

Design Principles of Programming Languages

Case Study: Featherweight Java

(slides based on Benjamin Pierce' slides)

Zhenjiang Hu, Haiyan Zhao, Yingfei Xiong

Peking University, Spring Term, 2014



The essence of objects

- Dynamic dispatch
- Encapsulation of state with behavior
- Behavior-based subtyping
- Inheritance (incremental definition of behaviors)
- Access of super class
- Open recursion through [this](#)



What's missing (wrt. Java, say)

We haven't really captured the peculiar status of classes which are *both run-time and compile-time* things) — we've captured the run-time aspect, but not the way in which classes get used as *types* in Java.

Also not *named* types with *declared* subtyping

Nor recursive types

Nor run-time type analysis (casting, etc.)

(... nor lots of other stuff)



Modeling Java



About models (of things in general)

No such thing as a “*perfect model*” — The nature of a model is to abstract away from details!

So models are never just “good” [or “bad”]: they are always “good [or bad] for *some specific set of purposes.*”



Models of Java

Lots of different purposes → lots of different kinds of models

- Source-level *vs.* bytecode level
- Large (inclusive) *vs.* small (simple) models
- Models of type system *vs.* models of run-time features (not entirely separate issues)
- Models of specific features (exceptions, concurrency, reflection, class loading, ...)
- Models designed for extension



Featherweight Java

Purpose: model “core OO features” and their types and *nothing else*.

History:

- Originally proposed by a Penn visiting student (Atsushi Igarashi) as a tool for analyzing GJ (“Java plus generics”), which later became Java 1.5
- Since used by many others for studying a wide variety of Java features and proposed extensions



Things left out of FJ

- Reflection, concurrency, class loading, inner classes, ...
- Exceptions, loops, ...
- Interfaces, overloading, ...
- Assignment (!!)



Things left in FJ

- Classes and objects
- Methods and method invocation
- Fields and field access
- Inheritance (including open recursion through [this](#))
- Casting



Example

```
class A extends Object { A() { super(); } }
```

```
class B extends Object { B() { super(); } }
```

```
class Pair extends Object {  
    Object fst;  
    Object snd;  
  
    Pair(Object fst, Object snd) {  
        super(); this.fst = fst; this.snd = snd; }  
  
    Pair setfst(Object newfst) {  
        return new Pair(newfst, this.snd); }  
}
```



Conventions

For syntactic regularity...

- Always include superclass (even when it is **Object**)
- Always write out constructor (even when trivial)
- Always call **super** from constructor (even when no arguments are passed)
- Always explicitly name receiver object in method invocation or field access (even when it is **this**)
- Methods always consist of a single **return** expression
- Constructors always
 - Take same number (and types) of parameters as fields of the class
 - Assign constructor parameters to “local fields”
 - Call **super** constructor to assign remaining fields
 - Do nothing else



Formalizing FJ



Nominal type systems

Big dichotomy in the world of programming languages:

➤ *Structural* type systems:

- What matters about a type (for typing, subtyping, etc.) is just its structure.
- Names are just convenient (but inessential) abbreviations.

➤ *Nominal* type systems:

- Types are always named.
- Typechecker mostly manipulates names, not structures.
- Subtyping is declared explicitly by programmer (and checked for consistency by compiler).



Advantages of Structural Systems

Somewhat simpler, cleaner, and more elegant (no need to always work wrt. a set of “*name definitions*”)

Easier to extend (e.g. with parametric polymorphism)

Caveat: when recursive types are considered, some of this simplicity and elegance slips away...



Advantages of Nominal Systems

Recursive types fall out easily

Using names everywhere makes typechecking (and subtyping, etc.) easy and efficient

Type names are also useful at run-time (for casting, type testing, reflection, ...).

Java (like most other mainstream languages) is a nominal system.



Representing objects

Our decision to omit assignment has a *nice side effect*...

The only ways in which two objects can differ are (1) their classes and (2) the parameters passed to their constructor when they were created.

All this information is available in the **new** expression that creates an object. So we can *identify* the created object with the **new** expression.

Formally: object values have the form **new** C(\bar{v})



FJ Syntax



Syntax (terms and values)

$t ::=$

x

$t.f$

$t.m(\bar{t})$

$\text{new } C(\bar{t})$

$(C) t$

terms

variable

field access

method invocation

object creation

cast

$v ::=$

$\text{new } C(\bar{v})$

values

object creation



Syntax (methods and classes)

$K ::=$ *constructor declarations*
 $C(\bar{C} \ \bar{f}) \ \{\text{super}(\bar{f}); \ \text{this}.\bar{f}=\bar{f};\}$

$M ::=$ *method declarations*
 $C \ m(\bar{C} \ \bar{x}) \ \{\text{return } t;\}$

$CL ::=$ *class declarations*
 $\text{class } C \ \text{extends } C \ \{\bar{C} \ \bar{f}; \ K \ \bar{M}\}$



Subtyping



Subtyping

As in Java, subtyping in FJ *is declared*.

Assume we have a (global, fixed) *class table* CT mapping class names to definitions.

$$\frac{CT(C) = \text{class } C \text{ extends } D \{ \dots \}}{C \prec: D}$$

$$C \prec: D$$

$$C \prec: C$$

$$\frac{C \prec: D \quad D \prec: E}{C \prec: E}$$

$$C \prec: E$$


More auxiliary definitions

From the class table, we can read off a number of other useful properties of the definitions (which we will need later for typechecking and operational semantics)...



Field(s) lookup

$$fields(Object) = \emptyset$$

$$CT(C) = \text{class } C \text{ extends } D \{ \bar{C} \ \bar{f}; K \ \bar{M} \}$$

$$fields(D) = \bar{D} \ \bar{g}$$

$$fields(C) = \bar{D} \ \bar{g}, \bar{C} \ \bar{f}$$



Method type lookup

$$CT(C) = \text{class } C \text{ extends } D \{ \bar{C} \ \bar{f}; \ K \ \bar{M} \}$$

$$B \ m \ (\bar{B} \ \bar{x}) \ \{ \text{return } t; \} \in \bar{M}$$

$$mtype(m, C) = \bar{B} \rightarrow B$$

$$CT(C) = \text{class } C \text{ extends } D \{ \bar{C} \ \bar{f}; \ K \ \bar{M} \}$$

$$m \text{ is not defined in } \bar{M}$$

$$mtype(m, C) = mtype(m, D)$$



Method body lookup

$CT(C) = \text{class } C \text{ extends } D \{ \bar{C} \bar{f}; K \bar{M} \}$
 $B \ m \ (\bar{B} \ \bar{x}) \ \{ \text{return } t; \} \in \bar{M}$

$$mbody(m, C) = (\bar{x}, t)$$

$CT(C) = \text{class } C \text{ extends } D \{ \bar{C} \bar{f}; K \bar{M} \}$
 $m \text{ is not defined in } \bar{M}$

$$mbody(m, C) = mbody(m, D)$$



Valid method overriding

$mtype(m, D) = \bar{D} \rightarrow D_0$ implies $\bar{C} = \bar{D}$ and $C_0 = D_0$

$override(m, D, \bar{C} \rightarrow C_0)$



Evaluation



The example again

```
class A extends Object { A() { super(); } }
```

```
class B extends Object { B() { super(); } }
```

```
class Pair extends Object {  
    Object fst;  
    Object snd;
```

```
    Pair(Object fst, Object snd) {  
        super(); this.fst = fst; this.snd = snd; }
```

```
    Pair setfst(Object newfst) {  
        return new Pair(newfst, this.snd); }
```

```
}
```



Evaluation

Projection:

`new Pair(new A(), new B()).snd` \longrightarrow `new B()`



Evaluation

Casting:

```
(Pair)new Pair(new A(), new B())  
→ new Pair(new A(), new B())
```



Evaluation

Method invocation:

```
new Pair(new A(), new B()).setfst(new B())
```

```
→ [ newfst ↦ new B(),  
    this ↦ new Pair(new A(), new B()) ]  
new Pair(newfst, this.snd)
```

```
i.e., new Pair(new B(), new Pair(new A(), new B()).snd)
```

```
class A extends Object { A() { super(); } }  
class B extends Object { B() { super(); } }  
class Pair extends Object {  
    Object fst;  
    Object snd;  
    Pair(Object fst, Object snd) {  
        super(); this.fst = fst; this.snd = snd; }  
    Pair setfst(Object newfst) {  
        return new Pair(newfst, this.snd); }  
}
```



Evaluation

Method invocation:

((Pair) (new Pair(new Pair(new A(), new B()), new A())
 .fst).snd

→ ((Pair) new Pair(new A(), new B())).snd

→ new Pair(new A(), new B()).snd

→ new B()

```
class A extends Object { A() { super(); } }
class B extends Object { B() { super(); } }
class Pair extends Object {
    Object fst;
    Object snd;
    Pair(Object fst, Object snd) {
        super(); this.fst = fst; this.snd = snd; }
    Pair setfst(Object newfst) {
        return new Pair(newfst, this.snd); }
}
```



Evaluation rules

$$\frac{fields(C) = \bar{c} \ \bar{f}}{(new \ C(\bar{v})) . f_i \longrightarrow v_i} \quad (E\text{-PROJNEW})$$

$$\frac{mbody(m, C) = (\bar{x}, t_0)}{(new \ C(\bar{v})) . m(\bar{u}) \longrightarrow [\bar{x} \mapsto \bar{u}, \text{this} \mapsto new \ C(\bar{v})] t_0} \quad (E\text{-INVKNOW})$$

$$\frac{C <: D}{(D) (new \ C(\bar{v})) \longrightarrow new \ C(\bar{v})} \quad (E\text{-CASTNEW})$$



Evaluation rules

$$\frac{t_0 \longrightarrow t'_0}{t_0.f \longrightarrow t'_0.f} \quad (\text{E-FIELD})$$

$$\frac{t_0 \longrightarrow t'_0}{t_0.m(\bar{t}) \longrightarrow t'_0.m(\bar{t})} \quad (\text{E-INVK-RECV})$$

$$\frac{t_i \longrightarrow t'_i}{v_0.m(\bar{v}, t_i, \bar{t}) \longrightarrow v_0.m(\bar{v}, t'_i, \bar{t})} \quad (\text{E-INVK-ARG})$$

$$\frac{t_i \longrightarrow t'_i}{\text{new } C(\bar{v}, t_i, \bar{t}) \longrightarrow \text{new } C(\bar{v}, t'_i, \bar{t})} \quad (\text{E-NEW-ARG})$$

$$\frac{t_0 \longrightarrow t'_0}{(C)t_0 \longrightarrow (C)t'_0} \quad (\text{E-CAST})$$



Typing



Notes

FJ has no rule of subsumption (because we want to follow Java). The typing rules are algorithmic.

(Where would this make a difference?...)



Typing rules

$$\frac{x:C \in \Gamma}{\Gamma \vdash x : C}$$

(T-VAR)



Typing rules

$$\frac{\Gamma \vdash t_0 : C_0 \quad \text{fields}(C_0) = \bar{c} \ \bar{f}}{\Gamma \vdash t_0.f_j : C_j} \quad (\text{T-FIELD})$$



Typing rules

$$\frac{\Gamma \vdash t_0 : D \quad D <: C}{\Gamma \vdash (C)t_0 : C} \quad (\text{T-UCAST})$$

$$\frac{\Gamma \vdash t_0 : D \quad C <: D \quad C \neq D}{\Gamma \vdash (C)t_0 : C} \quad (\text{T-DCAST})$$



Typing rules

$$\frac{\begin{array}{l} \Gamma \vdash t_0 : C_0 \\ mtype(m, C_0) = \bar{D} \rightarrow C \\ \Gamma \vdash \bar{t} : \bar{C} \quad \bar{C} <: \bar{D} \end{array}}{\Gamma \vdash t_0.m(\bar{t}) : C} \quad (\text{T-INVK})$$

Note that this rule “has subsumption built in” — i.e., the typing relation in FJ is written in the *algorithmic* style of chapter 16, not the declarative style of chapter 15.



Java typing is algorithmic

The Java typing relation is defined in the algorithmic style, for (at least) two reasons:

1. In order to perform static *overloading resolution*, we need to be able to speak of “the type” of an expression
2. We would otherwise run into trouble with typing of conditional expressions



Java typing must be algorithmic

We haven't included them in FJ, but full Java has both *interfaces* and *conditional expressions*.

The two together actually make the declarative style of typing rules unworkable!



Java conditionals

$$\frac{t_1 \in \text{bool} \quad t_2 \in T_2 \quad t_3 \in T_3}{t_1 ? t_2 : t_3 \in ?}$$

Actual Java rule (algorithmic):

$$\frac{t_1 \in \text{bool} \quad t_2 \in T_2 \quad t_3 \in T_3}{t_1 ? t_2 : t_3 \in \min(T_2, T_3)}$$



More standard (declarative) rule

$$\frac{t_1 \in \text{bool} \quad t_2 \in T \quad t_3 \in T}{t_1 ? t_2 : t_3 \in T}$$

Algorithmic version

$$\frac{t_1 \in \text{bool} \quad t_2 \in T_2 \quad t_3 \in T_3}{t_1 ? t_2 : t_3 \in T_2 \vee T_3}$$

Requires *Joins* !



Java has no joins

But, in full Java (with interfaces), there are types that have no join!

E.g.:

```
interface I {...}
```

```
interface J {...}
```

```
interface K extends I,J {...}
```

```
interface L extends I,J {...}
```

K and **L** have no join (least upper bound) — both **I** and **J** are common upper bounds, but neither of these is less than the other.



FJ Typing rules

$$\frac{\begin{array}{l} \text{fields}(C) = \bar{D} \ \bar{f} \\ \Gamma \vdash \bar{t} : \bar{C} \quad \bar{C} <: \bar{D} \end{array}}{\Gamma \vdash \text{new } C(\bar{t}) : C}$$

(T-NEW)



Typing rules (methods, classes)

$$\frac{
 \begin{array}{l}
 \bar{x} : \bar{C}, \text{this} : C \vdash t_0 : E_0 \quad E_0 <: C_0 \\
 CT(C) = \text{class } C \text{ extends } D \{ \dots \} \\
 \text{override}(m, D, \bar{C} \rightarrow C_0)
 \end{array}
 }{
 C_0 \text{ m } (\bar{C} \bar{x}) \{ \text{return } t_0; \} \text{ OK in } C
 }$$

$$\frac{
 \begin{array}{l}
 K = C(\bar{D} \bar{g}, \bar{C} \bar{f}) \{ \text{super}(\bar{g}); \text{this}.\bar{f} = \bar{f}; \} \\
 \text{fields}(D) = \bar{D} \bar{g} \quad \bar{M} \text{ OK in } C
 \end{array}
 }{
 \text{class } C \text{ extends } D \{ \bar{C} \bar{f}; K \bar{M} \} \text{ OK}
 }$$



Properties



Progress

Problem: well-typed programs can get stuck.

How?

Cast failure:

(A)new Object()



Formalizing Progress

Solution: Weaken the statement of the progress theorem to

*A well-typed FJ term is either a **value** or can **reduce one step** or is **stuck at a failing cast**.*

Read the book for the concrete solution.



Preservation

Theorem [Preservation]: If $\Gamma \vdash t : C$ and $t \rightarrow t'$, then $\Gamma \vdash t' : C'$ for some $C' \leq C$.

Proof: Straightforward induction.

???



Preservation?

Surprise: well-typed programs can step to ill-typed ones!
(How?)

(A) (Object)new B() \longrightarrow (A)new B()



Solution: “Stupid Cast” typing rule

Add *another typing rule*, marked “*stupid*” to indicate that an implementation should generate a warning if this rule is used.

$$\frac{\Gamma \vdash t_0 : D \quad C \not\leq D \quad D \not\leq C \quad \textit{stupid warning}}{\Gamma \vdash (C)t_0 : C} \quad (\text{T-SCAST})$$

This is an example of a modeling technicality; not very interesting or deep, but we have to get it right if we’re going to claim that the model is an accurate representation of (this fragment of) Java.



Correspondence with Java

Let's try to state precisely what we mean by “FJ corresponds to Java”:

Claim:

1. Every syntactically well-formed FJ program is also a syntactically well-formed Java program.
2. A syntactically well-formed FJ program is typable in FJ (without using the T-SCast rule.) iff it is typable in Java.
3. A well-typed FJ program behaves the same in FJ as in Java. (E.g., evaluating it in FJ diverges iff compiling and running it in Java diverges.)

Of course, without a formalization of full Java, we cannot prove this claim. But it's still very useful to say precisely what we are trying to accomplish—e.g., it provides a rigorous way of judging counterexamples. (Cf. “conservative extension” between logics.)



Homework😊

- 18.11.1
- Please submit electronically

