An RPO-based ordering modulo permutation equations and its applications to rewrite systems

Dohan Kim and Christopher Lynch

Clarkson University, Potsdam, NY, USA

Abstract

Rewriting modulo equations has been researched for several decades but due to the lack of suitable orderings, there are some limitations to rewriting modulo permutation equations. Given a finite set of permutation equations E, we present a new RPO-based ordering modulo E using (permutation) group actions and their associated orbits. It is an E-compatible reduction ordering on terms with the subterm property and is E-total on ground terms. We also present a completion and ground completion method for rewriting modulo a finite set of permutation equations E using our ordering modulo E. We show that our ground completion modulo E always admits a finite ground convergent (modulo E) rewrite system, which allows us to obtain the decidability of the word problem of ground theories modulo E.

1 Introduction

Equations with permutations of variables occur frequently in mathematics and computer science. An equation is called a *permutation equation* [1] if it is of the form $f(x_1, \ldots, x_n) = f(x_{\rho(1)}, \ldots, x_{\rho(n)})$, where ρ is a permutation on $[n]$ (i.e. the set $\{1, \ldots, n\}$). A suitable ordering modulo permutation equations in the context of term rewriting has not been well-studied, although the modulo approach is natural for term rewriting with permutation equations. (For example, a simple permutation equation, such as $f(x, y) \approx f(y, x)$, cannot be oriented into a rewrite rule by well-founded orderings.) If there existed an E-compatible reduction ordering $\succ_E$ for a set of permutation equations E, then it can be used for the *extended rewrite system* for R modulo E, denoted by R, E [11,20]. (In this paper, an ordering modulo E and an E-compatible ordering are used interchangeably.) In particular, such an ordering $\succ_E$ provides a simple termination criterion for R, E, i.e., R, E is terminating if $l \succ_E r$ for all rules $l \to r \in R$ [11, 20].

The *recursive path ordering* (RPO) [3, 11, 24] is one of the most well-known orderings for term rewriting and equational theorem proving. The main underlying idea of RPO is that, roughly speaking, two terms are first compared by their top symbols and the collections of their immediate subterms are recursively compared. Given a total precedence $\succ_{\mathcal{F}}$ on a finite set of function symbols $\mathcal{F}$,[1] the *recursive path ordering with status* [3, 10, 11, 24, 27] on $T(\mathcal{F}, \mathcal{X})$ is defined in such a way that $s \succ x$ if and only if $s \neq x$ and x is a variable in s, or else $s = f(s_1, \ldots, s_m) \succ g(t_1, \ldots, t_n) = t$ if and only if
(i) $s_i \succeq t$ for some $i \in [m]$, or

[1] In this paper, we assume that a set of function symbols $\mathcal{F}$ in $T(\mathcal{F}, \mathcal{X})$ is finite and each function symbol in $\mathcal{F}$ has a fixed (bounded) arity. We also assume that a precedence $\succ_{\mathcal{F}}$ on $\mathcal{F}$ is total on $\mathcal{F}$.

(ii) $f \succ_{\mathcal{F}} g$ and $s \succ t_i$ for all $i \in [n]$, or
(iii) $f = g \in Lex$ (and hence $m = n$), $<s_1, \ldots, s_m> \succ^{lex} <t_1, \ldots, t_m>$, and $s \succ t_i$ for all $i \in [m]$, or
(iv) $f = g \in Mul$ (and hence $m = n$), and $\{s_1, \ldots, s_m\} \succ^{mul} \{t_1, \ldots, t_m\}$,
where Lex (resp. Mul) denotes the set of function symbols with the lexicographic (resp. multiset) status, and $\succ^{lex}$ (resp. $\succ^{mul}$) denotes the lexicographic (resp. multiset) extension of $\succ$.

In [18, 26–28], RPO is adapted for an AC-compatible (resp. A-compatible) simplification ordering on terms that is AC-total (resp. A-total) on ground terms, where AC (resp. A) denotes the associative and commutative (resp. associativity) theory (cf. [23]). (There is also an RPO-like termination relation for a certain class of equations including associativity (see [8, 9] for details).) An RPO is also briefly described in Section 6.1 of [24] for an ordering modulo some simple permutation equations without providing a formal proof.[2] To our knowledge, an E-compatible simplification ordering on terms that is E-total on ground terms for any finite set of permutation equations E has not been studied in the literature.

Meanwhile, a completion procedure [5, 6, 20, 21] for a rewrite system provides a decision procedure for proving the validity of an equational theorem if the procedure generates a finite convergent rewrite system. A completion procedure was extended to a completion procedure modulo a set of equations E [6, 16, 25] for constructing a rewrite system that admits a unique normal form w.r.t. the congruence induced by E. In particular, ground completion modulo E for a ground rewrite systems R provides a decision procedure for the word problem of ground theories modulo E if it generates a finite convergent (modulo E) rewrite system.

In this paper, we present an RPO-based E-compatible simplification ordering $\succ_E$ on terms that is E-total on ground terms for a finite set of permutation equations E. Then we adapt the existing completion modulo a congruence approach to our completion modulo E procedure using the ordering $\succ_E$. We also present our ground completion modulo E and show that it always admits a finite ground convergent (modulo E) rewrite system for a finite set of permutation equations E.

2 Preliminaries

We assume that the reader has some familiarity with term rewriting [11, 20]. The definitions in this section can be found in [3–5, 11, 24, 27]. (For general references on RPOs, see Section 2.2 in [24], Section 5.4.2 in [3], Section 4 in [11], and [10].) In this paper, we usually denote variables by x, y, z, etc., constants by a, b, c, etc., function symbols by f, g, h, etc., and terms by r, s, t, etc., possibly with subscripts. We denote by $[n]$ the set $\{1, \ldots, n\}$.

We denote by $T(\mathcal{F}, \mathcal{X})$ the set of terms over a finite set of function symbols $\mathcal{F}$ and a denumerable set of variables $\mathcal{X}$. An *equation* is an expression $s \approx t$, where s and t are (first-order) terms built from $\mathcal{F}$ and $\mathcal{X}$. A *ground term* (resp. *ground equation*) is a term (resp. an equation) which does not contain any variable.

We write $s[u]$ if u is a subterm of s and denote by $s[t]_p$ the term that is obtained from s by replacing the subterm at position p of s by t.

An *equivalence* is a reflexive, transitive, and symmetric binary relation. An equivalence $\sim$ on terms is a *congruence* if $s \sim t$ implies $u[s]_p \sim u[t]_p$ for all terms s, t, u and positions p.

An *equational theory* is a set of equations. We denote by $\approx_E$ the least congruence on $T(\mathcal{F}, \mathcal{X})$ that is stable under substitutions and contains a set of equations E. If $s \approx_E t$ for two terms s and t, then s and t are *E-equivalent*.

[2] Our approach uses orbits discussed in the next section, which takes polynomial time for finding them [13]. Without using the group-theoretical approach, the problem of finding the corresponding equivalence classes using permutation equations may take exponential time if one uses traditional equational reasoning approaches [2].

A (strict) ordering $\succ$ on terms is an irreflexive and transitive relation on $T(\mathcal{F}, \mathcal{X})$.

An ordering $\succ$ on terms is *monotonic* if $s \succ t$ implies $u[s] \succ u[t]$ for all s, t, and non-empty contexts u. An ordering $\succ$ on terms is *stable under substitutions* if $s \succ t$ implies $s\sigma \succ t\sigma$ for all s, t, and substitutions σ.

An ordering $\succ$ on terms is a *rewrite ordering* if it is monotonic and stable under substitutions. A well-founded rewrite ordering is a *reduction ordering*.

An ordering $\succ$ on terms has the *subterm property* if $t[s]_p \succ s$ for all s, t, and $p \neq \lambda$. (We denote by λ the top position.) An ordering $\succ$ on terms is a *simplification ordering* if it is a rewrite ordering with the subterm property. (We do not need the *deletion property* [11] for a simplification ordering because we assume that each function symbol has a fixed bounded arity in this paper.)

An ordering $\succ$ on terms is *well-founded* if there is no infinite sequence $t_1 \succ t_2 \succ \cdots$.

An ordering $\succ$ on terms is *E-compatible* if $s' \approx_E s \succ t \approx_E t'$ implies $s' \succ t'$ for all s, s', t and t'. An ordering $\succ$ on ground terms is *E-total* if $s \not\approx_E t$ implies $s \succ t$ or $t \succ s$ for all ground terms s and t.

Given a rewrite system R and a set of equations E, the rewrite relation $\rightarrow_{R,E}$ on $T(\mathcal{F}, \mathcal{X})$ is defined by $s \rightarrow_{R,E} t$ if there is a non-variable position p in s, a rewrite rule $l \rightarrow r \in R$, and a substitution σ such that $s|_p \approx_E l\sigma$ and $t = s[r\sigma]_p$. (In this case, we may also write $s \rightarrow_{R,E}^{l \rightarrow r, \sigma} t$ or simply $s \rightarrow_{R,E}^{l \rightarrow r} t$.) The transitive and reflexive closure of $\rightarrow_{R,E}$ is denoted by $\stackrel{*}{\rightarrow}_{R,E}$. We say that a term t is a *R, E-normal form* if there is no term t' such that $t \rightarrow_{R,E} t'$.

The rewrite relation $\rightarrow_{R/E}$ on $T(\mathcal{F}, \mathcal{X})$ is defined by $s \rightarrow_{R/E} t$ if there are terms u and v such that $s \approx_E u$, $u \rightarrow_R v$, and $v \approx_E t$. We simply say the rewrite relation $\rightarrow_{R/E}$ (resp. $\rightarrow_{R,E}$) on $T(\mathcal{F}, \mathcal{X})$ as the rewrite relation R/E (resp. R, E).

The rewrite relation R, E is *Church-Rosser modulo E* if for all terms s and t with $s \stackrel{*}{\leftrightarrow}_{R \cup E} t$, there are terms u and v such that $s \stackrel{*}{\rightarrow}_{R,E} u \stackrel{*}{\leftrightarrow}_E v \stackrel{*}{\leftarrow}_{R,E} t$. The rewrite relation R, E is *convergent modulo E* if R, E is Church-Rosser modulo E and R/E is well-founded.

The substitution σ is *more general modulo E* on X than the substitution θ, denoted by $\sigma \leq_E^X \theta$, if there exists a substitution τ such that $x\theta \approx_E x\sigma\tau$ for all $x \in X$.

Let s and t be terms, and let V be the set of all variables occurring in s and t. Then s and t are *E-unifiable* if there exists a substitution σ, called an *E-unifier*, such that $s\sigma \approx_E t\sigma$. A set of E-unifiers of s and t is *complete*, denoted by $CSU_E(s, t)$, if for every E-unifier τ of s and t, there exists a substitution $\sigma \in CSU_E(s, t)$ such that $\sigma \leq_E^V \tau$. A complete set of E-unifiers of s and t is *minimal*, denoted by $\mu CSU_E(s, t)$, if for all σ and σ' in $CSU_E(s, t)$, $\sigma \leq_E^V \sigma'$ implies $\sigma = \sigma'$.

The *multiset extension of* $\approx_E$ is defined as the smallest relation $\approx_E^{mul}$ on multisets of terms such that $\emptyset \approx_E^{mul} \emptyset$ and $M \cup \{s\} \approx_E^{mul} M' \cup \{t\}$ if $s \approx_E t \wedge M \approx_E^{mul} M'$.

Let $\succ_e$ be an E-compatible ordering on terms. The *lexicographic extension* of $\succ_e$ w.r.t. $\approx_E$ is the relation $\succ_e^{lex}$ on n-tuples of terms defined by $<s_1, \ldots, s_n> \succ_e^{lex} <t_1, \ldots, t_n>$ if $s_1 \approx_E t_1, \ldots, s_{k-1} \approx_E t_{k-1}$ and $s_k \succ_e t_k$ for some $k \in [n]$. The *multiset extension of* $\succ_e$ w.r.t. $\approx_E$ is defined as the smallest ordering $\succ_e^{mul}$ on multisets of terms such that $M \cup \{s\} \succ_e^{mul} N \cup \{t_1, \ldots, t_n\}$ if $M \approx_E^{mul} N$ and $s \succ_e t_i$ for all $i \in [n]$.

Lemma 1. *Let $\succ_e$ be an E-compatible ordering on terms.*
(i) If $\succ_e$ is transitive, then both $\succ_e^{lex}$ and $\succ_e^{mul}$ are transitive.
(ii) If $M' \approx_E^{mul} M \succ_e^{mul} N \approx_E^{mul} N'$, then $M' \succ_e^{mul} N'$ for all multisets of terms M, M', N and N'.

2.1 Leaf permutative equations and permutation groups

We will mainly use the notations and definitions of leaf permutative equations and permutation groups given in [2,15].

An equation of the form $s \approx s'$ is *leaf permutative* [2] if s and s' are *linear terms* (i.e. no variable occurs twice in s and s') that have the same set of variables and are variants of each other. (Two terms are *variants* if they are instances of each other.) A set of leaf permutative equations $\{s_1 \approx t_1, \ldots, s_n \approx t_n\}$ is *uniform* if for all i and j, s_i and s_j are variants.

If $C[x_1, \ldots, x_n] \approx C[x_{\rho(1)}, \ldots, x_{\rho(n)}]$ is a leaf permutative equation for which all variables are indicated explicitly, then C is the *context* of this equation. We use variable naming in such a way that the left-hand side of each equation in a uniform set of leaf permutative equations has the same name of variables $x_1, \ldots, x_k$ from left to right.

If $e := C[x_1, \ldots, x_n] \approx C[x_{\rho(1)}, \ldots, x_{\rho(n)}]$ is a leaf permutative equation for which all variables are indicated explicitly, then ρ is the permutation of this equation. We denote by $\pi[e]$ the permutation of e. For example, ρ is the permutation of the leaf permutative equation $e' := f(g(x_1, x_2), x_3) \approx f(g(x_1, x_3), x_2)$ (i.e. $\pi[e'] = \rho$) with $\rho(1) = 1, \rho(2) = 3$, and $\rho(3) = 2$.

Let E be a uniform set of leaf permutative equations. Then $\Pi[E]$ is defined as $\Pi[E] := \{\pi[e] \mid e \in E\}$. The permutation group generated by $\Pi[E]$ is denoted by $<\Pi[E]>$.

Theorem 2. *[2, Theorem 1.4] Let E be a set of leaf permutative equations and let e be a leaf permutative equation such that $E \cup \{e\}$ is uniform. Then $E \models e$ if and only if $\pi[e] \in <\Pi[E]>$.*

Example 1. Let $E = \{f(x_1, x_2, x_3, x_4) \approx f(x_2, x_1, x_3, x_4), f(x_1, x_2, x_3, x_4) \approx f(x_2, x_3, x_4, x_1)\}$. Then $\Pi[E]$ consists of two cycles $\{(1\,2), (1\,2\,3\,4)\}$. Since the two cycles $(1\,2)$ and $(1\,2\,3\,4)$ generate the symmetric group S_4, $<\Pi[E]>$ is S_4. Then $f(x_1, \ldots, x_4) \approx_E f(x_{\rho(1)}, \ldots, x_{\rho(4)})$ for any permutation $\rho \in S_4$ by Theorem 2.

Let G be a group with the identity element I. A (left) *action* of G on a set X is a function $G \times X \to X$ such that for all $x \in X$ and all $g_1, g_2 \in G$: (i) $Ix = x$, and (ii) $(g_1 g_2)x = g_1(g_2 x)$. When such an action is given, we say that G *acts* (left) on the set X, and X is a *G-set*.

Let X be a G-set. For $x_i, x_j \in X$, let $x_i \sim x_j$ if and only if there exists some $g \in G$ such that $gx_i = x_j$. Then, $\sim$ is an equivalence relation on X. The equivalence classes on X determined by $\sim$ are *orbits* of G on X.

Example 2. Let $E = \{f(x_1, x_2, x_3, x_4) \approx f(x_2, x_1, x_3, x_4), f(x_1, x_2, x_3, x_4) \approx f(x_1, x_2, x_4, x_3)\}$. Then $\Pi[E]$ consists of two cycles $\{(1\,2), (3\,4)\}$. Let $<\Pi[E]>$ act on the set $X = \{x_1, x_2, x_3, x_4\}$ by $gx_i = x_{g(i)}$ for all $g \in <\Pi[E]>$. Then the orbits of $<\Pi[E]>$ on X are $\{x_1, x_2\}$ and $\{x_3, x_4\}$.

3 An ordering modulo a set of permutation equations

An equation of the form $f(x_1, \ldots, x_n) \approx f(x_{\rho(1)}, \ldots, x_{\rho(n)})$ is a *permutation equation* [1] if ρ is a permutation on $[n]$, which is a restricted form of a leaf permutative equation. In this section, given a set of permutation equations E, we provide an E-compatible simplification ordering on terms that is E-total on ground terms.

Let E be a finite set of permutation equations, where a permutation equation is a restricted form of a leaf permutative equation. Then E can be uniquely decomposed as $\bigcup_{i=1}^{n} E_i$ such that (i) each E_i is a finite set of permutation equations, and (ii) E_j and E_k with $j \neq k$ are disjoint such that if $s_j \approx t_j \in E_j$ and $s_k \approx t_k \in E_k$, then s_j and s_k do not have the same top symbol (and are not variants of each other). Since we assume that each function symbol has a fixed arity, each distinct function symbol occurring in E corresponds to a distinct E_i in E. We

denote by $Eq(f)$ the corresponding equational theory with terms headed by such a function symbol f. We also denote by $\mathcal{F}_E$ the set of all function symbols occurring in E and by Lex the set of all other function symbols in $\mathcal{F}$ in $T(\mathcal{F},\mathcal{X})$ so that $\mathcal{F}$ is split into $\mathcal{F}_E$ and Lex, i.e., $\mathcal{F} = \mathcal{F}_E \cup Lex$. (For comparison, given a total precedence $\succ_{\mathcal{F}}$ on $\mathcal{F}$, if $\mathcal{F}$ is simply $\mathcal{F} = Lex$, then the recursive path ordering $\succ$ (see the *lexicographic path ordering* (LPO) [11]) is total on ground terms, but not necessarily E-compatible on ground terms.)

Given $t = f(s_1,\ldots,s_n)$ with $f(x_1,\ldots,x_n) \approx f(x_{p(1)},\ldots,x_{p(n)}) \in E$ for some permutation p on $[n]$, let $<\Pi[Eq(f)]>$ act on the set $X = \{x_1,\ldots,x_n\}$ by $\rho x_i = x_{\rho(i)}$ for all $\rho \in <\Pi[Eq(f)]>$. We denote each orbit of $<\Pi[Eq(f)]>$ on X by $O_k(f,E)$. (Here X is understood from $f \in \mathcal{F}_E$ and E.) By $Orbit_k(f,t)$ we denote that each x_i in $O_k(f,E)$ is substituted by s_i. (Note that $S = \{s_1,\ldots,s_n\}$ can be a multiset, so we first let $<\Pi[Eq(f)]>$ act on the set $X = \{x_1,\ldots,x_n\}$ instead of a (possibly) multiset $S = \{s_1,\ldots,s_n\}$, and then replace each x_i in $O_k(f,E)$ with s_i in order to obtain $Orbit_k(f,t)$.) The number k in $O_k(f,E)$ is assigned (consecutively starting with 1) in a natural way such that if $k_i < k_j$ for $O_{k_i}(f,E)$ and $O_{k_j}(f,E)$, then $r_i < r_j$ for x_{r_i} and x_{r_j}, where x_{r_i} (resp. x_{r_j}) is the variable with the smallest index in $O_{k_i}(f,E)$ (resp. $O_{k_j}(f,E)$). For example, consider $E = \{f(x_1,x_2,x_3,x_4) \approx f(x_2,x_1,x_3,x_4), f(x_1,x_2,x_3,x_4) \approx f(x_1,x_2,x_4,x_3)\}$ (see Example 2) and $t = f(a,b,c,d)$. Then we have $O_1(f,E) = \{x_1,x_2\}$, $O_2(f,E) = \{x_3,x_4\}$, $Orbit_1(f,t) = \{a,b\}$, and $Orbit_2(f,t) = \{c,d\}$. Note that we only need to compute $O_k(f,E)$ once using $<\Pi[Eq(f)]>$. Then it is easy to obtain $Orbit_k(f,t)$ from $O_k(f,E)$ for any term t headed by $f \in \mathcal{F}_E$. In the following definition, we assume that a total precedence $\succ_{\mathcal{F}}$ on a finite set of function symbols $\mathcal{F}$ is given. We denote by $s \succeq_E t$ either $s \succ_E t$ or $s \approx_E t$.

Definition 3. *Given a finite set of permutation equations E, let $s = f(s_1,\ldots,s_m)$ and $t = g(t_1,\ldots,t_n)$ be terms in $T(\mathcal{F},\mathcal{X})$. Then $s \succ_E x$ if and only if x is a variable in s, or else $s \succ_E t$ if and only if*
(i) $s_i \succeq_E t$ for some $i \in [m]$, or
(ii) $f \succ_{\mathcal{F}} g$ and $s \succ_E t_i$ for all $i \in [n]$, or
(iii) $f = g \in Lex$, $<s_1,\ldots,s_m> \succ_E^{lex} <t_1,\ldots,t_m>$, and $s \succ_E t_i$ for all $i \in [m]$, or
(iv) $f = g \in \mathcal{F}_E$ and there is some positive j such that $Orbit_1(f,s) \approx_E^{mul} Orbit_1(g,t),\ldots,$ $Orbit_{j-1}(f,s) \approx_E^{mul} Orbit_{j-1}(g,t)$, $Orbit_j(f,s) \succ_E^{mul} Orbit_j(g,t)$, and $s \succ_E t_i$ for all $i \in [m]$.

The following lemma directly follows from the definition of $Orbit_j(f,t)$ and $\approx_E$.

Lemma 4. *Given a finite set of permutation equations E, let $s = f(s_1,\ldots,s_n)$ and $t = f(t_1,\ldots,t_n)$ be terms in $T(\mathcal{F},\mathcal{X})$ with $f \in \mathcal{F}_E$. Then $s \approx_E t$ if and only if $Orbit_1(f,s) \approx_E^{mul} Orbit_1(f,t),\ldots,Orbit_k(f,s) \approx_E^{mul} Orbit_k(f,t)$, where k is the number of orbits of $<\Pi[Eq(f)]>$ on $X = \{x_1,\ldots,x_n\}$.*

Example 3. Let $E = \{f(x_1,x_2,x_3,x_4) \approx f(x_2,x_1,x_3,x_4), f(x_1,x_2,x_3,x_4) \approx f(x_2,x_3,x_4,$ $x_1)\}$ (see Example 1) and consider two terms $s = f(d,c,b,g(a))$ and $t = f(a,b,c,d)$ with $f \succ_{\mathcal{F}} g \succ_{\mathcal{F}} a \succ_{\mathcal{F}} b \succ_{\mathcal{F}} c \succ_{\mathcal{F}} d$. Then E is simply decomposed into $E = E_1$. We have $s \succ_E t$ by Case (iv), since $Orbit_1(f,s) = \{d,c,b,g(a)\} \succ_E^{mul} \{a,b,c,d\} = Orbit_1(f,t)$, $s \succ_E a$, $s \succ_E b$, $s \succ_E c$, and $s \succ_E d$. It is easy to verify that $\{d,c,b,g(a)\} \succ_E^{mul} \{a,b,c,d\}$ since $g(a) \succ_E a$ by Case (i). We leave it to the reader to verify that $s \succ_E a$, $s \succ_E b$, $s \succ_E c$, and $s \succ_E d$. (This is clear once we have the subterm property of $\succ_E$ (see Lemma 7).)

Example 4. Let $E = \{f(x_1,x_2,x_3,x_4) \approx f(x_2,x_1,x_3,x_4), f(x_1,x_2,x_3,x_4) \approx f(x_1,x_2,x_4,$ $x_3)\}$ (see Example 2) and consider two terms $s = f(x,a,c,a)$ and $t = f(a,x,b,c)$ with $f \succ_{\mathcal{F}} a \succ_{\mathcal{F}} b \succ_{\mathcal{F}} c$. Then E is simply decomposed into $E = E_1$. We have $s \succ_E t$ by Case (iv), since $Orbit_1(f,s) = \{x,a\} \approx_E^{mul} \{a,x\} = Orbit_1(f,t)$, $Orbit_2(f,s) = \{c,a\} \succ_E^{mul} \{b,c\} =$

$Orbit_2(f,t)$, $s \succ_E a$, $s \succ_E x$, $s \succ_E b$, and $s \succ_E c$. It is easy to verify that $\{c,a\} \succ_E^{mul} \{b,c\}$ since $a \succ_E b$. We leave it to the reader to verify that $s \succ_E a$, $s \succ_E x$, $s \succ_E b$, and $s \succ_E c$.

Example 5. Let $E = \{f(x_1,x_2) \approx f(x_2,x_1), g(x_1,x_2,x_3) \approx g(x_2,x_1,x_3), g(x_1,x_2,x_3) \approx g(x_1,x_3,x_2)\}$ and consider two terms $s = h(f(a,g(b,a,x)),a)$ and $t = h(f(g(a,x,b),a),b)$ with $h \succ_\mathcal{F} f \succ_\mathcal{F} g \succ_\mathcal{F} a \succ_\mathcal{F} b$. Then E is decomposed into $E_1 \cup E_2$, where $E_1 = \{f(x_1,x_2) \approx f(x_2,x_1)\}$ and $E_2 = \{g(x_1,x_2,x_3) \approx g(x_2,x_1,x_3), g(x_1,x_2,x_3) \approx g(x_1,x_3,x_2)\}$. We have $s \succ_E t$ by Case (iii), since $f(a,g(b,a,x)) \approx_E f(g(a,x,b),a)$ by Lemma 4, $a \succ_E b$, $s \succ_E f(g(a,x,b),a)$, and $s \succ_E b$. We may verify that $s \succ_E f(g(a,x,b),a)$ by Case (i) and Lemma 4. We leave it to the reader to verify that $s \succ_E b$.

Example 6. Let $E = \{f(x_1,x_2) \approx f(x_2,x_1), g(x_1,x_2,x_3) \approx g(x_2,x_1,x_3)\}$ and consider two terms $s = f(c,g(b,a,a))$ and $t = f(g(a,b,b),c)$ with $f \succ_\mathcal{F} g \succ_\mathcal{F} a \succ_\mathcal{F} b \succ_\mathcal{F} c$. Then E is decomposed into $E_1 \cup E_2$, where $E_1 = \{f(x_1,x_2) \approx f(x_2,x_1)\}$ and $E_2 = \{g(x_1,x_2,x_3) \approx g(x_2,x_1,x_3)\}$. We have $s \succ_E t$ by Case (iv), since $Orbit_1(f,s) = \{c, g(b,a,a)\} \succ_E^{mul} \{g(a,b,b),c\} = Orbit_1(f,t)$ by $g(b,a,a) \succ_E g(a,b,b)$, $s \succ_E g(a,b,b)$, and $s \succ_E c$. We may verify that $g(b,a,a) \succ_E g(a,b,b)$ by Case (iv), since $Orbit_1(g,g(b,a,a)) = \{b,a\} \approx_E^{mul} \{a,b\} = Orbit_1(g,g(a,b,b))$, $Orbit_2(g,g(b,a,a)) = \{a\} \succ_E^{mul} \{b\} = Orbit_2(g,g(a,b,b))$, $g(b,a,a) \succ_E a$, and $g(b,a,a) \succ_E b$. We leave it to the reader to verify that $s \succ_E g(a,b,b)$, $s \succ_E c$, $g(b,a,a) \succ_E a$, and $g(b,a,a) \succ_E b$.

In the following, we denote by $Vars(t)$ the set of variables occurring in t and by $top(t)$ the top symbol of t.

Lemma 5. *$\succ_E$ is E-compatible.*

Proof. Let s, s', t, and t' be terms with $s' \approx_E s \succ_E t \approx_E t'$. We show that $s' \succ_E t'$. If t is a variable, then $s \neq t$ and $t \in Vars(s)$. We may infer that $t = t'$ and s' is not a variable. Since s' is not a variable with $Vars(s) = Vars(s')$, we have $s' \neq t'$ and $t' \in Vars(s')$, and thus $s' \succ_E t'$. Therefore, we assume that t is not a variable and let $s = f(s_1,\ldots,s_m)$ and $t = g(t_1,\ldots,t_n)$. We proceed by induction on $|s| + |t|$. (Note that we do not need to consider $s' \approx_E s$ (resp. $t \approx_E t'$) on the top position for the following 1 (resp. 2)).

1. If $s \succ_E t$ by Case (i), then we have $s_i \succeq_E t$ for some $i \in [m]$. Then s' is of the form $s' = f(s'_1,\ldots,s'_m)$ with $s_k \approx_E s'_{\rho(k)}$ for all $k \in [m]$ and some (permutation) $\rho \in S_m$. Since $s'_{\rho(i)} \succeq_E t'$ for some $i \in [m]$ by induction hypothesis, we have $s' \succ_E t'$ by Case (i).

2. If $s \succ_E t$ by Case (ii), then we have $f \succ_\mathcal{F} g$ and $s \succ_E t_i$ for all $i \in [n]$. Then t' is of the form $t' = g(t'_1,\ldots,t'_n)$ with $t_k \approx_E t'_{\pi(k)}$ for all $k \in [n]$ and some $\pi \in S_n$. Since $top(s') = f \succ_\mathcal{F} g = top(t')$ and $s' \succ_E t'_{\pi(i)}$ for all $i \in [n]$ by induction hypothesis, we have $s' \succ_E t'$ by Case (ii).

3. If $s \succ_E t$ by Case (iii), then we have $f = g \in Lex$, $<s_1,\ldots,s_m> \succ_E^{lex} <t_1,\ldots,t_m>$, and $s \succ_E t_i$ for all $i \in [m]$. Then s' is of the form $s' = f(s'_1,\ldots,s'_m)$ with $s_k \approx_E s'_k$ for all $k \in [m]$ and t' is of the form $t' = g(t'_1,\ldots,t'_m)$ with $t_k \approx_E t'_k$ for all $k \in [m]$. By induction hypothesis, we have $<s'_1,\ldots,s'_m> \succ_E^{lex} <t'_1,\ldots,t'_m>$ and $s' \succ_E t'_i$ for all $i \in [m]$, and thus we have $s' \succ_E t'$ by Case (iii).

4. If $s \succ_E t$ by Case (iv), then we have $f = g \in \mathcal{F}_E$, and there is some positive j such that $Orbit_1(f,s) \approx_E^{mul} Orbit_1(g,t), \ldots, Orbit_{j-1}(f,s) \approx_E^{mul} Orbit_{j-1}(g,t)$, $Orbit_j(f,s) \succ_E^{mul} Orbit_j(g,t)$, and $s \succ_E t_i$ for all $i \in [m]$. Then s' is of the form $s' = f(s'_1,\ldots,s'_m)$ with $s_k \approx_E s'_{\rho(k)}$ for all $k \in [m]$ and some $\rho \in <\Pi[Eq(f)]>$ and t' is of the form $t' = g(t'_1,\ldots,t'_m)$ with $t_k \approx_E t'_{\pi(k)}$ for all $k \in [m]$ and some $\pi \in <\Pi[Eq(g)]>$. By the definition of $\approx_E^{mul}$, we have $Orbit_k(f,s') \approx_E^{mul} Orbit_k(f,s)$ and $Orbit_k(g,t) \approx_E^{mul} Orbit_k(g,t')$ for all $k \in [j-1]$, which

implies that $Orbit_k(f, s') \approx_E^{mul} Orbit_k(g, t')$ for all $k \in [j-1]$. Furthermore, by induction hypothesis and Lemma 1(ii), we have $Orbit_j(f, s') \succ_E^{mul} Orbit_j(g, t')$ and $s' \succ_E t'_{\pi(i)}$ for all $i \in [m]$, and thus we have $s' \succ_E t'$ by Case (iv). (We may apply Lemma 1(ii) here because the induction hypothesis implies that $\succ_E$ is E-compatible for all terms r and u with $r \succ_E u$ and $|r| + |u| < |s| + |t|$.) □

Lemma 6. *$\succ_E$ is transitive.*

Proof. Suppose that $r \succ_E s$ and $s \succ_E t$. Then r and s cannot be variables by Definition 3. Let $r = f(r_1, \ldots, r_l)$ and $s = g(s_1, \ldots, s_m)$. If t is a variable, then $t \in Vars(s)$. We leave it to the reader to verify that $t \in Vars(r)$ as well, which shows that $r \succ_E t$. Therefore, we assume that t is not a variable and let $t = h(t_1, \ldots, t_n)$. We show that $r \succ_E t$ by induction on $|r| + |s| + |t|$.

1. If $r \succ_E s$ by Case (i), then $r_i \succeq_E s$ for some $i \in [l]$. By induction hypothesis and the E-compatibility of $\succ_E$, we have $r_i \succeq_E t$, and thus $r \succ_E t$ by Case (i).

2. If $s \succ_E t$ by Case (i) and $r \succ_E s$ by Case (ii), (iii), or (iv), then we have $r \succ_E s_i$ for all $i \in [m]$ and $s_j \succeq_E t$ for some $j \in [m]$. It follows that $r \succ_E s_j \succeq_E t$ for some $j \in [m]$, and thus $r \succ_E t$ by induction hypothesis and the E-compatibility of $\succ_E$.

3. If $r \succ_E s$ and $s \succ_E t$ by Case (ii), (iii), or (iv), then $f \succeq_{\mathcal{F}} h$ and $s \succ_E t_i$ for all $i \in [n]$.

3.1. If $f \succ_{\mathcal{F}} h$, then we have $r \succ_E t_i$ for all $i \in [n]$ by induction hypothesis, and thus $r \succ_E t$ by Case (ii).

3.2. If $f = g = h \in Lex$ with $r \succ_E s$ and $s \succ_E t$ by Case (iii), then we have $<r_1, \ldots, r_l> \succ_E^{lex} <t_1, \ldots, t_l>$ and $r \succ_E t_i$ for all $i \in [l]$ by induction hypothesis and Lemma 1(i) (using the E-compatibility of $\succ_E$), and thus $r \succ_E t$ by Case (iii).

3.3. If $f = g = h \in \mathcal{F}_E$ with $r \succ_E s$ and $s \succ_E t$ by Case (iv), then there is some positive j such that $Orbit_1(f, r) \approx_E^{mul} Orbit_1(h, t), \ldots, Orbit_{j-1}(f, r) \approx_E^{mul} Orbit_{j-1}(h, t)$, $Orbit_j(f, r) \succ_E^{mul} Orbit_j(h, t)$, and $r \succ_E t_i$ for all $i \in [l]$ by induction hypothesis and Lemma 1(i) and (ii) (using the E-compatibility of $\succ_E$), and thus $r \succ_E t$ by Case (iv). □

Lemma 7. *$\succ_E$ has the subterm property.*

Proof. By the transitivity of $\succ_E$, it suffices to show that $s = f(\ldots t \ldots) \succ_E t$. If t is a variable, then we have $t \in Vars(s)$, and thus $s \succ_E t$. Therefore, we assume that t is not a variable. Since $t \succeq_E t$, we have $s \succ_E t$ by Case (i). □

Lemma 8. *$\succ_E$ is irreflexive.*

Proof. Suppose, towards a contradiction, that there exists some t such that $t \succ_E t$. If t is a variable, then $t \succ_E t$ is not possible by Definition 3, which is a contradiction. Therefore, we assume that t is not a variable and let $t = f(t_1, \ldots, t_n)$. We proceed by induction on $|t|$.

1. If $t \succ_E t$ by Case (i), then $t_i \succeq_E t$. On the other hand, we have $t \succ_E t_i$ by the subterm property of $\succ_E$. Then by the E-compatibility and transitivity of $\succ_E$, we have $t_i \succ_E t_i$, which is a contradiction by induction hypothesis.

2. If $t \succ_E t$ by Case (iii) or (iv), then there must exist some $i \in [n]$ such that $t_i \succ_E t_i$, which is a contradiction by induction hypothesis. (Note that $t \succ_E t$ by Case (ii) is not possible.) □

Lemma 9. *$\succ_E$ is monotonic.*

Proof. Let $s \succ_E t$. We show that $r = f(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n) \succ_E f(s_1, \ldots, s_{i-1}, t, s_{i+1}, \ldots, s_n) = u$, since the monotonicity of $\succ_E$ directly follows from this replacement property of $\succ_E$. By the subterm property of $\succ_E$, we have $r \succ_E s_j$ for all $j \in \{1, \ldots, i-1, i+1, \ldots, n\}$. By the subterm property and transitivity of $\succ_E$, we also have $r \succ_E t$.

1. If $f \in Lex$, then $r \succ_E u$ by Case (iii) because we have $s_1 \approx_E s_1, \ldots, s_{i-1} \approx_E s_{i-1}$ and

$s \succ_E t$.

2. If $f \in \mathcal{F}_E$, then there is some positive j such that $s \in Orbit_j(f, r)$ and $t \in Orbit_j(f, u)$ and all other $Orbit_k(f, r)$ and $Orbit_k(f, u)$ are the same w.r.t. $\approx_E^{mul}$. Since $Orbit_j(f, r)$ and $Orbit_j(f, u)$ differ by only s and t, we have $Orbit_j(f, r) \succ_E^{mul} Orbit_j(f, u)$ by the definition of $\succ_E^{mul}$, and thus $r \succ_E u$ by Case (iv). □

Lemma 10. *$\succ_E$ is stable under substitutions.*

Proof. Let $s = f(s_1, \ldots, s_m) \succ_E t$. If t is a variable, then $t \in Vars(s)$ and $t\sigma$ is a strict subterm of $s\sigma$ for all substitutions σ. By the subterm property of $\succ_E$, we have $s\sigma \succ_E t\sigma$. Therefore, we assume that t is not a variable and let $t = g(t_1, \ldots, t_n)$. We show that $s\sigma \succ_E t\sigma$ for all substitutions σ by induction on $|s| + |t|$.

1. If $s \succ_E t$ by Case (i), then $s_i \succeq_E t$ for some $i \in [m]$. By induction hypothesis and the stability under substitutions of $\approx_E$, we have $s_i\sigma \succeq_E t\sigma$, and thus $s\sigma \succ_E t\sigma$ by Case (i).

2. If $s \succ_E t$ by Case (ii), then $f \succ_{\mathcal{F}} g$ and $s \succ_E t_i$ for all $i \in [n]$. Since $top(s\sigma) = f \succ_{\mathcal{F}} g = top(t\sigma)$ and $s\sigma \succ_E t_i\sigma$ for all $i \in [n]$ by induction hypothesis, we have $s\sigma \succ_E t\sigma$ by Case (ii).

3. If $s \succ_E t$ by Case (iii), then $f = g \in Lex$, $<s_1, \ldots, s_m> \succ_E^{lex} <t_1, \ldots, t_m>$, and $s \succ_E t_i$ for all $i \in [m]$. Then we have $top(s\sigma) = f = g = top(t\sigma) \in Lex$, $<s_1\sigma, \ldots, s_m\sigma> \succ_E^{lex} <t_1\sigma, \ldots, t_m\sigma>$, and $s\sigma \succ_E t_i\sigma$ for all $i \in [m]$ by induction hypothesis and the stability under substitutions of $\approx_E$. Thus, $s\sigma \succ_E t\sigma$ by Case (iii).

4. If $s \succ_E t$ by Case (iv), then $f = g \in \mathcal{F}_E$, and there is some positive j such that $Orbit_1(f, s) \approx_E^{mul} Orbit_1(g, t), \ldots, Orbit_{j-1}(f, s) \approx_E^{mul} Orbit_{j-1}(g, t)$, $Orbit_j(f, s) \succ_E^{mul} Orbit_j(g, t)$, and $s \succ_E t_i$ for all $i \in [m]$. Then we have $top(s\sigma) = f = g = top(t\sigma) \in \mathcal{F}_E$ and there is some positive j such that $Orbit_1(f, s\sigma) \approx_E^{mul} Orbit_1(g, t\sigma), \ldots, Orbit_{j-1}(f, s\sigma) \approx_E^{mul} Orbit_{j-1}(g, t\sigma)$, $Orbit_j(f, s\sigma) \succ_E^{mul} Orbit_j(g, t\sigma)$, and $s\sigma \succ_E t_i\sigma$ for all $i \in [m]$ by induction hypothesis and the stability under substitutions of $\approx_E$. Thus, $s\sigma \succ_E t\sigma$ by Case (iv). □

Lemma 11. *$\succ_E$ is E-total on ground terms.*

Proof. Let s and t be ground terms such that $s = f(s_1, \ldots, s_m)$ and $t = g(t_1, \ldots, t_n)$. We show that either $s \succ_E t$ or $t \succ_E s$ or $s \approx_E t$ by induction on $|s| + |t|$. In the following, for all s' and t' with $|s'| + |t'| < |s| + |t|$, we have either $s' \succ_E t'$ or $t' \succ_E s'$ or $s' \approx_E t'$ by induction hypothesis.

1. If $s_i \succeq_E t$ for some $i \in [m]$, then $s \succ_E t$ by Case (i).

2. Otherwise, if $t \succ_E s_i$ for all $i \in [m]$, then we consider the following subcases:

2.1. If $t_i \succeq_E s$ for some $i \in [n]$, then $t \succ_E s$ by Case (i).

2.2. Otherwise, if $s \succ_E t_i$ for all $i \in [n]$, then we consider the following subcases:

2.2.1 If $f \succ_{\mathcal{F}} g$, then $s \succ_E t$ by Case (ii).

2.2.2 If $g \succ_{\mathcal{F}} f$, then $t \succ_E s$ by Case (ii).

2.2.3. If $f = g$ (and hence $m = n$), then we consider the following subcases:

2.2.3.1. If $s_k \approx_E t_k$ for all $k \in [m]$, then $s \approx_E t$.

2.2.3.2. If $f = g \in Lex$ and $s_1 \approx_E t_1, \ldots, s_{j-1} \approx_E t_{j-1}$, and $s_j \succ_E t_j$ (resp. $t_j \succ_E s_j$) for some $j \in [m]$, then $s \succ_E t$ (resp. $t \succ_E s$) by Case (iii).

2.2.3.3. If $f = g \in \mathcal{F}_E$ and $Orbit_1(f, s) \approx_E^{mul} Orbit_1(g, t), \ldots, Orbit_{j-1}(f, s) \approx_E^{mul} Orbit_{j-1}(g, t)$, and $Orbit_j(f, s) \succ_E^{mul} Orbit_j(g, t)$ (resp. $Orbit_j(g, t) \succ_E^{mul} Orbit_j(f, s)$) for some positive j, then $s \succ_E t$ (resp. $t \succ_E s$) by Case (iv).

2.2.3.4. If $f = g \in \mathcal{F}_E$ and $Orbit_1(f, s) \approx_E^{mul} Orbit_1(g, t), \ldots, Orbit_k(f, s) \approx_E^{mul} Orbit_k(g, t)$, where k is the number of orbits of $<\Pi[Eq(f)]>$ on $X = \{x_1, \ldots, x_m\}$, then $s \approx_E t$.

Thus, we have either $s \succ_E t$ or $t \succ_E s$ or $s \approx_E t$ for each of the above cases by induction hypothesis. □

Lemmas 5–11 now amount to the following theorem.

Theorem 12. *Let E be a finite set of permutation equations. Then $\succ_E$ is an E-compatible simplification ordering on terms and is E-total on ground terms.*

Since every simplification ordering on terms (i.e. $T(\mathcal{F}, \mathcal{X})$) is a reduction ordering [3,24], we have the following corollary from Theorem 12. (Recall that $\mathcal{F}$ is finite in this paper.)

Corollary 13. *Let E be a finite set of permutation equations. Then $\succ_E$ is an E-compatible reduction ordering on terms with the subterm property and is E-total on ground terms.*

Given a total precedence $\succ_{\mathcal{F}}$ on a finite set of function symbols $\mathcal{F}$ and two terms s and t, one can determine whether $s \succ_{rpo} t$ in time $O(n^2)$ (measured in $n = |s|+|t|$) using the dynamic programming approach [30,31], where $\succ_{rpo}$ is the recursive path ordering with status. Given a finite set of permutation equations E and two terms s and t, one can also determine whether $s \approx_E t$ in time $O(n^2)$ (measured in $n = |s|+|t|$) using an additional table that can be constructed in polynomial time [1]. In the following theorem, we assume that this additional table and the orbits $O_k(f, E)$ for each $f \in \mathcal{F}_E$ are given for a (fixed) finite set of permutation equations E. Note that $O_k(f, E)$ can be computed only once in polynomial time [13] for each $f \in \mathcal{F}_E$. Once we have the orbits $O_k(f, E)$, it is easy to see that every $Orbit_k(f, t)$ can be immediately obtained for any term t headed by $f \in \mathcal{F}_E$. For the proof of the following theorem, we use the dynamic programming-like technique found in Section 5 of [17]. Recall that our ordering $\succ_E$ assumes a total precedence $\succ_{\mathcal{F}}$ on a finite set of function symbols $\mathcal{F}$.

Theorem 14. *Given a finite set of permutation equations E, we can determine whether $s \succ_E t$ for two terms s and t in time $O(n^4)$ (measured in $n = |s| + |t|$).*

Proof. We construct a 2-dimensional array A of size $|s| \cdot |t|$ using a bottom-up approach. First, we assume that all subterms of s have already been compared to all subterms of t with the exception of s and t themselves. We also assume that the results are stored and easily accessible in A in such a way that if s_i is a subterm of s at position p and t_j is a subterm of t at position q with $p \neq \lambda$ or $q \neq \lambda$, then $A[p, q]$ indicates whether $s_i \approx_E t_j$, $s_i \succ_E t_j$, $t_j \succ_E s_i$, or s_i and t_j are incomparable.

Now we show that the time required to compare s and t, denoted by $TCOMP(s, t)$, takes $O(n^2)$ time using the above assumptions. We first test whether $s \approx_E t$ in $O(n^2)$ time. If $s \not\approx_E t$, then we proceed by case analysis in Definition 3. The straightforward comparisons of all s_i with t for Case (i), and s with all t_i for Case (ii) in the worst case using the existing entries of A takes $O(n)$ time. Similarly, it takes $O(n)$ time to compare s and t for Case (iii) using the existing entries of A. For Case (iv), since we already have the orbits $O_k(f, E)$, it takes at most $O(n)$ time to find every $Orbit_k(f, s)$ (and $Orbit_k(g, t)$ too). Then all s_i are compared to all t_j in the worst case using the existing entries of A, which takes $O(n^2)$ time. This shows that $TCOMP(s, t)$ takes $O(n^2)$ time.

Finally, it remains to sum up all possible $TCOMP(s_i, t_j)$ in a bottom-up way, where s_i is a subterm of s and t_j is a subterm of t. Since the number of subterms of s (resp. t) is bounded above by $O(|s|)$ (resp. $O(|t|)$), we have $\sum TCOMP(s_i, t_j) = O(|s| \cdot |t| \cdot TCOMP(s, t))$, where $TCOMP(s, t)$ takes $O(n^2)$ time. Thus, $s \succ_E t$ can be determined in time $O(n^4)$. □

4 Completion modulo a set of permutation equations

Knuth-Bendix completion [21] (or simply *completion*) is a technique using equations as rewrite rules and is used for solving the word problem for a finite set of equations. It is often parameterized by a reduction ordering to ensure that the resulting rewrite system terminates. If the

procedure succeeds, then it yields a convergent rewrite system, which allows one to solve the word problem for a given finite set of equations. If the procedure encounters an unorientable equation w.r.t. a given reduction ordering, then it fails, i.e., the procedure cannot be continued.

A permutation equation (e.g. a commutativity equation) often cannot be oriented into a rewrite rule without losing the termination property, which causes the failure of the completion procedure. Therefore, it is natural to view permutation equations as *structural axioms* [5] (defining a congruence on terms) instead of viewing them as *simplifiers* (defining a terminating rewrite relation on terms). In this situation, we need to consider completion modulo E for a finite set of permutation equations E in order to construct a convergent (modulo E) rewrite system R, where normal forms w.r.t. R are unique up to the congruence induced by E. Here we are mainly concerned with the rewrite relation R, E instead of R/E because R/E tends to be less efficient than R, E [5]. We give an adapted version of completion modulo E in [5, 6, 20] for a finite set of permutation equations E using R, E in this section. We first give the necessary definitions used in completion modulo E. In the following, we denote by $\mathcal{FP}os(t)$ the set of non-variable positions of t.

Definition 15. [5, 20] Let R be a rewrite system and E be a finite set of equations.
1. A proof for $t \approx t'$ is a *rewrite proof modulo* E for R if for some t_1 and t'_1, there is a proof of the form $t \stackrel{*}{\rightarrow}_{R,E} t_1 \stackrel{*}{\leftrightarrow}_E t'_1 \stackrel{*}{\leftarrow}_{R,E} t'$.
2. A *peak* is a proof of the form $t_1 \leftarrow_R t \rightarrow_{R,E} t_2$ and a *cliff* is a proof of the form $t_1 \leftrightarrow_E t \rightarrow_{R,E} t_2$ or $t_1 \rightarrow_{R,E} t \leftrightarrow_E t_2$.
3. Given two rules $s \rightarrow t$ and $l \rightarrow r$ such that $Vars(s) \cap Vars(l) = \emptyset$ and $s|_p$ and l are E-unifiable at position p of $\mathcal{FP}os(s)$ with a minimal complete set of E-unifiers Ψ, the set $\{u \approx v \,|\, u = s[r]_p\sigma, v = t\sigma, \sigma \in \Psi\}$ is called a *set of E-critical pairs* of the rule $l \rightarrow r$ on $s \rightarrow t$ at position p of $\mathcal{FP}os(s)$.
4. The set of E-critical pairs between the rules in a rewrite system R is denoted by $CP_E(R)$. The set of E-critical pairs of the rules in R on the equations in E is denoted by $CP_E(R, E)$, where an equation $s \approx t \in E$ is considered as a rule $s \rightarrow t$ or $t \rightarrow s$.

If R, E is Church-Rosser modulo E, then every peak or cliff (see Definition 15) can be replaced by a rewrite proof modulo E, where a proof is a rewrite proof modulo E if and only if it contains no peak or cliff [5,6]. (Note that non-overlap peaks (resp. cliffs) and variable overlap peaks (resp. cliffs) can always be replaced by rewrite proofs modulo E (see [5,6]).) Conversely, if R, E is not Church-Rosser modulo E and R/E is terminating, then there is some peak or cliff which cannot be replaced by a rewrite proof modulo E [5,6]. In completion modulo E (or *extended completion* [5,6]), $CP_E(R)$ is used to eliminate peaks that are proper overlaps, while either $CP_E(R, E)$ or $EXT_E(R)$ in the following definition is used to eliminate cliffs that are proper overlaps (see [5, 20]). We denote by $\overrightarrow{E}$ the set $\{s \rightarrow t, t \rightarrow s \,|\, s \approx t \in E\}$.

Definition 16. [5, 16] Let $l \rightarrow r \in R$ and $u \rightarrow v \in \overrightarrow{E}$ with $Vars(l) \cap Vars(u) = \emptyset$, such that some proper non-variable subterm $u|_p$ of u is E-unifiable with l. Then $u[l]_p \rightarrow u[r]_p$ is the *extended rule* of $l \rightarrow r$ w.r.t. E. The set of all extended rules in R w.r.t. E is denoted by $EXT_E(R)$.

Observe that if E is a set of permutation equations, then $EXT_E(R)$ is the empty set for any rewrite system R because every proper subterm $u|_p$ of u in Definition 16 is a variable. Therefore, extended completion in [5, 6] can be easily adapted for completion modulo a finite set of permutation equations E without taking $EXT_E(R)$ into account. Note that we do not need to compute $CP_E(R, E)$ either because cliffs that are proper overlaps do not occur with E, which is also the reason why $EXT_E(R)$ is empty.

The *proper encompassment ordering modulo* E [20] is defined in such a way that $l \sqsupset_E g$

ORIENT:	$\dfrac{P \cup \{p \approx q\}; R}{P; R \cup \{p \to q\}}$	if $p \succ_E q$.
DEDUCE:	$\dfrac{P; R}{P \cup \{p \approx q\}; R}$	if $p \approx q \in CP_E(R)$.
SIMPLIFY:	$\dfrac{P \cup \{p \approx q\}; R}{P \cup \{p' \approx q\}; R}$	if $p \to_{R,E} p'$.
DELETE:	$\dfrac{P \cup \{p \approx q\}; R}{P; R}$	if $p \overset{*}{\leftrightarrow}_E q$.
COMPOSE:	$\dfrac{P; R \cup \{l \to r\}}{P; R \cup \{l \to r'\}}$	if $r \to_{R,E} r'$.
COLLAPSE:	$\dfrac{P; R \cup \{l \to r\}}{P \cup \{l' \approx r\}; R}$	if $l \to^{g \to d, \sigma}_{R,E} l'$ for $g \to d \in R$ and $l \to r >>_E g \to d$.

Above, $\succ_E$ is our E-compatible reduction ordering on terms and $\sqsupset_E$ denotes a proper encompassment ordering modulo E, where E is a finite set of permutation equations.

Figure 1. Completion modulo a finite set of permutation equations E

if there is some substitution σ such that $l|_p \overset{*}{\leftrightarrow}_E g\sigma$ with $p \neq \lambda$, or $l \approx_E g\sigma$ and σ is not a renaming. In Figure 1, $>>_E$ is defined as follows: $l \to r >>_E g \to d$ if $l \sqsupset_E g$ or l and g are subsumption equivalent (w.r.t. $\approx_E$) and $r \succ_E d$ (see Section 18.3 and 18.4 in [20]).

In the remainder of this section, we denote by P a set of equations, R a set of rewrite rules, E a finite set of permutation equations, and by $\succ_E$ our E-compatible simplification ordering on terms. Now we write $P; R \vdash P'; R'$ to indicate that $P'; R'$ can be obtained from $P; R$ by application of an inference rule in Figure 1. A *derivation* is a sequence of states $P_0; R_0 \vdash P_1; R_1 \vdash \cdots$. Let $P_0; R_0 \vdash P_1; R_1 \vdash \cdots$ be a derivation. Then P_∞ denotes *the set of persisting equations* $\bigcup_i \bigcap_{j \geq i} P_j$. Similarly, R_∞ denotes *the set of persisting rules* $\bigcup_i \bigcap_{j \geq i} R_j$. A derivation is said to be *fair* [7] if any transition rule that is (continuously) enabled is applied eventually. If a derivation $P_0; R_0 \vdash P_1; R_1 \vdash \cdots$ is fair and $P_\infty = \emptyset$ (i.e. *non-failing*), then $CP_E(R_\infty)$ is a subset of $\bigcup_k P_k$ [5]. Since a finite permutation theory E has a finite complete unification algorithm [1], and $\succ_E$ is E-compatible with the subterm property, the following theorem is a direct adaptation of Theorem 18.4 in [20] and Theorem 3.21 in [5].

Theorem 17. *Let $P_0; R_0 \vdash P_1; R_1 \vdash \cdots$ be a fair derivation such that P_0 is a finite set of equations with $R_0 = \emptyset$, and $P_\infty = \emptyset$. Then R_∞, E is convergent modulo E.*

ORIENT: $\dfrac{P \cup \{p \approx q\}; R}{P; R \cup \{p \to q\}}$ if $p \succ_E q$.

SIMPLIFY: $\dfrac{P \cup \{p \approx q\}; R}{P \cup \{p' \approx q\}; R}$ if $p \to_{R,E} p'$.

DELETE: $\dfrac{P \cup \{p \approx q\}; R}{P; R}$ if $p \overset{*}{\leftrightarrow}_E q$.

COMPOSE: $\dfrac{P; R \cup \{l \to r\}}{P; R \cup \{l \to r'\}}$ if $r \to_{R,E} r'$.

COLLAPSE: $\dfrac{P; R \cup \{l \to r\}}{P \cup \{l' \approx r\}; R}$ if $l \to^{g \to d}_{R,E} l'$ for $g \to d \in R$, and if $l \overset{*}{\leftrightarrow}_E g$, then $r \succ_E d$.

Above, $\succ_E$ is our E-compatible total reduction ordering on ground terms with the subterm property for a finite set of permutation equations E.

Figure 2. Ground completion modulo a finite set of permutation equations E

5 Ground completion modulo a set of permutation equations

It is known that the word problem of ground theories[3] modulo E is decidable by using ground completion modulo E for $E = AC$, $AC \cup U$ (unit), $AC \cup I$ (idempotent), AG (abelian group theory), and undecidable for $E = A$ (associativity), $AC \cup D$ (distributivity), and G (group theory) (see [22] for details). We show that our ground completion modulo a finite set of permutation equations E always admits a finite ground convergent (modulo E) rewrite system, allowing us to provide a decision procedure for the word problem of ground theories modulo E. In this section, we denote by P a set of ground equations, R a set of ground rewrite rules, E a finite set of permutation equations, and by $\succ_E$ our E-compatible simplification ordering on terms that is E-total on ground terms.

Note that the DEDUCE inference rule in Figure 1 is no longer needed for our ground completion modulo E in Figure 2 because the inference steps by DEDUCE can be replaced by other simplification inference steps, especially by COLLAPSE in Figure 2. Furthermore, an encompassment ordering modulo E in Figure 1 is also no longer needed for the COLLAPSE inference rule in Figure 2 for the ground case. We write $P; R \vdash P'; R'$ to indicate that $P'; R'$ can be obtained from $P; R$ by application of an inference rule in Figure 2.

Lemma 18. *If $P; R \vdash P'; R'$, then the congruence relations $\overset{*}{\leftrightarrow}_{E \cup P \cup R}$ and $\overset{*}{\leftrightarrow}_{E \cup P' \cup R'}$ on $T(\mathcal{F})$ are the same.*

Proof. We consider each application of an inference rule τ for $P; R \vdash P'; R'$. If τ is ORIENT, SIMPLIFY, DELETE, or COMPOSE, then the conclusion can be easily verified. If τ is COLLAPSE, then let $R = R'' \cup \{l \to r\}$, $P' = P \cup \{l' \approx r\}$, and $R' = R''$. Since

[3]By a ground theory, we mean an equational theory defined by a *finite* set of ground equations throughout this paper.

$(P \cup R) - (P' \cup R') = \{l \to r\}$, we need to show that $l \overset{*}{\leftrightarrow}_{E \cup P' \cup R'} r$. As $l \overset{*}{\leftrightarrow}_E \hat{l} \to^{g \to d}_{R'} l' \leftrightarrow_{P'} r$ for some $g \to d \in R''$, we have $l \overset{*}{\leftrightarrow}_{E \cup P' \cup R'} r$. Conversely, since $(P' \cup R') - (P \cup R) = \{l' \approx r\}$, we also need to show that $l' \overset{*}{\leftrightarrow}_{E \cup P \cup R} r$. As $l' \leftarrow^{g \to d}_{R} \hat{l} \overset{*}{\leftrightarrow}_E l \to_R r$ for some $g \to d \in R''$, we have $l' \overset{*}{\leftrightarrow}_{E \cup P \cup R} r$. Thus, the conclusion follows. □

Definition 19. Let $s = s[u\sigma] \leftrightarrow s[v\sigma] = t$ be a proof step with the equation (or rule) $u \approx v \in E \cup P \cup R$. The *complexity* of this proof step is defined as follows:

(i) $(\{s\}, \bot, t)$ if $u \approx v \in E$
(ii) $(\{s, t\}, \bot, \bot)$ if $u \approx v \in P$
(iii) $(\{s\}, u, t)$ if $u \to v \in R$
(iv) $(\{t\}, v, s)$ if $v \to u \in R$

Complexities of proof steps are lexicographically compared by $\succ_E^{mul}$ in the first component, and $\succ_E$ in the second and the third component, where $\bot$ is a new constant symbol and is assumed to be minimal (w.r.t. $\succ_E$). The *complexity of a proof* is the multiset of the complexities of its proof steps [5, 7]. The ordering on proofs, denoted by $\succ_{\mathcal{C}}$, is the multiset extension of the ordering on the complexities of proof steps. Since the multiset/lexicographic extension of a well-founded ordering is still well-founded and $\succ_E$ is well-founded, we may infer that $\succ_{\mathcal{C}}$ is well-founded. By a *ground proof* in $E \cup P \cup R$ of an equation $s \approx t$ with $s, t \in T(\mathcal{F})$, we mean a sequence of proof steps such that $t_0 = s, t_n = t$ and for all $t_i \in T(\mathcal{F})$, $0 < i \leq n$, one of $t_{i-1} \leftrightarrow_E t_i$, $t_{i-1} \leftrightarrow_P t_i$, $t_{i-1} \to_R t_i$, $t_{i-1} \leftarrow_R t_i$ holds.

Lemma 20. *If $P; R \vdash P'; R'$, then for any ground proof ρ in $E \cup P \cup R$ of an equation $s \approx t$, there is a ground proof ρ' in $E \cup P' \cup R'$ of the equation $s \approx t$ such that $\rho \succeq_{\mathcal{C}} \rho'$.*

Proof. We show that each equation in $(P \cup R) - (P' \cup R')$ has a smaller proof (w.r.t. $\succ_{\mathcal{C}}$) in $E \cup P' \cup R'$ by considering each case for $P; R \vdash P'; R'$.

(i) ORIENT: The proof $p \leftrightarrow_P q$ is transformed to the proof $p \to_{R'} q$. Since $\{(\{p, q\}, \bot, \bot)\} \succ_{\mathcal{C}} \{(\{p\}, p, q)\}$, the newer proof $p \to_{R'} q$ is smaller (w.r.t. $\succ_{\mathcal{C}}$) than the proof $p \leftrightarrow_P q$.

(ii) SIMPLIFY: The proof $p \leftrightarrow_P q$ is transformed to the proof $p \overset{*}{\leftrightarrow}_E \hat{p} \to_{R'} p' \leftrightarrow_{P'} q$. The newer proof is smaller (w.r.t. $\succ_{\mathcal{C}}$) because $p \leftrightarrow_P q$ with the complexity $\{(\{p, q\}, \bot, \bot)\}$ is bigger (w.r.t. $\succ_{\mathcal{C}}$) than all proof steps in $p \overset{*}{\leftrightarrow}_E \hat{p}$, $\hat{p} \to_{R'} p'$ and $p' \leftrightarrow_{P'} q$ in the first component.

(iii) DELETE: The proof $p \leftrightarrow_P q$ is transformed to the proof $p \overset{*}{\leftrightarrow}_E q$. The proof $p \leftrightarrow_P q$ with the complexity $\{(\{p, q\}, \bot, \bot)\}$ is bigger (w.r.t. $\succ_{\mathcal{C}}$) than all proof steps in $p \overset{*}{\leftrightarrow}_E q$ in the first component.

(iv) COMPOSE: The proof $l \to_R r$ is transformed to the proof $l \to_{R'} r' \leftarrow_{R'} \hat{r} \overset{*}{\leftrightarrow}_E r$. The newer proof is smaller (w.r.t. $\succ_{\mathcal{C}}$) because $l \to_R r$ with the complexity $\{(\{l\}, l, r)\}$ is bigger (w.r.t. $\succ_{\mathcal{C}}$) than (a) the proof step in $l \to_{R'} r'$ in the third component, (b) the proof step $r' \leftarrow_{R'} \hat{r}$ in the first component, and (c) all proof steps in $\hat{r} \overset{*}{\leftrightarrow}_E r$ in the first component.

(v) COLLAPSE: The proof $l \to_R r$ is transformed to the proof $l \overset{*}{\leftrightarrow}_E \hat{l} \to^{g \to d}_{R'} l' \leftrightarrow_{P'} r$ for some $g \to d \in R'$. The newer proof is smaller (w.r.t. $\succ_{\mathcal{C}}$) because $l \to_R r$ with the complexity $\{(\{l\}, l, r)\}$ is bigger (w.r.t. $\succ_{\mathcal{C}}$) than (a) all proof steps in $l \overset{*}{\leftrightarrow}_E \hat{l}$ in the second component, (b) the proof step $\hat{l} \to^{g \to d}_{R'} l'$ in the second (resp. third) component if $l \not\overset{*}{\leftrightarrow}_E g$ (resp. $l \overset{*}{\leftrightarrow}_E g$), and (c) the proof step $l' \leftrightarrow_{P'} r$ in the first component. □

Note that if $P_0; R_0 \vdash P_1; R_1 \vdash \cdots$ is a fair derivation, then $P_\infty = \emptyset$ (i.e. non-failing) because $\succ_E$ is E-total on ground terms.

Theorem 21. *Let $P_0; R_0 \vdash P_1; R_1 \vdash \cdots$ be a fair derivation such that P_0 is a finite set of ground equations with $R_0 = \emptyset$. Then the set of persisting rules R_∞ is finite and R_∞, E is ground convergent modulo E.*

Proof. Suppose that $P_0; R_0 \vdash P_1; R_1 \vdash \cdots$ is a fair derivation such that P_0 is a finite set of ground equations with $R_0 = \emptyset$. We first define a simple measure of a state $P_k; R_k$ as the multiset $\{\{\{s,t\}\} \mid s \approx t \in P_k\} \cup \{\{\{s\},\{t\}\} \mid s \to t \in R_k\}$ (cf. [7]). Two states are compared by these measures using the threefold multiset extension of $\succ_E$. It is easy to see that any application of an inference rule for a transition $P_k; R_k \vdash P_{k+1}; R_{k+1}$ reduces this measure. Since the multiset extension of a well-founded ordering is still well-founded and $\succ_E$ is well-founded, we may infer that any fair derivation starting from $P_0; R_0$ is finite. Therefore, R_∞ is finite with $P_\infty = \emptyset$. Since $l \succ_E r$ for all rules $l \to r \in R_\infty$, R_∞/E is also terminating.

Now it remains to show that R_∞, E is ground Church-Rosser modulo E. We show that all minimal (w.r.t. $\succ_{\mathcal{C}}$) proofs in $E \cup R_\infty$ are rewrite proofs modulo E.

Suppose that a proof is a minimal proof but not a rewrite proof modulo E. Then it should contain either a peak (or a cliff) that is a proper overlap (cf. [5]). (Note that every peak or cliff that is a non-overlap or a variable overlap can be replaced by a rewrite proof modulo E (see pp. 47–50 in [5]), which is smaller (w.r.t. $\succ_{\mathcal{C}}$) than the original peak or cliff, so this is not the case.)

Now consider such a peak $t_1 \leftarrow_{R_\infty} t \rightarrow_{R_\infty,E} t_2$ that is a proper overlap. (Since $EXT_E(R)$ is empty, we do not need to consider a cliff that is a proper overlap.) By the *Extended Critical Pair Lemma* [6, 16], it can be replaced by a proof $t_1 \overset{*}{\leftrightarrow}_E t' \leftrightarrow_{CP_E(R_\infty)} t'' \overset{*}{\leftrightarrow}_E t_2$. Since $CP_E(R_\infty) \subseteq \bigcup_k P_k$ by fairness of the derivation, there is a ground proof $t_1 \overset{*}{\leftrightarrow}_E t' \leftrightarrow_{P_k} t'' \overset{*}{\leftrightarrow}_E t_2$ for some k. We name this proof as ρ. We see that the ground proof ρ in $E \cup P_k$ is strictly smaller (w.r.t. $\succ_{\mathcal{C}}$) than the original peak $t_1 \leftarrow_{R_\infty} t \rightarrow_{R_\infty,E} t_2$. Since $P_\infty = \emptyset$, there is a ground proof ρ' in $E \cup R_\infty$ such that $\rho \succeq_{\mathcal{C}} \rho'$ by Lemma 20. Now we may infer that ρ' is strictly smaller (w.r.t. $\succ_{\mathcal{C}}$) than the original peak $t_1 \leftarrow_{R_\infty} t \rightarrow_{R_\infty,E} t_2$, which is the required contradiction. □

By Theorem 21, the rewrite system R_∞ constructed from a fair derivation $P_0; R_0 \vdash P_1; R_1 \vdash \cdots$ may serve as a decision procedure for the word problem of ground theories P_0 modulo E.

Corollary 22. *Given a finite set of permutation equations E, the word problem of ground theories modulo E is decidable.*

The following example is a variant of the *reachability problem* [32] modulo a finite set of permutation equations E.

Example 7. Consider the following set of permutation equations:

$$\begin{aligned} E = \{ & f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10}) \approx f(x_2,x_1,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10}), \\ & f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10}) \approx f(x_2,x_3,x_4,x_5,x_1,x_6,x_7,x_8,x_9,x_{10}), \\ & f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10}) \approx f(x_1,x_2,x_3,x_4,x_5,x_7,x_6,x_8,x_9,x_{10}), \\ & f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10}) \approx f(x_1,x_2,x_3,x_4,x_5,x_7,x_8,x_9,x_{10},x_6)\}. \end{aligned}$$

In this example, we may view each variable x_i as a vertex in a graph with ten vertices, where each vertex will be assigned to one of three colors: blue (b), red (r), and white (w). Therefore, each ground term $f(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9,c_{10})$ with $c_i = b, r$, or w represents a certain coloring of this graph. There is a transition function with a function symbol $g \notin \mathcal{F}_E$, which transforms one coloring to another coloring of the graph. We assign the precedence as $g \succ_{\mathcal{F}} f \succ_{\mathcal{F}} b \succ_{\mathcal{F}} r \succ_{\mathcal{F}} w$. We see that $\prod[E] = \{(1\,2), (1\,2\,3\,4\,5), (6\,7), (6\,7\,8\,9\,10)\}$, which means that $f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10}) \approx_E f(x_{\rho(1)},x_{\rho(2)},x_{\rho(3)},x_{\rho(4)},x_{\rho(5)},x_6,x_7,x_8,x_9,x_{10})$ for

any permutation ρ on the set $\{1,2,3,4,5\}$ and $f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10}) \approx_E f(x_1,x_2,x_3,x_4,x_5,x_{\pi(6)},x_{\pi(7)},x_{\pi(8)},x_{\pi(9)},x_{\pi(10)})$ for any permutation π on the set $\{6,7,8,9,10\}$ (see Thereom 2). Therefore, ten vertices are partitioned into two equivalence classes. We may view them as two components, i.e. $\{x_1,x_2,x_3,x_4,x_5\}$ and $\{x_6,x_7,x_8,x_9,x_{10}\}$, where the order of a coloring does not matter in each component. For example, $f(r,r,b,b,b,w,w,b,b,b) \approx_E f(b,b,r,b,r,w,b,b,b,w)$. We start with the following set of ground equations:[4]

1. $g(f(b,b,b,b,b,b,b,b,b,b)) \approx f(r,b,b,b,b,b,b,b,b,b)$
2. $g(f(b,b,r,b,b,b,b,b,b,b)) \approx f(r,b,b,b,b,r,b,b,b,b)$
3. $f(r,b,b,b,b,b,b,b,b,b) \approx f(w,b,b,b,b,b,b,b,b,b)$
4. $f(r,b,b,b,b,r,b,b,b,b) \approx f(w,b,b,b,b,w,b,b,b,b)$
5. $g(f(w,b,b,b,b,w,b,b,b,b)) \approx f(w,w,b,b,b,w,w,b,b,b)$
6. $f(w,w,b,b,b,w,w,b,b,b) \approx f(r,r,b,b,b,r,r,b,b,b))$
7. $g(f(r,b,b,b,r,r,b,b,b,r)) \approx f(r,r,r,r,r,r,r,r,r,r)$

The problem is to determine if there is some i such that $g^i(f(b,b,b,b,b,b,b,b,b,b)) = f(r,r,r,r,r,r,r,r,r,r)$, where $f(b,b,b,b,b,b,b,b,b,b)$ is the initial state and $f(r,r,r,r,r,r,r,r,r,r)$ is the target state. (Here $g^i(t)$ denotes that the function symbol g is applied to term $g^{i-1}(t)$ with $g^0(t)$ denoting t.) Now ground completion modulo E works (roughly) as follows:

$1(a)$.	$g(f(b,b,b,b,b,b,b,b,b,b)) \to f(r,b,b,b,b,b,b,b,b,b)$	ORIENT 1
$2(a)$.	$g(f(b,b,r,b,b,b,b,b,b,b)) \to f(r,b,b,b,b,r,b,b,b,b)$	ORIENT 2
$3(a)$.	$f(r,b,b,b,b,b,b,b,b,b) \to f(w,b,b,b,b,b,b,b,b,b)$	ORIENT 3
$1(b)$.	$g(f(b,b,b,b,b,b,b,b,b,b)) \to f(w,b,b,b,b,b,b,b,b,b)$	COMPOSE 1(a), 3(a)
$2(b)$.	$g(f(w,b,b,b,b,b,b,b,b,b)) \approx f(r,b,b,b,b,r,b,b,b,b)$	COLLAPSE 2(a), 3(a)
$2(c)$.	$g(f(w,b,b,b,b,b,b,b,b,b)) \to f(r,b,b,b,b,r,b,b,b,b)$	ORIENT 2(b)
$4(a)$.	$f(r,b,b,b,b,r,b,b,b,b) \to f(w,b,b,b,b,w,b,b,b,b)$	ORIENT 4
$2(d)$.	$g(f(w,b,b,b,b,b,b,b,b,b)) \to f(w,b,b,b,b,w,b,b,b,b)$	COMPOSE 2(c), 4(a)
$5(a)$.	$g(f(w,b,b,b,b,w,b,b,b,b)) \to f(w,w,b,b,b,w,w,b,b,b)$	ORIENT 5
$6(a)$.	$f(r,r,b,b,b,r,r,b,b,b)) \to f(w,w,b,b,b,w,w,b,b,b)$	ORIENT 6
$7(a)$.	$g(f(w,w,b,b,b,w,w,b,b,b)) \approx f(r,r,r,r,r,r,r,r,r,r)$	SIMPLIFY 6(a), 7
$7(b)$.	$g(f(w,w,b,b,b,w,w,b,b,b)) \to f(r,r,r,r,r,r,r,r,r,r)$	ORIENT 7(a)

We eventually obtain the ground convergent (modulo E) rewrite system R_∞ (with $P_\infty = \emptyset$), which consists of the rewrite rules $1(b), 2(d), 3(a), 4(a), 5(a), 6(a)$, and $7(b)$. (It is easy to see that the remaining rules $1(a), 2(a)$ and $2(c)$, and the remaining equations $2(b)$ and $7(a)$ are not persistent.) Now we see that $g^4(f(b,b,b,b,b,b,b,b,b,b)) \to_{R_\infty,E} g^3(f(w,b,b,b,b,b,b,b,b,b)) \to_{R_\infty,E} g^2(f(w,b,b,b,b,w,b,b,b,b)) \to_{R_\infty,E} g(f(w,w,b,b,b,w,$
$w,b,b,b)) \to_{R_\infty,E} f(r,r,r,r,r,r,r,r,r,r)$. Therefore, we may interpret that $f(r,r,r,r,r,r,r,r,r,r)$ is reachable from $f(b,b,b,b,b,b,b,b,b,b)$ by means of iterative applications of the state transition function with symbol g. Note that if $g(f(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9,c_{10}))$ is a normal form w.r.t. R_∞, E, then we may also interpret that $f(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9,c_{10})$ is a fixed state (or a stable state) and cannot be further transformed to another state by an application of the state transition function with symbol g.

[4]We may consider the additional state transitions using a transformation function with symbol g, or partition vertices in a different way with a different number of vertices using a different set of permutation equations.

6 Conclusion

We have presented an RPO-based E-compatible simplification ordering $\succ_E$ on terms that is E-total on ground terms for a finite set of permutation equations E. Since permutation groups naturally arise in sets of permutation equations, we have used permutation group theory for $\succ_E$, especially permutation group actions and their associated orbits. Our ordering is simple and can be adapted from the standard RPO widely used for rewrite systems and theorem proving. Also, the computation of orbits in permutation groups can be done efficiently using the existing permutation group algorithms [29] and software tools (e.g. GAP [12]). We have shown that given two terms s and t, we can determine whether $s \succ_E t$ in polynomial time.

Our ordering $\succ_E$ provides a simple termination criterion for R, E (resp. R/E), that is, R, E (resp. R/E) is terminating if $l \succ_E r$ for all rules $l \to r \in R$. We have used $\succ_E$ for a completion and ground completion procedure for R, E. Furthermore, our ground completion modulo E always terminates with a finite ground convergent (modulo E) rewrite system, which allows us to provide a decision procedure for the word problem of ground theories modulo E. (It is also an interesting question whether other ground completion approaches and formalisms (e.g. the *abstract completion* of [14]) can be extended for ground completion modulo E for a finite set of permutation equations E using $\succ_E$.)

Since permutations and combinations are widely used in mathematics and many fields of science including computer science, developing applications of term rewriting and equational theorem proving [19] with built-in permutation equations is one of the promising future directions of the research discussed in this paper. For example, one may consider reachability problems modulo E and its applications to hardware and software verification using our ordering and rewriting modulo E approach for a finite set of permutation equations E.

References

[1] Jürgen Avenhaus. Efficient Algorithms for Computing Modulo Permutation Theories. In David Basin and Michaël Rusinowitch, editors, *Automated Reasoning - IJCAR 2004, Cork, Ireland, July 4–8*, pages 415–429, Berlin, Heidelberg, 2004. Springer.

[2] Jürgen Avenhaus and David A. Plaisted. General algorithms for permutations in equational inference. *Journal of Automated Reasoning*, 26(3):223–268, 2001.

[3] Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, Cambridge, UK, 1998.

[4] Franz Baader and Wayne Snyder. Unification Theory. In *Handbook of Automated Reasoning*, Volume I, chapter 8, pages 445 – 532. Elsevier, Amsterdam, 2001.

[5] Leo Bachmair. *Canonical Equational Proofs.* Birkhäuser, Boston, 1991.

[6] Leo Bachmair and Nachum Dershowitz. Completion for rewriting modulo a congruence. *Theoretical Computer Science*, 67(2):173–201, 1989.

[7] Leo Bachmair, Ashish Tiwari, and Laurent Vigneron. Abstract congruence closure. *Journal of Automated Reasoning*, 31(2):129–168, 2003.

[8] Frédéric Blanqui. Termination of rewrite relations on λ-terms based on Girard's notion of reducibility. *Theoretical Computer Science*, 611:50–86, 2016.

[9] Frédéric Blanqui. Rewriting Modulo in Deduction Modulo. In Robert Nieuwenhuis, editor, *Rewriting Techniques and Applications*, pages 395–409, Berlin, Heidelberg, 2003. Springer.

[10] Nachum Dershowitz. Orderings for term-rewriting systems. *Theoretical Computer Science*, 17(3):279 – 301, 1982.

[11] Nachum Dershowitz and David A. Plaisted. Rewriting. In *Handbook of Automated Reasoning*, Volume I, chapter 9, pages 535 – 610. Elsevier, Amsterdam, 2001.

[12] GAP Group. *Groups, Algorithms, Programming, Version 4.8*, 2016. http://www.gap-system.org.

[13] Sumanta Ghosh and Piyush P. Kurur. *Permutation Groups and the Graph Isomorphism Problem*, pages 183–202. Springer, Cham, 2014.

[14] Nao Hirokawa, Aart Middeldorp, Christian Sternagel, and Sarah Winkler. Abstract Completion, Formalized. *Logical Methods in Computer Science*, 15:19:1–19:42, 2019.

[15] Thomas W. Hungerford. *Algebra*. Springer, New York, NY, 1980.

[16] Jean-Pierre Jouannaud and Hélène Kirchner. Completion of a set of rules modulo a set of equations. *SIAM Journal on Computing*, 15(4):1155–1194, 1986.

[17] Deepak Kapur, Paliath Narendran, and G. Sivakumar. A path ordering for proving termination of term rewriting systems. In Hartmut Ehrig, Christiane Floyd, Maurice Nivat, and James Thatcher, editors, *Mathematical Foundations of Software Development*, pages 173–187, Berlin, Heidelberg, 1985. Springer Berlin Heidelberg.

[18] Deepak Kapur and G. Sivakumar. Proving Associative-Commutative Termination Using RPO-Compatible Orderings. In R. Caferra and Gernot Salzer, editors, *Automated Deduction in Classical and Non-Classical Logics*, pages 39–61, Berlin, Heidelberg, 2000. Springer.

[19] Dohan Kim and Christopher Lynch. Equational Theorem Proving Modulo. In *Automated Deduction - CADE 28: The 28th International Conference on Automated Deduction, Carnegie Mellon University, Pittsburgh, PA (Virtual Conference), July 11-16, to appear*. Springer, 2021.

[20] Claude Kirchner and Helene Kirchner. Rewriting, Solving, Proving, 1999. Preliminary version of a book: `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.144.5349`.

[21] Donald. E. Knuth and Peter B. Bendix. Simple word problems in universal algebras. In Jörg H. Siekmann and Graham Wrightson, editors, *Automation of Reasoning: 2: Classical Papers on Computational Logic 1967–1970*, pages 342–376. Springer, Berlin, Heidelberg, 1983.

[22] Claude Marché. Normalized rewriting: an alternative to rewriting modulo a set of equations. *Journal of Symbolic Computation*, 21(3):253 – 288, 1996.

[23] Paliath Narendran and Michaël Rusinowitch. Any ground associative-commutative theory has a finite canonical system. In R. V. Book, editor, *Rewriting Techniques and Applications*, pages 423–434, Berlin, Heidelberg, 1991. Springer.

[24] Robert Nieuwenhuis and Albert Rubio. Paramodulation-based theorem proving. In *Handbook of Automated Reasoning*, Volume I, chapter 7, pages 371–443. Elsevier, Amsterdam, 2001.

[25] Gerald E Peterson and Mark E Stickel. Complete sets of reductions for some equational theories. *Journal of the ACM (JACM)*, 28(2):233–264, 1981.

[26] Albert Rubio. Theorem Proving modulo Associativity. In H. Kleine Büning, editor, *Computer Science Logic*, pages 452–467, Berlin, Heidelberg, 1996. Springer.

[27] Albert Rubio. A Fully Syntactic AC-RPO. *Inf. Comput.*, 178(2):515 – 533, 2002.

[28] Albert Rubio and Robert Nieuwenhuis. A total AC-compatible ordering based on RPO. *Theoretical Computer Science*, 142(2):209 – 227, 1995.

[29] Charles C Sims. *Computation with finitely presented groups*, volume Vol. 48. Cambridge University Press, Cambridge, UK, 1994.

[30] Wayne Snyder. On the complexity of recursive path orderings. *Information Processing Letters*, 46(5):257 – 262, 1993.

[31] Joachim Steinbach. On the complexity of simplification orderings. Technical Report Technical Report SR-93-18 (SFB), SEKI University of Kaiserslautern, 1993.

[32] Christian Sternagel and Akihisa Yamada. Reachability analysis for termination and confluence of rewriting. In *Tools and Algorithms for the Construction and Analysis of Systems*, pages 262–278, Cham, 2019. Springer International Publishing.