorphic) recursion is handled. We believe our approach will scale more easily to analyses that are either not conservative extensions of the underlying type system, or require more expressive effects (see Section 1.8).

### 1.7.2 $\lambda^{\cup}$-calculus

Tannen (1988), Okada (1989), and Tannen and Gallier (1991) prove that if a simply typed $\lambda$-calculus is extended with a many-sorted algebraic rewrite system $R$ (by introducing the symbols of the algebraic theory as higher-order constants in the $\lambda$-calculus), then the combined rewrite system $\beta\eta R$ is confluent and strongly normalizing if $R$ is confluent and strongly normalizing.

Révész (1992) introduced an untyped $\lambda$-calculus with applicative lists. A model is given by Durfee (1997). This calculus satisfies the equations

$$\langle t_1, ..., t_n \rangle\ t' = \langle t_1\ t', ..., t_n\ t' \rangle \qquad (\gamma_1)$$

$$\lambda x.\langle t_1, ...t_n \rangle = \langle \lambda x.t_1, ..., \lambda x.t_n \rangle \qquad (\gamma_2)$$

similar to our typed $\lambda^{\cup}$-calculus.

### 1.7.3 Exception analyses

Several exception analyses have been described in the literature; these primarily target the detection of uncaught exceptions in ML. The exception analysis by Yi (1994) is based on abstract interpretation. Guzmán and Suárez (1994) and Fähndrich et al. (1998) describe type-based exception analyses. Leroy and Pessaux (2000) presents a row-based type system for exception analysis that contains a data-flow analysis component targeted towards tracking value-carrying exceptions.

Glynn et al. (2002) developed the first exception analysis for a non-strict language; a type-based analysis using Boolean constraints. Koot and Hage (2015) present a constraint-based type system for exception analysis of a non-strict language, where the exception-flow could depend on the data-flow using conditional constraints. This increases the accuracy in the presence of exceptions raised by pattern-matching failures.

## 1.8 Further research

**Can we infer types for Kennedy's higher-ranked $\Lambda_{\delta\omega}$?** One problem that immediately presents itself is that this type system is not a conservative extension of the underlying type system: programs can be rejected because they, while being type correct in the underlying type system, may still be dimensionally inconsistent. Unlike the system in this paper, the annotations on function arguments will no longer be of the simple form (patterns) required for the straightforward matching step in the type inference algorithm. Instead, we suspect we have to solve a higher-order equational (pre)unification problem, which is only semi-decidable. Snyder (1990), Nipkow and Qian (1991) and Qian and Wang (1996) do give us semi-algorithms for solving such problems.

**Can we further improve the precision of exception types?** Koot and Hage (2015) argue that an accurate exception typing system for non-strict languages should also take the data flow of the program into account, as many exceptions that can be raised in non-strict languages are caused by incomplete case-analyses during pattern-matching. The canonical example is the

*risers* function—which splits a list into monotonically increasing subsegments; for example, *risers* $[1,3,5,1,2]$ evaluates to $[[1,3,5],[1,2]]$—by Mitchell and Runciman (2008):

$$
\begin{array}{l}
\mathit{risers} \ : [\mathbf{int}] \to [[\mathbf{int}]] \\
\mathit{risers}\ [\,] \qquad\qquad\quad = [\,] \\
\mathit{risers}\ [x] \qquad\qquad\quad = [[x]] \\
\mathit{risers}\ (x_1 :: x_2 :: xs) = \\
\quad \mathbf{if}\ x_1 \leqslant x_2\ \mathbf{then}\ (x_1 :: y) :: ys\ \mathbf{else}\ [x_1] :: (y :: ys) \\
\qquad \mathbf{where}\ (y :: ys) = \mathit{risers}\ (x_2 :: xs)
\end{array}
$$

The inference algorithm in Figure 1.15 assigns *risers* the type

$$
\begin{array}{l}
\forall e_1 :: \textsc{exn}.\forall e_2 :: \textsc{exn}. \\
\quad [\widehat{\mathbf{int}}\langle e_2\rangle]\langle e_1\rangle \to [[\widehat{\mathbf{int}}\langle e_2\rangle]\langle\varnothing\rangle]\langle e_1 \cup e_2 \cup \{\mathbf{E}\}\rangle \ \&\ \varnothing
\end{array}
$$

where **E** is the label of the exception raised when the pattern-match in the **where**-clause fails.[5] However, the pattern-match happens on the result of the recursive call *risers* $(x_2 :: xs)$. When *risers* is given a non-empty list (such as $x_2 :: xs$) as an argument, it always returns a non-empty list as its result. The pattern-match can thus never fail, and the exception labelled **E** can thus never be raised.

Koot and Hage demonstrate how this exception can be elided by having the exception flow depend on the data flow. The $\lambda^{\cup}$-calculus terms that form the effect annotations cannot express this dependence, however. Koot and Hage use a slightly ad hoc form of conditional constraints to model this dependence. We believe that extending a $\lambda$-calculus with an equational theory of Boolean rings may form the basis of a more principled approach. Boolean rings have already been successfully used to design type systems for strictness analysis Wright (1991), records Kennedy (1996b) and exception tracking Benton and Buchlovsky (2007).

**Metatheory** We have not yet worked out the metatheory of the type system presented in this paper. Of particular interest are the (syntactic) soundness, completeness and totality of the inference step for recursive definitions. We

[5] This exception is left implicit in the above program, but becomes explicit when the code is desugared into our core language.

expect that soundness and completeness can be shown by a similar argument as in Mycroft (1984) and Dussart et al. (1995).

We conjectured the totality of our inference algorithm. We have a good reason to do so: we only expect the fixpoint iteration to diverge if no fixpoint exists—that is to say, the program is type incorrect. Assuming the program is well-typed in the underlying type system, there are no type incorrect programs in our exception typing system, however.

To show the fixpoint iteration is guaranteed to terminate in their binding-time analysis, Dussart et al. (1995) note that only a finite number of type constraints and therefore constrained type schemes can be formed over a finite number of variables (after constraints have been simplified). As it is still possible to form an infinite number of $\lambda^{\cup}$-normal forms over a finite number of variables, such an argument is not going to work directly.

## 1.9 Conclusion

We show that it is feasible to extend non-strict higher-order languages with exception-annotated types, as is already done in some strict first-order languages. We argue that higher-ranked exception polymorphic types with exception set operators *à la* System $F_\omega$ are not only more accurate, but are also more readable when presented to the programmer *vis-à-vis* constrained type schemes: the exception terms in the annotations more closely mirror what is happening at the term level than constraint sets do.

$$
\begin{array}{l}
\mathcal{R} : \mathbf{TyEnv} \times \mathbf{KiEnv} \times \mathbf{Tm} \to \mathbf{ExnTm} \times \mathbf{ExnTy} \times \mathbf{Exn} \\
\mathcal{R}(\Gamma; \Delta; x) \qquad = x : \Gamma(x) \\
\mathcal{R}(\Gamma; \Delta; c_\tau) \qquad = c_\tau : \bot_\tau \mathbin{\&} \emptyset \\
\mathcal{R}(\Gamma; \Delta; \lightning^\ell_\tau) \qquad = \lightning^\ell_\tau : \bot_\tau \mathbin{\&} \{\ell\} \\
\mathcal{R}(\Gamma; \Delta; \lambda x : \tau.t) = \\
\quad \textbf{let } \widehat{\tau}_1 \mathbin{\&} e \triangleright \overline{e_i :: \kappa_i} = \mathcal{C}(\emptyset; \tau) \\
\qquad\quad t' : \widehat{\tau}_2 \mathbin{\&} \xi_2 \qquad = \mathcal{R}(\Gamma, x : \widehat{\tau}_1 \mathbin{\&} e; \Delta, \overline{e_i :: \kappa_i}; t) \\
\quad \textbf{in } \Lambda \overline{e_i :: \kappa_i}. \lambda x : \widehat{\tau}_1 \mathbin{\&} e.t' : \forall \overline{e_i :: \kappa_i}. \widehat{\tau}_1 \langle e \rangle \to \widehat{\tau}_2 \langle \xi_2 \rangle \mathbin{\&} \emptyset \\
\mathcal{R}(\Gamma; \Delta; t_1\ t_2) \quad = \\
\quad \textbf{let } t'_1 : \widehat{\tau}_1 \mathbin{\&} \xi_1 \qquad = \mathcal{R}(\Gamma; \Delta; t_1) \\
\qquad\quad t'_2 : \widehat{\tau}_2 \mathbin{\&} \xi_2 \qquad = \mathcal{R}(\Gamma; \Delta; t_2) \\
\qquad\quad \widehat{\tau}'_2 \langle e'_2 \rangle \to \widehat{\tau}' \langle \xi' \rangle \triangleright \overline{e_i :: \kappa_i} = \mathcal{I}(\widehat{\tau}_1) \\
\qquad\quad \theta \qquad = [e'_2 \mapsto \xi_2] \circ \mathcal{M}(\emptyset; \widehat{\tau}'_2; \widehat{\tau}_2) \\
\quad \textbf{in } t'_1 \ \langle \overline{\theta e_i} \rangle \ t'_2 : [\![ \theta \widehat{\tau}' ]\!]_\Delta \mathbin{\&} [\![ \theta \xi' \cup \xi_1 ]\!]_\Delta \\
\mathcal{R}(\Gamma; \Delta; \textbf{fix } x : \tau.t) = \\
\quad \textbf{do } i; \widehat{\tau}_0 \mathbin{\&} \xi_0 \leftarrow 0; \bot_\tau \mathbin{\&} \emptyset \\
\qquad \textbf{repeat } t'_{i+1} : \widehat{\tau}_{i+1} \mathbin{\&} \xi_{i+1} \leftarrow \mathcal{R}(\Gamma, x : \widehat{\tau}_i \mathbin{\&} \xi_i; \Delta; t) \\
\qquad\qquad\quad i \qquad\qquad\qquad\quad \leftarrow i + 1 \\
\qquad \textbf{until } \widehat{\tau}_i \mathbin{\&} \xi_i \equiv \widehat{\tau}_{i-1} \mathbin{\&} \xi_{i-1} \\
\qquad \textbf{return fix } x : \widehat{\tau}_i \mathbin{\&} \xi_i. t'_i : \widehat{\tau}_i \mathbin{\&} \xi_i \\
\mathcal{R}(\Gamma; \Delta; t_1 \ \textbf{seq} \ t_2) = \\
\quad \textbf{let } t'_1 : \widehat{\tau}_1 \mathbin{\&} \xi_1 = \mathcal{R}(\Gamma; \Delta; t_1) \\
\qquad\quad t'_2 : \widehat{\tau}_2 \mathbin{\&} \xi_2 = \mathcal{R}(\Gamma; \Delta; t_2) \\
\quad \textbf{in } t'_1 \ \textbf{seq} \ t'_2 : \widehat{\tau}_2 \mathbin{\&} [\![ \xi_1 \cup \xi_2 ]\!]_\Delta \\
\mathcal{R}(\Gamma; \Delta; t_1 \oplus t_2) = \\
\quad \textbf{let } t'_1 : \widehat{\textbf{int}} \mathbin{\&} \xi_1 = \mathcal{R}(\Gamma; \Delta; t_1) \\
\qquad\quad t'_2 : \widehat{\textbf{int}} \mathbin{\&} \xi_2 = \mathcal{R}(\Gamma; \Delta; t_2) \\
\quad \textbf{in } t'_1 \oplus t'_2 : \widehat{\textbf{bool}} \mathbin{\&} [\![ \xi_1 \cup \xi_2 ]\!]_\Delta \\
\mathcal{R}(\Gamma; \Delta; \textbf{if } t_1 \textbf{ then } t_2 \textbf{ else } t_3) = \\
\quad \textbf{let } t'_1 : \widehat{\textbf{bool}} \mathbin{\&} \xi_1 = \mathcal{R}(\Gamma; \Delta; t_1) \\
\qquad\quad t'_2 : \widehat{\tau}_2 \mathbin{\&} \xi_2 \qquad = \mathcal{R}(\Gamma; \Delta; t_2) \\
\qquad\quad t'_3 : \widehat{\tau}_3 \mathbin{\&} \xi_3 \qquad = \mathcal{R}(\Gamma; \Delta; t_3) \\
\quad \textbf{in } \textbf{if } t'_1 \textbf{ then } t'_2 \textbf{ else } t'_3 : [\![ \widehat{\tau}_2 \sqcup \widehat{\tau}_3 ]\!]_\Delta \mathbin{\&} [\![ \xi_1 \cup \xi_2 \cup \xi_3 ]\!]_\Delta \\
\mathcal{R}(\Gamma; \Delta; [\,]_\tau) \qquad = [\,]_\tau : [\bot_\tau \langle \emptyset \rangle] \mathbin{\&} \emptyset \\
\mathcal{R}(\Gamma; \Delta; t_1 :: t_2) = \\
\quad \textbf{let } t'_1 : \widehat{\tau}_1 \mathbin{\&} \xi_1 \qquad = \mathcal{R}(\Gamma; \Delta; t_1) \\
\qquad\quad t'_2 : [\widehat{\tau}_2 \langle \xi'_2 \rangle] \mathbin{\&} \xi_2 \ = \mathcal{R}(\Gamma; \Delta; t_2) \\
\quad \textbf{in } t'_1 :: t'_2 : [\![ [(\widehat{\tau}_1 \sqcup \widehat{\tau}_2) \langle \xi_1 \cup \xi'_2 \rangle] ]\!]_\Delta \mathbin{\&} \xi_2 \\
\mathcal{R}(\Gamma; \Delta; \textbf{case } t_1 \textbf{ of } \{[\,] \mapsto t_2; x_1 :: x_2 \mapsto t_3\}) = \\
\quad \textbf{let } t'_1 : \left[\widehat{\tau}_1 \langle \xi'_1 \rangle\right] \mathbin{\&} \xi_1 = \mathcal{R}(\Gamma; \Delta; t_1) \\
\qquad\quad \Gamma' \qquad\qquad = \Gamma, x_1 : \widehat{\tau}_1 \mathbin{\&} \xi'_1, x_2 : \left[\widehat{\tau}_1 \langle \xi'_1 \rangle\right] \mathbin{\&} \xi_1 \\
\qquad\quad t'_2 : \widehat{\tau}_2 \mathbin{\&} \xi_2 \qquad = \mathcal{R}(\Gamma; \Delta; t_2) \\
\qquad\quad t'_3 : \widehat{\tau}_3 \mathbin{\&} \xi_3 \qquad = \mathcal{R}(\Gamma'; \Delta; t_3)
\end{array}
$$

$$
\begin{array}{l}
\mathcal{M} : \mathbf{KiEnv} \times \mathbf{ExnTy} \times \mathbf{ExnTy} \to \mathbf{Subst} \\
\mathcal{M}(\Delta; \widehat{\mathbf{bool}};\ \ \widehat{\mathbf{bool}}) = \emptyset \\
\mathcal{M}(\Delta; \widehat{\mathbf{int}};\ \ \widehat{\mathbf{int}}) = \emptyset \\
\mathcal{M}(\Delta;\ [\widehat{\tau}'\langle e'\ \overline{e_i}\rangle];\ [\widehat{\tau}\langle\xi\rangle]) \\
\qquad = \left[e' \mapsto \lambda\overline{e_i :: \Delta_{e_i}}.\xi\right] \circ \mathcal{M}(\Delta; \widehat{\tau}'; \widehat{\tau}) \\
\mathcal{M}(\Delta; \widehat{\tau}_1\langle e\rangle \to \widehat{\tau}_2'\langle e'\ \overline{e_i}\rangle; \widehat{\tau}_1\langle e\rangle \to \widehat{\tau}_2\langle\zeta\rangle) \\
\qquad = \left[e' \mapsto \lambda\overline{e_i :: \Delta_{e_i}}.\xi\right] \circ \mathcal{M}(\Delta; \widehat{\tau}_2'; \widehat{\tau}_2) \\
\mathcal{M}(\Delta; \forall e :: \kappa.\widehat{\tau}';\ \ \forall e :: \kappa.\widehat{\tau}) = \mathcal{M}(\Delta, e :: \kappa; \widehat{\tau}'; \widehat{\tau})
\end{array}
$$

Figure 1.16: Exception type matching ($\mathcal{M}$)

$$
\begin{array}{llll}
\sqcup : \mathbf{ExnTy} \times \mathbf{ExnTy} \to \mathbf{ExnTy} & & & \\
\widehat{\mathbf{bool}} & \sqcup\, \widehat{\mathbf{bool}} & = \widehat{\mathbf{bool}} \\
\widehat{\mathbf{int}} & \sqcup\, \widehat{\mathbf{int}} & = \widehat{\mathbf{int}} \\
[\widehat{\tau}\langle\xi\rangle] & \sqcup\, [\widehat{\tau}'\langle\xi'\rangle] & = [(\widehat{\tau} \sqcup \widehat{\tau}')\langle\xi \cup \xi'\rangle] \\
\widehat{\tau}_1\langle e\rangle \to \widehat{\tau}_2\langle\xi\rangle & \sqcup\, \widehat{\tau}_1\langle e\rangle \to \widehat{\tau}_2'\langle\xi'\rangle & = \widehat{\tau}_1\langle e\rangle \to (\widehat{\tau}_2 \sqcup \widehat{\tau}_2')\langle\xi \cup \xi'\rangle \\
\forall e :: \kappa.\widehat{\tau} & \sqcup\, \forall e :: \kappa.\widehat{\tau}' & = \forall e :: \kappa.(\widehat{\tau} \sqcup \widehat{\tau}')
\end{array}
$$

Figure 1.17: Exception types: least upper bounds ($\sqcup$)

$$
\begin{array}{rll}
e[\xi/e] & \equiv \xi & \\
e'[\xi/e] & \equiv e' & \text{if } e \neq e' \\
\{\ell\}[\xi/e] & \equiv \{\ell\} & \\
\emptyset[\xi/e] & \equiv \emptyset & \\
\left(\lambda e' : \kappa.\xi'\right)[\xi/e] & \equiv \lambda e' : \kappa.\xi'[\xi/e] & \text{if } e \neq e' \text{ and } e' \notin \mathrm{fv}(\xi) \\
(e_1\ e_2)\,[\xi/e] & \equiv (e_1[\xi/e])\ \ (e_2[\xi/e]) & \\
(e_1 \cup e_2)\,[\xi/e] & \equiv e_1[\xi/e] \cup e_2[\xi/e] &
\end{array}
$$

Figure 1.18: Annotation substitution

$$
\begin{array}{rll}
x[t/x] & \equiv t & \\
x'[t/x] & \equiv x' & \text{if } x \neq x' \\
c_\tau[t/x] & \equiv c_\tau & \\
\left(\lambda x' : \widehat{\tau}.t'\right)[t/x] & \equiv \lambda x' : \widehat{\tau}.t'[t/x] & \text{if } x \neq x' \text{ and } x' \notin \mathrm{fv}(t) \\
& \cdots &
\end{array}
$$

Figure 1.19: Term substitution

# Appendix A

# Old stuff

## A.1 $\lambda^{\cup}$-calculus

**Values** Values $v$ are terms of the form

$$\lambda x_1 : \tau_1 . \cdots \lambda x_i : \tau_i . \{c_1\} \cup (\cdots \cup (\{c_j\} \cup (x_1\ v_{11} \cdots v_{1m} \cup (\cdots \cup x_k\ v_{k1} \cdots v_{kn}))))$$

### A.1.1 Reduction relation (wrong!)

- To do. Do not match the rules in the prototype (those are sensitive to the order in which they are tried).
- To do. In the second rule only one term is applied; contrast this with the other rules involing applications.
- To do. Should make use of the fact the everything is fully applied (and $\eta$-expanded/-long?): all atoms are of the form $k\ \overline{t_i}$, where $k$ is $c$ or $x$ and the number of arguments fixed by the arity of $k$. Then try to factor out the commutativity rules by taking "sets" of these atoms. That might simplify stuff a whole lot...
- To do. Can we restrict the typing rule T-Union to only allow sets and not functions on both sides? This would remove the 2nd and 3rd rewrite rules and make the system a more traditional higher-order rewrite system: it's "just" higher-order pattern E-unification (decidable), boolean

rings are easy to integrate, and higher-ranked dimension types becomes higher-order E-unification (semi-decidable). Open question: how to represent e.g. $U(e_2(e_1), e_1) = [e_2 \mapsto \lambda e_1.e_1]$ without abstractions? (Reinterpret $e_1$ as $f(e_1)$ with $f = id$?)

**Definition 6.** Let $\prec$ be a strict total order on $\mathbf{Con} \cup \mathbf{Var}$, with $c \prec x$ for all $c \in \mathbf{Con}$ and $x \in \mathbf{Var}$.

$$
\begin{aligned}
(\lambda x : \tau.t_1)\ t_2 &\longrightarrow t_1[t_2/x] && (\beta\text{-reduction})\\
(t_1 \cup t_2)\ t_3 &\longrightarrow t_1\ t_3 \cup t_2\ t_3 &&\\
(\lambda x : \tau.t_1) \cup (\lambda x : \tau.t_2) &\longrightarrow \lambda x : \tau.\,(t_1 \cup t_2) && (\text{congruences})\\
x\ t_1 \cdots t_n \cup x\ t'_1 \cdots t'_n &\longrightarrow x\ \left(t_1 \cup t'_1\right) \cdots \left(t_n \cup t'_n\right) &&\\
(t_1 \cup t_2) \cup t_3 &\longrightarrow t_1 \cup (t_2 \cup t_3) && (\text{associativity})\\
\emptyset \cup t &\longrightarrow t && (\text{unit})\\
t \cup \emptyset &\longrightarrow t &&\\
x \cup x &\longrightarrow x && (\text{idempotence})\\
x \cup (x \cup t) &\longrightarrow x \cup t &&\\
\{c\} \cup \{c\} &\longrightarrow \{c\} &&\\
\{c\} \cup (\{c\} \cup t) &\longrightarrow \{c\} \cup t &&\\
x\ t_1 \cdots t_n \cup \{c\} &\longrightarrow \{c\} \cup x\ t_1 \cdots t_n && (A.1)\\
x\ t_1 \cdots t_n \cup (\{c\} \cup t) &\longrightarrow \{c\} \cup (x\ t_1 \cdots t_n \cup t) && (A.2)\\
x\ t_1 \cdots t_n \cup x\ t'_1 \cdots t'_n &\longrightarrow x\ t'_1 \cdots t'_n \cup x\ t_1 \cdots t_n \quad \text{if } x' \prec x && (A.3)\\
x\ t_1 \cdots t_n \cup \left(x\ t'_1 \cdots t'_n \cup t\right) &\longrightarrow x\ t'_1 \cdots t'_n \cup (x\ t_1 \cdots t_n \cup t) \quad \text{if } x' \prec x && (A.4)\\
\{c\} \cup \{c'\} &\longrightarrow \{c'\} \cup \{c\} \quad \text{if } c' \prec c && (A.5)\\
\{c\} \cup \left(\{c'\} \cup t\right) &\longrightarrow \{c'\} \cup (\{c\} \cup t) \quad \text{if } c' \prec c && (A.6)
\end{aligned}
$$

**Conjecture 1.** *The reduction relation $\longrightarrow$ preserves meaning.*

**Conjecture 2.** *The reduction relation $\longrightarrow$ is strongly normalizing.*

**Conjecture 3.** *The reduction relation $\longrightarrow$ is locally confluent.*

**Corollary 1.** *The reduction relation $\longrightarrow$ is confluent.*

*Proof.* Follows from SN, LC and Newman's Lemma. □

**Corollary 2.** *The $\lambda^{\cup}$-calculus has unique normal forms.*

**Corollary 3.** *Equality of $\lambda^{\cup}$-terms can be decided by normalization.*

### A.1.2 Semantics

- To do.Combine the lemma and the theorem and make the "extensionally" explicit.
- To do.Is the case for applications rigorous? Relies on the monotonicity of $\varphi : V_{\tau_1} \to V_{\tau_2}$ (separate lemma, require in the denotational semantics?); this might fail for anything other than set union?

**Lemma 7.** $[\![t]\!]_{\rho[x\mapsto v_1]} \cup [\![t]\!]_{\rho[x\mapsto v_2]} \subseteq [\![t]\!]_{\rho[x\mapsto v_1\cup v_2]}$ *(extensionally).*

*Proof.* By induction on the term $t$.

Case "$t = x$": $[\![x]\!]_{\rho[x\mapsto v_1]} \cup [\![x]\!]_{\rho[x\mapsto v_2]} = \rho[x \mapsto v_1](x) \cup \rho[x \mapsto v_2](x) = v_1 \cup v_2 = \rho[x \mapsto v_1 \cup v_2](x) = [\![x]\!]_{\rho[x\mapsto v_1\cup v_2]}$.

Case "$t = y\ (y \neq x)$": $[\![y]\!]_{\rho[x\mapsto v_1]} \cup [\![y]\!]_{\rho[x\mapsto v_2]} = \rho[x \mapsto v_1](y) \cup \rho[x \mapsto v_2](y) = \rho(y) \cup \rho(y) = \rho(y) = \rho[x \mapsto v_1 \cup v_2](y) = [\![y]\!]_{\rho[x\mapsto v_1\cup v_2]}$.

Case "$t = t_1\ t_2$":

$$
\begin{aligned}
&[\![t_1\ t_2]\!]_{\rho[x\mapsto v_1]} \cup [\![t_1\ t_2]\!]_{\rho[x\mapsto v_2]} \\
&= \bigcup \left\{ \varphi([\![t_2]\!]_{\rho[x\mapsto v_1]}) \mid \varphi \in [\![t_1]\!]_{\rho[x\mapsto v_1]} \right\} \cup \bigcup \left\{ \varphi([\![t_2]\!]_{\rho[x\mapsto v_2]}) \mid \varphi \in [\![t_1]\!]_{\rho[x\mapsto v_2]} \right\} \\
&\overset{!}{\subseteq} \bigcup \left\{ \varphi([\![t_2]\!]_{\rho[x\mapsto v_1]}) \cup \varphi([\![t_2]\!]_{\rho[x\mapsto v_2]}) \mid \varphi \in [\![t_1]\!]_{\rho[x\mapsto v_1]} \cup [\![t_1]\!]_{\rho[x\mapsto v_2]} \right\} \\
&\overset{!}{\subseteq} \bigcup \left\{ \varphi([\![t_2]\!]_{\rho[x\mapsto v_1]} \cup [\![t_2]\!]_{\rho[x\mapsto v_2]}) \mid \varphi \in [\![t_1]\!]_{\rho[x\mapsto v_1]} \cup [\![t_1]\!]_{\rho[x\mapsto v_2]} \right\} \\
&\overset{\text{i.h.}}{\subseteq} \bigcup \left\{ \varphi([\![t_2]\!]_{\rho[x\mapsto v_1\cup v_2]}) \mid \varphi \in [\![t_1]\!]_{\rho[x\mapsto v_1\cup v_2]} \right\} \\
&= [\![t_1 \cup t_2]\!]_{\rho[x\mapsto v_1\cup v_2]}
\end{aligned}
$$

Case "$t = \emptyset$": $[\![\emptyset]\!]_{\rho[x\mapsto v_1]} \cup [\![\emptyset]\!]_{\rho[x\mapsto v_2]} = \emptyset = [\![\emptyset]\!]_{\rho[x\mapsto v_1\cup v_2]}$.

Case "$t = \{c\}$": $[\![\{c\}]\!]_{\rho[x\mapsto v_1]} \cup [\![\{c\}]\!]_{\rho[x\mapsto v_2]} = \{c\} = [\![\{c\}]\!]_{\rho[x\mapsto v_1\cup v_2]}$.

Case "$t = t_1 \cup t_2$": $[\![t_1 \cup t_2]\!]_{\rho[x\mapsto v_1]}[\![t_1 \cup t_2]\!]_{\rho[x\mapsto v_2]} = [\![t_1]\!]_{\rho[x\mapsto v_1]} \cup [\![t_1]\!]_{\rho[x\mapsto v_2]} \cup [\![t_2]\!]_{\rho[x\mapsto v_1]} \cup [\![t_2]\!]_{\rho[x\mapsto v_2]} \overset{\text{i.h.}}{\subseteq} [\![t_1]\!]_{\rho[x\mapsto v_1\cup v_2]} \cup [\![t_2]\!]_{\rho[x\mapsto v_1\cup v_2]} = [\![t_1 \cup t_2]\!]_{\rho[x\mapsto v_1\cup v_2]}$. □

The inequality of Lemma 7 is not an equality.

**Counterexample 1.** Let app $= \lambda f.\lambda x.f\ x$, then app $(\lambda x.\emptyset)\ \{C\} \cup$ app $(\lambda x.x)\emptyset \rightsquigarrow \emptyset$, but app $((\lambda x.\emptyset) \cup (\lambda x.x))\ (\{C\} \cup \emptyset) \rightsquigarrow \{C\}$.

### A.1.3 Normalization (with widening)

– To do: We can make union only work on base types (as we not longer *need* to distribute unions over applications)? Then the denotation of the function space would be simpler and might generalize to other structures..

To reduce $\lambda^{\cup}$-terms to a normal form we combine the $\beta$-reduction rule of the simply typed $\lambda$-calculus with rewrite rules that deal with the associativity, commutativity, idempotence and identity (ACI1) properties of set-union operator.

If a term $t$ is $\eta$-long it can be written in the form

$$t = \lambda x_1 \cdots x_n.\{f_1(t_{11}, ..., t_{1q_1}), ..., f_p(t_{p1}, ..., t_{pq_p})\}$$

where $f_i$ can be a free or bound variable, a singleton-set constant, or another $\eta$-long term; and $q_i$ is equal to the arity of $f_i$ (for all $1 \leqslant i \leqslant p$). The notation $\{f_1(t_{11}, ..., t_{1q_1}), ..., f_p(t_{p1}, ..., t_{pq_p})\}$ is a shorthand for $f_1(t_{11}, ..., t_{1q_1}) \cup \cdots \cup f_p(t_{p1}, ..., t_{pq_p})\}$, where we forget the associativity of the set-union operator and any empty-set constants. Note that despite the suggestive notation, this is not a true set, as there may still be duplicate elements $f_i(t_{i1}, ..., t_{iq_i})$.

A normal form $v$ of a term $t$ can be written as

$$v = \lambda x_1 \cdots x_n.\{k_1(v_{11}, ..., v_{1q_1}), ..., k_p(v_{p1}, ..., v_{pq_p})\}$$

where $k_i$ can be a free or bound variable, or a singleton-set constant, but not a term as this would form a $\beta$-redex.[1] For each $k_i, k_j$ with $i < j$ we must also have that $k_i < k_j$ for some total order on $\mathbf{Var} \cup \mathbf{Con}$. Not only does this imply that each ter m $k_i(v_{i1}, ..., v_{iq_i})$ occurs only once in $k_1(v_{11}, ..., v_{1q_1}), ..., k_p(v_{p1}, ..., v_{pq_p})$, but also the stronger condition that $k_i \neq k_j$ for all $i \neq j$.

[1] Technically, terms that bind at least one variable would form a $\beta$-redex. Terms that do not bind any variables do not occur either as they merely form a subsequence of $k_1(v_{11}, ..., v_{1q_1}), ..., k_p(v_{p1}, ..., v_{pq_p})$ in this notation.

$$
\begin{array}{l}
\quad \text{-- normalization of terms} \\
\llbracket \cdot \rrbracket :: \mathbf{Tm} \to \mathbf{Nf} \\
\llbracket \lambda x_1 \cdots x_n.T \rrbracket = \\
\quad \lambda x_1 \cdots x_n.\wr\{ \lfloor f_i(\llbracket t_{i1} \rrbracket, ..., \llbracket t_{iq_i} \rrbracket) \rfloor \mid f_i(t_{i1}, ..., t_{iq_i}) \in T \}\wr \\
\quad \text{-- } \beta\text{-reduction} \\
\lfloor k(v_1, ..., v_q) \rfloor \\
\quad = k(v_1, ..., v_q) \\
\lfloor (\lambda y_1 \cdots y_q.T)\ (v\_1, \cdots, v\_q) \rfloor \\
\quad = SUBST\ x\ y\ z \\
\quad \text{-- set-rewriting} \\
\wr\{\cdots, k\_i\ (\cdots), \cdots, k\_j\ (\cdots), \cdots\}\wr \\
\quad \mid k\_j < k\_i = \wr\{\cdots, k\_i\ (\cdots), \cdots, k\_j\ (\cdots), \cdots\}\wr \\
\wr\{\cdots, k\ (\cdots), k\ (\cdots), \cdots\}\wr \\
\quad = \wr\{\cdots, k\ (\cdots), \cdots\}\wr \\
\wr T\wr \\
\quad = T
\end{array}
$$

Figure A.1: To do.Normalization algorithm of $\lambda^{\cup}$-terms.

## A.2 Type inference

$$
\begin{array}{l}
\mathcal{R}(\Gamma; \Delta; \mathbf{fix}\ x : \tau.t) = \\
\quad \mathbf{let}\ \widehat{\tau}\ \&\ \xi \qquad\qquad\qquad\qquad\qquad = \mathcal{R}(\Gamma; \Delta; t) \\
\qquad \widehat{\tau}'\langle e' \rangle \to \widehat{\tau}''\langle \xi'' \rangle\ \&\ \overline{e_i :: \kappa_i} = \mathcal{I}(\widehat{\tau}) \\
\quad \mathbf{in}\ \ \mathit{Triple}\ \widehat{\tau}_0\ \xi_0\ i \leftarrow \mathit{Triple}\ \bot_\tau\ \emptyset\ 0 \\
\qquad \mathbf{do}\ \theta \qquad\qquad\qquad\qquad\quad \leftarrow [e' \mapsto \xi_i] \circ \mathcal{M}(\emptyset; \widehat{\tau}'; \widehat{\tau}_i) \\
\qquad\quad \mathit{Triple}\ \widehat{\tau}_{i+1}\ \xi_{i+1}\ i \leftarrow \mathit{Triple}\ \llbracket \theta\widehat{\tau}'' \rrbracket_\Delta\ \llbracket \theta\xi'' \rrbracket_\Delta\ (i+1) \\
\qquad \mathbf{until}\ \widehat{\tau}_i\ \&\ \xi_i \equiv \widehat{\tau}_{i-1}\ \&\ \xi_{i-1} \\
\qquad \mathbf{return}\ \widehat{\tau}_i\ \&\ \llbracket \xi \cup \xi_i \rrbracket_\Delta
\end{array}
$$

## A.3 Completion

The completion procedure as an algorithm:

$\mathcal{C}(\cdot;\cdot) : \mathbf{Env} \times \mathbf{Ty} \to \widehat{\tau} \times \xi \times \mathbf{Env}$
$\mathcal{C}(\overline{e_i :: \kappa_i}; \mathbf{bool}) =$
  **let** *e be fresh*
  **in** $\langle \widehat{\text{bool}}; e\ \overline{e_i}; e : \overline{\kappa_i \Rightarrow} \text{ EXN} \rangle$

## A.4 TODO

- naming and ordering of quantified exception set variables in the examples is inconsistent.
- notation of type signatures in the examples is inconsisten.
- standard polyrec examples (DHM + GSM)
- polyrec does not "come for free"
- type inference: we have a fixpoint a la DHM
- widening
- "algebraic" effects?
- unexpected decidablity
- ack: Vincent + Femke; Andrew + Jeremy + Stephanie + Andres; ST-RC
- check wiki and folder for notes
- exception type of twice (and other h-o funs)
- no slanted-greek for lambda and Lambda
- typeset System $F_\omega$ correctly
- roll Metatheory into earlier sections, add new section Analysis (also add to Overview)
- Untracked exceptions can break information flow security.
- Elaborte in the subsection "Contributions". Mention prototype?
- : vs ::
- add function composition as an additional example

## Abstract

– title: Higher-order effect types

### A.4.1 Introduction

– In the final example (map (const undefined)) no non-exceptional values will be *actually* present in the resulting list

– Why not $\alpha\langle e_1\rangle \xrightarrow{e_3} \beta\langle e_2\rangle$?! Give some examples why higher-rankedness is needed. The example on the poster/*map* isn't sufficient. Postpone to a later section?

– Need an example that clearly demonstrates why HRP is *needed* (May be difficult without also constructing a complete subtyping-based analysis?)

### A.4.2 The $\lambda^{\cup}$-calculus

– To DO: We can make union only work on base types (as we not longer *need* to distribute unions over applications)? Only need during widening, now...

– To DO: Prove more Lemmas about reduction rules (esp. $\gamma_1$)

– Add reduction rules for $\emptyset$ and idempotence to the Figure. (Do wee need the bars above the rules?)

– Prove semantics is ACI1. We have a different unit for each type!

– $\mathcal{P}(V_{\tau_1} \to V_{\tau_2}) \simeq V_{\tau_1} \to \mathcal{P}(V_{\tau_2})$? Cardinallity suggests not: $2^{(\beta^\alpha)} \neq (2^\beta)^\alpha$.

– If we don't distribute unions over applications, can we ever get them deep inside terms?

– If we don't *and* the outermost lambdas are not there because is always of kind star, can we get non-trivial terms? I.e. something other than $e_1(e_{11}, ..., e_{1n_1}) \cup \cdots \cup e_k(e_{k1}, ..., e_{kn_k})$ (note: $e$ and not $t$ as arugments).

**Widening**

- Does this give us any bounds on the complexity? (Or do the fact that we have arguments prevent this?)
- Footnote about *narrowing*.
- Note that this is the reason $\cup$ needs to be higher-order.

### A.4.3 Source language

- We either need to omit the type annotations on $\lightning^{\ell}_{\tau}$, or add them to **if then else** and **case of** $\{[] \mapsto; :: \mapsto\}$.
- We do not have a rule E-AnnAppExn. Check that the canonical forms lemma gives us that terms of universally quantified type cannot be exceptional values.
- Replace the arrow with another one? (This one clashes with the reduction relation from $\lambda^{\cup}$.)
- Define the meaning of the double brackets in the redecution rule E-Op.
- Let-bindings can be defined in terms of abstractions (because HRP)

### A.4.4 Exception types

- "Type signatures are denoted as ..." there are several other ways used to write this
- The syntax of environments is omitted from the "syntax" figure
- Merge the figures with syntax and well-formedness?
- Elaborate on well-formedness
- Prove that $\overset{*}{\leftrightarrow} \iff \simeq$.
- To do: Rename stuff in T-App in the elaboration system (now subtype/-effect of the result instead of the argument and clashes with the indices enumerated over by $i$!

- To do: T-AnnAbs: $e \notin \mathrm{fv}(\Gamma)$
- $e \in$ **ExnVar**
- Well-formedness of exception types: embed conservativity / full-flexibility?
- Can we roll Univ and Arr into a single construct: $\forall e :: \kappa.\widehat{\tau}_1\langle e\rangle \to \widehat{\tau}_2\langle\xi(e)\rangle$? Still need to deal with the well-formedness of $\widehat{\tau}_1$... Also may need to quantify over more than one variable simultaneously...

**Subtyping**

- Is S-Refl an admissable/derivable rule, or should we drop S-Bool and S-Int?
- Possibly useful lemma: $\widehat{\tau}_1 = \widehat{\tau}_2 \iff \widehat{\tau}_1 \leqslant \widehat{\tau}_2 \wedge \widehat{\tau}_2 \leqslant \widehat{\tau}_1$.

**Conservative types**

- To do: Atomicity: $e_1 \cup e_2 \to [e_1\langle e_2\rangle]$ is not useful, because no introspection
- To do.check all examples types against prototype
- To do.properly typeset example types
- To do.Skolemization and explicit existential quantification over unification variables?

**Declarative type system**

- To do: Exception type erasure relation
- To do: Least upper bounds (declaratively, as subtypes)
- In T-AnnAbs, $\Gamma, \xi = \Delta$?
- In T-Abs and T-AnnAbs, should the term-level term-abstraction also have an explicit effect annotation?
- In T-AnnAbs, might need a side condition stating that $e$ is not free in $\Delta$.

- In T-App, note the double occurence of $\xi$ when typing $t_1$. Is subeffecting sufficient here? Also note that we do *not* expect an exception variable in the left-hand side annotation of the function space constructor.
- In T-AnnApp, note the substitution. We need a substitution lemma for annotations.
- In T-Fix, the might be some universal quantifiers in our way. Do annotation applications in $t$ take care of this, already? Perhaps we do need to change **fix** $t$ into a binding construct to resolve this? Also, there is some implicit subeffecting going on between the annotations and effect.
- In T-Case, note the use of explicit subeffecting. Can this be done using implicit subeffecting?
- For T-Sub, should we introduce a term-level coercion, as in Dussart–Henglein–Mossin? We now do shape-conformant subtyping, is subeffecting sufficient?
- Do we need additional kinding judgements in some of the rules? Can we merge the kinding judgement with the subtyping and/or -effecting judgement? Kind-preserving substitutions.

**Type elaboration system**

- In T-App and T-Fix, note that there are substitutions in the premises of the rules. Are these inductive? (Probably, as these premises are not "recursive" ones.)

### A.4.5 Type inference

- Complexity: reduction corresponds to agressive constraint simplification
- alternative (faster?) version of Kleene-Mycroft
- In R-App and R-Fix: check that the fresh variables generated by $\mathcal{I}(\cdot)$ are subsituted away by the substitution $\theta$ created by $\mathcal{M}(\cdot;\cdot;\cdot)$. Also, we don't need those variables in the algorithm if we don't generate the elaborated term.

- In R-Fix we could get rid of the auxillary underlying type function if the fixpoint construct was replaced with a binding variant with an explicit type annotation.
- For R-Fix, make sure the way we handle fixpoints of exceptional value in a manner that is sound w.r.t. to the operational semantics we are going to give to this.
- Note that we do not construct the elaborated term, as it is not useful other than for metatheoretic purposes.
- Lemma: The algorithm maintains the invariant that exception types and exceptions are in normal form.
- Typesetting issues $[\![\cdot]\!]$.

### A.4.6 Related work

- linear-algebriac lambda-calculi (Arrighi and Dowek, Vaux)
- More differences between Holdermans and Hage (2010) (e.g. data types)?
- Christian Mossin. "Exact flow types" (intersection types, also non-elementary recursive by Statman)
- algebraic lambda calculus: higher-order $\to$ second-order?

### A.4.7 Future research

- higher-ranked algebraic effect types, Koka

# Bibliography

Ole Agesen. The cartesian product algorithm: Simple and precise type inference of parametric polymorphism. In *Proceedings of the 9th European Conference on Object-Oriented Programming*, ECOOP '95, pages 2–26. Springer-Verlag, 1995. ISBN 3-540-60160-0.

Alexander Aiken and Edward L. Wimmers. Type inclusion constraints and type inference. In *Proceedings of the Conference on Functional Programming Languages and Computer Architecture*, FPCA '93, pages 31–41. ACM, 1993. ISBN 0-89791-595-X.

Matthias Baaz. Note on the existence of most-general semi-unifiers. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, pages 19–28. Oxford University Press, 1993. ISBN 0-19-853690-9.

Nick Benton and Peter Buchlovsky. Semantics of an effect analysis for exceptions. In *Proceedings of the 2007 ACM SIGPLAN International Workshop on Types in Languages Design and Implementation*, TLDI '07, pages 15–26. ACM, 2007. ISBN 1-59593-393-X.

Luis Damas and Robin Milner. Principal type-schemes for functional programs. In *Proceedings of the 9th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '82, pages 207–212. ACM, 1982. ISBN 0-89791-065-6.

Gilles Dowek. Higher-order unification and matching. In Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, pages 1009–1062. Elsevier Science Publishers, 2001. ISBN 0-444-50812-0.

Glenn Durfee. A model for a list-oriented extension of the lambda calculus. MSc thesis, Carnegie Mellon University, 1997.

Dirk Dussart, Fritz Henglein, and Christian Mossin. Polymorphic recursion and subtype qualifications: Polymorphic binding-time analysis in polynomial time. In *Proceedings of the Second International Symposium on Static Analysis*, SAS '95, pages 118–135. Springer-Verlag, 1995. ISBN 3-540-60360-3.

Manuel Fähndrich, Jeffrey Foster, Jason Cu, and Alexander Aiken. Tracking down exceptions in Standard ML programs. Technical Report UCB/CSD-98-996, University of California at Berkeley, 1998.

Karl-Filip Faxén. Polyvariance, polymorphism and flow analysis. In *Selected Papers from the 5th LOMAPS Workshop on Analysis and Verification of Multiple-Agent Languages*, pages 260–278. Springer-Verlag, 1997. ISBN 3-540-62503-8.

Jean-Yves Girard. *Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre supérieur*. PhD thesis, Université Paris 7, 1972.

Kevin Glynn, Peter J. Stuckey, Martin Sulzmann, and Harald Søndergaard. Exception analysis for non-strict languages. In *Proceedings of the seventh ACM SIGPLAN international conference on Functional programming*, ICFP '02, pages 98–109. ACM, 2002. ISBN 1-58113-487-8.

Juan Carlos Guzmán and Ascánder Suárez. An extended type system for exceptions. In *Proceedings of the ACM SIGPLAN Workshop on ML and its Applications*, ML '94, pages 127–135, 1994.

Fritz Henglein. Type inference with polymorphic recursion. *ACM Transactions on Programming Languages and Systems*, 15(2):253–289, April 1993. ISSN 0164-0925.

J. Roger Hindley. The principal type-scheme of an object in combinatory logic. *Transactions of the American Mathematical Society*, 146:29–60, 1969. ISSN 0002-9947.

Stefan Holdermans and Jurriaan Hage. Polyvariant flow analysis with higher-ranked polymorphic types and higher-order effect operators. In *Proceedings of the 15th ACM SIGPLAN International Conference on Functional Programming*, ICFP '10, pages 63–74. ACM, 2010. ISBN 1-60558-794-X.

Pierre Jouvelot and David K. Gifford. Algebraic reconstruction of types and effects. In *Proceedings of the 18th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '91, pages 303–310. ACM, 1991. ISBN 0-89791-419-8.

Andrew J. Kennedy. Dimension types. In *Proceedings of the 5th European Symposium on Programming: Programming Languages and Systems*, ESOP '94, pages 348–362. Springer, 1994. ISBN 3-540-57880-3.

Andrew J. Kennedy. *Programming Languages and Dimensions*. PhD thesis, University of Cambridge, 1996a.

Andrew J. Kennedy. Type inference and equational theories. Technical Report LIX-RR-96-09, Laboratoire D'Informatique, École Polytechnique, 1996b.

Assaf J. Kfoury, Jerzy Tiuryn, and Paweł Urzyczyn. ML typability is DEXPTIME-complete. In *Proceedings of the Fifteenth Colloquium on Trees in Algebra and Programming*, CAAP '90, pages 206–220. Springer-Verlag, 1990a. ISBN 0-387-52590-4.

Assaf J. Kfoury, Jerzy Tiuryn, and Paweł Urzyczyn. The undecidability of the semi-unification problem. In *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, STOC '90, pages 468–476. ACM, 1990b. ISBN 0-89791-361-2.

Assaf J. Kfoury, Jerzy Tiuryn, and Paweł Urzyczyn. Type reconstruction in the presence of polymorphic recursion. *ACM Transactions on Programming Languages and Systems*, 15(2):290–311, April 1993. ISSN 0164-0925.

Ruud Koot and Jurriaan Hage. Type-based exception analysis for non-strict higher-order functional languages with imprecise exception semantics. In *Proceedings of the 2015 Workshop on Partial Evaluation and Program Manipulation*, PEPM '15, pages 127–138. ACM, 2015. ISBN 978-1-4503-3297-2.

Xavier Leroy and François Pessaux. Type-based analysis of uncaught exceptions. *ACM Transactions on Programming Languages and Systems*, 22(2):340–377, March 2000. ISSN 0164-0925.

John M. Lucassen and David K. Gifford. Polymorphic effect systems. In *Proceedings of the 15th ACM SIGPLAN-SIGACT Symposium on Principles of*

*Programming Languages*, POPL '88, pages 47–57. ACM, 1988. ISBN 0-89791-252-7.

Harry G. Mairson. Deciding ML typability is complete for deterministic exponential time. In *Proceedings of the 17th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '90, pages 382–401. ACM, 1990. ISBN 0-89791-343-4.

Dale Miller. A logic programming language with lambda-abstraction, function variables, and simple unification. In Peter Schroeder-Heister, editor, *Extensions of Logic Programming*, volume 475 of *Lecture Notes in Computer Science*, pages 253–281. Springer, 1991. ISBN 3-540-53590-X.

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

Neil Mitchell and Colin Runciman. Not all patterns, but enough: an automatic verifier for partial but sufficient pattern matching. In *Proceedings of the first ACM SIGPLAN symposium on Haskell*, Haskell '08, pages 49–60. ACM, 2008. ISBN 1-60558-064-3.

Alan Mycroft. Polymorphic type schemes and recursive definitions. In Manfred Paul and Bernard Robinet, editors, *International Symposium on Programming*, volume 167 of *Lecture Notes in Computer Science*, pages 217–228. Springer, 1984. ISBN 3-540-12925-1.

Tobias Nipkow and Zhenyu Qian. Modular higher-order E-unification. In Ronald V. Book, editor, *Rewriting Techniques and Applications*, volume 488 of *Lecture Notes in Computer Science*, pages 200–214. Springer, 1991. ISBN 3-540-53904-2.

Mitsuhiro Okada. Strong normalizability for the combined system of the typed lambda calculus and an arbitrary convergent term rewrite system. In *Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation*, ISSAC '89, pages 357–363. ACM, 1989. ISBN 0-89791-325-6.

Simon Peyton Jones, Alastair Reid, Fergus Henderson, Tony Hoare, and Simon Marlow. A semantics for imprecise exceptions. In *Proceedings of the ACM SIGPLAN 1999 Conference on Programming Language Design and Implementation*, PLDI '99, pages 25–36. ACM, 1999. ISBN 1-58113-094-5.

Zhenyu Qian and Kang Wang. Modular higher-order equational preunification. *Journal of Symbolic Computation*, 22(4):401–424, 1996. ISSN 0747-7171.

György E. Révész. A list-oriented extension of the lambda-calculus satisfying the Church–Rosser theorem. *Theoretical Compututer Science*, 93(1):75–89, February 1992. ISSN 0304-3975.

Mikael Rittri. Semi-unification of two terms in abelian groups. *Information Processing Letters*, 52(2):61–68, October 1994. ISSN 0020-0190.

Mikael Rittri. Dimension inference under polymorphic recursion. In *Proceedings of the Seventh International Conference on Functional Programming Languages and Computer Architecture*, FPCA '95, pages 147–159. ACM, 1995. ISBN 0-89791-719-7.

Olin G. Shivers. *Control-Flow Analysis of Higher-Order Languages*. PhD thesis, Carnegie Mellon University, 1991. Available as CMU Technical Report CMU-CS-91-145.

Scott F. Smith and Tiejun Wang. Polyvariant flow analysis with constrained types. In Gert Smolka, editor, *Programming Languages and Systems*, volume 1782 of *Lecture Notes in Computer Science*, pages 382–396. Springer Berlin Heidelberg, 2000. ISBN 3-540-67262-1.

Wayne Snyder. Higher order E-unification. In *Proceedings of the Tenth International Conference on Automated Deduction*, CADE '90, pages 573–587. Springer-Verlag, 1990. ISBN 3-540-52885-7.

Richard Statman. The typed $\lambda$-calculus is not elementary recursive. *Theoretical Computer Science*, 9(1):73–81, 1979. ISSN 0304-3975.

Jean-Pierre Talpin and Pierre Jouvelot. Polymorphic type, region and effect inference. *Journal of Functional Programming*, 2(3):245–271, 1992. ISSN 1469-7653.

Jean-Pierre Talpin and Pierre Jouvelot. The type and effect discipline. *Information and Computation*, 111(2):245–296, June 1994. ISSN 0890-5401.

Val Tannen. Combining algebra and higher-order types. In *Proceedings of the Third Annual Symposium on Logic in Computer Science*, LICS '88, pages 82–90. IEEE, 1988. ISBN 0-8186-0853-6.

Val Tannen and Jean Gallier. Polymorphic rewriting conserves algebraic strong normalization. *Theoretical Computer Science*, 83(1):3 – 28, 1991. ISSN 0304-3975.

Mads Tofte and Jean-Pierre Talpin. Implementation of the typed call-by-value $\lambda$-calculus using a stack of regions. In *Proceedings of the 21st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '94, pages 188–201. ACM, 1994. ISBN 0-89791-636-0.

David A. Wright. A new technique for strictness analysis. In Samson Abramsky and Tom. S. E. Maibaum, editors, *Fourth International Joint Conference on Theory and Practice of Software Development*, volume 494 of *Lecture Notes in Computer Science*, pages 235–258. Springer, 1991. ISBN 3-540-53981-6.

Kwangkeun Yi. Compile-time detection of uncaught exceptions in Standard ML programs. In Baudouin Charlier, editor, *Static Analysis*, volume 864 of *Lecture Notes in Computer Science*, pages 238–254. Springer, 1994. ISBN 3-540-58485-4.