An Interval-based Inference of Variant Parametric Types *

Florin Craciun¹, Wei-Ngan Chin², Guanhua He¹, and Shengchao Qin¹

¹ Department of Computer Science, Durham University, UK
² Department of Computer Science, National University of Singapore, Singapore

Abstract. Variant parametric types represent the successful integration of subtype and parametric polymorphism to support a more flexible subtyping for Java-like languages. A key feature that helps strengthen this integration is the use-site variance. Depending on how the fields are used, each variance denotes a covariant, a contravariant, an invariant or a bivariant subtyping. By annotating variance properties on each type argument to a parametric class, programmers can choose various desirable variance properties for each use of the parametric class. Although Java library classes have been successfully refactored to use variant parametric types, these mechanisms are often criticized, due to the difficulty of choosing appropriate variance annotations. Several algorithms have been proposed for automatically refactoring legacy Java code to use generic libraries, but none can support the full flexibility of the use-site variance-based subtyping. This paper addresses this difficulty by proposing a novel interval-based approach to inferring both the variance annotations and the type arguments. Each variant parametric type is regarded as an interval type with two type bounds, a lower bound for writing and an upper bound for reading. We propose a constraint-based inference algorithm that works on a per method basis, as a summary-based analysis.

1 Introduction

Recently, several mainstream object-oriented languages, such as Java and C#, have successfully integrated traditional subtype polymorphism and parametric polymorphism to support better type-safe reusable code with significant reduction of runtime cast operations. Subtype polymorphism is a nominal relation, based on a given class hierarchy. Parametric polymorphism allows a data or a function to be parameterized by types and supports structural subtyping [1]. In handling objects with mutable fields, a crucial feature that helps strengthen the integration of subtype and parametric polymorphism is the adoption of variance. Variance annotations predict the flow of values for fields and provide a richer subtyping hierarchy. Depending on how the fields are being accessed, each variance denotes a covariant, a contravariant, an invariant or a bivariant subtyping. Generics types of Java 5 (also called Wildcard Types) [23, 24, 12] are based on the variant parametric types (or VPTs) [14]. VPTs is based on use-site variance whereby each use of a class type is marked with suitable variances that indicate how the fields are to be accessed.

* The work is supported in part by the EPSRC project EP/E021948/1.
Variant Parametric Types. Consider a variant parametric class Pair with two fields which are captured as type parameters:

```java
class Pair(A, B) { A fst; B snd; ... }
```

Assume three methods to retrieve the first field, to set the second field and to swap the two fields for a Pair object. In these methods, the parameter this is the Pair object whose variant parametric type must be provided with suitable variances. The type of this parameter is specified prior to delimiter ‘|’ (as in [4]):

```java
Pair(⊕A, ⊖) | C getFst(A, C) where A<:C { return this.fst; }
Pair(⊖, ⊖B) | void setSnd(B, C y) where C<:B { this.snd=y; }
Pair(⊖A, ⊖B) | void swap(A)(){A y = this.fst; this.fst = this.snd; this.snd = y; }
```

As can be seen, four kinds of variance annotations (denoted by α) are possible: (i) α = ⊗ captures a flow-out from the field to support covariant subtyping; (ii) α = ⊖ captures a flow-in to the field to support contravariant subtyping; (iii) α = ⊖ captures both flow-in and flow-out to support invariant subtyping; and (iv) α = ⊖ captures no access for the field to support bivariant subtyping. For simplicity, ⊖t can be abbreviated as ⊖. More generally, given an object with variant parametric type c₁(α₁t₁), we may pass it to a location with type c₂(α₂t₂), in accordance with the following subsumption relations:

```
\[
\begin{align*}
\frac{c_1 < c_2}{c_1(\alpha_1 t_1) < c_2(\alpha_2 t_2)} && (\alpha_1 <: \odot) \frac{\alpha_1 t_1 = t_2}{\alpha_1 <: \odot t_2} && (\alpha_1 <: \odot \land t_1 <: t_2) \lor t_2 = \text{Object} \\
\frac{\alpha_1 t_1 <: \odot t_2}{\alpha_1 t_1 <: \odot t_2} && (\alpha_1 <: \odot \land t_2 <: t_1) \lor t_2 = \bot
\end{align*}
\]
```

The bottom of the class hierarchy is ⊥ denoting the type of null value, while the top of the class hierarchy is Object. For simplicity, the first rule assumes that each class constructor has only a single inheritable type parameter. The above rules use nominal subtyping c₁ < c₂ from traditional class hierarchy and also a reflexive and transitive variance subtyping with a simple hierarchy: ⊖ < ⊖ < ⊖ < ⊖ < ⊖. The < operator is overloaded to handle variance subtyping, nominal class subtyping and two VPT subtypings for τ and ατ, respectively. The above subsumption relations form the basis of the VPT system to provide a richer subtyping system. Two provisos highlighted in the above rules for parametric fields are (i) to allow each such field to be retrievable as an Object, and (ii) a null value (of ⊥ type) to be written into any such field, regardless of its variant annotation. Types ⊖Object and ⊖⊥ are essentially equivalent to ⊖.

Motivation. Although VPT mechanisms have now been validated in the full-scale implementation of Java 5 [12] and Java library classes have been successfully refactored to use variant parametric types, these mechanisms are often criticized, due to the difficulty of choosing appropriate variance annotations. By annotating variance properties on each type argument to a parametric class, programmers can choose various desirable variance properties for each use of the parametric class. For example, the types Pair(⊕A, ⊖B) or Pair(⊖A, ⊖B) are still correct types for the receiver of the above method getFst. However, the best generic type is Pair(⊖A, ⊖), since the first field is read and the second field is not accessed. In order to establish the most flexible correct variance annotations (those which do not restrict the code genericity) for a type declaration, the programmer has to analyse all the places where that type declaration is used in the program. Although several algorithms have been proposed for refactoring legacy Java code [9, 8, 7, 11], they are restricted either to parametric types [1] or to variant parametric types with known variance annotations. No one can support the full flexibility of the use-site variance-based subtyping. Moreover these algorithms require global analysis.
**Contributions.** We propose a novel approach to automatically inferring the variance annotations and the type variables for the variant parametric types of method parameters (including receiver), method result and method body’s local variables. In addition, the expected value flow that may arise from the method body is captured as a precondition. The inference is designed as a *summary-based analysis* that works on a per method basis: the variant parametric types of a method are inferred only based on how they are used in the method body, while each call site is a specific instance of the method’s type declaration. Our inference is guided by a dependency graph such that all the methods which are called by the current method have been already analyzed. Our inference also assumes that the generic class hierarchy is known. In order to support the full flexibility of the subtyping based on the use-site variance, our inference algorithm starts with unknown variance annotations. Each variant parametric type is represented as an *interval type* [2], namely two type bounds that allow us to distinguish a *read flow* from a *write flow* for each object’s field. Based on a flow-based approach for VPTs [4], we reduce the problem of inferring variance annotations and type arguments to the problem of solving specialized flow constraints. To the best of our knowledge this is *the first algorithm* that decouples variance inference from the type inference itself. In order to allow more generic types for the method parameters we introduce *dual types* to support *unknown variance flow*. Dual types make a distinction between flow via an object, *object flow* and the flow via the object’s fields, *field flow*. We also use *intersection and union types* to capture the *divergent flow* and *convergent flow*, respectively. A safe yet precise approximation is used to avoid disjunctive constraints. We also provide special solutions to handle runtime cast operations and method overriding.

**Related Work.** The task of introducing generics to an existing Java code [9, 8, 7, 11, 16] consists of two distinct problems, parameterization and instantiation. Class parameterization selects the class fields that can be promoted as class type parameters. Since class parameterization decisions may be quite hard to automate due to trade-offs in the possible design outcomes, our solution is to let programmers focus on high-level design decisions for parameterization, while leaving the more tedious annotations on value flows of methods to be automatically inferred. Previous algorithms for instantiation have been restricted to parametric types based on invariant subtyping [9, 8, 7, 11]. Although the most recent Java refactoring paper [16] claims being able to infer wildcard types, it conservatively assumes invariant subtyping even with wildcard types.

At each call site, Java compiler [12] performs a local inference of the method’s type parameters. The algorithm follows the local type inference designed for parametric types [17]. Recently, a significant revision of Java local inference has been proposed in [21]. The new proposal has introduced two bounds for a type variable similar to our interval types. However it does not perform variance inference since the variance annotations are known. Our approach is more general and subsuming the local type inference.

Our variant parametric type inference algorithm produces subtyping (flow) constraints. To solve them, we work on a closed constraint graph employing techniques from [25, 18, 22, 10]. It seems also possible to formalize our constraint solver on a pre-transitive graph [13] to have a more scalable implementation. In general the constraint solving techniques assume that the polarities of term constructors are known. However the inference of variant parametric types may generate term constructors with un-
known polarities (variances). Therefore our approach uses an interval type (a contravariant lower bound and a covariant upper bound) to represent each unknown polarity of a term constructor. The idea of using interval types for updatable values has already been applied to reference type [20, 19] and also in the context of object calculi [2]. An open problem (discussed in [2]) is whether the interval types can be used to infer types with variance information from non-annotated terms. Our variance inference provides a constraint-based solution to this open problem.

Outline. The following section presents our interval-based view of VPTs. Section 3 introduces the key features of our approach. Section 4 formalizes our inference algorithm. Section 5 solves the method overriding problem. A brief conclusion is then given.

2 Variant Parametric Types as Interval Types

The underlying idea behind our solution is to view each variant parametric type $\alpha X$ as an interval (of types) with a low-bound $X_L$ and a high-bound $X_H$ such that $X_L < X_H$. The low-bound variable captures each value of type $t_1$ that may flow into $\alpha X$ using the constraint $t_1 < X_L$, while the high-bound variable captures each value of type $t_2$ that may flow out of $\alpha X$ using $X_H < t_2$. By default, it is always safe for each low-bound $X_L$ to be bounded by $\bot < X_L$ and each high-bound can be bounded by $X_H < \text{Object}$. For example, given a variant parametric type $c(\alpha X)$ (where $X$ is a type variable) denoting a class with a field of type $\alpha X$, it can always be translated into an interval type as follows:

<table>
<thead>
<tr>
<th>$X = X_H$</th>
<th>$X = X_L$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$c(\bot X) \iff c(\bot, X_H)$</td>
<td>$c(\bot X) \iff c(\bot, X_L)$</td>
</tr>
<tr>
<td>$c(\rho X) \iff c(\bot, \text{Object})$</td>
<td>$c(\rho X) \iff c([X, X])$</td>
</tr>
<tr>
<td>$X_L = \text{fresh}()$</td>
<td>$X_H = \text{fresh}()$</td>
</tr>
</tbody>
</table>

Translation rules are bidirectional where the variance is known. The last rule is a key rule for variance inference, as it splits a type variable with an unknown variance into two type variables. Thus, field selection (reading) uses the type $X.H$, while field updating (writing) is based on type $X.L$.

The interval type subtyping subsumes VPT subtyping and is defined as a contravariant subtyping on low-bounds and a covariant subtyping on high-bounds, as follows:

$$c_1 <: c_2 \quad t_2.L <: t_1.L \quad t_1.H <: t_2.H \quad \Rightarrow \quad c_1([t_1.L, t_1.H]) <: c_2([t_2.L, t_2.H])$$

The annotations $L$ and $H$ make a flow-based distinction among the types, such that:

- $X.L$ denotes a type that expects a write flow (flow in),
- $X.H$ denotes a type that expects a read flow (flow out),
- $X$ (without annotation) denotes a type that expects both read and write flows.

Using the flow expectations, we identified a special group of flow constraints that we called closed flow constraints. They denote a matching of a flow-out with a flow-in, namely a consumption of a read flow by a write flow.

Definition 1 (Closed Flow Constraint). A closed flow constraint is a flow constraint that has one of the following forms: $X.H <: X_2.L$, $X.H <: X_2$, $X_1 <: X_2.L$, and $X_1 <: X_2$, where $X_1, X_2$ are different from Object and $\bot$.

Proposition 1 (Variance Inference Rule-1). If a low-bound type variable $X.L$ does not occur in any closed flow constraint, it is resolved to be $\bot$. If a high-bound type variable $X.H$ does not occur in any closed flow constraint, it is resolved to be Object.
3 Inference of Variant Parametric Types

3.1 Main Algorithm

This section illustrates the main steps of our inference algorithm using the following method of a non-generic Pair class:

Pair | Object move(Pair a) { Object y = a.getFst(); this.setSnd(y); return y; }

Our goal is to infer its generic version that corresponds to the variant parametric class Pair(A, B). Internally, our algorithm works with interval types to generate and solve the flow constraints. Therefore, we use the following interval type based specifications of the methods getFst and setSnd of the variant parametric class Pair(A, B):

Pair([⊥, A.H], [⊥, Object]) | C getFst(A.H, C)() where A.H <: C {}
Pair([⊥, Object], [B.L, Object]) | void setSnd(B.L, C)(C y) where C <: B.L {}

Step 0. Decoration with Fresh Interval Types. This is a pre-processing step. It consists of the annotation with fresh type variables of the non-generic types and non-generic methods. We use the following naming conventions: the letters \( V_i \) for the global type variables (visible outside the method), the letter \( Y \) for the method result, the letters \( N_i \) for the arguments of new expressions, and the letters \( T_i \) for other annotations:

Pair([\( V_1 \), L, H], [\( V_2 \), L, H]) | Y move(Pair([\( V_3 \), L, H], [\( V_4 \), L, H]) a)
\( \{T_0 \ y = a . \text{getFst} (T_1, T_2)(); \ \text{this.setSnd}(T_1, L, T_4)(y); \ \text{return} \ y; \} \)

Step 1. Collect Flow Constraints. This step gathers the constraints from the method body using the type inference rules given in Section 4.1, as follows:

Pair([\( V_1 \), L, H], [\( V_4 \), L, H]) <: Pair([\( ⊥ \), \( T_1 \), H], [\( ⊥ \), Object]) \& \( T_1, H <: T_2 \land T_2 <: T_0 \land T_0 <: T_3 \land T_3, L \land \) Pair([\( V_1 \), L, H], [\( V_2 \), L, H]) <: Pair([\( ⊥ \), Object], [\( T_3 \), L, Object]) \land T_0 <: Y

Step 2. Simplify Flow Constraints. This is a closure algorithm that iteratively decomposes the constraints into their elementary components. It primarily applies the interval subtyping rules with transitivity. The closure algorithm is invoked each time a new constraint is added to the set. For brevity, in the following examples, we omit the transitivity and the default constraints like \( ⊥ <: X, X <: \text{Object}, \) and \( X.L <: X.H. \) The result of this step is the following:

\( V_3, H <: T_1, H \land T_1, H <: T_2 \land T_2 <: T_0 \land T_0 <: T_3 \land T_3, L \land T_3, L <: V_3, L \land T_0 <: Y \)

Step 3. Variance Inference. This step generates a set of closed flow constraints and then applies the variance inference rule from Section 2. Since \( V_1, L, V_4, L, V_3, H, V_2, H, V_3, L \) do not occur in any closed flow constraint, they are accordingly solved as follows:

\( V_1, L = ⊥ \land V_1, H = \text{Object} \land V_4, L = ⊥ \land V_4, H = \text{Object} \land V_2, H = \text{Object} \land V_3, L = ⊥ \)

Step 4. Type Variables Inference. This step solves the type variables \( T_i, N_i, \) and \( Y \) in term of the global type variables \( V_i \) and ground types (which are types without type variables). It consists of three substeps:

1. Cycle elimination: This causes all type variables of a cycle to be equal. Note that there isn’t a cycle in the current example.
2. Ordering: The type variables are ordered based on the number of constraints in which they appear as an upper bound.
3. Unification: Following the order defined before, the type variables are solved by equating to their low bounds. Type variables occurring in fewer constraints have a higher priority.
For our example, the result of the unification is summarized by the last column of the following table. The first column contains the constraints in which the type variables from the second column occur as upper bounds. Multiple type variables in the second column denote type variables having the same priority.

<table>
<thead>
<tr>
<th>Constraints</th>
<th>TVars</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>V₃,H:&lt;T₁,H</td>
<td>{T₁,H}</td>
<td>T₁,H:=V₃,H</td>
</tr>
<tr>
<td>V₃,H&lt;T₂&lt;T₁,H&lt;H&lt;T₂</td>
<td>{T₂}</td>
<td>T₂:=V₃,H</td>
</tr>
<tr>
<td>V₃,H&lt;T₀&lt;T₁,H&lt;T₀&lt;T₂&lt;T₀</td>
<td>{T₀}</td>
<td>T₀:=V₃,H</td>
</tr>
<tr>
<td>V₃,H&lt;T₄&lt;T₃,H&lt;T₄&lt;T₅&lt;T₂&lt;T₄&lt;T₀&lt;T₄&lt;T₀&lt;T₀</td>
<td>{T₄,Y}</td>
<td>T₄:=V₃,H</td>
</tr>
<tr>
<td>V₃,H&lt;T₁,H&lt;T₂&lt;T₀&lt;T₄&lt;T₃,L</td>
<td>{T₃,L}</td>
<td>T₃,L:=V₃,H</td>
</tr>
</tbody>
</table>

**Step 5. Result Refining.** This step simplifies the inferred types of the method. The goal is to reduce the number of the global type variables using the residual flow constraint (namely the remaining flow constraints among the global type variables). The residual flow constraint of the current example is: V₃,H:<V₂,L. These type variables can be unified to a fresh type variable V, such that V:=V₃,H:=V₂,L. Since V stands for both low-bound and high-bound, it is not marked with either. The result of our inference (including the above refinements) is the following:

```java
Pair([⊥, Object], [V, Object]) | V.move(V)(Pair([⊥, V], [⊥, Object]) a)
{V y=a.getFst(V, V); this.setSnd(V, V)(y); return y; }
```

**Step 6. VPT Result.** This step translates the inferred interval types into VPTs:

```java
Pair(⊕, ⊙V) | V.move(V)(Pair(⊕V, ⊙V) a)
{V y=a.getFst(V, V); this.setSnd(V, V)(y); return y; }
```

### 3.2 Interval Types versus Variant Parametric Types

The interval types are more expressive than variant parametric types, since they can support two different non-default bounds. A variant parametric type can only support two equal non-default bounds in the case of invariant subtyping ⊙. Note that the default low-bound is ⊥, while the default high-bound is Object. Considering the following code fragment, we like to infer the interval type of `obj`:

```java
class Cell(A) { A fst; ... } class Cell(Integer) extends Number{
    Cell(⊕A) | A.get(A)();
    Cell(⊙A) | void.set(A, y)();
    ... Cell([T.L, T.H]) obj = new Cell(Integer)(new Integer(1)); // T.L:<Integer:<T.H
    Number n = obj.get(T₃());           // T.H:<T₁:<Number
    MyInt m = new MyInt(2); obj.set(T₂)(m); // MyInt:<T₂:<T.L
```

Our algorithm can infer the interval type Cell([MyInt, Number]) for `obj`. However this interval type cannot be translated into a variant parametric type, since it consists of two different bounds. In order to keep the equivalence between interval types and variant parametric types, we add one more rule to the variance inference:

**Proposition 2 (Variance Inference Rule-2).** If both bounds X.L and X.H of an interval type occur in the closed flow constraints, then the default constraint of an interval type X.L<X:H is strengthened to the equality X.L=X.H.

In our example, adding T.L=T.H to the above set of constraints will generate a cycle such that T.L:<Integer:<T.H ∧ T.L=T.H. Cycle elimination generates T.L= Integer=T.H. Thus new inference result is the interval type Cell([Integer, Integer]), that can be directly translated into the variant parametric type Cell(⊙Integer).
3.3 Main Flow and Conditional Flow

Cast operations give rise to conditional flow constraints (or dynamic subtype constraints in [9]). These constraints are conditional in the sense that they are only required to hold if the corresponding dynamic downcasts succeed at runtime. Our analysis separates the main flow gathered from the method body without the cast operations and the conditional flow corresponding to the cast operations. Conditional constraints use a different subtyping notation (\(<\,.\>\). One benefit of our analysis is that it can guarantee that some of the cast operations are redundant, and therefore they can be safely eliminated at compile time. The number of the eliminated casts is used as an accuracy measure of generic type systems [8, 11, 4, 16]. The following example illustrates how our inference algorithm handles the cast operations:

<table>
<thead>
<tr>
<th>Original code</th>
<th>Inference Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>`Cell</td>
<td>void fill(Cell a) {Cell b = (Cell)a.fst:b.fst = this.fst; }`</td>
</tr>
</tbody>
</table>

Code annotated with Fresh Interval Types

| Cell(|V,L1|V,H|) | void fill(Cell(|V,2,L2|V,H|) a) {Cell(|T1,L1,T1,H|) b = (Cell(|T2,L2,T2,H|)|a.fst:b.fst = this.fst; } |

1. Collect

\(Cell(|T2,L,T2,H|) < \odot Cell(|T1,L,T1,H|) \land V_1 < \odot T_1\)

2. Simplify

\(V_1 < \odot T_1 < \odot T_2 \land T_2 < \odot T_1\)

3. Infer

\(V_1 < \odot T_1 < \odot T_2 \land T_2 < \odot T_1\)

4. Infer

\(\{T1,L\} < \odot T1,L = V1,H\)

Type Vars

\(\{T2,L\} < \odot T2,L = V1,H\)

5. Solve Conditional

\(V_2, H < \odot Cell(|V1,H, Object|) \Rightarrow V_2, H < \odot Cell(|V, H, Object|)\)

6. Refine Results

\(V = fresh\) \(\land V_1 = V \land V_2 = \odot Cell(|V, H, Object|)\)

Though the conditional flow is kept separately, it is still used by the variance inference in Step 3. If Step 3 ignores the conditional flow, it infers the incorrect result \(V_2,H = Object\). A new step (Step 5) is added to the main algorithm. This step combines together the conditional flow and the (already solved) main flow in order to find a common solution. In our example, adding the conditional constraint to the main flow does not generate any contradiction as the type variables \(V_2,H\) and \(V_1\) are unconstrained in the main flow. However it is not always possible to find a common solution for the main and conditional flow, as illustrated by the following example:

```java
V(oo2(Cell(|V4,L,V4,H|) obj) {...}
    if (...) {... return (Integer)obj.fst; } else {... return (Float)obj.fst; }
//Integer <\odot V3<\odot Float<\odot V4,V4,H<\odot Integer<\odot V4,H<\odot Float
```

In this example the conditional constraints can be added to the method precondition to be checked at each call site where the casts could be selectively eliminated (with the help of a polyvariant program specializer):

```java
Number foo2(Cell(|\(\bot\),V4,H|) obj) where V4,H<\odot Integer<\odot V4,H<\odot Float
```

3.4 Convergent Flow and Divergent Flow

Multiple low bounds denote a convergent flow, while multiple high bounds denote a divergent flow. Our analysis uses union types for multiple low bounds and intersection types for multiple high bounds. An union type \(\tau_1|\tau_2\) represents the least upper bound
of \( t_1 \) and \( t_2 \), while an intersection type \( t_1 \land t_2 \) is the greatest lower bound of \( t_1 \) and \( t_2 \). Some of their subtyping rules may generate disjunctions. In order to keep our analysis simple, we propose a safe yet precise approximation that avoids those disjunctions:

\[
\begin{align*}
\text{AND rules} & \quad \text{OR rules} & \quad \text{Our OR rules} \\
\text{t}_1 \land \text{t}_2 \leq \text{t} & \quad \text{t} \leq \text{t}_1 \lor \text{t} \leq \text{t}_2 & \quad \text{t} \leq \text{t}_1 \land \text{t}_2 \land \text{t} \leq \text{t}_1 \\
\text{t} \leq \text{t}_1 & \quad \text{t} \leq \text{t}_2 & \quad \text{t} \leq \text{t}_1 \land \text{t}_2 \land \text{t} \leq \text{t}_2 \\
\text{t} \leq \text{t}_1 \land \text{t} \leq \text{t}_2 & \quad \text{t} \leq \text{t}_1 & \quad \text{t} \leq \text{t}_1 \land \text{t}_2 \land \text{t} \leq \text{t}_2
\end{align*}
\]

where \( T_1 \) and \( T_2 \) are fresh type variables. Another solution to avoid disjunctions is the tautology \( t_1 \land t_2 \leq t_1 \lor t_2 \), but sometimes this approximation may lead to no solutions. One benefit of using union and intersection types is that they are more expressive so that more casts can be directly eliminated as the following example (from [8, 4]) can illustrate:

```java
class B1 extends A implements I {...}; class B2 extends A implements I {...};

Original code
void foo(Boolean b){
    Cell c1 = new Cell(new B1());
    Cell c2 = new Cell(new B2());
    Cell c = b?c1 : c2;
    A a = (A)c.get();
    I i = (I)c.get();
    B1 b1 = (B1)c1.get();
    B2 b2 = (B2)c2.get();
}

Code annotated with Fresh Interval Types
void foo(Boolean b){
    Cell c1 = new Cell(new B1());
    Cell c2 = new Cell(new B2());
    Cell c = b?c1 : c2;
    A a = (A)c.get();
    I i = (I)c.get();
    B1 b1 = (B1)c1.get();
    B2 b2 = (B2)c2.get();
}
```

The following table contains the inference steps for the above code with interval types. At the step 4.4, \( T_1, H \) is resolved as to the union type \( B1 \mid B2 \) due to two distinct flows converging to it, \( B1 <: T_3, H \land B2 <: T_3, H \). The solutions of the main flow can prove that all conditional constraints succeed, and therefore all casts can be eliminated.

<table>
<thead>
<tr>
<th>Step</th>
<th>Collect Constraints</th>
<th>Simplify</th>
<th>Infer Variance</th>
<th>Type Vars</th>
<th>Solve</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( B1 \leq N_1 \land \text{Cell}(N_1, N_1) \leq \text{Cell}(T_1, L, T_1) \land \text{Cell}(T_2, L, T_2) )</td>
<td>( B1 \leq N_1 \land \text{Cell}(N_1, N_1) \leq \text{Cell}(T_1, L, T_1) \land \text{Cell}(T_2, L, T_2) )</td>
<td>( T_1 \not\leq \text{Cell}(T_3, H) \land T_2 \not\leq \text{Cell}(T_3, H) )</td>
<td>( T_1 \not\leq \text{Cell}(T_3, H) \land T_2 \not\leq \text{Cell}(T_3, H) )</td>
<td>( B1 &lt;: A \land T_3 &lt;: I \land T_6 &lt;: B1 \land T_7 &lt;: B2 )</td>
</tr>
<tr>
<td>2</td>
<td>( B2 &lt;: N_2 \land \text{Cell}(N_2, N_2) \leq \text{Cell}(T_1, L, T_1) \land \text{Cell}(T_2, L, T_2) )</td>
<td>( B2 &lt;: N_2 \land \text{Cell}(N_2, N_2) \leq \text{Cell}(T_1, L, T_1) \land \text{Cell}(T_2, L, T_2) )</td>
<td>( T_1 \not\leq \text{Cell}(T_3, H) \land T_2 \not\leq \text{Cell}(T_3, H) )</td>
<td>( T_1 \not\leq \text{Cell}(T_3, H) \land T_2 \not\leq \text{Cell}(T_3, H) )</td>
<td>( B2 &lt;: A \land T_3 &lt;: I \land T_6 &lt;: B1 \land T_7 &lt;: B2 )</td>
</tr>
<tr>
<td>3</td>
<td>( T_1 =: T_2 =: T_3 =: I \land B1 &lt;: N_1 \land T_1, H \land B2 &lt;: N_2 &lt;: T_2, H )</td>
<td>( T_1 \not\leq \text{Cell}(T_3, H) \land T_2 \not\leq \text{Cell}(T_3, H) )</td>
<td>( T_1 \not\leq \text{Cell}(T_3, H) \land T_2 \not\leq \text{Cell}(T_3, H) )</td>
<td>( T_1 \not\leq \text{Cell}(T_3, H) \land T_2 \not\leq \text{Cell}(T_3, H) )</td>
<td>( B2 &lt;: A \land T_3 &lt;: I \land T_6 &lt;: B1 \land T_7 &lt;: B2 )</td>
</tr>
</tbody>
</table>

5. Solve \( B_1 \mid B_2 <: A \mid B_1 \mid B_2 <: A \)
3.5 Field Flow and Object Flow

A key feature of our approach is the distinction between the flow via an object, called object flow and the flow via the fields of that object, called field flow. We introduce a special type notation, that we called dual type to support these two views: (1) object as a black box, and (2) object as a glass box. For example, a dual type for a Pair is of the form $\mathsf{X} \vdash \mathsf{Pair}([V_1, L, V_t, H], [V_2, L, V_r, H])$, where the type variable $\mathsf{X}$ (called object part) is used for the flow of the entire object, while $\mathsf{Pair}([V_1, L, V_t, H], [V_2, L, V_r, H])$ (called field part) caters to the flow via its fields. This dualism can improve the generlicity of our inference results. Specifically, given the following method $\mathsf{dup}$ (from [4, 14]):

$$\mathsf{dup} \mathsf{Pair} \mathsf{a} \{ \mathsf{Pair} \mathsf{p} = \mathsf{new} \mathsf{Pair} \mathsf{a, return p}; \}$$

Without using the dual types, our inference can get the following types:

$$\mathsf{Pair} \mathsf{a} \{ \mathsf{Pair} \mathsf{p} = \mathsf{new} \mathsf{Pair} \mathsf{a, return p}; \}$$

The type of the method result is too imprecise, but still correct as fields are not accessed (bivariant $\odot$) in the method body. Using dual types our approach can get more precise types by inferring an intersection type for the method parameter $\mathsf{a}$, namely:

$$\mathsf{Pair} \mathsf{a} \{ \mathsf{Pair} \mathsf{p} = \mathsf{new} \mathsf{Pair} \mathsf{a, return p}; \}$$

The type variable $\mathsf{X}_i$ plays an important role, it allows the unknown variance to flow unchanged, such that the variance annotations of the parameter $\mathsf{a}$ fields are preserved in the type of the method result. As can be seen below, the type variable $\mathsf{X}_i$ comes from the object part of the dual type:

$$\mathsf{Y} \mathsf{dup} \mathsf{Pair} \mathsf{a} \{ \mathsf{Pair} \mathsf{p} = \mathsf{new} \mathsf{Pair} \mathsf{a, return p}; \}$$

1. Collect
2. Simplify
3. Simplify
4. Infer
5. Infer
6. Refine

A new step (Step 2) is added to the main algorithm in order to simplify the dual types. The simplification rules always prefer the object flow over the field flow (e.g. first constraint of Step 1 is reduced to $X_1 < N_1$). However, when the type variables of the field part are used by the other constraints, both flows are generated (e.g. the third constraint of Step 1 is decomposed into two constraints). The last step is adapted to refine the dual types. A dual type can be refined to an intersection type (e.g. first line of Step 6). Since an intersection type is the greatest lower bound of its parts, it could be further simplified (e.g. the second line of Step 6).
4 Inference Algorithm

We design our inference algorithm as a summary-based analysis, on a per method basis guided by a global method call graph. Our approach is flow-insensitive within each method, but context-sensitive across the methods. The algorithm takes as input a well-typed non-generic program and the VPT class hierarchy, before it outputs a program that uses VPTs.

We use two assumptions to avoid recursive constraints: (1) no F-bounded quantification over the VPT class hierarchy, and (2) no polymorphic recursion for the classes and the methods. Techniques for avoiding recursive constraints are presented in [4, 5]. Nevertheless, our algorithm can cope with F-bounds, as long as we use constraint solving techniques that support recursive constraints and inductive simplification (from [25, 18]). Our current approach can infer generic types for mutually-recursive methods under the monomorphic recursion assumption.

We formalize the algorithm on Variant Core-Java (Fig. 1), a core calculus for Java-like languages. Both input and output programs are encoded in Core-Java since VPTs can subsume non-generic types. For ease of presentation, the features related to static methods, exception handling, inner classes and overloading are omitted. Multiple interface inheritance is supported as in Java [12], each class may extend from a single super class but may implement multiple interfaces. VPT’s syntax is also shown in Fig. 1. There are two kinds of type variables: \( \kappa \) denoting a variance and a type together, and \( \nu \) denoting only a type. For simplicity, primitive types (e.g. bool, void) are represented by their corresponding classes (such as Boolean, Void). Specifically, for each method our analysis can be divided into two main steps: (1) gathering the flow constraints based on the type inference rules (Section 4.1), and (2) solving the flow constraints (Section 4.2).

4.1 Type Inference Rules

The inference process is driven by the following main rule for each method:

\[
G \vdash c_i \Rightarrow_{def} t_i \quad G; \{(v_i : t_i)_i\}_{i=2} \quad \text{this} : t_1 \vdash e \Rightarrow e' : t_1, \varphi_0 \quad Y = \text{fresh()} \quad Q_1 = \bigcup_{i=2}^{n} \varphi(v(t_i)) \quad G \vdash \varphi_0 \land t \land \nu ; Y : Q_1 \Rightarrow_{\text{solve}} \varphi(Q';\sigma) \quad \sigma(t_1 | \sigma Y \cup \{e\}) \quad G \vdash c_i [c_0 \quad \text{mm}((v_i)_i)]_{i=2} \quad \text{this} : t_1 \vdash e \Rightarrow \kappa_1 [\kappa \quad \text{mm}((\sigma Y)_i)]_{i=2} \quad \text{where} \ \psi \Rightarrow e''
\]

that takes a non-generic method and the VPT class hierarchy \( \mathcal{G} \), decorates the method parameters (\( \Rightarrow_{\text{def}} \)) with fresh interval types, collects the flow constraints (\( \Rightarrow_{\text{solve}} \)) from the method body, and then passes the constraints to the constraint solver (\( \Rightarrow_{\text{solve}} \)). The solver
Interval Type

\[ \tau ::= t \mid t.L \mid t.H \]

\[ t ::= X \mid d \mid e([\tau_{1L}, \tau_{1H}], \ldots, [\tau_{nL}, \tau_{nH}]) \]

\[ e ::= t_1 + t_2 \mid t_1 \mid \perp \mid Object \]

Dual Type

\[ d ::= X = e([\tau_{1L}, \tau_{1H}], \ldots, [\tau_{nL}, \tau_{nH}]) \]

Flow Constraint

\[ \varphi ::= \tau_1 = \tau_2 \mid \tau_1 < \tau_2 \mid \varphi \land \varphi \mid \text{true} \]

Substitution

\[ \sigma ::= X = \tau \mid X.L = \tau \mid X.H = \tau \mid d = t \]

Closed Flow Constraint

\[ \omega ::= t_1.H < t_2.L \mid t_1 < t_2.L \mid t_1.H < t_2 \]

\[ t_1.H < t_2.L \mid t_1 < t_2.L \mid t_1.H < t_2 \]

The goal is first to simplify the constraints \( \varphi \) to atomic constraints among type variables and ground types and then to solve the type variables in term of the ground type and the visible type variables \( \mathcal{Q} \). The result consists of a residual constraint \( \varphi \) among the visible type variables, a reduced set of type variables \( \mathcal{Q} \) and the solution itself given as a substitution \( \sigma \). Since our solver internally works with a set of constraints \( \mathcal{G} \) instead of a conjunction \( \varphi \), the judgments \( \Rightarrow_{\sigma} \) and \( \Rightarrow_{\mathcal{G}} \) make the corresponding translations. We summarize below the main steps of our solver (a complete description is in [5]).
Transitive Closure ($\Rightarrow_{tr}$). The constraint set is always closed by transitivity such that this step is performed each time a new constraint is added. The transitivity takes into account the conditional constraints, it generates a conditional constraint from a conditional constraint and non-conditional constraint. VPT subtyping (and also interval type subtyping) is transitive since the VPT class declarations are well-formed as in [15].

Simplification ($\Rightarrow_{simplify}$). It consists of a constraint decomposition $\Rightarrow_s$ followed by a transitive closure:

$$
\begin{align*}
G \vdash C_0 \Rightarrow_{simplify} C' & \quad \Rightarrow_{s} C'' \Rightarrow_{s} C \\
G \vdash C_0 \Rightarrow_{simplify} C
\end{align*}
$$

Constraint decomposition $\Rightarrow_s$ is performed with respect to the class subtyping given by the VPT class hierarchy $\mathcal{G}$, the interval subtyping rule and the subtyping rules for intersection and union types. Using the mechanism presented before the intersection and union type constraints always decompose into conjunctions. A conditional constraint is decomposed into new conditional constraints. The step is performed until the constraint set remains unchanged. In the solver, the first call of $\Rightarrow_{simplify}$ step decomposes the outermost intersection and union types to reduce the complexity of the step $\Rightarrow_{dual}$.

Dual Types Simplification ($\Rightarrow_{dual}$). It decomposes all the dual types from the input constraint set $C_0$. The result consists of a new constraint set $\mathcal{C}$ and the list of the decomposed dual types $D$:

$$
\vdash C_0 \Rightarrow_{dual} \mathcal{C} ; D
$$

The process is performed in two stages. In the first stage ($\Rightarrow_s$), all the flow constraints with dual types are decomposed. When it needs to choose, $\Rightarrow_s$ prefers the flow through the object part of a dual type rather than that through the field part. In the second stage ($\Rightarrow_{cd}$), the flow through the field part is selectively added to the constraint set when it is required by the other constraints.

Variance Inference ($\Rightarrow_{variance}$). It computes the high-bound type variables and the low-bound type variables that do not occur in the closed flow constraints, and resolves them to their default values by the substitutions $\sigma_{hl}$ and $\sigma_l$, respectively.

$$
\begin{align*}
L_H &= \{V.H \mid V.H < L_1 \in C_0 \vee V.H < L_2 \in C_0 \vee V.H < L_3 \in C_0 \vee V.H < L_4 \in \mathcal{C}_0 \} \\
L_L &= \{V.L \mid V.L < V.H \in C_0 \vee V.L < V.H \in C_0 \vee V.L < V.H \in \mathcal{C}_0 \vee V.L < V.H \in \mathcal{C}_0 \} \\
\sigma_H &= \{[V.H \rightarrow Object] \mid V.H \in \text{fv}(\mathcal{C}_0) \land V.H \notin \mathcal{L}_H \} \\
\sigma_L &= \{[V.L \rightarrow \bot] \mid V.L \in \text{fv}(\mathcal{C}_0) \land V.L \notin \mathcal{L}_L \} \\
\sigma_{HL} &= \{[V.H \rightarrow V, V.H \rightarrow V] \mid V.H \in \mathcal{L}_H \land V.L \in \mathcal{L}_L \} \\
Q &= \mathcal{Q}_0 \setminus \text{ran}(\sigma_{HL}) \setminus \text{dom}(\sigma_H) \cup \text{dom}(\sigma_L) \cup \text{dom}(\sigma_{HL}) \\
C &= \sigma_H \circ \sigma_L \circ \sigma_{HL} \circ C_0
\end{align*}
$$

The substitution $\sigma_{HL}$ implements the second variance inference rule, making equal the bounds of an interval when both of them occur in the closed flow constraints. The initial list of the visible type variables $Q$ can be affected by the variance inference. This step works on all constraints, either from conditional flow or from main flow.

Type Variables Inference ($\Rightarrow_{typvar}$). This step solves the non-visible type variables in terms of the visible type variables $Q_0$:

$$
\begin{align*}
\vdash C_0; Q_0 \Rightarrow_{cycle} C_1; Q_1; \sigma_1 & \quad \vdash C_1; Q_1 \Rightarrow_{order} L & \quad \vdash L; C_1 \Rightarrow_{typvar} C; \sigma_2 & \quad Q = Q_1 \cup \text{fv}(C) \\
\vdash C_0; Q_0 \Rightarrow_{typvar} C; Q; \sigma_2 \circ \sigma_1
\end{align*}
$$

First step $\Rightarrow_{cycle}$ makes equal all the type variables of a cycle. This process may also affect the visible type variables, resulting in a new set $Q_1$. We use techniques from [10]
to eliminate the cycles. The non-visible type variables are then solved \((\Rightarrow_{\text{unif}})\) in an order given by the number of their low bounds \((\Rightarrow_{\text{order}})\). The substep \(\Rightarrow_{\text{order}}\) iteratively computes the order taking into account the situations when the low bounds are class type parameterized with type variables. The substep \(\Rightarrow_{\text{unif}}\) unifies the type variables with their low-bounds producing a substitution \(\sigma_2\). Multiple low-bounds are combined together as an union type. Non-visible type variables of final constraint set \(\mathcal{C}\) are promoted as visible in \(\mathcal{G}\). Though this step works only on the main flow constraints, its computed substitutions are also applied on the constraints of the conditional flow.

**Solving conditional constraints** \((\Rightarrow_{\text{cond}})\). This step translates the conditional constraints into non-conditional constraints if the non-conditional constraints hold. Since it is always safe to add more constraints on the method interface type variables and the constraint set is transitively closed, this step only checks \(\langle\rightarrow\rangle\) the conditional constraints with the ground types with respect to the class hierarchy \(\mathcal{G}\). First check is for ground constraints, while the last two are to verify if an intersection and an union type can exist in \(\mathcal{G}\). If the checks do not hold, the conditional constraints are not translated.

\[
\begin{align*}
B = \{c_1 \ll c_2 \mid c_1 \ll c_2 \in C_0\} & \quad \Rightarrow_{\gamma} B \\
\forall V \in \text{ty}(C_0).G \Rightarrow \{c \mid V \ll c \in C_0\} & \quad \forall V \in \text{ty}(C_0).G \Rightarrow \{c \mid c \ll V \in C_0\} \\
C' = \{c_1 \ll c_2 \mid c_1 \ll c_2 \in C_0\} & \quad \Rightarrow_{\text{cond}} C' \cup C_0
\end{align*}
\]

**Refining the results** \((\Rightarrow_{\text{refine}})\). The goal of this step is to reduce the number of visible type variables of a method interface. The first three substitutions are based on the closed flow constraints which are in \(\mathcal{C}_0\). The last two substitutions are for the high bound (low bound) type variables occurring on low bound (high bound) positions. Dual types are also translated into intersection types by the substitution \(\sigma_d\).

\[
\begin{align*}
\sigma_1 = [V_1.H \rightarrow V, V_2.L \rightarrow V | V_1.H \ll V_2, L \in C_0 \wedge V = \text{fresh}] & \quad \sigma_2 = [V.H \ll t | V.H \ll t \in \sigma_1, C_0] \\
\sigma_3 = [V.L \ll t | t < V, L \in \sigma_2 \sigma_1 C_0] & \quad \sigma_4 = [V \ll t | t < V \in \sigma_3 \sigma_2 \sigma_1 C_0 \vee V < t \in \sigma_3 \sigma_2 \sigma_1 C_0] \\
\sigma' = \sigma_3 \sigma_2 \sigma_1 \sigma_1 & \quad \Rightarrow_{\text{refinedual}} \sigma_d \\
\sigma' = [V.H \rightarrow V | V_1.L \rightarrow V.H \in \sigma' \wedge V = \text{fresh}] & \quad \sigma' = [V.L \rightarrow V | V_1.H \rightarrow V.L \in \sigma' \wedge V = \text{fresh}] \\
\sigma = \sigma_d \sigma_1 \sigma_2 \sigma_3 \sigma_4 & \quad \rightleftharpoons \sigma_0 \sigma_2 \sigma_3 \sigma_4 \sigma_5
\end{align*}
\]

\[
\begin{align*}
\Rightarrow_{\text{refine}} C_0; D; Q_0; \sigma_0 \Rightarrow_{\text{refine}} C_0; \sigma Q_0; \sigma
\end{align*}
\]

5 **Method Overriding**

Consider the following method overriding example, where the method boo of the class Cell is overridden by the subclass Pair (note that class Pair extends Cell{..}):

```java
Cell | Object boo(Cell a) {this.fst = a.fst; return a.fst;} 
Pair | Object boo(Cell a) {fst = this.fst; this.snd = a.fst; return a.fst;}
```

Applying our inference to each method, we obtain the following results:

- Cell\(\langle\odot P\rangle\) | P boo(Cell\(\langle\odot P\rangle\) a){..}
- Pair\(\langle\odot P_1, \odot P_2\rangle\) | P_1 boo(Cell\(\langle\odot P_1\rangle\) a){..}

The method overriding is sound only if the overriding method is a subtype of the overridden method and the overriding method’s receiver is a subtype of the overridden method’s receiver [3]. As can be seen, this property does not hold for the above inferred methods:

```java
Pair(\langle\odot P_1, \odot P_2\rangle) < Cell(\langle\odot P\rangle) \quad Cell(\langle\odot P\rangle) < Cell(\langle\odot P_1\rangle) \quad P_1 < P
```

To ensure this property, we augment our inference algorithm with the following considerations: (i) we can strengthen the receiver type and the result type of the overriding method; (ii) we can add the parameters types and the precondition of the overridden method. Thus the method overriding problem is solved as follows:
1. Infer the overridden method as: \( \text{Cell}([P, \text{Object}]) \mid \text{P boo} (\text{Cell}([L, P])) a \)
2. Undo the variance of the overridden method parameters by using fresh interval type variables \((P_1, H)\) and \((P_1, L)\) that keep the relation with the other type variables of the receiver and the result: \( \text{Cell}([P, \text{Object}]) \mid \text{P boo} (\text{Cell}([P_1, L, P_1, H])) a \) where \( P_1, H \) \( \leftarrow P \\
3. Do inference for the overriding method: The process starts with the sound overriding assumptions (Step 1):

\[
\begin{array}{c|c}
\text{Pair}(\langle [V_1, L, V_1, H], [V_2, L, V_2, H] \rangle) & \text{Y boo} (\text{Cell}([V_3, L, V_3, H])) a \\
\{ \text{a.fst} = \text{this.fst}, \text{this.snd} = \text{a.fst} \; \text{return} \; \text{a.fst} \}
\end{array}
\]

1. **Overridding Assumptions**

\[
\begin{array}{c|c}
\text{Pair}(\langle [V_1, L, V_1, H], [V_2, L, V_2, H] \rangle) & \text{Cell}(\{P, L, P_1, H\}) \leftarrow \text{Cell}(\{V_1, L, V_3, H\}) \land P_1, H \leftarrow P \\
\end{array}
\]

2. **Collect Constraints**

\[
\begin{array}{c|c}
V_1, H \leftarrow V_1, L \land V_3, H \leftarrow V_3, L \land V_3, H \leftarrow Y \\
\end{array}
\]

3. **Simplify**

\[
\begin{array}{c|c}
P \leftarrow V_1, L \land Y \leftarrow P \land V_3, L \leftarrow P_1, L \land V_3, H \leftarrow P_1, H \leftarrow P \land V_1, H \leftarrow V_3, L \land V_3, H \leftarrow Y \\
\end{array}
\]

4. **Infer Variance**

\[
\begin{array}{c|c}
V_2, H = \text{Object} \land V_1, L = V_1, H \land V_3, L = V_3, H \land P_1, L = P_1, H \\
\end{array}
\]

5. **Infer Type Vars**

\[
\begin{array}{c|c}
P = P_1, H = P_1, L = V_1, H = V_1, L = V_2, L = V_3, H = V_3, L \\
\end{array}
\]

4. The result of the previous step is applied on both overridden and overriding methods and we obtain the following sound result:

\[
\text{Cell}(\odot P) \mid \text{P boo} (\text{Cell}(\odot P)) a \quad \text{Pair}(\odot P, \odot P) \mid \text{P boo} (\text{Cell}(\odot P)) a
\]

### 6 Conclusion

We have formalized a novel constraint-based algorithm to infer variant parametric types for non-generic Java code. In contrast to the previous refactoring algorithms [9, 8, 7, 11, 16] which mainly support invariant subtyping and are designed as whole program analyses, our approach offers full support for use-site variance based subtyping and it is designed as a summary-based analysis that works on a per method basis. The main technical novelty of our approach is a systematic variance inference based on interval types. With the full support for use-site variance based subtyping, our approach can generate better generic types than those derived by existing systems. For instance, none of the previous algorithms can automatically infer the examples from Section 3.4 and Section 3.5.

Although our inference algorithm internally works with sophisticated mechanisms, its output is expressed in terms of variant parametric types extended with restricted forms of intersection/union types as used in [4]. We have proven the soundness of our inference algorithm with respect to our variant parametric type system in [4]. However the completeness requirement is a difficult problem since the decidability of nominal subtyping with use-site variance is still an open problem as was discussed in [15].

We have built an inference prototype which works for a core subset of Java. Our previous VPT checker from [4] is used to validate the inferred results. In our initial experiments we have tested the quality of our inference system results on a small set of non-generic programs by comparing the inferred generic types with the best generic types that one can manually provide. In all the cases, our system was able to infer the same types as those manually provided. The inference time was less than one second for each test program. Currently we are working to extend our experiments to larger programs by using our translator of Java to a core subset [6].
References