ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь—декабрь 1999. Серия 1. Том 6, № 4, 44–48

УДК 519.72

О НИЖНЕЙ ОЦЕНКЕ ЧИСЛА СОВЕРШЕННЫХ ДВОИЧНЫХ КОДОВ*)

С. А. Малюгин

Доказывается, что число совершенных двоичных кодов длины n больше $2^{2^{\frac{n+1}{2}-\log(n+1)}} \cdot 2^{2^{\frac{n-3}{4}}}$.

Введение

Ю. Л. Васильевым [2] были впервые построены нелинейные совершенные двоичные коды и получена следующая оценка для числа $F(n)$ совершенных двоичных кодов длины n:

$$F(n) > 2^{2^{\frac{n+1}{2}-\log(n+1)}} \cdot 2^{2^{\frac{n+5}{4}-\log(n+1)}} \tag{1}$$

(в таком виде эта оценка приведена в [5]). Позднее появились другие конструкции совершенных кодов, обзор которых имеется в [3, 4]. Однако количество новых кодов незначительно отличалось от нижней оценки (1). Более высокая оценка была получена в [1]:

$$F(n) > 2^{2^{\frac{n+1}{2}-\log(n+1)}} \cdot 6^{2^{\frac{n+5}{4}-\log(n+1)}}. \tag{2}$$

В настоящей статье мы усиливаем оценку (2) до следующей:

$$F(n) > 2^{2^{\frac{n+1}{2}-\log(n+1)}} \cdot 2^{2^{\frac{n-3}{4}}}. \tag{3}$$

1. Обозначения и основные определения

Пусть E^n — векторное пространство размерности n над полем Галуа $GF(2)$ (его также называют двоичным n-мерным кубом). Сумму векторов $\mathbf{u}, \mathbf{v} \in E^n$ будем обозначать через $\mathbf{u} \oplus \mathbf{v}$. Число ненулевых координат в векторе $\mathbf{u} \in E^n$ называют *весом*. Базисный вектор, у которого i-я координата равна единице, обозначаем через $\mathbf{e}_i$, $i = 1, \ldots, n$. Пусть $n = 2^k - 1$ ($k \in \mathbf{N}$). Множество $C \subseteq E^n$ называется *совершенным кодом* длины n

*) Работа выполнена при финансовой поддержке Федеральной целевой программы «Интеграция» (проект 1997–473).

с расстоянием 3, если в C содержится 2^{n-k} векторов, а расстояние Хэмминга между любыми двумя векторами из C не меньше 3. Совершенный код, являющийся подпространством в E^n, называется *кодом Хэмминга.* Множество ненулевых координат вектора веса 3 из совершенного кода C называется его *тройкой Штейнера.*

Сдвигом множества $S \subseteq E^n$ по координате i называем множество $S \oplus \mathbf{e}_i$. Подмножество S в совершенном коде C называется *i-компонентой* кода C, если множество $C' = (C \setminus S) \cup (S \oplus \mathbf{e}_i)$ является совершенным кодом. Определение i-компоненты и перечисленные ниже свойства имеются в [1] (предложения 6, 8 и 9). Если $S_1, \ldots, S_m$ — такие непересекающиеся подмножества кода C, что S_p является i_p-компонентой кода C для каждого $p = 1, \ldots, m$, то множество

$$C' = \left(C \setminus \bigcup_{p=1}^{m} S_p\right) \cup \left(\bigcup_{p=1}^{m} (S_p \oplus \mathbf{e}_{i_p})\right)$$

является совершенным кодом.

В коде Хэмминга H^n рассмотрим подпространство R_i, порожденное всеми векторами веса 3, в которых i-я координата равна единице. Всевозможные классы смежности $R_i^{\mathbf{u}} = R_i \oplus \mathbf{u}$ $(\mathbf{u} \in H^n)$ представляют собой совокупность всех минимальных по мощности i-компонент кода Хэмминга H^n, $i = 1, \ldots, n$. Введем обозначения: $R_{ij} = R_i \oplus R_j$ и $R_{ijk} = R_i \oplus R_j \oplus R_k$. Если множество индексов $\{i, j, k\}$ является тройкой Штейнера кода H^n, то $R_{ij} = R_{ik} = R_{jk} = R_{ijk}$. В этом случае множество R_{ijk} является (i, j, k)-компонентой, т. е. i-компонентой, j-компонентой и k-компонентой, а размерности пространств R_i и R_{ijk} равны соответственно $(n-1)/2$ и $(3n-5)/4$. Пусть $N_1 = 2^{\frac{n-3}{4}}$ и $N_2 = 2^{\frac{n+5}{4} - \log(n+1)}$. Известно [1], что R_{ijk} разбивается на N_1 непересекающихся i-компонент, а код Хэмминга H^n — на N_2 непересекающихся (i, j, k)-компонент $R_{ijk}^{\mathbf{u}} = R_{ijk} \oplus \mathbf{u}$ $(\mathbf{u} \in H^n)$.

2. Конструкция новых совершенных кодов

Рассматриваемая здесь конструкция является усовершенствованием конструкции кодов, предложенной в [1]. Фиксируем тройку Штейнера $\{i, j, k\}$ и в коде Хэмминга H^n рассмотрим подпространство P, дополнительное к подпространству R_{ijk}, т. е. $R_{ijk} \cap P = \{\mathbf{0}\}$ и $R_{ijk} \oplus P = H^n$. Точно так же в компоненте R_{ijk} выделяем подпространство Q^k, дополняющее R_k. Очевидно, что размерности пространств Q^k и P равны соответственно $\log N_1$ и $\log N_2$. Положив $Q_1 = Q^k$, в Q^k занумеруем все подпространства Q_l размерности $\log N_1 - 1$. Поскольку число таких подпространств равно $N_1 - 1$, то можно считать, что $l = 2, \ldots N_1$. Введя обозначение $Q_l^k = Q_l \cup \left((Q^k \setminus Q_l) \oplus \mathbf{e}_k\right)$, рассмотрим множества $R_{ijk}(l) = Q_l^k \oplus R_k$.

Лемма 1. *При фиксированном k и любом l, $1 \leqslant l \leqslant N_1$, множество $R_{ijk}(l)$ является (i,j,k)-компонентой некоторого кода Хэмминга длины n.*

Доказательство. Линейность множеств Q_l^k и $R_{ijk}(l)$ очевидна. Кроме этого, в силу предложений 2 и 3 из [1] множество $R_{ijk}(l)$ является (i,j,k)-компонентой в любом коде, в частности в линейном коде $R_{ijk}(l) \oplus P$, который может быть получен из кода H^n сдвигами его k-компонент, пересекающихся с множеством $(Q^k \setminus Q_l) \oplus P$. Лемма доказана.

В силу леммы 1 компонента $R_{ijk}(l)$ распадается на i-компоненты $R_i^q(l)$ и j-компоненты $R_j^q(l)$, $q = 1, \ldots, N_1$, кода Хэмминга $R_{ijk}(l) \oplus P$. Для любых функций

$$\mu : P \longrightarrow \{i,j\},$$
$$\nu : P \longrightarrow \{1,\ldots,N_1\},$$
$$\lambda : P \times \{1,\ldots,N_1\} \longrightarrow \{0,1\}$$

образуем множества

$$P^{\mathbf{u}}_{\mu,\nu,\lambda} = \bigcup_{q=1}^{N_1} \left(R^q_{\mu(\mathbf{u})}(\nu(\mathbf{u})) \oplus \lambda(\mathbf{u},q)\mathbf{e}_{\mu(\mathbf{u})} \oplus \mathbf{u} \right) (\mathbf{u} \in P),$$
$$C_{\mu,\nu,\lambda} = \bigcup \left\{ P^{\mathbf{u}}_{\mu,\nu,\lambda} : \mathbf{u} \in P \right\}.$$

Из определения видно, что множество $C_{\mu,\nu,\lambda}$ получается двумя последовательными сдвигами кода H^n. Сначала сдвигами непересекающихся k-компонент кода H^n мы можем построить код $C_{\mu,\nu,0}$. Затем, сдвигая непересекающиеся i-компоненты и j-компоненты этого кода, можно получить требуемое множество $C_{\mu,\nu,\lambda}$. Таким образом, справедливо следующее утверждение, аналогичное лемме 11 и теореме 1 из [1].

Лемма 2. *Для любых функций μ, ν и λ множество $C_{\mu,\nu,\lambda}$ является совершенным кодом.*

Набор функций (μ,ν,λ) называем *вырожденным*, если существует $\mathbf{u} \in P$ такое, что $\lambda(\mathbf{u},q)$ является постоянной по переменной q. В противном случае набор (μ,ν,λ) называем *невырожденным*.

Лемма 3. *Если для двух невырожденных наборов (μ,ν,λ) и (μ',ν',λ') имеет место равенство $C_{\mu,\nu,\lambda} = C_{\mu',\nu',\lambda'}$, то $(\mu,\nu,\lambda) = (\mu',\nu',\lambda')$.*

Доказательство. Из невырожденности набора (μ,ν,λ) следует, что для любого $\mathbf{u} \in P$ существует вектор $\mathbf{v} \in P^{\mathbf{u}}_{\mu,\nu,\lambda} \cap H^n$. Рассмотрим k-компоненту $R^{\mathbf{v}}_k$ кода H^n. Ясно, что при построении кодов $C_{\mu,\nu,\lambda}$ и $C_{\mu',\nu',\lambda'}$ некоторые векторы из компоненты $R^{\mathbf{v}}_k$ не сдвигаются, а другие сдвигаются на вектор $\mathbf{e}_{\mu(\mathbf{u})}$ для кода $C_{\mu,\nu,\lambda}$ и на вектор $\mathbf{e}_{\mu'(\mathbf{u})}$ для

кода $C_{\mu',\nu',\lambda'}$. Поэтому из равенства $C_{\mu,\nu,\lambda} = C_{\mu',\nu',\lambda'}$ следует равенство $\mu(\mathbf{u}) = \mu'(\mathbf{u})$. Теперь рассмотрим компоненту $R^q_{\mu(\mathbf{u})}(l) \oplus \mathbf{u}$, содержащую вектор $\mathbf{v}$, где $l = \nu(\mathbf{u})$. Пусть $l' = \nu'(\mathbf{u})$. Докажем, что $l = l'$. Если это не так, то при $l' > 1$ существует вектор $\mathbf{w} \in (Q^k_l \setminus Q^k_{l'}) \oplus \mathbf{u}$ (в случае $l' = 1$ мы лишь меняем ролями l и l'). Рассмотрим k-компоненту $R^{\mathbf{w}}_k$ кода H^n. Она также является k-компонентой линейного кода $R_{ijk}(l) \oplus P$. Компонента $R^{\mathbf{u}}_{ijk}(l)$ распадается на $\mu(\mathbf{u})$-компоненты, одной из которых является $R^q_{\mu(\mathbf{u})}(l) \oplus \mathbf{u}$. При построении $C_{\mu,\nu,\lambda}$ эта компонента не сдвигается. Поэтому пересечение $(R^q_{\mu(\mathbf{u})}(l) \oplus \mathbf{u}) \cap R^{\mathbf{w}}_k$ является частью кода $C_{\mu,\nu,\lambda}$. Любой вектор $\mathbf{w}' \in (R^q_{\mu(\mathbf{u})}(l) \oplus \mathbf{u}) \cap R^{\mathbf{w}}_k$ не принадлежит множеству $Q^k_{l'} \oplus R^{\mathbf{u}}_k$. Поэтому при построении кода $C_{\mu',\nu',\lambda'}$ он сдвигается либо на $\mathbf{e}_k$, либо на $\mathbf{e}_k \oplus \mathbf{e}_{\mu(\mathbf{u})}$, что противоречит совпадению кодов. Следовательно, $Q^k_l \subseteq Q^k_{l'}$. Но из совпадения размерностей пространств Q^k_l, $Q^k_{l'}$ следует равенство $l = l'$. Поэтому набор компонент $\{R^q_{\mu(\mathbf{u})}(l) \oplus \mathbf{u} \mid q = 1, \ldots, N_1\}$ совпадает с набором компонент $\{R^{q'}_{\mu'(\mathbf{u})}(l') \oplus \mathbf{u} \mid q' = 1, \ldots, N_1\}$. Из равенства $C_{\mu,\nu,\lambda} = C_{\mu',\nu',\lambda'}$ следует, что по координате $\mu(\mathbf{u}) = \mu'(\mathbf{u})$ должны сдвигаться компоненты в каждом из наборов с одними и теми же индексами q и q'. Это означает, что $\lambda(\mathbf{u}, q) = \lambda'(\mathbf{u}, q)$. Лемма доказана.

Теорема. *Число совершенных двоичных кодов длины n больше*

$$2^{2^{\frac{n+1}{2} - \log(n+1)}} \cdot 2^{2^{\frac{n-3}{4}}}.$$

Доказательство. С одной стороны, число всех наборов (μ, ν, λ) очевидно равно

$$(2N_1)^{N_2} \cdot 2^{N_1 N_2} = 2^{2^{\frac{n+1}{2} - \log(n+1)}} \cdot 2^{2^{\frac{n-3}{4}}}.$$

С другой стороны, число всех вырожденных наборов (μ, ν, λ) не больше

$$2N_2 \cdot 2^{N_1(N_2-1)} \cdot (2N_1)^{N_2}.$$

Теперь, как и в [1], рассмотрим еще одну тройку Штейнера $\{i', j', k'\}$, не пересекающуюся с тройкой $\{i, j, k\}$, и определим по ней новое семейство кодов $\{C_{\mu',\nu',\lambda'}\}$, которое пересекается с первоначальным семейством по единственному коду H^n. Так как число различных кодов второго семейства больше числа вырожденных троек (μ, ν, λ) и (μ', ν', λ'), то теорема доказана.

Автор выражает благодарность С. В. Августиновичу и Ф. И. Соловьевой за интерес к этой работе и полезные обсуждения.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьева Ф. И.** Построение совершенных двоичных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент // Проблемы передачи информации. 1997. Т. 33, вып. 3. С. 15–21.

2. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 75–78.
3. **Cohen G., Honkala I., Litsyn S., Lobstein A.** Covering Codes. North-Holland: Elsevier, 1998.
4. **Solov'eva F. I.** Constructions of perfect binary codes // Preprint 98–042. Univ. Bielefeld, 1998. 12 p.
5. **Vasil'ev Y. L., Solov'eva F. I.** Interdependence between perfect binary codes and their projections // Proc. Seventh Joint Swedish-Russian Intern. Workshop on Inform. Theory (St.-Peterburg, Russia. June, 1995). Moscow, 1995. P. 239–242.

Адрес автора:

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

Статья поступила
3 августа 1999 г.