System F

Alexandre Miquel — PPS & U. Paris 7

Alexandre.Miquel@pps.jussieu.fr

Types Summer School 2005

August 15–26 — Göteborg

Introduction

- **System F:** independently discovered by

Girard:	System F	(1970)
Reynolds:	The polymorphic λ-calculus	(1974)

- Quite different motivations...

Girard:	Interpretation of second-order logic
Reynolds:	Functional programming

... connected by the Curry-Howard isomorphism

- Significant influence on the development of Type Theory

– Interpretation of higher-order logic	[Girard, Martin-Löf]
– Type:Type	[Martin-Löf 1971]
– Martin-Löf Type Theory	[1972, 1984, 1990, ...]
– The Calculus of Constructions	[Coquand 1984]

Part I

System F: Church-style presentation

System F syntax

Definition

Types	A, B	$::=$	$\alpha \mid A \rightarrow B \mid \forall\alpha\, B$
Terms	t, u	$::=$	x
			$\mid\ \lambda x : A \,.\, t \mid tu$ (term abstr./app.)
			$\mid\ \Lambda\alpha \,.\, t \mid tA$ (type abstr./app.)

Notations

- Set of free (term) variables: $FV(t)$
- Set of free type variables: $TV(t)$, $TV(A)$
- Term substitution: $u\{x := t\}$
- Type substitution: $u\{\alpha := A\}$, $B\{\alpha := A\}$

Perform α-conversion to prevent captures of free (term/type) variables!

System F typing rules

Contexts $\Gamma ::= x_1 : A_1, \ \ldots, \ x_n : A_n$

Typing judgments $\Gamma \vdash t : A$

$$\frac{}{\Gamma \vdash x : A}\ {\scriptstyle (x:A)\in\Gamma}$$

$$\frac{\Gamma, \ x : A \vdash t : B}{\Gamma \vdash \lambda x : A \,.\, t : A \to B} \qquad \frac{\Gamma \vdash t : A \to B \qquad \Gamma \vdash u : A}{\Gamma \vdash tu : B}$$

$$\frac{\Gamma \vdash t : B}{\Gamma \vdash \Lambda\alpha \,.\, t : \forall\alpha\ B}\ {\scriptstyle \alpha \notin TV(\Gamma)} \qquad \frac{\Gamma \vdash t : \forall\alpha\ B}{\Gamma \vdash tA : B\{\alpha := A\}}$$

- Declaration of type variables is implicit (for each $\alpha \in TV(\Gamma)$)
- Type variables could be declared explicitly: $\alpha : *$ (cf PTS)
- One rule for each syntactic construct $\Rightarrow$ System is syntax-directed

Example: the polymorphic identity

- Set: $\quad \mathrm{id} \equiv \Lambda\alpha\,.\,\lambda x : \alpha\,.\,x$

- One has:

$$
\begin{array}{lcll}
\mathrm{id} & : & \forall\alpha\,(\alpha \to \alpha) & \\
\mathrm{id}\,B & : & B \to B & \text{for any type } B \\
\mathrm{id}\,B\,u & : & B & \text{for any term } u : B
\end{array}
$$

- In particular, if we take $\quad B \equiv \forall\alpha\,(\alpha \to \alpha) \quad$ and $\quad u \equiv \mathrm{id}$

$$
\begin{array}{lcl}
\mathrm{id}\,(\forall\alpha\,(\alpha \to \alpha)) & : & \forall\alpha\,(\alpha \to \alpha) \;\to\; \forall\alpha\,(\alpha \to \alpha) \\
\mathrm{id}\,(\forall\alpha\,(\alpha \to \alpha))\,\mathrm{id} & : & \forall\alpha\,(\alpha \to \alpha)
\end{array}
$$

$\Rightarrow$ Type system is impredicative (or cyclic)

Properties

Substitutivity (for types/terms):

- $\Gamma \vdash u : B \quad \Rightarrow \quad \Gamma\{\alpha := A\} \vdash u\{\alpha := A\} : B\{\alpha := A\}$
- $\Gamma, x : A \vdash u : B, \quad \Gamma \vdash t : A \quad \Rightarrow \quad \Gamma \vdash u\{x := t\} : B$

Uniqueness of type

$\Gamma \vdash t : A, \quad \Gamma \vdash t : A' \quad \Rightarrow \quad A = A' \quad (\alpha\text{-conv.})$

Decidability of type checking / type inference

1. Given Γ, t and A, decide whether $\Gamma \vdash t : A$ is derivable
2. Given Γ and t, compute a type A such that $\Gamma \vdash t : A$ if such a type exists, or fail otherwise.

Both problems are decidable

Reduction rules

Two kinds of redexes:

$$(\lambda x : A \,.\, t)u \;\succ\; t\{x := u\} \qquad \text{1st kind redex}$$

$$(\Lambda\alpha \,.\, t)A \;\succ\; t\{\alpha := A\} \qquad \text{2nd kind redex}$$

Other combinations of abstraction and application are meaningless (and rejected by typing)

Definitions

- One step β-reduction $t \succ t'$ $\equiv$
  contextual closure of both rules above
- β-reduction $t \succ^* t'$ $\equiv$
  reflexive-transitive closure of $\succ$
- β-convertibility $t \simeq t'$ $\equiv$
  reflexive-symmetric-transitive closure of $\succ$

Examples

- **The polymorphic identity, again**

$$\text{id}\ B\ u \quad \equiv \quad (\Lambda\alpha\,.\,\lambda x:\alpha\,.\,x)\ B\ u \quad \succ \quad (\lambda x:B\,.\,x)\ u \quad \succ \quad u$$

$$\text{id}\ (\forall\alpha\ (\alpha\to\alpha))\ \text{id}\ (\forall\alpha\ (\alpha\to\alpha))\ \cdots\ \text{id}\ (\forall\alpha\ (\alpha\to\alpha))\ \text{id}\, B\, u \quad \succ^* \quad u$$

- **A little bit more complex example...**

$$\begin{array}{l}\big(\Lambda\alpha\,.\,\lambda x:\alpha\,.\,\lambda f:\alpha\to\alpha\,.\,\overbrace{f\ (\cdots\ (f}^{32\ \text{times}}\ x)\cdots)\big)\\ \quad\big(\forall\alpha\ (\alpha\to(\alpha\to\alpha)\to\alpha)\big)\ \big(\Lambda\alpha\,.\,\lambda x:\alpha\,.\,\lambda f:\alpha\to\alpha\,.\,f\ x\big)\\ \quad\big(\lambda n:\forall\alpha\ (\alpha\to(\alpha\to\alpha)\to\alpha)\,.\,\Lambda\alpha\,.\,\lambda x:\alpha\,.\,\lambda f:\alpha\to\alpha\,.\,n\,\alpha\,(n\,\alpha\,x\,f)\,f\big)\end{array}$$

$$\succ^* \quad \Lambda\alpha\,.\,\lambda x:\alpha\,.\,\lambda f:\alpha\to\alpha\,.\,\underbrace{(f\ \cdots\ (f}_{4\,294\,967\,296\ \text{times}}\ x)\cdots)$$

Properties

Confluence

$$t \succ^* t_1 \;\wedge\; t \succ^* t_2 \quad \Rightarrow \quad \exists t' \, (t_1 \succ^* t' \;\wedge\; t_2 \succ^* t')$$

Proof. Roughly the same as for the untyped λ-calculus (adaptation is easy)

Church-Rosser

$$t_1 \simeq t_2 \quad \Leftrightarrow \quad \exists t' \, (t_1 \succ^* t' \;\wedge\; t_2 \succ^* t')$$

Subject-reduction

If $\Gamma \vdash t : A$ and $t \succ^* t'$ then $\Gamma \vdash t' : A$

Proof. By induction on the derivation of $\Gamma \vdash t : A$, with $t \succ t'$ (one step reduction)

Strong normalisation

All well-typed terms of system F are strongly normalisable

Proof. Girard and Tait's method of reducibility candidates (postponed)

Part II

Encoding data types

Booleans (1/3)

Encoding of booleans

$$\mathsf{Bool} \equiv \forall\gamma\,(\gamma \to \gamma \to \gamma)$$

$$\begin{array}{lcl} \mathsf{true} & \equiv & \Lambda\gamma\,.\,\lambda x, y : \gamma\,.\,x \quad : \quad \mathsf{Bool} \\ \mathsf{false} & \equiv & \Lambda\gamma\,.\,\lambda x, y : \gamma\,.\,y \quad : \quad \mathsf{Bool} \end{array}$$

$$\mathtt{if}_A\ u\ \mathtt{then}\ t_1\ \mathtt{else}\ t_2 \equiv u\ A\ t_1\ t_2$$

Correctness w.r.t. typing

$$\frac{\Gamma \vdash u : \mathsf{Bool} \qquad \Gamma \vdash t_1 : A \qquad \Gamma \vdash t_2 : A}{\Gamma \vdash \mathtt{if}_A\ u\ \mathtt{then}\ t_1\ \mathtt{else}\ t_2 : A}$$

Correctness w.r.t. reduction

$$\begin{array}{lcl} \mathtt{if}_A\ \mathsf{true}\ \mathtt{then}\ t_1\ \mathtt{else}\ t_2 & \succ^* & t_1 \\ \mathtt{if}_A\ \mathsf{false}\ \mathtt{then}\ t_1\ \mathtt{else}\ t_2 & \succ^* & t_2 \end{array}$$

Booleans (2/3)

Objection: We can do the same in the untyped λ-calculus!

$$\left.\begin{array}{lcl} \text{true} & \equiv & \lambda x, y \,.\, x \\ \text{false} & \equiv & \lambda x, y \,.\, y \\ \texttt{if}\ u\ \texttt{then}\ t_1\ \texttt{else}\ t_2 & \equiv & u\ t_1\ t_2 \end{array}\right\} \quad \text{Same reduction rules as before}$$

But nothing prevents the following computation:

$$\texttt{if}\ \underbrace{\lambda x \,.\, x}_{\text{bad bool}}\ \texttt{then}\ t_1\ \texttt{else}\ t_2 \ \equiv\ (\lambda x \,.\, x)\ t_1\ t_2 \ \succ\ \underbrace{t_1\, t_2}_{\text{meaningless result}}$$

Question: Does the type discipline of system F avoid this?

Booleans (3/3)

Principle (that should be satisfied by any functional programming language)

When a program P of type A evaluates to a value v, then v has one of the canonical forms expected by the type A.

In ML/Haskell, a value produced by a program of type `Bool` will always be `true` or `false` (i.e. the canonical forms of type `bool`).

In system F: Subject-reduction ensures that the normal form of a term of type Bool is a term of type Bool.

To conclude, it suffices to check that in system F:

Lemma (Canonical forms of type bool)

The terms $\text{true} \equiv \Lambda\gamma\,.\,\lambda x, y : \gamma\,.\,x$ and $\text{false} \equiv \Lambda\gamma\,.\,\lambda x, y : \gamma\,.\,y$ are the only closed normal terms of type $\text{Bool} \equiv \forall\gamma\ (\gamma\to\gamma\to\gamma)$

Proof. Case analysis on the derivation.

Cartesian product

Encoding of the cartesian product $A \times B$

$$\begin{aligned}
A \times B &\equiv \forall\gamma\ ((A{\rightarrow}B{\rightarrow}\gamma) \rightarrow \gamma) \\
\langle t_1, t_2\rangle &\equiv \Lambda\gamma\,.\,\lambda f : A \rightarrow B \rightarrow \gamma\,.\, f\ \ t_1\ \ t_2 \\
\mathrm{fst} &\equiv \lambda p : A \times B\,.\, p\ A\ (\lambda x : A\,.\,\lambda y : B\,.\,x) \quad : \quad A \times B \rightarrow A \\
\mathrm{snd} &\equiv \lambda p : A \times B\,.\, p\ B\ (\lambda x : A\,.\,\lambda y : B\,.\,y) \quad : \quad A \times B \rightarrow B
\end{aligned}$$

Correctness w.r.t. typing and reduction

$$\frac{\Gamma \vdash t_1 : A \qquad \Gamma \vdash t_2 : B}{\Gamma \vdash \langle t_1, t_2\rangle : A \times B}$$

$$\begin{aligned}
\mathrm{fst}\ \langle t_1, t_2\rangle &\succ^* t_1 \\
\mathrm{snd}\ \langle t_1, t_2\rangle &\succ^* t_2
\end{aligned}$$

Lemma (Canonical forms of type $A \times B$)

The closed normal terms of type $A \times B$ are of the form $\langle t_1, t_2\rangle$, where t_1 and t_2 are closed normal terms of type A and B, respectively.

Disjoint union

Encoding of the disjoint union $A + B$

$$A + B \equiv \forall\gamma\ ((A \to \gamma) \to (B \to \gamma) \to \gamma)$$

$$\mathsf{inl}(v) \equiv \Lambda\gamma\,.\,\lambda f : A \to \gamma\,.\,\lambda g : B \to \gamma\,.\,f\ v \quad : \quad A + B \qquad (\text{with } v : A)$$

$$\mathsf{inr}(v) \equiv \Lambda\gamma\,.\,\lambda f : A \to \gamma\,.\,\lambda g : B \to \gamma\,.\,g\ v \quad : \quad A + B \qquad (\text{with } v : B)$$

$$\mathsf{case}_C\ u\ \mathsf{of}\ \ \mathsf{inl}(x) \mapsto t_1 \ \mid\ \mathsf{inr}(y) \mapsto t_2 \ \equiv\ u\ C\ (\lambda x : A\,.\,t_1)\ (\lambda y : B\,.\,t_2)$$

Correctness w.r.t. typing and reduction

$$\frac{\Gamma \vdash u : A + B \qquad \Gamma,\ x : A \vdash t_1 : C \qquad \Gamma,\ y : B \vdash t_2 : C}{\Gamma \vdash \mathsf{case}_C\ u\ \mathsf{of}\ \ \mathsf{inl}(x) \mapsto t_1 \ \mid\ \mathsf{inr}(y) \mapsto t_2 : C}$$

$$\mathsf{case}_C\ \mathsf{inl}(v)\ \mathsf{of}\ \ \mathsf{inl}(x) \mapsto t_1 \ \mid\ \mathsf{inr}(y) \mapsto t_2 \ \succ^*\ t_1\{x := v\}$$

$$\mathsf{case}_C\ \mathsf{inr}(v)\ \mathsf{of}\ \ \mathsf{inl}(x) \mapsto t_1 \ \mid\ \mathsf{inr}(y) \mapsto t_2 \ \succ^*\ t_2\{y := v\}$$

+ Canonical forms of type $A + B$ (works as expected modulo η)

Finite types

Encoding of Fin_n $(n \geq 0)$

$$\mathsf{Fin}_n \equiv \forall\gamma\,(\underbrace{\gamma \to \cdots \to \gamma}_{n \text{ times}} \to \gamma)$$

$$\mathbf{e}_i \equiv \Lambda\gamma\,.\,\lambda x_1 : \gamma \ldots \lambda x_n : \gamma\,.\,x_i \quad : \quad \mathsf{Fin}_n \qquad (1 \leq i \leq n)$$

Again, $\mathbf{e}_1, \ldots, \mathbf{e}_n$ are the only closed normal terms of type Fin_n.

In particular:

Fin_2	$\equiv$	$\forall\gamma\,(\gamma \to \gamma \to \gamma)$	$\equiv$	Bool	(type of booleans)
Fin_1	$\equiv$	$\forall\gamma\,(\gamma \to \gamma)$	$\equiv$	Unit	(unit data-type)
Fin_0	$\equiv$	$\forall\gamma\;\gamma$	$\equiv$	$\bot$	(empty data-type)

(Notice that there is no closed normal term of type $\bot$.)

Natural numbers

Encoding of the type of Church numerals

$$
\begin{array}{lcl}
\mathsf{Nat} & \equiv & \forall\gamma\ (\gamma \to (\gamma \to \gamma) \to \gamma) \\
\\
\overline{0} & \equiv & \Lambda\gamma\,.\,\lambda x:\gamma\,.\,\lambda f:\gamma{\to}\gamma\,.\,x \\
\overline{1} & \equiv & \Lambda\gamma\,.\,\lambda x:\gamma\,.\,\lambda f:\gamma{\to}\gamma\,.\,f\ \ x \\
\overline{2} & \equiv & \Lambda\gamma\,.\,\lambda x:\gamma\,.\,\lambda f:\gamma{\to}\gamma\,.\,f\ \ (f\ \ x) \\
 & \vdots & \\
\overline{n} & \equiv & \Lambda\gamma\,.\,\lambda x:\gamma\,.\,\lambda f:\gamma{\to}\gamma\,.\,\underbrace{f(\cdots(f}_{n\ \text{times}}\,x)\cdots) \quad : \quad \mathsf{Nat} \\
 & \vdots &
\end{array}
$$

Lemma (Canonical forms of type Nat)

The terms $\overline{0}, \overline{1}, \overline{2}, \ldots$ are the only closed normal terms of type Nat.

Computing with natural numbers (1/2)

Intuition: Church numeral $\overline{n}$ acts as an iterator:

$$\overline{n}\ A\ f\ x \quad \succ^* \quad \underbrace{f\ (\cdots (f}_{n}\ \ x) \cdots) \qquad\qquad (f : A \to A, \quad x : A)$$

- Successor

$$\mathsf{succ} \quad \equiv \quad \lambda n : \mathsf{Nat} \,.\, \Lambda\gamma \,.\, \lambda x : \gamma \,.\, \lambda f : \gamma{\to}\gamma \,.\, f\ (n\ \gamma\ x\ f)$$

- Addition

$$\begin{aligned} \mathsf{plus} \quad &\equiv \quad \lambda n, m : \mathsf{Nat} \,.\, \Lambda\gamma \,.\, \lambda x : \gamma \,.\, \lambda f : \gamma{\to}\gamma \,.\, m\ \gamma\ (n\ \gamma\ x\ f)\ f \\ \mathsf{plus}' \quad &\equiv \quad \lambda n, m : \mathsf{Nat} \,.\, m\ \mathsf{Nat}\ n\ \mathsf{succ} \end{aligned}$$

- Multiplication

$$\begin{aligned} \mathsf{mult} \quad &\equiv \quad \lambda n, m : \mathsf{Nat} \,.\, \Lambda\gamma \,.\, \lambda x : \gamma \,.\, \lambda f : \gamma{\to}\gamma \,.\, n\ \gamma\ x\ (\lambda y : \gamma \,.\, m\ \gamma\ y\ f) \\ \mathsf{mult}' \quad &\equiv \quad \lambda n, m : \mathsf{Nat} \,.\, n\ \mathsf{Nat}\ \overline{0}\ (\mathsf{plus}\ \ m) \end{aligned}$$

Computing with natural numbers (2/2)

- Predecessor function $\text{pred} : \text{Nat} \to \text{Nat}$

$$\begin{array}{lcl} \text{pred } \overline{0} & \simeq & \overline{0} \\ \text{pred } (\overline{n+1}) & \simeq & \overline{n} \end{array}$$

$$\begin{array}{lcll} \text{fst} & \equiv & \lambda p : \text{Nat}\times\text{Nat} \,.\, p \text{ Nat } (\lambda x, y : \text{Nat} \,.\, x) & : \quad \text{Nat}\times\text{Nat} \to \text{Nat} \\ \text{snd} & \equiv & \lambda p : \text{Nat}\times\text{Nat} \,.\, p \text{ Nat } (\lambda x, y : \text{Nat} \,.\, y) & : \quad \text{Nat}\times\text{Nat} \to \text{Nat} \\ \text{step} & \equiv & \lambda p : \text{Nat}\times\text{Nat} \,.\, \langle \text{snd } p, \ \text{succ } (\text{snd } p) \rangle & : \quad \text{Nat}\times\text{Nat} \to \text{Nat}\times\text{Nat} \\ \text{pred} & \equiv & \lambda n : \text{Nat} \,.\, \text{fst } (n \text{ (Nat}\times\text{Nat) } \langle \overline{0}, \overline{0} \rangle \text{ step}) & : \quad \text{Nat} \to \text{Nat} \end{array}$$

- Ackerman function $\text{ack} : \text{Nat} \to \text{Nat} \to \text{Nat}$

$$\begin{array}{llllll} \text{ack} & \overline{0} & \overline{m} & \simeq & \overline{m+1} \\ \text{ack} & (\overline{n+1}) & \overline{0} & \simeq & \text{ack } \overline{n} \ \overline{1} \\ \text{ack} & (\overline{n+1}) & (\overline{m+1}) & \simeq & \text{ack } \overline{n} \ (\text{ack } (\overline{n+1}) \ \overline{m}) \end{array}$$

$$\begin{array}{lcll} \text{down} & \equiv & \lambda f : (\text{Nat}\to\text{Nat}) \,.\, \lambda p : \text{Nat} \,.\, p \text{ Nat } (f \ \overline{1}) \ f & : \quad (\text{Nat}\to\text{Nat}) \to (\text{Nat}\to\text{Nat}) \\ \text{ack} & \equiv & \lambda n, m : \text{Nat} \,.\, n \text{ (Nat}\to\text{Nat) succ down } m & : \quad \text{Nat} \to \text{Nat} \to \text{Nat} \end{array}$$

▷ SN theorem guarantees that all well-typed computations terminate

Part III

System F: Curry-style presentation

System F polymorphism

ML/Haskell polymorphism

Types	A, B	$::=$	$\alpha \mid A \to B \mid \cdots$ (user datatypes)
Schemes	S	$::=$	$\forall \vec{\alpha}\ B$

The type scheme $\forall \alpha\ B$ is defined after its particular instances $B\{\alpha := A\}$
$\Rightarrow$ Type system is predicative

System F polymorphism

Types	A, B	$::=$	$\alpha \mid A \to B \mid \forall \alpha\ B$

The type $\forall \alpha\ B$ and its instances $B\{\alpha := A\}$ are defined simultaneously

$$\forall \alpha\ (\alpha \to \alpha) \qquad \text{and} \qquad \forall \alpha\ (\alpha \to \alpha) \to \forall \alpha\ (\alpha \to \alpha)$$

$\Rightarrow$ Type system is impredicative, or cyclic

Extracting pure λ-terms

In Church-style system F, polymorphism is explicit:

$$\text{id} \equiv \Lambda\alpha\,.\,\lambda x:\alpha\,.\,x \qquad \text{and} \qquad \text{id Nat } 2$$

- Two kind of redexes $\quad (\lambda x:A\,.\,t)u \quad$ and $\quad (\Lambda\alpha\,.\,t)A$

Idea: Remove type abstractions/applications/annotations

Erasing function $t \mapsto |t|$

$$\begin{array}{rcl} |x| & = & x \\ |\lambda x:A\,.\,t| & = & \lambda x\,.\,|t| \\ |tu| & = & |t||u| \end{array} \qquad \begin{array}{rcl} |\Lambda\alpha\,.\,t| & = & |t| \\ |tA| & = & |t| \end{array}$$

- Target language is pure λ-calculus
- Second kind redexes are erased, first kind redexes are preserved

Extending the erasing function

Erased terms have a nice computational behaviour…

- Only one kind of redex, easy to execute (Krivine's machine)
- Irrelevant part of computation has been removed
- The essence of computation has been preserved (to be justified later)

… but what is their status w.r.t. typing?

The erasing function, defined on terms, can be extended to:

- The whole syntax
- The judgements
- The typing rules
- The derivations

$\Rightarrow$ Induces a new formalism: Curry-style system F

Curry-style system F [Leivant 83]

Types	A, B	$::=$	$\alpha \mid A \to B \mid \forall\alpha\, B$
Terms	t, u	$::=$	$x \mid \lambda x\,.\,t \mid tu$
Judgments	Γ	$::=$	$[] \mid \Gamma,\ x{:}A$

Reduction

$$(\lambda x\,.\,t)u \ \succ\ t\{x := u\}$$

Remarks:

- Types (and contexts) are unchanged
- Terms are now pure λ-terms
- Only one kind of redex

Curry-style system F: typing rules

$$\frac{}{\Gamma \vdash x : A} \quad (x{:}A) \in \Gamma$$

$$\frac{\Gamma,\ x : A \vdash t : B}{\Gamma \vdash \lambda x \,.\, t : A \rightarrow B} \qquad \frac{\Gamma \vdash t : A \rightarrow B \qquad \Gamma \vdash u : A}{\Gamma \vdash tu : B}$$

$$\frac{\Gamma \vdash t : B}{\Gamma \vdash t : \forall\alpha\ B} \quad \alpha \notin TV(\Gamma) \qquad \frac{\Gamma \vdash t : \forall\alpha\ B}{\Gamma \vdash t : B\{\alpha := A\}}$$

$\Rightarrow$ Rules are no more syntax directed

Curry-style system F: properties

Things that do not change

- Substitutivity + β-subject reduction
- Strong normalisation (postponed)

Things that change

- A term may have several types

$$
\begin{array}{rcll}
\Delta \equiv \lambda x\,.\,x\ x & : & \forall\alpha\,(\alpha\to\alpha) \ \to\ \forall\alpha\,(\alpha\to\alpha) & \\
& : & \forall\alpha\ \alpha \ \to\ \forall\alpha\ \alpha & \\
& : & \forall\alpha\ \alpha \ \to\ \forall\alpha\,(\alpha\to\alpha) & \\
& : & \mathsf{Bool}\to\mathsf{Bool}\to\mathsf{Bool} & \text{('or' function!)}
\end{array}
$$

- No principal type (cf later)
- Type checking/inference becomes undecidable [Wells 94]

Erasing and typing

Equivalence between Church and Curry's presentations

1. If $\Gamma \vdash t_0 : A$ (Church), then $\Gamma \vdash |t_0| : A$ (Curry)
2. If $\Gamma \vdash t : A$ (Curry), then $\Gamma \vdash t_0 : A$ (Church) for some t_0 s.t. $|t_0| = t$

The erasing function maps:

	Church's world		**Curry's world**	
1.	derivations	to	derivations	(isomorphism)
2.	valid judgements	to	valid judgements	(surjective only)

On valid judgements, erasing is not injective:

$$\begin{array}{rcl} \lambda f : (\forall\alpha\ (\alpha\to\alpha))\,.\,f(\forall\alpha\ (\alpha\to\alpha))f & : & \forall\alpha\ (\alpha\to\alpha)\ \to\ \forall\alpha\ (\alpha\to\alpha) \\ \lambda f : (\forall\alpha\ (\alpha\to\alpha))\,.\,\Lambda\alpha\,.\,f(\alpha\to\alpha)(f\alpha) & : & \forall\alpha\ (\alpha\to\alpha)\ \to\ \forall\alpha\ (\alpha\to\alpha) \\ \rightsquigarrow\quad \lambda f\,.\,ff & : & \forall\alpha\ (\alpha\to\alpha)\ \to\ \forall\alpha\ (\alpha\to\alpha) \end{array}$$

Erasing and reduction

Second-kind redexes are erased, first-kind redexes are preserved

$$
\begin{array}{llcccc}
\text{(Church)} & (\Lambda\alpha\,.\,\lambda x:\alpha\,.\,x)\,B\,y & \succ & (\lambda x:B\,.\,x)\,y & \succ & y \\
\quad\downarrow \text{Erasing} & & & & & \\
\text{(Curry)} & (\lambda x\,.\,x)\,y & \equiv & (\lambda x\,.\,x)\,y & \succ & y
\end{array}
$$

Fact 1 (Church to Curry):

If $t_0, t_0' \in \text{Church}$, then

$$t \succ^n t' \quad \Rightarrow \quad |t_0| \succ^p |t_0'| \qquad \text{(with } p \leq n\text{)}$$

Fact 2 (Curry to Church):

If $t_0 \in \text{Church}$, $t' \in \text{Curry}$ and t_0 well-typed, then

$$|t_0| \succ^p t' \quad \Rightarrow \quad \exists t_0' \; (|t_0'| = t' \;\wedge\; t_0 \succ^n t_0') \qquad \text{(with } n \geq p\text{)}$$

Normalisation equivalence

Fact 3 (Combinatorial argument):

1. During the contraction of a 1st-kind redex, the number of redexes of both kinds may increase
2. During the contraction of a 2nd-kind redex
   - the number of 1st-kind redexes may increase
   - the number of 2nd-kind redexes does not increase
   - the number of type abstractions $(\Lambda\alpha\,.\,t)$ decreases

Combining facts 1, 2 and 3, we easily prove:

Theorem (Normalisation equivalence):

The following statements are combinatorially equivalent:

1. All typable terms of syst. F-Church are strongly normalisable
2. All typable terms of syst. F-Curry are strongly normalisable

Subtyping

In Curry-style system F, subtyping is introduced as a macro:

$$A \leq B \quad \equiv \quad x : A \vdash x : B$$

Admissible rules

(Reflexivity, transitivity)

$$\frac{}{A \leq A} \qquad \frac{A \leq B \qquad B \leq C}{A \leq C}$$

(Polymorphism)

$$\frac{}{\forall\alpha\, B \leq B\{\alpha := A\}} \qquad \frac{A \leq B}{A \leq \forall\alpha\, B}\ \alpha \notin TV(A)$$

(Subsumption)

$$\frac{\Gamma \vdash t : A \qquad A \leq B}{\Gamma \vdash t : B}$$

Problem with η-redexes in Curry-style system F

- The (desired) subtyping rule for arrow-types

$$\frac{A \leq A' \qquad B \leq B'}{A' \to B \;\leq\; A \to B'}$$

  is not admissible

- In particular, we have: $f : \mathrm{Nat} \to \forall\beta\, \beta \;\not\vdash\; f \;:\; \forall\alpha\, \alpha \to \mathrm{Bool}$

  but if we η-expand: $f : \mathrm{Nat} \to \forall\beta\, \beta \;\vdash\; \lambda x\,.\,fx \;:\; \forall\alpha\, \alpha \to \mathrm{Bool}$

- This shows that:
  1. Curry-style system F does not enjoy η-subject reduction
  2. This problem is connected with subtyping in arrow-types

The well-typed term: $\lambda x\,.\,fx \;:\; (\forall\alpha\, \alpha) \to \mathrm{Bool}$ (Curry-style)

comes from the term $\underbrace{\lambda x : (\forall\alpha\, \alpha)\,.\, f\; (x\; \mathrm{Nat})\; \mathrm{Bool}}_{\text{not an } \eta\text{-redex}}$ (Church-style)

System F_η [Mitchell 88]

Extend Curry-style system F with a new rule

$$\frac{\Gamma \vdash \lambda x\,.\,tx : A}{\Gamma \vdash t : A}\ {\scriptstyle x \notin FV(t)}$$

to enforce η-subject reduction

Properties:

- Substitutivity, $\beta\eta$-subject-reduction, strong normalisation
- Subtyping rule $\dfrac{A \leq A' \qquad B \leq B'}{A' \to B \ \leq \ A \to B'}$ is now admissible

Expansion lemma

If $\Gamma \vdash t : A$ is derivable in F_η, then $\Gamma \vdash t' : A$ is derivable in system F for some η-expansion t' of the term t.

More subtyping

If we set

$$\begin{array}{rcl} \bot & := & \forall\gamma\ \gamma \\ A \times B & := & \forall\gamma\ ((A \to B \to \gamma) \to \gamma) \\ A + B & := & \forall\gamma\ ((A \to \gamma) \to (B \to \gamma) \to \gamma) \\ \mathsf{List}(A) & := & \forall\gamma\ (\gamma \to (A \to \gamma \to \gamma) \to \gamma) \end{array}$$

then, in F_η, the following subtyping rules are admissible:

$$\frac{}{\bot \ \leq \ A} \qquad \frac{A \ \leq \ A'}{\mathsf{List}(A) \ \leq \ \mathsf{List}(A')}$$

$$\frac{A \ \leq \ A' \qquad B \ \leq \ B'}{A \times B \ \leq \ A' \times B'} \qquad \frac{A \ \leq \ A' \qquad B \ \leq \ B'}{A + B \ \leq \ A' + B'}$$

But most typable terms have no principal type

Adding intersection types

Extend system F_η with binary intersections

$$\textbf{Types} \quad A, B \quad ::= \quad \alpha \quad | \quad A \rightarrow B \quad | \quad \forall\alpha\ B \quad | \quad A \cap B$$

$$\frac{\Gamma \vdash t : A \qquad \Gamma \vdash t : B}{\Gamma \vdash t : A \cap B} \qquad \frac{\Gamma \vdash t : A \cap B}{\Gamma \vdash t : A} \qquad \frac{\Gamma \vdash t : A \cap B}{\Gamma \vdash t : B}$$

- $\beta\eta$-subject reduction, strong normalisation, etc.
- Subtyping rules

$$\frac{}{A \cap B \ \leq\ A} \qquad \frac{}{A \cap B \ \leq\ B} \qquad \frac{C \leq A \qquad C \leq B}{C \ \leq\ A \cap B}$$

- All the strongly normalising terms are typable. . .
  . . . but nothing to do with $\forall$: already true in $\lambda{\rightarrow}\cap$
- All typable terms have a principal type
  $\lambda x : xx\,.\ \ :\ \forall\alpha\ \forall\beta\ ((\alpha{\rightarrow}\beta) \cap \alpha \rightarrow \beta)$

Part IV

The Strong Normalisation Theorem

The meaning of second-order quantification (1/2)

Question: What is the meaning of $\forall\alpha\ (\alpha \to \alpha)$?

First scenario: an infinite Cartesian product (à la Martin-Löf)

$$\begin{aligned}\forall\alpha\ (\alpha \to \alpha) \ &\approx\ \prod_{\alpha\ \text{type}} (\alpha \to \alpha) \\ &\approx\ (\bot \to \bot) \times (\mathsf{Bool} \to \mathsf{Bool}) \times (\mathsf{Nat} \to \mathsf{Nat}) \times \cdots\end{aligned}$$

Since all the types $A \to A$ are inhabited:

1. The cartesian product $\forall\alpha\ (\alpha{\to}\alpha)$ should be larger than all the types of the form $A \to A$
2. In particular, $\forall\alpha\ (\alpha{\to}\alpha)$ should be larger than its own function space $\forall\alpha\ (\alpha{\to}\alpha) \to \forall\alpha\ (\alpha{\to}\alpha)\ldots$

... seems to be very confusing!

The meaning of second-order quantification (2/2)

Second scenario: In F-Curry, both rules $\forall$-intro and $\forall$-elim

$$\frac{\Gamma \vdash t : B}{\Gamma \vdash t : \forall\alpha\ B}\ \alpha \notin TV(\Gamma) \qquad\qquad \frac{\Gamma \vdash t : \forall\alpha\ B}{\Gamma \vdash t : B\{\alpha := A\}}$$

suggest that $\forall$ is not a cartesian product, but an intersection

Taking back our example:

1. The intersection $\forall\alpha\ (\alpha\to\alpha)$ is smaller than all $A \to A$
2. In particular, $\forall\alpha\ (\alpha\to\alpha)$ is smaller than its own function space $\forall\alpha\ (\alpha\to\alpha) \to \forall\alpha\ (\alpha\to\alpha)\ldots$

... our intuition feels much better!

$\Rightarrow$ We will prove strong normalisation for Curry-style system F

Remember that SN(F-Church) $\Leftrightarrow$ SN(F-Curry) (combinatorial equivalence)

Strong normalisation: the difficulty

Try to prove that

$$\Gamma \vdash t : A \quad \Rightarrow \quad t \text{ is SN}$$

by induction on the derivation of $\Gamma \vdash t : A$

$$\frac{}{\Gamma \vdash x : A}\ {\scriptstyle (x:A)\in\Gamma}$$

$$\frac{\Gamma,\ x : A \vdash t : B}{\Gamma \vdash \lambda x\,.\,t : A \to B} \qquad \frac{\Gamma \vdash t : A \to B \qquad \Gamma \vdash u : A}{\Gamma \vdash tu : B}$$

$$\frac{\Gamma \vdash t : B}{\Gamma \vdash t : \forall\alpha\ B}\ {\scriptstyle \alpha\notin TV(\Gamma)} \qquad \frac{\Gamma \vdash t : \forall\alpha\ B}{\Gamma \vdash t : B\{\alpha := A\}}$$

All the cases successfully pass the test except application

Two terms t and u may be SN, whereas tu is not [Take $t \equiv u \equiv \lambda x\,.\,xx$]

$\Rightarrow$ The induction hypothesis "t is SN" is too weak (in general)

Reducibility candidates [Girard 1971]

To prove that

$$\Gamma \vdash t : A \quad \Rightarrow \quad t \text{ is SN},$$

the induction hypothesis "t is SN" is too weak.

$\Rightarrow$ Should replace it by an invariant that depends on the type A

Intuition:

The more complex the type, the stronger its invariant,
the smaller the set of terms that fulfill this invariant

Invariants are represented by suitable sets of terms:

- Reducibility candidates [Girard], or
- Saturated sets [Tait]

Outline of the proof

1. Define a suitable notion of reducibility candidate
   $=$ the sets of λ-terms that will interpret/represent types

   (Here, we use Tait's saturated sets)

2. Ensure that the notion of candidate captures the property of strong normalisation (which we want to prove)

   Each candidate should only contain strongly normalisable λ-terms as elements

3. Associate to each type A a reducibility candidate $[\![A]\!]$

   Type constructors '$\rightarrow$' and '$\forall$' have to be reflected at the level of candidates

4. Check (by induction) that $\Gamma \vdash t : A$ implies $t \in [\![A]\!]$

   This is actually a little bit more complex, since we must take care of the typing context

5. Conclude that any well-typed term t is SN by step 2.

Preliminaries (1/2)

- **Notations:**

Λ	$\equiv$	set of all untyped λ-terms (open & closed)
SN	$\equiv$	set of all strongly normalisable untyped λ-terms
Var	$\equiv$	set of all (term) variables
TVar	$\equiv$	set of all type variables

- A reduct of a term t is a term t' such that $t \succ t'$ (one step)

  The number of reducts of a given term is finite and bounded by the number of redexes

- A finite reduction sequence of a term t is a finite sequence $(t_i)_{i\in[0..n]}$ such that $t = t_0 \succ t_1 \succ \cdots \succ t_{n-1} \succ t_n$

  Infinite reduction sequences are defined similarly, by replacing $[0..n]$ by $\mathbb{N}$

- Finite reduction sequences of a term t form a tree, called the reduction tree of t

Preliminaries (2/2)

Definition (Strongly normalisable terms)

A term t is strongly normalisable if all the reduction sequences starting from t are finite

Proposition

The following assertions are equivalent:

1. t is strongly normalisable
2. All the reducts of t are strongly normalisable
3. The reduction tree of t is finite

Saturated sets [Tait]

Definition (Saturated set)

A set $S \subset \Lambda$ is saturated if:

$$
\begin{array}{lll}
\text{(SAT1)} & S \subset \mathrm{SN} & \\
\text{(SAT2)} & x \in \mathrm{Var}, \quad \vec{v} \in \mathrm{list}(\mathrm{SN}) \quad \Rightarrow \quad x\vec{v} \in S & \\
\text{(SAT3)} & t\{x := u\}\vec{v} \in S, \quad u \in \mathrm{SN} \quad \Rightarrow \quad (\lambda x\,.\,t)u\vec{v} \in S &
\end{array}
$$

- (SAT1) expresses the property we want to prove
- Saturated sets contain all the variables (SAT2)
  Extra-arguments $\vec{v} \in \mathrm{list}(\mathrm{SN})$ are here for technical reasons
- Saturated sets are closed under head β-expansion (SAT3)
  Notice the condition $u \in \mathrm{SN}$ to avoid a clash with (SAT1) for K-redexes
- The set of all saturated sets is written **SAT** $[\subset \mathfrak{P}(\mathrm{SN}) \subset \mathfrak{P}(\Lambda)]$

Properties of saturated sets

Proposition (Lattice structure)

1. SN is a saturated set
2. **SAT** is closed under arbitrary non-empty intersections/unions:

$$I \neq \varnothing, \quad (S_i)_{i \in I} \in \mathbf{SAT}^I \quad \Rightarrow \quad \Big(\bigcap_{i \in I} S_i\Big), \Big(\bigcup_{i \in I} S_i\Big) \in \mathbf{SAT}$$

$(\mathbf{SAT}, \subset)$ is a complete distributive lattice, with

$\top = \mathrm{SN}$ and $\bot = \{t \in \mathrm{SN} \mid t \succ^* x u_1 \cdots u_n\}$ (Neutral terms)

Realisability arrow: For all $S, T \subset \Lambda$ we set

$$S \to T \quad := \quad \{t \in \Lambda \mid \forall u \in S \quad tu \in T\}$$

Proposition (Closure under realisability arrow)

If $S, T \in \mathbf{SAT}$, then $(S \to T) \in \mathbf{SAT}$

Interpreting types (1/2)

Principle: Interpret syntactic types by saturated sets

- Type arrow $A \to B$ is interpreted by $S \to T$ (realisability arrow)
- Type quantification $\forall\alpha\ ..$ is interpreted by the intersection $\bigcap_{S \in \mathbf{SAT}} \cdots$

  Remark: this intersection is impredicative since S ranges over all saturated sets

Example: $\forall\alpha\ (\alpha \to \alpha)$ should be interpreted by $\bigcap_{S \in \mathbf{SAT}} (S \to S)$

To interpret type variables, use type valations:

Definition (Type valuations)

A type valuation is a function $\rho : \mathrm{TVar} \to \mathbf{SAT}$

The set of type valuations is written TVal $(= \mathrm{TVar} \to \mathbf{SAT})$

Interpreting types (2/2)

By induction on A, we define a function $[\![A]\!] : \text{TVal} \to \textbf{SAT}$

$$[\![A \to B]\!]_\rho = [\![A]\!]_\rho \to [\![B]\!]_\rho \qquad [\![\alpha]\!]_\rho = \rho(\alpha)$$

$$[\![\forall\alpha\ B]\!]_\rho = \bigcap_{S \in \textbf{SAT}} [\![B]\!]_{\rho;\alpha\leftarrow S}$$

Note: $(\rho;\alpha \leftarrow S)$ is defined by $\begin{cases}(\rho;\alpha\leftarrow S)(\alpha) = S \\ (\rho;\alpha\leftarrow S)(\beta) = \rho(\beta) \quad \text{for all } \beta \neq \alpha\end{cases}$

Problem: The implication

$$\Gamma \vdash t : A \quad \Rightarrow \quad t \in [\![A]\!]_\rho$$

cannot be proved directly. (One has to take care of the context)

$\Rightarrow$ Strengthen induction hypothesis using substitutions

Substitutions

Definition (Substitutions)

A substitution is a finite list $\sigma = [x_1 := u_1; \ldots; x_n := u_n]$
where $x_i \neq x_j$ (for $i \neq j$) and $u_i \in \Lambda$

Application of a substitution σ to a term t is written $t[\sigma]$

Exercise: Define it formally

Definition (Interpretation of contexts)

For all $\Gamma = x_1 : A_1; \ldots; x_n : A_n$ and $\rho \in \mathrm{TVal}$ set:

$$[\![\Gamma]\!]_\rho = \{\sigma = [x_1 := u_1; \ldots; x_n := u_n]; \quad u_i \in [\![A_i]\!]_\rho \ (i = 1..n)\}$$

Substitutions $\sigma \in [\![\Gamma]\!]_\rho$ are said to be adapted to the context Γ (in the type valuation ρ)

The strong normalisation invariant

Lemma (Strong normalisation invariant)

If $\Gamma \vdash t : A$ in Curry-style system F, then

$$\forall \rho \in \mathsf{TVal} \qquad \forall \sigma \in [\![\Gamma]\!]_\rho \qquad t[\sigma] \in [\![A]\!]_\rho$$

Proof. By induction on the derivation of $\Gamma \vdash t : A$.

Exercise: Write down the 5 cases completely

Theorem (Strong normalisation)

The typable terms of F-Curry are strongly normalisable

Corollary (Church-style SN)

The typable terms of F-Church are strongly normalisable

A remark on impredicativity

In the SN proof, interpretation of $\forall$ relies on the property:

> *If* $(S_i)_{i \in I}$ $(I \neq \varnothing)$ *is a family of saturated sets,*
> *then* $\bigcap_{i \in I} S_i$ *is a saturated set*

in the special case where $I = \mathbf{SAT}$ (impredicative intersection)

- In 'classical' mathematics, this construction is legal

  $\Rightarrow$ Standard set theories (Z, ZF, ZFC) are impredicative

- In (Bishop, Martin-Löf's style) constructive mathematics, this principle is rejected, mainly for philosophical reasons:
  - No convincing 'constructive' explanation
  - Suspicion about (this kind of) cyclicity

Impredicativity: An example (1/2)

Assume E is a vector space, S a set of vectors.
How to define the sub-vector space $\overline{S} \subset E$ generated by S in E ?

Standard 'abstract' method:

1. Consider the set: $\mathfrak{S} = \{F; \quad F \text{ is a sub-vector space of } E \text{ and } F \supset S\}$
2. Fact: $\mathfrak{S}$ is non empty, since $E \in \mathfrak{S}$
3. Take: $\overline{S} = \bigcap_{F \in \mathfrak{S}} F$
4. By definition, S is included in all the sub-spaces of E containing S
5. But $\overline{S}$ is itself a sub-vector space of E containing S (so that $\overline{S} \in \mathfrak{S}$)
6. So that $\overline{S}$ is actually the smallest of all such spaces

This definition is impredicative (step 3) (but legal in 'classical' mathematics)

The set $\overline{S}$ is defined *from* $\mathfrak{S}$, $\underbrace{\text{that already contains } \overline{S} \textit{ as an element}}_{\text{discovered a fortiori}}$

Impredicativity: An example (2/2)

But there are other ways of defining $\overline{S}$...

- **Standard 'concrete' definition, by linear combinations:**

  Let $\overline{S}$ be the set of all vectors of the form $v = \alpha_1 \cdot v_1 + \cdots + \alpha_n \cdot v_n$

  where (v_i) ranges over all the finite families of elements of S,
  and (α_i) ranges over all the finite families of scalars

- **Inductive definition:**

  Let $\overline{S}$ be the set inductively defined by:

  1. $\vec{0} \in \overline{S}$,
  2. If $v \in S$, then $v \in \overline{S}$,
  3. If $v \in \overline{S}$ and α is a scalar, then $\alpha \cdot v \in \overline{S}$
  4. If $v_1 \in \overline{S}$ and $v_2 \in \overline{S}$, then $v_1 + v_2 \in \overline{S}$.

$\Rightarrow$ Both definitions are predicative (and give the same object)