Tutorial on string rewriting systems and extensions of Gröbner bases

Susan Hermiller
Department of Mathematics and Statistics,
University of Nebraska, Lincoln, NE 68588-0323, USA
`smh@math.unl.edu`

Introduction

One of the fundamental questions in the study of groups and monoids is the solvability of the word problem. In general the word problem for finitely presented groups (or monoids) is not solvable; that is, given two words in the generators of the group, there may be no algorithm to decide whether the words in fact represent the same element of the group. For groups presented by a string rewriting system that is finite and complete however, the word problem is solved.

This tutorial will be expository, surveying known results in the study of rewriting systems for groups, with some connections to Gröbner bases in the last section. More specifically, the topics will cover:

1. Consequences of finite complete rewriting systems for groups and monoids. Looking at the same results from another perspective, this topic could also be labeled: Methods for checking that a group cannot have a finite complete rewriting system.

2. Infinite complete rewriting systems, particularly those with normal forms that are a regular language.

3. Orderings used to check termination, both for string rewriting systems and Gröbner bases.

The following is a brief overview of these topics.

Consequences of finite complete rewriting systems

A *(string) rewriting system* consists of a finite set Σ and a subset $R \subseteq \Sigma^* \times \Sigma^*$ of replacement *rules*, written $u \to v$ whenever $(u, v) \in R$, which give, for any $x, y \in \Sigma^*$, *rewritings* $xuy \to xvy$. A word that cannot be rewritten is called *irreducible*. There is a monoid associated to this rewriting system, presented by

$$M = \langle\ \Sigma \mid u = v \text{ if } (u, v) \in R\ \rangle.$$

The sets Σ and R give a rewriting system for a group G if, as a monoid, G is the monoid associated to this system. The rewriting system is *finite* if the sets Σ and R are finite, and the system is *complete* if the following conditions hold.

Termination: There is no infinite chain $x \to x_1 \to x_2 \to \cdots$ of rewritings.

Confluence: There is exactly one irreducible word representing each element of the monoid presented by the rewriting system.

Although a finite complete rewriting system solves the word problem, not every group with a solvable word problem has such a system. This was first proved through the connections between finite complete rewriting systems and homological finiteness conditions.

A monoid M satisfies the homological finiteness condition *left* FP_n if there is a projective resolution

$$P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to \mathbf{Z} \to 0$$

of finitely generated left $\mathbf{Z}M$-modules. If M satisfies the condition left FP_n for every natural number n, then M has type *left* FP_∞. Similarly, M has type *right* FP_n if there is a projective resolution of length n consisting of finitely generated right $\mathbf{Z}M$-modules, and type *right* FP_∞ if M is right FP_n for every natural number n. For a group, the left and right conditions are equivalent; if a group satisfies these conditions, it has type FP_n and type FP_∞, respectively.

The following theorem was first proved by Anick [An] in the context of associative algebras, and by Squier [Sq] for type FP_3 for groups. Since then many others [Br], [Fa], [Gr], [Ko], and [LP] have published proofs which further elaborate the possible projective resolutions and corresponding homology; see [Co] for a survey of these proofs.

Theorem. *If a monoid M has a finite complete rewriting system, then M satisfies the homological finiteness conditions left and right FP_∞.*

Since there are groups with solvable word problem that do not satisfy this finiteness condition, a consequence of this theorem is that there are groups with solvable word problem that cannot have a finite complete rewriting system.

Several other conditions must be satisfied by any group that has a finite complete rewriting system:

1. Finite derivation type, introduced by Squier [Sq2].
2. A combinatorial condition on elements of G, defined by Katsura and Kobayashi [KK].
3. Existence of a tame combing of the Cayley complex for G [HM].

Infinite complete rewriting systems

Rewriting systems that are not finite can be used to find other information about the group, particularly if further restrictions are placed on the system. If the rules of the system are recursive, the rewriting system will solve the word problem. Also, when the set of irreducible words is a regular language, one can check if these normal forms are a part of an automatic structure for the group.

Termination

In order to check termination of a rewriting system, it suffices to show that there is a well-founded ordering $>$ which is compatible with concatenation, known as a *division ordering*, for which $u > v$ for all rules $u \to v$ in the rewriting system.

In most cases, termination of a rewriting system is checked using a total division ordering. However, it is possible to have a complete rewriting system for which the rules do not decrease a total division ordering, although they do decrease a partial one [Es]. In the same way, the ideal membership problem can be solved with a finite Gröbner basis in which all of the polynomial replacements decrease a (partial) division ordering.

If all of the rules of a finite complete rewriting system for a group strictly reduce word length, then the congruence class of the identity of the group is a context-free language [Bo]. Combining this with results of Muller and Schupp [MS] shows that a group has a length-reducing finite complete rewriting system if and only if the group has a finite index subgroup which is a free group.

A rewriting system is *geodesic* if all of the rules either decrease or preserve word length; for example, if the rules decrease the shortlex ordering. If a group has a geodesic finite complete rewriting system, then the Cayley graph of the group must satisfy a geometric property known as almost convexity [HM]. There are groups with finite complete rewriting systems which are not almost convex, and hence cannot have geodesic systems.

For a given finite set of generators for a group, there are only finitely many different choices of orderings on the generators, and hence only finitely many different shortlex orderings on the set of words over those letters. However, there are uncountably many possible total division orderings on the set of words over the same letters. There are also monoids for which there are uncountably many distinct (infinite) complete rewriting systems using the same set of generators; for example, the free abelian monoid on three generators ([HMc],[Ma]).

References

[An] D.J. Anick, *On the homology of associative algebras*, Trans. Amer. Math. Soc. **296** (1986), 641–659.

[Bo] R.V. Book, *Confluent and other types of Thue systems*, J. Assoc. Comp. Mach. **29** (1982), 171–182.

[Br] K.S. Brown, *The geometry of rewriting systems: a proof of the Anick-Groves-Squier theorem*, in: Algorithms and Classification in Combinatorial Group Theory (G. Baumslag, C.F. Miller, eds.), MSRI Publications 23, Springer, New York, 1992, 121–136.

[Co] D.E. Cohen, *String rewriting – a survey for group theorists*, in: Geometric Group Theory, Vol. 1 (G.A. Niblo, M.A. Roller, eds.), London Math. Soc. Lecture Notes Ser. 181, Cambridge University Press, Cambridge, 1993, 37–47.

[Es] C. Eschenbach, *Die Verwendung von Zeichenkettenordnungen im Zusammenhang mit Semi-Thue Systemen*, Tech. Report FBI-HH-B-122/86, Fachbereich Informatik, Universität Hamburg, 1986.

[Fa] D.R. Farkas, *The Anick resolution*, J. Pure Appl. Algebra **79** (1992), 159–168.

[Gr] J.R.J. Groves, *Rewriting systems and homology of groups*, in: Groups – Canberra 1989 (L.G. Kovacs, ed.), Lecture Notes in Math. 1456, Springer, Berlin, 1991, 114–141.

[HMc] S. Hermiller and J. McCammond, in preparation.

[HM] S.M. Hermiller and J. Meier, *Tame combings, almost convexity, and rewriting systems for groups*, Math. Z. **225** (1997), 263–276.

[KK] M. Katsura and Y. Kobayashi, *Constructing finitely presented monoids which have no finite complete presentation*, Semigroup Forum, **54** (1997), 292–302.

[Ko] Y. Kobayashi, *Complete rewriting systems and homology of monoid algebras*, J. Pure Appl. Algebra **65** (1990), 263–275.

[LP] Y. LaFont and A. Prouté, *Church-Rosser property and homology of monoids*, Math. Structures Comput. Sci., **1** (1991), 297–326.

[Ma] U. Martin, private correspondence.

[MS] D. Muller and P. Schupp, *Groups, the theory of ends, and context-free languages*, J. Comput. System Sci. **26** (1983), 295–310.

[Sq] C.C. Squier, *Word problems and a homological finiteness condition for monoids*, J. Pure Appl. Algebra **49** (1987), 210–217.

[Sq2] C.C. Squier, F. Otto, and Y. Kobayashi, *A finiteness condition for rewriting systems.* Theoret. Comput. Sci. **131** (1994), 271–294.