Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7 DOI 10.17223/2226308X/15/1

ОБ ИНВАРИАНТНЫХ ПОДПРОСТРАНСТВАХ ФУНКЦИЙ, АФФИННО ЭКВИВАЛЕНТНЫХ ОБРАЩЕНИЮ ЭЛЕМЕНТОВ КОНЕЧНОГО ПОЛЯ[1]

Н. А. Коломеец, Д. А. Быков

Рассматриваются аффинные подпространства над $\mathbb{F}_p$ конечного поля $\mathbb{F}_{p^n}$, p — простое, образ которых под действием функции x^{-1}, обращающей элемент x поля (считаем, что $0^{-1} = 0$), также является аффинным подпространством. Доказано, что образ аффинного подпространства U, $|U| > 2$, является аффинным подпространством, если и только если $U = q\mathbb{F}_{p^k}$, где $q \in \mathbb{F}_{p^n}^*$ и $k|n$. Другими словами, все такие подпространства выражаются через подполя поля $\mathbb{F}_{p^n}$. В качестве следствия предложено достаточное условие, при котором функция $A(x^{-1}) + b$ не имеет инвариантных аффинных подпространств U мощности $2 < |U| < p^n$, где $A : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ — обратимое линейное преобразование, $b \in \mathbb{F}_{p^n}^*$. Приведены примеры функции, у которых, исключая само $\mathbb{F}_{p^n}$, отсутствуют инвариантные аффинные подпространства.

Ключевые слова: *конечные поля, обратный элемент, аффинные подпространства, инвариантные подпространства.*

В работе рассматриваются аффинные подпространства, образ которых под действием функции, обращающей элементы конечного поля, также является аффинным подпространством. Обозначим эту функцию через σ, т. е. $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, такая, что

$$\sigma(x) = \begin{cases} x^{-1}, & \text{если } x \neq 0, \\ 0, & \text{если } x = 0, \end{cases}$$

где $\mathbb{F}_{p^n}$ — конечное поле, состоящее из p^n элементов. Здесь и далее p — простое число. Под *линейным подпространством* L поля $\mathbb{F}_{p^n}$ мы подразумеваем его линейное подпространство над $\mathbb{F}_p$, другими словами, аддитивную подгруппу $\mathbb{F}_{p^n}$. Через $a+L$ обозначим *аффинное подпространство*. Отметим, что для любого множества $S \subseteq \mathbb{F}_{p^n}$, элемента $a \in \mathbb{F}_{p^n}$ и функции $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

$$a + S = \{a + s : s \in S\},\ aS = \{as : s \in S\} \text{ и } f(S) = \{f(s) : s \in S\}.$$

Известно, что у $\mathbb{F}_{p^n}$ существует подполе $\mathbb{F}_{p^k}$ тогда и только тогда, когда $k|n$. В этом случае будем полагать, что $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^n}$.

Рассмотрим аффинные подпространства $U \subseteq \mathbb{F}_{p^n}$, такие, что $\sigma(U)$ также является аффинным подпространством. Выделим *нетривиальные* подпространства, такие, что

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF–2022–0018).

$2 < |U| < p^n$, поскольку любое множество мощности 1, 2 (если $p = 2$) или p^n является аффинным подпространством.

Интерес к этим подпространствам обусловлен их связью с инвариантными подпространствами отображений. Знание всех таких U позволяет определить все инвариантные аффинные подпространства относительно функций, аффинно эквивалентных σ. Напомним, что множество $S \subseteq \mathbb{F}_{p^n}$ называется *инвариантным* относительно f, если $f(S) \subseteq S$. Функция σ, на базе которой построен S-блок AES [1, 2], а также её инвариантные подпространства интересны в криптографическом контексте. Например, они использовались для исследования групповых свойств раундовых функций у AES-подобных шифров [3 – 5]. В [6] предложена атака, использующая инвариантное подпространство для нескольких раундов шифрования, которая к настоящему времени рассмотрена для многих схем [7]. Известна также более общая атака [8], построение которой можно начинать с S-блоков [9]. Отметим, что все линейные подпространства, являющиеся инвариантными относительно σ, описаны в работах [10, 11]. Таким образом, мы обобщаем эти результаты, во-первых, на аффинные подпространства и, во-вторых, на подпространства, являющиеся инвариантными не для σ, а для некоторой функции, аффинно эквивалентной σ.

Если $f(U)$ не является аффинным подпространством для любого аффинного подпространства $U \subseteq \mathbb{F}_{2^n}$ размерности 2, то f принадлежит к классу APN-функций [12], имеющих большую криптографическую значимость. Более того, только APN-функции обладают этим свойством. С ними связано множество открытых вопросов [13].

Сначала покажем, что для функции σ достаточно рассматривать только линейные подпространства.

Теорема 1. Пусть U и $\sigma(U)$ — аффинные подпространства $\mathbb{F}_{p^n}$, $|U| > 2$. Тогда U является линейным подпространством $\mathbb{F}_{p^n}$.

Следующая теорема описывает все искомые подпространства U.

Теорема 2. Пусть U — аффинное подпространство $\mathbb{F}_{p^n}$, $|U| > 2$. Тогда $\sigma(U)$ является аффинным подпространством $\mathbb{F}_{p^n}$, если и только если

$$U = q\mathbb{F}_{p^k}, \text{ где } k|n \text{ и } q \in \mathbb{F}_{p^n}^*.$$

Доказательство теоремы использует тождество Хуа [14] аналогично рассмотренному в [10, 11] случаю линейных подпространств, инвариантных относительно σ. Теорема 2 также показывает, что при простых $n > 2$ существуют APN-функции, такие, что образ нетривиального аффинного подпространства (любой размерности, а не только размерности 2) никогда не является аффинным подпространством.

Покажем, что теоремы 1 и 2 позволяют построить с помощью σ функции без нетривиальных инвариантных подпространств, имеющие вид

$$\sigma_{A,b}(x) = A(\sigma(x)) + b,$$

где $A : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ — обратимая линейная функция; $b \in \mathbb{F}_{p^n}^*$ и $x \in \mathbb{F}_{p^n}$. Рассматривая линейные отображения, мы, аналогично подпространствам, подразумеваем, что $\mathbb{F}_{p^n}$ является векторным пространством над полем $\mathbb{F}_p$. Определим также подмножество поля

$$\mathcal{S}(\mathbb{F}_{p^n}) = \{x \in \mathbb{F}_{p^n} : x \notin \mathbb{F}_{p^k}, \text{ где } k|n \text{ и } k < n\}.$$

Другими словами, оно содержит все элементы $\mathbb{F}_{p^n}$, не лежащие в его подполях, и всегда является непустым.

Теорема 3. Пусть $A : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ — обратима и линейна, $b \in \mathbb{F}_{p^n}^*$, причём

$$b^{-1}\sigma_{A,b}(b) \in \mathcal{S}(\mathbb{F}_{p^n}). \tag{1}$$

Тогда не существует инвариантных аффинных подпространств U относительно $\sigma_{A,b}$, таких, что $2 < |U| < p^n$.

Даже если $\sigma_{A,b}$ не удовлетворяет условию (1), можно привести её к нужному виду.

Следствие 1. Пусть $A : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ — обратима и линейна, $b \in \mathbb{F}_{p^n}^*$. Определим функцию $A' : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ следующим образом:

$$A'(x) = \alpha\beta A(x), \text{ где } \alpha \in \mathcal{S}(\mathbb{F}_{p^n}) \text{ и } \beta = (b^{-1}A(b^{-1}))^{-1}.$$

Тогда функция $\sigma_{A',b}$ удовлетворяет условию (1).

Отметим, что S-блок $S_{\texttt{AES}}$ шифра AES, имеющий вид $\sigma_{A,b}$ в поле $\mathbb{F}_{2^8}$, удовлетворяет условию (1) теоремы 3. Тем не менее существует аффинное подпространство размерности 1, инвариантное относительно $S_{\texttt{AES}}$ [1, табл. 7]:

$$S_{\texttt{AES}}(\texttt{0x73}) = \texttt{0x8F} \text{ и } S_{\texttt{AES}}(\texttt{0x8F}) = \texttt{0x73}.$$

Таким образом, утверждения выше не гарантируют отсутствия инвариантных подпространств U, где $1 \leqslant |U| \leqslant 2$. В дополнение к примеру выше, функция вида $\sigma_{A,b}$ может удовлетворять условию (1), но при этом иметь неподвижные точки (т. е. инвариантные аффинные подпространства размерности 0). Следующая теорема гарантирует существование функций, единственным инвариантным подпространством которых является $\mathbb{F}_{p^n}$.

Теорема 4. Пусть $\sigma_{\alpha,b}(x) = \alpha\sigma(x) + b$, где $\alpha, b \in \mathbb{F}_{p^n}^*$, $x \in \mathbb{F}_{p^n}$. Тогда $\sigma_{\alpha,b}$ не имеет инвариантных аффинных подпространств, кроме $\mathbb{F}_{p^n}$, если и только если

— $\alpha b^{-2} \in M_2$ при $p = 2$, где

$$M_2 = \{x \in \mathcal{S}(\mathbb{F}_{2^n}) : \mathrm{tr}(x) = 1\},\ \mathrm{tr}(x) = x^{2^0} + x^{2^1} + \ldots + x^{2^{n-1}}; \tag{2}$$

— $\alpha b^{-2} + 4^{-1} \in M_p$ при $p \neq 2$, где

$$M_p = \{x \in \mathcal{S}(\mathbb{F}_{p^n}) : x \neq y^2 \text{ для любого } y \in \mathbb{F}_{p^n}\}. \tag{3}$$

Множества M_p, определённые в (2) и (3), всегда непустые. Однако функции $\sigma_{\alpha,b}$ из теоремы 4 имеют очень простую алгебраическую структуру. Заметим также, что при непростых n всегда существует некоторое линейное подпространство $L \neq \mathbb{F}_{p^n}$, такое, что $\sigma_{\alpha,b}(u + L) = v + L$ для некоторых $u, v \in \mathbb{F}_{p^n}$.

ЛИТЕРАТУРА

1. `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`. FIPS Publ. 197. Advanced Encryption Standard. 2001.
2. *Daemen J. and Rijmen V.* The Design of Rijndael: AES — the Advanced Encryption Standard. Springer Verlag, 2002.
3. *Caranti A., Volta F., and Sala M.* Imprimitive permutations groups generated by the round functions of key-alternating block ciphers and truncated differential cryptanalysis. `https://arxiv.org/abs/math/0606022`. 2006.

4. *Caranti A., Volta F., and Sala M.* An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher // Des. Codes Cryptogr. 2009. V. 52. P. 293–301.
5. *Caranti A., Volta F., and Sala M.* On some block ciphers and imprimitive groups // Appl. Algebra Eng. Commun. Comput. 2009. V. 20. P. 339–350.
6. *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.
7. *Трифонов Д. И., Фомин Д. Б.* Об инвариантных подпространствах в XSL-шифрах // Прикладная дискретная математика. 2021. № 54. С 58–76.
8. *Todo Y., Leander G., and Sasaki Y.* Nonlinear invariant attack: practical attack on full SCREAM, iSCREAM, and Midori64 // ASIACRYPT 2016. LNCS. 2016. V. 10032. P. 3–33.
9. *Буров Д. А.* О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов // Дискретная математика. 2021. Т. 33. № 2. С. 31–45.
10. *Mattarei S.* Inverse-closed additive subgroups of fields // Israel J. Math. 2007. V. 159. P. 343–347.
11. *Goldstein D., Guralnick R., Small L., and Zelmanov E.* Inversion-invariant additive subgroups of division rings // Pacific J. Math. 2006. V. 227. P. 287–294.
12. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
13. *Carlet C.* Open questions on nonlinearity and on APN Functions // LNCS. 2015. V. 9061. P. 83–107.
14. *Hua L.-K.* Some properties of a sfield // Proc. NAS USA. 1949. V. 35. P. 533–537.

УДК 519.214 DOI 10.17223/2226308X/15/2

ОБ АСИМПТОТИЧЕСКОЙ НОРМАЛЬНОСТИ ЧИСЛА КРАТНЫХ СОВПАДЕНИЙ ЦЕПОЧЕК В ПОЛНЫХ q-ИЧНЫХ ДЕРЕВЬЯХ И ЛЕСАХ СО СЛУЧАЙНЫМИ МЕТКАМИ

В. Г. Михайлов, В. И. Круглов

Рассматриваются полные q-ичные корневые деревья высоты H, каждой вершине которых независимо от остальных вершин присвоена случайная метка, выбираемая из множества $\{1, 2, \ldots, N\}$. Исследуются случайные величины, равные числу наборов из $r \geqslant 2$ путей одинаковой длины s, у которых совпадают соответствующие s-цепочки меток вершин. Представлена теорема о достаточных условиях асимптотической нормальности рассматриваемых случайных величин при неограниченном увеличении высоты дерева. При исследовании повторений цепочек в лесе деревьев предполагается, что имеется r деревьев, которые могут иметь разные высоты $H_1, \ldots, H_r$ и вершинам которых аналогичным образом поставлены в соответствие независимые в совокупности случайные метки. Изучается число наборов из r путей длины s, в которые входит по одному пути с каждого дерева, для которых совпадают соответствующие цепочки меток вершин, для этой случайной величины также получены достаточные условия асимптотической нормальности.

Ключевые слова: *деревья с метками, цепочки меток на дереве, повторения цепочек, условия асимптотической нормальности.*