



**HAL**  
open science

## Non-Ground Congruence Closure

Hendrik Leidinger, Christoph Weidenbach

► **To cite this version:**

Hendrik Leidinger, Christoph Weidenbach. Non-Ground Congruence Closure. Max-Planck-Institut für Informatik, Saarbrücken, Germany. 2024. hal-04845306

**HAL Id: hal-04845306**

**<https://inria.hal.science/hal-04845306v1>**

Submitted on 18 Dec 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

# Non-Ground Congruence Closure

Hendrik Leidinger, Christoph Weidenbach

Max Planck Institute for Informatics

Saarland Informatics Campus

Saarbrücken, Germany

{hleiding,weidenb}@mpi-inf.mpg.de

December 16, 2024

Congruence closure on ground equations is a well-established, efficient algorithm for deciding ground equalities. It computes an explicit representation of the ground equivalence classes on the basis of a set of ground input equations. Then equalities are decided by membership. We generalize the ground congruence closure algorithm to non-ground equations. The algorithm also computes an explicit representation of all non-ground equivalence classes. It is terminating due to an a priori bound on the term size. By experiments we compare our new algorithm with ground congruence closure.

## 1 Introduction

Equational logic is widely used in almost all aspects of formal reasoning about systems. Given a set of non-ground equations, in order to apply congruence closure (CC) [9] the non-ground equations must be grounded first. Then after applying CC to the grounded equations, ground equalities can be decided by testing membership in the generated congruence classes. CC is in particular useful compared to ground completion [14], if many different ground equalities are tested, in particular, with respect to the same set of input equations. For CC testing an equality amounts to a membership test, for completion normal forms need to be computed. In this paper we generalize CC to non-ground congruence closure ( $CC(\mathcal{X})$ ).

In  $CC(\mathcal{X})$  a (congruence) class is a set of *constrained terms*, also called a *constrained class*. A constraint is a conjunction of inequalities of the form  $t \preceq \beta$ , where  $t$  is a possibly non-ground term and  $\beta$  is a ground term. The *constraint* restricts the number of ground instances of the *constrained term* to those  $\preceq \beta$ . Initially, the set of classes consists of one constrained class for each input equation and for technical reasons one single term constrained class for each occurring non-variable symbol.  $CC(\mathcal{X})$  creates a solution for the whole ground input space  $\preceq \beta$ . It consists of two main rules *Merge* and

*Deduction* to build up the congruence classes. *Merge* creates a new class by unifying two terms in different classes and applying this unifier to the Union of these two classes. *Deduction* creates a new class by simultaneously unifying the arguments of two terms with the same top symbol in different classes with terms in the same class. Termination is guaranteed by a definition of subsumption between two classes and the fact that all terms are constrained by a maximum term  $\beta$ .

As an example, consider the equations  $g(x) \approx h(x)$ ,  $h(y) \approx f(y)$  and  $a \approx b$  and a maxterm  $\beta = f(a)$ . Furthermore, assume an ordering that orders the terms by the number of symbols they contain. Initially  $\text{CC}(\mathcal{X})$  would create the classes:

$$\begin{aligned} &\{g(x) \parallel g(x)\}, \{h(x) \parallel h(x)\}, \{f(x) \parallel f(x)\}, \{a \parallel a\}, \{b \parallel b\}, \\ &\{a, b \parallel a, b\}, \{g(x), h(x) \parallel g(x), h(x)\}, \{h(y), f(y) \parallel h(y), f(y)\} \end{aligned}$$

For readability we simply write  $\{g(x) \parallel g(x)\}$  instead of  $\{g(x) \preceq \beta \parallel g(x)\}$  omitting  $\preceq \beta$  within the constraint and use the notation  $\{\Gamma \parallel s_1 \dots, s_n\}$  to denote that the constraint  $\Gamma$  holds for all terms.  $\text{CC}(\mathcal{X})$  can now merge the classes  $\{g(x), h(x) \parallel g(x), h(x)\}$  and  $\{h(y), f(y) \parallel h(y), f(y)\}$  by unifying  $h(x)$  with  $h(y)$ . So we get  $\{g(x), h(x), f(x) \parallel g(x), h(x), f(x)\}$ . The new class subsumes the merged classes, so they can be deleted. Now we can apply *Deduction* followed by two merges to the new class by creating a variable disjoint copy and unifying the arguments, e.g., of  $f(x)$  and  $f(y)$  with  $a$  and  $b$  and unifying the resulting  $f(a)$  and  $f(b)$  with the new class to create  $\{g(a), h(a), f(a), g(b), h(b), f(b) \parallel g(a), h(a), f(a), g(b), h(b), f(b)\}$ . This class is not subsumed and does not subsume any class in the class set. Now the algorithm terminates, since the maxterm  $\beta$  restricts the creation of any new class. The final result without single term classes is

$$\begin{aligned} &\{g(x), h(x), f(x) \parallel g(x), h(x), f(x)\}, \{a, b \parallel a, b\}, \\ &\{g(a), h(a), f(a), g(b), h(b), f(b) \parallel g(a), h(a), f(a), g(b), h(b), f(b)\} \end{aligned}$$

**Related Work:** To the best of our knowledge, the only algorithm that is similar to ours is Joe Hurd’s Congruence Classes with Logic Variables [12]. The algorithm creates a set of classes, where each class consists of multiple, possibly non-ground terms. It incrementally finds all matchers between all pairs of classes and applies these matchers to extend these classes. Therefore, in order to test equality of two terms they need to be added and the algorithm restarted. The size of terms is not constrained by the algorithm so it may diverge. The author does not introduce a notion of redundancy. The semantics of the classes is with respect to an infinite signature. In contrast, we generate a complete classification of all considered ground terms, i.e., testing equality of two terms means testing membership in the same class. Due to a notion of redundancy, our algorithm always terminates (Lemma 21), and it is implemented (Section 4).

Satisfiability modulo theory (SMT) [11,21] solvers (e.g., [2,6,8,10,18]) make use of congruence closure (CC) [9,19,24]. It is well suited as an incremental algorithm that decides the validity of ground equations and is able to find a small subset of input equations that serves as a proof, all in time  $\mathcal{O}(n \log(n))$  [20]. For SMT solvers many techniques have been invented to instantiate non-ground input equations [3,22,23] in order to make them applicable to CC. All these techniques do not consider CC on equations with variables, instead the equations are grounded first. This applies in particular to [3] where equations

are assumed to be ground, but the equality to be tested may contain variables and the procedure aims at finding further potentially useful ground instances to the equations.

SCL(EQ) (Simple Clause Learning over Equations) [15] is a complete calculus for first-order logic with equality that only learns non-redundant clauses. Similar to CDCL (Conflict Driven Clause Learning) [4,13,17,25,27] it builds an explicit model assumption (trail) by (non-ground) literals where ground instances are finitely limited by a ground term  $\beta$ . Clauses are evaluated with respect to a trail, where  $CC(\mathcal{X})$  can then be immediately applied instead of grounding up to  $\beta$ .

The rest of the paper is organized as follows. Section 2 provides the necessary technical background notions needed for the development of our algorithm. Section 3 presents our new calculus including examples and proofs for soundness, Lemma 20, completeness, Lemma 22, and termination, Lemma 21. Section 4 presents refinements of the calculus towards an implementation. Section 5 compares the performance of  $CC(\mathcal{X})$  with  $CC$  by experiments. All experiments can be reproduced by the provided supplementary material. Section 6 concludes the paper.

## 2 Preliminaries

We assume a standard first-order language with equality and over a finite set of function symbols  $\Omega$ , where the only predicate symbol is equality  $\approx$ . We assume that  $\Omega$  contains at least one constant and one non-constant function symbol.  $t, s, l, r$  are terms from  $\mathcal{T}(\Omega, \mathcal{X})$  for an infinite set of variables  $\mathcal{X}$ ;  $f, g, h$  function symbols from  $\Omega$ ;  $a, b, c$  constants from  $\Omega$  and  $x, y, z$  variables from  $\mathcal{X}$ . The function  $\text{vars}$  returns all variables of a term. The function  $\#(x, t)$  returns the number of occurrences of a variable  $x$  in  $t$ .

By  $\sigma, \tau, \delta, \mu$  we denote substitutions. Let  $\sigma$  be a substitution, then its finite domain is defined as  $\text{dom}(\sigma) := \{x \mid x\sigma \neq x\}$  and its codomain is defined as  $\text{cdom}(\sigma) = \{t \mid x\sigma = t, x \in \text{dom}(\sigma)\}$ . We extend their application to terms and sets of terms in the usual way. A term, equation is *ground* if it does not contain any variable. A substitution  $\sigma$  is *ground* if  $\text{cdom}(\sigma)$  is ground. A substitution  $\sigma$  is *grounding* for a term  $t$ , equation  $s \approx t$  if  $t\sigma$ ,  $(s \approx t)\sigma$  is ground, respectively. The function  $\text{gnd}$  returns the set of all ground instances of a term, equation or sets thereof. The function  $\text{mgu}$  denotes the most general unifier of two terms, two equations, respectively. We assume that  $\text{mgu}$  do not introduce fresh variables and that they are idempotent. The size of a term  $t$  (equation  $E$ ) is denoted by  $\text{size}(t)$  ( $\text{size}(E)$ ), which is the number of symbols in  $t$  ( $E$ ).

Let  $\preceq$  be a total quasi-ordering on ground terms where the strict part is well-founded. The ordering is lifted to the non-ground case via instantiation: we define  $t \preceq s$  if for all grounding substitutions  $\sigma$  it holds  $t\sigma \preceq s\sigma$ . Given a ground term  $\beta$  then  $\text{gnd}_{\preceq\beta}$  computes the set of all ground instances of a term, equation, or sets thereof where all ground terms are smaller or equal to  $\beta$  with respect to  $\preceq$ . By  $\mathcal{T}_{\preceq\beta}(\Omega, \emptyset)$  or just  $\mathcal{T}_{\preceq\beta}$  we denote the set of all ground terms  $\preceq \beta$ .

We rely on standard first-order semantics and in particular write  $E \models s \approx t$  if any model of the implicitly universally quantified equations in  $E$  is also a model for the ground equation  $s \approx t$ .

Let  $E$  be a set of equations over  $T(\Omega, \mathcal{X})$  where all variables are implicitly universally quantified. The well-known inference system of equational logic comprises the following rules [1]

**Reflexivity**  $E \Rightarrow_{\text{EQ}} E \cup \{t \approx t\}$   
provided  $t$  is a term.

**Symmetry**  $E \cup \{t \approx t'\} \Rightarrow_{\text{EQ}} E \cup \{t \approx t', t' \approx t\}$

**Transitivity**  $E \cup \{t \approx t', t' \approx t''\} \Rightarrow_{\text{EQ}} E \cup \{t \approx t', t' \approx t'', t \approx t''\}$

**Congruence**  $E \cup \{t_1 \approx t'_1, \dots, t_n \approx t'_n\} \Rightarrow_{\text{EQ}} E \cup \{t_1 \approx t'_1, \dots, t_n \approx t'_n, f(t_1, \dots, t_n) \approx f(t'_1, \dots, t'_n)\}$

**Instance**  $E \cup \{t \approx t'\} \Rightarrow_{\text{EQ}} E \cup \{t \approx t, t\sigma \approx t'\sigma\}$   
provided  $\sigma$  is a substitution.

and by Birkhoff's theorem [1] we get for two ground terms  $t, s$ :  $E \models s \approx t$  iff  $E \Rightarrow_{\text{EQ}}^* \{t, s\} \cup E'$ . We will base our completeness proof, Lemma 22, on  $\Rightarrow_{\text{EQ}}$ .

Congruence Closure [9,19,24] is an algorithm for deciding satisfiability of ground equations. The initial state is  $(\Pi, E)$ , where  $\Pi$  is a partition of all ground subterms of terms in  $E$ , such that every term is in its own class, and  $E$  is the set of ground equations. The algorithm consists of the following three inference rules.

**Delete**  $(\{A\} \cup \Pi, E \cup \{s \approx t\}) \Rightarrow_{\text{CC}} (\{A\} \cup \Pi, E)$   
provided  $\{s, t\} \subseteq A$ .

**Merge**  $(\{A, B\} \cup \Pi, E \cup \{s \approx t\}) \Rightarrow_{\text{CC}} (\{A \cup B\} \cup \Pi, E)$   
provided  $s \in A, t \in B$  and  $A \neq B$ .

**Deduction**  $(\{A, B\} \cup \Pi, E) \Rightarrow_{\text{CC}} (\{A, B\} \cup \Pi, E \cup \{f(s_1, \dots, s_n) \approx f(t_1, \dots, t_n)\})$   
provided  $f(s_1, \dots, s_n) \in A, f(t_1, \dots, t_n) \in B, A \neq B$  and for each  $i$ , there exists a  $D_i \in \{A, B\} \cup \Pi$  such that  $\{s_i, t_i\} \in D_i$  and  $f(s_1, \dots, s_n) \approx f(t_1, \dots, t_n) \notin E$ .

The algorithm terminates if no rule is applicable anymore. The resulting set  $\Pi$  represents the set of congruence classes.

### 3 Non-Ground Congruence Closure

We now present our calculus in full detail.

**Definition 1.** A constrained term  $\Gamma \parallel s$  is a term  $s$  with a constraint  $\Gamma$ . The constraint  $\Gamma$  is a conjunction of atoms  $t \preceq \beta$ . A substitution  $\sigma$  is grounding for a constraint term  $\Gamma \parallel s$  if  $\Gamma\sigma$  and  $s\sigma$  are ground.

The constraint  $\Gamma$  restricts the possible ground instances of the term  $s$  to those instances  $s\sigma$  such that  $\Gamma\sigma$  evaluates to true. If it is clear from the context, we omit the  $\preceq \beta$  and just write the left hand-side of the inequation. A constraint class is a set of constraint terms. We distinguish between separating and free variables, where a separating variable occurs in all terms within the class whereas a free variable does not.

**Definition 2** (Congruence Class). A congruence class or simply class is a finite set of constraint terms  $\Gamma \parallel s$ . Let  $A = \{\Gamma_1 \parallel s_1, \dots, \Gamma_n \parallel s_n\}$  be a class. The set of separating variables  $X$  of  $A$  is defined as  $X = \text{vars}(s_1) \cap \dots \cap \text{vars}(s_n)$ . The set of free variables  $Y$  of  $A$  is defined as  $Y = (\text{vars}(s_1) \cup \dots \cup \text{vars}(s_n)) \setminus X$ . A substitution is grounding for  $A$  if it is grounding for all constraint terms  $\Gamma_i \parallel s_i$ .

If the terms in a congruence class all have the same constraint then we use  $\{\Gamma \parallel s_1, \dots, s_n\}$  as a shorthand for  $\{\Gamma \parallel s_1, \dots, \Gamma \parallel s_n\}$ . For example, with all shorthands we can now write  $\{g(x), h(x) \parallel g(x), h(x)\}$  instead of  $\{g(x) \preceq \beta, h(x) \preceq \beta \parallel g(x), g(x) \preceq \beta, h(x) \preceq \beta \parallel h(x)\}$ . In the calculus later on the constraints of each term within a class are always the same. Variables in a class can always be renamed.

**Definition 3.** Let  $A = \{\Gamma_1 \parallel s_1, \dots, \Gamma_n \parallel s_n\}$  be a class and  $\mu$  a substitution. We define  $A\mu$  as  $\{\Gamma_1\mu \parallel s_1\mu, \dots, \Gamma_n\mu \parallel s_n\mu\}$ . In particular, if  $\mu$  is grounding for  $A$  we overload its application by  $A\mu = \{s\mu \mid (\Gamma \parallel s \in A \text{ and } \Gamma\mu \text{ true})\}$ .

The semantics of a congruence class with variables is defined by creating a mapping to the corresponding ground classes. It is important to distinguish between separating and free variables here. Separating variables divide the non-ground class into several ground classes.

**Definition 4** (Congruence Class Semantics). Let  $A$  be a congruence class. Let  $X$  be the separating variables of  $A$ . Then the set  $\text{gnd}'(A)$  is defined as:

$$\bigcup_{\substack{\sigma \text{ ground,} \\ \text{dom}(\sigma)=X}} \{ \{(\Gamma\sigma \parallel s\sigma) \mid (\Gamma \parallel s) \in A \text{ and } \Gamma\sigma \text{ satisfiable} \} \}$$

and the set  $\text{gnd}(A)$  is defined as:

$$\bigcup_{B \in \text{gnd}'(A)} \left\{ \bigcup_{\sigma \text{ grounding for } B} \{s\sigma \mid (\Gamma \parallel s) \in B \text{ and } \Gamma\sigma \text{ true} \} \right\}$$

**Example 5.** Assume  $\Omega = \{g, h, a, b\}$ , a term  $\beta = g(a)$ , an ordering such that only  $a, b, g(a), g(b), h(a), h(b) \preceq g(a)$  and classes  $A = \{g(x), h(x) \parallel g(x), h(x)\}$ ,  $B = \{g(x), h(y) \parallel g(x), h(y)\}$  Then  $\text{gnd}(A) = \{\{g(a), h(a)\}, \{g(b), h(b)\}\}$  and  $\text{gnd}(B) = \{\{g(a), h(a), g(b), h(b)\}\}$

**Definition 6** (Normal Class). Let  $A$  be a class. The normal class  $\text{norm}(A)$  is defined as  $\{(\Gamma \wedge \Gamma\sigma \parallel s) \mid (\Gamma \parallel s) \in A\} \cup \{(\Gamma \wedge \Gamma\sigma \parallel s\sigma) \mid (\Gamma \parallel s) \in A \text{ and } s \text{ contains free variables}\}$  for a renaming  $\sigma$  on the free variables introducing only fresh variables.

A class can be turned into a normal class by generating exactly one renamed copy for all constrained terms containing free variables. The motivation for normal classes is of technical nature.  $\text{CC}(\mathcal{X})$  rules always operate on two terms out of a class. In case of terms with variables the two terms may be actually instances of the same term from the class. This can only happen for terms with free variables. By introducing one renamed copy for such terms, the style of  $\text{CC}(\mathcal{X})$  rules is preserved and

the rules do not need to distinguish between free and separated variables. For example, the class  $A = \{g(x), h(y) \parallel g(x), h(y)\}$  contains all ground terms build with top-symbols  $g$  and  $h$ . So for a  $\text{CC}(\mathcal{X})$  step picking  $g(a)$  and  $g(b)$  out of the class the term  $g(x)$  needs to be instantiated with two different constants. By using renamed copies  $\text{norm}(A) = \{g(x), g(x'), h(y), h(y') \parallel g(x), g(x'), h(y), h(y')\}$  this technical issue is removed. Obviously,  $\text{gnd}(A) = \text{gnd}(\text{norm}(A))$ , holding for all classes and their normal counterparts.

**Definition 7** (Subsumption). *A class  $B$  subsumes another class  $A$  if for all  $A' \in \text{gnd}(A)$  there exists a  $B' \in \text{gnd}(B)$  such that  $A' \subseteq B'$ .*

The following definitions and lemmas prepare termination, Lemma 21. We show that we can not create infinitely many classes restricted by  $\beta$  such that each new class is not subsumed by any existing class, guaranteeing termination.

**Definition 8.** *Let  $A = \{\Gamma_1 \parallel s_1, \dots, \Gamma_n \parallel s_n\}$  be a class and  $\beta$  a ground term.  $A$  is constrained by  $\beta$  (or  $\beta$ -constrained) iff  $s_i \preceq \beta \in \Gamma_i$  for all  $1 \leq i \leq n$ .*

**Lemma 9.** *Let  $\beta$  be a ground term and  $A$  a  $\beta$ -constrained class. Then  $\text{gnd}(A) \in \mathcal{P}(\mathcal{T}_{\preceq\beta})$ , the powerset of  $\mathcal{T}_{\preceq\beta}$ .*

*Proof.* For any  $B \in \text{gnd}'(A)$  there exists a  $\sigma$  such that  $B = \{(\Gamma\sigma \parallel s\sigma) \mid (\Gamma \parallel s) \in A \text{ and } \Gamma\sigma \text{ satisfiable}\}$ . Thus for any  $\Gamma\sigma \parallel s\sigma \in B$  we have  $s\sigma \preceq \beta \in \Gamma\sigma$ . Thus  $B$  is  $\beta$ -constrained. For any  $A' \in \text{gnd}(A)$  we have  $A' = \bigcup_{\sigma} \text{grounding for } B \{s\sigma \mid (\Gamma \parallel s) \in B \text{ and } \Gamma\sigma \text{ true}\}$  for some  $B \in \text{gnd}'(A)$ . Thus for any  $s\sigma \in A'$  we have  $s\sigma \preceq \beta$ , since  $B$  is  $\beta$ -constrained and  $s\sigma$  is ground. Thus  $A' \subseteq \mathcal{T}_{\preceq\beta}$ . Thus  $\text{gnd}(A) \subseteq \mathcal{P}(\mathcal{T}_{\preceq\beta})$ .  $\square$

**Lemma 10.** *Let  $\beta$  be a ground term. There exists no infinite chain of (possibly non-ground)  $\beta$ -constrained classes  $A_0, A_1, \dots$  such that for all  $i \geq 0$ ,  $A_i$  is not subsumed by any  $B \in \{A_0, \dots, A_{i-1}\}$ .*

*Proof.* Assume there exists such a chain. Let  $\mathcal{P}(\mathcal{T}_{\preceq\beta})$  be the powerset of  $\mathcal{T}_{\preceq\beta}$ . Since  $\mathcal{T}_{\preceq\beta}$  is finite,  $\mathcal{P}(\mathcal{T}_{\preceq\beta})$  is finite as well. There are only  $2^{|\mathcal{T}_{\preceq\beta}|}$  different subsets in  $\mathcal{P}(\mathcal{T}_{\preceq\beta})$ . For any  $A$  in the chain it holds  $\text{gnd}(A) \in \mathcal{P}(\mathcal{T}_{\preceq\beta})$  by Lemma 9. If there exist indices  $i \neq j$  such that  $\text{gnd}(A_i) = \text{gnd}(A_j)$  then  $A_j$  subsumes  $A_i$  and vice versa contradicting the assumption. Thus, for any pair of indices  $i \neq j$  in the chain it has to hold  $A_i \neq A_j$ . But there are only finitely many different subsets. Contradiction.  $\square$

**Definition 11.** *Let  $A = \{\Gamma_1 \parallel s_1, \dots, \Gamma_n \parallel s_n\}$  be a class. The set  $\text{vars}(A)$  is defined as  $\bigcup_{1 \leq i \leq n} (\bigcup_{t \in \Gamma_i} \text{vars}(t)) \cup \text{vars}(s_i)$ .*

A state of  $\text{CC}(\mathcal{X})$  is a finite set of congruence classes. For a state  $\Pi = \{A_1, \dots, A_n\}$  we define  $\text{gnd}(\Pi) = \text{gnd}(A_1) \cup \dots \cup \text{gnd}(A_n)$ . Let  $\Pi$  be a state. For any classes  $\{A, B\} \subseteq \Pi$  with  $A \neq B$ , we assume that  $\text{vars}(A) \cap \text{vars}(B) = \emptyset$  at any time during execution. Now given a set of equations  $E$ , where  $\text{gnd}_{\preceq\beta}(s \approx t) \neq \emptyset$  for all  $s \approx t \in E$  the initial state of  $\text{CC}(\mathcal{X})$  is

$$\Pi = \{ \{s \preceq \beta \wedge t \preceq \beta \parallel s, s \preceq \beta \wedge t \preceq \beta \parallel t\} \mid s \approx t \in E \} \cup \{ \{f_i(x_{1_i}, \dots, x_{k_i}) \preceq \beta \parallel f_i(x_{1_i}, \dots, x_{k_i})\} \mid f_i \in \Omega \}$$

In particular, the linear single term classes  $f_i(x_{1_i}, \dots, x_{k_i})$  are needed for rule Deduction to build terms that are not contained in  $E$  as a subterm but  $\preceq \beta$ . We present our algorithm in the form of two abstract rewrite rules:

**Merge**  $\Pi \cup \{A, B\} \Rightarrow_{CC(\mathcal{X})} \Pi \cup \{A, B, (A' \cup B')\mu\}$   
provided  $norm(A) = \{\Gamma_1 \parallel s_1, \dots, \Gamma_n \parallel s_n\}$ ,  $norm(B) = \{\Delta_1 \parallel t_1, \dots, \Delta_n \parallel t_n\}$ , there exist  $(\Gamma \parallel s) \in A, (\Delta \parallel t) \in B$  and  $\mu$  such that  $\mu = mgu(s, t)$ ,  $A' = \{\Gamma_1 \wedge \Gamma \wedge \Delta \parallel s_1, \dots, \Gamma_n \wedge \Gamma \wedge \Delta \parallel s_n\}$ ,  $B' = \{\Delta_1 \wedge \Gamma \wedge \Delta \parallel t_1, \dots, \Delta_n \wedge \Gamma \wedge \Delta \parallel t_n\}$ , there exists no  $A'' \in \Pi \cup \{A, B\}$  such that  $(A' \cup B')\mu$  is subsumed by  $A''$ .

The rule *Merge* takes as input two classes where a term in the first class is unifiable with a term in the second class. The result is the union of their normal classes with the unifier applied. For termination it is crucial to check if there exists a class that subsumes the newly generated class. Note that the *Merge* rule can be seen as a generalization of the *Merge* rule in  $\Rightarrow_{CC}$ .

**Deduction**  $\Pi \cup \{A, B\} \Rightarrow_{CC(\mathcal{X})} \Pi \cup \{A, B, \{\Gamma' \parallel f(s'_1, \dots, s'_n), \Gamma' \parallel f(t'_1, \dots, t'_n)\}\mu\}$   
provided  $\Gamma \parallel f(s_1, \dots, s_n) \in A, \Delta \parallel f(t_1, \dots, t_n) \in B$ , and for each  $0 < i \leq n$ , there exists a  $D_i \in \Pi$  such that  $\Gamma_i \parallel s'_i \in norm(D_i), \Delta_i \parallel t'_i \in norm(D_i)$ ,  $\mu$  is a simultaneous mgu of  $f(s'_1, \dots, s'_n) = f(s_1, \dots, s_n)$  and  $f(t'_1, \dots, t'_n) = f(t_1, \dots, t_n)$ ,  $\Gamma' = \Gamma \wedge \Delta \wedge \Gamma_1 \wedge \dots \wedge \Gamma_n \wedge \Delta_1 \wedge \dots \wedge \Delta_n$ , there exists no  $A' \in \Pi \cup \{A, B\}$  such that  $\{\Gamma' \parallel f(s'_1, \dots, s'_n), \Gamma' \parallel f(t'_1, \dots, t'_n)\}\mu$  is subsumed by  $A'$ .

The rule *Deduction* creates a new class if there exist terms with the same top symbol in two different (copies of) classes such that their arguments are unifiable with terms that are in the same class. Again *Deduction* is a generalization of the *Deduction* rule from  $\Rightarrow_{CC}$ . Note, that in *Merge* and *Deduction*  $A$  and  $B$  can be identical. In this case we assume the consideration of a renamed copy. Furthermore, in both rules we inherit all parent constraints for the new class. Using this invariant, we could also represent each class by a single constraint that is not dedicated to a term. We do not do so in order to get a nicer representation, the way constraints are composed depending on the term they belong to. Our way of constraint composition can also result in constraints containing variables that do not occur in any term of the class anymore. We'll take care of these constraints in Section 4.

Note that a large number of redundant classes can be created. While these redundant classes affect neither soundness nor completeness getting rid of redundant classes is essential for an efficient implementation. To this end we introduce a Subsumption rule that has precedence over all other rules.

**Subsumption**  $\Pi \cup \{A, B\} \Rightarrow_{CC(\mathcal{X})} \Pi \cup \{B\}$   
provided  $B$  subsumes  $A$ .

**Example 12.** Suppose we have the following equations:  $g(x) \approx a, h(y) \approx a, g(h(z)) \approx h(h(z))$ . Initially, without single term classes, we get

$$\Pi = \{\{g(x), a \parallel g(x), a\}, \{h(y), a \parallel h(y), a\}, \{g(h(z)), h(h(z)) \parallel g(h(z)), h(h(z))\}\}$$

Merging the last class with the second class we get

$$\{g(h(z)), h(h(z)), h(y), a \parallel g(h(z)), h(h(z)), h(y), a\}$$



We can now merge this new class with the first class to get:

$$\{g(h(z)), h(h(z)), a, h(y), g(x) \parallel g(h(z)), h(h(z)), a, h(y), g(x)\}$$

This class subsumes all other classes, for example in our ordering defined in section 4. So this would be the final result. Note that this result is independent of the chosen  $\beta$ . No matter how large  $\beta$  is the result of the calculus is always the same (assuming that  $\beta$  allows for the initial classes).

Another example where the number of classes is dependant on  $\beta$  is shown below.

**Example 13.** Suppose we have the single equation  $f(x) \approx g(x)$ . Initially we have  $\Pi = \{\{f(x), g(x) \parallel f(x), g(x)\}\}$ . Depending on the size of  $\beta$  we get more and more classes with the deduction rule, like  $\{f(f(x)), f(g(x)), f(x), g(x) \parallel f(f(x)), f(g(x))\}$  and  $\{g(f(x)), g(g(x)), f(x), g(x) \parallel g(f(x)), g(g(x))\}$ . Which we can again merge with the first class to get

$$\{f(f(x)), f(g(x)), g(f(x)), g(g(x)), f(x), g(x) \parallel \\ f(f(x)), f(g(x)), g(f(x)), g(g(x))\}$$

Increasing  $\beta$  further we get even larger classes. This is an example where we gain quite little compared to congruence closure.

The following example shows that Merge also has to be applied to two instances of the same class.

**Example 14.** Assume initial classes (without single term classes):

$$\Pi = \{\{f(x, y), g(x, y) \parallel f(x, y), g(x, y)\}, \\ \{f(x, y), g(y, x) \parallel f(x, y), g(y, x)\}\}$$

Now we can merge the classes by unifying  $f(x, y)$ :

$$\{f(x, y), g(x, y), g(y, x) \parallel f(x, y), g(x, y), g(y, x)\}$$

The new class subsumes both initial classes. To get the final result we have to merge this new class with itself by unifying  $g(x, y)$  and  $g(y, x)$  to get:

$$A = \{f(x, y), g(x, y), g(y, x), f(y, x) \parallel \\ f(x, y), g(x, y), g(y, x), f(y, x)\}$$

Otherwise, e.g.  $\{f(a, b), f(b, a)\} \not\subseteq A'$  for all  $A' \in \text{gnd}(A)$  for an appropriate set of function symbols in  $\Omega$ .

Note, that  $\text{CC}(\mathcal{X})$  does not always guarantee less or equally many Congruence Classes than CC. Consider the following example

**Example 15.** Let  $f(a) \approx h(a), g(a) \approx h(a), f(b) \approx h(b), g(b) \approx h(b), f(x) \approx g(x), a \approx f(a), b \approx f(b)$  be some input equations. Further assume that the ground terms occurring in the input equations are the only ground terms smaller than a given  $\beta$ . Initially  $CC(\mathcal{X})$  contains a class for the terms in each equation. Note, that Subsumption is not applicable in this state. Now, multiple Merge operations are possible, but no matter in which sequence they are applied the result is always

$$\{\{f(a), h(a), g(a), a \parallel f(a), h(a), g(a), a\}, \{f(b), h(b), g(b), b \parallel f(b), h(b), g(b), b\}, \\ \{f(x), g(x) \parallel f(x), g(x)\}\}$$

Subsumption is not applicable to this set of classes. In ground congruence closure, however, we only get two classes:

$$\{\{f(a), h(a), g(a), a\}, \{f(b), h(b), g(b), b\}\}$$

In the special case of equations with flat terms, where the left-hand side is variable disjoint to the right-hand side and every variable occurs only once,  $CC(\mathcal{X})$  terminates even without constraints as shown in the following lemma.

**Lemma 16.** Let  $E$  be a set of equations of the form  $f(x_1, \dots, x_n) \approx g(y_1, \dots, y_m)$ . Then  $CC(\mathcal{X})$  terminates on  $E$  with empty constraints.

*Proof.* We prove that

1. the terms stay flat, i.e. Deduction is never applicable and if Merge is applicable, then  $\mu$  is a renaming and
2. the number of Merge operations is at most  $|E| - 1$

Since there are no constraints and no separating variables, any subsumption check reduces to a check if there exists a term in the subsuming class and a matcher for the free variables for every term in the subsumed class.

Assume that Deduction is applicable. Then there exists a  $f(x_1, \dots, x_n)$  in  $A$  and  $f(y_1, \dots, y_n)$  in  $B$ . Deduction would now create a new class  $\{f(s_1, \dots, s_n), f(t_1, \dots, t_n)\}$ . But there already exists a class  $\{f(x_1, \dots, x_n), g(y_1, \dots, y_m), \dots\}$  with no constraints. Thus there exists two matchers  $\delta, \delta'$  such that  $f(x_1, \dots, x_n)\delta = f(s_1, \dots, s_n)$  and  $f(x_1, \dots, x_n)\delta' = f(t_1, \dots, t_n)$ . Thus  $\{f(s_1, \dots, s_n), f(t_1, \dots, t_n)\}$  is subsumed.

Assume that Merge is applicable to classes  $A$  and  $B$ . Then there exists a  $f(x_1, \dots, x_n)$  in  $A$  and  $f(y_1, \dots, y_n)$  in  $B$ . Then  $\mu$  is a renaming. If Merge is applied to the same class, i.e. if  $B$  is a renaming of  $A$ , then the resulting class is obviously subsumed by  $A$ . So  $A$  and  $B$  must be different. Let  $C$  be the resulting class.  $C$  subsumes  $A$  and  $B$ , since for every  $t \in A$  there exists a  $t' \in C$  such that there exists a matcher  $\delta$  such that  $t'\delta = t$  and the constraints are empty, and analogously for  $B$ .

Since Deduction is never applicable and Merge always creates a class that subsumes the merged classes, the number of Merge operations is at most  $|E| - 1$ , since every Merge operation reduces the total number of classes by 1. Thus  $CC(\mathcal{X})$  terminates with the correct result for empty constraints.  $\square$

We will now prove termination, soundness and completeness. We start with soundness.

**Lemma 17.** *Let  $A$  be a class. There exists a  $A' \in \text{gnd}(A)$  s.t. for all  $s, t: \{s, t\} \subseteq A'$  iff there exists a substitution  $\sigma'$  such that  $\{s, t\} \subseteq \text{norm}(A)\sigma'$ .*

*Proof.* Let  $X$  be the separating and  $Y$  be the free variables of  $A$ . Let  $\tau$  be the renaming that maps the free variables to fresh variables to create the normal class.

Assume  $\{s, t\} \subseteq A'$  for some  $A' \in \text{gnd}(A)$ . There must exist terms  $\{\Gamma \parallel s', \Delta \parallel t'\} \subseteq A$  and substitutions  $\sigma : X \rightarrow \mathcal{T}(\Omega, \emptyset), \delta : Y \rightarrow \mathcal{T}(\Omega, \emptyset), \delta' : Y \rightarrow \mathcal{T}(\Omega, \emptyset)$  such that  $s'\sigma\delta = s$  and  $t'\sigma\delta' = t$  by definition 4. Let  $\delta' = \{x_1 \rightarrow s_1, \dots, x_n \rightarrow s_n\}$ . Construct  $\delta'' = \{x_1\tau \rightarrow s_1, \dots, x_n\tau \rightarrow s_n\}$ . Now we can construct  $\sigma'$  to be  $\sigma\delta\delta''$  and we are done, since  $\{\Gamma' \parallel s', \Delta' \parallel t'\tau\} \subseteq \text{norm}(A)$  and  $s'\sigma' = s$  and  $t'\tau\sigma' = t$ .

Now assume there exists a substitution  $\sigma'$  such that  $\{\Gamma\sigma' \parallel s'\sigma', \Delta\sigma' \parallel t'\sigma'\} \subseteq \text{norm}(A)\sigma'$  and  $s'\sigma' = s$  and  $t'\sigma' = t$ . Define  $\sigma : X \rightarrow \mathcal{T}(\Omega, \emptyset)$  and  $\delta : (Y \cup Y\tau) \rightarrow \mathcal{T}(\Omega, \emptyset)$  such that  $\sigma' = \sigma\delta$ . Let  $\tau'$  be the reverse renaming of  $\tau$ . Let  $\delta = \{x_1 \rightarrow s_1, \dots, x_n \rightarrow s_n, y_1 \rightarrow t_1, \dots, y_m \rightarrow t_m\}$ , where the  $y_i$  are the fresh variables introduced by  $\tau$ . Construct  $\delta' = \{x_1 \rightarrow s_1, \dots, x_n \rightarrow s_n\}$  and  $\delta'' = \{y_1\tau' \rightarrow t_1, \dots, y_m\tau' \rightarrow t_m\}$ . Now there must exist  $\{\Gamma\tau' \parallel s'\tau', \Delta\tau' \parallel t'\tau'\} \subseteq A$  such that  $(s'\tau'\sigma'\delta' = s \text{ or } s'\tau'\sigma'\delta'' = s)$  and  $(t'\tau'\sigma'\delta'' = t \text{ or } t'\tau'\sigma'\delta' = t)$ .  $\square$

**Lemma 18.** *Let  $E$  be a finite set of possibly non-ground equations and  $\beta$  a ground term. Let  $A$  be a class where all constraints are the same,  $X$  separating variables,  $Y$  free variables of  $A$  and  $\text{gnd}_{\preceq\beta}(E) \models s\sigma \approx t\sigma$  for all  $\{s\sigma, t\sigma\} \subseteq A\sigma$  and grounding  $\sigma$ . Then for all  $\Gamma \parallel s \in A$  we have  $\text{gnd}_{\preceq\beta}(E) \models s\sigma\delta \approx s\sigma\delta'$  for all  $\sigma : X \rightarrow \mathcal{T}(\Omega, \emptyset), \delta : Y \rightarrow \mathcal{T}(\Omega, \emptyset)$  and  $\delta' = \{y \mapsto \alpha \mid \alpha \text{ a smallest term according to } \preceq, y \in Y\}$ ,  $\Gamma\sigma\delta$  satisfiable.*

*Proof.* Let  $Y'$  be the free variables of  $s$ . Choose  $y' \in Y'$ . There must exist a  $\Gamma \parallel t \in A$  s.t.  $y' \notin \text{vars}(t)$ . By assumption  $\text{gnd}_{\preceq\beta}(E) \models s\sigma\delta \approx t\sigma\delta$ . Now let  $\delta''$  be  $\delta$  but  $y'$  maps to  $\alpha$ . Then  $\text{gnd}_{\preceq\beta}(E) \models s\sigma\delta \approx t\sigma\delta''$  since  $t\sigma\delta = t\sigma\delta''$ , and by hypothesis  $\text{gnd}_{\preceq\beta}(E) \models t\sigma\delta'' \approx s\sigma\delta''$ . Obviously the constraints are still satisfiable since we replace by smallest term  $\alpha$ . Now we can continue analogously for  $s\sigma\delta''$  until we reach  $s\sigma\delta'$  which shows the lemma.  $\square$

**Corollary 19.** *Let  $E$  be a finite set of possibly non-ground equations and  $\beta$  a ground term. Let  $A$  be a class where all constraints are the same, and  $\text{gnd}_{\preceq\beta}(E) \models s\sigma \approx t\sigma$  for all  $\{s\sigma, t\sigma\} \subseteq A\sigma$  and grounding  $\sigma$ . Then  $\text{gnd}_{\preceq\beta}(E) \models s\sigma \approx t\sigma$  for all  $\{s\sigma, t\sigma\} \subseteq \text{norm}(A)\sigma$  and grounding  $\sigma$ .*

*Proof.* Follows from lemma 17 and 18.  $\square$

**Lemma 20** ( $\Rightarrow_{\text{CC}(\mathcal{X})}$  is sound). *Let  $E$  be a finite set of possibly non-ground equations and  $\beta$  a ground term. For any run of  $\Rightarrow_{\text{CC}(\mathcal{X})}$ , any state  $\Pi'$  in this run and for all terms  $s, t$  and grounding substitution  $\sigma$  such that there exists a class  $A \in \Pi'$  such that  $\{\Gamma \parallel s, \Delta \parallel t\} \subseteq \text{norm}(A)$ ,  $\Gamma\sigma$  and  $\Delta\sigma$  satisfiable, it holds that  $\text{gnd}_{\preceq\beta}(E) \models s\sigma \approx t\sigma$ .*

*Proof.* It suffices to show this lemma for all  $\{\Gamma \parallel s, \Delta \parallel t\} \subseteq A$ . Since constraints are always the same for each class in a run it follows for all  $\{\Gamma \parallel s, \Delta \parallel t\} \subseteq \text{norm}(A)$  by corollary 19. Proof by induction. Initially  $\Pi$  is such that  $\{s, t \parallel s, t\} \subseteq \Pi$  for all  $s \approx t \in E$ . Now assume a grounding substitution  $\sigma$  such that  $s\sigma \preceq \beta$  and  $t\sigma \preceq \beta$ . Then  $(s \approx t)\sigma \in \text{gnd}_{\preceq\beta}(E)$ . The initial  $\{f_i(x_1, \dots, x_{k_i}) \preceq \beta \parallel f_i(x_1, \dots, x_{k_i})\}$  are single term classes. So the assumption holds. Now assume that the assumption holds for  $\Pi$  and we apply a rule:

1) assume that *Subsumption* is applied. Then  $B$  subsumes  $A$ . Thus for all  $A' \in \text{gnd}(A)$  there exists a  $B' \in \text{gnd}(B)$  such that  $A' \subseteq B'$ . Thus we only remove redundant classes, so the assumption holds by i.h.

2) assume that *Merge* is applied. Then there exists  $\Gamma \parallel s \in A, \Delta \parallel t \in B$  and  $\mu = \text{mgu}(s, t)$ . We show that  $\text{gnd}_{\preceq\beta}(E) \models s'\mu\sigma \approx t'\mu\sigma$  for all  $\{\Gamma'\mu \parallel s'\mu, \Delta'\mu \parallel t'\mu\} \subseteq (A' \cup B')\mu$  and grounding  $\sigma$  such that  $\Gamma'\mu\sigma$  and  $\Delta'\mu\sigma$  satisfiable. Let  $\sigma' = \mu\sigma$ . By i.h.  $\text{gnd}_{\preceq\beta}(E) \models s'\sigma' \approx s\sigma'$  for  $\Gamma'' \parallel s' \in \text{norm}(A)$ , since  $\Gamma'' \subseteq \Gamma'$  and  $\Gamma \subseteq \Gamma'$ , and analogously for  $t'\sigma' \approx t\sigma'$ . Now we have  $s'\sigma' \approx s\mu\sigma = t\mu\sigma \approx t'\sigma'$ . Thus by transitivity of equality it holds  $\text{gnd}_{\preceq\beta}(E) \models s'\mu\sigma \approx t'\mu\sigma$ .

3) assume that *Deduction* is applied. By i.h.  $\text{gnd}_{\preceq\beta}(E) \models s'_i\sigma \approx t'_i\sigma$  for all grounding  $\sigma$  such that  $\Gamma_i\sigma$  and  $\Delta_i\sigma$  are satisfiable and  $1 \leq i \leq n$ . Thus, by congruence of equality,  $\text{gnd}_{\preceq\beta}(E) \models f(s'_1, \dots, s'_n)\sigma \approx f(t'_1, \dots, t'_n)\sigma$  for all  $\sigma$  such that  $\Gamma'\sigma$  satisfiable, since  $\Gamma' = \Gamma \wedge \Delta \wedge \Gamma_1 \wedge \dots \wedge \Gamma_n \wedge \Delta_1 \wedge \dots \wedge \Delta_n$ . Thus  $\text{gnd}_{\preceq\beta}(E) \models f(s'_1, \dots, s'_n)\mu\sigma \approx f(t'_1, \dots, t'_n)\mu\sigma$  for all  $\sigma$  such that  $\Gamma'\mu\sigma$  satisfiable, since  $f(s'_1, \dots, s'_n)\mu$  and  $f(t'_1, \dots, t'_n)\mu$  are instances of  $f(s'_1, \dots, s'_n)$  and  $f(t'_1, \dots, t'_n)$ .  $\square$

**Lemma 21** ( $\Rightarrow_{\text{CC}(\mathcal{X})}$  is Terminating). *Let  $E$  be a finite set of possibly non-ground equations and  $\beta$  a ground term. For any run of  $\Rightarrow_{\text{CC}(\mathcal{X})}$  we reach a state, where no rule of  $\Rightarrow_{\text{CC}(\mathcal{X})}$  is applicable anymore.*

*Proof.* By Lemma 10 there are only finitely many possible  $\beta$ -constrained classes that are not subsumed. Since all terms are constraint by  $\beta$  in  $\Rightarrow_{\text{CC}(\mathcal{X})}$  and *Merge* and *Deduction* check if the new class is subsumed by another class, they can be applied only finitely often. A class removed by *Subsumption* cannot be added again by *Merge* or *Deduction* since it is subsumed by another class in  $\Pi$ . Thus  $\Rightarrow_{\text{CC}(\mathcal{X})}$  is terminating.  $\square$

**Lemma 22** ( $\Rightarrow_{\text{CC}(\mathcal{X})}$  is Complete). *Let  $E$  be a finite set of possibly non-ground equations and  $\beta$  a ground term. Let  $\Pi$  be the result of a run of  $\Rightarrow_{\text{CC}(\mathcal{X})}$  such that no rule of  $\Rightarrow_{\text{CC}(\mathcal{X})}$  is applicable anymore. Then for all  $\{s, t\} \subseteq \mathcal{T}_{\preceq\beta}$  such that  $\text{gnd}_{\preceq\beta}(E) \models s \approx t$  there exists a class  $A \in \Pi$ ,  $\{\Gamma \parallel s', \Delta \parallel t'\} \subseteq \text{norm}(A)$  and grounding substitution  $\sigma$  such that  $s'\sigma = s$  and  $t'\sigma = t$  and  $\Gamma\sigma, \Delta\sigma$  satisfiable.*

*Proof.* We show by induction for any sequence  $E_1 \Rightarrow_{EQ} \dots \Rightarrow_{EQ} E_n$  of applications of  $\Rightarrow_{EQ}$  with  $E_1 = \text{gnd}_{\preceq\beta}(E)$  there exists a sequence  $\Pi_0 \Rightarrow_{\text{CC}(\mathcal{X})} \dots \Rightarrow_{\text{CC}(\mathcal{X})} \Pi_m$  of applications of  $\Rightarrow_{\text{CC}(\mathcal{X})}$  rules such that for all  $s \approx t \in E_n$ , where  $s \preceq \beta$  and  $t \preceq \beta$ , there exists a class  $A \in \Pi_m$ ,  $\Gamma \parallel l \in \text{norm}(A), \Delta \parallel r \in \text{norm}(A)$  and a substitution  $\sigma$  such that  $l\sigma \approx r\sigma = s \approx t$ ,  $\Gamma\sigma, \Delta\sigma$  satisfiable. Initially, this is true, since  $\{s, t \parallel s, t\} \in \Pi_0$  for

all  $s \approx t \in E$ . Since reasoning is based on ground terms only, we can ignore the *Instance* rule of  $\Rightarrow_{EQ}$ . Now assume we are in step  $i$ .

1) Reflexivity.  $E_i \Rightarrow_{EQ} E_i \cup \{t \approx t\}$ ,  $t = f(s_1, \dots, s_n) \preceq \beta$ . Then  $t \in (\{f_i(x_{1_i}, \dots, x_{k_i}) \preceq \beta \parallel f_i(x_{1_i}, \dots, x_{k_i})\} \sigma)$  for  $\sigma = \{x_{j_i} \mapsto s_j \mid 1 \leq j \leq n\}$ .

2) Symmetry.  $E_i \cup \{t \approx t'\} \Rightarrow_{EQ} E_i \cup \{t \approx t', t' \approx t\}$ ,  $t, t' \preceq \beta$ . Then by i.h. there exists a class  $A \in \Pi$  such that  $\{l\sigma, r\sigma\} \subseteq norm(A)\sigma$  and  $(l \approx r)\sigma = t \approx t'$  for some substitution  $\sigma$  because  $norm(A)$  is normal. But then also  $(r \approx l)\sigma = t' \approx t$ .

3) Transitivity.  $E_i = E'_i \cup \{s \approx t \wedge t \approx s'\} \Rightarrow_{EQ} E_i \cup \{s \approx s'\} = E_{i+1}$ ,  $s, s', t \preceq \beta$ . By hypothesis there must exist  $\{A, B\} \subseteq \Pi$ ,  $\{\Gamma \parallel l, \Delta \parallel r\} \subseteq norm(A)$ ,  $\{\Gamma' \parallel l', \Delta' \parallel r'\} \subseteq norm(B)$ , a grounding substitution  $\sigma$ , such that  $(l \approx r)\sigma = s \approx t$  and  $(l' \approx r')\sigma = t \approx s'$  and  $\Gamma\sigma, \Delta\sigma, \Gamma'\sigma, \Delta'\sigma$  all satisfiable. If  $(A' \cup B')\mu$  is subsumed by some  $C \in \Pi$ , then we are already done, since there exists a  $C' \in gnd(C)$  such that  $\{s, s'\} \subseteq C'$ . Otherwise *Merge* is applicable and  $(A' \cup B')\mu$  added to the state. Then  $\{\Gamma \wedge \Delta \wedge \Gamma' \parallel l, \Delta \wedge \Gamma' \parallel r, \Delta \wedge \Gamma' \parallel l', \Delta' \wedge \Delta \wedge \Gamma' \parallel r'\}\mu \subseteq (A' \cup B')\mu$  by the definition of *Merge*. Obviously,  $(\Gamma \wedge \Delta \wedge \Gamma' \wedge \Delta')\mu$  is satisfiable since  $(\Gamma \wedge \Delta \wedge \Gamma' \wedge \Delta')\sigma$  is satisfiable. Thus there exists a  $\sigma'$  such that  $\{s, s'\} \subseteq (A' \cup B')\mu\sigma'$ .

4) Congruence.  $E_i = E'_i \cup \{s_1 \approx t_1, \dots, s_m \approx t_m\} \Rightarrow_{EQ} E_i \cup \{f(s_1, \dots, s_m) \approx f(t_1, \dots, t_m)\} = E_{i+1}$ , where  $f(s_1, \dots, s_m), f(t_1, \dots, t_m) \preceq \beta$ . By hypothesis there must exist  $\{A_1, \dots, A_m\} \subseteq \Pi$ ,  $\{\Gamma_i \parallel l_i, \Delta_i \parallel r_i\} \subseteq norm(A_i)$  because  $norm(A_i)$  is normal and a grounding substitution  $\sigma$  such that  $(l_i \approx r_i)\sigma = s_i \approx t_i$  and  $\Gamma_i\sigma, \Delta_i\sigma$  satisfiable. Now take two renamed copies of  $\{f_i(x_{1_i}, \dots, x_{k_i}) \preceq \beta \parallel f_i(x_{1_i}, \dots, x_{k_i})\}$  and grounding substitutions  $\sigma_1, \sigma_2$  such that  $f(x'_1, \dots, x'_m)\sigma_1 = f(s_1, \dots, s_m)$  and  $f(y'_1, \dots, y'_m)\sigma_2 = f(t_1, \dots, t_m)$  where the respective constraints are obviously satisfied. Thus there must exist a simultaneous most general unifier  $\mu$  as defined in the *Deduction* rule. If  $\{\Gamma'\mu \parallel f(l_1, \dots, l_m)\mu, \Gamma'\mu \parallel f(r_1, \dots, r_m)\mu\}$  is subsumed by some  $C \in \Pi$ , then we are already done, since there exists a  $C' \in gnd(C)$  such that  $\{f(s_1, \dots, s_m), f(t_1, \dots, t_m)\} \subseteq C'$ . Otherwise *Deduction* is applicable and  $\{\Gamma'\mu \parallel f(l_1, \dots, l_m)\mu, \Gamma'\mu \parallel f(r_1, \dots, r_m)\mu\}$  added to the state. Since  $\Gamma'\sigma$  is satisfiable  $\{f(s_1, \dots, s_m), f(t_1, \dots, t_m)\} \subseteq \{\Gamma'\mu \parallel f(l_1, \dots, l_m)\mu, \Gamma'\mu \parallel f(r_1, \dots, r_m)\mu\}\sigma$  has to hold.  $\square$

## 4 Implementation

We have implemented  $\Rightarrow_{CC(\mathcal{X})}$  on top of SPASS-SATT [7] due to its linear integer arithmetic solving capabilities. We provide pseudo code of the implementation. The pseudo code is intended to give an idea of the implementation and not to present the concrete details of the implementation. For example, the use of path index and discrimination tree is missing.

We process classes using a *worked-off* and *usable* queue. Initially the *worked-off* queue contains all single-term classes and *usable* contains the initial classes that are created from the input equations. In each loop we select a class from the *usable* queue, perform all possible *Merge* and *Deduction* steps on it and add the class to the *worked-off* queue afterwards if not subsumed. Newly created classes are added to the usable queue.

Algorithm 1 shows the initial state and main loop of our implementation. There is also

a first optimisation option here, namely which classes should be picked from the usable queue first. Our heuristic selects the classes with the fewest terms and the most variables from the usable queue, or if the number of terms and variables are equal, then the class with the fewest separating variables. Various benchmarks have shown that this produces the best results.

---

**Algorithm 1** Main function of the algorithm

---

```

function MAIN( $E$ )
  for all  $s \approx t \in E$  do
     $C_{new \rightarrow terms} = \{s, t\}$ 
     $C_{new \rightarrow cstrs} = \{s, t\}$ 
     $us = \text{Push}(us, C_{new})$ 
  end for
  for all  $f \in \Omega$ ,  $\text{arity}(f) = n$  do
     $C_{new \rightarrow terms} = \{f(x_1, \dots, x_n)\}$ 
     $C_{new \rightarrow cstrs} = \{f(x_1, \dots, x_n)\}$ 
     $wo = \text{Push}(wo, C)$ 
  end for
  while  $us \neq \emptyset$  do
     $C = \text{Pop}(us)$ 
    Merge( $C$ )
    Deduct( $C$ )
     $wo = \text{Push}(wo, C)$ 
  end while
end function

```

---

Algorithm 2 sketches the implementation of the merge function. Here the implementation follows the rules, except that subsumption is checked directly after the new class is created and the code performs all possible merge operations of the input class. For the subsumption function, an order must be defined first, hence it will be given later.

In the following, we describe refinements and optimizations of the  $\text{CC}(\mathcal{X})$  calculus towards an implementation. We start with a simplification of the Deduction rule. It suffices to use only the single term classes for  $A$  and  $B$  in the Deduction rule.

**Lemma 23.** *Assume a state  $\Pi$  such that Deduction is applicable for some  $\{A, B\} \subseteq \Pi$  and  $\Gamma \parallel f(s_1, \dots, s_n) \in A, \Delta \parallel f(t_1, \dots, t_n) \in B$ . Let  $\mu$  be the resulting simultaneous mgu and  $\{\Gamma_i \parallel s'_i, \Delta_i \parallel t'_i\} \subseteq \text{norm}(D_i)$  for all  $1 \leq i \leq n$  such that  $\{\Gamma' \parallel f(s'_1, \dots, s'_n), f(t'_1, \dots, t'_n)\} \mu$  is the resulting new class. Then Deduction is applicable for two variable disjoint copies of the single term class  $\{f(x_1, \dots, x_n) \parallel f(x_1, \dots, x_n)\}$ .*

*Proof.* We build a unifier  $\mu' = \{x_1 \rightarrow s'_1, \dots, x_n \rightarrow s'_n, y_1 \rightarrow t'_1, \dots, y_n \rightarrow t'_n\}$  for the single term class and the renamed single term class  $\{f(y_1, \dots, y_n) \parallel f(y_1, \dots, y_n)\}$ . Then  $\Gamma'' = f(x_1, \dots, x_n) \preceq \beta \wedge f(y_1, \dots, y_n) \preceq \beta \wedge \Gamma_1 \wedge \dots \wedge \Gamma_n \wedge \Delta_1 \wedge \dots \wedge \Delta_n$ . The resulting class is thus  $\{\Gamma'' \parallel f(s'_1, \dots, s'_n), f(t'_1, \dots, t'_n)\} \mu'$ .  $\square$

---

**Algorithm 2** Merge function

---

```
function MERGE( $C_0$ )  
  for  $C_1$  in  $wo$  do  
    for each  $(t_0, t_1) \in \{(t_0, t_1) \mid t_0 \in C_0 \rightarrow terms \wedge t_1 \in C_1 \rightarrow terms\}$  do  
      if  $unifiable(t_0, t_1)$  then  
         $\mu = mgu(t_0, t_1)$   
         $C_{new} \rightarrow terms = (C_0 \rightarrow terms \cup C_1 \rightarrow terms)\mu$   
         $C_{new} \rightarrow cstrs = (C_0 \rightarrow cstrs \cup C_1 \rightarrow cstrs)\mu$   
        if  $SAT(C_{new} \rightarrow cstrs)$  then  
          for  $C$  in  $wo \cup us$  do  
            if  $CheckSubsumption(C, C_{new})$  then  
              return  
            end if  
          end for  
          for  $C$  in  $wo \cup us$  do  
            if  $CheckSubsumption(C_{new}, C)$  then  
               $wo = wo \setminus \{C\}$   
               $us = us \setminus \{C\}$   
            end if  
          end for  
           $us = us \cup \{C_{new}\}$   
        end if  
      end if  
    end for  
  end for  
end function
```

---

It is easy to see that the class created by the single term class is always more general than the other classes that can be created by Deduction. Algorithm 3 sketches the implementation of our deduction function. We assume that any function call creates a copy of the input to that function. Note that the constraints are always verified as soon as possible in the actual implementation. To keep the pseudocode simple, we only check the satisfiability of the constraints at the end. There are more optimizations possible here, e.g. the terms in the new class should have at least one argument replaced by terms in the input class. We also take care of this in the actual implementation.

A naive implementation of Subsumption, Definition 7, by ground instantiation results in a practically intractable procedure. Therefore, it is approximated by the below subsumption by matching rule that does not need ground instantiation and is practically tractable, see Section 5.

**Definition 24** (Subsumption by Matching). *Let  $A, B$  be classes. Let  $X$  be the separating variables of  $B$  and  $Y$  the free variables of  $B$ .  $B$  subsumes  $A$  by matching iff there exists a substitution  $\sigma : X \rightarrow \mathcal{T}(\Omega, \text{vars}(A))$  that maps every variable in  $X$ , such that for every  $\Gamma \parallel t \in A$  there is a  $\tau : Y \rightarrow \mathcal{T}(\Omega, \text{vars}(A))$  and  $(\Delta \parallel s)\sigma \in B\sigma$  such that  $t = s\sigma\tau$  and  $\forall\delta.(\Gamma\delta \rightarrow \exists\delta'.\Delta\sigma\tau\delta\delta')$ .*

**Lemma 25.** *Let  $A, B$  be classes. If  $B$  subsumes  $A$  by matching then  $B$  subsumes  $A'$  by matching for all  $A' \in \text{gnd}(A)$ .*

*Proof.* Assume  $B$  subsumes  $A$  by matching. By assumption there exists a substitution  $\sigma$  such that for all  $\Gamma \parallel t \in A$  there exists a  $(\Delta \parallel s)\sigma \in B\sigma$  and  $\tau$  such that  $t = s\sigma\tau$  and  $\forall\delta.(\Gamma\delta \rightarrow \exists\delta'.\Delta\sigma\tau\delta\delta')$ .  $\sigma$  matches all separating variables of  $B$  to terms containing only separating variables of  $A$ . If not, then every  $t \in A$  contains a free variable in  $\text{cdom}(\sigma)$ . But then these are separating variables. Contradiction.

Let  $A' \in \text{gnd}(A)$  and  $\mu : X \rightarrow \mathcal{T}(\Omega)$  be the substitution such that  $A\mu = A'$ , where  $X$  are the separating variables of  $A$ . Now construct substitution  $\sigma' = \sigma\mu$ . Then for all  $(\Gamma \parallel t)\mu \in A'$  there exists a  $(\Delta \parallel s)\sigma' \in B\sigma'$  and  $\tau' = \tau\mu$  such that  $t\mu = s\sigma'\tau'$  and  $\forall\delta.(\Gamma\mu\delta \rightarrow \exists\delta'.\Delta\sigma'\tau'\delta\delta')$ , since  $s\sigma'\tau' = s\sigma\mu\tau\mu = s\sigma\tau\mu$ .

Now let  $A'' \in \text{gnd}(A')$ . We have  $\text{gnd}(A') = \{A''\}$ . Then there exist grounding substitutions  $\sigma_1, \dots, \sigma_n$  such that  $A'' = A'\sigma_1 \cup \dots \cup A'\sigma_n$ . Now, construct  $\sigma'' = \sigma'$ . Then for all  $(\Gamma \parallel t)\mu\sigma_i \in A''$  there exists a  $(\Delta \parallel s)\sigma'' \in B\sigma''$  and  $\tau'' = \tau'\sigma_i$  such that  $t\mu\sigma_i = s\sigma''\tau''$  and  $\forall\delta.(\Gamma\mu\sigma_i\delta \rightarrow \exists\delta'.\Delta\sigma''\tau''\delta\delta')$ , since  $s\sigma''\tau'' = s\sigma\mu\tau\mu\sigma_i = s\sigma\tau\mu\sigma_i$ . □

**Lemma 26.** *Let  $A, B$  be classes. If  $B$  subsumes  $A$  by matching then  $B$  subsumes  $A$ .*

*Proof.* Assume that  $B$  does not subsume  $A$ . Then there exists an  $A' \in \text{gnd}(A)$  and an  $A'' \in \text{gnd}(A')$  such that there exists no  $B' \in \text{gnd}(B)$  such that  $A'' \subseteq B'$ . Now assume that there exists a  $\sigma$  such that for any  $(\Gamma \parallel t)\tau' \in A''$ ,  $\Gamma \parallel t \in A'$  there is a  $(\Delta \parallel s)\sigma \in B\sigma$  and  $\tau$  with  $s\sigma\tau = t\tau'$  and  $\forall\delta.(\Gamma\tau'\delta \rightarrow \exists\delta'.\Delta\sigma\tau\delta\delta')$ . So there exist  $\tau_1, \dots, \tau_n$  such that  $A'' \subseteq B\sigma\tau_1 \cup \dots \cup B\sigma\tau_n$ . Obviously, the free variables of  $B$  are also free variables of  $B\sigma$ .  $B\sigma$  has no separating variables, otherwise  $B\sigma\tau_i$  would not be ground for all  $1 \leq i \leq n$ .



---

**Algorithm 3** Deduction function

---

```
function DEDUCT( $C_0$ )
   $t = a$  with  $a \in \Omega$  and  $\text{arity}(a) = 0$ 
   $wo = wo \cup \{C_0\}$ 
  for each  $f \in \Omega$  with  $\text{arity}(f) = n$  and  $n > 0$  do
     $t_0 = f(t, \dots, t)$ 
     $t_1 = f(t, \dots, t)$ 
    DeductIntern( $t_0, t_1, 0, \text{arity}(f), C_{new}$ )
  end for
   $wo = wo \setminus \{C_0\}$ 
end function
function DEDUCTINTERN( $t_0, t_1, i, n, C_{new}$ )
  if  $i \neq n$  then
    for  $C \in wo$  do
       $C_{new \rightarrow cstrs} = C_{new \rightarrow cstrs} \cup C \rightarrow cstrs$ 
      for  $\{s_0, s_1\} \subseteq C \rightarrow terms$  do
         $t_0 = t_0[s_0]_i$ 
         $t_1 = t_1[s_1]_i$ 
        DeductIntern( $t_0, t_1, i + 1, n, C_{new}$ )
      end for
       $C_{new \rightarrow cstrs} = C_{new \rightarrow cstrs} \setminus C \rightarrow cstrs$ 
    end for
  else
     $C_{new \rightarrow terms} = \{t_0, t_1\}$ 
     $C_{new \rightarrow cstrs} = C_{new \rightarrow cstrs} \cup \{t_0, t_1\}$ 
    if SAT( $C_{new \rightarrow cstrs}$ ) then
      for  $C$  in  $wo \cup us$  do
        if CheckSubsumption( $C, C_{new}$ ) then
          return
        end if
      end for
      for  $C$  in  $wo \cup us$  do
        if CheckSubsumption( $C_{new}, C$ ) then
           $wo = wo \setminus \{C\}$ 
           $us = us \setminus \{C\}$ 
        end if
      end for
       $us = us \cup \{C_{new}\}$ 
    end if
  end if
end function
```

---

Thus  $\text{gnd}(B\sigma) = \{B''\}$  and  $B\sigma\tau_1 \cup \dots \cup B\sigma\tau_n \subseteq B''$ . Thus,  $A'' \subseteq B''$ , contradicting assumption. Thus, by lemma 25  $B$  cannot subsume  $A$  by matching.  $\square$

The converse of Lemma 26 does not hold. Consider symbols  $f, g, a, b, \beta$  such that only  $a, b, f(a), f(b), g(a), g(b) \preceq \beta$  and classes  $A = \{f(x), g(a), g(b) \parallel f(x), g(a), g(b)\}$  and  $B = \{f(a), f(b), g(x) \parallel f(a), f(b), g(x)\}$ . Then neither  $A$  subsumes  $B$  nor  $B$  subsumes  $A$  by subsumption by matching, although  $\text{gnd}(A) = \text{gnd}(B)$ . In addition, for the example in the introduction, the final ground class subsumes the first class with respect to  $\beta$ , but it does not subsume the first class by matching. However, in Section 5 we show that the subsumption by matching rule performs nicely in practice.

It remains to find an appropriate solver for the constraints. Performance is highly dependent on the underlying order that was chosen for the algorithm. In our implementation we decided for a simple ordering that counts the number of symbols of a term.

**Definition 27** (Symbol Count Order). *Let  $s, t$  be two terms. The Symbol Count Order  $\preceq$  is defined as  $s \preceq t$  if  $\text{size}(s) \leq \text{size}(t)$ .*

For example,  $f(x, g(a)) \preceq g(h(a), h(b))$  or  $x \preceq a$ . From now on we consider  $\preceq$  to be the above symbol counting order. Recall that the signature is finite, so the symbol counting order is well-founded. There always exist only finitely many smaller or syntactically equal ground terms for a given maximum term  $t$  and a finite signature. Solving  $\preceq$ -constraints is equivalent to solving linear integer arithmetic constraints. Note that a constraint  $\Gamma$  is satisfiable iff it is satisfiable without applying any substitution, because variables and constants are the smallest terms with symbol count order. Regarding the implication  $\forall\delta.(\Gamma\delta \rightarrow \exists\delta'.\Delta\sigma\tau\delta\delta')$ , see Definition 24, the quantifier alternation can be removed, so  $\forall\delta.(\Gamma\delta \rightarrow \exists\delta'.\Delta\sigma\tau\delta\delta')$  holds iff  $\forall\delta.(\Gamma\delta \rightarrow \Delta\sigma\tau\delta)$  holds.

**Definition 28** (LIA Constraint Abstraction). *Let  $t \preceq \beta$  be a constraint. Let  $\text{vars}(t) = \{x_1, \dots, x_n\}$ . Then  $\text{lic}(t \preceq \beta) = x_1 \geq 1 \wedge \dots \wedge x_n \geq 1 \wedge \#(x_1, t) * x_1 + \dots + \#(x_n, t) * x_n \leq \text{size}(\beta) - (\text{size}(t) - \sum_{1 \leq i \leq n} \#(x_i, t))$  is the linear arithmetic constraint of  $t \preceq \beta$ .*

**Lemma 29** (Correctness LIA Constraint Abstraction). *Let  $t \preceq \beta$  be a constraint,  $\text{vars}(t) = \{x_1, \dots, x_n\}$ .*

1. *For any ground substitution  $\sigma = \{x_i \mapsto s_i \mid 1 \leq i \leq n\}$ : if  $t\sigma \preceq \beta$  is true then  $\text{lic}(t \preceq \beta)\{x_i \mapsto \text{size}(s_i) \mid 1 \leq i \leq n\}$  is true.*
2. *For any substitution  $\sigma = \{x_i \mapsto k_i \mid 1 \leq i \leq n, k_i \in \mathbb{N}\}$ : if  $\text{lic}(t \preceq \beta)\sigma$  is true then  $t\delta \preceq \beta$  is true for all  $\delta = \{x_i \mapsto s_i \mid 1 \leq i \leq n\}$  where all  $s_i$  are ground, and  $\text{size}(s_i) = k_i$ .*

*Proof.* by applying the definitions  $\square$

**Lemma 30.** *Let  $\beta$  be a ground term and  $\Gamma_1 = \{s_1 \preceq \beta \wedge \dots \wedge s_n \preceq \beta\}$  and  $\Gamma_2 = \{t_1 \preceq \beta \wedge \dots \wedge t_m \preceq \beta\}$  be two constraints. Then  $\forall\sigma.(\Gamma_1\sigma \rightarrow \exists\sigma'.\Gamma_2\sigma\sigma')$  iff  $\text{lic}(s_1 \preceq \beta) \wedge \dots \wedge \text{lic}(s_n \preceq \beta) \rightarrow \text{lic}(t_1 \preceq \beta) \wedge \dots \wedge \text{lic}(t_m \preceq \beta)$ .*

*Proof.* Follows from Lemma 29 and the above observation that the quantifier alternation can be removed.  $\square$

Thus checking if a  $\preceq$ -constraint  $\Gamma$  models a  $\preceq$ -constraint  $\Gamma'$  reduces to a linear integer arithmetic implication test. We make use of the linear arithmetic solver implemented in SPASS-SATT [7]. Algorithm 4 shows our implementation of subsumption. The function *BuildLAC*(*constraints*) creates a linear arithmetic constraint as defined in 28 and *LAImplicationTest*(*LAC1*, *LAC0*) is the implementation of the implication test of the linear arithmetic solver.

---

**Algorithm 4** Subsumption function

---

```

function CHECKSUBSUMPTION( $C_0, C_1$ )
  if  $C_0 \rightarrow \text{separ}$  == 0 then
    CheckSubsumptionFreeVars( $C_0, C_1, \{\}$ )
  else
    for each  $(t_0, t_1) \in \{(t_0, t_1) \mid t_0 \in C_0 \rightarrow \text{terms} \wedge t_1 \in C_1 \rightarrow \text{terms}\}$  do
      if exists  $\sigma$  s.t.  $t_0\sigma = t_1$  then
         $\sigma = \sigma \setminus \{x \rightarrow t \mid x \rightarrow t \in \sigma \text{ and } x \text{ a free variable}\}$ 
        return CheckSubsumptionFreeVars( $C_0, C_1, \sigma$ )
      end if
    end for
  end if
  return FALSE
end function

function CHECKSUBSUMPTIONFREEVARS( $C_0, C_1, \sigma$ )
  for each  $t_1 \in C_1 \rightarrow \text{terms}$  do
     $result = FALSE$ 
    for each  $t_0 \in C_0 \rightarrow \text{terms}$  do
      if exists  $\delta$  s.t.  $t_0\sigma\delta = t_1$  then
         $LAC_0 = \text{BuildLAC}(\{t\sigma\delta \mid t \in C_0 \rightarrow \text{cstrs}\})$ 
         $LAC_1 = \text{BuildLAC}(C_1 \rightarrow \text{cstrs})$ 
        if LAImplicationTest( $LAC_1, LAC_0$ ) then
           $result = TRUE$ 
          break
        end if
      end if
    end for
  if not  $result$  then
    return FALSE
  end if
end for
  return TRUE
end function

```

---

Before creating a new class we rename all involved classes and then apply *Merge* or *Deduction*. Especially, after application of *Deduction* the new class may contain variables in a constraint that do not occur in any of the class terms. Subsequent merges then continuously increases the number of constraints and variables. Fortunately, only one extra variable is needed.

**Lemma 31.** *Let  $A = \{\Gamma \parallel s_1, \dots, s_n\}$  be a class. Let  $Y = \text{vars}(\Gamma) \setminus (\text{vars}(s_1) \cup \dots \cup \text{vars}(s_n))$  be the variables occurring in  $\Gamma$  but not in  $s_1, \dots, s_n$ . Let  $\sigma : Y \rightarrow \{y'\}$  for some fresh variable  $y' \in \mathcal{X}$ . Then  $A$  subsumes  $A\sigma$  and  $A\sigma$  subsumes  $A$ .*

*Proof.* A constraint is satisfiable with respect to the symbol counting order, if it is satisfiable by substituting a constant for all variables. Concerning the semantics of classes, variables only occurring in the constraint do not play a role as long as the constraint is satisfied. Thus  $\text{gnd}(A) = \text{gnd}(A\sigma)$ .  $\square$

We further reduce the number of constraints by removing terms that have the same variable occurrences and are smaller or equal to some other term in the constraint according to  $\preceq$ , e.g.  $f(x)$  can be removed if  $f(g(x))$  already exists.

To keep the number of constrained terms within classes small, we also need a new condensation rule:

**Condensation**  $\Pi \cup \{\{\Gamma_1 \parallel s_1, \dots, \Gamma_n \parallel s_n\}\} \Rightarrow_{\text{CC}(\mathcal{X})} \Pi \cup \{\{\Gamma_1 \parallel s_1, \dots, \Gamma_{j-1} \parallel s_{j-1}, \Gamma_{j+1} \parallel s_{j+1}, \dots, \Gamma_n \parallel s_n\} \delta\}$

provided there exists indices  $i, j$  and a matcher  $\delta$  such that  $s_i \delta = s_j$ ,  $\{\Gamma_1 \parallel s_1, \dots, \Gamma_{j-1} \parallel s_{j-1}, \Gamma_{j+1} \parallel s_{j+1}, \dots, \Gamma_n \parallel s_n\} \delta$  subsumes  $\{\Gamma_1 \parallel s_1, \dots, \Gamma_n \parallel s_n\}$ .

For example, the Condensation rule would reduce the class  $\{f(x), f(y), f(z) \parallel f(x), f(y), f(z)\}$  to  $\{f(x), f(y) \parallel f(x), f(y)\}$ . Condensation together with subsumption by matching ensures termination, because the number of separating variables is bounded. Condensation is an example where we could improve the performance of our implementation. It can be implemented without additional memory consumption, however, our current implementation copies the class, modifies it and then checks subsumption.

To keep the number of full subsumption checks to a minimum, we have also implemented fast pre-filtering techniques. It turns out that it is more efficient to first check whether for each term in the instance class there is a term in the general class that matches this term.

**Corollary 32.** *Let  $A, B$  be two classes. If there exists a  $\Gamma \parallel t \in A$  such that there exists no  $\Delta \parallel s \in B$  and no matcher  $\delta$  such that  $s\delta = t$ , then  $A$  is not subsumed by  $B$ .*

We use bit vectors to track the number of occurrences of top symbols of terms within a class to check the above filter. For each symbol we store in one bit whether there are 0, 1 or more terms in the class that contain this symbol as a top symbol, where  $[0]_{10} = [0]_2$ ,  $[1]_{10} = [1]_2$ . For two bit vectors  $\mathcal{V}_0$  of a general and  $\mathcal{V}_1$  of an instance class we compute  $\text{NOT}(\mathcal{V}_0) \text{ AND } \mathcal{V}_1$ , where NOT and AND are bitwise operators. Note that classes containing a variable term must be excluded from this check.

Finally we store if merges or subsumption checks on classes have already been applied. To find candidates for the subsumption rule we maintain an index for each term in which

classes it occurs. General terms are retrieved by a discrimination tree index, unifiables and instances of a term by a path index [16].

## 5 Evaluation

We evaluated our algorithm on all unit equality (UEQ) problems from TPTP-v8.2.0 [26]. From each problem we created two benchmark problems: one with all inequations removed and the other by turning inequations into equations. We choose a fixed nesting depth of 6 and 8 in order to construct  $\beta$ . It is constructed by nesting all function symbols in one argument up to the chosen depth and filling all other arguments with a constant. E.g., with function symbols  $a/0, f/1, g/2, h/1, i/2$  and nesting depth 4 we create the term  $\beta = i(h(g(f(a), a)), a)$ . Then the size of all terms is limited to 7 symbols. We compared the performance of our algorithm to the performance of a CC implementation based on the implementation in the veriT solver [5]. The resulting benchmark problems turn out to be challenging for both algorithms.

$CC(\mathcal{X})$  provides a solution to the entire ground input space smaller  $\beta$ . Therefore, for the comparison of the two algorithms, we feed all ground terms smaller  $\beta$  into CC.  $CC(\mathcal{X})$  also provides a solution to the entire ground input space. We skip all examples where no equation has ground instances  $\preceq \beta$ .

Experiments are performed on a Debian Linux server running AMD EPYC 7702 64-core CPUs with 3.35GHz and a total memory of 2TB. The time limit for each test is 30 minutes. The results of all runs as well as all input files and binaries can be found at <https://nextcloud.mpi-klsb.mpg.de/index.php/s/RjcHAQYR97H6ZMy>.

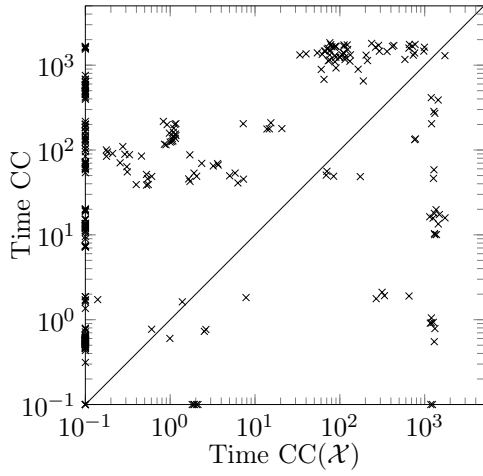
For a nesting depth of 6,  $CC(\mathcal{X})$  terminates on 519 and CC on 457 of the 2900 problems.  $CC(\mathcal{X})$  is faster on 474 problems and CC on 172.  $CC(\mathcal{X})$  terminated on 189 examples where CC timed out, and CC terminated on 127 examples where  $CC(\mathcal{X})$  timed out.

Figure 1a shows the results of all terminating test cases for the runtime and figure 1b shows the results for the number of classes. The performance of  $CC(\mathcal{X})$  currently drops if there are many different variables. This is mainly due to the current implementation of the redundancy checks. Concerning the number of classes, the number of classes generated by  $CC(\mathcal{X})$  is significantly smaller than the number in CC for almost all examples. Examples where this does not hold are border cases, i.e., they only contain few equations or contain only one constant.

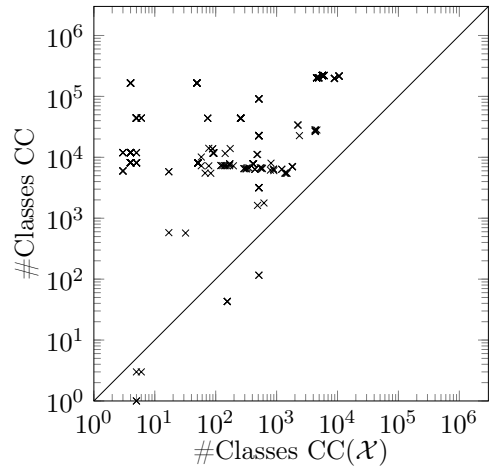
For a nesting depth of 8, 299 of 2900 problems terminate in  $CC(\mathcal{X})$  and 102 in CC.  $CC(\mathcal{X})$  is faster in 294 terminating examples and CC in 24.  $CC(\mathcal{X})$  terminated on 216 examples where CC timed out and CC terminated on 19 examples where  $CC(\mathcal{X})$  timed out.

Figure 2a shows the results of all terminating test cases for the runtime and figure 2b shows the results for the number of classes.  $CC(\mathcal{X})$  is particularly advantageous with a large  $\beta$ , where grounding is no longer feasible. The number of classes are again significantly smaller than in CC, except for the already mentioned border case examples.

The following table shows the average and median time and number of classes of  $CC(\mathcal{X})$

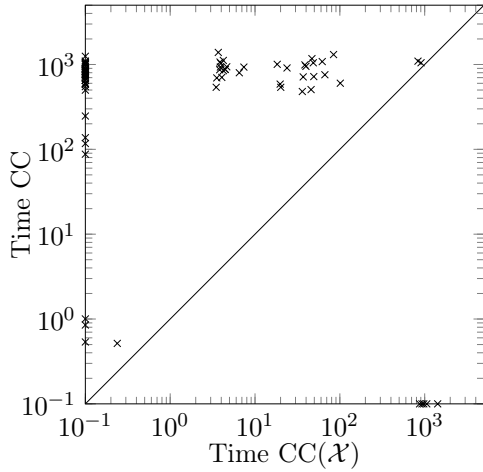


(a) Comparison of the runtime of CC and  $CC(\mathcal{X})$ .

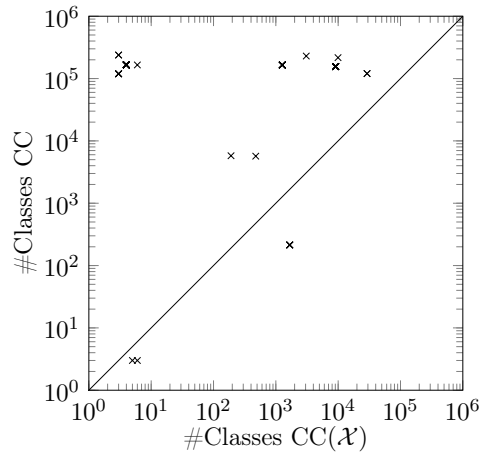


(b) Comparison of the number of classes of CC and  $CC(\mathcal{X})$ .

Figure 1: Benchmark results for a nesting depth of 6. Dots below the line indicate test cases where CC performs better (i.e. has less classes or took less time), and above indicate test cases where  $CC(\mathcal{X})$  performs better.



(a) Comparison of the runtime of CC and  $CC(\mathcal{X})$ .



(b) Comparison of the number of classes of CC and  $CC(\mathcal{X})$ .

Figure 2: Benchmark results for a nesting depth of 8.

and CC for nesting depth 6 and 8. One can see that  $CC(\mathcal{X})$  is significantly faster on average and produces only a fraction of the classes of the ground CC. The difference is even stronger when looking at the median. Here  $CC(\mathcal{X})$  only needs 1 second or less for half of all terminating examples whereas CC needs more than ten minutes.

Nesting Depth	Average				Median			
	Time		#Classes		Time		#Classes	
	$CC(\mathcal{X})$	CC	$CC(\mathcal{X})$	CC	$CC(\mathcal{X})$	CC	$CC(\mathcal{X})$	CC
6	201.2	394.6	2187	44248	0.5	58.6	170	8126
8	171.5	659.0	2071	125407	0.8	736.8	20	164857

## 6 Discussion and Conclusion

We presented the new calculus non-ground congruence closure ( $CC(\mathcal{X})$ ). It takes as input non-ground equations and computes the corresponding congruence classes for the overall set of ground terms smaller than a given maximum term  $\beta$ . The algorithm is sound, complete, and terminating due to a notion of redundancy and the finite ground input space. We developed and implemented a sophisticated redundancy concept, e.g., by introducing filters to expensive checks such as subsumption.

Still there is room for further improvement. From an implementation point of view, as already mentioned, *Condensation* modifies a copy of the class and checks for subsumption. In the *Merge* and *Deduction* rules, the number of copies of classes is also higher than necessary, especially when the generated class is subsumed. For some border cases CC outperforms  $CC(\mathcal{X})$ . Extending  $\Rightarrow_{CC(\mathcal{X})}$  to cope with input equations with only a few constants or few equations is a further line of research. Already now  $CC(\mathcal{X})$  can decide shallow equational classes, where the only arguments to functions are variables. This is independently of  $\beta$  and due to our notion of redundancy.

Equality checking between ground terms amounts to instance finding in a particular class, once the congruence closure algorithm is finished, both for CC and  $CC(\mathcal{X})$  where for the latter this has to be done modulo matching. Checking the equality of non-ground terms is much more involved both for  $CC(\mathcal{X})$  and CC. This is mainly due to the fact that we consider finite signature. If two non-ground terms are not in the same class this does not actually mean that they are not equal, since it could be the case that all instances of these terms are in the same class.

In general,  $CC(\mathcal{X})$  outperforms CC if the ratio of different variables to considered ground terms is on the ground term side. The other way round, if there are many variables but only a few ground terms to consider, then running CC is beneficial. This situation can be easily checked in advance, so  $CC(\mathcal{X})$  can be selected on problems where CC will fail extending the overall scope of applicability.

From an application point of view  $CC(\mathcal{X})$  can be immediately applied for detecting false or propagating clauses in SCL(EQ), even with respect to equations with variables. Unit equations need to be considered this way. In an SMT context it could immediately add to the ground CC in the following sense: Using the result of  $CC(\mathcal{X})$  with equations

before grounding in the theory combination and this way detecting additional ground instances needed.

## References

- [1] Baader, F., Nipkow, T.: Term Rewriting and All That. Cambridge University Press (1998)
- [2] Barbosa, H., Barrett, C.W., Brain, M., Kremer, G., Lachnitt, H., Mann, M., Mohamed, A., Mohamed, M., Niemetz, A., Nötzli, A., Ozdemir, A., Preiner, M., Reynolds, A., Sheng, Y., Tinelli, C., Zohar, Y.: cvc5: A versatile and industrial-strength SMT solver. In: Fisman, D., Rosu, G. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 28th International Conference, TACAS 2022, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2022, Munich, Germany, April 2-7, 2022, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13243, pp. 415–442. Springer (2022)
- [3] Barbosa, H., Fontaine, P., Reynolds, A.: Congruence closure with free variables. In: Legay, A., Margaria, T. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 23rd International Conference, TACAS 2017. Lecture Notes in Computer Science, vol. 10206, pp. 214–230 (2017)
- [4] Biere, A., Heule, M., van Maaren, H., Walsh, T. (eds.): Handbook of Satisfiability, Frontiers in Artificial Intelligence and Applications, vol. 185. IOS Press (2009)
- [5] Bouton, T., Caminha B. de Oliveira, D., Déharbe, D., Fontaine, P.: veriT: an open, trustable and efficient SMT-solver. In: International Conference on Automated Deduction. pp. 151–156. Springer (2009)
- [6] Bouton, T., Oliveira, D.C.B.D., Déharbe, D., Fontaine, P.: veriT: An open, trustable and efficient SMT-solver. In: Schmidt, R.A. (ed.) Automated Deduction - CADE-22, 22nd International Conference on Automated Deduction, Montreal, Canada, August 2-7, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5663, pp. 151–156. Springer (2009)
- [7] Bromberger, M., Fleury, M., Schwarz, S., Weidenbach, C.: SPASS-SATT - A CDCL(LA) solver
- [8] Cimatti, A., Griggio, A., Schaafsma, B.J., Sebastiani, R.: The MathSAT5 SMT solver. In: Piterman, N., Smolka, S.A. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 19th International Conference, TACAS 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings. vol. 7795, pp. 93–107. Springer (2013)
- [9] Downey, P.J., Sethi, R., Tarjan, R.E.: Variations on the common subexpression problem. *Journal of the ACM* **27**(4), 758–771 (1980)



- [10] Dutertre, B.: Yices 2.2. In: Biere, A., Bloem, R. (eds.) *Computer-Aided Verification (CAV'2014)*. Lecture Notes in Computer Science, vol. 8559, pp. 737–744. Springer (July 2014)
- [11] Ganzinger, H., Hagen, G., Nieuwenhuis, R., Oliveras, A., Tinelli, C.: DPLL(T): fast decision procedures. In: Alur, R., Peled, D.A. (eds.) *16th International Conference, CAV 2004*. LNCS '04, vol. 3114, pp. 176–188. Springer (2004)
- [12] Hurd, J.: Congruence classes with logic variables. *Log. J. IGPL* **9**(1), 53–69 (2001)
- [13] Jr., R.J.B., Schrag, R.: Using CSP look-back techniques to solve exceptionally hard SAT instances. In: Freuder, E.C. (ed.) *Proceedings of the Second International Conference on Principles and Practice of Constraint Programming, Cambridge, Massachusetts, USA, August 19-22, 1996*. LNCS, vol. 1118, pp. 46–60. Springer (1996)
- [14] Knuth, D.E., Bendix, P.B.: Simple word problems in universal algebras. In: Leech, I. (ed.) *Computational Problems in Abstract Algebra*, pp. 263–297. Pergamon Press (1970)
- [15] Leidinger, H., Weidenbach, C.: SCL(EQ): SCL for first-order logic with equality. *Journal of Automated Reasoning* **67**(3), 22 (2023)
- [16] McCune, W.: Experiments with discrimination-tree indexing and path indexing for term retrieval. *J. Autom. Reason.* **9**(2), 147–167 (1992)
- [17] Moskewicz, M.W., Madigan, C.F., Zhao, Y., Zhang, L., Malik, S.: Chaff: Engineering an efficient SAT solver. In: *Design Automation Conference, 2001. Proceedings*. pp. 530–535. ACM (2001)
- [18] de Moura, L., Bjørner, N.: Z3: An efficient SMT solver. In: *Tools and Algorithms for the Construction and Analysis of Systems, LNCS*, vol. 4963 (2008)
- [19] Nelson, G., Oppen, D.C.: Fast decision procedures based on congruence closure. *Journal of the ACM* **27**(2), 356–364 (1980)
- [20] Nieuwenhuis, R., Oliveras, A.: Fast congruence closure and extensions. *Information and Computation* **205**(4), 557–580 (2007)
- [21] Nieuwenhuis, R., Oliveras, A., Tinelli, C.: Solving SAT and SAT modulo theories: From an abstract Davis–Putnam–Logemann–Loveland procedure to DPLL(T). *Journal of the ACM* **53**, 937–977 (November 2006)
- [22] Reynolds, A., Barbosa, H., Fontaine, P.: Revisiting enumerative instantiation. In: Beyer, D., Huisman, M. (eds.) *Tools and Algorithms for the Construction and Analysis of Systems - 24th International Conference, TACAS 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings, Part II*. Lecture Notes in Computer Science, vol. 10806, pp. 112–131. Springer (2018)

- [23] Reynolds, A., Tinelli, C., de Moura, L.: Finding conflicting instances of quantified formulas in SMT. In: 2014 Formal Methods in Computer-Aided Design (FMCAD). pp. 195–202 (2014). <https://doi.org/10.1109/FMCAD.2014.6987613>
- [24] Shostak, R.E.: Deciding combinations of theories. *Journal of the ACM* **31**(1), 1–12 (1984)
- [25] Silva, J.P.M., Sakallah, K.A.: GRASP - a new search algorithm for satisfiability. In: International Conference on Computer Aided Design, ICCAD. pp. 220–227. IEEE Computer Society Press (1996)
- [26] Sutcliffe, G.: The TPTP problem library and associated infrastructure - from CNF to TH0, TPTP v6.4.0. *J. Autom. Reason.* **59**(4), 483–502 (2017)
- [27] Weidenbach, C.: Automated reasoning building blocks. In: Meyer, R., Platzter, A., Wehrheim, H. (eds.) *Correct System Design - Symposium in Honor of Ernst-Rüdiger Olderog on the Occasion of His 60th Birthday*, Oldenburg, Germany, September 8-9, 2015. Proceedings. *Lecture Notes in Computer Science*, vol. 9360, pp. 172–188. Springer (2015)