Math-Net.Ru

Общероссийский математический портал

С. Р. Сафин, Степени подмножеств свободных групп,
Матем. сб., 2011, том 202, номер 11, 97–102

DOI: <https://doi.org/10.4213/sm7811>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.210.77.194

26 апреля 2023 г., 13:14:47

УДК 512.544

С. Р. Сафин

Степени подмножеств свободных групп

Доказано, что $|A^n| \geq c_n \cdot |A|^{[(n+1)/2]}$ для любого конечного подмножества A свободной группы, содержащего хотя бы два некоммутирующих элемента, где $c_n > 0$ – некоторые константы, не зависящие от A . Несложные примеры показывают, что ни для какого $n > 0$ улучшить порядок этих оценок нельзя.

Библиография: 5 названий.

Ключевые слова: свободная группа, соотношения в свободной группе, подмножества свободной группы.

§ 1. Введение

Будем придерживаться следующих обозначений: F_m – свободная группа ранга m ; $|A|$ – мощность множества A ; AB – множество всевозможных произведений вида ab , где $a \in A$ и $b \in B$; A^n – множество всевозможных произведений вида $a_1 \cdots a_n$, где $a_i \in A$; $|a|$ – длина слова a в некотором алфавите; $[x]$ – целая часть вещественного числа x .

Мей-Чу Чанг (см. [1]) доказала, что существуют константы $c, \delta > 0$ такие, что для любого конечного подмножества A группы $SL_2(\mathbb{C})$, не содержащегося ни в какой почти абелевой подгруппе, справедлива оценка $|A^3| > c \cdot |A|^{1+\delta}$. В частности, такая оценка имеет место для любого конечного подмножества свободной группы, не содержащегося ни в какой циклической подгруппе. А. А. Разборов (см. [2]) улучшил оценку Чанг в этом частном случае: существует константа $c > 0$ такая, что для любого конечного подмножества A свободной группы, не содержащегося ни в какой циклической подгруппе, справедливо неравенство $|A \cdot A \cdot A| \geq \frac{|A|^2}{(\log |A|)^c}$. Нетрудно понять, что для квадрата подмножества никаких нетривиальных аналогов неравенства Чанг–Разборова не существует; наилучшая возможная оценка в этом случае линейная (более подробную информацию по этой теме можно найти в [3], [4]).

Следующая теорема показывает, в частности, что логарифм в оценке Разборова можно убрать.

ТЕОРЕМА 1. *Существуют такие константы $c_n > 0$, что для любого конечного подмножества A свободной группы, не содержащегося ни в какой циклической подгруппе, справедливо неравенство $|A^n| \geq c_n \cdot |A|^{[(n+1)/2]}$ при всех натуральных n .*

Нетрудно убедиться, что если $A = \{x, y, y^2, \dots, y^k\}$, то $|A^n| = O(k^{[(n+1)/2]})$ для каждого фиксированного $n \geq 1$, где x и y – свободные образующие свободной группы. Действительно, при $n = 1$ и $n = 2$ утверждение очевидно. Далее

по индукции получаем

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

Этот несложный пример, показывает, что ни для какого n улучшить порядок наших оценок нельзя.

Отметим еще, что приведенное ниже доказательство значительно проще, чем рассуждение из [2], но, с другой стороны, в [2] доказан более общий факт о числе элементов в произведении трех (возможно, различных) подмножеств свободной группы.

В коммутативном случае, т.е. когда множество A содержится в циклической группе, ситуация принципиально иная. Обзор результатов на эту тему можно найти в [2] и в литературе, там цитируемой.

Автор благодарит А. А. Клячко за постановку задачи, внимание к работе и ценные замечания.

§ 2. Вспомогательные леммы

Периодом или *левым периодом* слова w в некотором алфавите будем называть такое непустое слово $\tilde{w}$, не являющееся истинной степенью, что слово w представляется в виде $w = \tilde{w}^s \vec{w}$, где $s \geq 2$ и $\vec{w}$ – некоторое начало слова $\tilde{w}$ (возможно, пустое, но не совпадающее с $\tilde{w}$). Слово $\vec{w}$ в этой ситуации будем называть *хвостом* (или *правым хвостом*) слова w . Хорошо известно, что период и хвост периодического слова определены однозначно.

Правым периодом слова w в некотором алфавите будем называть такое непустое слово $\hat{w}$, не являющееся истинной степенью, что слово w представляется в виде $w = \overleftarrow{w} \hat{w}^s$, где $s \geq 2$ и $\overleftarrow{w}$ – некоторый конец слова $\hat{w}$ (возможно, пустой, но не совпадающий с $\hat{w}$). Слово $\overleftarrow{w}$ в этой ситуации будем называть *левым хвостом* слова w . Хорошо известно, что слово обладает правым периодом тогда и только тогда, когда оно обладает левым периодом (такие слова мы называем *периодическими*), причем либо оба хвоста $\overleftarrow{w}$ и $\vec{w}$ пусты, либо имеют место равенства $\tilde{w} = \vec{w} \overleftarrow{w}$ и $\hat{w} = \overleftarrow{w} \vec{w}$.

В следующей лемме мы собрали некоторые известные свойства периодических слов.

ЛЕММА 1. *Если у двух периодических слов совпадают левые периоды и совпадают правые периоды, то у них совпадают хвосты.*

Если для некоторых слов $u_1 v w_1 = u_2 v w_2$ и $0 < |u_2| - |u_1| \leq \frac{1}{2}|v|$ (т.е. некоторое слово имеет два вхождения слова v и эти вхождения пересекаются по слову длины по крайней мере $\frac{1}{2}|v|$), то слово v периодическое и u_2 заканчивается на $\tilde{v}$.

ДОКАЗАТЕЛЬСТВО. Докажем первое утверждение. Можно считать, что хвосты обоих слов непусты, иначе утверждение очевидно. Пусть $\tilde{u} = \tilde{v}$ и $\hat{u} = \hat{v}$, т.е. $\overrightarrow{u} \overleftarrow{u} = \overrightarrow{v} \overleftarrow{v}$ и $\overleftarrow{u} \overrightarrow{u} = \overleftarrow{v} \overrightarrow{v}$. Тогда

$$\overrightarrow{u} \overleftarrow{v} \tilde{v} = \overrightarrow{u} \overleftarrow{v} \overrightarrow{v} \overleftarrow{v} = \overrightarrow{u} \overleftarrow{u} \overrightarrow{u} \overleftarrow{v} = \overrightarrow{v} \overleftarrow{v} \overrightarrow{u} \overleftarrow{v} = \tilde{v} \overrightarrow{u} \overleftarrow{v},$$

т.е. $\overrightarrow{u} \overleftarrow{v}$ коммутирует с $\overrightarrow{v} \overleftarrow{v} = \tilde{v}$. Поскольку слово, не являющееся истинной степенью, может коммутировать только со своими степенями (см. [5]), мы получаем, что $\overrightarrow{u} \overleftarrow{v} = \tilde{v}^k = (\overrightarrow{v} \overleftarrow{v})^k$. Это означает, что $|\overrightarrow{u}| \geq |\overrightarrow{v}|$, т.е. $|\overrightarrow{u}| = |\overrightarrow{v}|$ в силу симметрии между u и v . Но тогда k обязательно будет единицей и $\overrightarrow{u} = \overrightarrow{v}$, что и требовалось доказать.

Доказательство второго утверждения мы оставляем читателю в качестве несложного упражнения. В работе [2] это утверждение (но с более грубой оценкой) называется второй леммой о наложении.

ЛЕММА 2. *Для любого конечного множества $A \subset F_2$ существуют слово $u \in F_2$ и множества $A_0, B_0 \subseteq uAu^{-1}$ такие, что $|A_0|, |B_0| \geq \frac{1}{62}|A|$ и:*

- 1) *для любых $a \in A_0$ и $b \in B_0$ слова ab и ba несократимы;*
- 2) *$|b| \geq |a|$ для всех $b \in B_0$ и $a \in A_0$.*

ДОКАЗАТЕЛЬСТВО. Обозначим буквами x_1, x_2 образующие свободной группы F_2 , а буквой e пустое слово. Будем доказывать лемму индукцией по суммарной длине слов из множества A . Разложим множество A в объединение шестнадцати непересекающихся подмножеств

$$A_{(x,y)} = \{\text{слова из } A, \text{ начинающиеся на } x \text{ и кончающиеся на } y\},$$

где $x, y \in \{x_1, x_1^{-1}, x_2, x_2^{-1}\}$.

(Если A содержит пустое слово, то присоединим его к $A_{(x_1, x_1)}$.)

Случай 1. $|A_{(x,y)}| \geq \frac{1}{31}|A|$ для некоторых x, y , не являющихся взаимнообратными. В этом случае в качестве A_0 возьмем $[\frac{1}{2}(|A_{(x,y)}| + 1)]$ наиболее коротких слов из $A_{(x,y)}$, а в качестве B_0 возьмем $[\frac{1}{2}(|A_{(x,y)}| + 1)]$ наиболее длинных слов из $A_{(x,y)}$. Ясно, что эти множества A_0 и B_0 являются искомыми (при $u = e$).

Случай 2. $|A_{(x, x^{-1})}| \geq \frac{1}{31}|A| \leq |A_{(y, y^{-1})}|$ для некоторых различных x, y . Без ограничения общности можно считать, что среднее по длине слово из $A_{(x, x^{-1})}$ не длиннее, чем среднее по длине слово из $A_{(y, y^{-1})}$. В этом случае в качестве A_0 возьмем $[\frac{1}{2}(|A_{(x, x^{-1})}| + 1)]$ наиболее коротких слов из $A_{(x, x^{-1})}$, а в качестве B_0 возьмем $[\frac{1}{2}(|A_{(y, y^{-1})}| + 1)]$ наиболее длинных слов из $A_{(y, y^{-1})}$. Ясно, что эти множества A_0 и B_0 являются искомыми (при $u = e$).

Если не выполнены условия ни случая 1, ни случая 2, то, очевидно, для некоторой буквы x

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

и, следовательно, суммарная длина слов множества $x^{-1}Ax$ меньше суммарной длины слов множества A . Ссылка на предположение индукции завершает доказательство.

ЛЕММА 3. *Пусть $U, V, W \subset F_2$ и все произведения UVW несократимы. Если $|v| \geq |u|$ для всех $u \in U$ и $v \in V$, то либо $|UVW| \geq \frac{1}{6}|U| \cdot |W|$, либо все слова из V периодичны с одним и тем же периодом. Аналогично, если $|v| \geq |w|$ для всех $w \in W$ и $v \in V$, то либо $|UVW| \geq \frac{1}{6}|U| \cdot |W|$, либо все слова из V периодичны с одним и тем же правым периодом.*

Эту лемму мы докажем позже, а пока докажем с помощью лемм 2 и 3 основной результат работы.

§ 3. Доказательство теоремы

В словах из A конечное количество различных букв. Значит, A содержится в свободной группе F_m конечного ранга. Поскольку, как известно, F_m вкладывается в F_2 (см. [5]), то можно считать, что $m = 2$. Ясно, что утверждение теоремы достаточно доказать для нечетных n , поэтому будем считать, что $n = 2k + 1$.

Применив лемму 2 к A , мы получим множества $A_0, B_0 \subseteq u^{-1}Au$. Заметим, что $|(uAu^{-1})^n| = |A^n|$, поэтому можно считать, что $u = e$.

Рассмотрим сначала случай, когда множество B_0 состоит из периодических слов с одинаковыми периодами p и одинаковыми хвостами t :

$$B_0 = \{p^{n_1}t, p^{n_2}t, \dots\}. \quad (1)$$

Если $t = e$, то существует слово $b \in A$, не коммутирующее с p , поскольку по условию множество A содержит некоммутирующие элементы. Группа, порожденная p и b , порождается ими свободно, так как любые два некоммутирующих слова свободно порождают свободную группу ранга 2 (см. [5]). Следовательно, все произведения вида $u_1b \cdots u_kbu_{k+1}$, где $u_i \in B_0$, различны и, значит, $|A^n| \geq |(B_0b)^k B_0| = |B_0|^{k+1} \geq O(|A|^{k+1})$.

Если $t \neq e$, то оценим $|B_0^n|$. Так как p и t не коммутируют¹, то они свободно порождают свободную группу ранга 2. Значит, все слова $\prod_{i=1}^n u_i$, где $u_i \in B_0$, различны и $|B_0^n| \geq O(|A|^n)$.

Теперь рассмотрим случай, когда B_0 не представимо в виде (1). Будем доказывать неравенство

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

индукцией по k . При $k = 0$ утверждение очевидно.

В силу леммы 1 либо не все левые периоды слов из B_0 совпадают, либо не все правые периоды слов из B_0 совпадают. Не умаляя общности, можно считать, что не совпадают левые периоды.

Применив лемму 3 к множествам $U = A_0$, $V = B_0$ и $W = (A_0B_0)^{k-1}A_0$, мы получим неравенство

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

которое и требовалось доказать.

§ 4. Доказательство леммы 3

ЛЕММА 4. Пусть слова $u_1, u_2, u_3, v, w_1, w_2, w_3 \in F_2$ такие, что u_i попарно различны, $u_1vw_1 = u_2vw_2 = u_3vw_3$, $|v| \geq |u_i|$ и все слова u_ivw_i несократимы. Тогда слово v периодически с периодом $\tilde{v}$ и одно из u_i оканчивается на $\tilde{v}$.

¹Поскольку коммутировать в свободной группе могут только степени одного элемента (см. [5]), период p не является истинной степенью и $|t| < |p|$.

ДОКАЗАТЕЛЬСТВО. В слове $f = u_1vw_1 = u_2vw_2 = u_3vw_3$ имеются, как мы видим, три вхождения подслова v . Не умаляя общности, можно считать, что $|u_1| < |u_2| < |u_3|$. Так как $|v| \geq |u_i|$, то любые два из этих вхождений v либо пересекаются, либо в крайнем случае расположены вплотную друг к другу (т.е. k -я буква является концом одного вхождения v , а $(k+1)$ -я буква является началом другого вхождения v). Поэтому второе вхождение v целиком покрывается первым и третьим вхождениями v и, следовательно, второе вхождение v пересекается с одним из остальных вхождений (будем считать, что с первым) по подслову длины по крайней мере $\frac{1}{2}|v|$. По второму утверждению леммы 1 это означает, что слово v периодически и слово u_2 заканчивается на $\tilde{v}$.

ЛЕММА 5. Пусть множества U , V и W удовлетворяют условиям леммы 3 и $v \in V$. Если в U нет слов, оканчивающихся на период слова v , либо слово v непериодическое, то $|UvW| \geq \frac{1}{2}|U| \cdot |W|$.

ДОКАЗАТЕЛЬСТВО. Из леммы 4 видно, что никакое слово не может быть представлено в виде произведения uvw , где $u \in U$ и $w \in W$, более чем двумя способами. Следовательно, $|UvW| \geq \frac{1}{2}|U| \cdot |W|$, что и требовалось.

ЛЕММА 6. Пусть α и β – непустые, циклически несократимые слова, не являющиеся истинными степенями, $|\beta| > |\alpha|$ и $a, b \in F_2$ – слова, оканчивающиеся на β^2 , причем a оканчивается на α^s . Тогда b оканчивается на α^s .

ДОКАЗАТЕЛЬСТВО. Если $|\alpha^s| \leq |\beta^2|$, то поскольку a и b оканчиваются на β^2 , они оканчиваются и на α^s , что и требовалось. Если же $|\alpha^s| > |\beta^2|$, то конец β^2 слова a имеет два различных правых периода, α и β , чего не может быть. Полученное противоречие завершает доказательство.

ЛЕММА 7. Пусть множества U , V и W удовлетворяют условиям леммы 3 и существует периодическое слово $v \in V$ с периодом $\tilde{v}$ такое, что все слова в U оканчиваются на $\tilde{v}^q$ и ни одно не оканчивается на $\tilde{v}^{q+1}$, где $q \geq 1$. Тогда $|UvW| \geq \frac{1}{2}|U| \cdot |W|$.

Эта лемма немедленно вытекает из леммы 5, если в ней в качестве U , V и W взять множества $U\tilde{v}^{-q}$, $\tilde{v}^qV$ и W соответственно, а в качестве v взять слово $\tilde{v}^qv$.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 3. Понятно, что достаточно доказать первое утверждение. По лемме 5 можно считать, что в множестве V все слова периодические.

Предположим, что в V есть два слова v_1 и v_2 с различными периодами $\tilde{v}_1$ и $\tilde{v}_2$. Будем считать, что $|\tilde{v}_1| \geq |\tilde{v}_2|$. Еще раз воспользовавшись леммой 5, можно сделать вывод, что либо доказываемое неравенство выполнено, либо существует множество $U_0 \subseteq U$ такое, что $|U_0| \geq \frac{1}{3}|U|$, и все слова в U_0 оканчиваются и на $\tilde{v}_1$, и на $\tilde{v}_2$. Это означает, в частности, что $\tilde{v}_1$ оканчивается на $\tilde{v}_2$ и $|\tilde{v}_1| > |\tilde{v}_2|$ (поскольку $\tilde{v}_1 \neq \tilde{v}_2$).

Пусть U_{00} – множество слов из U_0 , оканчивающихся на $\tilde{v}_2^2$. По лемме 6 все слова из U_{00} оканчиваются на $\tilde{v}_1^s$ и ни одно из них не оканчивается на $\tilde{v}_1^{s+1}$. По лемме 7 (в которой роль U играет U_{00} , а роль v играет v_1) мы имеем

$$|U_{00}v_1W| \geq \frac{1}{2}|U_{00}| \cdot |W|. \quad (2)$$

С другой стороны, в множестве $U_0 \setminus U_{00}$ все слова оканчиваются на $\tilde{v}_2$, но ни одно не оканчивается на $\tilde{v}_2^2$. Поэтому по лемме 7 (в которой роль U играет $U_0 \setminus U_{00}$, а роль v играет v_2) мы имеем

$$|(U_0 \setminus U_{00})v_2W| \geq \frac{1}{2}|U_0 \setminus U_{00}| \cdot |W|. \quad (3)$$

Из неравенств (2) и (3) следует, что

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

что и требовалось.

Список литературы

- [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 sum-sets*, Grad. Texts in Math., **165**, Springer-Verlag, New York, 1996.
- [4] T. Tao, V. H. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge Univ. Press, Cambridge, 2006.
- [5] А. Г. Курош, *Теория групп*, 3-е изд., Наука, М., 1967; англ. пер. 2-го изд.: A. G. Kurosch, *The theory of groups*, Chelsea Publ., New York, 1955.

С. Р. Сафин (S. R. Safin)

Механико-математический факультет
Московского государственного университета
им. М. В. Ломоносова
E-mail: stas.mail@mail.ru

Поступила в редакцию
31.10.2010