CS 4110 – Programming Languages and Logics
Lecture #31: Featherweight Java Properties and Object Encodings

In this lecture, we will develop a proof of type soundness for Featherweight Java in the usual way, as a corollary of progress and preservation. The details of these proofs will be a little different than the ones we have seen before, however, due to the presence of subtyping and casts. We will then develop a different way of formalizing object-oriented languages using object encodings.

1 Properties

1.1 Preservation

The proof of preservation relies on several supporting lemmas.

Lemma (Method Typing). *If* $mtype(m, C) = \overline{D} \to D$ *and* $mbody(m, C) = (\overline{x}, e)$ *then there exists types* C' *and* D' *such that* $\overline{x} : \overline{D}, \texttt{this} : C' \vdash e : D'$ *and* $D' \leq D$.

Lemma (Substitution). *If* $\Gamma, \overline{x} : \overline{B} \vdash e : C$ *and* $\Gamma \vdash \overline{u} : \overline{B'}$ *with* $\overline{B'} \leq \overline{B}$ *then there exists* C' *such that* $\Gamma \vdash [\overline{x} \mapsto \overline{u}]e : C'$ *and* $C' \leq C$.

Lemma (Weakening). *If* $\Gamma \vdash e : C$ *then* $\Gamma, x : B \vdash e : C$.

Lemma (Decomposition). *If* $\Gamma \vdash E[e] : C$ *then there exists a type* B *such that* $\Gamma \vdash e : B$

Lemma (Context). *If* $\Gamma \vdash E[e] : C$ *and* $\Gamma \vdash e : B$ *and* $\Gamma \vdash e' : B'$ *with* $B' \leq B$ *then there exists a type* C' *such that* $\Gamma \vdash E[e'] : C'$ *and* $C' \leq C$.

Lemma (Preservation). *If* $\Gamma \vdash e : C$ *and* $e \to e'$ *then there exists a type* C' *such that* $\Gamma \vdash e' : C'$ *and* $C' \leq C$.

Proof. By induction on $e \to e'$, with a case analysis of the last rule used in the derivation.

Case E-CONTEXT: $e = E[e_1]$ and $e_1 \to e_1'$ and $e' = E[e_1']$

By the decomposition lemma we have that there exists a type B such that $\Gamma \vdash e_1 : B$. By the induction hypothesis applied to e_1 we have that there exists a type B' such that $\Gamma \vdash e_1' : B'$ and $B' \leq B$. Then, by the context lemma we have that there exists a type C' such that $\Gamma \vdash E[e_1'] : C'$ and $C' \leq C$, as required.

Case E-PROJ: $e = \texttt{new}\ C_0(\overline{v}).f_i$ and $e' = v_i$ with *fields*$(C_0) = \overline{C\ f}$

As the typing rules for Featherweight Java are syntax-directed, the last rule used in the derivation of $\Gamma \vdash e : C$ must have been T-FIELD. Therefore we must also have a derivation $\Gamma \vdash \texttt{new}\ C_0(\overline{v}) : D_0$ with *fields*$(D_0) = \overline{D\ g}$ and $C = D_i$. By a similar argument, the last rule used in this derivation must have been T-NEW and so $D_0 = C_0$ and we have derivations $\Gamma \vdash \overline{v} : \overline{B}$ with $\overline{B} \leq \overline{D}$. From $D_0 = C_0$ (and as *fields* is a function) we have $\overline{C\ f} = \overline{D\ g}$, and hence $C = C_i$. Thus, $\Gamma \vdash v_i : B_i$ with $B_i \leq C_i$, as required.

Case E-INVK: $e = (\texttt{new}\ C_0(\overline{v})).m(\overline{u})$ and $e' = [\overline{x} \mapsto \overline{u}, \texttt{this} \mapsto \texttt{new}\ C_0(\overline{v})]e$ with *mbody*$(m, C_0) = (\overline{x}, e)$

By similar reasoning as in the previous case, the last two rules in the derivation of $\Gamma \vdash e : C$ must have been T-INVK and T-NEW with $\Gamma \vdash \texttt{new}\ C_0(\overline{v}) : C_0$ and $\Gamma \vdash \overline{u} : \overline{B}$ and *mtype*$(m, C_0) = \overline{C} \to C$ with $\overline{B} \leq \overline{C}$. By the method typing lemma, there exist types C_0' and C' such that $\overline{x} : \overline{C}, \texttt{this} : C_0' \vdash e : C'$. By the substitution lemma we have $\vdash [\overline{x} \mapsto \overline{u}, \texttt{this} \mapsto \texttt{new}\ C_0(\overline{v})]e : C''$ with $C'' \leq C'$. By weakening we have $\Gamma \vdash [\overline{x} \mapsto \overline{u}, \texttt{this} \mapsto \texttt{new}\ C_0(\overline{v})]e : C''$. The required result follows as $C'' \leq C$ by S-TRANS.

Case E-CAST: $e = (C)\ (\texttt{new}\ C_0(\overline{v}))$ and $e' = \texttt{new}\ C_0(\overline{v})$ with $C_0 \leq C$

By similar reasoning as the previous cases, the last two rules in the derivation of $\Gamma \vdash e : C$ must have been T-UCAST and T-NEW with $\Gamma \vdash \texttt{new}\ C_0(\overline{v}) : C_0$. The result is immediate as $C_0 \leq C$.

□

1.2 Progress

The proof of progress also relies on a few supporting lemmas.

Lemma (Canonical Forms)**.** *If* $\vdash v : C$ *then* $v = \texttt{new}\ C(\overline{v})$.

Lemma (Inversion)**.**

1. *If* $\vdash (\texttt{new}\ C(\overline{v})).f_i : C_i$ *then* $\texttt{fields}(C) = \overline{C\ f}$ *and* $f_i \in \overline{f}$.
2. *If* $\vdash (\texttt{new}\ C(\overline{v})).m(\overline{u}) : C$ *then* $\texttt{mbody}(m, C) = (\overline{x}, e)$ *and* $|\overline{u}| = |\overline{e}|$.

Lemma (Progress)**.** *Let* e *be an expression such that* $\vdash e : C$*. Then either:*

1. e *is a value,*
2. *there exists an expression* e' *such that* $e \to e'$*, or*
3. $e = E[(B)\ (\texttt{new}\ A(\overline{v}))]$ *with* $A \not\leq B$.

Proof. By induction on $\vdash e : C$, with a case analysis on the last rule used in the derivation.

Case T-VAR: $e = x$ with $\emptyset(x) = C$

Can't happen, as $\emptyset(x)$ is undefined.

Case T-FIELD: $e = e_0.f$ with $\vdash e_0 : C_0$ and *fields*$(C_0) = \overline{C\ f}$ and $C = C_i$

By the induction hypothesis applied to e_0 we have that either e_0 is a value, there exists e_0' such that $e_0 \to e_0'$, or there exists E such that $e_0 = E_0[(B)\ (\texttt{new}\ A(\overline{v}))]$ with $A \not\leq B$. We analyze each of these subcases:

1. If e_0 is a value then by the canonical forms lemma, $e_0 = \texttt{new}\ C_0(\overline{v})$ and by the inversion lemma $f \in \overline{f}$. By E-PROJ we have $e \to v_i$.
2. Alternatively, if there exists an expression such that $e_0 \to e_0'$ then by E-CONTEXT we have $e = E[e_0] \to E[e_0']$ where $E = [\cdot].f$.
3. Otherwise, if $e_0 = E_0[(B)\ (\texttt{new}\ A(\overline{v}))]$ with $A \not\leq B$ then we have $e = E[(B)\ (\texttt{new}\ A(\overline{v}))]$ where $E = [\cdot].f$, which finishes the case.

Case T-INVK: $e = e_0.m(\overline{e})$ with $\vdash e_0 : C_0$ and *mtype*$(m, C_0) = \overline{B} \to C$ and $\vdash \overline{e} : \overline{A}$ and $\overline{A} \leq \overline{B}$

By the induction hypothesis applied to e_0 we have that either e_0 is a value, there exists e_0' such that $e_0 \to e_0'$, or there exists E such that $e_0 = E_0[(B)\ (\texttt{new}\ A(\overline{v}))]$ with $A \not\leq B$. We analyze each of these subcases:

1. If e_0 is a value then by the canonical forms lemma, $e_0 = \texttt{new}\ C_0(\overline{v})$. If $\overline{e}$ is a list of values $\overline{u}$, then by the inversion lemma we have $|\overline{u}| = |\overline{x}|$ where *mbody*$(m, C_0) = (\overline{x}, e_0')$. By E-INVK we have $e \to [\overline{x} \mapsto \overline{u}, \texttt{this} \mapsto \texttt{new}\ C_0(\overline{v})]e_0'$. Otherwise, let i be the least index of an expression in $\overline{e}$ that is not a value. By the induction hypothesis applied to e_i we have that e_i is a value, or there exists e_i' such that $e_i \to e_i'$ or there exists E_i such that $e_i = E_i[(B)\ (\texttt{new}\ A(\overline{v}))]$ and $A \not\leq B$. In the first subsubcase, then we have a contradiction to our assumption that i is the index of the least expression in $\overline{e}$ that is not a value. Otherwise let $E = (\texttt{new}\ C_0(\overline{v})).m(e_1, \ldots, e_{i-1}, E_i, e_{i+1}, \ldots |\overline{e}|)$. In the second subcase, we have $e = E[e_i] \to E[e_i']$ by E-CONTEXT. In the third subcase, we have $e = E[(B)\ (\texttt{new}\ A(\overline{v}))]$ with $A \not\leq B$.
2. Alternatively, if there exists an expression such that $e_0 \to e_0'$ then by E-CONTEXT we have $E[e_0] \to E[e_0']$ where $E = [\cdot].m(\overline{e})$.
3. Otherwise, if $e_0 = E_0[(B)\ (\texttt{new}\ A(\overline{v}))]$ with $A \not\leq B$ then we have $e = E[(B)\ (\texttt{new}\ A(\overline{v}))]$ where $E = [\cdot].m(\overline{e})$, which finishes the case.

Case T-NEW: $e = \texttt{new}\ C(\overline{e})$ and *fields*$(C) = \overline{C\ f}$ and $\vdash \overline{e} : \overline{B}$ and $\overline{B} \leq \overline{C}$

If $\overline{e}$ is a list of values $\overline{u}$, then e is a value. Otherwise, let i be the least index of an expression in $\overline{e}$ that is not a value. By the induction hypothesis applied to e_i we have that e_i is a value, or there exists e_i' such that $e_i \to e_i'$ or there exists E_i such that $e_i = E_i[(B)\ (\texttt{new}\ A(\overline{v}))]$ and $A \not\leq B$. We analyze each of these subcases:

1. If e_i is a value then we have a contradiction to our assumption that i is the index of the least expression in $\overline{e}$ that is not a value.

2. If there exists e_i' such that $e_i \to e_i'$ then let $E = (\texttt{new}\ C(e_1, \ldots, e_{i-1}, E_i, e_{i+1}, \ldots, |\overline{e}|)$. By E-CONTEXT we have $e = E[e_i] \to E[e_i']$.
3. Otherwise, if there exists E_i with $e_i = E_i[(B)\ (\texttt{new}\ A(\overline{v}))]$ and $A \not\leq B$ then let $E = (\texttt{new}\ C(e_1, \ldots, e_{i-1}, E_i, e_{i+1}, \ldots, |\overline{e}|)$. By construction we have $e = E[(B)\ (\texttt{new}\ A(\overline{v}))]$, which finishes the case.

Case T-UCAST: $e = (C)\ e$ with $\vdash e_0 : D$ and $D \leq C$

By the induction hypothesis applied to e_0 we have that either e_0 is a value, there exists e_0' such that $e_0 \to e_0'$, or there exists E such that $e_0 = E_0[(B)\ (\texttt{new}\ A(\overline{v}))]$ with $A \not\leq B$. We analyze each of these subcases:

1. If e_0 is a value then by the canonical forms lemma, $e_0 = \texttt{new}\ D(\overline{v})$. By E-CAST we have $e \to \texttt{new}\ D(\overline{v})$.
2. Alternatively, if there exists an expression such that $e_0 \to e_0'$ then by E-CONTEXT we have $e = E[e_0] \to E[e_0']$ where $E = (C)\ [\cdot]$.
3. Otherwise, if $e_0 = E_0[(B)\ (\texttt{new}\ A(\overline{v}))]$ with $A \not\leq B$ then we have $e = E[(B)\ (\texttt{new}\ A(\overline{v}))]$ where $E = (C)\ [\cdot]$, which finishes the case.

Case T-DCAST: $e = (C)\ e$ with $\vdash e_0 : D$ and $C \leq D$ and $C \neq D$

By the induction hypothesis applied to e_0 we have that either e_0 is a value, there exists e_0' such that $e_0 \to e_0'$, or there exists E such that $e_0 = E_0[(B)\ (\texttt{new}\ A(\overline{v}))]$ with $A \not\leq B$. We analyze each of these subcases:

1. If e_0 is a value then by the canonical forms lemma we have that $e = \texttt{new}\ D(\overline{v})$. Let $E = [\cdot]$. We immediately $e = E[(C)\ \texttt{new}\ C(\overline{v})]$ with $D \not\leq C$.
2. Alternatively, if there exists an expression such that $e_0 \to e_0'$ then by E-CONTEXT we have $e = E[e_0] \to E[e_0']$ where $E = (C)\ [\cdot]$.
3. Otherwise, if $e_0 = E_0[(B)\ (\texttt{new}\ A(\overline{v}))]$ with $A \not\leq B$ then we have $e = E[(B)\ (\texttt{new}\ A(\overline{v}))]$ where $E = (C)\ [\cdot]$, which finishes the case.

Case T-SCAST: similar to the previous case.

□

2 Object Encodings

Another way to formalize the semantics of object-oriented languages is to define translations that map them into λ-calculus. In fact, with records, fixpoints, subtyping, and recursive/existential types, we have all of the tools needed to do this. We begin by briefly reviewing the main features of object-oriented languages.

Dynamic dispatch Dynamic dispatch allows the code executed when a message is sent to an object—e.g., $o.m(x)$—to be determined by run-time values and not (just) by compile-time information such as types. As a result, different objects may respond to the same message in different ways. For example, consider the following Java program:

```
interface Shape { ... void draw() { ... } }
class Circle extends Shape { ... void draw() { ... } }
class Square extends Shape { ... void draw() { ... } }
...
Shape s = ...; //could be a circle a square, or something else.
s.draw();
```

Invoking `s.draw()` could run the code for any of the methods shown in the program (or for any other class that extends `Shape`).

In Java, all methods (except for static methods) are dispatched dynamically. In C++, only virtual members are dispatched dynamically. Note that dynamic dispatch is not the same as overloading, which is usually resolved using the static types of the arguments to the function being called.

Encapsulation Encapsulation allows an object to hide the representations of certain internal data structures. For example, Java programmers often keep instance variables private and write public methods for accessing and modifying the data stored in those variables.

```
class Circle extends Shape {
  private Point center;
  private int radius;
  ...
  public Point getX() { return center.x }
  public Point getY() { return center.y }
}
```

the coordinates of the center of the circle can only be obtained by invoking the `getX` and `getY` methods. The result is that all interactions with the object must be performed by invoking the methods exposed in its public interface and not by directly manipulating its instance variables.

Subtyping Another characteristic feature of object-oriented languages is subtyping. Subtyping fits naturally with object-oriented languages because (ignoring languages such as Java that allow certain objects to manipulate instance variables directly) the only way to interact with an object is to invoke a method. As a result, an object that supports the same methods as another object can be used wherever the second is expected. For example, if we write a method that takes an object of type `Shape` above as a parameter, it is safe to pass `Circle`, `Square`, or any other subtype of `Shape`, because they each support the methods listed in the `Shape` interface.

Inheritance To avoid writing the same code twice, it is often useful to be able to reuse the definition of one kind of object to define another kind of object. In class-based languages, inheritance is often supported through subclassing. For example, in the following Java program,

```
class A {
  public int f(...) { ... g(...) ... }
  public bool g(...) { ... }
}
```

```
class B extends A {
  public bool g(...) { ... }
}
...
new B.f(...)
```

`B` inherits the `f` method of its superclass `A`.

One way to implement inheritance is by duplicating code but this wastes space. Most languages introduce a level of indirection instead so that the code compiled for the object being inherited from can be used directly by the object doing the inheriting.

Note that inheritance is different than subtyping: subtyping is a relation on types while inheritance is a relation on implementations. These two notions are conflated in some languages like Java but kept separate in languages like C++ (which allows a "private base class") as well as in languages that are not based on classes.

Open recursion Finally, many object-oriented languages allow objects to invoke their own methods using the special keyword `this` (or `self`). Implementing `this` in the presence of inheritance requires deferring the binding of `this` until the object is actually created. We will see an example of this in the next section.

2.1 Simple Record Encoding

Let us start with a simple example, developing a representation for two-dimensional point objects using records and references. Records provide both dynamic lookup and subtyping: given a value v of some record type τ, the expression $v.f$ evaluates to a value that is determined by v not by τ—i.e., dynamic dispatch! Moreover, because the subtyping relation on record types allows extension, code that expects an object to have type τ can be used with a value of any subtype of τ.

Here is a simple example showing how we can encode records using objects. For concreteness, we use OCaml syntax rather than λ-calculus. The notation `(fun x -⟩ e)` denotes a λ-abstraction.

```
type pointRep = { x:int ref;
                  y:int ref }

type point = { movex:int -> unit;
               movey:int -> unit }

let pointClass : pointRep -> point =
  (fun (r:pointRep) ->
    { movex = (fun d -> r.x := !(r.x) + d);
      movey = (fun d -> r.y := !(r.x) + d) })

let newPoint : int -> int -> point =
  (fun (x:int) ->
    (fun (y:int) ->
      pointClass { x=ref x; y = ref y }))
```

The `pointRep` type defines the representation for the object's instance variables—a record with a mutable reference for each field. The `pointClass` function takes a record with this type and builds an object—a record with functions `movex` and `movey`, which translate the point horizontally and vertically. The constructor `newPoint` takes two integers, `x` and `y`, and uses `pointClass` to build an object whose fields are initialized to those coordinates.

2.2 Inheritance

Just as in standard object-oriented languages, we can extend our two-dimensional point with an extra coordinate by defining a subclass that inherits the methods of its superclass.

```
type point3D = { movex:int -> unit;
                 movey:int -> unit;
                 movez:int -> unit }

let point3DClass : point3DRep -> point3D =
  (fun (r:point3DRep) ->
    let super = pointClass r in
    { movex = super.movex;
      movey = super.movey;
      movez = (fun d -> r.z := !(r.x) + d) } )

let newPoint3D : int -> int -> int -> point3D =
  (fun (x:int) ->
    (fun (y:int) ->
      (fun (z:int) ->
        point3DClass { x=ref x; y = ref y; z = ref z }))))
```

The most interesting part of this program is the `point3DClass` function. It takes an argument of type `point3DRep` and uses `pointClass` to build a `point` object `super`. It fills in the `movex` and `movey` methods for the object being constructed with the corresponding fields from `super`—i.e., it inherits those methods from the superclass—and defines the new method `movez` directly. Note that we can pass a record of type `point3DRep` to `pointClass` because `point3DRep` is a subtype of `pointRep`.

2.3 Self

Adding support for `self` is a bit trickier because we need `self` to be bound late. Here is an example that illustrates one possible implementation technique:

```
type altPointRep = { x:int ref;
                     y:int ref }

type altPoint = { movex:int -> unit;
                  movey:int -> unit;
                  move: int -> int -> unit }
```

```
let altPointClass : altPointRep -> altPoint ref -> altPoint =
  (fun (r:altPointRep) ->
    (fun (self:altPoint ref) ->
      { movex = (fun d -> r.x := !(r.x) + d);
        movey = (fun d -> r.y := !(r.y) + d);
        move  = (fun dx dy -> (!self.movex) dx; (!self.movey) dy) }))

let dummyAltPoint : altPoint =
  { movex = (fun d -> ());
    movey = (fun d -> ());
    move  = (fun dx dy -> ()) }

let newAltPoint : int -> int -> altPoint =
  (fun (x:int) ->
    (fun (y:int) ->
      let r = { x=ref x; y = ref y } in
      let cref = ref dummyAltPoint in
      cref := altPointClass r cref;
      !cref ))
```

For the sake of the example, we have added a method `move` that takes two integers and translates the point both horizontally and vertically. The implementation of `move` invokes the `movex` and `movey` methods from the current object—i.e., `self`.

To make `self` work as expected, we use a trick similar to the one we used to implement recursive definitions in our λ-calculus interpreter. Compared to our previous object encodings there are two key changes. First, the `newAltPointClass` now takes the `self` reference as an explicit parameter. This parameter is filled in with the actual object when it is constructed. Second, the `newAltPoint` constructor "ties the recursive knot" by allocating a reference cell for the object—filled in initially with a dummy value—and then "back-patching" the reference with the actual object returned by the class.

There is a small problem with this encoding of self: the `self` parameter to `altPointClass` has type `altPoint ref` and references have an *invariant* subtyping rule. As a result, the type system will not allow us to pass a reference to an object generated by a subclass. However, as we do not assign to `self`, it would be safe to use a *covariant* subtyping rule. See Pierce, Chapter 18 for details on how this issue can be resolved.

2.4 Encapsulation

The simple object encoding we have developed in this section already gives us basic encapsulation. After we build an object, the instance variables are totally hidden—we can only manipulate them using object's methods. More complicated forms of abstraction and information hiding can be obtained using existential types. For the details of how records and existential types can be combined to encode objects: see "Comparing Object Encodings", by Bruce, Cardelli, and Pierce, Information and Computation 155(1/2):108–133, 1999.