编程语言的设计原理

Design Principles of Programming Languages

Haiyan Zhao，Di Wang

赵海燕，王迪

Peking University, Spring Term 2024

Recapitulation

Reference

Syntax

We added to $\lambda_{\rightarrow}$ (with Unit) syntactic forms for *creating*, *dereferencing*, and *assigning* reference cells, plus a new type constructor Ref.

t ::=		*terms*
	unit	*unit constant*
	x	*variable*
	λx:T.t	*abstraction*
	t t	*application*
	ref t	*reference creation*
	!t	*dereference*
	t:=t	*assignment*
	l	store location

Evaluation

Evaluation becomes *a* relation with the states of store:

$$t \mid \mu \longrightarrow t' \mid \mu'$$

$$\frac{l \notin dom(\mu)}{\texttt{ref}\ \ v_1 \mid \mu \longrightarrow l \mid (\mu, l \mapsto v_1)} \qquad \text{(E-RefV)}$$

$$\frac{\mu(l) = v}{!l \mid \mu \longrightarrow v \mid \mu} \qquad \text{(E-DerefLoc)}$$

$$l := v_2 \mid \mu \longrightarrow \texttt{unit} \mid [l \mapsto v_2]\mu \qquad \text{(E-Assign)}$$

Typing

Typing becomes *a* *four-place* relation: $\Gamma \mid \Sigma \vdash t : T$

$$\frac{\Sigma(l) = T_1}{\Gamma \mid \Sigma \vdash l : \mathtt{Ref}\ T_1} \quad \text{(T-Loc)}$$

$$\frac{\Gamma \mid \Sigma \vdash t_1 : T_1}{\Gamma \mid \Sigma \vdash \mathtt{ref}\ t_1 : \mathtt{Ref}\ T_1} \quad \text{(T-Ref)}$$

$$\frac{\Gamma \mid \Sigma \vdash t_1 : \mathtt{Ref}\ T_{11}}{\Gamma \mid \Sigma \vdash !t_1 : T_{11}} \quad \text{(T-Deref)}$$

$$\frac{\Gamma \mid \Sigma \vdash t_1 : \mathtt{Ref}\ T_{11} \qquad \Gamma \mid \Sigma \vdash t_2 : T_{11}}{\Gamma \mid \Sigma \vdash t_1 := t_2 : \mathtt{Unit}} \quad \text{(T-Assign)}$$

Preservation

Theorem: if

$\Gamma \mid \Sigma \vdash t : T$

$\Gamma \mid \Sigma \vdash \mu$

$t \mid \mu \longrightarrow t' \mid \mu'$

then, for some $\Sigma' \supseteq \Sigma$,

$\Gamma \mid \Sigma' \vdash t' : T$

$\Gamma \mid \Sigma' \vdash \mu'$.

Progress

Theorem:

Suppose t is a *closed, well-typed* term, i.e.,

$$\emptyset \mid \Sigma \vdash \mathrm{t} : \mathrm{T} \quad \text{for some } \mathrm{T} \text{ and } \Sigma$$

Then either t is a value or else, for any store μ such that $\emptyset \mid \Sigma \vdash \mu$, there is some term t' and store μ' with $\mathrm{t} \mid \mu \longrightarrow \mathrm{t}' \mid \mu'$.

Chapter 14: Exceptions

Why exceptions

Raising exceptions (aborting whole program)

Handling exceptions

Exceptions carrying values

Exceptions

Why exceptions?

Real world programming is full of situations where a function needs to *signal to it caller* that it is *unable to perform its task* for :

- Division by zero
- Arithmetic overflow
- Array index out of bound
- Lookup key missing
- File could not be opened
- ……

Most programming languages *provide some mechanism* for interrupting *the normal flow of control* in a program to *signal some exceptional condition* (& the transfer of control flow)

Why exceptions?

type $'\alpha$ list = None | Some of $'\alpha$

```
# let head l = match l with
                 []  -> None
               | x::_   -> Some (x);;
```

Note that it is always possible to program *without exceptions* :

- instead of raising an exception, return None
- instead of returning result x normally, return Some(x)

Why exceptions?

```
# type 'α list = None | Some of 'α
# let head l  = match l with
                  []        -> None
                |    x::_      -> Some (x);;
```

What is the result of type inference?

val head: 'α list -> 'α Option = <fun>

What we expect

val head: 'α list -> 'α = <fun>

```
# let head l  =  match l with
                   []        ->  raise Not_found
                 |   x::_      ->  x;;
```

Why exceptions?

If we want to wrap every function application in a case to find out *whether it returned a result or an exception*?

It is much more convenient to *build this mechanism into the language,* and *provide mechanism* for interrupting *the normal flow of control* in a program to *signal some exceptional condition* (& the transfer of control flow).

Varieties of non-local control

There are many ways of adding "*non-local control flow*"

- exit(1)
- goto
- setjmp/longjmp
- raise/try (or catch/throw) in many variations
- callcc / continuations
- more esoteric variants (cf. many Scheme papers)

that allow programs to effect *non-local "jumps"* in the flow of control

Let's begin with the simplest of these.

Raising exceptions

(aborting whole program)

An "abort" primitive in $\lambda_{\rightarrow}$

Raising exceptions (but not catching them), which cause the *abort of the whole program*

Syntactic forms

$\texttt{t} ::= \ldots$		*terms*
	$\texttt{error}$	*run-time error*

Evaluation

$$\texttt{error}\ \texttt{t}_2 \longrightarrow \texttt{error} \qquad \text{(E-AppErr1)}$$

$$\texttt{v}_1\ \texttt{error} \longrightarrow \texttt{error} \qquad \text{(E-AppErr2)}$$

Typing

$$\Gamma \vdash \texttt{error} : \texttt{T} \qquad \text{(T-ERROR)}$$

New syntactic forms

$\texttt{t} ::= \ldots$ — *terms:*

$\texttt{error}$ — *run-time error*

New evaluation rules — $\boxed{\texttt{t} \longrightarrow \texttt{t}'}$

$\texttt{error}\ \texttt{t}_2 \longrightarrow \texttt{error}$ (E-APPERR1)

$\texttt{v}_1\ \texttt{error} \longrightarrow \texttt{error}$ (E-APPERR2)

New typing rules — $\boxed{\Gamma \vdash \texttt{t} : \texttt{T}}$

$\Gamma \vdash \texttt{error} : \texttt{T}$ (T-ERROR)

Typing errors

Note that the typing rule for error allows us to give it *any type* T.

$$\Gamma \vdash \texttt{error} : \texttt{T} \qquad \text{(T-ERROR)}$$

What if we had booleans and numbers in the language?

This means that both

$$if\ x > 0\ then\ 5\ else\ error$$

and

$$if\ x > 0\ then\ true\ else\ error$$

will typecheck

Aside: Syntax-directedness

Note: this rule

$$\Gamma \vdash \texttt{error} : \mathsf{T} \qquad \text{(T-ERROR)}$$

has a **problem** from the **point of view of implementation** :

it is **not syntax directed**

Aside: Syntax-directed rules

When we say a set of rules is *syntax-directed* we mean *two things*:

1. There is *exactly one rule* in the set that applies to each syntactic form (in the sense that we can tell *by the syntax of a term* which rule to use)
   - *e.g.,* to derive a type for t_1 t_2, we must use T-App
2. We *don't* have to "*guess*" an input (or output) for any rule
   - *e.g.,* to derive a type for t_1 t_2, we need to *derive a type for* t_1 and *a type for* t_2

Aside: Syntax-directedness

Note: this rule

$$\Gamma \vdash \texttt{error} : \mathtt{T} \qquad \text{(T-ERROR)}$$

has a *problem* from the *point of view of implementation* : it is *not syntax directed*

This will cause the *Uniqueness of Types* theorem to fail

For purposes of *defining the language and proving its type safety*, this is not a problem — *Uniqueness of Types* is not critical

Let's think a little about how the rule might be fixed ...

An alternative: Ascription

Can't we just *decorate the* error *keyword* with its *intended type*, as we have done to fix related problems with other constructs?

$$\Gamma \vdash (\texttt{error as T}) : \texttt{T} \qquad \text{(T-Error)}$$

An alternative : Ascription

Can't we just *decorate the error keyword* with its intended type, as we have done to fix related problems with other constructs?

$$\Gamma \vdash (\texttt{error as T}) : \texttt{T} \qquad \text{(T-Error)}$$

Unfortunately, this doesn't work!

e.g. assuming our language also has *numbers* and *booleans*:

$$\text{succ (if (error as Bool) then 3 else 8)}$$
$$\longrightarrow \text{succ (error as Bool)}$$

Another alternative: Variable type

In a system with *universal polymorphism* (like OCaml), the variability of typing for error can be dealt with by *assigning it a variable type* ?

$$\Gamma \vdash \text{error} : {}'\alpha \qquad \text{(T-ERROR)}$$

Another alternative: Variable type

In a system with *universal polymorphism* (like OCaml), the variability of typing for error can be dealt with by assigning it a variable type!

$$\Gamma \vdash \text{error} : {}'\alpha \qquad \text{(T-ERROR)}$$

In effect, we are replacing the uniqueness of typing property by a weaker (but still very useful) property called most general typing

– i.e., although a term may have many types, we always have a compact way of representing the set of all of its possible types

Yet another alternative : *minimal* type

Alternatively, in a system with subtyping (which will be discussed in chapter 15) and *a minimal* Bot type, we *can* give error a unique type:

Yet another alternative : *minimal* type

Alternatively, in a system with subtyping (which will be discussed in chapter 15) and *a minimal* Bot type, we *can* give error a unique type:

$$\Gamma \vdash \texttt{error} : \texttt{Bot} \qquad \text{(T-ERROR)}$$

Note :

What we've really done is *just pushed the complexity* of the old error rule *onto the* Bot *type* !

For now…

Let’s stick with the original rule

$$\Gamma \vdash \texttt{error} : \mathtt{T} \qquad \text{(T-Error)}$$

and live with the resulting *non-determinism* of the typing relation

Type safety

Property of preservation?

The preservation theorem requires *no changes* when we add error:

- if *a term* of type T reduces to $error$, that's fine, since $error$ has every type T

Type safety

Property of preservation?

The preservation theorem requires no changes when we add error: :

if a term of type T reduces to error, that's fine, since error has every type T.

Whereas,

Progress *requires a little more care*

Progress

First, *note that* we do *not* want to extend the set of ***values*** to include error, since this would make *our new rule* for *propagating errors* through applications

$$\texttt{v}_1\ \texttt{error} \longrightarrow \texttt{error} \qquad \text{(E-AppErr2)}$$

overlap with our *existing computation rule* for applications:

$$(\lambda\texttt{x:T}_{11}\texttt{.t}_{12})\ \texttt{v}_2 \longrightarrow [\texttt{x} \mapsto \texttt{v}_2]\texttt{t}_{12} \qquad \text{(E-AppAbs)}$$

e.g, the term

$$(\lambda\, x{:}\, \mathrm{Nat}.\, 0)\ \mathrm{error}$$

could evaluate to either 0 (which would be wrong) or error (which is what we intend).

Progress

Instead, we **keep** **error** **as a** ***non-value normal form***, and **refine the statement of progress** to explicitly mention the *possibility* that *terms may evaluate to* $error$ instead of to a value

Theorem [Progress]:

Suppose `t` *is a closed, well-typed normal form.*

Then either `t` *is a value or* $t = error$.

Handling exceptions

Catching exceptions

syntax

$$\texttt{t} ::= \ldots \qquad \textit{terms}$$

$$\texttt{try t with t} \qquad \textit{trap errors}$$

Evaluation

$$\texttt{try } \texttt{v}_1 \texttt{ with } \texttt{t}_2 \longrightarrow \texttt{v}_1 \qquad \text{(E-TryV)}$$

$$\texttt{try error with } \texttt{t}_2 \longrightarrow \texttt{t}_2 \qquad \text{(E-TryError)}$$

$$\frac{\texttt{t}_1 \longrightarrow \texttt{t}_1'}{\texttt{try } \texttt{t}_1 \texttt{ with } \texttt{t}_2 \longrightarrow \texttt{try } \texttt{t}_1' \texttt{ with } \texttt{t}_2} \qquad \text{(E-Try)}$$

Typing

$$\frac{\Gamma \vdash \texttt{t}_1 : \texttt{T} \qquad \Gamma \vdash \texttt{t}_2 : \texttt{T}}{\Gamma \vdash \texttt{try } \texttt{t}_1 \texttt{ with } \texttt{t}_2 : \texttt{T}} \qquad \text{(T-Try)}$$

Exceptions carrying values

Exceptions carrying values

When something unusual happened, it's useful to *send back some extra information* about *which unusual thing has happened* so that the handler can *take some actions* depending on this information.

t	::=	...	*terms*
		raise t	*raise exception*

Exceptions carrying values

When something unusual happened, it's useful to *send back some extra information* about *which unusual thing has happened* so that the handler can *take some actions* depending on this information.

t	::=	...	*terms*
		raise t	*raise exception*

Atomic term error is replaced by *a term constructor*

raise *t*

where *t* is the *extra information* that we want to *pass to the exception handler*

Evaluation

$$(\texttt{raise}\ \texttt{v}_{11})\ \texttt{t}_2 \longrightarrow \texttt{raise}\ \texttt{v}_{11} \qquad \text{(E-AppRaise1)}$$

$$\texttt{v}_1\ (\texttt{raise}\ \texttt{v}_{21}) \longrightarrow \texttt{raise}\ \texttt{v}_{21} \qquad \text{(E-AppRaise2)}$$

$$\frac{\texttt{t}_1 \longrightarrow \texttt{t}_1'}{\texttt{raise}\ \texttt{t}_1 \longrightarrow \texttt{raise}\ \texttt{t}_1'} \qquad \text{(E-Raise)}$$

$$\texttt{raise}\ (\texttt{raise}\ \texttt{v}_{11}) \longrightarrow \texttt{raise}\ \texttt{v}_{11} \qquad \text{(E-RaiseRaise)}$$

$$\texttt{try}\ \texttt{v}_1\ \texttt{with}\ \texttt{t}_2 \longrightarrow \texttt{v}_1 \qquad \text{(E-TryV)}$$

$$\texttt{try}\ \texttt{raise}\ \texttt{v}_{11}\ \texttt{with}\ \texttt{t}_2 \longrightarrow \texttt{t}_2\ \texttt{v}_{11} \qquad \text{(E-TryRaise)}$$

$$\frac{\texttt{t}_1 \longrightarrow \texttt{t}_1'}{\texttt{try}\ \texttt{t}_1\ \texttt{with}\ \texttt{t}_2 \longrightarrow \texttt{try}\ \texttt{t}_1'\ \texttt{with}\ \texttt{t}_2} \qquad \text{(E-Try)}$$

Evaluation

$$(\texttt{raise } v_{11})\ t_2 \longrightarrow \texttt{raise } v_{11} \qquad \text{(E-AppRaise1)}$$

$$v_1\ (\texttt{raise } v_{21}) \longrightarrow \texttt{raise } v_{21} \qquad \text{(E-AppRaise2)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{raise } t_1 \longrightarrow \texttt{raise } t_1'} \qquad \text{(E-Raise)}$$

$$\texttt{raise } (\texttt{raise } v_{11}) \longrightarrow \texttt{raise } v_{11} \qquad \text{(E-RaiseRaise)}$$

$$\texttt{try } v_1 \texttt{ with } t_2 \longrightarrow v_1 \qquad \text{(E-TryV)}$$

$$\texttt{try raise } v_{11} \texttt{ with } t_2 \longrightarrow t_2\ v_{11} \qquad \text{(E-TryRaise)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{try } t_1 \texttt{ with } t_2 \longrightarrow \texttt{try } t_1' \texttt{ with } t_2} \qquad \text{(E-Try)}$$

Evaluation

$$\texttt{(raise v}_{11}\texttt{) t}_2 \longrightarrow \texttt{raise v}_{11} \qquad \text{(E-AppRaise1)}$$

$$\texttt{v}_1 \texttt{ (raise v}_{21}\texttt{)} \longrightarrow \texttt{raise v}_{21} \qquad \text{(E-AppRaise2)}$$

$$\frac{\texttt{t}_1 \longrightarrow \texttt{t}_1'}{\texttt{raise t}_1 \longrightarrow \texttt{raise t}_1'} \qquad \text{(E-Raise)}$$

$$\texttt{raise (raise v}_{11}\texttt{)} \longrightarrow \texttt{raise v}_{11} \qquad \text{(E-RaiseRaise)}$$

$$\texttt{try v}_1 \texttt{ with t}_2 \longrightarrow \texttt{v}_1 \qquad \text{(E-TryV)}$$

$$\texttt{try raise v}_{11} \texttt{ with t}_2 \longrightarrow \texttt{t}_2 \texttt{ v}_{11} \qquad \text{(E-TryRaise)}$$

$$\frac{\texttt{t}_1 \longrightarrow \texttt{t}_1'}{\texttt{try t}_1 \texttt{ with t}_2 \longrightarrow \texttt{try t}_1' \texttt{ with t}_2} \qquad \text{(E-Try)}$$

Typing

To typecheck raise expressions, we need to *choose a type* for *the values* that are *carried along* with exceptions, let's call it T_{exn}

$$\frac{\Gamma \vdash t_1 : T_{exn}}{\Gamma \vdash \text{raise } t_1 : T} \qquad \text{(T-RAISE)}$$

$$\frac{\Gamma \vdash t_1 : T \qquad \Gamma \vdash t_2 : T_{exn} \rightarrow T}{\Gamma \vdash \text{try } t_1 \text{ with } t_2 : T} \qquad \text{(T-TRY)}$$

What is T_{exn} ?

Further, we need to decide ***what type*** to use as T_{exn}

There are *several possibilities*.

1. Numeric error codes: T_{exn} = Nat (as in Unix)
2. Error messages: T_{exn} = String
3. A *predefined* variant type:

```
Texn  =  <divideByZero:     Unit,
          overflow:         Unit,
          fileNotFound:     String,
          fileNotReadable:  String,
          ... >
```

4. An *extensible* variant type (as in Ocaml)
5. A *class* of "*throwable objects*" (as in Java)

Recapitulation: Error handling

→ *error* *try* — *Extends* $\lambda_{\to}$ *with errors (14-1)*

New syntactic forms

t ::=	...	*terms:*
	try t with t	*trap errors*

New evaluation rules — $t \longrightarrow t'$

$$\texttt{try } v_1 \texttt{ with } t_2 \longrightarrow v_1 \qquad \text{(E-TryV)}$$

$$\texttt{try error with } t_2 \longrightarrow t_2 \qquad \text{(E-TryError)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{try } t_1 \texttt{ with } t_2 \longrightarrow \texttt{try } t_1' \texttt{ with } t_2} \qquad \text{(E-Try)}$$

New typing rules — $\Gamma \vdash t : T$

$$\frac{\Gamma \vdash t_1 : T \qquad \Gamma \vdash t_2 : T}{\Gamma \vdash \texttt{try } t_1 \texttt{ with } t_2 : T} \qquad \text{(T-Try)}$$

Recapitulation: Exceptions carrying values

→ *exceptions* *Extends $\lambda_\to$ (9-1)*

New syntactic forms

t ::=	...	*terms:*
	raise t	*raise exception*
	try t with t	*handle exceptions*

New evaluation rules $t \longrightarrow t'$

$$(\texttt{raise}\ v_{11})\ t_2 \longrightarrow \texttt{raise}\ v_{11} \quad \text{(E-AppRaise1)}$$

$$v_1\ (\texttt{raise}\ v_{21}) \longrightarrow \texttt{raise}\ v_{21} \quad \text{(E-AppRaise2)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{raise}\ t_1 \longrightarrow \texttt{raise}\ t_1'} \quad \text{(E-Raise)}$$

$$\texttt{raise}\ (\texttt{raise}\ v_{11}) \longrightarrow \texttt{raise}\ v_{11} \quad \text{(E-RaiseRaise)}$$

$$\texttt{try}\ v_1\ \texttt{with}\ t_2 \longrightarrow v_1 \quad \text{(E-TryV)}$$

$$\texttt{try raise}\ v_{11}\ \texttt{with}\ t_2 \longrightarrow t_2\ v_{11} \quad \text{(E-TryRaise)}$$

$$\frac{t_1 \longrightarrow t_1'}{\texttt{try}\ t_1\ \texttt{with}\ t_2 \longrightarrow \texttt{try}\ t_1'\ \texttt{with}\ t_2} \quad \text{(E-Try)}$$

New typing rules $\Gamma \vdash t : T$

$$\frac{\Gamma \vdash t_1 : T_{exn}}{\Gamma \vdash \texttt{raise}\ t_1 : T} \quad \text{(T-Exn)}$$

$$\frac{\Gamma \vdash t_1 : T \qquad \Gamma \vdash t_2 : T_{exn} \to T}{\Gamma \vdash \texttt{try}\ t_1\ \texttt{with}\ t_2 : T} \quad \text{(T-Try)}$$

Recapitulation

Raising exception is *more than an error mechanism*: it's a *programmable control structure*

- Sometimes a way to quickly *escape from the computation.*
- And allow programs to effect *non-local "jumps"* in the flow of control by setting a *handler* during evaluation of an expression that may be invoked by raising an exception.
- Exceptions are *value-carrying* in the sense that one may pass a value to *the exception handler* when the exception is raised.
- Exception values have a single type, T_{exn} , which is *shared by all exception handler*.

Recapitulation

As an example, exceptions are used in OCaml as a *control mechanism*, either to signal errors, or to control the flow of execution.

- When an exception is raised, the current execution is aborted, and control is thrown to the most recently entered active exception handler, which may choose to handle the exception, or pass it through to the next exception handler.
- T_{exn} is defined to be an extensible data type, in the sense that new constructors may be introduced using $\mathrm{exception}$ declaration, with no restriction on the types of value that may be associated with the constructor

HW for chap14

- Read through chap 14
- Do exercise 14.3.1