

О ДИСТАНЦИОННЫХ КОДАХ ГРЕЯ *)

И. С. БЫКОВ^{1,a}, А. Л. Пережогин^{1,2,b}

¹Новосибирский гос. университет,
ул. Пирогова, 2, 630090 Новосибирск, Россия

²Институт математики им. С. Л. Соболева СО РАН,
пр. Акад. Коптюга, 4, 630090 Новосибирск, Россия

E-mail: ^apatrick.no10@gmail.com, ^bpereal@math.nsc.ru

Аннотация. Кодом Грея размерности n называется циклическая последовательность всех бинарных слов длины n такая, что два соседних слова отличаются ровно в одном символе. Назовём n -мерный код Грея *дистанционным кодом*, если расстояние Хэмминга между словами, находящимися в коде на расстоянии k , равно d . Свойство дистанционности обобщает известное понятие локальной равномерности кодов Грея. Доказано, что не существует дистанционных кодов Грея с параметром $d = 1$ при $k > 1$. Приведены примеры конструкций для построения дистанционных кодов Грея. Для одной бесконечной серии наборов параметров доказано, что дистанционных кодов Грея не существует. Табл. 5, библиогр. 9.

Ключевые слова: n -мерный куб, гамильтонов цикл, код Грея, равномерный код Грея, антиподальный код Грея.

Введение

Код Грея размерности n — это циклическая последовательность, состоящая из всех 2^n бинарных слов длины n , такая, что два соседних слова отличаются ровно в одном символе. Коду Грея размерности n соответствует гамильтонов цикл в графе n -мерного гиперкуба Q_n . Каждое ребро (u, v) в графе Q_n имеет *направление* $i \in \{1, \dots, n\}$ — номер позиции, в которой отличаются слова u и v . *Переходная последовательность* пути v_1, v_2, \dots, v_{m+1} в Q_n — это слово $T = (\tau_1, \tau_2, \dots, \tau_m)$ над алфавитом $\{1, 2, \dots, n\}$ такое, что τ_i — направление ребра (v_i, v_{i+1}) (в случае, если путь замкнутый, считаем, что T — циклическое слово). Необходимое и достаточное условие того, что переходная последовательность является переходной последовательностью гамильтонова цикла (кода Грея) хорошо известно и приводится, например, в [3].

*) Работа второго автора выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 14-01-00507).

Для произвольной переходной последовательности T можно определить набор чётности $S(T) = (S_1(T), S_2(T), \dots, S_n(T))$, где $S_i(T) = 0$ при $1 \leq i \leq n$, если буква i встречается в T чётное число раз, и $S_i(T) = 1$ в противном случае. Тогда $\text{supp}(S(T))$ — множество букв, встречающихся нечётное число раз в T . Нетрудно видеть, что если T — переходная последовательность пути v_1, v_2, \dots, v_m в Q_n , то $|\text{supp}(S(T))| = d(v_1, v_m)$ (здесь и далее d — расстояние Хэмминга).

Коды Грея имеют многочисленные практические применения [9]. При этом возникают вопросы о существовании и построении кодов Грея, обладающих заданными свойствами. Одним из таких свойств является локальная равномерность переходной последовательности кода, которая обеспечивает равномерное изнашивание контактов в реальных устройствах, использующих эти коды [6]. Ранее рассматривались следующие параметры равномерности.

Пусть $l_1(C)$ — максимальное число такое, что в каждом подслове длины $l_1(C)$ переходной последовательности кода C все буквы различны. Наибольшее значение, которое параметр $l_1(C)$ принимает на множестве всех n -мерных кодов Грея, обозначим через $l_1(n)$. Нижние оценки для $l_1(n)$ приведены в табл. 1 (звёздочкой отмечены точные значения $l_1(n)$) [3, 5]. В [2] получена первая нетривиальная нижняя оценка $l_1(n) \geq \frac{n}{2}$. Много позднее в [5] с помощью потоковой конструкции была получена наилучшая известная оценка:

$$l_1(n) \geq n - \lceil 2.001 \log n \rceil.$$

Верхняя оценка для параметра $l_1(n)$, отличная от тривиальной, неизвестна. Даже в частном случае задача отыскания $l_1(8)$ остаётся открытой и приводится в качестве нерешённой исследовательской задачи в [8]. Так как в [3] показано, что $l_1(8) \geq 6$, для её решения остаётся отнять единицу от тривиальной верхней оценки.

Т а б л и ц а 1

Нижние оценки для $l_1(n)$

n	2	3	4	5	6	7	8	9	10	11	12	13	14
$l_1(n) \geq$	2*	2*	2*	4*	4*	5*	6	6	8	8	8	9	9

Пусть $l_2(C)$ — минимальное число такое, что в каждом подслове длины $l_2(C)$ переходной последовательности кода C встречаются все буквы из алфавита $\{1, 2, \dots, n\}$. Наименьшее значение, которое параметр $l_2(C)$ принимает на множестве всех n -мерных кодов Грея, обозначим

через $l_2(n)$. Верхние оценки для $l_2(n)$ приведены в табл. 2 (звёздочкой отмечены точные значения $l_2(n)$) [1]. Для $l_2(n)$ следующие оценки являются наилучшими:

$$n + 1 \leq l_2(n) \leq n + 3 \lfloor \log n \rfloor;$$

верхняя оценка получена в [1], нижняя оценка тривиальна.

Т а б л и ц а 2

Верхние оценки для $l_2(n)$

n	2	3	4	5	6	7	8	9	10	11	12	13	14
$l_2(n) \leq$	2*	4*	6*	7*	8	9	14	14	16	16	18	18	20

Другим возможным свойством кода Грея является антиподальность. Код Грея размерности n называется (n, t) -антиподальным, если противоположные двоичные слова находятся на расстоянии t в коде. Антиподальные коды Грея изучались в [4, 7]. В частности, в [4] показано, что для любого чётного n существует $(n, 2^{n-1})$ -антиподальный код Грея.

Рассмотрим класс кодов Грея со свойством, в некотором смысле обобщающим понятие равномерности и антиподальности. Назовём n -мерный код $\langle d, k \rangle_n$ -дистанционным кодом Грея, если расстояние Хэмминга между словами, находящимися в коде на расстоянии k , равно d . Далее для краткости такой код будем называть $\langle d, k \rangle_n$ -кодом Грея. Связь между дистанционными и равномерными кодами Грея устанавливают следующие утверждения.

Утверждение 1. Код C является $\langle d, d \rangle_n$ -кодом тогда и только тогда, когда $l_1(C) \geq d$. В частности, код C является $\langle n-1, n-1 \rangle_n$ -кодом тогда и только тогда, когда $l_1(C) = n-1$.

ДОКАЗАТЕЛЬСТВО. Пусть C — $\langle d, d \rangle_n$ -код. Тогда для любого подслова T длины d его переходной последовательности имеет место равенство $|\text{supp}(S(T))| = d$. Отсюда все буквы в подслове переходной последовательности длины d (и меньше) различны. Утверждение 1 доказано.

Утверждение 2. Если для кода C верно равенство $l_2(C) = n+1$, то C является $\langle n-1, n+1 \rangle_n$ -кодом.

ДОКАЗАТЕЛЬСТВО. Пусть $l_2(C) = n+1$. Тогда в любом подслове T длины $n+1$ переходной последовательности кода C некоторая буква содержится дважды, а остальные — по одному разу. Это означает, что $|\text{supp}(S(T))| = n-1$. Утверждение 2 доказано.

В табл. 3 приведены все наборы значений параметров $1 < d < 5$ и k , для которых существует $\langle d, k \rangle_5$ -код.

Т а б л и ц а 3

 $\langle d, k \rangle_5$ -Коды Грея

n	d	k	Пример переходной последовательности кода
5	2	2	(1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5)
5	2	4	(1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5)
5	2	6	(1,2,1,3,1,2,4,2,1,3,1,2,1,3,5,2,1,2,3,1,2,1,4,3,2,3,1,2,3,2,5,3)
5	2	8	(1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5)
5	2	10	(1,2,1,3,1,2,1,4,1,3,2,5,1,3,4,2,1,4,1,3,1,4,1,2,1,3,4,5,1,3,2,4)
5	2	12	(1,2,1,3,1,2,1,4,1,2,1,3,1,5,1,3,1,2,1,4,1,2,1,3,1,2,1,4,1,5,1,4)
5	2	14	(1,2,1,3,1,2,1,4,1,2,1,3,1,2,5,2,1,4,1,2,1,3,1,2,1,4,1,2,1,3,5,4)
5	2	16	(1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5)
5	3	3	(1,2,3,1,2,4,3,1,5,3,1,4,2,1,4,3,5,1,4,5,1,2,3,5,4,2,1,5,3,2,4,5)
5	3	5	(1,2,1,3,1,4,5,1,2,1,4,3,4,5,2,5,1,4,1,3,1,2,5,1,4,1,2,3,2,5,4,5)
5	3	7	(1,2,1,3,1,2,4,1,4,5,4,2,4,1,4,5,1,3,1,5,1,2,5,1,5,3,4,3,2,1,2,5)
5	3	9	(1,2,1,3,1,2,1,4,1,5,2,5,3,2,5,4,3,2,1,2,4,2,5,3,2,5,2,1,4,1,2,5)
5	3	11	(1,2,1,3,1,2,1,4,1,2,1,3,5,1,5,2,5,3,2,1,2,4,2,1,2,3,2,1,2,4,5,4)
5	3	13	(1,2,1,3,1,2,1,4,1,2,1,3,1,5,1,2,5,1,5,3,2,1,2,4,2,1,2,3,2,1,2,5)
5	3	15	(1,2,1,3,1,2,1,4,1,2,1,3,2,1,2,5,2,1,2,3,2,1,2,4,2,1,2,3,1,2,1,5)
5	4	4	(1,2,3,4,1,2,3,5,1,4,3,2,1,4,3,5,1,2,3,4,1,2,3,5,1,4,3,2,1,4,3,5)
5	4	8	(1,2,1,3,2,1,2,4,1,2,1,3,2,1,2,5,1,2,1,3,2,1,2,4,1,2,1,3,2,1,2,5)
5	4	12	(1,2,1,3,1,2,4,3,1,2,1,3,1,2,5,3,1,2,1,3,1,2,4,3,1,2,1,3,1,2,5,3)
5	4	14	(1,2,1,3,1,2,1,4,1,3,1,2,1,3,1,5,1,2,1,3,1,2,1,4,1,3,1,2,1,3,1,5)
5	4	16	(1,2,1,3,1,2,1,4,1,2,1,3,1,5,3,1,2,1,3,5,1,5,2,4,1,2,3,2,1,2,3,5)

1. Свойства дистанционных кодов Грея

Из определения дистанционного кода и двудольности Q_n следует

Утверждение 3. Если $\langle d, k \rangle_n$ -код Грея существует, то он является $\langle d, 2^n - k \rangle_n$ -кодом Грея, при этом

- 1) $d \leq \min(k, 2^n - k)$;
- 2) d и k одной чётности.

В дальнейших рассуждениях будем подразумевать, что необходимые условия существования $\langle d, k \rangle_n$ -кода Грея из утверждения 3 выполнены, а именно d и k одной чётности и $d \leq \min(k, 2^n - k)$. Для дистанционных кодов Грея при $d = 1$ и $d = n$ имеют место утверждения 4 и 5 (здесь и далее операции в индексах выполняются по модулю 2^n).

Утверждение 4. При $1 < k < 2^n - 1$ не существует $\langle 1, k \rangle_n$ -кода Грея.

ДОКАЗАТЕЛЬСТВО. Пусть C — $\langle 1, k \rangle_n$ -код Грея. Рассмотрим подслово $T = \tau_{j+1}, \tau_{j+2}, \dots, \tau_{j+k-1}$ в переходной последовательности кода C . Без ограничения общности положим $\text{supp}(S(\tau_j T)) = \{a\}$. Тогда $\text{supp}(S(T)) = \{a, b\}$. Поскольку C есть $\langle 1, k \rangle_n$ -код Грея, имеем $\tau_{j+k} = a$ или $\tau_{j+k} = b$. При $\tau_{j+k} = b$ получаем $\text{supp}(S(\tau_j T \tau_{j+k})) = \emptyset$, что противоречит тому, что C — код Грея. Значит, $\tau_j = \tau_{j+k} = a$. Продолжив, получим $\tau_j = \tau_{j+k} = \tau_{j+2k} = \tau_{j+3k} = \dots$. Двигаясь по переходной последовательности с шагом k , целиком замостим её элементом a , так как k нечётное; противоречие. Следовательно, $\langle 1, k \rangle_n$ -кода Грея не существует. Утверждение 4 доказано.

Этот результат можно интерпретировать в терминах теории графов. Граф-циркулянт G_n^{1, r_1, \dots, r_t} — это цикл длины n , в котором проведены дополнительные рёбра: две вершины соединяются ребром, если расстояние между ними по циклу равно r_i . Заметим, что $\langle 1, k \rangle_n$ -коду Грея соответствует гамильтонов цикл в n -мерном гиперкубе $v_0, v_1, \dots, v_{2^n-1}$, причём вершины v_i и v_{i+k} смежны для любого $0 \leq i \leq 2^n - 1$. Такой цикл образует граф $G_{2^n}^{1, k}$. Тем самым из утверждения 4 вытекает

Следствие 1. Для любого $1 < k < 2^n$ граф $G_{2^n}^{1, k}$ не является подграфом графа Q_n .

Утверждение 5. $\langle n, k \rangle_n$ -Код Грея существует тогда и только тогда, когда n чётно и $k = 2^{n-1}$.

ДОКАЗАТЕЛЬСТВО. Пусть $v_0, v_1, \dots, v_{2^n-1}$ — $\langle n, k \rangle_n$ -код Грея. Тогда $v_i = \bar{v}_{i+k} = \bar{v}_{i-k}$ для любого i . Значит, $i + k \equiv i - k \pmod{2^n}$, что возможно тогда и только тогда, когда $k = 2^{n-1}$, а следовательно, n чётно по утверждению 3. В этом случае $(n, 2^{n-1})$ -антиподальный код Грея является искомым дистанционным кодом Грея. Утверждение 5 доказано.

Следствие 2. При чётном n существует $\langle n - 1, 2^{n-1} - 1 \rangle_n$ -код Грея.

2. Построение дистанционных кодов Грея

Приведём несколько способов построения дистанционных кодов Грея.

Утверждение 6. Пусть $\tau_0, \tau_1, \dots, \tau_{2^n-1}$ — переходная последовательность $\langle d, k \rangle_n$ -кода Грея. Если существует позиция i такая, что $\tau_i = a$ и в каждом из подслов

$$\begin{aligned} T_0 &= \tau_{i-k+1}, \tau_{i-k+2}, \dots, \tau_{i-1}, \tau_i, \\ T_1 &= \tau_{i-k+2}, \tau_{i-k+3}, \dots, \tau_i, \tau_{i+1}, \\ &\dots \end{aligned}$$

$$\begin{aligned} T_{k-2} &= \tau_{i-1}, \tau_i, \dots, \tau_{i+k-3}, \tau_{i+k-2}, \\ T_{k-1} &= \tau_i, \tau_{i+1}, \dots, \tau_{i+k-2}, \tau_{i+k-1}, \end{aligned}$$

буква a содержится нечетное число раз, то существует $\langle d, k \rangle_{n+1}$ -код Грея.

ДОКАЗАТЕЛЬСТВО. Легко убедиться, что последовательность

$$\tau_0, \tau_1, \dots, \tau_{i-1}, (n+1), \tau_{i+1}, \dots, \tau_{2^n-1}, \tau_0, \tau_1, \dots, \tau_{i-1}, (n+1), \tau_{i+1}, \dots, \tau_{2^n-1}$$

является переходной последовательностью $(n+1)$ -мерного кода Грея. Покажем, что этот код Грея является $\langle d, k \rangle_{n+1}$ -кодом. Рассмотрим подслово $T = \tau_j, \tau_{j+1}, \dots, \tau_{j+k-1}$ длины k полученной переходной последовательности. Если T не содержит буквы $(n+1)$, то $|\text{supp}(S(T))| = d$ в силу того, что T — подслово переходной последовательности исходного $\langle d, k \rangle_n$ -кода.

В противном случае, если подслово T содержит букву $(n+1)$, положим

$$T' = \tau_j, \tau_{j+1}, \dots, \tau_{i-1}, (n+1), \tau_{i+1}, \dots, \tau_{j+k-1}.$$

Заметим, что для всех $1 \leq i \leq n+1$, кроме $i = a$ и $i = n+1$, выполнено $S_i(T) = S_i(T')$. Для $i = a$ и $i = n+1$ имеем

$$S_a(T) = S_{n+1}(T') = 1, \quad S_{n+1}(T) = S_a(T') = 0,$$

откуда $|\text{supp}(S(T))| = |\text{supp}(S(T'))| = d$. Значит, построенная переходная последовательность является переходной последовательностью $\langle d, k \rangle_{n+1}$ -кода. Утверждение 6 доказано.

Следствие 3. Если в каждом подслове длины k переходной последовательности $\langle d, k \rangle_n$ -кода некоторая буква содержится нечётное число раз, то существует $\langle d, k \rangle_{n+1}$ -код Грея.

Заметим, что n -мерный двоично-отражённый код Грея удовлетворяет условию следствия 3 при следующих значениях d и k : он является $\langle 2, 2^t \rangle_n$ -кодом и $\langle 2, 2^n - 2^t \rangle_n$ -кодом при $1 \leq t \leq n-1$.

Следствие 4. Если в переходной последовательности $\langle d, k \rangle_n$ -кода существует вхождение некоторой буквы такое, что расстояние до ближайшего вхождения этой же буквы в переходной последовательности не меньше k , то существует $\langle d, k \rangle_{n+1}$ -код Грея.

Код Грея назовём *разделимым*, если в переходной последовательности кода некоторая буква встречается ровно два раза. Нетрудно видеть, что следствие 4 можно применять к разделимым $\langle d, k \rangle_n$ -кодам, получая $\langle d, k \rangle_{n+1}$ -коды (при $1 \leq k \leq 2^{n-1}$).

Другой класс кодов, к которым можно применять следствие 4, — это равномерные коды с высоким значением $l_1(C)$. Пусть для кода C выполнено $l_1(C) = d$, тогда C — $\langle d, d \rangle_n$ -код по утверждению 1. В переходной последовательности такого кода одинаковые буквы находятся друг от друга на расстоянии по крайней мере d .

Утверждение 7. Если существует (разделимый) $\langle d, k \rangle_n$ -код Грея, то существует (разделимый) $\langle d', 2k \rangle_{n+1}$ -код Грея, где

$$d' = \begin{cases} d, & \text{если } k \text{ чётно,} \\ d + 1, & \text{если } k \text{ нечётно.} \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Пусть $\tau_0, \tau_1, \tau_2, \dots, \tau_{2^n-1}$ — переходная последовательность $\langle d, k \rangle_n$ -кода Грея. Тогда легко проверить, что $\tau_0, (n+1), \tau_1, (n+1), \tau_2, (n+1), \dots, \tau_{2^n-1}, (n+1)$ — переходная последовательность $\langle d', 2k \rangle_{n+1}$ -кода Грея. При этом свойство делимости у обоих кодов имеется или отсутствует одновременно. Утверждение 7 доказано.

Утверждение 7 предоставляет рекурсивную конструкцию построения дистанционных кодов Грея.

Теорема 1. Следующие дистанционные коды Грея существуют:

- 1) $\langle 2, 2^k - 2^t \rangle_n$ при $t < k \leq n$;
- 2) $\langle d, 2^{t+d-1} \rangle_n$ при чётном d и $n \geq d + t$;
- 3) $\langle d, 2^{t+d-1} - 2^t \rangle_n$ при чётном d и $n \geq d + t$;
- 4) $\langle d, 2^t d \rangle_n$ при чётном $d \leq l_1(n - t)$;
- 5) $\langle d + 1, 2^t d \rangle_n$ при нечётном $d \leq l_1(n - t)$.

ДОКАЗАТЕЛЬСТВО. 1) Двоично-отражённый код Грея размерности k является $\langle 2, 2^k - 2^t \rangle_k$ -кодом. Заметим, что этот код делимый. По следствию 3 существует $\langle 2, 2^k - 2^t \rangle_{k+1}$ -код (делимость кода сохраняется). Теперь по следствию 4 можем увеличивать размерность кода с сохранением расстояний.

2) По утверждению 5 при чётном d существует $\langle d, 2^{d-1} \rangle_d$ -код. Заметим, что этот код делимый. Применяя к нему t раз утверждение 7, получаем $\langle d, 2^{t+d-1} \rangle_{d+t}$ -код (по-прежнему делимый). По следствию 4 можем увеличивать размерность кода с сохранением расстояний.

3) По следствию 2 при чётном d существует $\langle d - 1, 2^{d-1} - 1 \rangle_d$ -код, который также является делимым. Применяя к нему t раз утверждение 7, получаем $\langle d, 2^{t+d-1} - 2^t \rangle_{d+t}$ -код (по-прежнему делимый). Далее по следствию 4 увеличим размерность кода, сохраняя расстояния.

4) Пусть $d \leq l_1(n - t)$ чётное. Из утверждения 1 следует, что существует $\langle d, d \rangle_{n-t}$ -код. Применяя к нему t раз утверждение 7, получаем $\langle d, 2^t d \rangle_n$ -код.

5) Пусть $d \leq l_1(n - t)$ нечётное. Из утверждения 1 следует, что существует $\langle d, d \rangle_{n-t}$ -код. Применяя к нему t раз утверждение 7, получаем $\langle d + 1, 2^t d \rangle_n$ -код. Теорема 1 доказана.

3. $\langle n - 1, k \rangle_n$ -Дистанционные коды Грея

Для улучшения с помощью утверждений 1 и 2 верхней оценки $l_1(n)$ и нижней оценки $l_2(n)$, которые являются тривиальными, особый интерес представляет вопрос существования дистанционных кодов Грея при $d = n - 1$.

Теорема 2. Для любого чётного $n \geq 4$ дистанционный $\langle n - 1, k \rangle_n$ -код Грея существует тогда и только тогда, когда существует $\langle n - 1, k' \rangle_n$ -код Грея, где k и k' — пара взаимно обратных элементов в мультипликативной группе кольца вычетов по модулю 2^n .

ДОКАЗАТЕЛЬСТВО. Пусть $Q_n^{(n-1)}$ — граф на множестве двоичных слов длины n , в котором ребром соединены два слова, расстояние Хэмминга между которыми равно $n - 1$. Заметим, что при чётном n существует изоморфизм $\varphi: Q_n^{(n-1)} \rightarrow Q_n$:

$$\varphi(v) = \begin{cases} v, & \text{если вес } v \text{ чётный,} \\ \bar{v} & \text{иначе.} \end{cases}$$

Пусть $C = v_0, v_1, v_2, \dots, v_{2^n-1}$ — $\langle n - 1, k \rangle_n$ -код Грея. Нетрудно видеть, что $C^{(n-1)} = v_0, v_k, v_{2k}, \dots, v_{(2^n-1)k}$ — гамильтонов цикл в $Q_n^{(n-1)}$. Заметим, что расстояние в этом цикле между вершиной v_0 и v_1 равно k' , так как $k \cdot k' \equiv 1 \pmod{2^n}$. Поскольку φ — изоморфизм, цикл

$$C' = \varphi(v_0), \varphi(v_k), \varphi(v_{2k}), \dots, \varphi(v_{(2^n-1)k})$$

является n -мерным кодом Грея. Рассмотрим расстояние Хэмминга между словами $\varphi(v_0)$ и $\varphi(v_1)$. Так как веса слов v_0 и v_1 разной чётности, $d(\varphi(v_0), \varphi(v_1)) = n - 1$. Получили, что C' — $\langle n - 1, k' \rangle_n$ -код Грея. Теорема 2 доказана.

Следствие 5. Для любого чётного $n \geq 6$ не существует $\langle n - 1, k_i \rangle_n$ -кодов Грея, где k_i — обратный к $(2i + 1)$ элемент в мультипликативной группе кольца вычетов по модулю 2^n , при этом $n - 1 \leq k_i \leq 2^n - (n - 1)$, $1 \leq i \leq \frac{n-4}{2}$.

ДОКАЗАТЕЛЬСТВО. Так как k_i — обратный к $(2i+1)$ элемент в мультипликативной группе кольца вычетов по модулю 2^n , для некоторого $m \geq 1$ имеем $(2i+1)k_i = 2^nm + 1$. Значит, при $n \geq 6$

$$k_i \geq \frac{2^nm + 1}{(2i+1)} \geq \frac{2^nm + 1}{n-3} \geq n-1.$$

Пусть $k_i = (2^n - \bar{k}_i)$. Тогда $(2i+1)(2^n - \bar{k}_i) = 2^nm + 1$ для некоторого $m \geq 1$, откуда $\bar{k}_i(2i+1) \geq 2^n - 1$. При $n \geq 6$ имеем

$$\bar{k}_i \geq \frac{2^n - 1}{2i+1} \geq \frac{2^n - 1}{n-3} \geq n-1.$$

Следствие 5 доказано.

Так, например, поскольку $43 \cdot 3 \equiv 1 \pmod{64}$, по следствию 5 и утверждению 3 не существует $\langle 5, 21 \rangle_6$ -кода Грея. Все наборы параметров при $6 \leq n \leq 10$, для которых не существует $\langle n-1, k \rangle_n$ -кода Грея в силу следствия 5, приведены в табл. 4.

Т а б л и ц а 4

Наборы параметров, для которых
не существует $\langle d, k \rangle_n$ -кодов по следствию 5

n	d	k	2^n	$(2i+1)$	k_i
6	5	21	64	3	43
8	7	85	256	3	171
8	7	51	256	5	205
10	9	341	1024	3	683
10	9	205	1024	5	205
10	9	439	1024	7	439

Результат следствия 5 обобщается на произвольные значения n и d .

Теорема 3. Пусть $k = 2^p(2m+1)$ и k' является обратным элементом к $2m+1$ в мультипликативной группе кольца вычетов по модулю 2^{n-p} . Если $\frac{n-2^p}{d} > k'$, то $\langle d, k \rangle_n$ -код Грея не существует.

ДОКАЗАТЕЛЬСТВО. Пусть $C = v_0, v_1, v_2, \dots, v_{2^n-1}$ — $\langle d, k \rangle_n$ -код Грея. Нетрудно видеть, что $v_0, v_k, v_{2k}, \dots, v_{k \cdot k'}$ — простая цепь в $Q_n^{(n-d)}$, причём $v_{k \cdot k'} = v_{2^p}$. Отсюда $v_0, \bar{v}_k, v_{2k}, \dots, \bar{v}_{2^p}$ — цепь в $Q_n^{(d)}$. Далее заметим, что $d(v_0, \bar{v}_{2^p}) \leq dk'$. С другой стороны, $d(v_0, v_{2^p}) \leq 2^p$, а следовательно, $d(v_0, \bar{v}_{2^p}) \geq n - 2^p$. Получили, что если $n - 2^p > dk'$, то исходного $\langle d, k \rangle_n$ -дистанционного кода Грея не существует. Теорема 3 доказана.

В табл. 5 приведены некоторые наборы значений n , k и d , для которых несуществование $\langle d, k \rangle_n$ -кода Грея устанавливается с помощью теоремы 3.

Т а б л и ц а 5

Наборы параметров, для которых
не существует $\langle d, k \rangle_n$ -кодов по теореме 3

n	d	k	p	2^{n-p}	$(2m+1)$	k'
9	7	171	0	512	171	3
9	8	172	2	128	43	3
10	8	342	1	512	171	3
11	9	683	0	2048	683	3
11	10	410	1	1024	205	5
11	10	684	2	512	171	3
11	10	820	2	512	205	5
11	10	878	1	1024	439	7

4. Заключение

На данный момент не известно общих методов доказательства несуществования кодов Грея с заданными свойствами. Теорема 3 и следствие 5 для некоторых наборов параметров решают эту задачу для дистанционных кодов. К сожалению, вопрос существования $\langle n-1, n-1 \rangle_n$ - и $\langle n-1, n+1 \rangle_n$ -кодов остаётся открытым. Именно эти наборы представляют интерес: в случае несуществования таких кодов удастся улучшить тривиальные оценки для параметров равномерности $l_1(n)$ и $l_2(n)$. Важной задачей также представляется поиск рекурсивных по параметру n конструкций для $\langle d, k \rangle_n$ -кодов при $k \geq 2^{n-1}$, которые позволят находить дистанционные коды Грея для новых наборов параметров, а также существенно упростят схему их построения.

ЛИТЕРАТУРА

1. **Быков И. С.** О локально равномерных кодах Грея // Дискрет. анализ и исслед. операций. 2016. Т. 23, № 1. С. 51–64.
2. **Евдокимов А. А.** О нумерации подмножеств конечного множества // Методы дискретного анализа в решении комбинаторных задач: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1980. Вып. 34. С. 8–26.
3. **Пережогин А. Л.** Об автоморфизмах циклов в n -мерном булевом кубе // Дискрет. анализ и исслед. операций. 2007. Т. 14, № 3. С. 67–79.
4. **Chang G. J., Eu S.-P., Yeh C.-H.** On the (n, t) -antipodal Gray codes // Theor. Comput. Sci. 2007. Vol. 374, No. 1–3. P. 82–90.

5. **Goddyn L., Gvozdjak P.** Binary Gray codes with long bit runs // Electron. J. Comb. 2003. Vol. 10, No. R27. P. 1–10.
6. **Goddyn L., Lawrence G. M., Nemeth E.** Gray codes with optimized run lengths // Util. Math. 1988. Vol. 34. P. 179–192.
7. **Killian C., Savage C.** Antipodal Gray codes // Discrete Math. 2002. Vol. 281. P. 221–236.
8. **Knuth D. E.** The art of computer programming. Reading, MA: Addison-Wesley, 2004.
9. **Savage C.** A survey of combinatorial Gray codes // SIAM Rev. 1996. Vol. 39, No. 4. P. 605–629.

*Быков Игорь Сергеевич,
Пережогин Алексей Львович*

Статья поступила
19 мая 2016 г.
Исправленный вариант —
16 сентября 2016 г.

ON DISTANCE GRAY CODES

I. S. Bykov^{1,a} and A. L. Perezhogin^{1,2,b}¹Novosibirsk State University,

2 Pirogov St., 630090 Novosibirsk, Russia

²Sobolev Institute of Mathematics,

4 Acad. Koptuyug Ave., 630090 Novosibirsk, Russia

E-mail: ^apatrick.no10@gmail.com, ^bpereal@math.nsc.ru

Abstract. A Gray code of size n is a cyclic sequence of all binary words of length n such that two consecutive words differ exactly in one position. We say that the Gray code is a distance code if the Hamming distance between words located at distance k from each other is equal to d . The distance property generalizes the familiar concepts of a locally balanced Gray code. We prove that there are no distance Gray codes with $d = 1$ for $k > 1$. Some examples of constructing distance Gray codes are given. For one infinite series of parameters, it is proved that there are no distance Gray codes. Tab. 5, bibliogr. 9.

Keywords: n -cube, Hamiltonian cycle, Gray code, uniform Gray code, antipodal Gray code.

REFERENCES

1. I. S. Bykov, On locally balanced Gray codes, *Diskretn. Anal. Issled. Oper.*, **23**, No. 1, 51–64, 2016 [Russian]. Translated in *J. Appl. Ind. Math.*, **10**, No. 1, 78–85, 2016.
2. A. A. Evdokimov, On enumeration of subsets of a finite set, in *Metody diskretnogo analiza v reshenii kombinatornykh zadach* (Methods of Discrete Analysis for Solving Combinatorial Problems), Vol. 34, pp. 8–26, Izd. Inst. Mat., Novosibirsk, 1980 [Russian].
3. A. L. Perezhogin, On automorphisms of cycles in an n -dimensional Boolean cube, *Diskretn. Anal. Issled. Oper.*, Ser. 1, **14**, No. 3, 67–79, 2007 [Russian].
4. G. J. Chang, S.-P. Eu, and C.-H. Yeh, On the (n, t) -antipodal Gray codes, *Theor. Comput. Sci.*, **374**, No. 1–3, 82–90, 2007.
5. L. Goddyn and P. Gvozdjak, Binary Gray codes with long bit runs, *Electron. J. Comb.*, **10**, No. R27, 1–10, 2003.
6. L. Goddyn, G. M. Lawrence, and E. Nemeth, Gray codes with optimized run lengths, *Util. Math.*, **34**, 179–192, 1988.

7. **C. Killian** and **C. Savage**, Antipodal Gray codes, *Discrete Math*, **281**, 221–236, 2002.
8. **D. E. Knuth**, *The art of computer programming*, Addison-Wesley, Reading, MA, 2004.
9. **C. Savage**, A survey of combinatorial Gray codes, *SIAM Rev.*, **39**, No. 4, 605–629, 1997.

Igor S. Bykov,
Alexey L. Perezhogin

Received
19 May 2016
Revised
16 September 2016