

О РАНГАХ ПОДМНОЖЕСТВ ПРОСТРАНСТВА ДВОИЧНЫХ ВЕКТОРОВ, ДОПУСКАЮЩИХ ВСТРАИВАНИЕ СИСТЕМЫ ШТЕЙНЕРА $S(2, 4, v)^1$

Ю. В. Таранников

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

E-mail: taran@butovo.com

Получена оценка ранга подмножества X пространства $\mathbb{F}_2^n$ через радиус покрытия кода, лежащего в подпространстве линейных зависимостей векторов из X . Получена верхняя оценка радиуса покрытия кода, порождённого матрицей инцидентности системы Штейнера $S(2, 4, v)$. Получены верхняя точная и асимптотическая оценки ранга подмножества X пространства $\mathbb{F}_2^n$, допускающего встраивание системы Штейнера $S(2, 4, v)$.

Ключевые слова: ранг, аффинный ранг, оценки, линейное подпространство, линейный код, радиус покрытия, система Штейнера, булевы функции, носитель спектра.

Пусть $X \subseteq \mathbb{F}_2^n$. Рангом множества X называется размерность $\dim\langle X \rangle$ его линейной оболочки $\langle X \rangle$. Аффинным рангом множества X называется наименьшая размерность класса смежности линейного подпространства в $\mathbb{F}_2^n$, содержащего X . Пусть μ_X — взаимно-однозначное отображение векторов из X в компоненты пространства $\mathbb{F}_2^{|X|}$. Отображение μ_X индуцирует взаимно-однозначное сопоставление каждому подмножеству $A \subseteq X$ характеристического вектора $a = (a_1, \dots, a_{|X|}) = \xi_X(A)$ в $\mathbb{F}_2^{|X|}$, такого, что $a_i = 1$, если $\mu_X^{-1}(i) \in A$, и $a_i = 0$, если $\mu_X^{-1}(i) \notin A$, $i = 1, \dots, |X|$. Пусть $\mathcal{B}_X = \{B^1, \dots, B^s\}$ — совокупность всех таких подмножеств $B^i = \{x^{i_1}, \dots, x^{i_{k_i}}\}$ множества X , что $\sum_{j=1}^{k_i} x^{ij} = (0, \dots, 0)$. Тогда множество векторов $\xi_X(\mathcal{B}_X) = \{\xi_X(B^1), \dots, \xi_X(B^s)\}$, очевидно, является линейным подпространством в $\mathbb{F}_2^{|X|}$.

Лемма 1. Имеет место равенство $\dim\langle X \rangle = |X| - \dim \xi_X(\mathcal{B}_X)$.

Доказательство леммы 1 практически очевидно, потому что если $\dim \xi_X(\mathcal{B}_X) = r$, то в X найдется подмножество X' из $|X| - r$ линейно независимых векторов, а все векторы из $X \setminus X'$ могут быть выражены как линейные комбинации векторов из X' .

Из леммы 1 получаем

Следствие 1. Пусть $C \subseteq \xi_X(\mathcal{B}_X)$. Тогда

$$\dim\langle X \rangle \leq |X| - \dim\langle C \rangle.$$

Произвольное множество C , $C \subseteq \mathbb{F}_2^m$, называется кодом. Если C — линейное пространство в $\mathbb{F}_2^m$, то C называется линейным кодом. Расстоянием (Хэмминга) $d(a, b)$ между векторами a и b из $\mathbb{F}_2^m$ называется число компонент, в которых a и b различаются. Радиусом покрытия $R = R(C)$ кода C , $C \subseteq \mathbb{F}_2^m$, называется величина

¹Работа поддержана грантом РФФИ, проект №13-01-00183-а.

$R = R(C) = \max_{a \in \mathbb{F}_2^m} \min_{b \in C} d(a, b)$. Радиусу покрытия и связанным с ним вопросам теории кодирования посвящена монография [1]. Из определения радиуса покрытия сразу следует, что мощность кода C , $C \subseteq \mathbb{F}_2^m$, оценивается через его радиус покрытия $R(C)$ как

$$|C| \geq 2^m / \sum_{i=0}^{R(C)} \binom{m}{i}.$$

Отсюда, если C — линейный код, то

$$\dim C \geq m - \log_2 \sum_{i=0}^{R(C)} \binom{m}{i}. \quad (1)$$

Из (1) и следствия 1 получаем следующую теорему.

Теорема 1. Пусть $C \subseteq \xi_X(\mathcal{B}_X)$. Тогда

$$\dim \langle X \rangle \leq \log_2 \sum_{i=0}^{R(C)} \binom{|X|}{i}.$$

Системой Штейнера $S(t, k, v)$ называется пара $(V, \mathcal{B})$, где V — множество мощности v , а $\mathcal{B}$ — семейство k -элементных подмножеств V , называемых *блоками*, таких, что любое t -элементное подмножество V целиком принадлежит ровно одному блоку.

Будем говорить, что пара $(V, \mathcal{B})$, являющаяся системой Штейнера $S(t, k, v)$, *встраивается* во множество X , $X \subseteq \mathbb{F}_2^n$, если существует биекция $\varphi : V \rightarrow X$, такая, что для любого блока B , $B \in \mathcal{B}$, выполнено соотношение $\sum_{x \in B} \varphi(x) = (0, \dots, 0)$. Саму биекцию φ будем при этом называть *встраиванием*.

Заметим, что если такое встраивание существует, то семейство блоков $\mathcal{B} = \{B^1, \dots, B^b\}$ перейдёт в семейство $\varphi(\mathcal{B}) = \{\varphi(B^1), \dots, \varphi(B^b)\}$ подмножеств множества $\mathcal{B}_X$, которое, в свою очередь, соответствует множеству двоичных векторов $\xi_X(\varphi(\mathcal{B}))$, лежащему в $\xi_X(\mathcal{B}_X)$.

Следующая теорема справедлива, даже если биекция φ не обязательно является встраиванием. Фактически теорема устанавливает верхнюю оценку радиуса покрытия кода, порождённого матрицей инцидентности системы Штейнера $S(2, 4, v)$.

Теорема 2. Пусть $X \subseteq \mathbb{F}_2^n$, $|X| = v$; $(V, \mathcal{B})$ — система Штейнера $S(2, 4, v)$; φ — взаимно-однозначное отображение $V \rightarrow X$. Тогда для радиуса покрытия R линейного кода $C = \langle \xi_X(\varphi(\mathcal{B})) \rangle$ в $\mathbb{F}_2^v$ справедливо неравенство $R(C) \leq \sqrt{v}$.

Доказательство. Пусть a — произвольный вектор из $\mathbb{F}_2^v$. Надо доказать, что найдётся вектор u из $\langle \xi_X(\varphi(\mathcal{B})) \rangle$, для которого $d(a, u) \leq \sqrt{v}$. Для этого покажем, что если $|a| > \sqrt{v}$, где $|a|$ — вес вектора a , т. е. число ненулевых компонент в a , то найдётся вектор u^1 из $\langle \xi_X(\varphi(\mathcal{B})) \rangle$, такой, что $|a + u^1| < |a|$. Если $|a + u^1| > \sqrt{v}$, то применим эти же рассуждения к вектору $a + u^1$ и т. д. В силу конечности веса вектора a получим множество наборов $u^1, \dots, u^s$ из $\langle \xi_X(\varphi(\mathcal{B})) \rangle$, что $|a + u^1 + \dots + u^s| \leq \sqrt{v}$, т. е. $d(a, u^1 + \dots + u^s) \leq \sqrt{v}$, где $(u^1 + \dots + u^s) \in \langle \xi_X(\varphi(\mathcal{B})) \rangle$, что и требуется.

Итак, предположим, что $|a| > \sqrt{v}$. Напомним, что все векторы из $\xi_X(\varphi(\mathcal{B}))$ имеют вес 4. Выделим две достаточные для доказательства ситуации:

а) Если найдётся вектор u из $\xi_X(\varphi(\mathcal{B}))$, имеющий с набором a не менее трёх общих единиц, то, очевидно, $|a| < |a + u|$.

б) Если найдутся векторы u^1 и u^2 из $\xi_X(\varphi(\mathcal{B}))$, имеющие одну общую единицу между собой (но не более в силу определения системы Штейнера), причём в компоненте,

где в наборе a нуль, и каждый из них не менее двух общих единиц с набором a , то, очевидно, $|a| < |a + (u^1 + u^2)|$.

Обозначим за I множество всех компонент пространства $\mathbb{F}_2^v$, в которых вектор a имеет единицы. Для любых $i, j \in I$, $i \neq j$, в силу того, что $(V, \mathcal{B})$ — система Штейнера $S(2, 4, v)$, существует вектор $u^{(i,j)}$ из $\xi_X(\varphi(\mathcal{B}))$, имеющий единицы в компонентах i и j . Если $u^{(i,j)}$ имеет ещё хотя бы одну единицу в компоненте из I , то имеет место ситуация «а». Если для разных пар (i, j) и (i', j') векторы $u^{(i,j)}$ и $u^{(i',j')}$ имеют общую единицу в компоненте не из I , то имеет место ситуация «б». Поэтому все векторы $u^{(i,j)}$, $i, j \in I$, $i \neq j$, разные и никакие два из них не имеют общих единиц в компонентах не из I . Следовательно, число компонент не из I , равное $v - |a|$, оценивается как $v - |a| \geq 2|a|(|a| - 1)/2$. Отсюда $|a| \leq \sqrt{v}$, что доказывает теорему. ■

Объединяя утверждения теорем 1 и 2, получаем следующую теорему.

Теорема 3. Пусть $X \subseteq \mathbb{F}_2^n$ и существует встраивание системы Штейнера $S(2, 4, |X|)$ в X . Тогда

$$\dim \langle X \rangle \leq \min \left\{ n, \log_2 \sum_{i=0}^{\lfloor \sqrt{|X|} \rfloor} \binom{|X|}{i} \right\}.$$

Из теоремы 3 вытекает асимптотическая оценка.

Следствие 2. Пусть существует последовательность подмножеств $X \subseteq \mathbb{F}_2^n$, $n \rightarrow \infty$, $|X| \rightarrow \infty$, для каждого из которых существует встраивание системы Штейнера $S(2, 4, |X|)$ в X . Тогда

$$\dim \langle X \rangle \leq \frac{1}{2} \sqrt{|X|} \log_2 |X| (1 + o(1)).$$

Для доказательства следствия 2 достаточно воспользоваться неравенством $\sum_{k=0}^t \binom{n}{k} \leq 2^{nH(t/n)}$ при $1 \leq t \leq n/2$, где $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ — двоичная энтропия (см., например, [2, с. 37]).

Параметры линейных кодов, порождённых системами Штейнера $S(t, k, v)$, достаточно активно изучаются при $k = t + 1$ [3, 4]. Обсудим, почему нами выбраны именно системы Штейнера $S(2, 4, v)$. Это связано с исследованиями ранга и аффинного ранга носителей спектра булевых функций.

Булева функция от n переменных — это отображение из $\mathbb{F}_2^n$ в $\mathbb{F}_2$. *Преобразованием Уолша* булевой функции f называется целочисленная функция над $\mathbb{F}_2^n$, определяемая как $W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \langle u, x \rangle}$. Для каждого $u \in \mathbb{F}_2^n$ значение $W_f(u)$ называется *коэффициентом Уолша*. Коэффициенты Уолша называются *спектральными коэффициентами*, а совокупность всех 2^n коэффициентов Уолша — *спектром* булевой функции. Множество S_f всех наборов u , таких, что $W_f(u) \neq 0$, называется *носителем спектра* функции f .

Для коэффициентов Уолша булевой функции f над $\mathbb{F}_2^n$ справедлива теорема Титсворта (см., например, [5, с. 135]): для любого ненулевого $s \in \mathbb{F}_2^n$ выполнено равенство $\sum_{x \in \mathbb{F}_2^n} W_f(x) W_f(x + s) = 0$. Отсюда следует, что если носителю спектра S_f принадлежат наборы x и $x + s$, то в S_f должна лежать ещё хотя бы одна пара наборов, отличающаяся на s , скажем, y и $y + s$. Но тогда $x + (x + s) + y + (y + s) = (0, \dots, 0)$,

т. е. $\{x, x + s, y, y + s\}$ — четвёрка наборов, удовлетворяющая условию на встраивание. Конечно, система Штейнера $S(2, 4, v)$ — это достаточно специфический комбинаторный объект, существующий не при всех v . Известно [6], что система Штейнера $S(2, 4, v)$ существует тогда и только тогда, когда $v \equiv 1, 4 \pmod{12}$. Однако этому условию удовлетворяет мощность носителя спектра платовидной функции. Булева функция называется *платовидной*, если её коэффициенты Уолша принимают ровно три возможных значения: 0 и $\pm 2^h$ для некоторого h . Платовидные функции представляют большой интерес для изучения бент-функций (например, потому, что при разложении бент-функций по переменной возникают две платовидные функции), а также потому, что многие криптографически важные функции являются платовидными (например, m -устойчивые функции с максимально возможной для них нелинейностью $2^{n-1} - 2^{m+1}$). Возможные значения аффинного ранга платовидных функций исследовались в [7]. Из равенства Парсеваля $\sum_{u \in \mathbb{F}_2^n} W_f^2(u) = 4^n$ сразу следует, что мощность носителя спектра равна $|S_f| = 4^{n-h} \equiv 4 \pmod{12}$. Кроме того, из теоремы Титсворта видно, что для любого ненулевого $s \in \mathbb{F}_2^n$ носитель спектра платовидной функции содержит чётное число пар наборов, отличающихся на s , что даёт надежду сгруппировать наборы в совокупность четвёрок, являющихся встраиванием системы Штейнера $S(2, 4, v)$. В [8] построены бесконечные последовательности платовидных функций с растущей мощностью носителей спектров, как допускающих, так и не допускающих встраивание системы Штейнера $S(2, 4, v)$.

ЛИТЕРАТУРА

1. Cohen G., Honkala I., Litsyn S., and Lobstein A. Covering codes. Elsevier Science, 1997.
2. Чашкин А. В. Дискретная математика. М.: Академия, 2012.
3. Зиновьев В. А., Зиновьев Д. В. Системы Штейнера $S(v, k, k - 1)$: компоненты и ранг // Проблемы передачи информации. 2011. Т. 47. № 2. С. 52–71.
4. Ковалевская Д. И., Соловьева Ф. И. Системы четверок Штейнера малых рангов и расширенные совершенные двоичные коды // Дискретный анализ и исследование операций. 2013. Т. 20. Вып. 4. С. 46–64.
5. Таранников Ю. В. Комбинаторные свойства дискретных структур и приложения к криптологии. М.: МЦНМО, 2011.
6. Reid C. and Rosa A. Steiner systems $S(2, 4, v)$ — a survey // Electron. J. Combinator. 2010. DS18.
7. Таранников Ю. В. О значениях аффинного ранга носителя спектра платовидной функции // Дискретная математика. 2006. Т. 18. Вып. 3. С. 120–137.
8. Урбанович Т. А. О дизайнах специального вида на подмножествах булева куба: дипломная работа / механико-математический факультет МГУ им. М. В. Ломоносова. М., 2012.