Polymorphism, Subtyping, and Type Inference in MLsub

Stephen Dolan and Alan Mycroft
November 8, 2016

Computer Laboratory
University of Cambridge
The *select* function

\[
\text{select } p \; v \; d = \text{if } (p \; v) \text{ then } v \text{ else } d
\]

In ML, *select* has type scheme

\[
\forall \alpha. (\alpha \rightarrow \text{bool}) \rightarrow \alpha \rightarrow \alpha \rightarrow \alpha
\]
Data flow in select

\[
\text{select } p \lor d = \text{if } (p \lor) \text{ then } v \text{ else } d
\]
Data flow in `select`

\[
\text{select } p \lor d = \text{if } (p \lor) \text{ then } v \text{ else } d
\]

In MLsub, `select` has this type scheme:

\[
\forall \alpha, \beta. (\alpha \rightarrow \text{bool}) \rightarrow \alpha \rightarrow \beta \rightarrow (\alpha \sqcup \beta)
\]
The MLsub Type System
Γ ⊢ e : τ
Γ ⊢ e : τ
Expressions of MLsub

We have functions

\[ x \quad \lambda x.e \quad e_1 e_2 \]

... and records

\[ \{ \ell_1 = e_1, \ldots, \ell_n = e_n \} \quad e.\ell \]

... and booleans

\[ \text{true} \quad \text{false} \quad \text{if } e_1 \text{ then } e_2 \text{ else } e_3 \]

... and let

\[ \hat{x} \quad \text{let } \hat{x} = e_1 \text{ in } e_2 \]
Γ ⊢ e : τ
MLsub is

\[ \text{ML} + \]

\[
\frac{
\Gamma \vdash e : \tau_1 \\
\tau_1 \leq \tau_2 \\
\Gamma \vdash e : \tau_2
}{
(\text{SUB})
\]
Γ ⊢ \text{e} : \tau
Constructing Types

The standard definition of types looks like:

\[ \tau ::= \bot \mid \tau \rightarrow \tau \mid \top \]

(ignoring records and booleans for now)
Constructing Types

The standard definition of types looks like:

$$\tau ::= \bot \mid \tau \rightarrow \tau \mid \top$$

(ignoring records and booleans for now)

with a subtyping relation like:

$$\begin{align*}
\bot & \leq \tau \\
\tau & \leq \top \\
\tau_1 \rightarrow \tau_2 & \leq \tau_1' \rightarrow \tau_2'
\end{align*}$$
These types form a lattice:

- least upper bounds $\tau_1 \sqcup \tau_2$
- greatest lower bounds $\tau_1 \sqcap \tau_2$
These types form a lattice:

- least upper bounds $\tau_1 \sqcup \tau_2$
- greatest lower bounds $\tau_1 \sqcap \tau_2$

$$
\begin{array}{ll}
  e_1 : \tau_1 & e_2 : \tau_2 \\
\hline
  \text{if rand () then } e_1 \text{ else } e_2 : \tau_1 \sqcup \tau_2
\end{array}
$$
Is this true, for all $\alpha$?

\[ \alpha \rightarrow \alpha \leq \bot \rightarrow \top \]
Is this true, for all $\alpha$?

$$\alpha \rightarrow \alpha \leq \bot \rightarrow \top$$

How about this?

$$\left( \bot \rightarrow \top \right) \rightarrow \bot \leq \left( \alpha \rightarrow \bot \right) \sqcup \alpha$$
Bizzarely difficult questions

Is this true, for all $\alpha$?

$$\alpha \to \alpha \leq \bot \to \top$$

How about this?

$$(\bot \to \top) \to \bot \leq (\alpha \to \bot) \sqcup \alpha$$

Yes, it turns out, by case analysis on $\alpha$. 
Bizzarely difficult questions

Is this true, for all $\alpha$?

$$\alpha \rightarrow \alpha \leq \bot \rightarrow \top$$

How about this?

$$(\bot \rightarrow \top) \rightarrow \bot \leq (\alpha \rightarrow \bot) \sqcup \alpha$$

Yes, it turns out, by case analysis on $\alpha$.

And only by case analysis.
Let’s add a new type of function $\tau_1 \circ \rightarrow \tau_2$. 
Extensibility

Let’s add a new type of function $\tau_1 \circ \rightarrow \tau_2$. It’s a supertype of $\tau_1 \rightarrow \tau_2$

“function that may have side effects”
Let’s add a new type of function $\tau_1 \circ \to \tau_2$.

It’s a supertype of $\tau_1 \to \tau_2$

“function that may have side effects”

Now we have a counterexample:

$$\alpha = (\top \circ \to \bot) \circ \to \bot$$
Extensible type systems

Two techniques give us an extensible system:

- Add explicit type variables as indeterminates
  *gets rid of case analysis*
Extensible type systems

Two techniques give us an extensible system:

- Add explicit type variables as indeterminates
  
  *gets rid of case analysis*

- Require a distributive lattice
  
  *gets rid of vacuous reasoning*
Combining types

How to combine different types into a single system?

\[ \tau ::= \text{bool} \mid \tau_1 \rightarrow \tau_2 \mid \{ \ell_1 : \tau_1, \ldots, \ell_n : \tau_n \} \]
Combining types

How to combine different types into a single system?

\[ \tau ::= \text{bool} \mid \tau_1 \rightarrow \tau_2 \mid \{ \ell_1 : \tau_1, \ldots, \ell_n : \tau_n \} \]

We should read ‘|’ as coproduct
Concrete syntax

Build an actual syntax for types, by writing down all the operations on types:

\[ \tau ::= \text{bool} \mid \tau_1 \rightarrow \tau_2 \mid \{ \ell_1 : \tau_1, \ldots, \ell_n : \tau_n \} \mid \alpha \mid \top \mid \bot \mid \tau \sqcup \tau \mid \tau \sqcap \tau \]
Concrete syntax

Build an actual syntax for types, by writing down all the operations on types:

\[ \tau ::= \text{bool} \mid \tau_1 \to \tau_2 \mid \{\ell_1 : \tau_1, \ldots, \ell_n : \tau_n\} \mid \alpha \mid \top \mid \bot \mid \tau \sqcup \tau \mid \tau \sqcap \tau \]

then quotient by the equations of distributive lattices, and the subtyping order.
Resulting types

We end up with all the standard types
Resulting types

We end up with all the standard types

... with the same subtyping order
Resulting types

We end up with all the standard types

... with the same subtyping order

... but we identify fewer of the weird types

\( \{\text{foo} : \text{bool}\} \sqcap (\top \rightarrow \top) \not\subseteq \text{bool} \)
Principality
Γ ⊢ e : τ
Intuitively,

*For any* $e$ *typeable under* $\Gamma$, *there’s a best type* $\tau$
Intuitively,

For any $e$ typeable under $\Gamma$, there’s a best type $\tau$

but it’s a bit more complicated than that:

For any $e$ typeable under $\Gamma$, there’s a $\tau$ and a substitution $\sigma$ such that every possible typing of $e$ under $\Gamma$ is a substitution instance of $\sigma \Gamma, \tau$. 
The complexity arises because $\Gamma$ is part question, part answer.
Reformulating the typing rules

The complexity arises because $\Gamma$ is part question, part answer.

Instead, split $\Gamma$:

- $\Delta$ maps $\lambda$-bound $x$ to a type $\tau$
- $\Pi$ maps let-bound $\hat{x}$ to a typing schemes $[\Delta]_\tau$
Π ⊢ e : [Δ]^τ
question \[\Pi \vdash e : [\Delta]^\tau\] answer
Subsumption

Define $\leq^\forall$ as the least relation closed under:

- *Instatiation*, replacing type variables with types
- *Subtyping*, replacing types with supertypes
A principal typing scheme for $e$ under $\Pi$ is a $[\Delta]_\tau$ that subsumes any other.
The choose function

choose takes two values and returns one of them:

\[
\text{choose} : \forall \alpha. \alpha^1 \rightarrow \alpha^2 \rightarrow \alpha^3
\]
The choose function

choose takes two values and returns one of them:

\[
\text{choose} : \forall \alpha. \alpha^1 \rightarrow \alpha^2 \rightarrow \alpha^3
\]

In ML, \(\alpha^1 = \alpha^2 = \alpha^3\).

With subtyping, \(\alpha^1 \leq \alpha^3\), \(\alpha^2 \leq \alpha^3\), but \(\alpha^1\) and \(\alpha^2\) may be incomparable.
The choose function

choose takes two values and returns one of them:

\[
\text{choose} : \forall \alpha. \alpha^1 \to \alpha^2 \to \alpha^3
\]

In ML, \(\alpha^1 = \alpha^2 = \alpha^3\).

With subtyping, \(\alpha^1 \leq \alpha^3\), \(\alpha^2 \leq \alpha^3\), but \(\alpha^1\) and \(\alpha^2\) may be incomparable.

\[
\text{choose} : \forall \alpha \beta. \alpha \to \beta \to \alpha \sqcup \beta
\]
The choose function

choose takes two values and returns one of them:

\[ \text{choose} : \forall \alpha. \alpha^1 \rightarrow \alpha^2 \rightarrow \alpha^3 \]

In ML, \( \alpha^1 = \alpha^2 = \alpha^3 \).

With subtyping, \( \alpha^1 \leq \alpha^3 \), \( \alpha^2 \leq \alpha^3 \), but \( \alpha^1 \) and \( \alpha^2 \) may be incomparable.

\[ \text{choose} : \forall \alpha \beta. \alpha \rightarrow \beta \rightarrow \alpha \sqcap \beta \]

These are equivalent (\( \equiv^\forall \)): subsume each other
Type Inference with Polar Types
Input and output types

\( \tau \sqcup \tau' \): produces a value which is a \( \tau \) or a \( \tau' \)

\( \tau \sqcap \tau' \): requires a value which is a \( \tau \) and a \( \tau' \)

\( \sqcup \) is for outputs, and \( \sqcap \) is for inputs.
Input and output types

\( \tau \sqcup \tau' \): produces a value which is a \( \tau \) or a \( \tau' \)

\( \tau \sqcap \tau' \): requires a value which is a \( \tau \) and a \( \tau' \)

\( \sqcup \) is for outputs, and \( \sqcap \) is for inputs.

Divide types into

- output types \( \tau^+ \)
- input types \( \tau^- \)
Polar types

\[
\tau^+ ::= \text{bool} \mid \tau_1^- \rightarrow \tau_2^+ \mid \{\ell_1 : \tau_1^+, \ldots, \ell_n : \tau_n^+\} \mid \\
\alpha \mid \tau_1^+ \sqcup \tau_2^+ \mid \bot \mid \mu\alpha.\tau^+
\]

\[
\tau^- ::= \text{bool} \mid \tau_1^+ \rightarrow \tau_2^- \mid \{\ell_1 : \tau_1^-, \ldots, \ell_n : \tau_n^-\} \mid \\
\alpha \mid \tau_1^- \sqcap \tau_2^- \mid \top \mid \mu\alpha.\tau^-
\]
Cases of unification

In HM inference, unification happens in three situations:

- Unifying two input types
- Unifying two output types
- Using the output of one expression as input to another
Cases of unification

In HM inference, unification happens in three situations:

- Unifying two input types
  \[ \text{Introduce} \sqcup \]

- Unifying two output types
  \[ \text{Introduce} \sqcap \]

- Using the output of one expression as input to another
  \[ \tau^+ \leq \tau^- \text{ constraint} \]
Suppose we have an identity function

\[ \alpha \rightarrow \alpha \]
Eliminating variables, ML-style

Suppose we have an identity function, which uses its argument as a $\tau$

$$\alpha \rightarrow \alpha \mid \alpha = \tau$$
Suppose we have an identity function, which uses its argument as a $\tau$

$$\alpha \rightarrow \alpha \mid \alpha = \tau$$

$$\forall \tau \rightarrow \tau$$
Eliminating variables, ML-style

Suppose we have an identity function, which uses its argument as a $\tau$

\[
\alpha \rightarrow \alpha \mid \alpha = \tau \\
\equiv \forall \tau \rightarrow \tau
\]

The substitution $[\tau/\alpha]$ solves the constraint $\alpha = \tau$
What does it mean to solve a constraint?

1. $[\tau/\alpha]$ trivialises the constraint $\alpha = \tau$
   (it is a unifier),
   and all other unifiers are an instance of it
   (it is a most general unifier)
What does it mean to **solve** a constraint?

1. $[\tau/\alpha]$ trivialises the constraint $\alpha = \tau$  
   (it is a *unifier*),  
   and all other unifiers are an instance of it  
   (it is a *most general unifier*)

2. For any type $\tau'$, the following sets agree:  
   the instances of $\tau'$, subject to $\alpha = \tau$  
   the instances of $[\tau/\alpha]\tau'$
Definition 2, now with subtyping

Suppose we have an identity function, which uses its argument as a $\tau^-$. 

$$\alpha \rightarrow \alpha \mid \alpha \leq \tau^-$$
Suppose we have an identity function, which uses its argument as a $\tau^-$. 

\[
\alpha \rightarrow \alpha \mid \alpha \leq \tau^-
\equiv \forall (\alpha \sqcap \tau^-) \rightarrow (\alpha \sqcap \tau^-)
\]
Definition 2, now with subtyping

Suppose we have an identity function, which uses its argument as a $\tau^-$.

\[
\alpha \rightarrow \alpha \mid \alpha \leq \tau^-
\]

\[
\equiv \forall (\alpha \cap \tau^-) \rightarrow (\alpha \cap \tau^-)
\]

\[
\equiv \forall (\alpha \cap \tau^-) \rightarrow \alpha
\]
Suppose we have an identity function, which uses its argument as a $\tau^-$. 

\[
\begin{align*}
\alpha \rightarrow \alpha &\mid \alpha \leq \tau^- \\
\equiv \forall (\alpha \cap \tau^-) \rightarrow (\alpha \cap \tau^-) \\
\equiv \forall (\alpha \cap \tau^-) \rightarrow \alpha
\end{align*}
\]

The *bisubstitution* $[\alpha \cap \tau^-/\alpha^-]$ solves $\alpha \leq \tau^-$.
Decomposing constraints

We only need to decompose constraints of the form $\tau^+ \leq \tau^-$. 

\[
\tau_1 \sqcup \tau_2 \leq \tau_3 \equiv \tau_1 \leq \tau_3, \ \tau_2 \leq \tau_3
\]

\[
\tau_1 \leq \tau_2 \sqcap \tau_3 \equiv \tau_1 \leq \tau_2, \ \tau_1 \leq \tau_3
\]

Thanks to the input/output type distinction, the hard cases of $\tau_1 \sqcap \tau_2 \leq \tau_3$ and $\tau_1 \leq \tau_2 \sqcup \tau_3$ can never come up.
Combining solutions

We solve a system of multiple constraints $C_1, C_2$ by:

- Solving $C_1$, giving a bisubstitution $\xi$
- Applying that to $C_2$
- Solving $\xi C_2$, giving a bisubstitution $\zeta$

Then $\xi \circ \zeta$ solves the system $C_1, C_2$. 
Putting it all together

biunify(\(C\)) takes a set of constraints \(C\), and produces a bisubstitution solving them.

\[
\text{biunify}(\emptyset) = []
\]

\[
\text{biunify}(\alpha \leq \alpha, C) = \text{biunify}(C)
\]

\[
\text{biunify}(\alpha \leq \tau, C) = \text{biunify}(\theta_{\alpha \leq \tau} H; \theta_{\alpha \leq \tau} C) \circ \theta_{\alpha \leq \tau}
\]

\[
\text{biunify}(\tau \leq \alpha, C) = \text{biunify}(\theta_{\tau \leq \alpha} H; \theta_{\tau \leq \alpha} C) \circ \theta_{\tau \leq \alpha}
\]

\[
\text{biunify}(c, C) = \text{biunify}(\text{decompose}(c), C)
\]
Putting it all together

biunify(\(C\)) takes a set of constraints \(C\), and produces a bisubstitution solving them.

\[
\begin{align*}
\text{biunify}(\emptyset) &= [] \\
\text{biunify}(\alpha \leq \alpha, C) &= \text{biunify}(C) \\
\text{biunify}(\alpha \leq \tau, C) &= \text{biunify}(\theta_{\alpha \leq \tau} H; \theta_{\alpha \leq \tau} C) \circ \theta_{\alpha \leq \tau} \\
\text{biunify}(\tau \leq \alpha, C) &= \text{biunify}(\theta_{\tau \leq \alpha} H; \theta_{\tau \leq \alpha} C) \circ \theta_{\tau \leq \alpha} \\
\text{biunify}(c, C) &= \text{biunify}(\text{decompose}(c), C)
\end{align*}
\]

Replace the \(\leq\) with \(=\) and we have Martelli and Montanari’s unification algorithm.
MLsub infers types by walking the syntax of the program, but must deal with subtyping constraints rather than just equalities. Thanks to:

- algebraically well-behaved types
- polar types, restricting occurrences of $\sqcap$ and $\sqcup$
- a careful definition of “solves”

the biunify algorithm can always handle these constraints, producing a principal type.
Questions?

http://www.cl.cam.ac.uk/~sd601/mlsub
stephen.dolan@cl.cam.ac.uk
Mutable references

References are generally considered “invariant”.

Instead, consider \texttt{ref} a two-argument constructor

\[(\alpha, \beta) \\texttt{ref}\]

with operations:

\[
\texttt{make} : (\alpha, \alpha) \\texttt{ref} \\
\texttt{get} : (\bot, \beta) \\texttt{ref} \rightarrow \beta \\
\texttt{set} : (\alpha, \top) \\texttt{ref} \rightarrow \alpha \rightarrow \text{unit}
\]