Strong Symmetrization, Semi-Compatibility of Normalized Rewriting and First-Order Theorem Proving

Jürgen Stuber[*]
Max-Planck-Institut für Informatik

1 Introduction

In automated first-order theorem proving the problems often contain such basic algebraic objects as abelian groups or commutative rings. Theorem provers which treat the axioms of such structures in the same way as the problem-specific part often run into a combinatoric explosion of the search space, due to prolific axioms like associativity, commutativity, distributivity and the inverse law. Our goal is to reduce this search space by incorporating common algebraic theories into specialized calculi. In general we assume that the theory is given as a convergent term rewriting system T modulo some equational axioms E. By systematically considering the interaction between T and problem-specific rules not in T one can show that many inferences become redundant.

A central concept of our approach is symmetrization, which has been invented in the context of (non-abelian) group theory (Le Chenadec 1986). A set S of rewrite rules is symmetrized with respect to T, if all critical peaks between a rule in T and a rule in S converge. Critical peaks between rules in S are not considered. For many important theories the symmetrization is simple enough to immediately read it off ground rewrite rules in a certain normal form, instead of running a completion-like process. And, since the structure of the symmetrization is known beforehand, one can analyse overlaps between two symmetrizations and develop strong critical pair criteria for specific theories.

We introduce strong symmetrization, which goes slightly beyond symmetrization in that it considers overlaps of rules from S within the symmetrization of a single rule. Less strictly speaking, these are overlaps between variants with respect to the theory of a single rule. Fortunately, the symmetrizations of commutative theories which we are interested in are also strong symmetrizations. This is not the case in general; for instance in the context of (non-abelian) groups, rules can have non-trivial overlaps with themselves.

The advantage of strong symmetrization is that it implies that normalized rewriting is *semi-compatible*. That is, if we put a context around a normalized rewrite step $s \to t$ there exists a normalized valley proof $u[s] \downarrow u[t]$. In completeness proofs for first-order theorem proving with respect to a built-in theory we often have the situation that by induction hypothesis a proof exist for a simpler case, and we want to prove that a more complicated case doesn't need to be considered by an inference rule. The main technique is to take the simple proof and transform it into a proof of the more complicated equation by putting a suitable context around every term in it. However, the induction imposes a bound on the terms in the proof. In cases where terms cancel each other this bound is violated by the terms with context, but may be satisfied by their normal forms. Now by semi-

[*]Address: Max-Planck-Institut für Informatik, Im Stadtwald, D-66123 Saarbrücken, Germany. Phone: +49-681-9325-228, Fax: +49-681-9325-299, Email: `juergen@mpi-sb.mpg.de`

compatibility every rewrite step in the original proof is transformed into a valley proof, which is bounded by the terms on its ends. Hence all terms in the new proof stay below the bound. In our completeness proofs we use this technique both for proving critical pair criteria and for simplifying equations to normal form. As an example we will show such a simplification for the case of commutative rings. Previously, Bachmair, Ganzinger and Stuber (1995) could not handle this case in their calculus for commutative rings, because their completeness proof was based on a different technique.

Our work generalizes and makes explicit the construction of Bündgen (1996). He considers the special case of polynomial rings in order to formalize the relation between Knuth-Bendix completion and Gröbner-base computation. Normalized rewriting is due to Marché (1996), who develops Knuth-Bendix completion for built-in theories. For abelian groups he also defines normal forms (which he calls symmetrization), but he explicitly adds extended rules to obtain convergence with the theory. He doesn't consider special critical pair criteria for overlaps of symmetrizations. Note that the construction in this paper is needed for rings but not for abelian groups or integer modules (Stuber 1996).

2 Preliminaries

We assume that the reader is familiar with term rewriting (Dershowitz and Jouannaud 1990). We write $s \overset{!}{\rightarrow} t$ if $s \overset{*}{\rightarrow} t$ and t is irreducible; that is, t is a normal form of s. We write $T(s)$ for the normal form of s with respect to a convergent term rewriting system T. We use $\approx$ for object-level equality. For commutative rings we use the following well-known term rewriting system *CR* modulo *AC* of Peterson and Stickel (1981):

$$\begin{aligned} x + 0 &\rightarrow x & -(x+y) &\rightarrow (-x) + (-y) \\ x + (-x) &\rightarrow 0 & x \cdot 0 &\rightarrow 0 \\ x + y + (-y) &\rightarrow x & x \cdot 1 &\rightarrow x \\ -0 &\rightarrow 0 & x \cdot (y+z) &\rightarrow (x \cdot y) + (x \cdot z) \\ -(-x) &\rightarrow x & x \cdot (-y) &\rightarrow -(x \cdot y) \end{aligned}$$

Function symbols not occurring in *CR* are called *free*, terms with a free symbol at the root are called *CR-atomic*, and terms of the form $t_1 \cdots t_k$ where $t_1, \ldots, t_k$ are atomic are called *products* and denoted by ϕ.

Lemma 2.1 (Peterson and Stickel 1981) *CR is convergent modulo AC.*

We use a simplification ordering $\succ$ which is AC-compatible, total on ground terms, and which orients the rules in *CR* and in the symmetrization below left-to-right. Such an ordering can be constructed as the lexicographic combination of the MAPO of Delor and Puel (1993), the polynomial ordering of Peterson and Stickel (1981), and the AC-RPO of Rubio and Nieuwenhuis (1993).

3 Symmetrization

A set of rewrite rules S is called *symmetrized* with respect to T modulo E if for all peaks $t_1 \leftarrow_{E\backslash T} t \rightarrow_{E\backslash S} t_2$ and for all cliffs $t_1 \leftrightarrow_E t \rightarrow_{E\backslash S} t_2$ we have $t_1 \downarrow_{E\backslash(T\cup S)} t_2$. The set S is called *strongly symmetrized* with respect to T modulo E if it can be partitioned into sets $S_i,\ i \in I$, such that $T \cup S_i$ is convergent modulo E for all $i \in I$.

Proposition 3.1 *If a set of rewrite rules S is strongly symmetrized with respect to T modulo E then S is symmetrized with respect to T modulo E.*

Proof: Consider some peak $t_1 \leftarrow_{E\backslash T} t \rightarrow_{E\backslash S} t_2$ or cliff $t_1 \leftrightarrow_E t \rightarrow_{E\backslash S} t_2$. The rule from S is in some S_i, and by convergence of $T \cup S_i$ we get the desired valley proof. □

Note that S being strongly symmetrized implies that peaks of the form $t_1 \leftarrow_{E\backslash S_i} t \rightarrow_{E\backslash S_i} t_2$ converge, which is not guaranteed if S is symmetrized but not strongly symmetrized.

In order to give a simple correspondence between equations and their symmetrizations we restrict the computation of symmetrizations to a certain subset of ground equations Norm_T. The equations in Norm_T are said to be in *T-normal form.* Then a (strong) *symmetrization function* $\mathcal{S}_T$ (for T) maps each equation $l \approx r$ in T-normal form to a (strongly) symmetrized set of rewrite rules $\mathcal{S}_T(l \approx r)$ such that $E \cup T \cup \{l \approx r\} \models \mathcal{S}_T(l \approx r)$ and $l \downarrow_{E\backslash(T \cup \mathcal{S}_T(l \approx r))} r$. We call a rule $l' \rightarrow r'$ in $\mathcal{S}_T(l \rightarrow r) \backslash \{l \rightarrow r\}$ an *extension* (of $l \rightarrow r$).

For commutative rings we say that a ground equation is in *CR-normal form* if it is of one of the forms (i) $0 \approx 0$; (ii) $n\phi \approx r$ where $n \geq 1$ and $\phi \succ r$. Note that the right-hand side cannot contain ϕ. Also, r need not be irreducible with respect to *CR*, in order to avoid unneccessary *CR*-rewrite steps which would lead to additional inferences. The symmetrization function can be determined by hand by starting with an equation in normal form and adding critical pairs. For commutative rings we obtain:

$$\begin{aligned}
\mathcal{S}_{CR}(0 \approx 0) &= \emptyset && (1)\\
\mathcal{S}_{CR}(t \approx r) &= \{t \rightarrow r\} && (2)\\
\mathcal{S}_{CR}(\phi \approx r) &= \{\phi \rightarrow r\} && (3)\\
&\quad \cup \{u\phi \rightarrow u \cdot r \mid u \text{ ground term}\} && (4)\\
\mathcal{S}_{CR}(n\phi \approx r) &= \{n\phi \rightarrow r\} && (5)\\
&\quad \cup \{n(u\phi) \rightarrow u \cdot r \mid u \text{ ground term}\} && (6)\\
&\quad \cup \{u + n\phi \rightarrow u + r \mid u \text{ ground term}\} && (7)\\
&\quad \cup \{u_1 + n(u_2\phi) \rightarrow u_1 + u_2 r \mid u_1 \text{ and } u_2 \text{ ground terms}\} && (8)\\
&\quad \cup \{-\phi \rightarrow (n-1)\phi + (-r)\} && (9)\\
&\quad \cup \{-(u\phi) \rightarrow (n-1)(u\phi) + u(-r) \mid u \text{ ground term}\} && (10)
\end{aligned}$$

Proposition 3.2 *$\mathcal{S}_{CR}$ is a strong symmetrization function for CR modulo AC.*

Proof: By case analysis on all peaks and cliffs in $\mathit{CR} \cup \mathcal{S}_{CR}(l \approx r)$ for all $l \approx r$. Each S_i is chosen as the symmetrization of a single equation. We have also used the Cime system of Marché to verify this for some special cases of n and ϕ. □

4 Unrestricted vs. Normalized Rewriting

Normalized rewriting gives rules from T priority over rules from S. It is due to Marché (1996). For rewrite relations $\rightarrow_{E\backslash R}$ and $\rightarrow_{E\backslash T}$ we define *T-normalized rewriting with R* by $s \rightarrow_{E\backslash(T!R)} t$ if and only if $s \overset{!}{\rightarrow}_{E\backslash T} u$ and $u \rightarrow_{E\backslash R} t$. We write $s \downarrow_{E\backslash(T!R)} t$ for a valley proof of the form $s \overset{*}{\rightarrow}_{E\backslash(T!R)} s' \overset{*}{\leftrightarrow}_E t' \overset{*}{\leftarrow}_{E\backslash(T!R)} t$ and say that $E\backslash(T!R)$ is *Church-Rosser modulo E* if $s \overset{*}{\leftrightarrow}_{E \cup T \cup R} t$ implies that $s \downarrow_{E\backslash(T \cup R)} t$ for all terms s and t.

Lemma 4.1 *Let $T \cup R$ be terminating modulo E. Then $E\backslash(T \cup R)$ is Church-Rosser modulo E if and only if $E\backslash(T!R)$ is Church-Rosser modulo E.*

Proof: Since $\downarrow_{E\backslash(T!R)} \subseteq \downarrow_{E\backslash(T \cup R)}$ the if-direction is trivial. For the only-if-direction the proof is by induction on the following proof ordering: Let $\succ$ be $\overset{*}{\rightarrow}_{(T \cup R)/E}$ extended by a new minimal element $\bot$. We order proof steps with respect to $\succ$ according to the complexity measure

$$\begin{aligned} c(s \rightarrow_{E\backslash R} t) = c(t \leftarrow_{E\backslash R} s) &= s \\ c(s \rightarrow_{E\backslash T} t) = c(t \leftarrow_{E\backslash T} s) &= \bot \\ c(s \leftrightarrow_{E} t) &= \bot, \end{aligned}$$

i.e., only the larger sides of R-steps count. As the proof ordering we use the multiset extension of the ordering on proof steps. Consider some proof $s \overset{*}{\leftrightarrow}_{E \cup T \cup R} t$. Then $s \downarrow_{E\backslash(T\cup R)} t$. Suppose $s \not\downarrow_{E\backslash(T!R)} t$, then there exists an R-step $u \rightarrow_{E\backslash R} v$ (or $v \leftarrow_{E\backslash R} u$) in $s \downarrow_{E\backslash(T\cup R)} t$ whose larger side u is reducible by T. For $u' \leftarrow_{E\backslash T} u \rightarrow_{E\backslash R} v$ there exists a proof $u' \downarrow_{E\backslash(T\cup R)} v$, and we may replace the subproof $u \rightarrow_{E\backslash R} v$ by the smaller subproof $u \rightarrow_{E\backslash T} u' \downarrow_{E\backslash(T\cup R)} v$. All in all we obtain a smaller proof $s \downarrow_{E\backslash(T\cup R)} u' \downarrow_{E\backslash(T\cup R)} v \downarrow_{E\backslash(T\cup R)} t$ and by induction hypothesis $s \downarrow_{E\backslash(T!R)} t$, a contradiction. □

This suggests that T-normalized rewriting with R can be interchanged with rewriting with $T \cup R$, without a change in the critical pairs to be considered.

5 Semi-Compatibility of Normalized Rewriting

A relation $\rightarrow_R$ is *semi-compatible* if $s \rightarrow_R t$ implies $u[s] \downarrow_R u[t]$ for all terms s and t and contexts u. Semi-compatibility was introduced by Bündgen (1996).

Lemma 5.1 *Let S be a set of ground rewrite rules which is strongly symmetrized with respect to T modulo E. Then T-normalized rewriting with R modulo E is semi-compatible.*

Proof: Consider a rewrite step $s \rightarrow_{E\backslash(T!S)} t$ and a context u. Then there exists a not necessarily normalized valley proof of $u[s] \approx u[t]$ by putting the context u around every term in the proof that represents the normalized rewrite step. Since this proof contains only one S-step all needed rules are in $T \cup S_i$ for some $i \in I$, where $(S_i)_{i\in I}$ is the partition of S in the definition of strong symmetrization. Since $T \cup S_i$ is convergent modulo E, by Lemma 4.1 there also exists a valley proof of $u[s] \approx u[t]$ by normalized rewriting. □

Without strong symmetrization it is not possible to remove all peaks between two rules from S, which are introduced when the symmetrization property is applied to remove several S/T-peaks consecutively. These S/S-peaks are not bounded by the normal form of a term in the original proof with added context. In contrast to this, strong symmetrization and in turn semi-compatibility of normalized rewriting lead to proofs which are bounded by the T-normal forms of the terms in the proof with added context.

$$\begin{tikzcd}
u[t_1] \arrow[d, "T"', "!"] & & & u[t_2] \arrow[d, "T"', "!"] & & & u[t_3] \arrow[d, "T"', "!"] \\
T(u[t_1]) \arrow[dr, "*", "T\cup S"'] & & & T(u[t_2]) \arrow[dl, "*"', "T\cup S"] \arrow[dr, "*", "T\cup S"'] & & & T(u[t_3]) \arrow[dl, "*"', "T\cup S"] \\
& \cdot \arrow[r, leftrightarrow, "*", "E"'] & \cdot & & \cdot \arrow[r, leftrightarrow, "*", "E"'] & \cdot &
\end{tikzcd}$$

6 An Application to First-Order Theorem Proving

In the calculus specialized to commutative rings we have the following special case of the Isolation ground inference, which is used to bring negative literals into T-normal form:

$$\frac{p \not\approx -\phi + q}{\phi \not\approx q + (-p)}$$

where $\phi \succ p$ and $\phi \succ q$. In the completeness proof we have to infer from the existence of a valley proof $p \downarrow_{T \cup S} -\phi + q$ that there exists a proof of $\phi \approx q + (-p)$ which is bounded by $-\phi + q$. The following diagram shows how this is achieved:

$$\begin{tikzcd}
\phi + (-p) + \boxed{p} \arrow[dd, "*"', "CR"] \arrow[dr, dashed, "*", "CR\cup S"'] & & \boxed{-\phi + q} + \phi + (-p) \arrow[dl, dashed, "*"', "CR\cup S"] \arrow[dd, "*"', "CR"] \\
& \phi + (-p) + \boxed{t_0} & \\
\phi \arrow[rr, dotted, leftrightarrow, bend right, "\preceq -\phi+q", "AC\cup CR\cup S"'] & & (-p) + q
\end{tikzcd}$$

The dotted proof results from taking the dashed proof, which operates on the boxed formulas, putting the context $\phi + (-p) + [\,]$ around it, and using the construction of the previous section. Finally, the dotted proof stays below the bound $-\phi$, because the normal forms in the transformed proof contain no negated occurrence of the maximal term ϕ, and the ordering is constructed in such a way that any number of positive occurrences is always smaller than one negative occurrence.

Acknowledgments

I thank Uwe Waldmann for his helpful comments on this paper.

References

BACHMAIR, L., GANZINGER, H. AND STUBER, J. (1995). Combining algebra and universal algebra in first-order theorem proving: The case of commutative rings. In *Proc. 10th Workshop on Specification of Abstract Data Types*, Santa Margherita, Italy, LNCS 906. Springer.

BÜNDGEN, R. (1996). Buchberger's algorithm: The term rewriter's point of view. *Theoretical Computer Science* **159**: 143–190.

DELOR, C. AND PUEL, L. (1993). Extension of the associative path ordering to a chain of associative commutative symbols. In *Proc. 5th Int. Conf. on Rewriting Techniques and Applications*, LNCS 690, pp. 389–404. Springer.

DERSHOWITZ, N. AND JOUANNAUD, J.-P. (1990). Rewrite systems. In J. van Leeuwen (ed.), *Handbook of Theoretical Computer Science: Formal Models and Semantics*, Vol. B, chapter 6, pp. 243–320. Elsevier/MIT Press.

LE CHENADEC, P. (1986). *Canonical Forms in Finitely Presented Algebras.* Pitman, London.

MARCHÉ, C. (1996). Normalised rewriting: an alternative to rewriting modulo a set of equations. *Journal of Symbolic Computation* **21**: 253–288.

PETERSON, G. E. AND STICKEL, M. E. (1981). Complete sets of reductions for some equational theories. *Journal of the ACM* **28**(2): 233–264.

RUBIO, A. AND NIEUWENHUIS, R. (1993). A precedence-based total AC-compatible ordering. In *Proc. 5th Int. Conf. on Rewriting Techniques and Applications*, LNCS 690, pp. 374–388. Springer.

STUBER, J. (1996). Superposition theorem proving for abelian groups represented as integer modules. In H. Ganzinger (ed.), *Proc. 7th Int. Conf. on Rewriting Techniques and Applications*, New Brunswick, NJ, USA, LNCS 1103, pp. 33–47. Springer.