Powers of sets in free groups

S. R. Safin

Abstract. We prove that $|A^n| \geq c_n \cdot |A|^{[(n+1)/2]}$ for any finite subset $A$ of a free group if $A$ contains at least two noncommuting elements, where the $c_n > 0$ are constants not depending on $A$. Simple examples show that the order of these estimates is best possible for each $n > 0$.

Bibliography: 5 titles.

Keywords: free group, relations in a free group, subsets of a free group.

§ 1. Introduction

We use the following notation: $F_m$ is a free group of rank $m$; $|A|$ is the cardinality of a set $A$; $AB$ is the set of all products of the form $ab$, where $a \in A$ and $b \in B$; $A^n$ is the set of all products of the form $a_1 \cdots a_n$, where $a_i \in A$; $|a|$ is the length of a word $a$ in some alphabet; $[x]$ is the largest integer not exceeding a real number $x$.

Chang [1] proved that there exist constants $c, \delta > 0$ such that $|A^3| > c \cdot |A|^{1+\delta}$ for any finite subset $A$ of the group $SL_2(\mathbb{C})$ not contained in any virtually Abelian subgroup. In particular, this estimate is valid for any finite subset of a free group not contained in any cyclic subgroup. Razborov [2] improved Chang’s estimate in this special case: there exists a constant $c > 0$ such that $|A \cdot A \cdot A| > |A|^2 \left(\log |A|\right)^c$ for any finite subset $A$ of a free group not contained in any cyclic subgroup.

It is easy to see that the squares of subsets satisfy no nontrivial analogues of Chang and Razborov’s inequality; the best possible estimate is linear in this case. (Most of the material briefly surveyed in this section can be found in the comprehensive monographs [3] and [4].) The following theorem shows, in particular, that the logarithm in Razborov’s estimate can be removed.

Theorem 1. There exist constants $c_n > 0$ such that for any finite subset $A$ of a free group not contained in any cyclic subgroup we have $|A^n| \geq c_n \cdot |A|^{[(n+1)/2]}$ for all positive integers $n$.

It is easy to show that if $A = \{x, y, y^2, \ldots, y^k\}$, then $|A^n| = O(k^{[(n+1)/2]})$ for each fixed $n \geq 1$, where $x$ and $y$ are free generators of a free group. Indeed, for $n = 1$ and $n = 2$ the assertion is obvious. Further, by induction

$|A^n| = |A^{n-2} A^2| \leq O(k^{[(n-1)/2]}) \cdot |A^2| = O(k^{[(n-1)/2]}) \cdot O(k) = O(k^{[(n+1)/2]})$.

This simple example shows that the order of our estimates is best possible for each $n$. Note also that the proof below is significantly simpler than the argument from [2]; but, on the other hand, in [2], a more general fact about the number of

AMS 2010 Mathematics Subject Classification. Primary 20E05.
elements in the product of three (possibly, different) subsets of a free group was proved.

In the commutative case, that is, when the set \( A \) is contained in a cyclic group, the situation is quite different. A survey of results on this subject can be found in [2] and in the literature cited therein.

The author thanks A. A. Klyachko for setting the problem, attention to the work, and several valuable remarks.

§ 2. Auxiliary lemmas

The period or the left period of a word \( w \) in some alphabet is a nonempty word \( \bar{w} \) not being a proper power such that the word \( w \) has the form \( w = \bar{w}^s \bar{w} \), where \( s \geq 2 \) and \( \bar{w} \) is a beginning of the word \( \bar{w} \) (\( \bar{w} \) may be empty, but must not coincide with \( \bar{w} \)). The word \( \bar{w} \) is called the tail (or the right tail) of the word \( w \). It is well known that the period and the tail of a periodic word are uniquely determined.

The right period of a word \( w \) in some alphabet is a nonempty word \( \hat{w} \) not being a proper power such that the word \( w \) has the form \( w = \hat{w} \hat{w}^s \), where \( s \geq 2 \) and \( \hat{w} \) is an end of the word \( \hat{w} \) (\( \hat{w} \) may be empty, but must not coincide with \( \hat{w} \)). The word \( \hat{w} \) is called the left tail of the word \( w \). It is well known that the word has a right period if and only if it has a left period (such words are called periodic); in addition, either both tails \( \bar{w} \) are empty \( \bar{w} \) or \( \hat{w} = \bar{w} \hat{w} \) and \( \hat{w} = \bar{w} \hat{w} \).

In the following lemma, we collect some known properties of periodic words.

**Lemma 1.** If two periodic words have the same left periods and the same right periods, then the tails of these words coincide too.

If, for some words, \( u_1 v w_1 = u_2 v w_2 \) and \( 0 < |u_2| - |u_1| \leq \frac{1}{2} |v| \) (that is, a word contains two occurrences of a word \( v \) and these occurrences intersect in a word of length at least \( \frac{1}{2} |v| \)), then the word \( v \) is periodic and \( u_2 \) ends with \( \bar{v} \).

**Proof.** Let us prove the first assertion. We assume that the tails of both words are nonempty; otherwise, the assertion is obvious. Suppose that \( \bar{u} = \bar{v} \) and \( \hat{u} = \hat{v} \), that is, \( \bar{u} \bar{u} = \bar{v} \bar{v} \) and \( \hat{u} \hat{u} = \hat{v} \hat{v} \). Then

\[
\bar{u} \bar{v} \hat{v} = \bar{u} \bar{v} \hat{v} = \bar{u} \bar{u} \hat{u} \hat{v} = \bar{u} \bar{v} \hat{u} \hat{v} = \bar{u} \bar{v} \hat{v} = \hat{u} \hat{u} \hat{v},
\]

that is, \( \bar{u} \bar{v} \hat{v} \) commutes with \( \bar{v} \hat{v} \). Since a word which is not a proper power can commute only with its powers [5], we obtain \( \bar{u} \bar{v} \hat{v} = \bar{v}^k = (\bar{v} \bar{v})^k \). This means that \( |\bar{u}| \geq |\bar{v}| \), that is, \( |\bar{u}| = |\bar{v}| \) by virtue of the symmetry between \( u \) and \( v \). Hence \( k \) must be 1 and \( \bar{u} = \bar{v} \), as required.

The proof of the second assertion we leave to the reader as an exercise. In [2], this assertion (but with rougher estimate) was called the second overlapping lemma.

**Lemma 2.** For any finite set \( A \subset F_2 \), there exist a word \( u \in F_2 \) and sets \( A_0, B_0 \subseteq uAu^{-1} \) such that \( |A_0|, |B_0| \geq \frac{1}{62} |A| \) and

1) for any \( a \in A_0 \) and \( b \in B_0 \) the words \( ab \) and \( ba \) are reduced;
2) \( |b| \geq |a| \) for all \( b \in B_0 \) and \( a \in A_0 \).
Proof. Let \( x_1 \) and \( x_2 \) be free generators of the group \( F_2 \), and let \( e \) denote the empty word. We prove the lemma by induction on the sum of lengths of words from the set \( A \). Let us decompose \( A \) into the union of the 16 disjoint subsets

\[
A(x,y) = \{ \text{words from } A \text{ beginning with } x \text{ and ending with } y \},
\]

where \( x, y \in \{ x_1, x_1^{-1}, x_2, x_2^{-1} \} \).

(If \( A \) contains the empty word, then we include it in \( A(x_1, x_1)^* \).)

Case 1. \(|A(x,y)| \geq \frac{1}{31}|A|\) for some not mutually inverse \( x \) and \( y \). In this case we put \( A_0 \) to be the set of \( \left[ \frac{1}{2}(|A(x,y)| + 1) \right] \) shortest words from \( A(x,y) \), and put \( B_0 \) to be the set of \( \left[ \frac{1}{2}(|A(x,y)| + 1) \right] \) longest words from \( A(x,y) \). Clearly, these sets \( A_0 \) and \( B_0 \) are as required (with \( u = e \)).

Case 2. \(|A(x,x^{-1})| \geq \frac{1}{31}|A| < |A(y,y^{-1})|\) for some different \( x \) and \( y \). Without loss of generality, we assume that a mean (by length) word from \( A(x,x^{-1}) \) is no longer than a mean word from \( A(y,y^{-1}) \). In this case we put \( A_0 \) to be the set of \( \left[ \frac{1}{2}(|A(x,x^{-1})| + 1) \right] \) shortest words from \( A(x,x^{-1}) \) and put \( B_0 \) to be the set of \( \left[ \frac{1}{2}(|A(y,y^{-1})| + 1) \right] \) longest words from \( A(y,y^{-1}) \). Clearly, these sets \( A_0 \) and \( B_0 \) are as required (with \( u = e \)).

If the conditions of neither Case 1 nor Case 2 hold, then, obviously, for some letters \( x \),

\[
|A(x,x^{-1})| > \left( 1 - \frac{15}{31} \right) |A| = \frac{16}{31} |A| > \frac{1}{2} |A|
\]

and therefore, the total length of words of the set \( x^{-1}Ax \) is less than the total length of words of the set \( A \). The application of the induction hypothesis completes the proof.

Lemma 3. Suppose that \( U, V, W \subseteq F_2 \) and all products \( UVW \) are reduced. If \( |v| \geq |u| \) for all \( u \in U \) and \( v \in V \), then either \( |UVW| \geq \frac{1}{5}|U| \cdot |W| \) or all words from \( V \) are periodic with the same period. Similarly, if \( |v| \geq |w| \) for all \( w \in W \) and \( v \in V \), then either \( |UVW| \geq \frac{1}{6}|U| \cdot |W| \) or all words from \( V \) are periodic with the same right period.

We prove the lemma in what follows. Now let us derive the theorems from Lemmas 2 and 3.

§ 3. Proof of the theorem

The words from \( A \) have only finitely many different letters. Therefore, \( A \) is contained in a free group \( F_m \) of finite rank. Since, as is known, \( F_m \) embeds into \( F_2 \) [5], we can assume that \( m = 2 \). Clearly, it is sufficient to prove the assertion of the theorem for odd \( n \), so we assume that \( n = 2k + 1 \).

Applying Lemma 2 to \( A \) we obtain sets \( A_0, B_0 \subseteq u^{-1}Au \). Note that \(|(uAu^{-1})^n| = |A^n|\), and therefore we can assume that \( u = e \).

First, consider the case where the set \( B_0 \) consists of periodic words with the same period \( p \) and the same tail \( t \):

\[
B_0 = \{ p^{n_1}t, p^{n_2}t, \ldots \}.
\] (1)
If $t = e$, then there exists a word $b \in A$ not commuting with $p$ because by hypothesis, the set $A$ contains noncommuting elements. The group generated by $p$ and $b$ is generated by them freely because any two noncommuting words freely generate a free group of rank 2 (see [5]). Therefore, all products of the form $u_1b \cdots u_kbuk+1$, where $u_i \in B_0$, are different and, hence, $|A^n| \geq |(B_0b)^kB_0| = |B_0|^{k+1} \geq O(|A|^{k+1})$.

If $t \neq e$, then we estimate $|B_0^n|$. Since $p$ and $t$ do not commute,\(^1\) they freely generate a free group of rank 2. Therefore, all words $\prod_{i=1}^n u_i$, where $u_i \in B_0$, are different and $|B_0^n| \geq O(|A^n|).

Now consider the case when $B_0$ is not of the form (1). Let us prove the inequality

$$|(A_0B_0)^kA_0| \geq O(|A|^{k+1})$$

by induction on $k$. For $k = 0$, the assertion is obvious.

By Lemma 1 either not all left periods of words from $B_0$ coincide, or not all right periods of words from $B_0$ coincide. Without loss of generality, we assume that the left periods do not coincide.

Applying Lemma 3 to the sets $U = A_0$, $V = B_0$ and $W = (A_0B_0)^{k-1}A_0$ we obtain the required inequality

$$|A_0 \cdot B_0 \cdot (A_0B_0)^{k-1}A_0| \geq O(|A_0| \cdot |(A_0B_0)^{k-1}A_0|) \geq O(|A|^{k+1}).$$

\section*{§ 4. Proof of Lemma 3}

\textbf{Lemma 4.} Suppose that words $u_1, u_2, u_3, v, w_1, w_2, w_3 \in F_2$ are such that the $u_i$ are pairwise different, $u_1w_1 = u_2w_2 = u_3w_3$, $|v| \geq |u_i|$, and all the words $u_iw_i$ are reduced. Then the word $v$ is periodic with period $\tilde{v}$ and one of the words $u_i$ ends with $\tilde{v}$.

\textbf{Proof.} We see that the word $f = u_1w_1 = u_2w_2 = u_3w_3$ has three occurrences of the subword $v$. Without loss of generality, we can assume that $|u_1| < |u_2| < |u_3|$. Since $|v| \geq |u_i|$, any two of these three occurrences of $v$ either intersect or, at least, are adjacent to each other (that is, the $k$th letter of $f$ is the end of one occurrence of $v$ and the $(k+1)$th letter of $f$ is the beginning of the other occurrence of $v$). Therefore, the second occurrence of $v$ is completely covered by the first and third occurrences of $v$ and, hence, the second occurrence of $v$ intersects with one of the other occurrences (say, the first) in a subword of length at least $\frac{1}{2}|v|$. By the second assertion of Lemma 1, this means that the word $v$ is periodic and the word $u_2$ ends with $\tilde{v}$.

\textbf{Lemma 5.} Suppose that sets $U$, $V$ and $W$ satisfy the conditions of Lemma 3 and $v \in V$. If $U$ contains no words ending with the period of $v$ or the word $v$ is non-periodic, then $|UvW| \geq \frac{1}{2}|U| \cdot |W|$.

\textbf{Proof.} Lemma 4 shows that no word has more than two representations as a product $uvw$, where $u \in U$ and $w \in W$. Therefore, $|UvW| \geq \frac{1}{2}|U| \cdot |W|$, as required.

\(^1\)Because, in a free group, only powers of the same element commute [5], the period $p$ is not a proper power, and $|t| < |p|$.
Lemma 6. Suppose that \( \alpha \) and \( \beta \) are nonempty cyclically reduced words that are not proper powers, \( |\beta| > |\alpha| \), \( a, b \in F_2 \) are words ending with \( \beta^2 \), and \( a \) ends with \( \alpha^s \). Then \( b \) also ends with \( \alpha^s \).

Proof. If \( |\alpha^s| \leq |\beta^2| \), then since \( a \) and \( b \) end with \( \beta^2 \), they end with \( \alpha^s \), as required. If \( |\alpha^s| > |\beta^2| \), then the end \( \beta^2 \) of \( a \) has two different right periods, \( \alpha \) and \( \beta \); this contradiction completes the proof.

Lemma 7. Suppose that sets \( U, V \) and \( W \) satisfy the conditions of Lemma 3 and there exists a periodic word \( v \in V \) with period \( \tilde{v} \) such that all words in \( U \) end with \( \tilde{v}^q \) and none of them ends with \( \tilde{v}^{q+1} \), where \( q \geq 1 \). Then \( |UvW| \geq \frac{1}{2} |U| \cdot |W| \).

This lemma follows immediately from Lemma 5 in which for \( U, V \) and \( W \) the sets \( U\tilde{v}^{-q}, \tilde{v}^qV \) and \( W \), respectively, are taken and the word \( \tilde{v}^qv \) is taken for \( v \).

Proof of Lemma 3. Clearly, it is sufficient to prove the first assertion. By Lemma 5, we may assume that the set \( V \) consists of periodic words.

Suppose that \( V \) has two words \( v_1 \) and \( v_2 \) with different periods \( \tilde{v}_1 \) and \( \tilde{v}_2 \). Suppose that \( |\tilde{v}_1| \geq |\tilde{v}_2| \). Applying Lemma 5 once again we obtain that either the required inequality holds or there exists a set \( U_0 \subseteq U \) such that \( |U_0| \geq \frac{1}{3} |U| \) and all words in \( U_0 \) end with both \( \tilde{v}_1 \) and \( \tilde{v}_2 \). This means, in particular, that \( \tilde{v}_1 \) ends with \( \tilde{v}_2 \) and \( |\tilde{v}_1| > |\tilde{v}_2| \) (because \( \tilde{v}_1 \neq \tilde{v}_2 \)).

Let \( U_{00} \) be the set of words from \( U_0 \) ending with \( \tilde{v}_2^2 \). By Lemma 6, all words from \( U_{00} \) end with \( \tilde{v}_1^s \), and none of them ends with \( \tilde{v}_1^{s+1} \). By Lemma 7 (in which the role of \( U \) is played by \( U_{00} \) and the role of \( v \) is played by \( v_1 \) ), we have

\[
|U_{00}v_1W| \geq \frac{1}{2} |U_{00}| \cdot |W|.
\]  

On the other hand, in the set \( U_0 \setminus U_{00} \), all words end with \( \tilde{v}_2 \), but none ends with \( \tilde{v}_2^2 \). Therefore, by Lemma 7 (in which the role of \( U \) is played by \( U_0 \setminus U_{00} \), and the role of \( v \) is played by \( v_2 \) ), we have

\[
|(U_0 \setminus U_{00})v_2W| \geq \frac{1}{2} |U_0 \setminus U_{00}| \cdot |W|.
\]  

Inequalities (2) and (3) imply

\[
|U_0 \cdot (\{v_1\} \cup \{v_2\}) \cdot W| \geq \frac{1}{2} |U_0| \cdot |W| = \frac{1}{6} |U| \cdot |W|,
\]

as required.

Bibliography

[1] M.-Ch. Chang, “Product theorems in SL_2 and SL_3”, J. Inst. Math. Jussieu 7:1 (2008), 1–25.
[2] A. A. Razborov, A product theorem in free groups, preprint, 2007; http://people.cs.uchicago.edu/~razborov/files/free_group.pdf.
[3] M. B. Nathanson, Additive number theory. Inverse problems and the geometry of sumsets, Grad. Texts in Math., vol. 165, Springer-Verlag, New York 1996.
[4] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., vol. 105, Cambridge Univ. Press, Cambridge 2006.

[5] A. G. Kurosch, *The theory of groups*, 3rd ed., Nauka, Moscow 1967; English transl of the 2nd ed., Chelsea Publ., New York 1955.

S. R. Safin

Faculty of Mechanics and Mathematics, Moscow State University

E-mail: stas.mail@mail.ru

Received 31/OCT/10

Translated by S. SAFIN