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 :` $\forall\alpha.\mu\beta.\textbf{unit} + (\alpha * \beta)$

`cons:` $\forall\alpha.\alpha \rightarrow (\mu\beta.\textbf{unit} + (\alpha * \beta)) \rightarrow (\mu\beta.\textbf{unit} + (\alpha * \beta))$

...

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):

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

where:

- τ_1 is $\{\ \textbf{mt} : \alpha,\ \textbf{cons} : \textbf{int} \to \alpha \to \alpha,\ \textbf{decons} : \alpha \to \textbf{unit} + (\textbf{int} * \alpha),\ \ldots\ \}$
- τ_2 is $\mu\beta.\textbf{unit} + (\textbf{int} * \beta)$
- $list\_client$ projects from record x to get list functions
- $list\_library$ is the record of list functions

Evaluating ADT via Type Application

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

Plus:

- Effective
- Straightforward use of System F

Minus:

- The library does not say `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 hashset_lib else listset_lib`
  - Wish: values *produced* by different libraries must have *different* types, but *libraries* can have the *same* type

The OO Approach

Use recursive types and records:

$$\textbf{mt\_list} : \mu\beta.\ \{\ \ \textbf{cons} : \textbf{int} \rightarrow \beta,\ \textbf{decons} : \textbf{unit} \rightarrow (\textbf{unit} + (\textbf{int} * \beta)),\ \ldots\}$$

mt_list is an *object* — a record of functions plus private data

The **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

$$\begin{array}{lcl} e & ::= & \ldots \mid \textsf{pack } \tau, e \textsf{ as } \exists\alpha.\tau \mid \textsf{unpack } e \textsf{ as } \alpha, x \textsf{ in } e \\ v & ::= & \ldots \mid \textsf{pack } \tau, v \textsf{ as } \exists\alpha.\tau \\ \tau & ::= & \ldots \mid \exists\alpha.\tau \end{array}$$

$$\frac{e \to e'}{\textsf{pack } \tau_1, e \textsf{ as } \exists\alpha.\tau_2 \to \textsf{pack } \tau_1, e' \textsf{ as } \exists\alpha.\tau_2}$$

$$\frac{e \to e'}{\textsf{unpack } e \textsf{ as } \alpha, x \textsf{ in } e_2 \to \textsf{unpack } e' \textsf{ as } \alpha, x \textsf{ in } e_2}$$

$$\frac{}{\textsf{unpack } (\textsf{pack } \tau_1, v \textsf{ as } \exists\alpha.\tau_2) \textsf{ as } \alpha, x \textsf{ in } e_2 \to e_2[\tau_1/\alpha][v/x]}$$

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

$$\frac{\Delta; \Gamma \vdash e_1 : \exists\alpha.\tau' \qquad \Delta, \alpha; \Gamma, x{:}\tau' \vdash e_2 : \tau \qquad \Delta \vdash \tau \qquad \alpha \notin \Delta}{\Delta; \Gamma \vdash \textsf{unpack } e_1 \textsf{ as } \alpha, x \textsf{ in } e_2 : \tau}$$

List library with $\exists$

The list library is an existential package:

$$\begin{array}{ll} \textbf{pack}\ (\mu\alpha.\textbf{unit} + (\textbf{int} * \alpha)), \mathit{list\_library}\ \textbf{as} & \\ \exists\beta.\ \{ & \textbf{empty} : \beta, \\ & \textbf{cons} : \textbf{int} \rightarrow \beta \rightarrow \beta, \\ & \textbf{decons} : \beta \rightarrow \textbf{unit} + (\textbf{int} * \beta), \\ & \ldots \} \end{array}$$

Another library would "pack" a *different* type and implementation, but have the *same* overall type

Binary operations work fine, e.g., **append :** $\beta \rightarrow \beta \rightarrow \beta$

Libraries are first-class, but a *use* of a library must be in a scope that "remembers which β" describes data from that library

- (If use two libraries in same scope, can't pass the result of one's **cons** to the other's **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:

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

- Implementation:

```
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):

```
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*`$\leq$`void*`) instead of α:

- Client must provide an `f` that downcasts argument back to `t*`
- Typechecker lets library pass any `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):

```
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 τ

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)

$$\begin{array}{rcl} \tau & ::= & \textsf{bool} \mid \tau \to \tau \mid \tau * \tau \\ e & ::= & x \mid \textsf{true} \mid \textsf{false} \mid \lambda x.\ e \mid e\ e \mid (e, e) \mid e.1 \mid e.2 \\ & \mid & \textsf{if}\ e\ e\ e \mid \textsf{raise}\ s \mid \textsf{try}\ e\ \textsf{handle}\ s\ e \end{array}$$

$\boxed{\Gamma \vdash e : \tau}$

$$\frac{}{\Gamma \vdash x : \Gamma(x)} \qquad \frac{}{\Gamma \vdash \textsf{true} : \textsf{bool}} \qquad \frac{}{\Gamma \vdash \textsf{false} : \textsf{bool}}$$

$$\frac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x.\ e : \tau_1 \to \tau_2} \qquad \frac{\Gamma \vdash e_1 : \tau_2 \to \tau_1 \qquad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash e_1\ e_2 : \tau_1}$$

$$\frac{\Gamma \vdash e_1 : \tau_1 \qquad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash (e_1, e_2) : \tau_1 * \tau_2} \qquad \frac{\Gamma \vdash e : \tau_1 * \tau_2}{\Gamma \vdash e.1 : \tau_1} \qquad \frac{\Gamma \vdash e : \tau_1 * \tau_2}{\Gamma \vdash e.2 : \tau_2}$$

$$\frac{\Gamma \vdash e_1 : \textsf{bool} \qquad \Gamma \vdash e_2 : \tau \qquad \Gamma \vdash e_3 : \tau}{\Gamma \vdash \textsf{if}\ e_1\ e_2\ e_3 : \tau}$$

$$\frac{}{\Gamma \vdash \textsf{raise}\ s : \tau} \qquad \frac{\Gamma \vdash e_1 : \tau \qquad \Gamma \vdash e_2 : \tau}{\Gamma \vdash \textsf{try}\ e_1\ \textsf{handle}\ s\ e_2 : \tau}$$

Add effects

$$
\begin{array}{rcl}
\epsilon & ::= & \text{...sets of strings...} \\
\tau & ::= & \textbf{bool} \mid \tau \xrightarrow{\epsilon} \tau \mid \tau * \tau \\
e & ::= & x \mid \textbf{true} \mid \textbf{false} \mid \lambda x.\ e \mid e\ e \mid (e, e) \mid e.1 \mid e.2 \\
 & \mid & \textbf{if}\ e\ e\ e \mid \textbf{raise}\ s \mid \textbf{try}\ e\ \textbf{handle}\ s\ e
\end{array}
$$

$$\boxed{\Gamma \vdash e : \tau; \epsilon} \qquad \frac{}{\Gamma \vdash x : \Gamma(x); \emptyset} \qquad \frac{}{\Gamma \vdash \textbf{true} : \textbf{bool}; \emptyset} \qquad \frac{}{\Gamma \vdash \textbf{false} : \textbf{bool}; \emptyset}$$

$$\frac{\Gamma, x : \tau_1 \vdash e : \tau_2; \epsilon}{\Gamma \vdash \lambda x.\ e : \tau_1 \xrightarrow{\epsilon} \tau_2; \emptyset} \qquad \frac{\Gamma \vdash e_1 : \tau_2 \xrightarrow{\epsilon_3} \tau_1; \epsilon_1 \qquad \Gamma \vdash e_2 : \tau_2; \epsilon_2}{\Gamma \vdash e_1\ e_2 : \tau_1; \epsilon_1 \cup \epsilon_2 \cup \epsilon_3}$$

$$\frac{\Gamma \vdash e_1 : \tau_1; \epsilon_1 \qquad \Gamma \vdash e_2 : \tau_2; \epsilon_2}{\Gamma \vdash (e_1, e_2) : \tau_1 * \tau_2; \epsilon_1 \cup \epsilon_2} \qquad \frac{\Gamma \vdash e : \tau_1 * \tau_2; \epsilon}{\Gamma \vdash e.1 : \tau_1; \epsilon} \qquad \frac{\Gamma \vdash e : \tau_1 * \tau_2; \epsilon}{\Gamma \vdash e.2 : \tau_2; \epsilon}$$

$$\frac{\Gamma \vdash e_1 : \textbf{bool}; \epsilon_1 \qquad \Gamma \vdash e_2 : \tau; \epsilon_2 \qquad \Gamma \vdash e_3 : \tau; \epsilon_3}{\Gamma \vdash \textbf{if}\ e_1\ e_2\ e_3 : \tau; \epsilon_1 \cup \epsilon_2 \cup \epsilon_3}$$

$$\frac{}{\Gamma \vdash \textbf{raise}\ s : \tau; \{s\}} \qquad \frac{\Gamma \vdash e_1 : \tau; \epsilon_1 \qquad \Gamma \vdash e_2 : \tau; \epsilon_2}{\Gamma \vdash \textbf{try}\ e_1\ \textbf{handle}\ s\ e_2 : \tau; (\epsilon_1 - \{s\}) \cup \epsilon_2}$$

Key facts

Soundness: If $\cdot \vdash e : \tau; \epsilon$ 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 functiont types is covariant in latent effects

$$\frac{\Gamma \vdash \tau : e; \epsilon \qquad \epsilon \subseteq \epsilon'}{\Gamma \vdash \tau : e; \epsilon'} \qquad \frac{\tau_3 \leq \tau_1 \qquad \tau_2 \leq \tau_4 \qquad \epsilon \subseteq \epsilon'}{\tau_1 \xrightarrow{\epsilon} \tau_2 \leq \tau_3 \xrightarrow{\epsilon'} \tau_4}$$

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 **fix** e effect *false*
  - Give values effect *true*
  - Treat $\cup$ as *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