

A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

Edlira Kuci¹, Sebastian Erdweg², Oliver Bračevac¹, Andi Bejleri¹,
and Mira Mezini^{1,3}

¹ Technische Universität Darmstadt, Germany

² TU Delft, The Netherlands

³ Lancaster University, UK

Abstract

This paper addresses compositional and incremental type checking for object-oriented programming languages. Recent work achieved incremental type checking for structurally typed functional languages through *co-contextual typing rules*, a constraint-based formulation that removes any context dependency for expression typings. However, that work does not cover key features of object-oriented languages: Subtype polymorphism, nominal typing, and implementation inheritance. Type checkers encode these features in the form of class tables, an additional form of typing context inhibiting incrementalization.

In the present work, we demonstrate that an appropriate co-contextual notion to class tables exists, paving the way to efficient incremental type checkers for object-oriented languages. This yields a novel formulation of Igarashi et al.’s Featherweight Java (FJ) type system, where we replace class tables by the dual concept of class table requirements and class table operations by dual operations on class table requirements. We prove the equivalence of FJ’s type system and our co-contextual formulation. Based on our formulation, we implemented an incremental FJ type checker and compared its performance against javac on a number of realistic example programs.

1998 ACM Subject Classification D.3.3 Language Constructs and Features, F.3.1 Specifying and Verifying and Reasoning about Programs, F.3.2 Semantics of Programming Languages

Keywords and phrases type checking; co-contextual; constraints; class table; Featherweight Java

1 Introduction

Previous work [6] presented a *co-contextual formulation* of the PCF type system with records, parametric polymorphism, and subtyping by duality of the traditional contextual formulation. The contextual formulation is based on a typing context and operations for looking up, splitting, and extending the context. The co-contextual formulation replaces the typing context and its operations with the dual concepts of context requirements and operations for generating, merging, and satisfying requirements. This enables bottom-up type checking that starts at the leaves of an expression tree. Whenever a traditional type checker would look up variable types in the typing context, the bottom-up co-contextual type checker generates fresh type variables and generates context requirements stating that these type variables need to be bound to actual types; it merges and satisfies these requirements as it visits the syntax tree upwards to the root. The co-contextual type formulation of PCF enables incremental type checking giving rise to order-of-magnitude speedups [6].

These results motivated us to investigate co-contextual formulation of the type systems for statically typed object-oriented (OO) languages, the state-of-the-art programming technology for large-scale systems. We use Featherweight Java [8] (FJ) as a representative calculus for



© Edlira Kuci, Sebastian Erdweg, Oliver Bračevac, Andi Bejleri, and Mira Mezini;
licensed under Creative Commons License CC-BY

XX:2 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

```
new List().add(1).size() + new LinkedList().add(2).size();
```

$$\begin{array}{ll} (R_1) \text{ List.init()} & (R_4) \text{ LinkedList.init()} \\ (R_2) \text{ List.add : Int} \rightarrow U_1 & (R_5) \text{ LinkedList.add : Int} \rightarrow U_2 \\ (R_3) \text{ } U_1.\text{size} : () \rightarrow U_3 & (R_6) \text{ } U_2.\text{size} : () \rightarrow U_4 \end{array}$$

Figure 1 Requirements generated from co-contextually type checking the `+` expression.

these languages. Specifically, we consider two research questions: (a) Can we formulate an equivalent co-contextual type system for FJ by duality to the traditional formulation, and (b) if yes, how to define an incremental type checker based on it with significant speedups? Addressing these questions is an important step towards a general theory of incremental type checkers for statically typed OO languages, such as Java, C#, or Eiffel.

We observe that the general principle of replacing the typing context and its operations with co-contextual duals carries over to the *class table*. The latter is propagated top-down and completely specifies the available classes in the program, e.g., member signatures and super classes. Dually, a co-contextual type checker propagates *class table requirements* bottom-up. This data structure specifies requirements on classes and members and accompanying operations for generating, merging, and removing these requirements.

However, defining appropriate merge and remove operations on co-contextual class table requirements poses significant challenges, as they substantially differ from the equivalent operations on context requirements. Unlike the global namespace and structural typing of PCF, FJ features context dependent member signatures (subtype polymorphism), a declared type hierarchy (nominal typing), and inherited definitions (implementation inheritance).

For an intuition of class table requirements and the specific challenges concerning their operations, consider the example in Figure 1. Type checking the operands of `+` yields the class table requirements R_1 to R_6 . Here and throughout the paper we use metavariable U to denote unification variables as placeholders for actual types. For example, the invocation of method `add` on `new List()` yields a class table requirement R_2 . The goal of co-contextual type checking is to avoid using any context information, hence we cannot look up the signature of `List.add` in the class table. Instead, we use a placeholder U_1 until we discover the definition of `List.add` later on. As consequence, we lack knowledge about the receiver type of any subsequent method call, such as `size` in our example. This leads to requirement R_3 , which states that (yet unknown) class U_1 should exist that has a method `size` with no arguments and (yet unknown) return type U_3 . Assuming `+` operates on integers, type checking the `+` operator later unifies U_3 and U_4 with `Int`, thus refining the class table requirements.

To illustrate issues with merging requirements, consider the requirements R_3 and R_6 regarding `size`. Due to nominal typing, the signature of this method depends on U_1 and U_2 , where it is yet unknown how these classes are related to each other. It might be that U_1 and U_2 refer to the same class, which implies that these two requirements overlap and the corresponding types of `size` in R_3 and R_6 are unified. Alternatively, it might be the case that U_1 and U_2 are distinct classes, individually declaring a method `size`. Unifying the types of `size` from R_3 and R_6 would be wrong. Therefore, it is locally indeterminate whether a merge should unify or keep the requirements separate.

To illustrate issues with removing class requirements, consider the requirement R_5 . Suppose that we encounter a declaration of `add` in `LinkedList`. Just removing R_5 is not sufficient because we do not know whether `LinkedList` overrides `add` of a yet unknown superclass U , or not. Again, the situation is locally indeterminate. In case of overriding,

$L ::= \text{class } C \text{ extends } D \{ \overline{C} \overline{f}; K \overline{M} \}$	class declaration
$K ::= C(\overline{C} \overline{f})\{\text{super}(\overline{f}); \text{this.}\overline{f} = \overline{f}\}$	constructor
$M ::= C m(\overline{C} \overline{x})\{ \text{return } e; \}$	method declaration
$e ::= x \text{this} e.f e.m(\overline{e}) \text{new } C(\overline{e}) (C)e$	expression
$\Gamma ::= \emptyset \Gamma; x : C \Gamma; \text{this} : C$	typing contexts

■ **Figure 2** Featherweight Java syntax and typing context.

FJ requires that the signatures of overriding and overridden methods be identical. Hence, it would necessary add constraints equating the two signatures. However, it is equally possible that `LinkedList.add` overrides nothing, so that no additional constraints are necessary. If, however, `LinkedList` inherits `add` from `List` without overriding it, we need to record the inheritance relation between these two classes, in order to be able to replace U_2 with the actual return type of `size`.

The example illustrates that a co-contextual formulation for nominal typing with subtype polymorphism and implementation inheritance poses new research questions that the work on co-contextual PCF did not address. A key contribution of the work presented in this paper is to answer these questions. The other key contribution is an incremental type checker for FJ based on the co-contextual FJ formulation. We evaluate the initial and incremental performance of the co-contextual FJ type checker on synthesized FJ programs and realistic java programs by comparison to javac and a context-based implementation of FJ.

To summarize, the paper makes the following contributions:

- We present a co-contextual formulation of FJ’s type system by duality to the traditional type system formulation by Igarashi et al. [8]. Our formulation replaces the class table by its dual concept of class table requirements and it replaces field/method lookup, class table duplication, and class table extension by the dual operations of requirement generation, merging, and removing. In particular, defining the semantics of merging and removing class table requirements in the presence of nominal types, OO subtype polymorphism, and implementation inheritance constitute a key contribution of this work.
- We present a method to derive co-contextual typing rules for FJ from traditional ones and provide a proof of equivalence between contextual and co-contextual FJ.
- We provide a description of type checker optimizations for co-contextual FJ with incrementalization and a performance evaluation.

2 Background and Motivation

In this section, we present the FJ typing rules from [8] and give an example to illustrate how contextual and co-contextual FJ type checkers work.

2.1 Featherweight Java: Syntax and Typing Rules

Featherweight Java [8] is a minimal core language for modeling Java’s type system. Figure 2 shows the syntax of classes, constructors, methods, expressions, and typing contexts. Metavariables C , D , and E denote class names and types; f denotes fields; m denotes method names; `this` denotes the reference to the current object. As is customary, an overline denotes a sequence in the metalanguage. Γ is a set of bindings from variables and `this` to types.

The type system (Figure 3) ensures that variables, field access, method invocation, constructor calls, casting, and method and class declarations are well-typed. The typing

XX:4 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

$$\begin{array}{c}
\text{T-VAR} \frac{\Gamma(x) = C}{\Gamma; CT \vdash x : C} \quad \text{T-FIELD} \frac{\Gamma; CT \vdash e : C_e \quad \text{field}(f_i, C_e, CT) = C_i}{\Gamma; CT \vdash e.f_i : C_i} \\
\\
\text{T-INVK} \frac{\Gamma; CT \vdash e : C_e \quad \Gamma; CT \vdash \bar{e} : \bar{C} \quad \text{mtype}(m, C_e, CT) = \bar{D} \rightarrow C \quad \bar{C} <: \bar{D}}{\Gamma; CT \vdash e.m(\bar{e}) : C} \\
\\
\text{T-NEW} \frac{\Gamma; CT \vdash \bar{e} : \bar{C} \quad \text{fields}(C, CT) = C.\text{init}(\bar{D}) \quad \bar{C} <: \bar{D}}{\Gamma; CT \vdash \mathbf{new} C(\bar{e}) : C} \\
\\
\text{T-UCAST} \frac{\Gamma; CT \vdash e : D \quad D <: C}{\Gamma; CT \vdash (C)e : C} \quad \text{T-DCAST} \frac{\Gamma; CT \vdash e : D \quad C <: D \quad C \neq D}{\Gamma; CT \vdash (C)e : C} \\
\\
\text{T-SCAST} \frac{\Gamma; CT \vdash e : D \quad C \not<: D \quad D \not<: C}{\Gamma; CT \vdash (C)e : C} \\
\\
\text{T-METHOD} \frac{\begin{array}{c} \bar{x} : \bar{C}; \mathbf{this} : C; CT \vdash e : E_0 \quad E_0 <: C_0 \\ \text{extends}(C, CT) = D \end{array} \quad \text{if } \text{mtype}(m, D, CT) = \bar{D} \rightarrow D_0, \text{then } \bar{C} = \bar{D}; C_0 = D_0}{C; CT \vdash C m(\bar{C} \bar{x})\{\text{return } e\} \text{ OK}} \\
\\
\text{T-CLASS} \frac{\begin{array}{c} K = C(\bar{D}' \bar{g}, \bar{C}' \bar{f})\{\mathbf{super}(\bar{g}); \mathbf{this}.\bar{f} = \bar{f}\} \quad \text{fields}(D, CT) = D.\text{init}(\bar{D}') \\ C; CT \vdash \bar{M} \text{ OK} \end{array}}{CT \vdash \mathbf{class} C \text{ extends } D \{\bar{C} \bar{f}; K \bar{M}\} \text{ OK}} \\
\\
\text{T-PROGRAM} \frac{CT = \bigcup_{L' \in \bar{L}} (\text{addExt}(L') \cup \text{addCtor}(L') \cup \text{addFs}(L') \cup \text{addMs}(L')) \quad (CT \vdash L' \text{ OK})_{L' \in \bar{L}}}{\bar{L} \text{ OK}}
\end{array}$$

 **Figure 3** Typing rules of Featherweight Java.

judgment for expressions has the form $\Gamma; CT \vdash e : C$, where Γ denotes the typing context, CT the class table, e the expression under analysis, and C the type of e . The typing judgment for methods has the form $C; CT \vdash M \text{ OK}$ and for classes $CT \vdash L \text{ OK}$.

In contrast to the FJ paper [8], we added some cosmetic changes to the presentation. For example, the class table CT is an implicit global definition in FJ. Our presentation explicitly propagates CT top-down along with the typing context. Another difference to Igarashi et al. is in the rule T-NEW: Looking up all fields of a class returns a constructor signature, i.e., $\text{fields}(C, CT) = C.\text{init}(\bar{D})$ instead of returning a list of fields with their corresponding types. We made this subtle change because it clearer communicates the intention of checking the constructor arguments against the declared parameter types. Later on, these changes pay off, because they enable a systematic translation of typing rules to co-contextual FJ (Sections 3 and 4) and give a strong and rigorous equivalence result for the two type systems (Section 5).

Furthermore, we explicitly include a typing rule T-PROGRAM for programs, which is implicit in Igarashi et al.'s presentation. The typing judgment for programs has the form $\bar{L} \text{ OK}$: A program is well-typed if all class declarations are well-typed. The auxiliary functions addExt, addCtor, addFs, and addMs extract the supertype, constructor, field and method declarations from a class declaration into entries for the class table. Initially, the class table

is empty, then it is gradually extended with information from every class declaration by using the above-mentioned auxiliary functions. This is to emphasize that we view the class table as an additional form of typing context, having its own set of extension operations. We describe the class table extension operations and their co-contextual duals formally in Section 3.

2.2 Contextual and Co-Contextual Featherweight Java by Example

We revisit the example from the introduction to illustrate that, in absence of context information, maintaining requirements on class members is non-trivial:

`new List().add(1).size() + new LinkedList().add(2).size()`

```
class List extends Object {
    Int size() {...}
    List add(Int a){...}
}
class LinkedList extends List { }
```

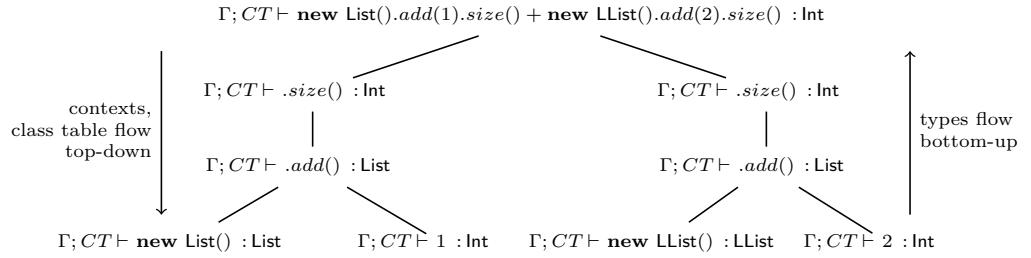
Here we assume the class declarations on the right-hand side: `List` with methods `add()` and `size()` and `LinkedList` inheriting from `List`. As before, we assume there are typing rules for numeric `Int` literals and the `+` operator over `Int` values. We use `LList` instead of `LinkedList` in Figure 4 for space reasons.

Figure 4 (a) depicts standard type checking with typing contexts in FJ. The type checker in FJ visits the syntax tree “down-up”, starting at the root. Its inputs (propagated downwards) are the context Γ , class table CT , and the current subexpression e . Its output (propagated upwards) is the type C of the current subexpression. The output is computed according to the currently applicable typing rule, which is determined by the shape of the current subexpression. The class table used by the standard type checker contains classes `List` and `LinkedList` shown above. The type checker retrieves the signatures for the method invocations of `add` and `size` from the class table CT .

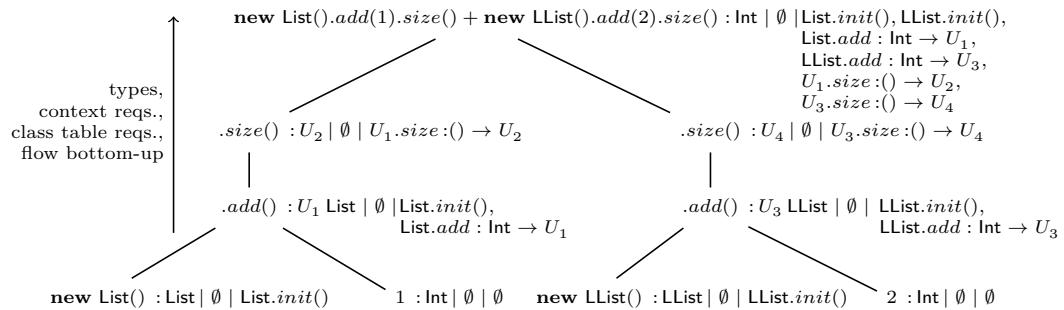
To recap, while type checking constructor calls, method invocations, and field accesses the context and the class table flow top-down; types of fields/methods are looked up in the class table. Figure 4 (b) depicts type checking of the same expression in co-contextual FJ. Here, the type checker starts at the leaves of the tree with no information about the context or the class table. The expression type T , the context requirements R , and class table requirements CR all are outputs and only the current expression e is input to the type checker, making the type checker context-independent. At the leaves, we do not know the signature of the constructors of `List` and `LinkedList`. Therefore, we generate requirements for the constructor calls `List.init()` and `LinkedList.init()` and propagate them as class table requirements. For each method invocation of `add` and `size` in the tree, we generate requirements on the receiver type and propagate them together with the requirements of the subexpressions.

In addition to generating requirements and propagating them upwards as shown in Figure 4 (b), a co-contextual type checker also *merges requirements* when they have compatible receiver types. In our example, we have two requirements for method `add` and two requirements for method `size`. The requirements for method `add` have incompatible ground receiver types and therefore cannot be merged. The requirements for method `size` both have placeholder receivers and therefore cannot be merged just yet. However, for the `size` requirements, we can already extract a conditional constraint that must hold if the requirements become mergeable, namely ($U_2 = U_4$ if $U_1 = U_3$). This constraint ensures the signatures of both `size` invocations are equal in case their receiver types U_1 and U_3 are equal. This way, we enable early error detection and incremental solving of constraints. Constraints can be solved continuously as soon as they have been generated in order to not wait for the whole program to be type checked. We discuss incremental type checking in more detail in Section 6.

XX:6 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)



(a) Contextual type checking propagates contexts and class tables top-down.



(b) Co-contextual type checking propagates context and class table requirements bottom-up.

Figure 4 Contextual and co-contextual type checking.

After type checking the `+` operator, the type checker encounters the class declarations of `List` and `LinkedList`. When type checking the class header `LinkedList extends List`, we have to record the inheritance relation between the two classes because methods can be invoked by `LinkedList`, but declared in `List`. For example, if `List` is not known to be a superclass of `LinkedList` and given the declaration `List.add`, then we cannot just yet satisfy the requirement `LinkedList.add : Num → U3`. Therefore, we duplicate the requirement regarding `add` having as receiver `List`, i.e., `List.add : Num → U3`. By doing so, we can deduce the actual type of `U3` for the given declaration of `add` in `List`. Also, requirements regarding `size` are duplicated.

In the next step, the method declaration of `size` in `List` is type checked. Hence, we consider all requirements regarding `size`, i.e., `U1.size : () → U2` and `U3.size : () → U4`. The receivers of `mathit{size}` in both requirements are unknown. We cannot yet satisfy these requirements because we do not know whether `U1` and `U3` are equal to `List`, or not. To solve this, we introduce conditions as part of the requirements, to keep track of the relations between the unknown required classes and the declared ones. By doing so, we can deduce the actual types of `U2` and `U4`, and satisfy the requirements later, when we have more information about `U1` and `U3`.

Next, we encounter the method declaration `add` and satisfy the corresponding requirements. After satisfying the requirements regarding `add`, the type checker can infer the actual types of `U1` and `U3`. Therefore, we can also satisfy the requirements regarding `size`.

To summarize, during the co-contextual type checking of constructor calls, method invocations, and field accesses, the requirements flow bottom-up. Instead of looking up types of fields/methods in the class table, we introduce new class table requirements. These requirements are satisfied when the actual types of fields/methods become available.

3 Co-Contextual Structures for Featherweight Java

In this section, we present the dual structures and operations for the co-contextual formulation of FJ’s type system. Specifically, we introduce bottom-up propagated *context and class table requirements*, replacing top-down propagated typing contexts and class tables.

3.1 Class Variables and Constraints

For co-contextual FJ, we reuse the syntax of FJ in Figure 2, but extend the type language to *class types*:

$$\begin{array}{ll} U, V, \dots & \text{Class Variable} \\ T ::= C \mid U & \text{Class Type} \end{array}$$

We use constraints for refining class types, i.e., co-contextual FJ is a constraint-based type system. That is, next to class names, the type system may assign *class variables*, designating unknowns in constraints. We further assume that there are countably many class variables, equality of class variables is decidable and that class variables and class names are disjoint.

During bottom-up checking, we propagate sets S of constraints:

$$\begin{array}{ll} s ::= T = T \mid T \neq T \mid T <: T \mid T \not< T \mid T = T \text{ if } cond & \text{constraint} \\ S ::= \emptyset \mid S; s & \text{constraint set} \end{array}$$

A constraint s either states that two class types must be equal, non-equal, in a subtype relation, non-subtype, or equal if some condition holds, which we leave underspecified for the moment.

3.2 Context Requirements

A typing context is a set of bindings from variables to types, while a context requirement is a set of bindings from variables to class variables U . Below we show the operations on typing contexts and their co-contextual correspondences, reproduced from [6]. Operations on typing context are lookup, extension, and duplication; their respective requirement context duals are: generating, removing, and merging. Co-contextual FJ adopts context requirements and operations for method parameters and **this** unchanged.

Contextual	Co-contextual
Context syntax $\Gamma ::= \emptyset \mid \Gamma; x:T$	Requirements $R \subset x \times T$ map variables to their types
Context lookup $\Gamma(x) = T$	Requirement introduction $R = \{x:U\}$ with fresh unification variable U
Context extension $\Gamma; x:T$	Requirement satisfaction $R - x$ if $(R(x) = T)$ holds
Context duplication $\Gamma \rightarrow (\Gamma, \Gamma)$	Requirement merging $merge_R(R_1, R_2) = R _S$ if all constraints $(T_1 = T_2) \in S$ hold
Context is empty $\Gamma = \emptyset$	No unsatisfied requirements $R \stackrel{!}{=} \emptyset$

3.3 Structure of Class Tables and Class Table Requirements

In the following, we describe the dual notion of a class table, called *class table requirements* and their operations. We first recapitulate the structure of FJ class tables [8], then stipulate the structure of class table requirements. Figure 5 shows the syntax of both. A class table

Contextual	Co-Contextual
$CT ::= \emptyset$	class table
$CTcls \cup CT$	$(CReq, cond) \cup CR$
$CTcls ::=$	$CReq ::=$
$C \text{ extends } D$	extends clause
$C.\text{init}(\bar{C})$	ctor clause
$C.f : C'$	field clause
$C.m : \bar{C} \rightarrow C'$	method clause
	$T .\text{extends}: T'$
	$T.\text{init}(\bar{T})$
	$T.f : T'$
	$T.m : \bar{T} \rightarrow T'$
	$(T.m : \bar{T} \rightarrow T')_{opt}$
	$cond ::= \emptyset \mid T = T'; cond$
	$ T \neq T'; cond$

■ **Figure 5** Class Table and Class Table Requirements Syntax.

is a collection of class definition clauses $CTcls$ defining the available classes.¹ A clause is a class name C followed by either the superclass, the signature of the constructor, a field type, or a method signature of C 's definition.

As Figure 5 suggests, class tables and definition clauses in FJ have a counterpart in co-contextual FJ. Class tables become *class table requirements* CR , which are collections of pairs $(CReq, cond)$, where $CReq$ is a *class requirement* and $cond$ is its *condition*. Each class definition clause has a corresponding class requirement $CReq$, which is one of the following:

- A *inheritance requirement* $T .\text{extends}: T'$, i.e., class type T must inherit from T' .
- A *constructor requirement* $T.\text{init}(\bar{T})$, i.e., class type T 's constructor signature must match \bar{T} .
- A *field requirement* $T.f : T'$, i.e., class T (or one of its *supertypes*) must declare field f with class type T' .
- A *method requirement* $T.m : \bar{T}' \rightarrow T''$, i.e., class T (or one of its *supertypes*) must declare method m matching signature $\bar{T}' \rightarrow T''$.
- An *optional method requirement* $(T.m : \bar{T}' \rightarrow T'')_{opt}$, i.e., if the class type T declares the method m , then its signature must match $\bar{T}' \rightarrow T''$. While type checking method declarations, this requirement is used to ensure that method overrides in subclasses are well-defined. An optional method requirement is used as a counterpart of the conditional method lookup in rule T-METHOD of standard FJ, i.e., if $\text{mtype}(m, D, CT) = \bar{D} \rightarrow D_0$, then $\bar{C} = \bar{D}$; $C_0 = D_0$, where D is the superclass of the class C , in which the method declaration m under scrutiny is type checked, and \bar{C} , C_0 are the parameter and returned types of m as part of C .

A condition $cond$ is a conjunction of equality and nonequality constraints on class types. Intuitively, $(CReq, cond)$ states that if the condition $cond$ is satisfied, then the requirement $CReq$ must be satisfied, too. Otherwise, we have unsolvable constraints, indicating a typing error. With conditional requirements and constraints, we address the feature of nominal typing and inheritance for co-contextual FJ. In the following, we will describe their usage.

¹ To make the correspondence to class table requirements more obvious, we show a decomposed form of class tables. The original FJ formulation [8] groups clauses by the containing class declaration.

Contextual	Co-contextual
Field name lookup $\text{field}(f_i, C, CT) = C_i$	Class requirement for field $(C.f_i : U, \emptyset)$
Fields lookup $\text{fields}(C, CT) = C.\text{init}(\bar{C})$	Class requirement for constructor $(C.\text{init}(\bar{U}), \emptyset)$
Method lookup $\text{mtype}(m, C, CT) = \bar{C} \rightarrow C$	Class requirement for method $(C.m : \bar{U} \rightarrow U, \emptyset)$
Conditional method override $\text{if } \text{mtype}(m, C, CT) = \bar{C} \rightarrow C$	Optional class requirement for method $(C.m : \bar{U} \rightarrow U, \emptyset)_{opt}$
Super class lookup $\text{extends}(C, CT) = D$	Class requirement for super class $(C.\text{extends}: U, \emptyset)$
Class table duplication $CT \rightarrow (CT, CT)$	Class requirement merging $\text{merge}_{CR}(CR_1, CR_2) = CR _S$ if all constraints in S hold

Figure 6 Operations on class table and their co-contextual correspondence.

3.4 Operations on Class Tables and Requirements

In this section, we describe the co-contextual dual to FJ’s class table operations as outlined in Figure 6. We first consider FJ’s lookup operations on class tables, which appear in premises of typing rules shown in Figure 3 to look up (1) fields, (2) field lists, (3) methods and (4) superclass lookup. The dual operation is to introduce a corresponding class requirement for the field, list of fields, method, or superclass.

Let us consider closely field lookup, i.e., $\text{field}(f_i, C, CT) = C_i$, meaning that class C in the class table CT has as member a field f_i of type C_i . We translate it to the dual operation of introducing a new class requirement $(C.f_i : U, \emptyset)$. Since we do not have any information about the type of the field, we choose a *fresh* class variable U as type of field f_i . At the time of introducing a new requirement, its condition is empty.

Consider the next operation $\text{fields}(C, CT)$, which looks up all field members of a class. This lookup is used in the constructor call rule T-NEW; the intention is to retrieve the *constructor signature* in order to type check the subtyping relation between this signature and the types of expressions as parameters of the *constructor call*, i.e., $\bar{C} <: \bar{D}$ (rule T-NEW). As we can observe, the field names are not needed in this rule, only their types. Hence, in contrast to the original FJ rule [8], we deduce the constructor signature from fields lookup, rather than field names and their corresponding types, i.e., $\text{fields}(C, CT) = C.\text{init}(\bar{D})$. The dual operation on class requirements is to add a new class requirement for the constructor, i.e., $(C.\text{init}(\bar{U}), \emptyset)$. Analogously, the class table operations for method signature lookup and super class lookup map to corresponding class table requirements.

Finally, standard FJ uses class table duplication to forward the class table to all parts of an FJ program, thus ensuring all parts are checked against the same context. The dual co-contextual operation, merge_{CR} , merges class table requirements originating from different parts of the program. Importantly, requirements merging needs to assure all parts of the program require compatible inheritance, constructors, fields, and methods for any given class. To merge two sets of requirements, we first identify the field and method names used in both sets and then compare the classes they belong to. The result of merging two sets of class requirements CR_1 and CR_2 is a new set CR of class requirements and a set of constraints, which ensure compatibility between the two original sets of overlapping requirements. Non-overlapping requirements get propagated unchanged to CR whereas

$$\begin{aligned}
CR_m = & \{(T_1.m : \overline{T_1} \rightarrow T'_1, cond_1 \cup (T_1 \neq T_2)) \\
& \cup (T_2.m : \overline{T_2} \rightarrow T'_2, cond_2 \cup (T_1 \neq T_2)) \\
& \cup (T_1.m : \overline{T_1} \rightarrow T'_1, cond_1 \cup cond_2 \cup (T_1 = T_2)) \\
& | (T_1.m : \overline{T_1} \rightarrow T'_1, cond_1) \in CR_1 \wedge (T_2.m : \overline{T_2} \rightarrow T'_2, cond_2) \in CR_2\} \\
\\
S_m = & \{(T'_1 = T'_2 \text{ if } T_1 = T_2) \cup (\overline{T_1 = T_2} \text{ if } T_1 = T_2) \\
& | (T_1.m : \overline{T_1} \rightarrow T'_1, cond_1) \in CR_1 \wedge (T_2.m : \overline{T_2} \rightarrow T'_2, cond_2) \in CR_2\}
\end{aligned}$$

■ **Figure 7** Merge operation of method requirements CR_1 and CR_2 .

potentially overlapping requirements receive special treatment depending on the requirement kind.

The full merge definition appears in Appendix A; Figure 7 shows the merge operation for overlapping method requirements, which results in a new set of requirements CR_m and constraints S_m . To compute CR_m , we identify method requirements on the equally-named methods m in both sets and distinguish two cases. First, if the receivers are different $T_1 \neq T_2$, then the requirements are not actually overlapping. We retain the two requirements unchanged, except that we remember the failed condition for future reference. Second, if the receivers are equal $T_1 = T_2$, then the requirements are actually overlapping. We merge them into a single requirement and produce corresponding constraints in S_m . One of the key benefits of keeping track of conditions in class table requirements is that often these conditions allow us to discharge requirements early on when their conditions are unsatisfiable. In particular, in Section 6 we describe a compact representation of conditional requirements that facilitates early pruning and is paramount for good performance. However, the main reason for conditional class table requirements is their removal, which we discuss subsequently.

3.5 Class Table Construction and Requirements Removal

Our formulation of the contextual FJ type system differs in the presentation of the class table compared to the original paper [8]. Whereas Igarashi et al. assume that the class table is a pre-defined static structure, we explicitly consider its formation through a sequence of operations. The class table is initially empty and gradually extended with class table clauses $CTcls$ for each class declaration L of a program. Dual to that, class table requirements are initially unsatisfied and gradually removed. We define an operation for *adding* clauses to the class table and a corresponding co-contextual dual operation on class table requirements for *removing* requirements. Figure 8 shows a collection of adding and removing operations for every possible kind of class table clause $CTcls$.

In general, clauses are added to the class table starting from superclass to subclass declarations. For a given class, the class header with **extends** is added before the other clauses. Dually, we start removing requirements that correspond to clauses of a subclass, followed by those corresponding to clauses of superclass declarations. For a given class, we first remove requirements corresponding to method, fields, or constructor clauses, then those corresponding to the class header **extends** clause. Note that our sequencing still allows for mutual class dependencies. For example, the following is a valid sequence of clauses where A depends on B and vice versa:

Contextual	Co-contextual
Class table empty $CT = \emptyset$	Unsatisfied class requirements CR
Adding extend $\text{addExt}(L, CT)$	Remove extend $\text{removeExt}(L, CR)$
Adding constructor $\text{addCtor}(L, CT)$	Remove constructor $\text{removeCtor}(L, CR)$
Adding fields $\text{addFs}(L, CT)$	Remove fields $\text{removeFs}(L, CR)$
Adding methods $\text{addMs}(L, CT)$	Remove methods $\text{removeMs}(L, CR)$

■ **Figure 8** Constructing class table and their co-contextual correspondence.

$$\begin{aligned} \text{addMs}(C, \overline{M}, CT) &= \overline{C.m : \overline{C} \rightarrow C'} \cup CT \\ \text{removeM}(C, C' m(\overline{C} \bar{x}) \{\text{return } e\}, CR) &= CR'|_S \\ \text{where } CR' &= \{(T.m : \overline{T} \rightarrow T', \text{cond} \cup (T \neq C)) \mid (T.m : \overline{T} \rightarrow T', \text{cond}) \in CR\} \\ &\quad \cup (CR \setminus \{(T.m : \overline{T} \rightarrow T', \text{cond})\}) \\ S &= \{(T' = C' \text{ if } T = C) \cup (\overline{T = C} \text{ if } T = C) \mid (T.m : \overline{T} \rightarrow T', \text{cond}) \in CR\} \\ \text{removeMs}(C, \overline{M}, CR) &= CR'|_S \\ \text{where } CR' &= \{CR_m \mid (C' m(\overline{C} \bar{x}) \{\text{return } e\}) \in \overline{M} \\ &\quad \wedge \text{removeM}(C, C' m(\overline{C} \bar{e}) \{\text{return } e\}, CR) = CR_m|_{S_m}\} \\ S &= \{S_m \mid (C' m(\overline{C} \bar{x}) \{\text{return } e\}) \in \overline{M} \\ &\quad \wedge \text{removeM}(C, C' m(\overline{C} \bar{x}) \{\text{return } e\}, CR) = CR_m|_{S_m}\} \end{aligned}$$

$$\begin{aligned} \text{addExt(class } C \text{ extends } D, CT) &= (C \text{ extends } D) \cup CT \\ \text{removeExt(class } C \text{ extends } D, CR) &= CR'|_S \\ \text{where } CR' &= \{(T.\text{extends} : T', \text{cond} \cup (T \neq C)) \mid (T.\text{extends} : T', \text{cond}) \in CR\} \\ &\quad \cup \{(T.m : \overline{T} \rightarrow T', \text{cond} \cup (T \neq C)) \\ &\quad \quad \cup (D.m : \overline{T} \rightarrow T', \text{cond} \cup (T = C)) \mid (T.m : \overline{T} \rightarrow T', \text{cond}) \in CR\} \\ &\quad \cup \{(T.m : \overline{T} \rightarrow T', \text{cond} \cup (T \neq C))_{opt} \\ &\quad \quad \cup (D.m : \overline{T} \rightarrow T', \text{cond} \cup (T = C))_{opt} \\ &\quad \quad \mid (T.m : \overline{T} \rightarrow T', \text{cond})_{opt} \in CR\} \\ &\quad \cup \{(T.f : T', \text{cond} \cup (T \neq C)) \cup (D.f : T', \text{cond} \cup (T = C)) \\ &\quad \quad \mid (T.f : T', \text{cond}) \in CR\} \\ S &= \{(T' = D \text{ if } T = C) \mid (T.\text{extends} : T', \text{cond}) \in CR\} \end{aligned}$$

■ **Figure 9** Add and remove operations of method and extends clauses.

```
class A extends Object; class B extends Object; A.m: () → B; B.m: () → A.
```

The full definition of the addition and removal operations for all cases of clause definition appears in Appendix A; Figure 9 presents the definitions of adding and removing method and **extends** clauses.

Remove operations for method clauses. The function removeMs removes a list of methods by applying the function removeM to each of them. removeM removes a single

XX:12 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

method declaration defined in class C . To this end, removeM identifies requirements on the same method name m and refines their receiver to be different from the removed declaration's defining class. That is, the refined requirement $(T.m : \dots, \text{cond} \cup (T \neq C))$ only requires method m if the receiver T is different from the defining class C . If the receiver T is, in fact, equal to C , then the condition of the refined requirement is unsatisfiable and can be discharged. To ensure the required type also matches the declared type, removeM also generates conditional constraints in case $T = C$. Note that whether $T = C$ can often not be determined immediately because T may be a placeholder type U .

We illustrate the removal of methods using the class declaration of `List` shown in Section 2.2. Consider the class requirement set $CR = (U_1.\text{size}() \rightarrow U_2, \emptyset)$. Encountering the declaration of method `add` has no effect on this set because there is no requirement on `add`. However, when encountering the declaration of method `size`, we refine the set as follows:

$$\text{removeM}(\text{List}, \text{Int } \text{size}() \{ \dots \}, CR) = \{(U_1.\text{size} : () \rightarrow U_2, U_1 \neq \text{List})\}|_S$$

with a new constraint $S = \{U_2 = \text{Int if } U_1 = \text{List}\}$. Thus, we have satisfied the requirement in CR for $U_1 = \text{List}$, only leaving the requirement in case U_1 represents another type. In particular, if we learn at some point that U_1 indeed represents `List`, we can discharge the requirement because its condition is unsatisfiable. This is important because a program is only closed and well-typed if its requirement set is empty.

Remove operations for extends clauses. The function removeExt removes the `extends` clauses (C . `extends` D). This function, in addition to identifying the requirements regarding `extends` and following the same steps as above for removeM , duplicates all requirements for fields and methods. The duplicate introduces a requirement the same as the existing one, but with a different receiver, which is the superclass D that potentially declares the required fields and methods. The conditions also change. We add to the existing requirements an inequality condition $(T \neq C)$, to encounter the case when the receiver T is actually replaced by C , but it is required to have a certain field or method, which is declared in D , the superclass of T . This requirement should be discharged because we know the actual type of the required field or method, which is inherited from the given declaration in D . Also, we add an equality condition to the duplicate requirement $T = C$, because this requirement will be discharged when we encounter the actual declarations of fields or methods in the superclass.

We illustrate the removal of `extends` using the class declaration `LinkedList extends List`. Consider the requirement set $CR = (U_3.\text{size} : () \rightarrow U_4, \emptyset)$. We encounter the declaration for `LinkedList` and the requirement set changes as follows:

$$\begin{aligned} \text{removeExt}(\text{class } \text{LinkedList } \text{extends } \text{List}, CR) = \\ \{(U_3.\text{size} : () \rightarrow U_4, U_3 \neq \text{LinkedList}), (\text{List.size} : () \rightarrow U_4, U_3 = \text{LinkedList})\}|_S, \end{aligned}$$

where $S = \emptyset$. S is empty, because there are no requirements on `extends`. If we learn at some point that $U_3 = \text{LinkedList}$, then the requirement $(U_3.\text{size} : () \rightarrow U_4, U_3 \neq \text{LinkedList})$ is discharged because its condition is unsatisfiable. Also, if we learn that `size` is declared in `List`, then $(\text{List.size} : () \rightarrow U_4, U_3 = \text{LinkedList})$ is discharged applying removeM , as shown above, and U_4 can be replaced by its actual type.

Usage and necessity of conditions. As shown throughout this section, conditions play an important role to enable merging and removal of requirements over nominal receiver types and to support inheritance. Because of nominal typing, field and method lookup depends on the name of the defining context and we do not know the actual type of the receiver class when encountering a field or method reference. Thus, it is impossible to deduce their types

until more information is known. Moreover, if a class is required to have fields/methods, which are actually declared in a superclass of the required class, then we need to deduce their actual type/signature and meanwhile fulfill the respective requirements. For example, considering the requirement $U_3.size : () \rightarrow U_4$, if $U_3 = \text{LinkedList}$, `LinkedList` extends `List`, and `size` is declared in `List`, then we have to deduce the actual type of U_4 and satisfy this requirement. To overcome these obstacles we need additional structure to maintain the relations between the required classes and the declared ones, and also to reason about the partial fulfillment of requirements. Conditions come to place as the needed structure to maintain these relations and indicate the fulfillment of requirements.

4 Co-Contextual Featherweight Java Typing Rules

In this section we derive co-contextual FJ's typing rules systematically from FJ's typing rules. The main idea is to transform the rules into a form that eliminates any context dependencies that require top-down propagation of information.

Concretely, context and class table requirements (Section 3) in output positions to the right replace typing contexts and class tables in input positions to the left. Additionally, co-contextual FJ propagates constraint sets S in output positions. Note that the program typing judgment does not change, because programs are closed, requiring neither typing context nor class table inputs. Correspondingly, neither context nor class table requirements need to be propagated as outputs.

Figure 10 shows the co-contextual FJ typing rules (the reader may want to compare against contextual FJ in Figure 3). In what follows, we will discuss the rules for each kind of judgment.

4.1 Expression Typing

Typing rule `TC-VAR` is dual to the standard variable lookup rule `T-VAR`. It marks a distinct occurrence of x (or the self reference `this`) by assigning a fresh class variable U . Furthermore, it introduces a new context requirement $\{x : U\}$, as the dual operation of context lookup for variables x ($\Gamma(x) = C$) in `T-VAR`. Since the latter does not access the class table, dually, `TC-VAR` outputs empty class table requirements.

Typing rule `TC-FIELD` is dual to `T-FIELD` for field accesses. The latter requires a field name lookup (field), which, dually, translates to a new class requirement for the field f_i , i.e., $(T_e.f_i : U, \emptyset)$ (cf. Section 3). Here, T_e is the class type of the receiver e . U is a fresh class variable, marking a distinct occurrence of field name f_i , which is the class type of the entire expression. Furthermore, we merge the new field requirement with the class table requirements CR_e propagated from e . The result of merging is a new set of requirements CR and a new set of constraints S_{cr} . Just as the context Γ is passed into the subexpression e in `T-FIELD`, we propagate the context requirements for e for the entire expression. Finally, we propagate both the constraints S_e for e and the merge constraints S_f as the resulting output constraints.

Typing rule `TC-INVK` is dual to `T-INVK` for method invocations. Similarly to field access, the dual of method lookup is introducing a requirement for the method m and merge it with the requirements from the premises. Again, we choose fresh class variables for the method signature $\bar{U} \rightarrow U'$, marking a distinct occurrence of m . We type check the list \bar{e} of parameters, adding a subtype constraint $\bar{T} <: \bar{U}$, corresponding to the subtype check in `T-INVK`. Finally, we merge all context and class table requirements propagated from the receiver e and the parameters \bar{e} , and all the constraints.

XX:14 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

$$\begin{array}{c}
\text{TC-VAR} \frac{U \text{ is fresh}}{x : U \mid \emptyset \mid x : U \mid \emptyset} \\[10pt]
\text{TC-FIELD} \frac{e : T_e \mid S_e \mid R_e \mid CR_e \quad CR|_{S_f} = \text{merge}_{CR}(CR_e, (T_e.f_i : U, \emptyset)) \quad U \text{ is fresh}}{e.f_i : U \mid S_e \cup S_f \mid R_e \mid CR} \\[10pt]
\text{TC-INVK} \frac{\begin{array}{c} e : T_e \mid S_e \mid R_e \mid CR_e \quad \overline{e : T \mid S \mid R \mid CR} \\ CR_m = (T_e.m : \overline{U} \rightarrow U', \emptyset) \quad S_s = \{T <: U\} \quad U', \overline{U} \text{ are fresh} \\ R'|_{S_r} = \text{merge}_R(R_e, \overline{R}) \quad CR'|_{S_{cr}} = \text{merge}_{CR}(CR_e, CR_m, \overline{CR}) \end{array}}{e.m(\overline{e}) : U' \mid \overline{S} \cup S_e \cup \overline{S_s} \cup S_r \cup S_{cr} \mid R' \mid CR'} \\[10pt]
\text{TC-NEW} \frac{\begin{array}{c} e : T \mid S \mid R \mid CR \\ \overline{U} \text{ is fresh} \quad CR_f = (C.\text{init}(\overline{U}), \emptyset) \quad S_s = \{T <: U\} \\ R'|_{S_r} = \text{merge}_R(\overline{R}) \quad CR'|_{S_{cr}} = \text{merge}_{CR}(CR_f, \overline{CR}) \end{array}}{\text{new } C(\overline{e}) : C \mid \overline{S} \cup \overline{S_s} \cup S_r \cup S_{cr} \mid R' \mid CR'} \\[10pt]
\text{TC-UCAST} \frac{e : T_e \mid S_e \mid R_e \mid CR_e \quad S_s = \{T_e <: C\}}{(C)e : C \mid S_e \cup S_s \mid R_e \mid CR_e} \\[10pt]
\text{TC-DCAST} \frac{e : T_e \mid S_e \mid R_e \mid CR_e \quad S_s = \{C <: T_e\} \quad S_n = \{C \neq T_e\}}{(C)e : C \mid S_e \cup S_s \cup S_n \mid R_e \mid CR_e} \\[10pt]
\text{TC-SCAST} \frac{e : T_e \mid S_e \mid R_e \mid CR_e \quad S_s = \{C \not<: T_e\} \quad S'_s = \{T_e \not<: C\}}{(C)e : C \mid S_e \cup S_s \cup S'_s \mid R_e \mid CR_e} \\[10pt]
\text{TC-METHOD} \frac{\begin{array}{c} e : T_e \mid S_e \mid R_e \mid CR_e \quad \overline{S_x} = \{C = R_e(x) \mid x \in \text{dom}(R_e)\} \\ S_c = \{U_c = R_e(\text{this}) \mid \text{this} \in \text{dom}(R_e)\} \quad S_s = \{T_e <: C_0\} \\ R_e - \text{this} - \overline{x} = \emptyset \quad U_c, U_d \text{ are fresh} \\ CR|_{S_{cr}} = \text{merge}_{CR}(CR_e, (U_c .\text{extends}: U_d, \emptyset), (U_d.m : \overline{C} \rightarrow C_0, \emptyset)_{opt}) \end{array}}{C_0 m(\overline{C} \ \overline{x}) \{\text{return } e\} \text{ OK} \mid S_e \cup S_s \cup S_c \cup S_{cr} \cup \overline{S_x} \mid U_c \mid CR} \\[10pt]
\text{TC-CLASS} \frac{\begin{array}{c} K = C(\overline{D}' \ \overline{g}, \overline{C}' \ \overline{f}) \{\text{super}(\overline{g}); \text{this}.f = \overline{f}\} \quad \overline{M} \text{ OK} \mid S \mid U \mid CR \\ CR'|_{S_{cr}} = \text{merge}_{CR}((D.\text{init}(\overline{D}'), \emptyset), \overline{CR}) \quad \overline{S_{eq}} = \{U = C\} \end{array}}{\text{class } C \text{ extends } D\{\overline{C} \ \overline{f}; \ K \ \overline{M}\} \text{ OK} \mid \overline{S} \cup \overline{S_{eq}} \cup S_{cr} \mid CR'} \\[10pt]
\text{TC-PROGRAM} \frac{\begin{array}{c} L \text{ OK} \mid S \mid CR \quad \text{merge}_{CR}(\overline{CR}) = CR'|_{S'} \\ \uplus_{L' \in \overline{L}} (\text{removeMs}(CR', L') \uplus \text{removeFs}(CR', L') \uplus \text{removeCtor}(CR', L') \\ \uplus \text{removeExt}(CR', L')) = \emptyset|_S \end{array}}{\overline{L} \text{ OK} \mid \overline{S} \cup S' \cup S}
\end{array}$$

 **Figure 10** A co-contextual formulation of the type system of Featherweight Java.

Typing rule TC-NEW is dual to T-NEW for object creation. We add a new class requirement $C.\text{init}(\overline{U})$ for the constructor of class C , corresponding to the *fields* operation in FJ. We cannot look up the fields of C in the class table, therefore we assign fresh class variables \overline{U} for the constructor signature. We add the subtyping constraint $\overline{T} <: \overline{U}$ for the parameters,

analogous to the subtype check in T-NEW. As in the other rules, we propagate a collective merge of the propagated requirement structures/constraints from the subexpressions with the newly created requirements/constraints.

Typing rules for casts, i.e., TC-UCAST, TC-DCAST and TC-SCAST are straightforward adaptions of their contextual counterparts following the same principles. These three type rules do overlap. We do not distinguish them in the formalization, but to have an algorithmic formulation, we implement different node names for each of them. That is, typing rules for casts are syntactically distinguished.

4.2 Method Typing

The typing rule TC-METHOD is dual to T-METHOD for checking method declarations. For checking the method body, the contextual version extends the empty typing context with entries for the method parameters \bar{x} and the self-reference **this**, which is implicitly in scope. Dually, we remove the requirements on the parameters and self-reference in R_e propagated from the method body. Corresponding to extending an empty context, the removal should leave no remaining requirements on the method body. Furthermore, the equality constraints $\overline{S_x}$ ² ensure that the annotated class types for the parameters agree with the class types in R_e .² This corresponds to binding the parameters to the annotated classes in a typing context. Analogously, the constraints S_c deal with the self-reference. For the latter, we need to know the associated class type, which in the absence of the class table is at this point unknown. Hence, we assign a fresh class variable U_c for the yet to be determined class containing the method declaration. The contextual rule T-METHOD further checks if the method declaration correctly overrides another method declaration in the superclass, that is, if it exists in the superclass must have the same type. We choose another fresh class variable U_d for the yet to be determined superclass of U_c and add appropriate supertype and optional method override requirements. We assign to the optional method requirement $U_d.m$ the type of m declared in U_c . If later is known that there exists a declaration for m in the actual type of U_d , the optional requirement is considered and equality constraints are generated. These constraints ensure that the required type of m in the optional requirement is the same as the provided type of m in the actual superclass of U_c . Otherwise this optional method requirement is invalidated and not considered. By doing so, we enable the feature of subtype polymorphism for co-contextual FJ. Finally, we add the subtype constraint ensuring that the method body's type is conforming to the annotated return type.

4.3 Class Typing

Typing rule TC-CLASS is used for checking class declarations. A declaration of a given class C provides definite information on the identity of its superclass D , constructor, fields, and methods signatures. Dual to the fields lookup for superclass D in T-CLASS, we add the constructor requirement $D.\text{init}(\overline{D}')$. We merge this requirement with all requirements generated from type checking C 's method declarations \overline{M} . Recall that typing of method m yields a distinct class variable U for the enclosing class type, because we type check each method declaration independently. Therefore, we add the constraints $\overline{\{U = C\}}$, effectively completing the method declarations with their enclosing class C .

² Note that a parameter x occurs in the method body if and only if there is a requirement for x in R_e (i.e., $x \in \text{dom}(R_e)$), which is due to the bottom-up propagation. The same holds for the self-reference **this**.

4.4 Program Typing

Type rule `TC-PROGRAM` checks a list of class declarations \bar{L} . Class declarations of all classes provide a definite information on the identity of their super classes, constructor, fields, methods signatures. Dual to adding clauses in the class table by constructing it, we remove requirements with respect to the provided information from the declarations. Hence, dually to class table being fully extended with clauses from all class declarations, requirements are empty. The result of removing different clauses is a new set of requirement and a set of constraints. Hence, we use notation \uplus to express the union of the returned tuples (requirements and constraints), i.e., $CR|_S \uplus CR'|_{S'} = CR \cup CR'|_{S \cup S'}$. After applying `remove` to the set of requirements, the set should be empty at this point. A class requirement is discharged from the set, either when performing `remove` operation (Section 3), or when it is satisfied (all conditions hold).

As shown, we can systematically derive co-contextual typing rules for Featherweight Java through duality.

5 Typing Equivalence

In this section, we prove the typing equivalence of expressions, methods, classes, and programs between FJ and co-contextual FJ. That is, (1) we want to convey that an expression, method, class and program is type checked in FJ if and only if it is type checked in co-contextual FJ, and (2) that there is a correspondence relation between typing constructs for each typing judgment.

We use σ to represent substitution, which is a set of bindings from class variables to class types ($\{U \mapsto C\}$). `projExt(CT)` is a function that given a class table CT returns the immediate subclass relation Σ of classes in CT . That is, $\Sigma := \{(C_1, C_2) \mid (C_1 \text{ extends } C_2) \in CT\}$. Given a set of constraints S and a relation between class types Σ , where $\text{projExt}(CT) = \Sigma$, then the solution to that set of constraints is a substitution, i.e., $\text{solve}(S, \Sigma) = \sigma$. Also we assume that every element of the *class table*, i.e., super types, constructors, fields and methods types are class type, namely ground types. Ground types are types that cannot be substituted.

Initially, we prove equivalence for expressions. Let us first delineate the *correspondence relation*. Correspondence states that *a*) the types of expressions are the same in both formulations, *b*) provided variables in context are more than required ones in context requirements and *c*) provided class members are more than required ones. Intuitively, an expression to be well-typed in co-contextual FJ should have all requirements satisfied. Context requirements are satisfied when for all required variables, we find the corresponding bindings in context. Class table requirements are satisfied, when for all valid requirements, i.e., all conditions of a requirement hold, we can find a corresponding declaration in a class of the same type as the required one, or in its superclasses. The relation between class table and class requirements is formally defined in the Appendix B.

► **Definition 1** (Correspondence relation for expressions). Given judgments $\Gamma; CT \vdash e : C$, $e : T \mid S \mid R \mid CR$, and $\text{solve}(\Sigma, S) = \sigma$, where $\text{projExt}(CT) = \Sigma$. The correspondence relation between Γ and R , CT and CR , written $(C, \Gamma, CT) \triangleright \sigma(T, R, CR)$, is defined as:

- a) $C = \sigma(T)$
- b) $\Gamma \supseteq \sigma(R)$
- c) CT satisfies $\sigma(CR)$

We stipulate two different theorems to state both directions of equivalence for expressions.

► **Theorem 2** (Equivalence of expressions: \Rightarrow). Given e, C, Γ, CT , if $\Gamma; CT \vdash e : C$, then there exists $T, S, R, CR, \Sigma, \sigma$, where $\text{projExt}(CT) = \Sigma$ and $\text{solve}(\Sigma, S) = \sigma$, such that $e : T \mid S \mid R \mid CR$ holds, σ is a ground solution and $(C, \Gamma, CT) \triangleright \sigma(T, R, CR)$ holds.

► **Theorem 3** (Equivalence of expressions: \Leftarrow). Given e, T, S, R, CR, Σ , if $e : T \mid S \mid R \mid CR$, $\text{solve}(\Sigma, S) = \sigma$, and σ is a ground solution, then there exists C, Γ, CT , such that $\Gamma; CT \vdash e : C$, $(C, \Gamma, CT) \triangleright \sigma(T, R, CR)$ and $\text{projExt}(CT) = \Sigma$.

Theorems 2 and 3 are proved by induction on the typing judgment of expressions. The most challenging aspect consists in proving the relation between the class table and class table requirements. In Theorem 2, the class table is given and the requirements are a collective merge of the propagated requirement from the subexpressions with the newly created requirements. In Theorem 3, the class table is not given, therefore we construct it through the information retrieved from *ground class requirements*. We ensure class table correctness and completeness with respect to the given requirements. First, we ensure that the class table we construct is correct, i.e., types of **extends**, fields, and methods clauses we add in the class table are equal to the types of the same **extends**, fields, and methods if they already exist in the class table. Second, we ensure that the class table we construct is complete, i.e., the constructed class table satisfies all given requirements.

Next, we present the theorem of equivalence for methods. The difference from expressions is that there is no context, therefore no relation between context and context requirements is required. Instead, the fresh class variable introduced in co-contextual FJ as a placeholder for the actual class, where the method under scrutiny is type checked in, after substitution should be the same as the class where the method is type checked in FJ.

► **Theorem 4** (Equivalence of methods: \Rightarrow). Given m, C, CT , if $C; CT \vdash C_0 m(\bar{C} \bar{x}) \{ \text{return } e \}$ OK, then there exists S, T, CR, Σ, σ , where $\text{projExt}(CT) = \Sigma$ and $\text{solve}(\Sigma, S) = \sigma$, such that

$C_0 m(\bar{C} \bar{x}) \{ \text{return } e_0 \}$ OK $\mid S \mid T \mid CR$ holds, σ is a ground solution and $(C, CT) \triangleright_m \sigma(T, CR)$ holds.

► **Theorem 5** (Equivalence of methods: \Leftarrow). Given m, T, S, CR, Σ , if $C_0 m(\bar{C} \bar{x}) \{ \text{return } e_0 \}$ OK $\mid S \mid T \mid CR$, $\text{solve}(\Sigma, S) = \sigma$, and σ is a ground solution, then there exists C, CT , such that $C; CT \vdash C_0 m(\bar{C} \bar{x}) \{ \text{return } e \}$ OK holds, $(C, CT) \triangleright_m \sigma(T, CR)$ and $\text{projExt}(CT) = \Sigma$.

Theorems 5 and 6 are proved by induction on the typing judgment. The difficulty increases in proving equivalence for methods because we have to consider the optional requirement, as introduced in the previous sections. It requires a different strategy to prove the relation between the class table and optional requirements; we accomplish the proof by using case distinction. We have a detailed proof for method declaration, and also how this affects class table construction, and we prove a correct and complete construction of it.

Lastly, we present the theorem of equivalence for classes and programs.

► **Theorem 6** (Equivalence of classes: \Rightarrow). Given C, CT , if $CT \vdash$ class C extends $D \{ \bar{C} \bar{f}; K \bar{M} \}$ OK, then there exists S, CR, Σ, σ , where $\text{projExt}(CT) = \Sigma$ and $\text{solve}(\Sigma, S) = \sigma$, such that class C extends $D \{ \bar{C} \bar{f}; K \bar{M} \}$ OK $\mid S \mid CR$ holds, σ is a ground solution and $(CT) \triangleright_c \sigma(CR)$ holds.

► **Theorem 7** (Equivalence of classes: \Leftarrow). Given C, CR, Σ , if class C extends $D \{ \bar{C} \bar{f}; K \bar{M} \}$ OK $\mid S \mid CR$, $\text{solve}(\Sigma, S) = \sigma$, and σ is a ground solution, then there exists CT , such that $CT \vdash$ class C extends $D \{ \bar{C} \bar{f}; K \bar{M} \}$ OK holds, $(CT) \triangleright_c \sigma(CR)$ holds and $\text{projExt}(CT) = \Sigma$.

Theorems 8 and 9 are proved by induction on the typing judgment. Class declaration requires to prove only the relation between the class table and class table requirements since there is no context.

Typing rule for programs does not have as inputs context and class table, therefore there is no relation between context, class table and requirements. The equivalence theorem describes that a program in FJ and co-contextual FJ is well-typed.

► **Theorem 8** (Equivalence for programs: \Rightarrow). *Given \bar{L} , if $\bar{L} \text{ OK}$, then there exists S, Σ, σ , where $\text{projExt}(\bar{L}) = \Sigma$ and $\text{solve}(\Sigma, S) = \sigma$, such that $\bar{L} \text{ OK} \mid S$ holds and σ ground solution.*

► **Theorem 9** (Equivalence for programs: \Leftarrow). *Given \bar{L} , if $\bar{L} \text{ OK} \mid S$, $\text{solve}(\Sigma, S) = \sigma$, where $\text{projExt}(\bar{L}) = \Sigma$, and σ is a ground solution, then $\bar{L} \text{ OK}$ holds.*

Theorems 10 and 11 are proved by induction on the typing judgment. In here, we prove that a class table containing all clauses provided from the given class declarations is dual to empty class table requirements in the inductive step.

Omitted definitions, lemmas and proofs can be found at the Appendix B.

6 Efficient Incremental FJ Type Checking

The co-contextual FJ model from Section 3 and 4 was designed such that it closely resembles the formulation of the original FJ type system, where all differences are motivated by dually replacing contextual operations with co-contextual ones. As such, this model served as a good basis for the equivalence proof from the previous section. However, to obtain a type checker implementation for co-contextual FJ that is amenable to efficient incrementalization, we have to employ a number of behavior-preserving optimizations. In the present section, we describe these optimization and the resulting *incremental* type checker implementation for co-contextual FJ. The source code is available online at <https://github.com/seba--/incremental>.

Condition normalization. In our formal model from Section 3 and 4, we represent context requirements as a set of conditional class requirements $CR \subset Creq \times cond$. Throughout type checking, we add new class requirements using function merge, but we only discharge class requirements in rule TC-PROGRAM at the very end of type checking. Since merge generates $3 * m * n$ conditional requirements for inputs with m and n requirements respectively, requirements quickly become intractable even for small programs.

The first optimization we conduct is to eagerly normalize conditions of class requirements. Instead of representing conditions as a list of type equations and inequations, we map receiver types to the following condition representation (shown as Scala code):

```
case class Condition(notGround: Set[CName], notVar: Set[UCName],
                     sameVar: Set[UCName], sameGroundAlternatives: Set[CName]).
```

A condition is true if the receiver type is different from all ground types (CName) and unification variables (UCName) in notGround and notVar, if the receiver type is equal to all unification variables in sameVar, and if sameGroundAlternatives is either empty or the receiver type occurs in it. That is, if sameGroundAlternatives is non-empty, then it stores a set of alternative ground types, one of which the receiver type must be equal to.

When adding an equation or inequation to the condition over a receiver type, we check whether the condition becomes unsatisfiable. For example, when equating the receiver type to the ground type C and notGround.contains(C), we mark the resulting condition to be unsatisfiable. Recognizing unsatisfiable conditions has the immediate benefit of allowing us

to discard the corresponding class requirements right away. Unsatisfiable conditions occur quite frequently because merge generates both equations and inequations for all receiver types that occur in the two merged requirement sets.

If a condition is not unsatisfiable, we normalize it such that the following assertions are satisfied: (i) the receiver type does not occur in any of the sets, (ii) `sameGroundAlternatives.isEmpty` || `notGround.isEmpty`, and (iii) `notVar.intersect(sameVar).isEmpty`. Since normalized conditions are more compact, this optimization saves memory and time required for memory management. Moreover, it makes it easy to identify irrefutable conditions, which is the case exactly when all four sets are empty, meaning that there are no further requisites on the receiver type. Such knowledge is useful when merge generates conditional constraints, because irrefutable conditions can be ignored. Finally, condition normalization is a prerequisite for the subsequent optimization.

In-depth merging of conditional class requirements. In the work on co-contextual PCF [6], the number of requirements of an expression was bound by the number of free variables that occur in that expression. To this end, the merge operation used for co-contextual PCF identifies subexpression requirements on the same free variable and merges them into a single requirement. For example, the expression $x + x$ has only one requirement $\{x : U_1\}|_{\{U_1=U_2\}}$, even though the two subexpressions propagate two requirements $\{x : U_1\}$ and $\{x : U_2\}$, respectively.

Unfortunately, the merge operation of co-contextual FJ given in Section 3.2 does not enjoy this property. Instead of merging requirements, it merely collects them and updates their conditions. A more in-depth merge of requirements is possible whenever two code fragments require the same member from the same receiver type. For example, the expression `this.x + this.x` needs only one requirement $\{U_1.x() : U_2\}|_{\{U_1=U_3, U_2=U_4\}}$, even though the two subexpressions propagate two requirements $\{U_1.x() : U_2\}$ and $\{U_3.x() : U_4\}$, respectively. Note that $U_1 = U_3$ because of the use of `this` in both subexpressions, but $U_2 = U_4$ because of the in-depth merge.

However, conditions complicate the in-depth merging of class requirements: We may only merge two requirements if we can also merge their conditions. That is, for conditional requirements $(creq_1, cond_1)$ and $(creq_2, cond_2)$ with the same receiver type, the merged requirement must have the condition $cond_1 \vee cond_2$. In general, we cannot express $cond_1 \vee cond_2$ using our Condition representation from above because all fields except `sameGroundAlternatives` represent conjunctive prerequisites, whereas `sameGroundAlternatives` represents disjunctive prerequisites. Therefore, we only support in-depth merging when the conditions are identical up to `sameGroundAlternatives` and we use the union operator to combine their `sameGroundAlternatives` fields.

This optimization may seem a bit overly specific to certain use cases, but it turns out it is generally applicable. The reason is that function `removeExt` creates requirements of the form $(D.f : T', cond \cup (T = C_i))$ transitively for all subclasses C_i of D where no class between C_i and D defines field f . Our optimization combines these requirements into a single one, roughly of the form $(D.f : T', cond \cup (T = \bigvee_i C_i))$. Basically, this requirement concisely states that D must provide a field f of type T' if the original receiver type T corresponds to any of the subclasses C_i of D .

Incrementalization and continuous constraint solving. We adopt the general incrementalization strategy from co-contextual PCF [6]: Initially, type check the full program bottom-up and memoize the typing output for each node (including class requirements and constraint system). Then, upon a change to the program, recheck each node from the change to the root of the program, reusing the memoized results from unchanged subtrees. This

way, incremental type checking asymptotically requires only $\log n$ steps for a program with n nodes.

In our formal model of co-contextual FJ, we collect constraints during type checking and solve them at the end to yield a substitution for the unification variables. As was discussed by Erdweg et al. for co-contextual PCF [6], this strategy is inadequate for incremental type checking, because we would memoize unsolved constraints and thus only obtain an incremental constraint generator, but even a small change would entail that all constraints had to be solved from scratch. In our implementation, we follow Erdweg et al.'s strategy of continuously solving constraints as soon as they are generated, memoizing the resulting partial constraint solutions. In particular, equality constraints that result from merge and remove operations can be solved immediately to yield a substitution, while subtype constraints often have to be deferred until more information about the inheritance hierarchy is available. In the context of FJ with its nominal types, continuous constraint solving has the added benefit of enabling additional requirement merging, for example, because two method requirements share the same receiver type after substitution.

Tree balancing. Even with continuous constraint solving, co-contextual FJ as defined in Section 4 still does not yield satisfactory incremental performance. The reason is that the syntax tree is deformed due to the root node, which consists of a sequence of *all* class declarations in the program. Thus, the root node has a branching factor only bound by the number of classes in the program, whereas the rest of the tree has a relative small branching factor bound by the number of arguments to a method. Since incremental type checking recomputes each step from the changed node to the root node, the type checker would have to repeat discharging class requirements at the root node after every code change, which would seriously impair incremental performance.

To counter this effect, we apply tree balancing as our final optimization. Specifically, instead of storing the class declarations as a sequence in the root node, we allow sequences of class declarations to occur as inner nodes of the syntax tree:

$$L ::= \bar{L} \mid \text{class } C \text{ extends } D \{\bar{C} \bar{f}; K \bar{M}\}$$

This allows us to layout a program's class declarations structurally as in $((((C_1 C_2) C_3) (C_4 C_5)) (C_6 C_7))$, thus reducing the costs for rechecking any path from a changed node to the root node. As part of this optimization, to satisfy requirements of classes that occur in different tree nodes such as C_1 and C_6 , we also need to propagate *class facts* such as actual method signatures upwards. As consequence, we can now link classes in any order without changing the type checking result.

We have implemented an incremental co-contextual FJ type checker in Scala using the optimizations described here. In the following section, we present our run-time performance evaluation.

7 Performance Evaluation

We have benchmarked the initial and incremental run-time performance of co-contextual FJ implementation. However, this evaluation makes no claim to be complete, but rather is intended to confirm the feasibility and potential of co-contextual FJ for incremental type checking.

7.1 Evaluation on synthesized FJ programs

Input data. We synthesized FJ programs with 40 root classes that inherit from `Object`. Each root class starts a binary tree in the inheritance hierarchy of height 5. Thus, each root-class hierarchy contains 31 FJ class declarations. In total, our synthesized programs have $31 * 40 + 3 = 1243$ class declarations, since we always require classes for natural numbers `Nat`, `Zero`, and `Succ`.

Each class has at least a field of type `Nat` and each class has a single method that takes no arguments and returns a `Nat`. We generated the method body according to one of three schemes:

- *AccumSuper*: The method adds the field’s value of this class to the result of calling the method of the super class.
- *AccumPrev*: Each class in root hierarchy $k > 1$ has an additional field that has the type of the class at the same position in the previous root hierarchy $k - 1$. The method adds the field’s value of this class to the result of calling the method of the class at the same position in the previous root hierarchy $k - 1$, using the additional field as receiver object.
- *AccumPrevSuper*: Combines the other two schemes; the method adds all three numbers.

We also varied the names used for the generated fields and methods:

- *Unique*: Every name is unique.
- *Mirrored*: Root hierarchies use the same names in the same classes, but names within a single root hierarchy are unique.
- *Override*: Root hierarchies use different names, but all classes within a single root hierarchy use the same names for the same members.
- *Mir+Over*: Combines the previous two schemes, that is, all classes in all root hierarchies use the same names for the same members.

For evaluating the incremental performance, we invalidate the memoized results for the three `Nat` classes. This is a critical case because all other classes depend on the `Nat` classes and a change is traditionally hard to incrementalize.

Experimental setup. First, we measured the wall-clock time for the initial check of each program using our co-contextual FJ implementation. Second, we measured the wall-clock time for the incremental reanalysis after invalidating the memoized results of the three `Nat` classes. Third, we measured the wall-clock time of checking the synthesized programs on `javac` and on a straightforward implementation of contextual FJ for comparison. Contextual FJ is the standard FJ described in Section 2, that uses contexts and class tables during type checking. Our implementation of contextual FJ is up to 2-times slower than `javac`, because it is not production quality. We used `Scalameeter`³ to take care of JIT warm-up, garbage-collection noise, etc. All measurements were conducted on a 3.1GHz duo-core MacBook Pro with 16GB memory running the Java HotSpot 64-Bit Server VM build 25.111-b14 with 4GB maximum heap space. We confirmed that confidence intervals were small.

Results. We show the measurement results in table 1. All numbers are in milliseconds. We also show the speedups of initial and incremental run of co-contextual type checking relative to both `javac` and contextual type checking.

As this data shows, the initial performance of co-contextual FJ is subpar: The initial type check takes up to 68-times and 61-times longer than using `javac` and a standard contextual checker respectively.

³ <https://scalameeter.github.io/>

Super	javac / contextual	co-contextual init	co-contextual inc
unique	70.00 / 93.99	3117.73 (0.02x / 0.03x)	23.44 (2.9x / 4x)
mirrored	68.03 / 88.73	1860.18 (0.04x / 0.05x)	15.17 (4.5x / 6x)
override	73.18 / 107.83	513.44 (0.14x / 0.21x)	16.92 (4.3x / 6x)
mir+over	72.64 / 132.09	481.07 (0.15x / 0.27x)	16.60 (4.4x / 8x)
Prev	javac / contextual	co-contextual init	co-contextual inc
unique	82.16 / 87.66	3402.28 (0.02x / 0.02x)	23.43 (3.5x / 4x)
mirrored	81.19 / 84.94	2136.42 (0.04x / 0.04x)	15.46 (5.3x / 5x)
override	81.51 / 120.60	840.14 (0.09x / 0.14x)	17.37 (4.7x / 7x)
mir+over	79.71 / 120.46	816.16 (0.09x / 0.15x)	16.61 (4.8x / 7x)
PrevSuper	javac / contextual	co-contextual init	co-contextual inc
unique	93.12 / 104.03	6318.69 (0.01x / 0.02x)	26.26 (3.5x / 4x)
mirrored	95.41 / 100.00	5014.12 (0.02x / 0.02x)	15.71 (6.1x / 6x)
override	92.88 / 130.01	3601.44 (0.03x / 0.04x)	17.35 (5.4x / 7x)
mir+over	93.37 / 126.57	3579.90 (0.03x / 0.04x)	16.61 (5.6x / 8x)

■ **Table 1** Performance measurement results with $k = 40$ root classes in **Milliseconds**. Numbers in parentheses indicate speedup relative to (javac/contextual) base lines.

However, co-contextual FJ consistently yields high speedups for incremental checks. In fact, it only takes between 3 and 21 code changes until co-contextual type checking is faster overall. In an interactive code editing session where every keystroke or word could be considered a code change, incremental co-contextual type checking will quickly break even and outperform a contextual type checker or javac.

The reason that the initial run of co-contextual FJ induces such high slowdowns is because the occurrence of class requirements is far removed from the occurrence of the corresponding class facts. This is true for the `Nat` classes that we merge with the synthesized code at the top-most node as well as for dependencies from one root hierarchy to another one. Therefore, the type checker has to propagate and merge class requirements for a long time until finally discovering class facts that discharge them. We conducted an informal exploratory experiment that revealed that the performance of the initial run can be greatly reduced by bringing requirements and corresponding class facts closer together. On the other hand, incremental performance is best when the changed code occurs as close to the root node as possible, such that a change entails fewer rechecks. In future work, when scaling our approach to full Java, we will explore different layouts for class declarations (e.g., following the inheritance hierarchy or the package structure) and for reshuffling the layout of class declarations during incremental type checking in order to keep frequently changing classes as close to the root as possible.

7.2 Evaluation on real Java program

Input data. We conduct an evaluation for our co-contextual type checking on realistic FJ programs. We wrote about 500 SLOCs in Java, implementing purely functional data structures for binary search trees and red black trees. In the Java code, we only used features supported by FJ and mechanically translated the Java code to FJ. For evaluating the incremental performance, we invalidate the memoized results for the three `Nat` classes as in the experiment above.

Experimental setup. Same as above.

Results. We show the measurements in milliseconds for the 500 lines of Java code.

javac / contextual	co-contextual init	co-contextual inc
14.88 / 3.74	48.07 (0.31x / 0.08x)	9.41 (1.6x / 0.39x)

Our own non-incremental contextual type checker is surprisingly fast compared to javac, and not even our incremental co-contextual checker gets close to that performance. When comparing javac and the co-contextual type checker, we observe that the initial performance of the co-contextual type checker improved compared to the previous experiment, whereas the incremental performance degraded. While the exact cause of this effect is unclear, one explanation might be that the small input size in this experiment reduces the relative performance loss of the initial co-contextual check, but also reduces the relative performance gain of the incremental co-contextual check.

8 Related work

The work presented in this paper on co-contextual type checking for OO programming languages, specifically for Featherweight Java, is inspired by the work on co-contextual type checking for PCF [6]. OO languages and FJ impose features like nominal typing, subtype polymorphism, and inheritance that are not covered in the work for co-contextual PCF [6]. In particular, here we developed a solution for merging and removing requirements in presence of nominal typing.

Introducing type variables as placeholders for the actual types of variables, classes, fields, methods is a known technique in type inference [10, 11]. The difference is that we introduce a fresh class variable for each occurrence of a method m or fields in different branches of the typing derivation. Since fresh class variables are generated independently, no coordination is required while moving up the derivation tree, ensuring context and class table independence. Type inference uses the context to coordinate type checking of m in different branches, by using the same type variable. In contrast to type inference where context and class table are available, we remove them (no actual context and class table). Hence, in type inference inheritance relation between classes and members of the classes are given, whereas in co-contextual FJ we establish these relations through requirements. That is, classes are required to have certain members with unknown types and unknown inheritance relation, dictated from the surrounding program.

Also, in contrast to bidirectional type checking [4, 5] that uses two sets of typing rules one for inference and one for checking, we use one set of co-contextual type rules, and the direction of type checking is all oriented bottom-up; types and requirements flow up. As in type inference, bidirectional type checking uses context to look up variables. Whereas co-contextual FJ has no context or class table, it uses requirements as a structure to record the required information on fields, methods, such that it enables resolving class variables of the required fields, methods to their actual types.

Co-contextual formulation of type rules for FJ is related to the work on principal typing [9, 16], and especially to principal typing for Java-like languages [2]. A principal typing [2] of each fragment (e.g., modules, packages, or classes) is associated with a set of type constraints on classes, which represents all other possible typings and can be used to check compatibility in all possible contexts. That is, principle typing finds the strongest type of a source fragment in the weakest context. This is used for type inference and separate compilation in FJ. They can deduce exact type constraints using a type inference

algorithm. We generalize this and do not only infer requirements on classes but also on method parameters and the current class. Moreover, we developed a duality relation between the class table and class requirements that enables the systematic development of co-contextual type systems for OO languages beyond FJ.

Related to our co-contextual FJ is the formulations used in the context of compositional compilation [1] (continuation of the work on principal typing [2]) and the compositional explanation of type errors [3]. This type system [1] partially eliminate the class table, namely only inside a fragment, and does not eliminate the context. Hence, type checking of parameters and **this** is coordinated and subexpressions are coupled through dependencies on the usage of context. In our work, we eliminate both class table (not only partially) and context, therefore all dependencies are removed. By doing so we can enable compositional compilation for individual methods. To resolve the type constraints on classes, compositional compilation [2] needs a linker in addition to an inference algorithm (to deduce exact type constraints), whereas, we use a constraint system and requirements. We use duality to derive a co-contextual type system for FJ and we also ensure that both formulations are equivalent (5). That is, we ensure that an expression, method, class, or program is well-typed in FJ if and only if it is well-typed in co-contextual FJ, and that all requirements are fulfilled. In contrast, compositional compilation rules do not check whether the inferred collection of constraints on classes is satisfiable; they actually allow to derive judgments for any fragment, even for those that are not statically correct.

Refactoring for generalization using type constraints [15, 14] is a technique Tip et al. used to manipulate types and class hierarchies to enable refactoring. That work uses variable type constraints as placeholders for changeable declarations. They use the constraints to restrict when a refactoring can be performed. Tip et al. are interested to find a way to represent the actual class hierarchy and to use constraints to have a safe refactoring and a well-typed program after refactoring. The constraint system used by Tip et al. is specialized to refactoring, because different variable constraints and solving techniques are needed. In contrast, in our work, we use class variables as placeholders for the actual type of required extends, constructors, fields, and methods of a class, in the lack of the class table. We want to gradually learn the information about the class hierarchy. We are interested in the type checking technique and how to co-contextualize it and use constraints for type refinement.

Adaption [7] is a programming language where the runtime system traces memory reads and writes and selectively replays dependent computations when a memory change occurs. In principle, this can be used to define an “incremental” contextual type checker. However, due to the top-down threading of the context, most of the computation will be sensitive to context changes and will have to be replayed, thus yielding unsatisfactory incremental performance. Given a co-contextual formulation as developed in our paper, it might be possible to define an efficient implementation in Adaption.

The works on smart/est recompilation [12, 13] has a different purpose from ours, namely to achieve separate compilation they need algorithms for the inference and also the linking phase which are specific to SML. In contrast, we use duality as a guiding principle to enable the translation from FJ to co-contextual FJ. This technique allows us to do perform a systematic (but yet not mechanical) translation from a given type system to the co-contextual one. Our type system facilitates incremental type checking because we decouple the dependencies between subexpressions and the smallest unit of compilation is any node in the syntax tree. Moreover, we have investigated optimizations for facilitating the early solving of requirements and constraints.

9 Conclusion and Future Work

In this paper, we presented a co-contextual type system for FJ by transforming the typing rules in the traditional formulation into a form that replaces top-down propagated contexts and class tables with bottom-up propagated *context and class table requirements*. We used duality as a technique to derive co-contextual FJ's typing rules from FJ's typing rules. To make the correspondence between class table and requirements, we presented class tables that are gradually extended with information from the class declarations, and how to map operations on contexts and class tables to their dual operations on context and class table requirements. To cover the OO features of nominal typing, subtype polymorphism, and implementation inheritance, co-contextual FJ uses conditional requirements, inequality conditions, and conditional constraints. Also, it changes the set of requirements by adding requirements with the different receiver from the ones defined by the surrounding program, in the process of merging and removing requirements as the type checker moves upwards and discovers class declarations. We proved the typing equivalence of expressions, methods, classes, and programs between FJ and co-contextual FJ.

The co-contextual formulation of FJ typing rules enables incremental type checking because it removes dependencies between subexpressions. We implemented an incremental co-contextual FJ type checker. Also, we evaluated its performance on synthesized programs up to 1243 FJ classes and 500 SLOCs of java programs.

There are several interesting directions for future work. In short term, we want to explore parallel co-contextual type checking for FJ. A next step would be to develop a co-contextual type system for full Java. Another interesting direction is to investigate co-contextual formulation for gradual type systems.

Acknowledgments. This work has been supported by the European Research Council, grant No. 321217.

References

- 1 Davide Ancona, Ferruccio Damiani, Sophia Drossopoulou, and Elena Zucca. Polymorphic bytecode: Compositional compilation for Java-like languages. In *Proceedings of Symposium on Principles of Programming Languages (POPL)*, 2005. doi:[10.1145/1040305.1040308](https://doi.org/10.1145/1040305.1040308).
- 2 Davide Ancona and Elena Zucca. Principal typings for Java-like languages. In *Proceedings of Symposium on Principles of Programming Languages (POPL)*, 2004. doi:[10.1145/964001.964027](https://doi.org/10.1145/964001.964027).
- 3 Olaf Chitil. Compositional explanation of types and algorithmic debugging of type errors. In *Proceedings of International Conference on Functional Programming (ICFP)*, 2001. doi:[10.1145/507635.507659](https://doi.org/10.1145/507635.507659).
- 4 David Raymond Christiansen. Bidirectional typing rules: A tutorial, 2013.
- 5 Joshua Dunfield and Neelakantan R. Krishnaswami. Complete and easy bidirectional type-checking for higher-rank polymorphism. In *Proceedings of International Conference on Functional Programming (ICFP)*, 2013. doi:[10.1145/2500365.2500582](https://doi.org/10.1145/2500365.2500582).
- 6 Sebastian Erdweg, Oliver Braćevac, Edlira Kuci, Matthias Krebs, and Mira Mezini. A co-contextual formulation of type rules and its application to incremental type checking. In *Proceedings of Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA)*, 2015. doi:[10.1145/2814270.2814277](https://doi.org/10.1145/2814270.2814277).
- 7 Matthew A. Hammer, Khoo Yit Phang, Michael Hicks, and Jeffrey S. Foster. Adaption: Composable, demand-driven incremental computation. In *Proceedings of Conference on*

XX:26 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

- Programming Language Design and Implementation (PLDI)*, 2014. doi:10.1145/2666356.2594324.
- 8 Atsushi Igarashi, Benjamin C. Pierce, and Philip Wadler. Featherweight Java: A minimal core calculus for Java and GJ. *Transactions on Programming Languages and Systems (TOPLAS)*, 2001. doi:10.1145/503502.503505.
 - 9 Trevor Jim. What are principal typings and what are they good for? In *Proceedings of Symposium on Principles of Programming Languages (POPL)*, 1996. doi:10.1145/237721.237728.
 - 10 Benjamin C Pierce. *Types and programming languages*. MIT press, 2002.
 - 11 Benjamin C. Pierce and David N. Turner. Local type inference. In *Proceedings of Symposium on Principles of Programming Languages (POPL)*, 1998. doi:10.1145/268946.268967.
 - 12 Zhong Shao and Andrew W. Appel. Smartest recompilation. In *Proceedings of Symposium on Principles of Programming Languages (POPL)*, 1993. doi:10.1145/158511.158702.
 - 13 Walter F. Tichy. Smart recompilation. *Transactions on Programming Languages and Systems (TOPLAS)*, 1986. doi:10.1145/5956.5959.
 - 14 Frank Tip, Robert M. Fuhrer, Adam Kiežun, Michael D. Ernst, Ittai Balaban, and Bjorn De Sutter. Refactoring using type constraints. *Transactions on Programming Languages and Systems (TOPLAS)*, 2011. doi:10.1145/1961204.1961205.
 - 15 Frank Tip, Adam Kiezun, and Dirk Bäumer. Refactoring for generalization using type constraints. In *Proceedings of Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA)*, 2003. doi:10.1145/949305.949308.
 - 16 J. B. Wells. The essence of principal typings. In *Proceedings of International Colloquium on Automata, Languages and Programming (ICALP)*, 2002. doi:10.1007/3-540-45465-9_78.

A Auxiliary definitions; merge, add, remove

We give the definition of merge_{CR} for all cases of the clause definition ⁴.

$$\text{merge}_{CR}(CR_1, CR_2) = CR|_S$$

$$\begin{aligned} \text{where } CR = & \{ ((CR_1 \setminus (\overline{T_1}.\text{extends} : T_2, \text{cond}_1)) \cup (\overline{T_1}.\text{init}(\overline{T_1}), \text{cond}_1) \cup (\overline{T_1}.f : T_2, \text{cond}_1) \\ & \cup (\overline{T_1}.m : \overline{T_1} \rightarrow T_2, \text{cond}_1)) \cup ((CR_2 \setminus (\overline{T_2}.\text{extends} : T_3, \text{cond}_2) \\ & \cup (\overline{T_2}.\text{init}(\overline{T_2}), \text{cond}_2) \cup (\overline{T_2}.f : T_3, \text{cond}_2) \cup (\overline{T_2}.m : \overline{T_2} \rightarrow T_3, \text{cond}_2)) \\ & \cup CR_e \cup CR_k \cup CR_f \cup CR_m) \} \end{aligned}$$

$$S = S_e \cup S_k \cup S_f \cup S_m$$

$$\begin{aligned} \text{where } CR_e = & \{ (T_1.\text{extends} : T'_1, \text{cond}_1, (T_1 \neq T_2)), (T_2.\text{extends} : T'_2, \text{cond}_2 \cup \\ & (T_1 \neq T_2)), (T_1.\text{extends} : T'_1, (\text{cond}_1 \cup \text{cond}_2 \cup (T_1 = T_2)) \\ & | (T_1.\text{extends} : T'_1, \text{cond}_1) \in CR_1 \wedge (T_2.\text{extends} : T'_2, \text{cond}_2) \in CR_2) \} \end{aligned}$$

$$\begin{aligned} S_e = & \{ (T'_1 = T'_2 \text{ if } T_1 = T_2) | (T_1.\text{extends} : T'_1, \text{cond}_1) \in CR_1 \\ & \wedge (T_2.\text{extends} : T'_2, \text{cond}_2) \in CR_2 \} \end{aligned}$$

$$\begin{aligned} \text{where } CR_k = & \{ (T_1.\text{init}(\overline{T_1}), \text{cond}_1 \cup (T_1 \neq T_2)) \cup (T_2.\text{init}(\overline{T_2}), \text{cond}_2 \cup (T_1 \neq T_2)) \\ & (T_1.\text{init}(\overline{T_1}), \text{cond}_1 \cup \text{cond}_2 \cup (T_1 = T_2)) | (T_1.\text{init}(\overline{T_1}), \text{cond}_1) \in CR_1 \\ & \wedge (T_2.\text{init}(\overline{T_2}), \text{cond}_2) \in CR_2 \} \end{aligned}$$

$$\begin{aligned} S_k = & \{ (\overline{T_1} = \overline{T_2} \text{ if } T_1 = T_2) | (T_1.\text{init}(\overline{T_1}), \text{cond}_1) \in CR_1 \\ & \wedge (T_2.\text{init}(\overline{T_2}), \text{cond}_2) \in CR_2 \} \end{aligned}$$

$$\begin{aligned} \text{where } CR_f = & \{ (T_1.f : T'_1, \text{cond}_1 \cup (T_1 \neq T_2)) \cup (T_2.f : T'_2, \text{cond}_2 \cup (T_1 \neq T_2)) \\ & \cup (T_1.f : T'_1, \text{cond}_1 \cup \text{cond}_2 \cup (T_1 = T_2)) | (T_1.f : T'_1, \text{cond}_1) \in CR_1 \\ & \wedge (T_2.f : T'_2, \text{cond}_2) \in CR_2 \} \end{aligned}$$

$$\begin{aligned} S_f = & \{ (T'_1 = T'_2 \text{ if } T_1 = T_2) | (T_1.f : T'_1, \text{cond}_1) \in CR_1 \\ & \wedge (T_2.f : T'_2, \text{cond}_2) \in CR_2 \} \end{aligned}$$

$$\begin{aligned} \text{where } CR_m = & \{ (T_1.m : \overline{T_1} \rightarrow T'_1, \text{cond}_1 \cup (T_1 \neq T_2)) \cup (T_2.m : \overline{T_2} \rightarrow T'_2, \text{cond}_2 \\ & (T_1 \neq T_2)) \cup (T_1.m : \overline{T_1} \rightarrow T'_1, \text{cond}_1 \cup \text{cond}_2 \cup (T_1 = T_2)) | (T_1. \\ & m : \overline{T_1} \rightarrow T'_1, \text{cond}_1) \in CR_1 \wedge (T_2.m : \overline{T_2} \rightarrow T'_2, \text{cond}_2) \in CR_2 \} \end{aligned}$$

$$\begin{aligned} S_m = & \{ (T'_1 = T'_2 \text{ if } T_1 = T_2) \cup (\overline{T_1} = \overline{T_2} \text{ if } T_1 = T_2) | (T_1.m : \overline{T_1} \rightarrow T'_1, \\ & \text{cond}_1) \in CR_1 \wedge (T_2.m : \overline{T_2} \rightarrow T'_2, \text{cond}_2) \in CR_2 \} \end{aligned}$$

⁴ Merge operation for optional methods is the same as merge for methods.

XX:28 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

Next we define add and remove operations for all cases of the clause definition.

$$\begin{aligned}
 addExt(class C \text{ extends } D, CT) &= (C \text{ extends } D) \cup CT \\
 removeExt(class C \text{ extends } D, CR) &= CR'|_S \\
 \text{where } CR' &= \{(T.\text{extends} : T', \text{cond} \cup (T \neq C)) \mid (T.\text{extends} : T', \text{cond}) \in CR\} \\
 &\quad \cup \{(T.m : \bar{T} \rightarrow T', \text{cond} \cup (T \neq C)) \\
 &\quad \quad \cup (D.m : \bar{T} \rightarrow T', \text{cond} \cup (T = C)) \mid (T.m : \bar{T} \rightarrow T', \text{cond}) \in CR\} \\
 &\quad \cup \{(T.m : \bar{T} \rightarrow T', \text{cond} \cup (T \neq C))_{opt} \\
 &\quad \quad \cup (D.m : \bar{T} \rightarrow T', \text{cond} \cup (T = C))_{opt} \\
 &\quad \quad \mid (T.m : \bar{T} \rightarrow T', \text{cond})_{opt} \in CR\} \\
 &\quad \cup \{(T.f : T', \text{cond} \cup (T \neq C)) \cup (D.f : T', \text{cond} \cup (T = C)) \\
 &\quad \quad \mid (T.f : T', \text{cond}) \in CR\} \\
 S &= \{(T' = D \text{ if } T = C) \mid (T.\text{extends} : T', \text{cond}) \in CR\}
 \end{aligned}$$

$$\begin{aligned}
 addCtor(C, (\bar{D} \ \bar{g}, \bar{C} \ \bar{f}), CT) &= (C.\text{init}(\bar{D}; \bar{C})) \cup CT \\
 removeCtor(C, (\bar{D} \ \bar{g}, \bar{C} \ \bar{f}), CR) &= CR'|_S \\
 \text{where } CR' &= \{(T.\text{init}(\bar{T})), \text{cond} \cup (T \neq C)) \mid (T.\text{init}(\bar{T})), \text{cond} \in CR\} \\
 &\quad \cup (CR \setminus (T.\text{init}(\bar{T}), \text{cond})) \\
 S &= \{(\bar{T} = \bar{D} \ \bar{C} \text{ if } T = C) \mid (T.\text{init}(\bar{T}), \text{cond}) \in CR\}
 \end{aligned}$$

$$\begin{aligned}
 addFs(C, \bar{C}_f \ \bar{f}, CT) &= \bar{C}.f : \bar{C}_f \cup CT \\
 removeF(C, C_f \ f, CR) &= CR'|_S \\
 \text{where } CR' &= \{(T.f : T', \text{cond} \cup (T \neq C)) \mid (T.f : T', \text{cond}) \in CR\} \\
 &\quad \cup (CR \setminus (T.f : T', \text{cond})) \\
 S &= \{(T' = C_f \text{ if } T = C) \mid (T.f : T', \text{cond}) \in CR\} \\
 removeFs(C, \bar{C}_f \ f, CR) &= CR'|_S \\
 \text{where } CR' &= \{CR_f \mid (C_f \ f) \in \bar{C}_f \ f \wedge removeF(CR, C, C_f \ f) = CR_f|_{S_f}\} \\
 S &= \{S_f \mid (C_f \ f) \in \bar{C}_f \ f \wedge removeF(CR, C, C_f \ f) = CR_f|_{S_f}\}
 \end{aligned}$$

$$\begin{aligned}
 addMs(C, \bar{M}, CT) &= \bar{C}.m : \bar{C} \rightarrow \bar{C}' \cup CT \\
 removeM(C, C' \ m(\bar{C} \ \bar{x}) \ \{\text{return } e\}, CR) &= CR'|_S \\
 \text{where } CR' &= \{(T.m : \bar{T} \rightarrow T', \text{cond} \cup (T \neq C)) \mid (T.m : \bar{T} \rightarrow T', \text{cond}) \in CR\} \\
 &\quad \cup (CR \setminus (T.m : \bar{T} \rightarrow T', \text{cond})) \\
 S &= \{(T' = C' \text{ if } T = C) \cup (\bar{T} = \bar{C} \text{ if } T = C) \mid (T.m : \bar{T} \rightarrow T', \text{cond}) \in CR\}
 \end{aligned}$$

$\text{removeMs}(C, \overline{M}, CR) = CR'|_S$
where $CR' = \{CR_m \mid (C' m(\overline{C} \bar{x}) \{\text{return } e\}) \in \overline{M}$
 $\quad \wedge \text{removeM}(C, C' m(\overline{C} \bar{e}) \{\text{return } e\}, CR) = CR_m|_{S_m}\}$
 $S = \{S_m \mid (C' m(\overline{C} \bar{x}) \{\text{return } e\}) \in \overline{M}$
 $\quad \wedge \text{removeM}(C, C' m(\overline{C} \bar{x}) \{\text{return } e\}, CR) = CR_m|_{S_m}\}$
 $\text{removeOptM}(C, C' m(\overline{C} \bar{x}) \{\text{return } e\}, CR) = CR'|_S$
where $CR' = \{(T.m : \overline{T} \rightarrow T', \text{cond} \cup (T \neq C))_{opt} \mid (T.m : \overline{T} \rightarrow T', \text{cond})_{opt} \in CR\}$
 $\quad \cup (CR \setminus (T.m : \overline{T} \rightarrow T', \text{cond}_{opt}))$
 $S = \{(T' = C' \text{ if } T = C) \cup (\overline{T} = \overline{C} \text{ if } T = C) \mid (T.m : \overline{T} \rightarrow T', \text{cond})_{opt} \in CR\}$
 $\text{removeOptMs}(C, \overline{M}, CR) = (CR' \cup (CR \setminus CR'))|_S$
where $CR' = \{CR_m \mid (C' m(\overline{C} \bar{x}) \{\text{return } e\}) \in \overline{M}$
 $\quad \wedge \text{removeOptM}(CR, C, C' m(\overline{C} \bar{e}) \{\text{return } e\}) = CR_m|_{S_m}\}$
 $S = \{S_m \mid (C' m(\overline{C} \bar{x}) \{\text{return } e\}) \in \overline{M}$
 $\quad \wedge \text{removeOptM}(CR, C, C' m(\overline{C} \bar{x}) \{\text{return } e\}) = CR_m|_{S_m}\}$

B Equivalence of Contextual and Co-Contextual FJ

In here we describe a detailed proof of typing equivalence between FJ and co-contextual FJ. Co-contextual FJ is constraint based type system. We present the formal definitions for substitution, and Figures 11, 12 give formal definition how to retrieve the immediate subclass relation Σ from rep. class table, and a list of class declaration. That is, a projection from class table/list of declarations to a set of tuples, which represent the relation between two classes in an extends clause.

$$\begin{array}{c}
 \frac{}{\text{projExt}(\emptyset) = \emptyset} \quad \frac{}{\text{projExt}(C \text{ extends } D) = (C, D)} \quad \frac{}{\text{projExt}(C.f : C') = \emptyset} \\[10pt]
 \frac{}{\text{projExt}(C.m() : \overline{C} \rightarrow C') = \emptyset} \quad \frac{}{\text{projExt}(C.\text{init}(\overline{C})) = \emptyset} \\[10pt]
 \frac{\text{projExt}(CTcls_1) = \Sigma_1 \quad \text{projExt}(CTcls_2) = \Sigma_2}{\text{projExt}(CTcls_1 \cup CTcls_2) = \Sigma_1 \cup \Sigma_2}
 \end{array}$$

Figure 11 Projection of Class Table to Extends.

$$\begin{array}{c}
 \frac{}{\text{projExt}(\emptyset) = \emptyset} \quad \frac{}{\text{projExt}(\text{class } C \text{ extends } D \{\overline{C} \bar{f}; K \overline{M}\}) = (C, D)} \\[10pt]
 \frac{\text{projExt}(L_1) = \Sigma_1 \quad \text{projExt}(L_2) = \Sigma_2}{\text{projExt}(L_1; L_2) = \Sigma_1 \cup \Sigma_2}
 \end{array}$$

Figure 12 Projection of Class Declarations to Extends.

► **Definition 10** (Subtyping relative to Σ). Let Σ be a binary relation on class names, C, D class names. Then C is a subtype of D relative to Σ ($C <:_{\Sigma} D$), if and only if $(C, D) \in \Sigma^*$, where Σ^* is the reflexive, transitive closure of Σ .

► **Definition 11** (Substitution σ). Given sets of context and class requirements R, CR, σ is a set of mappings from class variables to class types, i.e., $\sigma = \{U \mapsto C \mid U \in \text{freshU}(R) \cup \text{freshU}(CR)\}$.

► **Definition 12** (Constraint Satisfaction). Let s be a constraint on class types, σ a substitution from class variables to class types, Σ a binary relation on class names. The pair (Σ, σ) satisfies s ($\text{sat}(\Sigma, \sigma, s)$) if and only if one of the following holds:

1. If $s = (T <: T')$, then $T\sigma <:_{\Sigma} T'\sigma$.
2. If $s = (T = T')$, then $T\sigma = T'\sigma$.
3. If $s = (T = T' \text{ if } cond)$ and for all $s' \in cond$, $\text{sat}(\Sigma, \sigma, s')$ then $T\sigma = T'\sigma$.
4. If $s = (T \neq T')$, then $T\sigma \neq T'\sigma$.
5. If $s = (T \not<: T')$, then $T\sigma \not<:_{\Sigma} T'\sigma$.

► **Assumption 13** (Properties of solve). Let Σ be a binary relation on class names, S a set of constraints on class types:

1. $\text{solve}(\Sigma, S)$ terminates.
2. If $\text{solve}(\Sigma, S) = \sigma$. Then for all $s \in S$, $\text{sat}(\Sigma, \sigma, s)$.
3. If $\text{solve}(\Sigma, S) = \perp$. Then there exists $s \in S$, where $\text{sat}(\Sigma, \sigma, s)$ does not hold.

► **Definition 14** (Ground context requirement). $\sigma(R)$ is ground, if for all $(x : T) \in R$ then $\sigma(T)$ is ground.

► **Definition 15** (Ground class table requirements). $\sigma(CR)$ is ground, if for all $(CReq, cond) \in CR$ then $\sigma(CReq)$ is ground and $\sigma(cond)$ is ground.

► **Definition 16** (Ground class requirement).

$$\sigma(CReq) \text{ ground} = \begin{cases} \sigma(T.\text{extends} : T') \text{ ground} & \text{if } (CReq) = (T.\text{extends} T') \wedge \\ & \sigma(T), \sigma(T') \text{ ground} \\ \sigma(T.f : T') \text{ ground} & \text{if } (CReq) = (T.f : T') \wedge \\ & \sigma(T), \sigma(T') \text{ ground} \\ \sigma(T.m : \bar{T} \rightarrow T') \text{ ground} & \text{if } (CReq) = (T.m : \bar{T} \rightarrow T') \wedge \\ & \sigma(T), \sigma(\bar{T}) \text{ ground} \\ & \wedge \sigma(T') \text{ ground} \\ \sigma(T.init : \bar{T}) \text{ ground} & \text{if } (CReq) = (T.init(\bar{T})) \wedge \\ & \sigma(T), \sigma(\bar{T}) \text{ ground} \end{cases} \quad (1)$$

► **Definition 17** (Ground conditions). $\sigma(cond)$ is ground, if for all $(T = T'), (T'' \neq T^*) \in cond$ then $\sigma(T), \sigma(T'), \sigma(T''), \sigma(T^*)$ are ground.

► **Definition 18** (Ground Solution σ). For a given type T , a set of constraints S , where $\sigma = \text{solve}(S)$, we lift substitution σ to sets of context requirements R , class requirements CR and σ is a ground solution if:

- 1) $\sigma(T)$ is ground

$$\begin{array}{c}
\text{FIELD-LOOKUP} \frac{C.f_i : C_i \in \text{fields}(C, CT)}{\text{field}(f_i, C, CT) = C_i} \quad \text{EXTENDS} \frac{(C.\text{extends} = D) \in CT}{\text{extends}(C, CT) = D} \\
\\
\text{S-EXTEND} \frac{(C.\text{extends} = D) \in CT}{CT \text{ satisfy } (C.\text{extends} : D, \text{cond})} \\
\\
\text{S-CONSTRUCTOR} \frac{\text{fields}(C, CT) = \overline{C.f : C_f}}{CT \text{ satisfy } (C.\text{init}(\overline{C_f}), \text{cond})} \\
\\
\text{S-FIELD} \frac{\text{field}(f, C, CT) = C'}{CT \text{ satisfy } (C.f : C', \text{cond})} \\
\\
\text{S-METHOD} \frac{\text{if } \text{mtype}(m, C, CT) = \overline{C} \rightarrow C'}{CT \text{ satisfy } (C.m : \overline{C} \rightarrow C', \text{cond})} \\
\\
\text{SATISFY} \frac{(\text{cond hold} \Rightarrow CT \text{ satisfy } (CReq, \text{cond})) \quad \forall(CReq, \text{cond}) \in CR}{CT \text{ satisfy } CR}
\end{array}$$

Figure 13 Judgment for Satisfy.

- 2) $\sigma(R)$ is ground
- 3) $\sigma(CR)$ is ground

The two first rules of Figure.13 define the field lookup and extends lookup. The other rules formally define the relation between the class table and class table requirements. We assume that class table requirements are ground.

► **Lemma 19.** Let $\text{merge}_R(R_1, R_2) = R|_S$, $\Gamma \supseteq \sigma_1(R_1)$, $\Gamma \supseteq \sigma_2(R_2)$, and $\sigma_1(R_1)$, $\sigma_2(R_2)$ are ground. Then $\sigma_1 \circ \sigma_2$ solves S .

Proof. By the definition of merge_R , $S = \{R_1(x) = R_2(x) \mid x \in \text{dom}(R_1) \cap \text{dom}(R_2)\}$. Since $\Gamma \supseteq \sigma_i(R_i)$, we know $\Gamma(x) = \sigma_i(R_i(x))$ for all $x \in \text{dom}(R_i)$. In particular, $\Gamma(x) = \sigma_1(R_1(x)) = \sigma_2(R_2(x))$ for all $x \in \text{dom}(R_1) \cap \text{dom}(R_2)$. Thus, $\sigma_1 \circ \sigma_2$ solves C because $(\sigma_1 \circ \sigma_2)(R_1(x)) = \sigma_1(R_1(x)) = \sigma_2(R_2(x)) = (\sigma_1 \circ \sigma_2)(R_2(x))$ for all $x \in \text{dom}(R_1) \cap \text{dom}(R_2)$, because $\sigma_1(R_1)$ and $\sigma_2(R_2)$ are ground. ◀

► **Lemma 20.** Let $\text{merge}_{CR}(CR_1, CR_2) = CR|_S$, $\sigma_1(CR_1)$, $\sigma_2(CR_2)$ are ground, and CT satisfies $\sigma_1(CR_1)$, CT satisfies $\sigma_2(CR_2)$. Then $\sigma_1 \circ \sigma_2$ solves S .

Proof. By the definition of merge_{CR} , $S = S_c \cup S_e \cup S_k \cup S_f \cup S_m$, where $S_f = \{(T'_1 = T'_2 \text{ if } T_1 = T_2) \mid (T_1.f : T'_1, \text{cond}_1) \in CR_1 \wedge (T_2.f : T'_2, \text{cond}_2) \in CR_2\}$.

Since CT satisfies $\sigma_i(CR_i)$, we know $\sigma_i(T_i.f : T'_i, \text{cond}_i) \in CT$, for all $f \in \text{dom}(CR_i)$, where $\sigma_i(\text{cond}_i)$ hold. In particular, for all $f \in \text{dom}(CR_1) \cap \text{dom}(CR_2)$, where $(T_1.f : T'_1, \text{cond}_1) \in CR_1$, $(T_2.f : T'_2, \text{cond}_2) \in CR_2$, $\sigma_1(T'_1) = \sigma_2(T'_2)$ if $\sigma_1(T_1) = \sigma_2(T_2)$. Thus, $\sigma_1 \circ \sigma_2$ solves S because $(\sigma_1 \circ \sigma_2)(T'_1) = \sigma_1(T'_1) = \sigma_2(T'_2) = (\sigma_1 \circ \sigma_2)(T'_2)$, if $\sigma_1(T_1) = \sigma_2(T_2)$, because $\sigma_1(CR_1)$ and $\sigma_2(CR_2)$ are ground.

The same procedure we follow for methods, i.e., a given method m that we find a match in $CR_1(C)$, and $CR_2(C)$, S_m is the set of constraints for the method as result of unifying return type and types of the parameters from the two different class requirements(CR_1, CR_2). ◀

► **Lemma 21.** If CT satisfy $\sigma_1(CR_1)$, $\sigma_1(CR_1)$ is ground, and CT satisfy $\sigma_2(CR_2)$, $\sigma_2(CR_2)$ is ground, then CT satisfy $\sigma(CR)$, where $\sigma = \sigma_1 \circ \sigma_2$ and $CR_S = \text{merge}_{CR}(CR_1, CR_2)$.

Proof. First we have to show that the new set of constraints S generated from merging is solvable, and this holds by Lemma 20.

Then we show that CT satisfies $\sigma(CR)$. For sake of brevity we consider clauses common in both requirements sets CR_1 and CR_2 . Let us consider the field f , such that $(T_1.f : T'_1, cond_1) \in CR_1$ and $(T_2.f : T'_2, cond_2) \in CR_2$, and by assumption we have that CT satisfy $\sigma_1((T_1.f : T'_1, cond_1))$ and CT satisfy $\sigma_2((T_2.f : T'_2, cond_2))$. By the definition of merge_{CR} the conditions of these two requirements are updated, i.e., $(T_1.f : T'_1, cond_1 \cup (T_1 \neq T_2))$ and $(T_2.f : T'_2, cond_2 \cup (T_1 \neq T_2))$, and a new requirement is added, i.e., $(T_1.f : T'_1, cond_1 \wedge cond_2 \cup (T_1 = T_2))$. Suppose that CT satisfies the three of the new and updated requirements, namely all their conditions should hold by rule T-SATISFY, but this is contradiction, because two types cannot be at the same time not equal and equal. Therefore there are two possibilities:

- 1) either the conditions of the updated field requirements hold, i.e., $(T_1.f : T'_1, cond_1 \cup (T_1 \neq T_2))$, $(T_2.f : T'_2, cond_2 \cup (T_1 \neq T_2))$, and $(T_1 \neq T_2)$ holds.
 - 2) or the conditions of the new field requirement hold, i.e., $(T_1.f : T'_1, cond_1 \wedge cond_2 \cup (T_1 = T_2))$, and $(T_1 = T_2)$ holds.
- If 1) is possible then CT satisfies $\sigma_1 \circ \sigma_2(T_1.f : T'_1, cond_1 \cup (T_1 \neq T_2) \cup T_2.f : T'_2, cond_2 \cup (T_1 \neq T_2))$ because by assumption CT satisfy $\sigma_1((T_1.f : T'_1, cond_1))$ and CT satisfies $\sigma_2((T_2.f : T'_2, cond_2))$. The new class requirement $(T_1.f : T'_1, cond_1 \wedge cond_2 \cup (T_1 = T_2))$ is satisfiable by default since one of its conditions $(T_1 = T_2)$ does not hold, namely is not a valid requirement.
 - If 2) is possible then CT satisfies $\sigma_1 \circ \sigma_2(T_1.f : T'_1, cond_1 \wedge cond_2 \cup (T_1 = T_2))$, because $(T_1 = T_2)$, CT satisfy $\sigma_1((T_1.f : T'_1, cond_1))$ and CT satisfies $\sigma_2((T_2.f : T'_2, cond_2))$. The updated class requirements $(T_1.f : T'_1, cond_1 \cup (T_1 \neq T_2))$ and $(T_2.f : T'_2, cond_2 \cup (T_1 \neq T_2))$ are satisfiable by default since one of their conditions $(T_1 \neq T_2)$ does not hold, namely are not valid requirements.

As a result CT satisfies the resulting set of requirements after merging for the given field f .

The same we argue for methods, optional methods, current class, and extend clauses. ◀

► **Proposition 22** (Independent derivation in co-contextual type checking). Given a set of otherwise independent derivations of class requirement $CR = \{CR_1 \cup \dots \cup CR_n\}$, $\forall i, j \in [1..n]$. $\text{freshU}(CR_i) \cap \text{freshU}(CR_j) = \emptyset$, where $\text{freshU}(CR_i) = \{U_1^i, \dots, U_n^i\}$

Proof. It is straightforward by the rules and how the type checking is performed, i.e., for every rules of the type checking we always introduce fresh class names U , therefore U s in one derivation do not appear to another independent derivation. ◀

► **Corollary 23** (Associative feature for substitution). Given CR , σ_1 and σ_2 then it holds that $(\sigma_1 \circ \sigma_2)(CR) = (\sigma_2 \circ \sigma_1)(CR)$

Proof. Follows directly from Proposition 22. ◀

► **Definition 24** (Correspondence relation for expressions). Given judgments $\Gamma; CT \vdash e : C$, $e : T \mid S \mid R \mid CR$, and $\text{solve}(\Sigma, S) = \sigma$, where $\text{projExt}(CT) = \Sigma$. The correspondence relation between Γ and R , CT and CR , written $(C, \Gamma, CT) \triangleright \sigma(T, R, CR)$, is defined as:

- a) $C = \sigma(T)$
- b) $\Gamma \supseteq \sigma(R)$

c) CT satisfies $\sigma(CR)$

► **Theorem 25** (Equivalence of expressions: \Rightarrow). Given e, C, Γ, CT , if $\Gamma; CT \vdash e : C$, then there exists $T, S, R, CR, \Sigma, \sigma$, where $\text{projExt}(CT) = \Sigma$ and $\text{solve}(\Sigma, S) = \sigma$, such that $e : T \mid S \mid R \mid CR$ holds, σ is a ground solution and $(C, \Gamma, CT) \triangleright \sigma(T, R, CR)$ holds.

Proof. We proceed by induction on the typing judgment of expression e .

■ Case T-VAR with $\Gamma; CT \vdash x : C$.

By inversion, $\Gamma(x) = C$.

Let U fresh, $S = \emptyset$, $R = \{x : U\}$, $CR = \emptyset$ and $\sigma = \{U \mapsto C\}$.

Then $e : C' \mid S' \mid R \mid CR$ holds by rule TC-VAR. Since $S = \emptyset$, then σ solves S . σ is ground solution because:

- 1) $\sigma(U)$ is ground because $\sigma(U) = C$.
- 2) $R = \{x : U\}$ and $\sigma = \{U \mapsto C\}$ implies $\sigma(R) = \{x : C\}$ is ground.
- 3) $CR = \emptyset$ implies that $\sigma(CR) = \emptyset$ is ground.

The correspondence relation holds because;

- a) $C = \sigma(U)$
- b) Since $\Gamma(x) = C$ by inversion, then $\Gamma \supseteq \{x : C\} = \sigma(R)$.
- c) $CR = \emptyset$ and $\sigma(CR) = \emptyset$ implies that CT satisfies $\sigma(CR)$.

■ Case T-FIELD with $\Gamma; CT \vdash e.f_i : C_i$.

By inversion, $\Gamma; CT \vdash e : C_e$ and $\text{field}(f_i, C_e, CT) = C_i$. By IH, $e : T'_e \mid S_e \mid R_e \mid CR_e$, where $\text{solve}(\text{projExt}(CT), S_e) = \sigma_e$, $\sigma_e(T'_e)$, $\sigma_e(R_e)$, $\sigma_e(CR_e)$ are ground and the correspondence relation holds, i.e., $C_e = \sigma_e(T'_e)$, $\Gamma \supseteq \sigma_e(R_e)$, CT satisfies $\sigma_e(CR_e)$.

Let U be fresh, $CR|_{S_f} = \text{merge}_{CR}(CR_e, (T'_e.f_i : U, \emptyset))$, $S = S_e \cup S_f$ and $\sigma = \{U \mapsto C_i\} \circ \sigma_e$. Then $e.f_i : U \mid S \mid R_e \mid CR$ holds by rule TC-FIELD.

σ solves S because it solves S_e and S_f as shown below:

- $\text{solve}(\text{projExt}(CT), S_e) = \sigma_e$ by IH and $\sigma = \{U \mapsto C_i\} \circ \sigma_e$ implies σ solves S_e
- $\sigma_e(CR_e)$ is ground by IH.

(*) $\sigma(T'_e.f_i : U, \emptyset)$ is ground, because $\sigma(T'_e.f_i : U) = (\sigma(T'_e).f_i : \sigma(U)) = (C_e.f_i : C_i)$ and $C_e.f_i : C_i$ is ground.

CT satisfies $\sigma_e(CR_e)$ by IH.

(**) CT satisfy $\sigma(T'_e.f : U, \emptyset)$ because $\text{field}(f_i, C_e, CT) = C_i$ hence by rule S-FIELD holds that CT satisfy $(C_e.f : C_i, \emptyset)$, and $\sigma(T'_e.f_i : U) = C_e.f_i : C_i$.

As a result by Lemma 20 σ solves S_f .

σ is a ground solution because:

- 1) $\sigma(U)$ is ground because $\sigma(U) = C_i$.
- 2) $\sigma(R_e)$ is ground because $\sigma(R_e) = (\{U \rightarrow C_i\} \circ \sigma_e)(R_e) = \{U \rightarrow C_i\}(\sigma_e(R_e))$, since $\sigma_e(R_e)$ is ground by IH then $\{U \rightarrow C_i\}(\sigma_e(R_e)) = \sigma_e(R_e)$, i.e., $\sigma(R_e) = \sigma_e(R_e)$.
- 3) $\sigma(CR_e)$ is ground because $\sigma(CR_e) = (\{U \rightarrow C_i\} \circ \sigma_e)(CR_e) = \{U \rightarrow C_i\}(\sigma_e(CR_e))$, $\{U \rightarrow C_i\}(\sigma_e(CR_e)) = \sigma_e(CR_e)$ because $\sigma_e(CR_e)$ is ground by IH. $\sigma(T'_e.f_i : U, \emptyset)$ is ground by (*). As a result $\sigma(CR)$ is ground by definition of merge_{CR} .

The correspondence relation holds because:

- a) $C_i = \sigma(U)$
- b) $\Gamma \supseteq \sigma(R_e)$, because $\Gamma \supseteq \sigma_e(R_e)$ by IH, and from 2) $\sigma(R_e) = \sigma_e(R_e)$.
- c) CT satisfy $\sigma(CR_e)$, because CT satisfy $\sigma_e(CR_e)$ by IH, and from 3) $\sigma(CR_e) = \sigma_e(CR_e)$. CT satisfy $\sigma(T'_e.f : U, \emptyset)$ by (**). As a result CT satisfy $\sigma(CR_e) \cup \sigma(T'_e.f : U, \emptyset)$, i.e., CT satisfy $\sigma(CR)$ by Lemma 21.

XX:34 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

- Case T-INV_K with $\Gamma; CT \vdash e.m(\bar{e}) : C$.

By inversion, $\Gamma; CT \vdash e : C_e$, $mtype(m, C_e, CT) = \bar{D} \rightarrow C$, $\Gamma; CT \vdash \bar{e} : \bar{C}$ and $\bar{C} <: \bar{D}$.

By IH, $e : T_e \mid S_e \mid R_e \mid CR_e$, where $solve(\text{projExt}(CT), S_e) = \sigma_e$, $\sigma_e(T_e)$, $\sigma_e(R_e)$, $\sigma_e(CR_e)$ are ground and the correspondence relation hold, i.e., $C_e = \sigma_e(T'_e)$, $\Gamma \supseteq \sigma_e(R_e)$, $CT \text{ satisfy } \sigma_e(CR_e)$.

By IH $\bar{e} : \bar{T} \mid \bar{S} \mid \bar{R} \mid \bar{CR}$, $\forall i \in [1..n]$. $solve(\text{projExt}(CT), S_i) = \sigma_i$, $\sigma_i(T_i)$, $\sigma_i(R_i)$, $\sigma_i(CR_i)$ are ground, and the correspondence relation holds, i.e., $C_i = \sigma_i(T_i)$, $\Gamma \supseteq \sigma_i(R_i)$, $CT \text{ satisfy } \sigma_i(CR_i)$.

Let U' , \bar{U} be fresh, $R|_{S_r} = merge_R(R_e, R_1, \dots, R_n)$,

$CR|_{S_{cr}} = merge_{CR}(CR_e, CR_1, \dots, CR_n, (T_e.m : \bar{U} \rightarrow U', \emptyset))$, $S = S_e \cup \bar{S} \cup S_r \cup S_{cr} \cup \{\bar{T} <: \bar{U}\}$ and $\sigma = \{U' \mapsto C\} \circ \{U_i \mapsto D_i\}_{i \in [1..n]} \circ \sigma_e \circ \{\sigma_i\}_{i \in [1..n]}$

Then $e.m(\bar{e}) : U \mid S \mid R \mid CR$ holds by rule TC-INV_K.

σ solves S because it solves S_e , \bar{S} , S_r , S_{cr} , and $\{\bar{T}' <: \bar{U}\}$ as shown below:

- $solve(\text{projExt}(CT), S_e) = \sigma_e$ and $\sigma = \{U \mapsto C\} \circ \{U_i \mapsto D_i\}_{i \in [1..n]} \circ \sigma_e \circ \{\sigma_i\}_{i \in [1..n]}$ implies that σ solves S_e
- $\{solve(\text{projExt}(CT), S_i) = \sigma_i\}_{i \in [1..n]}$ and $\sigma = \{U \mapsto C\} \circ \{U_i \mapsto D_i\}_{i \in [1..n]} \circ \sigma_e \circ \{\sigma_i\}_{i \in [1..n]}$ implies that σ solves \bar{S}
- σ solves S_r by Lemm 19.
- $\sigma_e(CR_e)$, $\forall i \in [1..n]$. $\sigma_i(CR_i)$ are ground by IH.
- (*) $\sigma(T_e.m : \bar{U} \rightarrow U', \emptyset)$ is ground because $\sigma(T_e.m : \bar{U} \rightarrow U') = (\sigma(T_e).m : \sigma(\bar{U}) \rightarrow \sigma(U')) = C_e.m : \bar{D} \rightarrow C$ and $C_e.m : \bar{D} \rightarrow C$ is ground.

CT satisfies $\sigma_e(CR_e)$, $\forall i \in [1..n]$. CT satisfies $\sigma_i(CR_i)$ by IH.

(**) CT satisfy $\sigma(T_e.m : \bar{U} \rightarrow U', \emptyset)$ because $mtype(m, C_e, CT) = \bar{D} \rightarrow C$ hence by rule S-METHOD holds that CT satisfy $(C_e.m : \bar{D} \rightarrow C, \emptyset)$, and $\sigma(T_e.m : \bar{U} \rightarrow U') = C_e.m : \bar{D} \rightarrow C$.

As a result σ solves S_{cr} by Lemma 20.

- Since $\{\bar{C} <: \bar{D}\}$ holds and $\sigma(\{\bar{T} <: \bar{U}\}) = \{\bar{C} <: \bar{D}\}$, then $\sigma(\{\bar{T} <: \bar{U}\})$ holds σ is ground solution because

- $\sigma(U')$ is ground because $\sigma(U') = C$
- $\sigma(R_e)$ is ground because $\sigma(R_e) = (\{U' \mapsto C\} \circ \{U_i \mapsto D_i\}_{i \in [1..n]} \circ \sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(R_e) = (\sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(R_e)$ because U' , \bar{U} are defined fresh.
 $(\sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(R_e) = (\{\sigma_i\}_{i \in [1..n]} \circ \sigma_e)(R_e)$ by Corollary 23.
 $(\{\sigma_i\}_{i \in [1..n]} \circ \sigma_e)(R_e) = (\{\sigma_i\}_{i \in [1..n]})(\sigma_e(R_e)) = \sigma_e(R_e)$ because $\sigma_e(R_e)$ is ground by IH.
 $\forall i \in [1..n]$. $\sigma(R_i)$ is ground because $\sigma(R_i) = (\{U' \mapsto C\} \circ \{U_i \mapsto D_i\}_{i \in [1..n]} \circ \sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(R_i) = (\sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(R_i)$ because U' , \bar{U} are defined fresh.
 $(\sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(R_i) = (\sigma_e \circ \{\sigma_j\}_{j \in [1..i-1, i+1..n]} \circ \sigma_i)(R_i)$ by Corollary 23.
 $(\sigma_e \circ \{\sigma_j\}_{j \in [1..i-1, i+1..n]})(\sigma_i(R_i)) = \sigma_i(R_i)$ because $\sigma_i(R_i)$ is ground by IH. As a result $\sigma(R)$ is ground by definition of $merge_R$.
- $\sigma(CR_e)$ is ground because $\sigma(CR_e) = (\{U' \mapsto C\} \circ \{U_i \mapsto D_i\}_{i \in [1..n]} \circ \sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(CR_e) = (\sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(CR_e)$ because U' , \bar{U} are defined fresh.
 $(\sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(CR_e) = (\{\sigma_i\}_{i \in [1..n]} \circ \sigma_e)(CR_e)$ by Corollary 23.
 $(\{\sigma_i\}_{i \in [1..n]} \circ \sigma_e)(CR_e) = (\{\sigma_i\}_{i \in [1..n]})(\sigma_e(CR_e)) = \sigma_e(CR_e)$ because $\sigma_e(CR_e)$ is ground by IH.
 $\forall i \in [1..n]$. $\sigma(CR_i)$ is ground because $\sigma(CR_i) = (\{U' \mapsto C\} \circ \{U_i \mapsto D_i\}_{i \in [1..n]} \circ \sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(CR_i) = (\sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(CR_i)$ because U' , \bar{U} are defined fresh.
 $(\sigma_e \circ \{\sigma_i\}_{i \in [1..n]})(CR_i) = (\sigma_e \circ \{\sigma_j\}_{j \in [1..i-1, i+1..n]} \circ \sigma_i)(CR_i)$ by Corollary 23.

$(\sigma_e \circ \{\sigma_j\}_{j \in [1..i-1,i+1..n]})(\sigma_i(CR_i)) = \sigma_i(CR_i)$ because $\sigma_i(CR_i)$ is ground by *IH*. $\sigma(T_e.m : \overline{U} \rightarrow U, \emptyset)$ is ground by (*). As a result $\sigma(CR)$ is ground by definition of $merge_{CR}$,

The correspondence relation holds because:

- a) $C = \sigma(U)$
- b) $\Gamma \supseteq \sigma(R_e)$ because $\Gamma \supseteq \sigma_e(R_e)$ by *IH*, and from 2) $\sigma(R_e) = \sigma_e(R_e)$. $\forall i \in 1..n$. $\Gamma \supseteq \sigma(R_i)$ because $\Gamma \supseteq \sigma_i(R_i)$ by *IH*, and from 2) $\sigma(R_i) = \sigma_i(R_i)$. As a result $\Gamma \supseteq \sigma(R)$ by definition of $merge_R$.
- c) CT satisfy $\sigma(CR_e)$ because CT satisfy $\sigma_e(CR_e)$, and from 3) $\sigma(CR_e) = \sigma_e(CR_e)$. $\forall i \in 1..n$. CT satisfy $\sigma(CR_i)$ because CT satisfy $\sigma_i(CR_i)$ by *IH*, and from 3) $\sigma(CR_i) = \sigma_i(CR_i)$. CT satisfy $\sigma(T'_e.m : \overline{U} \rightarrow U', \emptyset)$ by (**). As a result CT satisfy $\sigma(CR_e) \cup \sigma(CR_1) \dots \cup \sigma(CR_n) \cup \sigma(T'_e.m : \overline{U} \rightarrow U')$, i.e., CT satisfies $\sigma(CR)$ by Lemma 21.

— Case T-NEW with $\Gamma; CT \vdash new C(\bar{e}) : C$.

By inversion, $\Gamma; CT \vdash \bar{e} : \overline{C}$, $fields(C, CT) = C.init(\overline{D})$ and $\overline{C} <: \overline{D}$.

By *IH*, $\bar{e} : \overline{T} \mid \overline{S} \mid \overline{R} \mid CR$, $\forall i \in 1..n$. $solve(\text{projExt}(CT), S_i) = \sigma_i$, $\sigma_i(T_i)$, $\sigma_i(R_i)$, $\sigma_i(CR_i)$ are ground, and the correspondence relation holds, i.e., $C_i = \sigma_i(T_i)$, $\Gamma \supseteq \sigma_i(R_i)$, CT satisfy $\sigma_i(CR_i)$.

Let \overline{U} be fresh, $merge_R(R_1, \dots, R_n) = R|_{S_r}$,

$CR|_{S_{cr}} = merge_{CR}(CR_1, \dots, CR_n, (C.init(\overline{U}, \emptyset)))$. $S = \overline{S} \cup S_r \cup S_{cr} \cup \{\overline{T} <: \overline{U}\}$ and $\sigma = \{U_i \mapsto D_i\}_{i \in [1..n]} \circ \{\sigma_i\}_{i \in [1..n]}$.

Then $C.init(\bar{e}) : C \mid S \mid R \mid CR$ holds by rule TC-NEW.

σ solves S because it solves \overline{S} , S_r , S_{cr} , and $\{\overline{T} <: \overline{U}\}$ as shown below:

- $\{solve(\text{projExt}(CT), S_i) = \sigma_i\}_{i \in [1..n]}$ and $\sigma = \{U_i \mapsto D_i\}_{i \in [1..n]} \circ \{\sigma_i\}_{i \in [1..n]}$ implies that σ solves \overline{S}
- σ solves S_r by Lemma 19
- $\forall i \in [1..n]$. $\sigma_i(CR_i)$ are ground by *IH*.
- (*) $\sigma(C.init(\overline{U}), \emptyset)$ is ground because $\sigma(C.init(\overline{U})) = (\sigma(C).init(\sigma(\overline{U}))) = C.init(\overline{D})$ and $C.init(\overline{D})$ is ground.
- $\forall i \in [1..n]$. CT satisfies $\sigma_i(CR_i)$ by *IH*.
- (*) CT satisfy $\sigma(C.init(\overline{U}), \emptyset)$ because $fields(C, CT) = \overline{C}.f : \overline{D}$ hence by rule S-CONSTRUCTOR holds that CT satisfy $(C.init(\overline{D}), \emptyset)$, and $\sigma(C.init(\overline{U})) = C.init(\overline{D})$.

As a result σ solves S_{cr} by Lemma 20.

- Since $\{\overline{C} <: \overline{D}\}$ holds and $\sigma(\{\overline{T} <: \overline{U}\}) = \{\overline{C} <: \overline{D}\}$, then $\sigma(\{\overline{T} <: \overline{U}\})$ holds

σ is ground solution because:

- 1) $\sigma(C)$ is ground because C is ground.
- 2) $\forall i \in [1..n]$. $\sigma(R_i)$ is ground because $\sigma(R_i) = (\{U_i \mapsto D_i\}_{i \in [1..n]} \circ \{\sigma_i\}_{i \in [1..n]}) (R_i) = \{\sigma_i\}_{i \in [1..n]}(R_i)$ because \overline{U} are defined fresh.
 $(\{\sigma_i\}_{i \in [1..n]})(R_i) = (\{\sigma_j\}_{j \in [1..i-1,i+1..n]} \circ \sigma_i)(R_i)$ by Corollary 23.
 $(\{\sigma_j\}_{j \in [1..i-1,i+1..n]})(\sigma_i(R_i)) = \sigma_i(R_i)$ because $\sigma_i(R_i)$ is ground by *IH*. As a result $\sigma(R)$ is ground by definition of $merge_R$.
- 3) $\forall i \in [1..n]$. $\sigma(CR_i)$ is ground because $\sigma(CR_i) = (\{U_i \mapsto D_i\}_{i \in [1..n]} \circ \{\sigma_i\}_{i \in [1..n]})(CR_i) = (\{\sigma_i\}_{i \in [1..n]})(CR_i)$ because \overline{U} are defined fresh.
 $(\{\sigma_i\}_{i \in [1..n]})(CR_i) = (\{\sigma_j\}_{j \in [1..i-1,i+1..n]} \circ \sigma_i)(CR_i)$ by Corollary 23.
 $(\{\sigma_j\}_{j \in [1..i-1,i+1..n]})(\sigma_i(CR_i)) = \sigma_i(CR_i)$ because $\sigma_i(CR_i)$ is ground by *IH*. $\sigma(C.init(\overline{U}), \emptyset)$ is ground by (*). As a result $\sigma(CR)$ is ground by definition of $merge_{CR}$.

XX:36 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

The correspondence relation holds because:

- a) $C = \sigma(C)$
 - b) $\forall i \in 1 \dots n. \Gamma \supseteq \sigma(R_i)$ because $\Gamma \supseteq \sigma_i(R_i)$ by *IH*, and from 2) $\sigma(R_i) = \sigma_i(R_i)$. As a result $\Gamma \supseteq \sigma(R)$ by definition of merge_R .
 - c) $\forall i \in 1 \dots n. CT \text{ satisfy } \sigma(CR_i)$ because $CT \text{ satisfy } \sigma_i(CR_i)$ by *IH*, and from 3) $\sigma(CR_i) = \sigma_i(CR_i)$. $CT \text{ satisfy } \sigma(C.\text{init}(\bar{U}), \emptyset)$ by (**).
- As a result $CT \text{ satisfy } \sigma(CR_1) \dots \cup \sigma(CR_n) \cup \sigma(C.\text{init}(\bar{U}), \emptyset)$, i.e., $CT \text{ satisfies } \sigma(CR)$ by Lemma 21.

■ Case T-UCAST with $\Gamma; CT \vdash (C)e : C$.

By inversion, $\Gamma; CT \vdash e : D$ and $D <: C$.

By *IH*, $e : T_e \mid S_e \mid R_e \mid CR_e$, where $\text{solve}(\text{projExt}(CT), S_e) = \sigma_e$, $\sigma_e(T_e)$, $\sigma_e(R_e)$, $\sigma_e(CR_e)$ are ground and the correspondence relation holds, i.e., $D = \sigma_e(T_e)$, $\Gamma \supseteq \sigma_e(R_e)$, $CT \text{ satisfies } \sigma_e(CR_e)$.

Let $\sigma = \sigma_e$, and $S = S_e \cup \{T_e <: C\}$.

Then $(C)e : C \mid S \mid R_e \mid CR_e$ holds by rule T-UCAST.

σ solves S , because it solves S_e , and $\{T_e <: C\}$ as shown below:

- Since $\sigma = \sigma_e$ and σ_e solves S_e then σ solves S_e .
- Since $\{D <: C\}$ holds and $\sigma(\{T_e <: C\}) = \{D <: C\}$ then $\sigma(\{T_e <: C\})$ holds.

σ is ground solution because:

- 1) $\sigma(C)$ is ground because C is ground as a given class in CT
- 2) $\sigma(R_e)$ is ground because $\sigma_e(R_e)$ is ground by *IH* and $\sigma = \sigma_e$
- 3) $\sigma(CR_e)$ is ground because $\sigma_e(CR_e)$ is ground by *IH* and $\sigma = \sigma_e$

The correspondence relation $(C, \Gamma, CT) \triangleright (C, R_e, CR_e, \sigma)$ holds because:

- a) $C = \sigma(C)$
- b) $\Gamma \supseteq \sigma(R_e)$, because $\Gamma \supseteq \sigma_e(R_e)$ by *IH* and $\sigma = \sigma_e$
- c) $CT \text{ satisfy } \sigma(CR_e)$, because $CT \text{ satisfy } \sigma_e(CR_e)$ by *IH* and $\sigma = \sigma_e$

The proof is symmetric for T-DCAST, and T-SCAST, as in the case of T-UCAST.

► **Definition 26** ($CReq(CR)$). $CReq(CR) = \{T.\text{extends} : T' \mid (T.\text{extends} : T', \text{cond}) \in CR\} \cup \{T.\text{init}(\bar{T}) \mid (T.\text{init}(\bar{T}), \text{cond}) \in CR\} \cup \{T.f : T' \mid (T.f : T', \text{cond}) \in CR\} \cup \{T.m : \bar{T} \rightarrow T' \mid (T.m : \bar{T} \rightarrow T', \text{cond}) \in CR\}$

► **Definition 27** (Domain of Class Table Clause).

$$domCl(CTcls) = \begin{cases} (C.\text{extends}) & \text{if } (CTcls) = (C.\text{extends} = D) \\ (C.f) & \text{if } (CTcls) = (C.f : C_f) \\ (C.m) & \text{if } (CTcls) = (C.m : \bar{C} \rightarrow C_r) \\ (C.\text{init}) & \text{if } (CTcls) = (C.\text{init}(\bar{C})) \end{cases} \quad (2)$$

► **Definition 28** (Domain of CT). $dom(CT) = \{domCl(CTcls) \mid CTcls \in CT\}$

► **Definition 29** (translate a class requirements to class table entries). It is given a ground class requirement clause $CReq$.

$$translate(CReq) = \begin{cases} (C.\text{extends} = D) & \text{if } (CReq) = (C.\text{extends} : D) \\ (C.f : C_f) & \text{if } (CReq) = (C.f : C_f) \\ (C.m : \bar{C} \rightarrow C_r) & \text{if } (CReq) = (C.m : \bar{C} \rightarrow C_r) \\ (C.\text{init}(\bar{C})) & \text{if } (CReq) = (C.\text{init}(\bar{C})) \end{cases} \quad (3)$$

► **Definition 30** (translate a class table entry to a class requirement $CReq$). It is given a class table clause $CTcls$.

$$translate^*(CTcls) = \begin{cases} (C.\text{extends} : D) & \text{if } (CTcls) = (C.\text{extends} = D) \\ (C.f : C_f) & \text{if } (CTcls) = (C.f : C_f) \\ (C.m : \bar{C} \rightarrow C_r) & \text{if } (CTcls) = (C.m : \bar{C} \rightarrow C_r) \\ (C.\text{init}(\bar{C})) & \text{if } (CTcls) = (C.\text{init}(\bar{C})) \end{cases} \quad (4)$$

► **Definition 31** (Clauses of supertypes of $CReq$).

$$\{(CReq, CR)\}_{\ll} = \begin{cases} (T.\text{extends} : T') & \text{for } CReq = (T.\text{extends} : T') \\ \{(T.\text{init}(\bar{T}'))\} & \text{for } (T.\text{init}(\bar{T}')) \in CReq(CR) \\ & \wedge CReq = (T.\text{init}(\bar{T})) \wedge \bar{T} <: \bar{T}' \\ \{(T'.f : T'_f)\} & \text{for } (T'.f : T'_f) \in CReq(CR) \\ & \wedge CReq = (T.f : T_f) \wedge T <: T' \\ \{(T'.m : \bar{T}' \rightarrow T'_r)\} & \text{for } (T'.m : \bar{T}' \rightarrow T'_r) \in CReq(CR) \\ & \wedge CReq = (T.m : \bar{T} \rightarrow T_r) \wedge T <: T' \end{cases} \quad (5)$$

► **Definition 32** (Clauses of subtypes of $CReq$).

$$\{(CReq, CR)\}_{\gg} = \begin{cases} (T.\text{extends} : T') & \text{for } CReq = (T.\text{extends} : T') \\ \{(T.\text{init}(\bar{T}'))\} & \text{for } (T.\text{init}(\bar{T}')) \in CReq(CR) \\ & \wedge CReq = (T.\text{init}(\bar{T})) \wedge \bar{T}' <: \bar{T} \\ \{(T'.f : T'_f)\} & \text{for } (T'.f : T'_f) \in CReq(CR) \\ & \wedge CReq = (T.f : T_f) \wedge T' <: T \\ \{(T'.m : \bar{T}' \rightarrow T'_r)\} & \text{for } (T'.m : \bar{T}' \rightarrow T'_r) \in CReq(CR) \\ & \wedge CReq = (T.m : \bar{T} \rightarrow T_r) \wedge T' <: T \end{cases} \quad (6)$$

► **Definition 33** (Clauses of superclasses of CTcls).

$$\{(CTcls, CT)\}_{\ll^*} = \begin{cases} (C.extends : D) & \text{for } CTcls = (C.extends = D) \\ \{(C.init(\bar{C}')\} & \text{for } (C.init(\bar{C}')) \in CT \\ & \quad \wedge CTcls = (C.init(\bar{C})) \wedge \bar{C} <: \bar{C}' \\ \{(D.f : D')\} & \text{for } (D.f : D') \in CT \\ & \quad \wedge CTcls = (C.f : C') \wedge C <: D \\ \{(D.m : \bar{D} \rightarrow D_r)\} & \text{for } (D.m : \bar{D} \rightarrow D_r) \in CT \\ & \quad \wedge CTcls = (C.m : \bar{C} \rightarrow C_r) \wedge C <: D \end{cases} \quad (7)$$

► **Definition 34** (Compatible class requirements). Given two class requirements $CReq, CReq'$, compatibility of two class requirements $CReq \sim CReq'$ is defined over all cases of clauses:

- $(T.extends : T_1) \sim (T'.extends : T_2)$ if $(T = T') \wedge (T_1 = T_2)$
- $T.init(\bar{T}) \sim (T'.init(\bar{T}'))$ if $(T = T')$
- $(T.f : T_f) \sim (T'.f : T'_f)$ if $(T <: T') \vee (T >: T')$
- $(T.m : \bar{T} \rightarrow T_r) \sim (T'.m : \bar{T}' \rightarrow T'_r)$ if $(T <: T') \vee (T >: T')$

► **Definition 35** (Compatibility between a class requirement and a class table clause). Given a class table clause $CTcls$, a class requirement $CReq$, and a ground solution σ , such that $\sigma(CReq)$ ground, compatibility $CReq \sim CReq'$ is defined over all cases of clauses:

- $\sigma(T.extends : T') \sim (C.extends = D)$ if $(\sigma(T) = C) \wedge (\sigma(T) = D)$
- $\sigma(T.init(\bar{T})) \sim (C.init(\bar{C}))$ if $(\sigma(T) = C)$
- $\sigma(T.f : T') \sim (C.f : C')$ if $(\sigma(T) >: C) \vee (\sigma(T) <: C)$
- $\sigma(T.m : \bar{T} \rightarrow T_r) \sim (C.m : \bar{C} \rightarrow C')$ if $(\sigma(T) >: C) \vee (\sigma(T) <: C)$

► **Lemma 36** (Weakening for context). If $\Gamma \vdash t : T$, and $x \notin \text{dom}(\Gamma)$, then $\Gamma; x : C \vdash t : T$.

Proof. Straightforward induction on typing derivations. ◀

► **Lemma 37** (Weakening for a single class requirement). Given CT , a class table clause $CTcls$, a class requirement $(CReq, cond)$ and σ , such that $\sigma(CReq, cond)$ is ground, if CT satisfy $\sigma(CReq, cond)$ and $\forall CTcls' \in \{(CTcls, CT)\}_{\ll^*}$ such that $CTcls' \notin CT$, then $CT \cup CTcls$ satisfy $\sigma(CReq, cond)$.

Proof. We proceed by case analysis on the definition of $CReq$.

- Case $CReq = (T.f : T')$. We consider $\sigma(T.f : T', cond) = (C.f : C', cond_g)$. We have to show that $CT \cup CTcls$ satisfies $(C.f : C', cond_g)$. It is given that CT satisfies $(C.f : C', cond_g)$, therefore by inversion $\text{field}(f, C, CT) = C'$ (rule S-FIELD). To show that the extended class table still satisfies the given class requirement, we distinguish the following cases on the definition of $CTcls$:
 - 1) $CTcls = (D.g : D')$, such that $f \neq g$. Moreover, consider the class table $CT \cup (D.g : D')$. We know that since f is not the same as g :
 $(*) \text{field}(f, C, CT) = \text{field}(f, C, CT \cup (D.g : D')) = C'$.
As a result $CT \cup CTcls$ satisfies $(C.f : C', cond_g)$ by rule S-FIELD and $(*)$.
 - 2) $CTcls = (A.f : A')$. Since by inversion $\text{field}(f, C, CT) = C'$, then there exists D , such that $C <: D$ and $(D.f : C') \in CT$. To proceed with the proof we distinguish two subcases:

- a) A and D belong to the same class hierarchy (subtyping relation).

$$A <: D$$

This case does not hold by the assumption that $\forall(CTcls') \in \{(A.f : A', CT)\}_{\ll^*}$ such that $CTcls' \notin CT$, i.e., D is a supertype of A , and $D.f : C'$ is an existing clause of the class table.

$$A :> D$$

Since $C <: D$, then by transitivity we have $C <: A$. Thus the type of $C.f$ does not depend on the type of $A.f$, because by field lookup rule, the type of $C.f$ is defined by the first supertype we find starting from left to right; since $C <: D <: A$, then $D.f$ is considered to define the type of $C.f$. Moreover, consider the class table $CT \cup (A.f : A')$. We know that since $A :> D$, $A :> C$, from field lookup definition:

$$(*) \text{field}(f, C, CT) = \text{field}(f, C, CT \cup (A.f : A')) = C'.$$

As a result $CT \cup CTcls$ satisfies $(C.f : C', cond_g)$ by $(*)$ and rule S-FIELD.

- b) A and D do not belong to the same class hierarchy (subtyping relation). We consider the class table $CT \cup (A.f : A')$. Since the field declaration for f of class A is unnecessary to define the type of $C.f$, because $C <: D$, and $D \not<: A$, $D \not>: A$, as a result $C \not<: A$, $C \not>: A$, then :

$$(*) \text{field}(f, C, CT) = \text{field}(f, C, CT \cup (A.f : A')) = C'.$$

As a result $CT \cup CTcls$ satisfies $(C.f : C', cond_g)$ by $(*)$ and rule S-FIELD.

- 3) $CTcls$ is different from a field clause.

We consider the class table $CT \cup \text{translate}(CReq')$. We know that since $CReq'$ is different from field clause for class requirements:

$$(*) \text{field}(f, C, CT) = \text{field}(f, C, CT \cup CTcls) = C'.$$

As a result $CT \cup CTcls$ satisfies $(C.f : C', cond_g)$ by $(*)$ and rule S-FIELD.

■ $CReq = (T.m : \overline{U} \rightarrow U')$

◀

► **Lemma 38** (Class Table Weakening). *Given CT , a class table clause $CTcls$, a set of class requirements CR , and a ground solution σ , such that $\sigma(CR)$ is ground, if CT satisfy $\sigma(CR)$ and $\forall CTcls' \in \{(CTcls, CT)\}_{\ll^*}$ such that $CTcls' \notin CT$, then $CT \cup CTcls$ satisfy $\sigma(CR)$.*

Proof. We proceed by mathematical induction on the set of class requirements CR .

Initial step: Show that the lemma holds for one single class requirement, i.e., $CR = \{(CReq, cond)\}$. It is given a class table clause $CTcls$, $\sigma(CReq, cond)$ is ground and CT satisfies $\sigma(CReq, cond)$, then $CT \cup CTcls$ satisfies $\sigma(CReq, cond)$ by Lemma 37.

Inductive step: We suppose that the lemma is true for a set of class requirements $CR = CR'$, i.e., $CT \cup CTcls$ satisfies $\sigma(CR')$, where $\sigma(CR')$ is ground.

We prove the lemma for $CR = (CReq, cond) \cup CR'$, i.e., $CT \cup CTcls$ satisfies $\sigma(CR)$.

Union of class requirements is realized by merge_{CR} function, i.e.,

$CR|_S = \text{merge}(CR', (CReq, cond))$. $\sigma(CReq, cond)$ is ground from the initial step and $\sigma(CR')$ is ground from the inductive step, then $\text{sigma solve } S$ by Lemma 20. $CT \cup CTcls$ satisfies $\sigma(CReq, cond)$ from the initial step, and $CT \cup CTcls$ satisfies $\sigma(CR')$ from the inductive step, as a result $CT \cup CTcls$ satisfies $\sigma(CReq, cond) \cup \sigma(CR')$, i.e., $CT \cup CTcls$ satisfies $\sigma(CR)$ by Lemma 21.

◀

► **Lemma 39** (Compatible clause in CT and not in CR). *Given $CT', CR', (CReq\emptyset), \sigma$, such that $CR|_S = \text{merge}(CR', (CReq, \emptyset))$, σ solves S , and $\sigma(CR)$ is ground, if CT' satisfy $\sigma(CR')$, $\exists(CReq', cond) \in CR'$. $CReq \sim CReq'$, and $\exists CTcls \in CT'$. $\sigma(CReq) \sim CTcls$, then there exists a class table CT , such that CT satisfy $\sigma(CR)$.*

Proof. We proceed by case analyses on the definition of CReq.

- $CReq = (T.f : U)$, and $(D.f : D') \in CT'$ for some D , by assumption. We distinguish two cases regarding the subtyping relation between the CReq and the class table clause:

- 1) $D > \sigma(T)$. Since $(D.f : D') \in CT'$ is already a member of the class table, and D is supertype of $\sigma(T)$, then $\sigma(U) = D'$. We take $CT = CT'$. $\text{field}(f, \sigma(T), CT) = D'$, therefore CT satisfies $(\sigma(T).f : D', \emptyset)$ by rule S-FIELD, i.e., CT satisfies $(\sigma(T).f : D', \emptyset)$, and CT satisfies $\sigma(CR')$, as a result CT satisfies $\sigma(CR)$ by Lemma 21.
- 2) $D <: \sigma(T)$. We take $CT = CT' \cup \text{translate}(\sigma(T.f : U))$, then CT satisfies $\sigma(T.f : U, \emptyset)$ by construction and CT satisfies $\sigma(CR')$ by Class Table Weakening Lemma 38. As a result CT satisfies $\sigma(CR)$ by Lemma 21.

- $CReq = (T.m : \overline{U} \rightarrow U)$ Analogous to the case of field clause.

◀

► **Lemma 40** (Compatible clause in CT and in CR). *Given $CT', CR', (CReq\emptyset), \sigma$, such that $CR|_S = \text{merge}(CR', (CReq, \emptyset))$, σ solves S and $\sigma(CR)$ is ground, if CT' satisfy $\sigma(CR')$, $\exists(CReq', cond) \in CR'$. $CReq \sim CReq'$, $\exists CTcls \in CT'$. $\sigma(CReq) \sim CTcls$, then there exists a class table CT , such that CT satisfy $\sigma(CR)$.*

Proof. We proceed by case analyses on the definition of CReq.

$CReq = (T.f : U)$.

By assumption $(T'.f : T_f, cond') \in CR'$ for some T' , and $(D.f : D') \in CT'$, for some D , $\sigma(T') <: D$. To show that CT satisfies $\sigma(CR)$ we consider the case where $\sigma(cond') \Downarrow \text{true}$ ⁵. $\sigma(cond) \Downarrow \text{true}$, i.e., all conditions in $cond$ do hold. CT' satisfy $\sigma(CR')$, and $(T'.f : T_f, cond') \in CR'$, therefore CT' satisfies $\sigma(T'.f : T_f, cond')$, by inversion $\text{field}(f, T', CT') = D'$ (rule S-FIELD), where $\sigma(T_f) = D'$. We distinguish to cases with respect to the subtyping relation between D and $\sigma(T)$:

- 1) $D > \sigma(T)$
 $D > \sigma(T)$, $D > \sigma(T')$, let us consider $(*)$ $(\sigma(T).extends = D \in CT', (\sigma(T').extends = D) \in CT'$ and $(D.f : D') \in CT'$. The class requirements we are interested in are $(T.f : U, cond)$, $(T'.f : U', cond')$. After applying merging for the two requirements and remove for the two extend clauses the resulting valid requirements, that is the requirements where their conditions hold, are $(D.f : U, cond_t)$ and $(D.f : U', cond_{t'})$ (for sake of brevity we omit the detailed steps and the non interesting requirements for us). Then after applying remove for the field clause results that $\sigma(U) = \sigma(U') = D'$. $\text{field}(f, \sigma(T'), CT') = D' = \sigma(U')$, $\text{field}(f, \sigma(T), CT') = D' = \sigma(U)$, therefore CT' satisfies $\sigma(T.f : U, \emptyset)$ by rule S-FIELD. We take $CT = CT'$. CT satisfies $\sigma(CR')$, and CT satisfies $\sigma(T.f : U, \emptyset)$, as a result CT satisfies $\sigma(CR)$ by Lemma 21.

⁵ We do not consider when it is false because the requirement is not valid requirement and it is a case as in Lemma 39 and the proof follows the same

2) $D <: \sigma(T)$

By transitivity $\sigma(T') <: \sigma(T)$. D is subtype of $\sigma(T)$ and $D.f$ is unnecessary to determine the type of $\sigma(T).f$ by field lookup rule. We take $CT = CT' \cup \text{translate}(\sigma(T.f : U))$. CT satisfies $\sigma(T.f : U, \emptyset)$ by class table construction, and $\sigma(T') <: D <: \sigma(T)$ then CT satisfies $\sigma(CR')$ by Class Table Weakening Lemma 38.

As a result CT satisfies $\sigma(CR)$ by Lemma 21.

$CReq = (T.m : \overline{U} \rightarrow U)$ Proof is analogous to case field clause. \blacktriangleleft

► **Lemma 41** (Add Clause Definition in CT). *Given a class table clause $CTcls$ declaration, a class table CT and a ground set of requirements CR , if $CTcls \notin CT$, and CT satisfies CR , then $CT \cup CTcls$ satisfies CR*

Proof. Tedious but straightforward. \blacktriangleleft

► **Theorem 42** (Equivalence of expressions: \Leftrightarrow). *Given e, T, S, R, CR, Σ , if $e : T \mid S \mid R \mid CR$, $\text{solve}(\Sigma, S) = \sigma$, and σ is a ground solution, then there exists C, Γ, CT , such that $\Gamma; CT \vdash e : C$, $(C, \Gamma, CT) \triangleright \sigma(T, R, CR)$ and $\text{projExt}(CT) = \Sigma$.*

We proceed by induction on the typing derivation.

■ Case TC-VAR with $x : U \mid \emptyset \mid x : U \mid \emptyset$

Let σ be a ground solution, such that $\sigma(U)$ is ground by assumption.

By inversion, U is fresh, $S = \emptyset$, $R = \{x : U\}$, $CR = \emptyset$.

By IH, $\Gamma_x = \{x : \sigma(U)\}$

Let $\sigma(U) = C$, for some C we know it is ground.

Then $\Gamma; CT \vdash x : C$ by rule $T - Var$, and the correspondence relation holds:

a) $\sigma(U) = C$

b) We take $\Gamma = \Gamma_x$, and $\Gamma = \{x : C\} \supseteq \sigma(R) = \sigma(\{x : U\})$.

c) We take $CT = \emptyset$, since $CR = \emptyset$, and $\sigma(CR) = \emptyset$, then CT satisfies $\sigma(CR)$

■ Case TC-FIELD with $e.f_i : U \mid S \mid R_e \mid CR$

Let $S = S_e \cup S_f$, σ be a ground solution, such that $\text{solve}(S, \Sigma) = \sigma$, i.e., it solves S_e, S_f , and $\sigma(U), \sigma(R_e), \sigma(CR)$ are ground by assumption.

By inversion, $e : T_e \mid S_e \mid R_e \mid CR_e$, $\sigma(T_e), \sigma(R_e), \sigma(CR_e)$ are ground. $CR|_{S_f} = \text{merge}_{CR}(CR_e, (T_e.f_i : U, \emptyset))$, and U is fresh.

By IH, $\Gamma_e; CT_e \vdash e : C_e$, the correspondence relation holds, i.e., $C_e = \sigma(T_e)$, $\Gamma_e \supseteq \sigma(R_e)$, CT_e satisfy $\sigma(CR_e)$. $\text{projExt}(CT_e) = \Sigma_e$

Let $C_i = \sigma(U)$, for some C_i we know is ground.

We consider three cases to construct the class table CT :

- (1) $\{(C_e.f : C_i, CT_e)\}_{\ll^*} = \emptyset$. Since no entry of class C_e or its superclasses exist for field f in the given class table CT_e , we add a new entry in the class table, i.e., $CT = CT_e \cup (C_e.f : C_i)$.
- (2) $\{(T'_e.f : U, CR_e)\}_{\ll} \cup \{(T'_e.f : U, CR_e)\}_{\gg} = \emptyset$, $(D.f : D') \in CT_e$ for some D, D' , then by Lemma 39 CT is constructed.
- (3) $(T'.f : T_f, cond') \in CR_e$, for some T' , $cond'$, $(D.f : D') \in CT_e$ for some D, D' , $\sigma(T') <: D$, then by Lemma 40 CT is constructed.

From above we have that $\text{field}(f_i, C_e, CT) = C_i$, and no extends clauses are added to the class table CT_e , therefore $\text{projExt}(CT) = \Sigma_e = \Sigma$.

Then $\Gamma; CT \vdash e.f_i : C_i$ holds by rule $T\text{-FIELD}$, and the correspondence relation holds because:

a) $\sigma(U) = C_i$

XX:42 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

- b) We take $\Gamma = \Gamma_e$, and $\Gamma \supseteq \sigma(R_e)$ by IH .
 - c) What it is left to be shown is that CT satisfy $\sigma(CR)$, we distinguish the following cases depending on the class table construction:
 - (1)' In addition to (1), $\sigma(T'_e.f : U) = \sigma(T'_e).f : \sigma(U) = C_e.f : C_i$, therefore CT satisfy $\sigma(T'_e.f : U, \emptyset)$ by construction of CT .
 CT_e satisfies $\sigma(CR_e)$ by IH , and $\{(C_e.f : C_i)\}_{\ll^*} \notin CT_e$ therefore CT satisfies $\sigma(CR_e)$ by Class Table Weakening Lemma 38.
As a result CT satisfy $\sigma(CR_e) \cup \sigma(T'_e.f : U, \emptyset)$, i.e., CT satisfy $\sigma(CR)$ by Lemma 21.
 - (2)' In addition to (2), CT_e satisfy $\sigma(CR_e)$ by IH , then there is CT , CT satisfy $\sigma(CR)$ by Lemma 39.
 - (3)' In addition to (3), CT_e satisfy $\sigma(CR_e)$ by IH , then there is CT , CT satisfy $\sigma(CR)$ by Lemma 40.
- Case $TC\text{-INVK}$ with $e.m(\bar{e}) : U \mid S \mid R \mid CR$.
Let $S = S_e \cup \bar{S} \cup S_r \cup S_s \cup S_{cr} \cup \{\bar{T} <: \bar{U}\}$, and σ be a ground solution, such that it solves S , i.e., σ solves $S_e, \bar{S}, S_s, S_{cr}, \{\bar{T} <: \bar{U}\}$, and $\sigma(U'), \sigma(R), \sigma(CR)$ are ground.
By inversion, $e : T_e \mid S_e \mid R_e \mid CR_e, \sigma(T_e), \sigma(R_e), \sigma(CR_e)$ are ground, $\bar{e} : \bar{T} \mid \bar{S} \mid \bar{R} \mid \bar{CR}, \forall i \in [1..n]. \sigma(T_i), \sigma(R_i), \sigma(CR_i)$ are ground, $R|_{S_r} = merge_R(R_e, R_1, \dots, R_n), CR'|_{S_s} = merge_{CR}(CR_e, CR_1, \dots, CR_n), CR|_{S_{cr}} = merge_{CR}(CR', (T_e.m : \bar{U} \rightarrow U', \emptyset))$, and U', \bar{U} are fresh.
By IH , $\Gamma_e; CT_e \vdash e : C_e$, the correspondence relation holds, with $C_e = \sigma(T_e), \Gamma_e \supseteq \sigma(R_e), CT_e$ satisfy $\sigma(CR_e)$. $\text{projExt}(CT_e) = \Sigma_e$
By IH , $\bar{T}; \bar{CT} \vdash \bar{e} : \bar{C}$, the correspondence relation holds, $\forall i \in [1..n]. C_i = \sigma(T'_i), \Gamma_i \supseteq \sigma(R_i), CT_i$ satisfy $\sigma(CR_i)$. $\text{projExt}(CT_s) = \Sigma_s$, where:

$$\Gamma_s = \bigcup_{i \in [1..n]} \{\Gamma_i\} \quad CT_s = \bigcup_{i \in [1..n]} \{CT_i\}$$

(*) $\{freshU(CT_e) \cap freshU(CT_s)\} = \emptyset$, and $\bigcap_{i \in [1..n]} \{freshU(CT_i)\} = \emptyset$, by Proposition 22. $\{CT_e \cup CT_s\}$ satisfies $\sigma(CR_e)$.
 $\forall i \in [1..n]. \{CT_e \cup CT_s\}$ satisfies $\sigma(CR_i)$ by Class Table Weakening Lemma 38, therefore $\{CT_e \cup CT_s\}$ satisfy $\sigma(CR_e) \cup \sigma(CR_1) \dots \cup \sigma(CR_n)$, i.e.,
 $\{CT_e \cup CT_s\}$ satisfy $\sigma(CR')$ by Lemma 21.

Let $C = \sigma(U')$, $\bar{D} = \sigma(\bar{U})$ for some C, \bar{D} we know are ground. $\bar{C} <: \bar{D}$ holds because $\sigma(\{\bar{T} <: \bar{U}\})$ holds.

We consider three cases to construct the class table CT :

- (1) $\{(C_e.m : \bar{D} \rightarrow C, \{CT_e \cup CT_s\})\}_{\ll^*} = \emptyset$. Since no entry of class C_e or its superclasses exist for method m in the given class table $\{CT_e \cup CT_s\}$, we add a new entry in the class table, i.e., $CT = \{CT_e \cup CT_s\} \cup \{C_e.m : \bar{D} \rightarrow C\}$.
- (2) $\{(T_e.m : \bar{U} \rightarrow U', CR')\}_{\ll} \cup \{(T_e.m : \bar{U} \rightarrow U', CR')\}_{\gg} = \emptyset, (D.m : \bar{D} \rightarrow D') \in \{CT_e \cup CT_s\}$ for some D, \bar{D}, D' , then by Lemma 39 CT is constructed.
- (3) $(T'.m : \bar{T} \rightarrow T_r, cond') \in CR'$, for some $T', \bar{T}, T_r, cond', (D.m : \bar{D} \rightarrow D') \in \{CT_e \cup CT_s\}$ for some D, \bar{D}, D' , $\sigma(T') <: D$, then by Lemma 40 CT is constructed.

From above we have that $mtype(m, C_e, CT) = \bar{D} \rightarrow C$, and no extends clauses are added to the class table $\{CT_e \cup CT_s\}$, therefore $\text{projExt}(CT) = \Sigma_e \cup \Sigma_s = \Sigma$.

Then $\Gamma; CT \vdash e.m(\bar{e}) : C$ holds by rule $T\text{-INVK}$, and the correspondence relation holds because:

- a) $C = \sigma(U)$
- b) We take $\Gamma = \Gamma_e \cup \Gamma_s$, $\Gamma \supseteq \sigma(R_e)$, because $\Gamma_e \supseteq \sigma(R_e)$ by IH and Context Weakening Lemma 36, $\Gamma \supseteq \sigma(R_1) \dots \Gamma \supseteq \sigma(R_n)$, because $\Gamma_i \supseteq R_i$ by IH and Context Weakening Lemma 36, therefore $\Gamma \supseteq \sigma(R)$ by definition of merge_R .
- c) What is left to be shown is that CT satisfy $\sigma(CR)$. We distinguish the following cases:
 - (1)' In addition to (1), $\sigma(T_e.m : \bar{U} \rightarrow U') = \sigma(T_e).m : \sigma(\bar{U}) \rightarrow \sigma(U') = C_e.m : \bar{D} \rightarrow C$ therefore CT satisfy $\sigma(T_e.m : \bar{U} \rightarrow U', \emptyset)$ by construction of CT . $\{CT_e \cup CT_s\}$ satisfies $\sigma(CR')$ by (*) therefore CT satisfies $\sigma(CR')$ by Class Table Weakening Lemma 38.
As a result CT satisfy $\sigma(CR') \cup \sigma(T'_e.m : \bar{U} \rightarrow U, \emptyset)$, i.e.,
 CT satisfy $\sigma(CR)$ by Lemma 21.
 - (2)' In addition (2), $\{CT_e \cup CT_s\}$ satisfy $\sigma(CR')$ by (*), then there is CT ,
 CT satisfy $\sigma(CR)$ by Lemma 39.
 - (3)' In addition to (3) , $\{CT_e \cup CT_s\}$ satisfy $\sigma(CR')$ by (*), then there is CT ,
 CT satisfy $\sigma(CR)$ by Lemma 40.

■ Case TC-NEW with new $C(\bar{e}) : C \mid S \mid R \mid CR$

Let $S = \bar{S} \cup S_r \cup S_{cr} \cup \{\bar{T} <: \bar{U}\}$, σ be a ground solution, such that it solves S , i.e., σ solves $\bar{S}, S_r, S_{cr}, \{\bar{T} <: \bar{U}\}$, and $\sigma(C), \sigma(R), \sigma(CR)$ are ground.

By inversion, $\bar{e} : \bar{T} \mid \bar{S} \mid \bar{R} \mid \bar{CR}, \forall i \in [1..n]. \sigma(T_i), \sigma(R_i), \sigma(CR_i)$ are ground, $R|_{S_r} = \text{merge}_R(R_1, \dots, R_n), CR_s|_{S_s} = \text{merge}_{CR}(CR_1, \dots, CR_n), CR|_{S_{cr}} = \text{merge}_{CR}(CR_s, (C.\text{init}(\bar{U}), \emptyset))$, and $\{U_i\}_{i \in [1..n]}$ are fresh.

By IH, $\bar{\Gamma}; \bar{CT} \vdash \bar{e} : \bar{C}$, the correspondence relation holds, $\forall i \in [1..n]. C_i = \sigma(T_i), \Gamma_i \supseteq \sigma(R_i), CT_i$ satisfy $\sigma(CR_i)$. $\text{projExt}(CT_s) = \Sigma_s$, where:

$$\Gamma_s = \bigcup_{i \in [1..n]} \{\Gamma_i\} \quad CT_s = \bigcup_{i \in [1..n]} \{CT_i\}$$

(*) $\bigcap_{i \in [1..n]} \{freshU(CT_i)\} = \emptyset$, by Proposition 22.

$\forall i \in 1 \dots n. CT_s$ satisfies $\sigma(CR_i)$ by Class Table Weakening Lemma 38, therefore

CT_s satisfies $\sigma(CR_1) \dots \cup \sigma(CR_n)$, i.e., CT_s satisfies $\sigma(CR_s)$ by Lemma 21.

Let $\{U_i = D_i\}_{i \in [1..n]}$ for some C, \bar{D} we know are ground. $\bar{C} <: \bar{D}$ holds because $\sigma(\bar{T} <: \bar{U})$ holds.

We consider three cases to construct the class table CT :

- (1) $\{(C.\text{init}(\bar{D}), CT_s)\}_{\ll^*} = \emptyset$. Since no entry of class C exist for the constructor init in the given class table CT_s , we add a new entry in the class table, i.e., $CT = CT_s \cup (C.\text{init}(\bar{D}))$.
- (2) $\{(C.\text{init}(\sigma(\bar{U})), \sigma(CR_s))\}_{\ll} \cup \{(C.\text{init}(\sigma(\bar{U})), \sigma(CR_s))\}_{\gg} = \emptyset$,
 $(C.\text{init}(\bar{D}')) \in CT_s$, for some \bar{D}' , then by Lemma 39 CT is constructed.
- (3) $\{(C.\text{init}(\sigma(\bar{U}')), \sigma(cond')) \in \sigma(CR_s)$, for some $\bar{U}', cond'$, $(C.\text{init}(\bar{D}')) \in CT_s$, for some \bar{D}' , then by Lemma 40 CT is constructed.

From above we have that $fields(C, CT) = C.\text{init}(\bar{D})$, and no extends clauses are added to the class table CT_s , therefore $\text{projExt}(CT) = \Sigma_s = \Sigma$.

Then $\Gamma; CT \vdash C.\text{init}(\bar{e}) : C$ holds, the correspondence relation holds because:

- a) $C = \sigma(C)$
- b) We take $\Gamma = \Gamma_s$. $\Gamma_1 \supseteq \sigma(R_1) \dots \Gamma_n \supseteq \sigma(R_n)$ by IH, then by Context Weakening Lemma 36 $\Gamma \supseteq \sigma(R)$ by definition of merge_R .

XX:44 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

- c) What is left to be shown is that CT satisfy $\sigma(CR)$. We distinguish the following cases:
- (1)' In addition to (1), $\sigma(C.init(\bar{U})) = \sigma(C).init(\sigma(\bar{U})) = C.init(\bar{D})$ therefore CT satisfy $\sigma(C.init(\bar{U}), \emptyset)$ by construction of CT .
 CT_s satisfies $\sigma(CR_s)$ by (*), therefore CT satisfies $\sigma(CR_s)$ by Class Table Weakening Lemma 38. As a result CT satisfy $\sigma(CR_s) \cup \sigma(C.init(\bar{U}), \emptyset)$, i.e., CT satisfy $\sigma(CR)$ by Lemma 21.
 - (2)' In addition to (2), CT_s satisfy $\sigma(CR_s)$ by (*), then there is CT , CT satisfy $\sigma(CR)$ by Lemma 39.
 - (3)' In addition to (2), $\sigma(\bar{U}') <: \bar{D}'$, and CT_s satisfy $\sigma(CR_s)$ by (*), then there is CT , CT satisfy $\sigma(CR)$ by Lemma 40.

■ Case TC-UCAST with $(C)e : C \mid S \mid R_e \mid CR_e$

Let $S = S_e \cup \{T'_e <: C\}$, σ be a ground solution, such that it solves S , i.e., σ solves S_e , $\{T'_e <: C\}$, and $\sigma(C)$, $\sigma(R_e)$, $\sigma(CR_e)$ are ground.

By inversion, $e : T_e \mid S_e \mid R_e \mid CR_e$, $\sigma(T_e)$, $\sigma(R_e)$, $\sigma(CR_e)$ are ground.

By IH, $\Gamma_e; CT_e \vdash e : D$, and the correspondence relation holds, i.e., $C_e = \sigma(T_e)$, and $\Gamma_e \supseteq \sigma(R_e)$, CT_e satisfy $\sigma(CR_e)$. $\text{projExt}(CT_e) = \Gamma_e$
 $D <: C$ holds because $\sigma(\{T_e <: C\})$ holds.

Then $\Gamma; CT \vdash (C)e : C$ holds by rule T-UCAST, the correspondence relation holds because:

- a) $C = \sigma(C)$
- b) $\Gamma = \Gamma_e$, $\Gamma \supseteq \sigma(R_e)$ by IH
- c) $CT = CT_e$, CT satisfy $\sigma(CR_e)$ by IH

From above we have that no extends clauses are added to the class table CT_e , therefore $\text{projExt}(CT) = \Sigma_e = \Sigma$.

The proof is symmetric for T-DCAST, and T-SCAST, as in the case of T-UCAST.



► **Definition 43** (Correspondence relation for methods). Given judgments $C; CT \vdash C_0 m(\bar{C} \bar{x})\{\text{return } e\} OK$, $C_0 m(\bar{C} \bar{x})\{\text{return } e\}$

$OK | S | T | CR$, and $\text{solve}(\Sigma, S) = \sigma$, where $\text{projExt}(CT) = \Sigma$. The correspondence relation between CT and CR, written $(C, CT) \triangleright_m \sigma(T, CR)$, is defined as

- a) $C = \sigma(T)$
- b) CT satisfy $\sigma(CR)$

► **Theorem 44** (Equivalence of methods: \Rightarrow). Given m , C , CT , if $C; CT \vdash C_0 m(\bar{C} \bar{x})\{\text{return } e\} OK$, then there exists S , T , CR , Σ , σ , where $\text{projExt}(CT) = \Sigma$ and $\text{solve}(\Sigma, S) = \sigma$, such that $C_0 m(\bar{C} \bar{x})\{\text{return } e_0\} OK | S | T | CR$ holds, σ is a ground solution and $(C, CT) \triangleright_m \sigma(T, CR)$ holds.

Proof. By induction on the typing judgment.

Case T-METHOD with $C; CT \vdash C_0 m(\bar{C} \bar{x})\{\text{return } e\} OK$.

By inversion, $\bar{x} : \bar{C}; this : C; CT \vdash e : E_0$, $\{E_0 <: C_0\}$, $\text{extends}(C, CT) = D$, i.e., $(C.\text{extends} = D) \in CT$ by rule EXTENDS, and if $\text{mtype}(m, D, CT) = \bar{D} \rightarrow D_0$, then $\bar{C} = \bar{D}$; $C_0 = D_0$.

By Theorem 25, $e_0 : T_e | S_e | R_e | CR_e$, where $\text{solve}(\text{projExt}(CT), S_e) = \sigma_e$, $\sigma_e(T_e)$, $\sigma_e(R_e)$, $\sigma_e(CR_e)$ are ground and the relation holds, i.e., $E_0 = \sigma_e(T_e)$, $\{\bar{x} : \bar{C}; this : C\} \supseteq \sigma_e(R_e)$, CT satisfy $\sigma_e(CR_e)$.

We define the set of constraints S' and the solution σ' depending on the occurrence of $\bar{x}, this$ in R_e , and U_c is fresh.

- If $\bar{x} \in \text{dom}(R_e)$ and $this \in \text{dom}(R_e)$, then $\{R_e(x_i) = U_i\}_{i \in [1..n]}$, $R_e(this) = U_c$, for \bar{U} fresh. We choose $S' = \{C_i = R_e(x_i)\}_{i \in [1..n]}; \{C = R_e(this)\}$, $\sigma' = \{U_c \mapsto C\} \circ \{U_i \mapsto C_i\}_{i \in [1..n]}$.
- If $\bar{x} \in \text{dom}(R_e)$ and $this \notin \text{dom}(R_e)$, then $\{R_e(x_i) = U_i\}_{i \in [1..n]}$, for \bar{U} fresh. We choose $S' = \{C_i = R_e(x_i)\}_{i \in [1..n]}$, $\sigma' = \{U_c \mapsto C\} \circ \{U_i \mapsto C_i\}_{i \in [1..n]}$.
- If $\bar{x} \notin \text{dom}(R_e)$ and $this \in \text{dom}(R_e)$, then $R_e(this) = U_c$. We choose $S' = \{C = R_e(this)\}$, $\sigma' = \{U_c \mapsto C\}$.
- If $\bar{x} \notin \text{dom}(R_e)$ and $this \notin \text{dom}(R_e)$. We choose $S' = \emptyset$, $\sigma' = \{U_c \mapsto C\}$.

In all the cases above we have $\{U_c \mapsto C\}$, regardless the occurrence of $this$ in R_e , because U_c serves as a placeholder for the current class where the method m is declared as part of.

Let U_d be fresh, $R = R_e - this - \bar{x}$, $CR|_{S_{cr}} = \text{merge}_{CR}(CR_e, (U_c.\text{extends} : U_d, \emptyset), (U_d.m : \bar{C} \rightarrow C_0, \emptyset)_{opt})$, $S = S_e \cup \{T_e <: C_0\} \cup S_{cr} \cup S'$, $\sigma = \{U_d \mapsto D\} \circ \sigma' \circ \sigma_e$.

We show why R is \emptyset . The intuition behind it is that we know the actual types of the parameters since we have method declaration for m , and we know the actual type of $this$ since it is given the current class C where method m is declared as part of. $\Gamma \supseteq \sigma(R_e)$ by IH, i.e., all possible elements in R_e are \bar{X} , $this$ and $\Gamma = \{\bar{x} : \bar{C}; this : C\} - \bar{x} - this = \emptyset$, therefore $R = R_e - \bar{x} - this = \emptyset$.

Then $C_0 m(\bar{C} \bar{x})\{\text{return } e_0\} OK | S | U_c | CR$ holds by rule T-METHOD.

σ solves S because it solves S_e , S' , S_{cr} , and $\{T_e <: C_0\}$ as shown below:

- $\text{solve}(\text{projExt}(CT), S_e) = \sigma_e$ and $\sigma = \{U_d \mapsto D\} \circ \sigma' \circ \sigma_e$ implies that σ solves S_e
- σ solves S' by Lemma 19.

- $\sigma_e(CR_e)$ is ground by Theorem 25.

(*) $\sigma(U_c.\text{extends} : U_d, \emptyset)$ is ground because $\sigma(U_c.\text{extends} : U_c) = (C.\text{extends} : D)$ and $C.\text{extends} : D$ is ground.

(**) $\sigma((U_d.m : \bar{C} \rightarrow C_0, \emptyset)_{opt})$ is ground because $\sigma(U_d.m : \bar{C} \rightarrow C_0) = (\sigma(U_d).m :$

$\sigma(\bar{C}) \rightarrow \sigma(C_0)) = D.m : \bar{C} \rightarrow C_0$ and $D.m : \bar{C} \rightarrow C_0$ is ground.

CT satisfies $\sigma_e(CR_e)$ by Theorem 25.

(\star) CT satisfy $\sigma(U_c.\text{extends} : U_d, \emptyset)$ because $(C.\text{extends} = D) \in CT$ hence by rule S-EXTENDS holds that CT satisfy $(C.\text{extends} : D, \emptyset)$, and $\sigma(U_c.\text{extends} : U_d) = (C.\text{extends} : D)$.

To show that CT satisfy $\sigma((U_d.m : \bar{C} \rightarrow C_0, \emptyset)_{opt})$ we distinguish the following cases:

(\star') if $mtype(m, D, CT) = \bar{D} \rightarrow D_0$ is true then the optional class requirement $(U_d.m : \bar{C} \rightarrow C_0)_{opt}$ is considered and $\bar{C} = \bar{D}, C_0 = D_0$, i.e., type of m declared in D is the same as the type of m declared in C . $\sigma(U_d.m : \bar{D} \rightarrow D_0) = D.m : \bar{D} \rightarrow D_0$ and $mtype(m, D, CT) = \bar{D} \rightarrow D_0 = \bar{C} \rightarrow C_0$, therefore by rule S-METHOD holds that CT satisfy $\sigma(U_d.m : \bar{C} \rightarrow C_0, \emptyset)$.

(\star'') if $mtype(m, D, CT) = \bar{D} \rightarrow D_0$ is false, then the optional class requirement $(U_d.m : \bar{C} \rightarrow C_0)_{opt}$ is not considered. It is satisfiable by default since it is a not valid class requirement.

As a result σ solves S_{cr} by Lemma 20.

- Since $\{E_0 <: C_0\}$ holds and $\sigma(\{T_e <: C_0\}) = \{E_0 <: C_0\}$, then $\sigma(\{T_e <: C_0\})$ holds.

σ is ground solution because:

- 1) $\sigma(U)$ is ground because $\sigma(U) = C$ and C is ground.
- 2) $\sigma(CR_e)$ is ground because $\sigma(CR_e) = (\{U_d \rightarrow D\} \circ \sigma' \circ \sigma_e)(CR_e) = (\{U_d \rightarrow D\} \circ \sigma')(\sigma_e(CR_e)) = \sigma_e(CR_e)$ because $\sigma_e(CR_e)$ is ground by Theorem 25.
- 3) $\sigma(U_c.\text{extends} : U_d, \emptyset)$ is ground by (*). $\sigma((U_d.m : \bar{C} \rightarrow C_0, \emptyset)_{opt})$ is ground by (**). As a result $\sigma(CR)$ is ground by definition of merge_{CR} .

The correspondence relation holds because:

- a) $C = \sigma(U_c)$
- b) CT satisfies $\sigma(CR_e)$ because CT satisfies $\sigma_e(CR_e)$ by Theorem 25 and from 3) $\sigma(CR_e) = \sigma_e(CR_e)$. CT satisfy $\sigma(U_c.\text{extends} : U_d, \emptyset)$ by (\star). To show that CT satisfy $\sigma(CR)$, is left to scrutinize CT satisfy $\sigma((U_d.m : \bar{C} \rightarrow C_0, \emptyset)_{opt})$. We distinguish the following cases:
 - if $mtype(m, D, CT) = \bar{D} \rightarrow D_0$ is true then CT satisfy $\sigma(U_d.m : \bar{C} \rightarrow C_0, \emptyset)$ by (\star'). As a result CT satisfies $\sigma(CR_e) \cup \sigma(U_c.\text{extends} : U_d, \emptyset) \cup \sigma(U_d.m : \bar{C} \rightarrow C_0, \emptyset)$, i.e., CT satisfy $\sigma(CR)$ by Lemma 21.
 - if $mtype(m, D, CT) = \bar{D} \rightarrow D_0$ is false, then is not considered from (\star''). As a result CT satisfies $\sigma(CR_e) \cup \sigma(U_c.\text{extends} : U_d, \emptyset)$, i.e., CT satisfy $\sigma(CR)$ by Lemma 21.

◀

► **Theorem 45** (Equivalence of methods: \leftrightarrow). Given m, T, S, CR, Σ , if $C_0 m(\bar{C} \bar{x}) \{\text{return } e\}$ {return e } $OK | S | T | CR$, solve(Σ, S) = σ , and σ is a ground solution, then there exists C, CT , such that $C; CT \vdash C_0 m(\bar{C} \bar{x}) \{\text{return } e\}$ OK holds, $(C, CT) \triangleright_m \sigma(T, CR)$ and $\text{projExt}(CT) = \Sigma$.

Proof. By induction of the typing judgment, and case analysis of the class table construction.

Case TC-METHOD with $C_0 m(\bar{C} \bar{x}) \{\text{return } e\}$ $OK | S | U_c | CR$.

Let $S = S_e \cup \{T_e <: C_0\} \cup S_c \cup S_{cr} \cup S_x$, σ be a ground solution, such that $\text{solve}(\Sigma, S) = \sigma$, i.e., σ solves $S_e, S_x, S_{cr}, S_c, \{T_e <: C_0\}$, and $\sigma(U_c), \sigma(CR)$ are ground.

By inversion, $e : T_e | S_e | R_e | CR_e, \sigma(T_e), \sigma(R_e), \sigma(CR_e)$ are ground. $CR'|_{S'} = \text{merge}_{CR}(CR_e, (U_c.\text{extends} : U_d, \emptyset))$ $CR|_{S_{cr}} = \text{merge}_{CR}(CR', (U_d.m : \bar{C} \rightarrow C_0, \emptyset)_{opt})$, where U_c, U_d are fresh, $R_e - \text{this} - \bar{x} = \emptyset$. σ solves S' by Lemma 19.

By Theorem 42, $\Gamma_e; CT_e \vdash e : E_0$, the correspondence relation holds, i.e., $E_0 = \sigma(T_e)$, $\Gamma_e \supseteq \sigma(R_e)$, CT_e satisfy $\sigma(CR_e)$. $\Gamma_e = \{\bar{x} : \bar{C}; this : C\}$, because $R_e - this - \bar{x} = \emptyset$ and $\Gamma_e \supseteq \sigma(CR_e)$. $\text{projExt}(CT_e) = \Sigma_e$

Let $C = \sigma(U_c)$, $D = \sigma(U_d)$ for some C , D we know are ground. $E_0 <: C_0$ holds because $\sigma(T_e) <: C_0$ holds.

Context empty because $\Gamma_e - \{\bar{x} : \bar{C}; this : C\} = \emptyset$.

We proceed by construction of the class table in steps.

First we consider three cases to construct the class table CT' with respect to the requirement for *extends*:

- (1) **clause not in class table.** $(C.\text{extend} = D) \notin CT_e$, then
 $CT' = CT_e$; $(C.\text{extends} = D)$.
- (2) **clause in class table, but not in class requirements.** $(C.\text{extends} = D) \in CT_e$, and $(U_c.\text{extends} : U_d, \emptyset) \notin CR_e$, then $CT' = CT_e$.
- (3) **clause in class table and class requirements.** $(C.\text{extends} = D) \in CT_e$, and $(U_c.\text{extends} : U_d, \emptyset) \in CR_e$ is not a valid case, because U_c is defined fresh and in CR_e we do not have existing requirements regarding U_c for extend, because in method body we can have recursive method call or field access and not in extends, i.e., *this* can invoke the method itself or other methods and fields but not extends.

From above and by rule EXTENDS we have that $\text{extends}(C, CT') = D$, an extends is added to the class table CT_e , therefore $\text{projExt}(CT') = \Sigma_e \cup (C, D) = \Sigma'$

Second we consider three cases to construct the class table CT' with respect to the requirement for method m :

- (4) **clauses of superclasses not in class table.** $\{(D.m : \bar{D} \rightarrow D_0, CT')\}_{\ll^*} = \emptyset$, then $CT = CT'$
- (5) **compatible clauses in class table, but not in class requirements.** $\{(D.m : \bar{C} \rightarrow C', CR_e)\}_{\ll} \cup \{(D.m : \bar{D} \rightarrow D', CR_e)\}_{\gg} = \emptyset$, $(D'.m : \bar{D}' \rightarrow D_r) \in CT'$ for some D', \bar{D}', D_r , then by Lemma 39 CT' is constructed.
- (6) **compatible clauses in class table, and in class requirements.** $(D'.m : \bar{D}' \rightarrow D_r) \in CT'$ for some D', \bar{D}', D_r , and $(U_d.m\bar{C} \rightarrow C_0, \emptyset) \in CR_e$ is not a valid case because U_d is defined fresh and $U_d \neq R_e(this)$, i.e., it is possible to have in the body of m *this.m*, but it is impossible to have recursive call of m invoked by U_d , as it is defined fresh and different type than *this*.

From above we have that if $\text{mtype}(m, D, CT) = \bar{D} \rightarrow D_0$ then $\bar{C} = \bar{D}$; $C_0 = D_0$, no extends clauses are added to the class table CT' , therefore $\text{projExt}(CT) = \Sigma' = \Sigma$

Then $C; CT \vdash C_0 m(\bar{C} \bar{x})\{\text{return } e\}$ OK holds by rule T-METHOD, the correspondence relation holds because:

- a) $C = \sigma(U_c)$
- b) What is left to be shown is that CT satisfy $\sigma(CR)$, first we start by showing CT' satisfy $\sigma(CR')$ and we distinguish the following cases:
 - (1)' In addition to (1) $\sigma(U_c.\text{extends} : U_d) = \sigma(U_c).\text{extends} : \sigma(U_d) = C.\text{extends} : D$ therefore CT' satisfy $\sigma(U_c.\text{extends} : U_d, \emptyset)$ by construction. CT_e satisfies $\sigma(CR_e)$ by Theorem 42, and $\sigma(U_c.\text{extends} : U_d) \notin CT_e$, therefore CT' satisfies $\sigma(CR_e)$ by Class Table Weakening Lemma 38.

XX:48 A Co-contextual Type Checker for Featherweight Java (incl. Proofs)

As a result $CT' \text{ satisfy } \sigma(CR_e) \cup \sigma(U_c.\text{extends} : U_d, \emptyset)$, i.e.,
 $CT' \text{ satisfy } \sigma(CR)$ by Lemma 21.

- (2)' In addition to (2), $CT' \text{ satisfies } (C.\text{extends} : D, \emptyset)$ by rule S-EXTEND, and $(C.\text{extends} : D) = \sigma(U_c.\text{extends} : U_d)$, therefore $CT' \text{ satisfies } (U_c.\text{extends} : U_d, \emptyset)$.
 $CT' \text{ satisfies } \sigma(CR_e)$ by Theorem 42. As a result $CT' \text{ satisfy } \sigma(CR_e) \cup \sigma(U_c.\text{extends} : U_d, \emptyset)$, i.e., $CT' \text{ satisfy } \sigma(CR)$ by Lemma 21.

Second we show that $CT \text{ satisfy } \sigma(CR)$, and we distinguish the following cases:

- (3)' In addition to (4), the class requirement $(U_d.m : \overline{C} \rightarrow C_0)_{opt}$ is not considered since it is an optional requirement, therefore $CR = CR'$, $CT' \text{ satisfy } \sigma(CR')$. As a result $CT \text{ satisfies } \sigma(CR)$.
- (4)' In addition to (5), $CT \text{ satisfy } \sigma(CR)$ by Lemma 39.

Method declaration consist in adding method clause m in CT , whether it is already member of the CT or not. Also, adding the method m in CT does not affect the satisfaction of the class requirements. We are interested that the clause m with its actual type is part of class table. Namely resulting class table CT_r , such that $(C.m : \overline{C} \rightarrow C_0) \in CT_r$, $CT_r \text{ satisfies } \sigma(CR)$.

Lastly we show that $CT_r \text{ satisfy } \sigma(CR)$ and we distinguish the following cases:

- $(C.m : \overline{C} \rightarrow C_0) \notin CT$ then we add declaration in the class table, i.e., $CT_r = CT \cup (C.m : \overline{C} \rightarrow C_0)$ and $CT_r \text{ satisfy } \sigma(CR)$ by Lemma 41.
- $C.m \in \text{dom}(CT)$ then $CT_r = CT$. Hence, $CT_r \text{ satisfies } \sigma(CR)$.



► **Definition 46** (Correspondence relation for classes). Given $CT \vdash \text{class } C \text{ extends } D \{\bar{C} \bar{f}; K \bar{M}\} OK$ and $\text{class } C \text{ extends } D \{\bar{C} \bar{f}; K \bar{M}\} OK | S | CR$, and $\text{solve}(\Sigma, S) = \sigma$, where $\text{projExt}(CT) = \Sigma$. The correspondence relation between CT and CR, written $(CT) \triangleright_c \sigma(CR)$, is defined as:

a) $CT \text{ satisfy } \sigma(CR)$

► **Theorem 47** (Equivalence of classes: \Rightarrow). Given C, CT , if $CT \vdash \text{class } C \text{ extends } D \{\bar{C} \bar{f}; K \bar{M}\} OK$, then there exists S, CR, Σ, σ , where $\text{projExt}(CT) = \Sigma$ and $\text{solve}(\Sigma, S) = \sigma$, such that $\text{class } C \text{ extends } D \{\bar{C} \bar{f}; K \bar{M}\} OK | S | CR$ holds, σ is a ground solution and $(CT) \triangleright_c \sigma(CR)$ holds.

Proof. By induction on the typing judgment.

Case T-CLASS with $CT \vdash \text{class } C \text{ extends } D \{\bar{C} \bar{f}; K \bar{M}\} OK$.

By inversion, $K = C(\bar{D}' \bar{g}, \bar{C}' \bar{f})\{\text{super}(\bar{g}); \text{this.}\bar{f} = \bar{f}\}$, i.e., the constructor initializes all fields of $\text{fields}(D, CT) = D.\text{init}(\bar{D}')$, and $C; CT \vdash \bar{M} OK$.

By Theorem 44, $\bar{M} OK | \bar{S} | \bar{U} | \bar{CR}, \forall i \in 1..n. \text{solve}(\text{projExt}(CT), S_i) = \sigma'_i, \sigma_i = \{U_i \mapsto C\} \circ \sigma'_i, \sigma_i(U_i), \sigma_i(CR_i)$ are ground and the correspondence relation holds, i.e., $C = \sigma_i(U_i), CT \text{ satisfy } \sigma_i(CR_i)$.

Let $CR|_{S_{cr}} = \text{merge}_{CR}(CR_1, \dots, CR_n, D.\text{init}(\bar{D}'))$, $S = \bar{S} \cup S_{cr} \cup \{U_i = C\}_{i \in [1..n]} \cup \{C_i = D'_i\}_{i \in 1..k} \cup \{C_i = C'_i\}_{i \in k..n}$, where $k = |\bar{D}'|, n = |\bar{C}|, n - k = |\bar{C}'|$, and $\sigma = \{\sigma_i\}_{i \in [1..n]}$.

Then $\text{class } C \text{ extends } D \{\bar{C} \bar{f}; K \bar{M}\} OK | S | CR$ holds by rule TC-CLASS.

σ solves $\bar{S}, S_{cr}, \{U_i = C\}_{i \in [1..n]}$ and $\{C_i = D'_i\}_{i \in 1..k} \cup \{C_i = C'_i\}_{i \in k..n}$ as shown below:

- σ solves \bar{S} because $\sigma = \{U_i \mapsto C\} \circ \sigma'_i\}_{i \in [1..n]}$, and $\forall i \in [1..n]. \text{solve}(\text{projExt}(CT), S_i) = \sigma_i$.
- $\forall i \in [1..n]. \sigma_i(CR_i)$ are ground by Theorem 44.
- (*) $\sigma(D.\text{init}(\bar{D}'))$ is ground because $(D.\text{init}(\bar{D}'))$ is ground.
- $\forall i \in [1..n]. CT \text{ satisfies } \sigma_i(CR_i)$ by Theorem 44.
- (**) $CT \text{ satisfies } \sigma(D.\text{init}(\bar{D}), \emptyset)$ because $\text{fields}(D, CT) = D.\text{init}(\bar{D}')$ hence by rule S-CONSTRUCTOR holds that $CT \text{ satisfies } \sigma(D.\text{init}(\bar{D}'), \emptyset)$. As a result σ solves S_{cr} by Lemma 20.
- σ solves $\{U_i = C\}_{i \in [1..n]}$ because $\sigma = \{U_i \mapsto C\} \circ \sigma'_i\}_{i \in [1..n]}$.
- $\{C_i = D'_i\}_{i \in 1..k} \cup \{C_i = C'_i\}_{i \in k..n}$ holds because K initializes all fields of class C as it is given by inversion.

σ is ground solution because:

- 1) $\forall i \in 1..n. \sigma(CR_i)$ is ground because $\sigma(CR_i) = (\{\sigma_j\}_{j \in [1..i-1, i+1..n]} \circ \sigma_i)(CR_i)$ by Corollary 23.

$(\{\sigma_j\}_{j \in [1..i-1, i+1..n]})(\sigma_i(CR_i)) = \sigma_i(CR_i)$ because $\sigma_i(CR_i)$ is ground by Theorem 44.

$\sigma(D.\text{init}(\bar{D}'))$ is ground by (*). As a result $\sigma(CR)$ is ground by definition of merge_{CR}

The correspondence relation holds because:

- a) $\forall i \in 1..n. CT \text{ satisfy } \sigma(CR_i)$ because $CT \text{ satisfies } \sigma_i(CR_i)$ by Theorem 44, and from 1) $\sigma(CR_i) = \sigma_i(CR_i)$. $CT \text{ satisfies } \sigma(D.\text{init}(\bar{D}), \emptyset)$ by (**). As a result $CT \text{ satisfies } \sigma(CR_1) \dots \cup \sigma(CR_n) \cup \sigma(D.\text{init}(\bar{D}'))$, i.e., $CT \text{ satisfies } \sigma(CR)$ by Lemma 21.



► **Theorem 48** (Equivalence of classes: \Leftarrow). Given C, CR, Σ , if $\text{class } C \text{ extends } D \{\bar{C} \bar{f}; K \bar{M}\} OK | S | CR$, $\text{solve}(\Sigma, S) = \sigma$, and σ is a ground solution, then there exists CT , such that $CT \vdash \text{class } C \text{ extends } D \{\bar{C} \bar{f}; K \bar{M}\} OK$ holds, $(CT) \triangleright_c \sigma(CR)$ holds and $\text{projExt}(CT) = \Sigma$.



Proof. By induction on the typing judgment.

Case TC-CLASS with *class C extends D{C f; K M} OK | S | CR*.

Let $S = \bar{S} \cup S_{cr} \cup \{U_i = C\}_{i \in [1..n]} \cup \{C_i = D'_i\}_{i \in 1..k} \cup \{C_i = C'_i\}_{i \in k..n}$, where $k = |\bar{D}'|$, $n = |\bar{C}|$, $n - k = |\bar{C}'|$, σ be a ground solution, such that it solves S and $\sigma(CR)$ is ground.

By inversion, $\bar{M} OK | \bar{S} | \bar{U} | \bar{CR}, \forall i \in 1 \dots n. \sigma(U_i), \sigma(CR_i)$ are ground.

$merge_{CR}(CR_1, \dots, CR_n) = CR'|_{S_c}, merge_{CR}((D.init(\bar{D}')), CR') = CR|_{S_{cr}}$.

Let $\forall i \in 1 \dots n. \sigma(U_i) = C$ for C we know it is ground.

By Theorem 45 $C; \bar{CT} \vdash \bar{M} OK$, the correspondence relation holds, $\forall i \in 1 \dots n. C = \sigma(U_i), CT_i \text{ satisfies } \sigma(CR_i)$. $\text{projExt}(CT') = \Sigma'$, where $CT' = \bigcup_{i \in [1..n]} \{CT_i\}$.

(*) $\bigcap_{i \in [1..n]} \{freshU(CR_i)\} = \emptyset$ by Proposition 22. $\forall i \in 1 \dots n. CT' \text{ satisfies } \sigma(CR_i)$ by Class Table Weakening Lemma, therefore $CT' \text{ satisfies } \sigma(CR')$ by Lemma 21.

The constructor K initializes all fields of class C , i.e., $K = C(\bar{D}' \bar{g}, \bar{C}' \bar{f}) \{super(\bar{g}); this.\bar{f} = \bar{f}\}$, because σ solves $\{C_i = D'_i\}_{i \in 1..k} \cup \{C_i = C'_i\}_{i \in k..n}$.

We consider three cases to construct the class table CT :

- (1) $\{(D.init(\bar{D}'), CT')\}_{\ll^*} = \emptyset$. Since no entry of class D exist for the constructor $init$ in the given class table CT' , we add a new entry in the class table, i.e., $CT = CT' \cup (D.init(\bar{D}'))$.
- (2) $\{(D.init(\bar{D}'), \sigma(CR'))\}_{\ll} \cup \{(D.init(\bar{D}'), \sigma(CR'))\}_{\gg} = \emptyset, (D.init(\bar{D}'')) \in CT'$, for some \bar{D}'' , then by Lemma 39 CT is constructed.
- (3) $(D.init(\bar{A})cond') \in \sigma(CR')$, for some $\bar{A}, cond'$, $(D.init(\bar{D}'')) \in CT'$, for some \bar{D}'' , then by Lemma 40 CT is constructed.

From above we have that $fields(D, CT) = D.init(\bar{D}')$, no extends clauses are added to the class table CT' , therefore $\text{projExt}(CT) = \Sigma' = \Sigma$

Then $CT \vdash \text{class C extends D } \{\bar{C} \bar{f}; K \bar{M}\} OK | \bar{S}$ holds by rule T-CLASS.

The correspondence relation holds because:

a) We have to show is that CT satisfy $\sigma(CR)$, and we distinguish the following cases:

- (1)' In addition to (1) CT satisfies $\sigma(D.init(\bar{D}'))$ by construction, $CT' \text{ satisfies } \sigma(CR')$ by (*), therefore CT satisfies $\sigma(CR')$ by Class Table Weakening Lemma 38. As a result CT satisfies $\sigma(D.init(\bar{D}')) \cup \sigma(CR')$, i.e., CT satisfies $\sigma(CR)$ by definition of $merge_{CR}$.
- (2)' In addition to (2), CT satisfies $\sigma(CR')$ by (*), then there is CT , CT satisfies $\sigma(CR)$ by Lemma 39.
- (3)' In addition to (3), CT satisfies $\sigma(CR')$ by (*), then there is CT , CT satisfies $\sigma(CR)$, by Lemma 40.

Class declaration consists in adding the class C with all of its fields, methods, constructor and extend clauses in the class table, whether they are already member of the CT or not. Also, adding these clauses does not affect the satisfaction of the class requirements. Namely resulting class table CT_r , such that $C.extends = D \in CT_r, K \in CT_r, \{C.f_i : C_i\}_{i \in [1..n]} \in CT_r, \bar{M} \in CT_r, CT_r \text{ satisfies } \sigma(CR)$. We distinguish the following cases:

- $(C.extends = D) \notin CT$, or $(C.init(\bar{C})) \notin CT$, or $\{C.f_i : C_i\}_{i \in [1..n]} \notin CT$, or $\{C.m_i : \bar{C} \rightarrow C_0\}_{i \in [1..n]} \notin CT$ then $CT_r = CT \cup (C.extends = D); (C.init(\bar{C})) \cup \{C.f_i : C_i\}_{i \in [1..n]} \cup \{C.m_i : \bar{C} \rightarrow C_0\}_{i \in [1..n]}$, and CT_r satisfies $\sigma(CR)$ by Lemma 41.
- $\forall CTcls \in \{(C.extends = D) \cup (C.init(\bar{C})) \cup \{C.f_i : C_i\}_{i \in [1..n]} \cup \{C.m_i : \bar{C} \rightarrow C_0\}_{i \in [1..n]}\}$ such that $domCl(CTcls) \in dom(CT)$ then $CT_r = CT$. Hence, CT_r satisfies $\sigma(CR)$.



► **Lemma 49.** *Given a complete class table CT constructed from all possible class declarations \bar{L} , a set of requirements CR , $\biguplus_{L' \in \bar{L}} (\text{removeMs}(CR, L') \uplus \text{removeFs}(CR, L') \uplus \text{removeCtor}(CR, L') \uplus \text{removeExt}(CR, L')) = CR'|_S$, a substitution σ , such that $\sigma(CR)$ is ground, and CT satisfies $\sigma(CR)$. Then σ solves S .*

Proof. By the definitions of remove for different clauses, $S = S_c \cup S_e \cup S_k \cup S_f \cup S_m$. Let us consider constraints generated from field remove S_f . Suppose there exist $f \in \text{dom}(CR)$ such that $(T.f : T', \text{cond}) \in CR$ and $\sigma(\text{cond})$ hold.

Let $\sigma(T) = C$ and $\sigma(T') = C_f$, since $\sigma(CR)$ ground, C, C_f are ground.

Since CT satisfy $\sigma(CR)$, by inversion $\text{field}(f, C, CT) = C_f$, i.e., exist $D > C$ such that $D.f : \sigma(T') \in CT$. We distinguish two cases when f is declared in C or in one of its superclasses D :

- 1) $D = C$. By rule S-FIELD; $C.f : C_f \in CT$. We apply remove for field clause $C.f : C_f$. By definition of removeF the correspondent requirement is $(T.f : T', \text{cond}) \in CR$ and the new constraint generated is $S_f = (T' = C_f \text{ if } T = C)$. This constraint is solved, because the condition holds and $\sigma(T') = C_f$.
- 2) $D > C$. Then there exist C extends $D \in CT$ and $D.f : C_f \in CT$. In this case we have to apply remove for extends and field clauses. First, we apply remove of extends. By definition of removeExt the requirement under scrutiny is duplicated, i.e., $(T.f : T', \text{cond} \cup T \neq C), (D.f : T', \text{cond} \cup T = C)$. Second we apply remove of field f . By definition of removeFs the generated constrains are $S_f = \{(T' = C_f \text{ if } T = D), (T' = C_f) \text{ if } D = D\}$. The first constraint is not valid because the condition does not hold ($\sigma(T) \neq D$), therefore is not considered. the second constraint is solved because the condition holds and $\sigma(T') = C_f$

The same procedure we follow for extends, constructors and methods clauses. ◀

► **Lemma 50 (Class requirements empty).** *Given a complete class table CT constructed from all possible class declarations \bar{L} , a set of requirements CR , $\biguplus_{L' \in \bar{L}} (\text{removeMs}(CR, L') \uplus \text{removeFs}(CR, L') \uplus \text{removeCtor}(CR, L') \uplus \text{removeExt}(CR, L')) = CR'|_S$, and a substitution σ , such that $\sigma(CR)$ is ground, σ solves S , we have that if CT satisfy $\sigma(CR)$, then and $\sigma(CR') = \emptyset$.*

Proof. By contradiction.

By assumption $\sigma(CR') \neq \emptyset$, and $CR' = \{(CReq, cond) \mid \exists(T \neq T') \in cond\}$. From this, follows $\forall(CReq, cond) \in CR'$. $cond$ holds, i.e., all conditions of $cond$ do hold. This is derived after performing remove, we already know the exact types for classes and their extends, constructor, fields, method clauses. Therefore from remove we add inequalities to invalidate requirements for which we know their exact types, as result exist one their conditions that does not hold. Since by assumption the set is not empty then all conditions hold. For sake of brevity we consider only the conditions that are added after performing remove, because are the ones we are interested in.

First we consider the extend clauses in the requirement set. All conditions of the requirements corresponding extends clause do hold. Let us consider $\exists(T.\text{extends}T', cond) \in CR'$. $\forall(T \neq C) \in cond$. $\sigma(T) \neq C$ holds. By definition it is given that $\sigma(CR)$ is ground, namely $\sigma(T) = C', \sigma(T') = D'$, such that C', D' are ground. Since all the inequalities in $cond$ hold, this means that in the class table was not added any *extends clause*, such that $(C'.\text{extends} = D') \notin CT$. Therefore CT satisfies $\sigma(CR)$ does not hold.

This strategy of proof is used for constructor since from the definition of *removeCtor* only inequality conditions are added, and not considered while removing extends clause.

Second we consider field clauses. From the definition of removeFs and removeExt for every field clause we have a duplicated requirement corresponding to the parents type. All conditions of the requirements corresponding field clause do hold. By definition it is given that $\sigma(CR)$ is ground, namely $\sigma(T) = C'$, $\sigma(T_f) = C_f$, such that C' , C_f are ground. Let us consider $(C'.\text{extends} = D) \in CT$, and $\exists(T.f : T_f, \text{cond} \cup T \neq C'), (D.f : T_f, \text{cond}' \cup T = C') \in CR'$ such that $\forall(T \neq C), (T = C) \in \text{cond} \cup \text{cond}' \cup T = C' \cup T \neq C'$ ($\sigma(T) \neq C$), ($\sigma(T) = C$) hold. Since all the conditions in $\text{cond} \cup \text{cond}'$ hold, this means that in the class table was not added any *field clause*, such that f is declared in C' or in its parents, i.e., $\forall C'' \text{ such that } C' <: C'', \text{ then } (C''.f : C_f) \notin CT$.

Therefore CT satisfies $\sigma(CR)$ does not hold.

The same strategy of proving is used for methods. In contrast for the optional methods regardless all the conditions might hold they are removed in any case, because they are optional. The lack of inequality conditions that do not hold, only shows the given method is declared in a class of the class table but not in its parents.



► **Theorem 51** (Equivalence for programs: \Rightarrow). Given \bar{L} , if \bar{L} OK, then there exists S , Σ , σ , where $\text{projExt}(\bar{L}) = \Sigma$ and $\text{solve}(\Sigma, S) = \sigma$, such that \bar{L} OK | S holds and σ ground solution.

Proof. By induction on the typing judgment.

Case T-PROGRAM with $\bar{C} \bar{L}$ OK.

By inversion, *Class table construction* CT is
 $CT = \bigcup_{L' \in \bar{L}} (\text{addExt}(L') \cup \text{addCtor}(L') \cup \text{addFs}(L') \cup \text{addMs}(L'))$ and
 $CT \mid \bar{L}$ OK.

By Theorem 47, \bar{L} OK | $\bar{S} \mid \bar{C}\bar{R}$, $\forall i \in 1..n$. $\text{solve}(\text{projExt}(CT), S_i) = \sigma_i$, $\sigma_i(CR_i)$ is ground and the correspondence relation holds, i.e., CT satisfy $\sigma_i(CR_i)$.

Let $CR|_{S_{cr}} = \text{merge}_{CR}(CR_1, \dots, CR_n)$, $\biguplus_{L' \in \bar{L}} (\text{removeMs}(CR, L') \uplus \text{removeFs}(CR, L') \uplus \text{removeCtor}(CR, L') \uplus \text{removeExt}(CR, L')) = CR_f|_{S_r}$, $S = \bar{S} \cup S_{cr} \cup S_r$, and $\sigma = \{\sigma_i\}_{i \in [1..n]}$. From the Lemma 50 we have $\sigma(CR_f) = \emptyset$.

Then \bar{L} OK | S holds by rule TC-PROGRAM.

σ solves \bar{S} , and S_{cr} as shown below:

- σ solves \bar{S} because $\sigma = \{\sigma_i\}_{i \in [1..n]}$.
- $\forall i \in [1..n]$. $\sigma_i(CR)_i$ are ground by Theorem 47.
 $\forall i \in [1..n]$. CT satisfies $\sigma_i(CR_i)$ by Theorem 47.
As a result σ solves S_{cr} by Lemma 20.
- $\sigma(CR)$ is ground and CT satisfies $\sigma(CR)$ by Theorem 47, and given the class table CT , then σ solves S_r by Lemma 49.

σ is ground solution because:

- 1) $\forall i \in [1..n]$. $\sigma(\text{projExt}(CT), CR_i)$ is ground because $\sigma(CR_i) = (\{\sigma_j\}_{j \in [1..n]})$
 $(CR_i) = (\{\sigma_j\}_{j \in [1..i-1, i+1..n]} \circ \sigma_i)(CR_i)$ by Corollary 23.
 $(\{\sigma_j\}_{j \in [1..i-1, i+1..n]}) (\sigma_i(CR_i)) = \sigma_i(CR_i)$ because $\sigma_i(CR_i)$ is ground by Theorem 47. As a result $\sigma(CR)$ is ground by definition of merge_{CR} .



► **Lemma 52** (Class table satisfy class requirements). Given class declarations \bar{L} , such that $CT = \bigcup_{L' \in \bar{L}} (\text{addExt}(L') \cup \text{addCtor}(L') \cup \text{addFs}(L') \cup \text{addMs}(L'))$, a set of requirements CR , $\biguplus_{L' \in \bar{L}} (\text{removeMs}(CR, L') \uplus \text{removeFs}(CR, L') \uplus \text{removeCtor}(CR, L') \uplus \text{removeExt}(CR, L')) =$

$CR'|_S$, and a substitution σ , such that $\sigma(CR)$ is ground, σ solves S , we have that if $\sigma(CR') = \emptyset$, then CT satisfy $\sigma(CR)$.

Proof. By contradiction.

By assumption CT satisfies $\sigma(CR)$ does not hold. From this, follows $\exists(CReq, cond) \in CR$. $cond$ holds, i.e., all conditions of $cond$ do hold and no compatible clause with $CReq$ exists in CT .

As property of remove we add inequalities to invalidate requirements for which we know their exact types, as result exist at least one inequality condition that does not hold, and the requirement is removed, otherwise it remains in the requirements set.

First we consider the extend clauses in the requirements set. Let us consider $\exists(T.extendST', cond) \in CR$ such that $cond$ hold. By definition $\sigma(CR)$ is ground, namely $\sigma(T) = C'$, $\sigma(T') = D'$. By assumption $(C'.extends : D') \notin CT$, i.e., the clause it is not member of any of the class declarations \bar{L} that are used to realize removing. Therefore after performing remove $\#(\sigma(T) \neq C \in \sigma(cond'))$ such that $\sigma(T) \neq C$ does not hold, where $(T.extend : T', cond') \in CR'$, i.e., $\sigma(cond')$ hold.

Therefore $\sigma(CR') \neq \emptyset$.

This strategy of proof is used for constructor since from the definition of $removeCtor$ only inequality conditions are added, and not considered while removing extends clause.

Second we consider field clauses. From the definition of $removeFs$ and $removeExt$ for every field clause we have a duplicated requirement corresponding to the parents type.

Let us consider $\exists(T.f : T_f, cond) \in CR$. $cond$ hold. By definition $\sigma(CR)$ is ground, namely $\sigma(T) = C'$, $\sigma(T_f) = D'$. By assumption $\#(D.f : D') \in CT$, such that $\sigma(T) <: D$. This means that in the class table was not added any *field clause*, such that f is declared in C' or in its parents. Therefore after performing remove $(T.f : T_f, cond') \in CR'$ we have that $\#(\sigma(T) \neq C) \in \sigma(cond')$. $(\sigma(T) \neq C)$ does not hold. i.e., $\sigma(cond')$ hold.

Therefore $\sigma(CR) \neq \emptyset$.

The same strategy of proving is used for methods. ◀

► **Theorem 53** (Equivalence for programs: $\Leftarrow \Rightarrow$). Given \bar{L} , if $\bar{L} OK \mid S$, $solve(\Sigma, S) = \sigma$, where $projExt(\bar{L}) = \Sigma$, and σ is a ground solution, then $\bar{L} OK$ holds.

Proof. By induction on the typing judgment.

Case TC-PROGRAM with $\bar{L} OK \mid S$.

Let $S = \bar{S} \cup S_{cr} \cup S_r$, σ is ground solutions and $solve(projExt(\bar{L}), S) = \sigma$, i.e., σ solves \bar{S} , S_{cr} , S_r .

By inversion, $\bar{L} OK \mid \bar{S} \mid \bar{CR}$, $\forall i \in 1 \dots n$. $\sigma(CR_i)$ are ground.

$CR|_{S_c} = merge_{CR}(CR_1, \dots, CR_n)$.

$\biguplus_{L' \in \bar{L}} (removeMs(CR, L') \uplus removeFs(CR, L') \uplus removeCtor(CR, L') \uplus removeExt(CR, L')) = CR_f|_{S_r}$, and $\sigma(CR_f) = \emptyset$

By Theorem 48, $CT \mid \bar{L} OK$, and the correspondence relation holds, i.e., $\forall i \in [1..n]$. CT satisfy $\sigma(CR_i)$. CT satisfies $\sigma(CR_1) \cup \dots \cup \sigma(CR_n)$, i.e., CT satisfies $\sigma(CR)$ by Lemma 21.

Class table construction CT is $CT = \bigcup_{L' \in \bar{L}} (addExt(L') \cup addCtor(L') \cup addFs(L') \cup addMs(L'))$ by Lemma 52.

Then $\bar{L} OK$ holds by rule T-PROGRAM. ◀