ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7 DOI 10.17223/20710410/65/1

О ПОДСТАНОВКАХ, РАЗРУШАЮЩИХ СТРУКТУРУ ПОДПРОСТРАНСТВ ОПРЕДЕЛЁННЫХ РАЗМЕРНОСТЕЙ[1]

Н. А. Коломеец

Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия

E-mail: kolomeec@math.nsc.ru

Рассматриваются асимптотические оценки мощности множеств $\mathcal{P}_n^k$ обратимых функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, для которых любое $U \subseteq \mathbb{F}_2^n$ и его образ $F(U)$ не могут одновременно являться аффинными подпространствами $\mathbb{F}_2^n$ размерности k, где $3 \leqslant k \leqslant n-1$. Приведены нижние оценки мощности $\mathcal{P}_n^k$ и $\mathcal{P}_n^k \cap \ldots \cap \mathcal{P}_n^{n-1}$, усиливающие результаты 2007 г. (W. E. Clark, X. Hou, A. Mihailovs) о непустоте данных множеств. Доказано, что почти все подстановки на $\mathbb{F}_2^n$ принадлежат $\mathcal{P}_n^4 \cap \ldots \cap \mathcal{P}_n^{n-1}$. Для мощности множества $\mathcal{P}_n^3$ получены асимптотические оценки снизу и сверху с точностью до $o(2^n!)$: $o(1) \leqslant |\mathcal{P}_n^3|/2^n! - (1-\rho) \leqslant \rho^2/2 + o(1)$, где $\rho = 5/224$. Данные оценки справедливы и для мощности $\mathcal{P}_n^3 \cap \ldots \cap \mathcal{P}_n^{n-1}$. Схожим образом оценено снизу число функций из $\mathcal{P}_n^4 \cap \ldots \cap \mathcal{P}_n^{n-1}$, которые отображают ровно одно аффинное подпространство $\mathbb{F}_2^n$ размерности 3 в аффинное подпространство. Приведена связь ограничений компонентных функций F со случаем, когда и U, и $F(U)$ — аффинные подпространства $\mathbb{F}_2^n$. Предложена характеризация дифференциально 4-равномерных подстановок в рассматриваемых терминах.

Ключевые слова: *аффинные подпространства, асимптотические оценки, нелинейность, дифференциальная равномерность, APN-функции.*

ON PERMUTATIONS THAT BREAK SUBSPACES OF SPECIFIED DIMENSIONS

N. A. Kolomeec

Sobolev Institute of Mathematics, Novosibirsk, Russia

We consider the sets $\mathcal{P}_n^k$ consisting of invertible functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that any $U \subseteq \mathbb{F}_2^n$ and its image $F(U)$ are not simultaneously k-dimensional affine subspaces of $\mathbb{F}_2^n$, where $3 \leqslant k \leqslant n-1$. We present lower bounds for the cardinalities of all such $\mathcal{P}_n^k$ and $\mathcal{P}_n^k \cap \ldots \cap \mathcal{P}_n^{n-1}$ that improve the result of W. E. Clark, X. Hou, and A. Mihailovs, 2007, providing that these sets are not empty. We prove that almost all permutations of $\mathbb{F}_2^n$ belong to $\mathcal{P}_n^4 \cap \ldots \cap \mathcal{P}_n^{n-1}$. Asymptotic lower and upper bounds of $|\mathcal{P}_n^3|$ up to $o(2^n!)$ are obtained: $o(1) \leqslant |\mathcal{P}_n^3|/2^n! - (1-\rho) \leqslant \rho^2/2 + o(1)$, where $\rho = 5/224$. They are correct for $|\mathcal{P}_n^3 \cap \ldots \cap \mathcal{P}_n^{n-1}|$ as well. The number of functions from $\mathcal{P}_n^4 \cap \ldots \cap \mathcal{P}_n^{n-1}$ that map exactly one 3-dimensional affine subspace of $\mathbb{F}_2^n$ to an affine subspace is estimated.

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF–2022–0019).

The connection between the restrictions of component functions of F and the case when both U and $F(U)$ are affine subspaces of $\mathbb{F}_2^n$ is obtained. The characterization of differentially 4-uniform permutations in the mentioned terms is provided.

Keywords: *affine subspaces, asymptotic bounds, nonlinearity, differential uniformity, APN functions.*

Введение

В работе рассматриваются ограничения взаимно однозначных отображений на аффинные подпространства $\mathbb{F}_2^n$ в случае, когда их образ также является аффинным подпространством $\mathbb{F}_2^n$. Обозначая множество всех подстановок на $\mathbb{F}_2^n$ через $\mathcal{P}_n$, будем говорить, что $\pi \in \mathcal{P}_n$ *сохраняет структуру* аффинного подпространства $L \subseteq \mathbb{F}_2^n$, если $\pi(L) = \{\pi(x) : x \in L\}$ — аффинное подпространство $\mathbb{F}_2^n$; в противном случае π *разрушает структуру* L. Определим

$$\mathcal{L}_k(\pi) = \{L \subseteq \mathbb{F}_2^n : L \text{ и } \pi(L) \text{ — аффинные подпространства } \mathbb{F}_2^n \text{ размерности } k\} \quad (1)$$

и множества функций, разрушающих структуру подпространств определённых размерностей:

$$\mathcal{P}_n^k = \{\pi \in \mathcal{P}_n : \mathcal{L}_k(\pi) = \varnothing\} \quad \text{и} \quad \mathcal{P}_n^{\geqslant k} = \mathcal{P}_n^k \cap \mathcal{P}_n^{k+1} \cap \ldots \cap \mathcal{P}_n^{n-1}. \quad (2)$$

Основное внимание в работе будем уделять именно этим множествам. Заметим, что $\mathcal{P}_n^0$, $\mathcal{P}_n^1$ и $\mathcal{P}_n^n$ всегда пусты, так как все подмножества $\mathbb{F}_2^n$ из 1, 2 и 2^n элементов являются аффинными подпространствами. Будем называть такие размерности *тривиальными*.

Впервые данные свойства подстановок были рассмотрены в работе [1]. Сохранение структуры подпространства $L \subseteq \mathbb{F}_2^n$ функцией $\pi \in \mathcal{P}_n$ позволяет использовать $\pi|_L : L \to \pi(L)$ так же, как и $f|_L$ для булевой функции $f : \mathbb{F}_2^n \to \mathbb{F}_2$: зафиксировать некоторые базисы L и $\pi(L)$ и перейти к подстановке вида $\mathbb{F}_2^{\dim L} \to \mathbb{F}_2^{\dim L}$. При этом её криптографические свойства (см. [2–6]), инвариантные относительно применения обратимых аффинных преобразований, не зависят от выбора базисов. К таким свойствам, например, относятся алгебраическая степень, нелинейность и порядок дифференциальной равномерности. Одним из подходов к построению функций могут быть их конструкции как подфункций [7]. Для этого использовались и схожие концепции подфункций [8–10]. Разрушение структуры подпространств связано с инвариантными подпространствами отображений (см., например, [11]), которые могут быть использованы в атаке с помощью инвариантного подпространства [12] (см. также обобщение атаки [13] и работы о построении таких подпространств, начиная с S-блоков [14, 15]). Одним из важнейших классов криптографических функций является множество APN-подстановок [16], которое в точности совпадает с $\mathcal{P}_n^2$.

Во-первых, в работе рассматривается характеризация множеств $L \in \mathcal{L}_k(\pi)$ через компонентные функции $\pi \in \mathcal{P}_n$, постоянные на L (следствие 1). Данное свойство можно связать и с нелинейностью π. Также через свойства элементов $\mathcal{L}_2(\pi)$ охарактеризованы дифференциально 4-равномерные подстановки: мощность пересечения двух его различных элементов-множеств не должна превышать 1 (см. утверждение 4). Далее мы усиливаем результаты [1] о непустоте $\mathcal{P}_n^{\geqslant 3}$, т. е. о существовании функций, разрушающих структуру всех аффинных подпространств $\mathbb{F}_2^n$ размерностей от 3 до $n-1$. Для этого используется среднее число $\rho_{n,k}$ (и $\sigma_{n,k}$) элементов в $\mathcal{L}_k(\pi)$ (и $\mathcal{L}_k(\pi) \cup \ldots \cup \mathcal{L}_{n-1}(\pi)$) для $\pi \in \mathcal{P}_n$ (см. утверждения 5, 6 и 7 об их свойствах). Главным образом, результаты касаются их мощности при $n \to \infty$. Показано, что почти

все функции разрушают структуру всех аффинных подпространств $\mathbb{F}_2^n$ размерности от 4 до $n-1$, т. е. $|\mathcal{P}_n^{\geqslant 4}| = 2^n! - o(2^n!)$ (см. следствие 5). Получены следующие оценки для $|\mathcal{P}_n^3|$, справедливые и для $|\mathcal{P}_n^{\geqslant 3}|$: $o(1) \leqslant |\mathcal{P}_n^3|/2^n! - (1-\rho) \leqslant \rho^2/2 + o(1)$, где $\rho = 5/224$ (см. теорему 2). Оценено также количество функций, сохраняющих структуру ровно одного аффинного подпространства $\mathbb{F}_2^n$ (см. следствие 6).

1. Определения

Пусть $\mathbb{F}_2^n$ — векторное пространство размерности n над полем $\mathbb{F}_2$, состоящем из двух элементов. Сложение в $\mathbb{F}_2^n$ обозначим через $\oplus$. Для $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$ определим $\langle x, y\rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$. *Аффинное подпространство* $L \subseteq \mathbb{F}_2^n$ определяется как $L = a \oplus L' = \{a \oplus x : x \in L'\}$, где L' — линейное подпространство $\mathbb{F}_2^n$ и $a \in \mathbb{F}_2^n$, его размерность $\dim L$ равна $\log_2 |L|$. Множества всех линейных и аффинных подпространств $\mathbb{F}_2^n$ размерности k обозначим через $\mathcal{S}_n^k$ и $\widehat{\mathcal{S}}_n^k$ соответственно. Для $L' \in \mathcal{S}_n^k$ существует *ортогональное* подпространство $L'^{\perp} = \{y \in \mathbb{F}_2^n : \langle x, y\rangle = 0 \text{ для всех } x \in L'\}$, при этом $L'^{\perp} \in \mathcal{S}_n^{n-k}$. Через $\langle S\rangle$ и $\langle S\rangle_{\mathcal{A}}$ обозначим *линейную* и *аффинную оболочки* множества $S \subseteq \mathbb{F}_2^n$, т. е. пересечение всех $L \in \mathcal{S}_n^0 \cup \ldots \cup \mathcal{S}_n^n$ ($L \in \widehat{\mathcal{S}}_n^0 \cup \ldots \cup \widehat{\mathcal{S}}_n^n$), содержащих S.

Функция вида $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ называется *векторной булевой функцией*, а если $m = 1$, то *булевой функцией*. Её *компонентной функцией* называется $F_a : x \mapsto \langle a, F(x)\rangle$, где $a \in \mathbb{F}_2^m \setminus \{0\}$. Любая F может быть единственным образом представлена в виде *полинома Жегалкина* (*алгебраической нормальной формы, АНФ*):

$$F(x_1, x_2, \ldots, x_n) = \bigoplus_{a \in \mathbb{F}_2^n} g_a x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}, \text{ где } g_a \in \mathbb{F}_2^m \text{ и } 0^0 = 1.$$

Степенью $\deg F$ называется степень её полинома Жегалкина. Функция F называется *аффинной*, если $\deg F \leqslant 1$, и *квадратичной*, если $\deg F = 2$. *Вес Хэмминга* булевой функции $f : \mathbb{F}_2^n \to \mathbb{F}_2$ — количество $x \in \mathbb{F}_2^n$, таких, что $f(x) = 1$; f *сбалансирована*, если её вес равен 2^{n-1}. *Расстояние Хэмминга* между $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ — количество $x \in \mathbb{F}_2^n$, на которых $f(x) \neq g(x)$.

Нелинейностью N_f функции f называется расстояние Хэмминга от f до ближайшей к ней аффинной булевой функции. Нелинейность N_F векторной функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ определяется как

$$N_F = \min_{b \in \mathbb{F}_2^m \setminus \{0\}} N_{F_b}.$$

Это инвариант относительно *аффинной эквивалентности*: $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ аффинно эквивалентны, если существуют обратимые аффинные преобразования $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$ и $B : \mathbb{F}_2^m \to \mathbb{F}_2^m$, такие, что $G(x) = B(F(A(x)))$ для всех $x \in \mathbb{F}_2^n$. Нетрудно видеть, что $|\mathcal{L}_k(\pi)|$, определённое в (1), также является инвариантом относительно аффинной эквивалентности, а множества $\mathcal{P}_n^k$ и $\mathcal{P}_n^{\geqslant k}$ из (2) замкнуты относительно аффинной эквивалентности.

Более подробную информацию о функциях и их криптографических свойствах можно найти в [2–6].

2. Связь с криптографическими свойствами

Приведём связь множеств $\mathcal{L}_k(\pi)$ с компонентными функциями π, её нелинейностью и порядком дифференциальной равномерности. Начнём с тривиального свойства элементов $\mathcal{L}_0(\pi) \cup \ldots \cup \mathcal{L}_n(\pi)$.

Утверждение 1. Пусть $\pi \in \mathcal{P}_n$ сохраняет структуру аффинных подпространств $L, U \subseteq \mathbb{F}_2^n$. Тогда π сохраняет структуру $L \cap U$.

Доказательство. Ясно, что для любого $x \in L \cap U$ справедливо $x \in \pi(L) \cap \pi(U)$, т. е. $\pi(L \cap U) \subseteq \pi(L) \cap \pi(U)$. Учитывая существование π^{-1}, получаем $\pi(L \cap U) = \pi(L) \cap \pi(U)$. ■

2.1. Компонентные функции и нелинейность

Утверждение 2. Пусть $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ и U — подпространство $\mathbb{F}_2^n$. Тогда

$$\{a \in \mathbb{F}_2^m : x \in U \mapsto \langle a, F(x)\rangle \text{ — постоянна}\} = (F(u) \oplus \langle F(U)\rangle_{\mathcal{A}})^{\perp}, \text{ где } u \in U,$$

т. е. ровно $2^{m-\dim\langle F(U)\rangle_{\mathcal{A}}} - 1$ компонентных функций F постоянны на U.

Доказательство. Пусть $a \in \mathbb{F}_2^m$, $u \in U$, $v = F(u)$ и $V = F(U) \subseteq \mathbb{F}_2^m$. Тогда функция $F_a : x \mapsto \langle a, F(x)\rangle$ постоянна на U, если и только если

$$\langle a, v \oplus y\rangle = 0 \text{ для всех } y \in V.$$

Это эквивалентно тому, что $a \in \langle v \oplus V\rangle^{\perp}$. Убрав $a = 0$, получим ровно $2^{m-\dim\langle v\oplus V\rangle} - 1$ различных компонентных функций. Для завершения доказательства осталось показать, что

$$\langle V\rangle_{\mathcal{A}} = v \oplus \langle v \oplus V\rangle. \tag{3}$$

Действительно, любое аффинное подпространство $V' \subseteq \mathbb{F}_2^m$, содержащее V, содержит и v, т. е. $v \oplus V' \supseteq v \oplus V$ и $v \oplus V'$ — линейное. Следовательно, $v \oplus V'$ содержит $\langle v \oplus V\rangle$. Значит, $\langle V\rangle_{\mathcal{A}} \supseteq v \oplus \langle v \oplus V\rangle$. Но $v \oplus \langle v \oplus V\rangle$ — это также аффинное подпространство $\mathbb{F}_2^m$, содержащее V, т. е. (3) доказано. ■

Для взаимно однозначных функций справедлив следующий критерий.

Следствие 1. Пусть $\pi \in \mathcal{P}_n$ и U — аффинное подпространство $\mathbb{F}_2^n$. Тогда π сохраняет структуру U, если и только если ровно $2^{n-\dim U} - 1$ компонентных функций π постоянны на U.

Доказательство. Пусть $u \in U, V \subseteq \mathbb{F}_2^m, |V| = 2^{n-\dim U}, 0 \in V$ и $\langle v, \pi(x)\rangle$ постоянна на U тогда и только тогда, когда $v \in V$. Ясно, что V — линейное подпространство $\mathbb{F}_2^n$, так как множество постоянных функции замкнуто относительно сложения. Следовательно, $\pi(u) \oplus \pi(U) \subseteq V^{\perp}$. Но тогда $\dim\langle \pi(U)\rangle_{\mathcal{A}} \leqslant n - (n - \dim U) = \dim U$. С учётом взаимной однозначности π, $\pi(U)$ может быть только аффинным подпространством $\mathbb{F}_2^n$. Доказательство в другую сторону напрямую следует из утверждения 2. ■

Отметим, что булевы функции, постоянные на некотором аффинном подпространстве $\mathbb{F}_2^n$ размерности k, называются k-нормальными [17–19]. Если $\dim\langle F(U)\rangle_{\mathcal{A}} < m$ для $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ (или $U \in \mathcal{L}_k(F)$ в случае обратимой F и $k < n$), то F имеет $\dim U$-нормальную компонентную функцию. Известно, что нелинейность таких функций (а значит, и N_F) можно оценить сверху как $2^{n-1} - 2^{\dim U-1}$ [20, 21]. Эту и другие оценки нелинейности можно найти в работе [7]. Оценка $2^{n-1} - 2^{\dim U-1}$ при $U \in \mathcal{L}_k(F)$ следует также из [12]. Таким образом, функции с высокой нелинейностью разрушают структуру аффинных подпространств $\mathbb{F}_2^n$ больших размерностей.

Интересным является и критерий сохранения структуры гиперплоскостей, доказанный в одну сторону в [7].

Следствие 2. Пусть $\pi \in \mathcal{P}_n$. Тогда $L \in \mathcal{L}_{n-1}(\pi) \iff a \oplus L \in \mathcal{L}_{n-1}(\pi)$ для всех $a \in \mathbb{F}_2^n$. При этом

$$|\mathcal{L}_{n-1}(\pi)| = 2|\{b \in \mathbb{F}_2^n \setminus \{0\} : x \mapsto \langle b, \pi(x)\rangle \text{ — аффинна}\}|$$

и $N_\pi = 0 \iff \mathcal{L}_{n-1}(\pi) \neq \varnothing$.

Доказательство. Если $L \in \mathcal{L}_{n-1}(\pi)$, то $\pi(\mathbb{F}_2^n \setminus L) = \mathbb{F}_2^n \setminus \pi(L)$, где $\mathbb{F}_2^n \setminus L$ и $\mathbb{F}_2^n \setminus \pi(L)$ являются аффинными подпространствами $\mathbb{F}_2^n$ размерности $n-1$ (гиперплоскостями). Следовательно, $\mathbb{F}_2^n \setminus L \in \mathcal{L}_{n-1}(\pi)$, т. е. $\mathcal{L}_{n-1}(\pi)$ разбивается на пары $\{L, \mathbb{F}_2^n \setminus L\}$. При этом $\mathbb{F}_2^n \setminus L = a \oplus L$ для некоторого $a \in \mathbb{F}_2^n$, и в целом $s \oplus L$ для $s \in \mathbb{F}_2^n$ совпадает либо с L, либо с $\mathbb{F}_2^n \setminus L$.

Далее, по следствию 1: $L \in \mathcal{L}_{n-1}(\pi) \iff$ ровно одна компонентная функция π_b постоянна на L, $b \in \mathbb{F}_2^n \setminus \{0\}$. Но так как π обратима, её компонентная функция π_b должна быть сбалансированной [5]. Следовательно, π_b постоянна и на $\mathbb{F}_2^n \setminus L$, т. е. она является аффинной. Таким образом, пара $\{L, \mathbb{F}_2^n \setminus L\} \subseteq \mathcal{L}_{n-1}(\pi)$ соответствует некоторой одной аффинной π_b.

В обратную сторону справедливо аналогичное соответствие, так как аффинность некоторой компонентной функции означает, что она постоянна на некоторой гиперплоскости $L \in \mathcal{S}_n^k$ и её сдвиге $\mathbb{F}_2^n \setminus L$ [5], т. е. аффинная (и сбалансированная) π_b соответствует ровно одной паре $\{L, \mathbb{F}_2^n \setminus L\} \subseteq \mathcal{L}_{n-1}(\pi)$. Обратим внимание, что компонентные функции π_b и π_c при различных $b, c \in \mathbb{F}_2^n$, являющиеся аффинными, не могут иметь одно и то же L: тогда их сумма $\pi_b \oplus \pi_c$, являющаяся компонентной функцией $\pi_{b \oplus c}$, не будет сбалансированной.

Осталось воспользоваться определением: $N_\pi = 0 \iff$ некоторая из компонентных функций π аффинна. ■

2.2. Дифференциальная равномерность и APN-функции

Порядком дифференциальной равномерности $\delta(G)$ функции $G : u \oplus L \to u' \oplus L'$, где L и L' — линейные подпространства $\mathbb{F}_2^n$ и $\mathbb{F}_2^m$ соответственно, $u \in \mathbb{F}_2^n$ и $u' \in \mathbb{F}_2^m$, называется минимальное t, такое, что при любых параметрах $a \in L \setminus \{0\}$ и $b \in L'$ уравнение $G(x) \oplus G(x \oplus a) = b$ имеет не более t решений относительно $x \in u \oplus L$. Если $|L| = |L'|$ и $\delta(G) = 2$, то G называется *APN-функцией*. Обратим внимание, что в литературе также встречается термин *порядок разностной равномерности* (по аналогии с разностным криптоанализом).

Отметим, что свойства $\delta(G)$ полностью соответствуют свойствам $\delta(G')$ для функций $G' : \mathbb{F}_2^{\dim L} \to \mathbb{F}_2^{\dim L'}$; для $\pi \in \mathcal{P}_n$ и $L \in \mathcal{L}_k(\pi)$, выполняется $\delta(\pi|_L) \leqslant \delta(\pi)$. Данное свойство активно используется, например, в [7]. Одним из эквивалентных определений APN-подстановок является следующее: $\pi \in \mathcal{P}_n$ — APN-функция $\iff \mathcal{L}_2(\pi) = \varnothing$.

В общем случае сохранение структуры подпространств определённых размерностей не ограничивает порядок дифференциальной равномерности функции, примером чего является функция обращения элементов конечного поля, порядок дифференциальной равномерности которой равен 2 и 4 при нечётном и чётном числе переменных соответственно [16]. Согласно [11], справедливо следующее

Утверждение 3 (Н. А. Коломеец, Д. А. Быков, 2024). Пусть $\pi(x) = x^{2^n-2}$ для $x \in \mathbb{F}_{2^n}$ и $2 \leqslant k \leqslant n$. Тогда $|\mathcal{L}_k(\pi)| = (2^n - 1)/(2^k - 1)$ при $k \mid n$, иначе $\mathcal{L}_k(\pi) = \varnothing$.

Однако можно гарантировать пустоту некоторых $\mathcal{L}_k(\pi)$ в случае APN-подстановок.

Следствие 3. Пусть $n > 2$ и $\pi \in \mathcal{P}_n$ — APN-функция. Тогда $\mathcal{L}_2(\pi) = \mathcal{L}_4(\pi) = \mathcal{L}_{n-1}(\pi) = \varnothing$. Если π — квадратичная, то $\mathcal{L}_k(\pi) = \varnothing$ для всех чётных k, $1 \leqslant k \leqslant n$.

Доказательство. Пусть $L \in \mathcal{L}_k(\pi)$. Поскольку $\delta(\pi|_L) \leqslant \delta(\pi)$, $\pi|_L$ также должна быть APN-подстановкой. Таким образом, $\mathcal{L}_2(\pi)$ пусто в силу эквивалентного определения APN-подстановок. Множество $\mathcal{L}_4(\pi)$ пусто в силу несуществования APN-подстановок от 4 переменных; если $\mathcal{L}_{n-1}(\pi)$ непусто, то по следствию 2 нелинейность π равна 0, что также невыполнимо для APN-функции [4]. Из [22] известно, что не существует квадратичных APN-подстановок от чётного числа переменных. ■

Для некоторых небольших n существуют функции, разрушающие структуру всех подпространств $\mathbb{F}_2^n$ нетривиальных размерностей. Например, при $n \in \{3, 5, 7\}$ функция инверсии элементов конечного поля принадлежит $\mathcal{P}_n^{\geqslant 2}$. Множество $\mathcal{P}_4^{\geqslant 2}$ пусто, а вот $\mathcal{P}_6^{\geqslant 2}$ содержит APN-подстановку, найденную в [23]: $\mathcal{L}_2(\pi)$, $\mathcal{L}_4(\pi)$ и $\mathcal{L}_5(\pi)$ для неё пусты по следствию 3 и, согласно экспериментальным данным, $\mathcal{L}_3(\pi)$ также пусто.

2.3. Классификация функций с $\delta(\pi) = 4$

Нетрудно классифицировать дифференциально 4-равномерные функции, исходя из структуры $\mathcal{L}_2(\pi)$.

Утверждение 4. Пусть $\pi \in \mathcal{P}_n$ и $\mathcal{L}_2(\pi) \neq \varnothing$. Тогда $\delta(\pi) = 4 \iff$ любые два различных элемента $\mathcal{L}_2(\pi)$ пересекаются по не более чем одному элементу.

Доказательство. Условие $\mathcal{L}_2(\pi) \neq \varnothing$ гарантирует, что $\delta(\pi) \geqslant 4$.

Пусть $\delta(\pi) = 4$. От противного: пусть $|L \cap U| = 2$ для некоторых $L, U \in \mathcal{L}_2(\pi)$, т. е. в силу взаимной однозначности π справедливо $|\pi(L)| = |\pi(U)| = 4$ и $|\pi(L) \setminus \pi(L \cap U)| = |\pi(U) \setminus \pi(L \cap U)| = 2$.

Обозначим $L \cap U = \{a, a \oplus v\}$ и $\pi(L \cap U) = \{\pi(a), \pi(a) \oplus v')\}$, где $a, v, v' \in \mathbb{F}_2^n$ и $v, v' \neq 0$. Но тогда $L \setminus (L \cap U) = \{b, b \oplus v\}$ и $U \setminus (L \cap U) = \{c, c \oplus v\}$ для некоторых $b, c \in \mathbb{F}_2^n$, где a, b, c попарно различны, так как суммы всех элементов L и U должны быть равны нулю. Так как $\pi(L)$ и $\pi(U)$ — тоже аффинные подпространства $\mathbb{F}_2^n$, аналогично получаем $\pi(L) \setminus \pi(L \cap U) = \{\pi(b), \pi(b) \oplus v'\}$ и $\pi(U) \setminus \pi(L \cap U) = \{\pi(c), \pi(c) \oplus v'\}$. Отсюда уравнение $\pi(x) \oplus \pi(x \oplus v) = v'$ имеет как минимум шесть решений $a, a \oplus v, b, b \oplus v, c, c \oplus v$, что противоречит $\delta(\pi) = 4$. Таким образом, любые различные $L, U \in \mathcal{L}_2(\pi)$ либо не пересекаются, либо пересекаются по одному элементу.

Пусть любые различные $L, U \in \mathcal{L}_2(\pi)$ пересекаются по не более чем одному элементу. От противного: пусть $\delta(\pi) > 4$. Тогда для некоторых $a \in \mathbb{F}_2^n \setminus \{0\}$ и $b \in \mathbb{F}_2^n$ существуют шесть различных $x, x \oplus a$, $y, y \oplus a$, $z, z \oplus a$, $x, y, z \in \mathbb{F}_2^n$, таких, что $\pi(x) \oplus \pi(x \oplus a) = \pi(y) \oplus \pi(y \oplus a) = \pi(z) \oplus \pi(z \oplus a) = b$. Но тогда $\{\pi(x), \pi(x \oplus a), \pi(y), \pi(y \oplus a)\}$ и $\{\pi(z), \pi(z \oplus a), \pi(y), \pi(y \oplus a)\}$ являются аффинными подпространствами $\mathbb{F}_2^n$, размерность которых равна 2 в силу взаимной однозначности π, и пересекаются они ровно по двум элементам, т. е. мы пришли к противоречию. ■

Результаты работы [24] позволяют оценить сверху мощность $\mathcal{L}_2(\pi)$ при $\delta(\pi) = 4$. В ней рассматриваются количества четвёрок $x_1, x_2, x_3, x_1 \oplus x_2 \oplus x_3 \in \mathbb{F}_2^n$, таких, что $F(x_1) \oplus F(x_2) \oplus F(x_3) = F(x_1 \oplus x_2 \oplus x_3)$ для $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Если F взаимно однозначна, то это в точности $|\mathcal{L}_2(F)|$. Например, [24, теорема 2.3] позволяет по дифференциальному спектру подсчитать $|\mathcal{L}_2(F)|$:

$$|\mathcal{L}_2(F)| = \frac{1}{3} \sum_{a \in \mathbb{F}_2^n \setminus \{0\}} \sum_{b \in \mathbb{F}_2^n} \binom{\delta_{a,b}(F)/2}{2},$$

где $\delta_{a,b}(F)$ — количество решений уравнения $F(x) \oplus F(x \oplus a) = b$. Поскольку $\sum\limits_{b \in \mathbb{F}_2^n} \delta_{a,b}(F) = 2^n$, то для дифференциально 4-равномерных функций справедлива следующая оценка, достигающаяся в точности при $\delta_{a,b} \in \{0, 4\}$:

Следствие 4. Пусть $\pi \in \mathcal{P}_n$ и $\delta(\pi) = 4$. Тогда $|\mathcal{L}_2(\pi)| \leqslant \frac{1}{3}2^{n-2}(2^n - 1)$.

Нетрудно видеть, что оценка не является целым числом при нечётных n. При этом она гарантированно достигается при $n = 2m + 2$. Например, для функций Голда вида

$$F(x) = x^{2^{2i}+1}, \quad \text{где} \quad x \in \mathbb{F}_{2^{2m+2}},\ 1 \leqslant i \leqslant m \quad \text{и} \quad (i, m+1) = 1,$$

выполняется $\delta_{a,b} \in \{0, 2^{(2i,2m+2)}\}$, и они являются взаимно однозначными [3, 4, 25]. Таким образом, для них достигается оценка следствия 4. Данное количество для всех функций Голда (в том числе необратимых) на языке четвёрок подсчитано в [24, теорема 3.4]. Достигается ли данная оценка при $n = 4m$, остаётся открытым вопросом.

3. Подстановки, разрушающие структуру подпространств определённых размерностей

Имея заданную подстановку, непросто доказать, что она разрушает структуру каких-либо аффинных подпространств $\mathbb{F}_2^n$. Однако можно оценить число таких функций. Например, в [1] доказано, что $\mathcal{P}_n^{\geqslant 3}$ непусто. Оценим доли $|\mathcal{P}_n^k|$ и $|\mathcal{P}_n^{\geqslant k}|$ к $|\mathcal{P}_n|$ при $n \to \infty$. Введём следующие обозначения:

$$\rho_{n,k} = |\widehat{\mathcal{S}}_n^k|^2 \Big/ \binom{2^n}{2^k}, \quad \sigma_{n,k} = \sum_{i=k}^{n-1} \rho_{n,i}.$$

Напомним также, что

$$|\mathcal{S}_n^k| = \frac{\prod\limits_{i=0}^{k-1}(2^n - 2^i)}{\prod\limits_{i=0}^{k-1}(2^k - 2^i)} = \frac{\prod\limits_{i=0}^{k-1}(2^{n-i} - 1)}{\prod\limits_{i=0}^{k-1}(2^{i+1} - 1)} \quad \text{и} \quad |\widehat{\mathcal{S}}_n^k| = 2^{n-k}|\mathcal{S}_n^k|.$$

Из доказательства [1, теорема 2.1] можно заключить, что справедливы следующие оценки:

Теорема 1 (W. E. Clark, X. Hou, and A. Mihailovs, 2007). Пусть $3 \leqslant k < n$. Тогда

$$|\mathcal{P}_n^k| \geqslant (1 - \rho_{n,k})|\mathcal{P}_n| \quad \text{и} \quad |\mathcal{P}_n^{\geqslant k}| \geqslant (1 - \sigma_{n,k})|\mathcal{P}_n|.$$

Заметим, что числа $\rho_{n,k}$ и $\sigma_{n,k}$ имеют и более важное значение: это среднее количество аффинных подпространств $\mathbb{F}_2^n$ размерности k (размерности от k до $n-1$), которое сохраняет функция из $\mathcal{P}_n$. Действительно, если это средние значения, то

$$\rho_{n,k}|\mathcal{P}_n| = \sum_{\pi \in \mathcal{P}_n} |\mathcal{L}_k(\pi)| = \sum_{\pi \in \mathcal{P}_n \setminus \mathcal{P}_n^k} |\mathcal{L}_k(\pi)| \geqslant |\mathcal{P}_n \setminus \mathcal{P}_n^k| = |\mathcal{P}_n| - |\mathcal{P}_n^k|$$

и аналогично для $\sigma_{n,k}$, что является доказательством теоремы 1. Далее мы детально рассмотрим это и другие свойства $\rho_{n,k}$ и $\sigma_{n,k}$.

3.1. Среднее количество подпространств, структуру которых сохраняет подстановка

Начнём с утверждения о средней мощности $\mathcal{L}_k(\pi)$.

Утверждение 5. Среднее количество аффинных подпространств $\mathbb{F}_2^n$ размерности k, структуру которых сохраняет подстановка на $\mathbb{F}_2^n$, равно $\rho_{n,k}$, т. е.

$$\rho_{n,k} = \frac{1}{|\mathcal{P}_n|} \sum_{\pi \in \mathcal{P}_n} |\mathcal{L}_k(\pi)| \quad \text{и} \quad \sigma_{n,k} = \frac{1}{|\mathcal{P}_n|} \sum_{\pi \in \mathcal{P}_n} \sum_{i=k}^{n-1} |\mathcal{L}_i(\pi)|.$$

Доказательство. Пусть $\tau(\pi, L) = 1$, если $\pi(L) \in \widehat{\mathcal{S}}_n^k$, и 0 иначе, где $\pi \in \mathcal{P}_n$ и $L \in \widehat{\mathcal{S}}_n^k$. Перепишем сумму из условия следующим образом:

$$\sum_{\pi\in\mathcal{P}_n} |\mathcal{L}_k(\pi)| = \sum_{\pi\in\mathcal{P}_n} \sum_{L\in\widehat{\mathcal{S}}_n^k} \tau(\pi, L) = \sum_{L\in\widehat{\mathcal{S}}_n^k} \sum_{\pi\in\mathcal{P}_n} \tau(\pi, L) = \sum_{L\in\widehat{\mathcal{S}}_n^k} |\{\pi \in \mathcal{P}_n : \pi(L) \in \widehat{\mathcal{S}}_n^k\}|. \quad (4)$$

Выберем любое $L \in \widehat{\mathcal{S}}_n^k$ и подсчитаем количество различных $\pi \in \mathcal{P}_n$, для которых $\pi(L) \in \widehat{\mathcal{S}}_n^k$. Во-первых, мы можем выбрать любое из $\widehat{\mathcal{S}}_n^k$ в качестве $\pi(L)$, при этом разные $\pi(L)$ влекут и различие π, т. е. получаем $|\widehat{\mathcal{S}}_n^k|$ вариантов $\pi(L)$. Далее, $\pi|_L$ можно выбрать $|\pi(L)| = 2^k!$ способами, так как мы зафиксировали $\pi(L)$. Каждое такое $\pi|_L$ нужно продолжить на всё $\mathbb{F}_2^n$, т. е. оставшиеся $2^n - 2^k$ элементов нужно расположить всевозможными $(2^n - 2^k)!$ способами на $\mathbb{F}_2^n \setminus L$. Итого, учитывая, что начальное L из $|\widehat{\mathcal{S}}_n^k|$, запишем

$$\sum_{\pi\in\mathcal{P}_n} |\mathcal{L}_k(\pi)| = |\widehat{\mathcal{S}}_n^k| \cdot |\widehat{\mathcal{S}}_n^k| \cdot 2^k! \, (2^n - 2^k)!.$$

Поделив всё на $|\mathcal{P}_n| = 2^n!$, получим то, что требуется доказать. ■

Для тривиальных аффинных подпространств $\rho_{n,k}$ также находится тривиально:

$$\rho_{n,0} = 2^n, \quad \rho_{n,1} = 2^{n-1}(2^n - 1), \quad \rho_{n,n} = 1.$$

Приведём в явном виде выражения для $\rho_{n,2}$ и $\rho_{n,3}$.

Утверждение 6. Справедливо

$$\rho_{n,2} = \frac{2^{n-3}(2^n-1)(2^n-2)}{3(2^n-3)} = \frac{2^{2n-3}}{3} + \frac{1}{12} + \frac{1}{2^{n+2}-12},$$
$$\rho_{n,3} = \rho\frac{2^n(2^n-1)(2^n-2)(2^n-4)}{(2^n-3)(2^n-5)(2^n-6)(2^n-7)}, \quad \text{где} \quad \rho = \frac{5}{224}.$$

Для доказательства достаточно воспользоваться общей формулой и выполнить несложные приведения.

3.2. Свойства $\rho_{n,k}$ и $\sigma_{n,k}$ при $k \geqslant 3$

Рассмотрим свойства $\rho_{n,k}$ и $\sigma_{n,k}$ при $k \geqslant 3$, т. е. когда их значение меньше 1. Сосредоточим внимание на $\rho_{n,3}$, $\sigma_{n,3}$ и $\sigma_{n,4}$.

Лемма 1. Пусть $2 \leqslant k < n - 1$. Тогда

$$\rho_{n,k+1} < \frac{\rho_{n,k}}{2^{2n-6}(2^{n-k-1}-1)^{2^k-4}}.$$

Доказательство. Имеет место

$$|\widehat{\mathcal{S}}_n^{k+1}| = 2^{n-k-1}\frac{\prod\limits_{i=0}^{k}(2^{n-i}-1)}{\prod\limits_{i=0}^{k}(2^{i+1}-1)} = \frac{1}{2}\,\frac{2^{n-k}-1}{2^{k+1}-1}|\widehat{\mathcal{S}}_n^k| < \frac{2(2^{n-k-1}-1)}{2^{k+1}-1}|\widehat{\mathcal{S}}_n^k|.$$

При этом

$$\binom{2^n}{2^{k+1}} = \prod_{i=0}^{2^{k+1}-1}(2^n - i)/2^{k+1}! = \prod_{i=0}^{2^k-1}\frac{2^n - 2^k - i}{2^k + i + 1}\binom{2^n}{2^k} > (2^{n-k-1}-1)^{2^k}\binom{2^n}{2^k}.$$

Подставив неравенства в выражение для $\rho_{n,k+1}$ из утверждения 5, получим

$$\rho_{n,k+1} < \frac{4(2^{n-k-1}-1)^2\rho_{n,k}}{(2^{n-k-1}-1)^{2^k}(2^{k+1}-1)^2} = \frac{4\rho_{n,k}}{(2^{n-k-1}-1)^{2^k-4}(2^n-2^{n-k-1}-2^{k+1}+1)^2}.$$

Учитывая, что $2^n - 2^{n-k-1} - 2^{k+1} + 1 > 2^{n-2}$, получаем требуемое неравенство. ■

Рассмотрим поведение $\rho_{n,k}$ при увеличении n.

Лемма 2. Пусть $4 \leqslant k \leqslant n$. Тогда

$$\rho_{n+1,k} < 2^{2k+4-2^k}\rho_{n,k}. \tag{5}$$

Доказательство. Ясно, что

$$|\widehat{\mathcal{S}}^k_{n+1}| = 2^{n+1-k}\frac{\prod\limits_{i=0}^{k-1}(2^{n+1-i}-1)}{\prod\limits_{i=0}^{k-1}(2^{i+1}-1)} = \frac{2^{n+2}-2}{2^{n-k+1}-1}|\widehat{\mathcal{S}}^k_n| < \frac{2^{n+2}}{2^{n-k}}|\widehat{\mathcal{S}}^k_n| = 2^{k+2}|\widehat{\mathcal{S}}^k_n|.$$

В то же время $\binom{2^{n+1}}{2^k} = \prod\limits_{i=0}^{2^k-1}(2^{n+1}-i)/2^k! = \prod\limits_{i=0}^{2^k-1}\frac{2^{n+1}-i}{2^n-i}\binom{2^n}{2^k} \geqslant 2^{2^k}\binom{2^n}{2^k}$.
Подставив неравенства в формулу для $\rho_{n+1,k}$, получим (5). ■

Докажем основные свойства $\rho_{n,k}$ и $\sigma_{n,k}$ при $k \geqslant 3$.

Утверждение 7. Зафиксируем $k \geqslant 3$. Тогда последовательности $\rho_{n,k}$ и $\sigma_{n,k}$, $n = k+1, k+2, k+3, \ldots$ монотонно убывают, при этом

$$\lim_{n\to\infty}\rho_{n,k} = \lim_{n\to\infty}\sigma_{n,k} = \begin{cases}\rho, & \text{если } k=3,\\ 0, & \text{если } k \geqslant 4.\end{cases}$$

Доказательство. По утверждению 5

$$\rho_{n,3} = \rho\frac{2^n(2^n-1)(2^n-2)(2^n-4)}{(2^n-3)(2^n-5)(2^n-6)(2^n-7)} = \rho\,\frac{2^n}{2^n-3}\,\frac{2^n-1}{2^n-5}\,\frac{2^n-4}{2^n-6}\,\frac{2^n-4}{2^n-7},$$

т. е. оно представляется в виде произведения ρ и монотонно убывающих сомножителей.

Монотонное убывание $\rho_{n,k}$ при $k \geqslant 4$ следует из леммы 2:

$$2^{-4} \geqslant 2^{2k+4-2^k} > \frac{\rho_{n+1,k}}{\rho_{n,k}}. \tag{6}$$

Докажем, что $\sigma_{k,n} = \rho_{k,n} + \ldots + \rho_{n-1,n}$ также монотонно убывает. Учитывая убывание $\rho_{n,k}$, достаточно показать, что $\rho_{n,n-1} > \rho_{n+1,n-1} + \rho_{n+1,n}$. Так как $n \geqslant 4$, то $\rho_{n+1,n} < \rho_{n+1,n-1}$ по лемме 1. Далее достаточно воспользоваться (6).

Найдём пределы $\rho_{n,k}$ и $\sigma_{n,k}$. Очевидно, что $\rho_{n,3}$ стремится к ρ. Для нахождения всех оставшихся пределов достаточно показать, что $\sigma_{n,4}$ сходится к нулю. Воспользуемся убыванием $\sigma_{n,4}$ и леммой 1:

$$\sigma_{n,4} = \sum_{k=4}^{n-1}\rho_{n,k} < \frac{n-4}{2^{2n-6}}\cdot\rho_{n,3},$$

т. е. $\sigma_{n,4}$ сходится к нулю. ■

Таким образом, $\rho_{n,3} = \sigma_{n,3} = \rho + o(1)$ и $\rho_{n,k} = \sigma_{n,k} = o(1)$ при $k \geqslant 4$. Используя монотонное убывание $\rho_{n,k}$ и $\sigma_{n,k}$, можно оценивать сверху их значения при больших n начальными значениями. Например, $\rho_{n,3} < \rho_{5,3} < \rho_{4,3}$ для всех $n \geqslant 6$, где

$$\rho_{4,3} = \frac{10}{143} \quad \text{и} \quad \rho_{5,3} = \frac{124}{3393}.$$

В табл. 1 приведены округлённые значения наиболее используемых далее $\rho_{n,3}$, $\sigma_{n,3}$ и $\sigma_{n,4}$ для небольших n, при этом $\rho \approx 0{,}0223214285714286$. Заметим также, что вероятность события $\pi \in \mathcal{P}_n^{\geqslant 3}$ при случайном выборе $\pi \in \mathcal{P}_n$ превышает 93, 96 и 97 % для $n = 4$, 5 и $n \geqslant 6$ соответственно.

Таблица 1

Округлённые значения $\rho_{n,3}$, $\sigma_{n,3}$ и $\sigma_{n,4}$ для $4 \leqslant n \leqslant 12$

n	$\rho_{n,3}$	$\sigma_{n,3}$	$\sigma_{n,4}$
4	0,0699300699300699	0,0699300699300699	1
5	0,0365458296492779	0,0365522248005155	$6{,}3951512375906990 \cdot 10^{-06}$
6	0,0281384877529501	0,0281385016330859	$1{,}3880135807123695 \cdot 10^{-08}$
7	0,0249785705552490	0,0249785706508960	$9{,}5647023517238220 \cdot 10^{-11}$
8	0,0235940660426061	0,0235940660436301	$1{,}0240104891952223 \cdot 10^{-12}$
9	0,0229445264556499	0,0229445264556632	$1{,}3335844188797633 \cdot 10^{-14}$
10	0,0226297620233199	0,0226297620233201	$1{,}9054283870459533 \cdot 10^{-16}$
11	0,0224748023114524	0,0224748023114524	$2{,}8481291963864860 \cdot 10^{-18}$
12	0,0223979185358598	0,0223979185358598	$4{,}3530671380777510 \cdot 10^{-20}$

Далее для построения оценок воспользуемся тем, что $\rho_{n,k}$ и $\sigma_{n,k}$ меньше 1 при $k \geqslant 3$ и не будем рассматривать $\rho_{n,2}$. Однако среднее значение $\rho_{n,2} = \dfrac{2^{2n-3}}{3} + \dfrac{1}{12} + \dfrac{1}{2^{n+2} - 12}$ для $|\mathcal{L}_2(\pi)|$ по $\pi \in \mathcal{P}_n$ (см. утверждение 6) можно соотнести с верхней оценкой $|\mathcal{L}_2(\pi)|$ при $\delta(\pi) = 4$ (см. следствие 4), достижимой в случае $n = 2m+2$: $|\mathcal{L}_2(\pi)| \leqslant \dfrac{2^{2n-2} - 2^{n-2}}{3}$. Это подтверждает, что низкий порядок дифференциальной равномерности π в общем случае не является существенным ограничителем на количество элементов в $\mathcal{L}_k(\pi)$.

3.3. Мощность $\mathcal{P}_n^{\geqslant k}$ при $n \to \infty$

Воспользовавшись свойствами $\rho_{n,k}$ и $\sigma_{n,k}$, оценим асимптотику числа подстановок из $\mathcal{P}_n^k$ и $\mathcal{P}_n^{\geqslant k}$ при $k \geqslant 4$.

Следствие 5. Почти все $\pi \in \mathcal{P}_n$ разрушают структуру всех аффинных подпространств размерности от 4 до $n-1$, т. е.

$$\lim_{n \to \infty} \frac{|\mathcal{P}_n^{\geqslant 4}|}{|\mathcal{P}_n|} = 1.$$

Это справедливо и для каждого $\mathcal{P}_n^k$ и $\mathcal{P}_n^{\geqslant k}$ при $k \geqslant 4$.

Доказательство очевидно следует из теоремы 1 и утверждения 7.

Для получения асимптотики размера $\mathcal{P}_n^3$ и $\mathcal{P}_n^{\geqslant 3}$ нам потребуется следующая

Лемма 3. Пусть U — аффинное подпространство $\mathbb{F}_2^n$ размерности k. Тогда количество аффинных подпространств $\mathbb{F}_2^n$ размерности m, пересекающихся с U по аффинному подпространству размерности t, равно $2^{(k-t)(m-t)} \cdot |\widehat{\mathcal{S}}_k^t| \cdot |\mathcal{S}_{n-k}^{m-t}|$.

Доказательство. Без ограничения общности можно считать, что $\mathbb{F}_2^n = \mathbb{F}_2^{n-k} \times \mathbb{F}_2^k$ и $U = \{0\} \times \mathbb{F}_2^k$. Подсчитаем только линейные подпространства $\mathbb{F}_2^{n-k} \times \mathbb{F}_2^k$, для нахождения количества аффинных подпространств домножим полученный результат на 2^{k-t}.

Далее достаточно воспользоваться представлением базиса линейного подпространства $\mathbb{F}_2^n$ размерности m в виде приведённой ступенчатой матрицы (матрицы Гаусса — Жордана): первая слева единица в каждой её последующей строке находится правее предыдущей (эти единицы называются ведущими), и ведущая единица — единственный ненулевой элемент столбца. Любое линейное подпространство имеет единственную такую базисную матрицу [26]. Составим матрицу Гаусса — Жордана размера $m \times n$ из четырёх частей:

$$M = \begin{pmatrix} L & T \\ 0 & R \end{pmatrix},$$

где L и R — матрицы Гаусса — Жордана размера $(m-t) \times (n-k)$ и $t \times k$ соответственно; T — матрица размера $(m-t) \times k$ с единственным ограничением: над ведущими единицами R (их t штук) стоят нули. Пересечением U с линейным подпространством $\mathbb{F}_2^n$, базисом которого являются строки M, будет $\{0\} \times R'$, где R' — линейное подпространство $\mathbb{F}_2^k$, базис которого — строки R. Таким образом, чтобы перебрать все нужные M, требуется выбрать L ($|\mathcal{S}_{n-k}^{m-t}|$ способов), выбрать R ($|\mathcal{S}_k^t|$ способов) и оставшиеся элементы T ($2^{k(m-t)-t(m-t)}$ способов). ■

Теорема 2. Справедливо

$$o(1) \leqslant \frac{|\mathcal{P}_n^3|}{|\mathcal{P}_n|} - (1-\rho) \leqslant \frac{\rho^2}{2} + o(1).$$

Данные неравенства справедливы и для $|\mathcal{P}_n^{\geqslant 3}|$.

Доказательство. Оценка снизу напрямую следует из теоремы 1. Для доказательства оценки сверху воспользуемся утверждением 5 и равенством (4):

$$\rho_{n,k}|\mathcal{P}_n| = \sum_{\pi \in \mathcal{P}_n} |\mathcal{L}_k(\pi)| = \sum_{L \in \widehat{\mathcal{S}}_n^k} |\{\pi \in \mathcal{P}_n : \pi(L) \in \widehat{\mathcal{S}}_n^k\}|.$$

Пусть $m = |\widehat{\mathcal{S}}_n^3|$ и $\widehat{\mathcal{S}}_n^3 = \{L_1, L_2, \ldots, L_m\}$, т. е. пронумеруем все аффинные подпространства $\mathbb{F}_2^n$ размерности 3. Определим множества A_i, $i \in \{1, \ldots, m\}$, следующим образом:

$$A_i = \{\pi \in \mathcal{P}_n : \pi(L_i) \in \widehat{\mathcal{S}}_n^3\}, \text{ т. е. } |A_1| + \ldots + |A_m| = \rho_{n,3}|\mathcal{P}_n|. \tag{7}$$

Обозначив через $\overline{A_i}$ множество $\mathcal{P}_n \setminus A_i$, по методу включений — исключений получим

$$\mathcal{P}_n^3 = |\overline{A_1} \cap \ldots \cap \overline{A_m}| = |\mathcal{P}_n| - \sum_{1 \leqslant i \leqslant m} |A_i| + \sum_{1 \leqslant i < j \leqslant m} |A_i \cap A_j| + \ldots + (-1)^n |A_1 \cap \ldots \cap A_m|. \tag{8}$$

Мы не будем искать все пересечения, воспользуемся только следующей оценкой:

$$|\mathcal{P}_n^3| \leqslant |\mathcal{P}_n| - \sum_{1 \leqslant i \leqslant m} |A_i| + \sum_{1 \leqslant i < j \leqslant m} |A_i \cap A_j|. \tag{9}$$

Действительно, если какая-то $\pi \in \mathcal{P}_n$ принадлежит k различным A_i, то в выражении $|\mathcal{P}_n| - |A_1| - \ldots - |A_m|$ будет вычтена k раз из $|\mathcal{P}_n|$ вместо одного, т. е. лишние $(k-1)$ раз. Но после добавления пересечений она будет добавлена ещё $k(k-1)/2$ раз.

При этом $k(k-1)/2 \geqslant k-1$ при $k \geqslant 1$. При $k=0$ функция не будет вычтена, так как принадлежит $\mathcal{P}_n^3$. Таким образом, в правой части получим не меньше чем $|\mathcal{P}_n^3|$.

Следовательно, (7) и (9) гарантируют

$$\frac{|\mathcal{P}_n^3|}{|\mathcal{P}_n|} - (1-\rho_{n,3}) \leqslant \sum_{1\leqslant i<j\leqslant m} |A_i \cap A_j| = T_n. \tag{10}$$

Вместо точной формулы для T_n далее рассмотрим только её асимптотику по старшему слагаемому. Разделив все пары (i,j), $i<j$, по мощности пересечения $L_i \cap L_j$, разделим и T_n на соответствующие группы:

$$T_n = T_n^0 + T_n^1 + T_n^2 + T_n^{\varnothing},$$
$$\text{где} \quad T_n^t = \sum_{\substack{1\leqslant i<j\leqslant m,\\ \dim L_i\cap L_j = t}} |A_i \cap A_j| \quad \text{и} \quad T_n^{\varnothing} = \sum_{\substack{1\leqslant i<j\leqslant m,\\ L_i\cap L_j = \varnothing}} |A_i \cap A_j|.$$

1. Найдём T_n^t, т. е. $L_i \cap L_j \in \widehat{\mathcal{S}}_n^t$, где $0 \leqslant t \leqslant 2$. Зафиксируем некоторое t. Первое L_i можно выбрать $|\widehat{\mathcal{S}}_n^3|$ способами, т. е. произвольным образом. Далее лемма 3 гарантирует, что способов выбрать L_j существует ровно

$$2^{(3-t)^2} \cdot |\widehat{\mathcal{S}}_3^t| \cdot |\mathcal{S}_{n-3}^{3-t}|. \tag{11}$$

Таким образом, получаем $\dfrac{1}{2} 2^{(3-t)^2} \cdot |\widehat{\mathcal{S}}_3^t| \cdot |\mathcal{S}_{n-3}^{3-t}| \cdot |\widehat{\mathcal{S}}_n^3|$ способов выбрать $1 \leqslant i < j \leqslant m$, таких, что $\dim L_i \cap L_j = t$ (так как $i<j$, мы поделили общее количество способов выбора упорядоченной пары (L_i, L_j) на два). Найдём для них $|A_i \cap A_j|$. Аналогично предыдущим рассуждениям, образ $\pi(L_i)$ для $\pi \in A_i \cap A_j$ можем выбрать $\widehat{\mathcal{S}}_n^3$ способами, т. е. произвольно. Количество способов выбрать образ $\pi(L_j)$ равно (11), поскольку $|\pi(L_i) \cap \pi(L_j)| = |L_i \cap L_j|$.

Значения π на $L_i \cap L_j$ можно выбрать $2^t!$ способами, переставляя элементы $\pi(L_i) \cap \cap \pi(L_j)$; на оставшихся частях подпространств — $(2^3 - 2^t)!^2$ способами; вне $L_i \cup L_j$ — $(2^n - (16 - 2^t))!$ способами, т. е. получаем

$$T_n^t = \frac{1}{2} 2^{2(3-t)^2} \cdot |\widehat{\mathcal{S}}_3^t|^2 \cdot |\mathcal{S}_{n-3}^{3-t}|^2 \cdot |\widehat{\mathcal{S}}_n^3|^2 \cdot (2^n - (16-2^t))! \cdot 2^t! \cdot (2^3 - 2^t)!^2.$$

Но $T_n^t / 2^n! = o(1)$. Действительно,

$$\frac{T_n^t}{2^n!} = s_t \frac{|\mathcal{S}_{n-3}^{3-t}|^2 \cdot |\widehat{\mathcal{S}}_n^3|^2 \, (2^n - (16-2^t))!}{2^n!} = s_t \frac{|\mathcal{S}_{n-3}^{3-t}|^2 \cdot |\widehat{\mathcal{S}}_n^3|^2}{2^n(2^n-1)\dots(2^n-15+2^t)},$$

где s_t не зависит от n. При этом

$$|\widehat{\mathcal{S}}_n^3| = O(2^{4n}), \quad |\mathcal{S}_{n-3}^{3-t}| = O(2^{(3-t)n}), \quad 2^n(2^n-1)\dots(2^n-r+1) = O(2^{rn}). \tag{12}$$

Таким образом,

$$\frac{T_n^t}{2^n!} = O(2^{(2(3-t)+2\cdot 4-16+2^t)n}) = O(2^{(2^t-2t-2)n}).$$

Подставляя $t \in \{0,1,2\}$, получим $O(2^{-n})$, $O(2^{-2n})$ и $O(2^{-2n})$ соответственно. Это означает, что $T_n^0 + T_n^1 + T_n^2$ можно не учитывать.

2. Найдём $T_n^{\varnothing}$, т. е. $L_i \cap L_j = \varnothing$. Здесь L_i можем выбрать $|\widehat{\mathcal{S}}_n^3|$ способами, L_j — $|\widehat{\mathcal{S}}_n^3| - \sum\limits_{t=0}^{2} \left(2^{(3-t)^2} \cdot |\widehat{\mathcal{S}}_3^t| \cdot |\mathcal{S}_{n-3}^{3-t}|\right) - 1$ способами, согласно (11), и поделить на 2 в силу $i < j$.

Так как $L_i \cap L_j = \varnothing$, то и $\pi(L_i) \cap \pi(L_j) = \varnothing$. Аналогично подсчёту T_n^t, получим

$$T_n^{\varnothing} = \frac{1}{2}|\widehat{\mathcal{S}}_n^3|^2(|\widehat{\mathcal{S}}_n^3| - \sum_{t=0}^{3} \left(2^{(3-t)^2} \cdot |\widehat{\mathcal{S}}_3^t| \cdot |\mathcal{S}_{n-3}^{3-t}|) - 1\right)^2 \cdot 2^3! \cdot 2^3! \, (2^n - 16)!.$$

Согласно (12), старший член $T_n^{\varnothing}/2^n!$ равен

$$\frac{|\widehat{\mathcal{S}}_n^3|^4 \cdot 8! \cdot 8!}{2 \cdot 2^n(2^n-1)\dots(2^n-15)} = \frac{2^6 \cdot 7^2 \cdot 6^2 \cdot 5^2 \cdot 4^2 \cdot 6^2}{(8-1)^4(8-2)^4(8-4)^4 2^{13}} \, \frac{2^{4n}(2^n-1)^4(2^n-2)^4(2^n-4)^4}{2^n(2^n-1)\dots(2^n-15)}.$$

Таким образом,

$$\frac{T_n^{\varnothing}}{|\mathcal{P}_n|} = \frac{5^2}{7^2 2^{11}} + o(1) = \frac{\rho^2}{2} + o(1) \quad \text{и} \quad \frac{T_n}{|\mathcal{P}_n|} = \frac{\rho^2}{2} + o(1), \tag{13}$$

поскольку $T_n^t/|\mathcal{P}_n| = o(1)$. Неравенство (10) завершает доказательство. Оценки для $\mathcal{P}_n^{\geqslant 3}$ очевидно следуют из доказанного и следствия 5. ■

Можно оценить также количество функций, сохраняющих структуру ровно одного подпространства размерности 3.

Следствие 6. Количество $\pi \in \mathcal{P}_n^{\geqslant 4}$ с $|\mathcal{L}_3(\pi)| = 1$ не менее чем $\rho(1-\rho)2^n! + o(2^n!)$.

Доказательство. Обозначим через D_n количество функций из условия. Воспользуемся обозначениями $A_1, \dots, A_m$ из (7) и (8), а также суммой мощностей их пересечений T_n из (10). Тогда

$$D_n \geqslant |A_1| + \dots + |A_m| - 2T_n.$$

Действительно, если такая π принадлежит ровно k множествам из $A_1, \dots, A_m$ и $k = 1$, то функция будет учтена ровно один раз в обоих частях. Если $k \geqslant 2$, то до вычитания $2T_n$ будет учтена лишние k раз в правой части. Но затем при вычитании $2T_n$ данная функция будет вычтена $k(k-1)$ раз. Поскольку $k \leqslant k(k-1)$, то оценка верна. Согласно (7) и (13), получим

$$D_n \geqslant \rho|\mathcal{P}_n| - \rho^2|\mathcal{P}_n| + o(|\mathcal{P}_n|),$$

что влечёт оценку в следствии. ■

В табл. 2 приведены значения $|\mathcal{L}_k(S)|$, $2 \leqslant k \leqslant 5$, для S-блоков размера 8×8 различных шифров. Обратим внимание, что $|\mathcal{L}_6(S)| = |\mathcal{L}_7(S)| = 0$ для всех S из табл. 2. При построении S-блоков используются разные стратегии, поэтому данные значения имеют вариативность: некоторые схожи с таковыми у «случайных» функций, а некоторые — нет, см., например, S-блоки AES, ARIA и др., построенные с помощью инверсии элементов конечного поля ($|\mathcal{L}_k(S)|$ для них приведены в утверждении 3). Напомним, что утверждение 6 позволяет подсчитать среднее количество $\rho_{8,k}$ элементов в $\mathcal{L}_k(\pi)$ среди $\pi \in \mathcal{P}_8$:

$$\rho_{8,2} \approx 2730{,}7509881422924991,$$
$$\rho_{8,3} \approx 0{,}0235940660426061,$$
$$\sigma_{8,4} = \rho_{8,4} + \rho_{8,5} + \rho_{8,6} + \rho_{8,7} \approx 1{,}0240104891952223 \cdot 10^{-12}.$$

Таблица 2

Значения $|\mathcal{L}_k(S)|$ для S-блоков из $\mathcal{P}_8$

S-блок	$\lvert\mathcal{L}_2(S)\rvert$	$\lvert\mathcal{L}_3(S)\rvert$	$\lvert\mathcal{L}_4(S)\rvert$	$\lvert\mathcal{L}_5(S)\rvert$	N_S	$\delta(S)$
AES/ARIA/Camellia/SM4/	85	0	17	0	112	4
CLEFIA S_1/SNOW 3G S_1/ZUC S_1	85	0	17	0	112	4
Fantomas	6444	79	0	0	96	16
FLY	5968	576	16	0	96	16
Fox (8-bit)	4854	225	3	0	96	16
Kuznechik	1953	0	2	0	100	8
Scream	3104	228	6	0	96	10
iScream	5472	466	2	5	96	16
SKINNY $\mathcal{S}_8$	22688	3648	320	24	64	64
SNOW 3G S_2	2570	2	1	0	96	8
ZUC S_0	3360	100	0	0	96	8
Zorro	2691	4	0	0	96	10
Anubis	2590	0	0	0	94	8
BelT	1666	0	0	0	102	8
Enocoro	2767	0	0	0	96	10
Iceberg	2669	0	0	0	96	8
Khazad	2768	0	0	0	96	8
Skipjack	2469	0	0	0	100	12
Turing	2617	0	0	0	94	12
Whirlpool	2579	0	0	0	100	8

ЛИТЕРАТУРА

1. *Clark W. E., Hou X., and Mihailovs A.* The affinity of a permutation of a finite vector space // Finite Fields Their Appl. 2007. V. 13. P. 80–112.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. N.Y.: Academic Press, 2015.
3. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Springer, Cham, 2015.
4. *Carlet C.* Boolean Functions for Cryptography and Coding Theory. Cambridge: Cambridge University Press, 2021.
5. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.
6. *Панкратова И. А.* Булевы функции в криптографии: учеб. пособие. Томск: Издательский Дом Томского государственного университета, 2014.
7. *Carlet C. and Piccione E.* On vectorial functions mapping strict affine subspaces of their domain into strict affine subspaces of their co-domain, and the strong D-property // Adv. Math. Commun. 2024. https://www.aimsciences.org/article/doi/10.3934/amc.2024025.
8. *Городилова А. А.* Характеризация почти совершенно нелинейных функций через подфункции // Дискретная математика. 2015. Т. 27. № 3. С. 3–16.
9. *Idrisova V.* On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem" // Cryptogr. Commun. 2019. V. 11. No. 1. P. 21–39.
10. *Beierle C., Leander G., and Perrin L.* Trims and extensions of quadratic APN functions // Des. Codes Cryptogr. 2022. V. 90. P. 1009–1036.
11. *Kolomeec N. and Bykov D.* On the image of an affine subspace under the inverse function within a finite field // Des. Codes Cryptogr. 2024. V. 92. P. 467–476.
12. *Leander G., Abdelraheem M. A., AlKhzaimi H., and Zenner E.* A cryptanalysis of PRINTcipher: The invariant subspace attack // LNCS. 2011. V. 6841. P. 206–221.

13. *Todo Y., Leander G., and Sasaki Y.* Nonlinear invariant attack: practical attack on full SCREAM, iSCREAM, and Midori64 // LNCS. 2016. V. 10032. P. 3–33.
14. *Трифонов Д. И., Фомин Д. Б.* Об инвариантных подпространствах в XSL-шифрах // Прикладная дискретная математика. 2021. № 54. С. 58–76.
15. *Буров Д. А.* О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов // Дискретная математика. 2021. Т. 33. № 2. С. 31–45.
16. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 245–265.
17. *Charpin P.* Normal Boolean functions // J. Complexity. 2004. V. 20. No. 2–3. P. 245–265.
18. *Буряков М. Л., Логачев О. А.* Об уровне аффинности булевых функций // Дискретная математика. 2005. Т. 17. № 4. С. 98–107.
19. *Логачев О. А.* О значениях уровня аффинности для почти всех булевых функций // Прикладная дискретная математика. 2010. № 3(9). С. 17–21.
20. *Canteaut A., Carlet C., Charpin P., and Fontaine C.* On cryptographic properties of the cosets of $R(1, m)$ // IEEE Trans. Inform. Theory. 2001. V. 47. P. 1494–1513.
21. *Carlet C. and Feukoua S.* Three parameters of Boolean functions related to their constancy on affine spaces // Adv. Math. Commun. 2020. V. 14. No. 4. P. 651–676.
22. *Berger T., Canteaut A., Charpin P., and Laigle-Chapuy Y.* On almost perfect nonlinear functions // IEEE Trans. Inform. Theory. 2006. V. 52. No. 9. P. 4160–4170.
23. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN permutation in dimension six // Finite Fields: Theory Appl. 2010. Iss. 518. P. 33–42.
24. *Li S., Meidl W., Polujan A., et al.* Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application // IEEE Trans. Inform. Theory. 2020. V. 66. No. 11. P. 7101–7112.
25. *Blondeau C., Canteaut A., and Charpin P.* Differential properties of power functions // Int. J. Inform. Coding Theory. 2010. V. 1. No. 2. P. 149–170.
26. *Knuth D. E.* Subspaces, subsets, and partitions // J. Combinatorial Theory. Ser. A. 1971. V. 10. No. 2. P. 178–180.

REFERENCES

1. *Clark W. E., Hou X., and Mihailovs A.* The affinity of a permutation of a finite vector space. Finite Fields Their Appl., 2007, vol. 13, pp. 80–112.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. N.Y., Academic Press, 2015.
3. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Springer, Cham, 2015.
4. *Carlet C.* Boolean Functions for Cryptography and Coding Theory. Cambridge, Cambridge University Press, 2021.
5. *Logachev O. A., Salnikov A. A., and Yashchenko V. V.* Boolean Functions in Coding Theory and Cryptography. Providence, Rhode Island, AMS, 2012.
6. *Pankratova I. A.* Bulevy funktsii v kriptografii [Boolean Functions in Cryptography]. Tomsk, TSU Publ., 2014. (in Russian)
7. *Carlet C. and Piccione E.* On vectorial functions mapping strict affine subspaces of their domain into strict affine subspaces of their co-domain, and the strong D-property. Adv. Math. Commun., 2024, https://www.aimsciences.org/article/doi/10.3934/amc.2024025.
8. *Gorodilova A. A.* Characterization of almost perfect nonlinear functions in terms of subfunctions. Discrete Math. Appl., 2016, vol. 26, no. 4, pp. 193–202.

9. *Idrisova V.* On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem". Cryptogr. Commun., 2019, vol. 11, no. 1, pp. 21–39.
10. *Beierle C., Leander G., and Perrin L.* Trims and extensions of quadratic APN functions. Des. Codes Cryptogr., 2022, vol. 90, pp. 1009–1036.
11. *Kolomeec N. and Bykov D.* On the image of an affine subspace under the inverse function within a finite field. Des. Codes Cryptogr., 2024, vol. 92, pp. 467–476.
12. *Leander G., Abdelraheem M. A., AlKhzaimi H., and Zenner E.* A cryptanalysis of PRINTcipher: The invariant subspace attack. LNCS, 2011, vol. 6841, pp. 206–221.
13. *Todo Y., Leander G., and Sasaki Y.* Nonlinear invariant attack: practical attack on full SCREAM, iSCREAM, and Midori64. LNCS, 2016, vol. 10032, pp. 3–33.
14. *Trifonov D. I. and Fomin D. B.* Ob invariantnykh podprostranstvakh v XSL-shifrakh [Invariant subspaces in SPN block cipher]. Prikladnaya Diskretnaya Matematika, 2021, no. 54, pp. 58–76. (in Russian)
15. *Burov D. A.* On the existence of special nonlinear invariants for round functions of XSL-ciphers. Discrete Math. Appl., 2023, vol. 33, no. 2, pp. 65–75.
16. *Nyberg K.* Differentially uniform mappings for cryptography. LNCS, 1994, vol. 765, pp. 245–265.
17. *Charpin P.* Normal Boolean functions. J. Complexity, 2004, vol. 20, no. 2–3, pp. 245–265.
18. *Buryakov M. L. and Logachev O. A.* On the affinity level of Boolean functions. Discrete Math. Appl., 2005, vol. 15, no. 5, pp. 479–488.
19. *Logachev O. A.* O znacheniyakh urovnya affinnosti dlya pochti vsekh bulevykh funktsiy [On values of affinity level for almost all Boolean functions]. Prikladnaya Diskretnaya Matematika, 2010, no. 3(9), pp. 17–21. (in Russian)
20. *Canteaut A., Carlet C., Charpin P., and Fontaine C.* On cryptographic properties of the cosets of $R(1, m)$. IEEE Trans. Inform. Theory, 2001, vol. 47, pp. 1494–1513.
21. *Carlet C. and Feukoua S.* Three parameters of Boolean functions related to their constancy on affine spaces. Adv. Math. of Commun., 2020, vol. 14, no. 4, pp. 651–676.
22. *Berger T., Canteaut A., Charpin P., and Laigle-Chapuy Y.* On almost perfect nonlinear functions. IEEE Trans. Inform. Theory, 2006, vol. 52, no. 9, pp. 4160–4170.
23. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN permutation in dimension six. Finite Fields: Theory Appl., 2010, iss. 518, pp. 33–42.
24. *Li S., Meidl W., Polujan A., et al.* Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application. IEEE Trans. Inform. Theory, 2020, vol. 66, no. 11, pp. 7101–7112.
25. *Blondeau C., Canteaut A., and Charpin P.* Differential properties of power functions. Int. J. Inform. Coding Theory, 2010, vol. 1, no. 2, pp. 149–170.
26. *Knuth D. E.* Subspaces, subsets, and partitions. J. Combinatorial Theory, Ser. A, 1971, vol. 10, no. 2, pp. 178–180.