Associated Types and Constraint Propagation for Mainstream Object-Oriented Generics

Jaakko Järvi[1], Jeremiah Willcock[2], and Andrew Lumsdaine[2]

[1] Texas A&M University, Computer Science, College Station, TX 77843
jarvi@cs.tamu.edu
[2] Indiana University, Open Systems Lab, Bloomington, IN 47405
{jewillco|lums}@osl.iu.edu

Abstract. Support for object-oriented programming has become an integral part of mainstream languages, and more recently generic programming has gained widespread acceptance as well. A natural question is how these two paradigms, and their underlying language mechanisms, should interact. One particular design option, that of using subtyping to constrain the type parameters of generic functions, has been chosen for the generics extensions to Java and C#. Certain shortcomings have previously been identified in using subtyping for constraining parametric polymorphism in the context of generic programming. To address these, we propose the expansion of object-oriented interfaces and subtyping to include associated types and constraint propagation. Associated types are type members of interfaces and classes. Constraint propagation allows certain constraints on type parameters to be inferred from other constraints on those parameters and their use in base class type expressions. The paper demonstrates these extensions in the context of Generic C# and presents a formalism proving their safety. The formalism is applicable to other mainstream OO languages supporting F-bounded polymorphism, such as Java.

1 Introduction

Generic programming is an emerging programming paradigm for writing highly reusable libraries of algorithms. The generic programming approach has been used extensively within the C++ community; prime examples of generic libraries include the Standard Template Library (STL) [1,2], STAPL (a parallel STL) [3], Boost Graph Library [4] (BGL), Matrix Template Library [5], and Bioinformatics Template Library [6]. Common to these libraries is their extensive parameterization of algorithms with respect to the types of their arguments, allowing a single implementation of an algorithm to work on a broad class of different argument types. Such a high degree of type parameterization is less common in other mainstream object-oriented languages.

The major difference between generic programming in C++ vs. generics in, say, C# or Java, is that C++ does not require, or allow, any constraints on type parameters, whereas C# and Java do. Type checking of generic definitions in C++ is delayed until after concrete types are bound to type parameters. By contrast, in C# and Java, explicit subtype constraints on type parameters allow type checking of generic definitions separately from their uses.

In a previous study [7], we evaluated six mainstream programming languages with respect to their support for generic programming. The evaluation was based on the experiences in implementing a subset of the BGL in each of the languages under study. Mainstream object-oriented languages did not rank highly in this evaluation; practical problems encountered include verbose code, redundant code, and difficulties in composing separately defined generic components. Constraints naturally render generic method and class definitions in C# and Java more verbose than their counterparts in C++. Our experience with the BGL implementation showed, however, that the number and size of the required constraint expressions can become excessive in algorithms parameterized over several input types. First, the only means of expressing dependencies between generic types is by type parameterization. This prevents proper encapsulation of such dependencies into interfaces or abstract classes. Second, inheriting a generic class from another generic class does not mean inheriting constraints on type parameters. Rather, a generic class or method definition must often repeat type parameter constraints which are already induced by uses of these parameters in types of base classes or by uses in constraints.

This paper advocates *associated types* and *constraint propagation* as solutions to these problems. Associated types resemble member **typedef**s in C++, and virtual types [8,9], in a restricted form. Further, associated types share similarities with type members of ML signatures. Section 6 describes these connections in more detail. By constraint propagation we refer to a language mechanism that gathers type parameter constraints that are induced by uses of the type parameters of a generic component as arguments to other generic types, and makes those constraints implicitly part of the constraints of the generic component.

The contributions of this work are to introduce language extensions for associated types and constraint propagation within the context of languages that support F-bounded polymorphism [10], such as Java or C#. Our approach is motivated by the needs of practical generic programming, and by the techniques commonly used within that community. The proposed extensions are described using a series of examples, and then formalized using an FGJ-like approach [11]; the formalization is used to show that the extensions preserve type-safety. A translation from a simple OO language with these extensions to a standard object-oriented language with F-bounded polymorphism is then presented, to give a possible implementation of the extensions. We provide a formal proof that the translation preserves type-safety.

The paper is structured as follows: Section 2 describes generic programming, and the role of associated types in generic definitions. Section 3 discusses the consequences of representing associated types using type parameters, and the consequences of the lack of constraint propagation in constrained generics. As a remedy to these problems, Section 4 suggests two language extensions for C# and describes informally a source-to-source translation of these extensions to current

C#. Section 5 provides a formal account of the impact of these features in a setting similar to Featherweight Generic Java (FGJ) [11] and C# minor [12] and proves the soundness of the extensions in this simplified formalism. Section 6 surveys related work, both in object-oriented and in functional programming languages. Section 7 concludes the paper and outlines future work.

2 Background

Generic programming is a systematic approach to software reuse that focuses on finding the most general (or abstract) formulations of algorithms and their efficient implementations [13]. Fundamental to realizing generic algorithms is the notion of abstraction: generic algorithms are specified in terms of abstract properties of types, not in terms of particular types. In the terminology of generic programming, a *concept* is the formalization of an abstraction as a set of requirements on a type (or on several types) [14, 15]. These requirements may be semantic as well as syntactic. A concept may incorporate the requirements of another concept, in which case the first concept is said to *refine* the second. Types (or sequences of types) that meet the requirements of a concept are said to *model* the concept. Note that it is not necessarily the case that the requirements of a concept involve just one type: commonly a concept involves multiple types and specifies their relationships.

A concept consists of four different kinds of requirements: associated types, function signatures, semantic constraints, and complexity guarantees. The *associated types* of a concept specify mappings from the modeling type(s) to other collaborating types (such as the mapping from a container to the type of its elements). The *function signatures* specify the operations that must be defined for the modeling types. Alternatively, the operations are specified using *valid expressions* that must be syntactically valid for any types that model the concept. This is idiomatic in documenting concepts in C++ libraries, because a valid expression can be implemented with more than one function signature.

The above form of describing requirements on type parameters is wide-spread in the C++ community; the SGI STL documentation [16] is the archetypical example. The specification of the C++ standard library follows the same form as well. One reason for this is arguably the lack of language mechanisms for specifying constraints; structured concept descriptions provide some rigor in requirement descriptions. Another view is that concepts arise by examining concrete algorithms, grouping frequently occurring requirements into reusable entities. Concept descriptions are not bound by language constructs, and have had the freedom to evolve into a form that effectively captures the essential requirements that generic algorithms place on type parameters.

The following example shows a simplistic generic function first_neighbor for finding an adjacent vertex of another vertex in a graph:

```
template <class Graph>
typename Graph::vertex_type find(Graph g, typename Graph::vertex_type v)
{ return target(current(out_edges(v, g))); }

// Constraints:   Graph models Incidence Graph
```

The function constrains, though merely in documentation, its Graph type parameter using the concept Incidence Graph documented in Figure 1. This concept requires the existence of the associated types vertex_type, edge_type, and out_edge_iterator. In addition, it places requirements on these types: edge_type must be a model of the Graph Edge concept, and out_edge_iterator is required to model the Iterator concept. These two concepts are described in Figure 1. Furthermore, the Incidence Graph concept has two *same-type constraints* (cf. ML sharing constraints) to ensure that out_edge_iterator iterates over edges with the correct type, and that vertex_type coincides with the edge_type's associated type vertex_type. Concepts can be built from other concepts using refinement. For example, the concept Bidirectional Iterator contains all requirements of the Iterator concept, and adds the ability to move backward in a sequence. In C++, concepts are merely a documentation artifact, and thus structural conformance (presence of the correct associated types and function definitions) to the requirements suffices for a type to model a concept.

In the generic programming approach, taxonomies of concepts of the modeled domain guide the systematic organization of reusable libraries. Concept taxonomies can in principle be developed independently of a particular programming language; the implementation language of a generic library must, however, allow their expression. The directness of this varies among languages. For example, ML signatures and Haskell type classes have a relatively close correspondence to concepts. Classes and interfaces, the type parameter bounds of C# and Java, seem to be a less direct fit. In particular, representing associated types is accomplished in a round-about manner. The next section discusses representing concepts and generic algorithms with OO interfaces found in C# or Java generics.

3 Interfaces as concepts

In C# or Java, interfaces can capture the valid expression requirements of concepts as method signatures. We use C# syntax in our examples. The models relation between types and concepts can be represented as classes implementing interfaces and concept refinement can be represented as inheritance between interfaces. Although associated types do not have a direct counterpart in interfaces, a type parameter can be used to represent an associated type. In that case, constraints on associated types are simply constraints on type parameters. Representing associated types with type parameters is common practice. The C# IEnumerable<T> interface, from the Generic C# collection library, for iterating through containers serves as an example. When a type implements IEnumerable<T> it must bind a concrete value, the value type of the container, to the type parameter T.

Compare the two concepts in Figure 1, and their representations as C# interfaces (Figure 2). The three type parameters Vertex, Edge, and OutEdgeIterator in the generic IncidenceGraph interface correspond to the three associated types of the Incidence Graph concept. The constraints on these types are visible in

Incidence Graph concept. Type Graph is a model of Incidence Graph if the requirements below are satisfied. Object g is of type Graph and v is of type Graph::vertex_type

Expression	**Return Type or Description**
Graph::vertex_type	Associated vertex type
Graph::edge_type	Associated edge type
Graph::out_edge_iterator	Associated iterator type
edge_type models Graph Edge	
out_edge_iterator models Iterator	
edge_type::vertex_type == vertex_type	
out_edge_iterator::value_type == edge_type	
out_edges(v,g)	out_edge_iterator
out_degree(v,g)	**int**

Graph Edge concept. Type Edge is a model of Graph Edge if the following requirements are satisfied. Object e is of type Edge.

Expression	**Return Type or Description**
Edge::vertex_type	Associated vertex type
source(e)	Edge::vertex_type
target(e)	Edge::vertex_type

Iterator concept. Type Iter is a model of Iterator if the following requirements are satisfied. Object i is of type Iter.

Expression	**Return Type or Description**
Iter::value_type	Associated value type
next(i)	Iter
at_end(i)	**bool**
current(i)	Iter::value_type

Fig. 1. Typical C++ concept descriptions.

the **where** clause. Note that we use the standard interface IEnumerable as the interface for the iterator, rather than defining one based on the Iterator concept in Figure 1. The same-type constraint out_edge_iterator::value_type == edge_type is expressed by using the type parameter Edge in the constraint of OutEdgeIterator. Similarly, using Vertex as the type argument to GraphEdge establishes the constraint edge_type::vertex_type == vertex_type. Figure 3 contains the C# version of first_neighbor, which uses IncidenceGraph to constrain one of its type parameters.

The main problem with representing associated types as type parameters is that type parameters are not properly encapsulated in the interface. Every reference to an interface, whether the interface is being extended (concept refinement) or used as a type parameter constraint, must list all of the type parameters explicitly. In a concept with several associated types, this becomes burdensome. In the study described in [7], the number of type parameters in generic algo-

```
interface GraphEdge<Vertex> {
  Vertex source();
  Vertex target();
}
interface IncidenceGraph<Vertex, Edge, OutEdgeIterator>
  where Edge : GraphEdge<Vertex>,
        OutEdgeIterator : IEnumerable<Edge> {
  OutEdgeIterator out_edges(Vertex v);
  int out_degree(Vertex v);
}
```

Fig. 2. Graph Edge and Incidence Graph as C# interfaces

```
G_Vertex first_neighbor<G, G_Vertex, G_Edge, G_OutEdgeIterator>(G g, G_Vertex v)
  where G : IncidenceGraph<G_Vertex, G_Edge, G_OutEdgeIterator>,
        G_Edge : GraphEdge<G_Vertex>,
        G_OutEdgeIterator : IEnumerable<G_Edge> {
  return g.out_edges(v).Current.target();
}
```

Fig. 3. Example generic function in C#

rithms was often more than doubled due to this effect. Figure 3 demonstrates the problem. Even though the first_neighbor function only takes two parameters, the graph and vertex types, it has four type parameters. Note that these type parameters are not referred to in the parameter list or body of the method.

Another related problem is that interfaces fail to encapsulate constraints on associated types. Consider the type parameter constraints in the **where** clause of first_neighbor. The last two lines are a repetition of what is already specified in the **where** clause of the IncidenceGraph interface (see Figure 2). This repetition seems unnecessary: no type can be bound to G unless it inherits from the IncidenceGraph interface. This in turn requires that the types bound to the type parameters Vertex, Edge, and OutEdgeIterator must satisfy the constraints of the IncidenceGraph interface. Thus, based on the constraint on G above, the type-checker could safely assume that the type parameters G_Vertex, G_Edge, and G_OutEdgeIterator in the generic first_neighbor function also satisfy the constraints in IncidenceGraph. Such *constraint propagation*, as we refer to it, is not performed in current C#, and thus the last two subtype constraints of first_neighbor are necessary as direct evidence of all type arguments meeting their bounds. In our experience [7], lack of constraint propagation greatly increases the verbosity of generic functions and generic interfaces. It also adds extra dependencies on the exact form of generic interfaces; a slight change in a constraint on an associated type of an interface may require a change in every use of that interface.

4 Extending C# generics

We argue that direct support for associated types and support for constraint propagation would significantly improve support for generic programming in C#, without requiring drastic modifications to the language. In this section we describe associated types, in the form of member types in interfaces, and constraint propagation, as extensions to C#. Furthermore, we describe how these features can be translated to standard C#. The presentation is informal; Section 5 gives a detailed formal description of the features and their translations in an idealized model of the language.

4.1 Associated types

Our approach to associated types for Generic C# is to introduce *member types* in interfaces and classes. We allow interfaces to declare members which are placeholders for types, and place constraints, subtype or same-type, on these members. We adopt the syntax **type** A : B for declaring a member type A and requiring that any type bound to A must a subtype of B. The constraint can be omitted. Same-type constraints are expressed with the syntax **require** A == B. We also allow subtype constraints of the form **require** A : B in isolation of associated type declarations. The syntax E::A is used for accessing an associated type A of an interface or a class E. In particular, to access an associated type A in the current class or in one of its ancestors, one writes **this**::A, and we allow **this**:: to be omitted. The left-hand side of a subtype constraint, and one side of a same-type constraint, must be a *constrainable* type. We define a constrainable type as either a type parameter; **this**::A, where A is an associated type declared in the current class or interface, or in its ancestors; or as an associated type of a constrainable type. The right-hand side of a subtyping constraint must be an instance of a class or an interface.

An interface with member types that have not been bound to concrete types can only be used as type parameters' subtype constraints, or as a base interface of another interface or class. In particular, one cannot declare a variable, function parameter, or a field of such a type. Match-bounded polymorphism [17] includes a similar notion of interfaces that cannot be used as types. A derived interface can tighten constraints on associated types defined in its base interfaces. Classes that implement interfaces must bind concrete values to the member types. This binding cannot be changed in derived classes. These restrictions are necessary for preserving type-safety, and are in line with the restrictions of type-safe variations of virtual types [9, 18].

As an example, Figure 4 shows how the graph concepts from Figure 1 can be expressed using this extension. The GraphEdge interface declares the member type Vertex. The IncidenceGraph interface declares two associated types, Vertex and Edge, and places constraints on them: Edge must be a subtype of GraphEdge and Vertex must be the same type as the associated type, also named Vertex, of Edge. We can observe that the member types correspond directly to the associated types in Figure 1, subtype constraints correspond to requirements that types model concepts, and the same-type constraint has a direct equivalent as well. The constraint on OutEdgeIterator, however, is different: the Iterator concept is represented using the standard IEnumerable interface, where the associated type Edge is an extra type parameter rather than a member type. This demonstrates that the two styles of representation for associated types can coexist.

```
interface GraphEdge {
  type Vertex;
  Vertex source();
  Vertex target();
}
interface IncidenceGraph {
  type Vertex;
  type Edge : GraphEdge;
  type OutEdgeIterator : IEnumerable<Edge>;
  require Vertex == Edge::Vertex;

  OutEdgeIterator out_edges(Vertex v);
  int out_degree(Vertex v);
}
```

Fig. 4. Graph concepts represented as interfaces with associated types.

The rewrite of the first_neighbor function in Figure 5 demonstrates the effect of associated types: one type parameter, instead of four, suffices. The constraint on G itself is very concise, but the constraints on associated types of G are even more verbose. This is due to the need to provide explicit evidence that G satisfies all requirements of IncidenceGraph. The remedy is constraint propagation, explained in Section 4.2.

```
G::Vertex first_neighbor<G>(G g, G::Vertex v)
  where G : IncidenceGraph,
        G::Edge : GraphEdge,
        G::OutEdgeIterator : IEnumerable<G::Edge>,
        G::Vertex == G::Edge::Vertex {
  return g.out_edges(v).Current.target();
}
```

Fig. 5. The first_neighbor function that relies on support for associated types, but does not rely on constraint propagation.

Associated types are translated into type parameters as follows:

- Each associated type declaration in an interface is translated into a new type parameter of that interface. Subtype constraints on associated types are translated and moved to **where** clauses as constraints on the corresponding type parameters. The translation of the interfaces in Figure 4 results in the interfaces we showed in Figure 2. All three associated types of IncidenceGraph end up as type parameters. Note that, essentially, we are describing the automation of a translation that programmers are now doing by hand.
  Same-type constraints between two types are handled by unifying, in the logic programming sense, the translations of the types required to be equal. For example, in Figure 2 the type Vertex is used as the Vertex associated type for both GraphEdge and IncidenceGraph.
- The definitions of associated types in classes that implement interfaces are converted to type arguments of the interfaces. Figure 6 shows two such classes, implementing the GraphEdge and IncidenceGraph interfaces. The code in Figure 6(a) is written using the extension; Figure 6(b) contains the code translated to plain Generic C#. Obviously, this part of the translation must be coordinated with the translation of the corresponding interface definitions. Associated types that are referred to by name in the extended C# are identified based on their positions in the type parameter list in the translated code. Thus, the translation must ensure that the same names are always mapped to the same positions.
- Interfaces that contain associated types can occur in constraints of generic functions, or those of generic classes or interfaces. Any instance of such an interface requires an extra type argument for each associated type, so that the instantiation matches the translated definition of the instance. Also, references to associated types in the body and constraints of a generic function, class, or interface are converted to references to the corresponding type parameters. The IncidenceGraph and GraphEdge interfaces get three and one, respectively, extra type arguments in the translation of the first_neighbor function from the version in Figure 5 to the version in Figure 3. Again, same-type constraints are handled by using the same type parameter as a type argument to more than one generic interface, or in more than one argument position of one generic interface.

An interface that contains associated types is not a traditional object-oriented interface; in particular, such an interface is not a type. As the translation suggests, these interfaces cannot be used without providing, either implicitly or explicitly, the values of their associated types. As a consequence, interfaces with associated types can be used as constraints on type parameters, but not as types for variables or function parameters — uses that traditional interfaces allow. For example, the first_neighbor function in Figure 5 cannot be written as:

```
IncidenceGraph::Vertex first_neighbor(IncidenceGraph g, IncidenceGraph::Vertex v);
```

In this definition, the references to IncidenceGraph::Vertex are undefined; the abstract IncidenceGraph interface does not define a value for the Vertex associated

```
class AdjListEdge : GraphEdge {
  type Vertex = int;
  ...
}

class AdjacencyList : IncidenceGraph {
  type Vertex = int;
  type Edge = AdjListEdge;

  type OutEdgeIterator =
    IEnumerable<AdjListEdge>;

  OutEdgeIterator out_edges(Vertex v) {...}

  int out_degree(Vertex v) {...}
}
```

(a)

```
class AdjListEdge : GraphEdge<int> {
  ...
}

class AdjacencyList
  : IncidenceGraph<int, AdjListEdge,
       IEnumerable<AdjListEdge> > {

  IEnumerable<AdjListEdge>
    out_edges(Vertex v) {...}

  int out_degree(Vertex v) {...}
}
```

(b)

Fig. 6. Concrete graph and edge types that model the Incidence Graph and Graph Edge concepts.

type. This is a major difference between our translation and systems based on virtual types. In our translation, all associated types are looked up statically, and so the type of g is the interface IncidenceGraph, not a concrete class which implements IncidenceGraph.

For the translation described in this section to work with implicit instantiation, it is important to be able to infer the values of associated types from the types that are bound to the main type parameters. This is not currently supported in C# or Java; the Cecil programming language provides the feature. As an example of inferring types from constraints, consider the following equivalent formulation (we are assuming constraint propagation) of the first_neighbor function, which makes the use of the associated edge type more explicit:

```
G::Vertex first_neighbor<G>(G g, G::Vertex v) where G : IncidenceGraph {
    G::Edge first_edge = g.out_edges(v).Current;
    return first_edge.target();
}
```

In a call to first_neighbor, a concrete graph type is bound to G, and thus associated types, such as G::Edge, can be resolved. In the translated version, however, it is less obvious that associated types can be inferred automatically:

```
G_Vertex first_neighbor<G, G_Vertex, G_Edge, G_OutEdgeIterator>(G g, G_Vertex v)
  where G : IncidenceGraph<G_Vertex, G_Edge, G_OutEdgeIterator> {
    G_Edge first_edge = g.out_edges(v).Current;
    return first_edge.target();
}
```

The two type parameters G_Edge and G_OutEdgeIterator are not the types of any of the function arguments, and thus are not directly deducible. To infer their types, the particular graph type bound to G must be examined to find its associated type definitions; these are the type arguments to IncidenceGraph in an inheritance declaration in the declaration of the graph class.

4.2 Constraint propagation

Constraint propagation can apply when a type parameter is constrained by a generic class or interface, or when a generic class or interface inherits from another generic class or interface. Consider the process of type-checking the body of a generic class or function a. Suppose T is a type parameter of a, and T is used as a type argument in some instantiation Y<..., T, ...> occurring in one of the constraints of a, or as a base class or base interface of a. Constraint propagation then means that any constraints the definition of Y places on T in the instantiation Y<..., T, ...> can be assumed to be true while type-checking a.

As an example, consider the function in Figure 5. The type parameter G_Edge is used as a type argument to the IncidenceGraph interface. The **where** clause of this interface requires the second type parameter Edge to be a subtype of GraphEdge<Vertex>. Substituting G_Edge to Edge and G_Vertex to Vertex, as implied by the instantiation IncidenceGraph<G_Vertex, G_Edge, G_OutEdgeIterator>, we can assume that the constraint G_Edge : GraphEdge<G_Vertex> holds while type-checking first_neighbor. The translation can thus be implemented by copying the constraints, with appropriate substitutions, according to the above description.

Combining the two extensions, associated types and constraint propagation, the constraints of the first_neighbor function can be written very concisely:

```
G::vertex_type first_neighbor<G>(G g, G::Vertex v) where G : IncidenceGraph {
    return g.out_edges(v).Current.target();
}
```

Applying first the translation for associated types leads to the definition below, which, after constraint propagation, becomes the definition in Figure 3:

```
G_Vertex first_neighbor<G, G_Vertex, G_Edge, G_OutEdgeIterator>(G g, G_Vertex v)
  where G : IncidenceGraph<G_Vertex, G_Edge, G_OutEdgeIterator> {
    return g.out_edges(v).Current.target();
}
```

5 Formalization

To gain assurance of the soundness of the extensions of associated types and constraint propagation, we developed a formal model for an idealized language, based on Featherweight Generic Java (FGJ) [11], which captures the essential properties of the extensions in a language similar to C# and Java. We refer to this language as FGJ+APR. We then define a translation of programs in FGJ+APR into a version of FGJ extended with interfaces and multiple interface inheritance, denoted FGJ+I below; we assume this extension can be done while preserving type safety. We show that programs in FGJ+APR are translated into programs in

$$
\begin{array}{rll}
\text{(interface def) } id & ::= & \texttt{interface } I\texttt{<}\overline{X}\texttt{>} : \overline{M} \texttt{ where } \overline{rd} \\
 & & \{\texttt{type } \overline{A};\ \texttt{require } \overline{rd};\ \overline{ms}\} \\
\text{(class def) } cd & ::= & \texttt{class } C\texttt{<}\overline{X}\texttt{>} : \overline{M}, K \texttt{ where } \overline{rd} \\
 & & \{\texttt{type } \overline{A} = \overline{U};\ \overline{T}\ \overline{f};\ kd\ \overline{md}\} \\
\text{(constraint def) } rd & ::= & T : P \mid T == U \\
\text{(constructor def) } kd & ::= & C(\overline{T}\ \overline{f}) : \texttt{base}(\overline{f})\ \{\texttt{this}.\overline{f} = \overline{f};\} \\
\text{(method signature) } ms & ::= & T\ m(\overline{U}\ \overline{x}); \\
\text{(method def) } md & ::= & T\ m(\overline{U}\ \overline{x})\ \{\texttt{return } e;\} \\
\text{(expression) } e & ::= & x \mid e.f \mid e.m(\overline{e}) \mid \texttt{new } K(\overline{e}) \mid (T)e \\
\text{(constrainable type) } G, H & ::= & X \mid \texttt{this} :: A \mid G :: A \\
\text{(instantiated interface) } M, N & ::= & I\texttt{<}\overline{T}\texttt{>} \\
\text{(instantiated class) } K, L & ::= & C\texttt{<}\overline{T}\texttt{>} \\
\text{(instantiated class or interface) } O, P & ::= & M \mid K \\
\text{(type) } S, T, U, V, W & ::= & X \mid G \mid P \mid T :: A
\end{array}
$$

Fig. 7. Syntax of FGJ+APR

FGJ+I with the same type behavior, i.e., well-formedness of classes and interfaces is preserved, and translated expressions have their translated types. Because our language has exactly the same expressions as FGJ, and the translation does not alter the non-type content of expressions, we define our semantics through translation to FGJ+I. Our extended language is thus type-safe as long as FGJ+I is. FGJ allows type parameters both on methods and classes; we omit generic methods to reduce complexity. As we do not consider variance or implicit instantiation of type parameters, parameterized methods provide no new insights.

5.1 Syntax

Figure 7 shows the syntax of FGJ+APR; many of the rules are either directly from, or based on, FGJ [11]. We summarize the language and notation. The metavariables I and J range over interface names; C and D over class names; E and F over either interface or class names; A and B over associated type names; X, Y, and Z over type variables; S, T, U, V, and W over arbitrary types; M, N over instantiated interfaces; K, L over instantiated classes; O, P over instantiated interfaces or classes (we refer to these as *instances*); G, H over *constrainable* types (these are either type parameters, or possibly nested associated types of type parameters or `this`); d and e over expressions; f and g over field names; and x over method parameters.

Borrowing from the FGJ notation, a variable with a horizontal bar above it stands for a possibly empty sequence of elements from the variable's domain. The separator parameter is determined from the context. For example $\overline{A}$ is a shorthand for the comma separated sequence of associated types $A_1, A_2, \ldots, A_n$, and $\overline{ms}$; a sequence of method signatures delimited by semicolons. Further, $\overline{rd}$ represents a comma separated sequence of constraints. Such constraints can be of two forms: $T : P$ or $T == U$. We refer to the former kind as subtype constraints and the latter as same-type constraints. Note that in program code, the left-hand side of these constraints must be a constrainable type, but this restriction does not hold in the formalism in general. Horizontal bar is used with constraints as well: $\overline{T} : \overline{P}$ represents the sequence $T_1 : P_1, T_2 : P_2, \ldots, T_n : P_n$ and $\overline{T} == \overline{U}$ the sequence $T_1 == U_1, T_2 == U_2, \ldots, T_n == U_n$. The horizontal bar is also used with helper functions. For example, we define $\mathit{constr}(T)$ as the set of constraints induced by T, and take $\mathit{constr}(\overline{T})$ to mean $\mathit{constr}(T_1), \mathit{constr}(T_2), \ldots, \mathit{constr}(T_n)$. We write the type of a method $V\ m(\overline{U}\ \overline{x})\ \{\ \texttt{return}\ e; \}$ in class $C\texttt{<}\overline{T}\texttt{>}$ as $\overline{U} \to V$; its body is the pair $\langle \overline{x}, e \rangle$, accessed by $\mathit{mbody}(C\texttt{<}\overline{T}\texttt{>}.m)$.

We require that sequences of names of type parameters, methods, associated types, and method parameters do not contain duplicates. Also, we sometimes write a class definition as $\texttt{class}\ C\texttt{<}\overline{X}\texttt{>} : \overline{P} \ldots$, in which case we assume that at most one P_i is a class, and the other elements in $\overline{P}$ are interfaces. Further, we sometimes use the syntax $\texttt{class/interface}\ E\texttt{<}\overline{X}\texttt{>} : \overline{P} \ldots$ when describing behavior common to classes and interfaces; it is assumed that if E is an interface, all elements of $\overline{P}$ are interfaces.

We write $[\overline{T}/\overline{X}]U$ for the simultaneous substitution of types $\overline{T}$ for $\overline{X}$ in U. A substitution is well-formed in some environment $\mathit{\Delta}$ if $\overline{T}$ are well-formed in $\mathit{\Delta}$. Well-formedness is defined below in this section. The metavariable σ ranges over substitutions.

CT is a class table mapping the name of a class or interface to its definition. Then an FGJ+APR program is a fixed class table and a single expression e, whose evaluation is the program execution. We assume CT satisfies the following conditions: (1) $CT(C) = \texttt{class}\ C \ldots$ and $CT(I) = \texttt{interface}\ I \ldots$ for every $C, I \in \mathit{dom}(CT)$; (2) for every class or interface name E, appearing anywhere in CT, $E \in \mathit{dom}(CT)$; (3) there are no cycles in the subtype relation induced by CT; (4) and that associated type definitions in classes do not form a cycle. The fourth condition can be checked by following the definitions of each associated type in all classes, and ensuring that they eventually are bound to an instance or a constrainable type. For shorter presentation, we define another function $\mathcal{D}$ that looks up a class or interface from CT and performs simultaneous substitution of type arguments to type parameters and an instance type to `this` everywhere in the class or interface definition:

$$\frac{\begin{array}{c} CT(C) = \texttt{class}\ C\texttt{<}\overline{X}\texttt{>} : \overline{P}\ \texttt{where}\ \overline{rd}\ \{\texttt{type}\ \overline{A} = \overline{V};\ \overline{W}\ \overline{f};\ kd\ \overline{md}\} \\ |\overline{T}| = |\overline{X}| \qquad \sigma = [\overline{T}/\overline{X}, U/\texttt{this}] \end{array}}{\mathcal{D}(C\texttt{<}\overline{T}\texttt{>}, U) = \texttt{class}\ C\texttt{<}\overline{T}\texttt{>} : \sigma\overline{P}\ \texttt{where}\ \sigma\overline{rd}\ \{\texttt{type}\ \overline{A} = \sigma\overline{V};\ \sigma\overline{W}\ \overline{f};\ \sigma kd\ \sigma\overline{md}\}}$$

$$\frac{\begin{array}{c} CT(I) = \texttt{interface}\ I\texttt{<}\overline{X}\texttt{>} : \overline{M}\ \texttt{where}\ \overline{rd_1}\{\texttt{type}\ \overline{A};\ \texttt{require}\ \overline{rd_2};\ \overline{ms}; \} \\ |\overline{T}| = |\overline{X}| \qquad \sigma = [\overline{T}/\overline{X}, U/\texttt{this}] \end{array}}{\mathcal{D}(I\texttt{<}\overline{T}\texttt{>}, U) = \texttt{interface}\ I\texttt{<}\overline{T}\texttt{>} : \sigma\overline{M}\ \texttt{where}\ \sigma\overline{rd_1}\ \{\texttt{type}\ \overline{A}; \texttt{require}\ \sigma\overline{rd_2};\ \sigma\overline{ms}; \}}$$

5.2 Typing

We use two typing environments $\mathit{\Gamma}$ and $\mathit{\Delta}$. The environment $\mathit{\Gamma}$ maps variables (method parameters) to their types; its elements have the form $\overline{x} : \overline{T}$. The type environment $\mathit{\Delta}$ can contain three kinds of elements: type parameter names; subtype constraints, of the form $T : P$; and same-type constraints, of the form $T == U$. We define the helper function $\cdot_v$ for extracting the type variables from a type environment, and $\cdot_c$ for extracting the constraints. These two functions are used as $\mathit{\Delta}_v$ and $\mathit{\Delta}_c$. We use the metavariables Q and R to range over constraints. A typing judgment $\mathit{\Delta}; \mathit{\Gamma} \vdash e : T$ is read as "e has type T in the environments $\mathit{\Delta}; \mathit{\Gamma}$." The typing rules for expressions, shown in Figure 9, directly correspond to the ones in FGJ, except for TY-DCAST, which omits for brevity a technical condition not significant for our formalism.

In Figure 8, we define type equality $==$ as the symmetric, reflexive, and transitive congruence closure of the same-type constraints in the environment. The subtyping relation <: is defined as the closure, under type equality, reflexivity, and transitivity, of the subtype constraints in the environment. We include well-formedness rules for types, environments, constraints, class and interface definitions, and method signatures and definitions. Except for class and interface definitions, well-formedness is always defined with respect to some environment $\mathit{\Delta}$. The judgment $\mathit{\Delta} \vdash E\texttt{<}\overline{T}\texttt{>}\ \mathit{ok}$ is true if $\overline{T}$ satisfy the constraints the definition of E places on $\overline{X}$. This set of constraints, defined using the *propag-c* function shown in Figure 12, is the result of constraint propagation from E's ancestors and from all constraints explicitly expressed in E. For technical reasons, we define two forms of well-formedness for constraints: *semi-ok* and *ok*. A subtype or same-type constraint is *semi-ok* in some environment if both its left-hand and right-hand sides are *ok* in that environment. In the user syntax of FGJ+APR the left-hand side of a constraint must always be a constrainable type. This is the additional requirement for a constraint to be *ok*. Constraints with an instance on the left-hand side can, however, occur internally in the formalism; the definition of *semi-ok* allows this. A type environment is well formed if all constraints and types in it are well-formed.

The well-formedness rules for class and interface definitions, in Figure 10, use the *env-for-body* function to create the type environment $\mathit{\Delta}$, in which all subparts of the class or interface definition must be well-formed. The *env-for-body* function should result in the same environment that must be proven well-formed in the "instance *ok*" rules, and its definition in terms of *propag-c* does exactly this. The CLASS-DEF-OK rule also requires that all constraints propagated from the base interfaces are satisfied in the environment of the class definition. In this premise, the class being checked is substituted for `this` to ensure that the definitions for associated types given in the class are checked against the constraints placed on them by the class's base class and base interfaces.

In contrast to FGJ, in which only the direct constraints of type parameters comprise the environment for checking well-formedness of the subparts of the

TE-REFL

$$\frac{}{\Delta \vdash T == T}$$

TE-FROM-ENV

$$\frac{}{\Delta, T == U \vdash T == U}$$

TE-TRANS

$$\frac{\Delta \vdash T == U \qquad \Delta \vdash U == V}{\Delta \vdash T == V}$$

TE-SYM

$$\frac{\Delta \vdash T == U}{\Delta \vdash U == T}$$

TE-ASSOC-CRG

$$\frac{\Delta \vdash T == U}{\Delta \vdash T :: A == U :: A}$$

TE-TPARAM-CRG

$$\frac{\Delta \vdash \overline{T} == \overline{U}}{\Delta \vdash E\texttt{<}\overline{T}\texttt{>} == E\texttt{<}\overline{U}\texttt{>}}$$

TE-ASSOC-TYPE

$$\frac{\begin{array}{c}\mathcal{D}(C\texttt{<}\overline{T}\texttt{>}, U) = \texttt{class}\ C\texttt{<}\overline{T}\texttt{>} : \overline{M}\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A} = \overline{V};\ \overline{W}\ \overline{f};\ kd\ \overline{md}\} \\ \Delta \vdash U <: C\texttt{<}\overline{T}\texttt{>}\end{array}}{\Delta \vdash U :: A_i == V_i,\ \text{for all}\ i}$$

S-REFL

$$\frac{}{\Delta \vdash T <: T}$$

S-TRANS

$$\frac{\Delta \vdash T <: U \qquad \Delta \vdash U <: V}{\Delta \vdash T <: V}$$

S-FROM-ENV

$$\frac{}{\Delta, G : P \vdash G <: P}$$

S-VIA-EQ

$$\frac{\Delta \vdash T == U \qquad \Delta \vdash U <: V}{\Delta \vdash T <: V}$$

S-CLASS

$$\frac{\mathcal{D}(E\texttt{<}\overline{T}\texttt{>}, E\texttt{<}\overline{T}\texttt{>}) = \texttt{class/interface}\ E\texttt{<}\overline{T}\texttt{>} : \overline{P} \ldots}{\Delta \vdash E\texttt{<}\overline{T}\texttt{>} <: P_i,\ \text{for all}\ i}$$

WF-VAR

$$\frac{X \in \Delta}{\Delta \vdash X\, \mathit{ok}}$$

WF-INTERF-INSTANCE

$$\frac{\begin{array}{c}CT(I) = \texttt{interface}\ I\texttt{<}\overline{X}\texttt{>} \ldots \qquad \Delta \vdash \overline{T}\ \mathit{ok} \\ \Delta \vdash [\overline{T}/\overline{X}]\mathit{propag\text{-}c}(I\texttt{<}\overline{X}\texttt{>})\ \mathit{satisfied} \qquad \mathit{assoc\text{-}decl}(I\texttt{<}\overline{T}\texttt{>}) = \emptyset\end{array}}{\Delta \vdash I\texttt{<}\overline{T}\texttt{>}\ \mathit{ok}}$$

WF-CONSTRAINT-INTERF-INSTANCE

$$\frac{\begin{array}{c}CT(I) = \texttt{interface}\ I\texttt{<}\overline{X}\texttt{>} \ldots \qquad \Delta \vdash \overline{T}\ \mathit{ok} \\ \Delta \vdash [\overline{T}/\overline{X}]\mathit{propag\text{-}c}(I\texttt{<}\overline{X}\texttt{>})\ \mathit{satisfied}\end{array}}{\Delta \vdash I\texttt{<}\overline{T}\texttt{>}\ \mathit{ok\text{-}constraint}}$$

OK-IS-OK-CONSTRAINT

$$\frac{\Delta \vdash T\ \mathit{ok}}{\Delta \vdash T\ \mathit{ok\text{-}constraint}}$$

WF-CLASS-INSTANCE

$$\frac{\begin{array}{c}CT(C) = \texttt{class}\ C\texttt{<}\overline{X}\texttt{>} : \overline{M}, K\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A}\ = \overline{V};\ \overline{W}\ \overline{f};\ kd\ \overline{md}\} \\ \Delta \vdash \overline{T}\ \mathit{ok} \qquad \Delta \vdash [\overline{T}/\overline{X}]\mathit{propag\text{-}c}(C\texttt{<}\overline{X}\texttt{>})\ \mathit{satisfied}\end{array}}{\Delta \vdash C\texttt{<}\overline{T}\texttt{>}\ \mathit{ok}}$$

WF-ASSOC-TYPE-INTERF

$$\frac{\begin{array}{c}\mathcal{D}(I\texttt{<}T\texttt{>}, G) = \texttt{interface}\ I\texttt{<}\overline{T}\texttt{>} : \overline{M}\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A};\ \texttt{require}\ \overline{rd_2};\ \overline{ms};\} \\ \Delta \vdash G <: I\texttt{<}\overline{T}\texttt{>} \qquad \Delta \vdash G\ \mathit{ok}\ \text{or}\ G = \texttt{this}\end{array}}{\Delta \vdash G :: A_i\ \mathit{ok},\ \text{for all}\ i}$$

WF-ASSOC-TYPE-CLASS

$$\frac{\begin{array}{c}\mathcal{D}(C\texttt{<}T\texttt{>}, U) = \texttt{class}\ C\texttt{<}\overline{T}\texttt{>} : \overline{M}\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A} = \overline{V};\ \overline{W}\ \overline{f};\ kd\ \overline{md}\} \\ \Delta \vdash U <: C\texttt{<}\overline{T}\texttt{>} \qquad \Delta \vdash U\ \mathit{ok}\ \text{or}\ U = \texttt{this}\end{array}}{\Delta \vdash U :: A_i\ \mathit{ok},\ \text{for all}\ i}$$

Fig. 8. Subtyping, type equality, and well-formedness rules of FGJ+APR.

$$\textsc{ty-var}\quad \frac{}{\Delta; \Gamma \vdash x : \Gamma(x)} \qquad \textsc{ty-sub}\quad \frac{\Delta; \Gamma \vdash e : T \qquad \Delta \vdash T <: U}{\Delta; \Gamma \vdash e : U} \qquad \textsc{ty-new}\quad \frac{\Gamma; \Delta \vdash \overline{e} : \overline{W} \qquad \Delta \vdash K \ ok \\ \mathit{fields}(K) = \overline{W}\ \overline{f}}{\Delta \vdash \texttt{new}\ K(\overline{e}) : K}$$

$$\textsc{ty-fld}\quad \frac{\Delta; \Gamma \vdash e : K \qquad \mathit{fields}(K) = \overline{W}\ \overline{f}}{\Delta; \Gamma \vdash e_i.f_i : W_i} \qquad \textsc{ty-meth}\quad \frac{\Gamma \vdash e : P \qquad \Delta \vdash \overline{e} : \overline{T} \qquad \overline{T} <: \overline{U} \\ \langle m, \overline{U} \rightarrow V\rangle \in \mathit{msigs\text{-}decl}(P)}{\Delta; \Gamma \vdash e.m(\overline{e}) : V}$$

$$\textsc{ty-ucast}\quad \frac{\Delta; \Gamma \vdash e : T \\ \Delta \vdash T <: O \qquad \Delta \vdash O \ ok}{\Delta; \Gamma \vdash (O)e : O} \qquad \textsc{ty-dcast}\quad \frac{\Delta; \Gamma \vdash e : T \qquad \Delta \vdash O \ ok \\ \Delta \vdash O \neq T \qquad \Delta \vdash O <: T}{\Delta; \Gamma \vdash (O)e : O}$$

$$\textsc{ty-scast}\quad \frac{\Delta; \Gamma \vdash e : T \qquad \Delta \vdash O \ ok \qquad \Delta \vdash O \not<: T \qquad \Delta \vdash T \not<: O \\ T \text{ is a class instance} \qquad O \text{ is a class instance} \qquad \mathit{stupid\ warning}}{\Delta; \Gamma \vdash (O)e : O}$$

Fig. 9. Typing rules for expressions.

class, the environment in our formalism is larger as a result of constraint propagation. This amounts to fewer explicit constraints on type parameters being necessary. Note, however, that generic definitions are still type-checked separately. Type checking may require examining classes used as ancestors of the class being checked, or classes used in its constraints. This must be done recursively, but it is not significantly different than guaranteeing that, say, references to fields are valid. Regarding well-formed classes, the special class `object` is allowed to have no base class, and is assumed to be defined as an empty class with no bases.

Other helper definitions for these rules include *assoc-decl*, which collects the names of all associated types declared in a given class or interface or in its ancestors; *assoc-def* collects the names of associated types defined and bound to types in a given class or in its base classes. These definitions help to establish that no associated type is left unbound in a class definition. The functions *msigs-decl* and *msigs-def* serve a similar purpose for methods. The function *fields* collects all field definitions from a given class and its superclasses.

The rules for constraint propagation are defined in Figure 12. For some instance E<$\overline{T}$>, $\mathit{constr}(E$<$\overline{T}$>$)$ includes all direct constraints of E, both from **where** clauses and **require** clauses, and constraints for all instances that occur as direct bases or in direct constraints of E (recursively). This set may contain constraints of the form $N : M$, which are between two instances. Such constraints are filtered out using *propag-c*, and only constraints of the form $G : P$ or $G == T$ remain. We call such constraints *propagable.*

WF-SUBT-CONSTR

$$\frac{\Delta \vdash G\ \mathit{ok} \qquad \Delta \vdash L\ \mathit{ok\text{-}constraint}}{\Delta \vdash G : L\ \mathit{ok}}$$

WF-SAMET-CONSTR

$$\frac{\Delta \vdash G\ \mathit{ok} \qquad \Delta \vdash U\ \mathit{ok}}{\Delta \vdash G == U\ \mathit{ok}}$$

SEMI-WF-SUBT-CONSTR

$$\frac{\Delta \vdash O\ \mathit{ok} \qquad \Delta \vdash P\ \mathit{ok\text{-}constraint}}{\Delta \vdash O : P\ \mathit{semi\text{-}ok}}$$

SEMI-WF-SAMET-CONSTR

$$\frac{\Delta \vdash O\ \mathit{ok} \qquad \Delta \vdash P\ \mathit{ok}}{\Delta \vdash O == P\ \mathit{semi\text{-}ok}}$$

SEMI-WF-THIS-CONSTR

$$\frac{\Delta \vdash P\ \mathit{ok\text{-}constraint}}{\Delta \vdash \texttt{this} : P\ \mathit{semi\text{-}ok}}$$

$$\frac{\Delta \vdash U <: P \qquad \Delta \vdash U : P\ \mathit{semi\text{-}ok}}{\Delta \vdash U : P\ \mathit{satisfied}} \qquad \frac{\Delta \vdash U == T \qquad \Delta \vdash U == T\ \mathit{semi\text{-}ok}}{\Delta \vdash U == T\ \mathit{satisfied}}$$

CLASS-DEF-OK

$$\frac{\begin{array}{c} \Delta = \mathit{env\text{-}for\text{-}body}(C) \qquad \sigma = [C\texttt{<}\overline{X}\texttt{>}/\texttt{this}] \qquad \Delta \vdash \overline{M}\ \mathit{ok\text{-}constraint} \\ \Delta \vdash K\ \mathit{ok} \qquad \Delta \vdash \overline{rd_1}\ \mathit{ok} \qquad \mathit{assoc\text{-}decl}(\overline{M}) \subseteq \overline{A}, \mathit{assoc\text{-}def}(K) \\ \overline{A} \text{ and } \mathit{assoc\text{-}def}(K) \text{ disjoint} \qquad \Delta \vdash \sigma\overline{V}\ \mathit{ok} \qquad \Delta \vdash \sigma\overline{W}\ \mathit{ok} \\ \mathit{fields}(K) = \overline{U}\ \overline{g} \qquad \overline{f} \text{ and } \overline{g} \text{ disjoint} \qquad \mathit{kd} = C(\overline{U}\ \overline{g}, \overline{W}\ \overline{f})\{\texttt{base}(\overline{g}); \texttt{this}.\overline{f} = \overline{f};\} \\ \Delta \vdash \sigma\overline{\mathit{md}}\ \mathit{ok} \qquad \Delta \vdash \sigma(\mathit{propag\text{-}c}(C\texttt{<}\overline{X}\texttt{>}))\mathit{satisfied} \end{array}}{\texttt{class}\ C\texttt{<}\overline{X}\texttt{>} : \overline{M}, K\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A}\ = \overline{V};\ \overline{W}\ \overline{f};\ \mathit{kd}\ \overline{\mathit{md}}\}\ \mathit{ok}}$$

INTERFACE-DEF-OK

$$\frac{\begin{array}{c} \Delta = \mathit{env\text{-}for\text{-}body}(I) \\ \Delta \vdash \overline{M}\ \mathit{ok\text{-}constraint} \qquad \Delta \vdash \overline{rd_1}\ \mathit{ok} \qquad \Delta \vdash \overline{rd_2}\ \mathit{ok} \qquad \Delta \vdash \overline{\mathit{ms}}\ \mathit{ok} \\ \langle m, T\rangle \in \mathit{msigs\text{-}def}(\overline{M}) \text{ and } \langle m, U\rangle \in \mathit{msigs\text{-}def}(\overline{M}) \text{ implies } \Delta \vdash T == U \end{array}}{\texttt{interface}\ I\texttt{<}\overline{X}\texttt{>} : \overline{M}\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A};\ \texttt{require}\ \overline{rd_2};\ \overline{\mathit{ms}};\}\ \mathit{ok}}$$

$$\frac{\Delta \vdash T \text{ ok} \qquad \vdash \overline{V} \text{ ok}}{\Delta \vdash T\ m(\overline{V}\ \overline{x})\ \mathit{ok}} \qquad \frac{\begin{array}{c} \Delta \vdash T\ m(\overline{V}\ \overline{x})\ \mathit{ok} \qquad \Delta \vdash U <: T \\ \Delta; \overline{x} : \overline{V}, \texttt{this} : \texttt{this} \vdash e : U \end{array}}{\Delta \vdash T\ m(\overline{V}\ \overline{x})\ \{\texttt{return}\ e;\}\ \mathit{ok}}$$

$$\frac{CT(C) = \texttt{class}\ C\texttt{<}\overline{X}\texttt{>} : \overline{M}, K\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A}\ = \overline{V};\ \overline{W}\ \overline{f};\ \mathit{kd}\ \overline{\mathit{md}}\}}{\mathit{env\text{-}for\text{-}body}(C) = \overline{X}, \mathit{propag\text{-}c}(\overline{rd_1}), \mathit{propag\text{-}c}(\overline{M}, K), \texttt{this} : C\texttt{<}\overline{X}\texttt{>}}$$

$$\frac{CT(I) = \texttt{interface}\ I\texttt{<}\overline{X}\texttt{>} : \overline{M}\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A};\ \texttt{require}\ \overline{rd_2};\ \overline{\mathit{ms}};\}}{\mathit{env\text{-}for\text{-}body}(I) = \overline{X}, \mathit{propag\text{-}c}(\overline{M}), \mathit{propag\text{-}c}(\overline{rd_1}, \overline{rd_2}), \texttt{this} : I\texttt{<}\overline{X}\texttt{>}}$$

Fig. 10. Well-formed constraints, classes and interfaces, and necessary helper definitions.

$$\frac{CT(I) = \texttt{interface}\ I\texttt{<}\overline{X}\texttt{>} : \overline{M}\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A};\ \texttt{require}\ \overline{rd_2};\ \overline{ms};\}}{A_i \in \textit{assoc-decl}(I\texttt{<}\overline{T}\texttt{>}),\ \text{for all}}$$

$$\frac{CT(I) = \texttt{interface}\ I\texttt{<}\overline{X}\texttt{>} : \overline{M}\ \ldots \qquad B \in \textit{assoc-decl}(M_i),\ \text{for some } i}{B \in \textit{assoc-decl}(I\texttt{<}\overline{T}\texttt{>})}$$

$$\frac{CT(C) = \texttt{class}\ C\texttt{<}\overline{X}\texttt{>} : \overline{M}, K\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A}\ = \overline{V}; \overline{W}\ \overline{f};\ kd\ \overline{md}\}}{A_i \in \textit{assoc-def}(C\texttt{<}\overline{T}\texttt{>}),\ \text{for all } i}$$

$$\frac{CT(C) = \texttt{class}\ C\texttt{<}\overline{X}\texttt{>} : \overline{M}, K\ \ldots \qquad B \in \textit{assoc-def}(K)}{B \in \textit{assoc-def}(C\texttt{<}\overline{T}\texttt{>})} \qquad \frac{A \in \textit{assoc-def}(T)}{A \in \textit{assoc-decl}(T)}$$

$$\frac{\begin{array}{c}\mathcal{D}(C\texttt{<}\overline{T}\texttt{>}, \texttt{this}) =\ \texttt{class}\ C\texttt{<}\overline{T}\texttt{>} : \overline{M}, K\ \texttt{where}\ \overline{rd}\ \{\texttt{type}\ \overline{A} = \overline{W};\ \overline{U_1}\ \overline{f_1};\ kd\ \overline{md}\}\\ \textit{fields}(K) = \overline{U_2}\ \overline{f_2}\end{array}}{\textit{fields}(C\texttt{<}\overline{T}\texttt{>}) = \overline{U_2}\ \overline{f_2}, \overline{U_1}\ \overline{f_1}}$$

$$\frac{\begin{array}{c}\mathcal{D}(I\texttt{<}\overline{T}\texttt{>}, \texttt{this}) = \texttt{interface}\ I\texttt{<}\overline{X}\texttt{>} : \overline{M}\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A};\ \texttt{require}\ \overline{rd_2};\ \overline{ms};\}\\ V\ m(\overline{U}\ \overline{x}) \in \overline{ms}\end{array}}{\langle m, \overline{U} \to V\rangle \in \textit{msigs-decl}(I\texttt{<}\overline{T}\texttt{>})}$$

$$\frac{\begin{array}{c}\mathcal{D}(I\texttt{<}\overline{T}\texttt{>}, \texttt{this}) = \texttt{interface}\ I\texttt{<}\overline{T}\texttt{>} : \overline{M}\ \ldots\\ \langle m, \overline{U} \to V\rangle \in \textit{msigs-decl}(M_i),\ \text{for some } i\end{array}}{\langle m, \overline{U} \to V\rangle \in \textit{msigs-decl}(I\texttt{<}\overline{T}\texttt{>})}$$

$$\frac{\begin{array}{c}\mathcal{D}(C\texttt{<}\overline{T}\texttt{>}, \texttt{this}) = \texttt{class}\ C\texttt{<}\overline{T}\texttt{>} : \overline{M}, K\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A}\ = \overline{V}; \overline{W}\ \overline{f};\ kd\ \overline{md}\}\\ S\ m(\overline{U}\ \overline{x})\ \{\texttt{return}\ e;\} \in \overline{md}\end{array}}{\langle m, \overline{U} \to S\rangle \in \textit{msigs-def}(C\texttt{<}\overline{T}\texttt{>})}$$

$$\frac{\begin{array}{c}\mathcal{D}(C\texttt{<}\overline{T}\texttt{>}, \texttt{this}) = \texttt{class}\ C\texttt{<}\overline{X}\texttt{>} : \overline{M}, K\ \ldots\\ \langle m, \overline{U} \to S\rangle \in \textit{msigs-def}(K)\end{array}}{\langle m, \overline{U} \to S\rangle \in \textit{msigs-def}(C\texttt{<}\overline{T}\texttt{>})} \qquad \frac{\langle m, \overline{U} \to S\rangle \in \textit{msigs-def}(T)}{\langle m, \overline{U} \to S\rangle \in \textit{msigs-decl}(T)}$$

$$\frac{\begin{array}{c}\mathcal{D}(C\texttt{<}T\texttt{>}, \texttt{this}) =\ \texttt{class}\ C\texttt{<}\overline{T}\texttt{>} : \overline{P}\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A} = \overline{V};\ \overline{W}\ \overline{f};\ kd\ \overline{md}\}\\ S\ m(\overline{U}\ \overline{x})\ \{\texttt{return}\ e;\} \in \overline{md}\end{array}}{\textit{mbody}(C\texttt{<}\overline{T}\texttt{>}.m) = \langle \overline{x}, e\rangle}$$

$$\frac{\begin{array}{c}\mathcal{D}(C\texttt{<}\overline{T}\texttt{>}, \texttt{this}) =\ \texttt{class}\ C\texttt{<}\overline{T}\texttt{>} : \overline{M}, K\ \texttt{where}\ \overline{rd}\ \{\texttt{type}\ \overline{A} = \overline{V};\ \overline{W}\ \overline{f};\ kd\ \overline{md}\}\\ m\ \text{not defined in}\ \overline{md} \qquad \textit{mbody}(K.m) = \langle \overline{x}, e\rangle\end{array}}{\textit{mbody}(C\texttt{<}\overline{T}\texttt{>}.m) = \langle \overline{x}, e\rangle}$$

Fig. 11. Lookup functions for associated types, fields, method signatures, and bodies.

CPRG-RIGHT-SUB

$$\frac{\begin{array}{c} CT(E) = \texttt{class/interface}\ E\texttt{<}\overline{X}\texttt{>}\ \ldots \\ U : E\texttt{<}\overline{T}\texttt{>} \in \mathit{constr}(V) \qquad R \in \mathit{constr}(E\texttt{<}\overline{X}\texttt{>}) \end{array}}{[\overline{T}/\overline{X}, U/\texttt{this}]R \in \mathit{constr}(V)}$$

CPRG-INHERIT

$$\frac{\mathcal{D}(E\texttt{<}\overline{T}\texttt{>}, \texttt{this}) = \texttt{class/interface}\ E\texttt{<}\overline{T}\texttt{>} : \overline{P}\ \ldots}{E\texttt{<}\overline{T}\texttt{>} : P_i \in \mathit{constr}(E\texttt{<}\overline{T}\texttt{>}),\ \text{for all } i}$$

CPRG-CLASS-DEF

$$\frac{\mathcal{D}(C\texttt{<}\overline{T}\texttt{>}, \texttt{this}) = \texttt{class}\ C\texttt{<}\overline{T}\texttt{>} : \overline{P}\ \texttt{where}\ \overline{rd}\ \{\texttt{type}\ \overline{A} = \overline{U};\ \overline{W}\ \overline{f};\ kd\ \overline{md}\}}{\overline{rd} \subseteq \mathit{constr}(C\texttt{<}\overline{T}\texttt{>})}$$

CPRG-INTERF-DEF

$$\frac{\mathcal{D}(I\texttt{<}\overline{T}\texttt{>}, \texttt{this}) = \texttt{interface}\ I\texttt{<}\overline{T}\texttt{>} : \overline{M}\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A};\ \texttt{require}\ \overline{rd_2};\ \overline{ms};\}}{\overline{rd_1}, \overline{rd_2} \subseteq \mathit{constr}(I\texttt{<}\overline{T}\texttt{>})}$$

CPRG-COMB-SUB

$$\frac{\mathit{constr}(T) = \overline{rd_1} \qquad \mathit{constr}(P) = \overline{rd_2}}{\mathit{constr}(T : P) = T : P, \overline{rd_1}, \overline{rd_2}}$$

CPRG-COMB-SAME

$$\frac{\mathit{constr}(T) = \overline{rd_1} \qquad \mathit{constr}(U) = \overline{rd_2}}{\mathit{constr}(T == U) = T == U, \overline{rd_1}, \overline{rd_2}}$$

$$\frac{}{G : P\ \mathit{propagable}} \qquad \frac{}{G == U\ \mathit{propagable}}$$

$$\frac{R \in \mathit{constr}(T) \qquad R\ \mathit{propagable}}{R \in \mathit{propag\text{-}c}(T)} \qquad \frac{R \in \mathit{constr}(Q) \qquad R\ \mathit{propagable}}{R \in \mathit{propag\text{-}c}(Q)}$$

Fig. 12. Definitions of *constr* and *propag-c* used for constraint propagation.

$$\frac{\Delta \vdash T ==_{weak} E\texttt{<}\overline{U}\texttt{>}}{E\texttt{<}\overline{U}\texttt{>} \in \mathit{canon\text{-}weak\text{-}inst}_{\Delta}(T)} \qquad\qquad \frac{X \in \Delta \qquad \Delta \vdash T ==_{weak} X}{X \in \mathit{canon\text{-}weak\text{-}tvar}_{\Delta}(T)}$$

$$\frac{\Delta \vdash T ==_{weak} U :: A}{U :: A \in \mathit{canon\text{-}weak\text{-}assoc}_{\Delta}(T)}$$

$$\frac{}{\mathit{canon\text{-}weak}_{\Delta}(T) = \mathit{first}\begin{pmatrix} \mathit{order\text{-}set}(\mathit{canon\text{-}weak\text{-}inst}_{\Delta}(T)) \; + \\ \mathit{order\text{-}set}(\mathit{canon\text{-}weak\text{-}tvar}_{\Delta}(T)) \; + \\ \mathit{order\text{-}set}(\mathit{canon\text{-}weak\text{-}assoc}_{\Delta}(T)) \end{pmatrix}}$$

CANON-TVAR

$$\frac{\mathit{canon\text{-}weak}_{\Delta}(T) = X \qquad X \in \Delta_v}{\mathit{canon}_{\Delta}(T) = X}$$

CANON-INSTANCE

$$\frac{\mathit{canon\text{-}weak}_{\Delta}(T) = E\texttt{<}\overline{U}\texttt{>} \qquad \mathit{canon}_{\Delta}(\overline{U}) = \overline{W}}{\mathit{canon}_{\Delta}(T) = E\texttt{<}\overline{W}\texttt{>}}$$

CANON-ASSOC

$$\frac{\mathit{canon\text{-}weak}_{\Delta}(T) = U :: A \qquad \mathit{canon}_{\Delta}(U) = S \qquad \Delta \vdash S \not<: C\texttt{<}\overline{W}\texttt{>}, \text{for all } C}{\mathit{canon}_{\Delta}(T) = S :: A}$$

CANON-ASSOC-DEF

$$\frac{\begin{array}{c} \mathit{canon\text{-}weak}_{\Delta}(T) = U :: A_i \qquad \mathit{canon}_{\Delta}(U) = S \qquad \Delta \vdash S <: C\texttt{<}\overline{W}\texttt{>}, \text{for some } C \\ \mathcal{D}(C\texttt{<}\overline{W}\texttt{>}, S) = \texttt{class } C\texttt{<}\overline{W}\texttt{>} : \overline{M} \texttt{ where } \overline{rd_1} \; \{\texttt{type } \overline{A} = \overline{V};\; ...\} \qquad {V_i}' = \mathit{canon}_{\Delta}(V_i) \end{array}}{\mathit{canon}_{\Delta}(T) = {V_i}'}$$

$$\frac{\begin{array}{c} CT(I) = \texttt{interface } I\texttt{<}\overline{X}\texttt{>}\ldots \\ \mathit{assoc\text{-}decl}(I) = \overline{A} \end{array}}{\overline{X}, \overline{\texttt{this} :: A} \subseteq \mathit{full\text{-}assocs\text{-}tparams}(I)} \qquad\qquad \frac{\begin{array}{c} CT(C) = \texttt{class } C\texttt{<}\overline{X}\texttt{>}\ldots \\ \mathit{assoc\text{-}def}(C) = \overline{A} \end{array}}{\overline{X}, \overline{\texttt{this} :: A} \subseteq \mathit{full\text{-}assocs\text{-}tparams}(C)}$$

$$\frac{T \in \mathit{full\text{-}assocs\text{-}tparams}(E) \qquad \mathit{env\text{-}for\text{-}body}(E) \vdash T :: A \; \mathit{ok}}{T :: A \in \mathit{full\text{-}assocs\text{-}tparams}(E)}$$

$$\frac{G \in \mathit{full\text{-}assocs\text{-}tparams}(E) \qquad \Delta = \mathit{env\text{-}for\text{-}body}(E) \qquad \mathit{canon}_{\Delta}(G) = T}{T \in \mathit{full\text{-}tparams}(E)}$$

Fig. 13. Definitions of *canon* and *full-tparams* functions used in the translation.

5.3 Translation

The definition of the translation function $[\![\cdot]\!]_{\Delta}$ from FGJ+APR to FGJ+I is shown in Figure 14. Regarding notation, we apply the translation freely to a set of types, or constraints, and take it to mean that each element of the set is translated, and a new set produced as a result. In particular, type environments contain subtype and same-type constraints, and type parameter names. Translating such an environment means translating each element with the appropriate rule and combining the results into a set. Note that $\emptyset$ as the result of a translation in the constraint translation rules means that the constraint is removed in the translation. The interesting parts of the rules are the translations of constrainable types, instances, and class and interface definitions, particularly the coordination to ensure that the type parameters used to represent associated types match in their uses and definitions.

$$\frac{\mathit{canon}_{\Delta}(V) = E\texttt{<}\overline{T}\texttt{>} \qquad \mathit{CT}(E) = \texttt{class/interface}\ E\texttt{<}\overline{X}\texttt{>}\ldots}{\llbracket V \rrbracket_{\Delta} = E\texttt{<}\llbracket[\overline{T}/\overline{X}]\,\mathit{ord\text{-}full\text{-}tparams}(E)\rrbracket_{\Delta}\texttt{>}}$$

$$\frac{\mathit{canon}_{\Delta}(V) = G}{\llbracket V \rrbracket_{\Delta} = \mathit{translated\text{-}constrainable\text{-}type}(G)} \qquad \frac{}{\llbracket T\ m(\overline{U}\ \overline{x});\rrbracket_{\Delta} = \llbracket T \rrbracket_{\Delta}\ m(\llbracket\overline{U}\rrbracket_{\Delta}\ \overline{x});}$$

$$\frac{}{\llbracket T\ m(\overline{U}\ \overline{x})\{\texttt{return}\ e;\}\rrbracket_{\Delta} = \llbracket T \rrbracket_{\Delta}\ m(\llbracket\overline{U}\rrbracket_{\Delta}\ \overline{x})\{\texttt{return}\ \llbracket e\rrbracket_{\Delta};\}}$$

$$\frac{\mathit{CT}(E) = \texttt{class/interface}\ E\texttt{<}\overline{X}\texttt{>}\ldots \qquad \mathit{\Delta} = \mathit{env\text{-}for\text{-}body}(E)}{\mathit{transl\text{-}env\text{-}for\text{-}body}(E) = \llbracket \mathit{\Delta} \rrbracket_{\Delta}, \mathit{transl\text{-}ord\text{-}full\text{-}tparams}(E)}$$

$$\frac{\mathit{\Delta} = \mathit{env\text{-}for\text{-}body}(I) \qquad \mathit{transl\text{-}ord\text{-}full\text{-}tparams}(I) = \overline{Y}}{\begin{array}{c}\llbracket\texttt{interface}\ I\texttt{<}\overline{X}\texttt{>} : \overline{M}\ \texttt{where}\ \overline{rd_1}\ \{\texttt{type}\ \overline{A};\ \texttt{require}\ \overline{rd_2};\ \overline{ms};\}\rrbracket = \\ \texttt{interface}\ I\texttt{<}\overline{Y}\texttt{>} : \llbracket\overline{M}\rrbracket_{\Delta}\ \texttt{where}\ \llbracket\mathit{\Delta}\rrbracket_{\Delta}\{\llbracket\overline{ms}\rrbracket_{\Delta};\}\end{array}}$$

$$\frac{\mathit{\Delta} = \mathit{env\text{-}for\text{-}body}(C) \qquad \mathit{transl\text{-}ord\text{-}full\text{-}tparams}(C) = \overline{Y}}{\begin{array}{c}\llbracket\texttt{class}\ C\texttt{<}\overline{X}\texttt{>} : \overline{P}\ \texttt{where}\ \overline{rd}\ \{\texttt{type}\ \overline{A} = \overline{U};\ \overline{W}\ \overline{f};\ kd\ \overline{md}\}\rrbracket = \\ \texttt{class}\ C\texttt{<}\overline{Y}\texttt{>} : \llbracket\overline{P}\rrbracket_{\Delta}\ \texttt{where}\ \llbracket\mathit{\Delta}\rrbracket_{\Delta}\{\llbracket\overline{W}\rrbracket_{\Delta}\ \overline{f};\ \llbracket kd\rrbracket_{\Delta}\ \llbracket\overline{md}\rrbracket_{\Delta}\}\end{array}}$$

$$\frac{}{\llbracket\texttt{new}\ K(\overline{e})\rrbracket_{\Delta} = \texttt{new}\ \llbracket K\rrbracket_{\Delta}(\llbracket\overline{e}\rrbracket_{\Delta})} \qquad \frac{}{\llbracket T(e)\rrbracket_{\Delta} = \llbracket T\rrbracket_{\Delta}(\llbracket e\rrbracket_{\Delta})} \qquad \frac{}{\llbracket e.f\rrbracket_{\Delta} = (\llbracket e\rrbracket_{\Delta}).f}$$

$$\frac{}{\llbracket e.m(\overline{d})\rrbracket_{\Delta} = (\llbracket e\rrbracket_{\Delta}).m(\llbracket\overline{d}\rrbracket_{\Delta})} \qquad \frac{}{\llbracket x\rrbracket_{\Delta} = x} \qquad \frac{\llbracket U\rrbracket_{\Delta} \neq \texttt{this}}{\llbracket U : P\rrbracket_{\Delta} = \llbracket U\rrbracket_{\Delta} : \llbracket P\rrbracket_{\Delta}}$$

$$\frac{}{\llbracket\texttt{this} : T\rrbracket_{\Delta} = \emptyset} \qquad \frac{}{\llbracket T == U\rrbracket_{\Delta} = \emptyset}$$

Fig. 14. Definition of the translation function $\llbracket\cdot\rrbracket_{\Delta}$ from FGJ+APR to FGJ+I.

Translating some type T starts by finding a canonical form for T with the canon_{Δ} function, shown in Figure 13. This function selects one of the types that, based on $\mathit{\Delta}$, can be proven equal to T. The definition of canon_{Δ} is a bit involved. We first define the relation $==_{\mathit{weak}}$, which is a weaker form of the type equality relation $==$. The definition is obtained by substituting $==_{\mathit{weak}}$ for $==$ in the rules TE-REFL, TE-FROM-ENV, TE-TRANS, TE-SYM, TE-ASSOC-CRG, and TE-PARAM-CRG. Note that the substitution obviously does not apply to the $==$ on the left-hand side of $\vdash$ in the rule TE-FROM-ENV. Hence, $==_{\mathit{weak}}$ is the same as $==$, except that the rule TE-ASSOC-TYPE is excluded from the former.

The helper function $\mathit{canon\text{-}weak}_{\Delta}$ works by ordering equivalent types into a list, with all instances first, followed by all type variables, followed by all associated types; and picking the first element of this sequence. For this, we assume a function *order-set* that transforms a set of types into an ordered list, using some arbitrary but fixed order, e.g, lexicographical ordering based on the alphabetical ordering of the characters in the type expressions; and a function *first* that selects the first element from a list. The symbol + denotes list concatenation. If a type variable, the first element is already in canonical form. For an instance, the canonical form is obtained by canonicalizing the type arguments.

The translation of associated types, however, is more intricate. The two rules for associated types compensate for the TE-ASSOC-TYPE rule missing from the definition of $==_{weak}$, but in a way that would correspond to only applying TE-ASSOC-TYPE from left to right. A more straightforward definition without this restriction would be possible, we believe, but the current definition guarantees that canonicalization preserves the *ok* property of types, which make the safety proofs of the translation easier (see the proof of Lemma 9).

The *full-tparams* function collects the set of all associated types and type variables used in the definition of a given class or interface, recursing to its constraints and ancestors. The translated class or interface needs a type parameter for each element in this set. We can again use *order-set* to generate an ordered list from the set. We define $\textit{ord-full-tparams}(E) = \textit{order-set}(\textit{full-tparams}(E))$. To get a valid list of type parameter names, we also assume the existence of a *translated-constrainable-type* helper function that maps constrainable types into type variable names. The naming scheme can be arbitrary, as long as each distinct type is mapped into a distinct name, and to the same name every time. The *transl-ord-full-tparams* function, used in the translation rules, then applies *translated-constrainable-type* to each element of the ordered list obtained from the result of *ord-full-tparams*.

With the above tools the translation guarantees that the type argument list of the translation of any instance $E\texttt{<}\overline{T}\texttt{>}$ will match the type parameter list of the translation of the definition of the class or interface E.

Note that it is possible to write a class or interface definition with an inconsistent set of constraints. A class with inconsistent constraints can never be successfully instantiated. In particular, every environment in the program (generated by class and interface definitions) must satisfy the consistency rule that $\Delta \vdash E\texttt{<}\overline{T}\texttt{>} == F\texttt{<}\overline{U}\texttt{>}$ implies $E = F$ and $\Delta \vdash \overline{T} == \overline{U}$. We define programs violating this rule to be invalid; the translation is not guaranteed to work for invalid programs. Detecting inconsistencies that are troublesome for the translation can be accomplished by checking each class or interface definition prior to translation. The outline of an algorithm to perform this checking is as follows: (1) let Δ_1 be the environment generated from the class or interface using *env-for-body*; (2) generate a new environment Δ_2 by replacing each type in Δ_1 by its canonical form (computed using *canon*); (3) check that the canonical form of each instance $E\texttt{<}\overline{T}\texttt{>}$ in Δ_1 is some other instance of E; and (4) check that the transitive closure of the same-type constraints in Δ_2 is not inconsistent. Inconsistencies originating from subtype constraints that require a class to derive from two unrelated classes or interfaces are not detected with the above algorithm. Inconsistent constraints of this kind will, however, remain inconsistent in the translation, and are thus harmless.

5.4 Properties of the formalization

In order to show that our language extensions are type-safe and that our translation of these extensions into standard Generic C# is correct, we prove several properties of the extensions. We have defined translations on types, constraints, expressions, definitions, and environments; here, we show that these translations are consistent with each other and with vanilla FGJ+I. The semantics of our extensions are defined by translation into FGJ+I followed by evaluation in that system; the fact that our translation preserves program type behavior and typing then shows that our extensions are type-safe, as long as FGJ+I itself is type-safe. We start by establishing a number of minor results, and conclude with the theorems that state the main results about our language extensions.

Lemma 1.
a) If $\varDelta \vdash T == U$, then $\sigma\varDelta \vdash \sigma T == \sigma U$.
b) If $\varDelta \vdash T <: U$, then $\sigma\varDelta \vdash \sigma T <: \sigma U$.

Proof. a) This proof is by induction on the derivation that $\varDelta \vdash T == U$. For TE-REFL, TE-SYM, TE-TRANS, TE-ASSOC-CRG, TE-TPARAM-CRG, and TE-ASSOC-TYPE the result is trivial. For TE-FROM-ENV, the substitution to all constraints in the environment provides the desired result.

b) This proof is by induction on the derivation that $\varDelta \vdash T <: U$. For S-REFL, S-TRANS, and S-VIA-EQ, the result is trivial (S-VIA-EQ uses part (a) of this lemma). For S-FROM-ENV, the substitution to constraints in the environment provides the desired result. For S-CLASS, $\mathcal{D}(\sigma(E\texttt{<}\overline{V}\texttt{>}), \sigma(\texttt{this})) = \mathcal{D}(E\texttt{<}\sigma\overline{V}\texttt{>}, \sigma(\texttt{this})) = \sigma\mathcal{D}(E\texttt{<}\overline{V}\texttt{>}, \texttt{this})$ by the definitions of substitution and $\mathcal{D}$. Thus, the base classes and interfaces in $\overline{P}$ are also substituted appropriately, and so the subtype relationship still holds after applying σ.

Lemma 2. *If $\varDelta \vdash T$ ok, and $\varDelta \vdash \sigma$ ok, then $\sigma\varDelta \vdash \sigma T$ ok.*

Proof. The proof is by induction on the structure of T. If T is a type variable, it is either left alone by σ or is redefined to an *ok* type, since σ is *ok*. If T is a class or interface instance (say, $E\texttt{<}\overline{V}\texttt{>}$), all of the substituted type arguments $\sigma\overline{V}$ are *ok* by the induction hypothesis. They meet their bounds from E by Lemma 1 (the bounds in E have the correct substitution applied by WF-CLASS-INSTANCE and WF-INTERFACE-INSTANCE), and so $\sigma(E\texttt{<}\overline{V}\texttt{>}) = E\texttt{<}\sigma\overline{V}\texttt{>}$ is *ok*. Otherwise, T is an associated type $U :: A$. Thus, $\sigma T = \sigma U :: A$. It is known that σU is *ok* by the induction hypothesis, so all that remains is to show that σU has a member type A. Since $U :: A$ is *ok* in its unsubstituted form, $\varDelta$ must imply some constraint $U : F\texttt{<}\ldots\texttt{>}$, where $F\texttt{<}\ldots\texttt{>}$ has an associated type A. Thus, it must be true that $\varDelta \vdash U <: F\texttt{<}\ldots\texttt{>}$, and so $\varDelta \vdash \sigma U <: F\texttt{<}\ldots\texttt{>}$ by Lemma 1. Therefore, σU has an associated type A, and so $\sigma U :: A = \sigma T$ is *ok* in $\varDelta$.

The next lemma shows that if we have some environment $\varDelta$ where an instance is well-formed, some type U that would be well-formed in a class or interface definition, is well-formed in $\varDelta$ after substituting the instance's type arguments into any occurrences of type parameters in U.

Lemma 3. *If $\varDelta \vdash E\texttt{<}\overline{T}\texttt{>}$ ok-constraint, and $\varDelta \vdash W$ ok, and $\varDelta \vdash W <: E\texttt{<}\overline{T}\texttt{>}$, and $\sigma = [\overline{T}/\overline{X}, \overline{W}/\texttt{this}]$, and $CT(E) =$ `class/interface` $E\texttt{<}\overline{X}\texttt{>}$ ..., and env-for-body$(E) \vdash U$ ok, then $\varDelta \vdash \sigma U$ ok.*

Proof. Applying Lemma 2 to the assumption $\mathit{env\text{-}for\text{-}body}(E) \vdash U\ \mathit{ok}$ gives $\sigma(\mathit{env\text{-}for\text{-}body}(E)) \vdash \sigma U\ \mathit{ok}$. Under the assumption on CT, $\mathit{env\text{-}for\text{-}body}(E)$ consists of some type parameter names (which are all *ok* after substitution because $\Delta \vdash \overline{T}\ \mathit{ok}$) plus the requirements $\mathit{propag\text{-}c}(E\texttt{<}\overline{X}\texttt{>}), \texttt{this} : E\texttt{<}\overline{X}\texttt{>}$, and thus $\sigma(\mathit{propag\text{-}c}(E\texttt{<}\overline{X}\texttt{>}), \texttt{this} : E\texttt{<}\overline{X}\texttt{>}) \vdash \sigma U\ \mathit{ok}$ follows. This is the same as $\sigma(\mathit{propag\text{-}c}(E\texttt{<}\overline{X}\texttt{>})), W : E\texttt{<}\overline{T}\texttt{>} \vdash \sigma U\ \mathit{ok}$. We know that $\Delta \vdash W : E\texttt{<}\overline{T}\texttt{>}$ by assumption, and so it remains to show that $\Delta \vdash \sigma(\mathit{propag\text{-}c}(E\texttt{<}\overline{X}\texttt{>}))\ \mathit{satisfied}$. This is true since it follows from $\Delta \vdash W <: E\texttt{<}\overline{T}\texttt{>}$ (using CPRG-INHERIT and CPRG-RIGHT-SUB) that $\sigma(\mathit{constr}(E\texttt{<}\overline{X}\texttt{>}))$ is a subset of $\mathit{constr}(W)$, and so $\sigma(\mathit{propag\text{-}c}(E\texttt{<}\overline{X}\texttt{>}))$ is a subset of $\mathit{propag\text{-}c}(W)$.

Lemma 4. $\Delta \vdash T == \mathit{canon}_{\Delta}(T)$.

Proof. The proof is by induction on the derivation of $\mathit{canon}_{\Delta}(T)$ (i.e., the algorithm specified in the rules for computing $\mathit{canon}_{\Delta}(T)$). By the definition of *canon-weak*, $\mathit{canon\text{-}weak}_{\Delta}(T)$ is one of the types that satisfy $\Delta \vdash T ==_{\mathit{weak}} U$. Because $\Delta \vdash T ==_{\mathit{weak}} U$ implies $\Delta \vdash T == U$, it follows that $\Delta \vdash T == \mathit{canon\text{-}weak}_{\Delta}(T)$. Based on this observation, the CANON-TVAR case is trivial. By the induction hypothesis, the type arguments are equal to their canonical forms in the CANON-INSTANCE case; thus, the main result follows from TE-TPARAM-CRG. The CANON-ASSOC case is by the induction hypothesis and TE-ASSOC-CRG, using similar reasoning. In the CANON-ASSOC-DEF case, the fact that $\Delta \vdash T == U :: A$, for some U and A, follows from $\mathit{canon\text{-}weak}_{\Delta} = U :: A$. By the induction hypothesis and TE-ASSOC-CRG, $\Delta \vdash T == S :: A$, where S inherits from some class that binds some type V to the associated type A. Thus, by TE-ASSOC-TYPE, TE-SYM, and TE-TRANS, $\Delta \vdash T == V$, from which the result follows by the induction hypothesis.

Lemma 5. $\Delta \vdash T == U$ *if and only if* $\mathit{canon}_{\Delta}(T) = \mathit{canon}_{\Delta}(U)$.

Proof.
($\longleftarrow$) A consequence of Lemma 4, and the TE-SYM and TE-TRANS rules.
($\longrightarrow$) The proof is by induction on the derivation that $\Delta \vdash T == U$. For TE-REFL, TE-TRANS, and TE-SYM the property follows directly from the induction hypothesis and properties of equivalence ($=$) on types. For TE-FROM-ENV, $\Delta \vdash T ==_{\mathit{weak}} U$ follows from $\Delta \vdash T == U$ because $==_{\mathit{weak}}$ includes TE-FROM-ENV. Thus, $\mathit{canon\text{-}weak}_{\Delta}(T) = \mathit{canon\text{-}weak}_{\Delta}(U)$ by the definition of *canon-weak*, and thus by the definition of *canon*, also $\mathit{canon}_{\Delta}(T) = \mathit{canon}_{\Delta}(U)$. For TE-TPARAM-CRG, the property follows from CANON-INSTANCE and the induction hypothesis. TE-ASSOC-CRG uses the definition of *canon* for associated types (the CANON-ASSOC and CANON-ASSOC-DEF rules), and the induction hypothesis. The TE-ASSOC-TYPE case follows from the CANON-ASSOC-DEF rule.

The following lemma states that the name of the class or an interface is preserved in the translation:

Lemma 6. *Assume* $E \in \mathit{dom}(CT)$, $\Delta \vdash \Delta\ \mathit{ok}$, *and* $\Delta \vdash \overline{T}\ \mathit{ok}$.
$[\![E\texttt{<}\overline{T}\texttt{>}]\!]_{\Delta} = E\texttt{<}\overline{U}\texttt{>}$ *for some* $\overline{U}$.

Proof. Because Δ is consistent, $\Delta \vdash E\texttt{<}\overline{T}\texttt{>} == F\texttt{<}\overline{U}\texttt{>}$ implies $E = F$. Thus $\mathit{canon}_\Delta(E\texttt{<}\overline{T}\texttt{>}) = E\texttt{<}\overline{U}\texttt{>}$ for some $\overline{U}$. The lemma then follows from the definition of translation for instantiated classes or interfaces.

Theorem 1.
a) If $\Delta \vdash T == U$, then $[\![T]\!]_\Delta$ and $[\![U]\!]_\Delta$ are the same type in FGJ+I.
b) Assume $E \in \mathit{dom}(CT)$, $\Delta = \mathit{env\text{-}for\text{-}body}(E)$, and $\Delta' = \mathit{transl\text{-}env\text{-}for\text{-}body}(E)$. If $\Delta \vdash T <: P$, then $\Delta' \vdash [\![T]\!]_\Delta <: [\![P]\!]_\Delta$.

Proof. a) The translation of a type is defined as the translation of its canonicalization (computed by *canon*). Thus, the theorem follows directly from Lemma 5.

b) The proof is by induction on the derivation of $\Delta \vdash T <: P$, with case analysis on the last rule used. There are five subtyping rules: the cases for S-REFL and S-TRANS are straightforward; and the case for S-FROM-ENV follows because $\mathit{transl\text{-}env\text{-}for\text{-}body}(E)$ includes translations of all constraints in $\mathit{env\text{-}for\text{-}body}(E)$. The case for S-VIA-EQ follows from Theorem 1(a). In the final case S-CLASS, let $T = F\texttt{<...>}$. Lemma 6 ensures that the translation of T is of the form $F\texttt{<...>}$. The case, and thus the lemma, follows from the definition of the translation of class and interface definitions, which preserves inheritance declarations.

Lemma 7. *If $\Delta \vdash T ==_{weak} U$, $\Delta \vdash \Delta$ ok, and either $\Delta \vdash T$ ok or $\Delta \vdash U$ ok, then both $\Delta \vdash T$ ok and $\Delta \vdash U$ ok.*

Proof. The proof is by induction on the structure of the derivation that Δ proves $T ==_{weak} U$, with case analysis on the last rule used. The cases TE-REFL, TE-TRANS, TE-SYM, and TE-TPARAM-CRG are trivial. TE-FROM-ENV follows from $\Delta \vdash \Delta$ *ok*, because all constraints in Δ are *ok* in Δ, and so all types mentioned in those constraints are *ok* in Δ by the definition of a constraint being *ok*. For TE-ASSOC-CRG, let T be $V :: A$ and U be $W :: A$. Assume without loss of generality that $V :: A$ is *ok*. That means that V is *ok*, and so W is *ok* by the induction hypothesis. Therefore, W is a subtype of everything V is a subtype of by S-VIA-EQ, and in particular it is a subtype of whatever contains the associated type A. Therefore, W has the associated type A and W is *ok* so $W :: A$ is *ok*. This completes the last case and the proof.

Lemma 8. *If $\Delta \vdash T$ ok and $\Delta \vdash \Delta$ ok, then $\Delta \vdash \mathit{canon\text{-}weak}_\Delta(T)$ ok.*

Proof. Follows directly from Lemma 7 and from $\Delta \vdash T ==_{weak} \mathit{canon\text{-}weak}_\Delta(T)$, which is obvious by the definition of $\mathit{canon\text{-}weak}_\Delta$.

Lemma 9. *If $\Delta \vdash T$ ok and $\Delta \vdash \Delta$ ok, then $\Delta \vdash \mathit{canon}_\Delta(T)$ ok.*

Proof. The proof is by induction on the derivation of $\mathit{canon}_\Delta(T)$. The CANON-TVAR case follows from $\Delta \vdash \mathit{canon\text{-}weak}_\Delta(T)$ *ok*, which is true by Lemma 8. The CANON-INSTANCE case follows from the induction hypothesis and from Lemma 4. Similarly, the induction hypothesis together with Lemma 4 proves the CANON-ASSOC case. In the final case CANON-ASSOC-DEF, S in the premise of the rule is *ok* in Δ by induction hypothesis, and thus also for $C\texttt{<}\overline{W}\texttt{>}$ in the rule, $\Delta \vdash C\texttt{<}\overline{W}\texttt{>}$ *ok*, and thus by CLASS-DEF-OK and Lemma 3, $\Delta \vdash V_i$ *ok*.

$$\frac{\overline{T}\ \mathit{proper}}{C\texttt{<}\overline{T}\texttt{>}\ \mathit{proper}} \qquad \frac{\overline{T}\ \mathit{proper} \qquad \mathit{assoc\text{-}decl}(I\texttt{<}\overline{T}\texttt{>}) = \emptyset}{I\texttt{<}\overline{T}\texttt{>}\ \mathit{proper}} \qquad \frac{}{G\ \mathit{proper}}$$

Fig. 15. The definition of *proper* types.

In the next lemma we use the definition of *proper* types, shown in Figure 15. Intuitively, proper types exclude all types that are, or contain, interfaces that have associated types.

Lemma 10. *If $\Delta \vdash T$ ok, then $canon_\Delta(T)$ proper.*

Proof. The proof is by induction on the derivation of $canon_\Delta(T)$. The case for CANON-TVAR gives a proper type trivially. For CANON-ASSOC, we know by the induction hypothesis that the base of the resulting associated type is proper, and that this base does not inherit from any class (or associated type with interfaces, by Lemma 9); thus, the produced associated type is proper. For CANON-INSTANCE, the type arguments of the produced type are proper by the induction hypothesis, and the produced type is *ok* by Lemma 9; thus, the produced type itself is proper. In the CANON-ASSOC-DEF case, the type from the first part of the rule serves as input to *canon* again, and so the resulting type is proper by the induction hypothesis.

Lemma 11. *If $\Delta \vdash T <: U$, $\Delta \vdash T$ ok, $\Delta \vdash U$ ok, U inherits from some class instance, and $\Delta \vdash V$ ok, then $\Delta \vdash [T/\texttt{this}]V == [U/\texttt{this}]V$.*

Proof. The proof is by induction on the structure of V. If V is an instance, all of its type arguments are *ok*, and so by the induction hypothesis, this lemma is satisfied for them; the result then follows for V by TE-TPARAM-CRG. If V is a type variable, V is not affected by the substitutions for `this`, and so the result follows by TE-REFL. For associated types of `this`, the desired property is that $\Delta \vdash T :: A == U :: A$, which is true by CLASS-DEF-OK. For associated types of other types the induction hypothesis ensures that the base type of V satisfies the lemma, and thus the result is true for all of V by TE-ASSOC-CRG and the definition of substitution.

Lemma 12. *If $CT(E) =$ `class/interface` $E\texttt{<}\overline{X}\texttt{>}\ \ldots$,
and $\Delta \vdash E\texttt{<}\overline{W}\texttt{>}$ ok-constraint, then $\Delta \vdash constr(E\texttt{<}\overline{W}\texttt{>})$ semi-ok and satisfied.*

Proof. Given an arbitrary constraint Q in $constr(E\texttt{<}\overline{W}\texttt{>})$, the proof will be by induction on the structure of the derivation that $Q \in constr(E\texttt{<}\overline{W}\texttt{>})$. If Q is from CPRG-CLASS-DEF or CPRG-INTERFACE-DEF, it is trivially *semi-ok* and *satisfied* because it is propagable, and so it is a member of $[\overline{W}/\overline{X}]propag\text{-}c(E)$. From $\Delta \vdash E\texttt{<}\overline{W}\texttt{>}$ *ok*, we know that $\Delta \vdash [\overline{W}/\overline{X}]propag\text{-}c(E)$. If Q is from CPRG-INHERIT, Q is satisfied by the subtyping rule S-CLASS, and is *semi-ok* by the rules for a class or interface definition, and its instances, being *ok-constraint.* If

Q is from CPRG-RIGHT-SUB, there are two types T and $F\texttt{<}\overline{V}\texttt{>}$ (where F accepts type parameters $\overline{Y}$), and a constraint R, such that Q is of the form σR, where $\sigma = [\overline{V}/\overline{Y}, T/\mathtt{this}]$. By the induction hypothesis, $T : F\texttt{<}\overline{V}\texttt{>}$ is *semi-ok* and *satisfied* in Δ; R is *semi-ok* and *satisfied* in *env-for-body*(F) by CLASS/INTERFACE-DEF-OK. Thus, $\Delta \vdash F\texttt{<}\overline{V}\texttt{>}$ *ok* and it must be shown that $\Delta \vdash \sigma R$ *semi-ok* and *satisfied.* By WF-CLASS-INSTANCE or WF-INTERF-INSTANCE and the equivalence between *env-for-body*$_c$ and *propag-c*, $\Delta \vdash \sigma($*env-for-body*$(F))$ *satisfied.* By Lemmas 2 and 1, $\sigma($*env-for-body*$(F)) \vdash \sigma R$ *semi-ok* and *satisfied*; thus $\Delta \vdash Q$ *semi-ok* and *satisfied.*

Lemma 13. *If $E \in dom(CT)$ and $\Delta =$ env-for-body(E), then $\Delta \vdash \Delta$ ok.*

Proof. The environment Δ is *ok* whenever each of its members (types and constraints) is *ok*. All of the type parameters in Δ are *ok* trivially, just by being members of Δ. Thus, the only interesting case is those members of Δ which are constraints. Let Q be a constraint from Δ. Δ contains exactly the constraints resulting from *env-for-body*(E). This function can only produce constraints from two sources: constraints on `this` and constraints that come from *propag-c* and thus from *constr*. The constraints on `this` are *semi-ok* by SEMI-WF-THIS-CONSTR. The other kinds of constraints are also included in *constr*$(E\texttt{<}\overline{X}\texttt{>})$, and so are *semi-ok* in Δ by Lemma 12. All of these constraints are propagable, and so their being *semi-ok* implies that they are *ok*. Thus, all elements of Δ are *ok* in Δ, and so $\Delta \vdash \Delta$ *ok*.

Lemma 14.
Assume $CT(E) =$ `class/interface` $E\texttt{<}\overline{X}\texttt{>}\ldots$. If $\Delta \vdash E\texttt{<}\overline{T}\texttt{>}$ ok-constraint and there exists some type W so that $\Delta \vdash W$ ok and $\Delta \vdash W <: E\texttt{<}\overline{T}\texttt{>}$, then for all $U \in [\overline{T}/\overline{X}, W/\mathtt{this}]$ord-full-tparams$(E)$, $\Delta \vdash U$ ok.

Proof. From the definitions of *full-tparams* and *ord-full-tparams* and Lemma 9, all elements of *ord-full-tparams*(E) are *ok* in *env-for-body*(E). The result is then an immediate application of Lemma 3.

Lemma 15. *If $CT(F) =$ `class/interface` $F\texttt{<}\overline{Y}\texttt{>}\ \ldots$, $\Delta_1 =$ env-for-body(F), $\Delta_1 \vdash F\texttt{<}\overline{U}\texttt{>}$ ok, and $\Delta_2 \vdash T$ ok, then $[\llbracket[\overline{U}/\overline{Y}]$ord-full-tparams$(F)\rrbracket_{\Delta_1}/$ transl-ord-full-tparams$(F)]\llbracket T\rrbracket_{\Delta_2} = \llbracket[\overline{U}/\overline{Y}]T\rrbracket_{\Delta_1}$.*

Proof. Let V be *canon*$_{\Delta_2}(T)$. The proof is by induction on the structure of V, which can be either a constrainable type or an instance, since by Lemma 10, V is *proper*. If V is a constrainable type, $\llbracket T\rrbracket_{\Delta_2}$ is a type in *transl-ord-full-tparams*(F), and so V is its corresponding entry in *ord-full-tparams*(F). Therefore, the left side of the equality above reduces to $\llbracket[\overline{U}/\overline{Y}]V\rrbracket_{\Delta_1}$, which is exactly the right side. If V is an instance type, assume it has the form $E\texttt{<}\overline{W}\texttt{>}$. The left side of the equality is $E\texttt{<}[\llbracket[\overline{U}/\overline{Y}]$*ord-full-tparams*$(F)\rrbracket_{\Delta_1}/$*transl-ord-full-tparams*$(F)]\llbracket\overline{W}\rrbracket_{\Delta_2}\texttt{>}$. By the induction hypothesis, the inside of this can be replaced with the right side of the equality, and this produces $E\texttt{<}\llbracket[\overline{U}/\overline{Y}]\overline{W}\rrbracket_{\Delta_1}\texttt{>}$. This, after applying the translation rule for instances, is exactly the same as the right side of the desired equality.

Theorem 2.
Assume env-for-body$(E) = \Delta$ *and transl-env-for-body*$(E) = \Delta'$. *If* $\Delta \vdash T\,ok$*, then* $\Delta' \vdash \llbracket T \rrbracket_\Delta$ *ok.*

Proof. The proof is by induction on the structure of $\mathit{canon}_\Delta(T)$, which can either be a constrainable type or an instance. Lemma 13 shows that $\Delta \vdash \Delta$ *ok*; Lemma 9 then shows that $\Delta \vdash \mathit{canon}_\Delta(T)$ *ok*. If $\mathit{canon}_\Delta(T)$ is a constrainable type, its translation is a type variable, which is *ok* in Δ' because Δ' is the result of *transl-env-for-body*.

The more challenging case is when $\mathit{canon}_\Delta(T)$ is an instance. If $\mathit{canon}_\Delta(T)$ is an instance, its type arguments are valid types because $\mathit{canon}_\Delta(T)$ is *ok*. Let $F\texttt{<}\overline{U}\texttt{>}$ be $\mathit{canon}_\Delta(T)$, and let $\overline{V}$ be $[\overline{U}/\overline{Y}]\mathit{ord\text{-}full\text{-}tparams}(F)$, where $\overline{Y}$ are the declared type parameters of F. All of $\overline{V}$ is *ok* in Δ by Lemma 14.

Given that all of $\overline{V}$ is *ok* in Δ, $\llbracket \overline{V} \rrbracket_\Delta$ is *ok* in Δ' by the induction hypothesis (allowed because the type arguments of an instance returned by *canon* are the results of recursive applications of *canon*, by the definition of *canon*). By the definition of the translation function and the assumption of $\mathit{canon}_\Delta(T)$ being an instance, $\llbracket T \rrbracket_\Delta$ is an instance, and in particular is $F\texttt{<}\llbracket \overline{V} \rrbracket_\Delta\texttt{>}$.

The final part of showing that $F\texttt{<}\llbracket \overline{V} \rrbracket_\Delta\texttt{>}$ is *ok* in Δ' is to show that $\llbracket \overline{V} \rrbracket_\Delta$ meets its constraints from the translated definition of F. For this, let Δ_2 be *env-for-body*(F), and let Δ'_2 be $\llbracket \Delta_2 \rrbracket_{\Delta_2}$ (i.e., the constraints from the translation of F). It is known that $\Delta \vdash [\overline{U}/\overline{Y}]\Delta_2$ because $F\texttt{<}\overline{U}\texttt{>}$ is *ok* in Δ; this gives $\Delta' \vdash \llbracket [\overline{U}/\overline{Y}]\Delta_2 \rrbracket_\Delta$ by Theorem 1. By Lemma 15, this is the same as $\Delta' \vdash [\llbracket [\overline{U}/\overline{Y}]\mathit{ord\text{-}full\text{-}tparams}(F) \rrbracket_\Delta / \mathit{transl\text{-}ord\text{-}full\text{-}tparams}(F)]\Delta'_2$. This becomes $\Delta' \vdash [\llbracket \overline{V} \rrbracket_\Delta / \mathit{transl\text{-}ord\text{-}full\text{-}tparams}(F)]\Delta'_2$ by the definition of $\overline{V}$. This statement says exactly that the new type arguments $\llbracket \overline{V} \rrbracket_\Delta$ meet the constraints Δ'_2 in the translation of F.

That completes the proof of the case for those T where $\mathit{canon}_\Delta(T)$ is an instance. Since *canon* can only return constrainable types and instances, the full theorem is now proven.

Theorem 3.
Assume $E \in \mathit{dom}(CT)$*,* $\Delta = \mathit{env\text{-}for\text{-}body}(E)$*, and* $\Delta' = \mathit{transl\text{-}env\text{-}for\text{-}body}(E)$*. If* $\Delta; \Gamma \vdash e : T$*, then* $\Delta'; \llbracket \Gamma \rrbracket_\Delta \vdash \llbracket e \rrbracket_\Delta : \llbracket T \rrbracket_\Delta$

Proof. The proof is by induction on the derivation of $\Delta; \Gamma \vdash e : T$, with case analysis on the last rule used: TY-VAR is trivial; TY-SUB follows from Theorem 1(a); TY-NEW from Theorem 2; TY-FLD from the translation of class definitions; TY-METH from Theorem 1(a) and the translations of method signatures and definitions; TY-UCAST from Theorems 1(a) and 2; TY-DCAST from Theorems 1(a) and (b), and 2; and TY-SCAST from Theorems 1(a) and 2.

Lemma 16.
Assume $E \in \mathit{dom}(CT)$*,* $\Delta = \mathit{env\text{-}for\text{-}body}(E)$*, and* $\Delta' = \mathit{transl\text{-}env\text{-}for\text{-}body}(E)$*. If* $\Delta \vdash ms$ *ok, then* $\Delta' \vdash \llbracket ms \rrbracket_\Delta$ *ok. If* $\Delta \vdash md$ *ok, then* $\Delta' \vdash \llbracket md \rrbracket_\Delta$ *ok.*

Proof. Trivial based on Theorems 2 and 3.

Theorem 4.
If `class` C`<`$\overline{X}$`>`... *ok in* FGJ+APR*, then* $[\![$`class` C`<`$\overline{X}$`>`...$]\!]$ *ok in* FGJ+I.
If `interface` I`<`$\overline{X}$`>`... *ok in* FGJ+APR*, then* $[\![$`interface` I`<`$\overline{X}$`>`...$]\!]$ *ok in* FGJ+I.

Proof. A class or an interface is *ok*, both in FGJ+APR and in FGJ+I, if all of their ancestors, constraints, fields, and methods are *ok* in the environments generated from the type parameters and constraints of the class/interface. The above theorems and lemmas show that translation of each of these sub-parts, including translation of environments, preserves well-formedness. The theorem follows.

Theorem 5. *Assume* $\emptyset;\emptyset \vdash e : T$*,* $CT' = [\![CT]\!]$ *and* $e' = [\![e]\!]_\emptyset$*. If* $\langle CT, e\rangle$ *is a valid program in* FGJ+APR*, then* CT' *ok and* $\emptyset;\emptyset \vdash e' : [\![T]\!]_\emptyset$*. That is,* $\langle CT', e'\rangle$ *is a valid program in* FGJ+I.

Proof. Follows from Theorems 3 and 4.

6 Related work

Associated types described here can be seen as a type-safe variation of virtual types. Several other related formalisms and language features have been reported. Closest to ours is *nested inheritance* [19], a Java extension, that can be translated to standard Java with techniques similar to those described in this paper. Nested inheritance associates nested types with classes, rather than with individual objects as the original virtual type systems [8,9] do. Compared to our work, nested inheritance does not consider type parameters or binding member types to existing types; nested types must be bound to newly defined classes.

Virtual types are often viewed as an alternative for parameterized types. E.g., virtual types, as described in [8,9], do not include a mechanism for type parameterization (beyond that of virtual types); Thorup and Torgersen show that type parameterization is important even in the presence of virtual types [18]. Our formalism analogously combines type parameterization and associated types, and argues for the importance of constraint propagation in this combination.

Original virtual types require run-time type checks for full type safety. They associate nested types to objects, not classes. By introducing suitable restrictions (see, e.g. [9,20]), several systems manage to add partial or total static type safety to virtual types, while preserving this property. These restrictions are similar to the requirement we impose that associated types are not redefined in subclasses of the class in which they are defined. Family polymorphism [21] allows groups of nested types to be inherited, but imposes restrictions based on object identity: the member types of two objects can only be used as the same type if the two objects are provably the same; this limitation was also pointed out in [19]. This restricts the interoperability of associated types of two distinct parameters of a generic function. A recent formalization and improvement of family polymorphism, νObj, allows nested types to be aliases for existing types in addition to newly defined types. Furthermore, two nested types can be constrained to be the same [22]. The identity-based type restrictions of family polymorphism still remain, although mitigated by the presence of sameness constraints between types. νObj is presented as a foundational calculus for examining properties and behavior of nested types.

Structural virtual types allow virtual types to be used for some of the tasks that parameterized types are typically used for [18]. For example, two subclasses of the same class, with the same nested type definitions, are viewed as the same type. Also, a subtyping relation among parameterized types, such that the constraints of a parameterized class enter into the subtype relationship, is automatically defined. A polymorphic class is itself a type; adding more restrictions to its parameters produces a subtype of the original polymorphic type; instances of that polymorphic class are also subtypes of the uninstantiated class.

The work on *nested types* (distinct from nested inheritance) explores allowing constructions like ML signatures and structures, as well as objects, in one unified framework [23]. This work defines a formalization of records with type members and same-type constraints, but not in combination with parameterized types.

Support for associated types is also found in several languages which are not predominantly object-oriented. C++ supports associated types with member **typedef**s, or with type functions known as traits classes [24]. ML modules can contain both types and values (including functions), and thus provide a direct representation for associated types [25]. However, an ML module is an entity by itself, distinct from a type; thus, types cannot be directly associated with other types. Haskell's *functional dependencies* among type class parameters offer partial support for associated types [26]. Influenced by our results in [7], a more direct mechanism for associated types has been suggested [27]. This language extension allows type members within type classes. This mechanism, however, does not allow existing types to become members of type classes, and does not allow constraints requiring particular pairs of associated types to be the same; the authors of [27] are considering those extensions. The Haskell work does not consider the effects of an object-oriented type system, including subtype relationships, on associated types.

In contrast to systems related to associated types, work on constraint propagation appears infrequently in the literature. We are not aware of work formally defining constraint propagation, though the Cecil programming language includes it as a feature [28, § 4.2]. Also, Java's wildcard types allow a limited form of constraint propagation [29]. Systems which include full type inference for type constraints, such as type classes in Haskell [30], include the equivalent of constraint propagation, but also introduce restrictions, such as forbidding a function name to be used in more in one type class.

One unique characteristic of our work is the combination of associated types and constraint propagation. Associated types can be bound to existing types, not only to newly created classes. Furthermore, we define associated types and constraint propagation as extensions to mainstream object-oriented languages with constrained generics, and describe translation of the extensions to such a language. In particular, our work applies directly to the generics of C# and Java.

7 Conclusion

A high degree of parameterization on types, typical for libraries built with generic programming, stretches the practical limits of generics in languages such as Java or C#. Associated types, as described in this paper, can significantly improve the encapsulation of types required to implement a particular design. Furthermore, associated types and parameterized types are not mutually exclusive features; our work demonstrates that these features are useful together, and describes their interaction precisely. Associated types allow functional dependencies between types to be expressed well and encapsulated within interfaces, but do not directly encapsulate constraints on associated types or type parameters similarly. The full benefits of associated types depend on the other proposed extension: constraint propagation. These two extensions can be implemented separately, but together they allow a very concise expression of constraints for generic methods and classes, while still allowing separate type-checking.

The paper gives a rigorous description of both associated types and constraint propagation in a form that is directly applicable to mainstream OO languages supporting F-bounded polymorphism, such as C# and Java. We suggest a translation from the extensions to a language without the extensions, but obviously a direct implementation is feasible. We have implemented an experimental type checker for FGJ+APR, and a translation to C# with generics; work is currently under way to implement the proposed extensions in the Mono C# compiler [31]. The proposed language features provide a significant improvement in the level of support for generic programming in these languages.

8 Acknowledgments

This work was supported by NSF grant EIA-0131354 and a grant from the Lilly Endowment. The second author was supported by a Department of Energy High Performance Computer Science Fellowship. We are grateful to Jeremy Siek and Amr Sabry for their helpful comments on this work.

References

1. Stepanov, A., Lee, M.: The Standard Template Library. Technical Report HPL-94-34(R.1), Hewlett-Packard Laboratories (1994) `http://www.hpl.hp.com/techreports`.
2. Stepanov, A.: The Standard Template Library — how do you build an algorithm that is both generic and efficient? Byte Magazine **20** (1995)
3. An, P., Jula, A., Rus, S., Saunders, S., Smith, T., Tanase, G., Thomas, N., Amato, N., Rauchwerger, L.: STAPL: An adaptive, generic parallel C++ library. In: Languages and Compilers for Parallel Computing. Volume 2624 of Lecture Notes in Computer Science. Springer (2001) 193–208
4. Siek, J., Lee, L.Q., Lumsdaine, A.: The Boost Graph Library: User Guide and Reference Manual. Addison-Wesley (2002)

5. Siek, J., Lumsdaine, A.: A modern framework for portable high performance numerical linear algebra. In: Modern Software Tools for Scientific Computing. Birkhäuser (1999)
6. Pitt, W.R., Williams, M.A., Steven, M., Sweeney, B., Bleasby, A.J., Moss, D.S.: The Bioinformatics Template Library–generic components for biocomputing. Bioinformatics **17** (2001) 729–737
7. Garcia, R., Järvi, J., Lumsdaine, A., Siek, J., Willcock, J.: A comparative study of language support for generic programming. In: Proceedings of the 18th ACM SIGPLAN conference on Object-oriented programing, systems, languages, and applications, ACM Press (2003) 115–134
8. Madsen, O.L., Moller-Pedersen, B.: Virtual classes: a powerful mechanism in object-oriented programming. In: OOPSLA, ACM Press (1989) 397–406
9. Thorup, K.K.: Genericity in Java with virtual types. In: ECOOP. Volume 1241 of Lecture Notes in Computer Science. (1997) 444–471
10. Canning, P., Cook, W., Hill, W., Olthoff, W., Mitchell, J.C.: F-bounded polymorphism for object-oriented programming. In: Proceedings of the fourth international conference on functional programming languages and computer architecture. (1989)
11. Igarashi, A., Pierce, B., Wadler, P.: Featherweight Java: A minimal core calculus for Java and GJ. In Meissner, L., ed.: ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages & Applications. Volume 34 of ACM SIGPLAN Notices., N. Y. (1999) 132–146
12. Kennedy, A., Syme, D.: Transposing F to C#: Expressivity of polymorphism in an object-oriented language. Concurrency and Computation: Practice and Experience **16** (2004)
13. Jazayeri, M., Loos, R., Musser, D., Stepanov, A.: Generic Programming. In: Report of the Dagstuhl Seminar on Generic Programming, Schloss Dagstuhl, Germany (1998)
14. Kapur, D., Musser, D.: Tecton: a framework for specifying and verifying generic system components. Technical Report RPI–92–20, Department of Computer Science, Rensselaer Polytechnic Institute, Troy, New York 12180 (1992)
15. Austern, M.H.: Generic Programming and the STL. Professional computing series. Addison-Wesley (1999)
16. Silicon Graphics, Inc.: SGI Implementation of the Standard Template Library. (2004) `http://www.sgi.com/tech/stl/`.
17. Bruce, K.B., Fiech, A., Petersen, L.: Subtyping is not a good "match" for object-oriented languages. In: ECOOP. Number 1241 in LNCS, Springer-Verlag (1997) 104–127
18. Thorup, K.K., Torgersen, M.: Unifying genericity — combining the benefits of virtual types and parameterized classes. In: ECOOP, Springer-Verlag (1999) 186–204
19. Nystrom, N., Chong, S., Myers, A.C.: Scalable extensibility via nested inheritance. In: OOPSLA, ACM Press (2004) 99–115
20. Torgersen, M.: Virtual types are statically safe. In: The Fifth International Workshop on Foundations of Object-Oriented Languages. (1998) `http://pauillac.inria.fr/~remy/fool/`.
21. Ernst, E.: Family polymorphism. In: ECOOP. Volume 2072 of Lecture Notes in Computer Science., Springer (2001) 303–326
22. Odersky, M., Cremet, V., Röckl, C., Zenger, M.: A nominal theory of objects with dependent types. In: ECOOP. Volume 2743 of LNCS., Springer-Verlag (2003) 201–224

23. Odersky, M., Zenger, C.: Nested types. In: Workshop on Foundations of Object-Oriented Languages (FOOL 8). (2001)
24. Myers, N.C.: Traits: a new and useful template technique. C++ Report (1995)
25. Milner, R., Tofte, M., Harper, R.: The Definition of Standard ML. MIT Press (1990)
26. Jones, M.P.: Type classes with functional dependencies. In: European Symposium on Programming. Number 1782 in LNCS, Springer-Verlag (2000) 230–244
27. Chakravarty, M., Keller, G., Jones, S.P., Marlow, S.: Associated types with class. In: POPL. (2005) submitted.
28. Chambers, C., the Cecil Group: The Cecil Language: Specification and Rationale, Version 3.1. University of Washington, Computer Science and Engineering. (2002) `www.cs.washington.edu/research/projects/cecil/`.
29. Torgersen, M., Hansen, C.P., Ernst, E., von der Ahé, P., Bracha, G., Gafter, N.: Adding wildcards to the Java programming language. In: ACM Symposium on Applied computing, ACM Press (2004) 1289–1296
30. Wadler, P., Blott, S.: How to make ad-hoc polymorphism less ad-hoc. In: ACM Symposium on Principles of Programming Languages, ACM (1989) 60–76
31. —: Mono .NET framework. `http://www.mono-project.com/` (2004)