Constrained Types for Object-Oriented Languages

Vijay Saraswat [*]

vsaraswa@us.ibm.com

Nathaniel Nystrom [*]

nystrom@us.ibm.com

Jens Palsberg [†]

palsberg@cs.ucla.edu

Christian Grothoff [‡]

christian@grothoff.org

Abstract

X10 is a modern object-oriented language designed for productivity and performance in concurrent and distributed systems. In this setting, dependent types offer significant opportunities for detecting design errors statically, documenting design decisions, eliminating costly runtime checks (e.g., for array bounds, null values), and improving the quality of generated code.

We present the design and implementation of *constrained types*, a natural, simple, clean, and expressive extension to object-oriented programming: A type `C(:c)` names a class or interface `C` and a *constraint* `c` on the immutable state of `C` and in-scope final variables. Constraints may also be associated with class definitions (representing class invariants) and with method and constructor definitions (representing preconditions). Dynamic casting is permitted. The system is parametric on the underlying constraint system: the compiler supports a simple equality-based constraint system but, in addition, supports extension with new constraint systems using compiler plugins.

1. Introduction

X10 is a modern statically typed object-oriented language designed for high productivity in the high performance computing (HPC) domain [47]. Built essentially on the im-perative sequential Java™ core, X10 introduces constructs for distribution and fine-grained concurrency (asynchrony, atomicity, ordering).

X10, like most object-oriented languages is designed around the notion of objects as instances of *classes*. However, X10 places equal emphasis on *arrays*, a central data-structure in high performance computing. In particular, X10 supports dense, distributed multi-dimensional arrays of value and reference types, built over index sets known as *regions*, and mappings from index sets to places, known as *distributions*. X10 supports a rich algebra of operations over regions, distributions and arrays.

A central design goal of X10 is to rule out large classes of error by design. For instance, the possibility of indexing a 2-d array with 3-d points should simply be ruled out at compile-time. This means that one must permit the programmer to express types such as `region(2)`, the type of all two-dimensional regions; `int[5]`, the type of all arrays of `int` of length 5; `int[region(2)]`, the type of all `int` arrays over two-dimensional regions; and `Object!`, the type of all `Object` located on the current node. For concurrent computations, one needs the ability to statically check that a method is being invoked by an activity that is registered with a given clock (i.e., dynamic barrier) [47].

In this paper we describe X10's support for *constrained types*. Constrained types are a form of *dependent type* [27, 54, 36, 6, 7, 3, 13]—types parametrized by values—defined on top of predicates over the *immutable* state of objects. Such types statically capture many common invariants that naturally arise in code. For instance, typically the shape of an array (the number of dimensions (the rank) and the size of each dimension) is determined at run time, but is fixed once the array is constructed. Thus, the shape of an array is part of its immutable state.

X10 provides a framework for specifying and checking constrained types that achieves certain desirable properties:

- **Ease of use.** The syntax of constrained types is a simple and natural extension of Java's types. Constrained types can interoperate smoothly with Java libraries.

---

[*] IBM T. J. Watson Research Center, P.O. Box 704, Yorktown Heights NY 10598 USA

[†] UCLA Computer Science Department, Boelter Hall, Los Angeles CA 90095 USA

[‡] Department of Computer Science, University of Denver, 2360 S. Gaylord Street, John Green Hall, Room 214, Denver CO, 80208 USA

```
1   class List(int(:self >= 0) n) {
2     Object head = null;
3     List(n-1) tail = null;
4
5     List(0)() { property(0); }
6     List(1)(Object head) { this(head, new List());}
7     List(tail.n+1)(Object head, List tail) {
8       property(tail.n+1);
9       this.head = head;
10      this.tail = tail;
11    }
12
13    List(n+arg.n) append(final List arg) {
14      return (n==0) ? arg : new List(head, tail.append(arg));
15    }
16
17    List(n) reverse() { return rev(new List()); }
18    List(n+acc.n) rev(final List acc) {
19      return (n==0) ? acc : tail.rev(new List(head, acc));
20    }
21
22    List(:self.n <= this.n) filter(Predicate f) {
23      if (n==0) return this;
24      List(:self.n <= this.n-1) l = tail.filter(f);
25      return (f.isTrue(head)) ? new List(head,l) : l;
26    }
27  }
```

Figure 1. This program implements a mutable list of Objects. The size of a list does not change through its lifetime, even though at different points in time its head and tail might point to different structures.

- **Flexibility.** The framework permits the development of concrete, specific type systems tailored to the application area at hand. X10's compiler permits extension with different constraint systems via compiler plugins, enabling a kind of pluggable type system [10]. The framework is parametric in the kinds of expressions used in the type system, permitting the installed constraint system to interpret the constraints.

- **Modularity.** The rules for type-checking are specified once in a way that is independent of the particular vocabulary of operations used in the dependent type system. The type system supports separate compilation.

- **Static checking.** The framework permits mostly static type-checking. The user is able to escape the confines of static type-checking using dynamic casts, as is common for Java-like languages.

1.1 Constrained types

We permit the definition of a class C to specify a list of typed parameters or *properties*, $T_1 \, x_1, \dots, T_k \, x_k$, similar in syntactic structure to a method formal parameter list. Each property in this list is treated as a `public final` instance field. We also permit the specification of a *class invariant*, a *where clause* [14] in the class definition. A class invariant is a boolean expression on the properties of the class. The compiler ensures that all instances of the class created at run time satisfy the invariant. Syntactically, the class invariant is separated from the property list with a ":". For instance, we may specify a class `List` with an `int length` property as follows:

```
class List(int length: length >= 0) {...}
```

Given such a definition for a class C, types can be constructed by *constraining* the properties of C. In principle, *any* boolean expression over the properties specifies a type: the type of all instances of the class satisfying the boolean expression. Thus, `List(:length == 3)` is a permissible type, as are `List(:length <= 42)` and even `List(:length * f() >= g())` where `f` and `g` are functions on the immutable state of the `List` object and the variables in scope where the type appears. In practice, the constraint expression is restricted by the particular constraint system in use.

In general, a *constrained type* is of the form $C(:e)$, the name of a class or interface[1] C, called the *base class*, followed by a *condition* e, a boolean expression on the properties of the base class and the `final` variables in scope at the type. Such a type represents a refinement of C: the set of all instances of C whose immutable state satisfies the condition e.

For brevity, we write C as a type as well; it corresponds to the (vacuously) constrained type $C(:\text{true})$. We also permit the syntax $C(e_1, \dots, e_k)$ for the type $C(x_1==e_1, \dots, x_k==e_k)$, assuming that the property list for C specifies the k properties $x_1, \dots, x_k$, and each term e_i is of the correct type.

Constrained types may occur wherever normal types occur. In particular, they may be used to specify the types of properties, (possibly mutable) local variables or fields, arguments to methods, return types of methods; they may also be used in casts, etc.

Using the definitions above, `List(n)`, shown in Figure 1, is the type of all lists of length `n`. Intuitively, this definition states that a `List` has an `int` property `n`, which must be non-negative. In a constraint, the name `self` refers to the type being constrained (as opposed to `this`, which refers to an instance of the enclosing class). The class has two fields that hold the head and tail of the list. The properties of the class are set through the invocation of `property(...)` (analogously to `super(...)`) in the constructors.

Our basic approach to introducing constrained types into X10 is to follow the spirit of generic types, but to use values instead of types.

Constructors have "return types" that can specify an invariant satisfied by the object being constructed. The compiler verifies that the constructor return type and the class invariant are implied by the `property` statement and any `super` calls in the constructor body. The `List` class has three constructors: the first constructor returns an empty list; the second returns a singleton list of length `1`; the third returns a

---

[1] In X10, primitive types such as `int` and `double` are object types; thus, for example, `int(:self==0)` is a legal constrained type.

list of length `m+1`, where `m` is the length of the second argument.

In the third constructor (lines 7–11), as well as the `append` (line 13) and `rev` (line 18) methods, the return type depends on properties of the formal parameters. If an argument appears in a return type then the parameter must be declared `final`, ensuring the argument points to the same object throughout the evaluation of the method or constructor body. A parameter may also depend on another parameter in the argument list.

The use of constraints makes existential types very natural. Consider the return type of `filter` (line 22): it specifies that the list returned is of some unknown length. The only thing known about it is that its size is bounded by `n`. Thus, constrained types naturally subsume existential dependent types. Indeed, every base type `C` is an "existential" constrained type since it does not specify any constraint on its properties. Thus, code written with constrained types can interact seamlessly with legacy library code—using just base types wherever appropriate.

The return type of `filter` also illustrates the difference between `self` and `this`. Here, `self` refers to the `List` being returned by the method; `this` refers to the method's receiver.

1.2 Constraint system plugins

The X10 compiler allows programmers to extend the semantics of the language with compiler plugins. Plugins may be used to support different constraint systems to be used in constrained types. Constraint systems provide code for checking consistency and entailment.

The condition of a constrained type is parsed and type-checked as a normal boolean expression over properties and the `final` variables in scope at the type. Installed constraint systems translate the expression into an internal form, rejecting expressions that cannot be represented. A given condition may be a conjunction of constraints from multiple constraint systems. A Nelson–Oppen procedure [30] is used to check consistency of the constraints.

The X10 compiler implements a simple equality-based constraint system. Constraint solver plugins have been implemented for inequality constraints, for Presburger constraints using the CVC3 theorem prover [9], and for set-based constraints also using CVC3. These constraint systems are described in Section 3; the implementation is discussed in Section 4.

1.3 Claims

The paper presents constrained types in the X10 programming language. We claim that the design is natural, easy to use, and useful. Many example programs have been written using constrained types and are available at `x10.sf.net`.

As in staged languages [31, 51], the design distinguishes between compile-time and run-time evaluation. Constrained types are checked (mostly) at compile-time. The compiler uses a constraint solver to perform universal reasoning (e.g., "for all possible values of method parameters") for dependent type-checking. There is no run-time constraint-solving. However, run-time casts and `instanceof` checks involving dependent types are permitted; these tests involve arithmetic, not algebra—the values of all parameters are known.

The design supports separate compilation: a class needs to be recompiled only when it is modified or when the method and field signatures or invariants of classes on which it depends are modified.

We claim that the design is flexible. The language design is parametric on the constraint system being used. The compiler supports integration of different constraint solvers into the language. Dependent clauses are also form the basis of a general user-definable annotation framework we have implemented separately [34].

We claim the design is clean and modular. We present a simple core language CFJ, extending FJ [24] with constrained types on top of an arbitrary constraint system. We present rules for type-checking CFJ programs that are parametric in the constraint system and establish subject reduction and progress theorems.

Rest of this paper. Section 2 describes the syntax and semantics of constrained types. Section 3 works through a number of examples using a variety of constraint systems. The compiler implementation, including support for constraint system plugins, is described Section 4. A formal semantics for a core language with constrained types is presented in Section 5, and a soundness proof is presented in the appendix. Section 6 reviews related work. The paper concludes in Section 7 with a discussion of future work.

2. Constrained types

This section describes constrained types in X10.

2.1 Properties

A property is a `public final` instance field of the class that cannot be overridden by subclassing. Like any other field, a property is typed, and its type need not necessarily be primitive. Thus, properties capture the immutable public state of an object, initialized when the object is created, that can be classified by constrained types. Syntactically, properties are specified in a parameter list right after the name of the class in a class definition. The class body may contain specifications of other fields; these fields are considered mutable.

Properties may be of arbitrary type. For instance, the class `region` has an `int` property called `rank`. In turn, the class `dist` has a `region` property, called `region`, and also an `int` property `rank`. The invariant for `dist` ensures that `rank == region.rank`. Similarly, an array has properties `dist`, `region`, and `rank` and appropriate constraints ensuring that the statically available information about them is consis-

tent.[2] In this way, rich constraints on the immutable portion of the object reference graph, rooted at the current object and utilizing objects at user-defined types, may be specified.

2.2 Constraints

A constrained type is of the form `C(:e)`, consisting of a *base class* `C` and a *condition* `e`, a boolean expression on the properties of the base class and the `final` variables in scope at the type. Constraints specify (possibly) partial information about the variables of interest. The type `C(:e)` represents the set of all instances of `C` whose immutable state satisfies the condition `e`.

Constraints may use the special variable `self` to stand for the object whose type is being defined. Thus, `int(:self >= 0)` is the set of natural numbers, and `point(:x *x + y*y <= 1.0)` represents the interior of a circle (for a class `point` with two `float` properties `x` and `y`). The type `C(:self != null)` represents all instances of C. When there is no ambiguity, a property reference `self.x` may be abbreviated to `x`. The type `int(:self==v)` represents a "singleton" type, an `int` is of this type only if it has the same value as `v`.

To be clear, `self` is not the same as `this`. In the `List` example of Figure 1, the `filter` method (line 22) returns a list with type `List(:self.n <= this.n)`; the term `self.n` is the length of the returned `List`; the term `this.n` is the length of the receiver of the call to `filter`.

Constraints are specified in terms of an underlying constraint system [48]—a pre-defined logical vocabulary of functions and predicates with algorithms for consistency and entailment. The X10 compiler permits different constraint systems to be installed using compiler plugins [10]. Constraint system plugins define a language of constraints by symbolically interpreting the boolean expression specifying a type's condition; plugins may report an error if the condition cannot be interpreted.

In principle, types may be constrained by any boolean expression over the properties. For practical reasons, restrictions need to be imposed to ensure constraint checking is decidable.

The condition of a constrained type must be a pure function only of the properties of the base class. Because properties are `final` instance fields of the object, this requirement ensures that whether or not an object belongs to a constrained type does not depend on the *mutable* state of the object. That is, the status of the predicate "this object belongs to this type" does not change over the lifetime of the object. Second, by insisting that each property be a *field* of the object, the question of whether an object is of a given type can be determined merely by examining the state of the object and evaluating a boolean expression. Of course,

an implementation is free to not *explicitly* allocate memory in the object for such fields. For instance, it may use some scheme of tagged pointers to implicitly encode the values of these fields.

Further, by requiring that the programmer distinguish certain `final` fields of a class as properties, we ensure that the programmer consciously controls *which* `final` fields should be available for constructing constrained types. A field that is "accidentally" `final` may not be used in the construction of a constrained type. It must be declared as a property.

2.3 Subtyping

Constrained types come equipped with a subtype relation that combines the nominal subtyping relation of classes and interfaces with the logical entailment relation of the constraint system. Namely, a constraint `C(:c)` is a subtype of `D(:d)` if C is a subtype of D and every value in C that satisfies `c` also satisfies `d`.

This definition implies that `C(:e1)` is a subtype of `C(:e2)` if `e1` implies `e2`. In particular, for all conditions `e`, `C(:e)` is a subtype of C. `C(:e)` is empty exactly when `e` conjoined with C's class invariant is inconsistent.

Two constrained types `C1(:e1)` and `C2(:e2)` are considered equivalent if `C1` and `C2` are the same base type and `e1` and `e2` are equivalent when considered as logical expressions. Thus, `C(:x*x==4)` and `C(:x==2 || x==-2)` are equivalent types.

2.4 Final variables

The use of `final` local variables, formal parameters, and fields in constrained types has proven to be particularly valuable in practice. The same variable that is being used in computation can also be used to specify types. There is no need to introduce separate, universally and existentially quantified "index" variables. During type-checking, `final` variables are turned into symbolic variables—some fixed but unknown value—of the same type. Computation is performed in a constraint-based fashion on such variables.

2.5 Method and constructor preconditions

Methods and constructors may specify preconditions on their parameters as where clauses. For an invocation of a method (or constructor) to be type-correct, the associated where clause must be statically known to be satisfied. Note that the where clause may contain constraints on the properties of `this`. Thus the where clause may be used to specify that a method is *conditionally* available on some objects of the class and not others.

The return type of a method may also contain expressions involving the arguments to the method. Any argument used in this way must be declared `final`, ensuring it is not mutated by the method body. For instance, the following is a valid method declaration:

---

[2] All constraint languages used in constrained types permit object references, field selection and equality. Such constraint systems have been studied extensively under the name of "feature structures" [2].

```
List(arg.length-1)
  tail(final List arg: arg.length > 0) {
    ...
}
```

It says that `tail` must be passed a non-empty list, and it returns a list whose length is one less than its argument.

2.6 Method overloading and overriding

The definitions of method overloading, overriding, hiding, shadowing and obscuring in X10 are the same as in Java [21], modulo the following considerations motivated by dependent types.

Our current implementation erases dependent type information when compiling to Java. Therefore it must be the case that a class does not have two different method definitions that conflict with each other when the constrained clauses in their types are erased.

A class C inherits from its direct superclass and superinterfaces all their methods that are visible according to the access modifiers and that are not hidden or overridden. A method `m1` in a class C overrides a method `m2` in a superclass D if `m1` and `m2` have signatures with equivalent (unerased) formal parameter types.

Dynamic method lookup does not take dependent type information into account, only the class hierarchy. This design decision ensures that serious errors such as method invocation errors are captured at compile-time. Such errors can arise because multiple incomparable methods with the same name and acceptable argument lists might be available at the dynamic dependent type of the subject.

2.7 Constructors for dependent classes

Constructors must ensure that the class invariants of the given class and its superclasses and superinterfaces hold. For instance, the nullary constructor for `List` ensures that the property `length` has the value `0`:

```
public List(0)() { property(0); }
```

The `property` statement is used to set all the properties of the new object simultaneously. Capturing this assignment in a single statement simplifies checking that the constructor postcondition and class invariant are established. If a class has properties, every path through the constructor must contain exactly one `property` statement.

Java-like languages permit constructors to throw exceptions. This is necessary to deal with the situation in which the arguments to a constructor for a class C are such that no object can be constructed that satisfies the invariants for C. Dependent types make it possible to perform some of these checks at compile-time. The class invariant of a class explicitly captures conditions on the properties of the class that must be satisfied by any instance of the class. Constructor preconditions capture conditions on the constructor arguments. The compiler's static check for non-emptiness of

the type of any variable captures these invariant violations at compile-time.

2.8 Extending dependent classes

A class may extend a constrained class, e.g., `class C( ...) extends D(:d)`. This documents the programmer's intention that every call to `super` in a constructor for C must ensure that the invariant `d` is established on the state of the class D. The expressions in the actual parameter list for the super class may involve only the properties of the class being defined.

2.9 Dependent interfaces

Java does not allow interfaces to specify instance fields. Rather all fields in an interface are final static fields (constants). However, since properties play a central role in the specification of refinements of a type, it makes sense to permit interfaces to specify properties. Similarly, an interface definition may specify an invariant on its properties. Methods in the body of an interface may have where clauses as well.

All classes implementing an interface must have a property with the same name and type (either declared in the class or inherited from the superclass) for each property in the interface. If a class implements multiple interfaces and more than one of them specify a property with the same name, then they must all agree on the type of the property. The class must have a single property with the given name and type.

The general form of a class declaration is now:

```
class C(T₁ x₁, ..., Tₖ xₖ)
    extends B(:c)
    implements I₁(:c₁), ..., Iₙ(:cₙ) {...}
```

For such a declaration to type-check, it must be that the class invariant of C implies $inv(I_i)$ & c_i, where $inv(I_i)$ is the invariant associated with interface I_i. Again, a constrained class or interface I is taken as shorthand for `I(:true)`. Further, every method specified in the interface must have a corresponding method in the class with the same signature whose precondition, if any, is implied by the precondition of the method in the interface.

2.10 Separation between compile-time and run-time computation

Our design distinguishes between compile-time execution (performed during type-checking) and run-time execution. At compile-time, the compiler processes the abstract syntax tree of the program generating queries to the constraint solver. The only computation engine running is the constraint solver, which operates on its own vocabulary of predicates and functions. Program variables (such as local variables) that occur in types are dealt with symbolically. They are replaced with logical variables—some fixed, but unknown value—of the same type. The constraint solver must

know how to process pieces of partial information about these logical variables in order to determine whether some constraint is entailed. At run time, the same program variable will have a concrete value and will perform "arithmetic" (calculations) where the compiler performed "algebra" (symbolic analysis).

Constrained types may occur in a class cast `(T) e`. Code is generated to check at run time that the expression `e` satisfies any constraints in `T`.

2.11 Equality-based constraints

The X10 compiler includes a simple equality-based constraint system. All constraint systems installed using plug-ins must support at least the core equality-based constraints. Constraints are conjunctions of equalities between constraint terms: properties, `final` variables, compile-time constants, and `self`:

$$
\begin{array}{llll}
\text{(C Term)} & \texttt{t} & ::= & \texttt{x} \mid \texttt{this} \mid \texttt{self} \mid \texttt{t.f} \mid n \\
\text{(Constraint)} & \texttt{c,d} & ::= & \texttt{true} \mid \texttt{t == t} \mid \texttt{c \& c} \\
& & \mid & \texttt{T x; c}
\end{array}
$$

We use the syntax `T x; c` for the constraint obtained by existentially quantifying the variable `x` of type `T` in `c`.

2.12 Existential quantification

Constrained types subsume existential types. For example, the length of the list returned by `filter` in Figure 1 is existentially quantified. Existential quantification may also be introduced explicitly: the following function computes the greatest common divisor of two integers:[3]

```
int(:int x; int y; a==x*self & b==y*self)
  gcd(final int a, final int b)
{
    if (b == 0) return a;
    else return gcd(b, a % b);
}
```

Operations on values of constrained type propagate constraints to the operation result by introducing existentially quantified variables. Consider the following assignment:

```
int(:self >= 0) product(int(:self >= 0) a,
                        int(:self >= 0) b) {
    return a*b;
}
```

We would like this function to type-check. During type-checking, the type of `a*b` is computed from the types of `a` and `b` to be the type:

```
int(:int x; int y; self==x*y & x>=0 & y>=0)
```

That is, there exist non-negative `int`s `x` and `y` whose product is `self`. The constraint on this type is strong enough to

---

[3] Checking this program requires a constraint system capable of reasoning about integer multiplication and division. We have not yet implemented such a system.

establish the constraint on the return type. If the computed constraint cannot be represented by any installed constraint system, the type of `a*b` is promoted to the unconstrained supertype `int`.

2.13 Query evaluation

Because object-oriented languages permit arbitrary mutual recursion between classes: classes `A` and `B` may have fields of type `B` and `A` respectively—the type/property graph may have cycles. The nodes in this graph are base types (class and interface names). There is an edge from node `A` to node `B` if `A` has a property whose base type is `B`.

Let us define the *real clause* of a constrained type `C(:c)` to be the set of constraints that must be satisfied by any instance of `C(:c)`. This includes not only the condition `c` but also constraints that hold for all instances of `C`, as determined by `C`'s class invariant. Let $rc(\texttt{C(:c)})$ denote the *real clause* of `C(:c)`. For simplicity, we consider only top-level classes; thus, the only free variable in $rc(\texttt{C(:c)})$ is `self`. We draw out `self` as a formal parameter and write $rc(\texttt{C(:c)},\texttt{X})$ for $rc(\texttt{C(:c[X/self]}))$.

Consider a general class definition:

```
class C(C_k(:c_1) x_1, ..., C_k(:c_k) x_k: c)
  extends D(:d) { ... }
```

From this, we get:

$$
rc(\texttt{C},\texttt{X}) \iff \begin{array}{l} (\texttt{c} \wedge \texttt{d})[\texttt{X/this}] \wedge rc(\texttt{D},\texttt{X}) \wedge \\ rc(\texttt{C}_1\texttt{(:c}_1\texttt{)},\texttt{X.x}_1) \wedge \cdots \wedge rc(\texttt{C}_k\texttt{(:c}_k\texttt{)},\texttt{X.x}_k) \end{array}
$$

That is, given a program P with classes $\texttt{C}_1,\ldots,\texttt{C}_k$, the set of real clauses for $\texttt{C}_1,\ldots,\texttt{C}_k$ are defined in a mutually recursive fashion through the Clark completion of a Horn clause theory (over an underlying constraint system).

The central algorithmic question now becomes whether given a constrained clause `d`, does $rc(\texttt{C(:c)},\texttt{X})$ entail `d`? From the above formulation the question is clearly semi-decidable. It is not clear however whether it is decidable. This is a direction for further work.

The X10 compiler is conservative and rejects programs with cyclic dependency graphs: programs where the real clause of the type of a property `p` itself constrains `p`. In practice, many data structures have non-cyclic dependency graphs. For such programs the real clause can be computed quickly and only a bounded number of questions to the constraint solver are generated during type-checking.

2.14 Parametric consistency

Consider the set of final variables that are referenced in a type `T = C(:c)`. These are the *parameters* of the type. A type is said to be *parametrically consistent* if its where clause `c` is solvable for each possible assignment of values to parameters. A parametrically consistent type has the property that its extension will never be empty. Types are required to be parametrically consistent.

Consider a variation of List from Figure 1:

```
class List(int(:self >= 0) n) {
  Object head;
  List(:self.n==this.n-1 & self!=null) tail;
  ...
}
```

The type of the field `tail` is not parametrically consistent. There exists a value for its parameter `n`, namely `0`, for which the real clause `self != null & self.n == this.n-1 & self.n >= 0` is not satisfiable.

The compiler will throw a type error when it encounters the initializer for this field in a constructor since it will not be able to prove that the initial value is of the given type.

3. Examples

The following section presents example uses of constrained types using several different constraint systems.

3.1 Equality constraints

The X10 compiler includes a simple equality-based constraint system, described in Section 2. Equalities constraints are used throughout X10 programs. For example, to ensure n-dimensional arrays are indexed only be n-dimensional index points, the array access operation requires that the array's `rank` property be equal to the index's `rank`.

3.2 Presburger constraints

Presburger constraints are linear integer inequalities. Presburger constraints are particularly useful in a high-performance computing setting where array operations are pervasive. Xi and Pfenning proposed using dependent types for eliminating array bounds checks [53]. A Presburger constraint system can be used to keep track of array dimensions and array indices to ensure bounds violations do not occur.

A Presburger constraint solver plugin was implemented using CVC3 [8, 9].

3.3 Set constraints: region-based arrays

Rather than using Presburger constraints, X10 takes another approach: following ZPL [11], arrays in X10 are defined over *regions*, sets of n-dimensional *index points* [22]. For instance, the region `[0:200,1:100]` specifies a collection of two-dimensional points `(i,j)` with `i` ranging from `0` to `200` and `j` ranging from `1` to `100`.

Regions and points were modeled in CVC3 [9] to create a constraint solver than ensures array bounds violations do not occur: an array access type-checks if the index point can be statically determined to be in the region over which the array is defined.

Region constraints are subset constraints written as calls to the `contains` method of the `region` class. The constraint solver does not actually evaluate the calls to the `contains` method, rather it interprets these calls symbolically as subset constraints at compile time.

```
1  const point(:rank==2) NORTH = point.factory.point(1,0);
2  const point(:rank==2) WEST  = point.factory.point(0,1);
3
4  void sor(double omega, final double[:rank==2] G, int iter)
5  {
6    region(:self==G.region & rank==2) outer = G.region;
7    region(:G.region.contains(self) & rank==G.region.rank)
8        inner = outer & (outer-NORTH) & (outer+NORTH)
9                     & (outer-WEST)  & (outer+WEST);
10
11   region d0 = inner.rank(0); // { i | (i,j) in inner }
12   region d1 = inner.rank(1); // { j | (i,j) in inner }
13
14   if (d1.size() == 0) return;
15
16   final int d1min = d1.low();
17   final int d1max = d1.high();
18
19   for (int off = 1; off <= iter*2; off++)
20     finish foreach (point[i]: d0)
21        if (i % 2 == off % 2)
22          for (point ij: inner & [i:i,d1min:d1max])
23            G[ij] = omega / 4.
24                  * (G[ij-NORTH] + G[ij+NORTH]
25                  + G[ij-WEST]   + G[ij+WEST])
26                  * (1. - omega) * G[ij];
27 }
```

Figure 2. Successive over-relaxation with regions

Constraints have the following syntax:

(Constraint)	c	::=	r.contains(r) $\mid$ ...
(Region)	r	::=	t $\mid$ [b_1:d_1,...,b_k:d_k]
		$\mid$	r $\mid$ r $\mid$ r & r $\mid$ r - r
		$\mid$	r + p $\mid$ r - p
(Point)	p	::=	t $\mid$ [b_1,...,b_k]
(Integer)	b,d	::=	t $\mid$ n

where `t` are constraint terms (properties and final variables) and `n` are integer literals.

Regions used in constraints are either constraint terms `t`, region constants, unions (`|`), intersections (`&`), or differences (`-`), or regions where each point is offset by another point `p` using `+` or `-`.

For example, the code in Figure 2 performs a successive over-relaxation [44] of a matrix `G` with rank 2. The function declares a region variable `outer` as an alias for `G`'s region and a region variable `inner` to be the subset of `outer` that excludes the boundary points, formed by intersecting the `outer` region with itself shifted up, down, left, and right by one). The function then declares two more regions `d0` and `d1`, where d_i is set of points x_i where (x_0, x_1) is in `inner`. The function iterates multiple times over points `i` in `d0`. The syntax `finish foreach` (line 20) tells the compiler to execute each loop iteration in parallel and to wait for all concurrent activities to terminate. The inner loop (line 22) iterates over a subregion of `inner`. The type-checker establishes that the `region` property of the point `ij` (line 22) is `inner & [i:i,d1min:d1max]`, and that this region is

a subset of `outer`, the region of the array `G` accessed within the loop body, ensuring that the access to the array is within the bounds of the array.

4. Implementation

The X10 compiler provides a framework for writing and checking constrained types. Constraints in the base X10 language are conjunctions of equalities over immutable side-effect-free expressions. Compiler plugins may be installed to support other constraint languages and solvers.

The X10 compiler is implemented as an extension of Java using the Polyglot compiler framework [32]. Expressions used in constrained types are type-checked as normal non-dependent X10 expressions; no constraint solving is performed on these expressions. During type-checking, constraints are generated and solved using the built-in constraint solver or using solvers provided by plugins. The system allows types to constrained by conjunctions of constraints in different constraint languages. If constraints cannot be solved, an error is reported.

4.1 Constraint checking

After type-checking a constraint as a boolean expression `e`, the abstract syntax tree for the boolean expression is transformed into a list of conjuncts, $e_1 \& \ldots \& e_k$. Each conjunct `ei` is given to the installed constraint system plugins, which symbolically evaluate the expression to create an internal representation of the conjunct. If no constraint system can handle the conjunct, an error is reported.

To interoperate, the constraint solvers must share a common vocabulary: constraint terms `t` range over the properties of the base type, the final variables in scope at the type (including `this`), the special variable `self` representing the a value of the type, and field selections `t.f`. All constraint systems are required to support the trivial constraint `true`, conjunction, existential quantification and equality on constraint terms.

In this form, the constraint is represented as a conjunction of constraints from different theories. Constraints are checked for satisfiability using a Nelson–Oppen procedure [30]. After constructing a constraint-system specific representation of a conjunct, each plugin computes the set of term equalities entailed by the conjunct. These equalities are propagated to the other conjuncts, which are again checked for satisfiability and any new equalities generated are propagated. If a conjunct is found to be unsatisfiable, an error is reported.

During type-checking, the type checker needs to determine if the type `C(:c)` is a subtype of `D(:d)`. This is true if the base type `C` is a subtype of `D` and if the constraint `c` entails `d`. To check entailment, each constraint solver is asked if a given conjunct of `d` is entailed by `c`. If any report false, the entailment does not hold and the subtyping check fails.

4.2 Translation

After constraint-checking, the X10 code is translated to Java in a straightforward manner. Each dependent class is translated into a single class of the same name without dependent types. The explicit properties of the dependent class are translated into `public final` (instance) fields of the target class. A `property` statement in a constructor is translated to a sequence of assignments to initialize the property fields.

For each property, a getter method is also generated in the target Java class. Properties declared in interfaces are translated into getter method signatures. Subclasses implementing these interfaces thus provide the required properties by implementing the generated interfaces.

Usually, constrained types are simply translated to non-constrained types by erasure; constraints are checked statically and need no run-time representation. However, dependent types may be used in casts and `instanceof` expressions. Because the constraint syntax in X10 is a subset of the X10 expression syntax, run-time tests of constrained types are translated to Java by evaluating the constraint with `self` bound to the expression being tested. For examples, casts are translated as:

```
⟦(C(:c)) e⟧ =
  new Object() {
    C cast(C self) {
      if (⟦c⟧) return self;
      throw new ClassCastException(); }
  }.cast((C) ⟦e⟧)
```

Wrapping the evaluation of `c` in an anonymous class ensures the expression `e` is evaluated only once.

To support separate compilation, abstract syntax trees for constraints are embedded into the generated Java code, and from there into the generated class file. The compiler reconstructs dependent types in referenced class files from their ASTs.

5. Formal semantics

In this section we formalize a small fragment of X10—an extension of Featherweight Java (FJ) [24] with constrained types—to illustrate the basic concepts behind constrained type-checking. A proof of soundness is given in the appendix.

The language is functional in that assignment is not admitted. However, it is not difficult to introduce the notion of mutable fields, and assignment to such fields. Since constrained types may only refer to immutable state, the validity of these types is not compromised by the introduction of state. Further, we do not formalize overloading of methods. Rather, as with FJ, we simply require that the input program be such that the class name `C` and method name `m` uniquely select the associated method on the class. We do model properties, constrained clauses, class invariants, where clauses in methods and constructors, and dependent type casts.

5.1 Constraint system

Constraints are assumed to be drawn from a fixed constraint system, $\mathcal{C}$, with inference relation $\vdash_{\mathcal{C}}$ [48]. All constraint systems are required to support the trivial constraint `true`, conjunction, existential quantification and equality on constraint terms. Constraint terms include `final` variables (including `this`), the special variable `self` (which may occur only in constraints `c` and not in expressions `e`), and field selections `t.f`.

The syntax for the language is specified in Figure 3. In the syntax, "," binds tighter than ";". We use the syntax `T x; c` for the constraint obtained by existentially quantifying the variable `x` of type `T` in `c`. `p` ranges over the collection of predicates supplied by the underlying constraint system, and `g` over the collection of functions.

A *class declaration* `class C(T̄ f̄ : c) extends D(: d) {M̄}` is declares a class `C` with the fields $\bar{f}$ (of type $\bar{T}$), a *declared class invariant* `c`, a *superclass invariant* `d` and a collection of methods $\bar{M}$. The constraints `c` and `d` are true for all instances of the class `C` (this is verified in the rule for type-checking constructors, T-NEW). In these constraints, `this` may be used to reference the current object; `self` does not have any meaning and must not be used.

A *method declaration* T_0 `m(T̄ x̄ : c){...}` specifies the type of the arguments and the result, as usual. The method arguments $\bar{x}$ may occur in the argument types $\bar{T}$ and the return type T_0. The constraint `c` specifies additional constraints on the arguments $\bar{x}$ and `this` that must hold for a method invocation to be legal. Note that `self` does not make sense in `c` (no type is being defined), and must not occur in `c`.

A type is taken to be of the form `C(:c)` where `C` is the name of a class or interface and `c` is a constraint; we say that `C` is the *base* of the type `C(:c)`. We use the following shorthand for types: For a type `T` equal to `C(:c)`, we will write `S x; T` for `C(:S x; c)`, and `d,T` for `C(:d,c)`.

We denote the application of the substitution $\theta = [\bar{t}/\bar{x}]$ to a constraint `c` by $c[\bar{t}/\bar{x}]$. Application of substitutions is extended to types by: $C(:c)\theta = C(:c\theta)$.

We summarize here properties of constraint systems described in [48] that are needed for the proofs: constraint systems may be thought of as presented via an intuitionistic Gentzen proof system supporting identity; affine and exchange on the left; existential quantification and conjunction on the left and right; and closure under substitution of terms. All constraint systems are required to satisfy: `new C(t̄).f`$_i$ = t_i provided that *fields*$(C) = \bar{T}\,\bar{f}$ (for some sequence of types $\bar{T}$).

5.2 Static semantics

Typing judgments, shown in Figure 4 are of the form $\Gamma \vdash T\,e$ where Γ is a multiset of type assertions `T x` and constraints `c`.[4] When Γ is empty, it is omitted.

(C Term)	t	::=	`x` | `self` | `t.f` | `new C(t̄)` | `g(t̄)`
(Constraint)	c,d	::=	`true` | `p(t̄)` | `t = t` | `c,c` | `T x; c`
(Class)	L	::=	`class C(T̄ f̄ : c) extends T {M̄}`
(Method)	M	::=	`T m(T̄ x̄ : c){return e;}`
(Expression)	e	::=	`x` | `e.f` | `e.m(ē)` | `new C(ē)` | `(T) e`
(Type)	S,T,U,Z	::=	`C(: d)`

Figure 3. CFJ Syntax

A type assertion `C(:c) x` constrains the variable `x` to contain references to only those objects `o` that are instances of (subclasses of) `C` and for which the constraint `c` is true provided that occurrences of `self` in `c` are replaced by `o`. Thus in the constraint `c` of a constrained type `C(:c)`, `self` may be used to reference the object whose type is being specified. Note that `self` is distinct from `this`—`this` is permitted to occur in the clause of a type `T` only if `T` occurs in an instance field declaration or instance method declaration of a class; as usual, `this` is considered bound to the instance of the class to which the field or method declaration applies.

The definition of *mtype*(C,m) (the signature of a method named `m` in class `C`), *mbody*(C,m), (the body associated with method `m` in type `C`) and *fields*(C) (the sequence of fields and their types inherited or defined at `C`) is essentially as specified in FJ [24] with the difference that the method of a signature is taken to be of the form $\bar{S}\,\bar{x}: c \to T$. The variables `x` are permitted to occur in the types $\bar{S}, T$, and are considered bound, and subject to alpha-renaming. The definitions of *mtype*, *mbody*, *fields* are extended to apply to constrained types by ignoring the constraint. For a substitution θ we define *mtype*(T,m,θ) as the signature obtained by applying θ to *mtype*(T,m), renaming bound variables as necessary. Similarly, for a substitution θ we define *fields*(T,θ) to be $\bar{S}\theta\,\bar{f}$, if the sequence of inherited and defined fields of the class underlying the type `T` is $\bar{S}\,\bar{f}$. We let *fields*(T,x) stand for *fields*$(T,[x/\texttt{self}])$.

We define $\sigma(\Gamma)$ to be the set of constraints obtained from Γ by replacing each type assertion `C(: d) x` in Γ with $d[x/\texttt{self}]$, *inv*(C,x) and retaining any constraint in Γ.

T-VAR extends the identity rule ($\Gamma, x : C \vdash x : C$) of FJ to take into account the constraint entailment relation.

T-CAST encapsulates the three inference rules of FJ: T-UCAST, T-DCAST and T-SCAST for upwards cast, downwards cast, and "stupid" cast respectively.

In T-FIELD, we postulate the existence of a receiver object `o` of the given static type (T_0). *fields*(T_0,o) is the set of typed fields for T_0 with all occurrences of `this` replaced by `o`. We record in the resulting constraint that `o.f`$_i$ = `self`.[5] This permits transfer of information that may have been recorded in T_0 about the field `f`$_i$.

---

[4] We use the non-standard notation `T x` rather than the more familiar `x : T` since `:` is used in the syntax of a type.

[5] A new name `o` is necessary to name this object since `e` cannot be used. Arbitrary term expressions `e` are not permitted in constraints; the functions used in `e` may not be known to the constraint system, and `e` may have side-effects.

$$\frac{\sigma(\Gamma, C(:c)\, x) \vdash_C d[x/\mathtt{self}]}{\Gamma, C(:c)\, x \vdash C(:d)\, x} \quad \text{(T-VAR)} \qquad \frac{\Gamma \vdash U\, e}{\Gamma \vdash T\, (T)e} \quad \text{(T-CAST)} \qquad \frac{\Gamma \vdash T_0\, e \quad \mathit{fields}(T_0, z_0) = \overline{U}\, \overline{f} \quad (z_0\ \text{fresh})}{\Gamma \vdash (T_0\, z_0; z_0.f_i = \mathtt{self}; U_i)\, e.f_i} \quad \text{(T-FIELD)}$$

$$\frac{\Gamma \vdash \overline{T}_{0:n}\, e_{0:n} \quad \mathit{mtype}(T_0, \mathtt{m}, z_0) = Z_{1:n}\, z_{1:n} : c \to U}{\Gamma, T_{0:n}\, z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n} \quad \sigma(\Gamma, T_{0:n}\, z_{0:n}) \vdash_C c \quad (z_{0:n}\ \text{fresh})}{\Gamma \vdash (T_{0:n}\, z_{0:n}; U)\, e_0.\mathtt{m}(e_{1:n})} \quad \text{(T-INVK)}$$

$$\frac{\Gamma \vdash \overline{T}\, \overline{e} \quad \theta = [\overline{f}/\mathtt{this}.\overline{f}] \quad \mathit{fields}(C, \theta) = \overline{Z}\, \overline{f}}{\Gamma, \overline{T}\, \overline{f} \vdash \overline{T} \sqsubseteq \overline{Z} \quad \sigma(\Gamma, \overline{T}\, \overline{f}) \vdash_C \mathit{inv}(C, \theta)}{\Gamma \vdash C(:\overline{T}\, \overline{f}; \mathtt{self}.\overline{f} = \overline{f})\, \mathtt{new}\, C(\overline{e})} \quad \text{(T-NEW)}$$

$$\frac{\overline{T}\, \overline{x}, C\, \mathtt{this}, c \vdash U\, e, U \sqsubseteq T}{T\, \mathtt{m}(\overline{T}\, \overline{x} : c)\{\mathtt{return}\ e;\}\ \text{OK in } C} \qquad \frac{\overline{M}\ \text{OK in } C}{\mathtt{class}\, C(\overline{T}\, \overline{f} : c)\ \mathtt{extends}\, D(:d)\, \{\overline{M}\}\ \text{OK}}$$

$$C \sqsubseteq C \qquad \frac{\mathtt{class}\, C(\ldots)\ \mathtt{extends}\, D(\ldots)\{\ldots\}}{C \sqsubseteq D} \qquad \frac{C \sqsubseteq D \quad D \sqsubseteq E}{C \sqsubseteq E} \qquad \frac{C \sqsubseteq D \quad \sigma(\Gamma, C(:c)\, x) \vdash_C d[x/\mathtt{self}] \quad (x\ \text{fresh})}{\Gamma \vdash C(:c) \sqsubseteq D(:d)}$$

$$\frac{\mathit{fields}(C) = \overline{C}\, \overline{f}}{(\mathtt{new}\, C(\overline{e})).f_i \to e_i} \quad \text{(R-FIELD)} \qquad \frac{\mathit{mbody}(\mathtt{m}, C) = \overline{x}.e_0}{(\mathtt{new}\, C(\overline{e})).\mathtt{m}(\overline{d}) \to [\overline{d}/\overline{x}, \mathtt{new}\, C(\overline{e})/\mathtt{this}]e_0} \quad \text{(R-INVK)}$$

$$\frac{\vdash C \sqsubseteq T[\mathtt{new}\, C(\overline{d})/\mathtt{self}]}{(T)(\mathtt{new}\, C(\overline{d})) \to \mathtt{new}\, C(\overline{d})} \quad \text{(R-CAST)} \qquad \frac{e_0 \to e_0'}{e_0.\mathtt{m}(\overline{e}) \to e_0'.\mathtt{m}(\overline{e})} \quad \text{(RC-INVK-RECV)}$$

$$\frac{e \to e'}{e.f_i \to e'.f_i} \quad \text{(RC-FIELD)} \qquad \frac{e_i \to e_i'}{e_0.\mathtt{m}(\ldots, e_i, \ldots) \to e_0.\mathtt{m}(\ldots, e_i', \ldots)} \quad \text{(RC-INVK-ARG)}$$

$$\frac{e \to e'}{(T)e \to (T)e'} \quad \text{(RC-CAST)} \qquad \frac{e_i \to e_i'}{\mathtt{new}\, C(\ldots, e_i, \ldots) \to \mathtt{new}\, C(\ldots, e_i', \ldots)} \quad \text{(RC-NEW-ARG)}$$

Figure 4. CFJ semantics

Similarly, in T-INVK we postulate the existence of a receiver object o of the given static type. For any type T, object o of type T and method name $\mathtt{m}$, let $\mathit{mtype}(T, \mathtt{m}, o)$ be a copy of the signature of the method with $\mathtt{this}$ replaced by o. We establish (under the assumption that the formals ($\overline{z}$) have the static type of the actuals)[6] that actual types are subtypes of the formal types, and the method constraint is satisfied. This permits us to record the constraint d on the return type, with the formal variables $\overline{z}$ existentially quantified.[7]

In T-NEW, similarly, we establish that the static types of the actual arguments to the constructor are subtypes of the declared types of the field, and contain enough information to satisfy the class invariant, c. The declared types (and c) contain references to $\mathtt{this}.\overline{f}$; these must be replaced by the formals $\overline{f}$, which carry information about the static type of the actuals. Note that the object o we hypothesized in an analogous situation in T-INVK does not exist; it will exist on successful invocation of the constructor. The constrained clause of the $\mathtt{new}$ expression contains all the information that can be gleaned from the static types of the actuals by assigning them to the corresponding fields of the object being created.

Let C be a class declared as

$$\mathtt{class}\, C(\overline{T}\, \overline{f} : c)\ \mathtt{extends}\, D(:d)\{\overline{M}\}.$$

Let θ be a substitution and the type T be based on C. We define $\mathit{inv}(T, \theta)$ as the conjunction $c\theta, d\theta$ and (recursively) $\mathit{inv}(D, \theta)$. We bottom out with $\mathit{inv}(\mathtt{Object}, \theta) = \mathtt{true}$. For a variable x, we use the shorthand $\mathit{inv}(C, x)$ to mean $\mathit{inv}(C, [x/\mathtt{self}])$.

We add a single subtyping rule to the rules of FJ to require that the subtype constraint entail the supertype constraint. Whenever we state an assumption of the form "x is fresh" in a rule we mean it is not free in the consequent of the rule.

The operational semantics are essentially those of FJ.

6. Related work

Constraint-based type systems enjoy a long history. The use of constraints for type inference and subtyping were developed by Mitchell [29] and Reynolds [46]. Trifonov and Smith [52] proposed a type system where types are refined by subtyping constraints. Dependent types are not supported. Pottier [40, 42] presents a constraint-based type system for an ML-like language with subtyping.

HM(X) [50, 41, 43] is a constraint-based framework for Hindley–Milner style type systems. The framework is parameterized on the specific constraint system X; instantiating X yields extensions of the HM type system. Constraints in HM(X) are over types, not values.

---

[6] This is stronger than assuming $\overline{Z}$.

[7] Recall that the $\overline{z}$ may occur in d but must not occur in a type in the calling environment; hence they must be existentially quantified in the resulting constraint.

Several systems have been proposed that refine types in a base type system through constraints. *Refinement types* [20] extend the Hindley–Milner type system with intersection, union, and constructor types, enabling specification and inference of more precise type information. *Conditional types* [1] extend refinement types to encode control-flow information in the types. Jones introduced *qualified types*, which permit types to be constrained by a finite set of predicates [25]. *Sized types* [23] annotate types with the sizes of recursive data structures. Sizes are linear functions of size variables. Size inference is performed using a constraint solver for Presburger arithmetic [45].

With hybrid type-checking [16, 17], types can be constrained by arbitrary boolean expressions. While typing is undecidable, dynamic checks are inserted into the program when necessary if the type-checker cannot determine type safety statically. In X10 dynamic type checks, including tests of dependent clauses, are inserted only at explicit casts.

Singleton types [5, 49] are dependent types containing only one value. In Stone's formulation [49], $S(e : \tau)$ is the type of all values of type τ that are equal to e. Term equivalence is constructed so that type-checking is decidable. The singleton $S(e : \tau)$ can be encoded in X10 as $\tau(:self == e)$.

Several languages—gbeta [15], Scala [35, 38], J& [33] and others [37, 36]—provide *path-dependent types*. For a final access path p, p.type in Scala is the singleton type containing the object p. In J&, p.class is a type containing all objects whose run-time class is the same as p's. Scala's p.type can be encoded in X10 using an equality constraint C(:self == p), where C is a supertype of p's static type.

Cayenne [7] is a Haskell-like language with fully dependent types. There is no distinction between static and dynamic types. Type-checking is undecidable. There is no notion of datatype refinement as in DML.

Epigram [28, 3] is a dependently typed functional programming language based on a type theory with inductive families. Epigram does not have a phase distinction between values and types.

ESC/Java [18] allow programmers to write object invariants and pre- and post-conditions that are enforced statically by the compiler using an automated theorem prover. Static checking is undecidable and, in the presence of loops, is unsound (but still useful) unless the programmer supplies loop invariants. ESC/Java can enforce invariants on mutable state.

Pluggable and optional type systems were proposed by Bracha [10] and provide another means of specifying refinement types. Type annotations, implemented in compiler plugins, serve only to reject programs statically that might otherwise have dynamic type errors. CQual [19] extends C with user-defined type qualifiers. These qualifiers may be flow-sensitive and may be inferred. CQual supports only a fixed set of typing rules for all qualifiers. In contrast, the *semantic type qualifiers* of Chin, Markstrum, and Millstein [12] allow programmers to define typing rules for qualifiers in a meta language that allows type-checking rules to be specified declaratively. JavaCOP [4] is a pluggable type system framework for Java. Annotations are defined in a meta language that allows type-checking rules to be specified declaratively. JSR 308 [26] is a proposal for adding user-defined type qualifiers to Java.

Our work is most closely related to DML, [54], an extension of ML with dependent types. DML is also built parametrically on a constraint solver. Types are refinement types; they do not affect the operational semantics and erasing the constraints yields a legal ML program.

At a conceptual level the intuitions behind the development of DML and constrained types are similar. Both are intended for practical programming by mainstream programmers, both introduce a strict separation between compile-time and run-time processing, are parametric on a constraint solver, and deal with mutually recursive data-structures, mutable state, and higher-order functions (encoded as objects in the case of constrained types). Both support existential types.

The most obvious distinction between the two lies in the target domain: DML is designed for functional programming, specifically ML, whereas constrained types are designed for imperative, concurrent OO languages. Hence technically our development of constrained types takes the route of an extension to FJ. But there are several other crucial differences as well.

First, DML achieves its separation by not permitting program variables to be used in types. Instead, a parallel set of (universally or existentially quantified) "index" variables are introduced. For instance the typing of the append operation on lists is provided by:

```
fun('a)
  append(nil, ys) = ys
| append(cons(x, xs), ys)
    = cons(x, append(xs,ys))
where append <| {m:nat}{n:nat}
    'a list(m) * 'a list(n) -> 'a list(m+n)
```

in contrast with the direct embedded expression with constrained types:

```
class List(int(:self >= 0) n) {
  Object item;
  List(n-1) tail;
  List(n+a.n) append(final List a) {
    return n==0
      ? a : new List(item, tail.app(a));
  }
  ...
}
```

Second, DML permits only variables of basic index sorts known to the constraint solver (e.g., bool, int, nat) to occur in types. In contrast, constrained types permit program variables at any type to occur in constrained types. As with

DML, only operations specified by the constraint system are permitted in types. However, these operations always include field selection and equality on object references. (As we have seen permitting arbitrary type/property graphs may lead to undecidability.) Note that DML style constraints are easily encoded in constrained types.

Third, DML does not permit any runtime checking of constraints (dynamic casts).

7. Conclusion and future work

We have presented the design and implementation of constrained types in X10. The design considerably enriches the space of statically checkable types expressible in the language. This is particularly important for data-structures such as lists and arrays. Several examples of constrained types were presented. Constrained types have been implemented in X10 and used for place types, clocked types, and array types.

The implementation supports extension with constraint solver plugins. In future work, we plan to investigate optimizations (such as array bounds check elimination) enabled by constrained types. We also plan to explore type inference for constrained types and to pursue more expressive constraint systems and extensions of constrained types for handling mutable state, control flow, and effects.

Acknowledgments

References

[1] Alexander Aiken, Edward L. Wimmers, and T. K. Lakshman. Soft typing with conditional types. In *Proceedings of the 21st Annual ACM SIGPLAN–SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 163–173, January 1994.

[2] Hassan Ait-Kaci. *A lattice theoretic approach to computation based on a calculus of partially ordered type structures (property inheritance, semantic nets, graph unification)*. PhD thesis, University of Pennsylvania, 1984.

[3] Thorsten Altenkirch, Conor McBride, and James McKinna. Why dependent types matter. `http://www.e-pig.org/downloads/ydtm.pdf`, April 2005.

[4] Chris Andreae, James Noble, Shane Markstrum, and Todd Millstein. A framework for implementing pluggable type systems. In *Proceedings of the 2006 ACM Conference on Object Oriented Programming Systems, Languages, and Applications (OOPSLA)*, October 2006.

[5] David Aspinall. Subtyping with singleton types. In *CSL '94: Selected Papers from the 8th International Workshop on Computer Science Logic*, volume 933 of *LNCS*, pages 1–15, London, UK, 1995. Springer-Verlag.

[6] David Aspinall and Martin Hofmann. *Dependent Types*, chapter 2. In Pierce [39], 2004.

[7] Lennart Augustsson. Cayenne: a language with dependent types. In *Proceedings of the ACM SIGPLAN International Conference on Functional Programming (ICFP '98)*, pages 239–250, 1998.

[8] Clark Barrett and Sergey Berezin. CVC Lite: A new implementation of the cooperating validity checker. In Rajeev Alur and Doron A. Peled, editors, *Proceedings of the 16th International Conference on Computer Aided Verification (CAV '04)*, volume 3114 of *Lecture Notes in Computer Science*, pages 515–518. Springer-Verlag, July 2004. Boston, Massachusetts.

[9] Clark Barrett, Cesare Tinelli, Alexander Fuchs, Yeting Ge, George Hagen, and Dejan Jovanovic. CVC3. `http://www.cs.nyu.edu/acsys/cvc3`.

[10] Gilad Bracha. Pluggable type systems. In *OOPSLA'04 Workshop on Revival of Dynamic Languages*, October 2004.

[11] Bradford L. Chamberlain, Sung-Eun Choi, Steven J. Deitz, and Lawrence Snyder. The high-level parallel language ZPL improves productivity and performance. In *Proceedings of the IEEE International Workshop on Productivity and Performance in High-End Computing*, 2004.

[12] Brian Chin, Shane Markstrum, and Todd Millstein. Semantic type qualifiers. In *Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)*, pages 85–95, 2005.

[13] Thierry Coquand and Gerard Huet. The Calculus of Constructions. *Information and Computation*, 76, 1988.

[14] Mark Day, Robert Gruber, Barbara Liskov, and Andrew C. Myers. Subtypes vs. where clauses: Constraining parametric polymorphism. In *Proceedings of the 1995 ACM Conference on Object-Oriented Programming Systems, Languages, and Applications (OOPSLA)*, pages 156–168, Austin, TX, October 1995.

[15] Erik Ernst. *gbeta: A Language with Virtual Attributes, Block Structure, and Propagating, Dynamic Inheritance*. PhD thesis, Department of Computer Science, University of Aarhus, Århus, Denmark, 1999.

[16] Cormac Flanagan. Hybrid type checking. In *Proceedings of the 33rd Annual Symposium on Principles of Programming Languages (POPL'06)*, pages 245–256, 2006.

[17] Cormac Flanagan, Stephen N. Freund, and Aaron Tomb. Hybrid types, invariants, and refinements for imperative objects. In *International Workshop on Foundations of Object-Oriented Programming (FOOL)*, 2006.

[18] Cormac Flanagan, K. Rustan M. Leino, Mark Lillibridge, Greg Nelson, James B. Saxe, and Raymie Stata. Extended static checking for Java. In *Proceedings of ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)*, June 2002.

[19] Jeffrey S. Foster, Tachio Terauchi, and Alex Aiken. Flow-sensitive type qualifiers. In *Proceedings of the 29th ACM SIGPLAN–SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 1–12. ACM Press, June 2002.

[20] Tim Freeman and Frank Pfenning. Refinement types for ML. In *Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)*, pages 268–277, June 1991.

[21] J. Gosling, W. Joy, G. Steele, and G. Bracha. *The Java Language Specification, Third Edition*. Addison Wesley, 2006.

[22] Christian Grothoff, Jens Palsberg, and Vijay Saraswat. Safe arrays via regions and dependent types. Technical Report RC23911, IBM T.J. Watson Research Center, 2006.

[23] John Hughes, Lars Pareto, and Amr Sabry. Proving the correctness of reactive systems using sized types. In *Proceedings of the 23rd ACM SIGPLAN–SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 410–423, 1996.

[24] A. Igarashi, B. Pierce, and P. Wadler. Featherweight Java: A minimal core calculus for Java and GJ. In *ACM Symposium on Object-Oriented Programming: Systems, Languages and Applications*, 1999.

[25] Mark P. Jones. *Qualified Types: Theory and Practice*. Cambridge University Press, 1994.

[26] JSR 308: Annotations on Java types. `http://jcp.org/en/jsr/detail?id=308`.

[27] Per Martin-Löf. *A Theory of Types*. 1971.

[28] Conor McBride and James McKinna. The view from the left. *Journal of Functional Programming*, 14(1):69–111, 2004.

[29] John C. Mitchell. Coercion and type inference. In *Proceedings of the 11th Annual ACM Symposium on Principles of Programming Languages (POPL'84)*, pages 174–185, 1984.

[30] G. Nelson and D. Oppen. Simplification by cooperating decision procedures. *ACM Transactions on Programming Languages and Systems*, 1(2), October 1979.

[31] Flemming Nielson and Hanne Riis Nielson. *Two-level functional languages*. Cambridge University Press, 1992.

[32] Nathaniel Nystrom, Michael R. Clarkson, and Andrew C. Myers. Polyglot: An extensible compiler framework for Java. In Görel Hedin, editor, *Compiler Construction, 12th International Conference, CC 2003*, number 2622 in LNCS, pages 138–152. Springer-Verlag, April 2003.

[33] Nathaniel Nystrom, Xin Qi, and Andrew C. Myers. J&: Nested intersection for scalable software extension. In *Proceedings of the 2006 ACM Conference on Object Oriented Programming Systems, Languages, and Applications (OOPSLA)*, pages 21–36, Portland, OR, October 2006.

[34] Nathaniel Nystrom and Vijay Saraswat. An annotation and compiler plugin system for X10. Technical Report RC24198, IBM T.J. Watson Research Center, 2007.

[35] Martin Odersky, Philippe Altherr, Vincent Cremet, Burak Emir, Sebastian Maneth, Stéphane Micheloud, Nikolay Mihaylov, Michel Schinz, Erik Stenman, and Matthias Zenger. An overview of the Scala programming language. Technical report, École Polytechnique Fédérale de Lausanne, June 2004. `http://scala.epfl.ch/docu/files/ScalaOverview.pdf`.

[36] Martin Odersky, Vincent Cremet, Christine Röckl, and Matthias Zenger. A nominal theory of objects with dependent types. In *Proceedings of 17th European Conference on Object-Oriented Programming (ECOOP 2003)*, volume 2743 of *LNCS*, pages 201–224. Springer-Verlag, July 2003.

[37] Martin Odersky and Christoph Zenger. Nested types. In *8th Workshop on Foundations of Object-Oriented Languages (FOOL)*, 2001.

[38] Martin Odersky and Matthias Zenger. Scalable component abstractions. In *OOPSLA05*, pages 41–57, San Diego, CA, USA, October 2005.

[39] Benjamin C. Pierce, editor. *Advanced Topics in Types and Programming Languages*. MIT Press, 2004.

[40] François Pottier. Simplifying subtyping constraints. In *Proceedings of the ACM SIGPLAN International Conference on Functional Programming (ICFP '96)*, pages 122–133, 1996.

[41] François Pottier. A semi-syntactic soundness proof for HM(X). Technical Report RR 4150, INRIA, March 2001.

[42] François Pottier. Simplifying subtyping constraints, a theory. *Information and Computation*, 170(2):153–183, November 2001.

[43] François Pottier and Didier Rémy. *The Essence of ML Type Inference*, chapter 10. In Pierce [39], 2004.

[44] W. H. Press, B. P. Flannery, S. A. Teukolsky, and W. T. Vetterling. *Numerical Recipes in FORTRAN: The Art of Scientific Computing*, pages 866–869. Cambridge University Press, 1992. Successive overrelaxation (SOR).

[45] William Pugh. The omega test: A fast and practical integer programming algorithm for dependence analysis. In *Supercomputing '91: Proceedings of the 1991 ACM/IEEE Conference on Supercomputing*, pages 4–13, 1991.

[46] John C. Reynolds. Three approaches to type structure. In *Proceedings of TAPSOFT/CAAP 1985*, volume 185 of *LNCS*, pages 97–138. Springer-Verlag, 1985.

[47] V. Saraswat et al. Report on the programming language X10. Technical report, IBM T.J. Watson Research Center, 2006.

[48] Vijay Saraswat. The category of constraint systems is Cartesian closed. In *LICS '92*, pages 341–345, 1992.

[49] Christopher A. Stone. *Singleton Types and Singleton Kinds*. PhD thesis, Carnegie–Mellon University, August 2000. Also availalble as CMU technical report CMU-CS-00-153.

[50] Martin Sulzmann, Martin Odersky, and Martin Wehr. Type inference with constrained types. In *Fourth International Workshop on Foundations of Object-Oriented Programming (FOOL 4)*, 1997.

[51] Walid Taha and Tim Sheard. Multi-stage programming with explicit annotations. In *ACM/SIGPLAN Workshop on Partial Evaluation and Semantics-Based Program Manipulation*, pages 203–217, 1997.

[52] Valery Trifonov and Scott Smith. Subtyping constrained types. In *Third International Static Analysis Symposium (SAS)*, number 1145 in LNCS, pages 349–365, 1996.

[53] Hongwei Xi and Frank Pfenning. Eliminating array bound checking through dependent types. In *Proceedings of ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)*, pages 249–257, Montreal, Canada, June 1998.

[54] Hongwei Xi and Frank Pfenning. Dependent types in practical programming. In *Proceedings of the 26th Annual ACM Symposium on Principles of Programming Languages (POPL'99)*, pages 214–227, San Antonio, TX, January 1999.

A. Soundness

Here we prove a soundness theorem for CFJ.

LEMMA A.1 (Substitution Lemma). *Assume* $\Gamma \vdash \overline{A}\,\overline{d}$, $\Gamma, \overline{A}\overline{x} \vdash \overline{A} \sqsubseteq \overline{B}$, *and* $\Gamma, \overline{B}\,\overline{x} \vdash T\ e$. *Then there exists a type* S *such that* $\Gamma \vdash S\ e[\overline{d}/\overline{x}]$ *and* $\Gamma \vdash S \sqsubseteq \overline{A}\ \overline{x}; T$.

PROOF. Straightforward. $\square$

LEMMA A.2 (Weakening). *If* $\Gamma \vdash T\ e$, *then* $\Gamma, S\ x \vdash T\ e$.

PROOF. Straightforward. $\square$

LEMMA A.3 (Body type). *If* $\mathrm{mtype}(C(:d),m,z_0) = \overline{T}\ \overline{x} : c \to S$, *and* $mbody(m,C) = \overline{x}.e$, *then there exists* U,V *such that* $C \sqsubseteq U$, $V \sqsubseteq S$, *and* $\overline{T}\ \overline{x}, U\ \texttt{this} \vdash V\ e$.

PROOF. Straightforward. $\square$

LEMMA A.4. *We have* $\Gamma \vdash T \sqsubseteq T$. *If* $\Gamma \vdash T_1 \sqsubseteq T_2$ *and* $\Gamma \vdash T_2 \sqsubseteq T_3$, *then* $\Gamma \vdash T_1 \sqsubseteq T_3$.

PROOF. Straightforward. $\square$

LEMMA A.5. *If* $\Gamma \vdash S \sqsubseteq T$, *then* $\mathrm{fields}(S,z)$ *has* $\mathrm{fields}(T,z)$ *as a prefix.*

PROOF. Immediate from the definition of *fields*. $\square$

LEMMA A.6. *If* $S \sqsubseteq T$, *then* $\mathrm{mtype}(S,m,z) = \mathrm{mtype}(T,m,z)$.

PROOF. Immediate from the definition of *mtype*. $\square$

LEMMA A.7. *If* $\Gamma \vdash S \sqsubseteq T$, *then*

$$(S\ z;\ c_0)[x/\texttt{self}] \vdash_C (T\ z;\ c_0)[x/\texttt{self}]$$

where x is fresh.

PROOF. Straightforward. $\square$

LEMMA A.8. *If* $\Gamma \vdash S \sqsubseteq T$, *and* $\sigma(\Gamma, T\ f) \vdash_C c_0$, *then* $\sigma(\Gamma, S\ f) \vdash_C c_0$,

PROOF. From $\Gamma \vdash S \sqsubseteq T$, we must have $S = C(:c)$ and $T = D(:d)$ where $C \sqsubseteq D$ and $\sigma(\Gamma, C(:c)\ x) \vdash_C d[x/\texttt{self}]$ with x fresh. From the definition of $\sigma(\cdot)$ we have

$$\sigma(\Gamma, S\ f) = \sigma(\Gamma), c[f/\texttt{self}], inv(C, f)$$

and

$$\sigma(\Gamma, T\ f) = \sigma(\Gamma), d[f/\texttt{self}], inv(D, f).$$

From $\Gamma \vdash S \sqsubseteq T$ we have $\sigma(\Gamma, C(:c)\ x) \vdash_C d[f/\texttt{self}]$. Additionally, from the definition of $inv(C, f)$ and from $C \sqsubseteq D$, we have that $inv(C, F)$ is a constraint that has $inv(D, f)$ as a conjunct so $inv(C, f) \vdash_C inv(D, f)$. We conclude $\sigma(\Gamma, S\ f) \vdash_C \sigma(\Gamma, T\ f)$. We have that $\vdash_C$ is transitive so from $\sigma(\Gamma, S\ f) \vdash_C \sigma(\Gamma, T\ f)$ and $\sigma(\Gamma, T\ f) \vdash_C c_0$, we have $\sigma(\Gamma, S\ f) \vdash_C c_0$. $\square$

LEMMA A.9. *if* $\Gamma, T\ f \vdash U \sqsubseteq U'$, *and* $\Gamma \vdash S \sqsubseteq T$, *then* $\Gamma, S\ f \vdash U \sqsubseteq U'$.

PROOF. From $\Gamma, T\ f \vdash U \sqsubseteq U'$ we must have $U = C(:c)$ and $U' = D(:d)$ where $C \sqsubseteq D$ and

$$\sigma(\Gamma, T\ f, C(:c)\ x) \vdash_C d[x/\texttt{self}]$$

with x fresh. From Lemma A.8, $\Gamma \vdash S \sqsubseteq T$, and

$$\sigma(\Gamma, T\ f, C(:c)\ x) \vdash_C d[x/\texttt{self}],$$

we have

$$\sigma(\Gamma, S\ f, C(:c)\ x) \vdash_C d[x/\texttt{self}].$$

So we can use $C \sqsubseteq D$ and

$$\sigma(\Gamma, S\ f, C(:c)\ x) \vdash_C d[x/\texttt{self}]$$

to derive $\Gamma, S\ f \vdash U \sqsubseteq U'$. $\square$

LEMMA A.10. *if* $\Gamma \vdash S \sqsubseteq T$, *then* $\Gamma \vdash E(S\ z; c_0) \sqsubseteq E(T\ z; c_0)$.

PROOF. To prove the desired conclusion $E(S\ z; c_0) \sqsubseteq E(T\ z; c_0)$ we need to show that

$$\sigma(\Gamma, E(:S\ z; c_0)\ x) \vdash_C (T\ z; c_0)[x/\texttt{self}].$$

We have

$$\sigma(\Gamma, E(:S\ z; c_0)\ x) = \sigma(\Gamma), (S\ z; c_0)[x/\texttt{self}], inv(E, x).$$

From Lemma A.7 and $\Gamma \vdash S \sqsubseteq T$, we have

$$(S\ z; c_0)[x/\texttt{self}] \vdash_C (T\ z; c_0)[x/\texttt{self}].$$

From

$$\sigma(\Gamma, E(:S\ z; c_0)\ x) = \sigma(\Gamma), (S\ z; c_0)[x/\texttt{self}], inv(E, x)$$

and

$$(S\ z; c_0)[x/\texttt{self}] \vdash_C (T\ z; c_0)[x/\texttt{self}],$$

we conclude

$$\sigma(\Gamma, E(:S\ z; c_0)\ x) \vdash_C (T\ z; c_0)[x/\texttt{self}].$$

$\square$

THEOREM A.11 (Subject Reduction). *If* $\Gamma \vdash T\ e$ *and* $e \to e'$, *then for some type S,* $\Gamma \vdash S\ e'$ *and* $\Gamma \vdash S \sqsubseteq T$.

PROOF. We proceed by induction on the structure of the derivation of $\Gamma \vdash T\ e$. We now have five cases depending on the last rule used in the derivation of $\Gamma \vdash T\ e$.

- T-VAR: The expression cannot take a step, so the conclusion is immediate.
- T-CAST: We have two subcases.
  - R-CAST: For the expression (T) o, where $o = $ new $C(\bar{d})$, we have from T-CAST that
    $$\Gamma \vdash \mathtt{C}(:\overline{U}\ \overline{f}; \mathtt{self}.\overline{f} = \overline{f})\ \mathtt{o}.$$
    Additionally, we have from R-CAST that $\vdash C \sqsubseteq T[o/\mathtt{self}]$. We now choose
    $$S = \mathtt{C}(:\overline{U}\ \overline{f}; \mathtt{self}.\overline{f} = \overline{f}; \mathtt{self} = \mathtt{o}).$$
    From
    $$\Gamma \vdash \mathtt{C}(:\overline{U}\ \overline{f}; \mathtt{self}.\overline{f} = \overline{f})\ \mathtt{o}$$
    we get $\Gamma \vdash S\ o$. From Lemma A.2 and $\vdash C \sqsubseteq T[o/\mathtt{self}]$ we get $\Gamma \vdash C \sqsubseteq T[o/\mathtt{self}]$. From $\Gamma \vdash C \sqsubseteq T[o/\mathtt{self}]$ we get $\Gamma \vdash S \sqsubseteq T$.
  - RC-CAST: For the expression (T) e, we have from T-CAST that $\Gamma \vdash U\ e$. Additionally, we have from RC-CAST that $e \to e'$. From the induction hypothesis, we have U' such that $\Gamma \vdash U'\ e'$ and $\Gamma \vdash U' \sqsubseteq U$. We now choose $S = T$. From $\Gamma \vdash U'\ e'$ and T-CAST we derive $\Gamma \vdash S$ (T) e'. From $S = T$ and Lemma A.4 we have $\Gamma \vdash S \sqsubseteq T$.
- T-NEW: We have a single case.
  - RC-NEW-ARG: For the expression new $C(\bar{e})$, we have from T-NEW that $\Gamma \vdash \overline{T}\ \overline{e}$, $\theta = [\overline{f}/\mathtt{this}.\overline{f}]$, $\mathit{fields}(C, \theta) = \overline{Z}\ \overline{f}$, $\Gamma, \overline{T}\ \overline{f} \vdash \overline{T} \sqsubseteq \overline{Z}$, and $\sigma(\Gamma, \overline{T}\ \overline{f}) \vdash_C \mathit{inv}(\mathtt{C}, \theta)$. Additionally, we have from RC-NEW-ARG that $e_i \to e'_i$. From the induction hypothesis, we have S_i such that $\Gamma \vdash S_i\ e'_i$ and $\Gamma \vdash S_i \sqsubseteq T_i$.
    For all j except i, define $S_j = T_j$ and $e'_j = e_j$. We have $\Gamma \vdash \overline{S}\ \overline{e}'$ and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$. From Lemma A.9, $\Gamma, \overline{T}\ \overline{f} \vdash \overline{T} \sqsubseteq \overline{Z}$, and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, we have $\Gamma, \overline{S}\ \overline{f} \vdash \overline{T} \sqsubseteq \overline{Z}$. From Lemma A.2 and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, we have $\Gamma, \overline{S}\ \overline{f} \vdash \overline{S} \sqsubseteq \overline{T}$. From Lemma A.4, $\Gamma, \overline{S}\ \overline{f} \vdash \overline{S} \sqsubseteq \overline{T}$, and $\Gamma, \overline{S}\ \overline{f} \vdash \overline{T} \sqsubseteq \overline{Z}$, we have $\Gamma, \overline{S}\ \overline{f} \vdash \overline{S} \sqsubseteq \overline{Z}$. From Lemma A.8, $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, and $\sigma(\Gamma, \overline{T}\ \overline{f}) \vdash_C \mathit{inv}(\mathtt{C}, \theta)$, we have $\sigma(\Gamma, \overline{S}\ \overline{f}) \vdash_C \mathit{inv}(\mathtt{C}, \theta)$.
    We now choose $S = C(:\overline{S}\ \overline{f}; \mathtt{self}.\overline{f} = \overline{f})$. From $\Gamma \vdash \overline{S}\ \overline{e}$, $\theta = [\overline{f}/\mathtt{this}.\overline{f}]$, $\mathit{fields}(C, \theta) = \overline{Z}\ \overline{f}$, $\Gamma, \overline{S}\ \overline{f} \vdash \overline{S} \sqsubseteq \overline{Z}$, $\sigma(\Gamma, \overline{S}\ \overline{f}) \vdash_C \mathit{inv}(\mathtt{C}, \theta)$, and T-NEW we derive $\Gamma \vdash S$ new $C(\overline{e}'$. We have $T = C(:\overline{T}\ \overline{f}; \mathtt{self}.\overline{f} = \overline{f})$.
    From Lemma A.10 and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, we have $\Gamma \vdash S \sqsubseteq T$.
- T-FIELD: We have two subcases.
  - R-FIELD: For the expression $(\mathtt{new}C(\bar{e})).\mathtt{f_i}$, we have from T-FIELD that $\Gamma \vdash T_0\ e$ and $\mathit{fields}(T_0, z_0) =$

$\overline{U}\ \overline{f}$, where z_0 is fresh. Additionally, we have from R-FIELD that $\mathit{fields}(C) = \overline{C}\ \overline{f}$.
We have $T_0 = C(:\overline{T}\ \overline{f}; \mathtt{self}.\overline{f} = \overline{f})$ and from T-NEW, $\Gamma \vdash \overline{T}\ \overline{e}$, $\theta = [\overline{f}/\mathtt{this}.\overline{f}]$, $\mathit{fields}(C, \theta) = \overline{Z}\ \overline{f}$, $\Gamma, \overline{T}\ \overline{f} \vdash \overline{T} \sqsubseteq \overline{Z}$, and $\sigma(\Gamma, \overline{T}\ \overline{f}) \vdash_C \mathit{inv}(\mathtt{C}, \theta)$.
From $\Gamma \vdash \overline{T}\ \overline{e}$, we have $\Gamma \vdash T_i\ e_i$. We now choose $S = T_i$.
Finally, it is straightforward to show
$$\Gamma \vdash S \sqsubseteq (T_0 z_0; z_0.f_i = \mathtt{self}; U_i).$$

  - RC-FIELD: For the expression $e.f_i$, we have from T-FIELD that $\Gamma \vdash T_0\ e$ and $\mathit{fields}(T_0, z_0) = \overline{U}\ \overline{f_i}$ where z_0 is fresh. Additionally, we have from RC-FIELD that $e \to e'$. From the induction hypothesis, we have S_0 such that $\Gamma \vdash S_0\ e'$ and $\Gamma \vdash S_0 \sqsubseteq T_0$.
    We now choose $S = (S_0\ z_0; z_0.f_i = \mathtt{self}; U_i)$. From $\Gamma \vdash S_0\ e'$, Lemma A.5, and T-FIELD, we derive $\Gamma \vdash Se'$.
    From $\Gamma \vdash S_0 \sqsubseteq T_0$ and Lemma A.10, we have $\Gamma \vdash S \sqsubseteq T$.

- T-INVK: We have three subcases.
  - R-INVK: For the expression $(\mathtt{new}\ C(\bar{e})).m(\bar{d})$ we have from T-INVK that $\Gamma \vdash T_0\ (\mathtt{new}\ C(\bar{e}))$, $\Gamma \vdash T_{1:n}\ d_{1:n}$, $\mathit{mtype}(T_0, m, z_0) = Z_{1:n}\ z_{1:n} : c \to U$, $\Gamma, T_{0:n}\ z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n}$, and $\sigma(\Gamma, T_{0:n}\ z_{0:n}) \vdash_C c$, where $z_{0:n}$ is fresh, and $T_0 = C(\overline{Af}; self.\overline{f} = \overline{f})$ and $\Gamma \vdash \overline{A}\overline{e}$.
    For simplicity, define $d_0 = (\mathtt{new}\ C(\bar{e}))$. Additionally, we have from R-INVK that $\mathit{mbody}(m, C) = \bar{x}.e_0$.
    From Lemma A.3, $\mathit{mtype}(T_0, m, z_0) = Z_{1:n}\ z_{1:n} : c \to U$, and $\mathit{mbody}(m, C) = \bar{x}.e_0$, we have D, V such that $C \sqsubseteq D, V \sqsubseteq U$, and $Z_{1:n}\ \bar{z}_{1:n}, D$ this $\vdash V\ e$.
    From Lemmas A.4 and A.2, $T_0 = C(\overline{Af}; \mathtt{self}.\overline{f} = \overline{f})$, $\Gamma \vdash T_0 \sqsubseteq C$ and $C \sqsubseteq D$, we have $\Gamma, T_{0:n}\ z_{0:n} \vdash T_0 \sqsubseteq D$.
    From Lemma A.2 and $Z_{1:n}\ \bar{z}_{1:n}, D$ this $\vdash V\ e_0$, we have $\Gamma, Z_{1:n}\ \bar{z}_{1:n}, D$ this $\vdash V\ e$.
    From Lemma A.1 and
    $$\begin{aligned} &\Gamma \vdash T_{0:n}\ d_{0:n}, \\ &\Gamma, T_{0:n}\ z_{0:n} \vdash T_0 \sqsubseteq D, \\ &\Gamma, T_{0:n}\ z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n}, \text{and} \\ &\Gamma, Z_{1:n}\ \bar{z}_{1:n}, D\ \mathtt{this} \vdash V\ e_0, \end{aligned}$$
    we have a type S such that $\Gamma \vdash S\ e_0[\bar{d}/z_{0:n}, \mathtt{new}\ C(\bar{e})/\mathtt{this}]$ and $\Gamma \vdash S \sqsubseteq \overline{T}\ z_{0:n}; V$.
  - RC-INVK-RECV: For the expression $e_0.m(\bar{e})$, we have from T-INVK that
    $$\begin{aligned} &\Gamma \vdash T_{0:n}\ e_{0:n}, \\ &\mathit{mtype}(T_0, m, z_0) = Z_{1:n}\ z_{1:n} : c \to U, \\ &\Gamma, T_{0:n}\ z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n}, \text{and} \\ &\sigma(\Gamma, T_{0:n}\ z_{0:n}) \vdash_C c \end{aligned}$$
    where $z_{0:n}$ is fresh.
    Additionally, from RC-INVK-RECV we have that $e_0 \to e'_0$. From the induction hypothesis, we have S_0

such that $\Gamma \vdash S_0\ e'_0$ and $\Gamma \vdash S_0 \sqsubseteq T_0$. For all $j > 0$, define $S_j = T_j$ and $e'_j = e_j$. We have $\Gamma \vdash \overline{S}\ \overline{e}'$ and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$.

From Lemma A.6 and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, we have

$$mtype(S_0, m, z) = mtype(T_0, m, z).$$

From Lemma A.9, $\Gamma, T_{0:n}\ z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n}$, and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, we have $\Gamma, S_{0:n}\ z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n}$,
From Lemma A.8, $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, and $\sigma(\Gamma, T_{0:n}\ z_{0:n}) \vdash_C c$ we have $\sigma(\Gamma, S_{0:n}\ z_{0:n}) \vdash_C c$.
We now choose $S = (S_{0:n}\ z_{0:n}; U)$. From $\Gamma \vdash S_{0:n}\ e'_{0:n}$, $mtype(S_0, m, z_0) = Z_{1:n}\ z_{1:n} : c \rightarrow U$, $\Gamma, S_{0:n}\ z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n}$, and $\sigma(\Gamma, S_{0:n}\ z_{0:n}) \vdash_C c$, and T-INVK we derive $\Gamma \vdash S\ e_0.m(e'_{1:n})$. We have $T = (T_{0:n}\ z_{0:n}; U)$.
From Lemma A.10 and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, we have $\Gamma \vdash S \sqsubseteq T$.

- RC-INVK-ARG: For the expression $e_0.m(\overline{e})$, we have from T-INVK that $\Gamma \vdash T_{0:n}\ e_{0:n}$, $mtype(T_0, m, z_0) = Z_{1:n}\ z_{1:n} : c \rightarrow U$, $\Gamma, T_{0:n}\ z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n}$, and $\sigma(\Gamma, T_{0:n}\ z_{0:n}) \vdash_C c$, where $z_{0:n}$ is fresh.
Additionally, from RC-INVK-ARG we have that, for $i > 0$, $e_i \rightarrow e'_i$. From the induction hypothesis, we have S_i such that $\Gamma \vdash S_i\ e'_i$ and $\Gamma \vdash S_i \sqsubseteq T_i$. For all j except i, define $S_j = T_j$ and $e'_j = e_j$. We have $\Gamma \vdash \overline{S}\ \overline{e}'$ and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$.
From Lemma A.9, $\Gamma, T_{0:n}\ z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n}$, and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, we have $\Gamma, S_{0:n}\ z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n}$,
From Lemma A.2 and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, we have $\Gamma, S_{0:n}\ z_{0:n} \vdash \overline{S} \sqsubseteq \overline{T}$.
From Lemma A.4, $\Gamma, S_{0:n}\ z_{0:n} \vdash \overline{S} \sqsubseteq \overline{T}$, and $\Gamma, S_{0:n}\ z_{0:n} \vdash T_{1:n} \sqsubseteq Z_{1:n}$, we have $\Gamma, S_{0:n}\ z_{0:n} \vdash \overline{S} \sqsubseteq Z_{1:n}$.
From Lemma A.8, $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, and $\sigma(\Gamma, T_{0:n}\ z_{0:n}) \vdash_C c$ we have $\sigma(\Gamma, S_{0:n}\ z_{0:n}) \vdash_C c$.
We now choose $S = (S_{0:n}\ z_{0:n}; U)$. From $\Gamma \vdash S_{0:n}\ e'_{0:n}$, $mtype(S_0, m, z_0) = Z_{1:n}\ z_{1:n} : c \rightarrow U$, $\Gamma, S_{0:n}\ z_{0:n} \vdash S_{1:n} \sqsubseteq Z_{1:n}$, and $\sigma(\Gamma, S_{0:n}\ z_{0:n}) \vdash_C c$, and T-INVK we derive $\Gamma \vdash S\ e_0.m(e'_{1:n})$. We have $T = (T_{0:n}\ z_{0:n}; U)$.
From Lemma A.10 and $\Gamma \vdash \overline{S} \sqsubseteq \overline{T}$, we have $\Gamma \vdash S \sqsubseteq T$.

$\square$

Let the normal form of expressions be given by *values* $v ::= $ new $C(\overline{v})$.

THEOREM A.12 (Progress). *If $\vdash T\ e$, then one of the following conditions holds:*

1. e *is a value* v,
2. e *contains a subexpression* (T) new $C(\overline{v})$ *such that* $\nvdash C \sqsubseteq T[$new $C(\overline{v})/$self$]$,
3. *there exists* e' *s.t.* $e \rightarrow e'$.

PROOF. The proof has a structure that is similar to the proof of Subject Reduction; we omit the details. $\square$

THEOREM A.13 (Type Soundness). *If $\vdash T\ e$ and $e \rightarrow^* e'$, with e' in normal form, then e' is either (1) a value v with $\vdash S\ v$ and $\vdash S \sqsubseteq T$, for some type S, or, (2) an expression containing a subexpression (T)new $C(\overline{v})$ where $\nvdash C \sqsubseteq T[$new $C(\overline{v})/$self$]$.*

PROOF. Combine Theorem A.11 and Theorem A.12. $\square$