Logical Methods in Computer Science
Volume 21, Issue 1, 2025, pp. 20:1–20:29
https://lmcs.episciences.org/

Submitted Oct. 10, 2023
Published Feb. 28, 2025

CONGRUENCE CLOSURE MODULO GROUPS

DOHAN KIM

Department of Computer Science, University of Innsbruck, Innsbruck, Austria
e-mail address: dohan.kim@uibk.ac.at

Abstract. This paper presents a new framework for constructing congruence closure of a finite set of ground equations over uninterpreted symbols and interpreted symbols for the group axioms. In this framework, ground equations are flattened into certain forms by introducing new constants, and a completion procedure is performed on ground flat equations. The proposed completion procedure uses equational inference rules and constructs a ground convergent rewrite system for congruence closure with such interpreted symbols. If the completion procedure terminates, then it yields a decision procedure for the word problem for a finite set of ground equations with respect to the group axioms. This paper also provides a sufficient terminating condition of the completion procedure for constructing a ground convergent rewrite system from ground flat equations containing interpreted symbols for the group axioms. In addition, this paper presents a new method for constructing congruence closure of a finite set of ground equations containing interpreted symbols for the semigroup, monoid, and the multiple disjoint sets of group axioms, respectively, using the proposed framework.

1. Introduction

Congruence closure procedures [DST80, NO80, Koz77] have been widely studied for several decades, and play important roles in software and hardware verification systems [NO80, CRSS94, SW15], satisfiability modulo theories (SMT) solvers [BT18, DMB11], etc. They can be used to determine whether another ground equation is a consequence of a given finite set of ground equations.

A rewrite-based congruence closure procedure in the framework of ground completion was proposed by Kapur [Kap97]. It is based on flattening nonflat terms appearing in the input set of ground equations by introducing new constants. In [Kap21, Kap23, BTV03], the associative and commutative (AC) congruence algorithms were presented for congruence closure with interpreted symbols satisfying the AC properties.

In [KL21], Kim and Lynch presented a framework for congruence closure modulo permutation equations (i.e., flat permutative equations). In [BK22], Baader and Kapur presented *semantic congruence closure* for constructing congruence closure with interpreted symbols axiomatized by *strongly shallow equations*. They also provided a congruence closure algorithm with *extensional* symbols.

Key words and phrases: Congruence Closure, Group Theory, Ground Rewrite System, Word Problem.
This research is supported by the Austrian Science Fund (FWF) project I 5943.

LOGICAL METHODS IN COMPUTER SCIENCE
DOI:10.46298/LMCS-21(1:20)2025

Meanwhile, *group theory* [Hun80] is fundamental in mathematics, and has a wide variety of applications in physics, biology, and computer science. The *group axioms* of a binary operator f, a unary operator i, and the unit element 1 are

$$f(f(x,y),z) \approx f(x,f(y,z)) \qquad f(x,1) \approx x \qquad f(1,x) \approx x$$
$$f(x,i(x)) \approx 1 \qquad f(i(x),x) \approx 1$$

The well-known convergent rewrite system for the group axioms is as follows [Che84]:

$$i(1) \to 1 \qquad f(x,1) \to x \qquad f(1,x) \to x$$
$$i(i(x)) \to x \qquad f(x,i(x)) \to 1 \qquad f(i(x),x) \to 1$$
$$f(i(x),f(x,y)) \to y \qquad f(x,f(i(x),y)) \to y \qquad i(f(x,y)) \to f(i(y),i(x))$$
$$f(f(x,y),z) \to f(x,f(y,z))$$

Above, the associative symbol f has a fixed arity. In this paper, *associative flattening* [DP01, BTV03] w.r.t. each associative symbol f is applied, so the arity of f becomes variadic. For example, $f(f(u,v),f(w,z))$ is associatively flattened to $f(u,v,w,z)$ for an associative symbol f. Rewriting on associatively flat terms (cf. [Mar96]) is also used, which does not need to introduce *extension rules* [DP01] during a completion procedure.

This paper presents a new framework for computing congruence closure of a finite set of ground equations over uninterpreted and interpreted symbols for the group axioms G. If the proposed completion procedure terminates, then one can decide whether a ground equation follows from a given finite set of ground equations containing the interpreted symbols for G.

The approach used in this paper is roughly illustrated as follows using a simple example. Let $E = \{f(h(a),h(a)) \approx 1, i(h(a)) \approx b\}$, where an associative symbol f, the inverse symbol i, and the unit 1 are the interpreted symbols for G, and h is an uninterpreted symbol. First, $f(h(a),h(a)) \approx 1$ and $i(h(a)) \approx b$ are flattened into $h(a) \approx c_1$, $f(c_1,c_1) \approx 1$, and $i(c_1) \approx b$ using a new constant c_1. Next, for each constant 1, a, b, and c_1, terms with the inverse symbol i are considered by adding $i(1) \approx 1$, $i(a) \approx c_2$, $i(c_2) \approx a$ (because $i(i(a)) \approx a$), and $i(b) \approx c_1$, where c_2 is a new constant. The equations $f(a,c_2) \approx 1, f(c_2,a) \approx 1, f(c_1,b) \approx 1, f(b,c_1) \approx 1$ are also added by taking the equations $f(x,i(x)) \approx 1$ and $f(i(x),x) \approx 1$ in the group axioms into account. The resulting set $S(E)$ of this procedure from $E = \{f(h(a),h(a)) \approx 1, i(h(a)) \approx b\}$ is $S(E) = \{h(a) \approx c_1, f(c_1,c_1) \approx 1, i(c_1) \approx b, i(1) \approx 1, i(a) \approx c_2, i(c_2) \approx a, i(b) \approx c_1, f(a,c_2) \approx 1, f(c_2,a) \approx 1, f(c_1,b) \approx 1, f(b,c_1) \approx 1\} \cup U(C)$, where $U(C)$ is the set of ground instantiations of $f(x,1) \approx x$ and $f(1,x) \approx x$ in the group axioms using the set of constant symbols C only. By adding certain ground flat equations entailed by the group axioms, the proposed completion procedure for constructing congruence closure modulo G w.r.t. E is only concerned with ground (flat) equations instead of taking the group axioms (containing variables) into account.

Now, the arguments of a term headed by an associative symbol f are represented by the corresponding string for ground flat equations. For example, $f(a,b,c,d)$ is represented by $f(abcd)$, where f is an associative symbol. Then, the proposed completion procedure using string-based equational inference rules is proceeded. Equation $c_1 \approx b$ can be inferred from $f(c_1c_1) \approx 1$ and $f(c_1b) \approx 1$ using an equational inference rule discussed later in this paper. Roughly speaking, $f(c_1c_1b) \approx b$ follows from $f(c_1c_1) \approx 1$, and $f(c_1c_1b) \approx c_1$ follows from $f(c_1b) \approx 1$, so $c_1 \approx b$ can be inferred from $f(c_1c_1) \approx 1$ and $f(c_1b) \approx 1$. The completion terminates with $S_\infty(E) = \{h(a) \approx b, f(bb) \approx 1, i(b) \approx b, i(1) \approx 1, i(a) \approx c_2, i(c_2) \approx a, f(ac_2) \approx$

$1, f(c_2a) \approx 1, c_1 \approx b\} \cup \bar{U}(C)$, where $c_1 \succ b$ and $U(C)$ is updated to $\bar{U}(C)$ by rewriting each occurrence of c_1 in $U(C)$ to b. Now, the rewrite system $S_\infty^\succ(E)$ can be obtained by orienting each equation in $S_\infty(E)$ into the rewrite rule using $\succ$ (defined in Section 3). Then each $f(u)$ for string $u = c_ic_{i+1}\cdots c_{i+j}$ in the rewrite system is restored into $f(c_i, c_{i+1}, \ldots, c_{i+j})$. The ground rewrite system for groups $R(G)$ (defined in Section 2) combined with $S_\infty^\succ(E)$ modulo associativity can decide whether a ground equation follows from E w.r.t. G. For example, $h(a) \approx i(i(b))$ follows from E w.r.t. G, where $h(a)$ can be rewritten to b and $i(i(b))$ can be rewritten to b using the rewrite system $S_\infty^\succ(E)$.

The key insight of the proposed approach is that only certain ground equations entailed by the group axioms are added for the completion procedure, while taking only ground flat equations into account during its entire completion procedure. This keeps the completion procedure from interacting with the (nonground) convergent rewrite system for groups directly. Now, a completion procedure for groups [HEO05, Sim94] using their monoid presentations is extended to the proposed approach in which the arguments of each term headed by an associativity symbol are represented by a string. (Roughly speaking, a *monoid presentation* of a group is represented by string relations and generators, adding the relations of the form $xx^{-1} \approx 1$ and $x^{-1}x \approx 1$ for each $x \in X$ to the relations of a presentation of the group, where X is the set of generators of the presentation of the group. See [HEO05] for details.)

Since the word problem for finitely presented groups is undecidable in general [HEO05], the word problem for a finite set of ground equations E w.r.t. G is undecidable in general too. The proposed completion procedure may not terminate and yield an infinite convergent rewrite system for congruence closure of E w.r.t. G. If it terminates, then it provides a decision procedure for the (ground) word problem for E w.r.t. G.

In addition, this paper discusses a sufficient terminating condition of the proposed completion procedure by attempting to associate a finite set of ground flat equations derived from E with a monoid presentation of a group. If it is a monoid presentation of a finite group, then it necessarily terminates and yields a finite ground convergent rewrite system for congruence closure of E w.r.t. G, providing a decision procedure for the word problem for E w.r.t. G.

Based on the proposed framework, this paper also presents a new approach to constructing a rewriting-based congruence closure of a finite set of ground equations w.r.t. the semigroup, monoid, and the multiple disjoint sets of group axioms, respectively. Interestingly, it shares the same proposed ground completion procedure and yields a (possibly infinite) ground convergent rewrite system for congruence closure of a finite set of ground equations w.r.t. the semigroup, monoid, and the multiple disjoint sets of group axioms, respectively.

2. Preliminaries

The reader is assumed to have some familiarity with rewrite systems [BN98, DP01]. This paper refers to [Kap97, Kap21, BK20, BK22, BTV03] for the definitions and notations of congruence closure.

Let Σ be a finite set of function symbols of arity ≥ 1 and C_0 be a finite set constant symbols (i.e., function symbols of arity 0). We denote by Σ_A the subset of Σ containing all the associative function symbols. We also denote by $C \supseteq C_0$ a finite set of constant symbols that may include (finitely many) new constant symbols other than the (original) constant symbols in C_0.

Terms are built from variables, constants (in C), and function symbols (in Σ). A *ground term* is a term not containing variables. We denote by $T(\Sigma, C_0)$ (resp. $T(\Sigma, C)$) the set of ground terms built from Σ and C_0 (resp. Σ and C). The symbols $x, y, z, \ldots$ along with their subscripts are used to denote variables.

An *equation* is an unordered pair of terms, written $s \approx t$.

Function symbols that require to satisfy additional *semantic properties* (often expressed by a set of nonground axioms) are called *interpreted symbols*, while function symbols that do not require such properties are called *uninterpreted symbols*.

For a fixed arity binary function symbol $f \in \Sigma_A$, $f(f(x,y),z) \approx f(x, f(y,z))$ defines the theory of associativity. Alternatively, the set of all equations A of the following form defines the theory of associativity for variadic terms (see [BTV03]).

$$f(x_1, \ldots, x_m, f(y_1, \ldots, y_i), z_1, \ldots, z_n) \approx f(x_1, \ldots, x_m, y_1, \ldots, y_i, z_1, \ldots, z_n),$$

where $f \in \Sigma_A$ and $\{m+n+1, m+n+i, i\} \subset \alpha(f)$ and $\alpha(f) = \{2, 3, 4, \ldots\}$. (Here, α denotes the arity function for Σ.) By *associatively flattening* of a term, we mean the normalization of a term w.r.t. A considered as a rewrite system in such a way that each equation $f(x_1, \ldots, x_m, f(y_1, \ldots, y_i), z_1, \ldots, z_n) \approx f(x_1, \ldots, x_m, y_1, \ldots, y_i, z_1, \ldots, z_n)$ in A is oriented as a rewrite rule $f(x_1, \ldots, x_m, f(y_1, \ldots, y_i), z_1, \ldots, z_n) \to f(x_1, \ldots, x_m, y_1, \ldots, y_i, z_1, \ldots, z_n)$. For example, $f(f(u,v), f(w,z))$ is associatively flattened to $f(u,v,w,z)$ for $f \in \Sigma_A$.

In the remainder of this paper, the *associativity axioms* (*semigroup axioms*) are the equations in A, the *unit axioms* are the equations $f(x,1) \approx x$ and $f(1,x) \approx x$, the *inverse axioms* are the equations $f(x, i(x)) \approx 1$ and $f(i(x), x) \approx 1$, the *monoid axioms* are the equations in $A \cup \{f(x,1) \approx x, f(1,x) \approx x\}$, and the *group axioms* are the equations in $A \cup \{f(x,1) \approx x, f(1,x) \approx x, f(x,i(x)) \approx 1, f(i(x),x) \approx 1\}$ for some $f \in \Sigma_A$. Unless otherwise stated, associative flattening w.r.t. each associative symbol $f \in \Sigma_A$ is always applied, and by G, we mean the set of group axioms.

Given a (finite) set of constant symbols C, we denote by $U(C) := \{f(c,1) \approx c \mid c \in C\} \cup \{f(1,c) \approx c \mid c \in C\}$ the set of ground instantiations of $f(x,1) \approx x$ and $f(1,x) \approx x$ in G using only the elements in C.

The *equational theory* induced by a set of equations E, denoted by $\approx_E$, is the smallest congruence that is closed under substitutions and contains E (i.e., the smallest congruence containing all instances of the equations of E). Two terms s and t are *equal modulo* A (associativity), denoted by $s \overset{*}{\leftrightarrow}_A t$, iff their associatively flat forms are equal. Each associatively flat term represents its A-equivalence class.

A term t is said to *A-match* another term s (and s is called an *A-instance* of t) iff there is a substitution σ such that $s \overset{*}{\leftrightarrow}_A t\sigma$. Note that if both s and t are ground terms in $T(\Sigma, C)$, then s A-matches t iff $s \overset{*}{\leftrightarrow}_A t$.

The *depth* of a term t is defined inductively as $depth(t) = 0$ if t is a variable or a constant and $depth(f(s_1, \ldots, s_n)) = 1 + \max\{depth(s_i) \mid 1 \leq i \leq n\}$.

The *size* of a term t, denoted by $|t|$, is the total number of occurrences of function and variable symbols in it.

A *rewrite system* is a set of rewrite rules. A rewrite relation $\to_{R/A}$ is defined as follows: $u \to_{R/A} v$ if there are terms s and t such that $u \approx_A s$, $s \to_R t$, and $t \approx_A v$. For example, if $f \in \Sigma_A$ and $f(b,c) \to e \in R$, then we have $f(a,b,c,d) \to_{R/A} f(a,e,d)$ because $f(a,b,c,d) \approx_A f(a, f(f(b,c),d)) \to_R f(a, f(e,d)) \approx_A f(a,e,d)$.

The transitive and reflexive closure of $\rightarrow_{R/A}$ is denoted by $\xrightarrow{*}_{R/A}$.

We simply denote by R/A the rewrite relation $\rightarrow_{R/A}$.

We say that a term t is in R/A-*normal form* if there is no term t' such that $t \rightarrow_{R/A} t'$. Otherwise, we say that t is R/A-*reducible*.

A rewrite relation R/A is *confluent* if for all terms r,s and t with $r \xrightarrow{*}_{R/A} s$ and $r \xrightarrow{*}_{R/A} t$, there are terms u an v such that $s \xrightarrow{*}_{R/A} u \xleftrightarrow{*}_{A} v \xleftarrow{*}_{R/A} t$. (Recall that each A-equivalence class is represented by a single associatively flat term.)

A rewrite relation R/A is *locally confluent* if for all terms r, s and t with $r \rightarrow_{R/A} s$ and $r \rightarrow_{R/A} t$, there are terms u and v such that $s \xrightarrow{*}_{R/A} u \xleftrightarrow{*}_{A} v \xleftarrow{*}_{R/A} t$. (In this paper, $\rightarrow_{R/A}$ is used to rewrite associatively flat ground terms and A-matching for $\rightarrow_{R/A}$ can be done using associatively flat ground terms. Also, the check for local confluence is simpler, i.e., R/A is locally confluent on associatively flat ground terms if for all associatively flat ground terms r, s and t with $r \rightarrow_{R/A} s$ and $r \rightarrow_{R/A} t$, there is an associatively flat ground term u such that $s \xrightarrow{*}_{R/A} u \xleftarrow{*}_{R/A} t$.)

A rewrite relation R/A is *terminating* if there is no infinite sequence $t_0 \rightarrow_{R/A} t_1 \rightarrow_{R/A} t_2 \rightarrow_{R/A} \cdots$.

A terminating rewrite relation R/A is confluent iff it is locally confluent.

A rewrite system R is *convergent modulo* A if the rewrite relation $\rightarrow_{R/A}$ is confluent and terminating.

We denote by Σ_G the interpreted symbols for the set of group axioms $G := A \cup \{f(x,1) \approx x, f(1,x) \approx x, f(x,i(x)) \approx 1, f(i(x),x) \approx 1\}$. Here, we have $f, i, 1 \in \Sigma_G$, where $f \in \Sigma_A$, $i \in \Sigma$, and $1 \in C_0$.

The convergent rewrite system for the set of group axioms G, denoted $R(G)$, on associatively flat terms is given as follows:

$$\begin{array}{llll} i(1) \rightarrow 1 & f(x,1) \rightarrow x & f(1,x) \rightarrow x & i(i(x)) \rightarrow x \\ f(x,i(x)) \rightarrow 1 & f(i(x),x) \rightarrow 1 & i(f(x,y)) \rightarrow f(i(y),i(x)) & \end{array}$$

where $f \in \Sigma_G$. Note that the extension rule [DP01] $f(x,i(x),y) \rightarrow y$ of $f(x,i(x)) \rightarrow 1$ and the extension rule $f(i(x),x,y) \rightarrow y$ of $f(i(x),x) \rightarrow 1$ can be simplified and are not needed by $R(G)/A$. In fact, extension rules can be dealt implicitly without explicitly generating them for rewriting on associatively flat terms. This is further discussed in the next section.

Lemma 2.1. *The rewrite system $R(G)$ is convergent modulo A.*

Given a finite set $E = \{s_i \approx t_i \mid 1 \leq i \leq m\}$ of ground equations where $s_i, t_i \in T(\Sigma, C_0)$, the *congruence closure* $CC(E)$ [Kap21, BK20] is the smallest subset of $T(\Sigma, C_0) \times T(\Sigma, C_0)$ containing E and is closed under the following rules: (i) for every $s \in T(\Sigma, C_0)$, $s \approx s \in CC(E)$ (*reflexivity*), (ii) if $s \approx t \in CC(E)$, then $t \approx s \in CC(E)$ (*symmetry*), (iii) if $s \approx t \in CC(E)$ and $t \approx u \in CC(E)$, then $s \approx u \in CC(E)$ (*transitivity*), and (iv) if $f \in \Sigma$ is an n-ary function symbol ($n > 0$) and $s_1 \approx t_1, \ldots, s_n \approx t_n \in CC(E)$, then $f(s_1, \ldots, s_n) \approx f(t_1, \ldots, t_n) \in CC(E)$ (*congruence*). Note that $CC(E)$ is also the equational theory induced by E.

Given a finite set E of ground equations between terms in $T(\Sigma, C_0)$, we also consider a set of nonground equations F such that the equations in F are also satisfied as well as the equations in E. Given $s, t \in T(\Sigma, C_0)$, $s \approx t$ *follows from* E w.r.t. F (written $s \approx_E^F t$) if $s^{\mathcal{A}} = t^{\mathcal{A}}$ holds in all models $\mathcal{A}$ of $E \cup F$. Therefore, $\approx_E^F$ is the restriction of $\approx_{E \cup F}$ (i.e., the equational theory induced by $E \cup F$) to the ground terms in $T(\Sigma, C_0)$ (or $T(\Sigma, C)$ by a slight abuse of notation). The *word problem* for E w.r.t. F is the relation $\approx_E^F$.

The *congruence closure of E w.r.t. F*, denoted by $CC^F(E)$, is the smallest subset of $T(\Sigma, C_0) \times T(\Sigma, C_0)$ that contains E and is closed under reflexivity, symmetry, transitivity, and congruence, and the following rule:

– if $l \approx r \in F$ and σ is a substitution that maps the variables in l, r to elements of $T(\Sigma, C_0)$, then $l\sigma \approx r\sigma \in CC^F(E)$.

Birkhoff's theorem says that $\approx_F$ coincides with $\overset{*}{\leftrightarrow}_F$, where $\overset{*}{\leftrightarrow}_F$ denotes the reflexive, transitive, and symmetric closure of $\rightarrow_F$. Observe that $CC^G(E)$ is the equational theory induced by $E \cup G$, which coincides with $\approx_E^G$ by Birkhoff's theorem. We also say $CC^G(E)$ as *congruence closure modulo G* for E.

3. Congruence Closure Modulo Groups

In this section, we denote by E a finite set of ground equations $s \approx t$ between (ground) terms $s, t \in T(\Sigma, C_0)$, and by G the set of group axioms $A \cup \{f(x, 1) \approx x, f(1, x) \approx x, f(x, i(x)) \approx 1, f(i(x), x) \approx 1\}$. We also denote by W an infinite set of constants taken from $\{c_1, c_2, \ldots\}$, where W is disjoint from C_0, C_1 a finite subset chosen from W, and $C := C_0 \cup C_1$.

3.1. Ground Completion using Ground Flat Equations.

Definition 3.1. By a *ground (fully) flat equation*, we mean an (associatively flattened) ground equation over $T(\Sigma, C)$ in one of the following three forms:

(i) A *C-constant equation* is an equation of the form $c_i \approx c_j$, where c_i and c_j are constants in C.

(ii) A *D-flat equation* is an equation of the form $g(c_1, \ldots, c_n) \approx c$, where $c_1, \ldots, c_n, c$ are constants in C, g is an n-ary function symbol with $n \geq 1$.[1]

(iii) An *A-flat equation* is an equation of the form $f(c_1, \ldots, c_m) \approx f(d_1, \ldots, d_n)$, where $f \in \Sigma_A$ and $c_1, \ldots, c_m, d_1, \ldots, d_n$ are constants in C.

By *ground (fully) flat terms*, we mean terms occurring in ground (fully) flat equations over $T(\Sigma, C)$.

The proposed approach to constructing congruence closure modulo G for E using a ground completion procedure consists of three phases. Roughly speaking, the first phase transforms a set of ground equations E into the set of ground flat equations E' (cf. [Kap97, BTV03]). The second phase adds certain ground flat equations entailed by G using E'. Call $S(E)$ the resulting set. Finally, the last phase applies a ground completion procedure on $S(E)$.

The key advantages of using ground flat equations are as follows: (i) the ground completion procedure is simple by taking only ground flat equations into account during its entire procedure, (ii) no complex ordering is needed, and (iii) the overlaps between ground flat equations and $R(G)$ are in restricted form, which simplifies the construction of a ground convergent rewrite system for congruence closure modulo G for E. In fact, by adding certain ground flat equations entailed by G, the proposed completion procedure does not interact

[1] If $g \in \Sigma_A$, then $g(c_1, \ldots, c_n)$ is an associatively flat ground term of depth 1.

with $R(G)$ at all and performs only on $S(E)$. In what follows, each phase is discussed in detail. We assume that multiple associative symbols are allowed (i.e., $|\Sigma_A| \geq 1$), but only one of them is used for G.

Phase I: Given a finite set of ground equations E between terms $s, t \in T(\Sigma, C_0)$,

(1) Perform associative flattening to each term in E. Call E_1 the output of this step, where all terms in E_1 are fully associatively flattened.
(2) Normalize each term in E_1 using the rewriting by $R(G)/A$. Call E_2 the output of this step, where all terms in E_2 are in $R(G)/A$-normal form and the trivial equations (i.e., the equations of the form $s \approx s$) are all removed.
(3) Flatten nonflat terms in E_2 using new constants from $W := \{c_1, c_2, \ldots\}$ in an iterative way so that the output of this step consists of only constant, D-flat, and A-flat equations. Here, each A-flat equation is not allowed to be further transformed, for example, into D-flat equations. In this step, if an equation with nonconstant flat terms is neither an A-flat equation nor a D-flat equation (e.g. $f(c_1) \approx g(c_2)$ with $f \in \Sigma_A$ and $g \notin \Sigma_A$), then it is further transformed into D-flat (or D-flat and constant) equations using new constants from W.

The output of Phase I is denoted by E', where all equations in E' are constant, D-flat, or A-flat equations. Also, $C := C_0 \cup C_1$ is a finite set of constants obtained after Phase I, where C_1 is a set of new constants introduced by flattening in step 3 of Phase I.

Example 3.2. Let $E = \{f(a,a) \approx f(h(a), f(i(h(a)), 1)), f(a, h(a)) \approx b, f(i(a), b) \approx b\}$, where $f \in \Sigma_G$ is an associative symbol, $i \in \Sigma_G$ is the inverse symbol, and $1 \in \Sigma_G$ is the unit for G.

For step 1 of Phase I, perform associative flattening to $f(h(a), f(i(h(a)), 1))$, which yields $f(h(a), i(h(a)), 1)$. Then E_1 is E with $f(a,a) \approx f(h(a), f(i(h(a)), 1))$ being replaced by $f(a,a) \approx f(h(a), i(h(a)), 1)$.

For step 2, term $f(h(a), i(h(a)), 1)$ is normalized to 1 by $R(G)/A$. Therefore, $E_2 = \{f(a,a) \approx 1, f(a, h(a)) \approx b, f(i(a), b) \approx b\}$.

Finally, for step 3, new constants c_1 and c_2 for $h(a)$ and $i(a)$ are introduced, respectively. Now, $E' = \{h(a) \approx c_1, i(a) \approx c_2, f(a,a) \approx 1, f(a, c_1) \approx b, f(c_2, b) \approx b\}$ and $C = \{1, a, b, c_1, c_2\}$.

Next, the purpose of Phase II is to add certain ground flat equations entailed by G using E'. Since $R(G)$ contains variables, this attempts to keep the ground flat equations in $S(E)$ (output of Phase II) from interacting with $R(G)$ during a completion procedure. In the following, $f \in \Sigma_G$ is an associative symbol, $i \in \Sigma_G$ is the inverse symbol, and $1 \in \Sigma_G$ is the unit in G.

Phase II: Given C and E' obtained from E by Phase I, copy C to C' and E' to E'':

(1) For each constant $c_k \in C'$ and $c_k \neq 1$, repeat the following step:
If neither $i(c_k) \approx c_i$ nor $i(c_j) \approx c_k$ appears in E'' for some $c_i, c_j \in C'$, then $E' := E' \cup \{i(c_k) \approx c_m\}$ and $C := C \cup \{c_m\}$ for a new constant c_m taken from W.
(2) Set $I(E') := \{i(1) \approx 1\} \cup \{i(c_n) \approx c_m \,|\, i(c_m) \approx c_n \in E'\} \cup \{f(c_m, c_n) \approx 1 \,|\, i(c_m) \approx c_n \in E'\} \cup \{f(c_n, c_m) \approx 1 \,|\, i(c_m) \approx c_n \in E'\}$.
(3) Set $S(E) := E' \cup I(E') \cup U(C)$ and return $S(E)$, where $U(C) := \{f(c, 1) \approx c \,|\, c \in C\} \cup \{f(1, c) \approx c \,|\, c \in C\}$.

Now, $S(E)$ is the output of Phase II. (Also, C can be updated during Phase II because new constants can be added in step 1 of Phase II.) No new constant is added to C after Phase II.

Example 3.3. (Continued from Example 3.2) After Phase I, we have $C = \{1, a, b, c_1, c_2\}$ and $E' = \{h(a) \approx c_1, i(a) \approx c_2, f(a,a) \approx 1, f(a, c_1) \approx b, f(c_2, b) \approx b\}$, where $f \in \Sigma_G$.

For step 1 of Phase II, add $i(b) \approx c_3$ and $i(c_1) \approx c_4$ to E', where c_3 and c_4 are the new constants taken from W. We now have $C = \{1, a, b, c_1, c_2, c_3, c_4\}$ and $E' = \{h(a) \approx c_1, i(a) \approx c_2, f(a,a) \approx 1, f(a, c_1) \approx b, f(c_2, b) \approx b, i(b) \approx c_3, i(c_1) \approx c_4\}$. For step 2, we have $I(E') = \{i(1) \approx 1, i(c_2) \approx a, i(c_3) \approx b, i(c_4) \approx c_1, f(a, c_2) \approx 1, f(c_2, a) \approx 1, f(b, c_3) \approx 1, f(c_3, b) \approx 1, f(c_1, c_4) \approx 1, f(c_4, c_1) \approx 1\}$. For step 3, we have $U(C) = \{f(1,1) \approx 1, f(a,1) \approx a, f(1,a) \approx a, f(b,1) \approx b, f(1,b) \approx b, f(c_1,1) \approx c_1, f(1,c_1) \approx c_1, f(c_2,1) \approx c_2, f(1,c_2) \approx c_2, f(c_3,1) \approx c_3, f(1,c_3) \approx c_3, f(c_4,1) \approx c_4, f(1,c_4) \approx c_4\}$. Finally, we have $S(E) = E' \cup I(E') \cup U(C)$ and return $S(E)$.

The proof of the following lemma is adapted from the proof of Lemma 3 in [BK22].

Lemma 3.4. *$S(E)$ w.r.t. G is a conservative extension of E w.r.t. G, i.e., $s_0 \approx_E^G t_0$ iff $s_0 \approx_{S(E)}^G t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$.*

Proof. To show the *if-direction*, assume that $s_0 \not\approx_E^G t_0$. Then, there is some algebra $\mathcal{A}$ over the signature $\Sigma \cup C_0$ satisfying all equations in $E \cup G$ such that $s_0^{\mathcal{A}} \neq t_0^{\mathcal{A}}$. Let $Sub(E)$ be the set of subterms of the terms occurring in E. First, observe that for each new constant $c_k \in C_1$, there is some term $s_k \in Sub(E) \setminus C_0$ such that $c_k \approx_{S(E)} s_k$. Now, we may expand $\mathcal{A}$ to the new constants in C_1 by interpreting each $c_k \in C_1$ as $s_k^{\mathcal{A}}$ for some term $s_k \in Sub(E) \setminus C_0$. We call this expanded algebra $\mathcal{B}$. Since $s_0^{\mathcal{B}} = s_0^{\mathcal{A}} \neq t_0^{\mathcal{A}} = t_0^{\mathcal{B}}$, it is sufficient to show that $\mathcal{B}$ satisfies each equation in $S(E) \cup G$. We know that $\mathcal{A}$ satisfies G, so its expansion $\mathcal{B}$ obviously satisfies G too. It remains to show that $\mathcal{B}$ satisfies $S(E)$. First, consider a C-constant equation $c_i \approx c_j \in S(E)$. Then, we have $s_i \approx s_j \in E$. Here, s_i (resp. s_j) is simply c_i (resp. c_j) if $c_i \in C_0$ (resp. $c_j \in C_0$). Now, we have $c_i^{\mathcal{B}} = s_i^{\mathcal{A}} = s_j^{\mathcal{A}} = c_j^{\mathcal{B}}$, and thus $\mathcal{B}$ satisfies $c_i \approx c_j$.

Next, consider an A-flat equation $f(c_1, \ldots, c_m) \approx f(c_{m+1}, \ldots, c_n) \in S(E)$, where $f \in \Sigma_A$ and $c_1, \ldots, c_n \in C$. Then we have $f(s_1, \ldots, s_m) \approx f(s_{m+1}, \ldots, s_n) \in E$ for some $s_1, \ldots s_n \in Sub(E)$. Again, s_k is simply c_k if $s_k \in C_0$. Now, we have $f^{\mathcal{B}}(c_1^{\mathcal{B}}, \ldots, c_m^{\mathcal{B}}) = f^{\mathcal{A}}(s_1^{\mathcal{A}}, \ldots, s_m^{\mathcal{A}}) = f^{\mathcal{A}}(s_{m+1}^{\mathcal{A}}, \ldots, s_n^{\mathcal{A}}) = f^{\mathcal{B}}(c_{m+1}^{\mathcal{B}}, \ldots, c_n^{\mathcal{B}})$, and thus $\mathcal{B}$ satisfies $f(c_1, \ldots, c_m) \approx f(c_{m+1}, \ldots, c_n)$. We omit the proof for the case of a D-flat equation in $S(E)$ because it is similar to the previous cases.

To show the *only-if-direction*, assume that $s_0 \not\approx_{S(E)}^G t_0$. Then, there is an algebra $\mathcal{B}$ over $\Sigma \cup C$ satisfying all equations in $S(E) \cup G$ such that $s_0^{\mathcal{B}} \neq t_0^{\mathcal{B}}$. Let $\mathcal{A}$ be the reduct of $\mathcal{B}$ to $\Sigma \cup C_0$ by forgetting the interpretation of the symbols in the set of new constants C_1. Since $s_0^{\mathcal{A}} = s_0^{\mathcal{B}} \neq t_0^{\mathcal{B}} = t_0^{\mathcal{A}}$, we only need to show that $\mathcal{A}$ satisfies the equations in $E \cup G$. Since $\mathcal{B}$ satisfies G, it is easy to see that $\mathcal{A}$ satisfies G too. It remains to show that $\mathcal{A}$ satisfies each equation in E. More specifically, it suffices to show that $\mathcal{A}$ satisfies each equation after step 1 and step 2 of Phase I from E because $\mathcal{A}$ satisfies G.

Let E_2 be the set of equations after step 1 and step 2 of Phase I from E. Observe also that for each term $s_k \in Sub(E_2) \setminus C_0$, there is a new constant $c_k \in C_1$. First, consider an equation of the form $a_i \approx b_j \in E_2$, where a_i and b_j are constants. Then, both a_i and b_j are the elements of C_0, so the reduct $\mathcal{A}$ obviously satisfies $a_i \approx b_j$, i.e., $a_i^{\mathcal{A}} = a_i^{\mathcal{B}} = b_j^{\mathcal{B}} = b_j^{\mathcal{A}}$.

DEDUCE: $\dfrac{S \cup \{f(u_1u_2) \approx s,\ f(u_2u_3) \approx t\}}{S \cup \{f(u_1t) \approx f(su_3), f(u_1u_2) \approx s, f(u_2u_3) \approx t\}}$

if (i) $f \in \Sigma_A$, (ii) $f(u_1u_2) \succ s$, (iii) $f(u_2u_3) \succ t$, and (iv) neither u_1 nor u_2 nor u_3 is the empty string, i.e., $|u_1| \neq 0$, $|u_2| \neq 0$, and $|u_3| \neq 0$.

SIMPLIFY: $\dfrac{S \cup \{f(u_1u_2u_3) \approx s,\ f(u_2) \approx t\}}{S \cup \{\bar{f}(u_1tu_3) \approx s,\ f(u_2) \approx t\}}$

if (i) $f \in \Sigma_A$, (ii) $f(u_2) \succ t$, and (iii) $s \succ t$ if $|u_1u_3| = 0$.

COLLAPSE: $\dfrac{S \cup \{s[u] \approx t,\ u \approx d\}}{S \cup \{s[d] \approx t,\ u \approx d\}}$

if (i) $s[u] \succ t$, (ii) $u \succ d$, (iii) $d \in C$, and (iv) u is not headed by a function symbol in Σ_A.

COMPOSE: $\dfrac{S \cup \{t \approx c,\ c \approx d\}}{S \cup \{t \approx d,\ c \approx d\}}$

if (i) $t \succ c$, (ii) $c \succ d$, and (iii) $c, d \in C$.

DELETE: $\dfrac{S \cup \{s \approx s\}}{S}$

Above, all the equations are assumed to be ground and flat, and S is a set of ground flat equations. In the SIMPLIFY rule, if $f \in \Sigma_A$ and u is a nonempty string over C, then $\bar{f}(u) := f(u)$ if $|u| \geq 2$, and $\bar{f}(u) := u$, otherwise (i.e., $|u| = 1$).

FIGURE 1. The inference System $\mathcal{I}$

Next, consider an equation of the form $f(s_1, \ldots, s_m) \approx f(s_{m+1}, \ldots, s_n) \in E_2$, where $f \in \Sigma_A$ and $s_1, \ldots, s_n \in Sub(E_2)$. Here, if $s_k \in Sub(E_2) \setminus C_0$, then there is a new constant $c_k \in C_1$ such that $c_k \approx_{S(E)} s_k$. (This can be shown easily by a simple structural induction on term s_k using Definition 3.1). Then we have $f(c_1, \ldots, c_m) \approx f(c_{m+1}, \ldots, c_n) \in S(E)$ for some $c_1, \ldots, c_n \in C$, where c_k is simply s_k if $s_k \in C_0$. Since $f^{\mathcal{B}}(c_1^{\mathcal{B}}, \ldots, c_m^{\mathcal{B}}) = f^{\mathcal{B}}(c_{m+1}^{\mathcal{B}}, \ldots, c_n^{\mathcal{B}})$, we have $f^{\mathcal{A}}(s_1^{\mathcal{A}}, \ldots, s_m^{\mathcal{A}}) = f^{\mathcal{B}}(c_1^{\mathcal{B}}, \ldots, c_m^{\mathcal{B}}) = f^{\mathcal{B}}(c_{m+1}^{\mathcal{B}}, \ldots, c_n^{\mathcal{B}}) = f^{\mathcal{A}}(s_{m+1}^{\mathcal{A}}, \ldots, s_n^{\mathcal{A}})$, and thus $\mathcal{A}$ satisfies $f(s_1, \ldots, s_m) \approx f(s_{m+1}, \ldots, s_n)$. We omit the proofs of the remaining cases because they are similar to the previous cases. □

Note that each argument of a term headed by an associative symbol f is a constant in C after Phase II. By a slight abuse of notation, the arguments of a term headed by an associative symbol f are converted into the corresponding string. We define the length of a string u over C. If $u \in C^*$, then the *length* of u, denoted $|u|$, is defined as: $|\lambda| := 0$, $|c| := 1$ for each $c \in C$, and $|sc| := |s| + 1$ for $s \in C^*$ and $c \in C$, where λ denotes the empty string.

Definition 3.5. Let $f \in \Sigma_A$ and u be a string over C such that $u := u_1 u_2 \cdots u_i$ and $|u| \geq 2$. Then, $f(u)$ denotes the term $f(u_1, \ldots, u_i)$. Each of $f(\lambda u)$, $f(u\lambda)$, and $f(\lambda u \lambda)$ also denotes $f(u)$, where λ is the empty string.

For example, if $f \in \Sigma_A$ and $f(a, b, c, d)$, we also write $f(abcd)$ for $f(a, b, c, d)$. Since f is variadic for associatively flat terms with the arity being at least 2, the distinction between two notations is clear from context. In the remainder of this paper, two notations are used interchangeably, and we assume that a total precedence on C_0 is always given.

Definition 3.6. Let W be an infinite set of constants $\{c_1, c_2, \ldots\}$ such that W is disjoint from C_0, C_1 a finite subset chosen from W, and $C := C_0 \cup C_1$. We define the order $\succ$ on ground (fully) flat terms in $T(\Sigma, C)$ as follows, assuming that a total precedence on C_0 is given:

(i) 1 is the minimal element (w.r.t. $\succ$),
(ii) $c_i \succ c_j$ if $i < j$ for all $c_i, c_j \in C_1$,
(iii) $c \succ c'$ if $c \in C_1$ and $c' \in C_0$,
(iv) $t \succ c$ if t is any term headed by a function symbol f in Σ and c is any constant in C,
(v) $f(s) \succ f(t)$ if $f \in \Sigma_A$ and $s \succ_L t$, where s and t are strings over C with $|s|, |t| \geq 2$ and $\succ_L$ is the *length-lexicographic ordering* on C^*.[2]

If a D-flat (resp. an A-flat) equation is oriented by $\succ$, then we call it the D-flat (resp. the A-flat) rule. Note that by (ii), C_1 is a totally ordered set.

We see that $\succ$ is well-founded on (associatively flattened) terms in $T(\Sigma, C)$. Note that $\succ$ is a strict partial order on (associatively flattened) terms in $T(\Sigma, C)$ and is a total order on C. Yet, it suffices for the inference system $\mathcal{I}$ in Figure 1. In Figure 1, DEDUCE is the only expansion rule, and the remaining rules in $\mathcal{I}$ are the contraction rules. (The DEDUCE and SIMPLIFY rules are adapted from finding critical pairs in string rewriting systems (or *semi-Thue systems*) [KN85b, HEO05].)

Now, the purpose of Phase III is to perform the ground completion procedure on $S(E)$. The final set of ground completion using Phase III provides a ground convergent rewrite system, where each equation is oriented by $\succ$.

Phase III: Given $S(E)$ obtained from Phase II, apply the ground completion procedure using the inference rules in Figure 1.

Definition 3.7. (i) We write $S \vdash S'$ to indicate that S' is obtained from S by application of an inference rule in $\mathcal{I}$ (see Figure 1), where S is a set of equations.
(ii) A *derivation* (w.r.t. $\mathcal{I}$) is a sequence of states $S_0 \vdash S_1 \vdash \cdots$.
(iii) A derivation $S_0 = S(E) \vdash S_1 \vdash \cdots$ is *fair* if any rule in $\mathcal{I}$ that is continuously enabled is applied eventually (cf. [BTV03]).
(iv) We denote by $S_\infty(E) = \bigcup_i \bigcap_{j \geq i} S_j$ a set of persisting equations obtained by a fair derivation (w.r.t. $\mathcal{I}$) starting with $S_0 = S(E)$.

Definition 3.8. Let S be a set of equations such that each equation is orientable by $\succ$. By $S^{\succ}$, we denote the rewrite system corresponding to S, where each equation $s \approx t \in S$ with $s \succ t$ is oriented into the rewrite rule $s \to t$.

[2]The length-lexicographic ordering $\succ_L$ on C^* is defined as follows: $s = s_1 \cdots s_i \succ_L t_1 \cdots t_j = t$ if $i > j$, or they have the same length and $s_1 \cdots s_i$ comes before $t_1 \cdots t_j$ lexicographically using a precedence on C.

It is easy to see that each equation in $S_0 = S(E)$ is orientable by $\succ$. Also, each equation in S_i in a derivation starting from S_0 is orientable by $\succ$ or a trivial equation because the conclusion of each inference rule in $\mathcal{I}$ is either orientable by $\succ$ or a trivial equation. This means that $S_\infty(E)$ is orientable by $\succ$ (cf. a *non-failing run* [BN98]).

When rewriting with associatively flat terms (cf. [Mar96]), one does not need to introduce *extension rules* [DP01] explicitly. This means that it is not needed to introduce new extension variables for extension rules, which simplifies the inference rules significantly. The notion of overlapping has to be generalized accordingly; two rewrite rules with the same top associative symbol f (at the top position) overlap if they either overlap in the standard way or overlap involving their extension rules. For example, if $f \in \Sigma_A$, then there is a critical overlap between $f(a,b) \to d$ and $f(b,c) \to e$ because $f(a,b,c)$ can be written either to $f(d,c)$ or $f(a,e)$, i.e., the critical pair obtained from $f(a,b) \to d$ and $f(b,c) \to e$ is $f(a,e) \approx f(d,c)$. Here, extension rules are dealt implicitly without explicitly generating them.

Definition 3.9. Let R be the rewrite system obtained from a set of ground flat equations oriented by $\succ$. The *critical pair* (*modulo associativity*) between two rewrite rules in R has one of the following forms:
(i) The critical pair obtained from $f(u_1u_2) \to s \in R$ and $f(u_2u_3) \to t \in R$ is $f(u_1t) \approx f(su_3)$, where $f \in \Sigma_A$, $|u_1| \neq 0, |u_2| \neq 0$, and $|u_3| \neq 0$.
(ii) The critical pair obtained from $f(u_1u_2u_3) \to s \in R$ and $f(u_2) \to t \in R$ is $\bar{f}(u_1tu_3) \approx s$, where $f \in \Sigma_A$, and $s \succ t$ if $|u_1u_3| = 0$.
(iii) The critical pair obtained from $s[u] \to t \in R$ and $u \to d \in R$ is $s[d] \approx t$, where u is not headed by a function symbol in Σ_A and $d \in C$.

By $CP_A(R)$, we denote the set of all critical pairs (modulo associativity) between the rewrite rules in R.

Lemma 3.10. *If a derivation $S_0 = S(E) \vdash S_1 \vdash \cdots$ is fair, then $CP_A(S^{\succ}_\infty(E)) \subseteq \bigcup_j S_j$.*

Proof. Suppose that a derivation $S_0 = S(E) \vdash S_1 \vdash \cdots$ is fair. Then any rule in $\mathcal{I}$ that is continuously enabled is applied eventually by Definition 3.7(iii). We consider each critical pair of the form in Definition 3.9 for the rewrite system $S^{\succ}_\infty(E)$. If a critical pair in $CP_A(S^{\succ}_\infty(E))$ was of the form in Definition 3.9(i), then the DEDUCE rule was applied. By fairness, this critical pair should be an element of $\bigcup_j S_j$. Similarly, if a critical pair in $CP_A(S^{\succ}_\infty(E))$ was of the form in Definition 3.9(ii), then the SIMPLIFY rule was applied. Again, by fairness, it should be an element of $\bigcup_j S_j$. Finally, if a critical pair in $CP_A(S^{\succ}_\infty(E))$ was of the form in Definition 3.9(iii), then the COLLAPSE rule was applied, so it should also be an element of $\bigcup_j S_j$ by fairness. □

Example 3.11. (Continued from Example 3.3) In Example 3.3 after Phase II, we have $E' = \{h(a) \approx c_1, i(a) \approx c_2, f(aa) \approx 1, f(ac_1) \approx b, f(c_2b) \approx b, i(b) \approx c_3, i(c_1) \approx c_4\}$ and $S(E) = E' \cup I(E') \cup U(C)$, where $C = \{1, a, b, c_1, c_2, c_3, c_4\}$ and $I(E') = \{i(1) \approx 1, i(c_2) \approx a, i(c_3) \approx b, i(c_4) \approx c_1, f(ac_2) \approx 1, f(c_2a) \approx 1, f(bc_3) \approx 1, f(c_3b) \approx 1, f(c_1c_4) \approx 1, f(c_4c_1) \approx 1\}$. Then,

$1' : f(bc_4) \approx a$ (DEDUCE by $f(ac_1) \approx b$ and $f(c_1c_4) \approx 1$. Then, SIMPLIFY replacing $f(a1)$ by a using $f(a1) \approx a \in U(C)$.)
$2' : f(c_3a) \approx c_4$ (DEDUCE by $f(c_3b) \approx 1$ and $1'$. Then, SIMPLIFY replacing $f(1c_4)$ by c_4 using $f(1c4) \approx c_4 \in U(C)$.)

$3' : f(c_2a) \approx f(bc_4)$ (DEDUCE by $f(c_2b) \approx b$ and $1'$.)
$4' : f(c_2a) \approx a$ (SIMPLIFY $3'$ by $1'$. $3'$ is deleted.)
$5' : a \approx 1$ (SIMPLIFY $4'$ by $f(c_2a) \approx 1$. $4'$ is deleted.)
$6' : f(1c_2) \approx 1$ (COLLAPSE $f(ac_2) \approx 1$ by $5'$. $f(ac_2) \approx 1$ is deleted.)
$7' : c_2 \approx 1$ (SIMPLIFY $f(1c_2) \approx c_2$ by $6'$. $f(1c_2) \approx c_2$ is deleted.)
$8' : f(1c_1) \approx b$ (COLLAPSE $f(ac_1) \approx b$ by $5'$. $f(ac_1) \approx b$ is deleted.)
$9' : c_1 \approx b$ (SIMPLIFY $f(1c_1) \approx c_1$ by $8'$. $f(1c_1) \approx c_1$ is deleted.)
$10' : h(1) \approx c_1$ (COLLAPSE $h(a) \approx c_1$ by $5'$. $h(a) \approx c_1$ is deleted.)
$11' : h(1) \approx b$ (COMPOSE $10'$ by $9'$. $10'$ is deleted.)
$12' : f(c_31) \approx c_4$ (COLLAPSE $2'$ by $5'$. $2'$ is deleted.)
$13' : c_3 \approx c_4$ (SIMPLIFY $f(c_31) \approx c_3$ by $12'$. $f(c_31) \approx c_3$ is deleted.)
...
Note that DEDUCE with the equations in $U(C)$ (e.g., $f(b1) \approx b$, $b \in C$) is not necessary. After several steps using the contraction rules, we have $S_\infty(E) = \{h(1) \approx b, c_2 \approx 1, a \approx 1, i(1) \approx 1, c_1 \approx b, c_3 \approx c_4, i(b) \approx c_4, i(c_4) \approx b, f(bc_4) \approx 1, f(c_4b) \approx 1\} \cup \bar{U}(C)$, where $\bar{U}(C) = \{f(11) \approx 1, f(b1) \approx b, f(1b) \approx b, f(c_41) \approx c_4, f(1c_4) \approx c_4\}$. (Here, 1 is minimal w.r.t. $\succ$ and $c_1 \succ c_2 \succ c_3 \succ c_4 \succ b$, where $c_1, c_2, c_3, c_4 \in C_1$ and $b \in C_0$ (see Definition 3.6).)

3.2. Ground Convergent Rewrite Systems for Congruence Closure Modulo Groups.

Recall that $R(G)$ denotes the convergent rewrite system for G modulo A. By $gr(R(G))$ we denote $gr(R(G)) := \{l\sigma \to r\sigma \mid l \to r \in R(G) \wedge \sigma \text{ is a ground substitution}\}$, and by $gr(A)$ we denote $gr(A) := \{e\sigma \mid e \in A \wedge \sigma \text{ is a ground substitution}\}$. Here, a ground substitution maps variables to (ground) terms in $T(\Sigma, C)$.

Lemma 3.12. *If $S \vdash S'$, then the congruence relations $\overset{*}{\longleftrightarrow}_{S \cup gr(A)}$ and $\overset{*}{\longleftrightarrow}_{S' \cup gr(A)}$ on $T(\Sigma, C)$ are the same.*

Proof. We consider each application of a rule τ for $S \vdash S'$.

If τ is DEDUCE, then we need to show that $f(u_1t) \overset{*}{\longleftrightarrow}_{S \cup gr(A)} f(su_3)$, where $S' - S = \{f(u_1t) \approx f(su_3)\}$. Since $f(u_1u_2u_3) \overset{*}{\longleftrightarrow}_{S \cup gr(A)} f(su_3)$ and $f(u_1u_2u_3) \overset{*}{\longleftrightarrow}_{S \cup gr(A)} f(u_1t)$, we have $f(u_1t) \overset{*}{\longleftrightarrow}_{S \cup gr(A)} f(su_3)$.

If τ is SIMPLIFY, then we consider two cases. First, suppose that $|u_1u_3| \neq 0$. Then, we show that $f(u_1tu_3) \overset{*}{\longleftrightarrow}_{S \cup gr(A)} s$, where $S' - S = \{f(u_1tu_3) \approx s\}$. Since $f(u_1u_2u_3) \overset{*}{\longleftrightarrow}_{S \cup gr(A)} s$ and $f(u_1u_2u_3) \overset{*}{\longleftrightarrow}_{S \cup gr(A)} f(u_1tu_3)$, we have $f(u_1tu_3) \overset{*}{\longleftrightarrow}_{S \cup gr(A)} s$. Conversely, we show that $f(u_1u_2u_3) \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} s$, where $S - S' = \{f(u_1u_2u_3) \approx s\}$. Since $f(u_1tu_3) \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} s$ and $f(u_1u_2u_3) \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} f(u_1tu_3)$, we have $f(u_1u_2u_3) \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} s$. Otherwise, suppose that $|u_1u_3| = 0$. Then, we need to show that $t \overset{*}{\longleftrightarrow}_{S \cup gr(A)} s$, where $S' - S = \{t \approx s\}$. Since $f(u_2) \overset{*}{\longleftrightarrow}_{S \cup gr(A)} s$ and $f(u_2) \overset{*}{\longleftrightarrow}_{S \cup gr(A)} t$, we have $t \overset{*}{\longleftrightarrow}_{S \cup gr(A)} s$. Conversely, we show that $f(u_2) \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} s$, where $S - S' = \{f(u_2) \approx s\}$. Since $t \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} s$ and $f(u_2) \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} t$, we have $f(u_2) \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} s$.

If τ is COLLAPSE, then we show that $s[d] \overset{*}{\longleftrightarrow}_{S \cup gr(A)} t$, where $S' - S = \{s[d] \approx t\}$. Since $s[u] \overset{*}{\longleftrightarrow}_{S \cup gr(A)} t$ and $u \overset{*}{\longleftrightarrow}_{S \cup gr(A)} d$, we have $s[d] \overset{*}{\longleftrightarrow}_{S \cup gr(A)} t$. Conversely, we show that $s[u] \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} t$, where $S - S' = \{s[u] \approx t\}$. Since $s[d] \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} t$ and $u \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} d$, we see that $s[u] \overset{*}{\longleftrightarrow}_{S' \cup gr(A)} t$.

If τ is COMPOSE, then we show that $t \xleftrightarrow{*}_{S\cup gr(A)} d$, where $S' - S = \{t \approx d\}$. Since $t \xleftrightarrow{*}_{S\cup gr(A)} c$ and $c \xleftrightarrow{*}_{S\cup gr(A)} d$, it is easy to see that $t \xleftrightarrow{*}_{S\cup gr(A)} d$. Conversely, since $t \xleftrightarrow{*}_{S'\cup gr(A)} d$ and $c \xleftrightarrow{*}_{S'\cup gr(A)} d$, we have $t \xleftrightarrow{*}_{S'\cup gr(A)} c$, where $S - S' = \{t \approx c\}$.

Finally, if τ is DELETE, then it is immediate that $s \xleftrightarrow{*}_{S'\cup gr(A)} s$. □

Lemma 3.13. *If $s_0, t_0 \in T(\Sigma, C_0)$, then $s_0 \approx t_0 \in CC^G(E)$ iff $s_0 \approx_{S_\infty(E)\cup gr(R(G))\cup gr(A)} t_0$, where the rewrite system $gr(R(G))$ is viewed as a set of equations.*

Proof. By Birkhoff's theorem, $CC^G(E)$ coincides with $\approx_E^G$. By Lemma 3.4, $s_0 \approx_E^G t_0$ iff $s_0 \approx_{S(E)}^G t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$. Also, $s_0 \approx_{S(E)}^G t_0$ iff $s_0 \approx_{S(E)\cup gr(R(G))\cup gr(A)} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$.

It remains to show that $s_0 \approx_{S(E)\cup gr(R(G))\cup gr(A)} t_0$ iff $s_0 \approx_{S_\infty(E)\cup gr(R(G))\cup gr(A)} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$, where $S_0 = S(E)$. By Lemma 3.12, if $S_i \vdash S_{i+1}$, then $\xleftrightarrow{*}_{S_i\cup gr(A)}$ and $\xleftrightarrow{*}_{S_{i+1}\cup gr(A)}$ on $T(\Sigma, C_0)$ are the same (i.e., $u \xleftrightarrow{*}_{S_i\cup gr(A)} v$ iff $u \xleftrightarrow{*}_{S_{i+1}\cup gr(A)} v$ for all $u, v \in T(\Sigma, C_0)$), and thus the conclusion follows. □

Definition 3.14. Let $s = s[u] \leftrightarrow s[v] = t$ be a proof step using an equation (rule) $u \approx v \in S \cup gr(A)$. The *complexity* of this proof step is defined as follows:

$(\{s\}, u, t)$	if $u \approx v \in S$ and $u \succ v$	$(\{t\}, v, s)$	if $u \approx v \in S$ and $v \succ u$
$(\{s, t\}, \bot, \bot)$	if $u \approx v \in S$ and $u = v$	$(\{s\}, \bot, t)$	if $u \approx v \in gr(A)$

In Definition 3.14, $\bot$ is a new constant symbol. We define the (strict) ordering $\gtrdot$ on $T(\Sigma, C) \cup \{\bot\}$ such that (i) $\bot$ is minimal w.r.t. $\gtrdot$, and (ii) $\gtrdot$ is simply $\succ$ on $T(\Sigma, C)$. (As usual, we assume that we use associative flattening for $\gtrdot$ whenever necessary.) Complexities of proof steps are compared lexicographically using the multiset extension of $\gtrdot$ in the first component, and $\gtrdot$ in the second and third component. The *complexity of a proof* is defined by the multiset of the complexities of its proof steps [BTV03, Bac91]. The *proof ordering*, denoted by $\succ_{\mathcal{C}}$, is the multiset extension of the ordering on the complexities of proof steps in order to compare the complexities of proofs. (The empty proof [Bac91] is assumed to be minimal w.r.t. $\succ_{\mathcal{C}}$.) As $\succ$ is well-founded on associatively flattened terms in $T(\Sigma, C)$, $\gtrdot$ is well-founded on associatively flattened terms in $T(\Sigma, C) \cup \{\bot\}$. Since the lexicographic extension and the multiset extension of a well-founded ordering are also well-founded [BN98], we may infer that $\succ_{\mathcal{C}}$ is well-founded.

In the following, if $f \in \Sigma_A$ and $u, v, w \in C^*$ such that $u := u_1 \cdots u_i$, $v := v_1 \cdots v_j$, $w := w_1 \cdots w_k$, and $|uw| \neq 0$ and $|v| \geq 2$, then $f(uf(v)w)$ denotes $f(u_1, \ldots, u_i, f(v_1, \ldots, v_j), w_1, \ldots, w_k)$ if $u, w \neq \lambda$, $f(u_1, \ldots, u_i, f(v_1, \ldots, v_j))$ if $u \neq \lambda$ and $w = \lambda$, and $f(f(v_1, \ldots, v_j), w_1, \ldots, w_k)$ if $u = \lambda$ and $w \neq \lambda$. For example, if $u = c_1$, $v = c_2c_3$, and $w = \lambda$, then $f(uf(v)w)$ denotes $f(c_1, f(c_2, c_3))$.

If $s = s[u] \leftrightarrow s[v] = t$ is a proof step using an equation $u \approx v \in S$ (resp. $u \approx v \in gr(A)$), then we also write $s \xleftrightarrow{u\approx v}_S t$ (resp. $s \xleftrightarrow{u\approx v}_{gr(A)} t$).

Lemma 3.15. *Suppose $S \vdash S'$. Then, for any two terms $s, t \in T(\Sigma, C)$, if ρ is a ground proof in $S \cup gr(A)$ of an equation $s \approx t$, then there is a ground proof ρ' in $S' \cup gr(A)$ of $s \approx t$ such that $\rho \succeq_{\mathcal{C}} \rho'$.*

Proof. We show that each equation in $S - S'$ has a smaller proof (w.r.t. $\succ_{\mathcal{C}}$) in $S' \cup gr(A)$ by considering each case of $S \vdash S'$ except by the application of the DEDUCE rule. (Note that the DEDUCE rule does not delete any equation, so the conclusion follows immediately.)

(i) SIMPLIFY: We consider two cases. First, suppose that $|u_1u_3| \neq 0$. Then the proof $f(u_1u_2u_3) \xleftrightarrow{f(u_1u_2u_3)\approx s}_S s$ is transformed to the proof $f(u_1u_2u_3) \xleftrightarrow{e_1}_{gr(A)} f(u_1f(u_2)u_3) \xleftrightarrow{e_2}_{S'} f(u_1tu_3) \xleftrightarrow{e_3}_{S'} s$, where $e_1 = f(u_1u_2u_3) \approx f(u_1f(u_2)u_3)$, $e_2 = f(u_2) \approx t$, and $e_3 = f(u_1tu_3) \approx s$. The newer proof is smaller (w.r.t. $\succ_{\mathcal{C}}$) because $f(u_1u_2u_3) \xleftrightarrow{f(u_1u_2u_3)\approx s}_S s$ with complexity $(\{f(u_1u_2u_3)\}, f(u_1u_2u_3), s)$ is bigger (w.r.t. $\succ_{\mathcal{C}}$) than the proof step $f(u_1u_2u_3) \xleftrightarrow{e_1}_{gr(A)} f(u_1f(u_2)u_3)$ with complexity $(\{f(u_1u_2u_3)\}, \perp, f(u_1f(u_2)u_3))$ in the second component, bigger than the proof step $f(u_1f(u_2)u_3) \xleftrightarrow{e_2}_{S'} f(u_1tu_3)$ with complexity $(\{f(u_1f(u_2)u_3)\}, f(u_2), f(u_1tu_3))$ in the second component, and bigger than the proof step $f(u_1tu_3) \xleftrightarrow{e_3}_{S'} s$ in the first component. (Here, both $f(u_1u_2u_3)$ and $f(u_1f(u_2)u_3)$ are equal w.r.t. $\gtrdot$ because their associatively flat forms are the same.)

Otherwise, suppose that $|u_1u_3| = 0$. Then the proof $f(u_2) \xleftrightarrow{f(u_2)\approx s}_S s$ is transformed to the proof $f(u_2) \xleftrightarrow{e_1}_{S'} t \xleftrightarrow{e_2}_{S'} s$, where $e_1 = f(u_2) \approx t$ and $e_2 = t \approx s$. Since $s \gtrdot t$ by the condition of the rule, we see that the newer proof is smaller (w.r.t. $\succ_{\mathcal{C}}$) because $f(u_2) \xleftrightarrow{f(u_2)\approx s}_S s$ with complexity $(\{f(u_2)\}, f(u_2), s)$ is bigger (w.r.t. $\succ_{\mathcal{C}}$) than the proof step $f(u_2) \xleftrightarrow{e_1}_{S'} t$ with complexity $(\{f(u_2)\}, f(u_2), t)$ in the last component, and bigger than the proof step $t \xleftrightarrow{e_2}_{S'} s$ with complexity $(\{s\}, s, t)$ in the first component.

(ii) COLLAPSE: The proof $s[u] \xleftrightarrow{s[u]\approx t}_S t$ is transformed to the proof $s[u] \xleftrightarrow{e_1}_{S'} s[d] \xleftrightarrow{e_2}_{S'} t$, where $e_1 = u \approx d$ and $e_2 = s[d] \approx t$. The newer proof is smaller (w.r.t. $\succ_{\mathcal{C}}$) because $s[u] \xleftrightarrow{s[u]\approx t}_S t$ with complexity $(\{s[u]\}, s[u], t)$ is bigger (w.r.t. $\succ_{\mathcal{C}}$) than the proof step $s[u] \xleftrightarrow{e_1}_{S'} s[d]$ in the second component and the proof step $s[d] \xleftrightarrow{e_2}_{S'} t$ in the first component.

(iii) COMPOSE: The proof $t \xleftrightarrow{t\approx c}_S c$ is transformed to the proof $t \xleftrightarrow{e_1}_{S'} d \xleftrightarrow{e_2}_{S'} c$, where $e_1 = t \approx d$ and $e_2 = d \approx c$. The newer proof is smaller (w.r.t. $\succ_{\mathcal{C}}$) because $t \xleftrightarrow{t\approx c}_S c$ with complexity $(\{t\}, t, c)$ is bigger (w.r.t. $\succ_{\mathcal{C}}$) than the proof step $t \xleftrightarrow{e_1}_{S'} d$ in the last component and the proof step $d \xleftrightarrow{e_2}_{S'} c$ in the first component.

(iv) DELETE: The proof $s \xleftrightarrow{s\approx s}_S s$ is transformed to the empty proof, where the proof $s \xleftrightarrow{s\approx s}_S s$ with complexity $(\{s, s\}, \perp, \perp)$ is bigger (w.r.t. $\succ_{\mathcal{C}}$) than the empty proof. □

A *peak* is a proof of the form $t_1 \leftarrow_{R/A} t \rightarrow_{R/A} t_2$ and a *cliff* is a proof of the form $t_1 \leftrightarrow_A t \rightarrow_{R/A} t_2$ or $t_1 \rightarrow_{R/A} t \leftrightarrow_A t_2$ for the rewrite relation $\rightarrow_{R/A}$. Note that a cliff is simply replaced by a rewrite step by R/A for associatively flat terms, i.e., $t_1 \rightarrow_{R/A} t_2$, so we do not need to consider cliffs on associatively flat terms. Also, recall that $S_\infty(E) = \bigcup_i \bigcap_{j\geq i} S_j$ denotes a set of persisting equations obtained by a fair derivation starting from $S_0 = S(E)$, and $S_\infty^\succ(E)$ denotes the rewrite system obtained from $S_\infty(E)$ by orienting each equation in $S_\infty(E)$ into the rewrite rule. Note that the ground rewrite system $S_\infty^\succ(E)$ can possibly be infinite.

Lemma 3.16. *The ground rewrite system $S_\infty^\succ(E)$ is convergent modulo A on $T(\Sigma, C)$.*

Proof. We omit the proof that $S_\infty^\succ(E)/A$ is terminating because it can be directly inferred from the proof of Lemma 3.20 below by using the ordering $\succ_{CM}$ on the complexity measures (D, S, W) (see Definition 3.18) or the simpler (lexicographic) complexity measures (S, W) of associatively flat ground terms in $T(\Sigma, C)$. (Note that $\succ$ is not necessarily a reduction order on associatively flat ground terms in $T(\Sigma, C)$.)

Now, we show that no peak of the form $u_1 \leftarrow_{S^{\succ}_{\infty}(E)/A} \cdot \rightarrow_{S^{\succ}_{\infty}(E)} u_2$ for $u_1, u_2 \in T(\Sigma, C)$ occurs in every minimal proof (w.r.t. $\succ_{\mathcal{C}}$) between u_1 and u_2 in $S^{\succ}_{\infty}(E) \cup gr(A)$. (Note that such a minimal proof exists because $\succ_{\mathcal{C}}$ is well-founded.)

Suppose, towards a contradiction, that such a peak exists. If a peak is a non-overlap[3] $t_1 \leftarrow_{S^{\succ}_{\infty}(E)/A} t \rightarrow_{S^{\succ}_{\infty}(E)/A} t_2$, then it consists of proof steps $t_1 \leftrightarrow_{S_\infty(E)} t'_1 \overset{*}{\leftrightarrow}_{gr(A)} t \overset{*}{\leftrightarrow}_{gr(A)} t'_2 \leftrightarrow_{S_\infty(E)} t_2$, where $t'_1 \succ t_1$ and $t'_2 \succ t_2$. This proof can be transformed to a proof $t_1 \rightarrow_{S^{\succ}_{\infty}(E)/A} t' \leftarrow_{S^{\succ}_{\infty}(E)/A} t_2$, which consists of proof steps $t_1 \overset{*}{\leftrightarrow}_{gr(A)} t''_1 \leftrightarrow_{S_\infty(E)} t' \leftrightarrow_{S_\infty(E)} t''_2 \overset{*}{\leftrightarrow}_{gr(A)} t_2$. We may infer that the newer proof is smaller because t is bigger than t_1 and t_2, i.e., t is bigger than each term in the newer proof, which is a contradiction.

Now, consider a peak $s_1 \leftarrow_{S^{\succ}_{\infty}(E)/A} s \rightarrow_{S^{\succ}_{\infty}(E)/A} s_2$ that is a proper overlap. It consists of proof steps $s_1 \leftrightarrow_{S_\infty(E)} s'_1 \overset{*}{\leftrightarrow}_{gr(A)} s \overset{*}{\leftrightarrow}_{gr(A)} s'_2 \leftrightarrow_{S_\infty(E)} s_2$, where $s'_1 \succ s_1$ and $s'_2 \succ s_2$. Then we have $s_1 \overset{*}{\leftrightarrow}_{gr(A)} s''_1 \leftrightarrow_{CP_A(S^{\succ}_{\infty}(E))} s''_2 \overset{*}{\leftrightarrow}_{gr(A)} s_2$, where $CP_A(S^{\succ}_{\infty}(E))$ consists of the equations created by the DEDUCE, SIMPLIFY, and COLLAPSE rule applied on the equations in $S_\infty(E)$. Since $CP_A(S^{\succ}_{\infty}(E)) \subseteq \bigcup_j S_j$ by Lemma 3.10, there is a proof $s_1 \overset{*}{\leftrightarrow}_{gr(A)} s''_1 \leftrightarrow_{S_k} s''_2 \overset{*}{\leftrightarrow}_{gr(A)} s_2$ for some $k \geq 0$. We name this proof as ρ. Observe that this ground proof ρ in $S_k \cup gr(A)$ is strictly smaller than the original peak $s_1 \leftarrow_{S^{\succ}_{\infty}(E)/A} s \rightarrow_{S^{\succ}_{\infty}(E)/A} s_2$ because s is bigger than each term in ρ. Also, there is a ground proof ρ' in $S_\infty(E) \cup gr(A)$ such that $\rho \succeq_{\mathcal{C}} \rho'$ by Lemma 3.15. Now, ρ' is strictly smaller than the original peak $s_1 \leftarrow_{S^{\succ}_{\infty}(E)/A} s \rightarrow_{S^{\succ}_{\infty}(E)/A} s_2$, a contradiction. □

We extend the standard definition of a *proper subterm* [DP01] for associatively flat ground terms in $T(\Sigma, C)$. We say that $f(u)$ is a *proper subterm* of $f(vuw)$ if $f \in \Sigma_A$ and $u, v, w \in C^*$, where $|u| \geq 2$ and $|vw| \neq 0$. The following lemma directly follows from the fairness of a derivation involving the SIMPLIFY, COLLAPSE, and COMPOSE rule.

Lemma 3.17. *For each rule $l \rightarrow r$ in $S^{\succ}_{\infty}(E)$, the right-hand side r is irreducible by $S^{\succ}_{\infty}(E)/A$ and every proper subterm of l is irreducible by $S^{\succ}_{\infty}(E)/A$.*

In the following, we define a complexity measure of an associatively flat ground term so that the measures are compared for each reduction step by $(S^{\succ}_{\infty}(E) \cup gr(R(G)))/A$. If the associated ordering on these measures is well-founded and each reduction step by $(S^{\succ}_{\infty}(E) \cup gr(R(G)))/A$ strictly reduces the measure, then $(S^{\succ}_{\infty}(E) \cup gr(R(G)))/A$ is terminating. First, the size of an associatively flat ground term alone is not a good measure. For example, by applying the rule $i(f(x_1, x_2)) \rightarrow f(i(x_2), i(x_1)) \in R(G)$, the associatively flat ground term $i(f(a, b))$ with size 4 is rewritten to the associatively flat ground term $f(i(b), i(a))$ with size 5. Also, a reduction step by an A-flat rule in $S^{\succ}_{\infty}(E)$ may preserve the size of a given associatively flat ground term.

Definition 3.18. Let t be an associatively flat ground term in $T(\Sigma, C)$.
(i) The *d-measure* of t is the multiset of all pairs (d, n), where d is the depth of each term headed by an occurrence of the inverse symbol $i \in \Sigma_G$ in t, and n is the arity of $f \in \Sigma_G$ occurring right below i. If the symbol occurring right below i is not $f \in \Sigma_G$, then n in (d, n) is simply 0. If there is no occurrence of $i \in \Sigma_G$ in t, then the corresponding multiset is simply empty.
(ii) The *s-measure* of t is the size of t.

[3] A simple example of a non-overlap peak is the case $f(c_1, c, d) \leftarrow_{S^{\succ}_{\infty}(E)/A} f(a, b, c, d) \rightarrow_{S^{\succ}_{\infty}(E)/A} f(a, b, c_2)$ if $f \in \Sigma_A$, $f(a, b) \rightarrow c_1 \in S^{\succ}_{\infty}(E)$, and $f(c, d) \rightarrow c_2 \in S^{\succ}_{\infty}(E)$.

(iii) Given a total precedence on the constant symbols in C, we define a weight function $w : C \to \mathbb{N}$ in such a way that for all $c_1, c_2 \in C$, if $c_1 \succ c_2$, then $w(c_1) > w(c_2)$, where $>$ is the usual order on natural numbers. The *w-measure* of t is the sum of the weights of all constants occurring in t.
(iv) The *complexity measure* of an associatively flat ground term is the triple (D, S, W), where D is the d-measure of it, S is the s-measure of it, and W is the w-measure of it. The associated ordering of the complexity measures on associatively flat ground terms, denoted by $\succ_{CM}$, is the lexicographic ordering using the lexicographic and multiset extension of $>$ for the first component, and $>$ for the second and third component, where $>$ is the usual order on natural numbers. (Since the lexicographic extension and the multiple extension of a well-founded order is well-founded, $\succ_{CM}$ on associatively flat ground terms is well-founded.)

Example 3.19. (i) Consider $i(h(i(f(a, b, c))))$ for $i, f \in \Sigma_G$. The d-measure of it is the multiset $\{(2, 3), (4, 0)\}$ because the depth of the term headed by i in $i(f(a, b, c))$ is 2 and the arity of f is 3. Meanwhile, the depth of the term headed by the outermost occurrence of i is 4, but the symbol occurring right below it is not $f \in \Sigma_G$, so the corresponding pair is $(4, 0)$. Now, consider an $gr(R(G))/A$-reduction step by a ground instance of the rule $i(f(x_1, x_2)) \to f(i(x_2), i(x_1)) \in R(G)$. For example, $i(h(i(f(a, b, c))))$ is rewritten to $i(h(i(f(b, c)), i(a)))$ by this reduction step. We see that the d-measure of $i(h(i(f(b, c)), i(a)))$ is $\{(1, 0), (2, 2), (4, 0)\}$. Note that the d-measure $\{(1, 0), (2, 2), (4, 0)\}$ of $i(h(i(f(b, c)), i(a)))$ is smaller than the d-measure $\{(2, 3), (4, 0)\}$ of $i(h(i(f(a, b, c))))$. (Recall that the reduction steps by $gr(R(G))/A$ are always done on associatively flat ground terms.)
(ii) Let $C = \{a, b, c_1, c_2\}$ with the precedence $c_1 \succ c_2 \succ a \succ b$. Then we may assign the weight of each symbol in such a way that $w(c_1) = 4$, $w(c_2) = 3$, $w(a) = 2$, and $w(b) = 1$. Now, consider an $S^{\succ}_{\infty}(E)/A$-reduction step by the A-flat rule $f(c_1, a) \to f(c_2, b)$. For example, $h(f(c_1, a))$ is rewritten to $h(f(c_2, b))$ by this reduction step. The w-measure of $h(f(c_2, b))$ is smaller than the w-measure of $h(f(c_1, a))$ because $w(f(c_1, a)) = 6$ and $w(f(c_2, b)) = 4$.

Lemma 3.20. *The ground rewrite relation $(S^{\succ}_{\infty}(E) \cup gr(R(G)))/A$ is terminating on $T(\Sigma, C)$.*

Proof. We use the complexity measure (D, S, W) of an associatively flat ground term in $T(\Sigma, C)$ (see Definition 3.18(iv)) and compare these measures w.r.t. $\succ_{CM}$ for each type of $(S^{\succ}_{\infty}(E) \cup gr(R(G)))/A$-reduction step. First, observe that the rules in $R(G)$ are size-reducing except the rule $i(f(x_1, x_2)) \to f(i(x_2), i(x_1)) \in R(G)$. Let t_1 and t_2 be associatively flat ground terms in $T(\Sigma, C)$ such that $(S^{\succ}_{\infty}(E) \cup gr(R(G)))/A$-reduction step exists from t_1 to t_2. Let $comp(t_1)$ and $comp(t_2)$ denote the complexity measure of t_1 and t_2, respectively. We consider each type of $(S^{\succ}_{\infty}(E) \cup gr(R(G)))/A$-reduction step from t_1 to t_2. If it is a $gr(R(G))/A$-reduction step by a ground instance of the rule $i(f(x_1, x_2)) \to f(i(x_2), i(x_1)) \in R(G)$, then $comp(t_2)$ is smaller (w.r.t. $\succ_{CM}$) than $comp(t_1)$ in the first component. If it is a $gr(R(G))/A$-reduction step by a ground instance from the other rules in $R(G)$, then $comp(t_2)$ is smaller (w.r.t. $\succ_{CM}$) than $comp(t_1)$ in the second component. (It could be the case that $comp(t_2)$ is smaller (w.r.t. $\succ_{CM}$) than $comp(t_1)$ in the other components too.) If it is an $S^{\succ}_{\infty}(E)/A$-reduction step by a D-flat rule, then $comp(t_2)$ is smaller (w.r.t. $\succ_{CM}$) than $comp(t_1)$ in the second component. If it is an $S^{\succ}_{\infty}(E)/A$-reduction step by an A-flat rule or a constant rule (i.e., $c_m \to c_n$ for some $c_m, c_n \in C$ with $c_m \succ c_n$), then $comp(t_2)$ is smaller (w.r.t. $\succ_{CM}$) than $comp(t_1)$ in the third component.

Since each $(S^{\succ}_{\infty}(E) \cup gr(R(G)))/A$-reduction step strictly reduces the complexity measure (w.r.t. $\succ_{CM}$) and $\succ_{CM}$ is well-founded on the complexity measures of the associatively flat ground terms in $T(\Sigma, C)$ (see Definition 3.18(iv)), the conclusion follows. □

Theorem 3.21. *The ground rewrite system $S^{\succ}_{\infty}(E) \cup gr(R(G))$ is convergent modulo A on $T(\Sigma, C)$.*

Proof. Since $(S^{\succ}_{\infty}(E) \cup gr(R(G)))/A$ is terminating on $T(\Sigma, C)$ by Lemma 3.20, we show that $(S^{\succ}_{\infty}(E) \cup gr(R(G)))/A$ confluent on $T(\Sigma, C)$ by showing that it is locally confluent on $T(\Sigma, C)$. In this proof, we omit the joinability of the pair obtained by rewriting within the substitution part (cf. *variable overlap*) involving the rules in $gr(R(G))$ from $R(G)$, which is discussed similarly in the literature [BN98, DP01]. We also omit the case of non-overlaps involving the rules in $gr(R(G))$ and $S^{\succ}_{\infty}(E)$, which is also discussed similarly in the literature [BN98, DP01].

Now, it suffices to consider the (critical) overlaps between the rules in $gr(R(G))$ and $S^{\succ}_{\infty}(E)$. Recall that for each rule $l \to r$ in $S^{\succ}_{\infty}(E)$, the right-hand side r is irreducible and every proper subterm of l is irreducible by $S^{\succ}_{\infty}(E)/A$ by Lemma 3.17.

Suppose that there is an overlap between a rule $i(i(a_i)) \to a_i$ in $gr(R(G))$ and a rule $i(a_i) \to c_{a_i}$ in $S^{\succ}_{\infty}(E)$ with the critical pair $i(c_{a_i}) \approx a_i$. Since $i(c_{a_i}) \to a_i$ in $S^{\succ}_{\infty}(E)$ by construction (see Phase II), $i(c_{a_i})$ and a_i are joinable by the rule in $S^{\succ}_{\infty}(E)$.

Suppose that there is an overlap between a rule $f(c, i(c)) \to 1$ (resp. $f(i(c), c) \to 1$) in $gr(R(G))$ and a rule $i(c) \to d$ in $S^{\succ}_{\infty}(E)$ with the critical pair $f(c, d) \approx 1$ (resp. $f(d, c) \approx 1$). Since $i(c) \to d$ in $S^{\succ}_{\infty}(E)$, we also have $f(c, d) \to 1$ and $f(d, c) \to 1$ in $S^{\succ}_{\infty}(E)$ (see Phase II), and thus $f(c, d)$ (resp. $f(d, c)$) and 1 are joinable by the rule in $S^{\succ}_{\infty}(E)$.[4]

Suppose that there is an overlap between a rule $f(u_1, \ldots, u_m, 1) \to f(u_1, \ldots, u_m)$ (resp. $f(1, u_1, \ldots, u_m) \to f(u_1, \ldots, u_m)$) in $gr(R(G))$ and a rule $f(u_m, 1) \to u_m$ (resp. $f(1, u_1) \to u_1$) in $S^{\succ}_{\infty}(E)$. Then, the critical pair $f(u_1, \ldots, u_m) \approx f(u_1, \ldots, u_m)$ is trivially joinable.

Suppose that there is an overlap between a rule of the form $i(f(u_1, \ldots, u_n)) \to f(i(\bar{f}(u_{m+1}, \ldots, u_n)), i(\bar{f}(u_1, \ldots, u_m)))$ in $gr(R(G))$ and a rule $f(u_1, \ldots, u_n) \to u_m$ in $S^{\succ}_{\infty}(E)$. (Here, $\bar{f}(u_k, \ldots, u_1)$ is $f(u_k, \ldots, u_1)$ if $k \geq 2$, and u_1, otherwise (i.e., $k = 1$).) We show that $f(i(\bar{f}(u_{m+1}, \ldots, u_n)), i(\bar{f}(u_1, \ldots, u_m)))$ and $i(u_m)$ are joinable by $\to_{S^{\succ}_{\infty}(E) \cup gr(R(G))/A}$. As $f(i(\bar{f}(u_{m+1}, \ldots, u_n)), i(\bar{f}(u_1, \ldots, u_m))) \xrightarrow{*}_{gr(R(G))/A} f(i(u_n), i(u_{n-1}), \ldots, i(u_1))$, we show that $f(i(u_n), i(u_{n-1}), \ldots, i(u_1))$ and $i(u_m)$ are joinable by $\to_{S^{\succ}_{\infty}(E)/A}$. By construction, we have some rules $i(u_1) \to c_{u_1}, i(u_2) \to c_{u_2}, \ldots, i(u_n) \to c_{u_n}$ and $i(u_m) \to c_{u_m}$ in $S^{\succ}_{\infty}(E)$, where $u_1, \ldots, u_n, u_m$ and $c_{u_1}, \ldots, c_{u_n}, c_{u_m}$ may not be distinct. We also have the rules $f(u_1, c_{u_1}) \to 1, f(c_{u_1}, u_1) \to 1, \ldots, f(u_n, c_{u_n}) \to 1, f(c_{u_n}, u_n) \to 1, f(u_m, c_{u_m}) \to 1, f(c_{u_m}, u_m) \to 1$ in $S^{\succ}_{\infty}(E)$. Now, it suffices to show that $f(c_{u_n}, \ldots, c_{u_1})$ and c_{u_m} are joinable by $\to_{S^{\succ}_{\infty}(E)/A}$. Since $f(u_1, \ldots, u_n) \to u_m$ in $S^{\succ}_{\infty}(E)$, we have $f(c_{u_m}, u_1, \ldots, u_n, c_{u_n}, \ldots, c_{u_1}) \to_{S^{\succ}_{\infty}(E)/A} f(c_{u_m}, u_m, c_{u_n}, \ldots, c_{u_1})$ by applying the same context to the rule $f(u_1, \ldots, u_n) \to u_m$ in $S^{\succ}_{\infty}(E)$. This means that $f(c_{u_m}, u_1, \ldots, u_n, c_{u_n}, \ldots, c_{u_1})$ and $f(c_{u_m}, u_m, c_{u_n}, \ldots, c_{u_1})$ are joinable by $\to_{S^{\succ}_{\infty}(E)/A}$. Since $f(c_{u_m}, u_1, \ldots, u_n, c_{u_n}, \ldots, c_{u_1}) \xrightarrow{*}_{S^{\succ}_{\infty}(E)/A} c_{u_m}$ and $f(c_{u_m}, u_m, c_{u_n}, \ldots, c_{u_1}) \xrightarrow{*}_{S^{\succ}_{\infty}(E)/A} f(c_{u_n}, \ldots, c_{u_1})$, by Lemma 3.16, we infer that $f(c_{u_n}, \ldots, c_{u_1})$ and c_{u_m} are joinable by $\to_{S^{\succ}_{\infty}(E)/A}$.

Finally, suppose that there is an overlap between a rule of the form $i(f(u_1, \ldots, u_n)) \to f(i(\bar{f}(u_{m+1}, \ldots, u_n)), i(\bar{f}(u_1, \ldots, u_m)))$ in $gr(R(G))$ and a rule $f(u_1, \ldots, u_n) \to f(v_1, \ldots, v_m)$ in $S^{\succ}_{\infty}(E)$. (Here, $\bar{f}(u_k, \ldots, u_1)$ is $f(u_k, \ldots, u_1)$ if $k \geq 2$, and u_1, otherwise.) We show

[4] If one also considers the overlapping involving *extension* [DP01] rules, it is easy to see that the case of overlapping between the ground instances of the extension of $f(c, i(c)) \to 1$ (resp. $f(i(c), c) \to 1$) in $gr(R(G))$ and $i(c) \to d$ in $S^{\succ}_{\infty}(E)$, along with the case of overlapping between the ground instances of the extension of $f(c, 1) \to c$ (resp. $f(1, c) \to 1$) in $gr(R(G))$ and $f(c, 1) \to c$ (resp. $f(1, c) \to c$) in $S^{\succ}_{\infty}(E)$ are both joinable.

that $f(i(\bar{f}(u_{m+1},\ldots,u_n)),\ i(\bar{f}(u_1,\ldots,u_m)))$ and $i(f(v_1,\ldots,v_m))$ are indeed joinable by $\rightarrow_{S^{\succ}_{\infty}(E)\cup gr(R(G))/A}$. Now, since $f(i(\bar{f}(u_{m+1},\ldots,u_n)), i(\bar{f}(u_1,\ldots,u_m))) \xrightarrow{*}_{gr(R(G))/A} f(i(u_n), i(u_{n-1}),\ldots,i(u_1))$, and $i(f(v_1,\ldots,v_m)) \xrightarrow{*}_{gr(R(G))/A} f(i(v_m),\ldots,i(v_1))$, we then show that $f(i(u_n),i(u_{n-1}),\ldots,i(u_1))$ and $f(i(v_m),\ldots,i(v_1))$ are joinable by $\rightarrow_{S^{\succ}_{\infty}(E)/A}$. By construction, we have some rules $i(u_1)\rightarrow c_{u_1}, i(u_2)\rightarrow c_{u_2},\ldots,i(u_n)\rightarrow c_{u_n}$, $i(v_1)\rightarrow c_{v_1},\ldots,i(v_m)\rightarrow c_{v_m}$ in $S^{\succ}_{\infty}(E)$, where $u_1,\ldots,u_n,v_1,\ldots,v_m,c_{u_1},\ldots,c_{u_n},c_{v_1},\ldots,c_{v_m}$ may not be distinct. It suffices to show that $f(c_{u_n},\ldots,c_{u_1})$ and $f(c_{v_m},\ldots,c_{v_1})$ are joinable by $\rightarrow_{S^{\succ}_{\infty}(E)/A}$. Since $f(u_1,\ldots,u_n)\rightarrow f(v_1,\ldots,v_m)\in S^{\succ}_{\infty}(E)$, we see that $f(c_{v_m},\ldots,c_{v_1},u_1,\ldots,u_n,c_{u_n},\ldots,c_{u_1}) \rightarrow_{S^{\succ}_{\infty}(E)/A} f(c_{v_m},\ldots,c_{v_1},v_1,\ldots,v_m,c_{u_n},\ldots,c_{u_1})$ by applying the same context to the rule $f(u_1,\ldots,u_n)\rightarrow f(v_1,\ldots,v_m)$ in $S^{\succ}_{\infty}(E)$, so $f(c_{v_m},\ldots,c_{v_1},u_1,\ldots,u_n,c_{u_n},\ldots,c_{u_1})$ and $f(c_{v_m},\ldots,c_{v_1},v_1,\ldots,v_m,c_{u_n},\ldots,c_{u_1})$ are joinable by $\rightarrow_{S^{\succ}_{\infty}(E)/A}$. Since $f(c_{v_m},\ldots,c_{v_1},u_1,\ldots,u_n,c_{u_n},\ldots,c_{u_1}) \xrightarrow{*}_{S^{\succ}_{\infty}(E)/A} f(c_{v_m},\ldots,c_{v_1})$ and $f(c_{v_m},\ldots,c_{v_1},v_1,\ldots,v_m,c_{u_n},\ldots,c_{u_1}) \xrightarrow{*}_{S^{\succ}_{\infty}(E)/A} f(c_{u_n},\ldots,c_{u_1})$, by Lemma 3.16, we infer that $f(c_{u_n},\ldots,c_{u_1})$ and $f(c_{v_m},\ldots,c_{v_1})$ are joinable by $\rightarrow_{S^{\succ}_{\infty}(E)/A}$. □

The following theorem says that given $s_0\approx t_0$, where $s_0,t_0\in T(\Sigma,C_0)$, the membership problem for $CC^G(E)$, written $s_0\overset{?}{\approx} t_0\in CC^G(E)$, is reduced to checking whether s_0 and t_0 have the same normal form w.r.t. $(S^{\succ}_{\infty}(E)\cup gr(R(G)))/A$.

Theorem 3.22. *If $s_0,t_0\in T(\Sigma,C_0)$, then $s_0\approx t_0\in CC^G(E)$ iff s_0 and t_0 have the same normal form w.r.t. $(S^{\succ}_{\infty}(E)\cup gr(R(G)))/A$.*

Proof. Assume that $s_0,t_0\in T(\Sigma,C_0)$. If $s_0\approx t_0\in CC^G(E)$, then $s_0\approx_{S_{\infty}(E)\cup gr(R(G))\cup gr(A)} t_0$ by Lemma 3.13. Since $S^{\succ}_{\infty}(E)\cup gr(R(G))$ is convergent modulo A on $T(\Sigma,C)$ by Theorem 3.21, s_0 and t_0 have the same normal form w.r.t. $(S^{\succ}_{\infty}(E)\cup gr(R(G))/A$.

Conversely, if s_0 and t_0 have the same normal form w.r.t. $(S^{\succ}_{\infty}(E)\cup gr(R(G))/A$, then we have $s_0\approx_{S_{\infty}(E)\cup gr(R(G))\cup gr(A)} t_0$, and thus $s_0\approx t_0\in CC^G(E)$ by Lemma 3.13. □

Remark 3.23. Note that $s_0,t_0\in T(\Sigma,C_0)$ with $s_0\approx t_0\in CC^G(E)$ in Theorem 3.22 may have the normal forms w.r.t. $(S^{\succ}_{\infty}(E)\cup gr(R(G)))/A$ in $T(\Sigma,C_1)$, but they are the same by Theorem 3.21 because $T(\Sigma,C_0)\subseteq T(\Sigma,C)$. (Recall that $C:=C_0\cup C_1$.)

Remark 3.24. Recall that $gr(R(G))$ in Theorem 3.22 is defined as $gr(R(G)):=\{l\sigma\rightarrow r\sigma\mid l\rightarrow r\in R(G)\wedge\sigma \text{ is a ground substitution}\}$. (Here, a ground substitution maps variables to (ground) terms in $T(\Sigma,C)$.) This means that $gr(R(G))$ can be infinite. However, instead of using the infinite ground rewrite system $gr(R(G))$ directly, we can still use the finite rewrite system $R(G)$ for rewriting steps w.r.t. $gr(R(G))/A$ by using A-matching on (ground) terms in $T(\Sigma,C)$.

Corollary 3.25. *Given a finite set of ground equations $E\subseteq T(\Sigma,C_0)\times T(\Sigma,C_0)$, if $S_{\infty}(E)$ is finite, then we can decide for any $s_0,t_0\in T(\Sigma,C_0)$ whether $s_0\approx^G_E t_0$ holds or not.*

Proof. By Birkhoff's theorem, $CC^G(E)$ coincides with $\approx^G_E$. By Theorem 3.22, we can decide whether $s_0\approx^G_E t_0$ using the normal forms of s_0 and t_0 w.r.t. $(S^{\succ}_{\infty}(E)\cup gr(R(G)))/A$, i.e., s_0 and t_0 have the same normal form w.r.t. $(S^{\succ}_{\infty}(E)\cup gr(R(G)))/A$ iff $s_0\approx^G_E t_0$. □

Example 3.26. (Continued from Example 3.11) Consider the word problem of deciding whether $i(i(f(h(a),f(i(b),a))))\approx^G_E 1$ holds or not using $S_{\infty}(E)$ in Example 3.11. Recall that two notations $f(u)$ and $f(u_1,\ldots,u_n)$ are used interchangeably if $f\in\Sigma_A$ and u is a string over C such that $u := u_1, \ldots, u_n$ and $|u| \geq 2$. Then, $S_\infty^\succ(E) = \{h(1) \to b, c_2 \to 1, a \to 1, i(1) \to 1, c_1 \to b, c_3 \to c_4, i(b) \to c_4, i(c_4) \to b, f(b, c_4) \to 1, f(c_4, b) \to 1\} \cup \bar{U}^\succ(C)$, where $\bar{U}^\succ(C) = \{f(1,1) \to 1, f(b,1) \to b, f(1,b) \to b, f(c_4, 1) \to c_4, f(1, c_4) \to c_4\}$. First, $i(i(f(h(a), f(i(b), a))))$ is associatively flattened to $i(i(f(h(a), i(b), a)))$.

Let $SG := S_\infty^\succ(E) \cup gr(R(G))$. Then, $i(i(f(h(a), i(b), a))) \to_{SG/A} f(h(a), i(b), a) \xrightarrow{*}_{SG/A} f(h(1), i(b), 1) \to_{SG/A} f(b, i(b), 1) \to_{SG/A} f(b, c_4, 1) \to_{SG/A} f(1,1) \to_{SG/A} 1$. Now, we see that $i(i(f(h(a), f(i(b), a)))) \approx_E^G 1$ holds and $i(i(f(h(a), f(i(b), a)))) \approx 1 \in CC^G(E)$ by Theorem 3.22.

Definition 3.27. Given $S_0 = S(E)$, let $R(E)$ be the set of D-flat and A-flat equations containing $f \in \Sigma_G$ in $S(E) - U(C)$ (see Phase II). Let $C(R)$ be the set of constant symbols appearing in $R(E)$ except 1. We say that $<C(R) \,|\, R(E)>$ is the *monoid presentation for* $S(E)$.

Example 3.28. Let $E = \{f(a,a,a) \approx 1, f(h(a), h(a)) \approx 1, f(a, h(a), a, h(a)) \approx 1\}$ and $f \in \Sigma_G$. Then $S(E) = \{f(aaa) \approx 1, h(a) \approx c_1, f(c_1c_1) \approx 1, f(ac_1ac_1) \approx 1, i(1) \approx 1, i(a) \approx c_2, i(c_2) \approx a, i(c_1) \approx c_3, i(c_3) \approx c_1, f(ac_2) \approx 1, f(c_2a) \approx 1, f(c_1c_3) \approx 1, f(c_3c_1) \approx 1\} \cup U(C)$, where $C = \{1, a, c_1, c_2, c_3\}$. Now, we have the monoid presentation $<C(R) \,|\, R(E)>$ for $S(E)$, where $C(R) = \{a, c_1, c_2, c_3\}$ and $R(E) = \{f(ac_2) \approx 1, f(c_2a) \approx 1, f(c_1c_3) \approx 1, f(c_3c_1) \approx 1, f(aaa) \approx 1, f(c_1c_1) \approx 1, f(ac_1ac_1) \approx 1\}$. This monoid presentation for $S(E)$ corresponds to a monoid presentation of the dihedral group of order 6 [HEO05] $<\alpha, \beta, \alpha^{-1}, \beta^{-1}, \,|\, \alpha\alpha^{-1} \approx 1, \alpha^{-1}\alpha \approx 1, \beta\beta^{-1} \approx 1, \beta^{-1}\beta \approx 1, \alpha^3 \approx 1, \beta^2 \approx 1, \alpha\beta\alpha\beta \approx 1>$ by renaming the symbols a to α, c_1 to β, c_2 to α^{-1}, and c_3 to β^{-1}.

It is known that the Knuth-Bendix completion terminates for finite groups using their monoid presentations [HEO05] with their associated length-lexicographic ordering. Similarly, if the monoid presentation for $S_0 = S(E)$ is a monoid presentation of a finite group, then $S_\infty(E)$ is finite (see Proposition 3.30), providing a decision procedure for the word problem for E w.r.t. G by Corollary 3.25.

Example 3.29. (Continued from Example 3.28) Given $S(E) = \{f(aaa) \approx 1, h(a) \approx c_1, f(c_1c_1) \approx 1, f(ac_1ac_1) \approx 1, i(1) \approx 1, i(a) \approx c_2, i(c_2) \approx a, i(c_1) \approx c_3, i(c_3) \approx c_1, f(ac_2) \approx 1, f(c_2a) \approx 1, f(c_1c_3) \approx 1, f(c_3c_1) \approx 1\} \cup U(C)$ and $C = \{1, a, c_1, c_2, c_3\}$ in Example 3.28, let $i \succ h \succ f \succ c_1 \succ c_2 \succ c_3 \succ a \succ 1$ (see Definition 3.6). In the following, we implicitly apply SIMPLIFY using $U(C)$ whenever applicable (cf. Example 3.11):

$1' : c_1 \approx c_3$ (DEDUCE by $f(c_1c_1) \approx 1$ and $f(c_1c_3) \approx 1$)
(By $1'$, each c_1 occurring in $S(E)$ is replaced by c_3 using COLLAPSE and COMPOSE.)
...
$2' : f(aa) \approx c_2$ (DEDUCE by $f(aaa) \approx 1$ and $f(ac_2) \approx 1$)
$3' : f(c_2c_2) \approx a$ (DEDUCE by $2'$ and $f(ac_2) \approx 1$)
$4' : f(ac_3a) \approx c_3$ (DEDUCE by $f(ac_3ac_3) \approx 1$ and $f(c_3c_3) \approx 1$)
$5' : f(c_2c_3) \approx f(c_3a)$ (DEDUCE by $4'$ and $f(c_2a) \approx 1$)
$6' : f(c_3c_2) \approx f(ac_3)$ (DEDUCE by $4'$ and $f(ac_2) \approx 1$)
$7' : f(c_3ac_3) \approx c_2$ (DEDUCE by $6'$ and $f(c_3c_3) \approx 1$)
...

After several steps using the contraction rules, we have the finite set $S_\infty(E) = \{h(a) \approx c_3, f(c_3c_3) \approx 1, i(1) \approx 1, i(a) \approx c_2, i(c_2) \approx a, i(c_3) \approx c_3, f(ac_2) \approx 1, f(c_2a) \approx 1\} \cup \bar{U}(C) \cup \{1', 2', 3', 4', 5', 6', 7'\}$, where $\bar{U}(C)$ is obtained from $U(C)$ by rewriting each occurrence of

c_1 in $U(C)$ to c_3. Now, we have the finite rewrite system $S_\infty^{\succ}(E)$, which is obtained from $S_\infty(E)$ by orienting each equation in $S_\infty(E)$ into the rewrite rule. Given $S_0 = S(E)$, the output depends on a given precedence on symbols, but the completion procedure necessarily terminates (see Proposition 3.30).

Proposition 3.30. *Given $S_0 = S(E)$, if the monoid presentation $<C(R)\,|\,R(E)>$ for $S(E)$ is a monoid presentation of a finite group, then $S_\infty(E)$ is finite.*

Proof. Let $X = C(R)$ and $f \in \Sigma_G$. If the monoid presentation $<X\,|\,R(E)>$ for $S(E)$ is a monoid presentation of a finite group, then there are only finitely many $\xleftrightarrow{*}_{R(E)\cup gr(A)}$ equivalence classes on $\{f(u)\,|\,u \in X^* \text{ and } |u| \geq 2\}$ (see Chapter 12 in [HEO05]).

Now, if X is not the same as C, then let $\bar{X}$ be the set obtained from X by adding each constant $c' \in C - X$ satisfying $c' \xleftrightarrow{*}_{S(E)} c$ for some $c \in X$ to X. (If either $X = C$ or $X \neq C$ but such c' does not exist, then we simply let $\bar{X} := X$.) Since there are finitely many $\xleftrightarrow{*}_{R(E)\cup gr(A)}$ equivalence classes on $\{f(u)\,|\,u \in X^* \text{ and } |u| \geq 2\}$, we may infer that there are also finitely many $\xleftrightarrow{*}_{S(E)\cup gr(A)}$ equivalence classes on $\{f(u)\,|\,u \in \bar{X}^* \text{ and } |u| \geq 2\}$.

By Lemma 3.12, we have $\xleftrightarrow{*}_{S(E)\cup gr(A)} = \xleftrightarrow{*}_{S_\infty(E)\cup gr(A)}$, so there are only finitely many $\xleftrightarrow{*}_{S_\infty(E)\cup gr(A)}$ equivalence classes on $\{f(u)\,|\,u \in \bar{X}^* \text{ and } |u| \geq 2\}$. Since $S_\infty^{\succ}(E)$ is convergent modulo A by Lemma 3.16, this means that there are only finitely many $S_\infty^{\succ}(E)/A$-normal forms of the terms in $\{f(u)\,|\,u \in \bar{X}^* \text{ and } |u| \geq 2\}$.

Suppose that $S_\infty(E)$ is an infinite set. Since non-Σ_A symbols have fixed arities and $\Sigma \cup C$ is finite, $S_\infty(E)$ must contain infinitely many equations with top symbol f. As there are only finitely many $S_\infty^{\succ}(E)/A$-normal forms of the terms in $\{f(u)\,|\,u \in \bar{X}^* \text{ and } |u| \geq 2\}$, there is some rule $f(u_1 \cdots u_n) \to t \in S_\infty^{\succ}(E)$ such that a proper subterm of $f(u_1 \cdots u_n)$ is reducible by $S_\infty^{\succ}(E)/A$. This is not possible by Lemma 3.17, a contradiction. □

4. Congruence closure modulo semigroups, monoids, and the multiple disjoint sets of group axioms

Given a finite set of ground equations E between terms $s, t \in T(\Sigma, C_0)$, by congruence closure modulo semigroups (resp. monoids), we mean congruence closure modulo the associativity (resp. monoid) axioms for E. In this section, we first discuss congruence closure modulo semigroups by considering multiple associative symbols. Then we discuss congruence modulo monoids by considering multiple associative symbols but only one of them is an interpreted symbol for the monoid axioms. We also discuss congruence closure modulo the multiple disjoint sets of group axioms. All these approaches only differ by Phases I and II in Section 3, but they use the same Phase III in Section 3. This means that one may use the same completion procedure for constructing congruence closure modulo the semigroup, monoid, and the multiple disjoint sets of group axioms, respectively.

4.1. Congruence closure modulo semigroups.

Unlike constructing congruence closure modulo the group axioms, constructing congruence closure modulo the semigroup axioms does not need to add certain ground flat equations entailed by the group axioms, so Phase II in Section 3 is not necessary. Also, normalizing each term using the rewriting by $R(G)/A$ is not necessary, either. Now, Phase I for constructing congruence modulo semigroups is the same as Phases I in Section 3 without step 2. The output of Phase I is denoted by $S(E)$, where all equations in $S(E)$ are constant, D-flat, or A-flat equations. Then one may apply Phase III in Section 3 directly using the same inference rules in Figure 1 with $S_0 = S(E)$ and have the same Lemmas 3.12 and 3.16. Now, we have the following results adapted from Lemma 3.13, Theorem 3.22 and Corollary 3.25, respectively.

Lemma 4.1. *If $s_0, t_0 \in T(\Sigma, C_0)$, then $s_0 \approx t_0 \in CC^A(E)$ iff $s_0 \approx_{S_\infty(E)\cup gr(A)} t_0$.*

Proof. By Birkhoff's theorem, $CC^A(E)$ coincides with $\approx_E^A$. Adapted from Lemma 3.4, we may infer that $s_0 \approx_E^A t_0$ iff $s_0 \approx_{S(E)}^A t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$. Also, $s_0 \approx_{S(E)}^A t_0$ iff $s_0 \approx_{S(E)\cup gr(A)} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$.

It remains to show that $s_0 \approx_{S(E)\cup gr(A)} t_0$ iff $s_0 \approx_{S_\infty(E)\cup gr(A)} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$, where $S_0 = S(E)$. By Lemma 3.12, if $S_i \vdash S_{i+1}$, then $\overset{*}{\leftrightarrow}_{S_i\cup gr(A)}$ and $\overset{*}{\leftrightarrow}_{S_{i+1}\cup gr(A)}$ on $T(\Sigma, C_0)$ are the same, and thus the conclusion follows. □

Lemma 4.2. *If $s_0, t_0 \in T(\Sigma, C_0)$, then $s_0 \approx t_0 \in CC^A(E)$ iff s_0 and t_0 have the same normal form w.r.t. $S_\infty^\succ(E)/A$.*

Proof. Assume that $s_0, t_0 \in T(\Sigma, C_0)$. If $s_0 \approx t_0 \in CC^A(E)$, then $s_0 \approx_{S_\infty(E)\cup gr(A)} t_0$ by Lemma 4.1. Since $S_\infty^\succ(E)$ is convergent modulo A by Lemma 3.16, s_0 and t_0 have the same normal form w.r.t. $S_\infty^\succ(E)/A$.

Conversely, if s_0 and t_0 have the same normal form w.r.t. $S_\infty^\succ(E)/A$, then we have $s_0 \approx_{S_\infty(E)\cup gr(A)} t_0$, and thus $s_0 \approx t_0 \in CC^A(E)$ by Lemma 4.1. □

Corollary 4.3. *Given a finite set of ground equations $E \subseteq T(\Sigma, C_0) \times T(\Sigma, C_0)$, if $S_\infty(E)$ is finite, then we can decide for any $s_0, t_0 \in T(\Sigma, C_0)$ whether $s_0 \approx_E^A t_0$ holds or not.*

In the remainder of this section, the examples are only concerned with a set of associatively flattened, ground fully flat equations E for simplicity. (See Example 3.2 in Section 3 for an example of the associatively flattening and the fully flattening step, respectively.)

Example 4.4. Let $E = \{f(a, b) \approx a, f(b, c) \approx b, c \approx d\}$ with $f \in \Sigma_A$ and $a \succ b \succ c \succ d$. Each term in E is already associatively flattened. Also, the equation in E is already a ground fully flat equation, so Phase I is not needed. Phase II is not needed either for $CC^A(E)$, so $S(E)$ is simply E itself. The following steps are performed in Phase III using $S_0 = S(E)$:

1′: $f(ab) \approx f(ac)$ (DEDUCE by $f(ab) \approx a$ and $f(bc) \approx b$.)
2′: $f(ac) \approx a$ (SIMPLIFY 1′ by $f(ab) \approx a$. 1′ is deleted.)
3′: $f(ad) \approx a$ (COLLAPSE 2′ by $c \approx d$. 2′ is deleted.)
4′: $f(bd) \approx b$ (COLLAPSE $f(b, c) \approx b$ by $c \approx d$. $f(b, c) \approx b$ is deleted.)

Now, we have $S_\infty^\succ(E) = \{f(ab) \to a, f(bd) \to b, c \to d, f(ad) \to a\}$. By Lemma 4.2 and Corollary 4.3, we can decide whether $f(a, b) \approx_E^A f(a, c)$. Since $f(ab) \to_{S_\infty^\succ(E)/A} a$ and $f(ac) \to_{S_\infty^\succ(E)/A} f(ad) \to_{S_\infty^\succ(E)/A} a$, we see that $f(a, b) \approx f(a, c) \in CC^A(E)$ and $f(a, b) \approx_E^A f(a, c)$.

The following example shows that $S_\infty(E)$ can be infinite. In this case, one cannot apply Corollary 4.3.

Example 4.5. (Adapted from [KN85a]) Let $E = \{f(a, b, a) \approx f(b, a, b)\}$ with $f \in \Sigma_A$. Each term in E is already associatively flattened. Also, each equation in E is already a ground fully flat equation, so Phase I is not needed. Phase II is not needed either for $CC^A(E)$, so $S(E)$

is simply E itself. The following steps are performed in Phase III using $S_0 = S(E)$ with $a \succ b$:

$1'$: $f(abbab) \approx f(babba)$ (DEDUCE by $f(aba) \approx f(bab)$ and itself.)
$2'$: $f(abbbab) \approx f(babbaa)$ (DEDUCE by $1'$ and $f(aba) \approx f(bab)$.)
...

Phase III does not terminate and we have the infinite $S^{\succ}_{\infty}(E) = \{f(aba) \to f(bab)\} \cup \{f(ab^n ab) \to f(babba^{n-1}) \,|\, n \geq 2\}$. Using the similar argument by Kapur and Narendran [KN85a], we see that Phase III does not terminate. (Here, the word problem for E w.r.t. A is decidable [KN85a].)

Remark 4.6. In Example 4.5, if we introduced a new constant c_1 to stand for $f(a, b)$ with $c_1 \succ b \succ a$, then we have $E' = \{f(a, b) \approx c_1, f(c_1, a) \approx f(b, c_1)\}$ from E. In this case, Phase III using $S_0 = E'$ terminates with the finite $S^{\succ}_{\infty}(E') = \{f(ab) \to c_1, f(c_1 a) \to f(bc_1), f(bc_1 b) \to f(c_1 c_1), f(c_1 c_1 b) \to f(ac_1 c_1)\}$ (cf. Section 6 in [KN85a]). This is beyond the scope of this paper because we do not introduce a new constant for an (already) ground flat equation in E for $CC^A(E)$.

4.2. **Congruence closure modulo monoids.** In this subsection, we denote by Σ_M the set $\{f, 1\}$, where $f \in \Sigma_A$ is the interpreted symbol for the monoid axioms $M := A \cup \{f(x, 1) \approx x, f(1, x) \approx x\}$ and $1 \in C_0$ is the unit in M. The convergent rewrite system for monoids, denoted $R(M)$, on associatively flat terms is simply given as follows: (i) $f(x, 1) \to x$ and (ii) $f(1, x) \to x$, where $f \in \Sigma_M$. In what follows, we assume that the multiple associative symbols are allowed (i.e., $|\Sigma_A| \geq 1$), but only one of them is used for the monoid axioms. Phases I and II for constructing congruence modulo monoids are slightly different from Phases I and II in Section 3, which do not need to take the inverse axioms into account. In Phase I, the rewrite relation $R(G)/A$ in step 2 in Phases I in Section 3 is simply replaced by the rewrite relation $R(M)/A$. The output of Phase I is denoted by E', where all equations in E' are constant, D-flat, or A-flat equations. The purpose of Phase II is to add certain ground instantiations of the unit axioms. Phase II is now described as follows. Here, $f \in \Sigma_M$, and 1 is the unit in M.

Phase II: Given C and E' obtained from E by Phase I:

(1) Set $S(E) := E' \cup U(C)$ and return $S(E)$, where $U(C) := \{f(c, 1) \approx c \,|\, c \in C\} \cup \{f(1, c) \approx c \,|\, c \in C\}$.

The output of Phase II is $S(E)$. Note that no new constant is added to C in Phase II. Using $S(E)$ obtained from Phase II, we may apply the same Phase III as in Section 3 using $S_0 = S(E)$. Now, the following results are adapted from Lemma 3.13, Theorem 3.22 and Corollary 3.25, respectively.

Lemma 4.7. *If $s_0, t_0 \in T(\Sigma, C_0)$, then $s_0 \approx t_0 \in CC^M(E)$ iff $s_0 \approx_{S_\infty(E) \cup gr(M) \cup gr(A)} t_0$.*

Proof. By Birkhoff's theorem, $CC^M(E)$ coincides with $\approx^M_E$. We have $s_0 \approx^M_E t_0$ iff $s_0 \approx^M_{S(E)} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$ using a simple adaption of Lemma 3.4. Also, $s_0 \approx^M_{S(E)} t_0$ iff $s_0 \approx_{S(E) \cup gr(R(M)) \cup gr(A)} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$.

Now, it remains to show that $s_0 \approx_{S(E) \cup gr(R(M)) \cup gr(A)} t_0$ iff $s_0 \approx_{S_\infty(E) \cup gr(R(M)) \cup gr(A)} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$, where $S_0 = S(E)$. By Lemma 3.12, if $S_i \vdash S_{i+1}$, then both $\overset{*}{\leftrightarrow}_{S_i \cup gr(A)}$ and $\overset{*}{\leftrightarrow}_{S_{i+1} \cup gr(A)}$ on $T(\Sigma, C_0)$ are the same, and thus the conclusion follows. $\square$

Lemma 4.8. *If $s_0, t_0 \in T(\Sigma, C_0)$, then $s_0 \approx t_0 \in CC^M(E)$ iff s_0 and t_0 have the same normal form w.r.t. $(S^{\succ}_{\infty}(E) \cup gr(R(M))/A$.*

Proof. Assume that $s_0, t_0 \in T(\Sigma, C_0)$. If $s_0 \approx t_0 \in CC^M(E)$, then $s_0 \approx_{S_\infty(E)\cup gr(R(M))\cup gr(A)} t_0$ by Lemma 4.7. Using a simple adaptation from Theorem 3.21 without taking the symbol for the inverse axioms into account, we may infer that $S^{\succ}_{\infty}(E) \cup gr(R(M))$ is convergent modulo A, and thus s_0 and t_0 have the same normal form w.r.t. $(S^{\succ}_{\infty}(E) \cup gr(R(M))/A$.

Conversely, if s_0 and t_0 have the same normal form w.r.t. $(S^{\succ}_{\infty}(E) \cup gr(R(M))/A$, then we have $s_0 \approx_{S_\infty(E)\cup gr(R(M))\cup gr(A)} t_0$, and thus $s_0 \approx t_0 \in CC^M(E)$ by Lemma 4.7. □

Corollary 4.9. *Given a finite set of ground equations $E \subseteq T(\Sigma, C_0) \times T(\Sigma, C_0)$, if $S_\infty(E)$ is finite, then we can decide for any $s_0, t_0 \in T(\Sigma, C_0)$ whether $s_0 \approx^M_E t_0$ holds or not.*

Example 4.10 (Continued from Example 4.4)**.** Consider $E = \{f(a, b) \approx a, f(b, c) \approx b, c \approx d\}$ with $f \in \Sigma_A$ and $a \succ b \succ c \succ d$ in Example 4.4 again. Again, Phase I is not needed. For Phase II, since $C = C_0 = \{a, b, c, d, 1\}$, we have $U(C) = \{f(1, 1) \approx 1, f(a, 1) \approx a, f(1, a) \approx a, f(b, 1) \approx b, f(1, b) \approx b, f(c, 1) \approx c, f(1, c) \approx c, f(d, 1) \approx d, f(1, d) \approx d\}$. Now, $S(E) = E \cup U(C)$ and the same equations as in Example 4.4 are generated by Phase III after some contraction steps. Therefore, $S^{\succ}_{\infty}(E) = \{f(ab) \to a, f(bd) \to b, c \to d, f(ad) \to a, f(11) \to 1, f(a1) \to a, f(1a) \to a, f(b1) \to b, f(1b) \to b, f(c1) \to c, f(1c) \to c, f(d1) \to d, f(1d) \to d\}$. By Lemma 4.8 and Corollary 4.9, we can decide whether $f(a, c, 1, d) \approx^A_E a$. Since $f(ac1d) \to_{(S^{\succ}_{\infty}(E)\cup gr(R(M)))/A} f(acd) \to_{(S^{\succ}_{\infty}(E)\cup gr(R(M)))/A} f(add) \to_{(S^{\succ}_{\infty}(E)\cup gr(R(M)))/A} f(ad) \to_{(S^{\succ}_{\infty}(E)\cup gr(R(M)))/A} a$, we see that $f(a, c, 1, d) \approx a \in CC^M(E)$ and $f(a, c, 1, d) \approx^M_E a$.

4.3. **Congruence closure modulo the multiple sets of group axioms.** Section 3 was concerned with congruence closure modulo a single set of group axioms. This subsection adapts Section 3 for constructing congruence closure of a finite set of ground equations with interpreted symbols for the multiple disjoint sets of group axioms.[5]

First, we consider the union of two sets of group axioms G_1 and G_2 with $\Sigma_{G_1} \cap \Sigma_{G_2} = \emptyset$, denoted by $G_1 \uplus G_2$, where $\Sigma_{G_1} = \{f_{G_1}, i_{G_1}, 1_{G_1}\}$ and $\Sigma_{G_2} = \{f_{G_2}, i_{G_2}, 1_{G_2}\}$. This means that both G_1 and G_2 are the sets of group axioms but they do not share any function symbols. Let $R(G_1)$ and $R(G_2)$ be the convergent rewrite systems for G_1 and G_2 on associatively flat terms, respectively (see Section 2). Now, the union of two rewrite systems R_1 and R_2 for $G_1 \uplus G_2$, denoted by $R(G_1) \uplus R(G_2)$, on associatively flat terms has the following rewrite rules:

$$
\begin{array}{llll}
i_{G_1}(1_{G_1}) \to 1_{G_1} & f_{G_1}(x, 1_{G_1}) \to x & f_{G_1}(1_{G_1}, x) \to x & i_{G_1}(i_{G_1}(x)) \to x \\
f_{G_1}(x, i_{G_1}(x)) \to 1_{G_1} & f_{G_1}(i_{G_1}(x), x) \to 1_{G_1} & \multicolumn{2}{l}{i_{G_1}(f_{G_1}(x, y)) \to f_{G_1}(i_{G_1}(y), i_{G_1}(x))} \\
\\
i_{G_2}(1_{G_2}) \to 1_{G_2} & f_{G_2}(x, 1_{G_2}) \to x & f_{G_2}(1_{G_2}, x) \to x & i_{G_2}(i_{G_2}(x)) \to x \\
f_{G_2}(x, i_{G_2}(x)) \to 1_{G_2} & f_{G_2}(i_{G_2}(x), x) \to 1_{G_2} & \multicolumn{2}{l}{i_{G_2}(f_{G_2}(x, y)) \to f_{G_2}(i_{G_2}(y), i_{G_2}(x))}
\end{array}
$$

It is known that termination is not a *modular property* [Ohl94] of rewrite systems, while confluence is a modular property of rewrite systems [Ohl94, Toy87]. It is also known that the disjoint union of two disjoint rewrite systems R_1 and R_2 is terminating if neither R_1 nor

[5] Recall that a single set of group axioms G has the following form in this paper: $G := A \cup \{f(x, 1) \approx x, f(1, x) \approx x, f(x, i(x)) \approx 1, f(i(x), x) \approx 1\}$. Alternatively, there are single axioms for groups [McC93]. In this paper, by a set of group axioms, we mean a set of group axioms having the form of G shown above.

R_2 contains *duplicating rules* [Ohl94, Rus87]. (A rewrite rule $l \to r$ is *duplicating* [Ohl94] if there exists some variable such that it has more occurrences in r than l.) In the above example, the union of $R(G_1)$ and $R(G_2)$ is confluent and terminating on associatively flat terms because $\Sigma_{G_1} \cap \Sigma_{G_2} = \emptyset$ and neither $R(G_1)$ nor $R(G_2)$ contains duplicating rules. In the remainder of this subsection, we denote by $\biguplus_{i=1}^{n} G_i := G_1 \uplus \cdots \uplus G_n$ the union of the sets of group axioms $G_1, \ldots, G_n$ such that $\Sigma_{G_i} \cap \Sigma_{G_j} = \emptyset$ for every $i \neq j$. We denote by $\biguplus_{i=1}^{n} R(G_i) := R(G_1) \uplus \cdots \uplus R(G_n)$ the union of $R(G_1), \ldots, R(G_n)$, where $R(G_k)$, $1 \leq k \leq n$, is the convergent rewrite system for G_k on associatively flat terms. Now, the next lemma follows from the above observation.

Lemma 4.11. *$\biguplus_{i=1}^{n} R(G_i)$ is convergent modulo A.*

Phases I and II for constructing congruence closure modulo $\biguplus_{i=1}^{n} G_i$ are adapted from Phases I and II in Section 3 by taking different interpreted symbols for the multiple disjoint sets of group axioms into account. The rewrite relation $R(G)/A$ in step 2 in Phases I in Section 3 is simply replaced by the rewrite relation $\biguplus_{i=1}^{n} R(G_i)/A$. The output of Phase I is denoted by E', where all equations in E' are constant, D-flat, or A-flat equations.

Next, Phase II is described as follows for $\biguplus_{i=1}^{n} G_i$ and their interpreted symbols $f_{G_l}, i_{G_l}, 1_{G_l}$ for all $1 \leq l \leq n$.

Phase II: Given C and E' obtained from E by Phase I, Copy C to C' and E' to E''. Then, for each set of group axioms G_l, $1 \leq l \leq n$, repeat the following procedure:

- For each constant $c_k \in C'$ and $c_k \neq 1_{G_l}$, repeat the following step:
  If neither $i_{G_l}(c_k) \approx c_i$ nor $i_{G_l}(c_j) \approx c_k$ appears in E'' for some $c_i, c_j \in C'$, then $E' := E' \cup \{i_{G_l}(c_k) \approx c_m\}$ and $C := C \cup \{c_m\}$ for a new constant c_m taken from W.

Next, for each set of group axioms G_l, $1 \leq l \leq n$, repeat the following steps:

- Set $I_{G_l}(E') := \{i_{G_l}(1_{G_l}) \approx 1_{G_l}\} \cup \{i_{G_l}(c_n) \approx c_m \,|\, i_{G_l}(c_m) \approx c_n \in E'\} \cup \{f_{G_l}(c_m, c_n) \approx 1_{G_l} \,|\, i_{G_l}(c_m) \approx c_n \in E'\} \cup \{f_{G_l}(c_n, c_m) \approx 1_{G_l} \,|\, i_{G_l}(c_m) \approx c_n \in E'\}$.
- Set $U_{G_l}(C) := \{f_{G_l}(c, 1_{G_l}) \approx c \,|\, c \in C\} \cup \{f_{G_l}(1_{G_l}, c) \approx c \,|\, c \in C\}$.

Finally, set $S(E) := E' \cup I_{G_1}(E') \cup \cdots \cup I_{G_n}(E') \cup U_{G_1}(C) \cup \cdots \cup U_{G_n}(C)$ and return $S(E)$. Here, $S(E)$ is the output of Phase II. Now, using $S(E)$ obtained from Phase II, one may apply the same Phase III as in Section 3 using $S_0 = S(E)$. The following lemma is a direct extension of Lemma 3.4.

Lemma 4.12. *Viewed as a set of equations, $S(E)$ w.r.t. $\widehat{G} := \biguplus_{i=1}^{n} G_i$ is a conservative extension of E w.r.t. $\widehat{G}$, i.e., $s_0 \approx_E^{\widehat{G}} t_0$ iff $s_0 \approx_{S(E)}^{\widehat{G}} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$.*

Similarly, the following results are adapted from Lemma 3.13, Theorem 3.22 and Corollary 3.25, respectively.

Lemma 4.13. *Let $\widehat{G} := \biguplus_{i=1}^{n} G_i$ and $R(\widehat{G}) := \biguplus_{i=1}^{n} R(G_i)$. If $s_0, t_0 \in T(\Sigma, C_0)$, then $s_0 \approx t_0 \in CC^{\widehat{G}}(E)$ iff $s_0 \approx_{S_\infty(E) \cup gr(R(\widehat{G})) \cup gr(A)} t_0$.*

Proof. First, $CC^{\widehat{G}}(E)$ is the same as $\approx_E^{\widehat{G}}$ by Birkhoff's theorem. Also, by Lemma 4.12, $s_0 \approx_E^{\widehat{G}} t_0$ iff $s_0 \approx_{S(E)}^{\widehat{G}} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$. Then, $s_0 \approx_{S(E)}^{\widehat{G}} t_0$ iff $s_0 \approx_{S(E) \cup gr(R(\widehat{G})) \cup gr(A)} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$.

Let $S_0 = S(E)$. Applying Lemma 3.12 yields that if $S_i \vdash S_{i+1}$, then $\overset{*}{\longleftrightarrow}_{S_i \cup gr(A)}$ and $\overset{*}{\longleftrightarrow}_{S_{i+1} \cup gr(A)}$ on $T(\Sigma, C_0)$ are the same, and thus $\overset{*}{\longleftrightarrow}_{S(E) \cup gr(A)}$ and $\overset{*}{\longleftrightarrow}_{S_\infty(E) \cup gr(A)}$ coincide. Thus, $s_0 \approx_{S(E) \cup gr(R(\widehat{G})) \cup gr(A)} t_0$ iff $s_0 \approx_{S_\infty(E) \cup gr(R(\widehat{G})) \cup gr(A)} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$. □

Lemma 4.14. *Let $\widehat{G} := \biguplus_{i=1}^n G_i$ and $R(\widehat{G}) := \biguplus_{i=1}^n R(G_i)$. If $s_0, t_0 \in T(\Sigma, C_0)$, then $s_0 \approx t_0 \in CC^{\widehat{G}}(E)$ iff s_0 and t_0 have the same normal form w.r.t. $(S_\infty^{\succ}(E) \cup gr(R(\widehat{G})))/A$.*

Proof. Assume that $s_0, t_0 \in T(\Sigma, C_0)$. If $s_0 \approx t_0 \in CC^{\widehat{G}}(E)$, then $s_0 \approx_{S_\infty(E) \cup gr(R(\widehat{G})) \cup gr(A)} t_0$ for all terms $s_0, t_0 \in T(\Sigma, C_0)$ by Lemma 4.13. By Theorem 3.21, we may infer that each $S_\infty^{\succ}(E) \cup gr(R(G_l))$, $1 \le l \le n$, is convergent modulo A. Now by Lemma 4.11 and a simple adaptation of Theorem 3.21, we may also infer that $S_\infty^{\succ}(E) \cup gr(R(\widehat{G}))$ is convergent modulo A, and thus s_0 and t_0 have the same normal form w.r.t. $(S_\infty^{\succ}(E) \cup gr(R(\widehat{G}))/A$.

Conversely, if s_0 and t_0 have the same normal form w.r.t. $(S_\infty^{\succ}(E) \cup gr(R(\widehat{G}))/A$, then we have $s_0 \approx_{S_\infty(E) \cup gr(R(\widehat{G})) \cup gr(A)} t_0$, and thus $s_0 \approx t_0 \in CC^{\widehat{G}}(E)$ by Lemma 4.13. □

Corollary 4.15. *Let $\widehat{G} := \biguplus_{i=1}^n G_i$. Given a finite set of ground equations $E \subseteq T(\Sigma, C_0) \times T(\Sigma, C_0)$, if $S_\infty(E)$ is finite, then we can decide for any $s_0, t_0 \in T(\Sigma, C_0)$ whether $s_0 \approx_E^{\widehat{G}} t_0$ holds or not.*

Example 4.16. Let G_1 and G_2 be the sets of group axioms with $\Sigma_{G_1} = \{f, i_f, 1_f\}$ and $\Sigma_{G_2} = \{g, i_g, 1_g\}$. Consider $E = \{f(a, b) \approx a, f(b, a) \approx b, g(a, b) \approx g(b, a), h(a) \approx b\}$ with $a \succ b \succ 1_f \succ 1_g$ and $h \in \Sigma$. Each equation in E is already a ground fully flat equation, so Phase I is not needed. (Note that equation $g(a, b) \approx g(b, a)$ is an A-flat equation.) After the first step of Phase II for G_1 and G_2, we have:

$E' = \{f(a, b) \approx a, f(b, a) \approx b, g(a, b) \approx g(b, a), h(a) \approx b\} \cup \{i_f(a) \approx c_1, i_f(b) \approx c_2, i_f(1_g) \approx c_3, i_g(a) \approx c_4, i_g(b) \approx c_5, i_g(1_f) \approx c_6\}$ and $C = C_0 \cup C_1$, where $C_0 = \{a, b, 1_f, 1_g\}$ and $C_1 = \{c_1, c_2, c_3, c_4, c_5, c_6\}$.

After the remaining steps of Phase II for G_1 and G_2, we have $I_{G_1}(E') = \{i_f(1_f) \approx 1_f, i_f(c_1) \approx a, i_f(c_2) \approx b, i_f(c_3) \approx 1_g, f(c_1, a) \approx 1_f, f(a, c_1) \approx 1_f, f(c_2, b) \approx 1_f, f(b, c_2) \approx 1_f, f(c_3, 1_g) \approx 1_f, f(1_g, c_3) \approx 1_f\}$ and $I_{G_2}(E') = \{i_g(1_g) \approx 1_g, i_g(c_4) \approx a, i_g(c_5) \approx b, i_g(c_6) \approx 1_f, g(c_4, a) \approx 1_g, g(a, c_4) \approx 1_g, g(c_5, b) \approx 1_g, g(b, c_5) \approx 1_g, g(c_6, 1_f) \approx 1_g, g(1_f, c_6) \approx 1_g\}$.

Also, we have $U_{G_1}(C) = \{f(c, 1_f) \approx c \,|\, c \in C\} \cup \{f(1_f, c) \approx c \,|\, c \in C\}$ and $U_{G_2}(C) = \{g(c, 1_g) \approx c \,|\, c \in C\} \cup \{g(1_g, c) \approx c \,|\, c \in C\}$.

After Phase II, $S(E) := E' \cup I_{G_1}(E') \cup I_{G_2}(E') \cup U_{G_1}(C) \cup U_{G_2}(C)$. Now, the following steps are performed in Phase III using $S_0 = S(E)$.

1: $f(ac_2) \approx f(a1_f)$ (DEDUCE by $f(ab) \approx a$ and $f(bc_2) \approx 1_f$.)
2: $f(ac_2) \approx a$ (SIMPLIFY 1 by $f(a1_f) \approx a$. 1 is deleted.)
3: $f(bc_2) \approx f(ba)$ (DEDUCE 2 by $f(ba) \approx b$.)
4: $f(ba) \approx 1_f$ (SIMPLIFY 3 by $f(bc_2) \approx 1_f$. 3 is deleted.)
5: $b \approx 1_f$ (SIMPLIFY 4 by $f(ba) \approx b$. 4 is deleted.)
6: $f(1_f c_2) \approx 1_f$ (COLLAPSE $f(bc_2) \approx 1_f$ by $b \approx 1_f$. $f(bc_2) \approx 1_f$ is deleted.)
7: $c_2 \approx 1_f$ (SIMPLIFY 6 by $f(1_f c_2) \approx c_2$. 6 is deleted.)
8: $f(1_f a) \approx b$ (COLLAPSE $f(ba) \approx b$ by $b \approx 1_f$. $f(ba) \approx b$ is deleted.)
9: $f(1_f a) \approx 1_f$ (COMPOSE 8 by $b \approx 1_f$. 8 is deleted.)
10: $a \approx 1_f$ (SIMPLIFY 9 by $f(1_f a) \approx a$. 9 is deleted.)

11: $f(1_f c_1) \approx 1_f$ (COLLAPSE $f(ac_1) \approx 1_f$ by $a \approx 1_f$. $f(ac_1) \approx 1_f$ is deleted.)
12: $c_1 \approx 1_f$ (SIMPLIFY 11 by $f(1_f c_1) \approx c_1$. 11 is deleted.)
13: $i_g(1_f) \approx c_4$ (COLLAPSE $i_g(a) \approx c_4$ by $a \approx 1_f$. $i_g(a) \approx c_4$ is deleted.)
14: $i_g(1_f) \approx c_5$ (COLLAPSE $i_g(b) \approx c_5$ by $b \approx 1_f$. $i_g(b) \approx c_5$ is deleted.)
15: $c_4 \approx c_5$ (COLLAPSE 13 by 14. 13 is deleted.)
16: $c_5 \approx c_6$ (COLLAPSE 14 by $i_g(1_f) \approx c_6$. 14 is deleted.)
$\cdots$

After several steps using the contraction rules, we have $S^{\succ}_{\infty}(E) = \{a \to 1_f, b \to 1_f, c_1 \to 1_f, c_2 \to 1_f, h(1_f) \to 1_f, i_f(1_f) \to 1_f, c_4 \to c_6, c_5 \to c_6, i_f(1_g) \to c_3, i_f(c_3) \to 1_g, f(c_3, 1_g) \to 1_f, f(1_g, c_3) \to 1_f, i_g(1_f) \to c_6, i_g(c_6) \to 1_f, i_g(1_g) \to 1_g, g(c_6, 1_f) \to 1_g, g(1_f, c_6) \to 1_g\} \cup \bar{U}^{\succ}(C)$, where $\bar{U}^{\succ}(C) = \{f(1_f, 1_f) \to 1_f, f(1_f, c_3) \to c_3, f(c_3, 1_f) \to c_3, f(1_f, c_6) \to c_6, f(c_6, 1_f) \to c_6, f(1_f, 1_g) \to 1_g, f(1_g, 1_f) \to 1_g\} \cup \{g(1_g, 1_g) \to 1_g, g(1_g, c_3) \to c_3, g(c_3, 1_g) \to c_3, g(1_g, c_6) \to c_6, g(c_6, 1_g) \to c_6, g(1_g, 1_f) \to 1_f, g(1_f, 1_g) \to 1_f\}$. By Lemma 4.14 and Corollary 4.15, we can decide whether $g(f(a, a), h(b)) \approx^{G_1 \uplus G_2}_{E} g(b, f(a, 1_f))$ holds or not. Let $MG := S^{\succ}_{\infty}(E) \cup gr(R(G_1) \uplus R(G_2))$. Then, we see that $g(f(a, a), h(b)) \xrightarrow{*}_{MG/A} g(f(1_f, 1_f), h(1_f)) \xrightarrow{*}_{MG/A} g(1_f, 1_f)$. Also, $g(b, f(a, 1_f)) \to_{MG/A} g(b, a) \xrightarrow{*}_{MG/A} g(1_f, 1_f)$. Now, we conclude that $g(f(a, a), h(b)) \approx^{G_1 \uplus G_2}_{E} g(b, f(a, 1_f))$ holds and $g(f(a, a), h(b)) \approx g(b, f(a, 1_f)) \in CC^{G_1 \uplus G_2}(E)$ by Lemma 4.14.

5. Conclusion

This paper has presented a new framework for computing congruence closure of a finite set of ground equations E over uninterpreted symbols and interpreted symbols for a set of group axioms G, which extends a rewrite-based congruence closure procedure in [Kap97] by taking G into account. In the proposed framework, ground equations in E are flattened into ground flat equations and certain ground flat equations entailed by G are added for a completion procedure. The proposed completion procedure is a ground completion procedure using strings, which adapts a completion procedure for string rewriting systems presenting groups [HEO05, Sim94]. The procedure yields a ground convergent rewrite system for congruence closure modulo G for E. It is simple and generic in the sense that it can also be used for constructing congruence closure w.r.t. the semigroup, monoid, and the multiple disjoint sets of group axioms for E by a slight change of Phase II, but without changing the completion procedure itself. Furthermore, it neither uses extension rules nor complex orderings.

In [Rub95], [Bac91], and [PS81], the authors pointed out that it is natural to view the associativity axiom (with a binary function symbol) as a “structural axiom” rather than viewing it as a “simplifier”. For example, from the given following simple rules $f(f(x, y), z) \to f(x, f(y, z))$, $f(a, b) \to b$, $f(a, f(x, b)) \to f(x, b)$, the standard completion may generate infinite rules $f(a, f(x, f(y, b))) \to f(x, f(y, b)), f(a, f(x, f(y, f(z, b)))) \to f(x, f(y, f(z, b))), \cdots$ [Bac91,Rub95]. Accordingly, this paper is concerned with a completion procedure for the rewrite relation $\to_{R/A}$ on associatively flat ground terms instead of the (plain) rewrite relation $\to_{R \cup A}$. Also, the proposed completion procedure does not use infinitary A-unification explicitly and simply use string matching for ground flat terms during the proposed (ground) completion procedure; note that, for example, $f(a, x)$ and

$f(x,a)$ have an infinite set of (independent) A-unifiers a, $f(a,a)$, $f(a,a,a)$, etc. (See [BS01] and [Rub95].)

Meanwhile, completion modulo A was considered in [Rub95], which is not well suited for constructing congruence closure modulo A. Besides, the approach uses the complex A-compatible reduction ordering and A-unification.

Completion modulo a set of axioms Ax for left-linear rules was considered in [Hue80]. This approach is also not suited for constructing congruence closure modulo G because $R(G)$ has a non-left linear rule, for example, $f(x,i(x)) \to 1$.

In [KKN85], the authors discussed an approach based on computing the Gröbner basis of polynomial ideals for solving word problems for finitely presented commutative algebraic structures including commutative rings with unity. This approach is also not suited for constructing congruence closure modulo G because the commutativity is not assumed in G.

The new results and the main contributions of this paper are the construction of a rewriting-based congruence closure of a finite set of ground equations modulo the semigroup, monoid, group, and the multiple disjoint sets of group axioms, respectively. No nonground equation is added for the above constructions during the proposed completion procedure, and they are all represented by convergent ground rewrite systems modulo associativity. In particular, if the proposed completion procedure terminates for a finite set of ground equations w.r.t. the semigroup, monoid, group, or the multiple disjoint sets of group axioms, then it yields a decision procedure for the word problem for a finite set of ground equations w.r.t. the corresponding axioms. Recall that the word problem for finitely presented semigroups, monoids, and groups are undecidable in general [BO93, HEO05].

The key insights of this paper are as follows. First, the arguments of an associatively flat ground term headed by each associative symbol f are represented by the corresponding string, which is possible by flattening nonflat ground terms occurring in the arguments of f by introducing new constants. Also, certain ground flat equations entailed by the group axioms (or the monoid axioms) are added for the proposed *ground* completion procedure so that one needs neither an A-compatible reduction ordering nor A-unification. This also allows the well-known completion procedure for string rewriting systems and its results (e.g. a monoid presentation of a finite group) to be adapted for the proposed framework of constructing congruence closure of ground equations modulo the semigroup, monoid, group, and the multiple disjoint sets of group axioms, respectively. It is left as a future work to translate the (known) sufficient termination criteria for the completion of string rewriting systems (or *Thue systems*) [KN85b, BO93, Str98] into the termination criteria of constructing congruence closure of ground equations modulo the semigroup, monoid, and the group axioms, respectively.

Since groups are one of the fundamental objects in mathematics, physics, and computer science, developing applications (e.g. integration of SMT solvers with the proposed approaches) using the proposed approaches remains as future research opportunities.

Finally, some of the potential extension of the results discussed in this paper can be the construction of a rewriting-based congruence closure of a finite set of ground equations modulo the following: (i) *involutive* [EM93] semigroups, monoids, and groups, (ii) *idempotent* [SS82] semigroups, monoids, and groups, and (iii) *cancellative* [NÓ89] semigroups, monoids, and groups, and their combinations. Construction of a rewriting-based congruence closure of a finite set of ground equations modulo two sets of group axioms with *homomorphisms* [BO93] can be another potential extension of the results discussed in this paper.

Acknowledgment

The author would like to thank Christina Kirk, Aart Middeldorp, Fabian Mitterwallner, Johannes Niederhauser, Teppei Saito, and Jonas Schöpf (in alphabetical order) for their valuable comments and feedback of this work during the regular TRS reading group meeting of the Computational Logic group at the University of Innsbruck, Austria.

The author also would like to thank the reviewers for their insightful suggestions and comments, which helped to improve this paper.

References

[Bac91] Leo Bachmair. *Canonical Equational Proofs*. Birkhäuser, Boston, 1991. doi:10.1007/978-1-4684-7118-2.

[BK20] Franz Baader and Deepak Kapur. Deciding the Word Problem for Ground Identities with Commutative and Extensional Symbols. In N. Peltier and V. Sofronie-Stokkermans, editors, *Proc. of the 10th Int. Joint Conf. on Automated Reasoning (IJCAR 2020)*, volume 12166 of *Lecture Notes in Computer Science*, pages 163–180. Springer, 2020. doi:10.1007/978-3-030-51074-9_10.

[BK22] Franz Baader and Deepak Kapur. Deciding the Word Problem for Ground and Strongly Shallow Identities w.r.t. Extensional Symbols. *J. Autom. Reason.*, 66(3):301–329, 2022. doi:10.1007/S10817-022-09624-4.

[BN98] Franz Baader and Tobias Nipkow. *Term Rewriting and All That*. Cambridge University Press, Cambridge, UK, 1998. doi:10.1017/CBO9781139172752.

[BO93] Ronald V. Book and Friedrich Otto. *String-Rewriting Systems*. Springer, New York, NY, 1993. doi:10.1007/978-1-4613-9771-7.

[BS01] Franz Baader and Wayne Snyder. Unification Theory. In *Handbook of Automated Reasoning*, Volume I, chapter 8, pages 445 – 532. Elsevier, Amsterdam, 2001. doi:10.1016/B978-044450813-3/50010-2.

[BT18] Clark Barrett and Cesare Tinelli. *Satisfiability Modulo Theories*, pages 305–343. Springer International Publishing, Cham, 2018. doi:10.1007/978-3-319-10575-8_11.

[BTV03] Leo Bachmair, Ashish Tiwari, and Laurent Vigneron. Abstract Congruence Closure. *Journal of Automated Reasoning*, 31(2):129–168, 2003. doi:10.1023/B:JARS.0000009518.26415.49.

[Che84] Philippe Le Chenadec. Canonical Forms in Finitely Presented Algebras. In *Proceedings of the 7th International Conference on Automated Deduction*, page 142–165, Berlin, Heidelberg, 1984. Springer-Verlag. doi:10.1007/978-0-387-34768-4_9.

[CRSS94] David Cyrluk, Sreeranga Rajan, Natarajan Shankar, and Mandayam K. Srivas. Effective theorem proving for hardware verification. In R. Kumar and T. Kropf, editors, *Theorem Provers in Circuit Design (TPCD 94)*, LNCS 901, pages 203–222. Springer, 1994. doi:10.1007/3-540-59047-1_50.

[DMB11] Leonardo De Moura and Nikolaj Bjørner. Satisfiability modulo theories: introduction and applications. *Communications of the ACM*, 54(9):69–77, 2011. doi:10.1145/1995376.1995394.

[DP01] Nachum Dershowitz and David A. Plaisted. Rewriting. In *Handbook of Automated Reasoning*, Volume I, chapter 9, pages 535 – 610. Elsevier, Amsterdam, 2001. doi:10.1016/B978-044450813-3/50011-4.

[DST80] Peter J. Downey, Ravi Sethi, and Robert Endre Tarjan. Variations on the Common Subexpression Problem. *J. ACM*, 27(4):758–771, 1980. doi:10.1145/322217.322228.

[EM93] David Easdown and WD Munn. On semigroups with involution. *Bulletin of the Australian Mathematical Society*, 48(1):93–100, 1993. doi:10.1017/S0004972700015495.

[HEO05] D. F. Holt, B. Eick, and E. A. O'Brien. *Handbook of computational group theory*. CRC Press, Boca Raton, FL, 2005. doi:10.1201/9781420035216.

[Hue80] Gérard P. Huet. Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems. *J. ACM*, 27(4):797–821, 1980. doi:10.1145/322217.322230.

[Hun80] Thomas W. Hungerford. *Algebra*. Springer, New York, NY, 1980. doi:10.1007/978-1-4612-6101-8.

[Kap97] Deepak Kapur. Shostak's Congruence Closure as Completion. In H. Comon, editor, *Proc. of the 8th Int. Conf. on Rewriting Techniques and Applications (RTA 1997)*, volume 1232 of *Lecture Notes in Computer Science*, pages 23–37. Springer, 1997. doi:10.1007/3-540-62950-5_59.

[Kap21] Deepak Kapur. A Modular Associative Commutative (AC) Congruence Closure Algorithm. In N. Kobayashi, editor, *Proc. of 6th International Conference on Formal Structures for Computation and Deduction, FSCD 2021*, volume 195, pages 15:1–15:21. LIPIcs, 2021. doi:10.4230/LIPICS.FSCD.2021.15.

[Kap23] Deepak Kapur. Modularity and Combination of Associative Commutative Congruence Closure Algorithms enriched with Semantic Properties. *Log. Methods Comput. Sci.*, 19(1), 2023. doi:10.46298/LMCS-19(1:19)2023.

[KKN85] Abdelilah Kandri-Rody, Deepak Kapur, and Paliath Narendran. An Ideal-Theoretic Approach to Word Problems and Unification Problems over Finitely Presented Commutative Algebras. In Jean-Pierre Jouannaud, editor, *Rewriting Techniques and Applications, First International Conference, RTA-85, Dijon, France, May 20-22, 1985, Proceedings*, volume 202 of *Lecture Notes in Computer Science*, pages 345–364. Springer, 1985. doi:10.1007/3-540-15976-2_17.

[KL21] Dohan Kim and Christopher Lynch. Congruence Closure Modulo Permutation Equations. In Temur Kutsia, editor, *Proc. of the 9th International Symposium on Symbolic Computation in Software Science, SCSS 2021*, volume 342 of *EPTCS*, pages 86–98, 2021. doi:10.4204/EPTCS.342.8.

[KN85a] Deepak Kapur and Paliath Narendran. A Finite Thue System with Decidable Word Problem and without Equivalent Finite Canonical System. *Theor. Comput. Sci.*, 35:337–344, 1985. doi:10.1016/0304-3975(85)90023-4.

[KN85b] Deepak Kapur and Paliath Narendran. The Knuth-Bendix Completion Procedure and Thue Systems. *SIAM J. Comput.*, 14(4):1052–1072, 1985. doi:10.1137/0214073.

[Koz77] Dexter Kozen. Complexity of Finitely Presented Algebras. In John E. Hopcroft, Emily P. Friedman, and Michael A. Harrison, editors, *Proc. of the 9th Annual ACM Symposium on Theory of Computing, May 4-6, 1977, Boulder, Colorado, USA*, pages 164–177. ACM, 1977. doi:10.1145/800105.803406.

[Mar96] Claude Marché. Normalized Rewriting: an Alternative to Rewriting modulo a Set of Equations. *Journal of Symbolic Computation*, 21(3):253–288, 1996. doi:10.1006/JSCO.1996.0011.

[McC93] William McCune. Single Axioms for Groups and Abelian Groups with Various Operations. *Journal of Automated Reasoning*, 10(1):1–13, 1993. doi:10.1007/BF00881862.

[NO80] Greg Nelson and Derek C. Oppen. Fast Decision Procedures Based on Congruence Closure. *J. ACM*, 27(2):356–364, 1980. doi:10.1145/322186.322198.

[NÓ89] Paliath Narendran and Colm Ó'Dúnlaing. Cancellativity in Finitely Presented Semigroups. *J. Symb. Comput.*, 7(5):457–472, 1989. doi:10.1016/S0747-7171(89)80028-8.

[Ohl94] Enno Ohlebusch. On the Modularity of Termination of Term Rewriting Systems. *Theor. Comput. Sci.*, 136(2):333–360, 1994. doi:10.1016/0304-3975(94)00039-L.

[PS81] Gerald E. Peterson and Mark E. Stickel. Complete Sets of Reductions for Some Equational Theories. *J. ACM*, 28(2):233–264, 1981. doi:10.1145/322248.322251.

[Rub95] Albert Rubio. Theorem Proving modulo Associativity. In Hans Kleine Büning, editor, *Computer Science Logic, 9th International Workshop, CSL '95, Annual Conference of the EACSL, Paderborn, Germany, September 22-29, 1995, Selected Papers*, volume 1092 of *Lecture Notes in Computer Science*, pages 452–467. Springer, 1995. doi:10.1007/3-540-61377-3_53.

[Rus87] Michaël Rusinowitch. On Termination of the Direct Sum of Term-Rewriting Systems. *Inf. Process. Lett.*, 26(2):65–70, 1987. doi:10.1016/0020-0190(87)90039-1.

[Sim94] C. C. Sims. *Computation with finitely presented groups*. Cambridge University Press, New York, NY, 1994. doi:10.1017/CBO9780511574702.

[SS82] Jorg Siekmann and P Szabó. A Noetherian and confluent rewrite system for idempotent semigroups. *Semigroup Forum*, 25(1):83–110, 1982. doi:10.1007/BF02573590.

[Str98] Polina Strogova. Finding a Finite Group Presentation Using Rewriting. In Manuel Bronstein, Volker Weispfenning, and Johannes Grabmeier, editors, *Symbolic Rewriting Techniques*, pages 267–276, Basel, 1998. Birkhäuser Basel. doi:10.1007/978-3-0348-8800-4_13.

[SW15] Vilhelm Sjöberg and Stephanie Weirich. Programming up to Congruence. *SIGPLAN Not.*, 50(1):369–382, 2015. doi:10.1145/2676726.2676974.

[Toy87] Yoshihito Toyama. On the Church-Rosser property for the direct sum of term rewriting systems. *J. ACM*, 34(1):128–143, 1987. doi:10.1145/7531.7534.