CS152: Programming Languages

Lecture 17 — Existential Types; Type-and-Effect Systems

Dan Grossman
Spring 2011
Back to our goal

Understand this interface and its nice properties:

type 'a mylist;
val mt_list : 'a mylist
val cons : 'a -> 'a mylist -> 'a mylist
val decons : 'a mylist -> (('a * 'a mylist) option)
val length : 'a mylist -> int
val map : ('a -> 'b) -> 'a mylist -> 'b mylist

So far, we can do it if we expose the definition of mylist

mt_list : \(\forall \alpha. \mu\beta.\text{unit} + (\alpha \times \beta)\)
cons: \(\forall \alpha. \alpha \rightarrow (\mu\beta.\text{unit} + (\alpha \times \beta)) \rightarrow (\mu\beta.\text{unit} + (\alpha \times \beta))\)
...

Abstract Types

Define an interface such that well-typed list-clients cannot break the list-library abstraction

- Hide the concrete definition of type mylist

Why?

- So clients cannot “forge” lists — always created by library
- So clients cannot rely on the concrete implementation, which lets us change the library in ways that we know will not break clients

To simplify the discussion very slightly, consider just myintlist

- mylist is a type constructor, a function that given a type gives a type
The Type-Application Approach

We can hide myintlist via type abstraction (like we hid file-handles):

\[(\Lambda \alpha. \lambda x: \tau_1. \text{list\_client}) \ [\tau_2] \ \text{list\_library}\]

where:

- $\tau_1$ is \{ $mt : \alpha$,
  $cons : \text{int} \rightarrow \alpha \rightarrow \alpha$,
  $decons : \alpha \rightarrow \text{unit} + (\text{int} \ast \alpha)$,
  ...
  \}

- $\tau_2$ is $\mu \beta. \text{unit} + (\text{int} \ast \beta)$

- list\_client projects from record $x$ to get list functions

- list\_library is the record of list functions
Evaluating ADT via Type Application

\[(\Lambda \alpha. \lambda x: \tau_1. \text{list}_\text{client}) [\tau_2] \text{list}_\text{library}\]

Plus:
- Effective
- Straightforward use of System F

Minus:
- The library does not say \text{myintlist} should be abstract
  - It relies on clients to abstract it
  - Can be “fixed” with a “structure inversion” (passing client to the library), but cure arguably worse than disease
- Different list-libraries have different types, so can’t choose one at run-time or put them in a data structure:
  - if \(n>10\) then \text{hashset}_\text{lib} else \text{listset}_\text{lib}
  - Wish: values \textit{produced} by different libraries must have \textit{different} types, but \textit{libraries} can have the \textit{same} type
The OO Approach

Use recursive types and records:

\[
\texttt{mt_list} : \mu \beta. \begin{align*}
\text{cons} & : \text{int} \to \beta, \\
\text{decons} & : \text{unit} \to (\text{unit} + (\text{int} \times \beta)), \\
\ldots
\end{align*}
\]

\texttt{mt_list} is an object — a record of functions plus private data

The \texttt{cons} field holds a function that returns a new record of functions

Implementation uses recursion and “hidden fields” in an essential way

- In ML, free variables are the “hidden fields”
- In OO, private fields or abstract interfaces “hide fields”

(See Caml code for a slightly different example)
Evaluating the Closure/OO Approach

Plus:

- It works in popular languages (no explicit type variables)
- Different list-libraries have the same type

Minus:

- Changed the interface (no big deal?)
- Fails on “strong” binary ((\(n > 1\))-ary) operations
  - Have to write append in terms of cons and decons
  - Can be impossible
    (silly example: see type t2 in ML file)
The Existential Approach

Achieved our goal two different ways, but each had some drawbacks

There is a direct way to model ADTs that captures their essence quite nicely: types of the form $\exists \alpha. \tau$

Next slide has a formalization, but we’ll mostly focus on
   ▶ The intuition
   ▶ How to use the idea to encode closures (e.g., for callbacks)

Why don’t many real PLs have existential types?
   ▶ Because other approaches kinda work?
   ▶ Because modules work well even if “second-class”? 
   ▶ Because have only been well-understood since the mid-1980s and “tech transfer” takes forever and a day?
Existential Types

\[ e ::= \ldots | \text{pack } \tau, e \text{ as } \exists \alpha.\tau | \text{unpack } e \text{ as } \alpha, x \text{ in } e \]

\[ v ::= \ldots | \text{pack } \tau, v \text{ as } \exists \alpha.\tau \]

\[ \tau ::= \ldots | \exists \alpha.\tau \]

\[
\frac{e \rightarrow e'}{\text{pack } \tau_1, e \text{ as } \exists \alpha.\tau_2 \rightarrow \text{pack } \tau_1, e' \text{ as } \exists \alpha.\tau_2}
\]

\[
\frac{e \rightarrow e'}{\text{unpack } e \text{ as } \alpha, x \text{ in } e_2 \rightarrow \text{unpack } e' \text{ as } \alpha, x \text{ in } e_2}
\]

\[
\text{unpack } (\text{pack } \tau_1, v \text{ as } \exists \alpha.\tau_2) \text{ as } \alpha, x \text{ in } e_2 \rightarrow e_2[\tau_1/\alpha][v/x]
\]

\[
\frac{\Delta; \Gamma \vdash e : \tau'[\tau/\alpha]}{\Delta; \Gamma \vdash \text{pack } \tau, e \text{ as } \exists \alpha.\tau' : \exists \alpha.\tau'}
\]

\[
\frac{\Delta; \Gamma \vdash e_1 : \exists \alpha.\tau' \quad \Delta, \alpha; \Gamma, x : \tau' \vdash e_2 : \tau \quad \Delta \vdash \tau \quad \alpha \not\in \Delta}{\Delta; \Gamma \vdash \text{unpack } e_1 \text{ as } \alpha, x \text{ in } e_2 : \tau}
\]
List library with $\exists$

The list library is an existential package:

$$\text{pack } (\mu \alpha. \text{unit} + (\text{int} \times \alpha)), \text{list\_library as } \exists \beta. \{ \text{empty} : \beta, \text{cons} : \text{int} \to \beta \to \beta, \text{decons} : \beta \to \text{unit} + (\text{int} \times \beta), \ldots \}$$

Another library would “pack” a different type and implementation, but have the same overall type.

Binary operations work fine, e.g., $\text{append} : \beta \to \beta \to \beta$

Libraries are first-class, but a use of a library must be in a scope that “remembers which $\beta$” describes data from that library.

- (If use two libraries in same scope, can’t pass the result of one’s $\text{cons}$ to the other’s $\text{decons}$ because the two libraries will use different type variables)
Closures and Existentials

There’s a deep connection between existential types and how closures are used/compiled

▶ “Call-backs” are the canonical example

Caml:

▶ Interface:

```ocaml```
val onKeyEvent : (int -> unit) -> unit
```

▶ Implementation:

```ocaml```
let callBacks : (int -> unit) list ref = ref []
let onKeyEvent f = callBacks := f :: (!callBacks)
let keyPress i = List.iter (fun f -> f i) !callBacks
```

Each registered function can have a different environment (free variables of different types), yet every function has type int->unit
Closures and Existentials

C:

typedef struct {void* env; void (*f)(void*,int);} * cb_t;

- Interface: void onKeyEvent(cb_t);
- Implementation (assuming a list library):

```c
list_t callBacks = NULL;
void onKeyEvent(cb_t cb){callBacks=cons(cb,callBacks);}
void keyPress(int i) {
    for(list_t lst=callBacks; lst; lst=lst->tl)
        lst->hd->f(lst->hd->env, i);
}
```

Standard problems using subtyping ($t^* \leq \text{void}^*$) instead of $\alpha$:
- Client must provide an $f$ that downcasts argument back to $t^*$
- Typechecker lets library pass any $\text{void}^*$ to $f$
Closures and Existentials

Cyclone (aka Dan’s thesis): (has $\forall \alpha. \tau$ and $\exists \alpha. \tau$ but not closures)

typedef struct {<'a> 'a env; void (*f)(‘a,int);} * cb_t;

- Interface: void onKeyEvent(cb_t);
- Implementation (assuming a list library):

```c
list_t<cb_t> callBacks = NULL;
void onKeyEvent(cb_t cb){callBacks=cons(cb,callBacks);}
void keyPress(int i) {
    for(list_t<cb_t> lst=callBacks; lst; lst=lst->tl) {
        let {<'a> x, y} = *lst->hd; // pattern-match
        y(x,i); // no other argument to y typechecks!
    }
}
```

Not shown: To create a cb_t, the “the types must match up”
Type-and-effect systems

New topic: An elegant framework to extend type systems to track “things that may happen” (effects) during evaluation

Plain-old type systems have judgments like $\Gamma \vdash e : \tau$ to mean:

- $e$ won’t get stuck
- If $e$ produces a value, that value has type $\tau$

Adding effects reuses the “plumbing” of typing rules to compute something about “how $e$ executes”

- There are many things we may want to conservatively approximate
  - Example: What exceptions might get thrown
- All effect systems are very similar, especially treatment of functions
  - Example: All values have no effect since their “computation” does nothing
First a type system

(In this example, exceptions raise constant strings \( s \))

\[
\tau ::= \text{bool} \mid \tau \rightarrow \tau \mid \tau \ast \tau
\]

\[
e ::= x \mid \text{true} \mid \text{false} \mid \lambda x.\ e \mid e\ e \mid (e, e) \mid e.1 \mid e.2
\]

\[
\mid \text{if } \ e\ e\ e \mid \text{raise } s \mid \text{try } e\ \text{handle } s\ e
\]

\[
\Gamma \vdash e : \tau
\]

- \[
\Gamma \vdash x : \Gamma(x)
\]
- \[
\Gamma \vdash \text{true} : \text{bool}
\]
- \[
\Gamma \vdash \text{false} : \text{bool}
\]

\[
\Gamma, x : \tau_1 \vdash e : \tau_2
\]

- \[
\Gamma \vdash \lambda x.\ e : \tau_1 \rightarrow \tau_2
\]

\[
\Gamma \vdash e_1 : \tau_1 \quad \Gamma \vdash e_2 : \tau_2
\]

- \[
\Gamma \vdash (e_1, e_2) : \tau_1 \ast \tau_2
\]

- \[
\Gamma \vdash \text{if } e_1\ e_2\ e_3 : \tau
\]

- \[
\Gamma \vdash \text{raise } s : \tau
\]

- \[
\Gamma \vdash \text{try } e_1\ \text{handle } s\ e_2 : \tau
\]
Add effects

\[ \epsilon ::= \ldots \text{sets of strings}\ldots \]

\[ \tau ::= \text{bool} \mid \tau \xrightarrow{\epsilon} \tau \mid \tau \ast \tau \]

\[ e ::= x \mid \text{true} \mid \text{false} \mid \lambda x. \ e \mid e \ e \mid (e, e) \mid e.1 \mid e.2 \]

\[ \text{if} \ e \ e \ e \mid \text{raise} \ s \mid \text{try} \ e \ \text{handle} \ s \ e \]

\[
\begin{align*}
\Gamma \vdash e : \tau; \epsilon &
\quad \Gamma \vdash x : \Gamma(x); \emptyset &
\quad \Gamma \vdash \text{true} : \text{bool}; \emptyset &
\quad \Gamma \vdash \text{false} : \text{bool}; \emptyset \\
\Gamma, x : \tau_1 \vdash e : \tau_2; \epsilon &
\quad \Gamma \vdash e_1 : \tau_2 \xrightarrow{\epsilon_3} \tau_1; \epsilon_1 &
\quad \Gamma \vdash e_2 : \tau_2; \epsilon_2 &
\quad \Gamma \vdash e_1 e_2 : \tau_1; \epsilon_1 \cup \epsilon_2 \cup \epsilon_3 \\
\Gamma \vdash \lambda x. \ e : \tau_1 \rightarrow \tau_2; \emptyset &
\quad \Gamma \vdash e_1 : \tau_1; \epsilon_1 &
\quad \Gamma \vdash e_2 : \tau_2; \epsilon_2 &
\quad \Gamma \vdash e : \tau_1 \ast \tau_2; \epsilon &
\quad \Gamma \vdash e.1 : \tau_1; \epsilon &
\quad \Gamma \vdash e.2 : \tau_2; \epsilon &
\quad \Gamma \vdash e_1 : \text{bool}; \epsilon_1 &
\quad \Gamma \vdash e_2 : \tau; \epsilon_2 &
\quad \Gamma \vdash e_3 : \tau; \epsilon_3 &
\quad \Gamma \vdash \text{if} \ e_1 e_2 e_3 : \tau; \epsilon_1 \cup \epsilon_2 \cup \epsilon_3 \\
\Gamma \vdash \text{raise} \ s : \tau; \{s\} &
\quad \Gamma \vdash \text{try} \ e_1 \ \text{handle} \ s \ e_2 : \tau; (\epsilon_1 - \{s\}) \cup \epsilon_2 
\end{align*}
\]
Key facts

Soundness: If $\vdash e : \tau; \epsilon$ and $e$ raises uncaught exception $s$, then $s \in \epsilon$

- Corollary to Preservation and Progress (once you define the operational semantics for exceptions)

All effect systems work this way:

- Values effectless
- Functions have latent effects
- Conservative due to if and try/handle

Only a couple rules special to this effect system

- Also, not always sets and $\cup$
More general rules

Every effect system also substantially more expressive via appropriate subsumption:

- Typing rule for subeffecting (also useful for Preservation)
- Subtyping of function types is covariant in latent effects

\[
\frac{\Gamma \vdash \tau : e; \epsilon \quad \epsilon \subseteq \epsilon'}{\Gamma \vdash \tau : e; \epsilon'} \quad \frac{\tau_3 \leq \tau_1 \quad \tau_2 \leq \tau_4 \quad \epsilon \subseteq \epsilon'}{
\tau_1 \epsilon \rightarrow \tau_2 \leq \tau_3 \epsilon' \rightarrow \tau_4}
\]

Not shown: Also want effect polymorphism (type variables ranging over effects) for higher-order functions like map
Other examples

- Definitely terminates (true) or possibly diverges (false)
  - Give \texttt{fix e} effect \texttt{false}
  - Give values effect \texttt{true}
  - Treat \texttt{∪} as \texttt{and}
  - No change to rules for functions, pairs, conditionals, etc.
- What type casts might occur (*)
- Are the right variables used in transactions (*)
- Does code obey a locking protocol (*)
- Does code only access memory regions that haven’t been deallocated (*)
- ...

Really a general way to lift static analysis to higher-order functions

(*) The core technique in a research paper Dan has written, though the idea of using effect systems for this sort of thing is not his
- Key is recognizing “from a mile away” when an effect system is the right tool