ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—август 2014. Том 21, № 4. С. 54–61

УДК 519.8

АФФИННО 3-НЕСИСТЕМАТИЧЕСКИЕ КОДЫ *)

С. А. Малюгин

Аннотация. Совершенный двоичный код C длины $n = 2^k - 1$ называется *аффинно* 3-*систематическим*, если в пространстве $\{0,1\}^n$ существует трёхмерное подпространство L такое, что любой его смежный класс $L + u$ либо не пересекается с кодом C, либо пересекается с ним ровно по одному элементу. В противном случае код C называется *аффинно* 3-*несистематическим*. В настоящей работе строятся аффинно 3-несистематические коды длины $n = 2^k - 1$, $k > 4$.

Ключевые слова: совершенный код, код Хемминга, несистематический код, аффинно несистематический код, аффинно 3-несистематический код, компонента.

Введение

Пусть $\{0,1\}^n$ — векторное пространство над полем из двух элементов 0 и 1. По определению это пространство состоит из всех последовательностей вида $u = (u_1, \ldots, u_n)$, где $u_i \in \{0,1\}$. Сумма векторов $u, v \in \{0,1\}^n$ определяется формулой $u+v = (u_1 \oplus v_1, \ldots, u_n \oplus v_n)$, где $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ и $u_i \oplus v_i$ — сумма элементов $u_i, v_i \in \{0,1\}$ в поле Галуа $GF(2)$ ($0 \oplus 0 = 0$, $1 \oplus 0 = 0 \oplus 1 = 1$, $1 \oplus 1 = 0$). Далее всегда будем рассматривать в пространстве $\{0,1\}^n$ стандартный базис $e_1, \ldots, e_n$, где $e_i = \big(0, \ldots, \underset{i}{1}, \ldots, n\big)$. Нулевой и единичный векторы обозначаем через $\mathbf{0}$ и $\mathbf{1}$. Число ненулевых координат вектора u называется его *весом*. *Носитель* вектора $u \in \{0,1\}^n$ — множество индексов i таких, что $u_i = 1$ — обозначается через $[u]$.

В коде Хемминга H^n рассмотрим подпространство R_i, порождённое всеми векторами веса 3 с i-й координатой, равной единице. Всевозможные смежные классы вида $R_i^u = R_i + u$, $u \in H^n$, называются i-*компонентами* кода H^n, $i = 1, \ldots, n$. Рассмотрим некоторое семейство $\mathcal{B} = \big\{R_{i_1}^{u_1}, \ldots, R_{i_m}^{u_m}\big\}$, состоящее из попарно не пересекающихся i_p-компонент, где

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 11–01–00997, 13–01–00463).

$u_p \in H^n$, $p = 1, \ldots, m$. Одна из основных конструкций нелинейных совершенных двоичных кодов состоит в том, что в коде H^n сдвигаются по координатам i_p все компоненты из семейства $\mathcal{B}$, т. е. множество

$$H^n(\mathcal{B}) = \left(H^n \setminus \bigcup_{p=1}^{m} R_{i_p}^{u_p} \right) \cup \left(\bigcup_{p=1}^{m} \left(R_{i_p}^{u_p} \oplus e_{i_p} \right) \right) \tag{1}$$

— совершенный код [1, 6, 9, 11]. Далее будем говорить, что код $H^n(\mathcal{B})$ построен из кода Хемминга H^n сдвигами компонент из семейства $\mathcal{B}$.

Совершенный двоичный код $C \subset \{0,1\}^n$ длины $n = 2^k - 1$ называется *систематическим*, если существует k-элементное подмножество $K \subset \{1, \ldots, n\}$ такое, что любые два неравных вектора $u, v \in C$ различаются хотя бы в одной координате с номером, не принадлежащим K. В противном случае код C называется *несистематическим*. Несистематические совершенные двоичные коды длины $n \geqslant 255$ впервые построены в [1] сдвигами i-компонент кода H^n для i, пробегающих все значения из $\{1, \ldots, n\}$. В [10] предложена модификация конструкции [1], позволяющая строить такие коды для всех $n \geqslant 63$. Для $n = 15$ и $n = 31$ несистематические коды найдены с помощью компьютера [6, 10].

В этой работе рассматривается более сильное понятие несистематичности.

Определение 1. Совершенный двоичный код C длины $n = 2^k - 1$ называется *аффинно t-систематическим*, если в пространстве $\{0,1\}^n$ существует t-мерное подпространство L такое, что любой его смежный класс $L + u$ либо не пересекается с кодом C, либо пересекается с ним ровно по одному элементу. В противном случае код C называем *аффинно t-несистематическим*.

Легко заметить, что совершенный двоичный код C аффинно t-систематический тогда и только тогда, когда существует t-мерное подпространство $L \subset \{0,1\}^n$ такое, что $L \cap (C + C) = \{\mathbf{0}\}$.

Если $t = k = \log(n+1)$, то аффинно t-систематический (аффинно t-несистематический) код называем просто *аффинно систематическим* (*аффинно несистематическим*). Определение аффинной систематичности предложено С. В. Августиновичем. Это свойство является аффинным инвариантом кода, т. е. оно сохраняется при любых невырожденных аффинных преобразованиях пространства $\{0,1\}^n$. С. В. Августиновичем также поставлен вопрос о существовании аффинно несистематических кодов. Ответ на него анонсирован в [3]. В [4] аффинно несистематические коды построены для всех $n = 2^k - 1$, $k \geqslant 4$. Из определения 1 следует,

что любой аффинно t-несистематический код является также аффинно t'-несистематическим при любом $t' \geqslant t$. При $t > k$ (при $t < 3$) любой совершенный код длины $n = 2^k - 1$ аффинно t-несистематический (аффинно t-систематический). Поэтому естественно рассматривать далее только нетривиальные случаи, когда $3 \leqslant t \leqslant k$. Случай $t = k$ (аффинной несистематичности) рассмотрен в [4]. В настоящей работе рассматривается другой крайний случай $t = 3$.

1. Конструкция аффинно 3-несистематических кодов

На множестве индексов $\{0, 1, \ldots, n\}$, $n = 2^k - 1$, можно ввести структуру линейного пространства следующим образом. Пусть $i = i_1 \ldots i_k$ — представление числа $0 \leqslant i \leqslant n$ в двоичной системе. *Бинарной* суммой $i \oplus j$ чисел $0 \leqslant i, j \leqslant n$ называется число, двоичное представление которого есть побитовая сумма двоичных представлений чисел i и j. Таким образом на множестве индексов $\{0, 1, \ldots, n\}$, $n = 2^k - 1$, вводится структура линейного пространства. При этом код Хемминга H^n определяется как множество всех векторов $u = (u_1, \ldots, u_n) \in \{0,1\}^n$, для которых $\bigoplus\limits_{i=1}^{n} u_i i = 0$.

k-Мерное подпространство $Q \subset \{0,1\}^n$ называем *дополнительным к коду Хемминга* H^n, если $Q \cap H^n = \{\mathbf{0}\}$. Так как $Q + H^n = \{0,1\}^n$, дополнительное подпространство Q пересекается с каждым смежным классом $H^n + e_i$ по единственному ненулевому элементу q_i, $i = 1, \ldots, n$.

Пусть $Q = \{q_0, q_1, \ldots, q_n\}$ — дополнительное подпространство к коду Хемминга H^n, где $q_0 = \mathbf{0}$, $q_i \in H^n + e_i$, $1 \leqslant i \leqslant n$. Тогда $q_{i \oplus j} = q_i + q_j$ для всех $1 \leqslant i, j \leqslant n$ (см. [4, лемма 1]).

Определение 2. Множество индексов $I = \{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$ называем *аффинно систематическим*, если существует такое дополнительное к коду Хемминга k-мерное подпространство $Q = \{q_0, q_1, \ldots, q_n\}$ ($q_0 = \mathbf{0}$), что $q_i \in H^n + e_i$, $i = 1, \ldots, n$, и $q_{i_s} \in R_{i_s} + e_{i_s}$, $s = 1, \ldots, m$, где R_{i_s} — i_s-компоненты кода Хемминга, содержащие нулевой вектор, $s = 1, \ldots, m$. В противном случае называем множество I *аффинно несистематическим*.

Множество всех векторов пространства $\{0,1\}^n$ разбивается на орбиты относительно группы перестановочных автоморфизмов $\mathrm{Sym}(H^n)$ кода Хемминга H^n. В определении 3 из [2] орбита, носители всех векторов которой являются систематическими множествами, названа систематической, а орбита, для которой это свойство не выполняется, несистематической. Согласно этой терминологии будем называть орбиту, носители

всех векторов которой являются аффинно систематическими множествами, *аффинно систематической*, а орбиту, для которой это свойство не выполнено, *аффинно несистематической*.

Как отмечено ранее, множество индексов $\{0,\dots,n\}$ тоже является линейным пространством размерности k, $n=2^k-1$, которое для краткости будем обозначать через $\{0,1\}^k$. Рассмотрим в этом пространстве некоторое подмножество $I=\{i_1,\dots,i_m\}$, ранг которого равен $r<k$. Выделим в I некоторый базисный набор $\{i_1,\dots,i_r\}$ и рассмотрим в $\{0,1\}^k$ подпространство M, порождённое векторами $i_1,\dots,i_r$. Пусть $n'=2^r-1$. В коде Хемминга H^n можно рассмотреть подкод $H^{n'}_M$, состоящий из всех векторов кода H^n, носители которых входят в $M\setminus\{0\}$. Очевидно, что этот подкод эквивалентен стандартному коду Хемминга $H^{n'}$ длины n'. Если множество индексов $I=\{i_1,\dots,i_m\}$ входит в $M\setminus\{0\}$, то можем говорить о его аффинной систематичности (или несистематичности) как относительно кода H^n, так и относительно кода $H^{n'}_M$. В лемме 3 из [4] доказано, что множество I аффинно систематическое относительно кода $H^{n'}_M$ тогда и только тогда, когда оно аффинно систематическое относительно кода H^n.

Рассмотрим любое семейство $\mathcal{B}=\left\{R^{u_1}_{i_1},\dots,R^{u_m}_{i_m}\right\}$ из попарно не пересекающихся компонент кода Хемминга H^n. Обозначим через $I(\mathcal{B})$ множество всех индексов i, для которых существуют i-компоненты, принадлежащие семейству $\mathcal{B}$.

Говорим, что семейство непересекающихся компонент $\mathcal{B}=\left\{R^{u_1}_{i_1},\dots,R^{u_m}_{i_m}\right\}$ *не имеет кратных компонент*, если все индексы $i_1,\dots,i_m$ различны. В этом случае $I(\mathcal{B})=\{i_1,\dots,i_m\}$.

Пусть $E(\mathcal{B})=H^n\setminus\left(\bigcup\limits_{p=1}^{m}R^{u_p}_{i_p}\right)$ — часть кода H^n, не занятая компонентами из семейства $\mathcal{B}$.

Рассмотрим следующие два условия на семейство компонент $\mathcal{B}$:

(a) для любого индекса $i_p\in I(\mathcal{B})$ и любого вектора $q\in H^n\setminus R_{i_p}$ пересечение $E(\mathcal{B})\cap R^{u_p+q}_{i_p}$ непусто;

(b) $H^n=E(\mathcal{B})+E(\mathcal{B})$.

В [4] доказано, что если $n=2^k-1>15$ и семейство компонент $\mathcal{B}$ не имеет кратных компонент, то для него выполняются условия (a) и (b).

Теперь всё готово для построения аффинно 3-несистематических кодов. В коде Хемминга H^n рассмотрим любое семейство из n непересекающихся компонент $\mathcal{B}_n$, не имеющее кратных компонент, т. е. $\mathcal{B}_n=\left\{R^{u_1}_1,\dots,R^{u_n}_n\right\}$ (нижний индекс указывает на число компонент в семействе).

Теорема 1. *Пусть* $\mathcal{B}_n = \left\{R_1^{u_1}, \ldots, R_n^{u_n}\right\}$ *— семейство из* n *непересекающихся* i*-компонент кода Хемминга* H^n, $i = 1, \ldots, n$. *Тогда совершенный двоичный код* $H^n(\mathcal{B}_n)$ *при* $n > 15$ *аффинно* 3*-несистематический.*

Доказательство. Рассмотрим в $\{0,1\}^n$ любое трёхмерное подпространство L. Пусть $u \in L \cap H^n$ и $u \neq \mathbf{0}$. Из свойства (b) следует, что $u \in E(\mathcal{B}_n)+E(\mathcal{B}_n) \subset (C+C)$, т. е. $L \cap (C+C) \neq \{\mathbf{0}\}$. В случае $L \cap H^n = \{\mathbf{0}\}$ можно расширить подпространство L до k-мерного подпространства Q, дополнительного к коду Хемминга H^n. Пусть $Q = \{q_0, q_1, \ldots, q_n\}$, где $q_0 = \mathbf{0}$, $q_i \in H^n + e_i$, $1 \leqslant i \leqslant n$. Подпространство L является частью этого множества, т. е. $L = \{q_0, q_{i_1}, \ldots, q_{i_7}\}$. В силу леммы 1 из [4] множество $M = \{0, i_1, \ldots, i_7\}$ является подпространством в пространстве индексов $\{0, 1, \ldots, n\}$ (изоморфном пространству $\{0,1\}^k$). Поэтому множество $\{i_1, \ldots, i_7\}$ аффинно несистематическое (как в коде H_M^7, так и в содержащем его коде H^n). Вектор с носителем $\{i_1, \ldots, i_7\}$ принадлежит орбите O_7^1. В силу лемм 3 и 4 из [4] орбита O_7^1 аффинно несистематическая. Поэтому для некоторого номера s, $1 \leqslant s \leqslant 7$, имеем $q_{i_s} \notin R_{i_s} + e_{i_s}$. По условию (a) существует вектор $v \in E(\mathcal{B}_n) \cap R_{i_s}^{u_{i_s}+q_{i_s}+e_{i_s}}$. Тем самым $v \in H^n(\mathcal{B}_n)$ и $w = v + q_{i_s} \in R_{i_s}^{u_{i_s}} + e_{i_s} \subset H^n(\mathcal{B}_n)$. Стало быть, $v + w = q_{i_s} \in L$. Теорема 1 доказана.

Известно, что семейства из n непересекающихся компонент без кратных компонент существуют в коде Хемминга H^n при любом $n > 15$ [1, 9]. Поэтому из теоремы 1 вытекает

Следствие 1. *Аффинно* 3*-несистематические коды длины* $n = 2^k - 1$ *существуют при любом* $k > 4$. *При этом несистематические коды, построенные в* [1, 9] (*при* $n > 15$), *аффинно* 3*-несистематические.*

2. Аффинно несистематические аффинно 3-систематические коды

Следуя [1] говорим, что совершенный код C *имеет полную систему троек*, если множество $C + C$ содержит все векторы веса 3 из $\{0,1\}^n$.

Лемма 1. *Если совершенный двоичный код* C *аффинно* 3*-несистематический, то* C *имеет полную систему троек.*

Доказательство. Любой вектор $u \in \{0,1\}^n$ веса 3 представляется при некоторых $i_1, i_2, i_3 \in \{1, \ldots, n\}$ в виде $u = e_{i_1} + e_{i_2} + e_{i_3}$. Трёхмерное подпространство L, порождённое базисными векторами $e_{i_1}, e_{i_2}, e_{i_3}$, должно пересекаться с множеством $C + C$ по некоторому ненулевому вектору v. Так как для кода C с расстоянием 3 множество $C + C$ не содержит

векторов веса 1 и 2, то $v = u$, т. е. множеству $C + C$ принадлежат все векторы веса 3. Лемма 1 доказана.

Из леммы 1 следует, что свойство аффинной 3-несистематичности кода является существенным усилением свойства кода иметь полную систему троек.

Определение 3. Семейство компонент $\mathcal{B} = \{R_{i_1}^{u_1}, \ldots, R_{i_m}^{u_m}\}$ называем *d-разделённым*, если расстояние Хемминга между любой парой компонент из $\mathcal{B}$ больше d.

Семейства из 4-разделённых компонент впервые использовались в [1] для построения несистематических кодов.

Теорема 2. *Пусть $\mathcal{B} = \{R_{i_1}^{u_1}, \ldots, R_{i_m}^{u_m}\}$ — 5-разделённое семейство компонент. Если $|I(\mathcal{B})| < n$, то совершенный код $C = H^n(\mathcal{B})$ аффинно 3-систематический.*

Доказательство. Рассмотрим любое 5-разделённое семейство компонент $\mathcal{B} = \{R_{i_1}^{u_1}, \ldots, R_{i_m}^{u_m}\}$. Пусть $i \notin I(\mathcal{B})$. Существует вектор $u \in H^n$ веса 4, у которого i-я координата равна 1, т. е. $u = e_i + e_{j_1} + e_{j_2} + e_{j_3}$. Пусть $v = e_{j_1} + e_{j_2} + e_{j_3}$. Допустим, что $v \in (C + C)$. Так как $i \notin I(\mathcal{B})$, должно быть $v \in \left(R_{i_p}^{u_p} + e_{i_p}\right) + \left(R_{i_q}^{u_q} + e_{i_q}\right)$ при некоторых i_p, i_q таких, что $i_p \oplus i_q = i$. Так как минимальный вес векторов из $R_{i_p}^{u_p} + R_{i_q}^{u_q}$ не меньше 6, минимальный вес вектора v не меньше 4. Это противоречие доказывает, что $v \notin (C + C)$, т. е. код C имеет неполную систему троек, и из леммы 1 следует, что он аффинно 3-систематический. Теорема 2 доказана.

Из мощностных оценок, аналогичных оценкам из [1], следует, что 5-разделённые семейства из 7 непересекающихся компонент существуют в любом коде Хемминга H^n, если $n \geqslant 31$, $k \geqslant 5$. Если ограничиться только семействами $\mathcal{B}$, состоящими из 7 непересекающихся компонент, то требование 5-удалённости лишнее.

Теорема 3. *Пусть $\mathcal{B} = \{R_{i_1}^{u_1}, \ldots, R_{i_7}^{u_7}\}$ — семейство из 7 непересекающихся компонент. Если $n \geqslant 31$, то совершенный код $C = H^n(\mathcal{B})$ аффинно 3-систематический.*

Доказательство. Если множество $I(\mathcal{B})$ аффинно систематическое, то по теореме 1 из [4] код $C = H^n(\mathcal{B})$ аффинно систематический. Следовательно, он является также аффинно 3-систематическим. Если $I(\mathcal{B})$ принадлежит одной из аффинно несистематических орбит O_7^1 или O_7^3, то по теореме 2 и лемме 4 из [4] код $H^n(\mathcal{B})$ аффинно несистематический. Более того, существует индекс $i \notin I(\mathcal{B})$ такой, что $i \neq i_p \oplus i_q$ ни для каких $i_p, i_q \in I(\mathcal{B})$. В случае орбиты O_7^1 (случай плоскости Фано) это

верно для всех индексов $i \notin I(\mathcal{B})$. Снова рассмотрим в H^n любой вектор вида $u = e_i + e_{j_1} + e_{j_2} + e_{j_3}$. Если $v = u + e_i \in (C + C)$, то должно быть $v \in \left(R_{i_p}^{u_p} + e_{i_p}\right) + \left(R_{i_q}^{u_q} + e_{i_q}\right)$ при некоторых $i_p, i_q \in I(\mathcal{B})$, $i_p \oplus i_q = i$. По вышесказанному таких индексов i_p, i_q не существует. Поэтому $v \notin (C + C)$ и код $C = H^n(\mathcal{B})$ имеет неполную систему троек, т. е. он аффинно 3-систематический. Теорема 3 доказана.

Одним из преимуществ теоремы 3 является то, что она справедлива также при $n = 15$. Так как в коде Хемминга существует семейство компонент $\mathcal{B} = \left\{R_{i_1}^{u_1}, \ldots, R_{i_7}^{u_7}\right\}$, для которого $I(\mathcal{B})$ принадлежит аффинно несистематической орбите O_7^3, код $H^{15}(\mathcal{B})$ аффинно несистематический аффинно 3-систематический. В классификации, полученной в [5], существует 6 попарно не эквивалентных несистематических кодов, имеющих неполную систему троек. Отметим, что всего существует 13 неэквивалентных несистематических кодов длины 15. Один из них, найденный в [7, 8] в результате компьютерного перечисления всех кодов длины 15, аффинно систематический. Ещё 12 несистематических кодов, перечисленных в [5], аффинно несистематические [4]. Среди этих кодов есть 6 кодов, имеющих полную систему троек. Из них 4 кода аффинно 3-несистематические (более подробно эти результаты будут изложены в следующей публикации). Теперь, подводя итоги, можно сформулировать

Следствие 2. *Для любого $n = 2^k - 1$, $k \geqslant 4$, существуют аффинно несистематические 3-систематические коды.*

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьева Ф. И.** О несистематических совершенных двоичных кодах // Пробл. передачи информ. — 1996. — Т. 32, вып. 3. — С. 47–50.
2. **Малюгин С. А.** Несистематические совершенные двоичные коды // Дискрет. анализ и исслед. операций. Сер. 1. — 2001. — Т. 8, № 1. — С. 55–76.
3. **Малюгин С. А.** Об аффинно несистематических кодах // Сб. докл. междунар. конф., посвящённой 90-летию со дня рождения А. А. Ляпунова (Новосибирск, 8–12 октября 2001 г.). — Новосибирск: Ин-т математики СО РАН, 2001. — С. 393–394. (http://www.sbras.nsc.ru/ws/ Lyap2001/2288)
4. **Малюгин С. А.** Аффинно несистематические коды // Дискрет. анализ и исслед. операций. — 2012. — Т. 19, № 4. — С. 73–85.
   Malyugin S. A. Affine nonsystematic codes // J. Appl. Industr. Math. — 2012. — Vol. 6, N 4. — P. 451–459.

5. **Малюгин С. А.** О перечислении неэквивалентных совершенных двоичных кодов длины 15 и ранга 15 // Дискрет. анализ и исслед. операций. Сер. 1. — 2006. — Т. 13, № 1. — С. 77–98.
Malyugin S. A. On enumeration of nonequivalent perfect binary codes of length 15 and rank 15 // J. Appl. Industr. Math. — 2007. — Vol. 1, N 1. — P. 77–80.
6. **Романов А. М.** О несистематических совершенных кодах длины 15 // Дискрет. анализ и исслед. операций. Сер. 1. — 1997. — Т. 4, № 4. — С. 75–78.
7. **Östergård P. R. J., Pottonen O.** The perfect binary one-error-correcting codes of length 15. Part I — classification // IEEE Trans. Inform. Theory. — 2009. — Vol. 55, N 10. — P. 4657–4660.
8. **Östergård P. R. J., Pottonen O., Phelps K. T.** The perfect binary one-error-correcting codes of length 15. Part II — properties // IEEE Trans. Inform. Theory. — 2009. — Vol. 56, N 6. — P. 2571–2582.
9. **Phelps K. T., LeVan M. J.** Kernels of nonlinear Hamming code // Des., Codes Criptogr. — 1995. — Vol. 6, N 3. — P. 247–257.
10. **Phelps K. T., Le Van M. J.** Nonsystematic perfect codes // SIAM J. Discrete Math. — 1999. — Vol. 12, N 1. — P. 27–34.
11. **Solov'eva F. I.** Switchings and perfect codes // Numbers, Information and Complexity. — Dordrecht: Kluwer Acad. Publ., 2000. — P. 311–324.

Малюгин Сергей Артемьевич,
e-mail: mal@math.nsc.ru

Статья поступила
23 декабря 2013 г.

Переработанный вариант —
17 января 2014 г.