Aleksandr Aleksandrovich Markov

Комбинаторная характеристика конечных базисоов чистых свободных полугрупп

Matematický časopis, Vol. 19 (1969), No. 2, 158--165

Persistent URL: http://dml.cz/dmlcz/127096

Matematický časopis 19 (1969), No. 2

КОМБИНАТОРНАЯ ХАРАКТЕРИСТИКА КОНЕЧНЫХ БАЗИСОВ ЧИСТЫХ СВОБОДНЫХ ПОЛУГРУПП

АЛЕКСАНДР АЛЕКСАНДРОВИЧ МАРКОВ, Горький (СССР)

1. Начиная с 1953 года, под влиянием проблематики теории кодирования в математике возник серьёзный интерес к строению неприводимых порождающих множеств (базисов) свободных полугрупп. Наряду с задачами, связанными с изучением полугрупп, порожденных базисами с заданными свойствами, большой интерес представляют обратные задачи, состоящие в характеристике базисов свободных полугрупп различных классов. Цель этой статьи — дать комбинаторную характеристику конечных базисов чистых свободных полугрупп.

Пусть $X = \{x_1, \ldots x_n\}$-алфавит, $[X]$ -порождённая им свободная полугруппа с единицей λ. Если $Y \subset [X]$, то $[Y]$ -подполугруппа $[X]$, порождённая множеством слов Y. В дальнейшем будем предполагать, что Y - конечное множество, образующее базис, и полугруппа $[Y]$ свободна, то есть каждый элемент $[Y]$ допускает лишь единственное представление в виде произведения элементов базиса. Если $y \in [X]$, то через $|y|_i$ обозначается число вхождений буквы x_i в слово y, $|y| = \sum_{i=1}^{n} |y|_i$ - длина слова y, $L = \max_{y \in Y} |y|$, $\pi(Y)$ — множество всех различных левых делителей слов из Y, включающее λ и сами слова Y.

Полугруппа $[Y]$ называется чистой справа (слева), если для любого $\alpha \in [X]$ существует такое $\beta \in [X]$, что $\alpha\beta \in [Y]$ ($\beta\alpha \in [Y]$). $[Y]$ называется унитарной справа (слева), если $\alpha\beta \in [Y]$ и $\beta \in [Y]$ ($\alpha \in [Y]$) влечёт $\alpha \in [Y]$ ($\beta \in [Y]$). Полугруппа называется чистой (унитарной), если она чиста (унитарна) как справа, так и слева. Требование одновременного выполнения свободности, чистоты и существования конечного базиса определяет довольно редкий и мало изученный класс унитарных полугрупп П, который, однако, играет важную роль при описании оптимальных кодов, имеющих синхронизационные свойства. Насколько известно автору, единственный опубликованный нетривиальный (то есть отличный от $[X^p]$) пример такой полугруппы принадлежит М. П. Шютценберже [1]. Базис построенной им полугруппы в алфа-

вите $X = \{0, 1\}$ состроит из 9 слов: $S = [01, 000, 100, 110, 111, 001о, 0011, 1010, 1011]$. В [2] Е. Н. Гильберт и Е. Ф. Мур сообщили, что ими найден ряд других примеров, но вновь привели только пример Шютценберже, так как остальные оказались очень громоздкими. Чтобы показать, что мы имеем дело не со слишком уж экзотическим классом полугрупп, в пп. 3 строится бесконечное семейство полугрупп этого класа, включающее, в частности, и полугруппу Шютценберже (см. так же п. 4, где охарактеризован еще один бесконечный подкласс П) В п. 4 виде следствия основного результата (п. 2) мы извлекаем некоторую информацию о базисах полугрупп класса П. В п. 5 содержагся применения предыдущих результатов к теории ориентированных графов. Мы будем считать известным (это легко следует, например, из [3], что $[Y] \in$ П в том и только том случае, если никакое слово в Y не имеет в Y ни левого, ни правоно собственного делителя (несобственные - λ и само слово), и

$$P_Y(z_1, \ldots z_n) = \sum_{y \in Y} z_1^{|y|_1} \ldots z_n^{|y|_n} \equiv 1 \tag{1}$$

при условии

$$\sum_{i=1}^{n} z_i = 1, \quad z_i > 0, \quad i = \overline{1, n}. \tag{2}$$

(P_Y -производящая функция, перечисляющая элементы Y как абелевы слова). Сформулируем теперь наш основной результат:

если $[Y] \in$ П, *то при условии* (2) *имеет место*

$$Q_Y(z_1, \ldots z_n) = \sum_{y \in Y} |y|\, z_1^{|y|_1} \ldots z_n^{|y|_n} \equiv E(Y), \tag{3}$$

где $E(Y)$ *-инвариант базиса, не зависящий от* $z_1, \ldots z_n$.

Соотношения (1) и (3) при условии (2) имеют очевидную теоретико-вероятностную интерпретацию. Стоит подчеркнуть, что доказательство (3) так же основано на вероятностных соображениях. Однако, (1) можно доказать и чисто комбинаторными средствами (аналогично тому, как в [4] доказано неравенство Мак-Миллана), в то время как комбинаторного доказательства (3) автору найти не удалось. Это связано с тем, что утверждение (3) относится к классу полугрупп, для которого мы не имеем сколько-нибудь удовлетворительного конструктивного описания и о котором у нас вообще очень мало информации. Заметим еще, что если в (3) взять $n = 2$ и $z_1 = z_2 = 1/2$, то мы получим

$$\sum_{y \in Y} |y|\, 2^{-|y|} = E(Y), \tag{3'}$$

откуда следует утверждение теоремы 16 из [2] -единственного известного к настоящему времени результата о базисах чистых свободных полугрупп. Наиболее важные сведения о строении свободных унитарных слева бинарных базисов содержатся так же в [2] и легко распространяются на случай произвольного алфавита X. Нам понадобятся следующие три леммы.

Лемма 1. *Если Y -конечный базис чистой слева свободной полугруппы, $\alpha \in \pi(Y)$ и $Y_\alpha = \{\beta \mid \alpha\beta \in Y\}$, то*

(*a*) *$[Y_\alpha]$ чиста слева и свободна;*

(*b*) *если $\alpha \in \pi(Y) \setminus Y$, то $\alpha X \subset \pi(Y)$;*

(*c*) *если $\alpha \in Y$, то $[(Y \setminus \alpha) \cup \alpha X]$ чиста слева и свободна.*

Лемма 2. *Если свободная полугруппа $[Y]$ чиста, то*

(a) *существует множество $U \subset X^{L-2}$ такое, что $Y \cap X^L = XUX$;*

(*b*) *если $Y \neq X$, то $Y \cap X = \Phi$.*

Лемма 3. *При условии* (2) *имеет место*

$Q_{(Y \setminus \alpha) \cup \alpha X} = Q_Y + P_\alpha > Q_Y$.

2. Пусть Y -конечный базис чистой свободной подполугруппы свободной полугруппы $[X]$. Рассмотрим последовательность испытаний с возможными исходами $x_1, x_2, \ldots, x_n$, вероятности которых — $z_1, z_2, \ldots, z_n$ соответственно. Мы определяем рекуррентное событие, наступающее после m -го испытания в том и только том случае, если последовательность исходов $x_{i_1} x_{i_2} \ldots x_{i_m} \in [Y]$. Этому событию соответствует конечная цепь Маркова с множеством состояний $\{Y_\alpha \mid \alpha \in \pi(Y)\}$, начальным состоянием Y_λ с условием $Y_\alpha = Y_\lambda$ при $\alpha \in Y$ и матрицей вероятностей переходов $\| P_{Y_\alpha, Y_\beta} \|$, где $P_{Y_\alpha, Y_\beta} = \sum_i z_i$ с суммированием по всем i, для которых $Y_{\alpha x_i} = Y_\beta$. Например, упомянутому выше базису S соответствует цепь Маркова с матрицей вероятностей переходов

$$\begin{vmatrix} 0 & z_0 & 0 & z_1 & 0 \\ z_1 & 0 & z_0 & 0 & 0 \\ z_0 & 0 & 0 & 0 & z_1 \\ 0 & 0 & z_0 & 0 & z_1 \\ 1 & 0 & 0 & 0 & 0 \end{vmatrix}$$

Теперь $P_Y(z_1, \ldots, z_n)$ есть вероятность возвращения в начальное состояние, а $Q_Y(z_1, \ldots, z_n)$ -математическое ожидание времени возвращения. Пусть $M \subset X^m$. Обозначим через $f(M)$ выражение

(4) $$\sum_{i_1, \ldots, i_n} l_{i_1 \ldots i_n}(M)\, z_1^{i_1} \ldots z_n^{i_n},$$

где $l_{i_1 \ldots i_n}(M)$ -число последовательностей $\alpha \in M$, для которых $|\alpha|_s = i_s$, $s = \overline{1, n}$. Для данной последовательности $\alpha \in X^m$ определим на множестве $\{0, 1, \ldots, m\}$ отношение τ_α: если $p < q$, то при $\alpha = x_{i_1} \ldots x_{i_m}$ $(p, q) \in \tau_\alpha \leftrightarrow (q, p) \in \tau_\alpha \leftrightarrow x_{i_{p+1}} \ldots x_{i_q} \in [Y]$, $(p, p) \in \tau_\alpha$.

Две следующие леммы непосредственно вытекают из определения класса П.

Лемма 4. *Если* $[Y] \in \Pi$, *то* τ_α *есть отношение эквивалентности.*

Пусть $E(Y, \alpha)$ - число классов τ_α - эквивалентности.

Лемма 5. *Если* $[Y] \in \Pi$, $|\alpha_1| \geq L$, $|\alpha_2| \geq L$, *то*

(5) $$E(Y_1 \alpha_1) = E(Y_1 \alpha_2).$$

На основании (5) мы можем обозначить через $E = E(Y)$ не зависящую от α величину $E(Y_1 \alpha)$ при $|\alpha| \geq L$.

Пусть $R_1, \ldots, R_E$ - классы τ_α - эквивалентности, r_i - наименьшее из чисел в R_i $(i = \overline{1, E})$, α_i получается из α отбрасыванием начального отрезка длины r_i. Нетрудно видеть, что $r_i < L$ для всех $i = \overline{1, E}$. Пусть ещё

$$T_{m, \varepsilon} = \left\{ \alpha \mid \alpha \in X^m, \left| \frac{N(\alpha)}{m} - \frac{1}{Q} \right| \leq \varepsilon \right\},$$

где $N(\alpha)$ - число возвращений источника в начальное состояние в процессе порождения им последовательности α. Переформулируя закон больших чисел для числа возвращений в начальное состояние (см. [5], стр. 403), получим

Лемма 6. *Если* $\varepsilon > 0$, *то* $\lim_{m \to \infty} j(T_{m, \varepsilon}) = 1$.

Кроме того, важно отметить, что если $[Y] \in \Pi$, то $N(\alpha_i) = \mathrm{card}(R_i)$ и имеет место

(6) $$\sum_{i=1}^{E} N(\alpha_i) = m + 1.$$

Лемма 7. *Каково бы ни было* $\varepsilon > 0$, *если* m *достаточно велико, то в* $T_{m, \varepsilon}$ *найдётся последовательность* α *такая, что для всех* $j = \overline{1, E}$ *имеет место* $\alpha_j \in T_{m - r_j, \varepsilon}$.

Предположим противное: для любой последовательности $\alpha_j \in T_{m, \varepsilon}$ найдётся j, $1 \leq j \leq E$, такое, что $\alpha_j \notin T_{m - r_j, \varepsilon}$. Рассмотрим тогда множество

$$T'_{m, \varepsilon} = \{\alpha_j \alpha_0 \mid \alpha_0 \alpha_j \in T_{m, \varepsilon}, \alpha_j \notin T_{m - r_j, \varepsilon}\}.$$

При достаточно большом m имеет место

(7) $$T_{m,\varepsilon} \cap T'_{m,\varepsilon} = \Phi.$$

Действительно, пусть $\alpha_j \alpha_0 \in T'_{m,\varepsilon}$. Тогда

$$\left| \frac{N(\alpha_j)}{m - r_j} - \frac{1}{Q} \right| = \varepsilon + \varepsilon' \qquad \text{где } \varepsilon' > 0 .$$

Имеем $\left| \frac{N(\alpha_j\alpha_0)}{m} - \frac{1}{Q} \right| = \left| \varepsilon + \varepsilon' + \frac{N(\alpha_j\alpha_0)}{m} - \frac{N(\alpha_j)}{m - r_j} \right| > \varepsilon$, то есть $\alpha_j \alpha_0 \notin T_{m,\varepsilon}$, если m настолько велико, что $\left| \frac{N(\alpha_j\alpha_0)}{m} - \frac{N(\alpha_i)}{m - r_j} \right| < \varepsilon'$, то есть начиная с некоторого m_0 (7) выполняется. Но $t_{i_2} \ldots_{i_n} (T'_{m,\varepsilon}) \geq$ $\geq \frac{1}{L} t_{i_1} \ldots_{in} (T_{m,\varepsilon})$, так как каждая последовательность $\beta \in T'_{m,\varepsilon}$ получается из некоторой последовательности $\alpha \in T_{m,\varepsilon}$ циклическим сдвигом на $r_j < L$ букв и, следовательно, может получиться не более, чем из L последовательностей множества $T_{m,\varepsilon}$. Отсюда следует, что $f(T'_{m,\varepsilon}) \geq$ $\geq \frac{1}{L} f(T_{m,\varepsilon})$ и используя (7) и лемму 6, получаем противоречие:

$$1 \geq \lim_{m\to\infty} f(T_{m,\varepsilon} \cup T'_{m,\varepsilon}) = \lim_{m\to\infty} f(T_{m,\varepsilon}) + \lim_{m\to\infty} f(T'_{m,\varepsilon}) \geq 1 + \frac{1}{L}$$

Докажем теперь (3). Пусть $\varepsilon > 0$ задано. По лемме 7 выбираем последовательность $\alpha \in T_{m,\varepsilon/2E}$. Из (6)

$$1 = \sum_{i=1}^{E} \frac{N(\alpha_i)}{m+1} = \frac{E}{Q} + \sum_{i=1}^{E} \left(\frac{N(\alpha_i)}{m - r_i} - \frac{1}{Q} \right) + \sum_{i=1}^{E} \left(\frac{N(\alpha_i)}{m} - \frac{N(\alpha_i)}{m - r_i} \right) - \frac{1}{m},$$

и $$\left| 1 - \frac{E}{Q} \right| \leq \left| \sum_{i=1}^{E} \left(\frac{N(\alpha_i)}{m - r_i} - \frac{1}{Q} \right) \right| + \left| \frac{1}{m} + \sum_{i=1}^{E} \frac{r_i N(\alpha_i)}{m(m - r_i)} \right| < \varepsilon,$$

так как, если $m > 2(1+EL)/\varepsilon$, то $\frac{1}{m} \left| 1 + \sum_{i=1}^{E} \frac{r_i N(\alpha_i)}{m - r_i} \right| < \varepsilon/2$,

а $\left| \frac{N(\alpha_i)}{m - r_i} - \frac{1}{Q} \right| < \varepsilon/2E$ для $i = \overline{1, E}$ по выбору α.

Но $\left| 1 - \frac{E}{Q} \right| < \varepsilon$ означает, что $Q(z_1, \ldots, z_n) \equiv E$, Ч. Т. Д.

3. Пусть $k < e < 2k$, $V \subset X^k$ и

(8) $$VX^{e-k} \cap X^{e-k} V = \Phi.$$

Рассмотрим множество слов

$$b\,(V_1 e) = V \cup \{X^e \setminus (VX^{e-k} \cup X^{k-e}V)\},\ \cup X^{e-k}\,VX^{e-k}.$$

Нетрудно показать, что $[b\,(V,\,e)] \in \Pi$ и $E\,(b(V,e)) = e$. В частности, базис полугруппы Шютценберже есть $b\,(\{01\},\,3)$. То, что никакое слово в $b(V,e)$ не является ни левым, ни правым делителем другого слова в $b\,(V,\,e)$, следует из условия (8). Проверим (1) (достаточно сделать это при $z_1 = \ldots = z_n = {}^1/_n$):

$$P\,({}^1/_n,\,\ldots,\,{}^1/_n) = \frac{\operatorname{card}(V)}{n^k} + \frac{n^e - 2\operatorname{card}(V)\,.\,n^{e-k}}{n^e} + \frac{n^{2e-2k}\operatorname{card}(V)}{n^{2e-k}} = 1.$$

Остаётся вычислить $E\,(b\,(v,e)$ (мы, конечно, можем сделать это при $z_1 = z_2 = \ldots = z_n = {}^1/_n$, так как (3) выполняется тождественно):

$$E\,(b(V_1 e)) = Q({}^1/_n,\,\ldots,\,{}^1/_n) = \frac{k.\operatorname{card}(v)}{n^k} + \frac{e(n^e - 2\operatorname{card}\,(v)\,.\,n^{e-k})}{n^e} +$$

$$+ \frac{(2e-k)\,.\,n^{2e-k}\,.\,\operatorname{card}\,(v)n}{n^{2e-k}} = e.$$

Заметим, что $X^s = b\,(\Phi, s)$.

4. Наличие инварианта $E(Y)$ позволяет провести естественную классификацию конечных базисов чистых свободных полугрупп: $\Pi = \bigcup\limits_{n,\,E=1}^{\infty} \Pi_n\,(E)$, полагая $[Y] \in \Pi_n\,[E] \leftrightarrow E(Y) = E$, $\operatorname{card}\,(X) = n$, $Y \in \Pi$. Как следствие тождества (3) мы получаем некоторую информацию о базисах в $\Pi_n\,(E)$. *Если* $[Y] \in \Pi_n\,(E)$, *то для каждого* $i = \overline{1,\,n}$ *слово* $x_i^E \in Y$ и Y *не содержит других слов, в которые одна буква входила бы* E *раз подряд.*

Далее $\Pi_n\,(1) = \{[b(\Phi, 1)]\}$, $\Pi_n\,(2) = \{[b(\Phi,2)]\}$ и первый нетривиальный класс есть $\Pi_n\,(3)$. Он же является и последним, который удалось охарактеризовать точно. Пусть множество $V_1 \subset X^2$. Определим рекурсивно цепочку множеств $D_2(V_1)$, $D_3(V_1), \ldots$, положив $D_2(V_1) = X^2 \setminus V_1$ и для каждого $i > 2$: $D_i(V_1) = D_{i-1}\,(V_1)\,X \cap X^{i-2}\,V_1$. Далее, пусть $V_i = D_i(V_1)\,X \setminus D_{i+1}\,(V_1) \subset X^{i+1}$ для $i = 2,\,3, \ldots$ и $B(V_1) = \bigcup\limits_{i=1}^{\infty} V_i$. Множество $B(V_1)$ конечно в том и только том случае, если для некоторого i имеет место $D_i(V_1) = \Phi$ (а, следовательно, и для всех $j > i$). Полугруппа $[B(V_1)]$ унитарна слева по построению, а унитарность справа вытекает из того, что ни одно из слов V_i не имеет правого делителя в V_1, в то время как из $v \in V_i$ и $v = v_1\,v_2$ с $v_1 \neq \lambda$ следует, что v_2 должно иметь левый делитель в V_1. Таким образом, если цепочка $\{D_i(V_1)\}$ конечна, то $B(V_1)$ - базис полугруппы из $\Pi_n(3)$ ($E = 3$ оче-

видно, так как $x_i^2 \notin V_1$ и значит $X_i^3 \in V_2$) Но используя лемму 1 легко показать, что если $Y \in \Pi_n$ (3), то $Y \subseteq \pi (B(Y \cap X^2))$, а ввиду леммы 3 и того, что $B(V_1) \in \Pi_n$ (3) мы заключаем, что $Y = B(Y \cap X^2)$. Условие конечности цепочки $\{D_i(V_1)\}$ легко сформулировать в терминах графов: если $G(V_1)$ - конечный ориентированный граф с множеством вершин X и множеством рёбер V_1, то цепочка $\{D_i(V_1)\}$ конечна в том и только том случае, когда $G(V_1)$ не содержит ни одного ориентированного цикла. Таким образом,

Π_n (3) $= \{B(V) | V \subset X^2$, $G(V)$ - ациклический граф$\}$. При этом $B(V)$ состоит из множества рёбер $G(V)$ и для $k \geq 3$ $X^k \cap B(V)$ состоит из всех слов вида $x_{i_1} p_{k-2} x_{ik}$, таких, что $p_{k-2} = x_{i_2} \ldots x_{ik-1}$ - ориентированный путь в G и $(x_{i_1}, x_{i_2}) \notin G$ и $(x_{ik-1}, x_{ik}) \notin G$ (отдельная вершина образует путь длины I).

5. Взаимно-однозначное соответствие, установленное между базисами Π_n (3) и конечными ориентированными графами без циклов с n вершинами, позволяет переносить результаты, полученные для базисов этого класса, на графы. Для примера мы сформулируем некоторые следствия тождеств (1) и (3). Пусть G - ориентированный ациклический граф с n вершинами и n рёбрами. Если σ - путь из вершины i в вершину j в графе G, то через $r^+(\sigma)$ мы обозначим полустепень захода вершины i, а через $r^-(\sigma)$ - полустепень исхода вершины j. $|\sigma|$ - длина пути σ, то есть число вершин, через которые он проходит. Тождества (1) и (3) при $z_1 = \ldots = z_n = 1/n$ после несложных преобразований приводят нас к соотношениям (1') и (3'') соответственно, которые тождественно выполняются для любого конечного ациклического ориентированного графа:

$$(1') \qquad \sum_{\sigma \in G} (n - r^+(\sigma))(n - r^-(\sigma)) n^{-|\sigma|} = n^2 - m,$$

$$(3'') \qquad \sum_{\sigma \in G} (n - r^+(\sigma))(n - r^-(\sigma)) |\sigma| n^{-|\sigma|} = n^2.$$

(3'') особенно интересно тем, что выражение в левой части оказывается не зависящим от числа рёбер графа.

6. Как видно, до исчерпывающей характеристики класса П очень далеко и мы сформулируем некоторые дальнейшие проблемы. Во-первых, интересно было бы охарактеризовать следующий класс Π_n (4). Непосредственной проверкой установлено, что Π_2 (4) состоит из 24 неэквивалентных базисов (базисы Y_1 и Y_2 мы считаем эквивалентными, если один из них получается из другого с помощью операций переименования букв и обращения всех слов), но уже не удалось найти компакт-

ного описания этого класса. Можно предположить, что card $(\Pi_n(E)) < \infty$ при любых конечных значениях n и E, но это не доказано. Наконец, интересно было бы распространить (1) и (3) на случай бесконечных базисов. Правда, тогда инвариант E не имеет того комбинаторного смысла, как для конечных базисов, — достаточно рассмотреть в качестве примера базис полугруппы всех двоичных последовательностей, в которые ноль входит чётное число раз:

$$[1, 00, 010, 0110, \ldots, \underbrace{011\ldots10}_{i \text{ раз}}, \ldots].$$

Нетрудно видеть, что для него $\sum_{y \in Y} |y|\ z^{|y|_0}(1-z)^{|y|_1} \equiv 2$,
но 11 не входит в базис.

В заключение пользуюсь случаем поблагодарить Макса Тая за обсуждение вероятностного аспекта этой статьи.

ЛИТЕРАТУРА

[1] Schützenberger M. P., *On an application of semigroups methods to some problems in coding*, JRE Trans. Inform. Theory, *2*, (1956), 47 — 60.
[2] Gilbert E. N., Moore E. F., *Variable - length binary encodings*, Bell System Techn. J., *38*, (1960), 933 — 967.
[3] Schützenberger M. P., Marcus R. S., *Full decodable Code-Word Sets*, JRE Trans. Inform. Theory, *5*, (1963), 12—15.
[4] Марков Ал. А., *Условие полноты для неравномерных кодов*, Проблемы кибернетики, *9*, (1963), 327 — 331.
[5] Феллер В., *Введение в теорию вероятностей и её приложения*, Москва, 1964.

Поступило 28. 1. 1967.

Научно-исследовательский институт прикладной математики и кибернетики при Горьковском Государственном университете им. Н. И. Лобачевского, Горький, СССР

Примечание: После того, как статья была сдана в печать, автору стало известно о работе М. П. Шютценберже „О специальном классе рекуррентных событий", *Annals Math. Statistics. v. 32, 1961, 1201-1213,* в которой другим путем цолучен результат, эквивалентный (3) и показано, что *Card* $(\Pi_n (E)) < \infty$. В настоящее время автору удалось получить обобщение результата п. 4 и охарактеризовать все классы $\pi_n(E)$ в терминах обобщенных ациклических графов.