2014 Прикладная теория кодирования и сжатия информации № 4(26)

DOI 10.17223/20710410/26/8

УДК 519.72

О РАДИУСЕ ПОКРЫТИЯ ЛИНЕЙНЫХ КОДОВ, ПОРОЖДЁННЫХ АФФИННЫМИ ГЕОМЕТРИЯМИ НАД ПОЛЕМ ИЗ ЧЕТЫРЁХ ЭЛЕМЕНТОВ

М. Э. Коваленко

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

E-mail: kovalenkomaryana@gmail.com

Рассматриваются линейные коды, порождённые аффинными геометриями над полем из четырёх элементов. Для данных кодов приводятся некоторые свойства и вычисляется точное значение радиуса покрытия равное 4.

Ключевые слова: *линейные коды, конечные аффинные геометрии, радиус покрытия, покрывающие коды.*

Введение и основные определения

Аффинная геометрия $\mathbb{EG}(n, p^s)$ представляет собой аффинное пространство $\mathbb{F}_{p^s}^n$, т. е. точки — это векторы из $\mathbb{F}_{p^s}^n$; прямые — одномерные подпространства $\mathbb{F}_{p^s}^n$ и их смежные классы (по операции сложения векторов); d-мерные плоскости — d-мерные подпространства $\mathbb{F}_{p^s}^n$ и их смежные классы. В работе используется ряд терминов, связанных с конечными геометриями, их можно найти, например, в [1].

Определение 1. *Матрицей инцидентности* аффинной геометрии называется матрица, строки и столбцы которой сопоставлены прямым и точкам аффинной геометрии соответственно, а элемент в пересечении строки b и столбца p равен 1, если точка p лежит на прямой b, и 0 иначе.

Рассмотрим строки матрицы инцидентности $\mathbb{EG}(h, 4)$ как двоичные векторы. Они порождают линейное подпространство $\mathbb{C}_h \subset \mathbb{F}_2^{4^h}$. По определению $\mathbb{C}_h$ является двоичным линейным кодом длины 4^h.

Расстоянием (*Хэмминга*) между двумя векторами из $\mathbb{F}_2^{4^h}$ называется количество координат, в которых они отличаются. Для каждого вектора пространства $\mathbb{F}_2^{4^h}$, не лежащего в $\mathbb{C}_h$, можно выбрать минимальное расстояние среди всех расстояний от него до каждого из векторов $\mathbb{C}_h$. Максимум из всех этих расстояний называется *радиусом покрытия* линейного кода. Обозначим его $r(\mathbb{C}_h)$. Для векторов $\mathbb{C}_h$ выберем минимальное расстояние между двумя различными векторами, это расстояние называется *кодовым*. Более подробно с приведёнными понятиями можно ознакомиться в [1, 2].

В работе исследуется вопрос нахождения точного значения радиуса покрытия кода $\mathbb{C}_h$, а именно доказывается, что при любой размерности кода радиус его покрытия равен 4.

Вопрос нахождения радиуса покрытия кода является одной из версий классической задачи покрытия: *даны n и r; какое наименьшее число шаров радиуса r в метрике Хэмминга можно разместить в n-мерном пространстве так, чтобы каждый вектор пространства принадлежал хотя бы одному из них.* С большей частью результатов, посвящённых покрывающим кодам, можно ознакомиться в [2].

Приведём некоторые свойства кодов $\mathbb{C}_h$, необходимые для дальнейшей работы.

Лемма 1. В коде $\mathbb{C}_h$ нет векторов нечётного веса и векторов веса 2.

Доказательство. Первая часть леммы очевидна, поскольку в силу строения порождающей матрицы базис подпространства составляют векторы веса 4. Докажем вторую часть.

Предположим, что в коде лежит вектор веса 2. Выберем соответствующую ему пару точек из $\mathbb{F}_4^h$, а у этих двух точек — координату, по которой они отличаются. Пусть это координата y_i, и у первой точки $y_{i,1} = \alpha$, а у второй $y_{i,2} = \beta$. Тогда красим гиперплоскость $\{y_i = \alpha\}$ в красный цвет, а $\{y_i = \beta\}$ — в синий. Из оставшихся двух гиперплоскостей ещё одну красим в синий и одну в красный. Итак, по фиксированной координате покрасили половину точек в красный, половину в синий цвет.

Любая прямая или целиком лежит в одной из этих плоскостей, или пересекает все четыре, а значит, содержит чётное число точек каждого цвета. Таким образом, прибавление векторов, соответствующих прямым, не изменит чётности количества точек каждого цвета, входящих в набор, то есть не существует линейной комбинации векторов, соответствующих прямым пространства $\mathbb{F}_4^h$, которая даёт выбранную пару точек, что противоречит предположению. ■

Замечание 1. Поскольку в выбранном коде лежит нулевой вектор и не лежат векторы веса 2, то кодовое расстояние данного кода равно 4.

1. Совокупность всех подмножеств $\mathbb{F}_4^h$ как векторное пространство над $\mathbb{F}_2$

Рассмотрим совокупность всех подмножеств множества $\mathbb{F}_4^h$ как векторное пространство над $\mathbb{F}_2$ с операцией симметрической разности. При этом под суммой прямых, точек и других подмножеств будем понимать сумму в смысле указанного векторного пространства. Такая операция устроена простым образом: точка из $\mathbb{F}_4^h$ принадлежит множеству, являющемуся результатом суммирования, тогда и только тогда, когда она принадлежит нечётному количеству множеств-слагаемых. В терминах такого пространства можно задавать вопросы, свойственные произвольным векторным пространствам: как выглядят порождающие системы векторов, какова размерность линейной оболочки данного набора векторов, можно ли один вектор выразить через другие (т. е. представить линейной комбинацией) и так далее. Обозначим это векторное пространство $\mathcal{A}(h)$ и $x_i(a)$ — i-ю координату элемента $a \in A \in \mathcal{A}(h)$ или, что то же самое, $a \in \mathbb{F}_4^h$. В пространстве $\mathcal{A}(h)$ выберем базис из одноточечных множеств e_j: $x_i(e_j) = \delta_{ij}$.

Пространство $\mathcal{A}(h)$ изоморфно пространству двоичных векторов размерности 4^h. Здесь и далее подразумевается, что поле $\mathbb{F}_4$ реализовано в виде фактор-алгебры $\mathbb{F}_2[x]/(x^2 + x + 1)$.

Далее выберем в $\mathcal{A}(h)$ все подмножества с чётным числом элементов, такие, что покоординатная сумма всех элементов каждого подмножества равна 0: $\mathcal{A}_0(h) = \{A \in \in \mathcal{A}(h) : |A| \equiv 0 \pmod 2 \ \& \ \forall i \sum\limits_{a \in A} x_i(a) = 0\}$. Под суммой здесь понимается сумма над $\mathbb{F}_4$; считается, что пустое множество удовлетворяет необходимому условию.

Лемма 2. Множество $\mathcal{A}_0(h)$ является подпространством $\mathcal{A}(h)$.

Доказательство. Очевидно, что операция симметрической разности сохраняет чётность количества точек в множестве. Рассмотрим $A_1 \triangle A_2$, где $A_1, A_2 \in \mathcal{A}_0(h)$; тогда $\sum\limits_{a \in A_1 \triangle A_2} x_i(a) = \sum\limits_{a \in A_1} x_i(a) + \sum\limits_{a \in A_2} x_i(a) = 0+0 = 0$, так как $\mathcal{A}(h)$ — пространство над полем характеристики 2. Таким образом, симметрическая разность двух элементов из $\mathcal{A}_0(h)$ также является элементом из $\mathcal{A}_0(h)$. ■

Каждый из элементов $a \in \mathbb{F}_4^h$, $a = (x^1 + Xy^1, \ldots, x^h + Xy^h)$, представим в виде $a = (x^1, y^1, \ldots, x^h, y^h)$, и всего множеств $A \subseteq \mathbb{F}_4^h$ ровно $2^{|\mathbb{F}_4^h|}$. Тогда множеств, у кото-

рых $\sum\limits_{a\in A} x^1(a) = 0$, ровно половина (у второй половины сумма равна 1), т. е. $2^{|\mathbb{F}_4^h|}/2$. Далее: тех множеств, у которых одновременно $\sum\limits_{a\in A} x^1(a) = 0$ и $\sum\limits_{a\in A} y^1(a) = 0$, ровно $2^{|\mathbb{F}_4^h|}/2^2$. Все пары x^i, y^j можно рассматривать независимо друг от друга; таким образом, продолжая подобные рассуждения, получим, что $|A| = 2^{|\mathbb{F}_4^h|}/2^{2h}$, где A — любое подмножество $\mathcal{A}(h)$, у которого покоординатная сумма всех элементов равна нулю. Заметим, что подмножеств с чётным числом элементов столько же, сколько и подмножеств с нечётным числом элементов, а значит, фактически вычислено $|\mathcal{A}_0(h)|$.

Введём обозначение $\mathbb{N}^* = \mathbb{N}\setminus\{1\}$.

Лемма 3. Для любого $h \in \mathbb{N}^*$ верно $|\mathcal{A}_0(h)| = 2^{2^{2h}-2h-1}$.

Поскольку $\mathcal{A}_0(h)$ — подпространство над полем характеристики 2, то можно посчитать его размерность.

Следствие 1. Для любого $h \in \mathbb{N}^*$ верно $\dim \mathcal{A}_0(h) = 2^{2h} - 2h - 1$.

Обозначим $\mathcal{A}_0^4(h) = \{A \in \mathcal{A}(h) : |A| = 4 \ \& \ \forall i \sum\limits_{a\in A} x_i(a) = 0\}$ — множество всех подмножеств из четырёх элементов, таких, что покоординатная сумма всех элементов подмножества равна 0; $\mathbb{B}_0(h)$ — все прямые. Здесь и далее будем использовать обозначение $\mathbb{B}_0(h)$ как для совокупности подмножеств над $\mathbb{F}_2$, так и для совокупности прямых в $\mathbb{F}_4^h$. Заметим, что $\langle\mathbb{B}_0(h)\rangle$ является подпространством $\langle\mathcal{A}_0^4(h)\rangle$.

Лемма 4. Для любого $h \in \mathbb{N}^*$ выполняется $\langle\mathcal{A}_0^4(h)\rangle = \mathcal{A}_0(h)$.

Доказательство. Построим выражение любого множества $\mathcal{A}_0(h)$ через множества $\mathcal{A}_0^4(h)$, для этого рассмотрим элемент $A \in \mathcal{A}_0(h)$, $A \neq \varnothing$, $|A| \geqslant 4$, поскольку множества из двух элементов удовлетворяют условию принадлежности $\mathcal{A}_0(h)$, только если состоят из двух одинаковых точек. Выберем любые три точки $a, b, c \in A$ и рассмотрим $A' = A \triangle \{a, b, c, a+b+c\}$, где $x_i(a+b+c) = x_i(a)+x_i(b)+x_i(c)$ — сумма над $\mathbb{F}_4$. Заметим, что A выражается множествами $\mathcal{A}_0^4(h)$, если и только если выражается A' и при этом $|A'| < |A|$. Получился спуск по весу; продолжаем этот спуск к A'', A''', …, $A^{(n)}$ до тех пор, пока не получим $|A^{(n)}| \leqslant 4$. Тем самым построено выражение любого множества $\mathcal{A}_0(h)$ через множества $\mathcal{A}_0^4(h)$, поскольку $A^{(n)}$ лежит в $\mathcal{A}_0^4(h)$. ■

Таким образом, в $\mathcal{A}_0^4(h)$ можно выбрать порождающую систему из $2^{2h} - 2h - 1$ множеств.

Лемма 5. Если одна четвёрка $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ порождается прямыми $\mathbb{B}_0(h)$, то все четвёрки $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ порождаются прямыми $\mathbb{B}_0(h)$, где $h \in \mathbb{N}^*$.

Замечание 2. Лемму также можно сформулировать следующим образом: или все четвёрки $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ порождаются прямыми $\mathbb{B}_0(h)$, или никакая четвёрка $\mathcal{A}_0^4(h) \setminus \setminus \mathbb{B}_0(h)$ не выражается через прямые $\mathbb{B}_0(h)$, где $h \in \mathbb{N}^*$.

Доказательство. Пусть какое-либо множество A из $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ выражается через прямые $\mathbb{B}_0(h)$. Рассмотрим любую четвёрку из $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ и шесть прямых, проходящих через пары точек выбранной четвёрки. В силу строения четвёрок эти прямые можно разбить на три пары параллельных прямых, которые будем называть *образующими* A.

Выберем аффинное преобразование, переводящее три точки рассматриваемой четвёрки в точки $(0, \ldots, 0)$, $(1, 0, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$. Тогда оставшаяся точка перейдёт в точку $(1, 1, 0, \ldots, 0)$ в силу того, что при аффинном преобразовании сохраняется параллельность прямых. Таким образом, выбранная четвёрка перейдет во множество $\{(0, \ldots, 0), (0, 1, 0, \ldots, 0), (1, 0, 0, \ldots, 0), (1, 1, 0, \ldots, 0)\}$. Поскольку любую четвёрку

$\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ можно эквивалентными аффинными преобразованиями перевести в четвёрку $\{(0,\dots,0),(0,1,0,\dots,0),(1,0,0,\dots,0),(1,1,0,\dots,0)\}$, то из того, что какая-либо четвёрка $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ выражается через прямые $\mathbb{B}_0(h)$, следует, что любая другая четвёрка выражается через прямые $\mathbb{B}_0(h)$. ■

Далее покажем, что на расстоянии 0 до $\mathbb{B}_0(h)$ в $\mathbb{F}_4^h$ не могут лежать четвёрки $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$; здесь и далее $h \in \mathbb{N}^*$. Из лемм 4 и 5 можно сделать важный вывод:

Следствие 2. В $\mathcal{A}_0(h)$ не существует базиса из прямых $\mathbb{B}_0(h)$, если и только если никакая четвёрка $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ не порождается прямыми $\mathbb{B}_0(h)$.

В работе [3] приводится точное значение размерности пространства $\langle \mathbb{B}_0(h) \rangle$.

Теорема 1 (о базисе $\mathbb{B}_0(h)$) [3]. В $\mathbb{B}_0(h)$ существует базис из $2^{2h} - h^2 - h - 1$ элементов, т. е. в $\mathbb{F}_4^h$

$$\dim \langle \mathbb{B}_0(h) \rangle = 2^{2h} - h^2 - h - 1.$$

Таким образом, любая достаточно большая система прямых $\mathbb{B}_0(h)$ линейно зависима в $\mathbb{F}_4^h$. Тогда по теореме о базисе $\mathbb{B}_0(h)$ и следствию 1 в $\mathcal{A}_0(h)$ не существует базиса из прямых $\mathbb{B}_0(h)$, а значит, по следствию 2 никакая четвёрка $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ не выражается через прямые $\mathbb{B}_0(h)$. Следовательно, множества $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ не могут лежать на расстоянии 0 до $\langle \mathbb{B}_0(h) \rangle$ в $\mathbb{F}_4^h$.

Более того, по лемме 1 множества $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ не могут лежать и на расстоянии 2 до $\langle \mathbb{B}_0(h) \rangle$ в $\mathbb{F}_4^h$. Тогда любая четвёрка $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ обязана лежать на расстоянии 4 до $\langle \mathbb{B}_0(h) \rangle$ в $\mathbb{F}_4^h$. Проверим, что никакие другие четвёрки не лежат на расстоянии больше 2 до $\langle \mathbb{B}_0(h) \rangle$ в $\mathbb{F}_4^h$.

Введём для $\mathbb{F}_4^h$ следующие обозначения для различных множеств по четыре точки: $\mathbb{B}_1$ содержит все четырёхточечные множества, пересекающиеся с какой-нибудь прямой ровно по трём точкам; $\mathbb{S}_i$ — множество четвёрок, никакие три точки которых не лежат на одной прямой, и среди трёх пар образующих их прямых ровно в i, $i > 0$, парах есть пересечение.

Заметим, что эти множества не пересекаются, а вместе с $\mathcal{A}_0^4(h)$ они исчерпывают все четырёхточечные множества $\mathbb{F}_4^h$. Для любой четвёрки из множества $\mathbb{B}_1$ выберем прямую, пересекающуюся с ней по трём точкам, а для $\mathbb{S}_i$, $i > 0$, выберем пересекающуюся пару прямых из трёх образующих пар (хотя бы одна обязательно найдется) — линейная комбинация указанных прямых и выбранной четвёрки оставляет множество из двух точек. То есть четвёрки из множеств $\mathbb{B}_1$ или $\mathbb{S}_i$, $i > 0$, лежат на расстоянии не больше 2 до $\langle \mathbb{B}_0(h) \rangle$ в $\mathbb{F}_4^h$. Таким образом, доказана следующая теорема:

Теорема 2. Для любого натурального $h \neq 1$ любое множество $F \in \mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$ лежит на расстоянии 4 до $\langle \mathbb{B}_0(h) \rangle$. При этом никакие другие четвёрки не лежат на расстоянии больше 2 до $\langle \mathbb{B}_0(h) \rangle$.

Итак, показано, что для векторов из $\mathbb{F}_2^{4^h}$, соответствующих четвёркам $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$, с ростом h сохраняется расстояние от них до кода.

2. Радиус покрытия $r(\mathbb{C}_h)$

Заметим, что по аффинной геометрии $\mathbb{EG}(h,4)$ можно построить систему Штейнера $S(2,4,4^h)$. *Системой Штейнера* $S(t,k,v)$ называется пара $(V,\mathcal{B})$, где V — множество из v элементов, а $\mathcal{B}$ — семейство k-элементных подмножеств V, называемых *блоками*, таких, что любое t-элементное подмножество V лежит ровно в одном блоке. С основными результатами по системам Штейнера с указанными параметрами можно ознакомиться, например, в [4].

Для кодов, порождённых матрицами инцидентности систем Штейнера $S(2,4,v)$, в [5] приводится верхняя оценка радиуса покрытия.

Теорема 3 [5]. Пусть $\mathbb{C}$ — код, порождённый матрицей инцидентности $S(2,4,v)$. Тогда $r(\mathbb{C}) \leqslant \sqrt{v}$.

Для кодов, рассматриваемых в данной работе, верхнюю оценку теоремы 3 удаётся улучшить. Для этого докажем несколько утверждений.

Лемма 6. Если в $\mathbb{F}_4^h$ множество из R точек лежит на расстоянии R от $\langle \mathbb{B}_0(h) \rangle$, то любое его S-элементное подмножество лежит на расстоянии S от $\langle \mathbb{B}_0(h) \rangle$.

Доказательство. Очевидно, что расстояние больше S ни для какого S-элементного подмножества достигаться не может. Предположим, для какого-то S-элементного подмножества можно построить линейную комбинацию прямых, такую, что на ней достигается расстояние меньше S. Тогда дополнение этого подмножества из $R-S$ элементов лежит от $\langle \mathbb{B}_0(h) \rangle$ на расстоянии не больше $R-S$. Но тогда для всего R-элементного множества есть линейная комбинация, на которой достигается расстояние меньше R. Противоречие. ■

Теорема 4. Расстояние в $\mathbb{F}_4^h$ от любого R-элементного подмножества, $R > 4$, до $\langle \mathbb{B}_0(h) \rangle$ не превосходит 4.

Доказательство. Поскольку $R > 4$, то в выбранном множестве есть как минимум пять различных точек $\{a, b, c, d_1, d_2\}$. Предположим, что расстояние от этого множества до $\langle \mathbb{B}_0(h) \rangle$ не меньше 5.

Рассмотрим два подмножества $\{a, b, c, d_1\}$ и $\{a, b, c, d_2\}$; по лемме 6 расстояние от них до $\langle \mathbb{B}_0(h) \rangle$ равно 4. Из теоремы 2 известно, что на расстоянии 4 от $\langle \mathbb{B}_0(h) \rangle$ могут лежать только четвёрки $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$, а значит, $a + b + c + d_1 = a + b + c + d_2 = 0$. Следовательно, $d_1 = d_2$. Противоречие. ■

Переформулируя эту теорему для кода $\mathbb{C}_h$, получим уточнение верхней оценки его радиуса покрытия.

Следствие 3. Пусть $\mathbb{C}_h$ — код, порождённый строками матрицы инцидентности $\mathbb{EG}(h,4)$. Тогда $r(\mathbb{C}_h) \leqslant 4$.

Доказательство. Предположим, что существует вектор в $\mathbb{F}_2^{4^h}$, который лежит от $\mathbb{C}_h$ на расстоянии больше 4. Поскольку 0 лежит в коде, то можно считать, что вес выбранного вектора больше или равен 5. Рассмотрим соответствующее этому вектору множество элементов $\mathbb{F}_4^h$, по предположению в нем не менее 5 элементов. По теореме 4 расстояние от этого множества до $\langle \mathbb{B}_0(h) \rangle$ не превосходит 4, поэтому существует линейная комбинация прямых, а значит, и линейная комбинация векторов в $\mathbb{F}_2^{4^h}$, лежащая на расстоянии не больше 4 до выбранного множества и соответствующего вектора. Противоречие. ■

Интерес к кодам, порождённым матрицами инцидентности систем Штейнера $S(2,4,v)$, связан с исследованием ранга и аффинного ранга носителей спектра булевых функций [5]. Открытым остаётся вопрос, выполняется ли уточнённая верхняя оценка радиуса покрытия из следствия 3 для кодов, порождённых системами Штейнера $S(2,4,v)$ с параметрами, отличными от $\mathbb{EG}(h,4)$.

Вернёмся к исследованию ранга выбранных кодов: в теореме 2 фактически показано, что на векторах $\mathbb{F}_2^{4^h}$, соответствующих четвёркам $\mathcal{A}_0^4(h) \setminus \mathbb{B}_0(h)$, достигается верхняя оценка из следствия 3. Таким образом, доказана следующая

Теорема 5 (о радиусе покрытия). Пусть $h \in \mathbb{N}^*$ и $\mathbb{C}_h$ — код, порождённый строками матрицы инцидентности $\mathbb{EG}(h, 4)$. Тогда $r(\mathbb{C}_h) = 4$.

ЛИТЕРАТУРА

1. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. *Cohen G., Honkala I., Litsyn S., and Lobstein A.* Covering Codes. North Holland: Elsevier, 1997.
3. *Коваленко М. Э., Урбанович Т. А.* О ранге матриц инцидентности точек и прямых конечных аффинных и проективных геометрий над полем из четырех элементов // Проблемы передачи информации. 2014. Т. 50. Вып. 1. С. 102–112.
4. *Reid C. and Rosa A.* Steiner systems $S(2, 4, v)$ — a survey // Electronic J. Combinatorics. 2010. `http://www.combinatorics.org/ojs/index.php/eljc/article/view/DS18`
5. *Таранников Ю. В.* О рангах подмножеств пространства двоичных векторов, допускающих встраивание системы Штейнера $S(2, 4, v)$ // Прикладная дискретная математика. 2014. № 1. С. 73–76.