S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 2, стр. 1–13 (2005) УДК 512.54+519.11+519.14
MSC 60B15, 20P05, 20E05

О СТРОГО РАЗРЕЖЕННЫХ ПОДМНОЖЕСТВАХ СВОБОДНОЙ ГРУППЫ

Я.С. АВЕРИНА, Е.В. ФРЕНКЕЛЬ

Abstract. This paper is motivated by needs of practical computations in finitely generated groups. In the most of the computations in finitely generated groups G the elements are represented as freely reduced words in the free group F. In [1] a family of probability measures was used for estimating the complexity of algorithms on groups and subsets of F were classified according to these measures. We find out which regular sets are sparse, i.e. small with respect to the probability measures.

1. Введение

Появление данной работы обусловлено потребностью практических вычислений в конечно порожденных группах. В большинстве компьютерных вычислений в конечно порожденных группах элементы группы G представляются редуцированными словами из свободной группы F, что связано с представлением $G = F \setminus N$. При изучении алгоритмов на конечно порожденных группах проводится стратификация входного множества F. Таким образом, возникают подмножества F, на которых алгоритм работает хорошо (например, за полиномиальное время), на которых алгоритм работает хуже и подмножества, для которых алгоритм не дает ответа. Если алгоритм достаточно хорош, то последние множества должны быть малыми. Как правило, описать эти множества достаточно трудно и поэтому их погружают в хорошие множества — например, регулярные. Следуя идеям статьи [1], мы провели формализацию понятия малого множества — это так называемое разреженное множество; исследовали, какие регулярные множества являются разреженными, то есть малыми относительно тех мер, которые будут введены в этой статье. Так что если алгоритм

Averina, Ya.S., Frenkel, E.V., On strictly sparse subsets of a free group.

Поступила 3 декабря 2004 г., опубликована 3 марта 2004 г.

не работает только лишь на разреженном множестве либо его подмножестве, то этот алгоритм можно по праву считать хорошим.

Мы выражаем благодарность нашему научному руководителю В.Н. Ремесленникову за помощь при написании данной работы.

2. Регулярные подмножества свободной группы

Пусть F — свободная группа ранга z над алфавитом $X = \{x_1, \dots, x_z\}$. Элементами группы F будем называть редуцированные слова (то есть такие слова, которые не содержат подслов вида xx^{-1} или $x^{-1}x$). Длиной слова f из F назовем длину редуцированного слова, будем обозначать ее $|f|$. Под S_j будем понимать множество элементов длины j в группе F. Можно показать, что $|S_j| = 2z(2z-1)^{j-1}$. Пусть $H \subset F$; обозначим через n_j число слов длины j в H, а $f_j = \dfrac{n_j}{|S_j|} = \dfrac{|S_j \cap H|}{|S_j|}$. Величины $f_j = f_j(H)$ называют относительными частотами для H. На F следующим образом вводится мера λ (см. [1]):

$\forall\ w \in F, \lambda(w) = \dfrac{1}{2z(2z-1)^{|w|}}$, если $w \neq 1$ и $\lambda(1) = 1$.

Тогда в приведенных выше обозначениях $\lambda(H) = \sum\limits_{w\in H} \lambda(w) = \sum\limits_{k=0}^{\infty} f_k(H)$. Таким образом, H является λ-измеримым, когда ряд $\sum\limits_{k=0}^{\infty} f_k(H)$ сходится.

При оценке множеств важны как асимптотические, так и вероятностные характеристики и Лемма 1 раскрывает связь между этими характеристиками подмножеств группы F. В нашей статье основное внимание уделяется асимптотическим характеристикам.

Приведем некоторые необходимые нам сведения о семействе атомарных вероятностных мер $\{\mu_s,\ s \in (0,1]\}$ для подмножеств группы F (подробнее см.[1]). Мера μ на счетном множестве X называется атомарной, если каждое подмножество $Y \subseteq X$ измеримо; при этом $\mu(Y) = \sum\limits_{y\in Y} \mu(y)$. Мера слова $w \in F$ определяется следующим образом:

$\mu_s(w) = \dfrac{s(1-s)^{|w|}}{2z(2z-1)^{|w|-1}}$ для $w \neq 1$ и $\mu_s(1) = s$.

Поскольку мера μ_s атомарна, то мера подмножества H находится по формуле:

$$\mu_s(H) = \sum_{w\in H} \mu_s(w).$$

Далее нам понадобится следующее определение, введенное в [2]. X-диграф Γ называют f-диграфом (folded digraph), если для всякой вершины v графа Γ и для всякой метки $x \in X$ в Γ существует не более одного ребра с меткой x и началом в v, а также не более одного ребра с меткой x и концом в v. [1] Напомним, что регулярное множество можно определять как множество, распознаваемое конечным детерминированным автоматом (это верно благодаря теореме Клини-Рабина-Скотта, см. [5]). В дальнейшем в данной работе будет

[1]Если диграф является f-диграфом, то соответствующий ему автомат является детерминированным. В [2] показано, что проведение над графом операции схлопывания (folding) не меняет распознаваемого графом языка. Поэтому без ограничения общности можно считать граф f-диграфом.

удобно иметь дело не с детерминированным автоматом, а с f-диграфом. Самое существенное отличие этих двух понятий заключается в том, что в случае f-диграфа одно и то же ребро последовательно не проходится в различных направлениях, то есть диграфом распознаются только редуцированные слова. Но поскольку множество всех редуцированных слов и множество, распознаваемое конечным детерминированным автоматом, регулярны, то множество, распознаваемое диграфом, регулярно как пересечение регулярных множеств.

Если H — регулярное множество, то для s из некоторой окрестности нуля последнюю формулу можно переписать (см. [1]) в виде степенного ряда:

$$\mu_s(H) = m_0 + m_1 s + m_2 s^2 + \dots.$$

В этом случае $\mu_0(H) = \lim\limits_{s\to 0^+} \mu_s(H) = m_0$. Пусть $\mu_1(H) = \lim\limits_{s\to 0^+} \dfrac{\mu_s(H)}{s}$.

Подмножество H называется разреженным, если $\mu_0(H) = 0$, $\mu_1(H)$ существует и $\mu_s(H) = \mu_1(H)s + \alpha_1(s)$, где $\lim\limits_{s\to 0^+} \dfrac{\alpha_1(s)}{s} = 0$.

Подмножество H называется сгущенным, если $\mu_0(H)$ существует, $\mu_0(H) > 0$ и $\mu_s(H) = \mu_0(H) + \alpha_0(s)$, где $\lim\limits_{s\to 0^+} \alpha_0(s) = 0$. Напомним, что для слов u и v из F запись $u \circ v$ означает отсутствие сокращений на стыке u и v, то есть uv — редуцированное произведение. В [1] показано, что множество $C(w) = \{w \circ f |\ f \in F\}$ является сгущенным множеством; $C(w)$ называется конусом.

Появление термина "разреженное множество" еще раз возвращает нас к идеям введения: разреженное множество и играет роль того самого, малого относительно введенных мер множества. Любое регулярное множество является либо разреженным, либо сгущенным, причем если множество — это подгруппа конечного индекса в F, то оно будет сгущенным (см.[1]).

Лемма 1. *Подмножество H группы F является разреженным тогда и только тогда, когда оно λ-измеримо.*

Доказательство. Пусть множество H λ-измеримо. По теореме Харди -Литтлвуда $\mu_0(H)$ равно следующему пределу по Чезаро:

$$\mu_0(H) = \lim_{s\to 0^+} \mu_s(H) = \lim_{n\to\infty} \frac{1}{n}(f_0 + f_1 + \dots + f_n),$$

который, в силу сходимости ряда из относительных частот, равен нулю, и, следовательно, $\mu_0(H) = 0$. Тогда

$$\mu_1(H) = \lim_{s\to 0^+} \frac{\mu_s(H) - \mu_0(H)}{s} = \lim_{s\to 0^+} \frac{s\sum\limits_{k=0}^{\infty} f_k(H)(1-s)^k}{s} = \sum_{k=0}^{\infty} f_k(H) < \infty.$$

Это и означает разреженность H.

Теперь предположим, что множество H – разреженное и докажем его λ-измеримость. В некоторой окрестности нуля верно равенство

$$\frac{\mu_1(H)s + \alpha_1(s)}{s} = \sum_{k=0}^{\infty} f_k(H)(1-s)^k.$$

Совершая предельный переход в этом равенстве при s, стремящемся к нулю, получаем сходимость ряда в правой части, так как предел левой части конечен и равен $\mu_1(H)$. Сходимость ряда $\sum\limits_{k=0}^{\infty} f_k(H)$ следует из того, что

$$\lim_{s\to 0^+}\sum_{k=0}^{\infty} f_k(H)(1-s)^k = \sum_{k=0}^{\infty}\lim_{s\to 0^+} f_k(H)(1-s)^k = \mu_1(H).$$

Значит, H λ-измеримо. $\square$

Приведем некоторые определения, связанные с используемыми в дальнейшем размеченными графами (X-диграфами).

X-диграф Γ называется X-полным, если для каждой его вершины v и каждой метки $x \in X\bigcup X^{-1}$ существует одно и только одно ребро с меткой x, выходящее из v (см.[2]).

X-диграф Γ называется связным, если для любых двух его вершин существуют путь, их соединяющий.

В [2] введено понятие $Core(\Gamma, v)$, где v — некоторая вершина графа Γ :

$$Core(\Gamma, v) = \bigcup\{p \mid p \text{ — редуцированный путь из } v \text{ в } v \text{ в графе } \Gamma\}.$$

Если $\Gamma = Core(\Gamma, v)$, то Γ называется *ядром* относительно вершины v.

Пусть u и v — две произвольные вершины конечного графа Γ. Диаметром d графа Γ назовем число $d = \max\limits_{u,v\in V\Gamma} |\pi(u,v)|$, где $\pi(u,v)$ – геодезический путь в Γ из u в v.

3. Определение и простейшие свойства строго разреженных множеств

Из леммы 1 следует, что разреженность множества H эквивалентна сходимости ряда из относительных частот для этого множества. Усилим требования к этому ряду, а именно, будем называть множество H *строго разреженным*, если существуют такие действительные числа q и $C > 0$, где $0 < q < 1$, что для всякого натурального k верно следующее неравенство

$$f_k < Cq^k.$$

Приведенному определению часто бывает удобно придать форму: множество называется строго разреженным, если начиная с некоторого номера $k > k_0$, верно $f_k < Cq^k$, где $k_0 > 0, C > 0$ и $0 < q < 1$. Нетрудно показать, что указанные определения эквивалентны (при должном подборе константы C).

Замечание 2. Дополнение к строго разреженному множеству — это строго генерическое множество. Определение и свойства генерических множеств можно найти в [4].

Рассмотрим некоторые свойства строго разреженных множеств.

1) Пусть R' — подмножество R и множество R — строго разрежено. Тогда и R' также является строго разреженным.

2) Пусть $R = \bigcup\limits_{i=1}^{m} R_i$, и каждое из множеств R_i – строго разрежено. Тогда R – строго разрежено.

Доказательства утверждений 1) и 2) очевидны.

3) Рассмотрим отображение $g : R \to S$, где R и S — подмножества свободной группы F. Пусть g обладает свойством: при фиксированном действительном числе $t > 0$ для всякого $r \in R$ выполняется $|\,|g(r)| - |r|\,| \le t$ (так называемое t-метрическое отображение).

Если R — строго разреженное множество, то и его образ $g(R)$ при t-метрическом отображении также будет разреженным.

Доказательство. Пусть $D = g(R)$ — образ множества R. Для относительных частот этого множества начиная с номера $k+t$ справедлива оценка:

$$f_k^D = \frac{n_k^D}{|S_k|} \le \frac{\sum\limits_{i=k-t}^{k+t} n_i^R}{|S_k|} = (f_{k-t}^R(2z-1)^{-t} + \ldots + f_{k+t}^R(2z-1)^t) =$$

$$= \sum_{i=-t}^{t} f_{k+i}^R (2z-1)^i < \sum_{i=-t}^{t} Cq^{k+i}(2z-1)^i < C(2z-1)^t \sum_{i=-t}^{t} q^{k+i} <$$

$$< C(2z-1)^t \cdot 2t \cdot q^{k-t} = C\left(\frac{2z-1}{q}\right)^t \cdot 2t \cdot q^k.$$

Значит, для множества D параметр q можно взять таким же, как и для R, а новая константа равна $C_D = C\left(\frac{2z-1}{q}\right)^t \cdot 2t$ и, таким образом, $D = g(R)$ становится строго разреженным. □

4) Пусть R, S — строго разреженные множества и $T = R \circ S = \{r \circ s | r \in R, s \in S\}$. В этом случае T тоже будет строго разреженным.

Доказательство. С некоторого номера k для относительных частот множества выполняется

$$f_k^T = \frac{n_k^T}{|S_k|} \le \frac{\sum\limits_{i=0}^{k} n_{k-i}^R n_i^S}{|S_k|} = \sum_{i=0}^{k} \frac{n_{k-i}^R}{|S_{k-i}|} \frac{n_i^S}{|S_i|} \frac{2z}{2z-1} < \frac{2z \cdot C_R \cdot C_S}{2z-1} \sum_{i=0}^{k} q_R^{k-i} q_S^i$$

Возможны следующие три ситуации:

а) имеет место неравенство $q_R > q_S$. Тогда

$$\sum_{i=0}^{k} q_R^{k-i} q_S^i = \frac{(q_R - q_S)}{(q_R - q_S)} \sum_{i=0}^{k} q_R^{k-i} q_S^i = \frac{(q_R^{k+1} - q_S^{k+1})}{(q_R - q_S)} = \frac{q_R^{k+1}\left(1 - \left(\frac{q_S}{q_R}\right)^{k+1}\right)}{(q_R - q_S)}.$$

Поскольку $0 < \left(1 - \left(\frac{q_S}{q_R}\right)^{k+1}\right) < 1$ в силу $q_R > q_S$, то

$$\frac{q_R^{k+1}\left(1 - \left(\frac{q_S}{q_R}\right)^{k+1}\right)}{(q_R - q_S)} < \frac{q_R^{k+1}}{(q_R - q_S)}$$

Возвращаясь к оценке f_k^T, получаем:

$$f_k^T < \frac{2z \cdot C_R \cdot C_S}{2z-1} \sum_{i=0}^{k} q_R^{k-i} q_S^i < \frac{2z \cdot C_R \cdot C_S}{2z-1} \cdot \frac{q_R^{k+1}}{(q_R - q_S)} = \frac{2z \cdot C_R \cdot C_S \cdot q_R}{(2z-1) \cdot (q_R - q_S)} \cdot q_R^k,$$

где, таким образом, $q_T = q_R$ и $C_T = \frac{2z \cdot C_R \cdot C_S \cdot q_R}{(2z-1) \cdot (q_R - q_S)}$ и множество T — строго разреженное.

б) имеет место неравенство $q_R < q_S$. Данная ситуация симметрична случаю а) и поэтому сразу выпишем параметры:

$q_T = q_S$ и $C_T = \frac{2z \cdot C_R \cdot C_S \cdot q_S}{(2z-1) \cdot (q_S - q_R)}$ и множество T – строго разреженное.

в) выполнено равенство $q_R = q_S$. Изменим один из параметров, например, q_R, следующим образом. Выберем q'_R так, что $q_R < q'_R < 1$. При этом неравенство строгой разреженности множества R выполняется и для нового параметра q'_R :

$$f_k^R < C_R q_R^k < C_R (q'_R)^k.$$

Таким образом, решение вопроса о строгой разреженности сводится к п. а). $\square$

5) Пусть R, S — строго разреженные множества и $P = R \underset{t}{*} S = \{rs : \forall r \in R, \forall s \in S\ |r| + |s| - |rs| \leq t\}$. Тогда P также строго разреженное.

Доказательство. С некоторого номера для относительных частот множества выполняется

$$f_k^P = \frac{n_k^P}{|S_k|} \leq \frac{\sum\limits_{i=0}^{k+t} n_{k+t-i}^R n_i^S}{|S_k|} =$$

$$= \sum_{i=0}^{k+t} \frac{n_{k+t-i}^R}{|S_{k+t-i}|} \frac{n_i^S}{|S_i|} \frac{2z}{(2z-1)^{t+1}} < \frac{2z \cdot C_R \cdot C_S}{(2z-1)^{t+1}} \sum_{i=0}^{k+t} q_R^{k+t-i} q_S^i.$$

Далее, как и в случае свойства 4, доказательство распадается на три случая, из которых мы рассмотрим один — остальные рассматриваются аналогично.

Предположим, что $q_R > q_S$. Тогда

$$\sum_{i=0}^{k+t} q_R^{k+t-i} q_S^i = \frac{(q_R - q_S)}{(q_R - q_S)} \sum_{i=0}^{k+t} q_R^{k+t-i} q_S^i = \frac{(q_R^{k+t+1} - q_S^{k+t+1})}{(q_R - q_S)} =$$

$$= \frac{q_R^{k+t+1}\left(1 - \left(\dfrac{q_S}{q_R}\right)^{k+t+1}\right)}{(q_R - q_S)} \leq \frac{q_R^{k+t+1}}{(q_R - q_S)}.$$

Значит,

$$f_k^P < \frac{2z \cdot C_R \cdot C_S}{(2z-1)^{t+1}} \sum_{i=0}^{k+t} q_R^{k+t-i} q_S^i < \frac{2z \cdot C_R \cdot C_S \cdot q_R^{t+1}}{(2z-1)^{t+1} \cdot (q_R - q_S)} \cdot q_R^k,$$

где, таким образом, $q_P = q_R$ и $C_P = \dfrac{2z \cdot C_R \cdot C_S \cdot q_R^{t+1}}{(2z-1)^{t+1} \cdot (q_R - q_S)}$ и множество P – строго разреженное. $\square$

6) Рассмотрим следующую конструкцию. Пусть M и T — строго разреженные множества. Рассмотрим множество M_0^T всех таких $m \in M$ и $t \in T$, для которых $m^t = t^{-1} \circ m \circ t$. Тогда множество $\bigcup\limits_{m,t \in M_0^T} m^t$ также является строго разреженным.

Доказательство указанного факта можно получить, пользуясь оценкой n_k — числа элементов длины k во множестве $\bigcup\limits_{m,t \in M_0^T} m^t$; оно оценивается следующим образом:

$$n_k \leq \sum_{p=0}^{[(k-1)/2]} n_p^T n_{(k-2p)}^M.$$

Дальнейшие рассуждения проводятся аналогично тому, как это делалось в свойствах 3)-5).

4. Критерий строгой разреженности множеств специального вида

Приведем теперь один из основных результатов данной работы.

Утверждение 1. *Пусть H — регулярное подмножество F, Γ — конечный автомат для H. Если Γ связный и не является X-полным, то H — строго разреженное в F множество.*

Доказательство. Для доказательства утверждения достаточно показать, что для относительных частот множества H начиная с некоторого k справедлива оценка $f_k < Cq^k$. Будем полагать, что $z \leq 2$, так как случай, когда группа F абелева тривиален. Поскольку по условию Γ не X-полный, то существуют вершина $v \in V\Gamma$ и буква $x \in X \bigcup X^{-1}$ такие, что из v не выходит ребра с меткой x. В силу сделанных выше оговорок будем далее отождествлять понятия размеченного диграфа и автомата для H. Пусть d — диаметр Γ. Для определенности будем полагать, что в Γ имеется только одна вершина (то есть v), из которой выходит менее $2z$ ребер. В противном случае, когда таких вершин несколько, число распознаваемых автоматом слов будет еще меньше и оценка самого множества — еще точнее. Расширим язык H, распознаваемый автоматом Γ, следующим образом: все вершины Γ объявим финальными и начальными. Полученный автомат $\overline{\Gamma}$ распознает язык R, содержащий префиксное замыкание H. Следовательно, согласно свойству 1 для строго разреженных множеств, достаточно получить требуемую в определении строгой разреженности оценку для языка R.

Обозначим через n_k число элементов длины k в R и n_k^v — число слов длины k, которым в $\overline{\Gamma}$ соответствуют пути длины k, оканчивающиеся в v. Покажем, что

$$\frac{n_k^v}{n_k} > \varepsilon, \tag{1}$$

для некоторого ε, где $0 < \varepsilon < 1$, $k > d$. Если граф X-полный, то пути длины $(k+1)$ получаются продлением путей длины k, причем каждый такой путь можно продлить $(2z-1)$ способом. Так как граф $\overline{\Gamma}$ таков, что все его вершины являются и начальными, и финальными, то для путей длины 2 верно неравенство $n_2 < n_1(2z-1)$. Аналогично, для путей длины $k > 1$ имеет место неравенство $n_{k+1} < n_k(2z-1)$, а, значит, $n_k < n_{k-d}(2z-1)^d$. Таким образом, для $k > d$, верно неравенство

$$\frac{n_{k-d}}{n_k} > \frac{1}{(2z-1)^d}.$$

Обозначим число $\dfrac{1}{(2z-1)^d}$ через ε. Значит, для $k > d$ предыдущее неравенство примет вид

$$\frac{n_{k-d}}{n_k} > \varepsilon. \tag{2}$$

Чтобы доказать неравенство (1), покажем сначала, что для $k > d$ выполнено $n_k^v > n_{k-d}$.

В самом деле, пусть p — редуцированный путь в $\overline{\Gamma}$ длины $k-d$. Поскольку $\overline{\Gamma}$ — связный граф с диаметром d, то из конечной вершины пути p существует по крайней мере один редуцированный путь p_l длины $l \leq d$ с конечной вершиной v. Конкатенацию путей p и p_l будем обозначать $\overline{p}$. Так как пути p и

p_l редуцированы, то есть не содержат фрагментов вида $e_i e_i^{-1}$ и $e_i^{-1} e_i$ (одно и тоже ребро последовательно не проходится в различных направлениях), следовательно, в $\overline{p}$ фрагменты указанного вида могут содержаться только на стыке p и p_l. Удаляя $e_i e_i^{-1}$ и $e_i^{-1} e_i$, проведем редукцию пути $\overline{p}$ и далее предполагаем, что он редуцированный. Если полученный путь $\overline{p}$ имеет длину t и $t < k$, то из условий, наложенных на $\overline{\Gamma}$, путь $\overline{p}$ всегда можно достроить (приписыванием ребер к началу $\overline{p}$) до пути длины k с конечной вершиной v.

Это означает, что $n_k^v > n_{k-d}$ при $k > d$, из чего в силу (2) получаем (1).

Покажем теперь, что относительные частоты ограничены сверху членами геометрической прогрессии, то есть что $\dfrac{n_k}{|S_k|} < Cq^k$. Последнему неравенству можно придать вид $\dfrac{n_k}{|S_k|} < cq^{-k_0} q^k$, для подходящего натурального k_0 и положительного действительного c.

Доказательство проведем методом индукции по длине пути. Проверим базу индукции, положив в оценке частот $k_0 = d$.

Оценим число путей длины $d + 2$. Для получения путей длины $d + 2$ мы продлеваем пути длины $d + 1$, причем пути, входящие в вершину v (ту самую, из которой не выходит ребро с меткой x) продлеваются не более, чем $2z - 2$ способами, а пути, входящие в другие вершины — не более чем $2z-1$ способами. Поэтому верно неравенство

$$n_{d+2} < n_{d+1}^v (2z - 2) + \sum_{w \in V\Gamma \setminus v} n_{d+1}^w (2z - 1).$$

Значит,

$$n_{d+2} < n_{d+1} \left(\frac{n_{d+1}^v}{n_{d+1}} (2z - 2) + \sum_{w \in V\Gamma \setminus v} \frac{n_{d+1}^w}{n_{d+1}} (2z - 1) \right).$$

Поскольку $d + 1 > d$, то можно использовать формулу (1). Получаем:

$$n_{d+2} < n_{d+1} \left(\varepsilon(2z - 2) + (1 - \varepsilon)(2z - 1) \right).$$

Тогда для относительных частот множества R :

$$f_{d+2} = \frac{n_{d+2}}{|S_{d+2}|} < \frac{n_{d+1} \left(\varepsilon(2z - 2) + (1 - \varepsilon)(2z - 1) \right)}{|S_{d+1}|(2z - 1)} < cq < cq^{-d} q^{d+1} = Cq^{d+1},$$

где $q = 1 - \dfrac{\varepsilon}{(2z - 1)}$. Сделаем теперь шаг индукции.

Рассуждения об оценке путей длины $k + 1$, где $k > k_0$, производятся совершенно аналогично тому, как это было сделано для путей длины $d + 2$, поэтому мы опустим здесь некоторые промежуточные выкладки и рассуждения. Верно неравенство

$$n_{k+1} < n_k^v (2z - 2) + \sum_{w \in V\Gamma \setminus v} n_k^w (2z - 1).$$

Значит,

$$n_{k+1} < n_k \left(\varepsilon(2z - 2) + (1 - \varepsilon)(2z - 1) \right).$$

Проведем оценку относительных частот множества R:

$$f_{k+1} = \frac{n_{k+1}}{|S_{k+1}|} < \frac{n_k \left(\varepsilon(2z - 2) + (1 - \varepsilon)(2z - 1) \right)}{|S_k|(2z - 1)} < Cq^k \left(1 - \frac{\varepsilon}{2z - 1} \right) < Cq^{k+1}.$$

Это и означает, что множество R строго разреженно. □

Замечание 1. Регулярное множество H, автомат для которого связен и X-полон, является сгущенным, так как его префиксное замыкание содержит конус (см. [1]). Значит, полученный результат действительно является критерием строгой разреженности множеств указанного вида.

Замечание 2. Более слабое утверждение о том, что регулярное множество, удовлетворяющее условиям утверждения 1, является разреженным, было опубликовано в статье [8].

Результаты утверждения 1 носят не только абстрактный характер; сформулируем далее пример его практического применения.

В работе [2] показано, что для произвольной подгруппы $H \leq F$ существует единственный с точностью до изоморфизма корневой X-диграф (Γ, v), такой что

(1) Граф Γ является связным и f-диграфом;
(2) Γ является ядром относительно вершины v;
(3) Язык, распознаваемый графом (Γ, v), совпадает с группой H.

Граф (Γ, v) называется подгрупповым графом для H. В дальнейшем будем обозначать подгрупповой граф через $\Gamma(H)$, а его корневую вершину — 1_H.

Следствие 1. *Пусть H — конечно порожденная подгруппа F бесконечного индекса, тогда H является строго разреженным подмножеством F.*

Доказательство. По теореме 8.3 из [2] подгрупповой граф для H является X-полным если и только если H – подгруппа конечного индекса. Следовательно, граф для H не X-полный и по утверждению 1 подгруппа H является строго разреженным подмножеством F. □

5. Конструкции над строго разреженными множествами

В этой части работы будет доказана строгая разреженность некоторых подмножеств свободной группы F. Пусть fA, Af — соответственно левый и правый смежные классы по подгруппе A. Сопряженную с A подгруппу будем записывать в виде $A^f = \{f^{-1}af | a \in A\}$, где f — произвольный неединичный элемент группы F. Оказывается, что если подгруппа A имеет бесконечный индекс в F, то указанные выше множества являются строго разреженными.

Утверждение 2. *В приведенных выше обозначениях множества Af, fA и A^f являются строго разреженными.*

Доказательство. В самом деле, рассмотрим множество Af (или fA) для произвольного элемента f из F. Пусть длина элемента f равна l. Так как при умножении на f в словах из A не происходит изменения длины большей, чем l, то, начиная с $k = l$, ряд для относительных частот легко оценить, применяя соответствующие оценки для исходной подгруппы A.

Строгая разреженность множества A^f показывается аналогично, с учетом того факта, что при сопряжении элемента его длина не может увеличиться или уменьшиться более, чем на $2l$. □

Замечание. В рассуждениях о строгой разреженности Af, fA или A^f нигде не используется групповая структура A и фактически доказано большее: для произвольного строго разреженного множества P множества Pf, fP и P^f также строго разреженны.

Утверждение 3. *Пусть H — конечно порожденная подгруппа бесконечного индекса в F, S_0 — строго разреженное подмножество множества S специальных представителей для подгруппы H. Тогда множество $M = \bigcup\limits_{s \in S_0} Hs$ также является строго разреженным.*

Доказательство. Напомним, что такое множество специальных представителей для подгруппы H. В каждом правом классе смежности по H мы выбираем представитель s, причем из единичного класса H выбираем представитель единицу. Более того, представители выбираем так, что каждый из них имеет минимальную длину в своем классе и вся система представителей является шрайеровой (такой выбор возможен, см., например, [6]). Специальные представители подразделяются на внутренние и внешние. Внутренних представителей конечное число, а именно, их столько, сколько вершин в подгрупповом графе $\Gamma(H)$. Каждому внутреннему представителю соответствует геодезический путь из начальной вершины 1_H в одну из вершин $\Gamma(H)$. Таким образом, каждому внутреннему представителю соответствует также и некоторая вершина $\Gamma(H)$ (см. [7]).

Перейдем теперь к доказательству строгой разреженности $M = \bigcup\limits_{s \in S_0} Hs$. В работе [7] показано, что множество специальных представителей S для подгруппы бесконечного индекса является конечным объединением конусов, каждый из которых начинается в одной из вершин подгруппового графа $\Gamma(H)$. Следовательно, S_0 есть объединение конечного числа строго разреженных подмножеств, лежащих в различных конусах множества S. Обозначим эти подмножества $S_0^i,\ i = 1, \ldots, m$, где $m \leq |V\Gamma(H)|$, тогда $S_0 = \bigcup\limits_{i=1}^{m} S_0^i$ и для множества M верно равенство

$$M = \bigcup_{i=1}^{m} \bigcup_{s \in S_0^i} Hs. \tag{3}$$

Так как конечное объединение строго разреженных множеств также строго разрежено, то для решения задачи достаточно рассмотреть случай, когда S_0 лежит только в одном из конусов, то есть в (3) m равно 1. Пусть $v_0 \in V\Gamma(H)$ — вершина конуса для S_0, s_0 — соответствующий ей внутренний представитель в $S_{in} \subset S$. Специальные представители соответствуют меткам некоторых геодезических путей с началом в 1_H, кроме того, множество S является шрайеровым, следовательно, все пути в расширенном графе $\overline{\Gamma}$, соответствующие элементам из S_0, длина которых больше расстояния между 1_H и s_0, имеют общее начало — геодезический путь p из 1_H в v_0 с меткой s_0.

А их конечные сегменты, начиная с вершины v_0, лежат вне подгруппового графа $\Gamma(H)$. Поэтому в словах из M длина сокращения на стыке слова из H и из S_0 не может быть больше длины пути p, обозначим ее k. Следовательно, по свойству 5) множество M является строго разреженным. □

Утверждение 4. *Пусть H — конечно порожденная подгруппа бесконечного индекса и $H^* = \bigcup\limits_{f \in F} H^f$. Тогда H^* является строго разреженным множеством.*

Доказательство. Пусть S — множество специальных представителей F по H. Тогда $H^* = \bigcup_{f\in F} H^f = \bigcup_{s\in S} H^s$. Зафиксируем в H нильсеновскую базу $H = \langle h_i \mid i \in I,\ |I| < \infty\rangle$ (поскольку H конечно порождена, то число элементов базы конечно). Для доказательства строгой разреженности множества H^* нужно оценить относительные частоты $f_k^{H^*}$ и, следовательно, получить оценку $n_k^{H^*}$ числа элементов длины k во множестве H^*. Так как s имеет минимальную длину в соответствующем правом классе смежности по H, то длина сокращения на стыке h с представителями не может быть более половины элемента нильсеновской базы, на который заканчивается и (или) начинается элемент h. Следовательно, верна формула

$$2|s| + |h| \leq |s^{-1}hs| + 2m, \tag{4}$$

где $m = \max_{i\in I} |h_i|$. Пусть длина элемента $s^{-1}hs$ составляет k, причем $h = l$, а $s = p$. Тогда, согласно (4), имеем соотношение $2p + l \leq k + 2m$.

Как уже говорилось выше, множество специальных представителей S для H является объединением конечного числа конусов, каждый из которых начинается в одной из вершин подгруппового графа $\Gamma(H)$. Пусть число конусов равняется N, тогда для числа элементов длины p во множестве S верна оценка:

$$n_p^S = 2zN(2z-1)^p$$

(иначе говоря, элементов в каждом конусе не более, чем в свободной группе). Пользуясь этим неравенством, перейдем к непосредственной оценке числа элементов длины k во множестве H^* :

$$n_k \leq \sum_{p=0}^{[(k+2m-1)/2]} n_p^S n_{k+2m-2p}^H$$

Для относительных частот множества H^* верно:

$$f_k = \frac{n_k}{|S_k|} \leq N \sum_{p=0}^{[(k+2m-1)/2]} \frac{n_{k+2m-2p}^H\ |S_p||S_{k-2p+2m}|}{|S_{k+2m-2p}||S_k|}$$
$$\leq 2zN(2z-1) \sum_{p=0}^{[(k+2m-1)/2]} \frac{f_{k+2(m-p)}^H}{(2z-1)^{(p+1)}}$$

Последнее неравенство гарантирует нам строгую разреженность H^* — доказательство производится аналогично рассуждениям из свойства 4). □

Продемонстрируем строгую разреженность еще одного множества.

Утверждение 5. *Пусть h — неединичный элемент группы F и h^F — класс сопряженных с h элементов: $h^F = \{f^{-1}hf | f \in F\}$. Тогда h^F является строго разреженным множеством.*

Доказательство. Достаточно решить задачу для случая, когда h — циклически редуцированный элемент, так как если h имеет вид $h = f^{-1}gf$, то $h^F = g^F$.

Пусть $H = C_F(h) =< h_0 >$ — централизатор элемента h в группе F, а S — множество специальных представителей F по H, где $h = h_0^l$ для некоторого $l > 0$. Тогда любой элемент из класса h^F однозначно записывается в виде $s^{-1}hs$. Обозначим длину h_0 через m.

В записи $s^{-1}hs$ сокращения на стыке элемента h с представителями могут происходить только с одной из двух сторон в силу циклической редуцированности h. Для доказательства строгой разреженности класса h^F необходимо оценить асимптотическое поведение относительных частот, и, значит, элементами малой длины можно пренебречь. Поэтому будем рассматривать только такие представители s из множества S, длина которых больше, чем $|h_0|$. В этом случае длина сокращения будет не больше, чем $|h_0|/2$, так как неравенство $|h_0 s| < |s|$ невозможно по причине минимальности s в своем классе смежности. Следовательно, верно неравенство:

$$2|s| + |h| = 2|s| + l|h_0| \leq |h^f| + |h_0|.$$

Пусть далее $|h^f| = k$. Тогда $|s| \leq \dfrac{k - (l-1)m}{2}$.

Тогда $n_k \leq n^S_{\frac{k-(l-1)m}{2}}$.

Поскольку S — это объединение не более чем m конусов (так как у графа для $H = C_F(h) =< h_0 >$ ровно m вершин), то для относительных частот будет верно следующее:

$$f_k \leq \frac{n^S_{\frac{k-(l-1)m}{2}}}{|S_k|} \leq \frac{m|S_{\frac{k-(l-1)m}{2}}|}{|S_k|} \leq \frac{m}{(2z-1)^{\frac{k+m(l-1)}{2}}}.$$

Последнее из неравенств влечет за собой необходимую оценку при параметрах $C = \dfrac{m}{(2z-1)^{\frac{m(l-1)}{2}}}$ и $q = \dfrac{1}{(2z-1)^{\frac{1}{2}}}$, а, значит, и строгую разреженность класса h^F. $\square$

Замечание. В работе [9] было доказано, что двойной класс смежности AfB для конечно порожденных подгрупп бесконечного индекса A и B является разреженным, в том числе и для случая, когда $f = 1$. Кроме того, известно, что обобщенный нормализатор подгруппы $N^*_F(H) = \{f \in F | H \bigcap H^f \neq 1\}$ представляет собой конечное объединение двойных классов смежности по H :

$$N^*_F(H) = \bigcup_{i=1}^{N} H g_i H.$$

Следовательно, обобщенный нормализатор конечно порожденной подгруппы бесконечного индекса является разреженным множеством.

Список литературы

[1] A.V. Borovik, A. G. Myasnikov, V. N. Remeslennikov, *Multiplicative measures on free groups,* International Journal of Algebra and Computation **13** (2003), 705–731.

[2] I. Kapovich, A. Myasnikov, *Stallings foldings and subgroups of free groups,* Journal of Algebra **248** (2002), 608–668.

[3] В.Магнус, А.Каррас, Д.Солитэр, *Комбинаторная теория групп*, М.: Наука, 1974.

[4] I. Kapovich, A. Myasnikov, P. Schupp, V. Shpilrain, *Generic-Case Complexity Decision Problems in Group Theory and Random Walks*, March 27, 2002.

[5] David B.A. Epstein et al., *Word Processing in Groups*, Jones and Bartlett Publishers, 1992.

[6] М.И. Каргаполов, Ю.И. Мерзляков,*Основы теории групп*, М.: Наука, 1977.

[7] A.V. Borovik, A. G. Myasnikov, V. N. Remeslennikov, *Algorithms for Amalgamated Products*, Manchester Center for Pure Mathematics Preprint Series, 2004.

[8] Я.С. Аверина, Е.В. Френкель, *Разреженность регулярных подмножеств свободной группы*, Вестник Омского Университета, 2004, выпуск 4, 16–18.

[9] Я.С. Аверина, Е.В. Френкель, *Разреженность классов смежности по подгруппам свободной группы*, Препринт №00-01, ОмГУ, 2004.

Яна Сергеевна Аверина, Елизавета Владимировна Френкель
Омский Государственный Университет,
пр. Мира 55а,
644077, Омск-077, Россия
E-mail address: ay@hotmail.ru, lizzy01@mail.ru