

СОХРАНЯЮЩИЕ РАССТОЯНИЯ ЦИКЛИЧЕСКИЕ КОДЫ НА ЛИНЕЙНОМ БАЗИСЕ*)

А. Я. Зантен, ван

Обсуждается подход к построению сохраняющих расстояние циклических кодов, основанный на выборе подходящего базиса линейного кода с расстоянием 2.

Введение

Пусть $\bar{u}_0, \bar{u}_1, \dots, \bar{u}_{N-1}$ — последовательность (иначе: список) слов длины n в алфавите $0, 1$. Такой список мы называем *упорядоченным кодом ранга n* . «Списочное» расстояние между двумя кодовыми словами \bar{u}_i и \bar{u}_j мы определяем как $d(\bar{u}_i, \bar{u}_j) = |i - j|$. Иногда такой список рассматривается как циклический код с циклическим списочным расстоянием

$$d(\bar{u}_i, \bar{u}_j) = \min\{N - |i - j|, |i - j|\}, \quad (1)$$

полагая $\bar{u}_N = \bar{u}_0$. Упорядоченный код называется *сохраняющим расстояние кодом с порогом m* , если выполняется следующее свойство:

списочное расстояние между любыми двумя словами равно расстоянию Хемминга между ними до тех пор, пока списочное расстояние не превышает m . (★)

Такой код мы называем $\langle m, n \rangle$ -кодом. Сохраняющие расстояние коды в наиболее общем виде введены и исследованы в [5]. Они обобщают понятие кода, сохраняющего разности [1, 2]. Если условие (★) выполняется в циклическом смысле, мы говорим о *циклическом $\langle m, n \rangle$ -коде*. В этой статье мы имеем дело только с циклическими $\langle m, n \rangle$ -кодами. И поэтому прилагательное «циклический» часто будем опускать.

Циклический $\langle m, n \rangle$ -код, или $\langle m, n \rangle$ -код, может быть охарактеризован его *переходной последовательностью*

$$T := t_0, t_1, \dots, t_{N-1}, \quad (2)$$

*) Перевод с английского доклада автора, прочитанного на Международной Сибирской конференции по исследованию операций, которая была проведена в Новосибирске с 22 по 27 июня 1998 г.

представляющей список целых чисел из множества $\{1, 2, \dots, n\}$ такой, что t_i указывает бит, который изменяется при переходе от i -го кодового слова к $(i + 1)$ -му слову, $0 \leq i < N$. Мы считаем, что позиции в кодовых словах занумерованы числами от 1 до n справа налево. Например, следующая переходная последовательность соответствует $\langle 4, 5 \rangle$ -коду:

$$3, 4, 2, 5, 1, 4, 3, 5, 2, 4, 3, 5, 1, 4, 2, 5, 3, 4, 2, 5, 1, 4, 3, 5, 2, 4, 3, 5, 1, 4, 2, 5. \quad (3)$$

Если $\langle m, n \rangle$ -код состоит из 2^n кодовых слов, то он называется *полным*. Так код из (3) является полным циклическим $\langle 4, 5 \rangle$ -кодом. Циклический код Грея, называемый обычно стандартным кодом Грея порядка n , является полным циклическим $\langle 2, n \rangle$ -кодом. Легко проверить, что переходная последовательность

$$1, 2, \dots, n, 1, 2, \dots, n \quad (4)$$

определяет $\langle n, n \rangle$ -код, который при $n > 2$ не является полным. Наибольший ранг циклического $\langle m, n \rangle$ -кода обозначим $s(m, n)$. Следовательно, $s(1, n) = s(2, n) = 2^n$ и, используя (4), легко проверить, что $s(n, n) = 2n$.

А. А. Евдокимов [1] дал метод построения $\langle m, n \rangle$ -кодов, использующий композицию таких кодов с меньшими значениями параметров. Ниже мы обсудим другой подход к конструированию $\langle m, n \rangle$ -кодов, основанный на равновесном базисе линейного $[n, k, 2]$ -кода.

1. Основы построения

Во избежание тривиальностей полагаем $1 < m < n$. Пусть $B = (\bar{b}_1, \bar{b}_2, \dots, \bar{b}_k)$ — такой базис $[n, k, 2]$ -кода C , что $\|\bar{b}_i\| = m$, $1 \leq i \leq k$. Пусть $G(k)$ — переходная последовательность стандартного кода Грея G_k порядка k . Известно (см., например, [3]), что в соответствии с кодом Грея G_k можно так линейно упорядочить все векторы кода C , что каждый вектор из этого списка будет отличаться от предшествующего вектора единственным базисным вектором \bar{b}_i при некотором i . Переходя к двоичным словам длины n , мы получаем такой циклический список, в котором каждое слово отличается от предыдущего точно в m позициях [3]. Более точно список C определяется так:

$$\bar{v}_0 = \bar{0}, \quad \bar{v}_{i+1} = \bar{v}_i + \bar{b}_{t_i} \quad (5)$$

для $0 \leq i < 2^k - 1$, где t_i является i -м элементом переходной последовательности $G(k)$. Далее мы заменяем \bar{v}_i на \bar{v}_{i+1} последовательно для каждого i в соответствии с данными 2^k подписками из m различных слов в каждом. Промежуточные слова будем обозначать $\bar{w}_i^1, \bar{w}_i^2, \dots, \bar{w}_i^{m-1}$. Конкатенация этих подписков, т. е.

$$D_k := \bar{v}_0, \bar{w}_0^1, \bar{w}_0^2, \dots, \bar{w}_0^{m-1}, \bar{v}_1, \bar{w}_1^1, \bar{w}_1^2, \dots, \bar{w}_{2^k-1}^{m-1}, \quad (6)$$

является упорядоченным списком из $m \cdot 2^k$ двоичных слов длины n . Будут ли все эти слова различны, зависит от порядка изменения позиции, который будет определен так называемыми *упорядоченными блоками*

$$b_i := (\alpha_1^i, \alpha_2^i, \dots, \alpha_m^i), \quad 1 \leq i \leq k, \quad (7)$$

где целые числа α_j^i указывают позиции единиц в \bar{b}_i , в соответствии с которыми сначала меняется значение позиции α_1^i , затем α_2^i и т. д. Следовательно, переходная последовательность, соответствующая списку (6), может быть записана в виде

$$T_k := b_1 b_2 b_1 \dots b_1 b_k b_1 \dots b_1 b_k, \quad (8)$$

где последовательность индексов соответствует стандартному коду Грея. Хотя это не следует из предыдущего, мы допускаем, что блоки b_i на различных позициях в (8) могут иметь различный внутренний порядок. Можно доказать, что если базисные векторы \bar{b}_i из B удовлетворяют некоторым дополнительным условиям, внутренний порядок в блоках b_i может быть выбран таким, что D_k из (6) будет $\langle m, n \rangle$ -кодом с переходной последовательностью (8).

2. Результаты

Для каждого i , $1 \leq i \leq k$, аналогично (8) введем

$$T_i := b_1 b_2 b_1 \dots b_1 b_i b_1 \dots b_1 b_i, \quad (9)$$

линейный подкод кода C

$$C_i := \langle \bar{b}_1, \bar{b}_2, \dots, \bar{b}_i \rangle \quad (10)$$

с $C_k = C$ и множества

$$C_i^j := \{\bar{w}_0^j, \bar{w}_1^j, \dots, \bar{w}_{2^i-1}^j\}, \quad 1 \leq j \leq m-1. \quad (11)$$

Кроме того, мы требуем, чтобы базисные векторы \bar{b}_i удовлетворяли следующим условиям:

- (i) $\|\bar{b}_i\| = m$, $\|\bar{b}_i + \bar{b}_{i+1}\| = 2$, $1 \leq i < k$;
- (ii) $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_k$ имеют $\lceil \frac{m}{2} \rceil$ общих единичных разрядов;
- (iii) если x является общей единицей в \bar{b}_1 и \bar{b}_j , но не в \bar{b}_{j+1} , то x есть общая единица в $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_j$, где $1 < j < k$.

В частности, если базис B удовлетворяет (i) и (ii), то в блоках b_i можно выбрать такой внутренний порядок, что все слова в (6) различны и, кроме того, чтобы все блоки b_i с одинаковым значением i имели один и тот же порядок. Этот порядок мы называем *начальным порядком*. Тогда список (6) является циклическим $\langle m', n \rangle$ -кодом для некоторого $m' \leq m$. Если B удовлетворяет еще и условию (iii), то появляется возможность переопределить порядок в b_i -блоках, чтобы получить циклический $\langle m, n \rangle$ -код. Базис B , удовлетворяющий условиям (i)–(iii), называем *допустимым базисом*. Сформулируем наш основной результат.

Теорема 1. Для каждого k , $1 \leq k \leq n - \lfloor \frac{m}{2} \rfloor$, можно так определить допустимый базис B и внутренний порядок для блоков в T_k , что результирующая последовательность (8) будет переходной последовательностью циклического $\langle m, n \rangle$ -кода ранга $m2^k$.

Доказательство индуктивное, а конструкция переходной последовательности является рекурсивной и состоит в преобразовании T_i из (9) в T_{i+1} , $1 \leq i < k$. Если по индукционному предположению T_i определяет циклический $\langle m, n \rangle$ -код ранга $m2^i$, то он вначале преобразовывается в T'_i заменой последнего блока b_i на b_{i+1} , где порядок в этих блоках первоначальный. Теперь последовательность $T_{i+1}^* := T'_i T'_i$ определяет циклический $\langle m', n \rangle$ -код ранга $m2^{i+1}$, где $m' \leq m$. Затем в некоторых блоках из T_{i+1}^* изменяется порядок, чтобы получить последовательность T_{i+1} , которая определяет циклический $\langle m, n \rangle$ -код ранга $m2^{i+1}$. Одновременно доказывается, что множества C_i^j из (11) являются смежными классами кода C_i , $1 \leq i \leq k$. За деталями этого доказательства мы отсылаем к [4]. Проиллюстрируем сказанное следующим поясняющим примером.

ПРИМЕР. Пусть $B = (\bar{b}_1, \bar{b}_2, \bar{b}_3)$ — базис для векторов постоянного веса, где $\bar{b}_1 = 11110$, $\bar{b}_2 = 11101$ и $\bar{b}_3 = 11011$. Легко проверяется, что B является допустимым. Начальный порядок блоков определим следующим образом: $b_1 = (2435)$, $b_2 = (1435)$, $b_3 = (1425)$. Последовательность

$$T_2 = 2435 \quad 1435 \quad 2435 \quad 1435$$

определяет циклический $\langle 4, 5 \rangle$ -код ранга 16 (мы опускаем очевидный случай T_1). Затем преобразуем T_2 в

$$T_3^* = 2435 \quad 1435 \quad 2435 \quad 1425 \\ 2435 \quad 1435 \quad 2435 \quad 1425.$$

Эта последовательность соответствует циклическому $\langle 2, 5 \rangle$ -коду. Меняя порядок в первом и пятом блоке, получаем циклический $\langle 4, 5 \rangle$ -код

$$T_3 = 3425 \quad 1435 \quad 2435 \quad 1425 \\ 3425 \quad 1435 \quad 2435 \quad 1425,$$

упомянутый во введении.

3. Циклические $\langle n - 1, n \rangle$ -коды

Конструкция, описанная в предыдущем разделе, является рекурсивной. В случае $m = n - 1$ можно дать явную конструкцию циклического $\langle n - 1, n \rangle$ -кода. (Некоторые результаты, относящиеся к циклическим $\langle n - 1, n \rangle$ -кодам, были получены в работе [6]. — *Примеч. переводчика.*) В этом случае мы имеем следующий допустимый базис:

$B = (\bar{b}_1, \bar{b}_2, \dots, \bar{b}_k)$, где $k = \lceil \frac{n}{2} \rceil$ и

$$\begin{aligned}\bar{b}_1 &= 111 \dots 11 \dots 110, \\ \bar{b}_2 &= 111 \dots 11 \dots 101, \\ \bar{b}_3 &= 111 \dots 11 \dots 011, \\ &\vdots \\ \bar{b}_k &= 111 \dots 10 \dots 111.\end{aligned}$$

В соответствии с построениями из [4] введем упорядоченные блоки $b_1 = (2, k+1, 3, k+2, \dots, k, n)$, $b_2 = (1, k+1, 3, k+2, \dots, k, n)$ и т. д. для нечетного n , и $b_1 = (k+1, 2, k+2, 3, \dots, k, n)$, $b_2 = (k+1, 1, k+2, 3, \dots, k, n)$ и т. д. для четного n . Следовательно, общие числа $k+1, k+2, \dots, n$ расположены в блоках чередуясь с числами $1, 2, \dots, k$. Поскольку позиции этих общих чисел не будут изменяться, в дальнейшем мы их опускаем, записывая упорядоченные блоки в виде

$$\begin{aligned}b_1 &= (2, 3, 4, \dots, k), \\ b_2 &= (1, 3, 4, \dots, k), \\ &\vdots \\ b_k &= (1, 2, 3, \dots, k-1).\end{aligned}$$

Кроме того, введем в рассмотрение следующие циклические перестановки второго порядка:

$$\sigma_i := (i+1, i+2), \quad 0 \leq i < k-1. \quad (12)$$

Все блоки в T_k занумеруем слева направо числами от 0 до $2^k - 1$. Тогда существует простая связь между двоичным представлением номера блока и перестановкой, которую необходимо применить к первоначальному порядку в блоке, чтобы получить итоговый порядок. Мы представляем результат в виде теоремы.

Теорема 2. Пусть

$$T_k = b_1 b_2 b_1 \dots b_1 b_k b_1 b_2 b_1 \dots b_1 b_k$$

является переходной последовательностью циклического $\langle n-1, n \rangle$ -кода длины $(n-1)2^k$. Если b — блок в T_k с номером j , $0 \leq j < 2^k$, и

$$(2^k - 1 - j)_2 = \varepsilon_{k-1} \varepsilon_{k-2} \varepsilon_{k-3} \dots \varepsilon_0$$

является двоичным представлением дополнения j , то итоговый порядок в блоке b получается из начального порядка применением следующей

перестановки:

$$\pi_j := \sigma_{k-2}^{\varepsilon_{k-2}} \sigma_{k-3}^{\varepsilon_{k-3}} \cdots \sigma_{l+1}^{\varepsilon_{l+1}},$$

где l — наименьшее целое такое, что $\varepsilon_l = 1$.

Для примера построим циклический $\langle 8, 9 \rangle$ -код. Имеем $n = 9$ и $k = 5$. Начинаем с упорядоченных блоков $b_1 = (2, 3, 4, 5)$, $b_2 = (1, 3, 4, 5)$, $b_3 = (1, 2, 4, 5)$, $b_4 = (1, 2, 3, 5)$, $b_5 = (1, 2, 3, 4)$. Как и раньше, мы опускаем общие числа 6, 7, 8 и 9. Так как $(2^5 - 1 - 0)_2 = 11111$, то имеем $\pi_0 = \sigma_3 \sigma_2 \sigma_1$. Тогда к числам блока с номером 0, который является b_1 -блоком, применяется перестановка $\pi_0 = (45)(34)(23)$ и получается блок $(5, 2, 3, 4)$. Аналогично имеем $\pi_1 = \sigma_3 \sigma_2 = (45)(34)$ и, применяя эту перестановку к блоку $(1, 3, 4, 5)$, получаем $(1, 5, 3, 4)$ и т. д. Применяя все перестановки и чередуя числа в полученных блоках с общими числами 6, 7, 8, 9, получаем следующую переходную последовательность циклического $\langle 8, 9 \rangle$ -кода длины 256:

56273849 16573849 26573849 16275849
 36275849 16375849 26375849 16273859
 46273859 16473859 26473859 16274859
 36274859 16374859 26374859 16273849
 56273849 16573849 26573849 16275849
 36275849 16375849 26375849 16273859
 46273859 16473859 26473859 16274859
 36274859 16374859 26374859 16273849

ЛИТЕРАТУРА

1. 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.
2. Preparata F. P., Nievergelt J. Difference-preserving codes // IEEE Trans. Inform. Theory. 1974. V. IT-20, N 5. P. 643–649.
3. van Zanten A. J. Minimal-change order and separability in linear codes // IEEE Trans. Inform. Theory. 1993. V. IT-39. N 6. P. 1988–1989.
4. van Zanten A. J., Lukito A. Construction of certain cyclic distance-preserving codes having linear-algebraic characteristics // Designs, Codes and Cryptography (in press).

5. **Евдокимов А. А.** Метрические свойства вложений и коды, сохраняющие расстояния // Модели и методы оптимизации. Новосибирск: Наука, 1988. С. 116–132. (Тр. / АН СССР. Сиб. отд-ние. Ин-т математики; Т. 10). (Добавлено при переводе.)
6. **Пережогин А. Л.** О локально изометрическом кодировании натуральных чисел // Дискрет. анализ и исслед. операций. 1996. Т. 3, № 4. С. 69–76. (Добавлено при переводе.)

Адрес автора:

A. J. van Zanten

Delft University of Technology,
Department of Mathematics,
P. O. Box 5031, 2600 GA Delft,
The Netherlands.

E-mail:

a.j.vanzanten@twi.tudelft.nl

Статья поступила

26 июня 1998 г.