ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—сентябрь 2007. Серия 1. Том 14, № 3. 67–79

УДК 519.174

ОБ АВТОМОРФИЗМАХ ЦИКЛОВ В n-МЕРНОМ БУЛЕВОМ КУБЕ*)

А. Л. Пережогин

Рассмотрены общие свойства автоморфизмов простых и, в частности, гамильтоновых циклов в n-мерном булевом кубе Q_n. Для некоторого подкласса гамильтоновых циклов в Q_n показано, что существуют гамильтоновы циклы в Q_9 с группой автоморфизмов порядка 32 и не существуют гамильтоновы циклы с группой автоморфизмов большего порядка ни для каких n. Получены новые экспериментальные данные для задачи построения простых циклов в Q_n, в которых любые k последовательных по циклу рёбер имеют различные направления.

Введение

Булевым n-мерным кубом Q_n называется граф, вершинами которого являются двоичные наборы длины n, и две вершины соединены ребром, если соответствующие наборы различаются в одной позиции.

Простому циклу $C = v_0, v_1, \ldots, v_{t-1}, v_t = v_0$ в Q_n поставим в соответствие слово $X = X(C) = x_0\,x_1\,\ldots\,x_{t-1}$ в алфавите $A_n = \{1, 2, \ldots, n\}$, где x_i — номер позиции, в которой различаются наборы v_i и v_{i+1}, $0 \leqslant i \leqslant t-1$. Такое слово назовём переходным словом цикла C.

При любых i и j, $0 \leqslant i \leqslant j \leqslant t-1$, слово

$$Y = x_i\,x_{i+1}\,\ldots\,x_j \tag{1}$$

назовём подсловом слова $X = x_0\,x_1\,\ldots\,x_{t-1}$. Если $i = 0$, то Y называется префиксом слова X, а если $j = t-1$, то Y называется его суффиксом.

Через $S(Y)$ обозначим набор состава слова Y по модулю 2. Иными словами, $S(Y) = (s_1, s_2, \ldots, s_n)$, где $s_m = 0$ $(m = 1, \ldots, n)$, если буква m встречается в Y чётное число раз, и $s_m = 1$ в противном случае.

---

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 05–01–00364).

Если $S(X) = \bar{0} = (0, 0, \ldots, 0)$, то слово X назовём циклическим. Кроме слов вида (1) подсловами циклического слова $X = x_0\, x_1\, \ldots\, x_{t-1}$ являются также слова вида

$$x_j\, x_{j+1}\, \ldots\, x_{t-1}\, x_0\, x_1\, \ldots\, x_i, \tag{2}$$

где $0 \leqslant i < j \leqslant t-1$. Везде ниже как для вершин циклов, так и для букв циклического слова индексы берутся по модулю длины цикла (циклического слова). Так, слово $x_j\, x_{j+1}\, \ldots\, x_{t+i}$ совпадает со словом (2). Очевидно

Утверждение 1. *Слово X в алфавите A_n является переходным словом некоторого простого цикла C в Q_n тогда и только тогда, когда X является циклическим и $S(Y) \neq \bar{0}$ для любого подслова $Y \neq X$.*

Через $\mathrm{supp}(X) = \mathrm{supp}(S(X))$ обозначим носитель набора $S(X)$, т. е. множество букв алфавита A_n, которые встречаются в слове X нечётное число раз. Таким образом, $\mathrm{supp}(X) = \varnothing$ тогда и только тогда, когда $S(X) = \bar{0}$.

Как обычно, простой цикл в Q_n, содержащий все вершины, называется гамильтоновым циклом в Q_n. Гамильтоновы циклы в Q_n часто называют кодами Грея [15]. Классическим примером является двоично отражённый код Грея, имеющий переходное слово T_n, которое строится следующим образом: $T_1 = 1\,1$; если $T_{i-1} = t_0\, t_1\, \ldots\, t_{2^{i-1}-1}$, то

$$T_i = t_0\, t_1\, \ldots\, t_{2^{i-1}-2}\, i\, t_0\, t_1\, \ldots\, t_{2^{i-1}-2}\, i.$$

Известно, что сдвиг куба Q_n на любой двоичный набор v длины n

$$Q_n \oplus v = \{u \oplus v \mid u \in V(Q_n)\},$$

где $\oplus$ — покоординатное сложение по модулю 2, является автоморфизмом графа Q_n. Подгруппу всех таких сдвигов группы автоморфизмов $\mathrm{Aut}(Q_n)$ n-мерного булева куба обозначим через $G(Q_n)$. Подгруппой группы $\mathrm{Aut}(Q_n)$ также является группа перестановок $S_n(Q_n)$ координат вершин куба. Более того, нетрудно видеть, что

$$\mathrm{Aut}(Q_n) = G(Q_n) \leftthreetimes S_n(Q_n),$$

где $\leftthreetimes$ — полупрямое (или нормальное) произведение (см., например, [7]). Тождественный автоморфизм куба обозначим через e.

§ 1. Группы автоморфизмов простых циклов в Q_n

Автоморфизмом простого цикла C в Q_n назовём автоморфизм Q_n, переводящий C в себя. Таким образом, $\mathrm{Aut}(C)$ является подгруппой группы $\mathrm{Aut}(Q_n)$.

Пусть φ — нетривиальный автоморфизм простого цикла $C = v_0, v_1, \ldots, v_{t-1}, v_t = v_0$ в Q_n. Тогда $\varphi(v_0) = v_i$ для некоторого i, $\varphi(v_1)$ совпадает либо с v_{i+1}, либо с v_{i-1}. В первом случае φ назовём прямым автоморфизмом (он сохраняет ориентацию цикла), во втором — обратным. Подгруппу прямых автоморфизмов цикла C обозначим через $\mathrm{Aut}_+(C)$.

Прямой автоморфизм φ простого цикла $C = v_0, v_1, \ldots, v_{t-1}, v_t = v_0$ в Q_n обозначим через φ_i^π, если $\varphi(C) = v_0 \oplus v_i \oplus \pi(C)$, где $\pi \in S_n(Q_n)$. Введём параметр $i(C)$ следующим образом. Если $\mathrm{Aut}_+ C \neq \{e\}$, то $i(C) = \min\{i \,|\, \varphi_i^\pi \in \mathrm{Aut}_+(C),\ i > 0\}$. В противном случае положим $i(C) = |C|$. Заметим, что $i(C)$ делит $|C|$, так как в противном случае найдётся такое натуральное число k, $k > 0$, что $(\varphi_{i(C)}^\pi)^k = \varphi_j^\pi$ для некоторого $j < i(C)$, что противоречит выбору $i(C)$. Пусть $n(C) = |C|/i(C)$.

Лемма 1. *Если C — простой цикл в Q_n, то $\mathrm{Aut}_+(C)$ является циклической группой с порождающим элементом $\varphi_{i(C)}^\pi$, т. е.*

$$\mathrm{Aut}_+(C) = \langle \varphi_{i(C)}^\pi \rangle_{n(C)} \cong Z_{n(C)}.$$

Лемма 2. *Если существует обратный автоморфизм цикла C, то*

$$\mathrm{Aut}(C) \cong Z_2 \leftthreetimes Z_{n(C)}.$$

Доказательство. Пусть φ — обратный автоморфизм цикла C. Очевидно, что $\varphi^2 = e$. Рассмотрим подгруппу $\{e, \varphi\}$ группы $\mathrm{Aut}(C)$. Так как $\mathrm{Aut}_+(C)$ — нормальный делитель группы $\mathrm{Aut}(C)$, $\mathrm{Aut}_+(C) \cap \{e, \varphi\} = e$ и $\mathrm{Aut}_+(C)\{e, \varphi\} = \mathrm{Aut}(C)$, то, используя лемму 1, имеем

$$\mathrm{Aut}(C) = \{e, \varphi\} \leftthreetimes \mathrm{Aut}_+(C) \cong Z_2 \leftthreetimes Z_{n(C)}.$$

Лемма 2 доказана.

Таким образом верна

Теорема 1. *Для любого простого цикла C в Q_n группа автоморфизмов $\mathrm{Aut}(C)$ изоморфна либо циклической группе порядка $n(C)$, либо группе $Z_2 \leftthreetimes Z_{n(C)}$ порядка $2n(C)$.*

Циклическое слово $X = x_0\, x_1\, \ldots\, x_{t-1}$ в алфавите A_n назовём *периодическим порядка k*, если:
1) k делит t;

2) существует такая перестановка $\pi \in S_n$, что $x_{i+t/k} = \pi(x_i)$ при любом i, $0 \leqslant i \leqslant t-1$.

Соответствующую перестановку π обозначим через $\pi(X)$. Таким образом, у периодического порядка k циклического слова длины t длина периода равна t/k.

Если циклическое слово X является периодическим порядка k и не является периодическим ни для какого большего порядка, то слово X назовём *периодическим максимального порядка* k и обозначим через $n(X) = k$. Если X не является периодическим, положим $n(X) = 1$. Заметим, что $\pi^{n(X)} = e$.

Лемма 3. *Если C простой цикл в Q_n с переходным словом $X = X(C)$, то $n(X) = n(C)$.*

Доказательство. По определению переходное слово $X(C)$ простого цикла C длины t в Q_n является периодическим порядка m тогда и только тогда, когда $\varphi^{\pi}_{t/m} \in \mathrm{Aut}_+(C)$. Следовательно, минимальная длина периода слова $X(C)$ равна $i(C)$. Лемма 3 доказана.

Циклическое слово $X = x_0\, x_1\, \ldots\, x_{t-1}$ в алфавите A_n назовём симметричным, если существуют перестановка $\pi \in S_n$ и целое m, $0 \leqslant m \leqslant t-1$, такие, что $x_{i+m} = \pi(x_{t-i})$ при любом i, $0 \leqslant i \leqslant t-1$.

Лемма 4. *У простого цикла C в Q_n имеется обратный автоморфизм тогда и только тогда, когда переходное слово $X(C)$ является симметричным.*

Леммы 3 и 4 показывают, что для исследования группы автоморфизмов простого цикла C в Q_n достаточно исследовать переходное слово $X(C)$ на периодичность и симметрию.

Пример 1. При любом $n \geqslant 3$ в графе Q_n с точностью до изоморфизма существуют единственный цикл длины 4 и два цикла длины 6. Их переходные слова имеют вид:

$$X(C_4) = 1\,2\,1\,2;\; X(C_6^1) = 1\,2\,3\,1\,2\,3;\; X(C_6^2) = 1\,2\,1\,3\,2\,3.$$

Эти слова являются симметричными и периодическими, причём

$$n(C_4) = 4, \quad n(C_6^1) = 6, \quad n(C_6^2) = 2.$$

Пример 2. Пусть B_k — подграф графа Q_{2k+1}, порождённый множеством вершин веса k и $k+1$. Известна (см., например, [19, 9, 13]) проблема: является ли граф B_k гамильтоновым при любом $k \geqslant 1$? В [2] показано, что если C является гамильтоновым циклом в графе B_k, то в слово $X(C)$ все буквы алфавита A_{2k+1} входят одинаковое число раз. Это ограничение выполняется, если строить циклы C с условием $n(C) = 2k+1$. Заметим, что единственные с точностью до изоморфизма гамильтоновы циклы в B_1 и B_2 удовлетворяют этому условию. В [16] с помощью компьютера были найдены периодические периода $2k+1$ симметричные переходные слова гамильтоновых циклов в B_k при всех $k,\ \ 1 \leqslant k \leqslant 15$.

Утверждение 2. *При любых простых p и q, $p \neq q$, в Q_{p+q} имеется такой простой цикл C, что $n(C) = 2pq$.*

Доказательство. Пусть $\{a_1, a_2, \dots, a_p\} = \{1, 2, \dots, p\}$ и $\{b_1, b_2, \dots, b_q\} = \{p+1, p+2, \dots, p+q\}$. Пусть перестановка π в циклическом представлении имеет вид $\pi = [a_1 a_2 \dots a_p][b_1 b_2 \dots b_q]$. Покажем, что слово

$$X = a_1 b_1 \pi(a_1)\pi(b_1)\pi^2(a_1)\pi^2(b_1)\dots\pi^{2pq-1}(a_1)\pi^{2pq-1}(b_1)$$

является переходным словом искомого цикла. Действительно, так как $a_1\pi(a_1)\pi^2(a_1)\dots\pi^{p-1}(a_1) = a_1 a_2 \dots a_p$, $b_1\pi(b_1)\pi^2(b_1)\dots\pi^{q-1}(b_1) = b_1 b_2 \dots b_q$, то $S(X) = \overline{0}$, причём X является симметричным и периодическим словом максимального порядка $2pq$. Поэтому если существует такое подслово Y длины $2i$ слова X, что $S(Y) = \overline{0}$, то $S(a_1 b_1 \pi(a_1)\pi(b_1)\dots\pi^i(a_1)\pi^i(b_1)) = \overline{0}$, то тогда i чётно, $i \equiv 0 \pmod p$ и $i \equiv 0 \pmod q$. Следовательно, $i = 2pq$. Утверждение 2 доказано.

Рассмотрим циклическое представление перестановки $\pi \in S_n$. Перестановку π назовём перестановкой типа $\langle\, \lambda_1, \lambda_2, \dots, \lambda_t \,\rangle$, если в разложении π на циклы имеется в точности λ_i циклов длины i, причём $\lambda_t \neq 0$.

Лемма 5. *Пусть $X = x_0 x_1 \dots x_{m2^k-1}$ — переходное слово простого цикла C в Q_n и $n(X) = 2^k$. Пусть $\pi = \pi(X)$ — перестановка типа $\langle\lambda_1, \lambda_2, \dots, \lambda_t\rangle$. Тогда если $\lambda_i \neq 0$, то i является степенью двойки, причём $t \geqslant 2^{k-1}$.*

Доказательство. Поскольку $\pi^{2^k} = e$, все циклы в циклическом представлении π имеют длину, равную степени 2. Если $t \leqslant 2^{k-2}$, то $\pi^{2^{k-2}} = e$. Следовательно, $x_0 x_1 \dots x_{m2^{k-2}-1} = x_{m2^{k-2}} x_{m2^{k-2}+1} \dots x_{m2^{k-1}-1}$. Но тогда $S(x_0 x_1 \dots x_{m2^{k-1}-1}) = \overline{0}$. Противоречие с утверждением 1. Таким образом, $t \geqslant 2^{k-1}$. Лемма 5 доказана.

Лемма 6. *Пусть $X = x_0 x_1 \dots x_{m2^k-1}$ — переходное слово простого цикла C в Q_n, $n(X) = 2^k$. Пусть $\pi = \pi(X)$ — перестановка типа $\langle\lambda_1, \lambda_2, \dots, \lambda_{2^{k-1}}\rangle$. Тогда в циклическом разложении перестановки π существует такой цикл $[a_1 a_2 \dots a_{2^{k-1}}]$, что если*

$$\{a_1, a_2, \dots, a_{2^{k-1}}\} \cap \operatorname{supp}(x_0 x_1 \dots x_{m-1}) = \{a_{i_1}, a_{i_2}, \dots, a_{i_t}\},$$

то число t нечётно.

Доказательство. Так как $n(X) = 2^k$, то

$$\{a_1, a_2, \dots, a_{2^{k-1}}\} \cap \operatorname{supp}(x_0 x_1 \dots x_{m-1}) = \{a_{i_1}, a_{i_2}, \dots, a_{i_t}\}$$
$$\{a_1, a_2, \dots, a_{2^{k-1}}\} \cap \operatorname{supp}(x_m x_{m+1} \dots x_{2m-1}) = \{\pi(a_{i_1}), \pi(a_{i_2}), \dots, \pi(a_{i_t})\}$$
$$\dots$$
$$\{a_1, a_2, \dots, a_{2^{k-1}}\} \cap \operatorname{supp}(x_{m(2^{k-1}-1)} x_{m(2^{k-1}-1)+1} \dots x_{m2^{k-1}-1}) = \{\pi^{2^{k-1}-1}(a_{i_1}), \pi^{2^{k-1}-1}(a_{i_2}), \dots, \pi^{2^{k-1}-1}(a_{i_t})\}.$$

Но в слове $a_{ij}\ \pi(a_{ij}) \dots \pi^{2^{k-1}-1}(a_{ij})$ при любом $j, 1 \leqslant j \leqslant t$, все буквы из $\{a_1, a_2, \dots, a_{2^{k-1}}\}$ встречаются ровно по 1 разу. Следовательно,

$$\{a_1, a_2, \dots, a_{2^{k-1}}\} \cap \operatorname{supp}(S(x_0 x_1 \dots x_{m2^{k-1}-1})) \neq \varnothing$$

тогда и только тогда, когда t нечётно. Остаётся заметить, что для любого цикла $[b_1 b_2 \dots b_{2^l}]$ в циклическом представлении перестановки π при $l < k-1$ имеем

$$\{b_1, b_2, \dots, b_{2^l}\} \cap \operatorname{supp}(x_0 x_1 \dots x_{m2^{k-1}-1}) = \varnothing.$$

Поскольку $S(x_0 x_1 \dots x_{m2^{k-1}-1}) \neq \overline{0}$, лемма 6 доказана.

Утверждение 3. *Если C — простой цикл в Q_n и $n(C) = 2^k$, то $n \geqslant 2^{k-1} + 1$.*

Доказательство. Пусть $X = X(C)$ и $\pi = \pi(X)$ — перестановка типа $\langle \lambda_1, \lambda_2, \dots, \lambda_t \rangle$. Так как по лемме 5 $t \geqslant 2^{k-1}$, то $n \geqslant 2^{k-1}$. Если $t = 2^{k-1}$, то по лемме 6 в циклическом разложении π имеется не менее двух циклов. Следовательно, $n > 2^{k-1}$. Утверждение 3 доказано.

Утверждение 4. *Если C — простой цикл в Q_n и $n(C) = p^k$, где $p > 2$ и p — простое, то $n \geqslant p^k$.*

Доказательство. Пусть $X = X(C) = x_0 x_1 \dots x_{mp^k-1}$ и $\pi = \pi(X)$ — перестановка типа $\langle \lambda_1, \lambda_2, \dots, \lambda_t \rangle$. Если $\lambda_i \neq 0$, то i является степенью числа p. Если $t \leqslant p^{k-1}$, то $(S(x_0 x_1 \dots x_{2mp^{k-1}-1})) = \overline{0}$. Так как $p > 2$, то имеем противоречие с утверждением 1. Следовательно, $t \geqslant p^k$. Поэтому $n \geqslant p^k$. Утверждение 4 доказано.

§ 2. Автоморфизмы гамильтоновых циклов в Q_n

Поскольку любой гамильтонов цикл H в Q_n имеет длину 2^n и $n(H)$ делит длину H, из утверждения 2 непосредственно следует

Теорема 2. *Если в Q_n имеется гамильтонов цикл H такой, что $n(H) = 2^k$, то $n \geqslant 2^{k-1} + 1$.*

Следствие 1. *Порядок группы автоморфизмов произвольного гамильтонова цикла в Q_n, $n \geqslant 2$, не превосходит $2^{\lfloor \log_2(n-1) \rfloor + 2}$.*

Пример 3. При любом $n \geqslant 2$ переходное слово двоично отраженного кода Грея T_n является симметричным и периодическим максимального порядка 4.

Пример 4. В Q_4 существует 9 классов эквивалентности гамильтоновых циклов [14]. Ровно один класс имеет тривиальную группу автоморфизмов:

$$X_1 = 121312142313 2314,$$

ещё один класс имеет несимметричное переходное слово

$$X_2 = 121321241312 3134, \quad n(X_2) = 2,$$

у остальных классов переходные слова являются симметричными, причём

$$X_3 = 1213141241432124, \quad n(X_3) = 1,$$

$$X_4 = 1213242313424314, \quad n(X_4) = 1,$$

$$X_5 = 1213121421232124, \quad n(X_5) = 2,$$

$$X_6 = 1213124312131243, \quad n(X_6) = 2,$$

$$X_7 = 1213124213121343, \quad n(X_7) = 2,$$

$$X_8 = 1213121412131214, \quad n(X_8) = 4,$$

$$X_9 = 1213212412132124, \quad n(X_9) = 4.$$

Пример 5. В Q_5 существует 237675 классов эквивалентности гамильтоновых циклов [8]. Из них 234543 имеют тривиальную группу автоморфизмов и ровно 3 являются периодическими максимального порядка 8, причём два из них с симметричными переходными словами

$$X_1 = 1215343521254345121534352125 4345,$$

$$X_2 = 1235234534154125123523453415 4125,$$

и один с несимметричным словом

$$X_3 = 1235314543252415123531454325 2415.$$

Утверждение 5. *Если гамильтонов цикл H в Q_n, $n \geqslant 3$, имеет обратный автоморфизм φ, причём $\varphi(H) = v \oplus \pi(H)$, то в двоичном наборе v имеется нечётное число единиц.*

Доказательство. Гамильтонов цикл в Q_n разбивается на два совершенных паросочетания M_1 и M_2. Если v имеет чётное число единиц, то автоморфизм φ n-мерного булева куба переводит M_1 в M_2. Но в [6] доказано, что два эквивалентных совершенных паросочетания в Q_n, $n \geqslant 3$, не могут образовывать гамильтонов цикл. Утверждение 5 доказано.

Следствие 2. *Для любого гамильтонова цикла H в Q_n, $n \geqslant 3$,* $\mathrm{Aut}(H) \cap S_n(Q_n) = e$.

Заметим, что для простых циклов утверждение 5 неверно. Например, цикл $12\ldots n12\ldots n$ состоит из двух изоморфных паросочетаний. Однако результаты, подобные утверждению 5, имеются и для некоторых негамильтоновых циклов. Так, для задачи, рассмотренной в примере 2, в [10] доказано, что два совершенных лексикографических паросочетания в B_k (а они все попарно эквивалентны) не могут образовывать один цикл, являющийся гамильтоновым в B_k.

Пусть $n = 2^{k-1} + 1$, $k \geqslant 2$. Переходное слово $X = x_0\, x_1 \ldots x_{2^n-1}$ гамильтонова цикла в Q_n назовём *граневым*, если выполнены следующие условия:

1) $n(X) = 2^k$;
2) $\pi(X) = [12\ldots n-1][n]$;
3) $x_0\, x_1 \ldots x_{2^{n-k}-2}$ — гамильтонова цепь в некоторой грани размерности $n-k$ в Q_{n-1}, $x_{2^{n-k}-1} = n$.

Заметим, что слово T_3 является граневым в Q_3, а слово X_1 из примера 5 является граневым в Q_5. Ниже будет построено граневое слово в Q_9 и показано, что для больших размерностей булевых кубов граневых слов нет.

Из слова T_5 переименованием букв построим такое слово $Y\,1$, что

$$Y = 3536353735363531353635373536353.$$

Пусть перестановка π в циклическом представлении имеет вид $\pi = [12 \ldots 8][9]$.

Утверждение 6. *Слово $X = Y\,9\,\pi(Y)\,9\,\pi^2(Y)\,9 \ldots \pi^{15}(Y)\,9$ является граневым в Q_9.*

Доказательство. Достаточно показать, что X является переходным словом гамильтонова цикла в Q_9. Пусть $X = x_0\, x_1 \ldots x_{511}$ и существует такое подслово $Z = x_i\, x_{i+1} \ldots x_j$ слова X, что $S(Z) = \overline{0}$. По построению $S(X) = \overline{0}$, т. е. $S(x_{j+1}\, x_{j+2}\, \ldots\, x_{i-1}) = \overline{0}$. Следовательно, без ограничения общности можно полагать, что $|Z| \leqslant |X|/2$. По построению из утверждения 1 следует, что $S(x_{i+32t}\, x_{i+1+32t}\, \ldots\, x_{j+32t}) = \overline{0}$ для любого t, $0 \leqslant t \leqslant 15$. Следовательно, Z можем выбрать так, что $0 \leqslant i \leqslant 31$. Но буква 9 встречается в Z чётное число раз. Поэтому слово Z может иметь только один из следующих четырех видов:

$$Z_0\, 9\, \pi(Y)\, 9\, \pi^2(Z_1), \tag{3}$$

$$Z_0\, 9\, \pi(Y)\, 9\, \pi^2(Y)\, 9\, \pi^3(Y)\, 9\, \pi^4(Z_1), \tag{4}$$

$$Z_0\, 9\, \pi(Y)\, 9\, \pi^2(Y)\, 9\, \ldots\, \pi^5(Y)\, 9\, \pi^6(Z_1), \tag{5}$$

$$Z_0\, 9\, \pi(Y)\, 9\, \pi^2(Y)\, 9\, \ldots\, \pi^7(Y)\, 9\, Z_1, \tag{6}$$

где Z_0 и Z_1 являются суффиксом и префиксом слова Y соответственно либо пустыми словами.

В случае (3) буква $2 \in \mathrm{supp}(\pi(Y))$, но в словах Y и $\pi^2(Y)$ буквы 2 нет. Следовательно, $2 \in \mathrm{supp}(Z_0\, 9\, \pi(Y)\, 9\, \pi^2(Z_1))$. Значит, слово Z не может иметь вид (3).

Аналогично показывается, что в любом слове вида (4) буква 4 встречается нечётное число раз, в словах вида (5) буква 2 встречается нечётное число раз, а в словах вида (6) три буквы 2, 4 и 8 встречаются нечётное число раз. Таким образом, в X нет подслова, отличного от X и от пустого, в котором все буквы встречаются чётное число раз. Утверждение 6 доказано.

Поскольку слово, построенное в утверждении 6, является симметричным, то верно

Следствие 3. *В Q_9 имеется гамильтонов цикл с группой автоморфизмов порядка* 32.

Заметим, что в утверждении 6 в качестве слова Y можно взять любое слово длины 31 в алфавите $\{1, 3, 5, 6, 7\}$, для которого циклическое слово $Y\,1$ удовлетворяет условиям утверждения 1, т. е. является переходным гамильтонова цикла в грани куба Q_9 с фиксированными направлениями 2, 4, 8 и 9.

Более того, если в качестве Y взять такое симметрическое слово, что $Y1$ является переходным словом гамильтонова цикла в грани куба Q_n, $n \geqslant 10$, с фиксированными направлениями 2, 4, 8 и 9 и с перестановкой $\pi = [12\ldots 8][9][10]\ldots[n]$, то слово из утверждения 6 будет переходным словом гамильтонова цикла в Q_n с группой автоморфизмов порядка 32.

Аналогично, слово X_1 из примера 5 порождает переходные слова гамильтоновых циклов в Q_n, $n \geqslant 6$, с группой автоморфизмов порядка 16.

Таким образом, верно

Следствие 4. *При любом* n, $2 \leqslant n \leqslant 16$, *в* Q_n *существует гамильтонов цикл с группой автоморфизмов порядка* $2^{\lfloor \log_2(n-1) \rfloor + 2}$.

Утверждение 7. *При любом* $k \geqslant 7$ *в* $Q_{2^{k-1}+1}$ *не существует гамильтонова цикла с граневым переходным словом.*

Доказательство. Пусть $n = 2^{k-1} + 1$, $k \geqslant 2$ и слово

$$X = X_1\, n\, X_2\, n\, \ldots\, X_{2^{k-1}}\, X_1\, n\, X_2\, n\, \ldots\, X_{2^{k-1}}$$

является граневым в Q_n, причём $X_2 = \pi(X_1)$. Покажем, что при любом i, $1 \leqslant i \leqslant 2^{k-2} - 1$, имеется такая буква, которой нет в словах X_1 и X_{2i+1}, а в слово $X_2\, X_3\, \ldots\, X_{2i}$ она входит нечётное число раз. Действительно, пусть $\mathrm{supp}(X_2\, X_3\, \ldots\, X_{2i}) = \{a_1,\, a_2,\, \ldots,\, a_t\}$ и все буквы из этого множества встречаются в слове X_1. По условию граневого слова X_1 является переходным словом гамильтоновой цепи в некоторой грани куба Q_n. Следовательно, существует такой суффикс U слова X_1, что $\mathrm{supp}(U) = \{a_1,\, a_2,\, \ldots,\, a_t\}$. Поэтому $S(U\, n\, X_2\, n\, X_3\, n\, \ldots\, X_{2i}\, n) = \overline{0}$. Противоречие с утверждением 1. Следовательно, в X_1 нет некоторой буквы из множества $\{a_1,\, a_2,\, \ldots,\, a_t\}$. Аналогично доказывается, что в слове X_{2i+1} нет некоторой буквы из этого множества. Предположим теперь, что

$$\{a_1,\, a_2,\, \ldots,\, a_t\} = \{b_1,\, b_2,\, \ldots,\, b_{t_1}\} \cup \{c_1,\, c_2,\, \ldots,\, c_{t_2}\} \cup \{d_1,\, d_2,\, \ldots,\, d_{t_3}\},$$

где буквы из $\{b_1,\, b_2,\, \ldots,\, b_{t_1}\}$ встречаются в X_{2i+1}, но не входят в слово X_1, буквы из $\{c_1,\, c_2,\, \ldots,\, c_{t_2}\}$ встречаются в X_1, но не входят в слово X_{2i+1}, а буквы из $\{d_1,\, d_2,\, \ldots,\, d_{t_3}\}$ встречаются в обоих словах. Тогда в слове X_{2i+1} существует такой префикс V, что $\mathrm{supp}(V) = \{b_1,\, b_2,\, \ldots,\, b_{t_1}\}$, а в слове X_1 существует такой суффикс U, что $\mathrm{supp}(U) = \{c_1,\, c_2,\, \ldots,\, c_{t_2}\}$ $\cup \{d_1,\, d_2,\, \ldots,\, d_{t_3}\}$. Следовательно, $S(U\, n\, X_2\, n\, X_3\, n\, \ldots\, X_{2i}\, n\, V) = \overline{0}$. Противоречие с утверждением 1. Таким образом, при любом i, $1 \leqslant i \leqslant 2^{k-2} - 1$, существует такая буква

$$a \in \mathrm{supp}(X_2\, X_3\, \ldots\, X_{2i}), \tag{7}$$

которой нет в словах X_1 и X_{2i+1}. По определению граневого слова в X_1 нет $k-1$ буквы. Пусть такими буквами являются $a_1,\, a_2,\, \ldots,\, a_{k-1}$. Тогда при любом i, $2 \leqslant i \leqslant 2^{k-2} - 1$, в слове X_{2i+1} нет букв $\pi^{2i}(a_1)$, $\pi^{2i}(a_2)$, …, $\pi^{2i}(a_{k-1})$. Но при любом j, $1 \leqslant j \leqslant k-1$, в слове $\pi^2(a_j)\, \pi^4(a_j)\, \ldots,$ $\pi^{2^{k-1}-2}(a_j)$ буквы a_j нет и каждая буква из множества $\{a_1,\, a_2,\, \ldots,\, a_{k-1}\} \backslash$

$\{a_j\}$ встречается в этом слове не более одного раза. Следовательно, для выполнения условия (7) необходимо, чтобы выполнялось неравенство

$$2^{k-2} - 1 \leqslant (k-2)(k-1).$$

Это неравенство верно только при $k \leqslant 6$. Утверждение 7 доказано.

Заметим, что небольшим перебором можно показать, что уже при $k = 5$ в Q_{17} нет гамильтонова цикла с граневым переходным словом.

§ 3. Приложение к задаче о $\langle m, n\rangle$-циклах

Пример 2 из § 1 показывает, что поиск циклов с заданными свойствами в Q_n иногда удобно вести в классе периодических слов, что даёт возможность находить решение для бóльших размерностей булева куба. Ниже приводятся полученные с помощью компьютерных вычислений новые оценки в задаче построения простых циклов в Q_n, в которых любые k последовательных по циклу рёбер имеют различные направления.

Простой цикл C длины l в Q_n назовём $\langle m, n\rangle$-циклом, а его переходное слово X назовём $\langle m, n\rangle$-словом, если в любом подслове длины m слова X все буквы различны.

В [1, 2, 11] рассматривалась задача нахождения максимального $m = m(n)$ при фиксированном n такого, что существует $\langle m, n\rangle$-слово длины $l = 2^n$. В [11] получена следующая оценка

$$m(n) \geqslant \lfloor n - 2{,}001 \log_2 n \rfloor.$$

В этой же статье приводятся экспериментальные результаты вычисления $m(n)$ при малых значениях n и неравенства $m(8) \geqslant 5$ и $m(9) \geqslant 6$. Также дана конструкция $\langle 8, 10\rangle$-слова длины 2^{10}.

В классе периодических порядка 8 переходных слов гамильтоновых циклов в Q_8 с использованием компьютера были найдены несколько $\langle 6, 8\rangle$-слов. В частности, если $\pi = [1425][3][6][7][8]$ и

$$X = 12345678345672345178263574813276,$$

то слово $X\,\pi(X)\,\pi^2(X)\,\ldots\,\pi^7(X)$ является $\langle 6, 8\rangle$-словом. Кроме того, было установлено, что среди периодических порядка 16 переходных слов гамильтоновых циклов в Q_9 не существует $\langle 7, 9\rangle$-слов.

В [4, 5, 3] рассматривалась задача нахождения $\langle m, n\rangle$-слова максимальной длины $l = l(m, n)$ как функции от m и n. Лучшая известная оценка получена в [5, 3] и имеет вид

$$l(m, n) \geqslant m2^{n - \lceil m/2 \rceil}.$$

Приведём таблицу нижних оценок для $l(m, n)$ при $m = n - 1$:

n	3	4	5	6	7	8	9	10
$l(n-1,n)$	8^*	12^*	32^*	40^*	100^*	200	288	576

Звёздочкой помечены точные значения. Заметим, что все $\langle m,n\rangle$-циклы длины $l(n-1,n)$ при $n \leqslant 7$ являются периодическими порядка 4. Установлено, что в классе периодических порядка 4 $\langle 7,8\rangle$-слов указанная в таблице оценка точна. Например, слово $X\,\pi(X)\,\pi^2(X)\,\pi^3(X)$, где $X = 12345678234567128456732845671234865723486172345687$ и

$$\pi = [1][23][4][56][7][8],$$

является периодическим порядка 4 $\langle 7,8\rangle$-словом длины 200.

С помощью компьютерных вычислений найдены периодические порядка 8 слова, усиливающие ранее известные оценки $l(n-1,n)$ для $n=9$ и $n=10$ до значений, указанных в таблице.

В заключение заметим, что хотя доля гамильтоновых циклов в Q_n с нетривиальной группой автоморфизмов при больших n мала, многие известные конструкции строят периодические гамильтоновы циклы. В этой связи интересным является следующий вопрос.

Верно ли, что для любого k существует такое $n = n(k)$, что в Q_n найдётся гамильтонов цикл с группой автоморфизмов порядка 2^k?

ЛИТЕРАТУРА

1. **Евдокимов А. А.** О нумерации подмножеств конечного множества // Методы дискретного анализа в решении комбинаторных задач: Сб. науч. тр. Вып. 34. Новосибирск: Ин-т математики СО АН СССР, 1980. С. 8–26.
2. **Евдокимов А. А., Пережогин А. Л.** Минимальные нумерации подмножеств конечного множества и проблема гамильтоновости графа средних слоев гиперкуба // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 4. С. 6–12.
3. **Зантен А. Я., ван.** Сохраняющие расстояния циклические коды на линейном базисе // Дискрет. анализ и исслед. операций. Сер. 1. 1998. Т. 5, № 4. С. 38–44.
4. **Пережогин А. Л.** О локально изометрическом кодировании натуральных чисел // Дискрет. анализ и исслед. операций. Сер. 1. 1996. Т. 3, № 4. С. 69–76.
5. **Пережогин А. Л.** О циклических $\langle m,n\rangle$-нумерациях // Дискрет. анализ и исслед. операций. Сер. 1. 1998. Т. 5, № 4. С. 61–70.
6. **Пережогин А. Л., Потапов В. Н.** О совершенных паросочетаниях в двоичном кубе // Дискретные модели в теории управляющих систем: VII Международная конференция (Покровское, 4–6 марта 2006 г.). Труды. М.: МАКС Пресс, 2006. С. 272–277.

7. **Холл М.** Теория групп. М.: Изд-во иностранной литературы, 1962.

8. **Dejter I. J., Delgado A. A.** Classes of Hamilton cycles in the 5-cube // J. Combin. Math. and Combin. Computing. To appear.

9. **Duffus D. A., Kierstead H. A., Snevily H. S.** An explicit 1-factorization in the middle of the Boolean lattice // J. Combin. Theory. Ser. A. 1994. V. 65, N 2. P. 334–342.

10. **Duffus D., Sands B., Woodrow R.** Lexicographic matchings cannot form Hamiltonian cycles // Order. 1988. V. 5, N 2. P. 149–161.

11. **Goddyn L., Gvozdjak P.** Binary Gray codes with long bit runs // The Electronic J. Combinatorics. 2003. 10. ♯R27.

12. **Goddyn L., Lawrence G. M., Nemeth E.** Gray codes with optimized run lengths // Utilitas Mathematica. 1988. V. 34. P. 179–192.

13. **Kierstead H. A., Trotter W. T.** Explicit matchings in the middle levels of the Boolean lattice // Order. 1988. V. 5, N 2. P. 163–171.

14. **Kreweras G.** Some remarks about Hamiltonian circuits and cycles on hypercubes // Bull. Inst. Comb. Appl. 1994. V. 12. P. 19–22.

15. **Savage C. D.** A survey of combinatorial Gray codes // SIAM Rev. 1997. V. 39, N 4. P. 605–629.

16. **Savage C. D., Shields I.** A Hamilton path heuristic with applications to the middle two levels problem // Congressus Numerantium. 1999. V. 140. P. 161–178.

17. **Savage C. D., Winkler P.** Monotone Gray codes and the middle two levels problem // J. Combinatorial Theory. Ser. A. 1995. V. 70, N 2. P. 230–248.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск,
Россия.
E-mail: pereal@math.nsc.ru

Статья поступила
1 марта 2007 г.