Knuth-Bendix Completion of Theories of Commuting Group Endomorphisms

Aaron Stump[a] and Bernd Löchner[b]

[a] *Computer Science and Engineering, Washington University, St. Louis, USA*

[b] *FB Informatik, Technische Universität Kaiserslautern, Kaiserslautern, Germany*

Abstract

Knuth-Bendix completions of the equational theories of $k \geq 2$ commuting group endomorphisms are obtained, using automated theorem proving and modern termination checking. This improves on modern implementations of completion, where the orderings implemented cannot orient the commutation rules. The result has applications in decision procedures for automated verification.

Key words: Knuth-Bendix completion, group theory, decision procedures

1 Introduction

Decision procedures for first-order theories like fragments of arithmetic or theories of arrays are the subject of current intensive study for their applications in automated verification. Modern decision procedures for satisfiability modulo such theories are built by combining techniques for fast propositional reasoning with theory specific reasoners. It has been empirically established that a tight interaction between the theory reasoner and the propositional reasoner is critical for high performance [1]. One point of interaction occurs when the theory reasoner detects that the assignment chosen by the propositional reasoner is inconsistent modulo the background theory. In this case, the theory solver should identify as small a subset as possible of the current assignment which is still inconsistent. Such a subset is used as the basis for a *conflict clause*, which is a crucial guide in the subsequent propositional search.

Recent works have explored ways to reduce the size of conflict clauses generated by theory reasoners for equality with uninterpreted functions [7,8,2]. The latter two cited works explicitly mine proofs of contradictions to obtain small conflict clauses. In the cited work by the first author, an algebraic approach to proof mining is described, where equality proofs are mined by transforming them according to certain algebraic laws. Under a natural assumption, used also in the other cited works, of independence of the asserted equations, it turns out that the algebra of equality proofs, viewed as first-order terms, is the theory of free groups. Reflexivity, viewed as a 0-ary proof term constructor proving $t = t$ for any term t, plays the role of the unit element; symmetry, viewed as taking a proof of $x = y$ as an argument and producing a proof of $y = x$, plays the role of the inverse operation; and transitivity, viewed as taking proofs of $x = y$ and $y = z$ as arguments and producing a proof of $x = z$, plays the role of the multiplication. For example, if D_1 is an assumption that $a = b$, then $\mathit{Trans}(D_1, \mathit{Symm}(D_1))$ proves $a = a$, which is also proved by *Refl*. We define proofs to be equivalent ($\cong$) iff they prove some theorem in common. Written in conventional syntax for group theory, this is the valid equation $D_1 * (D_1)^{-1} = 1$. The cited work takes advantage of the well-known 10-rule Knuth-Bendix completion of the free group axioms to put equality proofs into canonical form [5]. This form turns out to be minimal with respect to the set of assumptions used. Better, by studying the structure of the canonical forms, it is possible to devise an algorithm that mines the set of assumptions that would appear in the canonical form of a proof, without actually rewriting the proof. This algorithm appears to be more efficient than rewriting the proofs, and results in a two-fold speedup on large hardware verification benchmarks [8]. Note that, as described in the cited work, by taking proofs to be equivalent iff they prove a theorem in common, we ensure soundness of the equations (which are unsound with other notions of proof equivalence).

The work just described does not consider congruence proof rules. Subsequent unpublished work by the first author has shown that, under a generalization of the assumption of independence, the algebra of congruence proofs is the theory of commuting group endomorphisms. We have the following proof rule $Cong_{f,i}$ for each argument position $1 \leq i \leq n$ of each function symbol f of arity n, where $y_j \equiv x_j$ for all $1 \leq j \neq i \leq n$:

$$\frac{x_i = y_i}{f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)}$$

Congruence proofs satisfy the equations of Figure 1. The first shows that congruence rules function as endomorphisms, and the second (when $i \neq j$) that they commute. This motivates the search for Knuth-Bendix completions of the theory of k commuting group endomorphisms, CGE_k, for every $k \geq 2$. We begin by finding a completion for $k = 2$ (Section 2), and then show how to generalize this result to all $k > 2$ (Section 3).

$$\begin{aligned}
\mathit{Cong}_{f,i}(\mathit{Trans}(D_1, D_2)) &\cong \mathit{Trans}(\mathit{Cong}_{f,i}(D_1), \mathit{Cong}_{f,i}(D_2)) \\
\mathit{Trans}(\mathit{Cong}_{f,i}(D_1), \mathit{Cong}_{f,j}(D_2)) &\cong \mathit{Trans}(\mathit{Cong}_{f,j}(D_2), \mathit{Cong}_{f,i}(D_1))
\end{aligned}$$

Fig. 1. Equations for Congruence Rules.

$$\begin{array}{lll}
(x * y) * z = x * (y * z) & f(x * y) & = f(x) * f(y) \\
x^{-1} * x \quad = 1 & g(x * y) & = g(x) * g(y) \\
1 * x \quad\quad = x & f(x) * g(y) & = g(y) * f(x)
\end{array}$$

Fig. 2. The Theory of Two Commuting Group Endomorphisms

2 The Completed Theory of Two Commuting Endomorphisms

Figure 2 presents CGE$_2$, and Figure 3 gives a completion of this theory. Rules 1 through 10 are the completion, due to Knuth and Bendix, of the group axioms [5]. Rules 11 through 14 arise from the homomorphism law for f, and rules 15 through 18 from the homomorphism law for g. Rules 19 and 20 are for commutation of f and g. Independently written tools by the first and second author confirm that all 134 critical pairs of this rewrite system are joinable, and the powerful APROVE termination-checking tool easily certifies that the system is terminating [4]. So using Newman's Lemma and the Critical Pair Lemma, the system is confluent. The WALDMEISTER theorem prover confirms that the equational theories of the equations and the rules are the same [6]. Hence, the rules can be used to rewrite any term in the theory to a canonical form, and hence decide the theory.

Today's Knuth-Bendix completion tools cannot obtain a convergent comple-

1.	$(x * y) * z$	$\rightarrow x * (y * z)$	11.	$f(1)$	$\rightarrow 1$
2.	$x^{-1} * x$	$\rightarrow 1$	12.	$(f(x))^{-1}$	$\rightarrow f(x^{-1})$
3.	$x * x^{-1}$	$\rightarrow 1$	13.	$f(x) * f(y)$	$\rightarrow f(x * y)$
4.	$x * (x^{-1} * y)$	$\rightarrow y$	14.	$f(x) * (f(y) * z)$	$\rightarrow f(x * y) * z$
5.	$x^{-1} * (x * y)$	$\rightarrow y$	15.	$g(1)$	$\rightarrow 1$
6.	$(x * y)^{-1}$	$\rightarrow y^{-1} * x^{-1}$	16.	$(g(x))^{-1}$	$\rightarrow g(x^{-1})$
7.	$1 * x$	$\rightarrow x$	17.	$g(x) * g(y)$	$\rightarrow g(x * y)$
8.	$x * 1$	$\rightarrow x$	18.	$g(x) * (g(y) * z)$	$\rightarrow g(x * y) * z$
9.	1^{-1}	$\rightarrow 1$	19.	$f(x) * g(y)$	$\rightarrow g(y) * f(x)$
10.	$(x^{-1})^{-1}$	$\rightarrow x$	20.	$f(x) * (g(y) * z)$	$\rightarrow g(y) * (f(x) * z)$

Fig. 3. The Knuth-Bendix Completion of the Theory

tion of CGE_2, because, as the reader may confirm, the commutation axiom cannot be ordered using any Knuth-Bendix ordering (KBO) or recursive path ordering. These are the only orderings supported by modern completion tools, to the best of the authors' knowledge. The system of Figure 3 is obtained by hand, using custom code to generate critical pairs between a rule from a set of fixed rules, originally rules 1 through 10 for groups, and a focus rule. Beginning with focus rules $f(1) \rightarrow 1$ and $(f(x))^{-1} \rightarrow f(x^{-1})$, even though they are consequences of the homomorphism law for f, enables many later critical pairs to be simplified. Non-joinable critical pairs are oriented by hand. It appears crucial to orient rules 13 and 17 of Figure 3 as they are, in order

k	# R_k	# E_k	*# CPs*	*time (s)*
2	22	2	320	0.01
3	46	24	2676	0.12
4	146	420	229371	34.13
5	670	11240	118887623	81873.09

Fig. 4. For k endomorphisms, the numbers of rules, unoriented equations, critical pairs processed, and time for Waldmeister to complete CGE_k. Experiments were run on a machine with a 1 Ghz Pentium III processor and 4 GByte RAM.

for completion to terminate. When no non-joinable critical pairs remain, we use AProVE to check termination of the resulting system.

3 Generalizing to More Than Two Endomorphisms

Using ordered completion, Waldmeister can obtain a system of rules and unoriented equations with which ground terms can be rewritten using ordered rewriting to canonical form. To obtain the completion, a KBO with the following weights and precedences can be used: $\_^{-1} \mapsto 0, * \mapsto 1, f \mapsto 1, g \mapsto 1, 1 \mapsto 1$; and $\_^{-1} > * > f > g > 1$. This KBO causes rules 13 and 17 of Figure 3 to be oriented as they are. Unfortunately, as shown in Figure 3, this approach does not appear to scale as we increase the number of endomorphisms. Note that the completion for $k = 5$ is by far the largest successful completion the second author (an implementor of Waldmeister) has ever performed with Waldmeister.

A Knuth-Bendix completion of CGE_k with $k \geq 2$ consists of the group rules 1 through 10 of Figure 3; a set of four endomorphism rules exactly similar to rules 11 through 14 (rules 15 through 18 are also exactly similar) for each endomorphism; and then commutation rules, as follows. Fix a total ordering $\succ$ on the endomorphisms. Then for each endomorphism f, add the following rules $R_{f,g}$ for every endomorphism g with $f \succ g$:

$$\begin{aligned} f(x) * g(y) &\rightarrow g(y) * f(x) \\ f(x) * (g(y) * z) &\rightarrow g(y) * (f(x) * z) \end{aligned}$$

We have already reported that all critical pairs between commutation rules $R_{f,g}$, endomorphism rules for f and g, and the group rules are joinable. To show local confluence, it suffices to show that the critical pairs that arise between $R_{f,g}$ and $R_{g,h}$ are joinable. But since $f \succ g \succ h$, we have $f \succ h$, and so there are commutation rules $R_{f,h}$. These are used to join critical pairs beginning from terms like $f(x) * (g(y) * h(z))$.

To show termination, we study the proof produced by AProVE for the case of two endomorphisms. All rules can be removed from the termination problem using linear polynomial orderings, except for the commutation rules and the associativity rule. Using the dependency pairs method, the resulting rewrite system is terminating if for each cycle in the approximated dependency graph, there is a reduction quasi-ordering which weakly reduces all rules and all dependency pairs on the cycle, and also strongly reduces one dependency pair on the cycle [3]. Here, the approximated dependency graph consists of one strongly connected component (SCC) for the two dependency pairs coming from the associativity rule, and one SCC for each endomorphism f except the

$\succ$-minimal one. Each SCC is the complete graph on its nodes. The nodes of the SCC for an endomorphism f are the dependency pairs $f(x)\hat{*}(g(y) * z) \to f(x)\hat{*}z$ coming from $R_{f,g}$ for each g with $f \succ g$. A suitable reduction quasi-ordering is the one arising from the lexicographic path order with precedence $\hat{*} > * > f'_1 > \ldots > f'_k$ and argument filtering system $f_i(x) \to f'_i$ where $f_1 \succ \ldots \succ f_k$ are all the endomorphisms (in order), and $f'_1, \ldots, f'_k$ are new constants. This ordering in fact strongly reduces all rules and all dependency pairs on all SCCs. So the system with $k \geq 2$ is terminating[1].

Note that in the intended application, if there are n function symbols each with arity no greater than k, then the number of rules in the rewrite system is no greater than $10 + 4n + n \sum_{i=1}^{k-1} i = 10 + 4n + nk(k-1)/2$.

4 Conclusion

We have seen Knuth-Bendix completion of the equational theory of $k \geq 2$ commuting group endomorphisms using automated theorem proving and modern termination checking. The theory has application to proof simplification in the context of decision procedures for verification. Future work includes mining conflict clauses without actually putting congruence proofs into canonical form. We hope this work encourages the development of completion tools based on modern termination-checking techniques.

[1] Thanks to Jürgen Giesl for helpful comments on this termination argument.

References

[1] C. Barrett, D. Dill, and A. Stump. Checking Satisfiability of First-Order Formulas by Incremental Translation to SAT. In *14th International Conference on Computer-Aided Verification*, pages 236–249. Springer, 2002.

[2] L. de Moura, H. Rueß, and N. Shankar. Justifying Equality. *Electronic Notes in Theoretical Computer Science*, 125(3):69–85, 2005. Appeared at the 2nd International Workshop on Pragmatics of Decision Procedures in Automated Reasoning (2004).

[3] J. Giesl, T. Arts, and E. Ohlebusch. Modular Termination Proofs for Rewriting Using Dependency Pairs. *Journal of Symbolic Computation*, 34(1):21–58, 2002.

[4] J. Giesl, R. Thiemann, P. Schneider-Kamp, and S. Falke. Automated Termination Proofs with AProVE. In V. van Oostrom, editor, *the 15th International Conference on Rewriting Techniques and Applications*, pages 210–220. Springer, 2004.

[5] D. Knuth and P. Bendix. Simple Word Problems in Universal Algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Pergamon Press, 1970.

[6] B. Löchner and Th. Hillenbrand. A phytography of WALDMEISTER. *AI Communications*, 15(2–3):127–133, 2002.

[7] R. Nieuwenhuis and A. Oliveras. Proof-producing Congruence Closure. In J. Giesl, editor, *16th International Conference on Rewriting Techniques and Applications*, pages 453–468. Springer, 2005.

[8] A. Stump and L.-Y. Tan. The Algebra of Equality Proofs. In Jürgen Giesl, editor, *16th International Conference on Rewriting Techniques and Applications*, pages 469–483. Springer, 2005.