

Total Orders on Free Groups.

Well Orders on Free Monoids

The core of my dissertation concerns a further generalization of Grobner bases to associative algebras. The original problem that I considered for this research was to find a characterization of computable well orders on free monoids. This is the analogous problem for free associative algebras that has been solved neatly for polynomial rings.

Every total order on a free abelian monoid (these are the monomials of a polynomial ring) is characterized by Robbiano (*Term Orderings on the polynomial ring*. In Proc. EUROCAL '85, Springer LNCS **357**, p. 413...) as a lexicographic product of real-valued weighted degree orders. Further conditions limit the \mathbf{Q} -dimension of the weights in \mathbf{R} .

Paraphrasing Robbiano, every total order $<$ on a free abelian group of finite rank n is characterized by a type s where $1 \leq s \leq n$, a partition of $n = d_1 + \dots + d_s$ where $d_i > 0$ are integers, and finally linear forms $\Gamma_1, \dots, \Gamma_s$ with coefficients in \mathbf{R} such that $d(\Gamma_i) = d_i$ where $d(\Gamma)$ is the dimension of the \mathbf{Q} -vector space spanned by the coefficients of Γ in \mathbf{R} . The total order is defined by $t_2 < t_1$ if and only if

$$\begin{aligned}\Gamma_1(t_2) &= \Gamma_1(t_1) \\ &\dots \\ \Gamma_{p-1}(t_2) &= \Gamma_{p-1}(t_1) \\ \Gamma_p(t_2) &< \Gamma_p(t_1)\end{aligned}$$

for some $1 \leq p \leq s$.

There are many equivalent and independent formulations of this fact.

Although I was unaware of it when I began considering the same problem for the free associative algebra, the problem has not been solved. My original goal was to find a simple geometric description, but I had to settle for a generating algorithm. Because this problem remains unsolved and unstudied, I expect that computer exploration will provide the hints and insights needed to formulate a solution.

Levels of Abstraction

I have worked on reformulating the algorithmic enumeration at many different levels of abstraction, trying to identify what parts of the algorithm are special to the algebraic structure, and what parts are a simple consequence of computing relations on sets. Some of the levels of abstraction that I have considered are

1. Well orders on a (finite rank) free monoid.
2. Total orders on a free monoid.
3. Total orders on a free group.
4. Total orders on an (enumerable) set.
5. Quasi orders on a set.
6. Relations on a set.
7. An arbitrary class of subsets of a set.

Surprisingly, an outline of the technique can be given at the highest level of abstraction. The step from monoids to groups is an interesting one, which I solved in my dissertation by embedding the monoid in a group-like extension. I would like to state and prove the basic theorem for total orders on a free group. First I will sketch the idea at the highest level of abstraction.

Computing a Class of Subsets of an Enumerable Set.

Let \mathcal{R} be a class of subsets of \mathbf{N} . For $N \in \mathbf{N}$ and $r \subset \mathbf{N}$ define $r_N = r \cap \{1, \dots, N\}$. Then define $\mathcal{R}_N = \{r_N | r \in \mathcal{R}\}$. We will say that \mathcal{R} is **approximately computable** if for each N and $s \subset \{1, \dots, N\}$ there is an algorithm that decides whether $s \in \mathcal{R}_N$.

If \mathcal{R} is approximately computable then it is possible to both enumerate the elements of \mathcal{R} and decide membership in any given element of \mathcal{R} . If $r_N \in \mathcal{R}_N$, then either $r_N \in \mathcal{R}_{N+1}$ or $r_N \cup \{N+1\} \in \mathcal{R}_{N+1}$ or both, call these cases 0 and 1 respectively. Let $\mathbf{a} = a_1, a_2, \dots$ be an infinite sequence of 0 and 1 and start with $r_0 = \phi$ and $k_0 = 0$. Now assuming that r_N and k_N have been defined, if case 0 holds but not case 1 then let $r_{N+1} = r_N$ and $k_{N+1} = k_N$. If case 1 holds but not case 0 then let $r_{N+1} = r_N \cup \{N+1\}$ and $k_{N+1} = k_N$. If both cases 0 and 1 hold, then let $k = k_{N+1} = k_N + 1$ and if $a_k = 0$ then let $r_{N+1} = r_N$ and if $a_k = 1$ then let $r_{N+1} = r_N \cup \{N+1\}$. The union of the sets r_N is a subset of \mathbf{N} denoted $r_{\mathbf{a}}$. It is

not necessary that $r_{\mathbf{a}} \in \mathcal{R}$, this depends on whether \mathcal{R} is closed in a certain approximation topology. We also do not know a priori whether cases 0 or 1 will occur at all after a certain point in the construction, so the entire sequence may not be needed to determine $r_{\mathbf{a}}$. If it is possible to prove that the entire sequence is always needed, then there is a one-to-one correspondence between sequences and elements of \mathcal{R} . Finally, for any given computable sequence \mathbf{a} with the property that $r_{\mathbf{a}} \in \mathcal{R}$, and any $x \in \mathbf{N}$ there is an obvious algorithm for deciding if $x \in r_{\mathbf{a}}$.

Total Orders on Free Groups

With the idea of the abstraction in hand, we will skip to the statement of the main theorem for the case of free groups of finite rank. The reader can then consider how this fits into the abstract scheme for computing total orders on free groups.

Let G be a group. All orders are assumed to satisfy $a < b \Rightarrow ca < cb$ for all $a, b, c \in G$. Recall that if $P \subset G$ then $P = \{g | g > e\}$ for some total order if and only if P is a closed semigroup and $G = P \cup P^{-1} \cup \{e\}$. In that case $<$ is defined by $g > e \Leftrightarrow g \in P$ and we write $P = P_{<}$.

Now let $e = x_0, x_1, \dots$ be an enumeration of a free group G of finite rank such that the word lengths satisfy $|x_n| \leq |x_{n+1}|$. For $S \subset G$ write $S_N = S \cap \{x_0, x_1, \dots, x_N\}$.

Theorem. Let $S_N \subset \{x_1, \dots, x_N\}$ and let S_N^+ denote $S_N \cup (\{x_1, \dots, x_N\} \setminus S_N)^{-1}$ (that is the elements of S_N together with the inverse of the elements from $\{x_1, \dots, x_N\}$ not in S_N). Then the following are equivalent.

- i. there exists a total order $<$ on G satisfying $S = P_{<N}$
- ii. $\langle S_N^+ \rangle \cap \langle S_N^+ \rangle^{-1} = \phi$ (antisymmetric).

The notation $\langle S \rangle$ stands for the semigroup generated by S . Note that the condition $\{x_0, \dots, x_N\} \subset \langle S_N^+ \rangle \cup \langle S_N^+ \rangle^{-1} \cup \{e\}$ (total up to N) is automatically implied by the definition of S_N^+ . The condition $i \Rightarrow ii$ is obvious. We begin the demonstration of the converse by showing how to test that $\langle S \rangle \cap \langle S \rangle^{-1} = \phi$ using the notion of a strong basis.

Definition. Let $S \subset H \subset G$. Then H is a strong basis for S if and only if $H \subset \langle S \rangle$ and if $h_1, h_2 \in H$ and $|h_1 h_2| < \max(|h_1|, |h_2|)$ then $h_1 h_2 \in H$.

Note that $|h_1 h_2| \geq \max(|h_1|, |h_2|)$ if and only if not more than half of either h_1 or h_2 cancels in the product. (For a quick proof, suppose $|h_1| = a + b$ and $|h_2| = b + c$ where b terms cancel in the product. If $|h_1 h_2| \geq |h_1|$ then $a + c \geq a + b$ which implies $c \geq b$, in other words not more than half of h_2 was cancelled in the product.)

Finding a strong basis is actually simple. One starts with $H = S$ and take products of pairs from H . Whenever the length of a product is less than the largest of the lengths, it is added to H . Testing continues until all possible products from H have been tested.

Suppose $g \in \langle S \rangle$. Then we can write $g = h_{m_1} h_{m_2} \dots h_{m_n}$ where each $h_{m_k} \in H(S)$ and further we can arrange that $|h_{m_k} h_{m_{k+1}}| \geq \max(|h_{m_k}|, |h_{m_{k+1}}|)$. It is a simple lemma for free groups that $l_k = |h_{m_k} \dots h_{m_n}|$ is a nonincreasing sequence of integers. In particular this proves that $e \in \langle S \rangle$ if and only if $e \in H(S)$ where $H(S)$ is any strong basis of S . Consequently we know that $\langle S \rangle \cap \langle S \rangle^{-1} = \phi$ if and only if $e \notin H(S)$.

The strong basis makes it possible to decide for $g \in G$ whether $g \in \langle S \rangle$. For if it were, it would have an expression $g = h_{m_1} h_{m_2} \dots h_{m_n}$ with n as small as possible. Therefore for some $h \in H(S)$, $h^{-1}g$ has smaller or equal length as g and is also in $\langle S \rangle$. The search continues down all paths defined by choices of h , avoiding repetition, and therefore considers at most finitely many candidates. The algorithm will either find an element of $H(S)$, or in each considered path will terminate by failing to find an h for which $h^{-1}g$ does not increase in length.

A strong basis makes it possible to test condition (ii), and it will also make it convenient to prove the equivalence. Suppose S_N satisfies the conditions, we will show that either S_N or $S_N \cup \{x_{N+1}\}$ also satisfy the conditions. Once this is established, the process can be continued indefinitely to obtain a sequence S_M for $M \geq N$. It is then a routine matter to prove that the union of the S_M defines the positive set of a total order on G .

If $x_{N+1} \in \langle S_N^+ \rangle$ then it is obvious that $S_{N+1} = S_N \cup \{x_{N+1}\}$ satisfies the condition for $N + 1$. If $x_{N+1}^{-1} \in \langle S_N^+ \rangle$ then it is also obvious that $S_{N+1} = S_N$ satisfies the condition for $N + 1$. It is not possible that they both belong to $\langle S_N^+ \rangle$ so we now consider the possibility that neither one is. In that case we will be able to choose either extension. Consider for example $S_{N+1} = S_N \cup \{x_{N+1}\}$. We need only prove that S_{N+1} is antisymmetric. Let H denote all of the elements from x_1, \dots, x_N that are in $\langle S_N^+ \rangle$. Then it is

clear that H is a strong basis for $\langle S_N^+ \rangle$ and by hypothesis $e \notin H$. If we show that $H' = H \cup \{x_{N+1}\}$ is a strong basis for $\langle S_{N+1}^+ \rangle$ it follows that S_{N+1} is antisymmetric also. Suppose by way of contradiction that it is not a strong basis. Then for some $a, b \in H'$, $|ab| < \max(|a|, |b|)$ and $ab \notin H'$. Since the elements are ordered by nondecreasing length, ab is an element x_k for some $k < N + 1$. We have $ab \notin H$ and this can't happen if both a and b are in H , so one of them must be x_{N+1} . By construction $(ab)^{-1} \in H$. So for example if $ax_{N+1} = c^{-1}$ where $c \in H$ then $x_{N+1} = a^{-1}c^{-1}$. But since a and c are in H , $ca \in H$ and so $x_{N+1}^{-1} \in H$ contradicting that $x_{N+1}^{-1} \notin \langle S_N^+ \rangle$. A similar statement applies to $x_{N+1}a$. Finally we need to rule out the possibility that $a = b = x_{N+1}$, but then $ab = x_{N+1}^2$ and $|h^2| > |h|$ for all $h \neq e$ in G .

This completes the proof.