



ELSEVIER

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Journal of Symbolic Computation 40 (2005) 1285–1290

Journal of
Symbolic
Computation

www.elsevier.com/locate/jsc

On ordering free groups

Lawrence H. Smith*

*National Center for Biotechnology Information, National Institutes of Health Computational Biology Branch,
8600 Rockville Pike Building 38A, Rm 614D, Bethesda, MD 20894, USA*

Received 20 June 2002; accepted 20 May 2005
Available online 15 June 2005

Abstract

The positive cones of the left orders on a free group can be described by their finite subsets. An algorithm is given for recognizing when a finite subset of a free group lies in a positive cone. This is used to show how one can construct a sequence of finite subsets of a positive cone whose union is the positive cone. Moreover, the method gives an overview of the positive cones of a free group. It is still an open problem whether there are positive cones which can be generated as a subsemigroup by a finite subset.

© 2005 Elsevier Ltd. All rights reserved.

MSC: 20F60 (06F15)

Keywords: Computation; Ordered groups; Free groups

1. Introduction

Every total order on a finitely generated free abelian group is characterized by the lexicographic product of a finite list of partial orders determined simply by real linear forms as shown in [Robbiano \(1985\)](#). In contrast, relatively little is known about total orders on nonabelian free groups. Some special constructions are known, including an order determined by orders on the abelian factors of the lower central series, an order on a free product that extends orders of the free factors, both in [Powell \(1992\)](#), and several distinct

* Tel.: +1 301 435 8881; fax: +1 301 480 2290.
E-mail address: lsmith@ncbi.nlm.nih.gov.

orders extending a lexicographic order on the corresponding free monoid in Revesz (1986). An extensive bibliography on ordered algebraic structures, including ordered groups, can be found in Fuchs (1963).

The paper is self-contained, making use of little more than the definition of an ordered group and elementary properties of free groups. The main result (Section 3) is a computable condition that determines when a subset of a free group can be extended to a positive cone. This is preceded (Section 2) by some results on generating sets for subsemigroups of free groups; in particular a special generating set is introduced, called a *strong basis*, which is similar to a Nielsen basis for subgroups of free groups (Nielsen, 1955; or see Lyndon and Schupp, 1977).

Throughout this paper, G is a free nonabelian group (with identity element e), freely generated by a set of variables and their inverses, which may be infinite unless otherwise specified. The length of an element g of G is denoted as $|g|$. Given a subset $S \subset G$, the subsemigroup that it generates is denoted as $\langle S \rangle$. A total order relation $<$ on G is a *left-order* if for all $a, b, c \in G$, $a < b \Rightarrow ca < cb$. Recall that the *positive cone* of a left-order is $P = \{a \in G \mid e < a\}$ and it satisfies (i) (*semigroup*) $PP \subset P$, (ii) (*antisymmetry*) $P \cap P^{-1} = \phi$, or equivalently, $e \notin P$, and (iii) (*trichotomy*) $P \cup P^{-1} \cup \{e\} = G$; and conversely, if P satisfies (i)–(iii), then it is the positive cone of a left-order defined by $a < b \Leftrightarrow a^{-1}b \in P$. When G has rank 2 or more, it is an open question whether there exists a left-order on G whose positive cone is finitely generated as a subsemigroup.

2. Semigroups

A subset $S \subset G$ is called a *strong basis* (for the subsemigroup $\langle S \rangle$) if whenever $a, b \in S$ and $|ab| < \max(|a|, |b|)$ then $ab \in S$. Given a finite set S , a strong basis for $\langle S \rangle$ can be constructed by extending S to include ab whenever a, b are found that violate the definition, and this is a finite computation. The following is a simple condition that guarantees a set to be a strong basis.

Lemma 1. *Let $S \subset G$, with $m = \max_{x \in S} |x|$. If $s \in \langle S \rangle$ and $|s| < m \Rightarrow s \in S$ then S is a strong basis.*

Compare the definition of a strong basis with the definition of a Nielsen basis where $S = B \cup B^{-1}$ and B are generators of a subgroup. The length of a product satisfies the equation $|ab| = |a| + |b| - 2|c|$ where c is the portion of a and b that cancels. If $|ab| < \max(|a|, |b|)$ then $|c| > \min(|a|, |b|)/2$; that is, the portion that cancels is more than half of one of the two factors. If B is a Nielsen basis, this cannot occur by definition. It is always possible to transform a generating set B to a Nielsen basis by carefully adding and removing elements, and the advantage in doing so is that the resulting generators are free. But because these transformations involve inverses, they are not available in a semigroup. Still, by requiring that whenever half of a product cancels then the product itself can be found in S , any element of $\langle S \rangle$ can be expressed as a product from S where successive products do not cancel more than half, and this is essentially what is proved in the next theorem.

Theorem 2. Suppose $S \subset G$ is a strong basis, and $g \in \langle S \rangle$ is represented by $g = h_1 \cdots h_n$, where $h_i \in S$ and n is as small as possible. Then the successive (rightmost) products have non-decreasing length, that is

$$|h_{i+1} \cdots h_n| \leq |h_i h_{i+1} \cdots h_n|$$

for $i = 1, \dots, n - 1$.

Proof. Since S is a strong basis, it must be the case that $|h_i h_{i+1}| \geq \max(|h_i|, |h_{i+1}|)$; otherwise it would be possible to replace the pair with a single element of S and obtain a smaller n . Let the reduced word representations for h_i and h_{i+1} be written $h_i = x_i b_i$ and $h_{i+1} = b_i^{-1} y_{i+1}$ so that $h_i h_{i+1} = x_i y_{i+1}$ without cancellation in the product and $|h_i h_{i+1}| = |x_i| + |y_{i+1}|$. The inequalities $|h_i h_{i+1}| \geq \max(|h_i|, |h_{i+1}|)$ imply that $|b_i| \leq |y_{i+1}|$ and $|b_i| \leq |x_i|$. So in fact it is possible to write each $h_i = b_{i-1}^{-1} a_i b_i$ without cancellation ($b_0 = e$), and $|b_i| \leq |b_{i-1}| + |a_i|$. It follows that $h_{i+1} \cdots h_n = b_i^{-1} a_{i+1} \cdots a_n$ without cancellation, and so $|h_{i+1} \cdots h_n| = |b_i| + |a_{i+1}| + \cdots + |a_n| \leq |b_{i-1}| + |a_i| + |a_{i+1}| + \cdots + |a_n| = |h_i \cdots h_n|$. \square

This theorem can be used to solve the membership problem for subsemigroups as a recursive search algorithm. Explicitly, if S is a finite strong basis, then to determine whether $g \in \langle S \rangle$ it is enough to consider each of $h^{-1}g$ for $h \in S$ whenever $|h^{-1}g| < |g|$. If $h^{-1}g = e$ then $g \in \langle S \rangle$. Otherwise, the search continues a finite number of times until success occurs, or until the length cannot be shortened. If $g \in \langle S \rangle$, then Theorem 2 implies that the search terminates successfully and g is the product of the h_1, \dots, h_n recovered from the recursion.

If S is a strong basis, then by Theorem 2 if $e \in \langle S \rangle$ it can be expressed as a product of elements of S with successive products having non-decreasing length. Since there is only one element with length 0, the identity itself must be in S . Hence:

Corollary 3. The subsemigroup generated by a strong basis excluding e is antisymmetric.

3. Positive cones

In this section, G is a finitely generated free group with rank 2 or more. An arbitrary element g is the unique reduced product of the generators and their inverses, and the length of g is computable. We require an enumeration $g_0 = e, g_1, g_2, \dots$ of the elements of G that is non-decreasing in length ($|g_i| \leq |g_{i+1}|$) and that puts elements adjacent to their inverses ($g_{i+1} = g_i^{-1}$ for odd i). This can always be done algorithmically, since the number of elements of a given length is finite and $|g| = |g^{-1}|$. Given an enumeration, the notation $G_N = \{g_0, \dots, g_N\}$ will be used.

Theorem 4. Let $N > 0$ be even and $S \subset G_N$ such that for all $0 < i \leq N$ either $g_i \in S$ or $g_i^{-1} \in S$. Then S can be extended to a positive cone if and only if S is a strong basis and $e \notin S$.

Proof. Suppose S satisfies the hypothesis and P is a positive cone containing S . Then if $h \in P$ and $|h| < |g_N|$, then $h = g_i$ for some $i < N$. By hypothesis, either h or h^{-1} is in S .

But $h^{-1} \notin P$; therefore $h \in S$ and so S satisfies the conditions of Lemma 1. Consequently, S is a strong basis, and $e \notin S$ since $e \notin P$.

The converse will be proved by constructing a positive cone containing S inductively. This is done by showing that there exists an S_1 containing S satisfying the hypothesis of the theorem for $N + 2$, which is a strong basis not containing e . These extensions can continue indefinitely, and their union will be a positive cone.

Since S satisfies the hypothesis and is a strong basis excluding e , it follows that if $g_i \in \langle S \rangle$ for $i \leq N$, then $g_i \in S$, that is, in fact $S = G_N \cap \langle S \rangle$. Since, by Corollary 3, $e \notin \langle S \rangle$, only three cases are possible (note $g_{N+2} = g_{N+1}^{-1}$): (1) $g_{N+1} \in \langle S \rangle$ and $g_{N+2} \notin \langle S \rangle$, (2) $g_{N+1} \notin \langle S \rangle$ and $g_{N+2} \in \langle S \rangle$, and (3) $g_{N+1} \notin \langle S \rangle$ and $g_{N+2} \notin \langle S \rangle$. In case (1), let $S_1 = S \cup \{g_{N+1}\}$. Then $\langle S \rangle = \langle S_1 \rangle$ and it follows that $S_1 = G_{N+2} \cap \langle S \rangle$. By Lemma 1, S_1 is a strong basis. In case (2), $S_1 = S \cup \{g_{N+2}\}$ is a strong basis by similar reasoning as case (1).

In case (3), it will be shown that $S_1 = S \cup \{g_{N+1}\}$ satisfies the hypotheses of the theorem, and is a strong basis excluding e . The hypothesis of the theorem is satisfied since it is clear that for all $0 < i \leq N + 2$, either $g_i \in S_1$ or $g_i^{-1} \in S_1$. Reasoning by way of contradiction, suppose that S_1 is not a strong basis, that is, there exist $a, b \in S_1$ with $|ab| < \max(|a|, |b|)$ but $ab \notin S_1$. Note that since $|ab| < |g_{N+1}|$, ab is one of the g_i with $i \leq N$, and therefore $(ab)^{-1} \in S$. Since S is a strong basis, a and b cannot both belong to S . Therefore, either $a = g_{N+1}$ or $b = g_{N+1}$ or both. If $a = g_{N+1}$ and $b \in S$, then $g_{N+2} = b(ab)^{-1} \in \langle S \rangle$ is a contradiction. Or, if $b = g_{N+1}$ and $a \in S$, then $g_{N+2} = (ab)^{-1}a \in \langle S \rangle$ is a contradiction. Finally, if $a = b = g_{N+1}$, then $|ab| = |a^2| < |a|$ is a contradiction for all $a \neq e$ in a free group. It follows that S_1 is a strong basis. Since an enumeration could exchange g_{N+1} and g_{N+2} , this proof implies that $S_1 = S \cup \{g_{N+2}\}$ is also a strong basis, and so an arbitrary choice is possible in this case.

Continue to extend in this way to obtain $S \subset S_1 \subset S_2 \subset \dots$. The union P of $\langle S_i \rangle$ is a subsemigroup of G containing S . By construction and by Corollary 3, $e \notin \langle S_i \rangle$; therefore $e \notin P$. Furthermore, for all $k > 0$, and all $i > (k - N)/2$, either $g_k \in S_i$ or $g_k^{-1} \in S_i$. Therefore, $P \cup P^{-1} \cup \{e\} = G$. Thus P is a positive cone containing S . \square

The proof suggests an infinite procedure for constructing a positive cone on G from a sequence of sets $S_i \subset G_{2i}$ by using the algorithm of Section 2 to test $g_{2i+1} \in \langle S_i \rangle$ and $g_{2i+2} \in \langle S_i \rangle$, and by defining S_{i+1} as in the proof to include g_{2i+1} or g_{2i+2} , making a choice when required. For a given N all the elements of G_N in the cone are produced in finitely many steps. The number of required choices is probably unbounded as $N \rightarrow \infty$, which is equivalent to saying that positive cones are never finitely generated, but this has not been proven.

4. Examples

In these examples, G is a free group of rank 2 with free generators x and y .

Example 1: A strong basis for $S = \{y, x, yx^{-1}, y^{-1}x, yx^{-1}y^{-1}\}$. Examine all pairs $(a, b) \in S \times S$ and confirm that $|ab| < \max(|a|, |b|) \Rightarrow ab \in S$; therefore S is a strong basis.

Table 1

An enumeration of the free group generated by x and y up to length 3, with a positive cone underlined. The set S_i consists of the underlined elements up to g_{2i} ; doubly underlined elements were chosen randomly. \hat{x} and \hat{y} stand for x^{-1} and y^{-1} respectively, to improve readability

(1–10)	<u>y</u>	<u>ŷ</u>	<u>x̂</u>	<u>ẋ</u>	<u>yy</u>	<u>ŷŷ</u>	<u>yx</u>	<u>ẋŷ</u>	<u>yẋ</u>	<u>xŷ</u>
(11–20)	<u>xy</u>	<u>ŷx̂</u>	<u>xx̂</u>	<u>ẋẋ</u>	<u>ẋy</u>	<u>ŷx̂</u>	<u>yyy</u>	<u>ŷŷŷ</u>	<u>yyx</u>	<u>ẋŷŷ</u>
(21–30)	<u>yyx̂</u>	<u>xŷŷ</u>	<u>yxy</u>	<u>ŷx̂ŷ</u>	<u>yxx</u>	<u>xx̂ŷ</u>	<u>yxŷ</u>	<u>yẋŷ</u>	<u>yẋy</u>	<u>ŷxŷ</u>
(31–40)	<u>yẋx̂</u>	<u>xxŷ</u>	<u>xyy</u>	<u>ŷŷx̂</u>	<u>xyx</u>	<u>ẋŷx̂</u>	<u>xyx̂</u>	<u>xŷx̂</u>	<u>xx̂y</u>	<u>ŷx̂x̂</u>
(41–50)	<u>xxx</u>	<u>ẋẋx̂</u>	<u>x̂ŷx</u>	<u>ẋyẋ</u>	<u>ẋyy</u>	<u>ŷŷx</u>	<u>ẋyx</u>	<u>ẋŷx</u>	<u>ẋx̂y</u>	<u>ẋxx̂</u>
(51–52)	<u>ŷxy</u>	<u>ŷx̂y</u>								

Example 2: Membership in $\langle S \rangle$. To test $g \in \langle S \rangle$, search for length reductions, that is $h \in S$ with $|h^{-1}g| < |g|$. For $g = xy^{-1}x$ the only reduction is $h = x$ with product $y^{-1}x \in S$, so $xy^{-1}x \in \langle S \rangle$. For $g = x^{-1}yy$ there are no reductions, so $x^{-1}yy \notin \langle S \rangle$.

Example 3. A strong basis for $S' = S \cup \{x^{-1}yy\}$. As in Example 1, search $S' \times S'$ and find $(x, x^{-1}yy)$ violating the definition. Include the product in $S'' = S' \cup \{yy\}$ and verify that it is a strong basis.

Example 4. An enumeration of G satisfying the requirements of Theorem 4. Make a list of the elements of G for each length of interest. Sort each list in descending lexicographic order determined by $y >_{\text{lex}} x >_{\text{lex}} x^{-1} >_{\text{lex}} y^{-1}$. Finally, move list entries up to follow their inverses appearing earlier in the list. The resulting enumeration up to length 3 is shown in Table 1.

Example 5. The positive cone up to length 3 of some order on G . Referring to the list in Table 1, each step computes S_{i+1} from S_i , by underlining the element (g_{2i+1} or g_{2i+2}) that is included to yield S_{i+1} . Starting with $i = 0$ and $\langle S_0 \rangle = \phi$, the element g_1 is chosen arbitrarily and underlined. At each later step i , if either g_{2i+1} or g_{2i+2} are in S_i (and at most one can be) then underline it; otherwise make an arbitrary choice and underline it.

Since $S_i = \langle S_i \rangle \cap G_{2i}$, $g \in \{g_{2i+1}, g_{2i+2}\}$ is in $\langle S_i \rangle$ if and only if there exists an $h \in S_i$ such that $|h^{-1}g| < |g|$ and $h^{-1}g \in S_i$. For instance, testing $g_{27} = yxy^{-1}$ at step $i = 13$, the reducing $h \in S_{13}$ are y, yx, yxy and yxx , and the corresponding reductions are $xy^{-1}, y^{-1}, y^{-1}y^{-1}$ and $x^{-1}y^{-1}$. Since none of these reductions are in S_{13} , $yxy^{-1} \notin \langle S_{21} \rangle$. Similarly $g_{28} = yx^{-1}y^{-1} \notin \langle S_{13} \rangle$. In this case g_{28} was chosen at random and underlined to complete the step.

Acknowledgments

A variant of this algorithm appears in Smith (1998), for which I thank my advisor Jee H. Koh. I also thank Professors Boo Barkee and Mike Newman for valuable assistance in writing this paper.

References

- Fuchs, L., 1963. Partially Ordered Algebraic Systems. Pergamon Press, Oxford.
- Lyndon, R.C., Schupp, P.E., 1977. Combinatorial Group Theory. Springer-Verlag, New York.

- Nielsen, J., 1955. A basis for subgroups of free groups. *Math. Scand.* 3, 31–43.
- Powell, W.B., 1992. Total orders on free groups and monoids. In: *Words, Languages, and Combinatorics* (Kyoto, 1990). World Sci. Publishing, River Edge, NJ, pp. 427–434.
- Revesz, G., 1986. Full orders on free groups. In: *Algebra and Order* (Luminy-Marseille, 1984). In: *Res. Exp. Math.*, vol. 14. Heldermann, Berlin, pp. 105–111.
- Robbiano, L., 1985. Term orderings on the polynomial ring. In: *EUROCAL'85*, vol. 2. (Linz, 1985). In: *Lecture Notes in Comput. Sci.*, vol. 204. Springer, Berlin, pp. 513–517.
- Smith, L.H., 1998. Computing resolutions over associative algebras with ordered basis. Doctoral Dissertation. Indiana University, Bloomington, Indiana.