ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—сентябрь 2016. Том 23, № 3. С. 93–106

УДК 519.7 DOI: 10.17377/daio.2016.23.513

О МЕТРИЧЕСКОМ ДОПОЛНЕНИИ ПОДПРОСТРАНСТВ БУЛЕВА КУБА *)

А. К. Облаухов[1]
[1]Новосибирский гос. университет,
ул. Пирогова, 2, 630090 Новосибирск, Россия
e-mail: oblaukhov@gmail.com

Аннотация. Исследуются метрические дополнения подмножеств булева куба — множеств, максимально удалённых от данного. Получен общий вид метрического дополнения линейного подпространства и более точное его описание для класса подпространств с базисом специального вида. Доказано, что полностью регулярные (в том числе совершенные и равномерно упакованные) коды метрически регулярны. Библиогр. 9.

Ключевые слова: подпространство, метрически регулярное множество, метрическое дополнение, полностью регулярный код, бент-функция.

Введение

В работе рассматриваются некоторые метрические свойства подмножеств булева куба, в частности, линейных и аффинных подпространств, понятие *метрического дополнения* — множества, максимально удалённого от данного в метрике Хэмминга — и изучаются его свойства.

Задача исследования метрического дополнения множества возникает при изучении бент-функциий [6], множество которых является метрическим дополнением множества аффинных функций. Бент-функции часто используются в криптографии в силу высокой нелинейности. До сих пор не решены многие вопросы, связанные с бент-функциями, в частности, не найдены достаточно точные оценки их количества. В случае нечётного числа переменных про максимально нелинейные функции (которые аналогично бент-функциям определяются как максимально удалённые от аффинных) на данный момент известно и того меньше (см.,

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 15–31–20635).

например, [3, 4]). Подобно обычной нелинейности определяется нелинейность более высоких порядков — расстояние до кодов Рида — Маллера $RM(r, n)$ [1] (подпространств функций степени, не превышающей r). В [2, 7] исследуются метрические дополнения $RM(r, n)$, но функции, лежащие в них, и точные расстояния найдены лишь для малого числа переменных.

В [9] поставлена задача исследования метрически регулярных множеств. Множество называется *метрически регулярным*, если его двойное метрическое дополнение совпадает с самим множеством.

В статье описан общий вид метрических дополнений линейных подпространств булева куба, найдена оценка на удалённость метрического дополнения произвольного подпространства от самого подпространства. Получено точное описание метрических дополнений подпространств, базис Гаусса — Жордана которых удовлетворяет одному из следующих условий: (i) веса Хэмминга векторов базиса не превосходят 2, (ii) веса Хэмминга векторов базиса не превосходят 3, а все векторы базиса веса 3 имеют попарно пересекающиеся носители. Описаны двойные метрические дополнения подпространств, метрические дополнения которых являются аффинными подпространствами. Доказано, что полностью регулярные коды являются метрически регулярными множествами.

1. Определения

Пусть $\mathbb{F}_2^n$ — пространство двоичных векторов длины n. *Расстояние Хэмминга* $d(x, y)$ между двумя векторами $x, y \in \mathbb{F}_2^n$ равно числу координат, в которых эти векторы различаются. Число отличных от нуля координат вектора называют *весом Хэмминга* и обозначают через $wt(x)$. Очевидно, что $d(x, y) = wt(x \oplus y)$.

Пусть $X \subseteq \mathbb{F}_2^n$ — произвольное множество, $y \in \mathbb{F}_2^n$ — произвольный вектор. Расстояние от вектора y до множества X определяется как $d(y, X) = \min\limits_{x \in X} d(y, x)$. *Максимальным расстоянием* от множества X называется

$$d(X) = \max_{z \in \mathbb{F}_2^n} d(z, X).$$

Данный параметр множества известен также как радиус покрытия в теории кодирования. Вектор y называется *максимально удалённым* от множества X, если $d(y, X) = d(X)$.

Множество $Y \subseteq \mathbb{F}_2^n$, состоящее из всех максимально удалённых от множества X векторов, назовём *метрическим дополнением* множества X и обозначим через $\widehat{X}$. Если $\widehat{\widehat{X}} = X$, то множество X называется *метриче-*

ски регулярным. Заметим, что $d(X) = d(\widehat{X})$ для метрически регулярных множеств X.

Автоморфизмом множества $X \subseteq \mathbb{F}_2^n$ называется изометрическое отображение $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, переводящее множество X в себя. Группа всех автоморфизмов множества (относительно операции композиции отображений) обозначается через $\mathrm{Aut}(X)$.

Утверждение 1. *Пусть $X \subseteq \mathbb{F}_2^n$ — метрически регулярное множество. Тогда группы автоморфизмов множества X и его метрического дополнения совпадают*: $\mathrm{Aut}(X) = \mathrm{Aut}(\widehat{X})$.

Доказательство. Пусть $\varphi \in \mathrm{Aut}(X)$. Тогда $d(X) = d(y, X) = d(\varphi(y), \varphi(X)) = d(\varphi(y), X)$ для любого $y \in \widehat{X}$ в силу изометричности φ, т. е. $\varphi(y) \in \widehat{X}$. Аналогично, пусть $\psi \in \mathrm{Aut}(\widehat{X})$. Тогда для любого $x \in X$ в силу изометричности ψ выполняется $d(\widehat{X}) = d(x, \widehat{X}) = d(\psi(x), \psi(\widehat{X})) = d(\psi(x), \widehat{X})$, т. е. $\psi(x) \in \widehat{\widehat{X}} = X$. Утверждение 1 доказано.

Через $\mathrm{supp}(a)$ обозначается носитель вектора a:

$$\mathrm{supp}(a) = \{j \mid a_j = 1\},$$

через $|X|$ — мощность множества X.

Непустое множество $L \subseteq \mathbb{F}_2^n$ называется *линейным подпространством*, если для любых $x, y \in L$ сумма $x \oplus y$ лежит в L. Множество $A \subseteq \mathbb{F}_2^n$ называется *аффинным подпространством*, если $A = a \oplus L$, где $a \in \mathbb{F}_2^n$, а L — линейное подпространство. Запись $a \oplus X$ означает сдвиг X на вектор a, т. е. множество $\{a \oplus x \mid x \in X\}$. Пространство всевозможных сдвигов линейного подпространства L — множество $\{a \oplus L \mid a \in \mathbb{F}_2^n\}$ — называется *фактор-пространством* $\mathbb{F}_2^n$ по L и обозначается через $\mathbb{F}_2^n/L$.

2. Примеры метрических дополнений

Рассмотрим несколько типов множеств, для представителей которых нетрудно найти метрические дополнения.

1. Пусть множество X состоит из одного вектора $x \in \mathbb{F}_2^n$. Очевидно, что $d(X) = n$, $\widehat{X} = \{x \oplus \mathbf{1}\}$, где $\mathbf{1}$ — вектор, состоящий из единиц.

2. Рассмотрим шар радиуса r с центром в x:

$$Y = B(r, x) = \{y \in \mathbb{F}_2^n \mid d(x, y) \leqslant r\}.$$

Вектор $x \oplus \mathbf{1}$ удалён от Y на расстояние $n - r$, а для любого отличного от $x \oplus \mathbf{1}$ вектора z (неизбежно совпадающего с x в $l > 0$ координатах)

найдётся вектор y из шара $B(r,x)$, совпадающий с z в $r+l>r$ координатах, т. е. $d(y,z)<n-r$. Значит, $d(Y)=n-r$, $\widehat{Y}=\{x\oplus\mathbf{1}\}$. Более того, используя предыдущий пример, немедленно получаем, что $\widehat{\widehat{Y}}=\{x\oplus\mathbf{1}\oplus\mathbf{1}\}=\{x\}$, т. е. шар ненулевого радиуса не является метрически регулярным множеством. Однако, например, для сферы всё уже не так просто.

3. Пусть Z — сфера радиуса r с центром в x. Рассуждая, как при рассмотрении шара, заключаем, что

(a) если $r<\frac{n}{2}$, то $d(Z)=n-r$, $\widehat{Z}=\{x\oplus\mathbf{1}\}$;

(b) если $r>\frac{n}{2}$, то $d(Z)=r$, $\widehat{Z}=\{x\}$;

(c) если n чётно и $r=\frac{n}{2}$, то $\widehat{Z}=\{x,x\oplus\mathbf{1}\}$ и $\widehat{\widehat{Z}}=Z$, т. е. сфера будет являться метрически регулярным множеством.

Перейдём к подпространствам.

4. *Гранью размерности* $n-k$ называется множество всех векторов с фиксированными значениями в выбранных k координатах. Пусть X — $(n-k)$-мерная грань со значениями $a_1,a_2,\dots,a_k$ в координатах $1\leqslant i_1<i_2<\dots<i_k\leqslant n$ соответственно. Для любого вектора $y\in\mathbb{F}_2^n$ найдётся вектор x из грани, совпадающий с y в координатах $\{1,\dots,n\}\backslash\{i_r\mid r=1,\dots,k\}$, поэтому расстояние от y до X определяется только теми координатами y, которые в грани фиксированы. Легко заметить, что $d(X)=k$ и $\widehat{X}$ — $(n-k)$-мерная грань с противоположными значениями в тех же координатах, что и у X.

5. Пусть L — произвольное $(n-1)$-мерное линейное подпространство $\mathbb{F}_2^n$. Тогда L не содержит какого-то из ортов $e_1,\dots,e_n$ (так как иначе оно совпало бы с $\mathbb{F}_2^n$), скажем, e_1. Тогда $\mathbb{F}_2^n=L\cup(e_1\oplus L)$ и любой вектор пространства удалён от L не более чем на единицу. Отсюда $d(L)=1$ и $\widehat{L}=L\oplus e_1$.

6. Рассмотрим менее тривиальный пример. Пусть $\mathcal{A}_n\subseteq\mathbb{F}_2^{2^n}$ — $(n+1)$-мерное линейное подпространство всех аффинных булевых функций от n переменных, n чётно. По определению $\widehat{\mathcal{A}_n}=\mathcal{B}_n$ — множество бент-функций [6] от n переменных. В [8] доказано, что $\widehat{\mathcal{B}_n}=\mathcal{A}_n$, т. е. подпространство аффинных функций метрически регулярно.

Так как подпространство аффинных функций (а также коды Рида — Маллера более высоких порядков) линейно, возникает интерес к изучению метрических дополнений линейных подпространств $\mathbb{F}_2^n$. Структурные особенности линейных подпространств булева куба наталкивают на мысль о структурных особенностях их метрических дополнений. Этим особенностям и посвящён следующий раздел.

3. Метрические дополнения линейных подпространств

Пусть L — произвольное линейное подпространство $\mathbb{F}_2^n$. Общий вид $\widehat{L}$ описывается следующими утверждениями.

Лемма 1. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство, a — двоичный вектор длины n и $d(a, L) = k$. Тогда для любого вектора y из сдвига $a \oplus L$ имеет место $d(y, L) = k$.*

Доказательство. Пусть $y \in a \oplus L$, т. е. существует $x' \in L$ такой, что $y = a \oplus x'$. Тогда

$$d(y, L) = \min_{x \in L} d(x, y) = \min_{x \in L} d(x, a \oplus x') = \min_{x \in x' \oplus L} d(x, a) = \min_{x \in L} d(x, a) = d(a, L).$$

Предпоследнее равенство следует из того, что L — линейное подпространство. Лемма 1 доказана.

Следствие 1. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство, $a \in \mathbb{F}_2^n$ — произвольный вектор. Тогда расстояние от $a \oplus L$ до любого вектора из L совпадает с расстоянием от L до вектора a, а множество $\widehat{L}$ является объединением сдвигов подпространства L.*

С учётом леммы 1 удобно теперь работать с фактор-пространством $\widetilde{L} = \mathbb{F}_2^n / L$.

Приведём следующее утверждение без доказательства, которое не представляет особого труда, но выходит за рамки предмета обсуждения данной статьи.

Лемма 2. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k. Тогда в L существует единственный базис $e_1, \ldots, e_k$ такой, что матрица, составленная из векторов этого базиса, имеет вид*

$$M = \begin{array}{c} \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccccccccc} & & & s_1 & & s_2 & & s_3 & & & & s_k & \\ \end{array} \\ \begin{pmatrix} 0 & \ldots & 0 & 1 & * & 0 & * & 0 & * & \ldots & * & 0 & * \\ 0 & \ldots & \ldots & \ldots & 0 & 1 & * & 0 & * & \ldots & * & 0 & * \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & 1 & * & \ldots & \vdots & \vdots & \vdots \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & * & 0 & * \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & 1 & * \end{pmatrix} \end{array}.$$

(*Матрица такого вида называется матрицей Гаусса — Жордана.*)

Этот базис назовём *каноническим*, а его векторы в общем случае будем обозначать через $e_i(L)$. Понадобится также множество $S(L) =$

$\{s_i(L) \mid 1 \leqslant i \leqslant k\}$, где $s_i(L)$ — номер позиции, в которой у i-го вектора канонического базиса подпространства L стоит первая единица. Если из контекста ясно, о каком пространстве идёт речь, L иногда будет опускаться. Пусть $\overline{S} = \{1, \ldots, n\} \backslash S$.

Рассмотрим множество векторов X_L, у которых в координатах из множества $S(L)$ находятся нули. Нетрудно доказать, что в любом элементе фактор-пространства найдётся единственный вектор из множества X_L, поэтому каждому $A \in \widetilde{L}$ можно поставить в соответствие лежащий в нём $a \in X_L$. В дальнейшем нам пригодится вектор максимального веса из X_L, поэтому введём для него специальное обозначение: $a_{S(L)} = \arg\max\limits_{b \in X_L} wt(b)$. В силу леммы 1 векторов из X_L достаточно для полного исследования метрических свойств подпространства.

Введённый канонический базис позволяет получить оценки на максимальное расстояние от линейного подпространства.

Теорема 1. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k. Тогда*

$$d(L) \leqslant n - k.$$

Доказательство. Утверждение непосредственно следует из того, что вес любого $a \in X_L$ не превосходит $n - k$ (вес вектора a есть не что иное, как расстояние от a до нулевого вектора, который содержится во всяком линейном подпространстве), а также следствия 1. Теорема 1 доказана.

Метрические свойства метрического дополнения линейного подпространства напрямую связаны с метрическими свойствами самого подпространства.

Лемма 3. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство, $d(L) = k$. Тогда $d(\widehat{L}) = k$ и $L \subseteq \widehat{\widehat{L}}$.*

Доказательство. Очевидно, что для всякого $x \in L$ выполняется $d(x, \widehat{L}) = k$. Предположим, что $d(\widehat{L}) > k$, т. е. существует вектор z такой, что $d(z, \widehat{L}) = l > k$. Пусть $b \in X_L \cap \widehat{L}$. Тогда $d(z \oplus b, L) = d(z, b \oplus L) \geqslant d(z, \widehat{L}) = l > k$, что противоречит максимальности значения $d(L)$. Лемма 3 доказана.

4. Линейные подпространства с базисом малого веса

Рассмотрим подпространства, векторы канонического базиса которых имеют малые веса. Для некоторых из них нетрудно в явном виде найти метрическое дополнение.

Теорема 2. *Равенство в оценке теоремы* 1 *достигается тогда и только тогда, когда* $wt(e_i(L)) \leqslant 2$ *для всех* $i \in \{1, \ldots, k\}$. *В этом случае* $\widehat{L} = a_S \oplus L$,

$$a_S = \big(1 \quad \ldots \quad 1 \quad \overset{s_1}{0} \quad 1 \quad \ldots \quad 1 \quad \overset{s_2}{0} \quad 1 \quad \ldots \quad 1 \quad \overset{s_k}{0} \quad 1 \quad \ldots \quad 1\big).$$

Доказательство. ($\Rightarrow$) Если $d(L) = n - k$ и $d(L) \leqslant d(b, 0) = wt(b)$ для всякого $b \in X_L \cap \widehat{L}$, то $n-k$ не превосходит веса b, а значит, этот вес равен $n-k$. Таким образом, $X_L \cap \widehat{L} = a_S$. Если вес какого-либо вектора e_i канонического базиса превосходит 2, то, так как $|\mathrm{supp}(e_i) \cap S| = 1$, имеем $|\mathrm{supp}(e_i) \cap \overline{S}| = |\mathrm{supp}(e_i) \cap \mathrm{supp}(a_S)| > 1$, откуда

$$d(a_S, e_i) = wt(a_S \oplus e_i) = |\mathrm{supp}(a_S \oplus e_i)| = |\mathrm{supp}(a_S)| + |\mathrm{supp}(e_i) \cap S| - |\mathrm{supp}(e_i) \cap \overline{S}| < |\mathrm{supp}(a_S)| = wt(a) = n - k, \quad (1)$$

т. е. вектор a_S удалён от вектора e_i на расстояние, меньшее $n - k$, что противоречит $d(L) = n - k$.

($\Leftarrow$) Пусть веса векторов канонического базиса не превосходят 2. Тогда $|\mathrm{supp}(e_i) \cap S| = 1$, $|\mathrm{supp}(e_i) \cap \overline{S}| \leqslant 1$ для каждого e_i из канонического базиса. Покажем, что для любого $x \in L$ имеет место $wt(x \oplus a_S) \geqslant n - k$. Пусть $x \in L$ и $x = e_{i_1} \oplus \cdots \oplus e_{i_l}$ — разложение x по каноническому базису. Тогда $|\mathrm{supp}(x) \cap S| = l$ и $|\mathrm{supp}(x) \cap \overline{S}| \leqslant l$, как можно видеть из матрицы канонического базиса. Поскольку $\mathrm{supp}(a_S) = \overline{S}$, отсюда следует, что $wt(a_S \oplus x) \geqslant wt(a_S) + l - l = wt(a_S) = n - k$. Таким образом, $d(a_S, L) = n - k$ и $a_S \oplus L \subseteq \widehat{L}$. Включение можно заменить равенством в силу того, что вес любого $b \in X_L$, отличного от a_S, а с ним и расстояние до нулевого вектора, содержащегося в подпространстве, строго меньше $n - k$. Теорема 2 доказана.

Теорема 3. *Пусть* $L \subseteq \mathbb{F}_2^n$ *— линейное подпространство размерности* k, $wt(e_i) \leqslant 3$ *для всех* e_i *из канонического базиса и существует номер* j *такой, что* $wt(e_j) = 3$. *В этом случае* $d(L)$ *равно* $n - k - 1$ *тогда и только тогда, когда* $\mathrm{supp}(e_i) \cap \mathrm{supp}(e_j) \neq \varnothing$ *для всех* i, j *таких, что* $wt(e_i) = wt(e_j) = 3$. *При этом* $a_S \oplus L \subseteq \widehat{L}$. *Более того,*

(i) *если* $\bigcap\limits_{i:wt(e_i)=3} \mathrm{supp}(e_i) = \varnothing$, *то* $\widehat{L} = a_S \oplus L$;

(ii) *если* $\bigcap\limits_{i:wt(e_i)=3} \mathrm{supp}(e_i) = \{m\}$, *то* $\widehat{L} = (a_S \oplus L) \cup (b \oplus L)$, *где* $b \in X_L$ *— вектор веса* $n - k - 1$ *с нулями только в координатах* $\{m\} \cup S$;

(iii) *если* $\bigcap\limits_{i:wt(e_i)=3} \mathrm{supp}(e_i) = \{m, l\}$, *то* $\widehat{L} = (a_S \oplus L) \cup (b \oplus L) \cup (c \oplus L)$,

где $b, c \in X_L$ — векторы веса $n-k-1$ с нулями только в координатах $\{m\} \cup S$ и $\{l\} \cup S$ соответственно.

Доказательство. ($\Rightarrow$) Пусть $d(L) = n-k-1$. Предположим, что существуют i, j такие, что $wt(e_i) = wt(e_j) = 3$, но $\mathrm{supp}(e_i) \cap \mathrm{supp}(e_j) = \varnothing$. Тогда $wt(e_i \oplus e_j) = 6$, причём $|\mathrm{supp}(e_i \oplus e_j) \cap S| = 2$, $|\mathrm{supp}(e_i \oplus e_j) \cap \mathrm{supp}(a_S)| = 4$, откуда $d(a_S, e_i \oplus e_j) = wt(a_S \oplus e_i \oplus e_j) = wt(a_S) + 2 - 4 = n-k-2$.

Пусть $b \in X_L$ имеет вес $n-k-1$. Тогда у b только в одной координате из $\overline{S}$ стоит нуль, пусть в m-й. Либо у e_i, либо у e_j в позиции m также находится нуль, так как иначе бы их носители пересекались. Для определённости пусть у e_i, но тогда $d(b, e_i) = wt(b \oplus e_i) = wt(b) + 1 - 2 = n-k-2$.

Таким образом, никакой $b \in X_L$ веса больше $n-k-2$ не удалён от L на расстояние $n-k-1$ (а меньшего веса и подавно), что противоречит $d(L) = n-k-1$. Следовательно, носители любых двух векторов веса 3 пересекаются.

($\Leftarrow$) Пусть носители любых двух базисных векторов веса 3 пересекаются. Докажем, что $d(a_S, L) = n-k-1$. Заметим, что векторы канонического базиса, веса которых не превосходят 2, не влияют на расстояние до a_S, как было доказано в теореме 2. Пусть в разложении x присутствует чётное число векторов веса 3. Тогда их можно разбить на пары $\{e_{1i}, e_{2i}\}$, причём $|\mathrm{supp}(e_{i_1} \oplus e_{i_2}) \cap S| = 2$, а $|\mathrm{supp}(e_{i_1} \oplus e_{i_2}) \cap \overline{S}| \leqslant 2$, так как носители e_{1i} и e_{2i} пересекаются. Отсюда $d(a_S, x) = wt(a_S \oplus x) \geqslant wt(a_S) = n-k$. Если в разложении x нечётное число векторов веса 3, то, вычтя из x один из них, получим вектор y такой, что $d(a_S, y) \geqslant n-k$, в силу только что доказанного. Убранный вектор имеет одну единицу на позиции из S и две — на позициях из $\overline{S}$. Тем самым $d(a_S, x) \geqslant d(a_S, y) + 1 - 2 \geqslant n-k-1$. Таким образом, вектор a_S удалён от L на расстояние $n-k-1$.

(a) Пусть $b \in X_L, b \neq a_S$ имеет вес $n-k-1$. В $\overline{S}$ у вектора b есть нуль, так как пересечение носителей всех базисных векторов веса 3 пусто, существует базисный вектор e_i веса 3 с нулём в той же позиции, что и у b. Тогда $d(b, e_i) = wt(b \oplus e_i) = (n-k-1) + 1 - 2 = n-k-2$, т. е. вектор b не может (вместе с соответствующим сдвигом) лежать в метрическом дополнении.

(b) Пусть $\bigcap\limits_{i:wt(e_i)=3} \mathrm{supp}(e_i) = \{m\}$. Тогда, убрав m-ю координату у всех векторов пространства, получим k-мерное подпространство L' в $\mathbb{F}_2^{n-1}$, удовлетворяющее условиям теоремы 2. Значит, $d(L') = n-k-1$ и $\widehat{L'} = a_{S(L')} \oplus L'$. Вернув m-ю координату вектору $a_{S(L')}$ (заполнив её единицей

и нулём соответственно), получим n-мерные векторы $a_{S(L)}$ и b, причём

$$n-k-1=\min_{x'\in L'} d(a_{S(L')},x')\leqslant \min_{x\in L} d(a_{S(L)},x)=d(a_{S(L)},L).$$

Аналогично для вектора b. Тем самым $(a_{S(L)}\oplus L)\cup(b\oplus L)\subseteq \widehat{L}$. Доказательство отсутствия других сдвигов в $\widehat{L}$ проводится точно так же, как в п. (a).

(c) Повторяем доказательство п. (b) для m-й и l-й координат. Теорема 3 доказана.

При дальнейшем ослаблении ограничений на веса векторов канонического базиса анализ представляется трудноосуществимым.

5. Метрические дополнения аффинных подпространств

Нетрудно убедиться, что все приведённые выше результаты верны и для аффинных подпространств. В самом деле, пусть $A\subseteq \mathbb{F}_2^n$ — аффинное подпространство и $A=a\oplus L$, где L — линейное подпространство. Пусть $d(L)=k$. Тогда, поскольку сдвиг всего пространства $\mathbb{F}_2^n$ на вектор a является изометрией пространства (т. е. сохраняет расстояние между векторами), сразу заключаем, что $d(A)=k$ и $\widehat{A}=a\oplus\widehat{L}$. Это наблюдение позволяет свести задачу нахождения максимального расстояния и метрического дополнения аффинного подпространства к этой же задаче для соответствующего ему линейного подпространства, т. е. можно переформулировать результаты разд. 3 и 4 для аффинных подпространств.

6. Метрически регулярные подпространства

Известно, что подпространство аффинных функций метрически регулярно. Быть может, любое линейное подпространство обладает этим свойством? Оказывается, что нет.

Теорема 4. *Пусть $L\subseteq\mathbb{F}_2^n$ — линейное подпространство. В этом случае $x\in\widehat{\widehat{L}}$ тогда и только тогда, когда $\widehat{L}$ инвариантно относительно сдвига на x, т. е. $\widehat{L}=x\oplus\widehat{L}$.*

Доказательство. Напомним, что для линейных подпространств выполнено $d(L)=d(\widehat{L})$ (лемма 3).

($\Rightarrow$) Пусть $z\in\widehat{\widehat{L}}$. Это означает, что $d(z,y)\geqslant d(L)$ для любого $y\in\widehat{L}$. Зафиксируем произвольный y из $\widehat{L}$. Так как $y\oplus L$ целиком лежит в $\widehat{L}$

(см. следствие 1), $d(z, y \oplus x) \geqslant d(L)$ для всех $x \in L$, т. е. $d(z \oplus y, L) \geqslant d(L)$, а значит, $(z \oplus y) \in \widehat{L}$. В силу произвольности y имеем $\widehat{L} = z \oplus \widehat{L}$.

($\Leftarrow$) Пусть $\widehat{L} = z \oplus \widehat{L}$. Это в точности означает, что для любого $y \in \widehat{L}$ выполнено $d(z \oplus y, L) = d(L)$. Следовательно, $wt(z \oplus y) \geqslant d(L)$ для всех $y \in \widehat{L}$, т. е. $z \in \widehat{\widehat{L}}$, что и требовалось доказать. Теорема 4 доказана.

Следствие 2. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство, а $\widehat{L}$ — аффинное подпространство, т. е. $\widehat{L} = a \oplus L_1$, где $L_1 \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда $\widehat{\widehat{L}} = L_1$.*

С помощью следствия 2 и п. (b) теоремы 3 можно легко построить пример не являющегося метрически регулярным подпространства, так как объединение двух сдвигов линейного подпространства является аффинным подпространством.

Также, используя следствие 2, можно сразу выделить класс метрически регулярных подпространств таких, что $|L| = |\widehat{L}|$, т. е. максимально удалённый сдвиг всего один. Численные эксперименты для небольших n показали, что все линейные подпространства размерности 2 и $n-2$ с одним сдвигом в метрическом дополнении достигают верхней оценки значения $d(L)$. К сожалению, какой-либо общей оценки числа таких подпространств (как вычислительной, так и аналитической) найти не удалось.

Известно (см. разд. 2), что, например, все грани, $(n-1)$-мерные подпространства и подпространство аффинных функций от чётного числа переменных являются метрически регулярными подпространствами.

7. Метрическая регулярность полностью регулярных кодов

Интерес вызывают метрические свойства кодов. Определим полностью регулярный код, следуя [5]. Пусть $C \subseteq \mathbb{F}_2^n$ — произвольный код, r — его радиус покрытия, $C_i = \{x \in \mathbb{F}_2^n \mid d(x, C) = i\}$, $i = 0, \ldots, r$. Код C называется *полностью регулярным*, если для любого вектора x распределение его непосредственных соседей (векторов на расстоянии 1 от x) по множествам C_i зависит только от расстояния от x до кода C. Иными словами, если $x \in C_i$, то

$$|\{y \in C_{i-1} \mid d(x, y) = 1\}| = a_i, \quad |\{y \in C_{i+1} \mid d(x, y) = 1\}| = b_i,$$

где a_i, b_i — постоянные, зависящие от кода.

Теорема 5. *Пусть C — полностью регулярный код с радиусом покрытия r. Тогда C является метрически регулярным множеством, т. е. $\widehat{\widehat{C}} = C$.*

Доказательство. Зафиксируем произвольный вектор $x_r \in C_r$. Из определения расстояния Хэмминга следует, что существуют векторы x_0, $x_1, \ldots, x_{r-1}$ такие, что $x_i \in C_i$ и $d(x_i, x_{i+1}) = 1$, $i = 0, \ldots, r-1$. В силу полной регулярности C отсюда можно заключить, что для всех j у произвольного вектора $x \in C_j$ есть непосредственные соседи как в C_{j-1}, так и в C_{j+1} (если соответствующие множества определены). Следовательно, если $x \in C_i$ и $j > i$, то существует вектор $y \in C_j$ на расстоянии $j - i$ от x.

В терминах данной работы $\widehat{C} = C_r$, $d(C) = r$. Из только что доказанного следует, что для любого x из кода C выполняется $d(x, \widehat{C}) = r$. Пусть x — произвольный вектор длины n, который попадает в некоторое множество C_i, $i \leqslant r$. По доказанному существует $y \in C_r$ такой, что $d(x, y) = r - i \leqslant r$. Тем самым $d(\widehat{C}) = r$. Равенство $d(x, y) = r$ достигается тогда и только тогда, когда $i = 0$, т. е. когда $x \in C_0 = C$, откуда $C = \widehat{\widehat{C}}$. Теорема 5 доказана.

Обратное, вообще говоря, неверно. Например, линейный код $C = \{(000), (011)\}$ с радиусом покрытия $r = d(C) = 2$ и метрическим дополнением $\widehat{C} = \{(101), (110)\}$ метрически регулярный, но не полностью регулярный.

Заключение

Несмотря на то, что подпространство аффинных функций имеет малую размерность (в сравнении с размерностью пространства: $n + 1$ против 2^n), значительно приблизиться к каким-либо оценкам мощности его метрического дополнения (бент-функций) на данный момент не удалось. Тем не менее не исключено, что техника метрических дополнений может быть развита и использована для частичного или полного разрешения вопросов, связанных с бент-функциями и максимально нелинейными функциями в целом.

ЛИТЕРАТУРА

1. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
2. **Carlet C.** Lower bounds on the higher order nonlinearities of Boolean functions and their applications to the inverse function // Proc. IEEE Inf. Theory Workshop (Porto, May 5–9, 2008). Piscataway: IEEE, 2008. P. 333–337.
3. **Kavut S., Maitra S., Yucel M. D.** Search for Boolean functions with excellent profiles in the rotation symmetric class // IEEE Trans. Inf. Theory. 2007. Vol. 53, No. 5. P. 1743–1751.

4. **Maitra S., Sarkar P.** Maximum nonlinearity of symmetric Boolean functions on odd number of variables // IEEE Trans. Inf. Theory. 2002. Vol. 48, No. 9. P. 2626–2630.
5. **Neumaier A.** Completely regular codes // Discrete Math. 1992. Vol. 106. P. 353–360.
6. **Rothaus O. S.** On "bent" functions // J. Comb. Theory, Ser. A. 1976. Vol. 20, No. 3. P. 300–305.
7. **Sun G., Wu C.** The lower bound on the second-order nonlinearity of a class of Boolean functions with high nonlinearity // Appl. Algebra Eng. Commun. Comput. 2011. Vol. 22, No. 1. P. 37–45.
8. **Tokareva N. N.** Duality between bent functions and affine functions // Discrete Math. 2012. Vol. 312, No. 3. P. 666–670.
9. **Tokareva N. N.** Bent functions: results and applications to cryptography. San Diego: Acad. Press, 2015. 220 p.

Облаухов Алексей Константинович

Статья поступила
22 сентября 2015 г.

Исправленный вариант —
9 марта 2016 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
July–August 2016. Volume 23, No. 3. P. 93–106

UDC 519.7 DOI: 10.17377/daio.2016.23.513

METRIC COMPLEMENTS TO SUBSPACES IN THE BOOLEAN CUBE

A. K. Oblaukhov[1]
[1]Novosibirsk State University,
2 Pirogov St., 630090 Novosibirsk, Russia
e-mail: oblaukhov@gmail.com

Abstract. We study the *metric complements* to sets in the Boolean cube; i. e. the subsets maximally distant from given subset. We obtain the general form for the metric complement of a linear subspace and some more exact description for the class of subspaces with basis of a special form. It is proved that the completely regular codes (including perfect and uniformly packed) are metrically regular. Bibliogr. 9.

Keywords: subspace, metrically regular set, metric complement, completely regular code, bent-function.

REFERENCES

1. **F. J. MacWilliams** and **N. J. A. Sloane,** *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977 (North-Holland Math. Libr., Vol. 16). Translated under the title *Teoriya kodov, ispravlyayushchikh oshibki,* Svyaz', Moscow, 1979.
2. **C. Carlet,** Lower bounds on the higher order nonlinearities of Boolean functions and their applications to the inverse function, in *Proc. 2008 IEEE Inf. Theory Workshop, Porto, Portugal, May 5–9, 2008,* pp. 333–337, IEEE, Piscataway, 2008.
3. **S. Kavut, S. Maitra,** and **M. D. Yucel,** Search for Boolean functions with excellent profiles in the rotation symmetric class, *IEEE Trans. Inf. Theory,* **53**, No. 5, 1743–1751, 2007.
4. **S. Maitra** and **P. Sarkar,** Maximum nonlinearity of symmetric Boolean functions on odd number of variables, *IEEE Trans. Inf. Theory,* **48**, No. 9, 2626–2630, 2002.
5. **A. Neumaier,** Completely regular codes, *Discrete Math.,* **106**, 353–360, 1992.
6. **O. S. Rothaus,** On "bent" functions, *J. Comb. Theory, Ser. A*, **20**, No. 3, 300–305, 1976.
7. **G. Sun** and **C. Wu,** The lower bound on the second-order nonlinearity of a class of Boolean functions with high nonlinearity, *Appl. Algebra Eng. Commun. Comput.,* **22**, No. 1, 37–45, 2011.

8. N. N. Tokareva, Duality between bent functions and affine functions, *Discrete Math.,* **312**, No. 3, 666–670, 2012.

9. N. N. Tokareva, *Bent Functions: Results and Applications to Cryptography*, Academic Press, San Diego, 2015.

Alexey K. Oblaukhov

Received
22 September 2015

Revised
9 March 2016