COMP4161
Advanced Topics in Software Verification

Gerwin Klein, June Andronick, Miki Tanaka, Johannes Åman Pohjola

T3/2022

Last time...

- λ calculus syntax
- free variables, sub
- β reduction
- α and η conversion
- β reduction is confluent
- λ calculus is expressive (Turing complete)
- λ calculus is inconsistent (as a logic)

Content

- Foundations & Principles
  - Intro, Lamb[illegible], natural deduction [1,2]
  - Higher Orde[illegible]r (part 1) [2,3[a]]
  - Term rewriti[illegible] [3,4]

- Proof & Specification Techniques
  - Inductively defined sets, rule induction [4,5]
  - Datatype induction, primitive recursion [5,7]
  - General recursive functions, termination proofs [7[b]]
  - Proof automation, Isar (part 2) [8]
  - Hoare logic, proofs about programs, invariants [8,9]
  - C verification [9,10]
  - Practice, questions, exam prep [10[c]]

[a] a1 due; [b] a2 due; [c] a3 due

λ calculus is inconsistent

Can find term R such that $R\ R \ =_\beta\ \texttt{not}(R\ R)$

There are more terms that do not make sense:

$1\ 2$, $\texttt{true}\ \texttt{false}$, etc.

Solution: rule out ill-formed terms by using types.

(Church 1940)

Introducing types

Idea: assign a type to each “sensible” λ term.

Examples:

- ➜ for *term t has type α* write $t :: \alpha$
- ➜ if x has type α then $\lambda x.\ x$ is a function from α to α
  Write: $(\lambda x.\ x) :: \alpha \Rightarrow \alpha$
- ➜ for $s\ t$ to be sensible:
  s must be a function
  t must be right type for parameter

  If $s :: \alpha \Rightarrow \beta$ and $t :: \alpha$ then $(s\ t) :: \beta$

That's about it

Now formally again

Syntax for $\lambda^{\rightarrow}$

Terms: $t ::= v \mid c \mid (t\ t) \mid (\lambda x.\ t)$

$v, x \in V, \quad c \in C, \quad V, C$ sets of names

Types: $\tau ::= b \mid \nu \mid \tau \Rightarrow \tau$

$\mathtt{b} \in \{\mathtt{bool}, \mathtt{int}, \ldots\}$ base types

$\nu \in \{\alpha, \beta, \ldots\}$ type variables

$$\alpha \Rightarrow \beta \Rightarrow \gamma \quad = \quad \alpha \Rightarrow (\beta \Rightarrow \gamma)$$

Context Γ:

Γ: function from variable and constant names to types.

Term t has type τ in context Γ: $\quad \Gamma \vdash t :: \tau$

Examples

$\Gamma \vdash (\lambda x.\ x) :: \alpha \Rightarrow \alpha$

$[y \leftarrow \texttt{int}] \vdash y :: \texttt{int}$

$[z \leftarrow \texttt{bool}] \vdash (\lambda y.\ y)\ z :: \texttt{bool}$

$[] \vdash \lambda f\ x.\ f\ x :: (\alpha \Rightarrow \beta) \Rightarrow \alpha \Rightarrow \beta$

A term t is **well typed** or **type correct** if there are Γ and τ such that $\Gamma \vdash t :: \tau$

Type Checking Rules

Variables:
$$\frac{}{\Gamma \vdash x :: \Gamma(x)}$$

Application:
$$\frac{\Gamma \vdash t_1 :: \tau_2 \Rightarrow \tau \quad \Gamma \vdash t_2 :: \tau_2}{\Gamma \vdash (t_1\ t_2) :: \tau}$$

Abstraction:
$$\frac{\Gamma[x \leftarrow \tau_x] \vdash t :: \tau}{\Gamma \vdash (\lambda x.\ t) :: \tau_x \Rightarrow \tau}$$

Example Type Derivation:

$$\cfrac{\cfrac{\cfrac{}{[x \leftarrow \alpha, y \leftarrow \beta] \vdash x :: \alpha}\ \mathit{Var}}{[x \leftarrow \alpha] \vdash \lambda y.\ x :: \beta \Rightarrow \alpha}\ \mathit{Abs}}{[] \vdash \lambda x\ y.\ x :: \alpha \Rightarrow \beta \Rightarrow \alpha}\ \mathit{Abs}$$

Remember:

$$\frac{}{\Gamma \vdash x :: \Gamma(x)}\ \mathit{Var} \qquad \frac{\Gamma \vdash t_1 :: \tau_2 \Rightarrow \tau \quad \Gamma \vdash t_2 :: \tau_2}{\Gamma \vdash (t_1\ t_2) :: \tau}\ \mathit{App} \qquad \frac{\Gamma[x \leftarrow \tau_x] \vdash t :: \tau}{\Gamma \vdash (\lambda x.\ t) :: \tau_x \Rightarrow \tau}\ \mathit{Ab}$$

More complex Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash f :: \alpha \Rightarrow (\alpha \Rightarrow \beta)} \qquad \dfrac{}{\Gamma \vdash x :: \alpha}\,\mathit{Var}}{\Gamma \vdash f\ x :: \alpha \Rightarrow \beta}\,\mathit{App} \qquad \dfrac{}{\Gamma \vdash x :: \alpha}\,\mathit{Var}}{\Gamma \vdash f\ x\ x :: \beta}\,\mathit{App}}{[f \leftarrow \alpha \Rightarrow \alpha \Rightarrow \beta] \vdash \lambda x.\ f\ x\ x :: \alpha \Rightarrow \beta}\,\mathit{Abs}}{[] \vdash \lambda f\ x.\ f\ x\ x :: (\alpha \Rightarrow \alpha \Rightarrow \beta) \Rightarrow \alpha \Rightarrow \beta}\,\mathit{Abs}$$

$$\Gamma = [f \leftarrow \alpha \Rightarrow \alpha \Rightarrow \beta, x \leftarrow \alpha]$$

Remember:

More general Types

A term can have more than one type.

Example: $[] \vdash \lambda x.\ x :: \texttt{bool} \Rightarrow \texttt{bool}$

$[] \vdash \lambda x.\ x :: \alpha \Rightarrow \alpha$

Some types are more general than others:

$\tau \lesssim \sigma$ if there is a substitution S such that $\tau = S(\sigma)$

Examples:

$$\texttt{int} \Rightarrow \texttt{bool} \quad \lesssim \quad \alpha \Rightarrow \beta \quad \lesssim \quad \beta \Rightarrow \alpha \quad \not\lesssim \quad \alpha \Rightarrow \alpha$$

Most general Types

Fact: each type correct term has a most general type

Formally:

$$\Gamma \vdash t :: \tau \quad \Longrightarrow \quad [illegible] :: \sigma \wedge (\forall \sigma'.\ \Gamma \vdash t :: \sigma' \Longrightarrow \sigma' \lesssim \sigma)$$

It can be found by executing the typing rules backwards.

- ➜ **type checking:** checking if $\Gamma \vdash t :: \tau$ for given Γ and τ
- ➜ **type inference:** computing Γ and τ such that $\Gamma \vdash t :: \tau$

Type checking and type inference on $\lambda^{\rightarrow}$ are decidable.

What about β reduction?

Definition: β reduction stays the same.

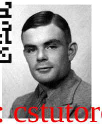
Fact: Well typed terms stay well typed during β reduction

Formally: $\Gamma \vdash s :: \tau \ \wedge \ s \longrightarrow_\beta t \Longrightarrow \Gamma \vdash t :: \tau$

This property is called **subject reduction**

What about termination?

β reduction in $\lambda^{\rightarrow}$ always terminates.



(Alan Turing, 1942)

- ➜ **$=_\beta$ is decidable**
  To decide if $s =_\beta t$, reduce s and t to normal form (always exists, because $\longrightarrow_\beta$ terminates), and compare result.
- ➜ **$=_{\alpha\beta\eta}$ is decidable**
  This is why Isabelle can automatically reduce each term to $\beta\eta$ normal form.

What does this mean for Expressiveness?

Checkpoint:

- ➜ untyped lambda c[illegible]uring complete (all computable fu[illegible]n be expressed)
- ➜ but it is inconsist[illegible]
- ➜ $\lambda^{\rightarrow}$ "fixes" the inconsistency problem by adding types
- ➜ Problem: it is not turing complete anymore!

Not all computable functions can be expressed in $\lambda^{\rightarrow}$!

(non terminating functions cannot be expressed)

But wait... typed functional languages are turing complete!

What does this mean for Expressiveness?

So...

- typed functional languages are turing complete
- but $\lambda^{\rightarrow}$ is not...
- How does this work?
- By adding one single constant, the Y operator (fix point operator), to $\lambda^{\rightarrow}$
- This introduces the non-termination that the types removed, but in a safe way that prevents inconsistency

$$Y :: (\tau \Rightarrow \tau) \Rightarrow \tau$$

$$Y\ t \longrightarrow_\beta t\ (Y\ t)$$

Fact: If we add Y to $\lambda^{\rightarrow}$ as the only constant, then each computable function can be encoded as closed, type correct $\lambda^{\rightarrow}$ term.

- Y is used for recursion
- lose decidability (what does $Y\ (\lambda x.\ x)$ reduce to?)

Types and Terms in Isabelle

Types: $\tau \;::=\; b \mid {'\nu} \mid {'\nu :: C} \mid \tau \Rightarrow \tau \mid (\tau, \ldots, \tau)\ K$

$b \in \{\texttt{bool}, \texttt{int}, \ldots\}$ base types

$\nu \in \{\alpha, \beta, \ldots\}$ type variables

$K \in \{\texttt{set}, \texttt{list}, \ldots\}$ type constructors

$C \in \{\texttt{order}, \texttt{linord}, \ldots\}$ type classes

Terms: $t \;::=\; v \mid c \mid ?v \mid (t\ t) \mid (\lambda x.\ t)$

$v, x \in V$, $\;c \in C$, $\;V, C$ sets of names

- ➜ **type constructors**: construct a new type out of a parameter type. Example: `int list`
- ➜ **type classes**: restrict type variables to a class defined by axioms. Example: $\alpha :: \mathit{order}$
- ➜ **schematic variables**: variables that can be instantiated.

Type Classes

➜ similar to Haskell's type classes, but with semantic properties

class order =
  assumes order_refl: "$x \le x$"
  assumes order_trans: "$[\![x \le y; y \le z]\!] \Longrightarrow x \le z$"
  ...

➜ theorems can be proved in the abstract

lemma order_less_trans:
"$\bigwedge x :: 'a :: order.\ [\![x < y; y < z]\!] \Longrightarrow x < z$"

➜ can be used for subtyping

class linorder = order +
  assumes linorder_linear: "$x \le y \vee y \le x$"

➜ can be instantiated

instance nat :: "{order, linorder}" **by** ...

Schematic Variables

$$\frac{X \quad Y}{X \wedge Y}$$

- ➜ X and Y must be **instantiated** to apply the rule

But: **lemma** "$x + 0 = 0 + x$"

- ➜ x is free
- ➜ convention: lemma must be true for all x
- ➜ **during the proof**, x must **not** be instantiated

Solution:

Isabelle has **free** (x), **bound** (x), and **schematic** (?X) variables.

Only schematic variables can be instantiated.

Free converted into schematic after proof is finished.

Higher Order Unification

Unification:
Find substitution σ on variables for terms s, t such that
$\sigma(s) = \sigma(t)$

In Isabelle:

Find substitution σ on schematic variables such that
$\sigma(s) =_{\alpha\beta\eta} \sigma(t)$

Examples:

$$
\begin{array}{lll}
?X \wedge ?Y & =_{\alpha\beta\eta} \; x \wedge x & [?X \leftarrow x, ?Y \leftarrow x] \\
?P\ x & =_{\alpha\beta\eta} \; x \wedge x & [?P \leftarrow \lambda x.\ x \wedge x] \\
P\ (?f\ x) & =_{\alpha\beta\eta} \; ?Y\ x & [?f \leftarrow \lambda x.\ x, ?Y \leftarrow P]
\end{array}
$$

Higher Order: schematic variables can be functions.

Higher Order Unification

- Unification modulo β (Higher Order Unification) is semi-decidable
- Unification modul[illegible]ndecidable
- Higher Order Uni[illegible]s possibly infinitely many solutions

But:

- Most cases are well-behaved
- Important fragments (like Higher Order Patterns) are decidable

Higher Order Pattern:

- is a term in β normal form where
- each occurrence of a schematic variable is of the form $?f\ t_1\ \dots\ t_n$
- and the $t_1\ \dots\ t_n$ are η-convertible into n distinct bound variables

We have learned so far...

- Simply typed lam… s: $\lambda^{\to}$
- Typing rules for λ… riables, type contexts
- β-reduction in λ^{-}… subject reduction
- β-reduction in $\lambda^{\to}$ always terminates
- Types and terms in Isabelle