Featherweight Java

A Minimal Core Calculus for Java and GJ

Atsushi Igarashi Benjamin Pierce
Dept. of Comp. & Info. Sci.
University of Pennsylvania
{igarasha,bcpierce}@saul.cis.upenn.edu

Philip Wadler
Bell Laboratories
Lucent Technologies
wadler@research.bell-labs.com

University of Pennsylvania
Technical Report MS-CIS-99-25

October 26, 1999

Abstract

Several recent studies have introduced lightweight versions of Java: reduced languages in which complex features like threads and reflection are dropped to enable rigorous arguments about key properties such as type safety. We carry this process a step further, omitting almost all features of the full language (including interfaces and even assignment) to obtain a small calculus, Featherweight Java, for which rigorous proofs are not only possible but easy.

Featherweight Java bears a similar relation to full Java as the lambda-calculus does to languages such as ML and Haskell. It offers a similar computational "feel," providing classes, methods, fields, inheritance, and dynamic typecasts, with a semantics closely following Java's. A proof of type safety for Featherweight Java thus illustrates many of the interesting features of a safety proof for the full language, while remaining pleasingly compact. The syntax, type rules, and operational semantics of Featherweight Java fit on one page, making it easier to understand the consequences of extensions and variations.

As an illustration of its utility in this regard, we extend Featherweight Java with *generic classes* in the style of GJ (Bracha, Odersky, Stoutamire, and Wadler) and give a detailed proof of type safety. The extended system formalizes for the first time some of the key features of GJ.

1 Introduction

"Inside every large language is a small language struggling to get out..."

Formal modeling can offer a significant boost to the design of complex real-world artifacts such as programming languages. A formal model may be used to describe some aspect of a design precisely, to state and prove its properties, and to direct attention to issues that might otherwise be overlooked. In formulating a model, however, there is a tension between completeness and compactness: the more aspects the model addresses at the same time, the more unwieldy it becomes. Often it is sensible to choose a model that is less complete but more compact, offering maximum insight for minimum investment. This strategy may be seen in a flurry of recent papers on the formal properties of Java, which omit advanced features such as concurrency and reflection and concentrate on fragments of the full language to which well-understood theory can be applied.

We propose Featherweight Java, or FJ, as a new contender for a *minimal* core calculus for modeling Java's type system. The design of FJ favors compactness over completeness almost obsessively, having just five forms of expression: object creation, method invocation, field access, casting, and variables. Its syntax, typing rules, and operational semantics fit comfortably on a single page. Indeed, our aim has been to omit as many features as possible – even assignment – while retaining the core features of Java typing. There is a direct correspondence between FJ and a purely functional core of Java, in the sense that every FJ program is literally an executable Java program.

FJ is only a little larger than Church's lambda calculus [3] or Abadi and Cardelli's object calculus [1], and is significantly smaller than previous formal models of class-based languages like Java, including those put forth by Drossopoulou, Eisenbach, and Khurshid [11], Syme [21], Nipkow and Oheimb [18], and Flatt, Krishnamurthi, and Felleisen [14, 15]. Being smaller, FJ lets us focus on just a few key issues. For example, we have discovered that capturing the behavior of Java's cast construct in a traditional "small-step" operational semantics is trickier than we would have expected, a point that has been overlooked or underemphasized in other models.

One use of FJ is as a starting point for modeling languages that extend Java. Because FJ is so compact, we can focus attention on essential aspects of the extension. Moreover, because the proof of soundness for pure FJ is very simple, a rigorous soundness proof for even a significant extension may remain manageable. The second part of the paper illustrates this utility by enriching FJ with generic classes and methods *à la* GJ [7]. The model omits some important aspects of GJ (such as "raw types" and type argument inference for generic method calls). Nonetheless, it led to the discovery and fix of one bug in the GJ compiler and, more importantly, has been a useful tool in clarifying our thought. Because the model is small, it is easy to contemplate further extensions, and we have begun the work of adding raw types to the model; so far, this has revealed at least one corner of the design that was underspecified.

Our main goal in designing FJ was to make a proof of type soundness ("well-typed programs don't get stuck") as concise as possible, while still capturing the essence of the soundness argument for the full Java language. Any language feature that made the soundness proof *longer* without making it significantly *different* was a candidate for omission. As in previous studies of type soundness in Java, we don't treat advanced features such as concurrency, inner classes, and reflection. Other Java features omitted from FJ include assignment, interfaces, overloading, messages to `super`, `null` pointers, base types (`int`, `bool`, etc.), abstract method declarations, shadowing of superclass fields by subclass fields, access control (`public`, `private`, etc.), and exceptions. The features of Java that we *do* model include mutually recursive class definitions, object creation, field access, method invocation, method override, method recursion through `this`, subtyping, and casting.

One key simplification in FJ is the omission of assignment. We assume that an object's fields are initialized by its constructor and never changed afterwards. This restricts FJ to a "functional" fragment of Java, in which many common Java idioms, such as use of enumerations, cannot be represented. Nonetheless, this fragment is computationally complete (it is easy to encode the lambda calculus into it), and is large enough to include many useful programs (many of the programs in Felleisen and Friedman's Java text [12] use a purely functional style). Moreover, most of the tricky typing issues in both Java and GJ are independent of assignment. An important exception is that the type inference algorithm for generic method invocation in GJ has some twists imposed on it by the need to maintain soundness in the presence of assignment. This paper treats a simplified version of GJ without type inference.

The remainder of this paper is organized as follows. Section 2 introduces the main ideas of Featherweight Java, presents its syntax, type rules, and reduction rules, and develops a type soundness proof. Section 3 extends Featherweight Java to Featherweight GJ, which includes generic classes and methods. Section 4 presents an erasure map from FGJ to FJ, modeling the techniques used to compile GJ into Java. Section 5 discusses related work, and Section 6 concludes.

2 Featherweight Java

In FJ, a program consists of a collection of class definitions plus an expression to be evaluated. (This expression corresponds to the body of the `main` method in Java.) Here are some typical class definitions in FJ.

```
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);
  }
}
```

For the sake of syntactic regularity, we always include the supertype (even when it is `Object`), we always write out the constructor (even for the trivial classes `A` and `B`), and we always write the receiver for a field access (as in `this.snd`) or a method invocation. Constructors always take the same stylized form: there is one parameter for each field, with the same name as the field; the `super` constructor is invoked on the fields of the supertype; and the remaining fields are initialized to the corresponding parameters. Here the supertype is always `Object`, which has no fields, so the invocations of `super` have no arguments. Constructors are the only place where `super` or `=` appears in an FJ program. Since FJ provides no side-effecting operations, a method body always consists of `return` followed by an expression, as in the body of `setfst()`.

In the context of the above definitions, the expression

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

evaluates to the expression

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

There are five forms of expression in FJ. Here, `new A()`, `new B()`, and `new Pair(e1,e2)` are *object constructors*, and `e3.setfst(e4)` is a *method invocation*. In the body of `setfst`, the expression `this.snd` is a *field access*, and the occurrences of `newfst` and `this` are *variables*. The syntax of FJ differs from Java in that `this` is a variable rather than a keyword.

The remaining form of expression is a *cast*. The expression

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

evaluates to the expression

```
new B().
```

Here, `((Pair)e7)`, where `e7` is `new Pair(...).fst`, is a cast. The cast is required, because `e7` is a field access to `fst`, which is declared to contain an `Object`, whereas the next field access, to `snd`, is only valid on a `Pair`. At run time, it is checked whether the `Object` stored in the `fst` field is a `Pair` (and in this case the check succeeds).

In Java, one may prefix a field or parameter declaration with the keyword `final` to indicate that it may not be assigned to, and all parameters accessed from an inner class must be declared `final`. Since FJ contains no assignment and no inner classes, it matters little whether or not `final` appears, so we omit it for brevity.

Dropping side effects has a pleasant side effect: evaluation can be easily formalized entirely within the syntax of FJ, with no additional mechanisms for modeling the heap. Moreover, in the absence of side effects, the order in which expressions are evaluated does not affect the final outcome, so we can define the operational semantics of FJ straightforwardly using a nondeterministic small-step reduction relation, following long-standing tradition in the lambda calculus. Of course, Java's call-by-value evaluation strategy is subsumed by this more general relation, so the soundness properties we prove for reduction will hold for Java's evaluation strategy as a special case.

There are three basic computation rules: one for field access, one for method invocation, and one for casts. Recall that, in the lambda calculus, the beta-reduction rule for applications assumes that the function is first simplified to a lambda abstraction. Similarly, in FJ the reduction rules assume the object operated upon is first simplified to a `new` expression. Thus, just as the slogan for the lambda calculus is "everything is a function," here the slogan is "everything is an object."

Here is the rule for field access in action:

$$\texttt{new Pair(new A(), new B()).snd} \longrightarrow \texttt{new B()}$$

Because of the stylized form for object constructors, we know that the constructor has one parameter for each field, in the same order that the fields are declared. Here the fields are `fst` and `snd`, and an access to the `snd` field selects the second parameter.

Here is the rule for method invocation in action (/ denotes substitution):

$$\begin{array}{ll} & \texttt{new Pair(new A(), new B()).setfst(new B())} \\ \longrightarrow & \left[\begin{array}{l}\texttt{new B()/newfst,} \\ \texttt{new Pair(new A(),new B())/this}\end{array}\right] \texttt{new Pair(newfst, this.snd)} \\ \text{i.e.,} & \texttt{new Pair(new B(), new Pair(new A(), new B()).snd)} \end{array}$$

The receiver of the invocation is the object `new Pair(new A(), new B())`, so we look up the `setfst` method in the `Pair` class, where we find that it has formal parameter `newfst` and body `new Pair(newfst, this.snd)`. The invocation reduces to the body with the formal parameter replaced by the actual, and the special variable `this` replaced by the receiver object. This is similar to the beta rule of the lambda calculus, $(\lambda\texttt{x.e0})\texttt{e1} \longrightarrow [\texttt{e1/x}]\texttt{e0}$. The key differences are the fact that the class of the receiver determines where to look for the body (supporting method override), and the substitution of the receiver for `this` (supporting "recursion through self"). Readers familiar with Abadi and Cardelli's Object Calculus will see a strong similarity to their ς reduction rule [1]. In FJ, as in the lambda calculus and the pure Abadi-Cardelli calculus, if a formal parameter appears more than once in the body this may lead duplication of the actual, but since there are no side effects this causes no problems.

Here is the rule for a cast in action:

$$\texttt{(Pair)new Pair(new A(), new B())} \longrightarrow \texttt{new Pair(new A(), new B())}$$

Once the subject of the cast is reduced to an object, it is easy to check that the class of the constructor is a subclass of the target of the cast. If so, as is the case here, then the reduction removes the cast. If not, as in the expression `(A)new B()`, then no rule applies and the computation is *stuck*, denoting a run-time error.

There are three ways in which a computation may get stuck: an attempt to access a field not declared for the class, an attempt to invoke a method not declared for the class ("message not understood"), or an attempt to cast to something other than a superclass of the class. We will prove that the first two of these never happen in well-typed programs, and the third never happens in well-typed programs that contain no downcasts (and no "stupid casts"—a technicality explained below).

As usual, we allow reductions to apply to any subexpression of an expression. Here is a computation for the second example expression, where the next subexpression to be reduced is underlined at each step.

$$\begin{array}{ll} & \texttt{((Pair)}\underline{\texttt{new Pair(new Pair(new A(), new B()), new A()).fst}}\texttt{).snd} \\ \longrightarrow & \underline{\texttt{((Pair)new Pair(new A(),new B()))}}\texttt{.snd} \\ \longrightarrow & \underline{\texttt{new Pair(new A(), new B()).snd}} \\ \longrightarrow & \texttt{new B()} \end{array}$$

We will prove a type soundness result for FJ: if an expression `e` reduces to expression `e'`, and if `e` is well typed, then `e'` is also well typed and its type is a subtype of the type of `e`.

With this informal introduction in mind, we may now proceed to a formal definition of FJ.

2.1 Syntax

The syntax, typing rules, and computation rules for FJ are given in Figure 1, with a few auxiliary functions in Figure 2.

The metavariables A, B, C, D, and E range over class names; f and g range over field names; m ranges over method names; x ranges over parameter names; d and e range over expressions; CL ranges over class declarations; K ranges over constructor declarations; and M ranges over method declarations.

We write $\overline{\mathtt{f}}$ as shorthand for $\mathtt{f}_1,\ldots,\mathtt{f}_n$ (and similarly for $\overline{\mathtt{C}}$, $\overline{\mathtt{x}}$, $\overline{\mathtt{e}}$, etc.) and write $\overline{\mathtt{M}}$ as shorthand for $\mathtt{M}_1\ldots\mathtt{M}_n$ (with no commas). We write the empty sequence as $\bullet$ and denote concatenation of sequences using a comma. The length of a sequence $\overline{\mathtt{x}}$ is written $\#(\overline{\mathtt{x}})$. We abbreviate operations on pairs of sequences in the obvious way, writing "$\overline{\mathtt{C}}\ \overline{\mathtt{f}}$" as shorthand for "$\mathtt{C}_1\ \mathtt{f}_1,\ldots,\mathtt{C}_n\ \mathtt{f}_n$", and similarly "$\overline{\mathtt{C}}\ \overline{\mathtt{f}};$" as shorthand for "$\mathtt{C}_1\ \mathtt{f}_1;\ldots\mathtt{C}_n\ \mathtt{f}_n;$", and "$\mathtt{this}.\overline{\mathtt{f}}=\overline{\mathtt{f}};$" as shorthand for "$\mathtt{this.f}_1=\mathtt{f}_1;\ldots;\mathtt{this.f}_n=\mathtt{f}_n;$". Sequences of field declarations, parameter names, and method declarations are assumed to contain no duplicate names.

A class table CT is a mapping from class names C to class declarations CL. A program is a pair $(CT, \mathtt{e})$ of a class table and an expression. To lighten the notation in what follows, we always assume a *fixed* class table CT.

The abstract syntax of FJ class declarations, constructor declarations, method declarations, and expressions is given at the top left of Figure 1. As in Java, we assume that casts bind less tightly than other forms of expression. We assume that the set of variables includes the special variable this, but that this is never used as the name of an argument to a method.

Every class has a superclass, declared with extends. This raises a question: what is the superclass of the Object class? There are various ways to deal with this issue; the simplest one that we have found is to take Object as a distinguished class name whose definition does *not* appear in the class table. The auxiliary functions that look up fields and method declarations in the class table are equipped with special cases for Object that return the empty sequence of fields and the empty set of methods. (In full Java, the class Object does have several methods. We ignore these in FJ.)

By looking at the class table, we can read off the subtype relation between classes. We write C <: D when C is a subtype of D – i.e., subtyping is the reflexive and transitive closure of the immediate subclass relation given by the extends clauses in CT. Formally, it is defined in the middle of the left column of Figure 1.

The given class table is assumed to satisfy some sanity conditions: (1) $CT(\mathtt{C}) = \mathtt{class\ C}\ldots$ for every $\mathtt{C} \in dom(CT)$; (2) $\mathtt{Object} \notin dom(CT)$; (3) for every class name C (except Object) appearing anywhere in CT, we have $\mathtt{C} \in dom(CT)$; and (4) there are no cycles in the subtype relation induced by CT – that is, the <: relation is antisymmetric.

For the typing and reduction rules, we need a few auxiliary definitions, given in Figure 2. The fields of a class C, written *fields*(C), is a sequence $\overline{\mathtt{C}}\ \overline{\mathtt{f}}$ pairing the class of a field with its name, for all the fields declared in class C and all of its superclasses. The type of the method m in class C, written *mtype*(m, C), is a pair, written $\overline{\mathtt{B}}\to\mathtt{B}$, of a sequence of argument types $\overline{\mathtt{B}}$ and a result type B. Similarly, the body of the method m in class C, written *mbody*(m, C), is a pair, written $(\overline{\mathtt{x}},\mathtt{e})$, of a sequence of parameters $\overline{\mathtt{x}}$ and an expression e. The predicate *override*($\mathtt{C}_0\to\overline{\mathtt{C}}$, m, D) judges if a method m with argument types $\overline{\mathtt{C}}$ and a result type $\mathtt{C}_0$ may be defined in a subclass of D. In case of overriding, if a method with the same name is declared in the superclass then it must have the same type.

2.2 Typing

The typing rules for expressions, method declarations, and class declarations are in the right column of Figure 1. An environment Γ is a finite mapping from variables to types, written $\overline{\mathtt{x}}:\overline{\mathtt{C}}$.

The typing judgment for expressions has the form $\Gamma \vdash \mathtt{e} \in \mathtt{C}$, read "in the environment Γ, expression e has type C." The typing rules are syntax directed, with one rule for each form of expression, save that there are three rules for casts. The typing rules for constructors and method invocations check that each actual parameter has a type that is a subtype of the corresponding formal. We abbreviate typing judgments on sequences in the obvious way, writing $\Gamma \vdash \overline{\mathtt{e}} \in \overline{\mathtt{C}}$ as shorthand for $\Gamma \vdash \mathtt{e}_1 \in \mathtt{C}_1, \ldots, \Gamma \vdash \mathtt{e}_n \in \mathtt{C}_n$ and writing $\overline{\mathtt{C}}$ <: $\overline{\mathtt{D}}$ as shorthand for $\mathtt{C}_1$ <: $\mathtt{D}_1, \ldots, \mathtt{C}_n$ <: $\mathtt{D}_n$.

One technical innovation in FJ is the introduction of "stupid" casts. There are three rules for type casts: in an *upcast* the subject is a subclass of the target, in a *downcast* the target is a subclass of the subject, and

Syntax:

$$\begin{array}{lcl}
\texttt{CL} & ::= & \texttt{class C extends C \{}\overline{\texttt{C}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \\
\texttt{K} & ::= & \texttt{C(}\overline{\texttt{C}}\ \overline{\texttt{f}}\texttt{) \{super(}\overline{\texttt{f}}\texttt{); this.}\overline{\texttt{f}}\texttt{ = }\overline{\texttt{f}}\texttt{;\}} \\
\texttt{M} & ::= & \texttt{C m(}\overline{\texttt{C}}\ \overline{\texttt{x}}\texttt{) \{return e;\}} \\
\texttt{e} & ::= & \texttt{x} \\
 & | & \texttt{e.f} \\
 & | & \texttt{e.m(}\overline{\texttt{e}}\texttt{)} \\
 & | & \texttt{new C(}\overline{\texttt{e}}\texttt{)} \\
 & | & \texttt{(C)e}
\end{array}$$

Subtyping:

$$\texttt{C <: C}$$

$$\frac{\texttt{C <: D} \qquad \texttt{D <: E}}{\texttt{C <: E}}$$

$$\frac{CT(\texttt{C}) = \texttt{class C extends D \{...\}}}{\texttt{C <: D}}$$

Computation:

$$\frac{\mathit{fields}(\texttt{C}) = \overline{\texttt{C}}\ \overline{\texttt{f}}}{\texttt{(new C(}\overline{\texttt{e}}\texttt{)).f}_i \longrightarrow \texttt{e}_i} \quad \text{(R-Field)}$$

$$\frac{\mathit{mbody}(\texttt{m}, \texttt{C}) = (\overline{\texttt{x}}, \texttt{e}_0)}{\texttt{(new C(}\overline{\texttt{e}}\texttt{)).m(}\overline{\texttt{d}}\texttt{)} \longrightarrow [\overline{\texttt{d}}/\overline{\texttt{x}}, \texttt{new C(}\overline{\texttt{e}}\texttt{)/this}]\texttt{e}_0} \quad \text{(R-Invk)}$$

$$\frac{\texttt{C <: D}}{\texttt{(D)(new C(}\overline{\texttt{e}}\texttt{))} \longrightarrow \texttt{new C(}\overline{\texttt{e}}\texttt{)}} \quad \text{(R-Cast)}$$

Congruence:

$$\frac{\texttt{e}_0 \longrightarrow \texttt{e}_0'}{\texttt{e}_0\texttt{.f} \longrightarrow \texttt{e}_0'\texttt{.f}} \quad \text{(RC-Field)}$$

$$\frac{\texttt{e}_0 \longrightarrow \texttt{e}_0'}{\texttt{e}_0\texttt{.m(}\overline{\texttt{e}}\texttt{)} \longrightarrow \texttt{e}_0'\texttt{.m(}\overline{\texttt{e}}\texttt{)}} \quad \text{(RC-Invk-Recv)}$$

$$\frac{\texttt{e}_i \longrightarrow \texttt{e}_i'}{\texttt{e}_0\texttt{.m(...,e}_i\texttt{,...)} \longrightarrow \texttt{e}_0\texttt{.m(...,e}_i'\texttt{,...)}} \quad \text{(RC-Invk-Arg)}$$

$$\frac{\texttt{e}_i \longrightarrow \texttt{e}_i'}{\texttt{new C(...,e}_i\texttt{,...)} \longrightarrow \texttt{new C(...,e}_i'\texttt{,...)}} \quad \text{(RC-New-Arg)}$$

$$\frac{\texttt{e}_0 \longrightarrow \texttt{e}_0'}{\texttt{(C)e}_0 \longrightarrow \texttt{(C)e}_0'} \quad \text{(RC-Cast)}$$

Expression typing:

$$\Gamma \vdash \texttt{x} \in \Gamma(\texttt{x}) \quad \text{(T-Var)}$$

$$\frac{\Gamma \vdash \texttt{e}_0 \in \texttt{C}_0 \qquad \mathit{fields}(\texttt{C}_0) = \overline{\texttt{C}}\ \overline{\texttt{f}}}{\Gamma \vdash \texttt{e}_0\texttt{.f}_i \in \texttt{C}_i} \quad \text{(T-Field)}$$

$$\frac{\begin{array}{c}\Gamma \vdash \texttt{e}_0 \in \texttt{C}_0 \\ \mathit{mtype}(\texttt{m}, \texttt{C}_0) = \overline{\texttt{D}} \to \texttt{C} \\ \Gamma \vdash \overline{\texttt{e}} \in \overline{\texttt{C}} \qquad \overline{\texttt{C}} <: \overline{\texttt{D}}\end{array}}{\Gamma \vdash \texttt{e}_0\texttt{.m(}\overline{\texttt{e}}\texttt{)} \in \texttt{C}} \quad \text{(T-Invk)}$$

$$\frac{\begin{array}{c}\mathit{fields}(\texttt{C}) = \overline{\texttt{D}}\ \overline{\texttt{f}} \\ \Gamma \vdash \overline{\texttt{e}} \in \overline{\texttt{C}} \qquad \overline{\texttt{C}} <: \overline{\texttt{D}}\end{array}}{\Gamma \vdash \texttt{new C(}\overline{\texttt{e}}\texttt{)} \in \texttt{C}} \quad \text{(T-New)}$$

$$\frac{\Gamma \vdash \texttt{e}_0 \in \texttt{D} \qquad \texttt{D} <: \texttt{C}}{\Gamma \vdash \texttt{(C)e}_0 \in \texttt{C}} \quad \text{(T-UCast)}$$

$$\frac{\Gamma \vdash \texttt{e}_0 \in \texttt{D} \qquad \texttt{C} <: \texttt{D} \qquad \texttt{C} \neq \texttt{D}}{\Gamma \vdash \texttt{(C)e}_0 \in \texttt{C}} \quad \text{(T-DCast)}$$

$$\frac{\begin{array}{c}\Gamma \vdash \texttt{e}_0 \in \texttt{D} \qquad \texttt{C} \not<: \texttt{D} \qquad \texttt{D} \not<: \texttt{C} \\ \textit{stupid warning}\end{array}}{\Gamma \vdash \texttt{(C)e}_0 \in \texttt{C}} \quad \text{(T-SCast)}$$

Method typing:

$$\frac{\begin{array}{c}\overline{\texttt{x}} : \overline{\texttt{C}}, \texttt{this} : \texttt{C} \vdash \texttt{e}_0 \in \texttt{E}_0 \qquad \texttt{E}_0 <: \texttt{C}_0 \\ CT(\texttt{C}) = \texttt{class C extends D \{...\}} \\ \mathit{override}(\texttt{m}, \texttt{D}, \overline{\texttt{C}} \to \texttt{C}_0)\end{array}}{\texttt{C}_0\ \texttt{m (}\overline{\texttt{C}}\ \overline{\texttt{x}}\texttt{) \{return e}_0\texttt{;\} OK IN C}} \quad \text{(T-Method)}$$

Class typing:

$$\frac{\begin{array}{c}\texttt{K = C(}\overline{\texttt{D}}\ \overline{\texttt{g}}\texttt{, }\overline{\texttt{C}}\ \overline{\texttt{f}}\texttt{) \{super(}\overline{\texttt{g}}\texttt{); this.}\overline{\texttt{f}}\texttt{ = }\overline{\texttt{f}}\texttt{;\}} \\ \mathit{fields}(\texttt{D}) = \overline{\texttt{D}}\ \overline{\texttt{g}} \qquad \overline{\texttt{M}}\texttt{ OK IN C}\end{array}}{\texttt{class C extends D \{}\overline{\texttt{C}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\} OK}} \quad \text{(T-Class)}$$

Figure 1: FJ: Main definitions

Field lookup:

$$\mathit{fields}(\texttt{Object}) = \bullet$$

$$\frac{CT(\texttt{C}) = \texttt{class C extends D \{}\overline{\texttt{C}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \qquad \mathit{fields}(\texttt{D}) = \overline{\texttt{D}}\ \overline{\texttt{g}}}{\mathit{fields}(\texttt{C}) = \overline{\texttt{D}}\ \overline{\texttt{g}}, \overline{\texttt{C}}\ \overline{\texttt{f}}}$$

Method type lookup:

$$\frac{CT(\texttt{C}) = \texttt{class C extends D \{}\overline{\texttt{C}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \qquad \texttt{B m (}\overline{\texttt{B}}\ \overline{\texttt{x}}\texttt{) \{return e;\}} \in \overline{\texttt{M}}}{\mathit{mtype}(\texttt{m}, \texttt{C}) = \overline{\texttt{B}} \rightarrow \texttt{B}}$$

$$\frac{CT(\texttt{C}) = \texttt{class C extends D \{}\overline{\texttt{C}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \qquad \texttt{m} \text{ is not defined in } \overline{\texttt{M}}}{\mathit{mtype}(\texttt{m}, \texttt{C}) = \mathit{mtype}(\texttt{m}, \texttt{D})}$$

Method body lookup:

$$\frac{CT(\texttt{C}) = \texttt{class C extends D \{}\overline{\texttt{C}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \qquad \texttt{B m (}\overline{\texttt{B}}\ \overline{\texttt{x}}\texttt{) \{return e;\}} \in \overline{\texttt{M}}}{\mathit{mbody}(\texttt{m}, \texttt{C}) = (\overline{\texttt{x}}, \texttt{e})}$$

$$\frac{CT(\texttt{C}) = \texttt{class C extends D \{}\overline{\texttt{C}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \qquad \texttt{m} \text{ is not defined in } \overline{\texttt{M}}}{\mathit{mbody}(\texttt{m}, \texttt{C}) = \mathit{mbody}(\texttt{m}, \texttt{D})}$$

Valid method overriding:

$$\frac{\mathit{mtype}(\texttt{m}, \texttt{D}) = \overline{\texttt{D}} \rightarrow \texttt{D}_0, \text{implies } \overline{\texttt{C}} = \overline{\texttt{D}} \text{ and } \texttt{C}_0 = \texttt{D}_0}{\mathit{override}(\texttt{m}, \texttt{D}, \overline{\texttt{C}} \rightarrow \texttt{C}_0)}$$

Figure 2: FJ: Auxiliary definitions

in a *stupid* cast the target is unrelated to the subject. The Java compiler rejects as ill typed an expression containing a stupid cast, but we must allow stupid casts in FJ if we are to formulate type soundness as a subject reduction theorem for a small-step semantics. This is because a sensible expression may be reduced to one containing a stupid cast. For example, consider the following, which uses classes `A` and `B` as defined as in the previous section:

$$\texttt{(A)}\underline{\texttt{(Object)new B()}} \longrightarrow \texttt{(A)new B()}$$

We indicate the special nature of stupid casts by including the hypothesis *stupid warning* in the type rule for stupid casts (T-SCast); an FJ typing corresponds to a legal Java typing only if it does not contain this rule. (Stupid casts were omitted from Classic Java [14], causing its published proof of type soundness to be incorrect; this error was discovered independently by ourselves and the Classic Java authors.)

The typing judgment for method declarations has the form `M OK IN C`, read "method declaration `M` is ok if it occurs in class `C`." It uses the expression typing judgment on the body of the method, where the free variables are the parameters of the method with their declared types, plus the special variable `this` with type `C`.

The typing judgment for class declarations has the form `CL OK`, read "class declaration `CL` is ok." It checks that the constructor applies `super` to the fields of the superclass and initializes the fields declared in this class, and that each method declaration in the class is ok.

The type of an expression may depend on the type of any methods it invokes, and the type of a method depends on the type of an expression (its body), so it behooves us to check that there is no ill-defined circularity here. Indeed there is none: the circle is broken because the type of each method is explicitly declared. It is possible to load and use the class table before all the classes in it are checked, so long as each class is eventually checked.

2.3 Computation

The reduction relation is of the form $\texttt{e} \longrightarrow \texttt{e}'$, read "expression `e` reduces to expression $\texttt{e}'$ in one step." We write $\longrightarrow^*$ for the reflexive and transitive closure of $\longrightarrow$.

The reduction rules are given in the bottom left column of Figure 1. There are three reduction rules, one for field access, one for method invocation, and one for casting. These were already explained in the introduction to this section. We write $[\overline{\texttt{d}}/\overline{\texttt{x}}, \texttt{e}/\texttt{y}]\texttt{e}_0$ for the result of replacing $\texttt{x}_1$ by $\texttt{d}_1$, ..., $\texttt{x}_n$ by $\texttt{d}_n$, and `y` by `e` in expression $\texttt{e}_0$.

The reduction rules may be applied at any point in an expression, so we also need the obvious congruence rules (if $\mathtt{e} \longrightarrow \mathtt{e}'$ then $\mathtt{e.f} \longrightarrow \mathtt{e}'\mathtt{.f}$, and the like), which also appear in the figure.

2.4 Properties

Formal definitions are fun, but the proof of the pudding is in... well, the proof. If our definitions are sensible, we should be able to prove a type soundness result, which relates typing to computation. Indeed we can prove such a result: if a term is well typed and it reduces to a second term, then the second term is well typed, and furthermore its type is a subtype of the type of the first term.

2.4.1 Theorem [Subject Reduction]: If $\Gamma \vdash \mathtt{e} \in \mathtt{C}$ and $\mathtt{e} \longrightarrow \mathtt{e}'$, then $\Gamma \vdash \mathtt{e}' \in \mathtt{C}'$ for some $\mathtt{C}' \mathrel{<:} \mathtt{C}$.

Before giving the proof, we develop a number of required lemmas.

2.4.2 Lemma: If $\mathit{mtype}(\mathtt{m},\mathtt{D}) = \overline{\mathtt{C}} \to \mathtt{C}_0$, then $\mathit{mtype}(\mathtt{m},\mathtt{C}) = \overline{\mathtt{C}} \to \mathtt{C}_0$ for all $\mathtt{C} \mathrel{<:} \mathtt{D}$.

Proof: Straightforward induction on the derivation of $\mathtt{C} \mathrel{<:} \mathtt{D}$. Note that whether $\mathtt{m}$ is not defined in $CT(\mathtt{C})$ or not, $\mathit{mtype}(\mathtt{m},\mathtt{C})$ should be the same as $\mathit{mtype}(\mathtt{m},\mathtt{E})$ where $CT(\mathtt{C}) = \mathtt{class\ C\ extends\ E\ \ldots.}$ ∎

2.4.3 Lemma [Term substitution preserves typing]: If $\Gamma, \overline{\mathtt{x}} : \overline{\mathtt{B}} \vdash \mathtt{e} \in \mathtt{D}$, and $\Gamma \vdash \overline{\mathtt{d}} \in \overline{\mathtt{A}}$ where $\overline{\mathtt{A}} \mathrel{<:} \overline{\mathtt{B}}$, then $\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e} \in \mathtt{C}$ for some $\mathtt{C} \mathrel{<:} \mathtt{D}$.

Proof: By induction on the derivation of $\Gamma, \overline{\mathtt{x}} : \overline{\mathtt{B}} \vdash \mathtt{e} \in \mathtt{D}$.

Case T-Var: $\quad \mathtt{e} = \mathtt{x} \qquad \mathtt{D} = \Gamma(\mathtt{x})$

If $\mathtt{x} \notin \overline{\mathtt{x}}$, then it's trivial since $[\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{x} = \mathtt{x}$. On the other hand, if $\mathtt{x} = \mathtt{x}_i$ and $\mathtt{D} = \mathtt{B}_i$, then, since $[\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{x} = \mathtt{d}_i$, letting $\mathtt{C} = \mathtt{A}_i$ finishes the case.

Case T-Field: $\quad \mathtt{e} = \mathtt{e}_0\mathtt{.f}_i \qquad \mathtt{D} = \mathtt{C}_i \qquad \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{B}} \vdash \mathtt{e}_0 \in \mathtt{D}_0 \qquad \mathit{fields}(\mathtt{D}_0) = \overline{\mathtt{C}}\ \overline{\mathtt{f}}$

By induction hypothesis, we have some $\mathtt{C}_0$ such that $\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0 \in \mathtt{C}_0$ and $\mathtt{C}_0 \mathrel{<:} \mathtt{D}_0$. Then, it is easy to show that

$$\mathit{fields}(\mathtt{C}_0) = \mathit{fields}(\mathtt{D}_0), \overline{\mathtt{D}}\ \overline{\mathtt{g}}$$

for some $\overline{\mathtt{D}}\ \overline{\mathtt{g}}$. Therefore, by the rule T-Field, $\Gamma \vdash ([\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0)\mathtt{.f}_i \in \mathtt{C}_i$.

Case T-Invk: $\quad \mathtt{e} = \mathtt{e}_0\mathtt{.m}(\overline{\mathtt{e}}) \qquad \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{B}} \vdash \mathtt{e}_0 \in \mathtt{D}_0 \qquad \mathit{mtype}(\mathtt{m},\mathtt{D}_0) = \overline{\mathtt{E}} \to \mathtt{D}$
$\quad \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{B}} \vdash \overline{\mathtt{e}} \in \overline{\mathtt{D}} \qquad \overline{\mathtt{D}} \mathrel{<:} \overline{\mathtt{E}}$

By induction hypothesis, we have some $\mathtt{C}_0$ and $\overline{\mathtt{C}}$ such that

$$\begin{array}{ll} \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0 \in \mathtt{C}_0 & \mathtt{C}_0 \mathrel{<:} \mathtt{D}_0 \\ \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\overline{\mathtt{e}} \in \overline{\mathtt{C}} & \overline{\mathtt{C}} \mathrel{<:} \overline{\mathtt{D}} \end{array}$$

By Lemma 2.4.2, $\mathit{mtype}(\mathtt{m},\mathtt{C}_0) = \overline{\mathtt{E}} \to \mathtt{D}$. Moreover, $\overline{\mathtt{C}} \mathrel{<:} \overline{\mathtt{E}}$ by transitivity of $<:$. Therefore, by the rule T-Invk, $\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0\mathtt{.m}([\overline{\mathtt{d}}/\overline{\mathtt{x}}]\overline{\mathtt{e}}) \in \mathtt{D}$.

Case T-New: $\quad \mathtt{e} = \mathtt{new\ C}(\overline{\mathtt{e}}) \qquad \mathit{fields}(\mathtt{C}) = \overline{\mathtt{D}}\ \overline{\mathtt{f}} \qquad \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{B}} \vdash \overline{\mathtt{e}} \in \overline{\mathtt{C}} \qquad \overline{\mathtt{C}} \mathrel{<:} \overline{\mathtt{D}}$

By induction hypothesis, we have $\overline{\mathtt{E}}$ such that $\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\overline{\mathtt{e}} \in \overline{\mathtt{E}}$ and $\overline{\mathtt{E}} \mathrel{<:} \overline{\mathtt{C}}$. Moreover $\overline{\mathtt{E}} \mathrel{<:} \overline{\mathtt{D}}$, by transitivity of $<:$. Therefore, by the rule T-New, $\Gamma \vdash \mathtt{new\ C}([\overline{\mathtt{d}}/\overline{\mathtt{x}}]\overline{\mathtt{e}}) \in \mathtt{C}$.

Case T-UCast: $\quad \mathtt{e} = (\mathtt{D})\mathtt{e}_0 \qquad \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{B}} \vdash \mathtt{e}_0 \in \mathtt{C} \qquad \mathtt{C} \mathrel{<:} \mathtt{D}$

By induction hypothesis, we have some $\mathtt{E}$ such that $\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0 \in \mathtt{E}$ and $\mathtt{E} \mathrel{<:} \mathtt{C}$. Moreover $\mathtt{E} \mathrel{<:} \mathtt{D}$ by transitivity of $<:$; it leads to $\Gamma \vdash (\mathtt{D})([\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0) \in \mathtt{D}$ by the rule T-UCast.

Case T-DCast: $\quad \mathtt{e} = (\mathtt{D})\mathtt{e}_0 \qquad \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{B}} \vdash \mathtt{e}_0 \in \mathtt{C} \qquad \mathtt{D} \mathrel{<:} \mathtt{C} \qquad \mathtt{D} \neq \mathtt{C}$

By induction hypothesis, we have some $\mathtt{E}$ such that $\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0 \in \mathtt{E}$ and $\mathtt{E} \mathrel{<:} \mathtt{C}$. If $\mathtt{E} \mathrel{<:} \mathtt{D}$ or $\mathtt{D} \mathrel{<:} \mathtt{E}$, then $\Gamma \vdash (\mathtt{D})([\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0) \in \mathtt{D}$ by the rule T-UCast or T-DCast, respectively. On the other hand, if both $\mathtt{D} \not\mathrel{<:} \mathtt{E}$ and $\mathtt{E} \not\mathrel{<:} \mathtt{D}$ hold, then $\Gamma \vdash (\mathtt{D})([\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0) \in \mathtt{D}$ with *stupid warning* by the rule T-SCast.

Case T-SCAST: $\quad$ $\mathtt{e} = (\mathtt{D})\mathtt{e}_0$ $\quad$ $\Gamma, \overline{\mathtt{x}} : \overline{\mathtt{B}} \vdash \mathtt{e}_0 \in \mathtt{C}$ $\quad$ $\mathtt{D} \not<: \mathtt{C}$ $\quad$ $\mathtt{C} \not<: \mathtt{D}$

By induction hypothesis, we have some E such that $\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0 \in \mathtt{E}$ and $\mathtt{E} <: \mathtt{C}$.

Suppose $\mathtt{E} <: \mathtt{D}$. By using that fact that, for every class F, there is only one class G such that $CT(\mathtt{F}) =$ `class F extends G ...`, we can show that either proof of $\mathtt{E} <: \mathtt{C}$ or $\mathtt{E} <: \mathtt{D}$ is a part of the other proof; it means $\mathtt{C} <: \mathtt{D}$ or $\mathtt{D} <: \mathtt{C}$, which contradicts the assumption. Therefore, $\mathtt{E} \not<: \mathtt{D}$. Furthermore, since $\mathtt{D} <: \mathtt{E}$ leading to $\mathtt{D} <: \mathtt{C}$ contradicts the assumption, $\mathtt{D} \not<: \mathtt{E}$. Then, $\Gamma \vdash (\mathtt{D})([\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0) \in \mathtt{D}$ with *stupid warning*, by the rule T-SCAST. ∎

2.4.4 Lemma [Weakening]: If $\Gamma \vdash \mathtt{e} \in \mathtt{C}$, then $\Gamma, \mathtt{x} : \mathtt{D} \vdash \mathtt{e} \in \mathtt{C}$.

Proof: By induction on the derivation of $\Gamma \vdash \mathtt{e} \in \mathtt{C}$. ∎

2.4.5 Lemma: If $mtype(\mathtt{m}, \mathtt{C}_0) = \overline{\mathtt{D}} \rightarrow \mathtt{D}$, and $mbody(\mathtt{m}, \mathtt{C}_0) = (\mathtt{x}, \mathtt{e})$, then for some $\mathtt{D}_0$ where $\mathtt{C}_0 <: \mathtt{D}_0$, there exists some $\mathtt{C} <: \mathtt{D}$ such that $\overline{\mathtt{x}} : \overline{\mathtt{D}}, \mathtt{this} : \mathtt{D}_0 \vdash \mathtt{e} \in \mathtt{C}$.

Proof: By induction on the derivation of $mbody(\mathtt{m}, \mathtt{C}_0)$. The base case (where m is defined in $\mathtt{C}_0$) is easy since m is defined in $CT(\mathtt{C}_0)$ and $\overline{\mathtt{x}} : \overline{\mathtt{D}}, \mathtt{this} : \mathtt{C}_0 \vdash \mathtt{e} \in \mathtt{C}$ by T-METHOD. The induction step is also straightforward. ∎

We can now give the proof of the type soundness theorem.

Proof of Theorem 2.4.1: By induction on a derivation of $\mathtt{e} \longrightarrow \mathtt{e}'$, with a case analysis on the reduction rule used.

Case R-FIELD: $\quad$ $\mathtt{e} = (\mathtt{new}\ \mathtt{C}_0(\overline{\mathtt{e}})).\mathtt{f}_i$ $\quad$ $\mathtt{e}' = \mathtt{e}_i$ $\quad$ $fields(\mathtt{C}_0) = \overline{\mathtt{D}}\ \overline{\mathtt{f}}$

By the rule T-FIELD, we have

$$\Gamma \vdash \mathtt{new}\ \mathtt{C}_0(\overline{\mathtt{e}}) \in \mathtt{D}_0$$
$$\mathtt{C} = \mathtt{D}_i$$

for some $\mathtt{D}_0$. Again, by the rule T-NEW,

$$\Gamma \vdash \overline{\mathtt{e}} \in \overline{\mathtt{C}}$$
$$\overline{\mathtt{C}} <: \overline{\mathtt{D}}$$
$$\mathtt{D}_0 = \mathtt{C}_0$$

In particular, $\Gamma \vdash \mathtt{e}_i \in \mathtt{C}_i$, finishing the case since $\mathtt{C}_i <: \mathtt{D}_i$.

Case R-INVK: $\quad$ $\mathtt{e} = (\mathtt{new}\ \mathtt{C}_0(\overline{\mathtt{e}})).\mathtt{m}(\overline{\mathtt{d}})$
$\mathtt{e}' = [\overline{\mathtt{d}}/\overline{\mathtt{x}}, \mathtt{new}\ \mathtt{C}_0(\overline{\mathtt{e}})/\mathtt{this}]\mathtt{e}_0$
$mbody(\mathtt{m}, \mathtt{C}_0) = (\overline{\mathtt{x}}, \mathtt{e}_0)$

By the rules T-INVK and T-NEW, we have

$$\Gamma \vdash \mathtt{new}\ \mathtt{C}_0(\overline{\mathtt{e}}) \in \mathtt{C}_0$$
$$\Gamma \vdash \overline{\mathtt{d}} \in \overline{\mathtt{C}}$$
$$\overline{\mathtt{C}} <: \overline{\mathtt{D}}$$
$$mtype(\mathtt{m}, \mathtt{C}_0) = \overline{\mathtt{D}} \rightarrow \mathtt{C}$$

By Lemma 2.4.5, $\overline{\mathtt{x}} : \overline{\mathtt{D}}, \mathtt{this} : \mathtt{D}_0 \vdash \mathtt{e}_0 \in \mathtt{B}$ for some $\mathtt{D}_0$ and B where $\mathtt{C}_0 <: \mathtt{D}_0$ and $\mathtt{B} <: \mathtt{C}$. By Lemma 2.4.4, $\Gamma, \overline{\mathtt{x}} : \overline{\mathtt{D}}, \mathtt{this} : \mathtt{D}_0 \vdash \mathtt{e}_0 \in \mathtt{B}$. Then, by Lemma 2.4.3, $\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}, \mathtt{new}\ \mathtt{C}_0(\overline{\mathtt{e}})/\mathtt{this}]\mathtt{e}_0 \in \mathtt{E}$ for some $\mathtt{E} <: \mathtt{B}$. By transitivity of <:, $\mathtt{E} <: \mathtt{C}$. Finally, letting $\mathtt{C}' = \mathtt{E}$ finishes this case.

Case R-CAST: $\quad$ $\mathtt{e} = (\mathtt{D})(\mathtt{new}\ \mathtt{C}_0(\overline{\mathtt{e}}))$ $\quad$ $\mathtt{e}' = \mathtt{new}\ \mathtt{C}_0(\overline{\mathtt{e}})$ $\quad$ $\mathtt{C}_0 <: \mathtt{D}$

The proof of $\Gamma \vdash (\mathtt{D})(\mathtt{new}\ \mathtt{C}_0(\overline{\mathtt{e}})) \in \mathtt{C}$ must end with the rule T-UCAST since the derivation ending with T-SCAST or T-DCAST contradicts the assumption $\mathtt{C}_0 <: \mathtt{D}$. By the rule T-UCAST, we have $\Gamma \vdash \mathtt{new}\ \mathtt{C}_0(\overline{\mathtt{e}}) \in \mathtt{C}_0$ and $\mathtt{D} = \mathtt{C}$, which finishes the case.

Cases for congruence rules are basically easy. But, it's worth showing the following case:

Case RC-CAST: $\quad$ $\mathtt{e} = \mathtt{(D)e_0}$ $\quad$ $\mathtt{e}' = \mathtt{(D)e_0}'$ $\quad$ $\mathtt{e_0} \longrightarrow \mathtt{e_0}'$

We have three subcases according to the last type rule used.

Subcase T-UCAST: $\quad$ $\Gamma \vdash \mathtt{e_0} \in \mathtt{C_0}$ $\quad$ $\mathtt{C_0} <: \mathtt{D}$ $\quad$ $\mathtt{D} = \mathtt{C}$

By induction hypothesis, $\Gamma \vdash \mathtt{e_0}' \in \mathtt{C_0}'$ for some $\mathtt{C_0}' <: \mathtt{C_0}$. By transitivity of $<:$, $\mathtt{C_0}' <: \mathtt{C}$. Therefore, by the rule T-UCAST, $\Gamma \vdash \mathtt{(C)e_0}' \in \mathtt{C}$ (without any additional *stupid warning*).

Subcase T-DCAST: $\quad$ $\Gamma \vdash \mathtt{e_0} \in \mathtt{C_0}$ $\quad$ $\mathtt{D} <: \mathtt{C_0}$ $\quad$ $\mathtt{D} = \mathtt{C}$

By induction hypothesis, $\Gamma \vdash \mathtt{e_0}' \in \mathtt{C_0}'$ for some $\mathtt{C_0}' <: \mathtt{C_0}$. If $\mathtt{C_0}' <: \mathtt{C}$ or $\mathtt{C} <: \mathtt{C_0}'$, then $\Gamma \vdash \mathtt{(C)e_0}' \in \mathtt{C}$ by the rule T-UCAST or T-DCAST (without any additional *stupid warning*). On the other hand, if both $\mathtt{C_0}' \not<: \mathtt{C}$ and $\mathtt{C} \not<: \mathtt{C_0}'$, then, $\Gamma \vdash \mathtt{(C)e_0}' \in \mathtt{C}$ with *stupid warning* by the rule T-SCAST.

Subcase T-SCAST: $\quad$ $\Gamma \vdash \mathtt{e_0} \in \mathtt{C_0}$ $\quad$ $\mathtt{D} \not<: \mathtt{C_0}$ $\quad$ $\mathtt{C_0} \not<: \mathtt{D}$ $\quad$ $\mathtt{D} = \mathtt{C}$

By induction hypothesis, $\Gamma \vdash \mathtt{e_0}' \in \mathtt{C_0}'$ for some $\mathtt{C_0}' <: \mathtt{C_0}$. Then, both $\mathtt{C_0}' \not<: \mathtt{C}$ and $\mathtt{C} \not<: \mathtt{C_0}'$ also hold. Therefore $\Gamma \vdash \mathtt{(C)e_0}' \in \mathtt{C}$ with *stupid warning*. ∎

We can also show that if a program is well typed, then the only way it can get stuck is if it reaches a point where it cannot perform a downcast.

2.4.6 Theorem [Progress]: Suppose $\mathtt{e}$ is a well-typed expression.

(1) If $\mathtt{e}$ includes $\mathtt{new\ C_0(\overline{e}).f}$ as a subexpression, then $\mathit{fields}(\mathtt{C_0}) = \overline{\mathtt{T}}\ \overline{\mathtt{f}}$ and $\mathtt{f} \in \overline{\mathtt{f}}$.

(2) If $\mathtt{e}$ includes $\mathtt{new\ C_0(\overline{e}).m(\overline{d})}$ as a subexpression, then $\mathit{mbody}(\mathtt{m}, \mathtt{C_0}) = (\overline{\mathtt{x}}, \mathtt{e_0})$ and $\#(\overline{\mathtt{x}}) = \#(\overline{\mathtt{d}})$.

Proof sketch: If $\mathtt{e}$ has $\mathtt{new\ C_0(\overline{e}).f}$ as a subexpression, then, by well-typedness of the subexpression, it's easy to check that $\mathit{fields}(\mathtt{C_0})$ is well-defined and $\mathtt{f}$ appears in it. Similarly, if $\mathtt{e}$ has $\mathtt{new\ C_0(\overline{e}).m(\overline{d})}$ as a subexpression, then, it's also easy to show $\mathit{mbody}(\mathtt{m}, \mathtt{C}) = (\overline{\mathtt{x}}, \mathtt{e_0})$ and $\#(\overline{\mathtt{x}}) = \#(\overline{\mathtt{d}})$ from the fact that $\mathit{mtype}(\mathtt{m}, \mathtt{C}) = \overline{\mathtt{C}} \rightarrow \mathtt{D}$ where $\#(\overline{\mathtt{x}}) = \#(\overline{\mathtt{C}})$. ∎

To state a similar property for casts, we say that an expression $\mathtt{e}$ is *safe* in Γ if the type derivations of the underlying CT and $\Gamma \vdash \mathtt{e} \in \mathtt{C}$ contain no downcasts or stupid casts (uses of rules T-DCAST or T-SCAST). In other words, a safe program includes only upcasts. Then we see that a safe expression always reduces to another safe expression, and, moreover, typecasts in a safe expression will never fail, as shown in the following pair of theorems.

2.4.7 Theorem [Reduction preserves safety]: If $\mathtt{e}$ is safe in Γ and $\mathtt{e} \longrightarrow \mathtt{e}'$, then $\mathtt{e}'$ is safe in Γ.

Proof sketch: Similar to the proof of Theorem 2.4.1. Note that, the derivation of $\mathtt{e}'$ will have additional *stupid warning* only if the derivation of $\mathtt{e}$ (and CT) uses the rules T-DCAST and/or T-SCAST. ∎

2.4.8 Theorem [Progress of safe programs]: Suppose $\mathtt{e}$ is safe in Γ. If $\mathtt{e}$ has $\mathtt{(C)new\ C_0(\overline{e})}$ as a subexpression, then $\mathtt{C_0} <: \mathtt{C}$.

Proof sketch: Easy from the fact that the subexpression $\mathtt{(C)new\ C_0(\overline{e})}$ is given type $\mathtt{C}$ by the rule T-UCAST. ∎

3 Featherweight GJ

Just as GJ adds generic types to Java, Featherweight GJ (or FGJ, for short) adds generic types to FJ. Here is the class definition for pairs in FJ, rewritten with generic type parameters in FGJ.

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

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

Both classes and methods may have generic type parameters. Here X and Y are parameters of the class, and Z is a parameter of the setfst method. Each type parameter has a *bound*; here X, Y, and Z are each bounded by Object.

In the context of the above definitions, the expression

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

evaluates to the expression

```
new Pair<B,B>(new B(), new B())
```

If we were being extraordinarily pedantic, we would write A<> and B<> instead of A and B, but we allow the latter as an abbreviation for the former in order that FJ is a proper subset of FGJ.

In GJ, type parameters to generic method invocations are inferred. Thus, in GJ the expression above would be written

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

with no <B> in the invocation of setfst. So while FJ is a subset of Java, FGJ is not quite a subset of GJ. We regard FGJ as an intermediate language – the form that would result after type parameters have been inferred. While parameter inference is an important aspect of GJ, we chose in FGJ to concentrate on modeling other aspects of GJ.

The bound of a type variable may not be a type variable, but may be a type expression involving type variables, and may be recursive (or even, if there are several bounds, mutually recursive). For example, if C<X> and D<Y> are classes with one parameter each, one may have bounds such as <X extends C<X>> or even <X extends C<Y>, Y extends D<X>>. For more on bounds, including examples of the utility of recursive bounds, see the GJ paper [7].

GJ and FGJ are intended to support either of two implementation styles. They may be implemented by *type-passing*, augmenting the run-time system to carry information about type parameters, or they may be implemented by *erasure*, removing all information about type parameters at run-time. This section explores the first style, giving a direct semantics for FGJ that maintains type parameters, and proving a type soundness theorem. Section 4 explores the second style, giving an erasure mapping from FGJ into FJ and showing a correspondence between reductions on FGJ expressions and reductions on FJ expressions. The second style corresponds to the current implementation of GJ, which compiles GJ into the Java Virtual Machine (JVM), which of course maintains no information about type parameters at run-time; the first style would correspond to using an augmented JVM that maintains information about type parameters.

3.1 Syntax

In what follows, for the sake of conciseness we abbreviate the keyword extends to the symbol $\triangleleft$ and the keywork return to the symbol $\uparrow$.

The syntax, typing rules, and computation rules for FGJ are given in Figure 3, with a few auxiliary functions in Figure 5. The metavariables X, Y, and Z range over type variables; T, U, and V range over types; and N, O and P range over nonvariable types (types other than type variables). We write $\overline{\mathtt{X}}$ as shorthand for $\mathtt{X}_1,\ldots,\mathtt{X}_n$ (and similarly for $\overline{\mathtt{T}}$, $\overline{\mathtt{N}}$, etc.), and assume sequences of type variables contain no duplicate names.

The abstract syntax of FGJ is given at the top left of Figure 3. We allow C<> and m<> to be abbreviated as C and m, respectively.

Syntax:

$$
\begin{array}{lcl}
\mathtt{CL} & ::= & \mathtt{class}\ \mathtt{C}\texttt{<}\overline{\mathtt{X}} \triangleleft \overline{\mathtt{N}}\texttt{>} \triangleleft \mathtt{N}\ \{\overline{\mathtt{T}}\ \overline{\mathtt{f}};\ \mathtt{K}\ \overline{\mathtt{M}}\} \\
\mathtt{K} & ::= & \mathtt{C}(\overline{\mathtt{T}}\ \overline{\mathtt{f}})\ \{\mathtt{super}(\overline{\mathtt{f}});\ \mathtt{this}.\overline{\mathtt{f}} = \overline{\mathtt{f}};\} \\
\mathtt{M} & ::= & \texttt{<}\overline{\mathtt{X}} \triangleleft \overline{\mathtt{N}}\texttt{>}\ \mathtt{T}\ \mathtt{m}\ (\overline{\mathtt{T}}\ \overline{\mathtt{x}})\ \{\uparrow \mathtt{e};\} \\
\mathtt{e} & ::= & \mathtt{x} \\
 & | & \mathtt{e.f} \\
 & | & \mathtt{e.m}\texttt{<}\overline{\mathtt{T}}\texttt{>}(\overline{\mathtt{e}}) \\
 & | & \mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}}) \\
 & | & (\mathtt{N})\mathtt{e} \\
\mathtt{T} & ::= & \mathtt{X} \\
 & | & \mathtt{N} \\
\mathtt{N} & ::= & \mathtt{C}\texttt{<}\overline{\mathtt{T}}\texttt{>}
\end{array}
$$

Subtyping:

$$\Delta \vdash \mathtt{T} <: \mathtt{T} \qquad \text{(S-Refl)}$$

$$\frac{\Delta \vdash \mathtt{S} <: \mathtt{T} \qquad \Delta \vdash \mathtt{T} <: \mathtt{U}}{\Delta \vdash \mathtt{S} <: \mathtt{U}} \qquad \text{(S-Trans)}$$

$$\Delta \vdash \mathtt{X} <: \Delta(\mathtt{X}) \qquad \text{(S-Var)}$$

$$\frac{CT(\mathtt{C}) = \mathtt{class}\ \mathtt{C}\texttt{<}\overline{\mathtt{X}} \triangleleft \overline{\mathtt{N}}\texttt{>} \triangleleft \mathtt{N}\ \{\ldots\}}{\Delta \vdash \mathtt{C}\texttt{<}\overline{\mathtt{T}}\texttt{>} <: [\overline{\mathtt{T}}/\overline{\mathtt{X}}]\mathtt{N}} \qquad \text{(S-Class)}$$

Computation:

$$\frac{\mathit{fields}(\mathtt{N}) = \overline{\mathtt{T}}\ \overline{\mathtt{f}}}{(\mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}})).\mathtt{f}_i \longrightarrow \mathtt{e}_i} \qquad \text{(GR-Field)}$$

$$\frac{\mathit{mbody}(\mathtt{m}\texttt{<}\overline{\mathtt{V}}\texttt{>}, \mathtt{N}) = (\overline{\mathtt{x}}, \mathtt{e}_0)}{\begin{array}{l}(\mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}})).\mathtt{m}\texttt{<}\overline{\mathtt{V}}\texttt{>}(\overline{\mathtt{d}}) \\ \longrightarrow [\overline{\mathtt{d}}/\overline{\mathtt{x}}, \mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}})/\mathtt{this}]\mathtt{e}_0\end{array}} \qquad \text{(GR-Invk)}$$

$$\frac{\emptyset \vdash \mathtt{N} <: \mathtt{O}}{(\mathtt{O})(\mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}})) \longrightarrow \mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}})} \qquad \text{(GR-Cast)}$$

Congruence:

$$\frac{\mathtt{e}_0 \longrightarrow \mathtt{e}_0{}'}{\mathtt{e}_0.\mathtt{f} \longrightarrow \mathtt{e}_0{}'.\mathtt{f}} \qquad \text{(GRC-Field)}$$

$$\frac{\mathtt{e}_0 \longrightarrow \mathtt{e}_0{}'}{\mathtt{e}_0.\mathtt{m}\texttt{<}\overline{\mathtt{T}}\texttt{>}(\overline{\mathtt{e}}) \longrightarrow \mathtt{e}_0{}'.\mathtt{m}\texttt{<}\overline{\mathtt{T}}\texttt{>}(\overline{\mathtt{e}})} \qquad \text{(GRC-Inv-Recv)}$$

$$\frac{\mathtt{e}_i \longrightarrow \mathtt{e}_i{}'}{\begin{array}{l}\mathtt{e}_0.\mathtt{m}\texttt{<}\overline{\mathtt{T}}\texttt{>}(\ldots,\mathtt{e}_i,\ldots) \\ \longrightarrow \mathtt{e}_0.\mathtt{m}\texttt{<}\overline{\mathtt{T}}\texttt{>}(\ldots\mathtt{e}_i{}',\ldots)\end{array}} \qquad \text{(GRC-Inv-Arg)}$$

$$\frac{\mathtt{e}_i \longrightarrow \mathtt{e}_i{}'}{\begin{array}{l}\mathtt{new}\ \mathtt{N}(\ldots,\mathtt{e}_i,\ldots) \\ \longrightarrow \mathtt{new}\ \mathtt{N}(\ldots\mathtt{e}_i{}',\ldots)\end{array}} \qquad \text{(GRC-New-Arg)}$$

$$\frac{\mathtt{e}_0 \longrightarrow \mathtt{e}_0{}'}{(\mathtt{N})\mathtt{e}_0 \longrightarrow (\mathtt{N})\mathtt{e}_0{}'} \qquad \text{(GRC-Cast)}$$

Figure 3: FGJ: Main definitions (1)

Well-formed types:

$$\Delta \vdash \texttt{Object ok} \qquad \text{(WF-Object)}$$

$$\frac{\texttt{X} \in dom(\Delta)}{\Delta \vdash \texttt{X ok}} \qquad \text{(WF-Var)}$$

$$\frac{\begin{array}{c} CT(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{...\}} \\ \Delta \vdash \overline{\texttt{T}} \text{ ok} \qquad \Delta \vdash \overline{\texttt{T}} \texttt{ <: } [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{N}} \end{array}}{\Delta \vdash \texttt{C<}\overline{\texttt{T}}\texttt{> ok}} \qquad \text{(WF-Class)}$$

Expression typing:

$$\Delta;\Gamma \vdash \texttt{x} \in \Gamma(\texttt{x}) \qquad \text{(GT-Var)}$$

$$\frac{\begin{array}{c} \Delta;\Gamma \vdash \texttt{e}_0 \in \texttt{T}_0 \\ \mathit{fields}(\mathit{bound}_\Delta(\texttt{T}_0)) = \overline{\texttt{T}}\ \overline{\texttt{f}} \end{array}}{\Delta;\Gamma \vdash \texttt{e}_0\texttt{.f}_i \in \texttt{T}_i} \qquad \text{(GT-Field)}$$

$$\frac{\begin{array}{c} \Delta;\Gamma \vdash \texttt{e}_0 \in \texttt{T}_0 \\ \mathit{mtype}(\texttt{m}, \mathit{bound}_\Delta(\texttt{T}_0)) = \texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{O}}\texttt{>}\overline{\texttt{U}}\texttt{→U} \\ \Delta \vdash \overline{\texttt{V}} \text{ ok} \qquad \Delta \vdash \overline{\texttt{V}} \texttt{ <: } [\overline{\texttt{V}}/\overline{\texttt{Y}}]\overline{\texttt{O}} \\ \Delta;\Gamma \vdash \overline{\texttt{e}} \in \overline{\texttt{S}} \qquad \Delta \vdash \overline{\texttt{S}} \texttt{ <: } [\overline{\texttt{V}}/\overline{\texttt{Y}}]\overline{\texttt{U}} \end{array}}{\Delta;\Gamma \vdash \texttt{e}_0\texttt{.m<}\overline{\texttt{V}}\texttt{>(}\overline{\texttt{e}}\texttt{)} \in [\overline{\texttt{V}}/\overline{\texttt{Y}}]\texttt{U}} \qquad \text{(GT-Invk)}$$

$$\frac{\begin{array}{c} \Delta \vdash \texttt{N ok} \qquad \mathit{fields}(\texttt{N}) = \overline{\texttt{T}}\ \overline{\texttt{f}} \\ \Delta;\Gamma \vdash \overline{\texttt{e}} \in \overline{\texttt{S}} \qquad \Delta \vdash \overline{\texttt{S}} \texttt{ <: } \overline{\texttt{T}} \end{array}}{\Delta;\Gamma \vdash \texttt{new N(}\overline{\texttt{e}}\texttt{)} \in \texttt{N}} \qquad \text{(GT-New)}$$

$$\frac{\Delta;\Gamma \vdash \texttt{e}_0 \in \texttt{T}_0 \qquad \Delta \vdash \mathit{bound}_\Delta(\texttt{T}_0) \texttt{ <: N}}{\Delta;\Gamma \vdash \texttt{(N)e}_0 \in \texttt{N}} \qquad \text{(GT-UCast)}$$

$$\frac{\begin{array}{c} \Delta;\Gamma \vdash \texttt{e}_0 \in \texttt{T}_0 \qquad \Delta \vdash \texttt{N ok} \\ \Delta \vdash \texttt{N <: } \mathit{bound}_\Delta(\texttt{T}_0) \\ \texttt{N} \neq \mathit{bound}_\Delta(\texttt{T}_0) \\ \mathit{downcast}(\texttt{N}, \mathit{bound}_\Delta(\texttt{T}_0)) \end{array}}{\Delta;\Gamma \vdash \texttt{(N)e}_0 \in \texttt{N}} \qquad \text{(GT-DCast)}$$

$$\frac{\begin{array}{c} \Delta;\Gamma \vdash \texttt{e}_0 \in \texttt{T}_0 \qquad \Delta \vdash \texttt{N ok} \\ \texttt{N} = \texttt{C<}\overline{\texttt{T}}\texttt{>} \qquad \mathit{bound}_\Delta(\texttt{T}_0) = \texttt{D<}\overline{\texttt{S}}\texttt{>} \\ \texttt{C} \not\trianglelefteq \texttt{D} \qquad \texttt{D} \not\trianglelefteq \texttt{C} \\ \mathit{stupid\ warning} \end{array}}{\Delta;\Gamma \vdash \texttt{(N)e}_0 \in \texttt{N}} \qquad \text{(GT-SCast)}$$

Method typing:

$$\frac{\begin{array}{c} \Delta = \overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}}, \overline{\texttt{Y}}\texttt{<:}\overline{\texttt{O}} \\ \Delta \vdash \overline{\texttt{T}} \text{ ok} \qquad \Delta \vdash \texttt{T ok} \qquad \Delta \vdash \overline{\texttt{O}} \text{ ok} \\ \Delta;\overline{\texttt{x}} : \overline{\texttt{T}}, \texttt{this} : \texttt{C<}\overline{\texttt{X}}\texttt{>} \vdash \texttt{e}_0 \in \texttt{S} \qquad \Delta \vdash \texttt{S <: T} \\ CT(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{...\}} \\ \mathit{override}(\texttt{m}, \texttt{N}, \texttt{<}\overline{\texttt{Z}} \triangleleft \overline{\texttt{P}}\texttt{>}\overline{\texttt{U}}\texttt{→U}) \end{array}}{\texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{O}}\texttt{> T m (}\overline{\texttt{T}}\ \overline{\texttt{x}}\texttt{) \{}\uparrow\texttt{e}_0\texttt{;\} OK IN C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>}} \qquad \text{(GT-Method)}$$

Class typing:

$$\frac{\begin{array}{c} \overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}} \vdash \overline{\texttt{N}} \text{ ok} \qquad \overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}} \vdash \texttt{N ok} \qquad \overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}} \vdash \overline{\texttt{T}} \text{ ok} \\ \mathit{fields}(\texttt{N}) = \overline{\texttt{U}}\ \overline{\texttt{g}} \qquad \overline{\texttt{M}} \texttt{ OK IN C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \\ \texttt{K} = \texttt{C(}\overline{\texttt{U}}\ \overline{\texttt{g}}\texttt{, }\overline{\texttt{T}}\ \overline{\texttt{f}}\texttt{) \{super(}\overline{\texttt{g}}\texttt{); this.}\overline{\texttt{f}}\texttt{ = }\overline{\texttt{f}}\texttt{;\}} \end{array}}{\texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{}\overline{\texttt{T}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\} OK}} \qquad \text{(GT-Class)}$$

Figure 4: FGJ: Main definitions (2)

Bound of type:

$$\begin{array}{rcl} \mathit{bound}_\Delta(\texttt{X}) & = & \Delta(\texttt{X}) \\ \mathit{bound}_\Delta(\texttt{N}) & = & \texttt{N}. \end{array}$$

Field lookup:

$$\mathit{fields}(\texttt{Object}) = \bullet \qquad \text{(F-Object)}$$

$$\frac{\begin{array}{c} \mathit{CT}(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{}\overline{\texttt{S}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \\ \mathit{fields}([\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N}) = \overline{\texttt{U}}\ \overline{\texttt{g}} \end{array}}{\mathit{fields}(\texttt{C<}\overline{\texttt{T}}\texttt{>}) = \overline{\texttt{U}}\ \overline{\texttt{g}}, [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{S}}\ \overline{\texttt{f}}} \qquad \text{(F-Class)}$$

Method type lookup:

$$\frac{\begin{array}{c} \mathit{CT}(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{}\overline{\texttt{S}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \\ \texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{O}}\texttt{> U m (}\overline{\texttt{U}}\ \overline{\texttt{x}}\texttt{) \{}\uparrow\texttt{e;\}} \in \overline{\texttt{M}} \end{array}}{\mathit{mtype}(\texttt{m}, \texttt{C<}\overline{\texttt{T}}\texttt{>}) = [\overline{\texttt{T}}/\overline{\texttt{X}}](\texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{O}}\texttt{>}\overline{\texttt{U}}\to\texttt{U})} \qquad \text{(MT-Class)}$$

$$\frac{\begin{array}{c} \mathit{CT}(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{}\overline{\texttt{S}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \\ \texttt{m} \text{ is not defined in } \overline{\texttt{M}} \end{array}}{\mathit{mtype}(\texttt{m}, \texttt{C<}\overline{\texttt{T}}\texttt{>}) = \mathit{mtype}(\texttt{m}, [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N})} \qquad \text{(MT-Super)}$$

Method body lookup:

$$\frac{\begin{array}{c} \mathit{CT}(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{}\overline{\texttt{S}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \\ \texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{O}}\texttt{> U m (}\overline{\texttt{U}}\ \overline{\texttt{x}}\texttt{) \{}\uparrow\texttt{e}_0\texttt{;\}} \in \overline{\texttt{M}} \end{array}}{\mathit{mbody}(\texttt{m<}\overline{\texttt{V}}\texttt{>}, \texttt{C<}\overline{\texttt{T}}\texttt{>}) = (\overline{\texttt{x}}, [\overline{\texttt{T}}/\overline{\texttt{X}}, \overline{\texttt{V}}/\overline{\texttt{Y}}]\texttt{e}_0)} \qquad \text{(MB-Class)}$$

$$\frac{\begin{array}{c} \mathit{CT}(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{}\overline{\texttt{S}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}} \\ \texttt{m} \text{ is not defined in } \overline{\texttt{M}} \end{array}}{\mathit{mbody}(\texttt{m<}\overline{\texttt{V}}\texttt{>}, \texttt{C<}\overline{\texttt{T}}\texttt{>}) = \mathit{mbody}(\texttt{m<}\overline{\texttt{V}}\texttt{>}, [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N})} \qquad \text{(MB-Super)}$$

Valid method overriding:

$$\frac{\begin{array}{c} \mathit{mtype}(\texttt{m}, \texttt{N}) = \texttt{<}\overline{\texttt{Z}} \triangleleft \overline{\texttt{P}}\texttt{>}\overline{\texttt{U}}\to\texttt{U} \text{ implies} \\ \overline{\texttt{O}}\texttt{,}\overline{\texttt{T}} = [\overline{\texttt{Y}}/\overline{\texttt{Z}}](\overline{\texttt{P}}\texttt{,}\overline{\texttt{U}}) \text{ and } \Delta \vdash \texttt{T <: } [\overline{\texttt{Y}}/\overline{\texttt{Z}}]\texttt{U} \end{array}}{\mathit{override}(\texttt{m}, \texttt{N}, \texttt{<}\overline{\texttt{Z}} \triangleleft \overline{\texttt{P}}\texttt{>}\overline{\texttt{U}}\to\texttt{U})}$$

Valid downcast:

$$\frac{\begin{array}{c} \Delta \vdash \texttt{C<}\overline{\texttt{S}}\texttt{> <: N} \text{ and } \Delta \vdash \texttt{C<}\overline{\texttt{S}}\texttt{>} \text{ ok} \\ \text{implies } \overline{\texttt{S}} = \overline{\texttt{T}} \text{ for all } \overline{\texttt{S}} \end{array}}{\mathit{downcast}(\texttt{C<}\overline{\texttt{T}}\texttt{>}, \texttt{N})}$$

Figure 5: FGJ: Auxiliary definitions

As before, we assume a fixed class table CT, which is a mapping from class names `C` to class declarations `CL`, obeying the essentially same sanity conditions as given previously. (For the condition (4), we use the relation, defined as the reflexive and transitive closure of the $\mathtt{C}\texttt{<}\overline{\mathtt{X}} \triangleleft \overline{\mathtt{N}}\texttt{>} \triangleleft \mathtt{D}\texttt{<}\overline{\mathtt{T}}\texttt{>}$ relation; we write `C ext D` for it.)

3.2 Typing

A type environment Δ is a finite mapping from type variables to nonvariable types, written $\overline{\mathtt{X}}$ `<:` $\overline{\mathtt{N}}$, that takes each type variable to its bound.

Bounds of types

We write $bound_{\Delta}(\mathtt{T})$ for the upper bound of `T` in Δ, as defined in Figure 5. Unlike calculi such as $F_{\leq}$ [9], this promotion relation does not need to be defined recursively: the bound of a type variable is always a nonvariable type.

Subtyping

The subtyping relation is defined in the left column of Figure 3. As before, subtyping is the reflexive and transitive closure of the $\triangleleft$ relation. Type parameters are *invariant* with regard to subtyping (for reasons explained in the GJ paper), so $\overline{\mathtt{T}}$ `<:` $\overline{\mathtt{U}}$ does *not* imply $\mathtt{C}\texttt{<}\overline{\mathtt{T}}\texttt{>}$ `<:` $\mathtt{C}\texttt{<}\overline{\mathtt{U}}\texttt{>}$.

Well-formed types

If the declaration of a class `C` begins $\mathtt{class}\ \mathtt{C}\texttt{<}\overline{\mathtt{X}} \triangleleft \overline{\mathtt{N}}\texttt{>}$, then a type like $\mathtt{C}\texttt{<}\overline{\mathtt{T}}\texttt{>}$ is well formed only if substituting $\overline{\mathtt{T}}$ for $\overline{\mathtt{X}}$ respects the bounds $\overline{\mathtt{N}}$, that is if $\overline{\mathtt{T}}$ `<:` $[\overline{\mathtt{T}}/\overline{\mathtt{X}}]\overline{\mathtt{N}}$. We write $\Delta \vdash \mathtt{T}$ ok if type `T` is well-formed in context Δ. The rules for well-formed types appear in Figure 3. Note that we perform a simultaneous substitution, so any variable in $\overline{\mathtt{X}}$ may appear in $\overline{\mathtt{N}}$, permitting recursion and mutual recursion between variables and bounds.

A type environment Δ is well formed if $\Delta \vdash \Delta(\mathtt{X})$ ok for all `X` in $dom(\Delta)$. We also say that an environment Γ is well formed with respect to Δ, written $\Delta \vdash \Gamma$ ok, if $\Delta \vdash \Gamma(\mathtt{x})$ ok for all `x` in $dom(\Gamma)$.

Field and method lookup

For the typing and reduction rules, we need a few auxiliary definitions, given in Figure 5; these are fairly straightforward adaptations of the lookup rules given previously. The fields of a nonvariable type `N`, written *fields*(`N`), are a sequence of corresponding types and field names, $\overline{\mathtt{T}}\ \overline{\mathtt{f}}$. The type of the method invocation `m` at nonvariable type `N`, written *mtype*(`m`, `N`), is a type of the form $\texttt{<}\overline{\mathtt{X}} \triangleleft \overline{\mathtt{N}}\texttt{>}\overline{\mathtt{U}} \rightarrow \mathtt{U}$. Similarly, the body of the method invocation `m` at nonvariable type `N` with type parameters $\overline{\mathtt{V}}$, written $mbody(\mathtt{m}\texttt{<}\overline{\mathtt{V}}\texttt{>}, \mathtt{N})$, is a pair, written $(\overline{\mathtt{x}}, \mathtt{e})$, of a sequence of parameters $\overline{\mathtt{x}}$ and an expression `e`.

Typing rules

Typing rules for expressions, methods, and classes appear in Figure 3.

The typing judgment for expressions is of form $\Delta; \Gamma \vdash \mathtt{e} \in \mathtt{T}$, read as "in the type environment Δ and the environment Γ, `e` has type `T`." Most of the subtleties are in the field and method lookup relations that we have already seen; the typing rules themselves are straightforward.

In the rule GT-DCAST, the last premise ensures that the result of the cast will be the same at run time, no matter whether we use the high-level (type-passing) reduction rules defined later in this section or the erasure semantics considered in Section 4. For example, suppose we have defined:

```
class List<X◁Object>◁Object { ... }
class LinkedList<X◁Object>◁List<X> { ... }
```

Now, if `o` has type `Object`, then the cast `(List<C>)o` is not permitted. (If, at run time, `o` is bound to `new List<D>()`, then the cast would fail in the type-passing semantics but succeed in the erasure semantics, since `(List<C>)o` erases to `(List)o` while both `new List<C>()` and `new List<D>()` erase to `new List()`.)

On the other hand, if `cl` has type `List<C>`, then the cast `(LinkedList<C>)cl` is permitted, since the type-passing and erased versions of the cast are guaranteed to either both succeed or both fail.

The typing rule for methods contains one additional subtlety. In FGJ (and GJ), unlike in FJ (and Java), covariant subtyping of method results is allowed. That is, the result type of a method may be a subtype of the result type of the corresponding method in the superclass, although the bounds of type variables and the argument types must be identical (modulo renaming of type variables).

As before, a class table is ok if all its class definitions are ok.

3.3 Reduction

The operational semantics of FGJ programs is only a little more complicated than what we had in FJ. The rules appear in Figure 3.

3.4 Properties

Type Soundness

FGJ programs enjoy subject reduction and progress properties exactly like programs in FJ (2.4.1 and 2.4.6). The basic structures of the proofs are similar to those of Theorem 2.4.1 and 2.4.6. For subject reduction, however, since we now have parametric polymorphism combined with subtyping, we need a few more lemmas. The main lemmas required are a term substitution lemma as before, plus similar lemmas about the preservation of subtyping and typing under *type* substitution. (Readers familiar with proofs of subject reduction for typed lambda-calculi like $F_{\leq}$ [9] will notice many similarities). We begin with the required lemmas including three substitution lemmas, which are proved by straightforward induction on a derivation of $\Delta \vdash \mathtt{S} <: \mathtt{T}$ or $\Delta; \Gamma \vdash \mathtt{e} \in \mathtt{T}$.

3.4.1 Lemma [Weakening]: Suppose $\Delta, \overline{\mathtt{X}}<:\overline{\mathtt{N}} \vdash \overline{\mathtt{N}}$ ok and $\Delta \vdash \mathtt{U}$ ok.

1. If $\Delta \vdash \mathtt{S} <: \mathtt{T}$, then $\Delta, \overline{\mathtt{X}}<:\overline{\mathtt{N}} \vdash \mathtt{S} <: \mathtt{T}$.
2. If $\Delta \vdash \mathtt{S}$ ok, then $\Delta, \overline{\mathtt{X}}<:\overline{\mathtt{N}} \vdash \mathtt{S}$ ok.
3. If $\Delta; \Gamma \vdash \mathtt{e} \in \mathtt{T}$, then $\Delta; \Gamma, \mathtt{x} : \mathtt{U} \vdash \mathtt{e} \in \mathtt{T}$, and $\Delta, \overline{\mathtt{X}}<:\overline{\mathtt{N}}; \Gamma \vdash \mathtt{e} \in \mathtt{T}$.

Proof: Each of them is proved by straightforward inducition on the derivation of $\Delta \vdash \mathtt{S} <: \mathtt{T}$ and $\Delta \vdash \mathtt{S}$ ok and $\Delta; \Gamma \vdash \mathtt{e} \in \mathtt{T}$. ∎

3.4.2 Lemma: If $\Delta \vdash \mathtt{E}\texttt{<}\overline{\mathtt{V}}\texttt{>} <: \mathtt{D}\texttt{<}\overline{\mathtt{U}}\texttt{>}$ and $\mathtt{D}\ \not\!\mathtt{ext}\ \mathtt{C}$ and $\mathtt{C}\ \not\!\mathtt{ext}\ \mathtt{D}$, then $\mathtt{E}\ \not\!\mathtt{ext}\ \mathtt{C}$ and $\mathtt{C}\ \not\!\mathtt{ext}\ \mathtt{E}$.

Proof: It is easy to see that $\Delta \vdash \mathtt{E}\texttt{<}\overline{\mathtt{V}}\texttt{>} <: \mathtt{D}\texttt{<}\overline{\mathtt{U}}\texttt{>}$ implies `E ext D`. The conclusions are easily proved by contradition. ∎

3.4.3 Lemma: If *downcast*$(\mathtt{C}\texttt{<}\overline{\mathtt{S}}\texttt{>}, \mathtt{E}\texttt{<}\overline{\mathtt{U}}\texttt{>})$ and `C ext D ext E`, then *downcast*$(\mathtt{C}\texttt{<}\overline{\mathtt{S}}\texttt{>}, \mathtt{D}\texttt{<}\overline{\mathtt{T}}\texttt{>})$ and *downcast*$(\mathtt{D}\texttt{<}\overline{\mathtt{T}}\texttt{>}, \mathtt{E}\texttt{<}\overline{\mathtt{U}}\texttt{>})$ for some $\overline{\mathtt{T}}$.

Proof: Easy. ∎

3.4.4 Lemma [Type substitution preserves subtyping]: If $\Delta_1, \overline{\mathtt{X}}<:\overline{\mathtt{N}}, \Delta_2 \vdash \mathtt{S} <: \mathtt{T}$ and $\Delta_1 \vdash \overline{\mathtt{U}} <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{N}}$ with $\Delta_1 \vdash \overline{\mathtt{U}}$ ok, and none of $\overline{\mathtt{X}}$ appearing in Δ_1, then $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{S} <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}$.

Proof: By induction on the derivation of $\Delta_1, \overline{\mathtt{X}}<:\overline{\mathtt{N}}, \Delta_2 \vdash \mathtt{S} <: \mathtt{T}$. Most cases are straightforward. The only interesting case is:

Case S-Var: $\quad \mathtt{S} = \mathtt{X} \qquad \mathtt{T} = (\Delta_1, \overline{\mathtt{X}} \mathtt{<:} \overline{\mathtt{N}}, \Delta_2)(\mathtt{X})$

If $\mathtt{X} \in dom(\Delta_1) \cup dom(\Delta_2)$, then it's trivial. On the other hand, if $\mathtt{X} = \mathtt{X}_i$, then, by assumption, we have $\Delta_1 \vdash \mathtt{U}_i \mathtt{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}_i$. Finally, Lemma 3.4.1 finishes the case. ∎

3.4.5 Lemma [Type substitution preserves type well-formedness]: If $\Delta_1, \overline{\mathtt{X}} \mathtt{<:} \overline{\mathtt{N}}, \Delta_2 \vdash \mathtt{T}$ ok and $\Delta_1 \vdash \overline{\mathtt{U}} \mathtt{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{N}}$ with $\Delta_1 \vdash \overline{\mathtt{U}}$ ok and none of $\overline{\mathtt{X}}$ appearing in Δ_1, then $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}$ ok.

Proof: By induction on the derivation of $\Delta_1, \overline{\mathtt{X}} \mathtt{<:} \overline{\mathtt{N}}, \Delta_2 \vdash \mathtt{T}$ ok, with a case analysis on the last rule used. The only interesting case is:

Case WF-Class: $\quad \mathtt{T} = \mathtt{C<}\overline{\mathtt{T}}\mathtt{>} \qquad \Delta_1, \overline{\mathtt{X}} \mathtt{<:} \overline{\mathtt{N}}, \Delta_2 \vdash \overline{\mathtt{T}}$ ok $\qquad \Delta_1, \overline{\mathtt{X}} \mathtt{<:} \overline{\mathtt{N}}, \Delta_2 \vdash \overline{\mathtt{T}} \mathtt{<:} [\overline{\mathtt{T}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}}$
$\qquad CT(\mathtt{C}) = \mathtt{class\ C<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\mathtt{>} \triangleleft \mathtt{N\ \{...\}}$

By induction hypothesis,

$$\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{T}} \text{ ok}.$$

On the other hand, by Lemma 3.4.4, $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{T}} \mathtt{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}][\overline{\mathtt{T}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}}$. Since $\overline{\mathtt{Y}} \mathtt{<:} \overline{\mathtt{P}} \vdash \overline{\mathtt{P}}$ by the rule GT-Class, $\overline{\mathtt{P}}$ does not include any of $\overline{\mathtt{X}}$ as a free variable. Thus, $[\overline{\mathtt{U}}/\overline{\mathtt{X}}][\overline{\mathtt{T}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}} = [[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{T}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}}$, and finally, we have $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \mathtt{C<}[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{T}}\mathtt{>}$ ok by WF-Class. ∎

3.4.6 Lemma: Suppose $\Delta_1, \overline{\mathtt{X}} \mathtt{<:} \overline{\mathtt{N}}, \Delta_2 \vdash \mathtt{T}$ ok and $\Delta_1 \vdash \overline{\mathtt{U}} \mathtt{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{N}}$ with $\Delta_1 \vdash \overline{\mathtt{U}}$ ok and none of $\overline{\mathtt{X}}$ appearing in Δ_1. Then, $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash bound_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}) \mathtt{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}](bound_{\Delta_1, \overline{\mathtt{X}} \mathtt{<:} \overline{\mathtt{N}}, \Delta_2}(\mathtt{T}))$.

Proof: The case where $\mathtt{T}$ is a nonvariable type is trivial. The case where $\mathtt{T}$ is a type variable $\mathtt{X}$ and $\mathtt{X} \in dom(\Delta_1) \cup dom(\Delta_2)$ is also easy. Finally, if $\mathtt{T}$ is a type variable $\mathtt{X}_i$, then $bound_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}) = \mathtt{U}_i$ and $[\overline{\mathtt{U}}/\overline{\mathtt{X}}](bound_{\Delta_1, \overline{\mathtt{X}} \mathtt{<:} \overline{\mathtt{N}}, \Delta_2}(\mathtt{T})) = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}_i$; the assupmtion $\Delta_1 \vdash \overline{\mathtt{U}} \mathtt{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{N}}$ (and Lemma 3.4.1) finish the proof. ∎

3.4.7 Lemma: If $\Delta \vdash \mathtt{S} \mathtt{<:} \mathtt{T}$ and $fields(bound_\Delta(\mathtt{T})) = \overline{\mathtt{T}}\ \overline{\mathtt{f}}$, then $fields(bound_\Delta(\mathtt{S})) = \overline{\mathtt{S}}\ \overline{\mathtt{g}}$ and $\mathtt{S}_i = \mathtt{T}_i$ and $\mathtt{g}_i = \mathtt{f}_i$ for all $i \leq \#(\overline{\mathtt{f}})$.

Proof: By simple induction on the derivation of $\Delta \vdash \mathtt{S} \mathtt{<:} \mathtt{T}$. ∎

3.4.8 Lemma: Suppose $\Delta = \Delta_1, \overline{\mathtt{X}} \mathtt{<:} \overline{\mathtt{N}}, \Delta_2$ where none of $\overline{\mathtt{X}}$ appears in Δ_1 and $\Delta_1 \vdash \overline{\mathtt{U}} \mathtt{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{N}}$ and $\Delta_1 \vdash \overline{\mathtt{U}}$ ok. If $fields(bound_\Delta(\mathtt{T}_0)) = \overline{\mathtt{T}}\ \overline{\mathtt{f}}$, then $fields(bound_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_0)) = \overline{\mathtt{S}}\ \overline{\mathtt{g}}$, and we have $\mathtt{f}_i = \mathtt{g}_i$ and $\mathtt{S}_i = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_i$ for $i \leq \#(\overline{\mathtt{f}})$.

Proof: If $\mathtt{T}_0$ is a nonvariable type $\mathtt{N}$, then

$$fields(bound_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N})) = fields([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}) = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{T}}\ \overline{\mathtt{f}}.$$

(The second equality is shown by straightforward induction on the derivation of $fields([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N})$.)

On the other hand, if $\mathtt{T}_0$ is a type variable $\mathtt{X}$, then we have three cases.

Case: $\quad \mathtt{X} \in dom(\Delta_1)$

Trivial because $bound_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{X}) = bound_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}(\mathtt{X}) = bound_\Delta(\mathtt{T}_0)$.

Case: $\quad \mathtt{X} \in dom(\Delta_2)$

Easy because $bound_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{X}) = bound_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}(\mathtt{X}) = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]bound_\Delta(\mathtt{X})$.

Case: $\quad \mathtt{X} = \mathtt{X}_i$

We have

$$fields(bound_\Delta(\mathtt{X}_i)) = fields(\mathtt{N}_i)$$

and

$$fields([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}_i) = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{T}}\ \overline{\mathtt{f}}.$$

The latter is shown by straightforward induction on the derivation of $fields(\mathtt{N})$. By Lemma 3.4.1, $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \mathtt{U}_i \mathtt{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}_i$. Finally, by Lemma 3.4.7,

$$fields(bound_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{X}_i)) = fields(bound_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}(\mathtt{U}_i)) = \overline{\mathtt{S}}\ \overline{\mathtt{g}}$$

where $\mathtt{f}_i = \mathtt{g}_i$ and $\mathtt{S}_i = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_i$ for $i \leq \#(\overline{\mathtt{f}})$. ∎

3.4.9 Lemma: If $\Delta \vdash \mathtt{T}$ ok and *mtype*(m, $bound_\Delta$(T)) = $\mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\mathtt{>}\overline{\mathtt{U}}\rightarrow\mathtt{U}_0$, then for any S such that $\Delta \vdash \mathtt{S} <: \mathtt{T}$ and $\Delta \vdash \mathtt{S}$ ok, we have *mtype*(m, $bound_\Delta$(S)) = $\mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\mathtt{>}\overline{\mathtt{U}}\rightarrow\mathtt{U}_0{}'$ and $\Delta, \overline{\mathtt{Y}}<:\overline{\mathtt{P}} \vdash \mathtt{U}_0{}' <: \mathtt{U}_0$.

Proof: By induction on the derivation of $\Delta \vdash \mathtt{S} <: \mathtt{T}$. The only interesting case is:

Case S-Class: $\mathtt{S} = \mathtt{C}\mathtt{<}\overline{\mathtt{T}}\mathtt{>}$ $\quad \mathtt{T} = [\overline{\mathtt{T}}/\overline{\mathtt{X}}]\mathtt{N}$ $\quad CT(\mathtt{C}) = \mathtt{class\ C}\mathtt{<}\overline{\mathtt{X}} \triangleleft \overline{\mathtt{N}}\mathtt{>} \triangleleft \mathtt{N}\ \{\ \ldots\ \overline{\mathtt{M}}\}$

If $\overline{\mathtt{M}}$ do not include m, it is easy to show the conclusion, since *mtype*(m, $bound_\Delta$(S)) = *mtype*(m, $bound_\Delta$(T)) by the rule MT-Super.

On the other hand, suppose $\overline{\mathtt{M}}$ includes a declaration of m. By straightforward induction on the derivation of *mtype*(m, T), we can show

$$mtype(\mathtt{m}, |\mathtt{T}|_\Delta) = mtype(\mathtt{m}, \mathtt{T}) = [\overline{\mathtt{T}}/\overline{\mathtt{X}}]\mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}'}\mathtt{>}\overline{\mathtt{U}'}\rightarrow\mathtt{U}_0{}'$$

where $\mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}'}\mathtt{>}\overline{\mathtt{U}'}\rightarrow\mathtt{U}_0{}' = mtype(\mathtt{m}, \mathtt{N})$. By GT-Method, it must be the case that

$$\mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}'}\mathtt{>}\ \mathtt{W}_0{}'\ \mathtt{m}\ (\overline{\mathtt{U}'}\ \overline{\mathtt{x}})\ \ldots \in \overline{\mathtt{M}}$$

and

$$\overline{\mathtt{X}}<:\overline{\mathtt{N}}, \overline{\mathtt{Y}}<:\overline{\mathtt{P}'} \vdash \mathtt{W}_0{}'<:\mathtt{U}_0{}'.$$

By Lemmas 3.4.4 and 3.4.1, we have

$$\Delta, \overline{\mathtt{Y}}<:\overline{\mathtt{P}} \vdash [\overline{\mathtt{T}}/\overline{\mathtt{X}}]\mathtt{W}_0{}'<:\mathtt{U}_0.$$

Since *mtype*(m, $bound_\Delta$(S)) = *mtype*(m, S) = $[\overline{\mathtt{T}}/\overline{\mathtt{X}}]\mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}'}\mathtt{>}\overline{\mathtt{U}'}\rightarrow\mathtt{W}_0{}'$ by MT-Class, letting $\mathtt{U}_0{}' = [\overline{\mathtt{T}}/\overline{\mathtt{X}}]\mathtt{W}_0{}'$ finishes the case. ∎

3.4.10 Lemma: Suppose $\Delta = \Delta_1, \overline{\mathtt{X}}<:\overline{\mathtt{N}}, \Delta_2$ where none of $\overline{\mathtt{X}}$ appears in Δ_1 and $\Delta_1 \vdash \overline{\mathtt{U}} <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{N}}$ and $\Delta_1 \vdash \overline{\mathtt{U}}$ ok. If *mtype*(m, $bound_\Delta(\mathtt{T}_0)$) = $\mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\mathtt{>}\overline{\mathtt{S}}\rightarrow\mathtt{U}$, then *mtype*(m, $bound_{\Delta_1,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_0)$) = $\mathtt{<}\overline{\mathtt{Y}} \triangleleft [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{P}}\mathtt{>}[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{S}}\rightarrow\mathtt{V}$ for some V such that $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2, \overline{\mathtt{Y}}<:[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{P}} \vdash \mathtt{V} <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{U}$.

Proof: Similar to the proof of Lemma 3.4.8.

If $\mathtt{T}_0$ is a nonvariable type N, then

$$mtype(\mathtt{m}, bound_{\Delta_1,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N})) = mtype(\mathtt{m}, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}) = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\mathtt{>}\overline{\mathtt{S}}\rightarrow\mathtt{U}.$$

(The second equality is shown by straightforward induction on the derivation of *mtype*(m, $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}$).) Without loss of generality, we can assume $\overline{\mathtt{Y}}$ and $\overline{\mathtt{X}}$ are distinct. Letting $\mathtt{V} = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{U}$ finishes the case.

On the other hand, if $\mathtt{T}_0$ is a type variable X, then we have three cases.

Case: $\mathtt{X} \in dom(\Delta_1)$

Trivial because $bound_{\Delta_1,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{X}) = bound_{\Delta_1,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}(\mathtt{X}) = bound_\Delta(\mathtt{X})$.

Case: $\mathtt{X} \in dom(\Delta_2)$

Easy because $bound_{\Delta_1,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{X}) = bound_{\Delta_1,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}(\mathtt{X}) = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]bound_\Delta(\mathtt{X})$.

Case: $\mathtt{X} = \mathtt{X}_i$

We have

$$mtype(\mathtt{m}, bound_\Delta(\mathtt{X}_i)) = mtype(\mathtt{m}, \mathtt{N}_i)$$

and

$$mtype(\mathtt{m}, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}_i) = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\mathtt{>}\overline{\mathtt{S}}\rightarrow\mathtt{U}.$$

Again, the latter is shown by straightforward induction on the derivation of *mtype*(m, $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}_i$). By Lemma 3.4.1, $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \mathtt{U}_i <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}_i$. Finally, by Lemma 3.4.9,

$$mtype(\mathtt{m}, bound_{\Delta_1,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{X}_i)) = mtype(\mathtt{m}, bound_{\Delta_1,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}(\mathtt{U}_i)) = \mathtt{<}\overline{\mathtt{Y}} \triangleleft [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{P}}\mathtt{>}[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{S}}\rightarrow\mathtt{V}$$

where

$$\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2, \overline{\mathtt{Y}}<:\overline{\mathtt{Q}} \vdash \mathtt{V} <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{U}.$$

∎

3.4.11 Lemma [Type substitution preserves typing]: If $\Delta_1, \overline{\mathtt{X}}$<:$\overline{\mathtt{N}}, \Delta_2; \Gamma \vdash \mathtt{e} \in \mathtt{T}$ and $\Delta_1 \vdash \overline{\mathtt{U}}$ <: $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{N}}$ where $\Delta_1 \vdash \overline{\mathtt{U}}$ ok and none of $\overline{\mathtt{X}}$ appears in Δ_1, then $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2; [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Gamma \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e} \in \mathtt{S}$ for some S such that $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \mathtt{S}$ <: $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}$.

Proof: By induction on the derivation of $\Delta_1, \overline{\mathtt{X}}$<:$\overline{\mathtt{N}}, \Delta_2; \Gamma \vdash \mathtt{e} \in \mathtt{T}$ with a case analysis on the last rule used. The interesting cases are:

Case GT-Field: $\quad \mathtt{e} = \mathtt{e}_0.\mathtt{f}_i \qquad \Delta_1, \overline{\mathtt{X}}$<:$\overline{\mathtt{N}}, \Delta_2; \Gamma \vdash \mathtt{e}_0 \in \mathtt{T}_0 \qquad \mathit{fields}(\mathit{bound}_{\Delta_1, \overline{\mathtt{X}}<:\overline{\mathtt{N}}, \Delta_2}(\mathtt{T}_0)) = \overline{\mathtt{T}}\ \overline{\mathtt{f}}$
$\mathtt{T} = \mathtt{T}_i$

By induction hypothesis, $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2; [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Gamma \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}_0 \in \mathtt{S}_0$ and $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \mathtt{S}_0$ <: $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_0$. By Lemmas 3.4.7 and 3.4.8, $\mathit{fields}(\mathit{bound}_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}(\mathtt{S}_0)) = \overline{\mathtt{S}}\ \overline{\mathtt{g}}$ and we have $\mathtt{f}_j = \mathtt{g}_j$ and $\mathtt{S}_j = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_j$ for $j \leq \#(\overline{\mathtt{f}})$. By the rule GT-Field, $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2; [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Gamma \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}_0.\mathtt{f}_i \in \mathtt{S}_i$. Lettig $\mathtt{S} = \mathtt{S}_i (= [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_i)$ finishes the case.

Case GT-Invk: $\quad \mathtt{e} = \mathtt{e}_0.\mathtt{m}$<$\overline{\mathtt{V}}$>$(\overline{\mathtt{e}}) \qquad \Delta_1, \overline{\mathtt{X}}$<:$\overline{\mathtt{N}}, \Delta_2; \Gamma \vdash \mathtt{e}_0 \in \mathtt{T}_0$
$\mathit{mtype}(\mathtt{m}, \mathit{bound}_{\Delta_1, \overline{\mathtt{X}}<:\overline{\mathtt{N}}, \Delta_2}(\mathtt{T}_0)) =$ <$\overline{\mathtt{Y}} \lhd \overline{\mathtt{P}}$>$\overline{\mathtt{W}} \to \mathtt{W}_0$
$\Delta_1, \overline{\mathtt{X}}$<:$\overline{\mathtt{N}}, \Delta_2 \vdash \overline{\mathtt{V}}$ ok $\qquad \Delta_1, \overline{\mathtt{X}}$<:$\overline{\mathtt{N}}, \Delta_2 \vdash \overline{\mathtt{V}}$ <: $[\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}}$
$\Delta_1, \overline{\mathtt{X}}$<:$\overline{\mathtt{N}}, \Delta_2; \Gamma \vdash \overline{\mathtt{e}} \in \overline{\mathtt{S}} \qquad \Delta_1, \overline{\mathtt{X}}$<:$\overline{\mathtt{N}}, \Delta_2 \vdash \overline{\mathtt{S}}$ <: $[\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{W}}$
$\mathtt{T} = [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{W}_0$

By induction hypothesis,

$$\begin{array}{l}\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2; [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Gamma \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}_0 \in \mathtt{S}_0\\ \Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \mathtt{S}_0 <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_0\end{array}$$

and

$$\begin{array}{l}\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2; [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Gamma \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{e}} \in \overline{\mathtt{S}}'\\ \Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \overline{\mathtt{S}}' <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{S}}.\end{array}$$

By Lemmas 3.4.10 and 3.4.9,

$$\begin{array}{l}\mathit{mtype}(\mathtt{m}, \mathit{bound}_{\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}(\mathtt{S}_0)) = \texttt{<}\overline{\mathtt{Y}} \lhd [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{P}}\texttt{>}[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{W}} \to \mathtt{W}_0{}'\\ \Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2, \overline{\mathtt{Y}} <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{P}} \vdash \mathtt{W}_0{}' <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{W}_0.\end{array}$$

By Lemma 3.4.5,

$$\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}} \text{ ok}$$

Without loss of generarity, we can assume that $\overline{\mathtt{X}}$ and $\overline{\mathtt{Y}}$ are distinct and that none of $\overline{\mathtt{Y}}$ appear in $\overline{\mathtt{U}}$, and thus $[\overline{\mathtt{U}}/\overline{\mathtt{X}}][\overline{\mathtt{V}}/\overline{\mathtt{Y}}] = [[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}][\overline{\mathtt{U}}/\overline{\mathtt{X}}]$. By Lemma 3.4.4,

$$\begin{array}{ll}\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}} <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}][\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}} & (= [[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}][\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{P}})\\ \Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{S}} <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}][\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{W}} & (= [[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}][\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{W}}).\end{array}$$

By the rule S-Trans,

$$\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \overline{\mathtt{S}}' <: [[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}][\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{W}}.$$

By Lemma 3.4.4, we have

$$\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{W}_0{}' <: [\overline{\mathtt{U}}/\overline{\mathtt{X}}][\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{W}_0 \quad (= [[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}][\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{W}_0).$$

Finally, by the rule GT-Invk,

$$\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Gamma \vdash ([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}_0).\mathtt{m}\texttt{<}[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}\texttt{>}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{d}}) \in \mathtt{S}$$

where $\mathtt{S} = [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{W}_0{}'$, finishing the case.

Case GT-DCast: $\quad \Delta = \Delta_1, \overline{\mathtt{X}}$<:$\overline{\mathtt{N}}, \Delta_2 \qquad \Delta; \Gamma \vdash \mathtt{e}_0 \in \mathtt{T}_0$
$\Delta \vdash \mathtt{N}$ <: $\mathit{bound}_\Delta(\mathtt{T}_0) \qquad \mathtt{N} \neq \mathit{bound}_\Delta(\mathtt{T}_0)$
$\mathit{downcast}(\mathtt{N}, \mathit{bound}_\Delta(\mathtt{T}_0))$

By induction hypothesis, $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2; [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Gamma \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}_0 \in \mathtt{S}_0$ for some $\mathtt{S}_0$ such that $\Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \mathtt{S}_0$ <: $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_0$. Let $\Delta' = \Delta_1, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2$. We have three subcases according to a relation between $\mathtt{S}_0$ and N.

Subcase: $\Delta' \vdash \mathit{bound}_\Delta(\mathtt{S}_0)$ <: N

By the rule GT-UCast, $\Delta'; \Gamma \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]((\mathtt{N})\,\mathtt{e}_0) \in \mathtt{N}$.

Subcase: $\Delta' \vdash \mathtt{N}$ <: $\mathit{bound}_{\Delta'}(\mathtt{S}_0)$ $\quad \mathtt{N} \neq \mathit{bound}_{\Delta'}(\mathtt{S}_0)$

Let $\mathtt{N} = \mathtt{C<\ldots>}$ and $\mathit{bound}_{\Delta'}(\mathtt{S}_0) = \mathtt{D<\ldots>}$ and $\mathit{bound}_\Delta(\mathtt{T}_0) = \mathtt{E<\ldots>}$. By using Lemma 3.4.6 and the fact that $\Delta \vdash \mathtt{S}$ <: T implies $\Delta \vdash \mathit{bound}_\Delta(\mathtt{S})$ <: $\mathit{bound}_\Delta(\mathtt{T})$, we have $\Delta' \vdash \mathit{bound}_{\Delta'}(\mathtt{S}_0)$ <: $[\overline{\mathtt{U}}/\overline{\mathtt{X}}](\mathit{bound}_\Delta(\mathtt{T}_0))$. Then, C ext D ext E. By Lemma 3.4.3, we have $\mathit{downcast}([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{N}, \mathtt{D<}\overline{\mathtt{V}}\mathtt{>})$ for some $\overline{\mathtt{V}}$; but $\mathtt{D<}\overline{\mathtt{V}}\mathtt{>}$ must be equal to $\mathit{bound}_{\Delta'}(\mathtt{S}_0)$ since $\mathit{downcast}(\mathtt{D<}\overline{\mathtt{V}}\mathtt{>}, [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathit{bound}_\Delta(\mathtt{T}_0))$. Finally, the rule GT-DCast finishes the subcase.

Subcase: $\Delta' \vdash \mathtt{N} \not<: \mathit{bound}_\Delta(\mathtt{S}_0)$ $\quad \Delta' \vdash \mathit{bound}_\Delta(\mathtt{S}_0) \not<: \mathtt{N}$

Let $\mathtt{N} = \mathtt{C<\ldots>}$ and $\mathit{bound}_{\Delta'}(\mathtt{S}_0) = \mathtt{D<\ldots>}$ and $\mathit{bound}_\Delta(\mathtt{T}_0) = \mathtt{E<\ldots>}$. By using Lemma 3.4.6 and the fact that $\Delta' \vdash \mathtt{S}$ <: T implies $\Delta' \vdash \mathit{bound}_\Delta(\mathtt{S})$ <: $\mathit{bound}_\Delta(\mathtt{T})$, we have $\Delta' \vdash \mathit{bound}_{\Delta'}(\mathtt{S}_0)$ <: $[\overline{\mathtt{U}}/\overline{\mathtt{X}}](\mathit{bound}_\Delta(\mathtt{T}_0))$. Now, we show that, by contradiction, that neither C $\not\text{e}$xt D nor D $\not\text{e}$xt C holds. Suppose C ext D. Then, there exist some $\overline{\mathtt{V}}'$ such that $\Delta' \vdash \mathtt{C<}\overline{\mathtt{V}}'\mathtt{>}$ <: $\mathit{bound}_\Delta(\mathtt{S}_0)$. By Lemma 3.4.3, we have $\mathit{downcast}(\mathtt{N}, \mathit{bound}_\Delta(\mathtt{S}_0))$, which implies $\mathtt{N} = \mathtt{C<}\overline{\mathtt{V}}'\mathtt{>}$, contradicting the assumption; thus, C $\not\text{e}$xt D. On the other hand, suppose D ext C. Since we have $\Delta' \vdash \mathit{bound}_{\Delta'}(\mathtt{S}_0)$ <: $[\overline{\mathtt{U}}/\overline{\mathtt{X}}](\mathit{bound}_\Delta(\mathtt{T}_0))$, we can have $\mathtt{C<}\overline{\mathtt{V}}'\mathtt{>}$ such that $\Delta' \vdash \mathit{bound}_{\Delta'}(\mathtt{S}_0)$ <: $\mathtt{C<}\overline{\mathtt{V}}'\mathtt{>}$ and $\Delta' \vdash \mathtt{C<}\overline{\mathtt{V}}'\mathtt{>}$ <: $[\overline{\mathtt{U}}/\overline{\mathtt{X}}](\mathit{bound}_\Delta(\mathtt{T}_0))$. Then, $\mathtt{N} = \mathtt{C<}\overline{\mathtt{V}}'\mathtt{>}$, contradicting the assumption $\Delta' \vdash \mathit{bound}_{\Delta'}(\mathtt{S}_0)$ <: N; thus, D $\not\text{e}$xt C. Finally, by the rule GT-SCast, $\Delta; \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]((\mathtt{N})\,\mathtt{e}_0) \in \mathtt{N}$ with *stupid warning*. ∎

3.4.12 Lemma [Term substitution preserves typing]: If $\Delta; \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{T}} \vdash \mathtt{e} \in \mathtt{T}$ and, $\Delta; \Gamma \vdash \overline{\mathtt{d}} \in \overline{\mathtt{S}}$ where $\Delta \vdash \overline{\mathtt{S}}$ <: $\overline{\mathtt{T}}$, then $\Delta; \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e} \in \mathtt{S}$ for some S such that $\Delta \vdash \mathtt{S}$ <: T.

Proof: By induction on the derivation of $\Delta; \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{T}} \vdash \mathtt{e} \in \mathtt{T}$. We will show only the interesting cases.

Case GT-Var: $\quad \mathtt{e} = \mathtt{x}$

If $\mathtt{x} \in \mathit{dom}(\Gamma)$, then it's trivial since $[\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{x} = \mathtt{x}$. On the other hand, if $\mathtt{x} = \mathtt{x}_i$ and $\mathtt{T} = \mathtt{T}_i$, then letting $\mathtt{S} = \mathtt{S}_i$ finishing the case.

Case GT-Field: $\quad \mathtt{e} = \mathtt{e}_0.\mathtt{f}_i \quad \Delta; \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{T}} \vdash \mathtt{e}_0 \in \mathtt{T}_0 \quad \mathit{fields}(\mathit{bound}_\Delta(\mathtt{T}_0)) = \overline{\mathtt{T}}\ \overline{\mathtt{f}} \quad \mathtt{T} = \mathtt{T}_i$

By induction hypothesis, $\Delta; \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0 \in \mathtt{S}_0$ for some $\mathtt{S}_0$ such that $\Delta \vdash \mathtt{S}_0$ <: $\mathtt{T}_0$. By Lemma 3.4.7, $\mathit{fields}(\mathit{bound}_\Delta(\mathtt{S}_0)) = \overline{\mathtt{S}}\ \overline{\mathtt{g}}$ such that $\mathtt{S}_j = \mathtt{T}_j$ and $\mathtt{f}_j = \mathtt{g}_j$ for all $j \leq \#(\overline{\mathtt{T}})$. Therefore, by the rule GT-Field, $\Delta; \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0.\mathtt{f}_i \in \mathtt{T}$

Case GT-Invk: $\quad \mathtt{e} = \mathtt{e}_0.\mathtt{m<}\overline{\mathtt{V}}\mathtt{>(}\overline{\mathtt{e}}\mathtt{)} \quad \Delta; \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{T}} \vdash \mathtt{e}_0 \in \mathtt{T}_0 \quad \mathit{mtype}(\mathtt{m}, \mathit{bound}_\Delta(\mathtt{T}_0)) = \mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\mathtt{>}\overline{\mathtt{U}} \to \mathtt{U}$
$\Delta \vdash \overline{\mathtt{V}}$ ok $\quad \Delta \vdash \overline{\mathtt{V}}$ <: $[\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}}$ $\quad \Delta; \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{T}} \vdash \overline{\mathtt{e}} \in \overline{\mathtt{S}}$
$\Delta \vdash \overline{\mathtt{S}}$ <: $[\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{U}}$ $\quad \mathtt{T} = [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}$

By induction hypothesis, $\Delta; \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0 \in \mathtt{S}_0$ for some $\mathtt{S}_0$ such that $\Delta \vdash \mathtt{S}_0$ <: $\mathtt{T}_0$ and $\Delta; \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\overline{\mathtt{e}} \in \overline{\mathtt{W}}$ for some $\overline{\mathtt{W}}$ such that $\Delta \vdash \overline{\mathtt{W}}$ <: $\overline{\mathtt{S}}$. By Lemma 3.4.9, $\mathit{mtype}(\mathtt{m}, \mathit{bound}_\Delta(\mathtt{S}_0)) = \mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\mathtt{>}\overline{\mathtt{U}} \to \mathtt{U}'$ and $\Delta, \overline{\mathtt{Y}}$<:$\overline{\mathtt{P}} \vdash \mathtt{U}'$ <: U. By Lemma 3.4.4, $\Delta \vdash [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}'$ <: $[\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}$. By the rule GT-Method, $\Delta; \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}](\mathtt{e}_0.\mathtt{m<}\overline{\mathtt{V}}\mathtt{>(}\overline{\mathtt{e}}\mathtt{)}) \in [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}'$. Letting $\mathtt{S} = [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}'$ finishes the case.

Case GT-DCast: $\quad \Delta; \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{T}} \vdash \mathtt{e}_0 \in \mathtt{T}_0 \quad \mathtt{N} = \mathtt{C<}\overline{\mathtt{U}}\mathtt{>} \quad \Delta \vdash \mathtt{C<}\overline{\mathtt{U}}\mathtt{>}$ <: $\mathit{bound}_\Delta(\mathtt{T}_0)$ $\quad \mathtt{C<}\overline{\mathtt{U}}\mathtt{>} \neq \mathit{bound}_\Delta(\mathtt{T}_0)$
$\Delta \vdash \mathtt{C<}\overline{\mathtt{S}}\mathtt{>}$ <: $\mathtt{T}_0$ and $\Delta \vdash \mathtt{C<}\overline{\mathtt{S}}\mathtt{>}$ ok imply $\overline{\mathtt{S}} = \overline{\mathtt{U}}$, for all $\overline{\mathtt{S}}$

By induction hypothesis, $\Delta; \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e}_0 \in \mathtt{S}_0$ for some $\mathtt{S}_0$ such that $\Delta \vdash \mathtt{S}_0$ <: $\mathtt{T}_0$. We have three subcases according to a relation between $\mathtt{S}_0$ and N.

Subcase: $\Delta \vdash \mathit{bound}_\Delta(\mathtt{S}_0)$ <: N

By the rule GT-UCast, $\Delta; \Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]((\mathtt{N})\,\mathtt{e}_0) \in \mathtt{N}$.

Subcase: $\Delta \vdash \mathtt{N}$ <: $\mathit{bound}_\Delta(\mathtt{S}_0)$ $\quad \mathtt{N} \neq \mathit{bound}_\Delta(\mathtt{S}_0)$

Since $\Delta \vdash \mathtt{S}_0$ <: $\mathtt{T}_0$ implies $\Delta \vdash \mathit{bound}_\Delta(\mathtt{S}_0)$ <: $\mathit{bound}_\Delta(\mathtt{T}_0)$, for any $\overline{\mathtt{S}}$ such that $\Delta \vdash \mathtt{C<}\overline{\mathtt{S}}\mathtt{>}$ <: $\mathit{bound}_\Delta(\mathtt{S}_0)$ and $\Delta \vdash \mathtt{C<}\overline{\mathtt{S}}\mathtt{>}$ ok, we have $\Delta \vdash \mathtt{C<}\overline{\mathtt{S}}\mathtt{>}$ <: $\mathit{bound}_\Delta(\mathtt{T}_0)$, which implies $\overline{\mathtt{S}} = \overline{\mathtt{U}}$ for all $\overline{\mathtt{S}}$. Finally, the rule GT-DCast finishes the subcase.

Subcase: $\Delta \vdash \mathtt{N} \not<: \mathit{bound}_\Delta(\mathtt{S}_0)$ $\quad \Delta \vdash \mathit{bound}_\Delta(\mathtt{S}_0) \not<: \mathtt{N}$

Let $\mathit{bound}_\Delta(\mathtt{S}_0) = \mathtt{D<}\overline{\mathtt{V}}\mathtt{>}$ and $\mathit{bound}_\Delta(\mathtt{T}_0) = \mathtt{E<}\overline{\mathtt{W}}\mathtt{>}$. We can show that, by contradiction, that C $\not\text{e}$xt D and D $\not\text{e}$xt C in a way similar to the third subcase in the case for GT-DCast of the previous proof.

Case GT-SCAST: $\quad \Delta;\Gamma,\overline{\mathtt{x}}:\overline{\mathtt{T}} \vdash \mathtt{e_0} \in \mathtt{T_0} \qquad \mathtt{N} = \mathtt{C}\texttt{<}\overline{\mathtt{U}}\texttt{>} \qquad \mathit{bound}_\Delta(\mathtt{T_0}) = \mathtt{D}\texttt{<}\overline{\mathtt{V}}\texttt{>}$

$\qquad\qquad\qquad\qquad \mathtt{C}\ \not\mathtt{e}\mathtt{xt}\ \mathtt{D} \qquad\qquad \mathtt{D}\ \not\mathtt{e}\mathtt{xt}\ \mathtt{C}$

By induction hypothesis, $\Delta;\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]\mathtt{e_0} \in \mathtt{S_0}$ for some $\mathtt{S_0}$ such that $\Delta \vdash \mathtt{S_0} \texttt{<:} \mathtt{T_0}$, which implies $\Delta \vdash \mathit{bound}_\Delta(\mathtt{S_0}) \texttt{<:} \mathit{bound}_\Delta(\mathtt{T_0})$. Let $\mathit{bound}_\Delta(\mathtt{S_0}) = \mathtt{E}\texttt{<}\overline{\mathtt{S}}\texttt{>}$. By Lemma 3.4.2, we have $\mathtt{E}\ \not\mathtt{e}\mathtt{xt}\ \mathtt{C}$ and $\mathtt{C}\ \not\mathtt{e}\mathtt{xt}\ \mathtt{E}$. Then, by the rule GT-SCAST, $\Delta;\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}]((\mathtt{N})\mathtt{e_0}) \in \mathtt{N}$ with *stupid warning.* ∎

3.4.13 Lemma: If $\mathit{mtype}(\mathtt{m}, \mathtt{C}\texttt{<}\overline{\mathtt{T}}\texttt{>}) = \texttt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\texttt{>}\overline{\mathtt{U}}\rightarrow\mathtt{U}$ and $\mathit{mbody}(\mathtt{m}\texttt{<}\overline{\mathtt{V}}\texttt{>}, \mathtt{C}\texttt{<}\overline{\mathtt{T}}\texttt{>}) = (\overline{\mathtt{x}}, \mathtt{e_0})$ where $\Delta \vdash \mathtt{C}\texttt{<}\overline{\mathtt{T}}\texttt{>}$ ok and $\Delta \vdash \overline{\mathtt{V}}$ ok and $\Delta \vdash \overline{\mathtt{V}} \texttt{<:} [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}}$, then there exist some $\mathtt{N}$ and $\mathtt{S}$ such that $\Delta \vdash \mathtt{C}\texttt{<}\overline{\mathtt{T}}\texttt{>} \texttt{<:} \mathtt{N}$ and $\Delta \vdash \mathtt{N}$ ok and $\Delta \vdash \mathtt{S} \texttt{<:} [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}$ and $\Delta \vdash \mathtt{S}$ ok and $\Delta;\overline{\mathtt{x}}:[\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{U}}, \mathtt{this}:\mathtt{N} \vdash \mathtt{e_0} \in \mathtt{S}$.

Proof: By easy induction on the derivation of $\mathit{mbody}(\mathtt{m}\texttt{<}\overline{\mathtt{V}}\texttt{>}, \mathtt{C}\texttt{<}\overline{\mathtt{T}}\texttt{>}) = (\overline{\mathtt{x}}, \mathtt{e})$ using Lemmas 3.4.4 and 3.4.11. ∎

3.4.14 Theorem [Subject reduction]: If $\Delta;\Gamma \vdash \mathtt{e} \in \mathtt{T}$ and $\mathtt{e} \longrightarrow \mathtt{e}'$, then $\Delta;\Gamma \vdash \mathtt{e}' \in \mathtt{T}'$, for some $\mathtt{T}'$ such that $\Delta \vdash \mathtt{T}' \texttt{<:} \mathtt{T}$.

Proof: By induction on the derivation of $\mathtt{e} \longrightarrow \mathtt{e}'$ with a case analysis on the reduction rule used. We will show main cases.

Case GR-FIELD: $\quad \mathtt{e} = \mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}})\mathtt{.f}_i \qquad \mathit{fields}(\mathtt{N}) = \overline{\mathtt{T}}\ \overline{\mathtt{f}} \qquad \mathtt{e}' = \mathtt{e}_i$

By the rules GT-FIELD and GT-NEW, we have

$$\Delta;\Gamma \vdash \mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}}) \in \mathtt{N} \quad \Delta;\Gamma \vdash \overline{\mathtt{e}} \in \overline{\mathtt{S}} \quad \Delta \vdash \overline{\mathtt{S}} \texttt{<:} \overline{\mathtt{T}}.$$

In particular, $\Delta;\Gamma \vdash \mathtt{e}_i \in \mathtt{S}_i$ finishes the case.

Case GR-INVK: $\quad \mathtt{e} = \mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}})\mathtt{.m}\texttt{<}\overline{\mathtt{V}}\texttt{>}(\overline{\mathtt{d}}) \qquad \mathit{mbody}(\mathtt{m}\texttt{<}\overline{\mathtt{V}}\texttt{>}, \mathtt{N}) = (\overline{\mathtt{x}}, \mathtt{e_0})$

$\qquad\qquad\qquad \mathtt{e}' = [\overline{\mathtt{d}}/\overline{\mathtt{x}}, \mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}})/\mathtt{this}]\mathtt{e_0}$

By the rules GT-INVK and GT-NEW, we have

$$\begin{array}{ll} \Delta;\Gamma \vdash \mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}}) \in \mathtt{N} & \mathit{mtype}(\mathtt{m}, \mathit{bound}_\Delta(\mathtt{N})) = \texttt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\texttt{>}\overline{\mathtt{U}}\rightarrow\mathtt{U} \\ \Delta \vdash \overline{\mathtt{V}}\ \text{ok} & \Delta \vdash \overline{\mathtt{V}} \texttt{<:} [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}} \\ \Delta;\Gamma \vdash \overline{\mathtt{d}} \in \overline{\mathtt{S}} & \Delta \vdash \overline{\mathtt{S}} \texttt{<:} [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{U}} \\ \mathtt{T} = [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U} & \Delta \vdash \mathtt{N}\ \text{ok} \end{array}$$

By Lemma 3.4.13, $\Delta;\overline{\mathtt{x}}:[\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{U}}, \mathtt{this}:\mathtt{O} \vdash \mathtt{e_0} \in \mathtt{S}$ for some $\mathtt{O}$ and $\mathtt{S}$ such that $\Delta \vdash \mathtt{N} \texttt{<:} \mathtt{O}$ where $\Delta \vdash \mathtt{O}$ ok, and $\Delta \vdash \mathtt{S} \texttt{<:} [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}$ where $\Delta \vdash \mathtt{S}$ ok. Then, by Lemmas 3.4.1 and 3.4.12, $\Delta;\Gamma \vdash [\overline{\mathtt{d}}/\overline{\mathtt{x}}, \mathtt{new}\ \mathtt{N}(\overline{\mathtt{e}})/\mathtt{this}]\mathtt{e_0} \in \mathtt{T_0}$ for some $\mathtt{T_0}$ such that $\Delta \vdash \mathtt{T_0} \texttt{<:} \mathtt{S}$. By the rule S-TRANS, we have $\Delta \vdash \mathtt{T_0} \texttt{<:} \mathtt{T}$. Finally, letting $\mathtt{T}' = \mathtt{T_0}$ finishes the case.

Case GRC-FIELD: $\quad \mathtt{e} = \mathtt{e_0}\mathtt{.f} \qquad \mathtt{e}' = \mathtt{e_0}'\mathtt{.f} \qquad \mathtt{e_0} \longrightarrow \mathtt{e_0}'$

By the rule GT-FIELD, we have

$$\begin{array}{l} \Delta;\Gamma \vdash \mathtt{e_0} \in \mathtt{T_0} \\ \mathit{fields}(\mathit{bound}_\Delta(\mathtt{T_0})) = \overline{\mathtt{T}}\ \overline{\mathtt{f}} \\ \mathtt{T} = \mathtt{T}_i \end{array}$$

By induction hypothesis, $\Delta;\Gamma \vdash \mathtt{e_0}' \in \mathtt{T_0}'$ for some $\mathtt{T_0}'$ such that $\Delta \vdash \mathtt{T_0}' \texttt{<:} \mathtt{T_0}$. By Lemma 3.4.7, $\mathit{fields}(\mathit{bound}_\Delta(\mathtt{T_0}')) = \overline{\mathtt{T}}'\ \overline{\mathtt{g}}$, and for $j \leq \#(\overline{\mathtt{f}})$, we have $\mathtt{g}_i = \mathtt{f}_i$ and Therefore, by the rule GT-FIELD, $\Delta;\Gamma \vdash \mathtt{e_0}'\mathtt{.f} \in \mathtt{T}_i'$. Letting $\mathtt{T}' = \mathtt{T}_i'$ finishes the case.

Case GRC-INV-RECV: $\quad \mathtt{e} = \mathtt{e_0}\mathtt{.m}\texttt{<}\overline{\mathtt{V}}\texttt{>}(\overline{\mathtt{e}}) \qquad \mathtt{e}' = \mathtt{e_0}'\mathtt{.m}\texttt{<}\overline{\mathtt{V}}\texttt{>}(\overline{\mathtt{e}}) \qquad \mathtt{e_0} \longrightarrow \mathtt{e_0}'$

By the rule GT-INVK, we have

$$\begin{array}{ll} \Delta;\Gamma \vdash \mathtt{e_0} \in \mathtt{T_0} & \mathit{mtype}(\mathtt{m}, \mathit{bound}_\Delta(\mathtt{T_0})) = \texttt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\texttt{>}\overline{\mathtt{T}}\rightarrow\mathtt{U} \\ \Delta \vdash \overline{\mathtt{V}}\ \text{ok} & \Delta \vdash \overline{\mathtt{V}} \texttt{<:} [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}} \\ \Delta \vdash \overline{\mathtt{e}} \in \overline{\mathtt{S}} & \Delta \vdash \overline{\mathtt{S}} \texttt{<:} [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{T}} \\ \mathtt{T} = [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U} & \end{array}$$

By induction hypothesis, $\Delta;\Gamma \vdash \mathtt{e_0}' \in \mathtt{T_0}'$ for some $\mathtt{T_0}'$ such that $\Delta \vdash \mathtt{T_0}' \texttt{<:} \mathtt{T_0}$. By Lemma 3.4.9, $\mathit{mtype}(\mathtt{m}, \mathit{bound}_\Delta(\mathtt{T_0}')) = \texttt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\texttt{>}\overline{\mathtt{T}}\rightarrow\mathtt{V}$ and $\Delta, \overline{\mathtt{Y}}\texttt{<:}\overline{\mathtt{P}} \vdash \mathtt{V} \texttt{<:} \mathtt{U}$. By Lemma 3.4.4, $\Delta \vdash [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{V} \texttt{<:} [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}$. Then, by the rule GT-INVK, $\Delta;\Gamma \vdash \mathtt{e_0}'\mathtt{.m}\texttt{<}\overline{\mathtt{V}}\texttt{>}(\overline{\mathtt{e}}) \in [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{V}$. Letting $\mathtt{T_0}' = [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{V}$ finishes the case.

Case GRC-CAST: $\quad \texttt{e} = \texttt{(N)e}_0 \quad \texttt{e}' = \texttt{(N)e}_0{}' \quad \texttt{e}_0 \longrightarrow \texttt{e}_0{}'$

There are three subcases according to the last typing rule. All the cases are fairly straightforward. Note that we use Lemma 3.4.2 for the case where the last rule is GT-SCAST. ∎

3.4.15 Theorem [Progress]: Suppose $\texttt{e}$ is a well-typed expression.

(1) If $\texttt{e}$ includes $\texttt{new N}_0\texttt{(}\overline{\texttt{e}}\texttt{).f}$ as a subexpression, then $\mathit{fields}(\texttt{N}_0) = \overline{\texttt{T}}\ \overline{\texttt{f}}$ and $\texttt{f} \in \overline{\texttt{f}}$.

(2) If $\texttt{e}$ includes $\texttt{new N}_0\texttt{(}\overline{\texttt{e}}\texttt{).m<}\overline{\texttt{V}}\texttt{>(}\overline{\texttt{d}}\texttt{)}$ as a subexpression, then $\mathit{mbody}(\texttt{m<}\overline{\texttt{V}}\texttt{>}, \texttt{N}_0) = (\overline{\texttt{x}}, \texttt{e}_0)$ and $\#(\overline{\texttt{x}}) = \#(\overline{\texttt{d}})$.

Proof: Similar to the proof of Theorem 2.4.6. ∎

Backward compatibility

FGJ is backward compatible with FJ. Intuitively, this means that an implementation of FGJ can be used to typecheck and execute FJ programs without changing their meaning. In the following statements, we use subscripts FJ or FGJ to show which set of rules is used.

3.4.16 Lemma: If CT is an FJ class table, then $\mathit{fields}_{\mathrm{FJ}}(\texttt{C}) = \mathit{fields}_{\mathrm{FGJ}}(\texttt{C})$ for all $\texttt{C} \in \mathit{dom}(CT)$.

3.4.17 Lemma: Suppose CT is an FJ class table. Then, $\mathit{mtype}_{\mathrm{FJ}}(\texttt{m}, \texttt{C}) = \overline{\texttt{C}} \rightarrow \texttt{C}$ if and only if $\mathit{mtype}_{\mathrm{FGJ}}(\texttt{m}, \texttt{C}) = \overline{\texttt{C}} \rightarrow \texttt{C}$.

3.4.18 Lemma: Suppose CT is an FJ class table. Then, $\mathit{mbody}_{\mathrm{FJ}}(\texttt{m}, \texttt{C}) = (\overline{\texttt{x}}, \texttt{e})$ if and only if $\mathit{mbody}_{\mathrm{FGJ}}(\texttt{m}, \texttt{C}) = (\overline{\texttt{x}}, \texttt{e})$.

Proof: All these lemmas are easy. Note that all substitutions in the derivations are empty and there are no polymorphic methods. ∎

We can show that a well-typed FJ program is always a well-typed FGJ program and that FJ and FGJ reduction correspond. (Note that it isn't quite the case that the well-typedness of an FJ program under the FGJ rules implies its well-typedness in FJ, because FGJ allows covariant overriding and FJ does not.)

3.4.19 Theorem [Backward compatibility]: If an FJ program $(\texttt{e}, CT)$ is well typed under the typing rules of FJ, then it is also well-typed under the rules of FGJ. Moreover, for all FJ programs $\texttt{e}$ and $\texttt{e}'$ (whether well typed or not), $\texttt{e} \longrightarrow_{\mathrm{FJ}} \texttt{e}'$ iff $\texttt{e} \longrightarrow_{\mathrm{FGJ}} \texttt{e}'$.

Proof: The first half is shown by straightforward induction on the derivation of $\Gamma \vdash \texttt{e} \in \texttt{C}$ (using FJ typing rules), followed by an analysis of the rules GT-METHOD and GT-CLASS. In the second half, both directions are shown by induction on a derivation of the reduction relation, with a case analysis on the last rule used. ∎

4 Compiling FGJ to FJ

We now explore the second implementation style for GJ and FGJ. The current GJ compiler works by translation into the standard JVM, which maintains no information about type parameters at run-time. We model this compilation in our framework by an *erasure* translation from FGJ into FJ. We show that this translation maps well-typed FGJ programs into well-typed FJ programs, and that the behavior of a program in FGJ matches (in a suitable sense) the behavior of its erasure under the FJ reduction rules.

A program is erased by replacing types with their erasures, inserting downcasts where required. A type is erased by removing type parameters, and replacing type variables with the erasure of their bounds. For example, the class `Pair<X,Y>` in the previous section erases to the following:

```
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);
  }
}
```

Similarly, the field selection

```
new Pair<A,B>(new A(), new B()).snd
```

erases to

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

where the added downcast `(B)` recovers type information of the original program. We call such downcasts inserted by erasure *synthetic.*

4.1 Erasure of Types

To erase a type, we remove any type parameters and replace type variables with the erasure of their bounds. Write $|\mathtt{T}|_\Delta$ for the erasure of type `T` with respect to type environment Δ

$$|\mathtt{T}|_\Delta = \mathtt{C}$$

where $\mathit{bound}_\Delta(\mathtt{T}) = \mathtt{C<}\overline{\mathtt{T}}\mathtt{>}$.

4.2 Field and Method Lookup

In FGJ (and GJ), a subclass may extend an instantiated superclass. This means that, unlike in FJ (and Java), the types of the fields and the methods in the subclass may not be identical to the types in the superclass. In order to specify a type-preserving erasure from FGJ to FJ, it is necessary to define additional auxiliary functions that look up the type of a field or method in the *highest* superclass in which it is defined.

For example, we previously defined the generic class `Pair<X,Y>`. We may declare a specialized subclass `PairOfA` as a subclass of the instantiation `Pair<A,A>`, which instantiates both `X` and `Y` to a given class `A`.

```
class PairOfA extends Pair<A,A> {
  PairOfA(A fst, A snd) {
    super(fst, snd);
  }
  PairOfA setfst(A newfst) {
    return new PairOfA(newfst, this.snd);
  }
}
```

Note that, in the `setfst` method, the argument type `A` matches the argument type of `setfst` in `Pair<A,A>`, while the result type `PairOfA` is a subtype of the result type in `Pair<A,A>`; this is permitted by FGJ's covariant subtyping, as discussed in the previous section. Erasing the class `PairOfA` yields the following:

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

Here arguments to the constructor and the method are given type `Object`, even though the erasure of `A` is itself; and the result of the method is given type `Pair`, even though the erasure of `PairOfA` is itself. In both cases, the types are chosen to correspond to types in `Pair`, the highest superclass in which the fields and method are defined.

We define variants of the auxiliary functions that find the types of fields and methods in the highest superclass in which they are defined. The maximum field types of a class `C`, written *fieldsmax*(`C`), is the sequence of pairs of a type and a field name defined as follows:

$$\mathit{fieldsmax}(\mathtt{Object}) = \bullet$$

$$\frac{\begin{array}{c} CT(\mathtt{C}) = \mathtt{class\ C<\overline{X} \triangleleft \overline{N}> \triangleleft D<\overline{U}>\ \{\overline{T}\ \overline{f};\ \ldots\ \}} \\ \Delta = \mathtt{\overline{X}<:\overline{N}} \qquad \mathtt{\overline{C}\ \overline{g}} = \mathit{fieldsmax}(\mathtt{D}) \end{array}}{\mathit{fieldsmax}(\mathtt{C}) = \mathtt{\overline{C}\ \overline{g}},\ |\mathtt{\overline{T}}|_\Delta\ \mathtt{\overline{f}}}$$

The maximum method type of `m` in `C`, written *mtypemax*(`m`, `C`), is defined as follows:

$$\frac{CT(\mathtt{C}) = \mathtt{class\ C<\overline{X} \triangleleft \overline{N}> \triangleleft D<\overline{U}>\ \{\ldots\}} \qquad \mathtt{<\overline{Y} \triangleleft \overline{O}>\overline{T}\to T} = \mathit{mtype}(\mathtt{m},\ \mathtt{D<\overline{U}>})}{\mathit{mtypemax}(\mathtt{m},\mathtt{C}) = \mathit{mtypemax}(\mathtt{m},\mathtt{D})}$$

$$\frac{\begin{array}{c} CT(\mathtt{C}) = \mathtt{class\ C<\overline{X} \triangleleft \overline{N}> \triangleleft D<\overline{U}>\ \{\ldots\}} \\ \mathit{mtype}(\mathtt{m},\ \mathtt{D<\overline{U}>}) \text{ undefined} \\ \mathtt{<\overline{Y} \triangleleft \overline{O}>\overline{T}\to T} = \mathit{mtype}(\mathtt{m}, \mathtt{C<\overline{X}>}) \qquad \Delta = \mathtt{\overline{X}<:\overline{N}},\ \mathtt{\overline{Y}<:\overline{O}} \end{array}}{\mathit{mtypemax}(\mathtt{m},\mathtt{C}) = |\mathtt{\overline{T}}|_\Delta \to |\mathtt{T}|_\Delta}$$

We also need a way to look up the maximum type of a given field. If *fieldsmax*(`C`) $=$ $\mathtt{\overline{D}\ \overline{f}}$ then we set *fieldsmax*(`C`)($\mathtt{f}_i$) $= \mathtt{D}_i$.

4.3 Erasure of Expressions

The erasure of an expression depends on the typing of that expression, since the types are used to determine which downcasts to insert. The erasure rules are optimized to omit casts when it is trivially safe to do so; this happens when the maximum type is equal to the erased type.

Write $|\mathtt{e}|_{\Delta,\Gamma}$ for the erasure of a well-typed expression `e` with respect to environment Γ and type environment Δ:

$$|\mathtt{x}|_{\Delta,\Gamma} = \mathtt{x} \tag{E-Var}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{e_0.f} \in \mathtt{T} \qquad \Delta;\Gamma \vdash \mathtt{e_0} \in \mathtt{T_0} \qquad \mathit{fieldsmax}(|\mathtt{T_0}|_\Delta)(\mathtt{f}) = |\mathtt{T}|_\Delta}{|\mathtt{e_0.f}|_{\Delta,\Gamma} = |\mathtt{e_0}|_{\Delta,\Gamma}\mathtt{.f}} \tag{E-Field}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{e_0.f} \in \mathtt{T} \qquad \Delta;\Gamma \vdash \mathtt{e_0} \in \mathtt{T_0} \qquad \mathit{fieldsmax}(|\mathtt{T_0}|_\Delta)(\mathtt{f}) \neq |\mathtt{T}|_\Delta}{|\mathtt{e_0.f}|_{\Delta,\Gamma} = (|\mathtt{T}|_\Delta)\ |\mathtt{e_0}|_{\Delta,\Gamma}\mathtt{.f}} \tag{E-Field-Cast}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{e_0.m<\overline{V}>(\overline{e})} \in \mathtt{T} \qquad \Delta;\Gamma \vdash \mathtt{e_0} \in \mathtt{T_0} \qquad \mathit{mtypemax}(\mathtt{m}, |\mathtt{T_0}|_\Delta) = \mathtt{\overline{C}\to D} \qquad \mathtt{D} = |\mathtt{T}|_\Delta}{|\mathtt{e_0.m<\overline{V}>(\overline{e})}|_{\Delta,\Gamma} = |\mathtt{e_0}|_{\Delta,\Gamma}\mathtt{.m(}|\mathtt{\overline{e}}|_{\Delta,\Gamma}\mathtt{)}} \tag{E-Invk}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{e_0.m<\overline{V}>(\overline{e})} \in \mathtt{T} \qquad \Delta;\Gamma \vdash \mathtt{e_0} \in \mathtt{T_0} \qquad \mathit{mtypemax}(\mathtt{m}, |\mathtt{T_0}|_\Delta) = \mathtt{\overline{C}\to D} \qquad \mathtt{D} \neq |\mathtt{T}|_\Delta}{|\mathtt{e_0.m<\overline{V}>(\overline{e})}|_{\Delta,\Gamma} = (|\mathtt{T}|_\Delta)\ |\mathtt{e_0}|_{\Delta,\Gamma}\mathtt{.m(}|\mathtt{\overline{e}}|_{\Delta,\Gamma}\mathtt{)}} \tag{E-Invk-Cast}$$

$$|\mathtt{new\ N(\overline{e})}|_{\Delta,\Gamma} = \mathtt{new}\ |\mathtt{N}|_\Delta\mathtt{(}|\mathtt{\overline{e}}|_{\Delta,\Gamma}\mathtt{)} \tag{E-New}$$

$$|\texttt{(N)e}_0|_{\Delta,\Gamma} = \texttt{(}|\texttt{N}|_\Delta\texttt{)}\ \ |\texttt{e}_0|_{\Delta,\Gamma} \tag{E-Cast}$$

(Strictly speaking, one should think of the erasure operation as acting on typing derivations rather than expressions. Since well-typed expressions are in 1-1 correspondence with their typing derivations, the abuse of notation creates no confusion.)

4.4 Erasure of Methods and Classes

The erasure of a method m with respect to type environment Δ in class C, written $|\texttt{M}|_{\Delta,\texttt{C}}$, is defined as follows:

$$\frac{\Gamma = \overline{\texttt{x}}\texttt{:}\overline{\texttt{T}}, \texttt{this} : \texttt{C<}\overline{\texttt{X}}\texttt{>} \qquad \Delta' = \overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}}, \overline{\texttt{Y}}\texttt{<:}\overline{\texttt{O}} \qquad \texttt{e}' = [\texttt{(}|\overline{\texttt{T}}|_{\Delta'}\texttt{)}\overline{\texttt{x}}'/\overline{\texttt{x}}]|\texttt{e}|_{\Delta',\Gamma} \qquad \mathit{mtypemax}(\texttt{m}, \texttt{C}) = \overline{\texttt{D}}{\rightarrow}\texttt{D}}{|\texttt{<}\overline{\texttt{Y}}\triangleleft\overline{\texttt{O}}\texttt{> T m (}\overline{\texttt{T}}\ \overline{\texttt{x}}\texttt{) \{}\uparrow\texttt{e;\}}|_{\overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}},\texttt{C}} = \texttt{D m (}\overline{\texttt{D}}\ \overline{\texttt{x}}'\texttt{) \{}\uparrow\texttt{e}'\texttt{;\}}} \tag{E-Method}$$

(In GJ, the actual erasure is somewhat more complex, involving the introduction of bridge methods, so that one ends up with two overloaded methods: one with the maximum type, and one with the instantiated type. We don't model that extra complexity here, because it depends on overloading of method names, which is not modeled in FJ.)

The erasure of constructors and classes is:

$$\begin{array}{l}|\texttt{C(}\overline{\texttt{U}}\ \overline{\texttt{g}}\texttt{, }\overline{\texttt{T}}\ \overline{\texttt{f}}\texttt{) \{super(}\overline{\texttt{g}}\texttt{); this.}\overline{\texttt{f}}\texttt{ = }\overline{\texttt{f}}\texttt{;\}}|_{\Delta,\texttt{C}} \\ = \texttt{C(}\mathit{fieldsmax}(\texttt{C})\texttt{) \{super(}\overline{\texttt{g}}\texttt{); this.}\overline{\texttt{f}}\texttt{ = }\overline{\texttt{f}}\texttt{;\}}\end{array} \tag{E-Constructor}$$

$$\frac{\Delta = \overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}}}{\begin{array}{c}|\texttt{class C<}\overline{\texttt{X}}\triangleleft\overline{\texttt{N}}\texttt{>}\triangleleft\texttt{N \{}\overline{\texttt{T}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}}| \\ = \texttt{class C}\triangleleft|\texttt{N}|_\Delta\texttt{\{}|\overline{\texttt{T}}|_\Delta\ \overline{\texttt{f}}\texttt{; }|\texttt{K}|_\Delta\ \ |\overline{\texttt{M}}|_{\Delta,\texttt{C}}\texttt{\}}\end{array}} \tag{E-Class}$$

4.5 Properties of Erasure

Having defined erasure, we may investigate some of its properties.

Preservation of Typing

First, a well-typed FGJ program erases to a well-typed FJ program, as expected:

4.5.1 Lemma: If $\Delta \vdash \texttt{S} \texttt{ <: } \texttt{T}$, then $|\texttt{S}|_\Delta \texttt{ <: } |\texttt{T}|_\Delta$.

Proof: Straightforward induction on the derivation of $\Delta \vdash \texttt{S} \texttt{ <: } \texttt{T}$. ∎

4.5.2 Lemma: If $\Delta_1, \overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}}, \Delta_2 \vdash \texttt{U}$ ok, then and $\Delta_1 \vdash \overline{\texttt{T}} \texttt{ <: } [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{N}}$, then $|[\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{U}|_{\Delta_1,\ [\overline{\texttt{T}}/\overline{\texttt{X}}]\Delta_2} \texttt{ <: } |\texttt{U}|_\Delta$.

Proof: If U is nonvariable or a type variable $\texttt{Y} \notin \overline{\texttt{X}}$, then the result is trivial. If U is a type variable $\texttt{X}_i$, on the other hand, it's also easy since $[\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{U} = \texttt{T}_i$ and, by Lemma 4.5.1, $|\texttt{T}_i|_{\Delta_1} \texttt{ <: } |[\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N}_i|_{\Delta_1} = |\texttt{N}_i|_{\Delta_1} = |\texttt{X}|_\Delta$. ∎

4.5.3 Lemma: If $\Delta \vdash \texttt{C<}\overline{\texttt{U}}\texttt{>}$ ok and $\mathit{fields}_{\text{FGJ}}(\texttt{C<}\overline{\texttt{U}}\texttt{>}) = \overline{\texttt{V}}\ \overline{\texttt{f}}$, then $\mathit{fieldsmax}(\texttt{C}) = \overline{\texttt{D}}\ \overline{\texttt{f}}$ and $|\overline{\texttt{V}}|_\Delta \texttt{ <: } \overline{\texttt{D}}$.

Proof: By induction on the derivation of $\mathit{fields}_{\text{FGJ}}(\texttt{C<}\overline{\texttt{U}}\texttt{>})$ using the fact that $\Delta \vdash \overline{\texttt{U}} \texttt{ <: } [\overline{\texttt{U}}/\overline{\texttt{X}}]\overline{\texttt{N}}$ derived from the rule WF-Class, where $CT(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}}\triangleleft\overline{\texttt{N}}\texttt{> ...}$, and Lemma 4.5.2. ∎

4.5.4 Lemma: If $\Delta \vdash \texttt{C<}\overline{\texttt{T}}\texttt{>}$ ok and $\mathit{mtype}_{\text{FGJ}}(\texttt{m}, \texttt{C<}\overline{\texttt{T}}\texttt{>}) = \texttt{<}\overline{\texttt{Y}}\triangleleft\overline{\texttt{P}}\texttt{>}\overline{\texttt{U}}{\rightarrow}\texttt{U}_0$ where $\Delta \vdash \overline{\texttt{V}} \texttt{ <: } [\overline{\texttt{V}}/\overline{\texttt{Y}}]\overline{\texttt{P}}$, then $\mathit{mtypemax}(\texttt{m}, \texttt{C}) = \overline{\texttt{C}}{\rightarrow}\texttt{C}_0$ and $|[\overline{\texttt{V}}/\overline{\texttt{Y}}]\overline{\texttt{U}}|_\Delta \texttt{ <: } \overline{\texttt{C}}$ and $|[\overline{\texttt{V}}/\overline{\texttt{Y}}]\texttt{U}_0|_\Delta \texttt{ <: } \texttt{C}_0$.

Proof: By induction on the length n of the canonical subtyping sequence for $\Delta \vdash \texttt{C<}\overline{\texttt{T}}\texttt{>} \texttt{ <: } \texttt{Object}$.

Case: $n = 2$

It must be the case that

$$\begin{array}{l} CT(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{Object \{ ...} \\ \qquad\qquad \texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{Q}}\texttt{>W}_0\ \texttt{m (}\overline{\texttt{W}}\ \overline{\texttt{x}}\texttt{) \{...\} ...\}.} \end{array}$$

By the definition of *mtypemax*, $\overline{\texttt{C}} = |\overline{\texttt{W}}|_{\overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}},\ \overline{\texttt{Y}}\texttt{<:}\overline{\texttt{Q}}}$ and $\texttt{C}_0 = |\texttt{W}_0|_{\overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}},\ \overline{\texttt{Y}}\texttt{<:}\overline{\texttt{Q}}}$. By the definition of $mtypeof_{\text{FGJ}}$,

$$\begin{array}{l} [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{Q}} = \overline{\texttt{P}} \\ [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{W}} = \overline{\texttt{U}} \\ [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{W}_0 = \texttt{U}_0, \end{array}$$

and thus

$$\Delta \vdash \overline{\texttt{V}} \texttt{ <: } [\overline{\texttt{V}}/\overline{\texttt{Y}}][\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{Q}}.$$

Moreover, by the rule WF-CLASS, we have

$$\Delta \vdash \overline{\texttt{T}} \texttt{ <: } [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{N}} \quad (= [\overline{\texttt{V}}/\overline{\texttt{Y}}][\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{N}}).$$

By Lemma 4.5.2, $|[\overline{\texttt{V}}/\overline{\texttt{Y}}][\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{W}}|_\Delta \texttt{ <: } \overline{\texttt{C}}$ and $|[\overline{\texttt{V}}/\overline{\texttt{Y}}][\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{W}_0|_\Delta \texttt{ <: } \texttt{C}_0$, finishing the case.

Case: $n = k + 1$

Suppose

$$CT(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{ ...\}.}$$

Now, we have three subcases:

Subcase: $mtype_{\text{FGJ}}(\texttt{m}, [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N})$ is not well defined.

The method `m` must be declared in `C`. Similarly for the base case above.

Subcase: $mtype_{\text{FGJ}}(\texttt{m}, [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N})$ is well defined and `m` is defined in `C`.

By the rule GT-METHOD, it must be the case that

$$mtype_{\text{FGJ}}(\texttt{m}, [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N}) = \texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{P}}\texttt{>}\overline{\texttt{U}} \rightarrow \texttt{U}_0{}'$$

where $\Delta, \overline{\texttt{Y}}\texttt{<:}\overline{\texttt{P}} \vdash \texttt{U}_0 \texttt{ <: } \texttt{U}_0{}'$. By Lemmas 3.4.4 and 4.5.1, $|[\overline{\texttt{V}}/\overline{\texttt{Y}}]\texttt{U}_0|_\Delta \texttt{ <: } |[\overline{\texttt{V}}/\overline{\texttt{Y}}]\texttt{U}_0{}'|_\Delta$. Induction hypothesis and transitivity of <: finish the subcase.

Subcase: $mtype_{\text{FGJ}}(\texttt{m}, [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N})$ is well defined and `m` is not defined in `C`.

It is easy because $mtype_{\text{FGJ}}(\texttt{m}, [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N}) = mtype_{\text{FGJ}}(\texttt{m}, \texttt{C<}\overline{\texttt{T}}\texttt{>})$, by the rule MT-SUPER. Induction hypothesis finishes the subcase. ∎

4.5.5 Lemma: If $\Delta \vdash \texttt{S <: T}$ and $\Delta \vdash \texttt{S}$ ok for some well-formed type environment Δ, then $\Delta \vdash \texttt{T}$ ok.

Proof: By induction on the derivation of $\Delta \vdash \texttt{S <: T}$ with a case analysis on the last rule used. The cases for S-REFL and S-TRANS are easy.

Case S-VAR: $\texttt{S} = \texttt{X} \qquad \texttt{T} = \Delta(\texttt{X})$

`T` must be well formed since Δ is well formed.

Case S-CLASS: $\begin{array}{lll} \texttt{S} = \texttt{C<}\overline{\texttt{T}}\texttt{>} & \texttt{T} = [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N} & CT(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{...\}} \\ \Delta \vdash \overline{\texttt{T}} \text{ ok} & \Delta \vdash \overline{\texttt{T}} \texttt{ <: } [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{N}} & \end{array}$

Since $CT(\texttt{C})$ is ok, we also have $\overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}} \vdash \texttt{N}$ ok by the rule GT-CLASS. Then, by Lemma 3.4.1, and Lemma 3.4.5, $\Delta \vdash [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{N}$ ok. ∎

4.5.6 Lemma: If $\Delta \vdash \texttt{N}$ ok for some well-formed type environment Δ and $fields_{\text{FGJ}}(\texttt{N}) = \overline{\texttt{U}}\ \overline{\texttt{f}}$, then $\Delta \vdash \overline{\texttt{U}}$ ok.

Proof: By induction on the derivation of $fields_{\text{FGJ}}(\texttt{N})$ with a case analysis on the last rule used. The case for F-OBJECT is trivial.

Case F-Class: $\quad$ $\texttt{N} = \texttt{C<}\overline{\texttt{T}}\texttt{>}$ $\quad$ $CT(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{P \{}\overline{\texttt{S}}\ \overline{\texttt{f}}\texttt{; K }\overline{\texttt{M}}\texttt{\}}$

$\quad$ $\mathit{fields}_{\text{FGJ}}([\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{P}) = \overline{\texttt{U}}\ \overline{\texttt{g}}$

By induction hypothesis, $\Delta \vdash \overline{\texttt{U}}$ ok. Since $\Delta \vdash \texttt{C<}\overline{\texttt{T}}\texttt{>}$ ok, we have $\Delta \vdash \overline{\texttt{T}}$ ok and $\Delta \vdash \overline{\texttt{T}}$ <: $[\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{N}}$ by the rule WF-Class. On the other hand, by the rule GT-Class, we have $\overline{\texttt{X}}$<:$\overline{\texttt{N}} \vdash \overline{\texttt{S}}$ ok. Finally, by Lemma 3.4.1 and 3.4.4, $\Delta \vdash [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{S}}$ ok finishes the case. ∎

4.5.7 Lemma: If $\Delta \vdash \texttt{N}$ ok for some well-formed type environment Δ and $\mathit{mtype}_{\text{FGJ}}(\texttt{m}, \texttt{N}) = \texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{P}}\texttt{>}\overline{\texttt{U}}\to\texttt{U}_0$, then $\Delta, \overline{\texttt{Y}}$<:$\overline{\texttt{P}} \vdash \texttt{U}_0$ ok.

Proof: By induction on the derivation of $\mathit{mtype}_{\text{FGJ}}(\texttt{m}, \texttt{N})$ with a case analysis on the last rule used.

Case MT-Class: $\quad$ $\texttt{N} = \texttt{C<}\overline{\texttt{T}}\texttt{>}$

$\quad$ $CT(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{P \{...}\ \ \overline{\texttt{M}}\texttt{\}}$

$\quad$ $\texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{Q}}\texttt{> S}_0\texttt{ m (}\overline{\texttt{S}}\ \overline{\texttt{x}}\texttt{) \{}\uparrow\texttt{e}_0\texttt{;\}} \in \overline{\texttt{M}}$

$\quad$ $[\overline{\texttt{T}}/\overline{\texttt{X}}](\texttt{<Y} \triangleleft \overline{\texttt{Q}}\texttt{>}\overline{\texttt{S}}\to\texttt{S}_0) = \texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{P}}\texttt{>}\overline{\texttt{U}}\to\texttt{U}_0$

By the rule GT-Method, we have

$$\overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}},\ \overline{\texttt{Y}}\texttt{<:}\overline{\texttt{Q}} \vdash \texttt{S}_0 \text{ ok.}$$

By the rule WF-Class, we have $\Delta \vdash \overline{\texttt{T}}$ ok and $\Delta \vdash \overline{\texttt{T}}$ <: $[\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{N}}$. By Lemma 3.4.1 and 3.4.5,

$$\Delta,\ \overline{\texttt{Y}}\texttt{<:}[\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{Q}} \vdash [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{S}_0 \text{ ok.}$$

By assumption, $[\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{Q}} = \overline{\texttt{P}}$ and $[\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{S}_0 = \texttt{U}_0$, finishing the case.

Case MT-Super:

Easy. Note that we have, by the rule S-Class, $\Delta \vdash \texttt{C<}\overline{\texttt{T}}\texttt{>}$ <: $[\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{P}$ and, by Lemma 4.5.5, $\Delta \vdash [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{P}$ ok. ∎

4.5.8 Lemma: If $\Delta \vdash \Gamma$ ok and $\Delta; \Gamma \vdash \texttt{e} \in \texttt{T}$ for some well-formed type environment Δ, then $\Delta \vdash \texttt{T}$ ok.

Proof: By induction on the derivation of $\Delta; \Gamma \vdash \texttt{e} \in \texttt{T}$ with a case analysis on the last rule used.

Case GT-Var:

Easy since $\Delta \vdash \Gamma(\texttt{x})$ for all $\texttt{x} \in \mathit{dom}(\Gamma)$.

Case GT-Field: $\quad$ $\Delta; \Gamma \vdash \texttt{e}_0 \in \texttt{T}_0$ $\quad$ $\mathit{fields}_{\text{FGJ}}(\mathit{bound}_\Delta(\texttt{T}_0)) = \overline{\texttt{T}}\ \overline{\texttt{f}}$

By induction hypothesis, $\Delta \vdash \texttt{T}_0$ ok. Since Δ is well formed, $\Delta \vdash \mathit{bound}_\Delta(\texttt{T}_0)$ ok. Then, by Lemma 4.5.6, we have $\Delta \vdash \overline{\texttt{T}}$ ok, finishing the case.

Case GT-Invk: $\quad$ $\Delta; \Gamma \vdash \texttt{e}_0 \in \texttt{T}_0$ $\quad$ $\mathit{mtype}_{\text{FGJ}}(\texttt{m}, \mathit{bound}_\Delta(\texttt{T}_0)) = \texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{P}}\texttt{>}\overline{\texttt{U}}\to\texttt{U}_0$

$\quad$ $\Delta \vdash \overline{\texttt{V}}$ ok $\quad$ $\Delta \vdash \overline{\texttt{V}}$ <: $[\overline{\texttt{V}}/\overline{\texttt{Y}}]\overline{\texttt{P}}$

$\quad$ $\Delta; \Gamma \vdash \overline{\texttt{e}} \in \overline{\texttt{S}}$ $\quad$ $\Delta \vdash \overline{\texttt{S}}$ <: $[\overline{\texttt{V}}/\overline{\texttt{Y}}]\overline{\texttt{U}}$

$\quad$ $\texttt{T} = [\overline{\texttt{V}}/\overline{\texttt{Y}}]\texttt{U}_0$

By induction hypothesis, $\Delta \vdash \texttt{T}_0$ ok. Since Δ is well formed, $\Delta \vdash \mathit{bound}_\Delta(\texttt{T}_0)$ ok. Then, by Lemma 4.5.7, $\Delta, \overline{\texttt{Y}}$<:$\overline{\texttt{P}} \vdash \texttt{U}_0$ ok. Finally, by Lemma 3.4.5, we have $\Delta \vdash [\overline{\texttt{V}}/\overline{\texttt{Y}}]\texttt{U}_0$ ok finishing the case.

Case GT-UCast: $\quad$ $\Delta; \Gamma \vdash \texttt{e}_0 \in \texttt{T}_0$ $\quad$ $\Delta \vdash \texttt{T}_0$ <: $\texttt{N}$

By induction hypothesis, $\Delta \vdash \texttt{T}_0$ ok. By Lemma 4.5.5, $\Delta \vdash \texttt{N}$ ok finishes the case.

Case GT-New, GT-DCast, GT-SCast:

Trivial since $\texttt{T}$ is well formed by assumption. ∎

4.5.9 Theorem [Erasure preserves typing]: If an FGJ class table CT is ok and $\Delta; \Gamma \vdash \texttt{e} \in \texttt{T}$, then $|CT|$ is ok using FJ rules and $|\Gamma|_\Delta \vdash |\texttt{e}|_{\Delta,\Gamma} \in |\texttt{T}|_\Delta$.

Proof: We prove the theorem in three steps: first, we show $|CT|$ is well defined; second, it is shown that, if $\Delta; \Gamma \vdash \texttt{e} \in \texttt{T}$, then $|\Gamma|_\Delta \vdash |\texttt{e}|_{\Delta,\Gamma} \in |\texttt{T}|_\Delta$; and third, we show $|CT|$ is ok.

The first part is easy because every method body is well typed and every type is well formed under appropriate (type) environments. Now, by definition of erasure, it is obvious that $\mathit{fields}_{\text{FJ}}(\texttt{C}) = \mathit{fieldsmax}(\texttt{C})$ and $\mathit{mtype}_{\text{FJ}}(\texttt{m}, \texttt{C}) = \mathit{mtypemax}(\texttt{m}, \texttt{C})$ for all $\texttt{m}$ and $\texttt{C}$.

The second part is proved by induction on the derivation of $\Delta; \Gamma \vdash \texttt{e} \in \texttt{T}$ with a case analysis on the last rule used.

Case GT-FIELD: $\quad \mathtt{e} = \mathtt{e}_0\mathtt{.f}_i \qquad \Delta;\Gamma \vdash \mathtt{e}_0 \in \mathtt{T}_0 \qquad \mathit{fields}_{\mathrm{FGJ}}(\mathit{bound}_\Delta(\mathtt{T}_0)) = \overline{\mathtt{T}}\ \overline{\mathtt{f}} \qquad \mathtt{T} = \mathtt{T}_i$

By induction hypothesis, we have $|\Gamma|_\Delta \vdash |\mathtt{e}_0|_\Delta \in |\mathtt{T}_0|_\Delta$. By Lemma 4.5.8, $\Delta \vdash \mathtt{T}_0$ ok. Then, whether $\mathtt{T}_0$ is a type variable or not, we have, by Lemma 4.5.3, $\mathit{fieldsmax}(|\mathtt{T}_0|_\Delta) = \overline{\mathtt{C}}\ \overline{\mathtt{f}}$ and $|\overline{\mathtt{T}}|_\Delta$ <: $\overline{\mathtt{C}}$. By the rule T-FIELD, we have $|\Gamma|_\Delta \vdash |\mathtt{e}_0|_{\Delta,\Gamma}\mathtt{.f}_i \in \mathtt{C}_i$.

If $|\mathtt{T}_i|_\Delta = \mathtt{C}_i$, then the equation $|\mathtt{e}_0\mathtt{.f}_i|_{\Delta,\Gamma} = |\mathtt{e}_0|_{\Delta,\Gamma}\mathtt{.f}_i$ derived from the rule E-FIELD finishes the case. On the other hand, if ($|\mathtt{T}_i|_\Delta \neq \mathtt{C}_i$), then

$$|\mathtt{e}_0\mathtt{.f}_i|_{\Delta,\Gamma} = \mathtt{(}|\mathtt{T}_i|_\Delta\mathtt{)}|\mathtt{e}_0|_{\Delta,\Gamma}\mathtt{.f}_i$$

by the rule E-FIELD-CAST and $|\Gamma|_\Delta \vdash \mathtt{(}|\mathtt{T}|_\Delta\mathtt{)}|\mathtt{e}_0|_{\Delta,\Gamma}\mathtt{.f}_i \in |\mathtt{T}|_\Delta$ by the rule T-DCAST.

Case GT-INVK:

Similar to the case above. We use Lemma 4.5.4 instead of Lemma 4.5.3.

Case GT-NEW, GT-UCAST, GT-DCAST, GT-SCAST:

Easy.

The third part ($|CT|$ is ok) follows from the first part with examination of the rules GT-METHOD and GT-CLASS. We show that, if `M OK IN C<X̄◁N̄>` and $|\mathtt{M}|_{\overline{\mathtt{X}}\texttt{<:}\overline{\mathtt{N}},\ \mathtt{C}} = \mathtt{M}'$, then $\mathtt{M}'$ `OK IN C`. Suppose

$$\begin{aligned}
&\mathtt{M} = \mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\mathtt{>}\ \mathtt{T}\ \mathtt{m}\ \mathtt{(}\overline{\mathtt{T}}\ \mathtt{x)}\ \mathtt{\{\uparrow e;\}}\\
&\mathtt{M}' = \mathtt{D}\ \mathtt{m}\ \mathtt{(}\overline{\mathtt{D}}\ \mathtt{x}'\mathtt{)}\ \mathtt{\{\uparrow e';\}}\\
&\mathit{mtypemax}(\mathtt{m},\mathtt{C}) = \overline{\mathtt{D}}{\to}\mathtt{D}\\
&\Gamma = \overline{\mathtt{x}} : \overline{\mathtt{T}}, \mathtt{this} : \mathtt{C<}\overline{\mathtt{X}}\mathtt{>}\\
&\Delta = \overline{\mathtt{X}}\texttt{<:}\overline{\mathtt{N}}, \overline{\mathtt{Y}}\texttt{<:}\overline{\mathtt{P}}\\
&\mathtt{e}' = [\mathtt{(}|\overline{\mathtt{T}}|_\Delta\mathtt{)x}'/\overline{\mathtt{x}}]|\mathtt{e}|_{\Delta,\,\Gamma}.
\end{aligned}$$

By the rule GT-METHOD, we have

$$\begin{aligned}
&\Delta \vdash \overline{\mathtt{T}}, \mathtt{T}, \overline{\mathtt{P}}\ \text{ok}\\
&\Delta;\Gamma, \mathtt{this} : \mathtt{C<}\overline{\mathtt{X}}\mathtt{>} \vdash \mathtt{e} \in \mathtt{S}\\
&\Delta \vdash \mathtt{S}\ \texttt{<:}\ \mathtt{T}\\
&\text{if } \mathit{mtype}_{\mathrm{FGJ}}(\mathtt{m},\mathtt{N}) = \mathtt{<}\overline{\mathtt{Z}} \triangleleft \overline{\mathtt{Q}}\mathtt{>}\overline{\mathtt{U}}{\to}\mathtt{U}\text{, then } \overline{\mathtt{P}}, \overline{\mathtt{T}} = [\overline{\mathtt{Y}}/\overline{\mathtt{Z}}](\overline{\mathtt{Q}}, \overline{\mathtt{U}}) \text{ and } \Delta \vdash \mathtt{T}\ \texttt{<:}\ [\overline{\mathtt{Y}}/\overline{\mathtt{Z}}]\mathtt{U}
\end{aligned}$$

where $CT(\mathtt{C}) = \mathtt{class\ C<}\overline{\mathtt{X}} \triangleleft \overline{\mathtt{N}}\mathtt{>} \triangleleft \mathtt{N}\ \mathtt{\{...\}}$. We must show that

$$\begin{aligned}
&\overline{\mathtt{x}}' : \mathtt{D}, \mathtt{this} : \mathtt{C} \vdash \mathtt{e}' \in \mathtt{E}\\
&\mathtt{E}\ \texttt{<:}\ \mathtt{D}\\
&\text{if } \mathit{mtype}_{\mathrm{FJ}}(\mathtt{m}, |\mathtt{N}|_\Delta) = \overline{\mathtt{E}}{\to}\mathtt{D}'\text{, then } \overline{\mathtt{E}} = \overline{\mathtt{D}} \text{ and } \mathtt{D}' = \mathtt{D}.
\end{aligned}$$

for some $\mathtt{E}$.

By the result of the second part, $|\Gamma|_\Delta, \mathtt{this} : \mathtt{C} \vdash |\mathtt{e}|_{\Delta,\Gamma} \in |\mathtt{S}|_\Delta$. Since, by Lemma 4.5.4, $|\mathtt{T}_i|_\Delta$ <: $\mathtt{D}_i$, we have $\mathtt{x}_i{}' : \mathtt{D}_i \vdash \mathtt{(}|\mathtt{T}_i|_\Delta\mathtt{)x}' \in |\mathtt{T}_i|_\Delta$. By Lemma 3.4.12,

$$\overline{\mathtt{x}}' : \overline{\mathtt{D}}, \mathtt{this} : \mathtt{C} \vdash \mathtt{e}' \in |\mathtt{S}|_\Delta.$$

On the other hand, by Lemma 4.5.4, $|\mathtt{T}|_\Delta$ <: $\mathtt{D}$. Since we have $|\mathtt{S}|_\Delta$ <: $|\mathtt{T}|_\Delta$ by Lemma 4.5.1, $|\mathtt{S}|_\Delta$ <: $\mathtt{D}$ by transitivity of <:.

Suppose $\mathit{mtypemax}(\mathtt{m}, |\mathtt{N}|_\Delta)$ is well defined. Then, $\mathit{mtype}_{\mathrm{FGJ}}(\mathtt{m}, \mathtt{N})$ is also well defined. By the definition of *mtypemax*, $\mathit{mtypemax}(\mathtt{m}, |\mathtt{N}|_\Delta) = \overline{\mathtt{D}}{\to}\mathtt{D}$. ∎

Preservation of Execution

More interestingly, we would intuitively expect that erasure from FGJ to FJ should also preserve the reduction behavior of FGJ programs:

$$\begin{tikzcd}
\mathtt{e} \arrow[r, "\text{reduce (FGJ)}"] \arrow[d, "\text{erase}"'] & \mathtt{e}' \arrow[d, dotted, "\text{erase}"] \\
|\mathtt{e}| \arrow[r, dotted, "\text{reduce (FJ)}"'] & |\mathtt{e}'|
\end{tikzcd}$$

Unfortunately, this is not quite true. For example, consider the FGJ expression

$$\texttt{e} = \texttt{new Pair<A,B>(a,b).fst},$$

where `a` and `b` are expressions of type `A` and `B`, respectively, and its erasure:

$$|\texttt{e}|_{\Delta,\Gamma} = \texttt{(A)new Pair(}|\texttt{a}|_{\Delta,\Gamma}\texttt{,}|\texttt{b}|_{\Delta,\Gamma}\texttt{).fst}$$

In FGJ, `e` reduces to `a`, while the erasure $|\texttt{e}|_{\Delta,\Gamma}$ reduces to $\texttt{(A)}|\texttt{a}|_{\Delta,\Gamma}$ in FJ; it does not reduce to $|\texttt{a}|_{\Delta,\Gamma}$ when `a` is not a `new` expression. (Note that it is not an artifact of our nondeterministic reduction strategy: it happens even if we adopt a call-by-value reduction strategy, since, after method invocation, we may obtain an expression like `(A)e` where `e` is not a `new` expression.) Thus, the above diagram does not commute even if one-step reduction ($\longrightarrow$) at the bottom is replaced with many-step reduction ($\longrightarrow^*$). In general, synthetic casts can persist for a while in the FJ expression, although we expect those casts will eventually turn out to be upcasts when `a` reduces to a `new` expression.

In the example above, an FJ expression `d` reduced from $|\texttt{e}|_{\Delta,\Gamma}$ had *more* synthetic casts than $|\texttt{e}'|_{\Delta,\Gamma}$. However, this is not always the case: `d` may have *less* casts than $|\texttt{e}'|_{\Delta,\Gamma}$ when the reduction step involves method invocation. Consider the following class (on the left) and its erasure (on the right):

```
class C<X extends Object> extends Object {
  X f;
  C(X f) { this.f = f; }
  C<X> m () { return new C<X>(this.f); }
}
```

```
class C extends Object {
  Object f;
  C (Object f) { this.f = f; }
  C m () { return new C(this.f); }
}
```

Now consider the FGJ expression

$$\texttt{e} = \texttt{new C<A>(new A()).m()}$$

and its erasure

$$|\texttt{e}|_{\Delta,\Gamma} = \texttt{new C(new A()).m()}.$$

In FGJ,

$$\texttt{e} \longrightarrow_{\text{FGJ}} \texttt{new C<A>(new C<A>(new A()).f)}.$$

In FJ, on the other hand, $|\texttt{e}|_{\Delta,\Gamma}$ reduces to `new C(new C(new A()).f)`, which has fewer synthetic casts than `new C((A)new C(new A()).f)`, which is the erasure of the reduced expression in FGJ. The subtlety we observe here is that, when the erased term is reduced, synthetic casts may become "coarser" than the casts inserted when the reduced term is erased, or may be removed entirely as in this example. (Removal of downcasts can be considered as a combination of two operations: replacement of `(A)` with the coarser cast `(Object)` and removal of the upcast `(Object)`, which does not affect the result of computation.)

To formalize both of these observations, we define an auxiliary relation that relates FJ expressions differing only by the addition and replacement of some synthetic casts. In the following discussion, we distinguish synthetic casts from typecasts derived from original FGJ programs by subscripting typecast expression: we write $\texttt{(C)}_S$ for synthetic casts. Except its notation, they behaves exactly the same as ordinary typecasts. Also, we assume typecasts inserted by the rules E-FIELD-CAST and E-INVK-CAST are synthetic and the other casts are not. Let us call a well-typed expression `d` an *expansion* of a well-typed expression `e`, written $\texttt{e} \overset{\text{exp}}{\Longrightarrow} \texttt{d}$, if `d` is obtained from `e` by some combination of (1) addition of zero or more synthetic upcasts, (2) replacement of some synthetic casts `(D)` with `(C)`, where `C` is a supertype of `D`, or (3) removal of some synthetic casts.

4.5.10 Lemma: Suppose $dom(\Gamma) = dom(\Gamma')$ and $\Delta = \Delta_1, \overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}}, \Delta_2$ where none of $\overline{\texttt{X}}$ appears in Δ_1. If $\Delta;\Gamma \vdash \texttt{e} \in \texttt{T}$ and $\Delta_1 \vdash \overline{\texttt{U}} \texttt{ <: } [\overline{\texttt{U}}/\overline{\texttt{X}}]\overline{\texttt{N}}$ where $\Delta_1 \vdash \overline{\texttt{U}}$ ok, and $\Delta_1, [\overline{\texttt{U}}/\overline{\texttt{X}}]\Delta_2 \vdash \Gamma'(\texttt{x}) \texttt{ <: } [\overline{\texttt{U}}/\overline{\texttt{X}}]\Gamma(\texttt{x})$ for all $\texttt{x} \in dom(\Gamma)$, then $|[\overline{\texttt{U}}/\overline{\texttt{X}}]\texttt{e}|_{\Delta_1,\,[\overline{\texttt{U}}/\overline{\texttt{X}}]\Delta_2,\Gamma'} \overset{\text{exp}}{\Longrightarrow} |\texttt{e}|_{\Delta,\Gamma}$.

Proof: By induction on the derivation of $\Delta;\Gamma \vdash \texttt{e} \in \texttt{T}$ with a case analysis on the last rule used.

Case GT-VAR**:**
Trivial.
Case GT-FIELD**:** $\quad \mathtt{e} = \mathtt{e}_0\mathtt{.f} \quad \Delta;\Gamma \vdash \mathtt{e}_0 \in \mathtt{T}_0 \quad \mathit{fields}_{\mathrm{FGJ}}(\mathit{bound}_\Delta(\mathtt{T}_0)) = \overline{\mathtt{T}}\ \overline{\mathtt{f}} \quad \mathtt{T} = \mathtt{T}_i$
By induction hypothesis, $|[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}_0|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2,\,\Gamma'} \stackrel{\mathrm{exp}}{\Longrightarrow} |\mathtt{e}_0|_{\Delta,\Gamma}$. By Lemmas 3.4.11 and 3.4.12,

$$\begin{array}{l}\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2;\Gamma' \vdash \mathtt{e}_0 \in \mathtt{S}_0\\ \Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \mathtt{S}_0 \mathrel{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_0\end{array}$$

By straightforward induction on the derivation of $\mathit{fieldsmax}(|\mathtt{T}_0|_\Delta)$, it is shown that $\mathit{fieldsmax}(|\mathtt{S}_0|_\Delta) = \mathit{fieldsmax}(|\mathtt{T}_0|_\Delta), \overline{\mathtt{D}}\ \overline{\mathtt{g}}$ for some $\overline{\mathtt{D}}\ \overline{\mathtt{g}}$. On the other hand, by Lemmas 3.4.7 and 3.4.8, $\mathit{fields}_{\mathrm{FGJ}}(\mathit{bound}_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}(\mathtt{S}_0)) = \overline{\mathtt{T}}'\ \overline{\mathtt{g}}$ and for any $i \leq \#(\overline{\mathtt{f}})$, we have $\mathtt{f}_i = \mathtt{g}_i$ and $\mathtt{T}_i{}' = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_i$. Then, by Lemma 4.5.2,

$$|\mathtt{T}_i{}'|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2} \mathrel{<:} |\mathtt{T}_i|_\Delta.$$

If the rule E-FIELD is applied for $\mathtt{e}$, we have $|[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}|_{\Delta,\,\Gamma'} \stackrel{\mathrm{exp}}{\Longrightarrow} |\mathtt{e}|_{\Delta,\Gamma}$ whether the rule for $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}$ is E-INVK or E-INVK-CAST. On the other hand, if the rule E-FIELD-CAST is applied for $\mathtt{e}$, the same rule must be applied for $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}$; synthetic casts for $\mathtt{e}$ and $\mathtt{e}'$ are $(|\mathtt{T}_i|_\Delta)_S$ and $(|\mathtt{T}_i{}'|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2})_S$. Thus, whether it is E-FIELD or E-FIELD-CAST, the same erasure rule applies and $|[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2,\,\Gamma'} \stackrel{\mathrm{exp}}{\Longrightarrow} |\mathtt{e}|_{\Delta,\Gamma}$.
Case GT-METHOD**:**

$$\begin{array}{lll}\mathtt{e} = \mathtt{e}_0\mathtt{.m<}\overline{\mathtt{V}}\mathtt{>(}\overline{\mathtt{d}}\mathtt{)} & \Delta;\Gamma \vdash \mathtt{e}_0 \in \mathtt{T}_0 & \mathit{mtype}_{\mathrm{FGJ}}(\mathtt{m},\,\mathit{bound}_\Delta(\mathtt{T}_0)) = \mathtt{<}\overline{\mathtt{Y}} \triangleleft \overline{\mathtt{P}}\mathtt{>}\overline{\mathtt{U}}\to\mathtt{U}_0\\ \Delta \vdash \overline{\mathtt{V}}\ \mathrm{ok} & \Delta \vdash \overline{\mathtt{V}} \mathrel{<:} [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}} & \\ \Delta;\Gamma \vdash \overline{\mathtt{d}} \in \overline{\mathtt{S}} & \Delta \vdash \overline{\mathtt{S}} \mathrel{<:} [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{U}} & \\ \mathtt{T} = [\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}_0 & & \end{array}$$

By induction hypothesis,

$$\begin{array}{l}|[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{d}}|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2,\,\Gamma'} \stackrel{\mathrm{exp}}{\Longrightarrow} |\overline{\mathtt{d}}|_{\Delta,\Gamma}\\ |[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}_0|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2,\,\Gamma'} \stackrel{\mathrm{exp}}{\Longrightarrow} |\mathtt{e}_0|_{\Delta,\Gamma}\end{array}$$

By Lemmas 3.4.11 and 3.4.12,

$$\begin{array}{l}\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2;\Gamma' \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}_0 \in \mathtt{S}_0\\ \Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash \mathtt{S}_0 \mathrel{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_0.\end{array}$$

By Lemmas 3.4.9 and 3.4.10, we have

$$\begin{array}{l}\mathit{mtype}_{\mathrm{FGJ}}(\mathtt{m},\,\mathit{bound}_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}(\mathtt{S}_0)) = \mathtt{<}\overline{\mathtt{Y}} \triangleleft [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{P}}\mathtt{>}[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{U}}\to\mathtt{U}_0{}'\\ \Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2,\,\overline{\mathtt{Y}}\mathrel{<:}[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{P}} \vdash \mathtt{U}_0{}' \mathrel{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{U}_0.\end{array}$$

By Lemma 3.4.4,

$$\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}} \mathrel{<:} [\overline{\mathtt{U}}/\overline{\mathtt{X}}][\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\overline{\mathtt{P}} \quad (= [[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}]([\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{P}}))$$

and by the same lemma,

$$\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2 \vdash [[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}_0{}' \mathrel{<:} [[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}][\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{U}_0 \quad (= [\overline{\mathtt{U}}/\overline{\mathtt{X}}][\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}_0 = [\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}),$$

and, by Lemma 4.5.1,

$$|[[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}_0{}'|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2} \mathrel{<:} |[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}.$$

Moreover, by Lemma 4.5.2,

$$|[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2} \mathrel{<:} |\mathtt{T}|_\Delta,$$

and, by transitivity of $\mathrel{<:}$,

$$|[[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}_0{}'|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2} \mathrel{<:} |\mathtt{T}|_\Delta.$$

On the other hand, it is easily shown, by induction, that

$$\mathit{mtypemax}(\mathtt{m},\,|\mathtt{S}_0|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}) = \mathit{mtypemax}(\mathtt{m},\,|[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{T}_0|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2}) = \mathit{mtypemax}(\mathtt{m},\,|\mathtt{T}_0|_\Delta).$$

If the rule E-INVK is applied for $\mathtt{e}$, we have $|[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2,\,\Gamma'} \stackrel{\mathrm{exp}}{\Longrightarrow} |\mathtt{e}|_{\Delta,\Gamma}$ whether the rule for $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}$ is E-INVK or E-INVK-CAST. On the other hand, if the rule E-INVK-CAST is applied for $\mathtt{e}$, the same rule must be applied for $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}$; synthetic casts for $\mathtt{e}$ and $[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}$ are $(|\mathtt{T}|_\Delta)_S$ and $(|[[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\overline{\mathtt{V}}/\overline{\mathtt{Y}}]\mathtt{U}_0{}'|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2})_S$, respectively. Therefore, $|[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\mathtt{e}|_{\Delta_1,\,[\overline{\mathtt{U}}/\overline{\mathtt{X}}]\Delta_2,\,\Gamma'} \stackrel{\mathrm{exp}}{\Longrightarrow} |\mathtt{e}|_{\Delta,\Gamma}$.

Case E-New, E-Cast:
Easy. ∎

4.5.11 Lemma: Suppose

1. $\mathit{mbody}_{\mathrm{FGJ}}(\texttt{m<}\overline{\texttt{V}}\texttt{>}, \texttt{C<}\overline{\texttt{T}}\texttt{>}) = (\overline{\texttt{x}}, \texttt{e})$,
2. $\mathit{mtype}_{\mathrm{FGJ}}(\texttt{m}, \texttt{C<}\overline{\texttt{T}}\texttt{>}) = \texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{P}}\texttt{>}\overline{\texttt{U}}\texttt{→U}$,
3. $\Delta \vdash \texttt{C<}\overline{\texttt{T}}\texttt{>}$ ok, and
4. $\Delta \vdash \overline{\texttt{V}} \texttt{ <: } [\overline{\texttt{V}}/\overline{\texttt{Y}}]\overline{\texttt{P}}$.

Then, $\mathit{mbody}_{\mathrm{FJ}}(\texttt{m}, \texttt{C}) = (\overline{\texttt{x}}, \texttt{e}')$ with respect to $|CT|$, and $|\texttt{e}|_{\Delta,\, \overline{\texttt{x}}:[\overline{\texttt{V}}/\overline{\texttt{Y}}]\overline{\texttt{U}},\texttt{this:C<}\overline{\texttt{T}}\texttt{>}} \stackrel{\mathrm{exR}}{\Longrightarrow} \texttt{e}'$.

Proof: By induction on the derivation of $\mathit{mbody}_{\mathrm{FGJ}}(\texttt{m<}\overline{\texttt{V}}\texttt{>}, \texttt{C<}\overline{\texttt{T}}\texttt{>})$ with a case analysis on the last rule used.

Case MB-Class: $\quad CT(\texttt{C}) = \texttt{class C<}\overline{\texttt{X}} \triangleleft \overline{\texttt{N}}\texttt{>} \triangleleft \texttt{N \{ ...}$
$\qquad\qquad \texttt{<}\overline{\texttt{Y}} \triangleleft \overline{\texttt{Q}}\texttt{> S m (}\overline{\texttt{S}}\texttt{ x) \{}\uparrow\texttt{e}_0\texttt{;\}}$
$\qquad [\overline{\texttt{T}}/\overline{\texttt{X}}][\overline{\texttt{V}}/\overline{\texttt{Y}}]\texttt{e}_0 = \texttt{e}$
$\qquad [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{Q}} = \overline{\texttt{P}}$
$\qquad [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{S}} = \overline{\texttt{U}}$
$\qquad [\overline{\texttt{T}}/\overline{\texttt{X}}]\texttt{S} = \texttt{U}$

Let $\Delta' = \overline{\texttt{X}}\texttt{<:}\overline{\texttt{N}}, \overline{\texttt{Y}}\texttt{<:}\overline{\texttt{P}}$ and $\Gamma = \overline{\texttt{x}} : \overline{\texttt{S}}, \texttt{this} : \texttt{C<}\overline{\texttt{X}}\texttt{>}$. Then, $\mathit{mbody}_{\mathrm{FJ}}(\texttt{m}, \texttt{C}) = (\overline{\texttt{x}}, |\texttt{e}_0|_{\Delta',\Gamma})$. By WF-Class, $\Delta \vdash \overline{\texttt{T}} \texttt{ <: } [\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{N}} \quad (= [\overline{\texttt{V}}/\overline{\texttt{Y}}][\overline{\texttt{T}}/\overline{\texttt{X}}]\overline{\texttt{N}})$. Finally, by Lemma 4.5.10,

$$|\texttt{e}|_{\Delta,\, \overline{\texttt{x}}:[\overline{\texttt{V}}/\overline{\texttt{Y}}]\overline{\texttt{U}},\texttt{this:C<}\overline{\texttt{T}}\texttt{>}} \stackrel{\mathrm{exR}}{\Longrightarrow} |\texttt{e}_0|_{\Delta,\, \Delta',\, \texttt{x}:\overline{\texttt{S}},\texttt{this:C<}\overline{\texttt{X}}\texttt{>}} = \texttt{e}'.$$

Case MB-Super:
Follows from induction hypothesis and Lemma 4.5.10. ∎

4.5.12 Lemma: If $\Delta;\Gamma \vdash \texttt{e} \in \texttt{T}$ and $\texttt{e} \longrightarrow_{\mathrm{FGJ}} \texttt{e}'$, then there exists some FJ expression $\texttt{d}'$ such that $|\texttt{e}'|_{\Delta,\Gamma} \stackrel{\mathrm{exR}}{\Longrightarrow} \texttt{d}'$ and $|\texttt{e}|_{\Delta,\Gamma} \longrightarrow_{\mathrm{FJ}} \texttt{d}'$. In other words, the following diagram commutes.

$$\begin{tikzcd}
\texttt{e} \arrow[r, "\text{reduce (FGJ)}"] \arrow[dd, "\text{erase}"'] & \texttt{e}' \arrow[d, dotted, "\text{erase}"] \\
 & |\texttt{e}'| \arrow[d, dotted, Rightarrow] \\
|\texttt{e}| \arrow[r, dotted, "\text{reduce (FJ)}"'] & \texttt{d}'
\end{tikzcd}$$

Proof: By induction on the derivation of $\texttt{e} \longrightarrow_{\mathrm{FGJ}} \texttt{e}'$ with a case analysis on the last reduction rule used. We show the main base cases.

Case GR-Field: $\quad \texttt{e} = \texttt{new N(}\overline{\texttt{e}}\texttt{).f}_i \quad \texttt{e}' = \texttt{e}_i \quad \mathit{fields}_{\mathrm{FGJ}}(\texttt{N}) = \overline{\texttt{T}}\ \overline{\texttt{f}}$

We have two subcases depending on whether erasure inserts a synthetic cast for this field access.

Subcase E-Field-Cast: $\quad |\texttt{e}|_{\Delta,\Gamma} = \texttt{(D)}_S\texttt{(new C(}|\overline{\texttt{e}}|_{\Delta,\Gamma}\texttt{).f}_i\texttt{)}$

We have $|\texttt{N}|_\Delta = \texttt{C}$ by definition of erasure. Since $\mathit{fields}_{\mathrm{FJ}}(\texttt{C}) = \overline{\texttt{C}}\ \overline{\texttt{f}}$ for some $\overline{\texttt{C}}$, we have $|\texttt{e}|_{\Delta,\Gamma} \longrightarrow_{\mathrm{FJ}} \texttt{(D)}_S|\texttt{e}_i|_{\Delta,\Gamma}$. On the other hand, by Theorem 3.4.14, $\Delta;\Gamma \vdash \texttt{e}_i \in \texttt{T}_i$ such that $\Delta \vdash \texttt{T}_i \texttt{ <: T}$. By Theorem 4.5.9, $|\texttt{T}|_\Delta = \texttt{D}$ and $|\Gamma|_\Delta \vdash |\texttt{e}_i|_{\Delta,\Gamma} \in |\texttt{T}_i|_\Delta$. Since $|\texttt{T}_i|_\Delta \texttt{ <: D}$ by Lemma 4.5.1, $\texttt{(D)}_S|\texttt{e}_i|_{\Delta,\Gamma}$ is obtained by adding an upcast to $|\texttt{e}_i|_{\Delta,\Gamma}$.

Subcase: $\quad |\texttt{e}|_{\Delta,\Gamma} = \texttt{new C(}|\overline{\texttt{e}}|_{\Delta,\Gamma}\texttt{).f}_i$

Follows from induction hypothesis.

Case GR-INVK: $\quad \mathtt{e} = \mathtt{new\ C<\overline{T}>(\overline{e}).m<\overline{V}>(\overline{d})} \qquad \mathtt{e}' = [\overline{\mathtt{d}}/\overline{\mathtt{x}}, \mathtt{new\ N(\overline{e})/this}]\mathtt{e}_0$
$\qquad mbody_{\mathrm{FGJ}}(\mathtt{m<\overline{V}>}, \mathtt{N}) = (\overline{\mathtt{x}}, \mathtt{e}_0)$

We have two subcases depending on whether erasure inserts a synthetic cast for this method invocation.

Subcase E-INVK-CAST: $\quad |\mathtt{e}|_{\Delta,\Gamma} = \mathtt{(D)}_S\mathtt{(new\ C(}|\overline{\mathtt{e}}|_{\Delta,\Gamma}\mathtt{).m(}|\overline{\mathtt{d}}|_{\Delta,\Gamma}\mathtt{))}$

By Theorem 4.5.9, we have $|\mathtt{T}|_\Delta = \mathtt{D}$. Since

$$|\mathtt{e}'|_{\Delta,\Gamma} = [|\overline{\mathtt{d}}|_{\Delta,\Gamma}/\overline{\mathtt{x}},\ |\mathtt{new\ N(\overline{e})}|_{\Delta,\Gamma}/\mathtt{this}]|\mathtt{e}_0|_{\Delta,\Gamma'}$$

where $\Gamma' = \Gamma, \overline{\mathtt{x}} : \overline{\mathtt{T}}, \mathtt{this} : \mathtt{N}$ and $\overline{\mathtt{T}}$ are types of $\overline{\mathtt{d}}$, we have, by Theorems 3.4.14 and 4.5.9,

$$|\Gamma|_\Delta \vdash [|\overline{\mathtt{d}}|_{\Delta,\Gamma}/\overline{\mathtt{x}},\ |\mathtt{new\ N(\overline{e})}|_{\Delta,\Gamma}/\mathtt{this}]|\mathtt{e}_0|_{\Delta,\Gamma'} \in |\mathtt{T}'|_\Delta$$

for some $\mathtt{T}'$ such that $\Delta \vdash \mathtt{T}' \mathrel{<:} \mathtt{T}$. By Lemma 4.5.1, $|\mathtt{T}'|_\Delta \mathrel{<:} \mathtt{D}$. Thus,

$$\mathtt{(D)}_S[|\overline{\mathtt{d}}|_{\Delta,\Gamma}/\overline{\mathtt{x}},\ |\mathtt{new\ N(\overline{e})}|_{\Delta,\Gamma}/\mathtt{this}]|\mathtt{e}_0|_{\Delta,\Gamma'}$$

is an expansion of

$$[|\overline{\mathtt{d}}|_{\Delta,\Gamma}/\overline{\mathtt{x}},\ |\mathtt{new\ N(\overline{e})}|_{\Delta,\Gamma}/\mathtt{this}]|\mathtt{e}_0|_{\Delta,\Gamma'}.$$

Now, by Lemma 4.5.11,

$$|\mathtt{e}_0|_{\Delta,\Gamma'} \overset{\mathrm{exp}}{\Longrightarrow} \mathtt{e}'$$

where $mbody_{\mathrm{FJ}}(\mathtt{m}, \mathtt{C}) = (\overline{\mathtt{x}}, \mathtt{e}')$. Therefore,

$$[|\overline{\mathtt{d}}|_{\Delta,\Gamma}/\overline{\mathtt{x}},\ |\mathtt{new\ N(\overline{e})}|_{\Delta,\Gamma}/\mathtt{this}]|\mathtt{e}_0|_{\Delta,\Gamma'}. \overset{\mathrm{exp}}{\Longrightarrow} \mathtt{(D)}_S[|\overline{\mathtt{d}}|_{\Delta,\Gamma}/\overline{\mathtt{x}},\ |\mathtt{new\ N(\overline{e})}|_{\Delta,\Gamma}/\mathtt{this}]\mathtt{e}',$$

finishing the subcase. Note that $\mathtt{(new\ C(}|\overline{\mathtt{e}}|_{\Delta,\Gamma}\mathtt{).m(}|\overline{\mathtt{d}}|_{\Delta,\Gamma}\mathtt{))} \longrightarrow_{\mathrm{FJ}} [|\overline{\mathtt{d}}|_{\Delta,\Gamma}/\overline{\mathtt{x}},\ |\mathtt{new\ N(\overline{e})}|_{\Delta,\Gamma}/\mathtt{this}]\mathtt{e}'$.

Subcase E-FIELD:

Similarly for the case above.

Case GR-CAST:

Easy. ■

4.5.13 Lemma: If $\Gamma \vdash \mathtt{e} \in \mathtt{C}$ and $\mathtt{e} \longrightarrow_{\mathrm{FJ}} \mathtt{e}'$ and $\mathtt{e} \overset{\mathrm{exp}}{\Longrightarrow} \mathtt{d}$, then there exists some FJ expression $\mathtt{d}'$ such that $\mathtt{e}' \overset{\mathrm{exp}}{\Longrightarrow} \mathtt{d}'$ and $\mathtt{d} \longrightarrow_{\mathrm{FJ}}{}^* \mathtt{d}'$. In other words, the following diagram commutes.

$$\begin{tikzcd}
\mathtt{e} \arrow[r, "\text{reduce (FJ)}"] \arrow[d, Rightarrow] & \mathtt{e}' \arrow[d, Rightarrow, dotted] \\
\mathtt{d} \arrow[r, dotted, "*", "\text{reduce (FJ)}"'] & \mathtt{d}'
\end{tikzcd}$$

Proof: By induction on the derivation of $\mathtt{e} \longrightarrow_{\mathrm{FJ}} \mathtt{e}'$ with a case analysis on the last reduction rule used.

Case R-FIELD: $\quad \mathtt{e} = \mathtt{new\ C(\overline{e}).f}_i \qquad fields_{\mathrm{FJ}}(\mathtt{C}) = \overline{\mathtt{C}}\ \overline{\mathtt{f}} \qquad \mathtt{e}' = \mathtt{e}_i$

The expansion $\mathtt{d}$ must have a form of $\mathtt{(D}_1\mathtt{)}_S \cdots \mathtt{(D}_n\mathtt{)}_S\mathtt{(new\ C(\overline{d}).f}_i\mathtt{)}$ where $\overline{\mathtt{d}}$ are expansions of $\overline{\mathtt{e}}$ respectively and $\mathtt{C} \mathrel{<:} \mathtt{D}_i$ for $1 \le i \le n$ because each $\mathtt{D}_i$ was introduced as an upcast. Thus, $\mathtt{d} \longrightarrow_{\mathrm{FJ}}{}^* \mathtt{new\ C(\overline{d}).f}_i \longrightarrow_{\mathrm{FJ}} \mathtt{d}_i$ which is an expansion of $\mathtt{e}_i$.

The other base cases are similar and induction steps are straightforward. ■

4.5.14 Theorem [Erasure preserves reduction modulo expansion]: If $\Delta;\Gamma \vdash \mathtt{e} \in \mathtt{T}$ and $\mathtt{e} \longrightarrow_{\text{FGJ}}{}^{*}$ $\mathtt{e}'$, then there exists some FJ expression $\mathtt{d}'$ such that $|\mathtt{e}'|_{\Delta,\Gamma} \stackrel{\text{exp}}{\Longrightarrow} \mathtt{d}'$ and $|\mathtt{e}|_{\Delta,\Gamma} \longrightarrow_{\text{FJ}} \mathtt{d}'$. In other words, the following diagram commutes.

$$
\begin{tikzcd}
\mathtt{e} \arrow[r, "\text{reduce (FGJ)}^{*}"] \arrow[dd, "\text{erase}"'] & \mathtt{e}' \arrow[d, dotted, "\text{erase}"] \\
 & |\mathtt{e}'| \arrow[d, Rightarrow, dotted] \\
|\mathtt{e}| \arrow[r, dotted, "\text{reduce (FJ)}"', "*"] & \mathtt{d}'
\end{tikzcd}
$$

Proof: By induction on the length n of reduction sequence $\mathtt{e} \longrightarrow_{\text{FGJ}}{}^{*} \mathtt{e}'$.

Case: $n = 0$

Trivial since $\mathtt{e} = \mathtt{e}'$.

Case: $\mathtt{e} \longrightarrow_{\text{FGJ}} \mathtt{e}' \longrightarrow_{\text{FGJ}}{}^{*} \mathtt{e}''$

We have the following commuting diagram.

$$
\begin{tikzcd}
\mathtt{e} \arrow[r, "\text{reduce (FGJ)}"] \arrow[ddd, "\text{erase}"'] \arrow[dddr, phantom, "(1)"] & \mathtt{e}' \arrow[r, "\text{reduce (FGJ)}^{*}"] \arrow[dd, dotted, "\text{erase}"'] \arrow[ddr, phantom, "(2)"] & \mathtt{e}'' \arrow[d, dotted, "\text{erase}"] \\
 & & |\mathtt{e}''| \arrow[d, Rightarrow, dotted] \\
 & |\mathtt{e}'| \arrow[r, dotted, "\text{reduce (FJ)}^{*}"] \arrow[d, Rightarrow, dotted] \arrow[dr, phantom, "(3)"] & \mathtt{d}' \arrow[d, Rightarrow, dotted] \\
|\mathtt{e}| \arrow[r, dotted, "\text{reduce (FJ)}"'] & \mathtt{d} \arrow[r, dotted, "\text{reduce (FJ)}"', "*"] & \mathtt{d}''
\end{tikzcd}
$$

Commutation (1) is proved by Lemma 4.5.12, (2) by induction hypothesis and (3) by Lemma 4.5.13. Note that $\stackrel{\text{exp}}{\Longrightarrow}$ is transitive. ∎

As easy corollaries of this theorem, it can be shown that, if an FGJ expression e reduces to a "fully-evaluated expression," then the erasure of e reduces to exactly its erasure, and that if FGJ reduction gets stuck at a stupid cast, then FJ reduction also gets stuck because of the same typecast. We use the metavariable v for fully evaluated expressions, defined as follows:

$$\mathtt{v} ::= \mathtt{new\ N(}\overline{\mathtt{v}}\mathtt{)}.$$

4.5.15 Corollary [Erasure preserves execution results]: If $\Delta;\Gamma \vdash \mathtt{e} \in \mathtt{T}$ and $\mathtt{e} \longrightarrow_{\text{FGJ}}{}^{*} \mathtt{v}$, then $|\mathtt{e}|_{\Delta,\Gamma} \longrightarrow_{\text{FJ}}{}^{*}$ $|\mathtt{v}|_{\Delta,\Gamma}$.

Proof: By Theorem 4.5.14, we have an FJ expression d such that $|\mathtt{e}|_{\Delta,\Gamma} \longrightarrow_{\text{FJ}}{}^{*}\mathtt{d}$ and $|\mathtt{v}|_{\Delta,\Gamma} \stackrel{\text{exp}}{\Longrightarrow} \mathtt{d}$. Since $|\mathtt{v}|_{\Delta,\Gamma}$ does not include any typecasts, d is obtained only by adding some (synthetic) upcasts. Therefore, d reduces to $|\mathtt{v}|_{\Delta,\Gamma}$. ∎

4.5.16 Corollary [Erasure preserves typecast errors]: If $\Delta;\Gamma \vdash \mathtt{e} \in \mathtt{T}$ and $\mathtt{e} \longrightarrow_{\text{FGJ}}{}^{*} \mathtt{e}'$, where $\mathtt{e}'$ has a stuck subexpression $\mathtt{(C<}\overline{\mathtt{S}}\mathtt{>)new\ D<}\overline{\mathtt{T}}\mathtt{>(}\overline{\mathtt{e}}\mathtt{)}$, then $|\mathtt{e}|_{\Delta,\Gamma} \longrightarrow_{\text{FJ}}{}^{*} \mathtt{d}'$ such that $\mathtt{d}'$ has a stuck subexpression $\mathtt{(C)new\ D(}\overline{\mathtt{d}}\mathtt{)}$, where $\overline{\mathtt{d}}$ are expansions of the erasures of $\overline{\mathtt{e}}$, in the same position (modulo synthetic casts) as the erasure of $\mathtt{e}'$.

Proof: Similar to the proof of Corollary 4.5.15. ∎

5 Related Work

Core calculi for Java. There are several known proofs in the literature of type soundness for subsets of Java. In the earliest, Drossopoulou and Eisenbach [11] (using a technique later mechanically checked by Syme [21]) prove soundness for a fairly large subset of sequential Java. Like us, they use a small-step operational semantics, but they avoid the subtleties of "stupid casts" by omitting casting entirely. Nipkow and Oheimb [18] give a mechanically checked proof of soundness for a somewhat larger core language. Their language does include casts, but it is formulated using a "big-step" operational semantics, which sidesteps the stupid cast problem. Flatt, Krishnamurthi, and Felleisen [14, 15] use a small-step semantics and formalize a language with both assignment and casting. Their system is somewhat larger than ours (the syntax, typing, and operational semantics rules take perhaps three times the space), and the soundness proof, though correspondingly longer, is of similar complexity. Their published proof of subject reduction in the earlier version is slightly flawed — the case that motivated our introduction of stupid casts is not handled properly — but the problem can be repaired by applying the same refinement we have used here.

Of these three studies, that of Flatt, Krishnamurthi, and Felleisen is closest to ours in an important sense: the goal there, as here, is to choose a core calculus that is as *small* as possible, capturing just the features of Java that are relevant to some particular task. In their case, the task is analyzing an extension of Java with Common Lisp style mixins – in ours, extensions of the core type system. The goal of the other two systems, on the other hand, is to include as *large* a subset of Java as possible, since their primary interest is proving the soundness of Java itself.

Other class-based object calculi. The literature on foundations of object-oriented languages contains many papers formalizing class-based object-oriented languages, either taking classes as primitive (e.g., [22, 8, 6, 5]) or translating classes into lower-level mechanisms (e.g., [13, 4, 1, 20]). Some of these systems (e.g. [20, 8]) include generic classes and methods, but only in fairly simple forms.

Generic extensions of Java. A number of extensions of Java with generic classes and methods have been proposed by various groups, including the language of Agesen, Freund, and Mitchell [2]; PolyJ, by Myers, Bank, and Liskov [17]; Pizza, by Odersky and Wadler [19]; GJ, by Bracha, Odersky, Stoutamire, and Wadler [7]; and NextGen, by Cartwright and Steele [10]. While all these languages are believed to be typesafe, our study of FGJ is the first to give rigorous proof of soundness for a generic extension of Java. We have used GJ as the basis for our generic extension, but similar techniques should apply to the forms of genericity found in the rest of these languages.

6 Discussion

We have presented Featherweight Java, a core language for Java modeled closely on the lambda-calculus and embodying many of the key features of Java's type system. FJ's definition and proof of soundness are both concise and straightforward, making it a suitable arena for the study of ambitious extensions to the type system, such as the generic types of GJ. We have developed this extension in detail, stated some of its fundamental properties, and given their proofs.

It was pleasing to discover that FGJ could be formulated as a straightforward extension of FJ, giving us additional confidence that the design of GJ was on the right track. Our investigation of FGJ led us to uncover one bug in the compiler, involving a subtle relation between subtyping and raw types. Most importantly, however, FGJ has given us useful vocabulary and notation for thinking about the design of GJ.

FJ itself is not quite complete enough to model some of the interesting subtleties found in GJ. In particular, the full GJ language allows some parameters to be instantiated by a special "bottom type" `*`, using a delicate rule to avoid unsoundness in the presence of assignment. Capturing the relevant issues in FGJ requires extending it with assignment and `null` values (both of these extensions seem straightforward, but cost us some of the pleasing compactness of FJ as it stands). Another subtle aspect of GJ that is not accurately modeled in FGJ is the use of bridge methods in the compilation from GJ to JVM bytecodes. To treat this compilation exactly as GJ does, we would need to extend FJ with overloading.

Our formalization of GJ also does not include *raw types*, a unique aspect of the GJ design that supports compatibility between old, unparameterized code and new, parameterized code. We are currently experimenting with an extension of FGJ with raw types.

Formalizing generics has proven to be a useful application domain for FJ, but there are other areas where its extreme simplicity may yield significant leverage. For example, work is under way on formalizing Java 1.1's *inner classes* using FJ [16].

Acknowledgments

This work was supported by the University of Pennsylvania and the National Science Foundation under grant CCR-9701826, *Principled Foundations for Programming with Objects.* Igarashi is a research fellow of the Japan Society for the Promotion of Science.

References

[1] Martín Abadi and Luca Cardelli. *A Theory of Objects.* Springer-Verlag, 1996.

[2] Ole Agesen, Stephen N. Freund, and John C. Mitchell. Adding type parameterization to the Java language. In *Object Oriented Programing: Systems, Languages, and Applications (OOPSLA)*, October 1997.

[3] H. P. Barendregt. *The Lambda Calculus.* North Holland, revised edition, 1984.

[4] Viviana Bono and Kathleen Fisher. An imperative first-order calculus with object extension. In *Proceedings of the European Conference on Object-Oriented Programming (ECOOP)*, 1998.

[5] Viviana Bono, Amit J. Patel, and Vitaly Shmatikov. A core calculus of classes and mixins. In *Proceedings of the European Conference on Object-Oriented Programming (ECOOP)*, volume 1628 of *Lecture Notes in Computer Science*, pages 43–66. Springer-Verlag, June 1999.

[6] Viviana Bono, Amit J. Patel, Vitaly Shmatikov, and John C. Mitchell. A core calculus of classes and objects. In *Fifteenth Confertence on the Mathematical Foundations of Programming Semantics*, April 1999.

[7] Gilad Bracha, Martin Odersky, David Stoutamire, and Philip Wadler. Making the future safe for the past: Adding genericity to the Java programming language. In Craig Chambers, editor, *Object Oriented Programing: Systems, Languages, and Applications (OOPSLA)*, ACM SIGPLAN Notices volume 33 number 10, pages 183–200, Vancouver, BC, October 1998.

[8] Kim B. Bruce. A paradigmatic object-oriented programming language: Design, static typing and semantics. *Journal of Functional Programming*, 4(2), April 1994. Preliminary version in POPL 1993, under the title "Safe type checking in a statically typed object-oriented programming language".

[9] Luca Cardelli, Simone Martini, John C. Mitchell, and Andre Scedrov. An extension of system F with subtyping. *Information and Computation*, 109(1–2):4–56, 1994. Preliminary version in TACS '91 (Sendai, Japan, pp. 750–770).

[10] Robert Cartwright and Guy L. Steele Jr. Compatible genericity with run-time types for the Java programming language. In Craig Chambers, editor, *Object Oriented Programing: Systems, Languages, and Applications (OOPSLA)*, SIGPLAN Notices 33(10), pages 201–215, Vancouver, BC, Octover 1998. ACM.

[11] S. Drossopoulou, S. Eisenbach, and S. Khurshid. Is the Java Type System Sound? *Theory and Practice of Object Systems*, 7(1):3–24, 1999. Preliminary version in ECOOP '97.

[12] Matthias Felleisen and Daniel P. Friedman. *A little Java, A few Patterns.* The MIT Press, Cambridge, Massachusetts, 1998.

[13] Kathleen Fisher and John C. Mitchell. On the relationship between classes, objects, and data abstraction. *Theory and Practice of Object Systems*, 4(1):3–25, 1998.

[14] Matthew Flatt, Shriram Krishnamurthi, and Matthias Felleisen. Classes and mixins. In *ACM Symposium on Principles of Programming Languages (POPL)*, San Diego, January 1998. ACM.

[15] Matthew Flatt, Shriram Krishnamurthi, and Matthias Felleisen. A programmer's reduction semantics for classes and mixins. Technical Report TR97-293, Computer Science Department, Rice University, February 1998. Corrected version appeared in June, 1999.

[16] Atsushi Igarashi and Benjamin C. Pierce. On inner classes, July 1999. Submitted for publication.

[17] Andrew C. Myers, Joseph A. Bank, and Barbara Liskov. Parameterized types for Java. In *ACM Symposium on Principles of Programming Languages (POPL)*, January 1997.

[18] Tobias Nipkow and David von Oheimb. Java$_{light}$ is type-safe — definitely. In *ACM Symposium on Principles of Programming Languages (POPL)*, pages 161–170, San Diego, January 1998. ACM.

[19] Martin Odersky and Philip Wadler. Pizza into Java: Translating theory into practice. In *ACM Symposium on Principles of Programming Languages (POPL)*, 1997.

[20] Benjamin C. Pierce and David N. Turner. Simple type-theoretic foundations for object-oriented programming. *Journal of Functional Programming*, 4(2):207–247, April 1994. Preliminary version in Principles of Programming Languages (POPL), 1993.

[21] Don Syme. Proving Java type soundness. Technical Report 427, Computer Laboratory, University of Cambridge, June 1997.

[22] Mitchell Wand. Type inference for objects with instance variables and inheritance. Technical Report NU-CCS-89-2, College of Computer Science, Northeastern University, February 1989. Also in Carl A. Gunter and John C. Mitchell, editors, *Theoretical Aspects of Object-Oriented Programming: Types, Semantics, and Language Design* (MIT Press, 1994).