ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.
3. *Фомичев В. М.* Свойства путей в графах и мультиграфах // Прикладная дискретная математика. 2010. № 1(7). С. 118–124.

УДК 519.7 DOI 10.17223/2226308X/8/4

О НЕКОТОРЫХ МЕТРИЧЕСКИХ СВОЙСТВАХ ЛИНЕЙНЫХ ПОДПРОСТРАНСТВ БУЛЕВА КУБА[1]

А. К. Облаухов

Исследуются метрические дополнения подмножеств булева куба. Дана общая характеризация метрических дополнений линейных подпространств. Доказано, что полностью регулярные коды являются метрически регулярными.

Ключевые слова: *подпространство, метрически регулярное множество, метрическое дополнение, полностью регулярный код.*

Через $\mathbb{F}_2^n$ в работе обозначается множество всех двоичных векторов длины n. *Расстоянием Хэмминга* от вектора $y \in \mathbb{F}_2^n$ до множества $X \subseteq \mathbb{F}_2^n$ называется $\mathrm{d}(y, X) = \min\limits_{x \in X} \mathrm{wt}(y \oplus x)$, $\mathrm{wt}(\cdot)$ — двоичный вес (число единиц в векторе). *Максимальным расстоянием* от множества $X \subseteq \mathbb{F}_2^n$ называется $\mathrm{d}(X) = \max\limits_{z \in \mathbb{F}_2^n} \mathrm{d}(z, X)$. Вектор y называется *максимально удалённым* от множества X, если $\mathrm{d}(y, X) = \mathrm{d}(X)$. Через $|X|$ обозначается мощность множества X, через $\mathrm{supp}(y)$ — носитель вектора y — множество $\{i : y_i = 1\}$. *Сдвигом* множества X на вектор $a \in \mathbb{F}_2^n$ называется множество $a \oplus X = \{a \oplus x : x \in X\}$.

Множество $Y \subseteq \mathbb{F}_2^n$, состоящее из всех максимально удалённых от множества X векторов, назовём *метрическим дополнением* множества X и обозначим $Y = \widehat{X}$. Множество $X \subseteq \mathbb{F}_2^n$ называется *метрически регулярным*, если $X = \widehat{\widehat{X}}$.

В [1] была поставлена задача классификации метрически регулярных множеств. Известно [2], что множество всех аффинных функций метрически регулярно.

Исследуются свойства метрических дополнений линейных подпространств. Множество $L \subseteq \mathbb{F}_2^n$ называется *линейным подпространством*, если для любых векторов $x, y \in L$ их сумма $x \oplus y$ лежит в L. Следующие два утверждения характеризуют метрические дополнения линейных подпространств.

Утверждение 1. Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда множество $\widehat{L}$ — это объединение сдвигов подпространства L. Пусть $a \in \mathbb{F}_2^n$ — произвольный вектор. Тогда расстояние от L до любого вектора из сдвига $a \oplus L$ совпадает с расстоянием от L до вектора a.

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

$$\mathrm{d}(L) \leqslant n - k.$$

У каждого линейного подпространства L существует единственный базис специального вида, который назовём *каноническим базисом*. Матрица из векторов этого базиса имеет вид

[1]Исследование выполнено при финансовой поддержке РФФИ (проект № 15-31-20635).

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

Каноническим представителем назовём вектор, у которого в координатах s_i, $i = 1, \dots, k$, находятся нули, а остальные координаты произвольны. Нетрудно доказать, что канонические представители определяют все сдвиги подпространства, причём два разных представителя определяют два разных сдвига.

Теорема 2. Равенство в оценке теоремы 1 достигается тогда и только тогда, когда $\mathrm{wt}(e_i) \leqslant 2$ для всех $i \in \{1, \dots, k\}$, где $\{e_i : i = 1, \dots, k\}$ — канонический базис L. Множество $\widehat{L}$ в таком случае совпадает со сдвигом $a \oplus L$, где a — канонический представитель максимального веса.

Теорема 3. Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k, $\mathrm{wt}(e_i) \leqslant 3$ для всех e_i из канонического базиса L и существует вектор канонического базиса веса 3. Тогда $\mathrm{d}(L) = n - k - 1$ тогда и только тогда, когда $\mathrm{supp}(e_i) \cap \mathrm{supp}(e_j) \neq \varnothing$ для всех i, j, таких, что $\mathrm{wt}(e_i) = \mathrm{wt}(e_j) = 3$. При этом сдвиг на канонический представитель максимального веса лежит в $\widehat{L}$.

При наложении дополнительных условий на базис добавляются дополнительные максимально удалённые сдвиги. Все приведённые выше результаты тривиально обобщаются на случай аффинных подпространств.

Известно, что подпространство аффинных функций является метрически регулярным. Однако не любое линейное подпространство обладает этим свойством.

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

Следствие 1. Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство, а $\widehat{L}$ — аффинное подпространство, то есть $\widehat{L} = a \oplus L_1$, где $L_1 \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда $\widehat{\widehat{L}} = L_1$.

Используя следствие 1, можно сразу выделить класс метрически регулярных подпространств, таких, что $|L| = |\widehat{L}|$.

Интерес также вызывают метрические свойства различных кодов. Следуя определению из [3], код $\mathcal{C} \subseteq \mathbb{F}_2^n$ называется *полностью регулярным*, если весовой спектр любого его сдвига $x \oplus \mathcal{C}$ зависит только от $\mathrm{d}(x, \mathcal{C})$. Полностью регулярные коды введены в [4], там же доказано, что всякий совершенный код и всякий равномерно упакованный код являются полностью регулярными.

Теорема 5. Пусть $\mathcal{C} \subseteq \mathbb{F}_2^n$ — полностью регулярный код. Тогда $\mathcal{C}$ метрически регулярно.

Обратное, вообще говоря, неверно. Например, линейный код $\mathcal{C} = \{(000), (011)\}$ является метрически регулярным множеством с $\mathrm{d}(\mathcal{C}) = 2$, $\widehat{\mathcal{C}} = \{(101), (110)\}$, но не является полностью регулярным.

ЛИТЕРАТУРА

1. *Tokareva N. N.* Bent functions: results and applications to cryptography. Acad. Press. Elsevier, 2015. 230 p.
2. *Tokareva N. N.* Duality between bent functions and affine functions // Discr. Math. 2012. V. 312. Iss. 3. P. 666–670.
3. *Solé P.* Completely regular codes and completely transitive codes // Discr. Math. 1990. V. 81. Iss. 2. P. 193–201.
4. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory. Thesis. Universite Catholique de Louvain, 1973.

УДК 519.7 DOI 10.17223/2226308X/8/5

СВОЙСТВА ГРУППЫ, ПОРОЖДЁННОЙ ГРУППАМИ СДВИГОВ ВЕКТОРНОГО ПРОСТРАНСТВА И КОЛЬЦА ВЫЧЕТОВ

Б. А. Погорелов, М. А. Пудовкина

Аддитивные группы кольца вычетов $\mathbb{Z}_{2^n}$ и векторного пространства V_n над полем GF(2), а также порождённая ими группа G_n имеют общие системы импримитивности и являются подгруппами силовской 2-подгруппы симметрической группы $S(\mathbb{Z}_{2^n})$. Данные группы возникают в криптографии при использовании в качестве способа наложения ключа относительно операций сложения из V_n и $\mathbb{Z}_{2^n}$. В работе приведено подстановочное строение подгрупп группы G_n. Показано, что подгруппами G_n являются группа нижнетреугольных $(n\times n)$-матриц над полем GF(2) и полная аффинная группа над кольцом вычетов $\mathbb{Z}_{2^n}$. Рассмотрена характеризация импримитивных подгрупп группы G_n.

Ключевые слова: *сплетение групп подстановок, импримитивная группа, силовская 2-подгруппа, аддитивная группа кольца вычетов, аддитивная группа векторного пространства, ARX-шифрсистема.*

Аддитивная группа $\mathbb{Z}_{2^n}^+$ кольца вычетов $\mathbb{Z}_{2^n}$ и аддитивная группа V_n^+ n-мерного векторного пространства V_n над полем GF(2), а также порождённая ими группа $G_n = \left\langle V_n^+, \mathbb{Z}_{2^n}^+ \right\rangle$ являются подгруппами силовской 2-подгруппы $P_n \in \mathrm{Syl}_2\left(S_{2^n}\right)$, описываемой операцией сплетения $P_n = P_2 \wr P_{n-1}$. Все эти группы имеют общие системы импримитивности $W^{(i,n)} = \left\{W_0^{(i,n)}, \ldots, W_{2^i-1}^{(i,n)}\right\}$, где

$$W_t^{(i,n)} = \left\{j \in \{0, \ldots, 2^n - 1\} : j \equiv t \,(\mathrm{mod}\ 2^i)\right\},\ i = 1, \ldots, n-1,\ t = 0, \ldots, 2^i - 1.$$

Заметим, что в криптографии группа G_n возникает в блочных шифрсистемах, использующих в качестве наложения ключа сложения в кольце вычетов и в векторном пространстве, например IDEA, ARX. В связи с наличием общих систем импримитивности у групп $\mathbb{Z}_{2^n}^+$, V_n^+ операции сложения $+$, $\oplus$ в кольце вычетов $\mathbb{Z}_{2^n}$ и в векторном пространстве V_n соответственно оказались достаточно близки.

Приведём подстановочное строение подгрупп группы G_n, из описания которого, в частности, следует известный порядок группы G_n, полученный ранее в [1].

Теорема 1. Пусть $n \geqslant 2$. Тогда:

1) если $\varphi_{n-1}^{(G_n)}$ — естественный гомоморфизм импримитивной группы G_n в группу, действующую на множестве блоков импримитивности $\{\{0, 2^{n-1}\}, \ldots, \{2^{n-1} - 1, 2^n - 1\}\}$, то $\mathrm{Im}\varphi_{n-1}^{(G_n)} \cong G_{n-1}$ и