Equational Theorem Proving Modulo

Dohan Kim and Christopher Lynch

Clarkson University, Potsdam, NY, USA

Abstract

Unlike other methods for theorem proving modulo with constrained clauses [12, 13], equational theorem proving modulo with constrained clauses along with its simplification techniques has not been well studied. We introduce a basic paramodulation calculus modulo equational theories E satisfying certain properties of E and present a new framework for equational theorem proving modulo E with constrained clauses. We propose an inference rule called Generalized E-Parallel for constrained clauses, which makes our inference system completely basic, meaning that we do not need to allow any paramodulation in the constraint part of a constrained clause for refutational completeness. We present a saturation procedure for constrained clauses based on relative reducibility and show that our inference system including our contraction rules is refutationally complete.

1 Introduction

Equations occur frequently in many areas of mathematics, logics, and computer science. Equational theorem proving [6, 8, 18, 21] is, in general, concerned with proving mathematical or logical statements in first-order clause logic with equality. While resolution [23] has been successful for theorem proving for first-order clause logic without equality, it has some limitations to deal with the equality predicate. For example, when dealing with the equality predicate using resolution, one must add the congruence axioms explicitly for each predicate and function symbol in order to express the properties of equality [8, 21].

Paramodulation [22] is based on the replacement of equals by equals, in order to improve the efficiency of resolution in equational theorem proving. However, paramodulation, in general, often produces a large amount of unnecessary clauses, so the search space for a refutation expands very rapidly. Therefore, various improvements have been developed for paramodulation. For example, it was shown that the functional reflexivity equations used by the traditional paramodulation rule [22] are not needed, and paramodulation into variables does not need to be allowed (see [8]).

Basic paramodulation [9,19] restricts paramodulation by forbidding paramodulation at (sub)terms introduced by substitutions from previous inference steps, and uses orderings on terms and literals in order to further restrict paramodulation inferences. In [20, 25], basic paramodulation had been extended to basic paramodulation modulo associativity and commutativity (AC) axioms. (See [24] also for basic paramodulation modulo the associativity (A) axiom.) Basic paramodulation modulo AC uses the symbolic constraints, overcoming a drawback of traditional paramodulation modulo AC (see [7, 26]) that often generates many slightly different permuted variants of clauses. For example, more than a million conclusions can possibly be generated by paramodulating the equation $x + x + x = x$ into the clause $P(y_1 + y_2 + y_3 + y_4)$ for which $+$ is an AC symbol, since a minimal complete set of AC-unifiers for $x + x + x$ and $y_1 + y_2 + y_3 + y_4$ contains more than a million AC-unifiers [20,25]. On the other hand, one only needs a single conclusion $P(x) \,||\, x + x + x \approx^?_{AC} y_1 + y_2 + y_3 + y_4$ for the above inference using basic paramodulation modulo AC with an equality constraint.

In this paper, we present a new basic paramodulation calculus modulo equational theories E (including $E = AC$) parameterized by a suitable E-compatible ordering $\succ$. Our main inference rule for basic paramodulation modulo E is given (roughly) as follows:

$$\frac{C \vee s \approx t \;||\; \phi_1 \qquad D \vee L[s'] \;||\; \phi_2}{C \vee D \vee L[t] \;||\; s \approx^?_E s' \wedge \phi_1 \wedge \phi_2}$$

The equality constraints are inherited and the accumulated E-unification problems are kept in the constraint part of conclusion. Instead of generating as many conclusions as minimal and complete E-unifiers of two terms s and s', a single conclusion is generated with its constraint keeping the E-unification problem of s and s'. Another key inference rule in our basic paramodulation calculus modulo E is the Generalized E-Parallel (or E-Parallel) rule, adapted from our recent work on basic narrowing modulo [17]. This rule allows our basic paramodulation calculus to adapt the free case (i.e. $E = \emptyset$) to the modulo E case (i.e. $E \neq \emptyset$).[1] For example, suppose that we have three clauses $1 : a+b \approx c$, $2 : a+(b+x) \approx c+x$, and $3 : (a+a)+(b+b) \not\approx c+c$, where $+$ is an AC symbol with $+ \succ a \succ b \succ c$. We use the E-Parallel rule from clause 1 and 2 and obtain the clause $4 : a + (b + (a + b)) \approx c + c$, which derives a contradiction with clause 3 because $a + (b + (a + b)) \approx_{AC} (a + a) + (b + b)$ (i.e. the equality constraint is satisfiable). The details of this inference rule are discussed in Section 4.

Throughout this paper, we assume that (i) we are given an E-compatible reduction ordering $\succ$ on terms with the subterm property that is E-total on ground terms, (ii) E has a finitary and complete unification algorithm, and (iii) E-congruence classes are finite. (If E satisfies condition (i), then E is necessarily *regular* [2].) With these assumptions of E, we can deal uniformly with different equational theories E in our framework and show that our inference

[1] If $E = \emptyset$, then we may disregard the Generalized E-Parallel (or E-Parallel) rule along with the E-Completion rule and replace E-unification with syntactic unification.

system including our contraction rules is refutationally complete.

The known practical theories satisfying the above assumptions of E are AC and finite *permutation theories* [1, 16]. (For example, if one considers an ACI symbol $+$ using our approach, then AC should be a modulo E part and the idempotency axiom $(I : x + x \approx x)$ should be a part of the input formulas.) Although associative (A)-unification is infinitary, our approach is also applicable to the case where $E = A$ in practice, since there is a tool for A-unification which is guaranteed to terminate with a finite and complete set of A-unifiers for a significantly large class of A-unification problems (see [14]).

2 Preliminaries

We assume that the reader has some familiarity with rewrite systems [3] (including the *extended rewrite system* for R *modulo* E (i.e. R, E) [11, 15]) and unification [4]. We use the standard terminology of paramodulation [6, 9, 21].

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 $T(\mathcal{F}, \mathcal{X})$. A *literal* is either an equation L (a *positive literal*) or a negative equation $\neg L$ (a *negative literal*). A *clause* is a finite multiset of literals, written as a disjunction of literals $\neg A_1 \vee \cdots \vee \neg A_m \vee B_1 \vee \cdots \vee B_n$ or as an implication $\Gamma \rightarrow \Delta$, where the multiset Γ is called the *antecedent* and the multiset Δ is called the *succedent* of the clause.

An *equational theory* is a set of equations. (In this paper, an equational theory and a set of axioms are used interchangeably.) We denote by $\approx_E$ the least congruence on $T(\mathcal{F}, \mathcal{X})$ that is closed 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*.

A (strict) ordering $\succ$ on terms is *monotonic* if $s \succ t$ implies $u[s]_p \succ u[t]_p$ for all s, t, u and positions p. 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 $p \neq \lambda$. (In this paper, λ denotes the top position.) A *simplification ordering* is a rewrite ordering with the subterm property. An ordering $\succ$ on terms is E-compatible if $s \succ t$, $s \approx_E s'$, and $t \approx_E t'$ 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 multiset S and an E-compatible ordering $\succ$ on S, we say that x is *maximal* (resp. *strictly maximal*) in S if there is no $y \in S$ (resp. $y \in S \setminus \{x\}$) with $y \succ x$ (resp. $y \succeq x$).

Clauses may also be considered as multisets of occurrences of equations. An occurrence of an equation $s \approx t$ in the antecedent of a clause is the multiset $\{\{s, t\}\}$, and in the succedent it is the multiset $\{\{s\}, \{t\}\}$. We denote ambiguously all those orderings on terms, equations and clauses by $\succ$.

An equational theory is *permutative* if each equation in the theory contains the same symbols on both sides with the same number of occurrences. The *depth* of a term t is defined as $depth(t) = 0$ if t is a variable or a constant and $depth(f(s_1, \ldots, s_n)) = 1 + \max\{depth(s_i) \,|\, 1 \leq i \leq n\}$. We say that an *equational theory has maximum depth at most* k if the maximum depth of all terms in the equations in the theory is less than or equal to k.

A *(Herbrand) interpretation* I is a congruence on ground terms. I *satisfies* (is a *model* of) a ground clause $\Gamma \rightarrow \Delta$, denoted by $I \models \Gamma \rightarrow \Delta$, if $I \not\supseteq \Gamma$ or $I \cap \Delta \neq \emptyset$. In this case, we say that $\Gamma \rightarrow \Delta$ is *true* in I. A ground clause C *follows* from a set of ground clauses $\{C_1, \ldots, C_k\} \models C$ if C is true in every model of $\{C_1, \ldots, C_k\}$.

3 Constrained clauses

Definition 1. (Constrained clauses) [21, 25] A *constrained clause* is a pair $C \,||\, \phi$, where C is a clause and ϕ is an equality constraint consisting of a conjunction of the form $s \approx_E^? t$ for terms s and t. The set of solutions of a constraint ϕ, denoted by $Sol(\phi)$, is the set of the ground substitutions defined inductively as:

$$Sol(\phi_1 \wedge \phi_2) = Sol(\phi_1) \cap Sol(\phi_2),$$
$$Sol(s \approx_E^? t) = \{\sigma \,|\, s\sigma \text{ and } t\sigma \text{ are } E\text{-equivalent}\},$$

A constraint ϕ is *satisfiable* if it admits at least one solution.

A constrained clause with an unsatisfiable constraint is a tautology. If every ground substitution with domain $Vars(\phi)$ of $C \,||\, \phi$ is a solution of ϕ, then ϕ is a tautological constraint. An unconstrained clause can also be considered as a constrained clause with a tautological constraint.

The main technical difficulties in lifting a reduced ground inference to an inference at the clause level in a basic paramodulation inference system involve a ground clause of the form $C\sigma := D\sigma \vee x\sigma \approx t\sigma$ with $C := D \vee x \approx t \,||\, \phi$ and $\sigma \in Sol(\phi)$, where $x\sigma \Rightarrow t\sigma \in R$ for a given ground rewrite system R. This motivates the following definition of irreducibility to lift a reduced ground inference to an inference at the clause level in our inference system. (See [9] also for *order-irreducibility* in the free case.)

Definition 2. (Order-irreducibility) Given a ground rewrite system R and an equational theory E, a ground literal $L[l']_p$ is *order-reducible* (at position p) by R, E with $l \Rightarrow r \in R$ if $l' \approx_E l, l \succ r$ and $L \succ l \approx r$. A literal $L[s]$ is *order-irreducible in* s by R, E if $L[s]$ is not order-reducible at any position of s.

In Definition 2, the condition $L \succ l \approx r$ is always true when L is a negative literal or else l' does not occur at the top (i.e. $p = \lambda$) of the largest term of L.

Definition 3. (Reduced ground instances) Given a ground rewrite system R and an equational theory E, $C\sigma$ is a *ground instance* of $C \,||\, \phi$ if σ is a solution of ϕ (i.e. $\sigma \in Sol(\phi)$). It is a *reduced ground instance* of $C \,||\, \phi$ w.r.t. R, E if σ

is a solution of ϕ and each ground literal $L[x\sigma]$ in $C\sigma$ is order-irreducible in $x\sigma$ by R, E for each variable $x \in Vars(C)$. In this case, σ is a *reduced solution* of $C \,||\, \phi$ w.r.t. R, E.

Definition 4. (A model of a constrained clause) An interpretation I *satisfies* (is a *model* of) a constrained clause $C \,||\, \phi$, denoted by $I \models C \,||\, \phi$, if it satisfies every ground instance of $C \,||\, \phi$ (i.e. every $C\sigma$ for which σ is a solution of ϕ).

Definition 5. (Reductiveness, weak reductiveness, semi-reductiveness, and weak maximality) An equation $s \approx t$ is *reductive* (resp. *weakly reductive*) for $C \,||\, \phi := D \vee s \approx t \,||\, \phi$ if there exists a ground instance $C\sigma$ such that $s\sigma \approx t\sigma$ is strictly maximal (resp. maximal) in $C\sigma$ with $s\sigma \succ t\sigma$. The clause $C \,||\, \phi$ is simply called *reductive* if there exists a reductive equation $s \approx t$ for $C \,||\, \phi$. A negative equation $u \not\approx v$ is *semi-reductive* (resp. *weakly reductive*) for $C \,||\, \phi := D \vee u \not\approx v \,||\, \phi$ if there exists a ground instance $C\sigma$ such that $u\sigma \succ v\sigma$ (resp. $u\sigma \succ v\sigma$ and $u\sigma \not\approx v\sigma$ is maximal in $C\sigma$). A literal L is *weakly maximal* for $C \,||\, \phi := D \vee L \,||\, \phi$ if there exists a ground instance $C\sigma$ such that $L\sigma$ is maximal in $C\sigma$.

4 Inference rules

The inference rules in our inference system are parameterized by a selection function $\mathcal{S}$ and an E-compatible reduction ordering $\succ$ with the subterm property that is E-total on ground terms, where $\mathcal{S}$ selects at most one (occurrence of a) negative literal in the clause part C of each (constrained) clause $C \,||\, \phi$. For technical convenience, if a literal L is selected in C, then we also say that L is selected in $C \,||\, \phi$. In our inference rules, a literal in a clause $C \,||\, \phi$ is involved in some inference if it is selected in C (by $\mathcal{S}$) or nothing is selected and it is maximal in C (cf. [8]). The following Basic Paramodulation rule is our main inference rule for equational theorem proving modulo E, where only the maximal sides of literals in clauses are involved in inferences by this rule. We rename variables in the premises in our inference rules if necessary so that no variable is shared between premises (i.e. standardized apart).

Basic Paramodulation

$$\frac{C \vee s \approx t \,||\, \phi_1 \qquad D \vee L[s'] \,||\, \phi_2}{C \vee D \vee L[t] \,||\, s \approx^?_E s' \wedge \phi_1 \wedge \phi_2} \quad \text{if}$$

1. s' is not a variable,
2. $s \approx t$ is reductive for the left premise, and C contains no selected literal,
3. either one of the following three conditions is met:
   (a) L is selected in the right premise, and
   L is of the form $u[s'] \not\approx v$ and is semi-reductive for the right premise.
   (b) nothing is selected in the right premise, and
   L is of the form $u[s'] \approx v$ and is reductive for the right premise.

(c) nothing is selected in the right premise, and
L is of the form $u[s'] \not\approx v$ and is weakly reductive for the right premise.

Equality Resolution

$$\frac{C \vee s \not\approx t \,||\, \phi}{C \,||\, s \approx^?_E t \wedge \phi} \quad \text{if}$$

$s \not\approx t$ is selected, or else nothing is selected and $s \not\approx t$ is weakly maximal for the premise.

E-Factoring

$$\frac{C \vee s \approx t \vee s' \approx t' \,||\, \phi}{C \vee t \not\approx t' \vee s' \approx t' \,||\, s \approx^?_E s' \wedge \phi} \quad \text{if}$$

$s \approx t$ is weakly reductive for the premise, and C contains no selected literal.

E-Completion

$$\frac{C \vee s \approx t \,||\, \phi}{C \vee e_1[t]_p \approx e_2 \,||\, s \approx^?_E s' \wedge \phi} \quad \text{if}$$

1. $e_1[s']_p \approx e_2 \in E$ and $p \neq \lambda$, where s' is not a variable,
2. $s \approx t$ is reductive for the premise, and C contains no selected literal.

The above E-Completion rule is an adaptation of the E-*closure* [26] rule using equality constraints (cf. E-*extension* [5]).

E-Parallel

$$\frac{C \vee s \approx t \,||\, \phi_1 \qquad D \vee l \approx r \,||\, \phi_2}{C \vee D\sigma \vee l\sigma \approx r\theta \,||\, \phi_1 \wedge \phi_2} \quad \text{if}$$

1. $s \approx t$ is reductive for the left premise, and C contains no selected literal,
2. $l \approx r$ is reductive for the right premise, and D contains no selected literal,
3. both l and s are not variables,
4. $\sigma = \{x \mapsto s\}$ and $\theta = \{x \mapsto t\}$ for some variable $x \in Vars(l) \cap Vars(r)$ with $x \notin Vars(\phi_2)$,
5. there is a term u' with $u' \approx_E l\sigma$, such that u' is R, E-reducible with $R = \{l \Rightarrow r, s \Rightarrow t\}$ only at the top position (i.e. no strict subterm of u' is R, E-reducible).

Generalized E-Parallel

$$\frac{C \vee s \approx t \,||\, \phi_1 \qquad D \vee l \approx r \,||\, \phi_2}{C \vee D\sigma \vee l\sigma \approx r\theta \,||\, \phi_1 \wedge \phi_2} \quad \text{if}$$

1. $s \approx t$ is reductive for the left premise, and C contains no selected literal,
2. $l \approx r$ is reductive for the right premise, and D contains no selected literal,
3. both l and s are not variables,
4. $e_1[u] \approx e_2 \in E$, where u is not a variable,
5. $\sigma = \{x \mapsto u[s]_p\}$ and $\theta = \{x \mapsto u[t]_p\}$ for some variable $x \in Vars(l) \cap Vars(r)$ with $x \notin Vars(\phi_2)$ and some position p,
6. there is a term u' with $u' \approx_E l\sigma$, such that u' is R, E-reducible with $R = \{l \Rightarrow r, s \Rightarrow t\}$ only at the top position.

We mark each clause produced by the Generalized E-Parallel (or E-Parallel) rule as "protected" so that it is protected from our contraction rules discussed in Section 5. (We simply say each marked clause is a protected clause.) Protected clauses behave the same way as other clauses in our inference rules, but our contraction rules are not applied to protected clauses (see Section 5 for details).

We may also use *predicate terms* [6] $P(t_1, \ldots, t_n)$ in our inference system, where a predicate term cannot be a proper subterm of any term. Note that a predicate term $P(t_1, \ldots, t_n)$ can be expressed as an equation $P(t_1, \ldots, t_n) \approx \top$, where $\top$ is a special constant symbol minimal in the ordering $\succ$ and P is considered as a function symbol. (In this sense, $\neg P(t_1, \ldots, t_n)$ can be expressed as $P(t_1, \ldots, t_n) \not\approx \top$.) In the remainder of this paper, by $\mathcal{BP}$ we denote the inference system consisting of the Basic Paramodulation, Equality Resolution, E-Factoring, E-Completion, and the Generalized E-Parallel rule. If E is a permutative theory with maximum depth at most 2 (e.g. $E = A, C$, or AC), then we use the simpler E-Parallel rule instead of the Generalized E-Parallel rule in $\mathcal{BP}$ (see Lemma 6).

Example 1. Let $+$ be an AC symbol (in infix notation) with $+ \succ a \succ b \succ 0$ and consider the following inconsistent set of clauses 1: $x + 0 \approx x$, 2: $a + a \approx 0$, 3: $b + b \approx 0$, and 4: $(a + b) + (a + b) \not\approx 0$. Now we show how the empty clause (with a satisfiable constraint) is derived:
5: $(x + y) + z \approx x + 0 \,||\, y + z \approx^?_{AC} a + a$ (E-Completion with 2 using the associativity axiom $x + (y + z) \approx (x + y) + z$.)
6: $((b + b) + y) + z \approx 0 + 0 \,||\, y + z \approx^?_{AC} a + a$ (E-Parallel with 3 into 5. In condition 5 of the E-Parallel rule, term u' corresponds to $(b + y) + (b + z)$ here.)
7: $0 + 0 \not\approx 0 \,||\, ((b + b) + y) + z \approx^?_{AC} (a + b) + (a + b) \wedge y + z \approx^?_{AC} a + a$ (Basic Paramodulation with 6 into 4)
8: $x \not\approx 0 \,||\, x + 0 \approx^?_{AC} 0 + 0 \wedge ((b + b) + y) + z \approx^?_{AC} (a + b) + (a + b) \wedge y + z \approx^?_{AC} a + a$ (Basic Paramodulation with 1 into 7)
9: $\square \,||\, x \approx^?_{AC} 0 \wedge x + 0 \approx^?_{AC} 0 + 0 \wedge ((b + b) + y) + z \approx^?_{AC} (a + b) + (a + b) \wedge y + z \approx^?_{AC} a + a$ (Equality Resolution on 8)

In contrast, the existing approaches for basic paramodulation modulo AC [20, 25] use clauses 2 and 4, for example, and produce clause 5′: $0 + x \not\approx 0 \,||\, x \approx^?_{AC} b + b$ and then clause 6′: $0 + y \not\approx 0 \,||\, x \approx^?_{AC} b + b \wedge y \approx^?_{AC} 0$ by their inference rules. Then 6′ is used to derive a contradiction with 1. It can be viewed that 6′ is obtained from 5′ by an indirect paramodulation with 3 in the constraint part. In our approach, we simply block clauses like 5′ from further inferences (see Definition 12), and no direct or indirect paramodulation is allowed in the constraint part of any clause.

Example 2. Consider $S = \{f(g(x)) \approx x, a \approx b, c \not\approx g(b)\}$ and $E = \{f(g(g(a))) \approx c\}$ with $f \succ g \succ a \succ b$, where E is a regular theory with maximum depth 3. The Generalized E-Parallel rule with premises $f(g(x)) \approx x$ and $a \approx b$ produces the conclusion $f(g(g(a))) \approx g(b)$. (Choose l as $f(g(x))$, s as a, and u as $g(a)$ in the Generalized E-Parallel rule.) Then it is used to derive a contradiction with clause $c \not\approx g(b)$ since $f(g(g(a))) \approx_E c$.

In the above example, a suitable E-compatible reduction ordering $\succ$ on ground terms is obtained in such a way that given two ground terms, we rewrite each occurrence of c in each ground term into $f(g(g(a)))$ at the same position with (the occurrence of) c and then use the standard *lexicographic path ordering* [3, 21] for comparing (rewritten) ground terms without any occurrence of c. Then we may compare terms with variables by considering ground substitutions and using this ordering on ground terms.

In what follows, by the Parallel rule we mean the E-Parallel or the Generalized E-Parallel rule. First, observe that we cannot derive a contradiction in both Examples 1 and 2 using inference rules in $\mathcal{BP}$ without the Parallel rule. The intuition behind the Parallel rule is that above all, a reductive ground clause corresponds to a reductive ground conditional rewrite rule [18] with positive and negative conditions. Therefore, roughly speaking, the premises of the Parallel rule are reductive conditional rewrite rules with positive and negative conditions. (The Parallel rule applies to only reductive clauses.) Now the conclusion of the Parallel rule combines two steps: (i) instantiating a "problematic" variable in a special and restricted way, and (ii) selectively rewriting an instantiated term if conditions are met. (Therefore, conditions C is included in the conclusion.) A problematic variable is often determined by a built-in equational theory E. It is mostly a variable produced by an E-Completion inference (see Example 1) for AC cases, which is the counterpart of an extension variable for AC-extension [7, 26].

Observe that the Generalized E-Parallel rule is more general than the E-Parallel rule. If p is always the top position for the Generalized E-Parallel rule, then they are equivalent. This is the case for permutative theories with maximum depth at most 2 (e.g. $E = A, C$, or AC).

Lemma 6. *If E is a permutative theory with maximum depth at most 2, then the E-Parallel rule and the Generalized E-Parallel rule are equivalent, i.e., they generate the same conclusion for the same input premises.*

Proof. First of all, if p is the top position in the Generalized E-Parallel rule, then we are done, since a term u in the condition $e_1[u] \approx e_2 \in E$ in the Generalized E-Parallel rule is immaterial for the conclusion, meaning that the Generalized E-Parallel rule and the E-Parallel rule coincide. We show that if p is not the top position and E is a permutative theory with maximum depth at most 2, then the Generalized E-Parallel rule does not generate any conclusion due to condition 6 in the Generalized E-Parallel rule.

Suppose that p is not the top position. Then it suffices to consider the case $l\{x \mapsto u[s]_p\} = e'_1\tau$ for some $e'_1 \approx e'_2 \in E$ with a substitution τ, where l, s, and u are not variables (see conditions 3 and 4 in the Generalized E-Parallel rule). Since E is a permutative theory with maximum depth at most 2 and p is not the top position, term s in $l\{x \mapsto u[s]_p\}$ occurs in $e'_1\tau$ also at a constant position or in the substitution part of e'_1.

Suppose that term s in $l\{x \mapsto u[s]_p\}$ occurs in $e'_1\tau$ at a constant position of e'_1. Since E is permutative, we may infer that any term E-equivalent to $l\{x \mapsto u[s]_p\}$ w.r.t. $e'_1 \approx e'_2 \in E$ is R, E-reducible with $R = \{l \Rightarrow r, s \Rightarrow t\}$ below the top position due to s. Thus, the conclusion is not generated due to condition 6 in the Generalized E-Parallel rule.

Now suppose that term s in $l\{x \mapsto u[s]_p\}$ occurs in $e'_1\tau$ in the substitution part of e'_1. Since E is regular (because of our assumption of $\succ$), we may also infer that any E-equivalent term of $l\{x \mapsto u[s]_p\}$ w.r.t. $e'_1 \approx e'_2 \in E$ is R, E-reducible with $R = \{l \Rightarrow r, s \Rightarrow t\}$ below the top position due to s. Thus, the conclusion is not generated due to condition 6 in the Generalized E-Parallel rule. $\square$

The following example is a simple variant of the *reachability problem* [15] modulo a *permutation theory* [1,16], where $\neg P(f(c,b,b,d,e))$ is the query from the initial configuration $P(f(a,b,c,d,e))$. We may view E in the following example as all permutations of variables x_1, x_2, x_3, x_4, and x_5, since the symmetric group S_5 is generated by two cycles $(1\,2)$ and $(1\,2\,3\,4\,5)$.

Note that the E-Completion and the Parallel rule are not always needed for every built-in equational theory E. In particular, the E-Completion and the E-Parallel rule are not needed for any permutation theory E. We see that for the E-Completion rule, condition 1 cannot be satisfied, i.e., s' is always a variable because p is not the top position. For the E-Parallel rule, condition 5 is not satisfied, which can be shown similarly to the proof of Lemma 6.

Example 3. Let $E = \{f(x_1,x_2,x_3,x_4,x_5) \approx f(x_2,x_1,x_3,x_4,x_5), f(x_1,x_2,x_3,x_4,x_5) \approx f(x_2,x_3,x_4,x_5,x_1)\}$ with $P \succ f \succ a \succ b \succ c \succ d \succ e$ and consider the following set of clauses 1: $\neg P(f(c,b,b,d,e))$, 2: $P(f(a,b,c,d,e))$, and 3: $f(a,b,x,y,z) \approx f(b,b,x,y,z)$. Basic Paramodulation with 3 into 2 yields clause 4: $P(f(b,b,x,y,z)) \,||\, f(a,b,x,y,z) \approx^?_E f(a,b,c,d,e)$. By applying Basic Paramodulation with 1 and 4 (using $P(f(c,b,b,d,e)) \not\approx \top$ and $P(f(b,b,x,y,z)) \approx \top \,||\, f(a,b,x,y,z) \approx^?_E f(a,b,c,d,e)$) and then applying Equality Resolution, we have clause 5: $\square \,||\, f(b,b,x,y,z) \approx^?_E f(c,b,b,d,e) \wedge f(a,b,x,y,z) \approx^?_E f(a,b,c,d,e)$. The equality constraint in 5 is satisfiable and we have a contradiction. Note that clause 4 schematizes the set of ground clauses $\{P(f(b,b,c,d,e)), P(f(b,b,c,e,d)), P(f(b,b,d,c,e)), P(f(b,b,d,e,c)), P(f(b,b,e,c,d)), P(f(b,b,e,d,c))\}$.

5 Redundancy criteria and contraction techniques

Definition 7. (Relative reducibility) Given an equational theory E, a ground instance $C\sigma_1$ of $C \,||\, \phi_1$ is *reduced relative to* a ground instance $D\sigma_2$ of $D \,||\, \phi_2$ if for any rewrite system R, $C\sigma_1$ is a reduced ground instance of $C \,||\, \phi_1$ w.r.t. R, E whenever $D\sigma_2$ is a reduced ground instance of $D \,||\, \phi_2$ w.r.t. R, E.

In what follows, the relation $\trianglelefteq$ on terms represents the subterm relation, i.e., $s \trianglelefteq t$ if s is a subterm of t. The relation $\sqsubseteq$ on sets of terms is defined as follows: $\{s_1, \ldots, s_m\} \sqsubseteq \{t_1, \ldots, t_n\}$ if for all $1 \leq i \leq m$, there is some $1 \leq j \leq n$ such that $s_i \trianglelefteq t_j$, and $\emptyset \sqsubseteq X$ for any set of terms X. Given a clause $C \,||\, \phi$, we denote by $Ran(\sigma|_{Vars(C)})$ for some $\sigma \in Sol(\phi)$ the range of the restriction of σ to the set of variables $Vars(C)$ if $Vars(C) \neq \emptyset$. If C is a ground clause with a tautological constraint (e.g. the empty constraint), then we set $Ran(\sigma|_{Vars(C)}) = \emptyset$. (Note that any ground substitution is a solution of a tautological constraint.)

We say that a clause $C \,||\, \phi$ is a clause with a *succedent top variable* [20] w.r.t. $\sigma \in Sol(\phi)$ if there is a variable $x \in Vars(C) \cap Vars(\phi)$ only appearing in equations $x \approx t$ of the succedent of C with $x\sigma \succ t\sigma$ for some t. The following lemma, which directly follows from Definition 7, is a sufficient syntactic condition for $C\sigma_1$ being reduced relative to $D\sigma_2$ in Definition 7 if $D \,||\, \phi_2$ is not a clause with a succedent top variable w.r.t. σ_2. If $D \,||\, \phi_2$ is a clause with a succedent top variable x w.r.t. some $\sigma_2 \in Sol(\phi_2)$, then one may (partially) instantiate x in D with σ_2 if possible, so that one may use the syntactic condition for checking whether $C\sigma_1$ is reduced relative to $D\sigma_2$ as in the following lemma.

Lemma 8. *Given an equational theory E, a ground instance $C\sigma_1$ of $C \,||\, \phi_1$ is reduced relative to a ground instance $D\sigma_2$ of $D \,||\, \phi_2$ if $Ran(\sigma_1|_{Vars(C)}) \sqsubseteq Ran(\sigma_2|_{Vars(D)})$ and $D \,||\, \phi_2$ is not a clause with a succedent top variable w.r.t. σ_2.*

In what follows, we denote by $E^{\prec C}$ (resp. $R^{\prec C}$) the set of ground instances of equations in E (resp. the set of ground rewrite rules in R) smaller than the ground clause C (w.r.t. $\succ$), and by S modulo E a set of clauses S with a built-in equational theory E.

Definition 9. (Redundancy) A clause $C \,||\, \phi$ is *redundant* in S modulo E (w.r.t. relative reducibility) if for every ground instance $C\sigma$, there exist ground instances $C_1\sigma_1, \ldots, C_k\sigma_k$ of clauses $C_1 \,||\, \phi_1, \ldots, C_k \,||\, \phi_k$ in S reduced relative to $C\sigma$, such that $C\sigma \succ C_i\sigma_i$, $1 \leq i \leq k$, and $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup R^{\prec C\sigma} \cup E^{\prec C\sigma} \models C\sigma$ for any ground rewite system R contained in $\succ$. (In this case, we also say that each $C\sigma$ is *redundant* in S modulo E (w.r.t. relative reducibility).)

Definition 10. (Basic E-simplification) An equation $l \approx r$ *simplifies* a clause $C \vee L[l']_p \,||\, \phi$ into $C \vee L[r\rho]_p \,||\, \phi$ if the following conditions are met:

(i) p is a non-variable position;

(ii) there is a substitution ρ such that $l\rho \approx_E l'$, $L[l'] \succ l\rho \approx r\rho$, $Vars(l\rho) \supseteq Vars(r\rho)$, $l\rho \succ r\rho$, and $C \vee L[l']_p \,||\, \phi$ is neither protected nor a clause with a succedent top variable w.r.t. any $\sigma \in Sol(\phi)$.

Lemma 11. *If an equation $l \approx r$ simplifies a clause $C \vee L[l']_p \,||\, \phi$ into $C \vee L[r\rho]_p \,||\, \phi$ as in Definition 10, then $C \vee L[l']_p \,||\, \phi$ is redundant in S modulo E, where $S = \{l \approx r, C \vee L[r\rho]_p \,||\, \phi\}$.*

Proof. Suppose that $l \approx r$ simplifies $C \vee L[l']_p \,||\, \phi$ into $C \vee L[r\rho]_p \,||\, \phi$ as in Definition 10. Then $l\rho \approx_E l'$, $L[l'] \succ l\rho \approx r\rho$, $l\rho \succ r\rho$, $Vars(l\rho) \supseteq Vars(r\rho)$, and $C \vee L[l']_p \,||\, \phi$ is neither protected nor a clause with a succedent top variable w.r.t. any $\sigma \in Sol(\phi)$. It follows that for all $\sigma \in Sol(\phi)$, we have $l\rho\sigma \approx_E l'\sigma$, and $L\sigma[l'\sigma] \succ l\rho\sigma \approx r\rho\sigma$. Let ρ'_R be a substitution such that $x\rho'_R = x\rho{\downarrow_R}$ for each $x \in Vars(l \approx r)$. Now we may infer that $\{l\rho'_R\sigma \approx r\rho'_R\sigma, C\sigma \vee L\sigma[r\rho'_R\sigma]\} \cup R^{\prec D\sigma} \cup E^{\prec D\sigma} \models D\sigma$ for all ground instances $D\sigma$ of $D := C \vee L[l']_p \,||\, \phi$ and any ground rewrite system R contained in $\succ$. Furthermore, since $Vars(l\rho) \supseteq Vars(r\rho)$, we see that for all $\sigma \in Sol(\phi)$, $l\rho'_R\sigma \approx r\rho'_R\sigma$ and $C\sigma \vee L\sigma[r\rho'_R\sigma]$ are reduced relative to $D\sigma$ by Lemma 8, and hence the conclusion follows. $\square$

The following definition extends the blocking rule in the free case (see [9]) to the modulo case, where a blocked clause does not contribute to finding a refutation during a theorem proving derivation w.r.t. $\mathcal{BP}$ (see Definition 16) starting with an initial set of unconstrained clauses.

Definition 12. (Basic E-blocking) A clause $C \,||\, \phi$ is *blocked* in S modulo E if the following conditions are met:

(i) $C \,||\, \phi$ is not a clause with a succedent top variable w.r.t. any $\tau \in Sol(\phi)$;

(ii) there is a variable $x \in Vars(C) \cap Vars(\phi)$ such that for every $\sigma \in Sol(\phi)$, there exist ground instances $C_1\sigma_1, \ldots, C_k\sigma_k$ of clauses $C_1 \,||\, \phi_1, \ldots, C_k \,||\, \phi_k$ in S reduced relative to $C\sigma$, such that $C\sigma \succ C_i\sigma_i, 1 \leq i \leq k$, and $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup E^{\prec C\sigma} \models x\sigma \approx s$ with $x\sigma \succ s$ for some ground term s.

Definition 13. (Basic E-instance) A clause $C \,||\, \phi$ is a *basic E-instance* in S modulo E if the following conditions are met:

(i) $C \,||\, \phi$ is protected;

(ii) there is a protected clause $D \,||\, \psi \in S$ such that for every ground instance $C\sigma$ (resp. $D\tau$) of $C \,||\, \phi$ (resp. $D \,||\, \psi$), there is a ground instance $D\tau$ (resp. $C\sigma$) of $D \,||\, \psi$ (resp. $C \,||\, \phi$) such that they are reduced relative to each other with $C\sigma = D\tau$.

Observe that protected clauses are produced in a restricted way (e.g. see condition 5 in the E-Parallel rule) and if two protected clauses are the same up to variable renaming, then they are basic E-instances of each other and they do not need to be distinguished.

Definition 14. (Redundancy of an inference) An inference π with conclusion $D \,||\, \phi$ is *redundant* in S modulo E (w.r.t. relative reducibility) if $D \,||\, \phi$ is blocked or a basic E-instance in S modulo E, or for every ground instance $\pi\sigma$ with maximal premise C and conclusion $D\sigma$, there exist ground instances $C_1\sigma_1, \ldots, C_k\sigma_k$

of clauses $C_1 \,||\, \phi_1, \ldots, C_k \,||\, \phi_k$ in S reduced relative to $D\sigma$, such that $C \succ C_i\sigma_i$, $1 \leq i \leq k$, and $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup R^{\prec C} \cup E^{\prec C} \models D\sigma$ for any ground rewrite system R contained in $\succ$.

The following lemma immediately follows from Definition 9 and the observation that if $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup E^{\prec C\sigma} \models C\sigma$, then $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup R^{\prec C\sigma} \cup E^{\prec C\sigma} \models C\sigma$ for any ground rewite system R contained in $\succ$, which serves as a sufficient condition for redundancy of clauses. Also, if an (unconstrained) clause C properly subsumes an (unconstrained) clause $C' \vee D$ in the classical sense, where C and C' are the same up to variable renaming, then it is easy to see that $C' \vee D$ is redundant in $\{C\}$ modulo E.

Lemma 15. *A clause $C \,||\, \phi$ is redundant in S modulo E if for every ground instance $C\sigma$, there exist ground instances $C_1\sigma_1, \ldots, C_k\sigma_k$ of clauses $C_1 \,||\, \phi_1, \ldots,$ $C_k \,||\, \phi_k$ in S reduced relative to $C\sigma$, such that $C\sigma \succ C_i\sigma_i$, $1 \leq i \leq k$, and $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup E^{\prec C\sigma} \models C\sigma$.*

Definition 16. (Theorem proving derivation) A *theorem proving derivation* is a sequence of sets of clauses $S_0 = S, S_1, \ldots$ such that:
(i) Deduction: $S_i = S_{i-1} \cup \{C \,||\, \phi\}$ for some $C \,||\, \phi$ if it can be deduced from premises in S_{i-1} by applying an inference rule in $\mathcal{BP}$ or basic E-simplification.
(ii) Deletion: $S_i = S_{i-1} \setminus \{D \,||\, \psi\}$ for some $D \,||\, \psi$ if it is not protected, and is redundant or blocked in S_{i-1} modulo E.

The set S_∞ of *persistent clauses* is defined as $\bigcup_i (\bigcap_{j \geq i} S_j)$, which is called the *limit* of the derivation. A theorem proving derivation $S_0, S_1, S_2, \ldots$ is *fair* [6] w.r.t. the inference system $\mathcal{BP}$ if every inference π by $\mathcal{BP}$ with premises in S_∞ is redundant in $\bigcup_j S_j$ modulo E.

Definition 17. (Saturation w.r.t. relative reducibility) Given an equational theory E, we say that S modulo E is *saturated* under $\mathcal{BP}$ w.r.t. relative reducibility if every inference by $\mathcal{BP}$ with premises in S is redundant in S modulo E.

In what follows, we say that a clause $C \,||\, \phi$ is *non-protected redundant* (resp. *non-protected blocked*) in S modulo E if it is not protected and is redundant (resp. blocked) in S modulo E. (If $C \,||\, \phi$ is non-protected redundant in S modulo E, then we also say that each ground instance $C\sigma$ of $C \,||\, \phi$ is *non-protected redundant* in S modulo E.)

Lemma 18. *(i) If $S \subseteq S'$, then any clause which is non-protected redundant or non-protected blocked in S modulo E is also non-protected redundant or non-protected blocked in S' modulo E.*
(ii) Let $S \subseteq S'$ such that all clauses in $S' \setminus S$ are non-protected redundant or non-protected blocked in S' modulo E. Then (ii.1) any clause which is non-protected redundant or non-protected blocked in S' modulo E is also non-protected redundant or non-protected blocked in S modulo E, and (ii.2) any inference which is redundant in S' modulo E is also redundant in S modulo E.

Proof. The proof of part (i) is immediate, so we only prove part (ii).

Suppose that a clause $C \,||\, \phi$ is non-protected redundant or non-protected blocked in S' modulo E, and let $C\sigma$ be a ground instance of $C \,||\, \phi$. Then there exist ground instances $C_1\sigma_1, \ldots, C_k\sigma_k$ of clauses $C_1 \,||\, \phi_1, \ldots, C_k \,||\, \phi_k$ in S' reduced relative to $C\sigma$, such that $C\sigma \succ C_i\sigma_i$, $1 \leq i \leq k$, and $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup R^{\prec C\sigma} \cup E^{\prec C\sigma} \models C\sigma$ for any ground rewrite system R contained in $\succ$, or $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup E^{\prec C\sigma} \models x\sigma \approx s$ with $x \in Vars(C) \cap Vars(\phi)$ and $x\sigma \succ s$ for some term s. (If $C \,||\, \phi$ is both non-protected redundant and non-protected blocked in S' modulo E, then we use the latter case in the above.) We will choose the minimal such set $\{C_1\sigma_1, \ldots, C_k\sigma_k\}$ w.r.t. $\succ$. Now we claim that all $C_i\sigma_i$ are neither non-protected redundant nor ground instances of non-protected blocked clauses in S' modulo E, which shows that $C \,||\, \phi$ is non-protected redundant or non-protected blocked in S modulo E. Suppose first, to the contrary, that some $C_j\sigma_j$ is non-protected redundant in S' modulo E w.r.t. the ground instances $D_1\tau_1, \ldots, D_n\tau_n$ of clauses $D_1 \,||\, \psi_1, \ldots, D_n \,||\, \psi_n$ in S' reduced relative to $C_j\sigma_j$ with $C_j\sigma_j \succ D_i\tau_i$, $1 \leq i \leq n$. Let $U := \{C_1\sigma_1, \ldots, C_{j-1}\sigma_{j-1}, D_1\tau_1, \ldots, D_n\tau_n, C_{j+1}\sigma_{j+1}, \ldots, C_k\sigma_k\}$. Then we have $U \cup R^{\prec C\sigma} \cup E^{\prec C\sigma} \models C\sigma$ for any ground rewrite system R contained in $\succ$, or $U \cup E^{\prec C\sigma} \models x\sigma \approx s$, which contradicts our minimal choice of $\{C_1\sigma_1, \ldots, C_k\sigma_k\}$. Similarly, if some $C_j\sigma_j$ is a ground instance of a non-protected blocked clause in S' modulo E, then a contradiction can be derived with our minimal choice of $\{C_1\sigma_1, \ldots, C_k\sigma_k\}$.

Next, suppose an inference π with conclusion $D \,||\, \psi$ is redundant in S' modulo E. The proof is immediate when $D \,||\, \psi$ is a basic E-instance in S' modulo E, so we assume that $D \,||\, \psi$ is not a basic E-instance in S' modulo E. Let $\pi\sigma$ be a ground instance of π such that C is the maximal premise and $D\sigma$ is the conclusion of $\pi\sigma$. Then there exist ground instances $D_1\sigma_1, \ldots, D_k\sigma_k$ of clauses $D_1 \,||\, \psi_1, \ldots, D_k \,||\, \psi_k$ in S' reduced relative to $D\sigma$, such that $C \succ D_i\sigma_i$, $1 \leq i \leq k$, and $\{D_1\sigma_1, \ldots, D_k\sigma_k\} \cup R^{\prec C} \cup E^{\prec C} \models D\sigma$ for any ground rewrite system R contained in $\succ$, or $\{D_1\sigma_1, \ldots, D_k\sigma_k\} \cup E^{\prec D\sigma} \models x\sigma \approx s$ with $x \in Vars(D) \cap Vars(\psi)$ and $x\sigma \succ s$ for some term s. We will choose the minimal such set $\{D_1\sigma_1, \ldots, D_k\sigma_k\}$ w.r.t. $\succ$. As above, we may infer that all $D_i\sigma_i$ are neither non-protected redundant nor ground instances of non-protected blocked clauses in S' modulo E, and hence $\pi\sigma$ is redundant in S modulo E. $\square$

Lemma 19. *Let $S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathcal{BP}$ such that S_0 is a set of unconstrained clauses. Then S_∞ modulo E is saturated under $\mathcal{BP}$ w.r.t. relative reducibility.*

Proof. If S_∞ contains the empty clause, then it is immediate that S_∞ modulo E is saturated under $\mathcal{BP}$ w.r.t. relative reducibility, so we assume that the empty clause is not in S_∞.

If a clause $C \,||\, \phi$ is deleted in a theorem proving derivation, then we see that it is non-protected redundant or non-protected blocked in some S_j modulo E. It is also non-protected redundant or non-protected blocked in $\bigcup_j S_j$ modulo E by Lemma 18(i). Similarly, every clause in $\bigcup_j S_j \setminus S_\infty$ is non-protected redundant or non-protected blocked in $\bigcup_j S_j$ modulo E.

Now by fairness of the derivation, every inference π by $\mathcal{BP}$ with premises in S_∞ is redundant in $\bigcup_j S_j$ modulo E. Then by Lemma 18(ii.2) and the above, π is also redundant in S_∞ modulo E. Thus, S_∞ modulo E is saturated under $\mathcal{BP}$ w.r.t. relative reducibility. $\square$

6 Refutational completeness

The soundness of $\mathcal{BP}$ (w.r.t. a fair theorem proving derivation) is straightforward, i.e., $S_i \cup E \models S_{i+1} \cup E$ for all $i \geq 0$. If the empty clause is in some S_j, then $S_0 \cup E$ is unsatisfiable by the soundness of $\mathcal{BP}$. The following theorem states that $\mathcal{BP}$ with our contraction rules (i.e. basic E-simplification and basic E-blocking) is refutationally complete. In order to prove the following theorem, we adapt a variant of *model construction techniques* [7–9,20,26]. In this section, we assume that the equality is the only predicate by expressing other predicates (i.e. predicate terms) as (predicate) equations as discussed in Section 4.

Theorem 20. *Let $S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathcal{BP}$ such that S_0 is a set of unconstrained clauses. Then $S_0 \cup E$ is unsatisfiable if and only if the empty clause is in some S_j.*

Definition 21. (Model construction) Let S be a set of (constrained) clauses. We use induction on $\succ$ to define the sets $Rules_C$, R_C, E_C, and I_C, for all ground instances C of clauses in S. Let C be such a ground instance of a clause in S and suppose that $Rules_{C'}$ has been defined for all ground instances C' of clauses in S for which $C \succ C'$. Then we define by $R_C = \bigcup_{C \succ C'} Rules_{C'}$ and by E_C the set of ground instances $e_1 \approx e_2$ of equations in E, such that $C \succ e_1 \approx e_2$, and e_1 and e_2 are both irreducible by R_C. We also define by I_C the interpretation $(R_C \cup E_C)^*$ (i.e. the least congruence containing $R_C \cup E_C$).

Now let $C := D \vee s \approx t$ be a reduced ground instance of a clause in S w.r.t. R_C such that C is not an instance of a clause with a selected literal. Then C produces the set of ground rewrite rules $Rules_C = \{u \Rightarrow t \,|\, u \approx_E s$ and u is irreducible by $R_C\}$ if the following conditions are met: (1) $I_C \not\models C$ (resp. $I_C \not\models D$) if C is an instance of a non-protected clause (resp. protected clause), (2) $I_C \not\models t \approx t'$ for every $s' \approx t'$ in D with $s' \approx_E s$, (3) $s \approx t$ is reductive for C, and (4) there exists u with $u \approx_E s$ for which u is irreducible by R_C. We say that C is *productive* and *produces $Rules_C$* if it satisfies all of the above conditions. Otherwise, $Rules_C = \emptyset$. Finally, we define $R_S = \bigcup_C R_C$, $E_S = \bigcup_C E_C$, and $I_S = (R_S \cup E_S)^*$.

We may include the special non-productive ground clause $tt \approx tt$ in S for the above (inductive) definition, where $tt \approx tt$ is assumed to be greater than all ground instances of clauses in $S \cup E$ w.r.t. $\succ$ other than $tt \approx tt$ itself (see [20,26]). (If C is the strictly maximal ground instance among ground instances of clauses in S and is productive, then R_S may not include $Rules_C$ by the above inductive definition of R_C without $tt \approx tt$.) In what follows, we say that a ground instance

$\pi\sigma$ of an inference π with premises in S is *reduced* if each premise and conclusion of $\pi\sigma$ is a reduced ground instance of a clause in $S \cup E$ w.r.t. R_S, E_S.

Definition 22. (Redundancy w.r.t. R_S, E_S) A clause $C \,||\, \phi$ is *redundant* in S modulo E w.r.t. R_S, E_S if for every reduced ground instance $C\sigma$ w.r.t. R_S, E_S, there exist reduced ground instances $C_1\sigma_1, \ldots, C_k\sigma_k$ of clauses $C_1 \,||\, \phi_1 \ldots C_k \,||\, \phi_k$ in S w.r.t. R_S, E_S, such that $C\sigma \succ C_i\sigma_i$, $1 \le i \le k$, and $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup R_S^{\prec C\sigma} \cup E^{\prec C\sigma} \models C\sigma$. (In this case, we also say that each $C\sigma$ is *redundant* in S modulo E w.r.t. R_S, E_S.)

An inference π with conclusion $D \,||\, \phi$ is *redundant* in S modulo E w.r.t. R_S, E_S if $D \,||\, \phi$ is blocked or a basic E-instance in S modulo E, or for every reduced ground instance $\pi\sigma$ with maximal premise C and conclusion $D\sigma$, there exist reduced ground instances $C_1\sigma_1, \ldots, C_k\sigma_k$ of clauses $C_1 \,||\, \phi_1, \ldots, C_k \,||\, \phi_k$ in S w.r.t. R_S, E_S, such that $C \succ C_i\sigma_i$, $1 \le i \le k$, and $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup R_S^{\prec C} \cup E^{\prec C} \models D\sigma$.

Definition 23. (Saturation w.r.t. R_S, E_S) Given an equational theory E, we say that S modulo E is *saturated* under $\mathcal{BP}$ w.r.t. R_S, E_S if every inference by $\mathcal{BP}$ with premises in S is redundant in S modulo E w.r.t. R_S, E_S.

Lemma 24. *(i) There are no overlaps among the left-hand sides of rules in R_S.*
(ii) A term t is reducible by R_S if and only if it is reducible by R_S, E_S at the same position.
(iii) For every $l \Rightarrow r, s \Rightarrow t \in R_S$, if $l \approx_E s$, then r and t are the same term.
(iv) R_S/E_S is terminating.
(v) For ground terms u and v, if $I_S \models u \approx v$, then $u \downarrow_{R_S,E_S} v$.
(vi) If a ground instance $C\theta := D\theta \vee l\theta \approx r\theta$ of a clause $C \,||\, \phi := D \vee l \approx r \,||\, \phi$ is productive, then it is a reduced ground instance of $C \,||\, \phi$ w.r.t. R_S, E_S.

The proofs of (i), (ii), and (iii) in Lemma 24 follow from the construction of R_S in Definition 21. For (iv), since R_S is contained in an E-compatible reduction ordering $\succ$ on terms that is E-total on ground terms, R_S/E_S is terminating. Meanwhile, Lemma 24(v) describes the ground *Church-Rosser property* [18] of R_S, E_S. Since R_S/E_S is terminating by (iv), this shows that R_S, E_S is ground convergent modulo E_S. In the following, we assume that any saturated clause set under $\mathcal{BP}$ is obtained from an initial set of clauses without constraints.

Lemma 25. *Let S modulo E be saturated under $\mathcal{BP}$ w.r.t. R_S, E_S not containing the empty clause and let C be a reduced ground instance of a clause in S w.r.t. R_S, E_S or a ground instance of an equation in E. Then C is true in I_S. More specifically,*
(i) C is not an instance of a blocked clause in S modulo E.
(ii) If C is redundant in S modulo E w.r.t. R_S, E_S, then it is true in I_S.
(iii) If C is an instance of a clause with a selected literal, then it is true in I_S.
(iv) If C contains a maximal negative literal (w.r.t. $\succ$) and is not an instance of a clause with a selected literal, then it is true in I_S.
(v) If C is an instance of an equation in E, then it is true in I_S.

(vi) If C is an instance of a protected clause or a basic E-instance of it, then it is true in I_S.
(vii) If C is non-productive, then it is true in I_S.
(viii) If $C := C' \vee s \approx t$ is productive and produces $Rules_C$ with $s \Rightarrow t \in Rules_C$, then C' is false and C is true in I_S.

Proof. We use induction on $\succ$ and assume that the properties (i)–(viii) hold for every D with $C \succ D$, where D is a reduced ground instance of a clause in S w.r.t. R_S, E_S or a ground instance of an equation in E.

(i) Suppose to the contrary that $C := C'\sigma'$ is a reduced ground instance of some blocked clause $C' \,||\, \phi'$ in S modulo E w.r.t. R_S, E_S. (Note that C cannot be an instance of an equation in E because each equation in E is unconstrained.) Then there exist reduced ground instances $C_1\sigma_1, \ldots, C_k\sigma_k$ of clauses $C_1 \,||\, \phi_1, \ldots, C_k \,||\, \phi_k$ in S w.r.t. R_S, E_S, such that $C \succ C_i\sigma_i, 1 \leq i \leq k$, and $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup E^{\prec C} \models x\sigma' \approx s$ with some $x \in Vars(C') \cap Vars(\phi')$ and $x\sigma' \succ s$ for some term s by Definitions 7 and 12. By the induction hypothesis, we know that $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup E^{\prec C}$ is true in I_S. Now we may infer that C is a reducible ground instance of $C' \,||\, \phi'$ w.r.t. R_S, E_S by Lemma 24(v), which is a contradiction. (Note also that if an inference π by $\mathcal{BP}$ generates a blocked clause in S modulo E, then the inference π does not have a reduced ground instance $\pi\sigma$ of π w.r.t. R_S, E_S.)

(ii) Suppose that a reduced ground instance $C := C'\sigma'$ of $C' \,||\, \phi'$ is redundant in S modulo E w.r.t. R_S, E_S. Then there exist reduced ground instances $C_1\sigma_1, \ldots, C_k\sigma_k$ of clauses $C_1 \,||\, \phi_1, \ldots, C_k \,||\, \phi_k$ in S w.r.t. R_S, E_S, such that $C \succ C_i\sigma_i$, $1 \leq i \leq k$, and $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup R_S^{\prec C} \cup E^{\prec C} \models C$. By the induction hypothesis, we know that $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup E^{\prec C}$ is true in I_S. Thus, C is true in I_S.

In the remainder of the proof this lemma, we may assume that C is neither redundant nor is it a ground instance of some blocked clause in S modulo E.

(iii) If C is an instance of a clause with a selected literal, then C is a reduced ground instance of a clause of the form $C' \vee s \not\approx t \,||\, \phi \in S$ w.r.t. R_S, E_S such that $s \not\approx t$ is selected[2] in $C' \vee s \not\approx t \,||\, \phi \in S$. Let $C := C'\sigma \vee s\sigma \not\approx t\sigma$ with some $\sigma \in Sol(\phi)$.

(iii.1) If $s\sigma \approx_{E_S} t\sigma$, then $C'\sigma$ is an equality resolvent of C and the equality resolution inferences can be lifted. By saturation of S modulo E under $\mathcal{BP}$ w.r.t. R_S, E_S and the induction hypothesis, $C'\sigma$ is true in I_S. Thus, C is true in I_S.

(iii.2) If $s\sigma \not\approx_{E_S} t\sigma$, then suppose to the contrary that C is false in I_S. Then we have $I_S \models s\sigma \approx t\sigma$, which implies that $s\sigma$ or $t\sigma$ is reducible by R_S, E_S by Lemma 24(v). We assume that, without loss of generality, $s\sigma$ is reducible by R_S, E_S with some rule $l\theta \Rightarrow r\theta \in R_S$ produced by a reduced productive ground instance $D\theta \vee l\theta \approx r\theta$ of a clause $D \vee l \approx r \,||\, \psi \in S$ w.r.t. R_S, E_S for which D contains no selected literal (see Definition 21 and Lemma 24(vi)). Then $s\sigma$ is of the form $s\sigma[s'\sigma]$ with $s'\sigma \approx_{E_S} l\theta$. Now consider the following inference by

[2] We assume that if $u \not\approx v$ is selected in $D \,||\, \psi$, then $u\sigma \not\approx v\sigma$ is also selected in $D\sigma$ for each $\sigma \in Sol(\psi)$.

Basic Paramodulation:

$$\frac{D \vee l \approx r \,||\, \psi \qquad C' \vee L[s'] \,||\, \phi}{D \vee C' \vee L[r] \,||\, l \approx^?_E s' \wedge \psi \wedge \phi}$$

where L is $s[s'] \not\approx t$ and selected in the right premise. Since σ is reduced w.r.t. R_S, E_S, s' is not a variable. As all the conditions for the above inference hold, the conclusion has a ground instance $C'' := D\mu \vee C'\mu \vee s\mu[r\mu] \not\approx t\mu$ with $\mu = \sigma \cup \theta$.[3] (We assume that each clause is standardized apart and leave it to the reader to verify that C'' is a reduced ground instance of the conclusion w.r.t. R_S, E_S.) By saturation of S modulo E under $\mathcal{BP}$ and the induction hypothesis, C'' is true in I_S and $D\mu$ is false in I_S. We also know that $s\mu[r\mu] \not\approx t\mu$ is false in I_S by Lemma 24(v). This implies that $C'\mu$ is true in I_S, and hence C is true in I_S. (Observe that $C := C'\sigma \vee s\sigma \not\approx t\sigma$ and if $C'\mu$ is true in I_S, then $C'\sigma$ is also true in I_S.) Thus, we have the required contradiction.

(iv) We omit the proof of this case because it is similar to that of case (iii).

(v) First, let C be a reduced ground instance of an equation $e_1 \approx e_2 \in E$ w.r.t. R_S, E_S with the form $C = e_1\sigma \approx e_2\sigma$. If both $e_1\sigma$ and $e_2\sigma$ are irreducible by R_S, E_S, then we are done. If one of $e_1\sigma$ and $e_2\sigma$ is reducible by R_S, E_S at the top position, then they are both reducible by R_S at the top position by Lemma 24(ii), and hence C is true in I_S by Lemma 24(iii). Otherwise, we assume that, without loss of generality, $e_1\sigma$ is reducible by R_S, E_S below the top position with some rule $l\theta \Rightarrow r\theta \in R_S$ produced by a reduced productive ground instance $D\theta \vee l\theta \approx r\theta$ of a clause $D \vee l \approx r \,||\, \psi \in S$ w.r.t. R_S, E_S, where D contains no selected literal. Then $e_1\sigma$ is of the form $e_1\sigma[s'\sigma]$ with $s'\sigma \approx_{E_S} l\theta$. Now consider the following inference by E-Completion:

$$\frac{D \vee l \approx r \,||\, \psi}{D \vee e_1[r]_p \approx e_2 \,||\, l \approx^?_E s' \wedge \psi}$$

where $e_1[s']_p \approx e_2 \in E$ with $p \neq \lambda$. Since σ is reduced w.r.t. R_S, E_S, s' is not a variable. As all the conditions for the above inference hold, the conclusion has a reduced ground instance $C'' := D\mu \vee e_1\mu[r\mu]_p \approx e_2\mu$ with $\mu = \sigma \cup \theta$. By saturation of S modulo E under $\mathcal{BP}$ w.r.t. R_S, E_S and the induction hypothesis, C'' is true in I_S and $D\mu$ is false in I_S from which it follows that $e_1\mu[r\mu]_p \approx e_2\mu$ is true in I_S. This implies that $e_1\mu[s'\mu]_p \approx e_2\mu$ is true in I_S, and hence C is true in I_S.

Now if C is a reducible ground instance of an equation $e := e_1 \approx e_2 \in E$ w.r.t. R_S, E_S with the form $C := e_1\sigma \approx e_2\sigma$, then let σ' be a ground substitution such that $x\sigma' = x\sigma{\downarrow}_{R_S,E_S}$ for each $x \in Vars(e)$. Then $e\sigma'$ is a reduced ground instance of an equation in E with $C \succ e\sigma'$, and hence C is also true in I_S by the induction hypothesis.

(vi) If C is a reduced ground instance of a protected clause w.r.t. R_S, E_S, then it is of the form $C := C'\tau \vee D'\sigma\tau \vee l\sigma\tau \approx r\theta\tau$ produced by an inference by Generalized E-Parallel:

[3] All inferences by $\mathcal{BP}$ are *monotone* [8] at the ground level, in the sense that conclusion is always smaller than the main premise (w.r.t. $\succ$).

$$\frac{C' \vee s \approx t \,||\, \phi_1 \qquad D' \vee l \approx r \,||\, \phi_2}{C' \vee D'\sigma \vee l\sigma \approx r\theta \,||\, \phi_1 \wedge \phi_2}$$

where $\sigma = \{x \mapsto u[s]_p\}$ and $\theta = \{x \mapsto u[t]_p\}$ for some variable $x \in Vars(l) \cap Vars(r)$ with $x \notin Vars(\phi_2)$, $e_1[u] \approx e_2 \in E$, and some position p. (Note that p is simply the top position for the E-Parallel rule.) Let θ' be a substitution such that $x\theta' = x\theta{\downarrow_{R_S,E_S}}$. Then we have $\{C'\tau \vee s\tau \approx t\tau, D'\theta'\tau \vee l\theta'\tau \approx r\theta'\tau\} \cup R_S^{\prec C} \cup E^{\prec C} \models C$, where $C'\tau \vee s\tau \approx t\tau$ and $D'\theta'\tau \vee l\theta'\tau \approx r\theta'\tau$ are smaller than C (w.r.t. $\succ$), and are reduced ground instances of $C' \vee s \approx t \,||\, \phi_1$ and $D' \vee l \approx r \,||\, \phi_2$, respectively, w.r.t. R_S, E_S. By the induction hypothesis, we may infer that C is redundant in S modulo E w.r.t. R_S, E_S, and hence is true in I_S by case (ii). If C is a reduced ground instance of a basic E-instance in S modulo E w.r.t. R_S, E_S, then the proof is almost analogous to the above and is omitted. (Note that protected clauses in S modulo E are redundant in S modulo E w.r.t. R_S, E_S, but inference with them are not. For comparison, the interested reader may refer to [7], where extended clauses are redundant in S modulo AC, but inferences with them are not.)

(vii) If C is non-productive, then we assume that C is neither an instance of a clause with a selected literal nor an instance of an equation in E nor an instance of a protected clause (or its basic E-instance) nor does it contain a maximal negative literal. Otherwise, we are done by (iii), (iv), (v), or (vi). Then C is a reduced ground instance of a clause of the form $C' \vee s \approx t \,||\, \phi \in S$ w.r.t. R_S, E_S with $C := C'\sigma \vee s\sigma \approx t\sigma$, such that $s\sigma \approx t\sigma$ is maximal in C for some $\sigma \in Sol(\phi)$. If $s\sigma \approx_{E_S} t\sigma$, then we are done because $I_S \models C$. Therefore, we assume that, without loss of generality, $s\sigma \succ t\sigma$. Since C is non-productive, this must be because (at least) one of the conditions in Definition 21 does not hold. If condition (1) does not hold, then $I_C \models C$ and we have $I_S \models C$ by construction of I_S. Therefore, we assume that condition (1) holds. If condition (1) holds but condition (2) does not hold, then $C'\sigma$ is of the form $C'\sigma := D'\sigma \vee s'\sigma \approx t'\sigma$ with $s\sigma \approx_{E_S} s'\sigma$ and $I_C \models t\sigma \approx t'\sigma$. It follows that we also have $I_S \models t\sigma \approx t'\sigma$ by construction of I_S in Definition 21. Now consider the following inference by E-Factoring:

$$\frac{D' \vee s \approx t \vee s' \approx t' \,||\, \phi}{D' \vee t \not\approx t' \vee s' \approx t' \;\,||\, s \approx^?_E s' \wedge \phi}$$

Since all the conditions for the above inference hold, the conclusion has a reduced ground instance $C'' := D'\sigma \vee t\sigma \not\approx t'\sigma \vee s'\sigma \approx t'\sigma$ w.r.t. R_S, E_S. (We leave it to the reader to verify that C'' is a reduced ground instance of the conclusion w.r.t. R_S, E_S.) By saturation of S modulo E under $\mathcal{BP}$ w.r.t. R_S, E_S and the induction hypthesis, C'' is true in I_S. Since $t\sigma \not\approx t'\sigma$ is false in I_S, we may infer that C is true in I_S. Suppose that conditions (1) and (2) hold but condition (3) does not hold. Then $s\sigma \approx t\sigma$ is only maximal in C, so we are in the previous case. (Either condition (1) does not hold (and condition (2) does not hold, either) or condition (1) holds but condition(2) does not hold.) Now we assume that conditions (1)–(3) hold but condition (4) does not hold. Then $s\sigma$ is reducible by some rule $l\theta \Rightarrow r\theta \in R_C$ produced by a reduced productive ground instance $D\theta \vee l\theta \approx r\theta$ of a clause $D \vee l \approx r \,||\, \psi \in S$ w.r.t. R_S, E_S for which D contains no selected literal. By construction of R_S, we also have $l\theta \Rightarrow r\theta \in R_S$. Then $s\sigma$ is of the form $s\sigma[s'\sigma]$ with $s'\sigma \approx_{E_S} l\theta$. Since σ is reduced w.r.t. R_S, E_S, s' cannot be a variable. Similarly to (iii.2), we consider the inference by Basic Paramodulation with premises $D \vee l \approx r \,||\, \psi$ and $C' \vee s[s'] \approx t \,||\, \phi$ and conclusion $D \vee C' \vee s[r] \approx t \,||\, l \approx^?_E s' \wedge \psi \wedge \phi$. The conclusion has a ground instance $C'' := D\mu \vee C'\mu \vee s\mu[r\mu] \approx t\mu$ with $\mu = \sigma \cup \theta$. (We leave it to the reader to verify that C'' is a reduced ground instance of the conclusion w.r.t. R_S, E_S.) By saturation of S modulo E under $\mathcal{BP}$ w.r.t. R_S, E_S and the induction hypothesis, C'' is true in I_S and $D\mu$ is false in I_S, so we may infer that C is true in I_S.

(viii) Suppose that $C := C' \vee s \approx t$ is productive and produces $Rules_C$ with $s \Rightarrow t \in Rules_C$. Then C is not an instance of a clause with a selected literal and is true in I_S by construction of I_S. We show that C' is false in I_S. Let $C' := \Gamma \rightarrow \Delta$. We have $I_C \not\models C'$ by Definition 21, which means that $I_C \cap \Delta = \emptyset$, $I_C \supseteq \Gamma$, and hence $I_S \supseteq \Gamma$. It remains to show that $I_S \cap \Delta = \emptyset$. For each rule $l' \Rightarrow r' \in R_S \setminus R_C$, it is not possible to order-reduce any term occurring in Δ with the rule since $l' \succeq s$ and s is maximal in C. The only remaining possibility of $I_S \cap \Delta \neq \emptyset$ is that there is some equation $s' \approx t'$ in Δ with $s \approx_{E_S} s'$ and $I_C \models t \approx t'$, which is not the case by condition (2) in Definition 21. □

We leave it to the reader to verify the following lemma using the definitions of redundancy of an inference w.r.t. relative reducibility and w.r.t. R_S, E_S, along with Lemma 19.

Lemma 26. *Let $S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathcal{BP}$ such that S_0 is a set of unconstrained clauses. Then S_∞ modulo E is saturated under $\mathcal{BP}$ w.r.t. $R_{S_\infty}, E_{S_\infty}$.*

Theorem 27. *Let $S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathcal{BP}$ such that S_0 is a set of unconstrained clauses. If S_∞ does not contain the empty clause, then $I_{S_\infty} \models S_0 \cup E$ (i.e., $S_0 \cup E$ is satisfiable).*

Proof. By Lemma 26, we know that S_∞ modulo E is saturated under $\mathcal{BP}$ w.r.t. $R_{S_\infty}, E_{S_\infty}$. Let C be a ground instance of an equation in E or a ground instance of a clause C' in S_0. By Lemma 25(v), if C is a ground instance of an equation in E, then it is true in I_{S_∞}. Therefore, we assume that C is not a ground instance of an equation in E. Suppose first that $C := C'\sigma'$ is a reduced ground instance of $C' \in S_0$ w.r.t. $R_{S_\infty}, E_{S_\infty}$. Then there are two cases to consider. If $C' \in S_\infty$, then C is true in I_{S_∞} by Lemma 25. Otherwise, if $C' \notin S_\infty$, then C' is (non-protected) redundant in some S_j modulo E w.r.t. relative reducibility because $C' \in S_0$ (with the empty constraint) is neither protected nor can it be a blocked clause in some S_j modulo E. Thus, C' is (non-protected) redundant in $\bigcup_j S_j$ modulo E w.r.t. relative reducibility, and hence is (non-protected) redundant in S_∞ modulo E w.r.t. relative reducibility by Lemma 18. It follows that there exist ground instances $C_1\sigma_1, \ldots, C_k\sigma_k$ of clauses $C_1 \,||\, \phi_1, \ldots, C_k \,||\, \phi_k$ in S_∞ reduced relative to C, such that $C \succ C_i\sigma_i$, $1 \leq i \leq k$, and $\{C_1\sigma_1, \ldots, C_k\sigma_k\} \cup R^{\prec C} \cup E^{\prec C} \models C$ for any ground rewrite system R contained in $\succ$. Since C is a reduced ground instance of C' w.r.t. $R_{S_\infty}, E_{S_\infty}$, we see that $C_i\sigma_i$, $1 \leq i \leq k$, are also reduced ground instances w.r.t. $R_{S_\infty}, E_{S_\infty}$ by Definition 7 and are true in I_{S_∞} by Lemma 25. Similarly, $R_{S_\infty}^{\prec C}$ and $E^{\prec C}$ are true in I_{S_∞} by Lemma 25, and hence we may infer that C is also true in I_{S_∞}.

Now suppose that $C := C'\sigma'$ is a reducible ground instance of $C' \in S_0$ w.r.t. $R_{S_\infty}, E_{S_\infty}$. Let σ'' be a ground substitution such that $x\sigma'' = x\sigma'\downarrow_{R_{S_\infty}, E_{S_\infty}}$ for each $x \in Vars(C')$. Since $C'\sigma''$ is a reduced ground instance of $C' \in S_0$ w.r.t. $R_{S_\infty}, E_{S_\infty}$, $C'\sigma''$ is true in I_{S_∞} by the previous paragraph, and hence C is also true in I_{S_∞}. $\square$

We may now present the proof that $\mathcal{BP}$ with our contraction rules is refutationally complete.

Proof of Theorem 20 Let $S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathcal{BP}$ such that S_0 is a set of unconstrained clauses. If the empty clause is in some S_j, then $S_0 \cup E$ is unsatisfiable by the soundness of $\mathcal{BP}$. Otherwise, if the empty clause is not in S_k for all k, then by the soundness of $\mathcal{BP}$, S_∞ does not contain the empty clause, and hence $S_0 \cup E$ is satisfiable by Theorem 27.

7 Conclusion

We have presented a basic paramodulation calculus modulo and provided a framework for equational theorem proving modulo equational theories E satisfying some properties of E using constrained clauses, where a constrained clause may schematize a set of unconstrained clauses by keeping E-unification problems in its constraint part. Our results imply that we can deal uniformly with different equational theories E in our equational theorem proving modulo framework. We only need a single refutational completeness proof for our basic paramodulation calculus modulo E for different equational theories E.

Our contraction techniques (i.e. basic E-simplification and basic E-blocking) for constrained clauses can also be applied uniformly for different equational theories E satisfying some properties of E in our equational theorem proving modulo framework. Since a constrained clause may schematize a set of unconstrained clauses, the simplification or deletion of a constrained clause may correspond to the simplification or deletion of a set of unconstrained clauses. We have proposed a saturation procedure for constrained clauses based on relative reducibility and showed the refutational completeness of our inference system using a saturated clause set (w.r.t. $\succ$).

Some possible improvements remain to be done. One of the main issues is the broadening the scope of our equational theorem proving modulo E to more equational theories E. This can be achieved by dropping or weakening some ordering requirements of $\succ$ (e.g. monotonicity of $\succ$) for a basic paramodulation calculus modulo E, while maintaining the refutational completeness of the calculus (cf. [10]). This can also be achieved by finding suitable E-compatible orderings for more equational theories E. In fact, we provided an E-compatible simplification ordering $\succ$ on terms that is E-total on ground terms for finite permutation theories E in [16], which allows us to provide a refutationally complete equational theorem proving with built-in permutation theories using the results of this paper. Since permutations play an important role in mathematics and many fields of science including computer science, we believe that developing applications for equational theorem proving with built-in permutation theories is another promising future research direction.

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] Franz Baader. Combination of compatible reduction orderings that are total on ground terms. In G. Winskel, editor, *Proceedings of the Twelfth Annual IEEE Symposium on Logic in Computer Science*, pages 2–13, Warsaw, Poland, 1997. IEEE Computer Society Press.

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

[6] Leo Bachmair and Harald Ganzinger. Rewrite-based Equational Theorem Proving with Selection and Simplification. *J. Log. Comput.*, 4(3):217–247, 1994.

[7] Leo Bachmair and Harald Ganzinger. Associative-commutative superposition. In N. Dershowitz and N. Lindenstrauss, editors, *Conditional and Typed Rewriting Systems*, pages 1–14, Berlin, Heidelberg, 1995. Springer.

[8] Leo Bachmair and Harald Ganzinger. Equational Reasoning in Saturation-Based Theorem Proving. In W. Bibel and P. Schmitt, editors, *Automated Deduction. A basis for applications*, Volume I, chapter 11, page 353–397. Kluwer, Dordrecht, Netherlands, 1998.

[9] Leo Bachmair, Harald Ganzinger, Christopher Lynch, and Wayne Snyder. Basic Paramodulation. *Information and Computation*, 121(2):172 – 192, 1995.

[10] Miquel Bofill and Albert Rubio. Paramodulation with Non-Monotonic Orderings and Simplification. *Journal of Automated Reasoning*, 50:51–98, 2013.

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

[12] Gilles Dowek. Polarized Resolution Modulo. In C. S. Calude and V. Sassone, editors, *Theoretical Computer Science*, pages 182–196, Berlin, Heidelberg, 2010. Springer.

[13] Gilles Dowek, Thérèse Hardin, and Claude Kirchner. Theorem Proving Modulo. *Journal of Automated Reasoning*, 31(1):33–72, 2003.

[14] F. Durán, S. Eker, S. Escobar, N. Martí-Oliet, J. Meseguer, and C. Talcott. Associative Unification and Symbolic Reasoning Modulo Associativity in Maude. In V. Rusu, editor, *Rewriting Logic and Its Applications*, pages 98–114, Cham, 2018. Springer.

[15] Santiago Escobar, Ralf Sasse, and José Meseguer. Folding variant narrowing and optimal variant termination. *The Journal of Logic and Algebraic Programming*, 81(7):898 – 928, 2012.

[16] Dohan Kim and Christopher Lynch. An RPO-based ordering modulo permutation equations and its applications to rewrite systems. In *6th International Conference on Formal Structures for Computation and Deduction, FSCD 2021, Buenos Aires, Argentina (Virtual Conference), July 17–24, to appear*, volume 195, pages 19:1–19:17. LIPIcs, 2021. preprint: `http://people.clarkson.edu/~dohkim/tech_reports/ERPO.pdf`.

[17] Dohan Kim, Christopher Lynch, and Paliath Narendran. Reviving Basic Narrowing Modulo. In A. Herzig and A. Popescui, editors, *Frontiers of Combining Systems*, pages 313–329, Cham, Switzerland, 2019. Springer.

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

[19] Robert Nieuwenhuis and Albert Rubio. Basic superposition is complete. In B. Krieg-Brückner, editor, *ESOP '92*, pages 371–389, Berlin, Heidelberg, 1992. Springer.

[20] Robert Nieuwenhuis and Albert Rubio. Paramodulation with Built-in AC-Theories and Symbolic Constraints. *Journal of Symbolic Computation*, 23(1):1 – 21, 1997.

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

[22] G. Robinson and L. Wos. Paramodulation and theorem-proving in first-order theories with equality. In B. Meltzer and D. Michie, editors, *Machine Intelligence 4*, pages 133–150. American Elsevier, New York, 1969.

[23] J. A. Robinson. A machine-oriented logic based on the resolution principle. *J. ACM*, 12(1):23–41, 1965.

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

[25] Laurent Vigneron. Associative-Commutative Deduction with Constraints. In A. Bundy, editor, *Automated Deduction - CADE-12*, pages 530–544, Berlin, 1994. Springer.

[26] Ulrich Wertz. First-order theorem proving modulo equations. Technical Report MPI-I-92-216, Max-Planck-Institut für Informatik, Saarbrücken, 1992.