MPRI, Typage

Didier Rémy
(With course material from François Pottier)

November 20, 2014

INRIA
Plan of the course

Introduction

Simply-typed \( \lambda \)-calculus

Polymorphism and System F

Type reconstruction

Existential types
Existential types
Contents

• Introduction

• Towards typed closure conversion

• Existential types
  • Implicitly-type existential types passing
  • Iso-existential types

• Typed closure conversion
  • Environment passing
  • Closure passing
Type-preserving compilation

Compilation is type-preserving when each intermediate language is *explicitly typed*, and each compilation phase transforms a typed program into a typed program in the next intermediate language.

Why *preserve types* during compilation?

- it can help debug the compiler;
- types can be used to drive optimizations;
- types can be used to produce *proof-carrying code*;
- proving that types are preserved can be the first step towards proving that the *semantics* is preserved [Chlipala, 2007].
Type-preserving compilation

Type-preserving compilation exhibits an encoding of programming constructs into programming languages with usually richer type systems.

The encoding may sometimes be used directly as a programming idiom in the source language.

For example:

- Closure conversion requires an extension of the language with existential types, which happens to be very useful on their own.
- Closures are themselves a simple form of objects.
- Defunctionalization may be done manually on some particular programs, e.g. in web applications to monitor the computation.
Type-preserving compilation

A classic paper by Morrisett *et al.* [1999] shows how to go from System F to Typed Assembly Language, while preserving types along the way. Its main passes are:

- **CPS conversion** fixes the order of evaluation, names intermediate computations, and makes all function calls tail calls;
- **closure conversion** makes environments and closures explicit, and produces a program where all functions are closed;
- allocation and initialization of tuples is made explicit;
- the calling convention is made explicit, and variables are replaced with (an unbounded number of) machine registers.
Translating types

In general, a type-preserving compilation phase involves not only a translation of terms, mapping \( M \) to \([M]\), but also a translation of types, mapping \( \tau \) to \([\tau]\), with the property:

\[
\Gamma \vdash M : \tau \quad \text{implies} \quad [\Gamma] \vdash [M] : [\tau]
\]

The translation of types carries a lot of information: examining it is often enough to guess what the translation of terms will be.
Contents

- Introduction

- Towards typed closure conversion

- Existential types
  - Implicitly-type existential types passing
  - Iso-existential types

- Typed closure conversion
  - Environment passing
  - Closure passing
Closure conversion

First-class functions may appear in the body of other functions. hence, their own body may contain free variables that will be bound to values during the evaluation in the execution environment.

Because they can be returned as values, and thus used outside of their definition environment, they must store their execution environment in their value.

A *closure* is the packaging of the code of a first-class function with its runtime environment, so that it becomes closed, *i.e.* independent of the runtime environment and can be moved and applied in another runtime environment.

Closures can also be used to represent recursive functions and objects (in the object-as-record-of-methods paradigm).
Source and target

In the following,

- the *source* calculus has *unary* $\lambda$-abstractions, which can have free variables;
- the *target* calculus has *binary* $\lambda$-abstractions, which must be *closed*.  

Closure conversion can be easily extended to n-ary functions, or n-ary functions may be *uncurried* in a separate, type-preserving compilation pass.
Variants of closure conversion

There are at least two variants of closure conversion:

- in the **closure-passing variant**, the closure and the environment are a single memory block;
- in the **environment-passing variant**, the environment is a separate block, to which the closure points.

The impact of this choice on the translation of terms is minor.

Its impact on the translation of types is more important: the closure-passing variant requires more type-theoretic machinery.
Closure-passing closure conversion

Let \( \{x_1, \ldots, x_n\} \) be \( \text{fv}(\lambda x. a) \):

\[
\begin{align*}
\llbracket \lambda x. a \rrbracket & = \text{let } code = \lambda (clo, x). \\
& \quad \text{let } (_, x_1, \ldots, x_n) = clo \text{ in } \llbracket a \rrbracket \text{ in} \\
& \quad (code, x_1, \ldots, x_n) \\

\llbracket a_1 \ a_2 \rrbracket & = \text{let } clo = \llbracket a_1 \rrbracket \text{ in} \\
& \quad \text{let } code = \text{proj}_0 \ clo \text{ in} \\
& \quad code (clo, \llbracket a_2 \rrbracket)
\end{align*}
\]

(The variables \( code \) and \( clo \) must be suitably fresh.)
Closure-passing closure conversion

Let \( \{x_1, \ldots, x_n\} \) be \( \operatorname{fv}(\lambda x. a) \):

\[
\begin{align*}
[\lambda x. a] &= \ \text{let code} = \lambda(clo, x). \\
& \quad \text{let } (\_, x_1, \ldots, x_n) = clo \text{ in } [a] \text{ in} \\
& \quad (\text{code}, x_1, \ldots, x_n)
\end{align*}
\]

\[
\begin{align*}
[a_1 \ a_2] &= \ \text{let } clo = [a_1] \text{ in} \\
& \quad \text{let code} = \text{proj}_0 \ clo \text{ in} \\
& \quad \text{code } (clo, [a_2])
\end{align*}
\]

Important! The layout of the environment must be known only at the closure allocation site, not at the call site. In particular, \( \text{proj}_0 \ clo \) need not know the size of \( clo \).
Environment-passing closure conversion

Let \( \{x_1, \ldots, x_n\} \) be \( \text{fv}(\lambda x. a) \):

\[
\left[ \lambda x. a \right] = \text{let } \text{code} = \lambda (env, x). \\
\quad \text{let } (x_1, \ldots, x_n) = env \text{ in } [a] \text{ in } \\
\quad (\text{code}, (x_1, \ldots, x_n))
\]

\[
\left[ a_1 \ a_2 \right] = \text{let } (\text{code}, env) = [a_1] \text{ in } \\
\quad \text{code } (env, [a_2])
\]
Environment-passing closure conversion

Let \( \{x_1, \ldots, x_n\} \) be \( \text{fv}(\lambda x. a) \):

\[
\left[ \lambda x. a \right] = \text{let } \text{code} = \lambda (env, x). \\
\text{let } (x_1, \ldots, x_n) = env \text{ in } \left[ a \right] \text{ in} \\
(\text{code}, (x_1, \ldots, x_n))
\]

\[
\left[ a_1 \ a_2 \right] = \text{let } (\text{code}, env) = \left[ a_1 \right] \text{ in} \\
\text{code} (env, \left[ a_2 \right])
\]

Questions: How can closure conversion be made \textit{type-preserving}?
Environment-passing closure conversion

Let \( \{x_1, \ldots, x_n\} \) be \( \text{fv}(\lambda x. a) \):

\[
\left\lfloor \lambda x. a \right\rfloor = \text{let code} = \lambda(env, x). \text{let (x_1, \ldots, x_n) = env in a in} \\
\text{(code, (x_1, \ldots, x_n))}
\]

\[
\left\lfloor a_1 a_2 \right\rfloor = \text{let (code, env) = a_1 in} \\
\text{code (env, a_2)}
\]

Questions: How can closure conversion be made type-preserving?

The key issue is to find a sensible definition of the type translation. In particular, what is the translation of a function type, \( \left\lfloor \tau_1 \rightarrow \tau_2 \right\rfloor \)?
Environment-passing closure conversion

Let \( \{x_1, \ldots, x_n\} \) be \( \text{fv}(\lambda x. a) \):

\[
\begin{align*}
\llbracket \lambda x. a \rrbracket &= \text{let code} = \lambda (env, x). \\
& \quad \text{let } (x_1, \ldots, x_n) = env \text{ in } \llbracket a \rrbracket \text{ in} \\
& \quad (\text{code}, (x_1, \ldots, x_n))
\end{align*}
\]

Assume \( \Gamma \vdash \lambda x. a : \tau_1 \rightarrow \tau_2 \).
Assume, \( w.l.o.g. \) \( \text{dom}(\Gamma) = \text{fv}(\lambda x. a) = \{x_1, \ldots, x_n\} \).

Write \( \llbracket \Gamma \rrbracket \) for the tuple type \( x_1 : \llbracket \tau'_1 \rrbracket ; \ldots ; x_n : \llbracket \tau'_n \rrbracket \) where \( \Gamma \) is \( x_1 : \tau'_1 ; \ldots ; x_n : \tau'_n \). We also use \( \llbracket \Gamma \rrbracket \) as a type to mean \( \llbracket \tau'_1 \rrbracket \times \ldots \times \llbracket \tau'_n \rrbracket \).

We have \( \Gamma, x : \tau_1 \vdash a : \tau_2 \), so in environment \( \llbracket \Gamma \rrbracket, x : \llbracket \tau_1 \rrbracket \), we have

- \( \text{env} \) has type \( \llbracket \Gamma \rrbracket \),
- \( \text{code} \) has type \( (\llbracket \Gamma \rrbracket \times \llbracket \tau_1 \rrbracket ) \rightarrow \llbracket \tau_2 \rrbracket \), and
- the entire closure has type \( ((\llbracket \Gamma \rrbracket \times \llbracket \tau_1 \rrbracket ) \rightarrow \llbracket \tau_2 \rrbracket ) \times \llbracket \Gamma \rrbracket \).

Now, \textbf{what should be the definition of} \( \llbracket \tau_1 \rightarrow \tau_2 \rrbracket \)?
Towards a type translation

Can we adopt this as a definition?

\[
\text{⟦τ}_1 \rightarrow \text{τ}_2 \text{⟧} = (\left(\left(\left[\text{Γ} \times \text{⟦τ}_1 \text{⟧}\right) \rightarrow \text{⟦τ}_2 \text{⟧}\right) \times \left[\text{Γ}\right]\right)
\]
Towards a type translation

Can we adopt this as a definition?

\[
\llbracket \tau_1 \to \tau_2 \rrbracket = (\llbracket \Gamma \times \tau_1 \rrbracket \to \llbracket \tau_2 \rrbracket) \times \llbracket \Gamma \rrbracket
\]

Naturally not. This definition is mathematically ill-formed: we cannot use \( \Gamma \) out of the blue.

Hmm... Do we really need to have a uniform translation of types?
Towards a type translation

Yes, we do.
Towards a type translation

Yes, we do.

*We need a uniform translation of types*, not just because it is nice to have one, but because it describes a *uniform calling convention*.

If closures with distinct environment sizes or layouts receive distinct types, then we will be unable to translate this well-typed code:
Towards a type translation

Yes, we do.

We need a uniform translation of types, not just because it is nice to have one, but because it describes a uniform calling convention.

If closures with distinct environment sizes or layouts receive distinct types, then we will be unable to translate this well-typed code:

\[
\text{if } \ldots \text{ then } \lambda x. x + y \text{ else } \lambda x. x
\]

Furthermore, we want function invocations to be translated uniformly, without knowledge of the size and layout of the closure’s environment.
Towards a type translation

Yes, we do.

*We need a uniform translation of types*, not just because it is nice to have one, but because it describes a *uniform calling convention*.

If closures with distinct environment sizes or layouts receive distinct types, then we will be unable to translate this well-typed code:

\[
\text{if } \ldots \text{ then } \lambda x. x + y \text{ else } \lambda x. x
\]

Furthermore, we want function invocations to be translated uniformly, without knowledge of the size and layout of the closure’s environment.

So, *what could be the definition of \( [\tau_1 \rightarrow \tau_2] \)?*
The type translation

The only sensible solution is:

\[
\llbracket \tau_1 \to \tau_2 \rrbracket = \exists \alpha. ((\alpha \times \llbracket \tau_1 \rrbracket) \to \llbracket \tau_2 \rrbracket) \times \alpha
\]

An *existential quantification* over the type of the environment abstracts away the differences in size and layout.

Enough information is retained to ensure that the application of the code to the environment is valid: this is expressed by letting the variable \( \alpha \) occur twice on the right-hand side.
The type translation

The existential quantification also provides a form of security: the caller cannot do anything with the environment except pass it as an argument to the code; in particular, it cannot inspect or modify the environment.

For instance, in the source language, the following coding style guarantees that $x$ remains even, no matter how $f$ is used:

$$
\text{let } f = \text{let } x = \text{ref } 0 \text{ in } \lambda(). x := (x + 2);!x
$$

After closure conversion, the reference $x$ is reachable via the closure of $f$. A malicious, untyped client could write an odd value to $x$. However, a well-typed client is unable to do so.

This encoding is not just type-preserving, but also fully abstract: it preserves (a typed version of) observational equivalence [Ahmed and Blume, 2008].
Contents

- Introduction

- Towards typed closure conversion

- Existential types
  - Implicitly-type existential types passing
  - Iso-existential types

- Typed closure conversion
  - Environment passing
  - Closure passing
Existential types

One can extend System F with *existential types*, in addition to universals:

$$\tau ::= \ldots | \exists \alpha . \tau$$

As in the case of universals, there are *type-passing* and *type-erasing* interpretations of the terms and typing rules... and in the latter interpretation, there are *explicit* and *implicit* versions.

Let’s just look at the type-erasing interpretation, with an explicit notation for introducing and eliminating existential types.
Existential types in explicit style

Here is how the existential quantifier is introduced and eliminated:

\[
\begin{align*}
\text{PACK} & \quad \Gamma \vdash M : [\alpha \mapsto \tau'] \tau \\
& \quad \Gamma \vdash \text{pack } \tau', M \text{ as } \exists \alpha. \tau : \exists \alpha. \tau \\
\text{UNPACK} & \quad \Gamma \vdash M_1 : \exists \alpha. \tau_1 \\
& \quad \Gamma, \alpha, x : \tau_1 \vdash M_2 : \tau_2 \\
& \quad \Gamma \vdash \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 : \tau_2
\end{align*}
\]
Existential types in explicit style

Here is how the existential quantifier is introduced and eliminated:

**Pack**
\[
\Gamma \vdash \text{Pack } \tau', M \quad \frac{\Gamma \vdash M : [\alpha \mapsto \tau']\tau}{\Gamma \vdash \text{pack } \tau', M \text{ as } \exists \alpha. \tau : \exists \alpha. \tau}
\]

**Unpack**
\[
\Gamma \vdash M_1 : \exists \alpha. \tau_1 \\
\Gamma, \alpha, x : \tau_1 \vdash M_2 : \tau_2 \\
\Gamma \vdash \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 : \tau_2
\]

Anything wrong?
Existential types in explicit style

Here is how the existential quantifier is introduced and eliminated:

\[
\begin{align*}
\text{Pack} & \quad \frac{\Gamma \vdash M : [\alpha \mapsto \tau']\tau}{\Gamma \vdash \text{pack } \tau', M \text{ as } \exists \alpha. \tau : \exists \alpha. \tau} \\
\text{Unpack} & \quad \frac{\Gamma \vdash M_1 : \exists \alpha. \tau_1}{\Gamma, \alpha, x : \tau_1 \vdash M_2 : \tau_2 \quad \alpha \not\equiv \tau_2} \frac{\Gamma \vdash \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 : \tau_2}{\Gamma \vdash \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 : \tau_2}
\end{align*}
\]

The side condition \( \alpha \not\equiv \tau_2 \) is mandatory here to ensure well-formedness of the conclusion.

The side condition may also be written \( \Gamma \vdash \tau_2 \) which implies \( \alpha \not\equiv \tau_2 \), given that the well-formedness of the last premise implies \( \alpha \not\in \text{dom}(\Gamma) \).
Existential types in explicit style

Here is how the existential quantifier is introduced and eliminated:

**Pack**
\[ \Gamma \vdash M : [\alpha \mapsto \tau'] \tau \]
\[ \Gamma \vdash \text{pack } \tau', M \text{ as } \exists \alpha. \tau : \exists \alpha. \tau \]

**Unpack**
\[ \Gamma \vdash M_1 : \exists \alpha. \tau_1 \]
\[ \Gamma, \alpha, x : \tau_1 \vdash M_2 : \tau_2 \]
\[ \alpha \not\# \tau_2 \]
\[ \Gamma \vdash \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 : \tau_2 \]

The side condition \( \alpha \not\# \tau_2 \) is mandatory here to ensure well-formedness of the conclusion.

The side condition may also be written \( \Gamma \vdash \tau_2 \) which implies \( \alpha \not\# \tau_2 \), given that the well-formedness of the last premise implies \( \alpha \notin \text{dom}(\Gamma) \).

Note the *imperfect duality* between universals and existentials:

**T\text{Abs}**
\[ \Gamma, \alpha \vdash M : \tau \]
\[ \Gamma \vdash \Lambda \alpha. M : \forall \alpha. \tau \]

**T\text{App}**
\[ \Gamma \vdash M : \forall \alpha. \tau \]
\[ \Gamma \vdash M \tau' : [\alpha \mapsto \tau'] \tau \]
On existential elimination

It would be nice to have a simpler elimination form, perhaps like this:

\[
\Gamma, \alpha \vdash M : \exists \alpha. \tau \\
\Gamma, \alpha \vdash \text{unpack } M : \tau
\]

Informally, this could mean that, if \( M \) has type \( \tau \) for some unknown \( \alpha \), then it has type \( \tau \), where \( \alpha \) is “fresh”...

Why is this broken?
On existential elimination

It would be nice to have a simpler elimination form, perhaps like this:

\[
\frac{\Gamma, \alpha \vdash M : \exists \alpha.\tau}{\Gamma, \alpha \vdash \text{unpack } M : \tau}
\]

Informally, this could mean that, if \( M \) has type \( \tau \) for some unknown \( \alpha \), then it has type \( \tau \), where \( \alpha \) is “fresh”...

Why is this broken?

We can immediately \textit{universally} quantify over \( \alpha \), and conclude that \( \Gamma \vdash \Lambda \alpha.\text{unpack } M : \forall \alpha.\tau \). This is nonsense!

Replacing the premise \( \Gamma, \alpha \vdash M : \exists \alpha.\tau \) by the conjunction \( \Gamma \vdash M : \exists \alpha.\tau \) and \( \alpha \in \text{dom}(\Gamma) \) would make the rule even more permissive, so it wouldn’t help.
On existential elimination

A correct elimination rule must force the existential package to be *used* in a way that does not rely on the value of $\alpha$.

Hence, the elimination rule must have control over the *user* of the package – that is, over the term $M_2$.

$$\text{UNPACK}$$

\[
\begin{align*}
\Gamma & \vdash M_1 : \exists \alpha. \tau_1 \\
\Gamma, \alpha; x : \tau_1 & \vdash M_2 : \tau_2 \\
\alpha \neq \tau_2 \\
\Gamma & \vdash \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 : \tau_2
\end{align*}
\]

The restriction $\alpha \neq \tau_2$ prevents writing "let $\alpha, x = \text{unpack } M_1 \text{ in } x"$, which would be equivalent to the unsound "unpack $M" of previous slide.

The fact that $\alpha$ is bound within $M_2$ forces it to be treated abstractly.

In fact, $M_2$ must be $???$ in $\alpha$. 

\[
\alpha \neq \tau_2
\]
On existential elimination

In fact, $M_2$ must be *polymorphic* in $\alpha$: the rule could be written

$$
\Gamma \vdash M_1 : \exists \alpha. \tau_1 \quad \Gamma \vdash \Lambda \alpha. \lambda x. M_2 : \forall \alpha. \tau_1 \to \tau_2 \quad \alpha \not\# \tau_2
$$

\[ \Gamma \vdash \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 : \tau_2 \]

or, if $N_2$ is $\Lambda \alpha. \lambda x. M_2$:

$$
\Gamma \vdash M_1 : \exists \alpha. \tau_1 \quad \Gamma \vdash N_2 : \forall \alpha. \tau_1 \to \tau_2 \quad \alpha \not\# \tau_2
$$

\[ \Gamma \vdash \text{unpack } M_1 \ N_2 : \tau_2 \]
On existential elimination

In fact, $M_2$ must be *polymorphic* in $\alpha$: the rule could be written

$$
\Gamma \vdash M_1 : \exists \alpha.\tau_1 \quad \Gamma \vdash \Lambda \alpha. \lambda x. M_2 : \forall \alpha. \tau_1 \rightarrow \tau_2 \quad \alpha \not\equiv \tau_2 \\
\Gamma \vdash \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 : \tau_2
$$

or, if $N_2$ is $\Lambda \alpha. \lambda x. M_2$:

$$
\Gamma \vdash M_1 : \exists \alpha.\tau_1 \quad \Gamma \vdash N_2 : \forall \alpha. \tau_1 \rightarrow \tau_2 \quad \alpha \not\equiv \tau_2 \\
\Gamma \vdash \text{unpack } M_1 \ N_2 : \tau_2
$$

One could even view "$\text{unpack}_{\exists \alpha.\tau_1}$" as a *constant* with all these types:

$$
\text{unpack}_{\exists \alpha.\tau_1} : (\exists \alpha.\tau_1) \rightarrow (\forall \alpha. (\tau_1 \rightarrow \tau_2)) \rightarrow \tau_2 \quad \alpha \not\equiv \tau_2
$$
On existential elimination

In fact, $M_2$ must be *polymorphic* in $\alpha$: the rule could be written

$$
\Gamma \vdash M_1 : \exists \alpha. \tau_1 \quad \Gamma \vdash \Lambda \alpha. \lambda x. M_2 : \forall \alpha. \tau_1 \rightarrow \tau_2 \quad \alpha \nmid \tau_2
$$

$$
\Gamma \vdash \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 : \tau_2
$$

or, if $N_2$ is $\Lambda \alpha. \lambda x. M_2$:

$$
\Gamma \vdash M_1 : \exists \alpha. \tau_1 \quad \Gamma \vdash N_2 : \forall \alpha. \tau_1 \rightarrow \tau_2 \quad \alpha \nmid \tau_2
$$

$$
\Gamma \vdash \text{unpack } M_1 \; N_2 : \tau_2
$$

One could even view “$\text{unpack}_{\exists \alpha. \tau_1}$” as a *constant* with all these types:

$$
\text{unpack}_{\exists \alpha. \tau_1} : \ (\exists \alpha. \tau_1) \rightarrow (\forall \alpha. (\tau_1 \rightarrow \tau_2)) \rightarrow \tau_2 \quad \alpha \nmid \tau_2
$$

Thus,

$$
\text{unpack}_{\exists \alpha. \tau} : \ \forall \beta. ((\exists \alpha. \tau) \rightarrow (\forall \alpha. (\tau \rightarrow \beta)) \rightarrow \beta)
$$
On existential elimination

In fact, $M_2$ must be *polymorphic* in $\alpha$: the rule could be written

\[
\frac{\Gamma \vdash M_1 : \exists \alpha. \tau_1}{\Gamma \vdash \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 : \tau_2}
\]

or, if $N_2$ is $\Lambda \alpha. \lambda x. M_2$:

\[
\frac{\Gamma \vdash M_1 : \exists \alpha. \tau_1 \quad \Gamma \vdash N_2 : \forall \alpha. \tau_1 \to \tau_2}{\Gamma \vdash \text{unpack } M_1 \ N_2 : \tau_2}
\]

One could even view "unpack$_{\exists \alpha. \tau_1}$" as a *constant* with all these types:

\[
\text{unpack}_{\exists \alpha. \tau_1} : (\exists \alpha. \tau_1) \to (\forall \alpha. (\tau_1 \to \tau_2)) \to \tau_2 \quad \alpha \not\# \tau_2
\]

Thus, \[\text{unpack}_{\exists \alpha. \tau} : \forall \beta. ((\exists \alpha. \tau) \to (\forall \alpha. (\tau \to \beta)) \to \beta)\]

or, better \[\text{unpack}_{\exists \alpha. \tau} : (\exists \alpha. \tau) \to \forall \beta. ((\forall \alpha. (\tau \to \beta)) \to \beta)\]

$\beta$ stands for $\tau_2$: it is bound prior to $\alpha$, so it cannot be instantiated to a type that refers to $\alpha$, which reflects the side condition $\alpha \not\# \tau_2$. 
On existential introduction

\[
\text{Pack} \\
\Gamma \vdash M : [\alpha \mapsto \tau']\tau \\
\Gamma \vdash \text{pack } \tau', M \text{ as } \exists \alpha. \tau : \exists \alpha. \tau
\]

If desired, “pack}_{\exists \alpha. \tau}” could also be viewed as a \textit{constant} with all the types:

\[
\text{pack}_{\exists \alpha. \tau} : \quad [\alpha \mapsto \tau']\tau \rightarrow \exists \alpha. \tau
\]

\textit{i.e.} with polymorphic type:

\[
\text{pack}_{\exists \alpha. \tau} : \quad \forall \alpha. (\tau \rightarrow \exists \alpha. \tau)
\]
Existentials as constants

In System F, existential types can also be presented as constants

\[
\text{pack}_{\exists \alpha. \tau} : \forall \alpha. (\tau \rightarrow \exists \alpha. \tau) \\
\text{unpack}_{\exists \alpha. \tau} : \exists \alpha. \tau \rightarrow \forall \beta. ((\forall \alpha. (\tau \rightarrow \beta)) \rightarrow \beta)
\]

Read:

- for any \( \alpha \), if you have a \( \tau \), then, for some \( \alpha \), you have a \( \tau \);
- if, for some \( \alpha \), you have a \( \tau \), then, (for any \( \beta \),) if you wish to obtain a \( \beta \) out of it, then you must present a function which, for any \( \alpha \), obtains a \( \beta \) out of a \( \tau \).

This is somewhat reminiscent of ordinary first-order logic:

\( \exists x. F \) is equivalent to, and can be defined as, \( \neg (\forall x. \neg F) \).

Is there an encoding of existential types into universal types?
Encoding existentials into universals

The type translation is *double negation*:

\[
\left[\exists \alpha. \tau\right] = \forall \beta. ((\forall \alpha. ([\tau] \rightarrow \beta)) \rightarrow \beta) \quad \text{if } \beta \neq \tau
\]

The term translation is:

\[
\left[\text{pack}_{\exists \alpha. \tau}\right] : \forall \alpha. ([\tau] \rightarrow [\exists \alpha. \tau])
\]

\[= ?
\]

\[
\left[\text{unpack}_{\exists \alpha. \tau}\right] : [\exists \alpha. \tau] \rightarrow \forall \beta. ((\forall \alpha. ([\tau] \rightarrow \beta)) \rightarrow \beta)
\]

\[= ?
\]
Encoding existentials into universals

The type translation is *double negation*:

\[
[\exists \alpha. \tau] = \forall \beta. ((\forall \alpha. ([\tau] \to \beta)) \to \beta) \quad \text{if } \beta \neq \tau
\]

The term translation is:

\[
\begin{align*}
\llbracket \text{pack}_{\exists \alpha. \tau} \rrbracket &: \forall \alpha. ([\tau] \to [\exists \alpha. \tau]) \\
&= \Lambda \alpha. \lambda x: [\tau]. \Lambda \beta. \lambda k: \forall \alpha. ([\tau] \to \beta). ? : \beta \\
\llbracket \text{unpack}_{\exists \alpha. \tau} \rrbracket &: [\exists \alpha. \tau] \to \forall \beta. ((\forall \alpha. ([\tau] \to \beta)) \to \beta) \\
&= ?
\end{align*}
\]
Encoding existentials into universals

The type translation is *double negation:*

\[ [\exists \alpha. \tau] = \forall \beta. ((\forall \alpha. ([\tau] \rightarrow \beta)) \rightarrow \beta) \quad \text{if } \beta \neq \tau \]

The term translation is:

\[ [\text{pack}_{\exists \alpha. \tau}] : \forall \alpha. ([\tau] \rightarrow [\exists \alpha. \tau]) \]
\[ = \Lambda \alpha. \lambda x: [\tau]. \Lambda \beta. \lambda k: \forall \alpha. ([\tau] \rightarrow \beta). k \alpha x \]

\[ [\text{unpack}_{\exists \alpha. \tau}] : [\exists \alpha. \tau] \rightarrow \forall \beta. ((\forall \alpha. ([\tau] \rightarrow \beta)) \rightarrow \beta) \]
\[ = ? \]
Encoding existentials into universals

The type translation is *double negation*:

$$\llbracket \exists \alpha. \tau \rrbracket = \forall \beta. ((\forall \alpha. (\llbracket \tau \rrbracket \rightarrow \beta)) \rightarrow \beta) \quad \text{if } \beta \not\equiv \tau$$

The term translation is:

$$\llbracket \text{pack}_{\exists \alpha. \tau} \rrbracket : \forall \alpha. (\llbracket \tau \rrbracket \rightarrow \llbracket \exists \alpha. \tau \rrbracket) = \Lambda \alpha. \lambda x: \llbracket \tau \rrbracket. \Lambda \beta. \lambda k: \forall \alpha. (\llbracket \tau \rrbracket \rightarrow \beta). k \alpha x$$

$$\llbracket \text{unpack}_{\exists \alpha. \tau} \rrbracket : \llbracket \exists \alpha. \tau \rrbracket \rightarrow \forall \beta. ((\forall \alpha. (\llbracket \tau \rrbracket \rightarrow \beta)) \rightarrow \beta) = \lambda x: \llbracket \exists \alpha. \tau \rrbracket. x$$

There is little choice, if the translation is to be type-preserving.

What is the computational content of this encoding?
Encoding existentials into universals

The type translation is \textit{double negation}:

\[
\llbracket \exists \alpha. \tau \rrbracket = \forall \beta. ((\forall \alpha. (\llbracket \tau \rrbracket \rightarrow \beta)) \rightarrow \beta) \quad \text{if } \beta \neq \tau
\]

The term translation is:

\[
\llbracket \text{pack}_{\exists \alpha. \tau} \rrbracket : \forall \alpha. (\llbracket \tau \rrbracket \rightarrow \llbracket \exists \alpha. \tau \rrbracket)
= \Lambda \alpha. \lambda x : [\tau]. \Lambda \beta. \lambda k : \forall \alpha. ([\tau] \rightarrow \beta). k \alpha x
\]

\[
\llbracket \text{unpack}_{\exists \alpha. \tau} \rrbracket : \llbracket \exists \alpha. \tau \rrbracket \rightarrow \forall \beta. ((\forall \alpha. (\llbracket \tau \rrbracket \rightarrow \beta)) \rightarrow \beta)
= \lambda x : [\exists \alpha. \tau]. x
\]

There is little choice, if the translation is to be type-preserving.

What is the computational content of this encoding?

A \textit{continuation-passing transform}.

This encoding is due to Reynolds [1983], although it has more ancient roots in logic.
The semantics of existential types

pack_{\exists \alpha. \tau} can be treated as a unary constructor, and unpack_{\exists \alpha. \tau} as a unary destructor. The $\delta$-reduction rule is:

$$\text{unpack}_{\exists \alpha. \tau_0} (\text{pack}_{\exists \alpha. \tau} \tau' V) \rightarrow \Lambda \beta. \lambda y: \forall \alpha. \tau \rightarrow \beta. y \tau' V$$

It would be more intuitive, however, to treat $\text{unpack}_{\exists \alpha. \tau_0}$ as a binary destructor:

$$\text{unpack}_{\exists \alpha. \tau_0} (\text{pack}_{\exists \alpha. \tau} \tau' V) \tau_1 (\Lambda \alpha. \lambda x: \tau. M) \rightarrow [\alpha \mapsto \tau'] [x \mapsto V] M$$

This does not quite fit in our generic framework for constants, which must receive all type arguments prior to value arguments.

But our framework could be extended.
The semantics of existential types

We extend values and evaluation contexts as follows:

\[
V ::= \ldots \text{pack } \tau', V \text{ as } \tau \\
E ::= \ldots \text{pack } \tau', [] \text{ as } \tau \mid \text{let } \alpha, x = \text{unpack } [] \text{ in } M
\]

We add the reduction rule:

\[
\text{let } \alpha, x = \text{unpack } (\text{pack } \tau', V \text{ as } \tau) \text{ in } M \rightarrow [\alpha \mapsto \tau'][x \mapsto V]M
\]

Exercise

Show that subject reduction and progress hold.
The semantics of existential types

The reduction rule for existentials destructs its arguments.

Hence, \( \text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 \) cannot be reduced unless \( M_1 \) is itself a packed expression, which is indeed the case when \( M_1 \) is a value (or in head normal form).

This contrasts with \( \text{let } x : \tau = M_1 \text{ in } M_2 \) where \( M_1 \) need not be evaluated and may be an application (e.g. with call-by-name or strong reduction strategies).
The semantics of existential types

Exercise

Find an example that illustrates why the reduction of 
let $\alpha, x = \text{unpack } M_1 \text{ in } M_2$ could be problematic when $M_1$ is not a value.
The semantics of existential types

Exercise

*Find an example that illustrates why the reduction of*

\[
\text{let } \alpha, x = \text{unpack } M_1 \text{ in } M_2 \text{ could be problematic when } M_1 \text{ is not a value.}
\]

*Need a hint?*

*Use a conditional*
The semantics of existential types

Exercise

Find an example that illustrates why the reduction of let $\alpha, x =$ unpack $M_1$ in $M_2$ could be problematic when $M_1$ is not a value.

Solution

Let $M_1$ be if $M$ then $V_1$ else $V_2$ where $V_i$ is of the form \texttt{pack $\tau_i$, $V_i$ as $\exists \alpha. \tau$} and the two witnesses $\tau_1$ and $\tau_2$ differ.

There is no common type for the unpacking of the two possible results $V_1$ and $V_2$. The choice between those two possible results must be made, by evaluating $M_1$, before unpacking.
Is pack too verbose?

Exercise

Recall the typing rule for pack:

\[ \Gamma \vdash M : [\alpha \mapsto \tau']\tau \]

\[ \Gamma \vdash \text{pack } \tau', M \text{ as } \exists \alpha. \tau : \exists \alpha. \tau \]

Isn't the witness type \( \tau' \) annotation superfluous?
Is pack too verbose?

Exercise

*Recall the typing rule for pack:*

\[
\Gamma \vdash M : [\alpha \mapsto \tau']\tau \\
\Gamma \vdash \text{pack } \tau', M \text{ as } \exists \alpha. \tau : \exists \alpha.\tau
\]

*Isn’t the witness type \( \tau' \) annotation superfluous?*

- The type \( \tau_0 \) of \( M \) is fully determined by \( M \). Given the type \( \exists \alpha.\tau \) of the packed value, checking that \( \tau_0 \) is of the form \([\alpha \mapsto \tau']\tau\) is the matching problem for second-order types, which is simple.
- However, the reduction rule need the witness type \( \tau' \). If it were not available, it would have to be computed during reduction. The reduction rule would then not be pure rewriting.

The explicitly-typed language need the witness type for simplicity, while in the surface language, it could be omitted and reconstructed.
• Introduction

• Towards typed closure conversion

• Existential types
  • Implicitly-type existential types passing
  • Iso-existential types

• Typed closure conversion
  • Environment passing
  • Closure passing
Implicitly-typed existential types

Intuitively, pack and unpack are just type annotations that could be dropped, leaving a let-binding instead of the unpack form.

Hence, the typing rule for implicitly-typed existential types:

\[
\text{Unpack} \quad \begin{array}{c}
\Gamma \vdash a_1 : \exists \alpha. \tau_1 \\
\Gamma, \alpha, x : \tau_1 \vdash a_2 : \tau_2 \\
\alpha \not\equiv \tau_2
\end{array} \quad \Gamma \vdash \text{let } x = a_1 \text{ in } a_2 : \tau_2
\]

\[
\text{Pack} \quad \begin{array}{c}
\Gamma \vdash a : [\alpha \mapsto \tau']\tau
\end{array} \quad \Gamma \vdash a : \exists \alpha. \tau
\]

Notice, however, that this let-binding is not typechecked as syntactic sugar for an immediate application!

The semantics of this let-binding is as before:

\[
E ::= \ldots | \text{let } x = E \text{ in } M \\
\text{let } x = V \text{ in } M \rightarrow [x \mapsto V]M
\]

Is the semantics type-erasing?
Implicitle-typed existential types

Yes, it is.

But there is a subtlety!
Yes, it is.

But there is a subtlety! What about the call-by-name semantics?
Implicitly-typed existential types

Yes, it is.

But there is a subtlety! What about the call-by-name semantics?

We chose a call-by-value semantics, but so far, as long as there is no side-effect, we could have chosen a call-by-name semantics (or even perform reduction under abstraction).

In a call-by-name semantics, the let-bound expression is not reduced prior to substitution in the body:

\[
\text{let } x = M_1 \text{ in } M_2 \longrightarrow [x \mapsto M_1]M_2
\]

With existential types, this breaks subject reduction!

Why?
Implicitly-typed existential types

Let $\tau_0$ be $\exists \alpha. (\alpha \to \alpha) \to (\alpha \to \alpha)$ and $v_0$ a value of type $bool$. Let $v_1$ and $v_2$ be two values of type $\tau_0$ with incompatible witness types, e.g. $\lambda f. \lambda x. 1 + (f (1 + x))$ and $\lambda f. \lambda x. \text{not} (f \text{ not } x)$.

Let $v$ be the function $\lambda b. \text{if } b \text{ then } v_1 \text{ else } v_2$ of type $bool \to \tau_0$.

$$a_1 = \text{let } x = v v_0 \text{ in } x (x (\lambda y. y)) \quad \rightarrow \quad v v_0 (v v_0 (\lambda y. y)) = a_2$$

We have $\emptyset \vdash a_1 : \exists \alpha. \alpha \to \alpha$ while $\emptyset \nvdash a_2 : \tau$.

What happened?
Implicitly-typed existential types

Let $\tau_0$ be $\exists \alpha. (\alpha \to \alpha) \to (\alpha \to \alpha)$ and $v_0$ a value of type $bool$. Let $v_1$ and $v_2$ be two values of type $\tau_0$ with incompatible witness types, e.g. $\lambda f. \lambda x. 1 + (f (1 + x))$ and $\lambda f. \lambda x. not (f (not x))$.

Let $v$ be the function $\lambda b. if \ b \ then \ v_1 \ else \ v_2$ of type $bool \to \tau_0$.

\[ a_1 = let \ x = v \ v_0 \ in \ x \ (x \ (\lambda y. y)) \quad \to \quad v \ v_0 \ (v \ v_0 \ (\lambda y. y)) = a_2 \]

We have $\emptyset \vdash a_1 : \exists \alpha. \alpha \to \alpha$ while $\emptyset \not\vdash a_2 : \tau$.

The term $a_1$ is well-typed since $v \ v_0$ has type $\tau_0$, hence $x$ can be assumed of type $(\beta \to \beta) \to (\beta \to \beta)$ for some unknown type $\beta$ and $\lambda y. y$ is of type $\beta \to \beta$.

However, without the outer existential type $v \ v_0$ can only be typed with $(\forall \alpha. \alpha \to \alpha) \to \exists \alpha. (\alpha \to \alpha)$, because the value returned by the function need different witnesses for $\alpha$. This is demanding too much on its argument and the outer application is ill-typed.
Implicitly-typed existential types

One could wonder whether the syntax should not allow the implicit introduction of unpacking (instead of requesting a let-binding).

One could argue that if some expression is the expansion of a well-typed let-binding, then it should also be well-typed:

$$
\Gamma \vdash a_1 : \exists \alpha. \tau_1 \\
\Gamma, \alpha, x : \tau_1 \vdash a_2 : \tau_2 \\
\alpha \nmid \tau_2
$$

$$
\Gamma \vdash [x \mapsto a_1] a_2 : \tau_2
$$

Comments?
Implicitly-typed existential types

One could wonder whether the syntax should not allow the implicit introduction of unpacking (instead of requesting a let-binding).

One could argue that if some expression is the expansion of a well-typed let-binding, then it should also be well-typed:

\[
\frac{\Gamma \vdash a_1 : \exists \alpha. \tau_1 \quad \Gamma, \alpha, x : \tau_1 \vdash a_2 : \tau_2 \quad \alpha \not\equiv \tau_2}{\Gamma \vdash [x \mapsto a_1]a_2 : \tau_2}
\]

Comments:

- This rule does not have a logical flavor...
- It fixes the previous example, but not the general case:
  \( \text{Pick } a_1 \text{ that is not yet a value after one reduction step.} \)
  \( \text{Then, after let-expansion reduce, one of the two occurrences of } a_1. \)
  \( \text{The result is no longer of the form } [x \mapsto a_1]a_2. \)
Implicitly-typed existential types

Existential types are trickier than they may appear at first.

The subject reduction property breaks if reduction is not restricted to expressions in head-normal forms.

Unrestricted reduction is still safe because well-typedness may eventually be recovered by further reduction steps—so that progress will never break.
Implicitly-typed existential types

Notice that the CPS encoding of existential types (1) enforces the evaluation of the packed value (2) before it can be unpacked (3) and substituted (4):

\[
\llbracket\text{unpack } a_1 \ (\lambda x. a_2)\rrbracket = \llbracket a_1 \rrbracket \ (\lambda x. \llbracket a_2 \rrbracket) \quad (1)
\]

\[
\rightarrow (\lambda k. \llbracket a \rrbracket \ k) \ (\lambda x. \llbracket a_2 \rrbracket) \quad (2)
\]

\[
\rightarrow (\lambda x. \llbracket a_2 \rrbracket) \ [a] \quad (3)
\]

\[
\rightarrow [x \mapsto \llbracket a \rrbracket] \llbracket a_2 \rrbracket \quad (4)
\]

In the call-by-value setting, \( \lambda k. \llbracket a \rrbracket \ k \) would come from the reduction of \( \llbracket \text{pack } a \rrbracket \), i.e. is \( (\lambda k. \lambda x. k \ x) \ [a] \), so that \( a \) is always a value \( v \).

However, \( a \) need not be a value. What is essential is that \( a_1 \) be reduced to some head normal form \( \lambda k. \llbracket a \rrbracket \ k \).
### Introduction

- Towards typed closure conversion

### Existential types

- Implicitly-type existential types passing
- Iso-existential types

### Typed closure conversion

- Environment passing
- Closure passing
Iso-existential types in ML

What if one wished to extend ML with existential types?

Full type inference for existential types is undecidable, just like type inference for universals.

However, introducing existential types in ML is easy if one is willing to rely on user-supplied *annotations* that indicate where to pack and unpack.
Iso-existential types in ML

This iso-existential approach was suggested by Läufer and Odersky [1994].

Iso-existential types are explicitly declared:

\[ D \bar{\alpha} \approx \exists \bar{\beta}. \tau \quad \text{if } \text{ftv}(\tau) \subseteq \bar{\alpha} \cup \bar{\beta} \quad \text{and} \quad \bar{\alpha} \neq \bar{\beta} \]

This introduces two constants, with the following type schemes:

\[
\begin{align*}
\text{pack}_D & : \forall \bar{\alpha} \bar{\beta}. \tau \to D \bar{\alpha} \\
\text{unpack}_D & : \forall \bar{\alpha} \gamma. D \bar{\alpha} \to (\forall \bar{\beta}. (\tau \to \gamma)) \to \gamma
\end{align*}
\]

(Compare with basic iso-recursive types, where \( \bar{\beta} = \emptyset \).)
Iso-existential types in ML

A few corners have been cut on the previous slide. The “type scheme:”

$$\forall \bar{\alpha} \gamma. D \bar{\alpha} \to (\forall \bar{\beta}. (\tau \to \gamma)) \to \gamma$$

is in fact *not* an ML type scheme. How could we address this?
Iso-existential types in ML

A few corners have been cut on the previous slide. The “type scheme:”

\[ \forall \vec{\alpha} \gamma. D \vec{\alpha} \to (\forall \vec{\beta}. (\tau \to \gamma)) \to \gamma \]

is in fact not an ML type scheme. How could we address this?

A solution is to make \( \text{unpack}_D \) a binary construct again (rather than a constant), with an ad hoc typing rule:

\[
\frac{
\Gamma \vdash M_1 : D \vec{\tau}
\Gamma \vdash M_2 : \forall \vec{\beta}. ([\vec{\alpha} \mapsto \vec{\tau}] \tau \to \tau_2) \quad \vec{\beta} \not\# \vec{\tau}, \tau_2
}{\Gamma \vdash \text{unpack}_D M_1 M_2 : \tau_2}
\]

where \( D \vec{\alpha} \approx \exists \vec{\beta}. \tau \)

We have seen a version of this rule in System F earlier; this in an ML version. The term \( M_2 \) must be polymorphic, which \( \text{GEN} \) can prove.
Iso-existential types in ML

Iso-existential types are perfectly compatible with ML type inference.

The constant $\text{pack}_D$ admits an ML type scheme, so it is unproblematic.

The construct $\text{unpack}_D$ leads to this constraint generation rule (see type inference):

$$
\begin{aligned}
\langle \text{unpack}_D \ M_1 \ M_2 : \tau_2 \rangle &= \exists \bar{\alpha}. \left( \langle M_1 : D \bar{\alpha} \rangle \quad \forall \bar{\beta}. \langle M_2 : \tau \rightarrow \tau_2 \rangle \right)
\end{aligned}
$$

where $D \bar{\alpha} \approx \exists \bar{\beta}. \tau$ and, w.l.o.g., $\bar{\alpha}\bar{\beta} \not\equiv M_1, M_2, \tau_2$.

A universally quantified constraint appears where polymorphism is \textit{required}. 

Iso-existential types in ML

In practice, Läufer and Odersky suggest fusing iso-existential types with algebraic data types.

This can be done in OCaml using GADTs (see last part of the course). The (somewhat bizarre) syntax for this in OCaml is:

\[
type D \vec{\alpha} = \ell : \tau \rightarrow D \vec{\alpha}
\]

where \(\ell\) is a data constructor and \(\vec{\beta}\) appears free in \(\tau\) but does not appear in \(\vec{\alpha}\). The elimination construct becomes:

\[
\llangle \text{match } M_1 \text{ with } \ell \, x \rightarrow M_2 : \tau_2 \rrangle = \exists \vec{\alpha}. \left( \llangle M_1 : D \vec{\alpha} \rrangle \quad \forall \vec{\beta}. \text{def } x : \tau \text{ in } \llangle M_2 : \tau_2 \rrangle \right)
\]

where, w.l.o.g., \(\vec{\alpha} \vec{\beta} \notin M_1, M_2, \tau_2\).
An example

Define $\textbf{Any} \approx \exists \beta. \beta$. An attempt to extract the raw content of a package fails:

$$\braket{\text{unpack}_{\textbf{Any}} M_1 \ (\lambda x. \ x) : \tau_2} = \braket{M_1 : \textbf{Any}} \land \forall \beta. \braket{\lambda x. \ x : \beta \rightarrow \tau_2} \models \forall \beta. \beta = \tau_2 \equiv false$$

(Recall that $\beta \not\approx \tau_2$.)
An example

Define

\[ D \alpha \approx \exists \beta. (\beta \to \alpha) \times \beta \]

A client that regards \( \beta \) as abstract succeeds:

\[
\langle \text{unpack}_D \ M_1 \ (\lambda (f, y). f \ y) : \tau \rangle \\
= \exists \alpha. (\langle M_1 : D \alpha \rangle \land \forall \beta. \langle \lambda (f, y). f \ y : ((\beta \to \alpha) \times \beta) \to \tau \rangle) \\
= \exists \alpha. (\langle M_1 : D \alpha \rangle \land \forall \beta. \text{def } f : \beta \to \alpha; y : \beta \text{ in } \langle f \ y : \tau \rangle) \\
= \exists \alpha. (\langle M_1 : D \alpha \rangle \land \forall \beta. \tau = \alpha) \\
= \exists \alpha. (\langle M_1 : D \alpha \rangle \land \tau = \alpha) \\
= \langle M_1 : D \tau \rangle
\]
Existential types calls for universal types!

**Exercise** We reuse the type $D \alpha \approx \exists \beta. (\beta \rightarrow \alpha) \times \beta$ of frozen computations. Assume given a list $l$ with elements of type $D \tau_1$.

Assume given a function $g$ of type $\tau_1 \rightarrow \tau_2$. Transform the list into a new list $l'$ of frozen computations of type $D \tau_2$ (without actually running any computation).

$$\text{List.map } (\lambda (z) \text{ let } D(f, y) = z \text{ in } D((\lambda (z) g (f z)), y))$$

Generalizing this example to a function that receives $g$ and $l$ and returns $l'$ does not typecheck:

$$\text{let lift g l =}$$
$$\text{List.map } (\lambda (z) \text{ let } D(f, y) = z \text{ in } D((\lambda (z) g (f z)), y))$$

In expression `let $\alpha, x = \text{unpack } M_1 \text{ in } M_2$`, occurrences of $x$ in $M_2$ can only be passed to external functions (free variables) that are polymorphic so that $x$ does not leak out of its context.
Uses of existential types

Mitchell and Plotkin [1988] note that existential types offer a means of explaining *abstract types*. For instance, the type:

\[
\exists stack. \{ \text{empty} : stack; \\
\text{push} : int \times stack \rightarrow stack; \\
\text{pop} : stack \rightarrow \text{option} (int \times stack) \}\]

specifies an abstract implementation of integer stacks.

Unfortunately, it was soon noticed that the elimination rule is too awkward, and that existential types alone do not allow designing *module systems* [Harper and Pierce, 2005].

Montagu and Rémy [2009] make existential types *more flexible* in several important ways, and argue that they might explain modules after all.
Existential types in OCaml

Existential types are available indirectly in OCaml as a degenerate case of GADT and via abstract types and first-class modules.

Via GADT (iso-existential types)

\[
\begin{align*}
\text{type } 'a \_d & = D : ('b \rightarrow 'a) \times 'b \rightarrow 'a \_d \\
\text{let freeze } f \_x & = D (f, x) \\
\text{let run } (D (f, x)) & = f \_x
\end{align*}
\]

Via first-class modules (abstract types)

\[
\begin{align*}
\text{module type } D & = \text{sig type } b \text{ type } a \text{ val } f : b \rightarrow a \text{ val } x : b \text{ end} \\
\text{let freeze (type } u \text) (\text{type } v) f \_x & = \\
\quad (\text{module struct type } b = u \text{ type } a = v \text{ let } f = f \text{ let } x = x \text{ end : D});; \\
\text{let unfreeze (type } u \text) (\text{module } M : D \text{ with type } a = u) & = M.f M.x
\end{align*}
\]
Contents

- Introduction
- Towards typed closure conversion
- Existential types
  - Implicitly-type existential types passing
  - Iso-existential types
- Typed closure conversion
  - Environment passing
  - Closure passing
• Introduction

• Towards typed closure conversion

• Existential types
  • Implicitly-type existential types passing
  • Iso-existential types

• Typed closure conversion
  • Environment passing
  • Closure passing
Typed closure conversion

Everything is now set up to prove that, in System F with existential types:

\[ \Gamma \vdash M : \tau \quad \text{implies} \quad [\Gamma] \vdash [M] : [\tau] \]
Environment-passing closure conversion

Assume $\Gamma \vdash \lambda x. M : \tau_1 \to \tau_2$ and $\text{dom}(\Gamma) = \{x_1, \ldots, x_n\} = \text{fv}(\lambda x. M)$.

\[
\left[ \lambda x: \tau_1. M \right] = \text{let } code : \lambda (env: \ , x: \ ) . \text{let } (x_1, \ldots, x_n : \ ) = env \text{ in } \\
[ M ] \text{ in } pack , (code , (x_1, \ldots, x_n))\]
as
Environment-passing closure conversion

Assume $\Gamma \vdash \lambda x. M : \tau_1 \rightarrow \tau_2$ and $\text{dom}(\Gamma) = \{x_1, \ldots, x_n\} = \text{fv}(\lambda x. M)$.

\[
\llbracket \lambda x : \tau_1 . M \rrbracket = \text{let code : } \lambda (env : [\Gamma], x : [\tau_1]) .
\begin{align*}
&\text{let } (x_1, \ldots, x_n : [\Gamma]) = env \text{ in } \\
&\llbracket M \rrbracket \\
&\text{in } \text{pack }, (code, (x_1, \ldots, x_n)) \text{ as }
\end{align*}
\]
Environment-passing closure conversion

Assume $\Gamma \vdash \lambda x. M : \tau_1 \to \tau_2$ and $\text{dom}(\Gamma) = \{x_1, \ldots, x_n\} = \text{fv}(\lambda x. M)$.

$$\llbracket \lambda x : \tau_1 . M \rrbracket = \text{let code : } ([\Gamma] \times [\tau_1]) \to [\tau_2] =
\lambda (env : [\Gamma], x : [\tau_1]).
\text{let } (x_1, \ldots, x_n : [\Gamma]) = env \text{ in}
\llbracket M \rrbracket
\text{in}
pack , (code, (x_1, \ldots, x_n))$$
Environment-passing closure conversion

Assume $\Gamma \vdash \lambda x. M : \tau_1 \rightarrow \tau_2$ and $\text{dom}(\Gamma) = \{x_1, \ldots, x_n\} = \text{fv}(\lambda x. M)$.

$$\left[\lambda x: \tau_1. M\right] = \text{let code : } ([\Gamma] \times [\tau_1]) \rightarrow [\tau_2] =$$

$$\lambda (env : [\Gamma], x : [\tau_1]).$$

$$\text{let } (x_1, \ldots, x_n : [\Gamma]) = env \text{ in}$$

$$[M]$$

$$\text{in}$$

$$\text{pack } [\Gamma], (code, (x_1, \ldots, x_n))$$

$$\text{as } \exists \alpha.((\alpha \times [\tau_1]) \rightarrow [\tau_2]) \times \alpha$$
Environment-passing closure conversion

Assume $\Gamma \vdash \lambda x. M : \tau_1 \rightarrow \tau_2$ and $\text{dom}(\Gamma) = \{x_1, \ldots, x_n\} = \text{fv}(\lambda x. M)$. 

$$\llbracket \lambda x:\tau_1. M \rrbracket = \begin{array}{l}
\text{let code} : ([\Gamma] \times [\tau_1]) \rightarrow [\tau_2] = \\
\lambda (env : [\Gamma], x : [\tau_1]). \\
\text{let } (x_1, \ldots, x_n : [\Gamma]) = env \text{ in} \\
[\llbracket M \rrbracket] \\
\text{in} \\
\text{pack } [\Gamma], (\text{code}, (x_1, \ldots, x_n)) \\
\text{as } \exists \alpha.((\alpha \times [\tau_1]) \rightarrow [\tau_2]) \times \alpha
\end{array}$$

We find $\llbracket \Gamma \rrbracket \vdash \llbracket \lambda x:\tau_1. M \rrbracket : [\tau_1 \rightarrow \tau_2]$, as desired.
Environment-passing closure conversion

Assume $\Gamma \vdash M : \tau_1 \to \tau_2$ and $\Gamma \vdash M_1 : \tau_1$.

$$\llbracket M \ M_1 \rrbracket = \text{let } \alpha, \ (\text{code} : (\alpha \times \llbracket \tau_1 \rrbracket) \to \llbracket \tau_2 \rrbracket, \ env : \alpha) = \text{unpack} \llbracket M \rrbracket \text{ in}$$

$$\text{code} \ (env, \llbracket M_1 \rrbracket)$$

We find $\llbracket \Gamma \rrbracket \vdash \llbracket M \ M_1 \rrbracket : \llbracket \tau_2 \rrbracket$, as desired.
Environment-passing closure conversion

*Recursive functions* can be translated in this way, known as the “fix-code” variant [Morrisett and Harper, 1998] (leaving out type information):

\[
\llbracket \mu f. \lambda x. M \rrbracket = \text{let rec code (env, x) =} \\
\text{let } f = \text{pack (code, env) in} \\
\text{let } (x_1, \ldots, x_n) = \text{env in} \\
\llbracket M \rrbracket \text{ in} \\
\text{pack (code, (x_1, \ldots, x_n))}
\]

where \( \{x_1, \ldots, x_n\} = \text{fv}(\mu f. \lambda x. M) \).

The translation of applications is unchanged: recursive and non-recursive functions have an identical calling convention.

What is the weak point of this variant?
Recursive functions can be translated in this way, known as the “fix-code” variant [Morrisett and Harper, 1998] (leaving out type information):

\[
\left[ \mu f. \lambda x. M \right] = \text{let rec code (env, x) =}
\]
\[
\quad \text{let } f = \text{pack (code, env) in}
\]
\[
\quad \text{let } (x_1, \ldots, x_n) = \text{env in}
\]
\[
\left[ M \right] \text{ in}
\]
\[
\quad \text{pack (code, (x_1, \ldots, x_n))}
\]

where \( \{x_1, \ldots, x_n\} = \text{fv(} \mu f. \lambda x. M \text{)} \).

The translation of applications is unchanged: recursive and non-recursive functions have an identical calling convention.

What is the weak point of this variant?

A new closure is allocated at every call.
Instead, the “fix-pack” variant [Morrisett and Harper, 1998] uses an extra field in the environment to store a back pointer to the closure:

\[
\llbracket \mu f. \lambda x. M \rrbracket = \text{let code} = \lambda (env, x). \\
\text{let } (f, x_1, \ldots, x_n) = env \text{ in} \\
\llbracket M \rrbracket \\
in \\
\text{let rec } clo = (code, (clo, x_1, \ldots, x_n)) \text{ in} \\
clo
\]

where \( \{x_1, \ldots, x_n\} = \text{fv}(\mu f. \lambda x. M) \).

This requires general, recursively-defined \textit{values}. Closures are now \textit{cyclic} data structures.
Here is how the “fix-pack” variant is type-checked. Assume \( \Gamma \vdash \mu f. \lambda x. M : \tau_1 \rightarrow \tau_2 \) and \( \text{dom}(\Gamma) = \{x_1, \ldots, x_n\} = \text{fv}(\mu f. \lambda x. M) \).

\[
\begin{align*}
\llbracket \mu f \quad . \lambda x. M \rrbracket &= \quad \text{let code : } \lambda (env : \quad , x : \quad ). \quad \text{let (f, x_1, \ldots, x_n) : } \quad \llbracket M \rrbracket \quad \text{in} \quad \text{let rec clo : } \quad \text{pack} \quad , (\text{code}, (\text{clo}, x_1, \ldots, x_n)) \quad \text{as} \quad \text{in} \text{clo}
\end{align*}
\]
Here is how the “fix-pack” variant is type-checked. Assume
\[ \Gamma \vdash \mu f. \lambda x. M : \tau_1 \to \tau_2 \] and \( \text{dom}(\Gamma) = \{x_1, \ldots, x_n\} = \text{fv}(\mu f. \lambda x. M) \).

\[
\llbracket \mu f : \tau_1 \to \tau_2, \lambda x. M \rrbracket = \\
\text{let} \ \text{code} : \\
\quad \lambda (env : \llbracket f : \tau_1 \to \tau_2, \Gamma \rrbracket, x : \llbracket \tau_1 \rrbracket). \\
\quad \text{let} \ (f, x_1, \ldots, x_n) : \llbracket f : \tau_1 \to \tau_2, \Gamma \rrbracket = env \ \text{in} \\
\quad \llbracket M \rrbracket \ \text{in} \\
\text{let rec} \ \text{clo} : \\
\quad \text{pack} \ \llbracket f : \tau_1 \to \tau_2, \Gamma \rrbracket, (\text{code}, (\text{clo}, x_1, \ldots, x_n)) \\
\quad \text{as} \\
\quad \text{in} \ \text{clo}
\]
Here is how the “fix-pack” variant is type-checked. Assume \( \Gamma \vdash \mu f.\lambda x. M : \tau_1 \rightarrow \tau_2 \) and \( \text{dom}(\Gamma) = \{x_1, \ldots, x_n\} = \text{fv}(\mu f.\lambda x. M) \).

\[
\begin{align*}
\llbracket \mu f : \tau_1 \rightarrow \tau_2. \lambda x. M \rrbracket &= \\
\text{let code : } & (\llbracket f : \tau_1 \rightarrow \tau_2; \Gamma \rrbracket \times \llbracket \tau_1 \rrbracket) \rightarrow \llbracket \tau_2 \rrbracket = \\
\lambda & (env : \llbracket f : \tau_1 \rightarrow \tau_2, \Gamma \rrbracket, x : \llbracket \tau_1 \rrbracket).
\text{let } & (f, x_1, \ldots, x_n) : \llbracket f : \tau_1 \rightarrow \tau_2, \Gamma \rrbracket = env \text{ in}
\llbracket M \rrbracket \text{ in}
\text{let rec clo : } & = \\
\text{pack } & \llbracket f : \tau_1 \rightarrow \tau_2, \Gamma \rrbracket, (code, (clo, x_1, \ldots, x_n))
\text{as}
\text{in clo}
\end{align*}
\]
Here is how the “fix-pack” variant is type-checked. Assume
\( \Gamma \vdash \mu f.\lambda x.M : \tau_1 \to \tau_2 \) and \( \text{dom}(\Gamma) = \{ x_1, \ldots, x_n \} = \text{fv}(\mu f.\lambda x.M) \).

\[
\llbracket \mu f : \tau_1 \to \tau_2.\lambda x.M \rrbracket = \\
\text{let code} : ([f : \tau_1 \to \tau_2; \Gamma] \times [\tau_1]) \to [\tau_2] = \\
\lambda (env : [f : \tau_1 \to \tau_2, \Gamma], x : [\tau_1]). \\
\text{let } (f, x_1, \ldots, x_n) : [f : \tau_1 \to \tau_2, \Gamma] = env \text{ in} \\
\llbracket M \rrbracket \text{ in} \\
\text{let rec clo : [\tau_1 \to \tau_2] =} \\
\text{pack } [f : \tau_1 \to \tau_2, \Gamma], (\text{code}, (\text{clo}, x_1, \ldots, x_n)) \\
as \\
in clo
\]
Here is how the “fix-pack” variant is type-checked. Assume
\( \Gamma \vdash \mu f.\lambda x.M : \tau_1 \to \tau_2 \) and \( \text{dom}(\Gamma) = \{x_1, \ldots, x_n\} = \text{fv}(\mu f.\lambda x.M) \).

\[
\llbracket \mu f : \tau_1 \to \tau_2, \lambda x.M \rrbracket = \\
\text{let } code : (\llbracket f : \tau_1 \to \tau_2; \Gamma \rrbracket \times \llbracket \tau_1 \rrbracket) \to \llbracket \tau_2 \rrbracket = \\
\lambda (env : \llbracket f : \tau_1 \to \tau_2, \Gamma \rrbracket, x : \llbracket \tau_1 \rrbracket). \\
\text{let } (f, x_1, \ldots, x_n) : \llbracket f : \tau_1 \to \tau_2, \Gamma \rrbracket = env \text{ in} \\
\llbracket M \rrbracket \text{ in} \\
\text{let rec } clo : \llbracket \tau_1 \to \tau_2 \rrbracket = \\
\text{pack } \llbracket f : \tau_1 \to \tau_2, \Gamma \rrbracket, (code, (clo, x_1, \ldots, x_n)) \\
\text{as } \exists \alpha((\alpha \times \llbracket \tau_1 \rrbracket) \to \llbracket \tau_2 \rrbracket) \times \alpha \\
in clo
Here is how the “fix-pack” variant is type-checked. Assume 

\[ \Gamma \vdash \mu f. \lambda x. M : \tau_1 \rightarrow \tau_2 \text{ and } \text{dom}(\Gamma) = \{x_1, \ldots, x_n\} = \text{fv}(\mu f. \lambda x. M). \]

\[
\llbracket \mu f : \tau_1 \rightarrow \tau_2. \lambda x. M \rrbracket = \\
\quad \text{let code} : ([f : \tau_1 \rightarrow \tau_2; \Gamma] \times [\tau_1]) \rightarrow [\tau_2] = \\
\quad \lambda (env : [f : \tau_1 \rightarrow \tau_2, \Gamma], x : [\tau_1]). \\
\quad \text{let } (f, x_1, \ldots, x_n) : [f : \tau_1 \rightarrow \tau_2, \Gamma] = env \text{ in } \\
\quad [M] \text{ in} \\
\quad \text{let rec clo : } [\tau_1 \rightarrow \tau_2] = \\
\quad \text{pack } [f : \tau_1 \rightarrow \tau_2, \Gamma], (\text{code}, (\text{clo}, x_1, \ldots, x_n)) \text{ as } \exists \alpha((\alpha \times [\tau_1]) \rightarrow [\tau_2]) \times \alpha \\
\quad \text{in } clo
\]

Problem?
Environment-passing closure conversion

The recursive function may be polymorphic, but recursive calls are monomorphic...

We can generalize the encoding afterwards,

\[
[\Lambda \vec{\beta}. \mu f : \tau_1 \to \tau_2. \lambda x. M] = \Lambda \vec{\beta}. [\mu f : \tau_1 \to \tau_2. \lambda x. M]
\]

whenever the right-hand side is well-defined.

This allows the *indirect* compilation of polymorphic recursive functions as long as the recursion is monomorphic.

Fortunately, the encoding can be straightforwardly adapted to *directly* compile polymorphically recursive functions into polymorphic closure.
Environment-passing closure conversion

\[
\begin{align*}
\llbracket \mu f : \forall \vec{\beta}. \tau_1 \rightarrow \tau_2, \lambda x. M \rrbracket &= \\
&\text{let } \text{code} : \forall \vec{\beta}. (\llbracket f : \forall \vec{\beta}. \tau_1 \rightarrow \tau_2, \Gamma \rrbracket \times \llbracket \tau_1 \rrbracket) \rightarrow \llbracket \tau_2 \rrbracket = \\
&\quad \lambda (env : \llbracket f : \forall \vec{\beta}. \tau_1 \rightarrow \tau_2, \Gamma \rrbracket, x : \llbracket \tau_1 \rrbracket).
\end{align*}
\]

\[
\begin{align*}
&\text{let } (f, x_1, \ldots, x_n) : \llbracket f : \forall \vec{\beta}. \tau_1 \rightarrow \tau_2, \Gamma \rrbracket = env \text{ in } \\
&\llbracket M \rrbracket \text{ in } \\
&\text{let rec } \text{clo} : \llbracket \forall \vec{\beta}. \tau_1 \rightarrow \tau_2 \rrbracket = \\
&\quad \Lambda \vec{\beta}. \text{pack} \llbracket f : \forall \vec{\beta}. \tau_1 \rightarrow \tau_2, \Gamma \rrbracket, (\text{code} \vec{\beta}, (\text{clo}, x_1, \ldots, x_n)) \\
&\quad \text{as } \exists \alpha ((\alpha \times \llbracket \tau_1 \rrbracket) \rightarrow \llbracket \tau_2 \rrbracket) \times \alpha) \\
&\quad \text{in } \text{clo}
\end{align*}
\]

The encoding is simple.

However, this requires the introduction of recursive non-functional values “let rec \(x = v\)”. While this is a useful construct, it really alters the operational semantics and requires updating the type soundness proof.
• Introduction

• Towards typed closure conversion

• Existential types
  • Implicitly-type existential types passing
  • Iso-existential types

• Typed closure conversion
  • Environment passing
  • Closure passing
Towards typed closure conversion

Existential types

Typed closure conversion

**Closure-passing closure conversion**

\[
\left[ \lambda x. M \right] = \text{let } code = \lambda (clo, x). \begin{array}{l}
  \text{let } (_, x_1, \ldots, x_n) = clo \text{ in } \\
  \left[ M \right] \\
  \text{in } (code, x_1, \ldots, x_n)
\end{array}
\]

\[
\left[ M_1 \ M_2 \right] = \text{let } clo = \left[ M_1 \right] \text{ in } \\
\text{let } code = \text{proj}_0 \ clo \text{ in } \\
\text{code } (clo, \left[ M_2 \right])
\]

where \( \{ x_1, \ldots, x_n \} = \text{fv}(\lambda x. M) \).
Closure-passing closure conversion

\[
\begin{align*}
[\lambda x. M] &= \text{let } code = \lambda (\text{clo}, x). \\
&\quad \text{let } (-, x_1, \ldots, x_n) = \text{clo in} \\
&\quad [M] \\
&\quad \text{in } (code, x_1, \ldots, x_n) \\

[ M_1 \ M_2 ] &= \text{let } \text{clo} = [ M_1 ] \text{ in} \\
&\quad \text{let } code = \text{proj}_0 \text{clo in} \\
&\quad code (\text{clo}, [ M_2 ]) \\
\end{align*}
\]

where \( \{ x_1, \ldots, x_n \} = \text{fv}(\lambda x. M) \).

How could we typecheck this? What are the difficulties?
Closure-passing closure conversion

\[
\begin{align*}
\llbracket \lambda x. M \rrbracket &= \text{let code} = \lambda (\text{clo}, x). \\
&\quad \text{let } (\_, x_1, \ldots, x_n) = \text{clo in} \\
&\quad \llbracket M \rrbracket \\
&\quad \text{in } (\text{code}, x_1, \ldots, x_n)
\end{align*}
\]

\[
\begin{align*}
\llbracket M_1 M_2 \rrbracket &= \text{let clo} = \llbracket M_1 \rrbracket \text{ in} \\
&\quad \text{let code} = \text{proj}_0 \text{ clo in} \\
&\quad \text{code} (\text{clo}, \llbracket M_2 \rrbracket)
\end{align*}
\]

There are two difficulties:

- a closure is a tuple, whose \textit{first} field should be \textit{exposed} (it is the code pointer), while the number and types of the remaining fields should be abstract;
- the first field of the closure contains a function that expects \textit{the closure itself} as its first argument.
Closure-passing closure conversion

There are two difficulties:

- a closure is a tuple, whose \textit{first} field should be \textit{exposed} (it is the code pointer), while the number and types of the remaining fields should be abstract;

- the first field of the closure contains a function that expects \textit{the closure itself} as its first argument.

What type-theoretic mechanisms could we use to describe this?
Closure-passing closure conversion

There are two difficulties:

- a closure is a tuple, whose *first* field should be *exposed* (it is the code pointer), while the number and types of the remaining fields should be abstract;
- the first field of the closure contains a function that expects *the closure itself* as its first argument.

What type-theoretic mechanisms could we use to describe this?

- existential quantification over the *tail* of a tuple (a.k.a. a *row*);
- *recursive types.*
Tuples, rows, row variables

The standard tuple types that we have used so far are:

\[ \tau ::= \ldots | \Pi R \quad \text{– types} \]
\[ R ::= \epsilon | (\tau; R) \quad \text{– rows} \]

The notation \((\tau_1 \times \ldots \times \tau_n)\) was sugar for \(\Pi (\tau_1; \ldots; \tau_n; \epsilon)\).

Let us now introduce row variables and allow quantification over them:

\[ \tau ::= \ldots | \Pi R | \forall \rho. \tau | \exists \rho. \tau \quad \text{– types} \]
\[ R ::= \rho | \epsilon | (\tau; R) \quad \text{– rows} \]

This allows reasoning about the first few fields of a tuple whose length is not known.
Typing rules for tuples

The typing rules for tuple construction and deconstruction are:

\[
\text{TUPLE} \quad \forall i. \in [1, n] \quad \Gamma \vdash M_i : \tau_i \\
\Gamma \vdash (M_1, \ldots, M_n) : \Pi (\tau_1; \ldots; \tau_n; \epsilon)
\]

\[
\text{PROJ} \quad \Gamma \vdash M : \Pi (\tau_1; \ldots; \tau_i; R) \\
\Gamma \vdash proj_i M : \tau_i
\]

These rules make sense with or without row variables.

Projection does not care about the fields beyond \(i\). Thanks to row variables, this can be expressed in terms of *parametric polymorphism*:

\[
proj_i : \forall \alpha. 1 \ldots \alpha_i \rho. \Pi (\alpha_1; \ldots; \alpha_i; \rho) \rightarrow \alpha_i
\]
About Rows

Rows were invented by Wand and improved by Rémy in order to ascribe precise types to operations on *records*.

The case of tuples, presented here, is simpler.

Rows are used to describe *objects* in Objective Caml [Rémy and Vouillon, 1998].

Rows are explained in depth by Pottier and Rémy [Pottier and Rémy, 2005].
Closure-passing closure conversion

Rows and recursive types allow to define the translation of types in the closure-passing variant:

\[
\llbracket \tau_1 \to \tau_2 \rrbracket = \exists \rho. \mu \alpha. \Pi (\alpha \times \llbracket \tau_1 \rrbracket) \to \llbracket \tau_2 \rrbracket;
\]

\(\rho\) describes the environment
\(\alpha\) is the concrete type of the closure
a tuple...
...that begins with a code pointer...
...and continues with the environment

See Morrisett and Harper’s “fix-type” encoding [1998].
Closure-passing closure conversion

Rows and recursive types allow to define the translation of types in the closure-passing variant:

\[
\llbracket \tau_1 \to \tau_2 \rrbracket = \exists \rho. \\
\mu \alpha. \\
\Pi ( \\
(\alpha \times \llbracket \tau_1 \rrbracket) \to \llbracket \tau_2 \rrbracket; \\
\rho \\
) \\
\]

\(\rho\) describes the environment
\(\alpha\) is the concrete type of the closure
a tuple...
...that begins with a code pointer...
...and continues with the environment

See Morrisett and Harper’s “fix-type” encoding [1998].

**Question:** Why is it \(\exists \rho. \mu \alpha. \tau\) and not \(\mu \alpha. \exists \rho. \tau\)
Closure-passing closure conversion

Rows and recursive types allow to define the translation of types in the closure-passing variant:

\[
\llbracket \tau_1 \to \tau_2 \rrbracket = \exists \rho. \mu \alpha. \Pi ( (\alpha \times \llbracket \tau_1 \rrbracket) \to \llbracket \tau_2 \rrbracket ; \rho)
\]

\(\rho\) describes the environment
\(\alpha\) is the concrete type of the closure
a tuple...
...that begins with a code pointer...
...and continues with the environment

See Morrisett and Harper’s “fix-type” encoding [1998].

**Question:** Why is it \(\exists \rho. \mu \alpha. \tau\) and not \(\mu \alpha. \exists \rho. \tau\)

*The type of the environment is fixed once for all and does not change at each recursive call.*
Closure-passing closure conversion

Rows and recursive types allow to define the translation of types in the closure-passing variant:

\[
\llbracket \tau_1 \rightarrow \tau_2 \rrbracket = \exists \rho. \mu \alpha. \Pi (\alpha \times \llbracket \tau_1 \rrbracket) \rightarrow \llbracket \tau_2 \rrbracket; \rho
\]

\(\rho\) describes the environment
\(\alpha\) is the concrete type of the closure

...that begins with a code pointer...
...and continues with the environment

See Morrisett and Harper’s “fix-type” encoding [1998].

**Question:** Notice that \(\rho\) appears only once. Any comments?
Closure-passing closure conversion

Rows and recursive types allow to define the translation of types in the closure-passing variant:

\[
\llbracket \tau_1 \rightarrow \tau_2 \rrbracket = \exists \rho. \mu \alpha. \Pi ( \alpha \times \llbracket \tau_1 \rrbracket \rightarrow \llbracket \tau_2 \rrbracket ; \rho)
\]

\(\rho\) describes the environment
\(\alpha\) is the concrete type of the closure
a tuple...
...that begins with a code pointer...
...and continues with the environment

See Morrisett and Harper’s “fix-type” encoding [1998].

**Question:** Notice that \(\rho\) appears only once. Any comments?

*Usually, an existential type variable appears both at positive and negative occurrences.*
Closure-passing closure conversion

Rows and recursive types allow to define the translation of types in the closure-passing variant:

\[
\llbracket \tau_1 \rightarrow \tau_2 \rrbracket = \exists \rho. \\
\mu \alpha. \\
\Pi \left( \left( \alpha \times \llbracket \tau_1 \rrbracket \right) \rightarrow \llbracket \tau_2 \rrbracket; \rho \right)
\]

\(\rho\) describes the environment
\(\alpha\) is the concrete type of the closure
a tuple...
...that begins with a code pointer...
...and continues with the environment

See Morrisett and Harper’s “fix-type” encoding [1998].

Question: Notice that \(\rho\) appears only once. Any comments?

Usually, an existential type variable appears both at positive and negative occurrences. Here, the variable appear only at a negative occurrence, but in a recursive part of the type that can be unfolded.
Closure-passing closure conversion

Let $\text{Clo}(R)$ abbreviate $\mu \alpha. \Pi ((\alpha \times [\tau_1]) \rightarrow [\tau_2]; R)$. 

Let $\text{UClo}(R)$ abbreviate its unfolded version, 
$\Pi ((\text{Clo}(R) \times [\tau_1]) \rightarrow [\tau_2]; R)$. 

We have $[\tau_1 \rightarrow \tau_2] = \exists \rho. \text{Clo}(\rho)$. 

$$
\begin{align*}
[\lambda x: \ . M] &= \text{let code : } \\
&= \lambda(\text{clo : }, x : ) . \\
&\quad \text{let } (\ , x_1, \ldots, x_n) : \\
&\quad [M] \text{ in } \\
&\quad \text{pack }, (\text{fold } (\text{code}, x_1, \ldots, x_n)) \\
&\quad \text{as } \\
\end{align*}
$$

$$
\begin{align*}
[M_1 \ M_2] &= \text{let } \rho, \text{clo }= \text{unpack } [M_1] \text{ in } \\
&\quad \text{let code : } \\
&\quad \text{proj}_0 (\text{unfold } \text{clo} \text{ in } \\
&\quad \text{code } (\text{clo}, [M_2]) \\
\end{align*}
$$
Closure-passing closure conversion

Let $Clo(R)$ abbreviate $\mu\alpha.\Pi ((\alpha \times [\tau_1]) \to [\tau_2]; R)$.

Let $UClo(R)$ abbreviate its unfolded version,
$\Pi ((Clo(R) \times [\tau_1]) \to [\tau_2]; R)$.

We have $[\tau_1 \to \tau_2] = \exists \rho. Clo(\rho)$.

\[
\begin{align*}
[\lambda x : [\tau_1]. M] &= \text{let code} : (Clo([\Gamma]) \times [\tau_1]) \to [\tau_2] = \\
&\quad \lambda (clo : Clo([\Gamma], x : [\tau_1])). \\
&\quad \text{let } (\_ , x_1, \ldots , x_n) : UClo[\Gamma] = \text{unfold } clo \text{ in} \\
&\quad [M] \text{ in} \\
&\quad \text{pack } [\Gamma], (\text{fold } (\text{code}, x_1, \ldots , x_n)) \\
&\quad \text{as } \exists \rho. Clo(\rho)
\end{align*}
\]

\[
\begin{align*}
[M_1 \; M_2] &= \text{let } \rho, clo = \text{unpack } [M_1] \text{ in} \\
&\quad \text{let code} : (Clo(\rho) \times [\tau_1]) \to [\tau_2] = \\
&\quad proj_0 (\text{unfold } clo) \text{ in} \\
&\quad \text{code} (clo, [M_2])
\end{align*}
\]
Closure-passing closure conversion

In the closure-passing variant, recursive functions can be translated as:

\[
\llbracket \mu f. \lambda x. M \rrbracket = \begin{align*}
&\text{let } code = \lambda (\text{clo}, x). \\
&\quad \text{let } f = \text{clo in} \\
&\quad \text{let } (\_, x_1, \ldots, x_n) = \text{clo in} \\
&\quad \llbracket M \rrbracket \\
&\quad \text{in } (\text{code}, x_1, \ldots, x_n)
\end{align*}
\]

where \( \{x_1, \ldots, x_n\} = \text{fv}(\mu f. \lambda x. M) \).

No extra field or extra work is required to store or construct a representation of the free variable \( f \): the closure itself plays this role.

However, this untyped code can only be typechecked when recursion is monomorphic.

**Exercise:**

Check well-typedness with monomorphic recursion.
Closure-passing closure conversion

The problem to adapt this encoding to polymorphic recursion is that recursive occurrences of $f$ are rebuilt from the current invocation of the closure, i.e. is monomorphic since the closure is invoked after type specialization.

By contrast, in the environment passing encoding, the environment contained a polymorphic binding for the recursive calls that was filled with the closure before its invocation, i.e. with a polymorphic type.

Fortunately, we may slightly change the encoding, using a recursive closure as in the type-passing version, to allow typechecking in System F.
Closure-passing closure conversion

Let $\tau$ be $\forall \vec{\alpha}. \tau_1 \to \tau_2$ and $\Gamma_f$ be $f : \tau, \Gamma$ where $\vec{\beta} \not\in \Gamma$

\[
[\mu f : \tau. \lambda x. M] = \text{let } \text{code} = \\
\quad \Lambda \vec{\beta}. \lambda (\text{clo} : \text{Clo}[\Gamma_f], x : [\tau_1]). \\
\quad \text{let } (\_\text{code}, f, x_1, \ldots, x_n) : \forall \vec{\beta}. \text{UClo}([\Gamma_f]) = \\
\quad \text{unfold } \text{clo in } \\
\quad [M] \text{ in } \\
\quad \text{let rec } \text{clo} : \forall \vec{\beta}. \exists \rho. \text{Clo}(\rho) = \Lambda \vec{\beta}. \\
\quad \quad \text{pack } [\Gamma], (\text{fold } (\text{code } \vec{\beta}, \text{clo}, x_1, \ldots, x_n)) \text{ as } \exists \rho. \text{Clo}(\rho) \\
\quad \quad \text{in } \text{clo}
\]

Remind that $\text{Clo}(R)$ abbreviates $\mu \alpha. \Pi ((\alpha \times [\tau_1]) \to [\tau_2]; R)$. Hence, $\vec{\beta}$ are free variables of $\text{Clo}(R)$.

Here, a polymorphic recursive function is directly compiled into a polymorphic recursive closure. Notice that the type of closures is unchanged, so the encoding of applications is also unchanged.
Mutually recursive functions

Can we compile mutually recursive functions?

\[ M \triangleq \mu(f_1, f_2). (\lambda x_1. M_1, \lambda x_2. M_2) \]

Environment passing:

\[ [M] = \]
Can we compile mutually recursive functions?

\[ M \triangleq \mu(f_1, f_2). (\lambda x_1. M_1, \lambda x_2. M_2) \]

Environment passing:

\[
\begin{align*}
\llbracket M \rrbracket & = \text{let } code_i = \lambda (env, x). \\
& \quad \text{let } (f_1, f_2, x_1, \ldots, x_n) = env \text{ in} \\
& \quad \llbracket M_i \rrbracket \\
& \quad \text{in} \\
& \quad \text{let rec } clo_1 = (code_1, (clo_1, clo_2, x_1, \ldots, x_n)) \\
& \quad \quad \text{and } clo_2 = (code_2, (clo_1, clo_2, x_1, \ldots, x_n)) \text{ in} \\
& \quad clo_1, clo_2
\end{align*}
\]
Can we compile mutually recursive functions?

\[ M \triangleq \mu(f_1, f_2). (\lambda x_1. M_1, \lambda x_2. M_2) \]

Environment passing:

\[
\begin{align*}
[ M ] &= \text{let } \text{code}_i = \lambda (\text{env}, x). \\
    &\text{let } (f_1, f_2, x_1, \ldots, x_n) = \text{env in} \\
    &\text{let } \text{rec } \text{clo}_1 = (\text{code}_1, (\text{clo}_1, \text{clo}_2, x_1, \ldots, x_n)) \\
    &\text{and } \text{clo}_2 = (\text{code}_2, (\text{clo}_1, \text{clo}_2, x_1, \ldots, x_n)) \text{ in} \\
    &\text{clo}_1, \text{clo}_2
\end{align*}
\]

Comments?
Mutually recursive functions

Can we compile mutually recursive functions?

\[ M \triangleq \mu(f_1, f_2). (\lambda x_1. M_1, \lambda x_2. M_2) \]

Environment passing:

\[
\begin{align*}
\llbracket M \rrbracket &= \text{let } code_i = \lambda (env, x). \\
&\quad \text{let } (f_1, f_2, x_1, \ldots, x_n) = env \ \text{in} \\
&\quad \llbracket M_i \rrbracket \\
&\quad \text{in} \\
&\quad \text{let rec } env = (clo_1, clo_2, x_1, \ldots, x_n) \\
&\quad \text{and } clo_1 = (code_1, env) \\
&\quad \text{and } clo_2 = (code_2, env) \ \text{in} \\
&\quad clo_1, clo_2
\end{align*}
\]
Mutually recursive functions

Can we compile mutually recursive functions?

\[ M \equiv \mu(f_1, f_2). (\lambda x_1. M_1, \lambda x_2. M_2) \]

Closure passing:

\[
\text{let } code_i = \lambda (\text{clo}, x). \\
\text{let } (\_ , f_1, f_2, x_1, \ldots, x_n) = \text{clo in } [M_i] \\
\text{in } \\
\text{let rec } \text{clo}_1 = (code_1, \text{clo}_1, \text{clo}_2, x_1, \ldots, x_n) \\
\text{and } \text{clo}_2 = (code_2, \text{clo}_1, \text{clo}_2, x_1, \ldots, x_n) \\
\text{in } \text{clo}_1, \text{clo}_2
\]
Mutually recursive functions

Can we compile mutually recursive functions?

\[ M \overset{\Delta}{=} \mu(f_1, f_2). (\lambda x_1. M_1, \lambda x_2. M_2) \]

Closure passing:

\[
\begin{align*}
\text{let } code_i &= \lambda (\text{clo}, x). \\
\text{let } (\_ , f_1, f_2, x_1, \ldots, x_n) &= \text{clo in } [M_i] \\
\text{in } \\
\text{let rec } clo_1 &= (\text{code}_1, clo_1, clo_2, x_1, \ldots, x_n) \\
\text{and } clo_2 &= (\text{code}_2, clo_1, clo_2, x_1, \ldots, x_n) \\
\text{in } clo_1, clo_2
\end{align*}
\]

Question: Can we share the closures \( c_1 \) and \( c_2 \) in case \( n \) is large?
Mutually recursive functions

Can we compile mutually recursive functions?

\[ M \overset{\Delta}{=} \mu(f_1, f_2). (\lambda x_1. M_1, \lambda x_2. M_2) \]

Closure passing:

\[
\begin{align*}
\text{let code}_1 &= \lambda(clo, x).
\text{let } (\_\text{code}_1, \_\text{code}_2, f_1, f_2, x_1, \ldots, x_n) &= clo \text{ in } [M_1] \text{ in } \\
\text{let code}_2 &= \lambda(clo, x).
\text{let } (\_\text{code}_2, f_1, f_2, x_1, \ldots, x_n) &= clo \text{ in } [M_2] \text{ in } \\
\text{let rec } clo_1 &= (\text{code}_1, \text{code}_2, clo_1, clo_2, x_1, \ldots, x_n) \text{ and } clo_2 = c_1.\text{tail} \\
in \text{clo}_1, \text{clo}_2
\end{align*}
\]

- \(clo_1.\text{tail}\) returns a pointer to the tail \((\text{code}_2, clo_1, clo_2, x_1, \ldots, x_n)\) of \(clo_1\) without allocating a new tuple.
- This is only possible with some support from the GC (and extra-complexity and runtime cost for GC)
Optimizing representations

Can closure passing and environment passing be mixed?
Optimizing representations

Can closure passing and environment passing be mixed?

No because the calling-convention (i.e., the encoding of application) must be uniform.

However, there is some flexibility in the representation of the closure. For instance, the following change is completely local:

\[\lbrack \lambda x. M \rbrack = \text{let } code = \lambda (\text{clo}, x). \]
\[\text{let } (\_, x_1, \ldots, x_n) = \text{clo in } \lbrack M \rbrack \text{ in } \]
\[(\text{code}, x_1, \ldots, x_n)\]

\[\lbrack M_1 M_2 \rbrack = \text{let } clo = \lbrack M_1 \rbrack \text{ in } \]
\[\text{let } code = \text{proj}_0 \text{ clo in } \]
\[\text{code (clo, } \lbrack M_2 \rbrack )\]

Applications? When many definitions share the same closure, the closure (or part of it) may be shared.
Can closure passing and environment passing be mixed?

No because the calling-convention (i.e., the encoding of application) must be uniform.

However, there is some flexibility in the representation of the closure. For instance, the following change is completely local:

\[
\begin{align*}
\llbracket \lambda x. M \rrbracket &= \text{let } code = \lambda (clo, x). \\
&\quad \text{let } (-, (x_1, \ldots, x_n)) = clo \text{ in } \llbracket M \rrbracket \text{ in } \\
&\quad (code, (x_1, \ldots, x_n))
\end{align*}
\]

\[
\begin{align*}
\llbracket M_1 \ M_2 \rrbracket &= \text{let } clo = \llbracket M_1 \rrbracket \text{ in } \\
&\quad \text{let } code = \text{proj}_0 \ clo \text{ in } \\
&\quad code (clo, \llbracket M_2 \rrbracket)
\end{align*}
\]

Applications? When many definitions share the same closure, the closure (or part of it) may be shared.
Encoding of objects

The closure-passing representation of mutually recursive functions is similar to the representations of objects in the object-as-record-of-functions paradigm:

A class definition is an object generator:

\[
\text{class } c \left( x_1, \ldots x_q \right) \{ \\
\quad \text{meth } m_1 = M_1 \\
\quad \ldots \\
\quad \text{meth } m_p = M_p \\
\}
\]

Given arguments for parameter \( x_1, \ldots x_1 \), it will build recursive methods \( m_1, \ldots m_n \).
Encoding of objects

A class can be compiled into an object closure:

\[
\text{let } m = \\
\quad \text{let } m_1 = \lambda(m, x_1, \ldots, x_q). M_1 \text{ in} \\
\quad \ldots \\
\quad \text{let } m_p = \lambda(m, x_1, \ldots, x_q). M_p \text{ in} \\
\quad \{m_1, \ldots, m_p\} \text{ in} \\
\quad \lambda x_1 \ldots x_q. (m, x_1, \ldots x_q)
\]

Each \( m_i \) is bound to the code for the corresponding method. The code of all methods are combined into a record of methods, which is shared between all objects of the same class.

Calling method \( m_i \) of an object \( p \) is

\[
(\text{proj}_0 p). m_i p
\]

How can we type the encoding?
Typed encoding of objects

Let $\tau_i$ be the type of $M_i$, and row $R$ describe the types of $(x_1, \ldots x_q)$.

Let $Clo(R)$ be $\mu \alpha. \Pi \{ (m_i : \alpha \to \tau_i)^{i \in 1..n} \}; R$ and $UClo(R)$ its unfolding.

Fields $R$ are hidden in an existential type $\exists \rho. \mu \alpha. \Pi \{ (m_i : \alpha \to \tau_i)^{i \in I} \}; \rho$:

$$\text{let } m = \{\text{let } m = \{\text{let } m = \{\text{let } m = \{
\begin{align*}
m_1 &= \lambda (m, x_1, \ldots x_q : UClo(R)). [M_1] \\
\vdots

m_p &= \lambda (m, x_1, \ldots x_q : UClo(R)). [M_p]
\end{align*}
\} \text{ in } \\
\lambda x_1. \ldots \lambda x_q. \text{pack } R, \text{fold } (m, x_1, \ldots x_q) \text{ as } \exists \rho. (M, \rho)
\}$$

Calling a method of an object $p$ of type $M$ is

$$p \# m_i \triangleq \text{let } \rho, z = \text{unpack } p \text{ in } (\text{proj}_0 \text{ unfold } z).m_i z$$

An object has a recursive type but it is not a recursive value.
Typed encoding of objects

Typed encoding of objects were first studied in the 90’s to understand what objects really are in a type setting.

These encodings are in fact type-preserving compilation of (primitive) objects.

There are several variations on these encodings. See [Bruce et al., 1999] for a comparison.

See [Rémy, 1994] for an encoding of objects in (a small extension of) ML with iso-existentials and universals.

Moral of the story

Type-preserving compilation is rather *fun*. (Yes, really!)

It forces compiler writers to make the structure of the compiled program *fully explicit*, in type-theoretic terms.

In practice, building explicit type derivations, ensuring that they remain small and can be efficiently typechecked, can be a lot of work.
Optimizations

Because we have focused on type preservation, we have studied only naïve closure conversion algorithms.

More ambitious versions of closure conversion require program analysis: see, for instance, Steckler and Wand [1997]. These versions can be made type-preserving.
Other challenges

Defunctionalization, an alternative to closure conversion, offers an interesting challenge, with a simple solution [Pottier and Gauthier, 2006].

Designing an efficient, type-preserving compiler for an object-oriented language is quite challenging. See, for instance, Chen and Tarditi [2005].
(Most titles have a clickable mark “▷” that links to online versions.)


