Object and Reference Immutability using Java Generics

Yoav Zibin  
MIT Computer Science and Artificial Intelligence Lab  
zyoav@csail.mit.edu

Alex Potanin  
Victoria University of Wellington  
alex@mcs.vuw.ac.nz

Shay Artzi Adam Kiełzun  
MIT Computer Science and Artificial Intelligence Lab  
{artzi|akiezun|mernst}@csail.mit.edu

Abstract
A compiler-checked immutability guarantee provides useful documentation, facilitates reasoning, and enables optimizations. This paper presents Immutability Generic Java (IGJ), a novel language extension that expresses immutability without changing Java’s syntax by building upon Java’s generics and annotation mechanisms. In IGJ, each class has one additional generic parameter that is Immutable, Mutable, or ReadOnly. IGJ guarantees both reference immutability (only mutable references can mutate an object) and object immutability (an immutable reference points to an immutable object). IGJ is the first proposal for enforcing object immutability, and its reference immutability is more expressive than previous work. IGJ also permits covariant changes of generic arguments in a type-safe manner, e.g., a readonly list of integers is a subtype of a readonly list of numbers. IGJ extends Java’s type system with a few simple rules. We formalize this type system and prove it sound. Our IGJ compiler works by type-erasure and generates byte-code that can be executed on any JVM without runtime penalty.

1. Introduction
Immutability information is useful in many software engineering tasks, such as modeling [7], verification [31], compile- and runtime optimizations [10, 25, 29], refactoring [17], test input generation [1], regression oracle creation [24,33], invariant detection [14], specification mining [11], and program comprehension [21]. Three varieties of immutability guarantee are:

Class immutability No instance of an immutable class may be changed; examples in Java include String and most subclasses of Number such as Integer and BigDecimal.

Object immutability An immutable object can not be modified, even if other instances of the same class can be. For example, some instances of List in a given program may be immutable, whereas others can be modified. Object immutability can be used for pointer analysis and optimizations, such as sharing between threads without synchronization, and to help prevent hard-to-detect bugs, e.g., the documentation of the Map interface in Java states that “Great care must be exercised if mutable objects are used as map keys. The behavior of a map is not specified if the value of an object is changed in a manner that affects equals comparisons while the object is a key in the map.”

Reference immutability A readonly reference [2,5,13,22,25,30,32] (or a const pointer in C++) cannot be used to modify its referent. (However, the referent might be modified using an aliasing mutable reference.) Reference immutability is required to specify interfaces, such as that a procedure may not modify its arguments (even if the caller retains the right to do so) or a client may not modify values returned from a module. However, past work does not guarantee object immutability, unless reference immutability is combined with an alias/escape analysis to guarantee that no aliases to an object exist.

This paper presents Immutability Generic Java (IGJ), a language that supports class, object, and reference immutability. Each object is either mutable or immutable, and each reference is Immutable, Mutable, or ReadOnly. Inspired by work that combines ownership and generics [27], the distinctions are expressed without changing Java’s syntax by adding one new generic parameter (at the beginning of the list of generic parameters):

1. // An immutable reference to an immutable date; mutating the referent is prohibited, via this or any other reference.
2. Date<Immutable> immutD = new Date<Immutable>();
3. // A mutable reference to a mutable date; mutating the referent is permitted, via this or any other mutable reference.
4. Date<Mutable> mutD = new Date<Mutable>();
5. // A readonly reference to any date; mutating the referent is prohibited via this reference, but the referent may be changed via an aliasing mutable reference.
6. Date<ReadOnly> roD = ... ? immutD : mutD;

Line 2 shows object immutability in IGJ, and line 6 shows reference immutability. See Fig. 4 for a larger example of IGJ code. Java prohibits changes to generic arguments, such as in line 6, to avoid a type loophole. However, if mutation is disallowed, then such covariant changes are type-safe, and indeed in IGJ List<ReadOnly,Integer> is a subtype of List<ReadOnly,Number>.

IGJ satisfies the following design principles:

Transitivity IGJ provides transitive (deep) immutability that protects the entire abstract state of an object. For example, an immutable graph can contain an immutable set of immutable edges. C++, for example, does not support such transitivity because C++’s const-guarantee does not traverse pointers, i.e., a pointer in a const object can mutate the object to which it points.

Moreover, IGJ supports shallow immutability, i.e., it is possible to exclude some fields from the abstract state. For example, fields used for caching can be mutated even in an immutable object.

Static There is no runtime representation for immutability, such as an “immutability bit” that is checked before assignments or method calls. Testing at runtime whether an object is immutable [30] hampers program understanding.

The IGJ compiler works by type-erasure, without any run-time representation of reference or object immutability, which enables executing the resulting code on any JVM without run-
time penalty. A similar approach was taken by Generic Java (GJ) [6] that extended Java 1.4. As with GJ, libraries must either be retrofitted with IGJ types, or fully converted to IGJ, before clients can be compiled. IGJ is backward compatible, i.e., every legal Java program is a legal IGJ program.

Polymorphism It is possible to abstract over immutability without code duplication, e.g., a method argument that is either mutable or immutable. For instance, all the collection classes in C++’s STL have two overloaded versions of iterator, operator[], etc. The underlying problem is the inability to return a reference whose immutability depends on the immutability of this:

```java
const Foo getFIeldF00() const;
Foo getFleldFoo();
```

Simplicity IGJ does not change Java’s syntax or typing rules. IGJ adds a small number of additional typing rules, that make IGJ more restrictive than Java. On the other hand, IGJ subtyping rules are more relaxed, allowing covariant changes in a type-safe manner.

The contributions of this paper are as follows: (i) a novel and simple design combining both reference and object immutability that naturally fits into Java’s generics framework, (ii) an implementation of an IGJ compiler, proving feasibility of the design, and (iii) a formalization of IGJ with a proof of type soundness. Our ideas, though demonstrated using Java, are applicable to any statically typed language with generics, such as C++, C#, and Eiffel.

Outline The remainder of this paper is organized as follows. Sec. 2 describes the IGJ language, which is compared to previous work in Sec. 3. Sec. 4 discusses our experimentation with IGJ, and Sec. 5 formalizes IGJ and gives a proof of soundness. Sec. 6 outlines future work. We conclude in Sec. 7.

2. IGJ language

IGJ provides three kinds of references: readonly, mutable, and immutable. The first generic argument of a class/type in IGJ is called the *immutability parameter*, and it must be Mutate, Immutable, or Readonly.

2.1 Type hierarchy

Fig. 1 depicts the type hierarchy of immutability parameters. The subtyping relation is denoted by $\leq$, e.g., Immutable $\leq$ Readonly. The immutability parameters Immutable, Immutable, and Readonly may not be extended, and they have no subtype relation with any other types in IGJ.

The root of the IGJ type hierarchy (excluding Readonly and its descendants) is Object<Readonly>. Fig. 2 depicts the subtype relation for the classes Object and Date.

In Java, all generic parameters are invariant. The subtyping rules for IGJ are more relaxed. IGJ permits covariant changes in the immutability parameter (the first generic argument), e.g.,

```
Date<Mutable> $\leq$ Date<ReadOnly>
```

This satisfies the polymorphism design principle, because a programmer can write a single method that accepts a reference of any immutability, for example:

```java
void print(Date<ReadOnly> d)
```

IGJ also permits covariant changes in other generic arguments if the immutability parameter is Readonly or Immutable, e.g.,

```
List<Readonly,Integer> $\leq$ List<Readonly,Number>
```

Covariant changes are safe only when the object is readonly or immutable because it cannot be mutated in a way which is not type-safe. Therefore the following pair is not in the subtype relation:

```
List<Mutable,Integer> $\not\leq$ List<Mutable,Number>
```

A type variable $X$ in class $C$ can be annotated with $\texttt{NoVariant}$ to prevent covariant changes, in which case we say that $X$ is no-variant and write $\texttt{NoVariant}(X,C)$. Otherwise we say that $X$ is co-variant and write $\texttt{CoVariant}(X,C)$. Sections 2.3 and 2.5 discuss when a type-variable should be no-variant. For example, the type variable $X$ in the interface $\texttt{Comparable}(I,X)$ is no-variant:

```
interface Comparable<I extends Readonly, \texttt{NoVariant} X> {
    @Readonly int compareTo(X o); }
```

For instance, $\texttt{Comparable<Readonly,Integer>}$ was written to compare itself to an Integer, thus it should not be a subtype of $\texttt{Comparable<Readonly,Number>}$, that can be passed a Number.

IGJ’s subtype definition for two types of the same class is given in Def. 2.1. The full subtype definition (formally given in Fig. 12 of Sec. 5) includes all of Java’s subtyping rules, therefore IGJ’s subtype relation is a superset of Java’s subtype relation.

**Definition 2.1.** Let $\langle x_1, x_2, \ldots, x_n \rangle$ be a class with $n \geq 0$ generic variables. Then, type $S = \langle C, S_1, \ldots, S_n \rangle$ is a subtype of $T = \langle C', T_1, \ldots, T_n \rangle$, written as $S \leq T$, iff $J \leq J'$ and for $i = 1, \ldots, n$, either $S_i = T_i$ or (Immutable $\iff J' \geq J$ and $S_i \leq T_i$, or $\texttt{NoVariant}(X_i,C)$).

**Example** Fig. 3 presents the subtype hierarchy for List<Object>. The types $\langle \text{List}'\langle\text{Object}\rangle, \text{List}'\langle\text{Integer}\rangle, \text{List}'\langle\text{Number}\rangle \rangle$ have a common mutable supertype $\text{List}'\langle\text{Object}\rangle$, $\text{List}'\langle\text{Object}\rangle$, $\text{List}'\langle\text{Object}\rangle$, but the only value that can be inserted in such a list is null. (See Sec. 3 for a discussion of Java’s wildcards.)

2.2 Reference immutability

This section gives the three key type rules of IGJ that enforce reference immutability: that is, only a reference immutability: that is, only a

```
const Foo getFieldFoo() const;
```

Figure 1. The type hierarchy of immutability parameters, which have special meaning when used as the first generic parameter, as in List<Mutable,T>. (See also Fig. 6 in Sec. 2.4)

Field can be assigned only by a mutable reference:

```
const Foo getFieldFoo() const;
```

Figure 2. The subtype hierarchy for Object and Date. The classes (in bold) still have an underlying tree structure.

- Annotating generic arguments will be available only in Java 7 [15]. In the meantime it is possible to annotate the class or interface instead, and specify which positions are no-variant.
Figure 3. The subtype hierarchy for List<Object>, abbreviated as L<0>. The types ReadOnly, Mutable, and Immutable are abbreviated as R, M, and I, respectively. The crossed-out arrows emphasize pairs that are not subtypes.

**FIELD-ASSIGNMENT RULE:**

\( o.\text{someField} = \ldots \) is legal iff \( I(o) = \text{Mutable} \).

Phrased differently, you cannot assign to fields of a readonly reference, e.g.,

Employee<ReadOnly> roE = \ldots;  
roE.address = \ldots; // Compilation error!

The immutability of this depends on the context, i.e., the method in which this appears:

**THIS RULE:** \( I(\text{this}) = I(m) \), in a method \( m \).

Because there is no obvious syntactic way to denote the immutability of this, IGJ uses method annotations: @ReadOnly, @Mutable, etc.²

For example, below we have \( I(\text{this}) = I(m) = \text{Mutable} \):

```java
@Mutable
void m() { \ldots this \ldots }
```

The default method annotation in IGJ is @Mutable, but for clarity of presentation, this paper explicitly annotates all methods.

The third type rule of IGJ states when a method call is legal:

**METHOD-INVOCATION RULE:** \( o.m(\ldots) \) is legal iff \( I(o) \leq I(m) \).

IGJ requires that \( I(o) \leq I(m) \), and not simply \( I(o) = I(m) \), to allow a mutable reference to call readonly methods, e.g.,

Employee<Mutable> o = \ldots;  
o.setAddress(\ldots); // OK: \( I(o) \leq I(\text{setAddress}) = \text{Mutable} \)  
o.getAddress();  
// OK: \( I(o) \leq I(\text{getAddress}) = \text{ReadOnly} \)  
\((\text{Employee<ReadOnly> o).setAddress(\ldots)}\);  
// Illegal!

**Example** Fig. 4 presents two IGJ classes: Edge and Graph. The immutability parameter I is declared in lines 1 and 11; by convention we always denote it by I. If the extends clause is missing from a class declaration, then we assume that class extends Object<0>, as in Fig. 3. We can use any subtype of ReadOnly in place of I, e.g., ReadOnly (on line 9), Mutable (on line 15), or another parameter such as I (on line 12) or M (on line 18).

We will now demonstrate the type-checking rules by example. The assignment `this.id = id` on line 5 is legal because according to **THIS RULE** we have that \( I(\text{this}) = I(\text{setId}) = \text{Mutable} \), and according to **FIELD-ASSIGNMENT RULE** a mutable reference can assign to a field. That assignment would be illegal if it was moved to line 6, because this is readonly in the context of method getId. The method call `this.setId(\ldots)` on line 3 is legal according to **METHOD-INVOCATION RULE** because \( I(\text{this}) \leq I(\text{setId}) \). That method call would be illegal on line 6.

Observe on line 9 that the static method `print()` does not have an annotation because it does not have an associated `this` object. According to Def. 2.1 of the subtype relation, an edge of any immutability can be passed to `print()`.

We call the field `edges` on line 12 this-mutable [32] because its immutability depends on the immutability of this: in a mutable object this field is mutable and in a readonly object it is readonly. C++ has similar behavior for fields without the keywords const or mutable. The advantage of IGJ syntax is that the concept of this-mutable is made explicit in the syntax: a class can pass its immutability parameter to its fields, and the underlying generic type system propagates the immutability information without the need for special type-rules. Using generics simplifies both the design and the implementation.

Moreover, C++ has no this-mutable local variables, return types, or parameters, whereas IGJ treats I as the regular generic parameter. For example, the parameter `edges` on line 13 and the return type on line 8 are both this-mutable.  

Recall that the **Transitivity** design principle states that the design must support transitive (deep) immutability. In our example, in a mutable Graph the field edges will contain a mutable list of mutable edges. The second usage of I in List<I,Edge<I>> is not expressible in C++.

### 2.3 Method overriding

IGJ respects the Java class hierarchy. An overriding method must preserve or strengthen the specification of the overridden method:

**METHOD-OVERLOADING RULE 1:**

If method \( m' \) overrides \( m \), then \( I(m) \leq I(m') \).

For example, overriding can change a @Mutable method to a @ReadOnly method, but not vice versa.

IGJ requires that the erased signature of an overriding method remain the same if that method is either readonly or immutable. The erased signature of a method is obtained by replacing type-variables with their bounds. When the erased signature of an overriding method changes, the compiler inserts a bridge method to cast the arguments to the correct type [6].

**METHOD-OVERLOADING RULE 2:**

If method \( m' \) overrides \( m \) and \( I(m) \leq I(m') \), then the erased signatures of \( m' \) and \( m \) (excluding no-variant type-variables) must be identical.

²The paper uses the annotation @ReadOnly whereas the IGJ compiler uses @ReadOnyMethod, because an annotation and a class cannot have the same qualified name. The same applies for the other three annotations.
2.4 Object immutability

One advantage of object immutability is enabling safe sharing between different threads without the cost of synchronization. Consider lines 6–7 in Fig. 4. A long read/write is not atomic in Java; synchronization is necessary. However, only an immutable Edge can use getIdImmutable() to avoid the cost of synchronization.

The referent of a readonly reference (Sec. 2.2) is not immutable: it could be changed via another pointer. A separate analysis can indicate some cases when such changes are impossible [32], but it is preferable for the type system to guarantee that the referent of immutable references cannot change.

The IGJ type system makes such a guarantee:

A mutable reference points to a mutable object, and
an immutable reference points to an immutable object.

(1)

In order to enforce this property, no immutable reference may be aliased by a mutable one; equivalently, no mutable reference may point to an immutable object.

2.4.1 Constructors and Annotation @AssignsFields

The rules given so far are sufficient to guarantee object immutability for IGJ with the exception of constructors. A constructor that is making an immutable object must be able to set fields in the object (which becomes immutable as soon as the constructor returns). It is not acceptable to mark the constructor of an immutable object as @Mutable, which would permit arbitrary side effects, possibly including making mutable aliases to this.

IGJ uses a fourth kind of reference immutability, AssignsFields, to permit constructors to perform limited side effects without permitting modification of immutable objects. Whereas a @Mutable method can assign and mutate the object’s fields, an @AssignsFields method can only assign (not mutate) the fields of this. A programmer can write the @AssignsFields method annotation but may not write the AssignsFields type in any other way, such as Edge<AssignsFields>. Therefore, in an AssignsFields constructor, this can only escape as ReadOnly. Fig. 6 shows the full hierarchy of immutability parameters.

AssignsFields is not transitive, i.e., you can assign to fields of this but not to fields of fields of this. Specifically, we relax FIELD-ASSIGNMENT RULE by allowing a field of this to be assigned in an @AssignsFields method:

FIELD-ASSIGNMENT RULE revised:

If overriding were legal, the bridge method of isIn(Integer) would cast an Object to an Integer

Fig. 5. An example of illegal method-overriding due to Method-Overriding Rule 2

Fig. 6. The type hierarchy of immutability parameters, including AssignsFields.
constructors are mutable, we can safely assume that this is mutable as well.

Remark 2.2. Before JSR 133 [28] immutable objects could have different values in different threads. The new memory model adds a “synchronization point” at the end of a constructor after which all assignments are guaranteed to be written. However, the programmer is warned (in the documentation only!) that immutable objects are thread-safe only if this does not escape its constructor. Therefore we plan to modify IGJ to issue a warning whenever this escapes, even though it is not dangerous to IGJ’s type system because only a readonly this can escape.

2.5 Mutable and assignable fields

A type system should guarantee facts about the abstract state of an object, not merely its concrete representation. Therefore, a transitive guarantee of immutability for all fields of an object may be too strong. For example, fields used for caching are not part of the abstract state. This section discusses how to permit a given field to be assigned or mutated even in a readonly or immutable object, and thus discusses special restrictions involving such fields.

Assignable fields An assignable field (denoted by the @assignable annotation) is in essence the reverse of a final field: a final field cannot be re-assigned whereas an assignable field can always be assigned (even using a readonly reference). IGJ uses to denote that annotation is in essence the reverse of a final field: a final field can always be mutated, even using a readonly reference. Therefore, a field is marked as mutable.

For example, consider this code snippet:

```java
private @assignable int memoizedHashCode = 0;
public @Readonly int hashCode() {
    if (memoizedHashCode == 0) {
        memoizedHashCode = ...;
    }
    return memoizedHashCode;
}
```

The assignment `memoizedHashCode = ...` is legal even though `hashCode()` is readonly, due to the @assignable annotation.

Mutable fields A mutable field can always be mutated, even using a readonly reference. No new linguistic mechanism is required to express a mutable field: its immutability parameter is Mutable.

For instance, `AccessOrderedSet` in Fig. 7 implements a set using a list (line 3), and as an optimization it maintains the list in access-order even during calls to readonly methods such as contains (line 7). Therefore, `l` is declared as a mutable field.

Covariant and no-variant type-variables Type-variable `X` in Fig. 7 must be annotated as @NoVariant (line 2) due to its use in the mutable field `l`. If `X` could change covariantly, we would have that:

- `AccessOrderedSet<ReadOnly, Integer >= AccessOrderedSet<ReadOnly, Number`

We could then add a `Number` to an `Integer` list using the contains method in line 3 of Fig. 7.

An assignable field or a mutable superclass have the same restriction as a mutable field:

- **NoVariant Rule**: A type-variable must be no-variant if it is used in a mutable field, an assignable field, a mutable superclass, or in the position of another no-variant type-variable. (See a formal definition in Fig. 11.)

The immutability parameter is a special generic variable that must be allowed to change covariantly, otherwise a mutable reference could not call a readonly method. In other words, `I` must be co-variant:

- **Covariant Rule**: CoVariant(x, c) must hold for any class `c`.

For example, declaring the following field is prohibited because the immutability parameter `I` must always be co-variant:

```java
@assignable Edge<I> f;
```

2.6 Inner classes

Nested classes that are static can be treated the same as normal classes. An inner class is a nested class that is not explicitly or implicitly declared static (see JLS 8.1.3 [18]). Inner classes have an additional field: this reference. Inner classes have an additional this reference: OuterClass.this. According to This RULE, the immutability of this depends on the immutability of the method. Because methods in IGJ have a single method annotation, the immutability of this and OuterClass.this should be the same. Therefore, in IGJ an inner class cannot have its own immutability parameter:

- **Inner-Class Rule**: An inner class inherits the immutability parameter of the outer class.

Consider the code in Fig. 8. Lines 1–5 show the declaration of the Iterator interface, in which the only mutable method is remove. The immutability of an iterator is inherited from its container. Therefore, even though method next changes the state of the iterator it does not change the state of the container and is thus considered state preserving for the container and declared as readonly. In contrast, method remove changes the container and is thus marked as mutable.

Now consider the class `ArrayList` and the inner class `ArrItr`.

We do not pass an immutability parameter to the inner class `ArrItr` on lines 7–8, because it inherits its immutability from `ArrayList`. On line 13 both these references are mutable because `remove()` is mutable. Finally, consider the creation of a new iterator on line 7. We handle this new operation using METHOD-INVOCATION RULE for method calls (instead of OBJECT-CREATION RULE): this method call is legal because this is readonly and the constructor of `ArrItr` is readonly. We do not use OBJECT-CREATION RULE because the inner object inherits the immutability of the outer object.

Anonymous inner classes can be considered identical to regular inner classes where the only exception is that we cannot write a constructor because the class has no name, making it impossible to annotate the constructor. For instance, the code in Fig. 8 can be converted to use an anonymous inner class:

```java
public @Readonly Iterator<I,E> iterator() {
    return new Iterator<I,E>() {
        ...
    };
}
```

However, we can safely assume that the immutability of the missing constructor is the same as the immutability of the method in which the inner class is declared, or else the new operation would...
be illegal in IGJ. In the example above the immutability of the constructor must be readonly because iterator() is readonly.

2.7 Exceptions, immutable classes, reflection, and arrays

In IGJ's syntax, the immutability is an integral part of the type. In Javari [32] (see Sec. 3) it is syntactically possible but semantically illegal to write this code:

```java
class Cell<X> { readonly X x; ... }
```

It is semantically illegal because the immutability of X is determined in the client code, e.g., Cell<readonly Date>. In comparison, IGJ's syntax does not even enable such a declaration: it is syntactically and semantically illegal.

`throwable` Generics and immutability naturally combine in another aspect: their usage limitations. For example, it is forbidden to throw a readonly reference because the catch can mutate that reference. Similarly, Java prohibits adding generic parameters to any subclass of `throwable` because the compiler cannot statically connect the throwing and catching positions. IGJ naturally inherits this usage limitation from the underlying generics mechanism.

Manifest classes and immutable classes IGJ supports manifest classes [27], which are classes without an immutability parameter. Manifest classes can be used to express class immutability, e.g.,

```java
class String extends Object<Immutable> ... 
```

IGJ treats all methods of String as if they were annotated with `@immutable`, and issues errors if mutable fields exist.

`reflection` It is discouraged in IGJ to use reflection or to remove the immutability parameter by casting to a raw type. The IGJ compiler issues a warning in both cases because they can create holes in the type system. (IGJ does not consider these errors because it might be necessary to call legacy code.)

`arrays` Java does not permit arrays to have generic parameters. IGJ supplies a wrapper class `Array<T>` that enables the creation of immutable arrays. IGJ treats an array type `T[]` as `Array<Immutable,T>`, i.e., arrays are mutable by default.

3. Previous Work

We are not aware of any work that proposed a static typing system for object immutability and not just reference immutability. Pechtchanski and Sarkar [25] describe various annotations for immutability assertions, such as `@Nonnull`, etc., and show that such assertions enable optimizations that can speed up some benchmarks by 5–10%. However they do not present any typing rules to enforce such assertions.

Java already includes various classes whose instances are immutable, and it supports a non-transitive form of immutability using `final1`. Functional languages such as ML default all fields to being immutable, with mutable fields being the exception. C++'s `const` mechanism has similar semantics to IGJ: a field can be declared as `const` (similar to readonly in IGJ), `mutable`, or by default as this-mutable. However, in contrast to IGJ, parameters to functions, return types, local variables, and generic parameters cannot be this-mutable. Other disadvantages are: (i) `const` can be cast away at any time, making it more a suggestion than a binding contract, (ii) `const` protects only the state of the enclosing object and not objects it points too, e.g., you cannot mutate an element inside a `const` node in a list, but the next node is mutable, and (iii) using `const` results in code duplication such as two versions of `operator[]` in every collection class in the STL.

Most of IGJ terminology was borrowed from Javari [32] such as `immutable`, `readonly`, `mutable`, etc. However, this-mutable fields in Javari are `mutable` as `value` and `readonly` as `value`. Javari does not support object immutability, whereas its reference immutability is more limited than that of IGJ for two reasons: (i) parameters to methods, return types, and local variables, cannot be this-mutable, and (ii) IGJ can use generics to abstract over the immutability parameter. Javari’s `readonly` is in essence a template over immutability. For instance, if you wish to find an edge in a graph, then the algorithm will be the same regardless if the graph contains mutable or readonly edges, however the return type changes depending on the immutability of the edges. In IGJ, instead of inventing a new template-like mechanism such as `readonly`, we use generics to achieve the same goal, as demonstrated by the static method `findEdge` on line 17 of Fig. 4. Javari also supports `this-assignable fields`, which pass the assignability (`final` or `assignable`) of this to a field. Finally, Javari uses `?readonly which is similar to Java’s wildcards. Consider, for instance, the class `Foo` written in Javari’s syntax:

```java
class Foo { public List<Object> list; } 
```

Then in a `readonly Foo the type of list is` `readonly List<? extends Object>` which is syntactic sugar for

```java
readonly List<? extends readonly Object super mutable Object> 
```

Thus, it is possible to insert only mutable elements to list, and retrieve only readonly elements.

1 A final field cannot be assigned a new value after the constructor finishes. However, this restriction can be circumvented using reflection.

---

Figure 8: Declaration of the interface `Iterator` and the class `ArrayList` with an inner class `ArrItr`. 

---

```java
1: interface Iterator<T extends ReadOnly,E> 
2: { 
3: @ReadOnly boolean hasNext();
4: @ReadOnly E next();
5: } 
6: class ArrayList<T extends ReadOnly, E> 
7: { 
8: public @ReadOnly Iterator<T, E> iterator() { return this.new ArrItr(); } // OK: I(this) ⊆ I(ArrItr) = Readonly 
9: class ArrItr implements Iterator<T, E> { // ArrItr has no explicit immutability parameter: it is inherited from the outer class 
10: private @assignable int currPos;
11: public @ReadOnly ArrItr() { this.currPos=0; } // OK: currPos is @assignable 
12: public @ReadOnly E next() { return ArrayList.this.get( this.currPos++ ); } // OK: I(this) ⊆ I(get) = Readonly 
13: public @Mutable void remove() { ArrayList.this.remove( this.currPos - 1 ); } // OK: I(this) ⊆ I(remove) = Mutable 
14: } 
15: }
```
Skoglund and Wrigstad [30] propose a system with read and write references with similar semantics to C++’s const. They also introduce a caseInsensitive construct which permits run-time checking of reference writeability.

Several papers proposed a mechanism of access rights. JAC [22] is a compile-time access right system with the following access right order: readnothing < readmutable < readonly < writeable, where readnothing cannot access fields of this (only the identity for equality), and readmutable can only access immutable state of this. JAC uses additional keywords (such as nontransferable) that address other concerns than immutability. Capabilities for sharing [5] are intended to generalize various other proposals for access rights, ownership and immutability, by giving a lower level semantics that can be enforced at compile- or run-time. A reference can possess any combination of these 7 access rights: read, write, identity (permitting address comparisons), exclusive read, exclusive write, exclusive identity, and ownership (giving the capability to assert rights). Immutability, for example, is represented by the lack of the write right and possession of the exclusive write right.

Boyland [4], concludes that readonly is useful but it does not address observational exposure, i.e., modifications on one side of an abstraction boundary that are observable on the other. However, IGJ’s immutable objects can be shared safely because their state cannot change. Boyland’s second criticism was that the transitivity principle (see Sec. 1), which is mandatory in all the designs above, should be selectively applied by the designer, because; “the elements in the container are not notionally part of the container” [4]. In IGJ, a programmer can solve this problem by using a different immutability for the container and its elements.

Non-null types [16] has a similar challenge that IGJ has in constructing immutable objects: a partially-initialized object may escape its constructor. IGJ uses @assignFields to mark a constructor of immutable objects, and a partially initialized object can escape only as ReadOnly. Non-null types uses a @raw annotation on references that might point to a partially-initialized object, and on methods to denote that the receiver can be @raw. A non-null field of a @raw object has different Ivalue and rvalue: it is possible to assign only non-null values to such field, whereas reading from such field may return null. Similarly to IGJ, non-null types cannot handle cyclic data-structures, nor can it express the staged initialization of immutable parts of this (only the identity for equality), andReadOnly can only access immutable state of this. IGJ uses additional keywords (such as nontransferable) that address other concerns than immutability. Capabilities for sharing [5] are intended to generalize various other proposals for access rights, ownership and immutability, by giving a lower level semantics that can be enforced at compile- or run-time. A reference can possess any combination of these 7 access rights: read, write, identity (permitting address comparisons), exclusive read, exclusive write, exclusive identity, and ownership (giving the capability to assert rights). Immutability, for example, is represented by the lack of the write right and possession of the exclusive write right.

3.1 Ownership types and readonly references

Ownership types [3,8,23] impose a structure on the references between objects in a program’s memory. Ownership-enabled languages such as Ownership Generic Java [27] prevent aliasing to the internal state of an object. While preventing exposure of owned objects, ownership does not address exposing immutable parts of an object that cannot break encapsulation.

One possible application of ownership types is the ability to reason about read and write effects [9] which has complimentary goals to object immutability. Universes [13] is a Java language extension combining ownership and reference immutability. Most ownership systems enforce that all reference chains to an owned object pass through the owner. Universes relaxes this demand by enforcing this rule only for mutable references, i.e., readonly references can be shared without restriction.

3.2 Covariant subtyping

Covariant subtyping is allowing covariant changes in generic parameters in a type-safe manner. Variant parametric types [20] attach a variance annotation to a type argument, e.g., Vector<+Number> or Vector<Number>. The subtype relation contains the following chain:

Vector<Integer> ≲ Vector<Number> ≲ Vector<Object> ≤ Vector<String>

The type checker prohibits calling someMethod(X) when the receiver is of type Foo<+Number>. For instance, suppose there is a field isIn(Number) in class Vector<Number>. Then, it is prohibited to call isIn(Number) on a reference of type Vector<Number>.

Java's wildcards have a similar chain in the subtype relation:

Vector<Integer> ≲ Vector<Number> ≤ Vector<Object>

Java's wildcards and variant parametric types are different in the legality of invoking isIn(Number) on a reference of type Vector<Number> while such an invocation is prohibited in variant parametric types. Java permits such an invocation, however the only value of type ? extends Number is null.

IGJ also contains a similar chain:

Vector<Mutable,Integer> ≲ VectorReadOnly,Integer ≤ VectorReadOnly,Number

However the restriction on method calls in IGJ is based on semantics (whether the method is readonly or not) rather than on method signature as in wildcards and variant parametric types. For example, IGJ allows calling isIn(Number) on a reference of type VectorReadOnly, Number if isIn is readonly.

3.3 Typestates for objects

In a typestates system, each object is in a certain state, and the set of applicable methods depends on the current state. Verifying typestates statically is challenging due to the existence of aliases, i.e., a state change in a particular object must affect all existing aliases to it. Typestates for objects [12] uses linear types to manage aliasing.

Object immutability can be partially expressed using typestates: by using two states (mutable and immutable) and declaring that mutating methods are applicable only in the mutable state. An additional method should mark the transition from a mutable state to an immutable state, and it should be called after the initialization of the object has finished. It remains to be seen if systems such as [12] can handle arbitrary aliases that occur in real programs, e.g., this references that escape in the constructor.

4. Experimentation

To illustrate the usability of IGJ we converted the programs of the jorden benchmark to IGJ, using an Eclipse plug-ins. We compiled those programs using the IGJ compiler, and we examined the code to find places that IGJ could provide stronger immutability guarantees.

Converting Java to IGJ

We have created two Eclipse plug-ins for converting Java code into IGJ. The first plug-in converts full classes into IGJ by adding type parameters (<I extends ReadOnly> to each class, and setting the immutability of fields, locals, and method to @mutable. The second plug-in generates IGJ skeletons of libraries’ public signatures. This allows the developer to use or change the immutability interface of library classes, while avoiding the need to modify the library code to reflect those changes.

Due to Java restrictions, type parameters are not added in the following cases:

1. Accessing static fields or methods
2. In the context of reflection (.class or instanceof)
3. Array construction
mutable classes: we made those classes extend and perimeter of a region in a binary image represented by a quad-tree.

Property (1) implies such theorem, or else it would be possible to

This section gives the type rules of a simplified version of IGJ

Proving soundness is essential in face of complexities such as the

5. Proof of Type Soundness

Proving soundness is essential in face of complexities such as the

Our type system, called Featherweight IGI (FIGJ), is based on

FIGJ models the essence of IGI: the fact that only mutable references can assign to fields, and the new subtype definition. Similar to the way FGJ removed many features from Java (such as null values, assignment, overloading, private, etc.), we removed from IGI all method annotations. In other words, all methods are read-only, with the exception of a single constructor that assigns its arguments to the object’s fields, thus making AssignFields redundant. Assignment must be done from the “outside”, i.e., instead of calling a setter method we must set the field from the outside (all fields are considered public in FIGJ).

Finally, we restrict each class in FIGJ to have a single immutability parameter which extends ReadOnly, i.e., FIGJ cannot express manifest classes such as String.

Sec. 5.1 describes the syntax of FIGJ. The FIGJ subtype relation is presented in Sec. 5.2. Sec. 5.3 modifies the FIGJ type checking rules to allow field assignment only by a mutable reference. Sec. 5.4 modifies FIGJ operational semantics (reduction rules) to get stuck when assigning to a field of an immutable object, and Sec. 5.5 proves that in a well-typed program this never happens.

5.1 Featherweight IGI Syntax

Because FIGJ models immutability, we had to add imperative extensions to FIGJ such as assignment to fields, object locations and a store [26]. We also add three special types: ReadOnly, Immutable, and Mutable.

Fig. 10 presents the syntax of FIGJ. It defines types (T), non-

variable types (η), immutability parameters (I), class declarations (L), method declarations (θ), and expressions (e). Expressions in FIGJ include the five expressions in FGI (method variable, field and method access, new instance creation, and cast), as well as our imperative extensions (field update and locations). Note that an immutability parameter is not a type in η, and the only places it appears in the syntax is as the first generic parameter of a type and the first generic variable of a class. The root of the class hierarchy is Object\x <: ReadOnly.

To support field assignment we define a store \( S = \{ 1 \mapsto \eta(1) \} \) that maps locations to created objects. Note that we do not need a store typing [26] because the store already contains the type of each location. For a simpler notation we use a single symbol \( \Delta \) to denote an environment that maps (i) variables to their types, (ii) type variables to their bounds (which are non-variable types): \( \Delta = \{ x : T \} \cup \{ x : \eta \} \). (The notation used in [26] is: typing context \( \Gamma \), environment \( \Delta \).)

The field, method type, and method body lookup functions are based on their counterparts in FIGJ and thus omitted from this paper. We define an additional auxiliary function that returns the immutability parameter \( I(\eta, x) = \eta \).

Fig. 11 defines which type-variables are no-variant. We use two auxiliary functions: (i) \( FV(T) \) is the set of free variables in \( T \), (ii) \( subterm(\eta) \) is the set of all subterms of types in \( \eta \). (We do not need to consider the superclass as in NoVariant rule because fields includes all fields of the superclass as well.)

After NoVariant reaches a fixed point on the class declarations, we can define Covariant(\( x, c<<x> \)) to be the negation of NoVariant. In order for the class declarations to be well-formed, the immutability parameter must always be in

\[ \text{Covariant}(x, c<<x>) \text{ for any class } c. \]  

We make the same assumptions as in FGI about the correctness of the class declarations (e.g., that there are no circles in the subclass relation, that we have no method overloading, etc). We also use the same judgements as in FIGJ, such as type, store, expressions,
method and class wellformedness, with minor differences (e.g., instead of \texttt{object} we use \texttt{object<T>}).

FIGJ is more strict than FGJ regarding method overriding because FIGJ requires that the erased signatures of methods be identical (up to renaming of type variables):

Definition 5.1. The erased signature of method \texttt{m(T x)} in class \texttt{C<X< T>}} is
\[
\lambda X.[t / X] T
\]

5.2 Subtyping

Fig. 12 shows FIGJ subtyping rules. The first four rules are the same as FGJ rules. Additionally, two special classes — \texttt{Mutable} and \texttt{Immutable} — are considered a separate class hierarchy extending \texttt{ReadOnly}. The rule \texttt{s1} is a formalization of Def. 2.1.

Observe that the subtype relation is reflexive and transitive. Note that from rule \texttt{s1} and \texttt{t2} we have that
\[
\text{if } T \subseteq T', \text{ then } C<T, T'> \subseteq C<T, T'>.
\]

We write \( T \subseteq T' \) as a shorthand for \( \Delta \vdash T \subseteq T' \). Observe in rule \texttt{s1} that the requirement \texttt{Immutable} \( \preceq T_1 \) is equivalent to \texttt{Y} \( \preceq \texttt{Mutable} \) and \texttt{T}' \( \not\preceq X \) (where \texttt{X} is a variable), because an immutability parameter can have only four values according to the syntax rule for \texttt{t1} in Fig. 10.

In Java, if \texttt{A} \( \preceq \texttt{B} \) and \texttt{f} is a field of \texttt{B}, then the type of field \texttt{f} in \texttt{A} and \texttt{B} is exactly the same, i.e., \texttt{A.f} \( \equiv \texttt{B.f} \). In FIGJ, we revise this property and demand that \texttt{A.f} \( \preceq \texttt{B.f} \). For instance, consider the field \texttt{edges} on line 12 of Fig. 4, and the following two variables:

\texttt{Graph<Mutable> mutG;}  
\texttt{Graph<ReadOnly> roG;}  
// \texttt{mutG.edges} has the type \texttt{List<Mutable,Edge<Mutable>>>}  
// \texttt{roG.edges} has the type \texttt{List<ReadOnly,Edge<ReadOnly>>>}

And indeed the first is a subtype of the latter.

Lemma 5.2. Let \( T \preceq T' \), \( T' \preceq T'' \). Then \( F \preceq F'' \).

Proof. It is trivial to prove that field \( f \) exists in \( \texttt{fields}(T) \). We will prove that \( F \preceq F'' \) by induction on the derivation of \( T \preceq T' \). Consider the last rule in the derivation sequence. The proof for the first six rules is immediate from the definition of \texttt{fields} and the fact that subtyping is transitive.

Now consider rule \texttt{s1}, where \( T = C<X,< T'> \), and \( T' = C<U',< T'> \):
\[
\text{Let } \mathcal{V} \text{ denote the type of field } f \text{ in } C<X>. \text{ Then we have that } F = \{u / X\} V \text{ and } F' = \{u' / X\} V. \text{ On the one hand, if } u_i = u'_i \text{ for all } i, \text{ then } T = T' \text{ and thus } F = F'.
\]

On the other hand, for some value \( i \), we have that \( u_i \neq u'_i \). Therefore we know from rule \texttt{s1} that \texttt{Immutable} \( \preceq u_i \), \( u_i \preceq u'_i \), and \texttt{CoVariant}(X_i, C<X>). \texttt{Let } t \text{ range over the integers in which } u_i \neq u'_i. \text{ We will prove by induction that for every subterm } \lambda x<S> \text{ in } \mathcal{V}, \text{ we have } \{u_i / x\} S \preceq \{u'_i / x\} S. \text{ From rule } \texttt{s1} \text{ we need to prove that for all } j: \text{ either } \{u_i / x\} S_j = \{u'_i / x\} S_j \text{ or,}
\]
\[
\texttt{If } X \notin \texttt{FV}(S_j), \text{ then } \{u_i / x\} S_j = \{u'_i / x\} S_j \text{. Thus assume that } X \in \texttt{FV}(S_j).
\]

If \( S_j = X_1 \), then \( \{u_i / x\} S_j = \{u'_i / x\} S_j \) and we already showed that \texttt{Immutable} \( \preceq u_i \). Otherwise \( \{u_i / x\} S_j = S_1 \), and we will show that \texttt{Immutable} \( \preceq S_1 \) by showing that \( S_1 \neq \texttt{Mutable} \) and \( S_1 \neq \texttt{NoVariant} \). According to rule \texttt{MC1} in Fig. 11, if \( S_1 = \texttt{NoVariant} \), then \texttt{NoVariant}(X_i, C<X>). \texttt{This is a contradiction. We also have that } S_1 \neq \texttt{I} \text{ because from } \texttt{Immutable} \( \preceq u_i \) \text{ we have that } u'_i \neq I \text{ and thus } V \text{ cannot contain } I \text{ as a free variable. From the induction we have } \{u_i / x\} S_j \preceq \{u'_i / x\} S_j. \text{ Finally we have that } \texttt{CoVariant}(Y_j, A<Y>) \text{, because, if } \texttt{NoVariant}(Y_j, A<Y>) \text{, according to rule } \texttt{MC2} \text{ in Fig. 11, we have the contradiction } \texttt{NoVariant}(X_i, C<X>). \]

It is easy to add covariant fields to FIGJ without breaking type-safety, because FIGJ does not include field assignment. Lem. 5.3 proves that whenever it is possible to assign to a field, it is never covariant. Intuitively, in a legal assignment \( e_1.f = e_2 \), where \( e_1 : T \), we have that \( T \vdash \text{Mutable} \), and we will show that in all subtypes \( T' \preceq T \) the field \( f \) has the same type.

Lemma 5.3. Let \( \Delta \vdash T \preceq T', f' \preceq f \in \texttt{fields}(\texttt{bound}(\Delta)(T')) \), \( F \preceq F'' \). Then \( F = F'' \).

Proof. By induction on the derivation of \( \Delta \vdash T \preceq T' \), similarly to Lemma A.2.8 in [19]. Because \( I(T') = \text{Mutable} \), we also have that \( I(T) = \text{Mutable} \), and whenever rule \texttt{s1} is applied, it can never be that \( I(T) \preceq \text{Immutable} \), \( T' \), thus we need to consider the same set of subtyping rules as in FGJ.

5.3 FIGJ Expressions

Fig. 13 presents the type checking rules in FIGJ. Rule \texttt{T-Field-Set} ensures that only a mutable reference can assign to a field.
Theorem 5.6. The only change from the proof in FIGJ is the extension. Then either

Suppose \( \Delta \vdash \text{IELD} \) and \( \Delta, S \vdash e : T \). Then \( \exists e' \) such that \( \Delta \vdash e' : T' \) and \( \Delta, S \vdash e' : T' \).

Proof. From Thm. 5.4 we have \( \Delta \vdash T \leq T \) and thus \( \Delta \vdash I(T) \leq I(T) \).

6. Future Work

We plan to add several features to the IGJ compiler, such as:
(i) a warning if this escapes (see Remark 2.2), (ii) field initializers in which this is mutable if all constructors are mutable, and (iii) a mechanism to suppress specific warnings such as @SuppressWarnings("object-cast"). Similarly to tools for inferring generic arguments, immutability annotations can also be produced automatically. A plugin for an IDE such as Eclipse may also increase adoption of IGJ. We mention four other areas for future work: a default for type-variables, an alternative syntax, runtime support, and a write-only immutability parameter.

IGJ’s syntax does not permit defining a default value for the immutability parameter. For example, in Java fields are immutable by default, and everything else is mutable by default. We propose to extend Java syntax to allow declarations such as

class Graph\{extends ReadOnly default Immutable

One drawback is that if a different default is chosen in a subclass, we can have non-intuitive errors. For instance, consider Graph3D which is by default immutable:

class Graph3D\{Implements\{ReadOnly default Immutable\}

A different alternative syntax can come from Java’s annotations, however, currently, they cannot appear on any use of a type. JSR 308 [15] proposed for Java 7 allows annotations to be used practically anywhere, e.g., @Immutable Document[@ReadOnly] and new @mutable ArrayList<@immutable Edge>(...).

A type can have four types of annotations: @Immutable, @Mutable, @ReadOnly, and @ThisMutable. Instead of using a generic method to abstract over the immutability parameter (like in line 18 of Fig. 4), we can use this.

Currently no representation of immutability exists at runtime. Java does not support check casts involving generics, (e.g., casting a vector of objects to a vector of integers always succeeds), so safe down-casting is not feasible.

In Javari [32] the following mechanism is suggested to safely cast a readonly reference to mutable, while still preventing side effects through the mutable reference. We set a bit in that reference which is checked before every mutating operation. That bit is propagated during reference assignment and when copying a reference to a field.

A different runtime mechanism is using a readonly proxy, i.e., adding to Object the method:

\(@ReadOnly Object<Mutable> Object.createReadOnlyProxy()\)

That is similar in spirit to Java’s methods
even in a writeonly type. The following example of a

\[
\begin{align*}
1 \notin \text{dom}(S) & \quad S = S[1 \mapsto N(1)] \\
\text{new } N(1), S \rightarrow 1, S' & \quad \text{(R-NEW)} \\
S[1] = N(1) & \quad \text{fields}(N) = T \\
1.f, S \rightarrow 1, S & \quad \text{(R-FIELD)} \\
S[1] = N(1) & \quad \text{Mutable fields}(N) = T \\
1.f = 1, S \rightarrow 1', S' & \quad \text{(R-FIELD-SET)} \\
S[1] = N(1) & \quad mbody(m<N, N> = x.e \\
1.m\langle x\rangle(1), S \rightarrow 1/x, 1/this|x|e, S & \quad \text{(R-METHOD)} \\
S[1] = N(1) & \quad N \subseteq P \\
(P)1, S \rightarrow 1, S & \quad \text{(R-CAST)} \\
\end{align*}
\]

\[S(l) = I_x[1] \Rightarrow S[l] = I_x[1'] \Rightarrow S[l] = I_x[1''] \Rightarrow \cdots \]

\[\text{double } l[l] = s[l] \]

\[\text{Collections.unmodifiable\{Set.List\}, etc.} \]

Figure 15. The type hierarchy for immutability parameters of

\begin{align*}
\text{None} \\
\text{WriteOnly} \\
\text{Readonly} \\
\text{AssignsFields} \\
\text{Immutable} \\
\text{Mutable}
\end{align*}

Fig. 6 extended with WriteOnly and None.

The IGJ compiler will automatically override this method in sub-
classes, covariantly changing the return type. The implementation
will return a new mutable object, but all mutating methods are over-
ridden to raise an exception. The compiler should issue a warning
if any fields are public, because they can be mutated directly, by-
passing the proxy protection.

Another challenge remaining is building an immutable cyclic
data-structure, because that requires setting at least one reference
after an immutable object has been created. A similar challenge ex-
ists in the staged initialization paradigm in which the object’s con-
struction continues after the constructor finished. Such challenges
can be solved using a different runtime operation that converts a
mutable object into an immutable one, i.e., not simply returning
an immutable shallow proxy but modifying the object and all its
fields which are this-mutable. Because it is impossible to inval-
idate all existing mutable references, the runtime system needs to
modify the virtual table and replace mutating methods by methods
that raise an exception (similarly to the proxy technique). In or-
der to make this technique thread-safe, this operation will require
similar synchronization as done at the end of a constructor (see Re-
mark 2.2).

IGJ can be extended with a writeonly notation as well, as can be
seen in Fig. 15. The parent of both WriteOnly and ReadOnly
is None which denotes a type that have neither read nor write
privileges. In a similar way that a readonly type can be changed
co-variantly, a writeonly type can be changed contra-variantly.

Similar to the assignable annotation for fields, we can add a
readonly annotation to denote that a field can always be read,
even in a writeonly type. The following example of a Vector class
shows where WriteOnly can be used:

```java
class Vector<T> extends None, T {
    @Readonly int size; ...
    @None int size() { return size; }
    @WriteOnly void add(T t) { ... }
    @WriteOnly void removeLast() { ... }
    @Mutable void remove(T t) { ... }
    @ReadOnly void get(int index) { ... }
}
```

Further research is needed to determine if the benefits outweigh the
increased complexity.

7. Conclusions

This paper presented Immutable Generic Java (IGJ), a design
for adding reference and object immutability on top of the exist-
ing generic mechanism in Java. IGJ satisfies the design principles
in Sec. 1: transitivity, static checking, polymorphism, and simplic-
ity. IGJ provides transitive immutability to protect the entire ab-
stract state, and one can control this transitivity by using multiple
immutability parameters, e.g., using different immutability for the
container and its elements. IGJ is purely static, incurring no run-
time penalties. IGJ does not lead to code duplication because it
supports a high degree of polymorphism using covariant subtyping
(Def. 2.1), and it is also possible to use generic methods to abstract
over the immutability parameter. Finally, IGJ is simple, does not
require changing Java’s syntax, and has a small number of type-
checking rules.

References

Finding the needles in the haystack: Generating legal test inputs for
[4] J. Boyland. Why we should not add readonly to Java (yet). In
FTTJP, July 2005.
generalisation of uniqueness and read-only. In ECOOP, pages 2–27,
future safe for the past: Adding genericity to the Java programming
[7] L. Burdy, Y. Cheon, D. Cok, M. D. Ernst, J. Kiniry, G. T. Leavens,
K. R. M. Leino, and E. Poll. An overview of JML tools and


A. Igarashi, B. C. Pierce, and P. Wadler. Featherweight Java: a minimal core calculus for Java and GIAC. ACM TOPLAS, 23(3):396–450, May 2001.


