Сибирский математический журнал
Март—апрель, 2009. Том 50, № 2

УДК 512.543.12

ВЕРОЯТНОСТЬ ПОРОЖДЕНИЯ r ЭЛЕМЕНТАМИ В СВОБОДНОЙ ГРУППЕ РАНГА n ПОДГРУППЫ РАНГА r

Н. В. Бускин

Аннотация. Зафиксируем натуральные числа $n \geq 2, r, R$ и рассмотрим в свободной группе F_n упорядоченные наборы из r элементов длины $\leq R$. Среди выделенных наборов подсчитаем число таких, которые порождают в F_n подгруппу ранга r, и разделим это число на число всех выделенных наборов. Известно (см. [1]), что предел этого отношения при $R \to \infty$ существует и равен 1. В настоящей статье приводится простое доказательство этого результата.

Ключевые слова: типическая подгруппа, случайная подгруппа.

Условимся количество элементов произвольного конечного множества A обозначать через $\#A$.

Пусть G — конечно порожденная группа. Наименьшее число порождающих группу G элементов мы будем называть *рангом группы* G и обозначать через $rk(G)$. Зафиксируем некоторый набор порождающих группы G. Тогда на группе G может быть задана стандартная метрика $d(u,v) = |uv^{-1}|$, где u, v — вершины левого графа Кэли группы G, на котором G действует правыми умножениями, $|w|$ — словарная длина элемента w.

Шар $G(R) \subset G$ *радиуса* R — это множество $\{v \in G \mid d(1,v) \leq R\}$.

Обозначим через G^r прямое произведение r экземпляров множества G и через $\mathbf{1}$ — набор $(1,\dots,1) \in G^r$. На множестве G^r индуцируется метрика D: если $u = (u_1,\dots,u_r) \in G^r$, $v = (v_1,\dots,v_r) \in G^r$, то $D(u,v) = \max\{d(u_i,v_i), i = 1,\dots,r\}$. Шар $G^r(R) \subset G^r$ — это множество $\{\mathbf{u} = (u_1,\dots,u_r) \in G^r \mid D(\mathbf{1},\mathbf{u}) \leq R\}$.

Заметим, что шар $G^r(R) \subset G^r$ радиуса R является прямым произведением шаров $\prod\limits_{i=1}^{r} G(R)$. Подсчитаем мощность шара $G^r(R)$ в случае, когда группа G является свободной группой ранга n, $G = F_n$. В группе F_n есть ровно один элемент нулевой длины (единица), элементов длины k, $k \geq 1$, имеется ровно $2n(2n-1)^{k-1}$ штук, так что

$$\#F_n(R) = 1 + 2n + 2n(2n-1) + \dots + 2n(2n-1)^{R-1}$$
$$= \frac{n}{n-1}(2n-1)^R - \frac{1}{n-1} < \frac{n}{n-1}(2n-1)^R.$$

Кроме того,

$$\#F_n(R) = \frac{n}{n-1}(2n-1)^R - \frac{1}{n-1} > \frac{n}{n-1}((2n-1)^R - 1).$$

Следовательно,

$$\left(\frac{n}{n-1}\right)^r ((2n-1)^R - 1)^r < \#F_n^r(R) < \left(\frac{n}{n-1}\right)^r (2n-1)^{rR}.$$

Эти оценки пригодятся нам в дальнейшем.

Зафиксируем теперь $r \geq 0$ и рассмотрим отношение

$$f_{r,R}(G) = \frac{\#\{(u_1,\dots,u_r) \in G^r(R) \mid rk(\langle u_1,\dots,u_r\rangle) = r\}}{\#G^r(R)}.$$

Вероятностью порождения r элементами группы G подгруппы ранга r называется предел $f_r(G) = \lim\limits_{R\to\infty} f_{r,R}(G)$, если только такой предел существует.

Далее в качестве группы G будет рассматриваться свободная группа F_n с любым базисом в качестве системы порождающих.

Простым упражнением является доказательство того, что $f_1(F_n) = 1$. Поэтому будем считать, что $r \geq 2$.

В работе [1] доказано, что $f_r(F_n) = 1$, т. е. доля независимых наборов стремится к 1. Приведем более короткое доказательство этого факта.

Теорема. *Пусть $n \geq 2, r \geq 2$. Тогда для всех натуральных R выполняется*

$$f_{r,R}(F_n) > 1 - \frac{cR}{(2n-1)^{\frac{R}{2}}},$$

где $c = r^2\left(\frac{3}{2}\right)^r$. В частности, вероятность порождения r элементами свободной группы ранга n подгруппы ранга r равна 1.

Доказательство. Введем необходимое в дальнейшем определение. Назовем набор $(u_1,\dots,u_r) \in F_n^r(R)$ *нередуцированным*, если для некоторых i, j, где $i \neq j$, выполнено одно из следующих трех условий:

(a) $|u_i u_j| \leq |u_j|$;
(b) $|u_i^{-1} u_j| \leq |u_j|$;
(c) $|u_i u_j^{-1}| \leq |u_j|$.

Фактически нередуцированность набора $(u_1,\dots,u_r)$ означает, что для некоторых $i \neq j$ в одном из произведений выше сокращается не менее половины слова $u_i^{\pm 1}$, т. е., например, в первом случае слова u_i, u_j представимы в виде $u_i = uv, u_j = v^{-1}w$, где произведения $uv, v^{-1}w$ свободно приведены и $|u_i| \leq 2|v|$.

Введем обозначение

$$D(R) = \big\{(u_1,\dots,u_r) \in F_n^r(R) \mid (u_1,\dots,u_r) \text{ нередуцирован}\big\}.$$

Ясно, что если набор $(u_1,\dots,u_r)$ лежит в множестве $F_n^r(R) \setminus D(R)$, то он является нильсеновски приведенным (см. [2]) и, следовательно, порождает в F_n подгруппу ранга r (последнее утверждение очевидно и без ссылки на [2]).

Перепишем неравенство из утверждения теоремы в следующем виде:

$$1 - f_{r,R}(F_n) < \frac{cR}{(2n-1)^{\frac{R}{2}}}.$$

Левая часть последнего неравенства — это в точности доля наборов $(u_1,\dots,u_r)$ в шаре $F_n^r(R)$, которые порождают в F_n подгруппу ранга строго меньше r (зависимых наборов). В частности, каждый такой набор должен быть нередуцированным и, следовательно, лежать в $D(R)$.

Оценим отношение $\frac{\#D(R)}{\#F_n^r(R)}$.

Пусть $(u_1, \ldots, u_r) \in D(R)$. Тогда для всех i выполнено $|u_i| \leq R$ и для некоторых u_i, u_j выполнено одно из условий (a)–(c). Для удобства пусть это будут u_1, u_2 и выполнено условие (a). Тогда, как замечалось выше, $u_1 = uv, u_2 = v^{-1}w$ и $|u_1| \leq 2|v|$. На элементы $u_3, \ldots, u_r$, вообще говоря, не налагается никаких ограничений, кроме требования $|u_k| \leq R$. Так как $|uv| \leq R$ и $|u| \leq |v|$, то $|u| \leq \frac{R}{2}$. Значит, в общем случае такой набор определяется словами u, v, w с соответствующими ограничениями на длины и словами $u_3, \ldots, u_r \in F_n(R)$.

Заметим, что задание набора $(u_1, \ldots, u_r)$ с помощью слов $u, v, w, u_3, \ldots, u_r$ эквивалентно заданию с помощью слов $u, u_2, u_3, \ldots, u_r$, где $|u| \leq |u_2|$ (на u_2 никаких дополнительных ограничений не налагается), и фиксирования длины начального отрезка слова u_2, который определит слово v^{-1}, а значит, и v.

Для выбора слова $u, |u| \leq \frac{R}{2}$, имеется не более $\#F_n\left(\frac{R}{2}\right)$ возможностей, для выбора $u_2, \ldots, u_r$ — не более $\#F_n^{r-1}(R)$ возможностей, для выбора начального отрезка слова u_2, определяющего v^{-1}, — не более R возможностей. Таким образом, для выбора $(u_1, \ldots, u_r) \in D(R)$ с условием сокращения на u_1 и u_2 имеется не более $R \cdot \#F_n\left(\frac{R}{2}\right) \cdot \#F_n^{r-1}(R)$ возможностей.

Произвол в выборе i, j, от которого мы отказались вначале, компенсируется умножением полученной оценки на r^2.

Применяя приведенную ранее оценку сверху для мощности шара в F_n^l к множителям $\#F_n(\frac{R}{2})$ и $\#F_n^{r-1}(R)$, получаем $\#D(R) < r^2\left(\frac{n}{n-1}\right)^r R(2n-1)^{(r-\frac{1}{2})R}$. Применяя оценку снизу для $\#F_n^r(R)$, получаем

$$\frac{\#D(R)}{\#F_n^r(R)} < \frac{r^2\left(\frac{n}{n-1}\right)^r R(2n-1)^{(r-\frac{1}{2})R}}{\left(\frac{n}{n-1}\right)^r((2n-1)^R - 1)^r}$$
$$= \frac{r^2 R(2n-1)^{-\frac{R}{2}}}{\left(1 - \frac{1}{(2n-1)^R}\right)^r} \leq \frac{r^2 R}{(2n-1)^{\frac{R}{2}}(1-1/3)^r} = \frac{r^2(3/2)^r R}{(2n-1)^{\frac{R}{2}}}.$$

Теорема доказана.

ЛИТЕРАТУРА

1. *Martino A., Turner E. C., Ventura E.* The density of injective endomorphisms of a free group. (Preprint / CRM; N 685). 2006. Available at: http://www.crm.cat

2. *Линдон Р., Шупп П.* Комбинаторная теория групп. М.: Мир, 1980.

Статья поступила 16 января 2008 г., окончательный вариант — 22 августа 2008 г.

Бускин Николай Владиславович
Новосибирский гос. университет, механико-математический факультет,
ул. Пирогова, 2, Новосибирск 630090
buskin1983@mail.ru