

УДК 511.321 + 519.111.1

DOI 10.17223/20710410/60/2

СВОЙСТВА ЭКСПОНЕНЦИАЛЬНЫХ ПРЕОБРАЗОВАНИЙ КОНЕЧНЫХ ПОЛЕЙ

А. А. Груба

*ООО «Центр сертификационных исследований», г. Москва, Россия***E-mail:** andreyka7kc@gmail.com

Изучаются экспоненциальные преобразования, действующие на множестве всех векторов заданной длины над простым полем. Для них исследуются степень нелинейности, разностная и линейная характеристики.

Ключевые слова: конечные поля, линейные рекуррентные последовательности, разностная характеристика, линейная характеристика.

PROPERTIES OF EXPONENTIAL TRANSFORMATIONS OF FINITE FIELD

A. A. Gruba

Certification Research Center, Moscow, Russia

We consider exponential transformations acting on the set $V_n(p)$ of all vectors of length n over a prime field $P_0 = \text{GF}(p)$ (p is a prime number). For every element $\gamma \in P = \text{GF}(p^n)$ with a minimal polynomial $F(x)$ of degree n over the field P_0 , consider the mapping $\hat{s} : P \rightarrow P$, where $\hat{s}(0) = 0$ and if $x \neq 0$, then $\hat{s}(x) = \gamma^{\sigma(x)}$, $\sigma : P \rightarrow \{0, 1, \dots, p^n - 1\}$ is a mapping that matches each element $x \in P$ with the number $\sigma(x) = x_0 + px_1 + \dots + p^n x_{n-1}$, $\mathbf{x} = (x_0, \dots, x_{n-1})$ is given by its coordinates in the basis α of the vector space P_{P_0} . Transformation $s = \tau^{-1} \cdot \hat{s} \cdot \varkappa$, where $\tau : P \rightarrow V_n(p)$ matches $x \in P$ to its set of coordinates in the basis α of P_{P_0} and the mapping $\varkappa : P \rightarrow V_n(p)$ matches x to its set of coordinates in the dual basis β of the basis α , is called an exponential transformation. We prove estimates for the degree of nonlinearity for an exponential transformation s : $(p-1)(n - \lceil \log_p(n+1) \rceil) \leq \deg s \leq n(p-1) - 1$, where $\lceil z \rceil$ is the minimum integer greater or equal to z . It is proved that $\deg s = n(p-1) - 1$ if and only if the system $\gamma/(\gamma-1), (\gamma/(\gamma-1))^p, \dots, (\gamma/(\gamma-1))^{p^{n-1}}$ is a basis of the vector space P_{P_0} . We also study some properties of the linear and differential characteristics of the transformation s .

Keywords: *finite fields, linear recurrence, difference characteristic, linear characteristic.*

Введение

В работе [1] предложен и изучен класс экспоненциальных подстановок, действующих на множестве всех двоичных векторов заданной длины. Данные подстановки были использованы при построении S-боксов в алгоритме блочного шифрования BelT [2]. Координатные функции подстановок задаются с использованием отрезков линейных рекуррентных последовательностей (ЛРП) над полем $\text{GF}(2)$ из двух элементов.

В данной работе исследуются более общий класс экспоненциальных преобразований, действующих на множестве всех векторов заданной длины над полем $\text{GF}(p)$, где p — простое число. Часть результатов работы [1] удаётся обобщить на предложенный класс преобразований.

Получены верхняя и нижняя оценки степени нелинейности экспоненциальных преобразований, приведены условия достижимости полученной верхней оценки, доказаны достижимые верхние и нижние оценки разностной характеристики. Для оценки линейной характеристики, которая сформулирована в асимптотическом виде в работе [3], удалось вычислить точные значения констант.

1. Определение экспоненциальных преобразований

Пусть $p \in \mathbb{N}$ — простое число, $P_0 = \text{GF}(p) = \{0, 1, \dots, p-1\}$ — поле из p элементов, $P = \text{GF}(p^n)$ — его расширение степени $n \geq 2$, $V_n(p) = P_0^n$ — множество всех n -мерных p -ичных векторов. Для каждого базиса $\alpha = (\alpha_0, \dots, \alpha_{n-1})$ векторного пространства P_{P_0} рассмотрим отображение $\tau : P \rightarrow V_n(p)$, действующее на каждый элемент $x \in P$ по правилу

$$\tau(x) = (x_0, x_1, \dots, x_{n-1}),$$

где $x = x_0\alpha_0 + \dots + x_{n-1}\alpha_{n-1}$, $x_i \in P_0$, $i = 0, 1, \dots, n-1$, т.е. τ сопоставляет каждому элементу $x \in P$ его набор координат в базисе α . Рассмотрим отображение $\sigma : P \rightarrow \{0, 1, \dots, p^n - 1\}$, сопоставляющее каждому элементу $x \in P$ с координатами $\mathbf{x} = (x_0, \dots, x_{n-1})$ число

$$\sigma(x) = x_0 + px_1 + \dots + p^{n-1}x_{n-1}.$$

Введём обозначение $v = \tau^{-1} \cdot \sigma$, т.е. отображение $v : V_n(p) \rightarrow \{0, 1, \dots, p^n - 1\}$ сопоставляет каждому вектору величину

$$v(\mathbf{x}) = v(x_0, \dots, x_{n-1}) = x_0 + px_1 + \dots + p^{n-1}x_{n-1}, \quad \mathbf{x} \in V_n(p).$$

Для каждого элемента γ поля P , имеющего минимальный многочлен $F(x)$ степени n над полем P_0 , рассмотрим преобразование $\hat{s} : P \rightarrow P$, заданное равенствами

$$\hat{s}(x) = \begin{cases} 0, & \text{если } x = 0, \\ \gamma^{\sigma(x)}, & \text{если } x \in P \setminus \{0\}. \end{cases} \quad (1)$$

Преобразование $\hat{s}$ однозначно задаётся элементом γ и базисом α .

Сопоставим преобразованию $\hat{s}$, определённое равенством (1), преобразование s на множестве $V_n(p)$. Пусть $\text{tr} = \text{tr}_{P_0}^P$ — функция «след» из поля P в подполе P_0 , определённая при всех $x \in P$ по правилу $\text{tr}(x) = x + x^p + \dots + x^{p^{n-1}}$. Обозначим через $\beta = (\beta_0, \dots, \beta_{n-1})$ базис, двойственный к базису α , т.е. удовлетворяющий условию

$$\text{tr}(\alpha_i\beta_j) = \begin{cases} 0, & \text{если } i \neq j, \\ 1, & \text{если } i = j. \end{cases}$$

Такой базис существует и находится однозначно [4]. Определим отображение $\varkappa : P \rightarrow V_n(p)$, которое сопоставляет каждому элементу $x \in P$ его набор координат $(y_0, \dots, y_{n-1})$ в базисе β :

$$\varkappa(x) = (y_0, \dots, y_{n-1}), \quad x = y_0\beta_0 + \dots + y_{n-1}\beta_{n-1}.$$

Пусть $\varkappa_i$ — i -я координатная функция отображения $\varkappa$, $i = 0, 1, \dots, n-1$. В силу линейности функции «след» имеем

$$\mathrm{tr}(\alpha_i x) = \mathrm{tr} \left(\alpha_i \sum_{j=0}^{n-1} y_j \beta_j \right) = \sum_{j=0}^{n-1} y_j \mathrm{tr}(\alpha_i \beta_j) = y_i = \varkappa_i(x). \quad (2)$$

Преобразование s на множестве $V_n(p)$, определённое по правилу

$$s = \tau^{-1} \cdot \hat{s} \cdot \varkappa, \quad (3)$$

будем называть *экспоненциальным преобразованием*.

Утверждение 1. Для всех $\mathbf{x} \in V_n(p) \setminus \{\mathbf{0}\}$

$$s(\mathbf{x}) = \varkappa(\gamma^{v(\mathbf{x})}) = (\mathrm{tr}(\alpha_0 \gamma^{v(\mathbf{x})}), \dots, \mathrm{tr}(\alpha_{n-1} \gamma^{v(\mathbf{x})})).$$

Доказательство. Пусть s_i — i -я координатная функция преобразования s , где $i = 0, 1, \dots, n-1$. Тогда в силу равенств (2) и (3) для всех $\mathbf{x} \in V_n(p) \setminus \{\mathbf{0}\}$ имеем

$$s_i(\mathbf{x}) = \varkappa_i(\hat{s}(\tau^{-1}(\mathbf{x}))) = \varkappa_i(\gamma^{\sigma(\tau^{-1}(\mathbf{x}))}) = \varkappa_i(\gamma^{v(\mathbf{x})}) = \mathrm{tr}(\alpha_i \gamma^{v(\mathbf{x})}).$$

Утверждение 1 доказано. ■

Установим связь экспоненциальных преобразований с ЛРП над полем P_0 . Выберем базис $u_0, u_1, \dots, u_{n-1}$ пространства $L_{P_0}(F)$ всех ЛРП над полем P_0 с характеристическим многочленом $F(x)$ [4–6]. Представим ЛРП u_j , $j = 0, 1, \dots, n-1$, с использованием функции «след» [4–6]:

$$u_j(i) = \mathrm{tr}(\theta_j \gamma^i), \quad i \geq 0. \quad (4)$$

Здесь θ_j — однозначно определённый элемент поля P . Пусть (0) — нулевая последовательность. Заметим, что для всех $c_0, \dots, c_{n-1} \in P_0$ соотношение $c_0 u_0 + \dots + c_{n-1} u_{n-1} = (0)$ равносильно условию $\mathrm{tr}((c_0 \theta_0 + \dots + c_{n-1} \theta_{n-1}) \gamma^i) = 0$ для всех $i \geq 0$, а это, в свою очередь, означает, что $c_0 \theta_0 + \dots + c_{n-1} \theta_{n-1} = 0$. Таким образом, $u_0, \dots, u_{n-1}$ — базис векторного пространства $L_{P_0}(F)$ тогда и только тогда, когда $\theta_0, \dots, \theta_{n-1}$ — базис векторного пространства P_{P_0} . Зададим отображение $\pi : P_0^n \rightarrow P_0^n$, действующее по правилу, указанному в табл. 1.

Т а б л и ц а 1

x_0	x_1	$\dots$	x_{n-2}	x_{n-1}	$\pi(x_0, \dots, x_{n-1})$
0	0	$\dots$	0	0	$\mathbf{0}$
1	0	$\dots$	0	0	$(u_0(0), \dots, u_{n-1}(0))$
2	0	$\dots$	0	0	$(u_0(1), \dots, u_{n-1}(1))$
		$\dots$			$\dots$
$p-1$	0	$\dots$	0	0	$(u_0(p-2), \dots, u_{n-1}(p-2))$
0	1	$\dots$	0	0	$(u_0(p-1), \dots, u_{n-1}(p-1))$
		$\dots$			$\dots$
$p-1$	$p-1$	$\dots$	$p-1$	$p-1$	$(u_0(p^n-2), \dots, u_{n-1}(p^n-2))$

Аргументы $\mathbf{x}$ в таблице перечисляются в лексикографическом порядке (в порядке возрастания величин $v(\mathbf{x})$). Если многочлен $F(x)$ является примитивным над полем P_0 , то среди векторов $(u_0(i), \dots, u_{n-1}(i))$, $i = 0, 1, \dots, p^n - 2$, появляются все ненулевые

векторы из $V_n(p)$, причём ровно по одному разу [7, 8], и отображение π является подстановкой на множестве $V_n(p)$.

Выберем $\theta_0 = \alpha_0\gamma, \dots, \theta_{n-1} = \alpha_{n-1}\gamma$, где $\alpha = (\alpha_0, \dots, \alpha_{n-1})$ — базис векторного пространства P_{P_0} . Ясно, что $\theta = (\theta_0, \dots, \theta_{n-1})$ также является базисом пространства P_{P_0} . Согласно равенству (4) и утверждению 1, для j -й координатной функции π_j , $j = 0, 1, \dots, n-1$, преобразования π имеем

$$\pi_j(\mathbf{x}) = u_j(v(\mathbf{x}) - 1) = \text{tr}(\theta_j \gamma^{v(\mathbf{x})-1}) = \text{tr}(\alpha_j \gamma^{v(\mathbf{x})}) = s_j(\mathbf{x}), \quad \mathbf{x} \in V_n(p) \setminus \{\mathbf{0}\}.$$

Таким образом, $s = \pi$. При фиксированном γ и произвольном выборе базисов α множество всех экспоненциальных преобразований совпадает с множеством всех преобразований π , соответствующих всем базисам θ векторного пространства P_{P_0} (или, что то же самое, всем базисам $u_0, u_1, \dots, u_{n-1}$ пространства $L_{P_0}(F)$).

Утверждение 2. Число всех экспоненциальных преобразований на множестве $V_n(p)$ находится по формуле

$$\frac{1}{n} (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) \sum_{d|n} \mu(d) p^{n/d},$$

где μ — функция Мебиуса.

Доказательство. При фиксированном корне γ неприводимого многочлена $F(x)$ число экспоненциальных преобразований равно числу базисов векторного пространства $L_{P_0}(F)$:

$$(p^n - 1)(p^n - p) \dots (p^n - p^{n-1}).$$

Если выбрать другой корень γ' многочлена $F(x)$, то получим такой же класс преобразований, что и при выборе элемента γ . При различных неприводимых многочленах $F_1(x)$ и $F_2(x)$ выполнено $L_{P_0}(F_1) \cap L_{P_0}(F_2) = \{(0)\}$ [4, 6]. Остаётся заметить [4, 6], что число неприводимых многочленов степени n над полем P_0 равно

$$\frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}.$$

Утверждение 2 доказано. ■

2. Степень нелинейности экспоненциальных преобразований

Рассмотрим степень нелинейности $\deg s$ экспоненциального преобразования (3). Она вычисляется [9] по формуле

$$\deg s = \min_{(a_0, \dots, a_{n-1}) \in V_n(p) \setminus \{\mathbf{0}\}} \deg(a_0 s_0(x_0, \dots, x_{n-1}) + \dots + a_{n-1} s_{n-1}(x_0, \dots, x_{n-1}))$$

и равна минимальной из степеней многочленов (алгебраически нормальных форм) всех нетривиальных линейных комбинаций координатных функций $s_0, \dots, s_{n-1}$ преобразования s .

Пусть $F(x)$ — неприводимый многочлен степени n над полем P_0 с периодом $T(F)$ [4, 6], равным $(p^n - 1)/d$, где d — некоторый делитель числа $p^n - 1$; γ — корень многочлена $F(x)$ в расширении P . Рассмотрим ненулевую ЛРП u с характеристическим многочленом $F(x)$ над полем P_0 . Построим функцию $f(x_0, \dots, x_{n-1}) = f_u(x_0, \dots, x_{n-1})$ по правилу, указанному в табл. 2.

Т а б л и ц а 2

x_0	x_1	$\dots$	x_{n-2}	x_{n-1}	$f(x_0, \dots, x_{n-1})$
0	0	$\dots$	0	0	0
1	0	$\dots$	0	0	$u(0)$
2	0	$\dots$	0	0	$u(1)$
		$\dots$			
$p-1$	0	$\dots$	0	0	$u(p-2)$
0	1	$\dots$	0	0	$u(p-1)$
		$\dots$			
$p-1$	$p-1$	$\dots$	$p-1$	$p-1$	$u(p^n-2)$

Обозначим через $B_n(F)$ множество всех функций $f_u(x_0, \dots, x_{n-1})$, где u пробегает всё множество ненулевых ЛРП над полем P_0 с характеристическим многочленом $F(x)$. Ясно, что $|B_n(F)| = |L_{P_0}(F) \setminus (0)| = p^n - 1$. Учитывая совпадение экспоненциальных преобразований с преобразованиями, построенными на основе ЛРП, получим

$$\deg s = \min_{f \in B_n(F)} \deg f.$$

Таким образом, необходимо изучить величину $\deg f$. Рассмотрим многочлен, задающий функцию $f(x_0, \dots, x_{n-1}) \in B_n(F)$:

$$f(x_0, \dots, x_{n-1}) = \sum_{\mathbf{a}=(a_0, \dots, a_{n-1}) \in V_n(p)} C(\mathbf{a}) x_0^{a_0} \dots x_{n-1}^{a_{n-1}}.$$

Обозначим через $\mathbf{b} = (p-1, \dots, p-1)$ вектор, у которого все координаты равны $p-1$. Тогда $C(\mathbf{b})$ — коэффициент в многочлене функции $f \in B_n(F)$ при мономе $x_0^{p-1} \dots x_{n-1}^{p-1}$.

Утверждение 3. Для любой функции $f_u \in B_n(F)$ выполнено $C(\mathbf{b}) = 0$. В частности, для экспоненциального преобразования s , определённого равенством (3), справедливо неравенство $\deg s \leq n(p-1) - 1$.

Доказательство. Пусть $f = f_u$. Согласно [10],

$$C(\mathbf{b}) = - \sum_{a_0, \dots, a_{n-1} \in P_0} f(a_0, \dots, a_{n-1}) = -(u(0) + u(1) + \dots + u(p^n - 2)).$$

Так как $T(F) = (p^n - 1)/d$, то

$$C(\mathbf{b}) = -d(u(0) + u(1) + \dots + u(T(F) - 1)).$$

Пусть $u(i) = \text{tr}(a\gamma^i)$, где $a \in P$, γ — корень многочлена $F(x)$ в поле P , $i \geq 0$. Получим

$$C(\mathbf{b}) = -d(\text{tr}(a) + \text{tr}(a\gamma) + \dots + \text{tr}(a\gamma^{T(F)-1})) = -d \text{tr} \left(a \frac{\gamma^{T(F)} - 1}{\gamma - 1} \right).$$

Мультипликативный порядок $\text{ord } \gamma$ элемента γ равен $T(F)$, следовательно, $\gamma^{T(F)} = 1$, а значит, $C(\mathbf{b}) = 0$. ■

Пусть $k \in \{0, 1, \dots, n-1\}$. Обозначим через

$$\mathbf{b}_k = (p-1, \dots, p-1, p-2, p-1, \dots, p-1) = (b_0, \dots, b_{n-1})$$

вектор, у которого $b_k = p-2$, а остальные координаты равны $p-1$. Тогда $C(\mathbf{b}_k)$ — коэффициент в многочлене, задающем функцию $f \in B_n(F)$, при мономе

$$x_0^{p-1} \dots x_{k-1}^{p-1} x_k^{p-2} x_{k+1}^{p-1} \dots x_{n-1}^{p-1}.$$

Теорема 1. Пусть $u \in L_{P_0}(F)$, $u(i) = \text{tr}(a\gamma^i)$, где $i \geq 0$, $a \in P$, γ — корень многочлена $F(x)$ в поле P . Тогда для любой функции $f = f_u \in B_n(F)$ верно равенство

$$C(\mathbf{b}_k) = \text{tr} \left(a\gamma^{-1} \left(\frac{\gamma}{\gamma-1} \right)^{p^{n-k-1}} \right), \quad k = 0, 1, \dots, n-1.$$

Доказательство. Обозначим через P_0^* мультипликативную группу поля P_0 . Согласно [10], имеем

$$\begin{aligned} C(\mathbf{b}_k) &= - \sum_{\mathbf{a}=(a_0, \dots, a_{n-1}) \in P_0^n} a_k f(\mathbf{a}) = - \sum_{a_k \in P_0^*} a_k \sum_{a_0, \dots, a_{k-1}, a_{k+1}, \dots, a_{n-1} \in P_0} f(\mathbf{a}) = \\ &= - \sum_{j=1}^{p-1} j \sum_{s=0}^{p^k-1} \sum_{i=0}^{p^{n-1-k}-1} u(sp^{n-k} + jp^{n-1-k} + i - 1). \end{aligned}$$

Так как $u(i) = \text{tr}(a\gamma^i)$, $i \geq 0$, то

$$C(\mathbf{b}_k) = - \sum_{j=1}^{p-1} j \sum_{s=0}^{p^k-1} \sum_{i=0}^{p^{n-1-k}-1} \text{tr} \left(a\gamma^{sp^{n-k} + jp^{n-1-k} + i - 1} \right).$$

В силу линейности функции «след» получим

$$\begin{aligned} C(\mathbf{b}_k) &= - \sum_{j=1}^{p-1} j \sum_{s=0}^{p^k-1} \text{tr} \left(a\gamma^{-1} \gamma^{sp^{n-k} + jp^{n-1-k}} \frac{\gamma^{p^{n-1-k}} - 1}{\gamma - 1} \right) = \\ &= - \sum_{j=1}^{p-1} j \text{tr} \left(a\gamma^{-1} \gamma^{jp^{n-1-k}} \frac{\gamma^{p^{n-1-k}} - 1}{\gamma - 1} \frac{(\gamma^{p^{n-k}})^{p^k} - 1}{\gamma^{p^{n-k}} - 1} \right). \end{aligned}$$

Так как $\text{ord } \gamma$ делит $p^n - 1$, то $\gamma^{p^n} = \gamma$. Значит,

$$C(\mathbf{b}_k) = - \sum_{j=1}^{p-1} \text{tr} \left(ja\gamma^{-1} \frac{\gamma^{p^{n-1-k}} - 1}{\gamma^{p^{n-k}} - 1} \gamma^{jp^{n-1-k}} \right).$$

Пусть $\tilde{\gamma} = \gamma^{p^{n-1-k}}$. Обозначим $S_{\tilde{\gamma}}^{(n)} = \tilde{\gamma} + \tilde{\gamma}^2 + \dots + \tilde{\gamma}^n = \tilde{\gamma} \frac{\tilde{\gamma}^n - 1}{\tilde{\gamma} - 1}$. Рассмотрим сумму

$$S = \sum_{j=1}^{p-1} j\tilde{\gamma}^j = \tilde{\gamma} + 2\tilde{\gamma}^2 + \dots + (p-1)\tilde{\gamma}^{p-1}.$$

Ясно, что $S = S_{\tilde{\gamma}}^{(p-1)} + \tilde{\gamma}S_{\tilde{\gamma}}^{(p-2)} + \dots + \tilde{\gamma}^{p-2}S_{\tilde{\gamma}}^{(1)}$. Тогда

$$\begin{aligned} S &= \tilde{\gamma} \frac{\tilde{\gamma}^{p-1} - 1}{\tilde{\gamma} - 1} + \tilde{\gamma} \left(\tilde{\gamma} \frac{\tilde{\gamma}^{p-2} - 1}{\tilde{\gamma} - 1} \right) + \dots + \tilde{\gamma}^{p-3} \left(\tilde{\gamma} \frac{\tilde{\gamma}^2 - 1}{\tilde{\gamma} - 1} \right) + \tilde{\gamma}^{p-2} \tilde{\gamma} = \\ &= \frac{\tilde{\gamma}}{\tilde{\gamma} - 1} ((\tilde{\gamma}^{p-1} - 1) + (\tilde{\gamma}^{p-1} - \tilde{\gamma}) + \dots + (\tilde{\gamma}^{p-1} - \tilde{\gamma}^{p-3}) + (\tilde{\gamma}^{p-1} - \tilde{\gamma}^{p-2})) = \\ &= \frac{\tilde{\gamma}}{\tilde{\gamma} - 1} \left((p-1)\tilde{\gamma}^{p-1} - \frac{\tilde{\gamma}^{p-1} - 1}{\tilde{\gamma} - 1} \right) = \frac{\tilde{\gamma}}{(\tilde{\gamma} - 1)^2} (1 - \tilde{\gamma}^p). \end{aligned}$$

Следовательно,

$$\begin{aligned} C(\mathbf{b}_k) &= -\operatorname{tr} \left(a\gamma^{-1} \frac{\gamma^{p^{n-k-1}} - 1}{\gamma^{p^{n-k}} - 1} \frac{\gamma^{p^{n-k-1}}}{(\gamma^{p^{n-k-1}} - 1)^2} \left(1 - \left(\gamma^{p^{n-k-1}} \right)^p \right) \right) = \\ &= \operatorname{tr} \left(a\gamma^{-1} \frac{\gamma^{p^{n-1-k}}}{\gamma^{p^{n-k-1}} - 1} \right). \end{aligned}$$

Таким образом,

$$C(\mathbf{b}_k) = \operatorname{tr} \left(a\gamma^{-1} \left(\frac{\gamma}{\gamma - 1} \right)^{p^{n-k-1}} \right).$$

Теорема 1 доказана. ■

Утверждение 4. Для каждой функции $f \in B_n(F)$ равенство $\deg f = n(p-1) - 1$ имеет место тогда и только тогда, когда система

$$\frac{\gamma}{\gamma - 1}, \left(\frac{\gamma}{\gamma - 1} \right)^p, \dots, \left(\frac{\gamma}{\gamma - 1} \right)^{p^{n-1}} \quad (5)$$

является базисом векторного пространства P_{P_0} .

Доказательство. Обозначим через P^* мультипликативную группу поля P . Положим для $k = 0, 1, \dots, n-1$

$$\widehat{\gamma}_k = \left(\frac{\gamma}{\gamma - 1} \right)^{p^k}.$$

Согласно теореме 1, доказываемый факт равносильно тому, что для всех $x \in P^*$

$$(\operatorname{tr}(x\widehat{\gamma}_0), \operatorname{tr}(x\widehat{\gamma}_1), \dots, \operatorname{tr}(x\widehat{\gamma}_{n-1})) \neq \mathbf{0}. \quad (6)$$

Пусть $\mathbf{x} = (x_0, \dots, x_{n-1})$ — координаты элемента x в базисе α , $\mathbf{A}_k = (a_0^{(k)}, \dots, a_{n-1}^{(k)})$ — координаты элемента $\widehat{\gamma}_k$, $k = 0, 1, \dots, n-1$, в базисе $\beta = (\beta_0, \beta_1, \dots, \beta_{n-1})$, который является двойственным к базису α . Тогда

$$\operatorname{tr}(x\widehat{\gamma}_k) = \operatorname{tr} \left(\sum_{i=0}^{n-1} x_i \alpha_i \sum_{j=0}^{n-1} a_j^{(k)} \beta_j \right) = \sum_{i=0}^{n-1} a_i^{(k)} x_i = \mathbf{A}_k x^\downarrow.$$

Пусть

$$A = \begin{pmatrix} \mathbf{A}_0 \\ \vdots \\ \mathbf{A}_{n-1} \end{pmatrix}_{n \times n},$$

тогда соотношение (6) равносильно неравенству $Ax^\downarrow \neq 0^\downarrow$. Таким образом, равенство (6) имеет место для всех $x \in P^*$ тогда и только тогда, когда матрица A обратима над полем P_0 , то есть система векторов (5) линейно независима. В свою очередь, это равносильно тому, что система

$$\left(\frac{\gamma}{\gamma - 1} \right)^{p^k}, \quad k = 0, 1, \dots, n-1,$$

является базисом векторного пространства P_{P_0} . ■

Следствие 1. Для экспоненциального преобразования s , определённого равенством (3), $\deg s = n(p-1) - 1$ тогда и только тогда, когда система (5) является базисом векторного пространства P_{P_0} .

Утверждение 5. Пусть $\delta = \gamma/(\gamma-1)$, где γ — корень неприводимого многочлена степени n над полем P_0 . Тогда δ — корень неприводимого многочлена степени n .

Доказательство. Рассмотрим $m_{\delta, P_0}(x)$ — минимальный многочлен элемента δ над полем P_0 . Пусть $k = \deg m_{\delta, P_0}(x)$. Согласно [6], k — наименьшее натуральное число, такое, что

$$\frac{\gamma}{\gamma-1} = \left(\frac{\gamma}{\gamma-1} \right)^{p^k},$$

т.е. $\gamma(\gamma^{p^k} - 1) = \gamma^{p^k}(\gamma - 1)$, а значит, $\gamma = \gamma^{p^k}$. Так как γ — корень неприводимого многочлена степени n , наименьшее число k с таким условием равно n . ■

Приведём нижнюю оценку степени нелинейности экспоненциального преобразования.

Теорема 2. Пусть $F(x)$ — неприводимый многочлен степени n над полем P_0 . Тогда для всех $f_u \in B_n(F)$ имеет место неравенство

$$\deg f_u \geq (p-1)(n - \lceil \log_p(n+1) \rceil),$$

где $\lceil z \rceil$ — минимальное целое число, которое больше либо равно z . В частности, для экспоненциального преобразования s , определённого равенством (3), справедлива оценка

$$\deg s \geq (p-1)(n - \lceil \log_p(n+1) \rceil).$$

Доказательство. Пусть $f = f_u$, где u — ЛРП с характеристическим многочленом $F(x)$. Тогда $u(i) = \text{tr}(\beta\gamma^i)$, $i \geq 0$, $\beta \in P^*$, и выполнены соотношения

$$f(\mathbf{0}) = 0, \quad f(\mathbf{x}) = u(v(\mathbf{x}) - 1) = \text{tr}(\beta\gamma^{v(\mathbf{x})-1}), \quad \mathbf{x} \neq \mathbf{0}.$$

Положим

$$\varepsilon = \begin{cases} 1, & \text{если } n \text{ нечётное,} \\ -1, & \text{если } n \text{ чётное.} \end{cases}$$

Тогда в силу того, что $\prod_{s=1}^{p-1} s = p-1 \pmod{p}$ [6], для всех $\mathbf{x} = (x_0, \dots, x_{n-1}) \in V_n(p)$ справедливо равенство

$$f(\mathbf{x}) = \text{tr} \left(\beta\gamma^{-1} \gamma^{\sum_{i=0}^{n-1} x_i p^i} \right) + \varepsilon \text{tr}(\beta\gamma^{-1}) \prod_{i=0}^{n-1} \prod_{s=1}^{p-1} (x_i - s).$$

Пусть $\gamma_i = \gamma^{p^i}$, $i = 0, 1, \dots, n-1$, значит,

$$f(\mathbf{x}) = \text{tr}(\beta\gamma^{-1} \gamma_0^{x_0} \gamma_1^{x_1} \dots \gamma_{n-1}^{x_{n-1}}) + \varepsilon \text{tr}(\beta\gamma^{-1}) \prod_{i=0}^{n-1} \prod_{s=1}^{p-1} (x_i - s).$$

Пусть $j \in \{0, 1, \dots, n-1\}$. Для всех $s \in P_0$ обозначим через $f_{x_j}^s$ функцию, полученную из f фиксацией переменной x_j значением s :

$$f(x_0, \dots, x_{j-1}, s, x_{j+1}, \dots, x_{n-1}) = f_{x_j}^s.$$

Рассмотрим оператор Δ_j взятия суммы всех элементов поля P_0 по переменной x_j в функции f , т. е.

$$\Delta_j f = \sum_{a_j \in P_0} f_{x_j}^{a_j}.$$

Тогда

$$\Delta_j f = \sum_{a_j \in P_0} \text{tr} \left(\beta \gamma^{-1} \gamma_0^{x_0} \dots \gamma_{j-1}^{x_{j-1}} \gamma_j^{a_j} \gamma_{j+1}^{x_{j+1}} \dots \gamma_{n-1}^{x_{n-1}} \right) + (-1)^p \varepsilon \text{tr}(\beta \gamma^{-1}) \prod_{i=0, i \neq j}^{n-1} \prod_{s=1}^{p-1} (x_i - s).$$

Следовательно,

$$\begin{aligned} \Delta_j f &= \text{tr} \left(\beta \gamma^{-1} \frac{\gamma_j^p - 1}{\gamma_j - 1} \gamma_0^{x_0} \dots \gamma_{j-1}^{x_{j-1}} \gamma_{j+1}^{x_{j+1}} \dots \gamma_{n-1}^{x_{n-1}} \right) + \\ &+ (-1)^p \varepsilon \text{tr}(\beta \gamma^{-1}) \prod_{i=0, i \neq j}^{n-1} \prod_{s=1}^{p-1} (x_i - s). \end{aligned} \quad (7)$$

С другой стороны,

$$\begin{aligned} \Delta_j f &= \sum_{c \in P_0} \sum_{\mathbf{a}=(a_0, \dots, a_{n-1}) \in V_n(p)} C(\mathbf{a}) x_0^{a_0} \dots x_{j-1}^{a_{j-1}} c^{a_j} x_{j+1}^{a_{j+1}} \dots x_{n-1}^{a_{n-1}} = \\ &= \sum_{a_j, c \in P_0} c^{a_j} \sum_{a_0, \dots, a_{j-1}, a_{j+1}, \dots, a_{n-1} \in P_0} C(\mathbf{a}) x_0^{a_0} \dots x_{j-1}^{a_{j-1}} x_{j+1}^{a_{j+1}} \dots x_{n-1}^{a_{n-1}}. \end{aligned}$$

Справедливо равенство [10]

$$\sum_{c \in P_0} c^{a_j} = \begin{cases} p-1, & \text{если } a_j = p-1, \\ 0, & \text{если } a_j < p-1. \end{cases}$$

Значит, если $\Delta_j f$ является ненулевой функцией, то переменная x_j входит в многочлен функции f в степени $p-1$ и $\sum_{a_j \in P_0} f(x_0, \dots, x_{j-1}, a_j, x_{j+1}, \dots, x_{n-1})$ содержит все те слагаемые (ненулевые), которые имеют вид

$$-C(a_0, \dots, a_{j-1}, p-1, a_{j+1}, \dots, a_{n-1}) x_0^{a_0} \dots x_{j-1}^{a_{j-1}} x_j^{p-1} x_{j+1}^{a_{j+1}} \dots x_{n-1}^{a_{n-1}}.$$

Следовательно, если $\Delta_j f$ — ненулевая функция, то

$$\deg f \geq p-1 + \deg(\Delta_j f). \quad (8)$$

Пусть $\Delta_k \dots \Delta_{n-2} \Delta_{n-1} f = g(x_0, \dots, x_{k-1})$, где $k = 0, 1, \dots, n-1$. Согласно (7), будем иметь

$$\begin{aligned} g(x_0, \dots, x_{k-1}) &= \\ &= \text{tr} \left(\beta \gamma^{-1} \frac{\gamma_k^p - 1}{\gamma_k - 1} \dots \frac{\gamma_{n-1}^p - 1}{\gamma_{n-1} - 1} \gamma_0^{x_0} \dots \gamma_{k-1}^{x_{k-1}} \right) + (-1)^{(n-k)p} \varepsilon \text{tr}(\beta \gamma^{-1}) \prod_{i=0}^{k-1} \prod_{s=1}^{p-1} (x_i - s). \end{aligned}$$

Рассмотрим вектор

$$\begin{aligned} (g(1, 0, \dots, 0), \dots, g(p-1, 0, \dots, 0), g(0, 1, 0, \dots, 0), \dots, g(p-1, \dots, p-1)) = \\ = (\omega(0), \omega(1), \dots, \omega(p^k - 2)), \end{aligned}$$

где

$$\omega(i) = \text{tr} \left(\beta \gamma^{-1} \frac{\gamma_k^p - 1}{\gamma_k - 1} \cdots \frac{\gamma_{n-1}^p - 1}{\gamma_{n-1} - 1} \gamma^i \right), \quad i \geq 0.$$

Так как $\gamma_0, \gamma_1, \dots, \gamma_{n-1}$ — корни многочлена $F(x)$ в поле P , то $\text{ord } \gamma_i = T(F)$, $i = 0, 1, \dots, n-1$ [4, 6],

$$\frac{\gamma_k^p - 1}{\gamma_k - 1} \cdots \frac{\gamma_{n-1}^p - 1}{\gamma_{n-1} - 1} \neq 0$$

и последовательность w является ЛРП с характеристическим многочленом $F(x)$. Если $p^k - 1 \geq n$, то любой отрезок длины $p^k - 1$ ЛРП w не является нулевым. Тогда если $k \geq \lceil \log_p(n+1) \rceil$, то $g(x_0, \dots, x_{k-1})$ — ненулевая функция. В итоге с использованием неравенства (8) получим

$$\deg f \geq (p-1)(n-k) + \deg g \geq (p-1)(n-k) \geq (p-1)(n - \lceil \log_p(n+1) \rceil).$$

Теорема 2 доказана. ■

Доказанная теорема обобщает на случай произвольного простого числа p и неприводимого многочлена $F(x)$ соответствующую теорему из работы [1].

3. Разностная характеристика экспоненциальных подстановок

Пусть на множестве $V_n(p)$ заданы две операции $*$ и $\circ$, причём $(V_n(p), *)$ и $(V_n(p), \circ)$ — абелевы группы с нейтральным элементом $\mathbf{0}$. Для преобразования $s : V_n(p) \rightarrow V_n(p)$, определённого равенством (3), и векторов $\mathbf{a}, \mathbf{b}$, где $\mathbf{a} \neq \mathbf{0}$, определим число

$$\rho_{\mathbf{a}, \mathbf{b}}(s) = |\{\mathbf{x} \in V_n(p) : s(\mathbf{x} * \mathbf{a}) = s(\mathbf{x}) \circ \mathbf{b}\}|.$$

Тогда величину

$$\rho_{*, \circ}(s) = \max_{\mathbf{a}, \mathbf{b} \in V_n(p), \mathbf{a} \neq \mathbf{0}} \rho_{\mathbf{a}, \mathbf{b}}(s)$$

назовём *разностной характеристикой* преобразования s относительно операций $*$ и $\circ$.

Рассмотрим четыре операции на $V_n(p)$, определённые для всех $\mathbf{x}, \mathbf{y} \in V_n(p)$ по правилам

$$\begin{aligned} \mathbf{x} \oplus \mathbf{y} &= \tau(\tau^{-1}(\mathbf{x}) + \tau^{-1}(\mathbf{y})), & \mathbf{x} \ominus \mathbf{y} &= \tau(\tau^{-1}(\mathbf{x}) - \tau^{-1}(\mathbf{y})), \\ \mathbf{x} \boxplus \mathbf{y} &= v^{-1}(v(\mathbf{x}) + v(\mathbf{y}) \bmod p^n), & \mathbf{x} \boxminus \mathbf{y} &= v^{-1}(v(\mathbf{x}) - v(\mathbf{y}) \bmod p^n), \end{aligned}$$

при этом справа в первых двух равенствах операции сложения и вычитания рассматриваются в поле P , а в последних двух — в кольце целых чисел. Операция $\ominus$ является симметричной относительно операции $\oplus$, а $\boxminus$ — относительно операции $\boxplus$. Для любого вектора $\mathbf{a} \in V_n(p)$ через $\boxminus \mathbf{a}$ будем обозначать симметричный вектор относительно операции $\boxplus$ для вектора $\mathbf{a}$. Для доказательства следующего результата воспользуемся методом, описанным в работе [1].

Теорема 3. Пусть s — экспоненциальная подстановка, определённая равенством (3). Тогда

- 1) если $p \geq 3$, то $2 \leq \rho_{\boxminus, \oplus}(s) \leq 3$;
- 2) если $p = 2$, то $2 \leq \rho_{\boxminus, \oplus}(s) \leq 4$, причём $\rho_{\boxminus, \oplus}(s) = 4$ тогда и только тогда, когда $F(x)$ делит хотя бы один из многочленов вида

$$x^{2^{n-1}} + x^t + 1, \quad t = 1, 2, \dots, 2^{n-1} - 1. \quad (9)$$

Доказательство. Заметим, что $\rho_{\boxplus, \boxplus}(s) \geq 2$. Действительно, если $\rho_{\boxplus, \boxplus}(s) = 1$, то для всех ненулевых $\mathbf{a} \in V_n(p)$ отображение $g_{\mathbf{a}} : V_n(p) \rightarrow V_n(p)$, действующее по правилу

$$g_{\mathbf{a}}(\mathbf{x}) = s(\mathbf{x} \boxplus \mathbf{a}) \ominus s(\mathbf{x}),$$

является биекцией. Следовательно, принимает значение $\mathbf{0}$, что противоречит биективности подстановки s . Зафиксируем вектор $\mathbf{a} \in V_n(p) \setminus \{\mathbf{0}\}$. Пусть $v(\mathbf{a}) = t_0$. Найдём наибольшее значение величины $\rho_{\mathbf{a}, \mathbf{b}}(s)$ при всех $\mathbf{b} \in V_n(p)$. Эта величина равна наибольшему числу появлений вектора $\mathbf{b} \in V_n(p)$ в мультимножестве (множестве с повторениями)

$$M(\mathbf{a}) = \{s(\mathbf{x} \boxplus \mathbf{a}) \ominus s(\mathbf{x}) : \mathbf{x} \in V_n(p)\}.$$

Заметим, что мультимножество $M(\mathbf{a})$ при замене $\mathbf{t} = \mathbf{x} \boxplus \mathbf{a}$ превращается в мультимножество

$$\{s(\mathbf{t}) \ominus s(\mathbf{t} \boxminus \mathbf{a}) : \mathbf{t} \in V_n(p)\}.$$

Следовательно, $\rho_{\mathbf{a}, \mathbf{b}}(s) = \rho_{\boxminus \mathbf{a}, \ominus \mathbf{b}}(s)$. Справедливы равенства

$$\begin{aligned} M(\mathbf{a}) &= \{s(\mathbf{a})\} \cup \{s(\boxminus \mathbf{a})\} \cup \{s(\mathbf{x} \boxplus \mathbf{a}) \ominus s(\mathbf{x}) : \mathbf{x} \in V_n(p), \mathbf{x} \neq \mathbf{0}, \mathbf{x} \neq \boxminus \mathbf{a}\} = \\ &= \{\varkappa(\gamma^{v(\mathbf{a})})\} \cup \{\varkappa(\gamma^{v(\boxminus \mathbf{a})})\} \cup \{\varkappa(\gamma^{v(\mathbf{x} \boxplus \mathbf{a})}) \ominus \varkappa(\gamma^{v(\mathbf{x})}) : \mathbf{x} \in V_n(p), \mathbf{x} \neq \mathbf{0}, \mathbf{x} \neq \boxminus \mathbf{a}\} = \\ &= \{\varkappa(\gamma^{v(\mathbf{a})})\} \cup \{\varkappa(\gamma^{v(\boxminus \mathbf{a})})\} \cup \{\varkappa(\gamma^{(v(\mathbf{x})+v(\mathbf{a})) \bmod p^n}) \ominus \varkappa(\gamma^{v(\mathbf{x})}) : \mathbf{x} \in V_n(p), \mathbf{x} \neq \mathbf{0}, \mathbf{x} \neq \boxminus \mathbf{a}\} = \\ &= \{\varkappa(\gamma^{v(\mathbf{a})})\} \cup \{\varkappa(\gamma^{v(\boxminus \mathbf{a})})\} \cup \{\varkappa(\gamma^{(v(\mathbf{x})+v(\mathbf{a})) \bmod p^n} - \gamma^{v(\mathbf{x})}) : \mathbf{x} \in V_n(p), \mathbf{x} \neq \mathbf{0}, \mathbf{x} \neq \boxminus \mathbf{a}\}. \end{aligned}$$

Рассмотрим мультимножество

$$N(\mathbf{a}) = \{\gamma^{v(\mathbf{a})}\} \cup \{\gamma^{v(\boxminus \mathbf{a})}\} \cup \{\gamma^{(v(\mathbf{x})+v(\mathbf{a})) \bmod p^n} - \gamma^{v(\mathbf{x})} : \mathbf{x} \in V_n(p), \mathbf{x} \neq \mathbf{0}, \mathbf{x} \neq \boxminus \mathbf{a}\}.$$

Ясно, что $\rho_{\mathbf{a}, \mathbf{b}}(s)$ равно числу появлений элемента $b = \varkappa^{-1}(\mathbf{b})$ среди элементов мультимножества $N(\mathbf{a})$. Так как $v(\mathbf{a}) = t_0$, то $v(\boxminus \mathbf{a}) = p^n - t_0$. Если $t = v(\mathbf{x})$ и $\mathbf{x}$ пробегает множество $V_n(p) \setminus \{\mathbf{0}, \boxminus \mathbf{a}\}$, то параметр t пробегает все значения из множества $\{0, 1, \dots, p^n - 1\} \setminus \{0, p^n - t_0\}$. Если $p \geq 3$, имеем

$$\begin{aligned} N(\mathbf{a}) &= \{\gamma^{t_0}, \gamma^{p^n - t_0}\} \cup \{\gamma^{t+t_0} - \gamma^t : t = 1, 2, \dots, p^n - t_0 - 1\} \cup \\ &\cup \{\gamma^{t+t_0} - \gamma^t : t = p^n - t_0 + 1, p^n - t_0 + 2, \dots, p^n - 1\}, \end{aligned}$$

причём все три мультимножества в этом объединении являются множествами. Отсюда получим, что $\rho_{\boxplus, \boxplus}(s) \leq 3$, и п. 1 доказан.

Докажем п. 2. Если $p = 2$ и $t_0 = 2^{n-1}$, то множество $\{\gamma^{t_0}, \gamma^{2^n - t_0}\}$ является мультимножеством. Следовательно, $\rho_{\boxplus, \boxplus}(s) \leq 4$, причём $\rho_{\boxplus, \boxplus}(s) = 4$ тогда и только тогда, когда найдётся такое число $t \in \{1, 2, \dots, 2^{n-1} - 1\}$, что выполнено равенство

$$\gamma^{2^{n-1}} = \gamma^{t+2^{n-1}} + \gamma^t.$$

Умножив левую и правую части на ненулевой элемент γ^{-t} , получим

$$\gamma^{2^{n-1}} + \gamma^{2^{n-1}-t} + 1 = 0.$$

Это означает, что минимальный многочлен $F(x)$ элемента γ делит некоторый многочлен вида (9). ■

4. Линейная характеристика экспоненциальных преобразований

Для любого $b \in P_0^*$ через χ_b будем обозначать аддитивный характер поля P_0 [4]:

$$\chi_b(x) = e^{2\pi ibx/p}, \quad x \in P_0.$$

В дальнейшем будем использовать обозначение $\chi_e = \chi$. Пусть $f, g : P_0^n \rightarrow P_0$ — некоторые функции. Определим коэффициент кросс-корреляции между функциями f и g [11] равенством

$$C_b(f, g) = \sum_{\mathbf{x} \in P_0^n} \chi_b(f(\mathbf{x}) - g(\mathbf{x})).$$

Введём обозначение

$$C(f, g) = \max_{b \in P_0^*} |C_b(f, g)|.$$

Обозначим через $\langle \mathbf{a}, \mathbf{x} \rangle$ скалярное произведение векторов $\mathbf{a}, \mathbf{x} \in P_0^n$. Пусть g пробегает всё множество аффинных функций от n переменных над полем P_0 , т. е.

$$g(\mathbf{x}) = g(x_0, \dots, x_{n-1}) = \langle \mathbf{a}, \mathbf{x} \rangle + c = a_0x_0 + a_1x_1 + \dots + a_{n-1}x_{n-1} + c,$$

где $a_0, \dots, a_{n-1}, c \in P_0$. Линейная характеристика функции f определяется по правилу [12, 13]

$$C(f) = \max_g C(f, g) = \max_g \max_{b \in P_0^*} |C_b(f, g)|,$$

где максимум берётся по всем аффинным функциям g от n переменных.

Пусть s — экспоненциальное преобразование, определённое равенством (3), $s_0, \dots, s_{n-1}$ — его координатные функции. Тогда линейная характеристика преобразования s определяется равенством

$$C(s) = \max_{(a_0, \dots, a_{n-1}) \in V_n(p) \setminus \{0\}} C(a_0s_0 + \dots + a_{n-1}s_{n-1}).$$

Таким образом,

$$C(s) = \max_{f \in B_n(F)} C(f) = \max_{f \in B_n(F)} \max_g \max_{b \in P_0^*} |C_b(f, g)|.$$

Приведём результат из работы [3], который был получен в асимптотическом виде. В доказательстве будем использовать более удобные обозначения и вычислим значения соответствующих констант.

Теорема 4. Пусть $T(F) \geq p^{n/2}n$. Тогда для любого n в случае $p \geq 3$ и для $n \geq 5$, если $p = 2$, для каждой функции $f \in B_n(F)$ справедлива оценка

$$|C(f)| \leq \frac{p^{n/4+1}}{n^{1/2}} + \left(p^{7n/4}n^{1/2} + \frac{p^{5n/4+1}}{n^{1/2}} \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) \right)^{1/2}.$$

Доказательство. Выберем число $r \in \{0, 1, \dots, n-1\}$, удовлетворяющее неравенствам

$$p^r \leq T(F)^{1/2}p^{n/4}n^{1/2} < p^{r+1}. \quad (10)$$

Такое число найдётся при выполнении неравенства

$$p^{3n/4}n^{1/2} < p^n,$$

которое имеет место всегда в случае $p \geq 3$ и при $n \geq 5$, если $p = 2$. Пусть $g(\mathbf{x}) = a_0x_0 + \dots + a_{n-1}x_{n-1} + c$, где $a_0, \dots, a_{n-1}, c \in P_0$. Рассмотрим для функции $f = f_u \in B_n(F)$, соответствующей ЛРП u , и функции g коэффициент кросс-корреляции

$$C_b(f, g) = \sum_{\mathbf{x} \in P_0^n} \chi_b(f(\mathbf{x}) - g(\mathbf{x})) = 1 + C,$$

где

$$C = \sum_{\mathbf{x} \in P_0^n \setminus \{\mathbf{0}\}} \chi_b(f(\mathbf{x}) - g(\mathbf{x})) = \sum_{\mathbf{x} \in P_0^n \setminus \{\mathbf{0}\}} \chi_b(u(v(\mathbf{x}) - 1) - a_0x_0 - \dots - a_{n-1}x_{n-1} - c),$$

$v(\mathbf{x}) = x_0 + px_1 + \dots + p^{n-1}x_{n-1}$. Тогда

$$C = \sum_{(x_0, \dots, x_{r-1}) \in V_r(p)} \chi_b(-a_0x_0 + \dots + a_{r-1}x_{r-1} - c) \times \\ \times \sum_{(x_r, \dots, x_{n-1}) \in V_{n-r}(p), \mathbf{x} \neq \mathbf{0}} \chi_b(u(v(\mathbf{x}) - 1) - a_r x_r - \dots - a_{n-1}x_{n-1})$$

и справедливы равенства

$$C = C_1 + C_2, \quad (11)$$

где

$$C_1 = \sum_{(x_r, \dots, x_{n-1}) \in V_{n-r}(p) \setminus \{\mathbf{0}\}} \chi_b(u(v(0, \dots, 0, x_r, \dots, x_{n-1}) - 1) - a_r x_r - \dots - a_{n-1}x_{n-1} - c), \\ C_2 = \sum_{(x_0, \dots, x_{r-1}) \in V_r(p) \setminus \{\mathbf{0}\}} \chi_b(-a_0x_0 - \dots - a_{r-1}x_{r-1} - c) \times \\ \times \sum_{(x_r, \dots, x_{n-1}) \in V_{n-r}(p)} \chi_b(u(v(\mathbf{x}) - 1) - a_r x_r - \dots - a_{n-1}x_{n-1}), \\ |C| \leq |C_1| + |C_2|, \quad |C_1| \leq p^{n-r} - 1.$$

Оценим величину C_2 . Имеем

$$|C_2| \leq \sum_{(x_0, \dots, x_{r-1}) \in V_r(p) \setminus \{\mathbf{0}\}} \left| \sum_{(x_r, \dots, x_{n-1}) \in V_{n-r}(p)} \chi_b((u(v(\mathbf{x}) - 1) - a_r x_r - \dots - a_{n-1}x_{n-1})) \right|.$$

Используя неравенство Коши — Буняковского — Шварца, получим

$$|C_2|^2 \leq (p^r - 1) \sum_{(x_0, \dots, x_{r-1}) \in V_r(p) \setminus \{\mathbf{0}\}} \left| \sum_{(x_r, \dots, x_{n-1}) \in V_{n-r}(p)} \chi_b((u(v(\mathbf{x}) - 1) - a_r x_r - \dots - a_{n-1}x_{n-1})) \right|^2.$$

В силу линейности функции «след» можем записать

$$|C_2|^2 \leq p^r \sum_{\substack{(x_0, \dots, x_{r-1}) \in \\ \in V_r(p) \setminus \{\mathbf{0}\}}} \sum_{\substack{(x_r, \dots, x_{n-1}), \\ (x'_r, \dots, x'_{n-1}) \in V_{n-r}(p)}} \chi_b \left(u(v(\mathbf{x}) - 1) - \sum_{i=r}^{n-1} a_i x_i - u(v(\mathbf{x}') - 1) + \sum_{i=r}^{n-1} a_i x'_i \right),$$

где $\mathbf{x}' = (x_0, \dots, x_{r-1}, x'_r, \dots, x'_{n-1})$. Отсюда

$$|C_2|^2 \leq p^r \sum_{\substack{(x_r, \dots, x_{n-1}), \\ (x'_r, \dots, x'_{n-1}) \in V_{n-r}(p)}} \left| \sum_{(x_0, \dots, x_{r-1}) \in V_r(p) \setminus \{\mathbf{0}\}} \chi_b(u(v(\mathbf{x}) - 1) - u(v(\mathbf{x}') - 1)) \right|.$$

Если $(x_r, \dots, x_{n-1}) = (x'_r, \dots, x'_{n-1})$, то

$$\left| \sum_{(x_0, \dots, x_{r-1}) \in V_r(p) \setminus \{0\}} \chi_b(u(v(\mathbf{x}) - 1) - u(v(\mathbf{x}') - 1)) \right| = p^r - 1.$$

Если $(x_r, \dots, x_{n-1}) \neq (x'_r, \dots, x'_{n-1})$, то знаки

$$u(v(\mathbf{x}) - 1) - u(v(\mathbf{x}') - 1), \quad (x_0, \dots, x_{r-1}) \in V_r(p) \setminus \{0\}$$

представляют собой знаки последовательности $w = x^t u - x^s u$, где $t, s \in \mathbb{N} \cup \{0\}$ и $t \neq s$. Без ограничения общности считаем, что $t > s$ и $t \leq T(F) - 1$. Последовательность w является ЛРП с характеристическим многочленом $F(x)$. В силу реверсивности $F(x)$ имеет место: $w = (0)$ тогда и только тогда, когда $(x^t - x^s)u = (0)$, что равносильно $F(x)|(x^t - x^s)$ и эквивалентно $F(x)|(x^{t-s} - 1)$. Это соотношение не выполняется. Значит, при $(x_r, \dots, x_{n-1}) \neq (x'_r, \dots, x'_{n-1})$ с использованием неравенства из [14–18] имеем

$$\left| \sum_{(x_0, \dots, x_{r-1}) \in V_r(p) \setminus \{0\}} \chi_b(u(v(\mathbf{x}) - 1) - u(v(\mathbf{x}') - 1)) \right| \leq \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) p^{n/2}.$$

Следовательно,

$$\begin{aligned} |C_2|^2 &\leq p^r \left(\sum_{(x_r, \dots, x_{n-1}) = (x'_r, \dots, x'_{n-1})} (p^r - 1) + \sum_{(x_r, \dots, x_{n-1}) \neq (x'_r, \dots, x'_{n-1})} \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) p^{n/2} \right) = \\ &= p^r (p^r - 1) p^{n-r} + p^r (p^{2(n-r)} - p^{n-r}) \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) p^{n/2} < \\ &< p^{n+r} + p^{2n-r} \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) p^{n/2}. \end{aligned}$$

Согласно (10), $r \leq 3n/4 + (\log_p n)/2$ и $r + 1 > 3n/4 + (\log_p n)/2$. Тогда

$$p^{2n-r} < p^{2n-3n/4-\log_p n^{1/2}+1} = \frac{p^{5n/4+1}}{n^{1/2}}, \quad p^{n+r} < p^{n+3n/4+(\log_p n)/2} = p^{7n/4} n^{1/2}$$

и справедливо неравенство

$$|C_2| < \left(p^{7n/4} n^{1/2} + \frac{p^{5n/4+1}}{n^{1/2}} \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) \right)^{1/2}. \quad (12)$$

В итоге в силу (11) и (12) имеем

$$|C| < \frac{p^{n/4+1}}{n^{1/2}} + \left(p^{7n/4} n^{1/2} + \frac{p^{5n/4+1}}{n^{1/2}} \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) \right)^{1/2}.$$

Теорема 4 доказана. ■

Следствие 2. В условиях теоремы 4 для экспоненциального преобразования, определённого равенством (3), справедлива оценка

$$|C(s)| \leq \frac{p^{n/4+1}}{n^{1/2}} + \left(p^{7n/4} n^{1/2} + \frac{p^{5n/4+1}}{n^{1/2}} \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) \right)^{1/2}.$$

Правая часть неравенства из следствия 2 при фиксированном p имеет вид $O(p^{7n/8} n^{1/4})$, где $n \rightarrow \infty$.

Заключение

В работе рассмотрен класс экспоненциальных преобразований, обобщающий класс, изученный в [1]. Удалось найти верхнюю и нижнюю оценки степени нелинейности экспоненциальных преобразований, условия достижимости верхней оценки, а также оценки разностной и линейной характеристик экспоненциальных преобразований.

ЛИТЕРАТУРА

1. Агиевич С. В., Афоненко А. А. О свойствах экспоненциальных подстановок // Вести НАН Беларуси. 2005. № 1. С. 106–112.
2. Агиевич С. В., Галинский В. А., Микулич Н. Д., Харин Ю. С. Об одном алгоритме блочного шифрования // Управление защитой информации. 2002. Т. 6. № 4. С. 404–412.
3. Shparlinski I. E. and Winterhof A. On nonlinearity of linear recurrence sequences // Appl. Math. Let. 2005. V. 19. No. 4. P. 340–344.
4. Лидл Р., Ниддерайтер Г. Конечные поля. М.: Мир, 1988. 808 с.
5. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A. Linear recurring sequences over rings and modules // J. Math. Sci. 1995. V. 76. No. 6. P. 2793–2915.
6. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. СПб.; М.; Краснодар: Лань, 2015. 608 с.
7. Лаксов Д. Линейные рекуррентные последовательности над конечными полями // Математика. Сборник переводов. 1967. Т. 11. № 6. С. 145–158.
8. Камловский О. В. Оценки числа появлений векторов на циклах линейных рекуррентных последовательностей над конечным полем // Дискретная математика. 2008. Т. 20. № 6. С. 102–112.
9. Черемушкин А. В. Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная математика. 2010. № 2(8). С. 22–33.
10. Кузьмин А. С., Нечаев А. А., Шишкин В. А. Бент- и гипербент-функции над конечным полем // Труды по дискретной математике. 2007. Т. 10. С. 97–122.
11. Golomb S. W. and Gong G. Signal for Good Correlation. For Wireless Communication, Cryptography, and Radar. Cambridge: Cambridge Univ. Press, 2005. 438 p.
12. Бугров Д. А. Кусочно-аффинные подстановки конечных полей // Прикладная дискретная математика. 2015. № 4(30). С. 5–23.
13. Камловский О. В., Панков К. Н. Классы сбалансированных функций над конечными полями, обладающих малым значением линейной характеристики // Проблемы передачи информации. 2022. Т. 58. Вып. 4. С. 103–117.
14. Камловский О. В. Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа // Математический сборник. 2009. Т. 200. № 4. С. 31–52.
15. Камловский О. В. Количество появлений элементов в выходных последовательностях фильтрующих генераторов // Прикладная дискретная математика. 2013. № 3(21). С. 11–25.
16. Коробов Н. М. Распределение невычетов и первообразных корней в рекуррентных рядах // Доклады АН СССР. 1953. Т. 88. № 4. С. 603–606.
17. Niederreiter H. Distribution properties of feedback shift register sequences // Problems Control Inform. Theory. 1986. V. 15. No. 1. P. 19–34.
18. Нечаев В. И. Распределение знаков в последовательности прямоугольных матриц над конечным полем // Труды матем. ин-та им. В. А. Стеклова. 1997. Т. 218. С. 335–442.

REFERENCES

1. *Agievich S. V. and Afonenko A. A.* O svoystvakh eksponentsial'nykh podstanovok [On properties of exponential substituons]. Vesti NAN Belarusi, 2005, no.1, pp.106–112. (in Russian)
2. *Agievich S. V., Galinskiy V. A., Mikulich N. D., and Kharin Yu. S.* Ob odnom algoritme blochnogo shifrovaniya [About one block cipher algorithm]. Upravlenie Zashchitoy Informatsii, 2002, vol.6, no.4, pp.404–412. (in Russian)
3. *Shparlinski I. E. and Winterhof A.* On nonlinearity of linear recurrence sequences. Appl. Math. Let., 2005, vol.19, no.4, pp.340–344.
4. *Lidl R. and Niederreiter H.* Finite Fields. Addison-Wesley Publ., 1983.
5. *Kurakin V. L., Kuz'min A. S., Mikhalev A. V., and Nechaev A. A.* Linear recurring sequences over rings and modules. J. Math. Sci., 1995, vol.76, no.6, pp.2793–2915.
6. *Glukhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra: Uchebnik [Algebra: Textbook]. Saint Petersburg; Moscow; Krasnodar, Lan Publ., 2015. 608 p. (in Russian)
7. *Laksov D.* Lineynye rekurrentnye posledovatel'nosti nad konechnymi polyami [Linear recurrences over finite fields]. Matematika. Sbornik Perevodov, 1967, vol.11, no.6, pp.145–158. (in Russian)
8. *Kamlovskiy O. V.* Otsenki chisla poyavleniy vektorov na tsiklakh lineynykh rekurrentnykh posledovatel'nostey nad konechnym polem [Estimates of the number of occurrences of vectors on cycles of linear recurring sequences over a finite field]. Diskretnaya Matematika, 2008, vol.20, no.6, pp.102–112. (in Russian)
9. *Cheremushkin A. V.* Additivnyy podkhod k opredeleniyu stepeni nelineynosti diskretnoy funktsii [An additive approach to nonlinear degree of discrete function]. Prikladnaya Diskretnaya Matematika, 2010, no.2(8), pp.22–33. (in Russian)
10. *Kuz'min A. S., Nechaev A. A., and Shishkin V. A.* Bent- i giperbent-funktsii nad konechnym polem [Bent and hyper-bent functions over the finite field]. Trudy po Diskretnoy Matematike, 2007, vol.10, pp.97–122. (in Russian)
11. *Golomb S. W. and Gong G.* Signal for Good Correlation. For Wireless Communication, Cryptography, and Radar. Cambridge, Cambridge Univ. Press, 2005. 438 p.
12. *Bugrov D. A.* Kusochno-affinnye podstanovki konechnykh poley [Piecewise-affine permutations of finite fields]. Prikladnaya Diskretnaya Matematika, 2015, no.4(30), pp.5–23. (in Russian)
13. *Kamlovskiy O. V. and Pankov K. N.* Klassy sbalansirovannykh funktsiy nad konechnymi polyami, obladayushchikh malym znacheniem lineynoy kharakteristiki [Some classes of balanced functions over finite fields with a small value of the linear characteristic]. Problemy Peredachi Informatsii, 2022, vol.58, iss.4, pp.103–117. (in Russian)
14. *Kamlovskiy O. V.* Chastotnye kharakteristiki lineynykh rekurrentnykh posledovatel'nostey nad kol'tsami Galua [Frequency characteristics of linear recurrence sequences over Galois rings]. Matematicheskiy Sbornik, 2009, vol.200, no.4, pp.31–52. (in Russian)
15. *Kamlovskiy O. V.* Kolichestvo poyavleniy elementov v vykhodnykh posledovatel'nostyakh fil'truyushchikh generatorov [Distribution properties of sequences produced by filtering generators]. Prikladnaya Diskretnaya Matematika, 2013, no.3(21), pp.11–25. (in Russian)
16. *Korobov N. M.* Raspredelenie nevychetov i pervoobraznykh korney v rekurrentnykh ryadakh [Distribution of non-residues and primitive roots in recurrent series]. Doklady USSR Academy of Sciences, 1953, vol.88, no.4, pp.603–606. (in Russian)

-
17. *Niederreiter H.* Distribution properties of feedback shift register sequences. Problems Control Inform. Theory, 1986, vol. 15, no. 1, pp. 19–34.
 18. *Nechaev V. I.* Raspredelenie znakov v posledovatel'nosti pryamougol'nykh matrits nad konechnym polem [Distribution of signs in a sequence of rectangular matrices over a finite field]. Proc. Steklov Mathematical Institut, 1997, vol. 218, pp. 335–342. (in Russian)