Proofcraft

UNSW SYDNEY

MP4161

Advanced Topics in Software Verification

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

T3/2022

Last time...

- ➜ λ calculus syntax
- ➜ free variables, substitution
- ➜ 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, Lambda [illegible]atural deduction [1,2]
  - Higher Order [illegible]part 1) [2,3[a]]
  - Term rewriting[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 $=_\beta$ `not`(R R)

There are more terms t make sense:

`1 2`, `true false`, etc.

λ calculus is inconsistent

Can find term R such that $R\ R =_\beta$ `not`$(R\ R)$

There are more terms that do not make sense:

`1 2`, `true 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:

Introducing types

Idea: assign a type to each "sensible" λ term.

Examples:

➜ for *term t has ty* $t :: \alpha$

Introducing types

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

Examples:

- for *term t has ty* $t :: \alpha$
- if x has type α then s a function from α to α
  Write: $(\lambda x.\ x) :: \alpha \Rightarrow \alpha$

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

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

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

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

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

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

Syntax for $\lambda^{\rightarrow}$

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

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

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

$b \in \{\texttt{bool}, \texttt{int}, \ldots\}$ 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.

Syntax for $\lambda^{\rightarrow}$

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

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

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

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

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

Examples

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

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

Examples

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

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

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

Examples

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

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

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

$[] \vdash \lambda f\ x.\ f\ x ::$

Examples

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

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

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

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

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

Type Checking Rules

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

Application: $$\frac{}{\Gamma \vdash (t_1 \;\; t_2) :: \tau}$$

Type Checking Rules

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

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

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

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:

$$\frac{}{[] \vdash \lambda x\ y.\ x ::}\ Abs$$

Remember:

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

Example Type Derivation:

$$\dfrac{\dfrac{}{[x \leftarrow \alpha] \vdash \lambda y.\ x ::}\ \mathit{Abs}}{[] \vdash \lambda x\ y.\ x :: \alpha \Rightarrow}\ \mathit{Abs}$$

Remember:

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

Example Type Derivation:

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

Remember:

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

Example Type Derivation:

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

Remember:

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

More complex Example

$$\frac{}{[] \vdash \lambda f\ x.\ f\ x\ x ::}\ \mathit{Abs}$$

Remember:

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

More complex Example

$$\frac{}{[] \vdash \lambda f\ x.\ f\ x\ x :: (\alpha \Rightarrow \alpha \Rightarrow \beta) \Rightarrow \alpha \Rightarrow \beta}\ \mathit{Abs}$$

Remember:

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

More complex Example

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

Remember:

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

More complex Example

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

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

Remember:

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

More complex Example

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash f\ \ldots}\ \textit{App}}{\Gamma \vdash f\ x\ x :: \beta}\ \textit{App}}{[f \leftarrow \alpha \Rightarrow \alpha \Rightarrow \beta] \vdash \lambda x.\ f\ x\ x :: \alpha \Rightarrow \beta}\ \textit{Abs}}{[] \vdash \lambda f\ x.\ f\ x\ x :: (\alpha \Rightarrow \alpha \Rightarrow \beta) \Rightarrow \alpha \Rightarrow \beta}\ \textit{Abs}$$

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

Remember:

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

More complex Example

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

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

Remember:

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

More complex Example

$$\cfrac{\cfrac{\cfrac{}{\Gamma \vdash f :: \alpha \Rightarrow (\alpha \ldots} \quad \ldots}{\Gamma \vdash f \ldots}\,App \qquad \cfrac{}{\Gamma \vdash x :: \alpha}\,Var}{\Gamma \vdash f\ x\ x :: \beta}\,App$$

$$\cfrac{\cfrac{\Gamma \vdash f\ x\ x :: \beta}{[f \leftarrow \alpha \Rightarrow \alpha \Rightarrow \beta] \vdash \lambda x.\ f\ x\ x :: \alpha \Rightarrow \beta}\,Abs}{[] \vdash \lambda f\ x.\ f\ x\ x :: (\alpha \Rightarrow \alpha \Rightarrow \beta) \Rightarrow \alpha \Rightarrow \beta}\,Abs$$

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

Remember:

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

More complex Example

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

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

Remember:

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

More general Types

A ter … e more than one type.

More general Types

A ter[illegible]e more than one type.

Example: $[] \vdash \lambda$[illegible]l $\Rightarrow$ `bool`
$[] \vdash \lambda x.\ x :: \alpha \Rightarrow \alpha$

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 $\tau = S(\sigma)$

More general Types

A ter[illegible]e more than one type.

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

Some types are more general than others:

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

Examples:

$\texttt{int} \Rightarrow \texttt{bool} \quad \lesssim \quad \alpha \Rightarrow \beta$

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:

$\texttt{int} \Rightarrow \texttt{bool} \quad \lesssim \quad \alpha \Rightarrow \beta \quad \lesssim \quad \beta \Rightarrow \alpha$

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

Most general Types

Fact: each type correct term has a most general type

Formally:

$$\Gamma \vdash t :: \tau \quad \Longrightarrow \quad \exists\sigma \ldots \wedge (\forall \sigma'.\ \Gamma \vdash t :: \sigma' \Longrightarrow \sigma' \lesssim \sigma)$$

Most general Types

Fact: each type correct term has a most general type

Formally:

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

It can be found by executing the typing rules backwards.

Most general Types

Fact: each type correct term has a most general type

Formally:

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

It can be found by executing the typing rules backwards.

➜ **type checking:** checking if $\Gamma \vdash t :: \tau$ for given Γ and τ

Most general Types

Fact: each type correct term has a most general type

Formally:

$$\Gamma \vdash t :: \tau \quad \Longrightarrow \quad \exists \ldots \wedge (\forall \sigma'.\ \Gamma \vdash t :: \sigma' \Longrightarrow \sigma' \lesssim \sigma)$$

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 $\Gamma \vdash t :: \tau$

Most general Types

Fact: each type correct term has a most general type

Formally:

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

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?

What about β reduction?

Definiti[illegible]duction stays the same.

What about β reduction?

Definition of β reduction stays the same.

Fact: Well typed terms stay well typed during β reduction

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

What about β reduction?

Definiti[illegible]duction stays the same.

Fact: Well typed terms stay well typed during β reduction

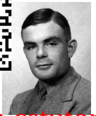
Formally: $\Gamma \vdash s :: \tau \ \wedge \ s \longrightarrow_\beta t \Longrightarrow \Gamma \vdash t :: \tau$

This property is called **subject reduction**

What about termination?

What about termination?

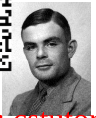
β redu[illegible] $\lambda^{\to}$ always terminates.



(Alan Turing, 1942)

What about termination?

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

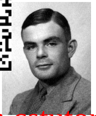


(Alan Turing, 1942)

➜ **$=_\beta$ is decidable**
To decide if $s =_\beta t$, reduce s and t to normal form (always exists, because $\longrightarrow_\beta$ terminates), and compare result.

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?

What does this mean for Expressiveness?

Checkpoint:

- ➜ untyped lambda calculus is turing complete (all computable functions can be expressed)
- ➜ but it is inconsistent
- ➜ $\lambda^{\rightarrow}$ "fixes" the inconsistency problem by adding types
- ➜ Problem: it is not turing complete anymore!

What does this mean for Expressiveness?

Checkpoint:

- ➜ untyped lambda calculus is turing complete
  (all computable functions can be expressed)
- ➜ but it is inconsistent
- ➜ $\lambda^{\rightarrow}$ "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)

What does this mean for Expressiveness?

Checkpoint:

- ➜ untyped lambda calculus is turing complete
  (all computable functions can be expressed)
- ➜ but it is inconsistent
- ➜ $\lambda^{\rightarrow}$ "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...

What does this mean for Expressiveness?

Checkpoint:

- ➜ untyped lambda cal… ng complete
  (all computable fun… e expressed)
- ➜ but it is inconsisten…
- ➜ $\lambda^{\to}$ "fixes" the inconsistency problem by adding types
- ➜ Problem: it is not turing complete anymore!

Not all computable functions can be expressed in $\lambda^{\to}$!
(non terminating functions cannot be expressed)

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

What does this mean for Expressiveness?

So...

- ➜ typed functional lan[illegible] turing complete
- ➜ but $\lambda^{\rightarrow}$ is not...
- ➜ How does this work

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

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

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

What does this mean for Expressiveness?

So...

- ➜ typed functional lan… 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?)
- ➜ (Isabelle/HOL doesn't have Y; recursion is more restricted)

Types and Terms in Isabelle

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

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

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

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

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

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

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

Types and Terms in Isabelle

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

$\mathtt{b} \in \{\mathtt{bool},$ [illegible] base types

$\nu \in \{\alpha, \beta,$ [illegible] variables

$K \in \{\mathtt{set},$ [illegible] type constructors

$C \in \{\mathtt{order}, \mathtt{linord}, \dots\}$ type classes

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

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

➜ **type constructors**: construct a new type out of a parameter type.
Example: `int list`

Types and Terms in Isabelle

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

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

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

$K \in \{\mathtt{set}, \ldots$ type constructors

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

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

$v, x \in V, \quad c \in C, \quad V, C$ 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: $\alpha :: order$

Types and Terms in Isabelle

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

$\mathsf{b} \in \{\texttt{bool},$ [illegible] base types

$\nu \in \{\alpha, \beta,$ [illegible] variables

$K \in \{\texttt{set},$ [illegible] type constructors

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

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

$v, x \in V, \quad c \in C, \quad V, C$ 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 , but with semantic properties

class order =

  assumes order_r

  assumes order_t $y; y \leq z\rrbracket \Longrightarrow x \leq z$"

  ...

Type Classes

➜ similar to Haskell's ..., but with semantic properties

class order =
  assumes order_r...
  assumes order_t... $y; y \le z] \Longrightarrow x \le z$"
  ...

➜ theorems can be proved in the abstract

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

Type Classes

- similar to Haskell's , but with semantic properties

  class order =
  assumes order_r
  assumes order_t $y; y \le z\rrbracket \Longrightarrow x \le z$"
  ...

- theorems can be proved in the abstract

  lemma order_less_trans: " $\bigwedge x ::' a :: order.\ \llbracket x < y; y < z \rrbracket \Longrightarrow x < z$"

- can be used for subtyping

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

Type Classes

- similar to Haskell's ... , but with semantic properties

  class order =

  assumes order_r...

  assumes order_t... $y; y \leq z \rrbracket \Longrightarrow x \leq z$"

  ...

- theorems can be proved in the abstract

  lemma order_less_trans: " $\bigwedge x ::' a :: order.\ \llbracket x < y; y < z \rrbracket \Longrightarrow x < z$"

- can be used for subtyping

  class linorder = order +

  assumes linorder_linear: " $x \leq y \vee y \leq x$"

- can be instantiated

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

Schematic Variables

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

- ➜ X and Y must be i[illegible] to apply the rule

Schematic Variables

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

- X and Y must be i[illegible] 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

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 or terms s, t such that $\sigma(s) = \sigma(t)$

Higher Order Unification

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

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

Higher Order Unification

Unification:
Find substitution σ on [illegible]or 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:

$$
\begin{array}{lll}
?X \wedge ?Y & =_{\alpha\beta\eta} & x \wedge x \\
?P\ x & =_{\alpha\beta\eta} & x \wedge x \\
P\ (?f\ x) & =_{\alpha\beta\eta} & ?Y\ x
\end{array}
$$

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:

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

Higher Order: schematic variables can be functions.

Higher Order Unification

➜ Unification modulo [illegible] Order Unification) is semi-decidable

Higher Order Unification

- ➜ Unification modulo [illegible] Order Unification) is semi-decidable
- ➜ Unification modulo [illegible]ecidable

Higher Order Unification

- Unification modulo … Order Unification) is semi-decidable
- Unification modulo … ecidable
- Higher Order Unific… ossibly infinitely many solutions

Higher Order Unification

➜ Unification modulo ... Order Unification) is semi-decidable

➜ Unification modulo ... ecidable

➜ Higher Order Unific... ossibly infinitely many solutions

But:

➜ Most cases are well-behaved

Higher Order Unification

- Unification modulo $\alpha\beta$ (Higher Order Unification) is semi-decidable
- Unification modulo $\alpha\beta\eta$ is semi-decidable
- Higher Order Unification has possibly infinitely many solutions

But:

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

Higher Order Unification

➜ Unification modulo β (Hi[illegible] Order Unification) is semi-decidable

➜ Unification modulo [illegible]ecidable

➜ Higher Order Unific[illegible]ossibly 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 lambd $\lambda^{\rightarrow}$

We have learned so far...

- Simply typed lamb [illegible] $\lambda^{\rightarrow}$
- Typing rules for $\lambda^{\rightarrow}$ [illegible] bles, type contexts

We have learned so far...

- Simply typed lambd $\lambda^{\to}$
- Typing rules for $\lambda^{\to}$ bles, type contexts
- β-reduction in $\lambda^{\to}$ ject reduction

We have learned so far...

- Simply typed lambda calculus: $\lambda^{\rightarrow}$
- Typing rules for $\lambda^{\rightarrow}$, type variables, type contexts
- β-reduction in $\lambda^{\rightarrow}$ satisfies subject reduction
- β-reduction in $\lambda^{\rightarrow}$ always terminates

We have learned so far...

- Simply typed lambda calculus: $\lambda^{\rightarrow}$
- Typing rules for $\lambda^{\rightarrow}$, type variables, type contexts
- β-reduction in $\lambda^{\rightarrow}$ satisfies subject reduction
- β-reduction in $\lambda^{\rightarrow}$ always terminates
- Types and terms in Isabelle