

УДК 621.391.15

© 2004 г. Н. Н. Токарева

О КОМПОНЕНТАХ КОДОВ ПРЕПАРАТЫ

Рассматривается взаимосвязь i -компонент произвольного кода P типа Препараты с i -компонентами совершенного кода C , содержащего этот код. Показано, что любая i -компонента кода P однозначно достраивается до i -компоненты кода C путем добавления определенного числа специальных кодовых слов кода C . Показано, что в характеристическом графе произвольной i -компоненты кода C множество вершин кода P образует совершенный код с расстоянием 3.

§ 1. Введение

Хорошо известно (см. [1]), что существуют только два нетривиальных бесконечных семейства кодов, являющихся одновременно максимальными и равномерно упакованными, – это семейства тесно связанных между собой совершенных кодов и кодов Препараты.

Статья посвящена выявлению еще одного свойства, отражающего связь кодов Препараты с совершенными кодами, их содержащими. Основными предметами исследования являются компоненты кодов Препараты и совершенных кодов, основным инструментом – метод свитчинга компонент.

Под компонентой кода понимается подмножество кодовых слов, допускающее преобразования специального вида, которые меняют код, не изменяя его параметров (длины кода, его мощности и кодового расстояния). В настоящий момент метод свитчинга (метод независимых преобразований различных компонент кода) играет одну из главных ролей в исследовании свойств совершенных кодов (см. [2–4]), но следует заметить, что к кодам Препараты он до сих пор не применялся.

Любой код Препараты содержится в некотором совершенном коде и притом единственном (см. [5]). Обратное, вообще говоря, не верно. Если с помощью свитчинга произвольной i -компоненты (определение см. в §2) перейти от кода Препараты P к коду Препараты P' , то каким образом окажутся связаны между собой совершенные коды C и C' , содержащие коды P и P' соответственно?

В статье показано, что любая i -компонента кода Препараты однозначно достраивается до i -компоненты совершенного кода, причем сдвиг i -компоненты в коде Препараты индуцирует в содержащем его совершенном коде сдвиг достроенной i -компоненты и только ее (теорема 1). Таким образом, коды C и C' получаются друг из друга свитчингом, в котором участвует только одна координата i . В качестве следствия получены оценки мощности минимальной i -компоненты кода Препараты. Показано, что в характеристическом графе произвольной i -компоненты совершенного кода множество вершин кода Препараты образует совершенный код с расстоянием 3 (теорема 2).

§ 2. Необходимые определения и утверждения

Рассмотрим n -мерное векторное пространство E^n над полем Галуа $GF(2)$ с заданной на нем метрикой Хэмминга: расстояние $d(x, y)$ между векторами x и y (будем называть их также вершинами) равно числу позиций, в которых они различаются. Вес $w(x)$ вершины x есть $d(x, 0^n)$, где 0^n – нулевая вершина, т.е. вершина, все координаты которой равны нулю. Множество $C \subseteq E^n$ называется кодом длины n , размерности k и с кодовым расстоянием d , если его мощность равна 2^k , а расстояние между любыми двумя кодовыми словами не меньше d .

Подмножество M кода C с кодовым расстоянием d называется i -компонентой кода C , если множество $C' = (C \setminus M) \cup (M \oplus e_i)$ также является кодом с расстоянием d , где e_i – вектор, имеющий только одну ненулевую координату $i \in \{1, 2, \dots, n\}$ (другими словами i -компонента кода – это компонента, в качестве преобразования которой выбрано инвертирование произвольной координаты i в каждом кодовом слове, – сдвиг по направлению i). Определение минимальной, т.е. неразложимой на меньшие, i -компоненты было введено в [6]. Согласно данному определению i -компонента кода может быть как минимальной, так и составленной из нескольких i -компонент.

Кодовая вершина u называется i -близкой к кодовой вершине v , если она находится от v на минимальном кодовом расстоянии и различается в i -й координате. Вектор w пространства E^n назовем i -направлением кодовой вершины v , если вершина $v \oplus w$ является i -близкой к вершине v . Таким образом, i -направления любой кодовой вершины представляют собой векторы веса d (не обязательно принадлежащие коду), которые в i -й координате содержат единицу. Для кодовой вершины v число всех ее i -направлений назовем i -степенью данной вершины.

Следуя работе [7], несложно доказать

Предложение 1. Подмножество M кода C является i -компонентой кода C тогда и только тогда, когда вместе с каждой своей вершиной оно содержит все i -близкие к ней.

Из предложения 1 непосредственно следует, что для произвольной координаты i любой код однозначно представим в виде объединения непересекающихся минимальных i -компонент. Код называется дистанционно-инвариантным, если количество кодовых вершин, находящихся на некотором расстоянии от данной кодовой вершины, не зависит от выбора этой вершины, а зависит только от длины кода и этого расстояния. Любой максимальный равномерно упакованный код является дистанционно-инвариантным (см. [1]).

Предложение 2. Пусть C – произвольный максимальный равномерно упакованный код, содержащий нулевую вершину 0^n и вершину из всех единиц 1^n . Тогда вершины 0^n и 1^n принадлежат одной минимальной i -компоненте кода C .

Приведем доказательство этого факта, являющегося прямым обобщением утверждения, доказанного в [8] для случая, когда C – совершенный код. Пусть вершины 0^n и 1^n принадлежат различным минимальным i -компонентам кода C . Перейдем к коду C' , сдвинув в коде C только i -компоненту, содержащую вершину 1^n . Коды C и C' относительно нулевой вершины должны иметь одинаковое весовое распределение. Однако это свойство дистанционной инвариантности нарушено, поскольку 1^n принадлежит C , но не принадлежит C' . ▲

Любой код можно представить в виде объединения двух непересекающихся множеств: i -четных и i -нечетных вершин. Кодовая вершина называется i -четной (i -нечетной), если ее проекция по направлению i имеет четный (нечетный) вес. Каждое из этих множеств образует i -компоненту кода, если код имеет нечетное кодовое расстояние. Такое разбиение называется тривиальным разбиением кода на i -компоненты. Действительно, если расстояние кода нечетно, то для произвольной

вершины все i -близкие к ней будут иметь ту же i -четность, что и данная вершина, а следовательно, принадлежать тому же множеству в разбиении.

Рассмотрим дистанционно-инвариантный код C с нечетным кодовым расстоянием, такой что все его вершины имеют одну и ту же i -степень для некоторой координаты i . Пусть эта i -степень отлична от числа всех кодовых вершин, находящихся на минимальном расстоянии от произвольной вершины кода. Тогда справедливо

Предложение 3. *Определенный выше код C разбивается по направлению i на две равномощные i -компоненты.*

Доказательство. Достаточно показать, что в таком коде множества C_0 и C_1 (i -четных и i -нечетных по i вершин соответственно) имеют равные мощности, тогда искомым разбиением кода на i -компоненты будет тривиальное. Рассмотрим двудольный граф на множестве вершин кода, в котором ребрами соединены вершины различной i -четности, расположенные на минимальном расстоянии друг от друга. Для любой кодовой вершины v кодовые слова, находящиеся от нее на минимальном расстоянии, состоят из множества вершин той же i -четности (это i -близкие к v вершины) и множества вершин i -четности, отличной от i -четности v . В силу условий, которым удовлетворяет код, мощности этих множеств не зависят от выбора вершины v . Рассматриваемый граф является однородным, а следовательно, его доли C_0 и C_1 должны иметь равные мощности. ▲

Перейдем теперь к интересующим нас кодам.

Код C длины n с расстоянием 3 называется *совершенным*, если непересекающиеся шары радиуса 1 с центрами в его кодовых вершинах покрывают все пространство E^n . Совершенные двоичные коды с расстоянием 3 существуют только для $n = 2^m - 1$, $m = 2, 3, \dots$, и имеют размерность $k = n - \log_2(n + 1)$.

Код P длины $n = 2^{2m} - 1$, $m = 2, 3, \dots$, называется кодом типа Препараты (далее именуемым *кодом Препараты*), если он имеет кодовое расстояние 5 и размерность $k = n - 2 \log_2(n + 1) + 1$.

Совершенные коды и коды Препараты являются максимальными равномерно упакованными и обладают свойством антиподальности: вершины v и $v \oplus 1^n$ принадлежат или не принадлежат коду одновременно.

Справедливо

Предложение 4 (см. [5]). *Любой код Препараты содержится в некотором совершенном коде и притом единственном.*

Обозначим через $C(P)$ совершенный код, содержащий код Препараты P . Напомним, что *рангом* множества векторов называется размерность его линейной оболочки.

Предложение 5 (см. [9]). *Ранг любого кода Препараты равен рангу совершенного кода, его содержащего.*

Каждый вектор веса k пространства E^n можно представить в виде набора (i_1, \dots, i_k) его ненулевых координат (такое представление будем использовать наряду с векторным, знак \oplus будет означать сложение по модулю 2 соответствующих векторов). Подмножество T множества векторов веса k пространства E^n называется t -(n, k, λ)-*схемой*, если любое t -элементное подмножество множества $\{1, 2, \dots, n\}$ содержится в наборах ненулевых координат в точности λ векторов из T . Кодовые слова минимального веса в приведенных (т.е. содержащих нулевую вершину) совершенном коде и коде Препараты образуют, соответственно, 2-($n, 3, 1$)- и 2-($n, 5, (n-3)/3$)-схемы (см. [1]). Это означает, что в каждом из этих кодов по любому направлению i все вершины имеют одинаковую i -степень. Поэтому из предложения 3 следует

Предложение 6. *Минимальная i -компонента в совершенном коде и коде Препараты по любому направлению i составляет не более половины кода.*

Следует отметить, что в случае совершенного кода эта оценка является точной. Точные верхняя и нижняя оценки мощности минимальной i -компоненты совершенного кода приведены в [7, 8] (см. также [10]).

Выберем любую координату i из множества $\{1, 2, \dots, n\}$, где $n = 2^{2m} - 1$, $m = 2, 3, \dots$. Через $N^P(v)$ и $D^P(v)$ обозначим, соответственно, множество i -близких кодовых вершин и множество i -направлений произвольной вершины v кода Препараты P . Аналогичные обозначения $N^C(u)$ и $D^C(u)$ введем для произвольной вершины u совершенного кода C .

Для совершенного кода легко вывести

Предложение 7. *Множество $D^C(u)$, состоящее из векторов веса 3, определяет разбиение множества $\{1, 2, \dots, n\} \setminus \{i\}$ на пары $\{j, k\}$, такие что каждая тройка (i, j, k) принадлежит $D^C(u)$. Справедливо соотношение $|D^C(u)| = (n-1)/2$.*

Предложение 8 (см. [1, 5]). *Множество $D^P(v)$, состоящее из векторов веса 5, для произвольной координаты $j \in \{1, 2, \dots, n\}$, $j \neq i$, определяет разбиение множества $\{1, 2, \dots, n\} \setminus \{i, j, k\}$ на подмножества $\{l, m, r\}$, такие что каждая пятерка (i, j, l, m, r) принадлежит $D^P(v)$, где (i, j, k) – тройка из множества $D^{C(P)}(v)$. Справедливо соотношение $|D^P(v)| = (n-1)(n-3)/12$.*

Согласно [1] каждая вершина w кода $C(P) \setminus P$ находится на расстоянии 3 от максимального числа $n/3$ вершин кода P , поэтому справедливо

Предложение 9 (см. [1, 5]). *Для произвольной вершины w кода $C(P) \setminus P$ множество $\{1, 2, \dots, n\}$ разбивается на подмножества $\{q, s, t\}$, такие что $w \oplus (q, s, t) \in P$.*

§ 3. Связь компонент кодов Препараты и совершенных кодов

Рассмотрим произвольный приведенный код Препараты P и содержащий его совершенный код $C = C(P)$. Пусть множество M является минимальной i -компонентой кода P для произвольной координаты i . Код Препараты, полученный из P сдвигом i -компоненты M по направлению i , обозначим через P' . Через C' обозначим код $C(P')$.

Определим взаимно однозначную функцию f , действующую из кода P в P' , по следующему правилу:

$$f(v) = \begin{cases} v \oplus e_i, & \text{если } v \in M, \\ v, & \text{если } v \in P \setminus M. \end{cases}$$

Лемма 1. *Пусть P , P' и C , C' – коды, определенные выше. Для любого вектора v из P справедливы равенства*

$$D^P(v) = D^{P'}(f(v)), \quad (1)$$

$$D^C(v) = D^{C'}(f(v)). \quad (2)$$

Доказательство. Пусть v – произвольный вектор из P . Равенство (1) очевидно следует из предложения 1 и способа, которым код P' получен из кода P . Докажем равенство множеств $D^C(v)$ и $D^{C'}(f(v))$. Пусть (i, j, k) – некоторая тройка из $D^C(v)$. Предположим, что (i, j, k) не принадлежит множеству $D^{C'}(f(v))$, тогда по предложению 7 в множестве $D^{C'}(f(v))$ существует тройка (i, j, l) и $l \neq k$. Согласно предложению 8 в множестве $D^P(v)$ найдется пятерка (i, j, l, m, r) для любой координаты $l, l \neq k$, и некоторых $m, r \in \{1, 2, \dots, n\} \setminus \{i, j, k\}$. Из (1) следует, что (i, j, l, m, r) принадлежит также множеству $D^{P'}(f(v))$. Получаем, что $d(f(v) \oplus (i, j, l, m, r), f(v) \oplus (i, j, k))$ равно 2, что меньше кодового расстояния совершенного кода C' . Противоречие.

Следовательно, тройка (i, j, k) принадлежит $D^{C'}(f(v))$, т.е. $D^C(v) \subseteq D^{C'}(f(v))$. Аналогично можно показать, что $D^{C'}(f(v)) \subseteq D^C(v)$. ▲

Теорема 1. Пусть множество M является минимальной i -компонентой кода Препараты P . Тогда множество $R = M \cup N^C(M)$ является i -компонентой совершенного кода C , где $N^C(M) = \bigcup_{v \in M} N^C(v)$.

Доказательство. Покажем, что для любого вектора v из R множество $N^C(v)$ содержится в R . Если $v \in M$, то $N^C(v)$ содержится в R по определению множества $N^C(M)$. Пусть $v \in N^C(M)$, тогда существует вектор $u \in M$ такой, что вектор v принадлежит $N^C(u)$. Вектор u содержится в множестве $N^C(v)$ и принадлежит R . Из предложения 9 следует, что в множестве $N^C(v)$ вектор u единственный из кода P , остальные векторы $N^C(v) \setminus \{u\}$ принадлежат множеству $C \setminus P$. Покажем, что они также содержатся в R . Выберем произвольный вектор v_1 из $N^C(v) \setminus \{u\}$. В силу того же предложения 9 найдется в точности один вектор $u_1 \in P$ такой, что v_1 принадлежит множеству $N^C(u_1)$. Если показать, что вектор u_1 содержится в M , тогда вектор v_1 будет принадлежать множеству $N^C(M)$ и, следовательно, множеству R . Предположим, что $u_1 \in P \setminus M$. Рассмотрим код P' . Вершина u принадлежит множеству M , поэтому под действием функции f она перейдет в вершину $u \oplus e_i$. По лемме 1 имеем $D^C(u) = D^{C'}(u \oplus e_i)$, следовательно, вершина $v \oplus e_i$ принадлежит коду C' . Согласно предположению справедливо равенство $f(u_1) = u_1$, а значит, вершина v_1 принадлежит коду C' . Тогда $d(v \oplus e_i, v_1) = 2$, что меньше кодового расстояния совершенного кода C' . Таким образом, вершина u_1 принадлежит множеству M и множество $N^C(v)$ содержится в R . ▲

Замечание. Построенная i -компонента R является наименьшей по мощности i -компонентой совершенного кода C , содержащей данную i -компоненту M кода Препараты P . Очевидно, что любая другая i -компонента кода C , содержащая M , должна содержать также множество $N^C(M)$, а следовательно, множество R .

Рассмотрим характеристический граф $G^{\tilde{R}} = (\tilde{R}, E)$ произвольной i -компоненты \tilde{R} совершенного кода C , где $E = \{(u, v) \mid u \in N^C(v)\}$. Граф $G^{\tilde{R}}$ является однородным степени $(n-1)/2$.

Из теоремы 1 вытекают следующие следствия.

Следствие 1. Справедливо $|R| = (n+1)|M|/2$.

Доказательство. В графе G^R найдем число ребер, соединяющих множества M и $N^C(M)$. С одной стороны, это число равно $(n-1)|M|/2$, а с другой стороны, равно $|N^C(M)|$. Используя соотношение $|R| = |M| + |N^C(M)|$, получаем требуемое равенство. ▲

Следствие 2. Справедливо $2^{\frac{n+1}{2} - \log_2(n+1)} \leq |M| \leq 2^{n-2\log_2(n+1)}$.

Доказательство. Нижнюю оценку получаем непосредственно из известной точной нижней оценки мощности минимальной i -компоненты совершенного кода (см. [8, 10]):

$$2^{\frac{n-1}{2}} \leq |R|.$$

Верхняя оценка следует из предложения 6. ▲

Согласно предложению 4 код C' однозначно определяется кодом P' , и справедливо равенство $C' = (C \setminus R) \cup (R \oplus e_i)$. Отсюда вытекает

Следствие 3. Сдвиг произвольной i -компоненты M в коде Препараты индуцирует в содержащем его совершенном коде сдвиг наименьшей i -компоненты R , включающей M .

Следствие 4. Ранг произвольной i -компоненты M кода Препараты равен рангу наименьшей i -компоненты R совершенного кода, содержащего данный код Препараты, такой, что $M \subset R$.

Доказательство в точности повторяет доказательство предложения 5, приведенное в [9]. Без ограничения общности можно считать (опираясь на дистанционную инвариантность кода Препараты), что i -компонента M содержит нулевую вершину 0^n , и следовательно, согласно предложению 2, вершину 1^n . Обозначим через $r(M)$ и $r(R)$ ранги i -компонент M и R соответственно. Множество M содержится в R , поэтому справедливо $r(M) \leq r(R)$. Покажем, что выполнено $r(M) \geq r(R)$, т.е. любой вектор v из R является линейной комбинацией векторов из M . Пусть v принадлежит множеству $R \setminus M$, тогда по определению R в множестве M найдется вершина u такая, что $v = u \oplus (i, j, k)$, где $(i, j, k) \in D^C(u)$. Согласно предложению 8 множество $D^P(u)$ содержит в точности $(n-3)/3$ векторов, имеющих единицы в координатах i, j и не пересекающихся по остальным координатам; пусть в множестве $N^P(u)$ им соответствуют вершины $u_1, \dots, u_{\frac{n-3}{3}}$. Тогда в силу четности числа $(n-3)/3$ имеем равенство $(i, j, k) = u_1 \oplus \dots \oplus u_{\frac{n-3}{3}} \oplus 1^n$, в котором правая часть есть линейная комбинация векторов из M . ▲

Характеристический граф рассмотрим как метрическое пространство с естественной метрикой: расстояние между двумя вершинами равно длине кратчайшего пути между ними.

Лемма 2. Пусть M и R – определенные выше i -компоненты кода Препараты P и совершенного кода C соответственно. Множество M является совершенным кодом с расстоянием 3 в характеристическом графе G^R .

Доказательство. Пусть v – произвольный вектор из множества R . Шаром радиуса 1 с центром в вершине v графа G^R является множество $\{v\} \cup N^C(v)$, его мощность равна $(n+1)/2$. Согласно следствию 1 множество M достигает границы сферической упаковки графа G^R шарами радиуса 1 с центрами в вершинах M . Остается показать, что никакие два из этих шаров не пересекаются. Действительно, если для некоторых вершин v_1, v_2 из M соответствующие шары пересекаются, то расстояние $d(v_1, v_2)$ меньше 5, что не верно, поскольку M – подмножество кода Препараты. ▲

Теорема 2. Пусть P – код Препараты, \tilde{R} – произвольная i -компонента совершенного кода $C(P)$. Тогда множество $P \cap \tilde{R}$ образует совершенный код с расстоянием 3 в характеристическом графе $G^{\tilde{R}}$.

Доказательство. Код Препараты P по направлению i разбивается на некоторое число минимальных i -компонент. Каждая из них однозначно достраивается до i -компоненты совершенного кода $C(P)$ способом, описанным в теореме 1. Таким образом, разбиение кода Препараты P на минимальные i -компоненты определяет разбиение совершенного кода $C(P)$ на i -компоненты не обязательно минимальные. Другими словами, характеристический граф любой достроенной i -компоненты может иметь несколько компонент связности. Из леммы 2 следует, что вершины кода Препараты в этих компонентах образуют совершенные коды. Поэтому справедливо, что в каждой компоненте связности графа $G^{C(P)}$ пересечение с кодом Препараты P является совершенным кодом. Утверждение теоремы вытекает из того, что произвольная i -компонента \tilde{R} кода $C(P)$ состоит из объединения минимальных i -компонент, а граф $G^{\tilde{R}}$, соответственно, из объединения компонент связности графа $G^{C(P)}$. ▲

Теорема 2 перекликается с замечанием работы [5] о том, что код Препараты P можно считать равномерно и плотно упакованным в совершенном коде $C(P)$ (в этом случае достаточно в качестве i -компоненты \tilde{R} взять весь код $C(P)$).

Остается заметить, что код Препараты P служит в некотором смысле “каркасом” для построения содержащего его совершенного кода $C(P)$ (см. предложения 4, 5). Теперь мы можем сказать больше: каждая i -компонента кода Препараты P составляет “каркас” некоторой i -компоненты совершенного кода $C(P)$.

Автор выражает глубокую благодарность участникам семинара “Теория кодирования” ИМ СО РАН им. С. Л. Соболева за ценные замечания и предложения.

СПИСОК ЛИТЕРАТУРЫ

1. *Семаков Н.В., Зинovieв В.А., Зайцев Г.В.* Равномерно упакованные коды // Пробл. передачи информ. 1971. Т. 7. № 1. С. 38–50.
2. *Августинoвич С.В., Соловьева Ф.И.* Новые конструкции и свойства совершенных кодов // Тр. Междунар. конф. “Дискретный анализ и исследование операций”. Новосибирск. Июнь, 2000. С. 5–10.
3. *Васильев Ю.Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 337–339.
4. *Etzion T., Vardy A.* Perfect Binary Codes: Constructions, Properties and Enumeration // IEEE Trans. Inform. Theory. 1994. V. 40. № 3. P. 754–763.
5. *Semakov N. V., Zinoviev V. A., Zaitsev G. V.* Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error correcting codes // Proc. Second Int. Sympos. Information Theory. Tsakhadsor, Armenia, 1971. Budapest: Akademia Kiado, 1973. P. 257–263.
6. *Augustinovich S. V., Solov'eva F. I.* Construction of perfect binary codes by the sequential translations of the i -components // Proc. Fifth Int. Workshop “Algebraic and Combinatorial Coding Theory”. Sozopol, Bulgaria. June, 1996. P. 9–13.
7. *Соловьева Ф.И.* О факторизации кодообразующих д.н.ф. // Методы дискретного анализа в исследовании функциональных систем. Новосибирск: Ин-т математики СО АН СССР, 1988. Вып. 47. С. 66–88.
8. *Соловьева Ф.И.* Точные границы связности кодообразующих д.н.ф.: Препринт № 10. Новосибирск: Ин-т математики СО АН СССР, 1990.
9. *Borges J., Phelps K. T., Rifa J., Zinoviev V. A.* On Z_4 -Linear Preparata-Like and Kerdock-Like Codes // IEEE Trans. Inform. Theory. 2003. V. 49. № 11. P. 2834–2843.
10. *Solov'eva F. I.* Structure of i -Components of Perfect Binary Codes // Discrete Appl. Math. 2001. V. 111. P. 189–197.

Токарева Наталья Николаевна
Новосибирский государственный университет
tokareva@ccfit.nsu.ru

Поступила в редакцию
03.11.2003

После переработки
19.02.2004