Mathematical Structures in Computer Science (2024), 1–24
doi:10.1017/S0960129524000112

PAPER

Equational theorem proving for clauses over strings

Dohan Kim

Department of Computer Science, University of Innsbruck, Innsbruck, Austria
Email: dohan.kim@uibk.ac.at

(Received 1 August 2023; revised 10 December 2023; accepted 21 March 2024)

Abstract

Although reasoning about equations over strings has been extensively studied for several decades, little research has been done for equational reasoning on general clauses over strings. This paper introduces a new superposition calculus with strings and present an equational theorem proving framework for clauses over strings. It provides a saturation procedure for clauses over strings and show that the proposed superposition calculus with contraction rules is refutationally complete. In particular, this paper presents a new decision procedure for solving word problems over strings and provides a new method of solving unification problems over strings w.r.t. a set of conditional equations R over strings if R can be finitely saturated under the proposed inference system with contraction rules.

Keywords: Equational theorem proving; superposition calculus; conditional completion; string rewriting; unification

1. Introduction

Strings are fundamental objects in mathematics and many fields of science, including computer science and biology. Reasoning about equations over strings has been widely studied in the context of string rewriting systems, formal language theory, word problems in semigroups, monoids, and groups (Book and Otto, 1993; Epstein et al., 1992), etc. Roughly speaking, reasoning about equations over strings replaces equals by equals w.r.t. a given reduction ordering $\succ$. For example, if we have two equations over strings $u_1u_2u_3 \approx s$ and $u_2 \approx t$ with $u_1u_2u_3 \succ s$ and $u_2 \succ t$, where u_2 is not the empty string, then we may infer the equation $u_1tu_3 \approx s$ by replacing u_2 in $u_1u_2u_3 \approx s$ with t. Meanwhile, if we have two equations over strings $u_1u_2 \approx s$ and $u_2u_3 \approx t$ with $u_1u_2 \succ s$ and $u_2u_3 \succ t$, where u_2 is not the empty string, then we should also be able to infer the equation $u_1t \approx su_3$. This can be done by concatenating u_3 to both sides of $u_1u_2 \approx s$ (i.e., $u_1u_2u_3 \approx su_3$) and then replacing u_2u_3 in $u_1u_2u_3 \approx su_3$ with t. Here, the *monotonicity property* of equations over strings is assumed, that is, $s \approx t$ implies $usv \approx utv$ for strings s, t, u, and v.[1]

This reasoning about equations over strings is the basic ingredient for *completion* (Book and Otto, 1993; Holt et al., 2005) of string rewriting systems. A completion procedure (Book and Otto, 1993) attempts to construct a finite convergent string rewriting system, where a finite convergent string rewriting system provides a decision procedure for its corresponding equational theory.

Unlike reasoning about equations over strings, equational reasoning on general clauses over strings has not been well studied, where clauses are often the essential building blocks for logical statements.

This paper proposes a superposition calculus and an equational theorem proving procedure with clauses over strings. The results presented here generalize the results about completion of equations over strings (Book and Otto, 1993; Holt et al., 2005). Throughout this paper, the

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

monotonicity property of equations over strings is assumed and considered in the proposed inference rules. This assumption is natural and common to equations over strings occurring in algebraic structures (e.g., semigroups and monoids), formal language theory, etc. The *cancelation property* of equations over strings is not assumed, that is, $su \approx tu$ implies $s \approx t$ for strings s, t, and a nonempty string u (cf. *non-cancellative* (Book and Otto, 1993) algebraic structures).

Now, the proposed superposition inference rule is given roughly as follows:

$$\textbf{Superposition:} \quad \frac{C \vee u_1 u_2 \approx s \qquad D \vee u_2 u_3 \approx t}{C \vee D \vee u_1 t \approx s u_3}$$

if u_2 is not the empty string, and $u_1 u_2 \succ s$ and $u_2 u_3 \succ t$.

Intuitively speaking, using the monotonicity property, $C \vee u_1 u_2 u_3 \approx s u_3$ can be obtained from the left premise $C \vee u_1 u_2 \approx s$. Then the above inference by Superposition can be viewed as an application of a conditional rewrite rule $D \vee u_2 u_3 \approx t$ to $C \vee u_1 u_2 u_3 \approx s u_3$, where $u_2 u_3$ in $C \vee u_1 u_2 u_3 \approx s u_3$ is now replaced by t, and D is appended to the conclusion. (Here, D can be viewed as consisting of the positive and negative conditions.) Note that both u_1 and u_3 can be the empty string in the Superposition inference rule. These steps are combined into a single Superposition inference step. For example, suppose that we have three clauses 1: $ab \approx d$, 2: $bc \approx e$, and 3: $ae \not\approx dc$. We use the Superposition inference rule with 1 and 2, and obtain 4: $ae \approx dc$ from which we derive a contradiction with 3. The details of the inference rules in the proposed inference system are discussed in Section 3.

The proposed superposition calculus is based on the simple string matching methods and the efficient length-lexicographic ordering instead of using equational unification and the more complex orderings, such as the lexicographic path ordering (LPO) (Dershowitz and Plaisted, 2001) and Knuth–Bendix ordering (KBO) (Baader and Nipkow, 1998).

This paper shows that a clause over strings can be translated into a clause over first-order terms, which allows one to use the existing notion of redundancy in the literature (Bachmair and Ganzinger, 1994; Nieuwenhuis and Rubio, 2001) for clauses over strings. Based on the notion of redundancy, one may delete redundant clauses using the contraction rules (i.e., Simplification, Subsumption, and Tautology) during an equational theorem proving derivation in order to reduce the search space for a refutation.

The *model construction techniques* (Bachmair and Ganzinger, 1994; Nieuwenhuis and Rubio, 2001) is adapted for the refutational completeness of the proposed superposition calculus. This paper also uses a Herbrand interpretation by translating clauses over strings into clauses over first-order terms, where each nonground first-order clause represents all its ground instances. Note that this translation is not needed for the proposed inference system itself.

The proposed equational theorem proving framework with clauses over strings also provides a new decision procedure for solving word problems over strings and a new approach to solving unification problems over strings w.r.t. a conditional equational theory R over strings if R can be finitely saturated under the proposed inference system with contraction rules.

A preliminary version of this paper was presented in the proceedings of 17th International Workshop on Logical and Semantic Frameworks with Applications (Kim, 2022). Among others, Section 7 has been added to discuss the new results of unification in conditional equational theories over strings. The present paper also includes a new method of deriving an equivalent convergent (unconditional) string rewriting system from a conditional equational theory R over strings if R can be finitely saturated under the proposed inference system with contraction rules.

2. Preliminaries

It is assumed that the reader has some familiarity with equational theorem proving (Bachmair and Ganzinger, 1994; Nieuwenhuis and Rubio, 2001) and string rewriting systems

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

(Book and Otto, 1993; Holt et al., 2005; Kapur and Narendran, 1985). The notion of conditional equations and Horn clauses are discussed in Dershowitz (1991).

An *alphabet* Σ is a finite set of symbols (or letters). The set of all strings of symbols over Σ is denoted Σ^* with the empty string λ.

If $s \in \Sigma^*$, then the *length* of s, denoted $|s|$, is defined as follows: $|\lambda| := 0$, $|a| := 1$ for each $a \in \Sigma$, and $|sa| := |s| + 1$ for $s \in \Sigma^*$ and $a \in \Sigma$.

A *multiset* is an unordered collection with possible duplicate elements. We denote by $M(x)$ the number of occurrences of an object x in a multiset M.

An *equation* is an expression $s \approx t$, where s and t are strings, that is, $s, t \in \Sigma^*$. A *literal* is either a positive equation L, called a *positive literal*, or a negative equation $\neg L$, called a *negative literal*. We also write a negative literal $\neg(s \approx t)$ as $s \not\approx t$. We identify a positive literal $s \approx t$ with the multiset $\{\{s\}, \{t\}\}$ and a negative literal $s \not\approx t$ with the multiset $\{\{s, t\}\}$. A *clause* (over Σ^*) 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 $\Gamma \to \Delta$, where $\Gamma = A_1 \wedge \cdots \wedge A_m$ and $\Delta = B_1 \vee \cdots \vee B_n$. We say that Γ is the *antecedent* and Δ is the *succedent* of clause $\Gamma \to \Delta$. A *Horn clause* is a clause with at most one positive literal. The *empty clause*, denoted $\square$, is the clause containing no literals.

A *conditional equation* is a clause of the form $(s_1 \approx t_1 \wedge \cdots \wedge s_n \approx t_n) \to l \approx r$. If $n = 0$, a conditional equation is simply an equation. A conditional equation is naturally represented by a Horn clause. A *conditional equational theory* is a set of conditional equations.

Any ordering $\succ_S$ on a set S can be extended to an ordering $\succ_S^{mul}$ on finite multisets over S as follows: $M \succ_S^{mul} N$ if (i) $M \neq N$ and (ii) whenever $N(x) > M(x)$ then $M(y) > N(y)$, for some y such that $y \succ_S x$.

Given a multiset M and an ordering $\succ$ on M, we say that x is *maximal* (resp. *strictly maximal*) in M if there is no $y \in M$ (resp. $y \in M \setminus \{x\}$) with $y \succ x$ (resp. $y \succ x$ or $x = y$).

An ordering $>$ on Σ^* is *terminating* if there is no infinite chain of strings $s > s_1 > s_2 > \cdots$ for any $s \in \Sigma^*$. An ordering $>$ on Σ^* is *admissible* if $u > v$ implies $xuy > xvy$ for all $u, v, x, y \in \Sigma^*$. An ordering $>$ on Σ^* is a *reduction ordering* if it is terminating and admissible.

The *lexicographic ordering* $\succ_{lex}$ induced by a total precedence ordering $\succ_{prec}$ on Σ ranks strings of the same length in Σ^* by comparing the letters in the first index position where two strings differ using $\succ_{prec}$. For example, if $a = a_1 a_2 \cdots a_k$ and $b = b_1 b_2 \cdots b_k$, and the first index position where a and b are differ is i, then $a \succ_{lex} b$ if and only if $a_i \succ_{prec} b_i$.

The *length-lexicographic ordering* $\succ$ on Σ^* is defined as follows: $s \succ t$ if and only if $|s| > |t|$, or they have the same length and $s \succ_{lex} t$ for $s, t \in \Sigma^*$. If Σ and $\succ_{prec}$ are fixed, then it is easy to see that we can determine whether $s \succ t$ for two (finite) input strings $s \in \Sigma^*$ and $t \in \Sigma^*$ in $O(n)$ time, where $n = |s| + |t|$. The length-lexicographic ordering $\succ$ on Σ^* is a reduction ordering. We also write $\succ$ for a multiset extension of $\succ$ if it is clear from context. In this paper, we assume that a total precedence $\succ_{prec}$ (simply written $\succ$) on Σ is always given, unless otherwise stated.

A *string rewriting system* R (over Σ^*) is a subset of $\Sigma^* \times \Sigma^*$. Let R be a string rewriting system over Σ^*. Then, $u \to_R v$ if there exist $x, y \in \Sigma^*$ such that $u = xly$ and $v = xry$ and $l \to r \in R$. By $\to_R^*$ (resp. $\overset{*}{\leftrightarrow}_R$), we denote the reflexive and transitive closure of R (resp. the reflexive, symmetric, and transitive closure of R). Note that the relation $\overset{*}{\leftrightarrow}_R$ is a congruence relation w.r.t. the concatenation of strings over Σ^*, which is called the *Thue congruence* associated with R.

$\to_R$ is *confluent* if for all $s, t, u \in \Sigma^*$ with $s \to_R^* t$ and $s \to_R^* u$ there exists some $w \in \Sigma^*$ such that $t \to_R^* w$ and $u \to_R^* w$.

$\to_R$ is *terminating* if there is no infinite sequence of strings $s_i \in \Sigma^*$ with $s_0 \to_R s_1 \to_R \cdots$.

A string rewriting system R (over Σ^*) is *convergent* if $\to_R$ is both confluent and terminating.

We say that $\approx$ has the *monotonicity property* over Σ^* if $s \approx t$ implies $usv \approx utv$ for all $s, t, u, v \in \Sigma^*$. Throughout this paper, it is assumed that $\approx$ has the monotonicity property over Σ^*.

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

3. Superposition with Strings

3.1 Inference rules

The following inference rules for clauses over strings are parameterized by a selection function $\mathscr{S}$ and the length-lexicographic ordering $\succ$, where $\mathscr{S}$ arbitrarily selects exactly one negative literal for each clause containing at least one negative literal (see Section 3.6 in Nieuwenhuis and Rubio (2001) or Section 6 in Bachmair and Ganzinger (1998)). In this strategy, an inference involving a clause with a selected literal is performed before an inference from clauses without a selected literal for a theorem proving process. The intuition behind the (eager) selection of negative literals is that, roughly speaking, one may first prove the whole antecedent of each clause from other clauses. Then clauses with no selected literals are involved in the main deduction process. This strategy is particularly useful when we consider Horn completion in Section 6 and a decision procedure for the word problems associated with it. In the following, the symbol $\bowtie$ is used to denote either $\approx$ or $\not\approx$.

Superposition: $$\frac{C \vee u_1u_2 \approx s \qquad D \vee u_2u_3 \approx t}{C \vee D \vee u_1t \approx su_3}$$

if (i) u_2 is not λ, (ii) C contains no selected literal, (iii) D contains no selected literal, (iv) $u_1u_2 \succ s$, and (v) $u_2u_3 \succ t$.[2]

Rewrite: $$\frac{C \vee u_1u_2u_3 \bowtie s \qquad D \vee u_2 \approx t}{C \vee D \vee u_1tu_3 \bowtie s}$$

if (i) $u_1u_2u_3 \bowtie s$ is selected for the left premise whenever $\bowtie$ is $\not\approx$, (ii) C contains no selected literal whenever $\bowtie$ is $\approx$, (iii) D contains no selected literal, and (iv) $u_2 \succ t$.[3]

Equality Resolution: $$\frac{C \vee s \not\approx s}{C}$$

if $s \not\approx s$ is selected for the premise.

The following Paramodulation and Factoring inference rules are used for non-Horn clauses containing positive literals only (cf. *Equality Factoring* (Bachmair and Ganzinger, 1994; Nieuwenhuis and Rubio, 2001) and *Merging Paramodulation* rule (Bachmair and Ganzinger, 1994)).

Paramodulation: $$\frac{C \vee s \approx u_1u_2 \qquad D \vee u_2u_3 \approx t}{C \vee D \vee su_3 \approx u_1t}$$

if (i) u_2 is not λ, (ii) C contains no selected literal, (iii) C contains a positive literal, (iv) D contains no selected literal, (v) $s \succ u_1u_2$, and (vi) $u_2u_3 \succ t$.

Factoring: $$\frac{C \vee s \approx t \vee su \approx tu}{C \vee su \approx tu}$$

if C contains no selected literal.

In the proposed inference system, finding whether a string s occurs within a string t can be done in linear time in the size of s and t by using the existing string matching algorithms such as the Knuth–Morris–Pratt (KMP) algorithm (Cormen et al., 2001). For example, the KMP algorithm can be used for finding u_2 in $u_1u_2u_3$ in the Rewrite rule and finding u_2 in u_1u_2 in the Superposition and Paramodulation rule.

In the remainder of this paper, we denote by $\mathfrak{S}$ the inference system consisting of the Superposition, Rewrite, Equality Resolution, Paramodulation, and the Factoring rule and denote

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

by S a set of clauses over strings. Also, by the *contraction rules* we mean the following inference rules–Simplification, Subsumption, and Tautology.

Simplification: $\dfrac{S \cup \{C \vee l_1 l l_2 \bowtie v,\ l \approx r\}}{S \cup \{C \vee l_1 r l_2 \bowtie v,\ l \approx r\}}$

if (i) $l_1 l l_2 \bowtie v$ is selected for $C \vee l_1 l l_2 \bowtie v$ whenever $\bowtie$ is $\not\approx$, (ii) l_1 is not λ, and (iii) $l \succ r$.

In the following inference rule, we say that a clause C *subsumes* a clause C' if C is contained in C', where C and C' are viewed as the finite multisets.

Subsumption: $\dfrac{S \cup \{C, C'\}}{S \cup \{C\}}$

if $C \subseteq C'$.

Tautology: $\dfrac{S \cup \{C \vee s \approx s\}}{S}$

Example 1. *Let $a \succ b \succ c \succ d \succ e$ and consider the following inconsistent set of clauses 1: $ad \approx b \vee ad \approx c$, 2: $b \approx c$, 3: $ad \approx e$, and 4: $c \not\approx e$. Now, we show how the empty clause is derived:*
5: $ad \approx c \vee ad \approx c$ (Paramodulation of 1 with 2)
6: $ad \approx c$ (Factoring of 5)
7: $c \approx e$ (Rewrite of 6 with 3)
8: $e \not\approx e$ ($c \not\approx e$ is selected for 4. Rewrite of 4 with 7)
9: $\square$ ($e \not\approx e$ is selected for 8. Equality Resolution on 8)

Note that there is no inference with the selected literal in 4 from the initial set of clauses 1, 2, 3, and 4. We produced clauses 5, 6, and 7 without using a selected literal. Once we have clause 7, there is an inference with the selected literal in 4.

Example 2. *Let $a \succ b \succ c \succ d$ and consider the following inconsistent set of clauses 1: $aa \approx a \vee bd \not\approx a$, 2: $cd \approx b$, 3: $ad \approx c$, 4: $bd \approx a$, and 5: $dab \not\approx db$. Now, we show how the empty clause is derived:*
6: $aa \approx a \vee a \not\approx a$ ($bd \not\approx a$ is selected for 1. Rewrite of 1 with 4)
7: $aa \approx a$ ($a \not\approx a$ is selected for 6. Equality resolution on 6)
8: $ac \approx ad$ (Superposition of 7 with 3)
9: $add \approx ab$ (Superposition of 8 with 2)
10: $ab \approx cd$ (Rewrite of 9 with 3)
11: $dcd \not\approx db$ ($dab \not\approx db$ is selected for 5. Rewrite of 5 with 10)
12: $db \not\approx db$ ($dcd \not\approx db$ is selected for 11. Rewrite of 11 with 2)
13: $\square$ ($db \not\approx db$ is selected for 12. Equality Resolution on 12)

3.2 Lifting properties

Recall that Σ^* is the set of all strings over Σ with the empty string λ. We let $T(\Sigma \cup \{\bot\})$ be the set of all first-order ground terms over $\Sigma \cup \{\bot\}$, where each letter from Σ is interpreted as a unary function symbol and $\bot$ is the only constant symbol. (The constant symbol $\bot$ does not have a special meaning (e.g., "false") in this paper.) We remove parentheses for notational convenience for each term in $T(\Sigma \cup \{\bot\})$. Since $\bot$ is the only constant symbol, we see that $\bot$ occurs only once at the end of each term in $T(\Sigma \cup \{\bot\})$. We may view each term in $T(\Sigma \cup \{\bot\})$ as a string ending with $\bot$. Now, the definitions used in Section 2 can be carried over to the case when Σ^* is replaced by $T(\Sigma \cup \{\bot\})$. In the remainder of this paper, we use the string notation for terms in $T(\Sigma \cup \{\bot\})$ unless otherwise stated.

Let $s \approx t$ be an equation over Σ^*. Then, we can associate $s \approx t$ with the equation $s(x) \approx t(x)$, where $s(x) \approx t(x)$ represents the set of all its ground instances over $T(\Sigma \cup \{\bot\})$. (Here, $\lambda(x)$

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

and $\lambda\perp$ correspond to x and $\perp$, respectively.) First, $s \approx t$ over Σ^* corresponds to $s\perp \approx t\perp$ over $T(\Sigma \cup \{\perp\})$. Now, using the monotonicity property, if we concatenate string u to both sides of $s \approx t$ over Σ^*, then we have $su \approx tu$, which corresponds to $su\perp \approx tu\perp$.

There is a similar approach in string rewriting systems. If S is a string rewriting system over Σ^*, then it is known that we can associate term rewriting system R_S with S in such a way that $R_S := \{l(x) \to r(x) \mid l \to r \in S\}$ (Book and Otto, 1993), where x is a variable and each letter from Σ is interpreted as a unary function symbol. We may rename variables (by standardizing variables apart) whenever necessary. This approach is particularly useful when we consider critical pairs between the rules in a string rewriting system. For example, if there are two rules $aa \to c$ and $ab \to d$ in S, then we have $cb \leftarrow aab \to ad$, where $<cb, ad>$ (or $<ad, cb>$) is a *critical pair* formed from these two rules. This critical pair can also be found if we associate $aa \to c \in S$ with $a(a(x)) \to c(x) \in R_S$ and $ab \to d \in S$ with $a(b(x)) \to d(x) \in R_S$. First, we rename the rule $a(b(x)) \to d(x) \in R_S$ into $a(b(y)) \to d(y)$. Then by mapping x to $b(z)$ and y to z, we have $c(b(z)) \leftarrow a(a(b(z))) \to a(d(z))$, where $<c(b(z)), a(d(z))>$ is a critical pair formed from these two rules. This critical pair can be associated with the critical pair $<cb, ad>$ formed from $aa \to c$ in S and $ab \to d$ in S.

However, if $s \not\approx t$ is a negative literal over strings, then we cannot simply associate $s \not\approx t$ with the negative literal $s(x) \not\approx t(x)$ over first-order terms. Suppose to the contrary that we associate $s \not\approx t$ with $s(x) \not\approx t(x)$. Then $s \not\approx t$ implies $su \not\approx tu$ for a nonempty string u because we can substitute $u(y)$ for x in $s(x) \not\approx t(x)$, and $su \not\approx tu$ can also be associated with $s(u(y)) \not\approx t(u(y))$. Using the contrapositive argument, this means that $su \approx tu$ implies $s \approx t$ for the nonempty string u. Recall that we do not assume the cancelation property of equations over strings in this paper.[4] Instead, we simply associate $s \not\approx t$ with $s\perp \not\approx t\perp$. The following lemma is based on the above observations. We denote by $T(\Sigma \cup \{\perp\}, X)$ the set of first-order terms built on $\Sigma \cup \{\perp\}$ and a denumerable set of variables X, where each symbol from Σ is interpreted as a unary function symbol and $\perp$ is the only constant symbol.

Lemma 3. *Let $C := s_1 \approx t_1 \vee \cdots \vee s_m \approx t_m \vee u_1 \not\approx v_1 \vee \cdots \vee u_n \not\approx v_n$ be a clause over Σ^* and P be the set of all clauses that follow from C using the monotonicity property. Let Q be the set of all ground instances of the clause $s_1(x_1) \approx t_1(x_1) \vee \cdots \vee s_m(x_m) \approx t_m(x_m) \vee u_1\perp \not\approx v_1\perp \vee \cdots \vee u_n\perp \not\approx v_n\perp$ over $T(\Sigma \cup \{\perp\}, X)$, where $x_1, \ldots, x_m$ are distinct variables in X and each letter from Σ is interpreted as a unary function symbol. Then there is a one-to-one correspondence between P and Q.*

Proof. For each element D of P, D has the form $D := s_1w_1 \approx t_1w_1 \vee \cdots \vee s_mw_m \approx t_mw_m \vee u_1 \not\approx v_1 \vee \cdots \vee u_n \not\approx v_n$ for some $w_1, \ldots, w_m \in \Sigma^*$. (If $w_i = \lambda$ for all $1 \leq i \leq m$, then D is simply C.) Now, we map each element D of P to D' in Q, where $D' := s_1w_1\perp \approx t_1w_1\perp \vee \cdots \vee s_mw_m\perp \approx t_mw_m\perp \vee u_1\perp \not\approx v_1\perp \vee \cdots \vee u_n\perp \not\approx v_n\perp$. Since $\perp$ is the only constant symbol in $\Sigma \cup \{\perp\}$, it is easy to see that this mapping is well defined and bijective. $\square$

Definition 4. *(i) We say that every term in $T(\Sigma \cup \{\perp\})$ is a* g-term. *(Recall that we remove parentheses for notational convenience.)*
(ii) Let $s \approx t$ (resp. $s \to t$) be an equation (resp. a rule) over Σ^*. We say that $su\perp \approx tu\perp$ (resp. $su\perp \to tu\perp$) for some string u is a g-equation *(resp. a* g-rule*) of $s \approx t$ (resp. $s \to t$).*
(iii) Let $s \not\approx t$ be a negative literal over Σ^*. We say that $s\perp \not\approx t\perp$ is a (negative) g-literal *of $s \not\approx t$.*
(iv) Let $C := s_1 \approx t_1 \vee \cdots \vee s_m \approx t_m \vee u_1 \not\approx v_1 \vee \cdots \vee u_n \not\approx v_n$ be a clause over Σ^*. We say that $s_1w_1\perp \approx t_1w_1\perp \vee \cdots \vee s_mw_m\perp \approx t_mw_m\perp \vee u_1\perp \not\approx v_1\perp \vee \cdots \vee u_n\perp \not\approx v_n\perp$ for some strings $w_1, \ldots, w_m$ is a g-clause *of clause C. Here, each $w_k\perp \in T(\Sigma \cup \{\perp\})$ for nonempty string w_k in the g-clause is said to be a* substitution part *of C.*
(v) Let π be an inference (w.r.t. $\mathfrak{S}$) with premises $C_1, \ldots, C_k$ and conclusion D. Then a g-instance *of π is an inference (w.r.t. $\mathfrak{S}$) with premises $C'_1, \ldots, C'_k$ and conclusion D', where $C'_1, \ldots, C'_k$ and D' are g-clauses of $C_1, \ldots, C_k$ and D, respectively.*

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

Since each term in $T(\Sigma \cup \{\bot\})$ is viewed as a string, we may consider inferences between g-clauses using $\mathfrak{S}$. Note that concatenating a (nonempty) string at the end of a g-term is not allowed for any g-term over $T(\Sigma \cup \{\bot\})$. For example, $abc\bot d$ is not a g-term, and $a\bot \not\approx b\bot \vee abc\bot d \approx def\bot d$ is not a g-clause. We emphasize that we are only concerned with inferences between (legitimate) g-clauses here.

We may also use the length-lexicographic ordering $\succ_g$ on g-terms. Given a total precedence ordering on $\Sigma \cup \{\bot\}$ for which $\bot$ is minimal, it can be easily verified that $\succ_g$ is a total reduction ordering on $T(\Sigma \cup \{\bot\})$. We simply denote the multiset extension $\succ_g^{mul}$ of $\succ_g$ as $\succ_g$ for notational convenience.[5] We denote ambiguously all orderings on g-terms, g-equations, and g-clauses over $T(\Sigma \cup \{\bot\})$ by $\succ_g$. Now, we consider the lifting of inferences of $\mathfrak{S}$ between g-clauses over $T(\Sigma \cup \{\bot\})$ to inferences of $\mathfrak{S}$ between clauses over Σ^*. Let $C_1, \ldots, C_n$ be clauses over Σ^* and let

$$\frac{C'_1 \ldots C'_n}{C'}$$

be an inference between their g-clauses, where C'_i is a g-clause of C_i for all $1 \leq i \leq n$. We say that this inference between g-clauses can be *lifted* if there is an inference

$$\frac{C_1 \ldots C_n}{C}$$

such that C' is a g-clause of C. In what follows, we assume that a g-literal L'_i in C'_i is selected in the same way as L_i in C_i, where L_i is a negative literal in C_i and L'_i is a g-literal of L_i.

Lifting of an inference between g-clauses is possible if it does not correspond to a g-instance of an inference (w.r.t. $\mathfrak{S}$) into a substitution part of a clause, which is not necessary (see, e.g., Bachmair and Ganzinger (1995); Nieuwenhuis and Rubio (2001)). Suppose that there is an inference between g-clauses $C'_1 \ldots C'_n$ with conclusion C' and there is also an inference between clauses $C_1 \ldots C_n$ over Σ^* with conclusion C, where C'_i is a g-clause of C_i for all $1 \leq i \leq n$. Then, the inference between g-clauses $C'_1 \ldots C'_n$ over $T(\Sigma \cup \{\bot\})$ can be lifted to the inference between clauses $C_1 \ldots C_n$ over Σ^* in such a way that C' is a g-clause of C. This can be easily verified for each inference rule in $\mathfrak{S}$.

Example 5. *Consider the following Superposition inference with g-clauses:*

$$\frac{ad\bot \approx cd\bot \vee aabb\bot \approx cbb\bot \qquad abb\bot \approx db\bot}{ad\bot \approx cd\bot \vee adb\bot \approx cbb\bot}$$

where $ad\bot \approx cd\bot \vee aabb\bot \approx cbb\bot$ (resp. $abb\bot \approx db\bot$) is a g-clause of $a \approx c \vee aa \approx c$ (resp. $ab \approx d$) and $aabb\bot \succ_g cbb\bot$ (resp. $abb\bot \succ_g db\bot$). This Superposition inference between g-clauses can be lifted to the following Superposition inference between clauses over Σ^*:

$$\frac{a \approx c \vee aa \approx c \qquad ab \approx d}{a \approx c \vee ad \approx cb}$$

where $aa \succ c$ and $ab \succ d$. We see that conclusion $ad\bot \approx cd\bot \vee adb\bot \approx cbb\bot$ of the Superposition inference between the above g-clauses is a g-clause of conclusion $a \approx c \vee ad \approx cb$ of this inference.

Example 6. *Consider the following Rewrite inference with g-clauses:*

$$\frac{a\bot \not\approx d\bot \vee aabb\bot \not\approx cd\bot \qquad abb\bot \approx cb\bot}{a\bot \not\approx d\bot \vee acb\bot \not\approx cd\bot}$$

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

where $aabb\bot \not\approx cd\bot$ is selected and $a\bot \not\approx d\bot \vee aabb\bot \not\approx cd\bot$ (resp. $abb\bot \approx cb\bot$) is a g-clause of $a \not\approx d \vee aabb \not\approx cd$ (resp. $ab \approx c$) with $abb\bot \succ_g cb\bot$. This Rewrite inference between g-clauses can be lifted to the following Rewrite inference between clauses over Σ^*:

$$\frac{a \not\approx d \vee aabb \not\approx cd \qquad ab \approx c}{a \not\approx d \vee acb \not\approx cd}$$

where $aabb \not\approx cd$ is selected and $ab \succ c$. We see that conclusion $a\bot \not\approx d\bot \vee acb\bot \not\approx cd\bot$ of the Rewrite inference between the above g-clauses is a g-clause of conclusion $a \not\approx d \vee acb \not\approx cd$ of this inference.

4. Redundancy and Contraction Techniques

By Lemma 3 and Definition 4, we may translate a clause $C := s_1 \approx t_1 \vee \cdots \vee s_m \approx t_m \vee u_1 \not\approx v_1 \vee \cdots \vee u_n \not\approx v_n$ over Σ^* with all its implied clauses using the monotonicity property into the clause $s_1(x_1) \approx t_1(x_1) \vee \cdots \vee s_m(x_m) \approx t_m(x_m) \vee u_1\bot \not\approx v_1\bot \vee \cdots \vee u_n\bot \not\approx v_n\bot$ over $T(\Sigma \cup \{\bot\}, X)$ with all its ground instances, where $x_1, \ldots, x_m$ are distinct variables in X, each symbol from Σ is interpreted as a unary function symbol, and $\bot$ is the only constant symbol. This allows us to adapt the existing notion of redundancy found in the literature (Bachmair and Ganzinger, 1994; Nieuwenhuis and Rubio, 2001).

Definition 7. *(i) Let R be a set of g-equations or g-rules. Then the congruence $\leftrightarrow_R^*$ defines an equality* Herbrand interpretation I, *where the domain of I is $T(\Sigma \cup \{\bot\})$. Each unary function symbol $s \in \Sigma$ is interpreted as the unary function s_I, where $s_I(u\bot)$ is the g-term $su\bot$. (The constant symbol $\bot$ is simply interpreted as the constant $\bot$.) The only predicate $\approx$ is interpreted by $s\bot \approx t\bot$ if $s\bot \leftrightarrow_R^* t\bot$. We denote by R^* the interpretation I defined by R in this way. I* satisfies *(is a* model *of) a g-clause $\Gamma \to \Delta$, denoted by $I \models \Gamma \to \Delta$, if $I \not\supseteq \Gamma$ or $I \cap \Delta \neq \emptyset$. In this case, we say that $\Gamma \to \Delta$ is* true *in I. We say that I* satisfies *a clause C over Σ^* if I satisfies all g-clauses of C. We say that I* satisfies *a set of clauses S over Σ^*, denoted by $I \models S$, if I satisfies every clause in S.*
(ii) A g-clause C follows *from a set of g-clauses $\{C_1, \ldots, C_n\}$, denoted by $\{C_1, \ldots, C_n\} \models C$, if C is true in every model of $\{C_1, \ldots, C_k\}$.*

Definition 8. *Let S be a set of clauses over Σ^*.*
(i) A g-clause C is redundant *w.r.t. S if there exist g-clauses $C'_1, \ldots, C'_k$ of clauses $C_1, \ldots, C_k$ in S, such that $\{C'_1, \ldots, C'_k\} \models C$ and $C \succ_g C'_i$ for all $1 \le i \le k$. A clause in S is* redundant *w.r.t. S if all its g-clauses are redundant w.r.t. S.*
(ii) An inference π with conclusion D is redundant *w.r.t. S if for every g-instance of π with maximal premise C' (w.r.t. $\succ_g$) and conclusion D', there exist g-clauses $C'_1, \ldots, C'_k$ of clauses $C_1, \ldots, C_k$ in S such that $\{C'_1, \ldots, C'_k\} \models D'$ and $C' \succ_g C'_i$ for all $1 \le i \le k$, where D' is a g-clause of D.*

Lemma 9. *If an equation $l \approx r$ simplifies a clause $C \vee l_1ll_2 \bowtie v$ into $C \vee l_1rl_2 \bowtie v$ using the Simplification rule, then $C \vee l_1ll_2 \bowtie v$ is redundant w.r.t. $\{C \vee l_1rl_2 \bowtie v, l \approx r\}$.*

Proof. Suppose that $l \approx r$ simplifies $D := C \vee l_1ll_2 \not\approx v$ into $C \vee l_1rl_2 \not\approx v$, where $l_1ll_2 \not\approx v$ is selected for D. Then, every g-clause D' of D has the form $D' := C' \vee l_1ll_2\bot \not\approx v\bot$, where C' is a g-clause of C. Now, we may infer that $\{D'', ll_2\bot \approx rl_2\bot\} \models D'$, where $D'' := C' \vee l_1rl_2\bot \not\approx v\bot$ is a g-clause of $C \vee l_1rl_2 \not\approx v$ and $ll_2\bot \approx rl_2\bot$ is a g-equation of $l \approx r$. We also have $D' \succ_g D''$ and $D' \succ_g ll_2\bot \approx rl_2\bot$, and thus the conclusion follows.

Otherwise, suppose that $l \approx r$ simplifies $D := C \vee l_1ll_2 \approx v$ into $C \vee l_1rl_2 \approx v$. Then every g-clause D' of D has the form $D' := C' \vee l_1ll_2w\bot \approx vw\bot$ for some $w \in \Sigma^*$, where C' is a g-clause of C. Now, we have $\{D'', ll_2w\bot \approx rl_2w\bot\} \models D'$, where $D'' := C' \vee l_1rl_2w\bot \approx vw\bot$ is a g-clause of $C \vee l_1rl_2 \approx v$ for some $w \in \Sigma^*$ and $ll_2w\bot \approx rl_2w\bot$ is a g-equation of $l \approx r$. We also have $D' \succ_g D''$

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

and $D' \succ_g ll_2w\bot \approx rl_2w\bot$ because l_1 is not λ in the condition of the rule (i.e., $l_1ll_2w\bot \succ_g ll_2w\bot$), and thus the conclusion follows. $\square$

Example 10. *Suppose that $a \approx b$ simplifies the clause $ab \not\approx c \vee bc \approx d \vee cd \approx e$ into $bb \not\approx c \vee bc \approx d \vee cd \approx e$ using the Simplification rule, where $ab \not\approx c$ is selected and $a \succ b \succ c \succ d \succ e$. Then each g-clause of $ab \not\approx c \vee bc \approx d \vee cd \approx e$ has the form $G := ab\bot \not\approx c\bot \vee bcw_1\bot \approx dw_1\bot \vee cdw_2\bot \approx ew_2\bot$ for some $w_1, w_2 \in \Sigma^*$ (see Definition 4(iv)). Now, we see that $\{ab\bot \approx bb\bot, bb\bot \not\approx c\bot \vee bcw_1\bot \approx dw_1\bot \vee cdw_2\bot \approx ew_2\bot\} \models G$, $G \succ_g ab\bot \approx bb\bot$, and $G \succ_g bb\bot \not\approx c\bot \vee bcw_1\bot \approx dw_1\bot \vee cdw_2\bot \approx ew_2\bot$. Here, $ab\bot \approx bb\bot$ is a g-clause of $a \approx b$ and $bb\bot \not\approx c\bot \vee bcw_1\bot \approx dw_1\bot \vee cdw_2\bot \approx ew_2\bot$ is a g-clause of $bb \not\approx c \vee bc \approx d \vee cd \approx e$. Thus, we may infer that $ab \not\approx c \vee bc \approx d \vee cd \approx e$ is redundant w.r.t. $\{a \approx b, bb \not\approx c \vee bc \approx d \vee cd \approx e\}$.*

We see that if C subsumes C' with C and C' containing the same number of literals, then they are the same when viewed as the finite multisets, so we can remove C'. Therefore, we exclude this case in the following lemma.

Lemma 11. *If a clause C subsumes a clause D and C contains fewer literals than D, then D is redundant w.r.t. $\{C\}$.*

Proof. Suppose that C subsumes D and C contains fewer literals than D. Then D can be denoted by $C \vee B$ for some nonempty clause B. Now, for every g-clause $D' := C' \vee B'$ of D, we have $\{C'\} \models D'$ with $D' \succ_g C'$, where C' and B' are g-clauses of C and B, respectively. Thus, D is redundant w.r.t. $\{C\}$. $\square$

Lemma 12. *A tautology $C \vee s \approx s$ is redundant.*

Proof. It is easy to see that for every g-clause $C' \vee su\bot \approx su\bot$ of $C \vee s \approx s$, we have $\models C' \vee su\bot \approx su\bot$, where $u \in \Sigma^*$ and C' is a g-clause of C. Thus, $C \vee s \approx s$ is redundant. $\square$

5. Refutational Completeness

In this section, we adapt the model construction and equational theorem proving techniques used in Bachmair and Ganzinger (1994), Nieuwenhuis and Rubio (2001), and Kim and Lynch (2021) and show that $\mathfrak{S}$ with the contraction rules is refutationally complete.

Definition 13. *A g-equation $s\bot \approx t\bot$ is* reductive *for a g-clause $C := D \vee s\bot \approx t\bot$ if $s\bot \approx t\bot$ is strictly maximal (w.r.t. $\succ_g$) in C with $s\bot \succ_g t\bot$.*

Definition 14. (Model Construction) *Let S be a set of clauses over Σ^*. We use induction on $\succ_g$ to define the sets R_C, E_C, and I_C for all g-clauses C of clauses in S. Let C be such a g-clause of a clause in S and suppose that $E_{C'}$ has been defined for all g-clauses C' of clauses in S for which $C \succ_g C'$. Then we define by $R_C = \bigcup_{C \succ_g C'} E_{C'}$. We also define by I_C the equality interpretation R_C^*, which denotes the least congruence containing R_C.*

Now, let $C := D \vee s\bot \approx t\bot$ such that C is not a g-clause of a clause with a selected literal in S. Then C produces $E_C = \{s\bot \to t\bot\}$ if the following conditions are met: (1) $I_C \not\models C$, (2) $I_C \not\models t\bot \approx t'\bot$ for every $s\bot \approx t'\bot$ in D, (3) $s\bot \approx t\bot$ is reductive for C, and (4) $s\bot$ is irreducible by R_C. We say that C is productive *and produces E_C if it satisfies all of the above conditions. Otherwise, $E_C = \emptyset$. Finally, we define I_S as the equality interpretation R_S^*, where $R_S = \bigcup_C E_C$ is the set of all g-rules produced by g-clauses of clauses in S.*

Lemma 15. *(i) R_S has the Church–Rosser property.*
(ii) R_S is terminating.
(iii) For g-terms $u\bot$ and $v\bot$, $I_S \models u\bot \approx v\bot$ if and only if $u\bot \downarrow_{R_S} v\bot$.
(iv) If $I_S \models s \approx t$, then $I_S \models usv \approx utv$ for nonempty strings $s, t, u, v \in \Sigma^*$.

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

Proof. (i) R_S is left-reduced because there are no overlaps among the left-hand sides of rewrite rules in R_S, and thus R_S has the Church–Rosser property.
(ii) For each rewrite rule $l\bot \to r\bot$ in R_S, we have $l\bot \succ_g r\bot$, and thus R_S is terminating.
(iii) Since R_S has the Church–Rosser property and is terminating by (i) and (ii), respectively, R_S is convergent. Thus, $I_S \models u\bot \approx v\bot$ if and only if $u\bot \downarrow_{R_S} v\bot$ for g-terms $u\bot$ and $v\bot$.
(iv) Suppose that $I_S \models s \approx t$ for nonempty strings s and t. Then, we have $I_S \models svw\bot \approx tvw\bot$ for all strings v and w by Definition 7(i). Similarly, since I_S is an equality Herbrand interpretation, we also have $I_S \models usvw\bot \approx utvw\bot$ for all strings u, which means $I_S \models usv \approx utv$ by Definition 7(i). □

Lemma 15(iv) says that the monotonicity assumption used in this paper holds w.r.t. a model constructed by Definition 14.

Definition 16. *Let S be a set of clauses over Σ^*. We say that S is* saturated *under $\mathfrak{S}$ if every inference by $\mathfrak{S}$ with premises in S is redundant w.r.t. S.*

Definition 17. *Let $C := s_1 \approx t_1 \vee \cdots \vee s_m \approx t_m \vee u_1 \not\approx v_1 \vee \cdots \vee u_n \not\approx v_n$ be a clause over Σ^*, and $C' = s_1w_1\bot \approx t_1w_1\bot \vee \cdots \vee s_mw_m\bot \approx t_mw_m\bot \vee u_1\bot \not\approx v_1\bot \vee \cdots \vee u_n\bot \not\approx v_n\bot$ for some strings $w_1, \ldots, w_m$ be a g-clause of C. We say that C' is a* reduced g-clause *of C w.r.t. a rewrite system R if every $w_i\bot$, $1 \le i \le m$, is not reducible by R.*

In the proof of the following lemma, we write $s[t]_{suf}$ to indicate that t occurs in s as a suffix and (ambiguously) denote by $s[u]_{suf}$ the result of replacing the occurrence of t (as a suffix of s) by u.

Lemma 18. *Let S be saturated under $\mathfrak{S}$ not containing the empty clause and C be a g-clause of a clause in S. Then C is true in I_S. More specifically,*
(i) If C is redundant w.r.t. S, then it is true in I_S.
(ii) If C is not a reduced g-clause of a clause in S w.r.t. R_S, then it is true in I_S.
(iii) If $C := C' \vee s\bot \approx t\bot$ produces the rule $s\bot \to t\bot$, then C' is false and C is true in I_S.
(iv) If C is a g-clause of a clause in S with a selected literal, then it is true in I_S.
(v) If C is nonproductive, then it is true in I_S.

Proof. We use induction on $\succ_g$ and assume that (i)–(v) hold for every g-clause D of a clause in S with $C \succ_g D$.

(i) Suppose that C is redundant w.r.t. S. Then there exist g-clauses $C'_1, \ldots, C'_k$ of clauses $C_1, \ldots, C_k$ in S, such that $\{C'_1, \ldots, C'_k\} \models C$ and $C \succ_g C'_i$ for all $1 \le i \le k$. By the induction hypothesis, each C'_i, $1 \le i \le k$, is true in I_S. Thus, C is true in I_S.

(ii) Suppose that C is a g-clause of a clause $B := s_1 \approx t_1 \vee \cdots \vee s_m \approx t_m \vee u_1 \not\approx v_1 \vee \cdots \vee u_n \not\approx v_n$ in S but is not a reduced g-clause w.r.t. R_S. Then C is of the form $C := s_1w_1\bot \approx t_1w_1\bot \vee \cdots \vee s_mw_m\bot \approx t_mw_m\bot \vee u_1\bot \not\approx v_1\bot \vee \cdots \vee u_n\bot \not\approx v_n\bot$ for $w_1, \ldots, w_m \in \Sigma^*$ and some $w_k\bot$ is reducible by R_S. Now, consider $C' = s_1w'_1\bot \approx t_1w'_1\bot \vee \cdots \vee s_mw'_m\bot \approx t_mw'_m\bot \vee u_1\bot \not\approx v_1\bot \vee \cdots \vee u_n\bot \not\approx v_n\bot$, where $w'_i\bot$ is the normal form of $w_i\bot$ w.r.t. R_S for each $1 \le i \le m$. Then, C' is a reduced g-clause of B w.r.t. R_S and is true in I_S by the induction hypothesis. Since each $w_i\bot \approx w'_i\bot$, $1 \le i \le m$, is true in I_S by Lemma 15(iii), we may infer that C is true in I_S.

In the remainder of the proof of this lemma, we assume that C is neither redundant w.r.t. S nor is it a reducible g-clause w.r.t. R_S of some clause in S. (Otherwise, we are done by (i) or (ii).)

(iii) Suppose that $C := C' \vee s\bot \approx t\bot$ produces the rule $s\bot \to t\bot$. Since $s\bot \to t\bot \in E_C \subset R_S$, we see that C is true in I_S. We show that C' is false in I_S. Let $C' := \Gamma \to \Delta$. Then $I_C \not\models C'$ by Definition 14, which implies that $I_C \cap \Delta = \emptyset$, $I_C \supseteq \Gamma$, and thus $I_S \supseteq \Gamma$. It remains to show that $I_S \cap \Delta = \emptyset$. Suppose to the contrary that Δ contains an equation $s'\bot \approx t'\bot$ which is true in I_S. Since $I_C \cap \Delta = \emptyset$, we must have $s'\bot \approx t'\bot \in I \setminus I_C$, which is only possible if $s\bot = s'\bot$ and $I_C \models t\bot \approx t'\bot$, contradicting condition (2) in Definition 14.

(iv) Suppose that C is of the form $C := B' \vee s\bot \not\approx t\bot$, where $s\bot \not\approx t\bot$ is a g-literal of a selected literal in a clause in S and B' is a g-clause of B.

(iv.1) If $s\bot = t\bot$, then B' is an equality resolvent of C and the Equality Resolution inferences can be lifted. By saturation of S under $\mathfrak{S}$ and the induction hypothesis, B' is true in I_S. Thus, C is true in I_S.

(iv.2) If $s\bot \neq t\bot$, then suppose to the contrary that C is false in I_S. Then we have $I_S \models s\bot \approx t\bot$, which implies that $s\bot$ or $t\bot$ is reducible by R_S by Lemma 15(iii). Without loss of generality, we assume that $s\bot$ is reducible by R_S with some rule $lu\bot \to ru\bot$ for some $u \in \Sigma^*$ produced by a productive g-clause $D' \vee lu\bot \approx ru\bot$ of a clause $D \vee l \approx r \in S$. This means that $s\bot$ has a suffix $lu\bot$. Now, consider the following inference by Rewriting:

$$\frac{B \vee s[lu]_{suf} \not\approx t \qquad D \vee l \approx r}{B \vee D \vee s[ru]_{suf} \not\approx t}$$

where $s[lu]_{suf} \not\approx t$ is selected for the left premise. The conclusion of the above inference has a g-clause $C' := B' \vee D' \vee s\bot[ru\bot]_{suf} \not\approx t\bot$. By saturation of S under $\mathfrak{S}$ and the induction hypothesis, C' must be true in I_S. Moreover, we see that $s\bot[ru\bot]_{suf} \not\approx t\bot$ is false in I_S by Lemma 15(iii), and D' are false in I_S by (iii). This means that B' is true in I_S, and thus C (i.e., $C = B' \vee s\bot \not\approx t\bot$) is true in I_S, which is the required contradiction.

(v) If C is nonproductive, then we assume that C is not a g-clause of a clause with a selected literal. Otherwise, the proof is done by (iv). This means that C is of the form $C := B' \vee su\bot \approx tu\bot$, where $su\bot \approx tu\bot$ is maximal in C and B' contains no selected literal. If $su\bot = tu\bot$, then we are done. Therefore, without loss of generality, we assume that $su\bot \succ_g tu\bot$. As C is nonproductive, it means that (at least) one of the conditions in Definition 14 does not hold.

If condition (1) does not hold, then $I_C \models C$, so we have $I_S \models C$, that is, C is true in I_S. If condition (1) holds but condition (2) does not hold, then C is of the form $C := B'_1 \vee su\bot \approx tu\bot \vee svw\bot \approx t'vw\bot$, where $su = svw$ (i.e., $u = vw$) and $I_C \models tu\bot \approx t'vw\bot$.

Suppose first that $tu\bot = t'vw\bot$. Then we have $t = t'$ since $u = vw$. Now, consider the following inference by Factoring:

$$\frac{B_1 \vee s \approx t \vee sv \approx tv}{B_1 \vee sv \approx tv}$$

The conclusion of the above inference has a g-clause $C' := B'_1 \vee svw\bot \approx tvw\bot$, that is, $C' := B'_1 \vee su\bot \approx tu\bot$ since $u = vw$. By saturation of S under $\mathfrak{S}$ and the induction hypothesis, C' is true in I_S, and thus C is true in I_S.

Otherwise, suppose that $tu\bot \neq t'vw\bot$. Then we have $tu\bot \downarrow_{R_C} t'vw\bot$ by Lemma 15(iii) and $tu\bot \succ_g t'vw\bot$ because $su\bot \approx tu\bot$ is maximal in C. This means that $tu\bot$ is reducible by R_C by some rule $l\tau\bot \to r\tau\bot$ produced by a productive g-clause $D' \vee l\tau\bot \approx r\tau\bot$ of a clause $D \vee l \approx r \in S$. Now, we need to consider two cases:

(v.1) If t has the form $t := u_1u_2$ and l has the form $l := u_2u_3$, then consider the following inference by Paramodulation:

$$\frac{B \vee s \approx u_1u_2 \qquad D \vee u_2u_3 \approx r}{B \vee D \vee su_3 \approx u_1r}$$

The conclusion of the above inference has a g-clause $C' := B' \vee D' \vee su_3\tau\bot \approx u_1r\tau\bot$ with $u = u_3\tau$. By saturation of S under $\mathfrak{S}$ and the induction hypothesis, C' is true in I_S. Since D' is false in I_S by (iii), either B' or $su_3\tau\bot \approx u_1r\tau\bot$ is true in I_S. If B' is true in I_S, so is C. If $su_3\tau\bot \approx u_1r\tau\bot$ is true in I_S, then $su\bot \approx tu\bot$ is also true in I_S by Lemma 15(iii), where $t = u_1u_2$ and $u = u_3\tau$. Thus, C is true in I_S.

(v.2) If t has the form $t := u_1u_2u_3$ and l has the form $l := u_2$, then consider the following inference by Rewrite:

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

$$\frac{B \vee s \approx u_1u_2u_3 \qquad D \vee u_2 \approx r}{B \vee D \vee s \approx u_1ru_3}$$

The conclusion of the above inference has a g-clause $C'' := B' \vee D' \vee su\bot \approx u_1ru_3u\bot$ with $\tau = u_3u$. By saturation of S under $\mathfrak{S}$ and the induction hypothesis, C'' is true in I_S. Since D' is false in I_S by (iii), either B' or $su\bot \approx u_1ru_3u\bot$ is true in I_S. Similarly to case (v.1), if B' is true in I_S, so is C. If $su\bot \approx u_1ru_3u\bot$ is true in I_S, then $su\bot \approx tu\bot$ is also true in I_S by Lemma 15(iii), where $t = u_1u_2u_3$. Thus, C is true in I_S.

If conditions (1) and (2) hold but condition (3) does not hold, then $su\bot \approx tu\bot$ is only maximal but is not strictly maximal, so we are in the previous case. (Since $\succ_g$ is total on g-clauses, condition (2) does not hold.) If conditions (1)–(3) hold but condition (4) does not hold, then $su\bot$ is reducible by R_C by some rule $l\tau\bot \to r\tau\bot$ produced by a productive g clause $D' \vee l\tau\bot \approx r\tau\bot$ of a clause $D \vee l \approx r \in S$. Again, we need to consider two cases:

(v.1') If s has the form $s := u_1u_2$ and l has the form $l := u_2u_3$, then consider the following inference by Superposition:

$$\frac{B \vee u_1u_2 \approx t \qquad D \vee u_2u_3 \approx r}{B \vee D \vee u_1r \approx tu_3}$$

The conclusion of the above inference has a g-clause $C' := B' \vee D' \vee u_1r\tau\bot \approx tu_3\tau\bot$ with $u = u_3\tau$. By saturation of S under $\mathfrak{S}$ and the induction hypothesis, C' is true in I_S. Since D' is false in I_S by (iii), either B' or $u_1r\tau\bot \approx tu_3\tau\bot$ is true in I_S. If B' is true in I_S, so is C. If $u_1r\tau\bot \approx tu_3\tau\bot$ is true in I_S, then $su\bot \approx tu\bot$ is also true in I_S by Lemma 15(iii), where $s = u_1u_2$ and $u = u_3\tau$. Thus, C is true in I_S.

(v.2') If s has the form $s := u_1u_2u_3$ and l has the form $l := u_2$, then consider the following inference by Rewrite:

$$\frac{B \vee u_1u_2u_3 \approx t \qquad D \vee u_2 \approx r}{B \vee D \vee u_1ru_3 \approx t}$$

The conclusion of the above inference has a g-clause $C'' := B' \vee D' \vee u_1ru_3u\bot \approx tu\bot$ with $\tau = u_3u$. By saturation of S under $\mathfrak{S}$ and the induction hypothesis, C'' is true in I_S. Since D' is false in I_S by (iii), either B' or $u_1ru_3u\bot \approx tu\bot$ is true in I_S. Similarly to case (v.1'), If B' is true in I_S, so is C. If $u_1ru_3u\bot \approx tu\bot$ is true in I_S, then $su\bot \approx tu\bot$ is also true in I_S by Lemma 15(iii), where $s = u_1u_2u_3$. Thus, C is true in I_S. □

Definition 19. *(i) A* theorem proving derivation *is a sequence of sets of clauses $S_0 = S, S_1, \ldots$ over Σ^* such that:*

(i.1) Deduction: $S_i = S_{i-1} \cup \{C\}$ if C can be deduced from premises in S_{i-1} by applying an inference rule in $\mathfrak{S}$.

(i.2) Deletion: $S_i = S_{i-1} \setminus \{D\}$ if D is redundant w.r.t. S_{i-1}.[6]

(ii) The set $S_\infty := \bigcup_i (\bigcap_{j \geq i} S_j)$ is the limit *of the theorem proving derivation:*

$$\frac{S \cup \{C \vee l_1ll_2 \bowtie v,\ l \approx r\}}{S \cup \{C \vee l_1rl_2 \bowtie v,\ l \approx r\}}$$

We see that the soundness of a theorem proving derivation w.r.t. the proposed inference system is straightforward, that is, $S_i \models S_{i+1}$ for all $i \geq 0$.

Definition 20. *A theorem proving derivation $S_0, S_1, S_2, \ldots$ is* fair *w.r.t. the inference system $\mathfrak{S}$ if every inference by $\mathfrak{S}$ with premises in S_∞ is redundant w.r.t. $\bigcup_j S_j$.*

Lemma 21. *Let S and S' be sets of clauses over Σ^*.*
(i) If $S \subseteq S'$, then any clause which is redundant w.r.t. S is also redundant w.r.t. S'.
(ii) If $S \subseteq S'$ and all clauses in $S' \setminus S$ are redundant w.r.t. S', then any clause or inference which is redundant w.r.t. S' is also redundant w.r.t. S.

Proof. The proof of part (i) is obvious. For part (ii), suppose that a clause C is redundant w.r.t. S' and let C' be a g-clause of it. Then there exists a minimal set $N := \{C'_1, \ldots, C'_n\}$ (w.r.t. $\succ_g$) of g-clauses of clauses in S' such that $N \models C'$ and $C' \succ_g C'_i$ for all $1 \leq i \leq n$. We claim that all C'_i in N are not redundant w.r.t. S', which shows that C' is redundant w.r.t. S. Suppose to the contrary that some C'_j is redundant w.r.t. S'. Then there exist a set $N' := \{D'_1, \ldots, D'_m\}$ of g-clauses of clauses in S' such that $N' \models C'_j$ and $C'_j \succ_g D'_i$ for all $1 \leq i \leq m$. This means that we have $\{C'_1, \ldots, C'_{j-1}, D'_1, \ldots, D'_m, C'_{j+1}, \ldots, C'_n\} \models C'$, which contradicts our minimal choice of the set $N = \{C'_1, \ldots, C'_n\}$.

Next, suppose an inference π with conclusion D is redundant w.r.t. S' and let π' be a g-instance of it such that B is the maximal premise and D' is the conclusion of π' (i.e., a g-clause of D). Then there exists a minimal set $P := \{D'_1, \ldots, D'_n\}$ (w.r.t. $\succ_g$) of g-clauses of clauses in S' such that $P \models D'$ and $B \succ_g D'_i$ for all $1 \leq i \leq n$. As above, we may infer that all D'_i in P are not redundant w.r.t. S', and thus π' is redundant w.r.t. S. □

Lemma 22. *Let $S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathfrak{S}$. Then S_∞ is saturated under $\mathfrak{S}$.*

Proof. If S_∞ contains the empty clause, then it is obvious that S_∞ is saturated under $\mathfrak{S}$. Therefore, we assume that the empty clause is not in S_∞.

If a clause C is deleted in a theorem proving derivation, then C is redundant w.r.t. some S_j. By Lemma 21(i), it is also redundant w.r.t. $\bigcup_j S_j$. Similarly, every clause in $\bigcup_j S_j \setminus S_\infty$ is redundant w.r.t. $\bigcup_j S_j$.

By fairness, every inference π by $\mathfrak{S}$ with premises in S_∞ is redundant w.r.t. $\bigcup_j S_j$. Using Lemma 21(ii) and the above, π is also redundant w.r.t. S_∞, which means that S_∞ is saturated under $\mathfrak{S}$. □

Theorem 23. *Let $S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathfrak{S}$. If S_∞ does not contain the empty clause, then $I_{S_\infty} \models S_0$ (i.e., S_0 is satisfiable.)*

Proof. Suppose that $S_0, S_1, \ldots$ is a fair theorem proving derivation w.r.t. $\mathfrak{S}$ and that its limit S_∞ does not contain the empty clause. Then S_∞ is saturated under $\mathfrak{S}$ by Lemma 22. Let C' be a g-clause of a clause C in S_0. If $C \in S_\infty$, then C' is true in I_{S_∞} by Lemma 18. Otherwise, if $C \notin S_\infty$, then C is redundant w.r.t. some S_j. It follows that C redundant w.r.t. $\bigcup_j S_j$ by Lemma 21(i), and thus redundant w.r.t. S_∞ by Lemma 21(ii). This means that there exist g-clauses $C'_1, \ldots, C'_k$ of clauses $C_1, \ldots, C_k$ in S_∞ such that $\{C'_1, \ldots, C'_k\} \models C'$ and $C' \succ_g C'_i$ for all $1 \leq i \leq k$. Since each C'_i, $1 \leq i \leq k$, is true in I_{S_∞} by Lemma 18, C' is also true in I_{S_∞}, and thus the conclusion follows. □

The following theorem states that $\mathfrak{S}$ with the contraction rules is refutationally complete for clauses over Σ^*.

Theorem 24. *Let $S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathfrak{S}$. Then S_0 is unsatisfiable if and only if the empty clause is in some S_j.*

Proof. Suppose that $S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathfrak{S}$. By the soundness of the derivation, if the empty clause is in some S_j, then S_0 is unsatisfiable. Otherwise, if the empty clause is not in S_k for all k, then S_∞ does not contain the empty clause by the soundness of the derivation. Applying Theorem 23, we conclude that S_0 is satisfiable. □

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

Superposition: $\dfrac{u_1u_2 \approx s \qquad u_2u_3 \approx t}{u_1t \approx su_3}$

if (i) u_2 is not λ, (ii) $u_1u_2 \succ s$, and (iii) $u_2u_3 \succ t$.

Rewrite: $\dfrac{C \vee u_1u_2u_3 \not\approx s \qquad u_2 \approx t}{C \vee u_1tu_3 \not\approx s}$

if (i) $u_1u_2u_3 \not\approx s$ is selected for the left premise, and (ii) $u_2 \succ t$.

Equality Resolution: $\dfrac{C \vee s \not\approx s}{C}$

if $s \not\approx s$ is selected for the premise.

Above, C is a conditional equation over Σ^*.

Figure 1. The inference system $\mathfrak{S}$ for conditional equations over Σ^*.

6. Conditional Completion

In this section, we present a saturation procedure under $\mathfrak{S}$ for a set of conditional equations over Σ^*, where a conditional equation is naturally written as an equational Horn clause. A saturation procedure under $\mathfrak{S}$ (with contraction rules) can be viewed as *conditional completion* (Dershowitz, 1991) for a set of conditional equations over Σ^*. If a set of conditional equations over Σ^* is simply a set of equations over Σ^*, then the proposed saturation procedure under $\mathfrak{S}$ (with contraction rules) corresponds to a completion procedure for a string rewriting system. Conditional string rewriting systems were considered in Deiß (1992) in the context of embedding a finitely generated monoid with decidable word problem into a monoid presented by a finite convergent conditional presentation. It neither discusses a conditional completion (or a saturation) procedure nor considers the word problems for conditional equations over Σ^* in general.

First, it is easy to see that a set of equations over Σ^* is consistent. Similarly, a set of conditional equations R over Σ^* is consistent because each conditional equation has always a positive literal and we cannot derive the empty clause from R using a saturation procedure under $\mathfrak{S}$ that is refutationally complete (cf. Section 9 in Dershowitz and Plaisted (2001)).

Figure 1 shows the inference rules of $\mathfrak{S}$ (with selection) for equational Horn clauses. Since we only consider equational Horn clauses in this section, we neither need to consider the Factoring rule nor the Paramodulation rule in $\mathfrak{S}$. In the remainder of this section, by a conditional equational theory R, we mean a set of conditional equations R over Σ^*.

Definition 25. *Given a conditional equational theory R and two finite words $s, t \in \Sigma^*$, a* word problem *w.r.t. R is of the form $\phi := s \approx^? t$. The* goal *of this word problem is $s \not\approx t$. We say that a word problem $s \approx^? t$ w.r.t. R is* decidable *if there is a decision procedure for determining whether $s \approx t$ is entailed by R (i.e., $R \models s \approx t$) or not (i.e., $R \not\models s \approx t$) .*

Given a conditional equational theory R, let $G := s \not\approx t$ be the goal of a word problem $s \approx^? t$ w.r.t. R. (Note that G does not have any positive literal.) Then we see that $R \cup \{s \approx t\}$ is consistent if and only if $R \cup \{G\}$ is inconsistent. This allows one to decide a word problem w.r.t. R using the equational theorem proving procedure discussed in Section 5.

Lemma 26. *Let R be a conditional equational theory finitely saturated under $\mathfrak{S}$. Then Rewrite together with Equality Resolution is terminating and refutationally complete for $R \cup \{G\}$, where G is the goal of a word problem w.r.t. R.*

Proof. Since R is already saturated under $\mathfrak{S}$, inferences among Horn clauses in R are redundant and remain redundant in $R \cup \{G\}$ for a theorem proving derivation starting with $R \cup \{G\}$. (Here, $\{G\}$ can be viewed as a *set of support* (Bachmair and Ganzinger, 1994) for a refutation of $R \cup \{G\}$.) Now, observe that G is a negative literal, so it should be selected. The only inference rules in $\mathfrak{S}$ involving a selected literal are the Rewrite and Equality Resolution rule. Furthermore, the derived literals from G w.r.t. Rewrite will also be selected eventually. Therefore, it suffices to consider positive literals as the right premise (because they contain no selected literal), and G and its derived literals w.r.t. Rewrite as the left premise for the Rewrite rule. Observe also that if G' is an immediate derived literal from G w.r.t. Rewrite, then we see that $G \succ G'$. If G or its derived literal from G w.r.t. Rewrite becomes of the form $u \not\approx u$ for some $u \in \Sigma^*$, then it will also be selected and an Equality Resolution inference yields the empty clause. Since $\succ$ is terminating and there are only finitely many positive literals in R, we may infer that the Rewrite and Equality Resolution inference steps on G and its derived literals are terminating. (The number of positive literals in R remains the same during a theorem proving derivation starting with $R \cup \{G\}$ using our selection strategy.)

Finally, since $\mathfrak{S}$ is refutationally complete by Thereom 24, Rewrite together with Equality Resolution is also refutationally complete for $R \cup \{G\}$. □

Given a finitely saturated conditional equational theory R under $\mathfrak{S}$, we provide a decision procedure for the word problems w.r.t. R in the following theorem.

Theorem 27. *Let R be a conditional equational theory finitely saturated under $\mathfrak{S}$. Then the word problems w.r.t. R are decidable by Rewrite together with Equality Resolution.*

Proof. Let $\phi := s \approx^? t$ be a word problem w.r.t. R and G be the goal of ϕ. We know that by Lemma 26, Rewrite together with Equality Resolution is terminating and refutationally complete for $R \cup \{G\}$. Let $R_0 := R \cup \{G\}, R_1, \ldots, R_n$ be a fair theorem proving derivation w.r.t. Rewrite together with Equality Resolution such that R_n is the limit of this derivation. If R_n contains the empty clause, then R_n is inconsistent, and thus R_0 is inconsistent, that is, $\{s \not\approx t\} \cup R$ is inconsistent by the soundness of the derivation. Since R is consistent and $\{s \not\approx t\} \cup R$ is saturated under $\mathfrak{S}$, we may infer that $R \models s \approx t$.

Otherwise, if R_n does not contain the empty clause, then R_n is consistent, and thus R_0 is consistent by Theorem 24, that is, $\{s \not\approx t\} \cup R$ is consistent. Since R is consistent and $\{s \not\approx t\} \cup R$ is saturated under $\mathfrak{S}$, we may infer that $R \not\models s \approx t$. □

The following corollary is a consequence of Theorem 27 and the following observation. Let $R = R_0, R_1, \ldots, R_n$ be a finite fair theorem proving derivation w.r.t. $\mathfrak{S}$ for an initial conditional equational theory R with the limit $\bar{R} := R_n$. Then $R \cup \{G\}$ is inconsistent if and only if $\bar{R} \cup \{G\}$ is inconsistent by the soundness of the derivation and Theorem 24.

Corollary 28. *Let $R = R_0, R_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathfrak{S}$ for a conditional equational theory R. If R can be finitely saturated under $\mathfrak{S}$, then the word problems w.r.t. R are decidable.*

Example 29. *Let $a \succ b \succ c$ and R be a conditional equational theory consisting of the following conditional equations 1: $aa \approx \lambda$, 2: $bb \approx \lambda$, 3: $ab \approx \lambda$, 4: $ab \not\approx ba \vee ac \approx ca$, and 5: $ab \not\approx ba \vee ac \not\approx ca \vee bc \approx cb$. We first saturate R under $\mathfrak{S}$:*

6: $\lambda \not\approx ba \vee ac \approx ca$ ($ab \not\approx ba$ is selected for 4. Rewrite of 4 with 3)
7: $\lambda \not\approx ba \vee ac \not\approx ca \vee bc \approx cb$ ($ab \not\approx ba$ is selected for 5. Rewrite of 5 with 3)
8: $a \approx b$ (Superposition of 1 with 3)
9: $\lambda \not\approx bb \vee ac \approx ca$ ($\lambda \not\approx ba$ is selected for 6. Rewrite of 6 with 8)
10: $\lambda \not\approx \lambda \vee ac \approx ca$ ($\lambda \not\approx bb$ is selected for 9. Rewrite of 9 with 2)
11: $ac \approx ca$ ($\lambda \not\approx \lambda$ is selected for 10. Equality Resolution on 10)
12: $\lambda \not\approx bb \vee ac \not\approx ca \vee bc \approx cb$ ($\lambda \not\approx ba$ is selected for 7. Rewrite of 7 with 8)

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

13: $\lambda \not\approx \lambda \vee ac \not\approx ca \vee bc \approx cb$ *(*$\lambda \not\approx bb$ *is selected for 12. Rewrite of 12 with 2)*
14: $ac \not\approx ca \vee bc \approx cb$ *(* $\lambda \not\approx \lambda$ *is selected for 13. Equality Resolution on 13)*
15: $ca \not\approx ca \vee bc \approx cb$ *(* $ac \not\approx ca$ *is selected for 14. Rewrite of 14 with 11)*
16: $bc \approx cb$ *(*$ca \not\approx ca$ *is selected for 15. Equality Resolution on 15)*
...
After some simplification steps, we have a saturated set $\bar{R}$ *for* R *under* $\mathfrak{S}$ *using our selection strategy (i.e., the selection of negative literals). We may infer that the positive literals in* $\bar{R}$ *are as follows.* $1' : bb \approx \lambda$, $2' : a \approx b$, *and* $3' : bc \approx cb$. *Note that only the positive literals in* $\bar{R}$ *are now needed to solve a word problem w.r.t.* R *because of our selection strategy.*

Now, consider the word problem $\phi := acbcba \approx^? bccaba$ *w.r.t.* R, *where the goal of* ϕ *is* $G := acbcba \not\approx bccaba$. *We only need the Rewrite and Equality Resolution steps on* G *and its derived literals from* G *using* $1'$, $2'$, *and* $3'$. *Note that all the following literals are selected except the empty clause.*

$4'$: $bcbcbb \not\approx bccbbb$ *(Rewrite steps of* G *and its derived literals from* G *using* $2'$*).*
$5'$: $bcbc \not\approx bccb$ *(Rewrite steps of* $4'$ *and its derived literals from* $4'$ *using* $1'$*).*
$6'$: $ccbb \not\approx ccbb$ *(Rewrite steps of* $5'$ *and its derived literals from* $5'$ *using* $3'$*).*
$7'$: $\Box$ *(Equality Resolution on* $6'$*)*

Since $\bar{R} \cup G$ *is inconsistent, we see that* $R \cup G$ *is inconsistent by the soundness of the derivation, where* R *and* $\bar{R}$ *are consistent. Therefore, we may infer that* $R \models acbcba \approx bccaba$.

7. Unification in Conditional Equational Theories

This section is concerned with unification in conditional equational theories over strings. It presents a complete method of solving unification problems over strings w.r.t. a conditional equational theory over strings if it is finitely saturated under $\mathfrak{S}$ with contraction rules.

Definition 30. *(i) A binary relation* $\sim$ *on* Σ^* *is* closed under monotonicity *if* $s \sim t$ *implies* $usv \sim utv$ *for all* $s, t, u, v \in \Sigma^*$.
(ii) Let S *be a set of conditional equations over* Σ^*. *A binary relation* $\sim$ *on* Σ^* *is* closed under the conditional equations in S *if* $(s_1 \approx t_1 \wedge \cdots \wedge s_n \approx t_n) \rightarrow l \approx r \in S$ *and* $s_i \sim t_i$ *for all* $1 \leq i \leq n$ *imply* $l \sim r$.[7]
(iii) Let S *be a set of conditional equations over* Σ^*. *We denote by* $\approx_S$ *on* Σ^* *the smallest equivalence relation closed under both monotonicity and the conditional equations in* S *(c.f. Kaplan (1987)).*

Definition 31. *Given a conditional equational theory* S *over* Σ^* *and two finite words* $u, v \in \Sigma^*$, *a* unification problem *w.r.t.* S *is of the form* $\phi := ux \approx^?_S vy$ *for some variables* $x, y \in X$. *We say that a unification problem* $\phi := ux \approx^?_S vy$ *has an* S-unifier *if there is a substitution* $\{x \mapsto w_1, y \mapsto w_2\}$ *for some* $w_1, w_2 \in \Sigma^*$ *such that* $uw_1 \approx_S vw_2$.

Example 32. *(i) Let* $S = \{ab \approx cdd\}$. *Then the unification problem* $ax \approx^?_S cy$ *has an* S*-unifier* $\{x \mapsto b, y \mapsto dd\}$ *since* $ab \approx_S cdd$.
(ii) Let $S = \{a \approx b, ad \approx bd \rightarrow cab \approx dab\}$. *Then the unification problem* $cx \approx^?_S dx$ *has an* S*-unifier* $\{x \mapsto ab\}$ *since* $a \approx_S b$, $ad \approx_S bd$ *(closed under monotonicity), and* $cab \approx_S dab$ *(closed under the conditional equations in* S*).*

Definition 33. *Given a conditional equational theory* S *over* Σ^*, *we denote by* $R(S)$ *the (unconditional) rewrite system obtained by orienting each nontrivial equation over* Σ^* *in* S *using* $\succ$. *(Recall that* $\succ$ *is a reduction order total on* Σ^* *and an equation over* Σ^* *is* trivial *if it has the form* $s \approx s$.*)*

In what follows, by the *contraction rules*, we mean the contraction rules in Section 3 for Horn clauses. We assume that the contraction rules are applied *eagerly* during a theorem proving derivation w.r.t. $\mathfrak{S}$ with the contraction rules, that is, the contraction rules are applied to a Horn clause set as soon as they become applicable. In this case, we see that the application of the Rewrite rule in $\mathfrak{S}$ can be replaced by the application of the Simplification rule for Horn clauses.

Lemma 34. *Let $S = S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathfrak{S}$ with the contraction rules for an initial conditional equational theory S over Σ^*. If S_n for some n is finitely saturated under $\mathfrak{S}$ with the contraction rules, then $R(S_n)$ is convergent on Σ^*.*

Proof. First, it is easy to see that $R(S_n)$ is terminating because $\rightarrow_{R(S_n)} \subset \succ$. Since S_n is finitely saturated under $\mathfrak{S}$ with the the contraction rules, it suffices to consider the overlaps between the rewrite rules in $R(S_n)$ of the form $u_1u_2 \rightarrow s \in R(S_n)$ and $u_2u_3 \rightarrow t \in R(S_n)$, where u_2 is not λ. Now, the critical pair $u_1t \approx su_3$ (in an equation form) are joinable using the Superposition rule in $\mathfrak{S}$ (see Figure 1). Observe that $u_1t \approx su_3$ could be further simplified, but it is still joinable by $R(S_n)$. Also, we do not need to consider the overlaps of the form $u_1u_2u_3 \rightarrow s \in R(S_n)$ and $u_2 \rightarrow t \in R(S_n)$ because S_n is saturated under $\mathfrak{S}$ with the contraction rules. Here, $u_1u_2u_3 \rightarrow s \in R(S_n)$ cannot occur in $R(S_n)$ because $u_1u_2u_3 \approx s$ with $u_1u_2u_3 \succ s$ would be simplified eagerly by $u_2 \approx t$ with $u_2 \succ t$. □

Lemma 35. *Let $S = S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathfrak{S}$ with the contraction rules for an initial conditional equational theory S over Σ^*. If S_n for some n is finitely saturated under $\mathfrak{S}$ with the contraction rules, then $\approx_S$ and $\approx_{R(S_n)}$ coincide, where the rewrite system $R(S_n)$ is viewed as a set of equations over Σ^*.*

Proof. We first show that a conditional equation generated by each inference rule in $\mathfrak{S}$ does not modify $\approx_{S_i}$ for all $0 \leq i < n$, where $S_0 = S$. Consider the Superposition rule and let $u_1u_2 \approx s \in S_k$ and $u_2u_3 \approx t \in S_k$ for some $0 \leq k < n$. Then, we have $u_1u_2 \approx_{S_k} s$ and $u_2u_3 \approx_{S_k} t$. The conclusion of this inference is $u_1t \approx su_3 \in S_{k+1}$. Since $\approx_{S_k}$ is an equivalence relation closed under monotonicity, we also have $u_1u_2u_3 \approx_{S_k} su_3$ and $u_1u_2u_3 \approx_{S_k} u_1t$, and thus $u_1t \approx_{S_k} su_3$.[8] Next, consider the Equality Resolution rule and let $C \vee s \not\approx s \in S_k$. Since $s \approx_{S_k} s$, the conclusion of this inference does not modify $\approx_{S_k}$. For the other contraction rules, removing or replacing the redundant Horn clauses by the contracted clauses does not change $\approx_{S_k}$, and thus $\approx_S$ and $\approx_{S_n}$ coincide.

Next, we show that $\approx_{S_n}$ and $\approx_{R(S_n)}$ coincide. Since S_n is saturated under $\mathfrak{S}$ with the contraction rules, each clause in S_n with the nonempty conditional part is now redundant in S_n. By Lemma 34, $R(S_n)$ is convergent, and thus $\approx_{R(S_n)}$ and $\downarrow_{R(S_n)}$ coincide. Now, we see that the unconditional part of each clause in S_n having the nonempty conditional part does not modify/expand $\approx_{R(S_n)}$ by Definition 30(iii). Since $\approx_{S_n}$ and $\approx_{R(S_n)}$ also coincide, the conclusion follows. □

The above lemma provides a method of deriving an equivalent convergent (unconditional) rewrite system over Σ^* from a conditional equational theory over Σ^* if it can be finitely saturated under $\mathfrak{S}$ with the contraction rules. In what follows, a rewrite system R over Σ^* oriented by $\succ$ can also be viewed as a set of equations over Σ^* (i.e., an equational theory over Σ^*).

If a conditional equational theory $S = S_0$ over Σ^* can be finitely saturated by a fair theorem proving derivation w.r.t. $\mathfrak{S}$ with the contraction rules in some S_n, then solving unification problems over strings w.r.t. S can be reduced to solving unification problems over strings w.r.t. $\approx_{R(S_n)}$ by Lemma 35. In this case, a unification problem $ux \approx^?_S vy$ is reduced to the unification problem $ux \approx^?_{R(S_n)} vy$ for two finite words $u, v \in \Sigma^*$ and $x, y \in X$.

Figure 2 shows the proposed inference system for solving unification problems over strings w.r.t. $\approx_{R(S_n)}$ over strings, which is adapted from the rule-based E-unification algorithm for an unconditional equational theory E in Baader and Snyder (2001). The computation of solving a unification problem can now be proceeded by applying the inference rules in Figure 2 with the initial system of the form $\{ux \approx^? vy\};\emptyset$ in an attempt to reach some terminal system of form $\emptyset;Q$ representing an $R(S_n)$-unifier σ_Q of u and v, which will be discussed in more detail.

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

Trivial: $\dfrac{\{ux \approx^? ux\} \cup P';Q}{P';Q}$ if $u \in \Sigma^*$ and $x \in X$.

Decomposition: $\dfrac{\{sux \approx^? sty\} \cup P';Q}{\{ux \approx^? ty\} \cup P';Q}$ if $s \in \Sigma^* \setminus \{\lambda\}$, $u \in \Sigma^*$, and $x, y \in X$.

Orientation: $\dfrac{\{uy \approx^? x\} \cup P';Q}{\{x \approx^? uy\} \cup P';Q}$ if $u \in \Sigma^* \setminus \{\lambda\}$ and $x, y \in X$.

Variable Elimination: $\dfrac{\{x \approx^? uy\} \cup P';Q}{P'\{x \mapsto uy\};Q\{x \mapsto uy\} \cup \{x \approx uy\}}$ if $u \in \Sigma^*$, $x, y \in X$, and $x \neq y$.

Lazy Paramodulation: $\dfrac{\{e[ux]\} \cup P';Q}{\{lz \approx^? ux, e[rz]\} \cup P';Q\}}$ if $u \in \Sigma^* \setminus \{\lambda\}$, $x \in X$, $l \to r \in R(S_n)$, $lz \to rz$ is a first-order representation of $l \to r$ using a fresh variable $z \in X$, and either u is a prefix of l or l is a prefix of u.

Above, $R(S_n)$ is the rewrite system obtained by orienting each equation in S_n using $\succ$, where S_n is a set of conditional equations finitely saturated under $\mathfrak{S}$ with contraction rules.

Figure 2. The rules of deduction for rule-based $R(S_n)$-unification.

We denote by $\mathfrak{I}$ the inference system consisting of Trivial, Decomposition, Orientation, Variable Elimination, and Lazy Paramodulation (see Figure 2). We denote by $\Longrightarrow$ a transformation on the systems $P;Q$, where a multiset P consists of $R(S_n)$-unification problems and a multiset Q consists of the equations in solved form. A set of equations $\{x_1 \approx t_1, \ldots, x_n \approx t_n\}$ is in *solved form* (Baader and Snyder, 2001) if each variable x_i has a single occurrence in the set. A substitution $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ may be represented by a set of equations in solved form, so for any set of equations Q in solved form, we denote by the corresponding substitution σ_Q. By $\stackrel{*}{\Longrightarrow}$ we denote a sequence of transformations on the systems $P;Q$ including the empty sequence.

Definition 36. *(i) Let $u \in \Sigma^*$ and $x \in X$. We say that $ux\theta$ is an* instance *of ux if $ux\theta \in \Sigma^*$.*
(ii) Let $u \in \Sigma^*$ and $x \in X$. We say that $ux\theta$ is a reduced instance *of ux w.r.t. a rewrite system R over Σ^* if $ux\theta$ is an instance of ux and $x\theta$ is in R-normal form.*
(iii) Let R be a rewrite system over Σ^*. We say that $lx\theta \to rx\theta$ for some substitution θ and $x \in X$ is an instance *of $l \to r \in R$ if $x\theta \in \Sigma^*$. It is a* reduced instance *of $l \to r \in R$ w.r.t. R if $x\theta$ is in R-normal form.*
(iv) Given a conditional equational theory S and a set of variables $V \subseteq X$, we say that a substitution θ is an instance *of a substitution σ on V w.r.t. S if there exists some $w \in \Sigma^*$ such that $x\theta \approx_S x\sigma w$ for all $x \in V$. We write $\sigma \preceq_S^V \theta$ if θ is an instance of σ on V w.r.t. S.*

Example 37. *Let $S = \{abb \approx cdd\}$ and $\phi : ax \approx_S^? cdy$. Then, an S-unifier $\theta = \{x \mapsto bba, y \mapsto da\}$ is an instance of an S-unifier $\sigma = \{x \mapsto bb, y \mapsto d\}$ on V, that is, $\sigma \preceq_S^V \theta$, where $V = \{x, y\}$.*

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

Recall that we write $s[t]_{suf}$ to indicate that t occurs in s as a suffix and (ambiguously) denote by $s[u]_{suf}$ the result of replacing the occurrence of t (as a suffix of s) by u. The following definition is adapted from Baader and Snyder (2001).

Definition 38. *Let R be a convergent rewrite system over Σ^* oriented by $\succ$, and let $ux\theta$ be an instance of ux for some substitution θ, where $u \in \Sigma^*$ and $x \in X$. A rewrite step $ux\theta \to_R u'$ is* constrained *on ux w.r.t. R if the string introduced by the substitution (i.e., $x\theta$) in $ux\theta$ is in R-normal form. A rewrite sequence $ux\theta \xrightarrow{*}_R t$ is* constrained *on ux w.r.t. R if either $ux\theta = t$ or it starts with a rewrite step constrained on ux w.r.t. R, for example,*

$$ux\theta = ux\theta[lz\rho]_{suf} \to_R ux\theta[rz\rho]_{suf} = ux[rz]_{suf}\theta\rho = ux[rz]_{suf}\theta' \xrightarrow{*}_R t$$

and the remainder is constrained on $ux[rz]_{suf}$ w.r.t. R, where $\theta' = \theta\rho$, $lz \to rz$ is a first-order representation of $l \to r \in R$ using a fresh variable $z \in X$ and $lz\rho \to rz\rho$ is a reduced instance of $l \to r \in R$ w.r.t. R. A rewrite proof $sx\theta \xrightarrow{*}_R \cdot \xleftarrow{*}_R ty\tau$ is constrained *for $sx\theta$ and $ty\tau$ w.r.t. R if the left-hand side is constrained on sx w.r.t. R and the right-hand side is constrained on ty w.r.t. R.*

Lemma 39. *Let R be a convergent rewrite system over Σ^* oriented by $\succ$. For any $s, t \in \Sigma^*$, $x, y \in X$, where $sx\theta$ (resp. $ty\theta$) is a reduced instance of sx (resp. ty) w.r.t. R for some substitution θ, the following are equivalent:*

(i) $sx\theta \approx_R ty\theta$, where R is viewed as a set of equations over Σ^*.
(ii) There exists a constrained rewrite proof for $sx\theta$ and $ty\theta$ w.r.t. R.

Proof. Since R is convergent on Σ^* by Lemma 34, $sx\theta \approx_R ty\theta$ if and only if there exists a rewrite proof for $sx\theta$ and $ty\theta$ using instances of rules from R.

It remains to show that such a rewrite proof can be a constrained rewrite proof for $sx\theta$ and $ty\theta$ w.r.t. R. Since R is convergent on Σ^*, we choose the *rightmost reduction* strategy for R, where the rightmost reduction strategy always contracts a rightmost redex (i.e., a redex occurring as a suffix) in a reducible string over Σ^* using instances of rules from R. At each step of a rewrite proof, among all the possible instances of rules from R that could be used for rightmost reduction, we choose one that is minimal w.r.t. $\succ^{lex}$ (i.e., the lexicographic extension of $\succ$ to pairs of strings over Σ^*). This means that for any instance $lz\rho \to rz\rho$ of $l \to r \in R$ with a fresh variable $z \in X$ used in a rewrite proof for $sx\theta$ and $ty\theta$, $lz\rho \to rz\rho$ must be a reduced instance of $l \to r$ w.r.t. R. Also, $sx\theta$ and $ty\theta$ are reduced instances of sx and ty w.r.t. R, respectively, so we may infer that there exists a constrained rewrite proof for $sx\theta$ and $ty\theta$ w.r.t. R. □

The following theorem shows the completeness of $\mathfrak{I}$ for solving an S-unification problem over Σ^* if a conditional equational theory S over Σ^* can be finitely saturated under $\mathfrak{S}$ with the contraction rules.[9] Note that unification in conditional equational theories over strings is undecidable in general because unification in (unconditional) equational theories over strings is undecidable (Otto et al., 1998). In what follows, given a set of S-unification problems P and a set of equations in solved form Q, by $Vars(P)$ and $Vars(Q)$, we denote the set of variables occurring in P and Q, respectively. Also, $Vars(P, Q)$ denotes the set of all variables occurring in P or Q. By $P\theta$, we denote a substitution θ applied to P in such a way that θ is applied to each of the equations in P. By $Dom\,\tau$ for a substitution τ, we denote $Dom\,\tau := \{x \in X \mid x\tau \neq x\}$. We say that a substitution θ is an *S-solution* of $P;Q$ if θ is an S-unifier of each of the equations in P and Q. It is a *reduced* S-solution of $P;Q$ over Σ^* if $x\theta$ is in $R(S)$-normal form for all $x \in Vars(P, Q)$.

Theorem 40. *Let $S = S_0, S_1, \ldots$ be a fair theorem proving derivation w.r.t. $\mathfrak{S}$ with the contraction rules and let S_n for some n be finitely saturated under $\mathfrak{S}$ with the contraction rules. If θ is an S-solution of $P;\emptyset$, then there exists a sequence $P;\emptyset \overset{*}{\Longrightarrow} \emptyset;Q$ (with Q in solved form) by the calculus $\mathfrak{I}$ such that $\sigma_Q \preceq_S^V \theta$ for $V = Vars(P)$.*

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

Proof. Since S_n is finitely saturated under $\mathfrak{S}$ with the contraction rules, $\approx_S$ and $\approx_{R(S_n)}$ coincide by Lemma 35. If θ is an S-solution of $P;\emptyset$, then we may instead consider a reduced $R(S_n)$-solution θ' of $P;\emptyset$ with $Dom\,\theta' = Dom\,\theta$ and $x\theta' \approx_S x\theta$ for all $x \in Dom\,\theta'$.

We now define a measure of $P;Q$ and its solution τ using a quadruple $< m, n_1, n_2, n_3 >$ (cf. Baader and Snyder (2001)), ordered by the well-founded lexicographic ordering on quadruples of natural numbers. Here,

$m =$ The total number of rewrite steps by $R(S_n)$ in all the minimal-length constrained rewrite proofs for equations in $P\tau$ w.r.t. $R(S_n)$;

$n_1 =$ The number of distinct variables occurring in equations $ux \approx^? vy \in P$, where $u, v \in \Sigma^*$, $x, y \in X$, $ux\tau = vy\tau$, and $ux\tau$ is in $R(S_n)$-normal form;

$n_2 =$ The number of symbols occurring in equations $ux \approx^? vy \in P$, where $u, v \in \Sigma^*$, $x, y \in X$, $ux\tau = vy\tau$, and $ux\tau$ is in $R(S_n)$-normal form;

$n_3 =$ The number of equations in P of the form $uy \approx^? x$, where $u \in \Sigma^* \setminus \{\lambda\}$, $x, y \in X$, $uy\tau = x\tau$, and $uy\tau$ is in $R(S_n)$-normal form.

We show by induction using this measure in such a way that if θ' is a $R(S_n)$-reduced solution of a system $P;Q'$ (with Q' in solved form), then there exists a transformation sequence $P;Q' \overset{*}{\Longrightarrow} \emptyset;Q$ by the calculus $\mathfrak{I}$, where $\sigma_Q \preceq^V_{R(S_n)} \theta'$ for $V = Vars(P, Q')$.

Let θ' be a $R(S_n)$-reduced solution of a system $P;Q'$. The base case is $\emptyset;Q$, which is straightforward because *a fortiori* $\sigma_Q \preceq^V_{R(S_n)} \theta'$ for $V = Vars(Q)$. For the induction step, suppose $P = \{ux \approx^? vy\} \cup P'$ for some $u, v \in \Sigma^*$ and $x, y \in X$. If $ux\theta' = vy\theta'$ and $ux\theta'$ is in $R(S_n)$-normal form, then we proceed a transformation step $P;Q' \Longrightarrow P';Q''$ using the Trivial, Decomposition, Orientation, or the Variable Elimination rule. Since $P';Q''$ is a smaller system w.r.t. the measure having the same $R(S_n)$-reduced solution θ' with $Vars(P', Q'') \subseteq Vars(P, Q')$, the induction hypothesis yields $P';Q'' \overset{*}{\Longrightarrow} \emptyset;Q$. Thus, we have $P;Q' \Longrightarrow P';Q'' \overset{*}{\Longrightarrow} \emptyset;Q$ such that $\sigma_Q \preceq^V_{R(S_n)} \theta'$ for $V = Vars(P, Q')$.

Otherwise, by Lemmas 34 and 39, there exists a constrained rewrite proof of the minimal length for $ux\theta'$ and $vy\theta'$ w.r.t. $R(S_n)$. Without loss of generality, consider a rewrite step from $ux\theta'$ in a minimal-length constrained rewrite proof $ux\theta'[u'x\theta']_{suf} \rightarrow_{R(S_n)} ux\theta'[rz\rho]_{suf} = ux[rz]_{suf}\theta'\rho \overset{*}{\rightarrow}_{R(S_n)} \cdot \overset{*}{\leftarrow}_{R(S_n)} vy\theta'$ w.r.t. $R(S_n)$, where $lz\rho \rightarrow rz\rho$ is a reduced instance of $l \rightarrow r \in R(S_n)$ w.r.t. $R(S_n)$ and $u'x\theta' = lz\rho$. Let $\theta'' = \theta'\rho$. Then, there exists a transformation step $\{ux[u'x]_{suf} \approx^? vy\} \cup P';Q' \Longrightarrow \{lz \approx^? u'x, ux[rz]_{suf} \approx^? vy\} \cup P';Q'$ by Lazy Paramodulation to a new system having a smaller complexity measure (in the first component) w.r.t. its new solution θ''. By the induction hypothesis, we have $\{lz \approx^? u'x, ux[rz]_{suf} \approx^? vy\} \cup P';Q' \overset{*}{\Longrightarrow} \emptyset;Q$ such that $\sigma_Q \preceq^{V'}_{R(S_n)} \theta''$ with $V' = Vars(l, r, P, Q')$. Since $x\theta' = x\theta''$ for every $x \in Vars(P, Q')$, we have $\sigma_Q \preceq^V_{R(S_n)} \theta'$ with $V = Vars(P, Q')$.

Now, we have $\sigma_Q \preceq^V_S \theta'$ for $V = Vars(P, Q')$ and $\theta' \preceq^V_S \theta$ for $V = Vars(P, Q')$, and thus $\sigma_Q \preceq^V_S \theta$ for $V = Vars(P, Q')$, where $\approx_S$ and $\approx_{R(S_n)}$ coincide by Lemma 35. □

Example 41. *Consider the conditional equational theory S consisting of the following conditional equations 1: $bb \approx \lambda$, 2: $a \approx b$, and 3: $bb \not\approx \lambda \vee a \not\approx b \vee bc \approx cb$ with $a \succ b \succ c$. We have a saturated set S_n for some n under $\mathfrak{S}$ with the contraction rules. It is easy to see that the rewrite system $R(S_n)$ consists of the following rules $1' : bb \rightarrow \lambda$, $2' : a \rightarrow b$, and $3' : bc \rightarrow cb$. We may infer that it is also convergent on Σ^*. Now, consider the unification problem problem $\phi := ccbx \approx^? cbay$ for $x, y \in X$ w.r.t. S. We have the following inference steps by $\mathfrak{I}$ using $R(S_n)$.*

(i) Let $P_0;\emptyset$, where $P = P_0 = \{ccbx \approx^? cbay\}$.
(ii) Decomposition: $P_1;\emptyset$, where $P_1 = \{cbx \approx^? bay\}$.
(iii) Lazy Paramodulation: $P_2;\emptyset$, where $P_2 = \{az_1 \approx^? ay\} \cup \{cbx \approx^? bbz_1\}$. Here, the "Lazy

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

Paramodulation" rule is applied to ay in P_1 using $2'$ with a fresh variable $z_1 \in X$ (i.e., $az_1 \to bz_1$).
(iv) Decomposition: P_3;$\emptyset$, where $P_3 = \{z_1 \approx^? y\} \cup \{cbx \approx^? bbz_1\}$.
(v) Lazy Paramodulation: P_4;$\emptyset$, where $P_4 = \{bbz_2 \approx^? bbz_1\} \cup \{z_1 \approx^? y\} \cup \{cbx \approx^? z_2\}$. Here, the "Lazy Paramodulation" rule is applied to bbz_1 in P_3 using $1'$ with a fresh variable $z_2 \in X$ (i.e., $bbz_2 \to z_2$).
(vi) Decomposition: P_5;$\emptyset$, where $P_5 = \{z_2 \approx^? z_1\} \cup \{z_1 \approx^? y\} \cup \{cbx \approx^? z_2\}$.
(vii) Variable Elimination: P_6;Q_1, where $P_6 = \{z_1 \approx^? y\} \cup \{cbx \approx^? z_1\}$ and $Q_1 = \{z_2 \approx z_1\}$.
(viii) Variable Elimination: P_7;Q_2, where $P_7 = \{cbx \approx^? y\}$ and $Q_2 = \{z_2 \approx y\} \cup \{z_1 \approx y\}$.
(ix) Orientation: P_8;Q_2, where $P_8 = \{y \approx^? cbx\}$ and $Q_2 = \{z_2 \approx y\} \cup \{z_1 \approx y\}$.
(x) Variable Elimination: P_9;Q_3, where $P_9 = \emptyset$ and $Q_3 = \{z_2 \approx cbx\} \cup \{z_1 \approx cbx\} \cup \{y \approx cbx\}$.

Now, we have the general form of S-unifiers $\{y \mapsto cbx\}$ for $\phi := ccbx \approx^? cbay$, where x can be mapped to any string $w \in \Sigma^*$. For instance, $\{x \mapsto \lambda, y \mapsto cb\}$ is an S-unifier for ϕ.

8. Related Work

Equational reasoning on strings has been studied extensively in the context of string rewriting systems and Thue systems (Book and Otto, 1993) and their related algebraic structures. The monotonicity assumption used in this paper is found in string rewriting systems and Thue systems in the form of a congruence relation (see, e.g., Book and Otto (1993); Kapur and Narendran (1985)). See Book and O'Dunlaing (1981); Cremanns and Otto (2002); Madlener et al. (1991); Otto et al. (1997) also for the completion of algebraic structures and decidability results using string rewriting systems, in particular *cross sections* for finitely presented monoids discussed by Otto et al. Otto et al. (1997). However, those systems are not concerned with equational theorem proving for general clauses over strings. If the monotonicity assumption is discarded, then equational theorem proving for clauses over strings can be handled by traditional superposition calculi or SMT with the theory of equality with uninterpreted functions (EUF) and their variants (Barrett et al., 2009) using a simple translation into first-order ground terms. Also, efficient SMT solvers for various string constraints were discussed in the literature, see for example Liang et al. (2016).

Meanwhile, equational theorem proving modulo associativity was studied in Rubio (1996), and equational theorem proving modulo equational theories satisfying certain properties was discussed in Kim and Lynch (2021). See also Kutsia (2002) for equational theorem proving with *sequence variables* and fixed or variadic arity symbols. In particular, the inference rules and the redundancy criteria used in both Rubio (1996) and Kim and Lynch (2021) are not directly applicable to equational theorem proving for general clauses over strings discussed in this paper. These approaches are not tailored toward strings, so we need an additional encoding for each string. Also, they are probably less efficient since they are not tailored toward (ground) strings. Furthermore, they neither provide a similar decision procedure for solving word problems in conditional equational theories over strings in Section 6 nor discuss a similar unification procedure in conditional equational theories over strings in Section 7.

An associative commutative (*AC*) congruence closure algorithm (Kapur, 2023) is concerned with the word problem for a finite set of ground equations containing *AC* symbols. (The *AC* properties are not considered in the proposed inference system $\mathfrak{S}$ for clauses over strings.) However, it is not yet known that it can be extended for an equational theorem proving procedure for general clauses, possibly using a string encoding for flat terms.

The proposed calculus is the first sound and refutationally complete equational theorem proving calculus for general clauses over strings under the monotonicity assumption. One may attempt to use the existing superposition calculi for clauses over strings with the proposed translation scheme, which translates clauses over strings into clauses over first-order terms discussed in Section 3.2. However, this does not work because of the Equality Factoring rule (Bachmair and

Ganzinger, 1994; Nieuwenhuis and Rubio, 2001) or the Merging Paramodulation rule (Bachmair and Ganzinger, 1994), which is essential for first-order superposition theorem proving calculi in general. For example, consider a clause $a \approx b \vee a \approx c$ with $a \succ b \succ c$, which is translated into a first-order clause $a(x) \approx b(x) \vee a(y) \approx c(y)$. The Equality Factoring rule yields $b(z) \not\approx c(z) \vee a(z) \approx c(z)$ from $a(x) \approx b(x) \vee a(y) \approx c(y)$, which cannot be translated back into a clause over strings (see Lemma 3). Similarly, a first-order clause produced by Merging Paramodulation may not be translated back into a clause over strings. If one is only concerned with refutational completeness, then the existing superposition calculi[10] can be adapted by using the proposed translation scheme. In this case, a saturated set may not be translated back into clauses over strings in some cases, which is an obvious drawback for its applications (see *programs* in Bachmair and Ganzinger (1994)).

As far as the author knows, conditional completion and unification in conditional equational theories over strings, assuming the monotonicity property of equations over strings, have not been considered in the literature.

Although conditional string rewriting systems were considered in Deiß (1992) for embedding a finitely generated monoid with decidable word problem into a monoid presented by a finite convergent conditional presentation, they are neither concerned with a conditional completion procedure nor concerned with the word problems for conditional equations over Σ^* in general.

Conditional completion and unification in conditional equational theories over Σ^* discussed in this paper are natural extension of completion of string rewriting systems (Book and Otto, 1993) and the first-order unification in equational theories over Σ^* (Otto et al., 1998), respectively, for conditional settings.

9. Conclusion

This paper has presented a new refutationally complete superposition calculus with strings and provided a framework for equational theorem proving for clauses over strings. The results presented in this paper generalize the results on completion of string rewriting systems and equational theorem proving using equations over strings. The proposed superposition calculus is based on the simple string matching methods and the efficient length-lexicographic ordering that allows one to compare two finite strings in linear time for a fixed signature with its precedence.

The proposed approach translates for a clause over strings into the first-order representation of the clause by taking the monotonicity property of equations over strings into account. Then the existing notion of redundancy and model construction techniques for the equational theorem proving framework for clauses over strings has been adapted.

This paper has provided a new decision procedure for solving word problems over strings and a new method of solving unification problems over strings w.r.t. a conditional equational theory S over strings if S can be finitely saturated under the proposed inference system with contraction rules. Here, a conditional equational theory S over Σ^* can be transformed into an equivalent (unconditional) string rewriting system over Σ^*, where an (unconditional) string rewriting system over Σ^* is often simpler and easier to handle in comparison with a conditional equational theory over Σ^*. This transformation can be achieved by rewriting and contracting the conditional part of each (Horn) clause eagerly using unconditional equations during a theorem proving derivation if S can be finitely saturated under the proposed inference system with contraction rules. Furthermore, it aims to make the results of (unconditional) string rewriting systems applicable to conditional equational theories over Σ^*.

Since strings are fundamental objects in mathematics, logic, and computer science including formal language theory, developing applications based on the proposed superposition calculus with strings may be a promising future research direction. Also, the results in this paper may have potential applications in verification systems and solving satisfiability problems (Armando et al., 2003). In addition, it would be an interesting future research direction to extend our superposition calculus with strings to superposition calculi with strings using built-in equational theories, such as commutativity, *idempotency* (Book and Otto, 1993), *nilpotency* (Guo et al., 1996), and their various combinations. For example, research on superposition theorem proving for *commutative monoids* (Rosales et al., 1999) is one such direction. Finally, it would be another potential future research direction to see whether the results discussed in Meseguer (2023) can be adapted for unification in conditional equational theories over strings.

Notes

1 Note that it suffices to assume the right monotonicity property of equations over strings, that is, $s \approx t$ implies $su \approx tu$ for strings s, t, and u, when finding overlaps between equations over strings under the monotonicity assumption.
2 We do not require that $u_1u_2 \approx s$ (resp. $u_2u_3 \approx t$) is strictly maximal in the left premise (resp. the right premise) because of the assumption on the monotonicity property of equations over strings (see also Lemma 3 in Section 3.2).
3 Note that $u_2 \succ t$ implies that u_2 cannot be the empty string λ.
4 One may assume the cancelation property and associate $s \not\approx t$ over strings with $s(x) \not\approx t(x)$ over first-order terms, which is beyond the scope of this paper.
5 Similarly to an equation $s \approx t$ and a negative literal $s \not\approx t$ over Σ^*, a g-equation $s\bot \approx t\bot$ is identified with the multiset $\{\{s\bot\}, \{t\bot\}\}$, while a negative g-literal $s\bot \not\approx t\bot$ is identified with the multiset $\{\{s\bot, t\bot\}\}$, and so on (see Section 2). For example, g-equation $ab\bot \approx bb\bot$ is identified with $\{\{ab\bot\}, \{bb\bot\}\}$, while negative g-literal $ab\bot \not\approx c\bot$ is identified with $\{\{ab\bot, c\bot\}\}$, so $ab\bot \not\approx c\bot \succ_g ab\bot \approx bb\bot$, where $a \succ b \succ c \succ \bot$.
6 Here, an inference by Simplification combines the Deduction step for $C \vee l_1rl_2 \bowtie v$ and the Deletion step for $C \vee l_1ll_2 \bowtie v$ (see the Simplification rule).
7 Note that if $\sim$ is closed under the conditional equations in S, then $l \approx r \in S$ simply implies $l \sim r$.
8 Recall that for Horn clauses, the application of the Rewrite rule in $\mathfrak{S}$ can be replaced by the application of the Simplification rule for the eager application of the contraction rules during a theorem proving derivation w.r.t. $\mathfrak{S}$ with the contraction rules, so we do not need to consider the Rewrite rule here.
9 The soundness of $\mathfrak{I}$ can be proved by a straightforward induction on the length of transformation sequences and hence is omitted (see Gallier and Snyder (1989)).
10 The reader is also encouraged to see *AVATAR modulo theories* (Reger et al., 2016), which is based on the concept of splitting.

References

Armando, A., Ranise, S. and Rusinowitch, M. (2003). A rewriting approach to satisfiability procedures. *Information and Computation* **183** (2) 140–164.

Baader, F. and Nipkow, T. (1998). *Term Rewriting and All That*. Cambridge University Press, Cambridge, UK.

Baader, F. and Snyder, W. (2001). Unification Theory. In: *Handbook of Automated Reasoning*, vol. I, chap. 8, Elsevier, 445–532.

Bachmair, L. and Ganzinger, H. (1994). Rewrite-based equational theorem proving with selection and simplification. *Journal of Logic and Computation* **4** (3) 217–247.

Bachmair, L. and Ganzinger, H. (1995). Associative-commutative superposition. In: Dershowitz, N. and Lindenstrauss, N. (eds.), *Conditional and Typed Rewriting Systems*, Springer, 1–14.

Bachmair, L. and Ganzinger, H. (1998). Equational reasoning in saturation-based theorem proving. In: Bibel, W. and Schmitt, P. H. (eds.), *Automated Deduction. A Basis for Applications*, vol. I, chap. 11. Kluwer, 353–397.

Barrett, C., Sebastiani, R., Seshia, S. A. and Tinelli, C. (2009). Satisfiability modulo theories. In: *Handbook of Satisfiability*, vol. 185. *Frontiers in Artificial Intelligence and Applications*, IOS Press, 825–885.

Book, R. V. and O'Dunlaing, C. P. (1981). Testing for the Church-Rosser property. *Theoretical Computer Science* **16** (2) 223–229.

Book, R. V. and Otto, F. (1993). *String-Rewriting Systems*, Springer.

Cormen, T. H., Leiserson, C. E., Rivest, R. L. and Stein, C. 2001. *Introduction to Algorithms, 2nd edition*. The MIT Press.

Cremanns, R. and Otto, F. (2002). A completion procedure for finitely presented groups that is based on word cycles. *Journal of Automated Reasoning* **28** (3) 235–256.

Deiß, T. (1992). Conditional semi-thue systems for presenting monoids. In: *Annual Symposium on Theoretical Aspects of Computer Science, STACS 1992*, Springer, 557–565.

Dershowitz, N. (1991). Canonical sets of Horn clauses. In: Albert, J. L., Monien, B. and Artalejo, M. R. (eds.), *Automata, Languages and Programming*, Springer Berlin Heidelberg, 267–278.

Dershowitz, N. and Plaisted, D. A. (2001). Rewriting. In: *Handbook of Automated Reasoning*, vol. I, chap. 9. Elsevier, 535–610.

Epstein, D. B. A., Paterson, M., Cannon, J. W., Holt, D. F., Levy, S. V. F. and Thurston, W. (1992). *Word Processing in Groups*. A. K. Peters, Ltd.

https://doi.org/10.1017/S0960129524000112 Published online by Cambridge University Press

Gallier, J. H. and Snyder, W. (1989). Complete Sets of transformations for general E-unification. *Theoretical Computer Science* **67** (2&3) 203–260.

Guo, Q., Narendran, P. and Wolfram, D. A. (1996). Unification and matching modulo nilpotence. In: McRobbie, M. A. and Slaney, J. K. (eds.), *The 13th International Conference on Automated Deduction (CADE-13)*, vol. 1104. *Lecture Notes in Computer Science*, Springer, 261–274.

Holt, D. F., Eick, B. and O'Brien, E. A. (2005). *Handbook of Computational Group Theory*. CRC Press.

Kaplan, S. (1987). Simplifying conditional term rewriting systems: Unification, termination and confluence. *Journal of Symbolic Computation* **4** (3) 295–334.

Kapur, D. (2023). Modularity and combination of associative commutative congruence closure algorithms enriched with semantic properties. *Logical Methods in Computer Science* **19** (1).

Kapur, D. and Narendran, P. (1985). The Knuth-Bendix completion procedure and Thue systems. *SIAM Journal on Computing* **14** (4) 1052–1072.

Kim, D. (2022). Equational theorem proving for clauses over strings. In: Nantes-Sobrinho, D. and Fontaine, P. (eds.), *Proceedings 17th International Workshop on Logical and Semantic Frameworks with Applications, LSFA 2022, Belo Horizonte, Brazil (Hybrid), 23–24 September 2022*, vol. 376. *EPTCS*, 49–66.

Kim, D. and Lynch, C. (2021). Equational theorem proving modulo. In: *The 28th International Conference on Automated Deduction (CADE-28)*, vol. 12699. *Lecture Notes in Computer Science*. Springer, 166–182.

Kutsia, T. (2002). Theorem proving with sequence variables and flexible arity symbols. In Baaz, M. and Voronkov, A. (eds.) *Logic for Programming, Artificial Intelligence, and Reasoning, 9th International Conference, LPAR 2002, Tbilisi, Georgia, October 14–18, 2002, Proceedings*, vol. 2514. *Lecture Notes in Computer Science*. Springer, 278–291.

Liang, T., Reynolds, A., Tsiskaridze, N., Tinelli, C., Barrett, C. and Deters, M. (2016). An efficient SMT solver for string constraints. *Formal Methods in System Design* **48** (3) 206–234.

Madlener, K., Narendran, P. and Otto, F. (1991). A specialized completion procedure for monadic string-rewriting systems presenting groups. In Albert, J. L., Monien, B. and Rodríguez-Artalejo, M. (eds.), *Automata, Languages and Programming, 18th International Colloquium, ICALP91, Madrid, Spain, July 8–12, 1991, Proceedings*, vol. 510. *Lecture Notes in Computer Science*. Springer, 279–290.

Meseguer, J. (2023). Variants and satisfiability in the infinitary unification wonderland. *Journal of Logical and Algebraic Methods in Programming* **134** 100877.

Nieuwenhuis, R. and Rubio, A. (2001). Paramodulation-based theorem proving. In: *Handbook of Automated Reasoning*, vol. I, chap. 7. Elsevier, 371–443.

Otto, F., Katsura, M. and Kobayashi, Y. (1997). Cross-sections for finitely presented monoids with decidable word problems. In: Comon, H. (ed.), *Rewriting Techniques and Applications, 8th International Conference, RTA-97, Sitges, Spain, June 2–5, 1997, Proceedings*, vol. 1232. *Lecture Notes in Computer Science*. Springer, 53–67.

Otto, F., Narendran, P. and Dougherty, D. J. (1998). Equational unification, word unification, and 2nd-order equational unification. *Theoretical Computer Science* **198** (1–2) 1–47.

Reger, G., Bjøner, N., Suda, M. and Voronkov, A. (2016). Avatar modulo theories. In Benzmüller, C., Sutcliffe, G. and Rojas, R. (eds.), *GCAI 2016. 2nd Global Conference on Artificial Intelligence*, vol. 41. *EPiC Series in Computing*, 39–52.

Rosales, J. C., García-Sánchez, P. A. and Urbano-Blanco, J. M. (1999). On presentations of commutative monoids. *International Journal of Algebra and Computation* **09** (05) 539–553.

Rubio, A. (1996). Theorem proving modulo associativity. In Büning, H. K. (ed.), *Computer Science Logic*, Springer, 452–467.

Cite this article: Kim D (2024). Equational theorem proving for clauses over strings. *Mathematical Structures in Computer Science*. https://doi.org/10.1017/S0960129524000112