

УДК 512.624

О ПОКАЗАТЕЛЕ НЕЛИНЕЙНОСТИ КУСОЧНО-ЛИНЕЙНЫХ ПОДСТАНОВОК АДДИТИВНОЙ ГРУППЫ ПОЛЯ $\mathbb{F}_{2^n}$

А. Е. Тришин

ООО «Центр сертификационных исследований», г. Москва, Россия

Получена нижняя оценка показателя нелинейности подстановок поля $\mathbb{F}_{2^n}$, ограничения которых на смежные классы группы $\mathbb{F}_{2^n}^*$ по её подгруппе H , $|H| = l$, $l \cdot r = 2^n - 1$, являются отображениями вида $x \mapsto A_j x$, $A_j \in \mathbb{F}_{2^n}^*$, $j = 0, \dots, r - 1$. В случаях $r = 3, 5$ найден спектр значений показателя нелинейности подстановок данного вида.

Ключевые слова: кусочно-линейная функция, подстановка конечного поля, показатель нелинейности.

DOI 10.17223/20710410/30/3

THE NONLINEARITY INDEX FOR A PIECEWISE-LINEAR SUBSTITUTION OF THE ADDITIVE GROUP OF THE FIELD $\mathbb{F}_{2^n}$

A. E. Trishin

*Certification Research Center, Moscow, Russia***E-mail:** Trishin17@yandex.ru

In this paper, we give a lower bound on the nonlinearity of permutations on a field $\mathbb{F}_{2^n}$ with restrictions to cosets of H in $\mathbb{F}_{2^n}^*$, $H < \mathbb{F}_{2^n}^*$, $|H| = l$, $l \cdot r = 2^n - 1$, being the maps $x \mapsto A_j x$, $A_j \in \mathbb{F}_{2^n}^*$, $j = 0, \dots, r - 1$. Nonlinearity spectra of this permutations are found in the cases $r = 3, 5$.

Keywords: piecewise-linear function, permutation of a finite field, nonlinearity.

Введение

Для натурального числа n введём обозначения: $V_n = \mathbb{F}_2^n$; (x, y) — стандартное скалярное произведение векторов $x, y \in V_n$.

Напомним некоторые определения [1].

Преобразованием Уолша — Адамара булевой функции $f : V_n \rightarrow \mathbb{F}_2$ называется целочисленная функция $W_f : V_n \rightarrow \mathbb{R}$, определяемая равенством

$$W_f(a) = \sum_{x \in V_n} (-1)^{f(x) + (a, x)} \text{ для всех } a \in V_n.$$

Здесь суммирование производится в действительной области, при этом считается, что $(-1)^0 = 1$, $(-1)^1 = -1$. Для каждого $a \in V_n$ значение $W_f(a)$ называется коэффициентом Уолша — Адамара функции f . Иногда используется термин «коэффициент Уолша — Адамара второго рода».

Нелинейностью N_f булевой функции $f : V_n \rightarrow \mathbb{F}_2$ называется расстояние по Хэммингу между функцией f и множеством всех аффинных функций $\mathcal{A}_n = \{f :$

$V_n \rightarrow \text{GF}(2) : \deg f \leq 1$. Здесь через $\deg f$ обозначена алгебраическая степень функции f , равная степени её многочлена Жегалкина. Известно выражение нелинейности N_f через коэффициенты Уолша — Адамара функции f :

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in V_n} |W_f(a)|.$$

Напомним, что любое отображение $F : V_n \rightarrow V_m$ задаётся набором координатных функций $(f_1, \dots, f_m)$, таких, что

$$F(x) = (f_1(x), \dots, f_m(x)) \text{ для всех } x \in V_n.$$

В этом случае пишут $F = (f_1, \dots, f_m)$.

Нелинейностью или показателем нелинейности [2] отображения F называется число N_F , определяемое равенством

$$N_F = \min_{\beta \in V_m \setminus \{0\}} N_{\beta F},$$

где $\beta F = \beta_1 f_1 + \dots + \beta_m f_m$ для произвольного вектора $\beta \in V_m$ и $F = (f_1, \dots, f_m)$. Выражение показателя нелинейности N_F через коэффициенты Уолша — Адамара координатных функций $f_1, \dots, f_m$ имеет вид

$$N_F = 2^{n-1} - \frac{1}{2} \max_{\beta \in V_m \setminus \{0\}} \max_{a \in V_n} |W_{\beta F}(a)|.$$

Рассмотрим поле $\mathbb{F}_q$ из $q = 2^n$ элементов с нулём 0 и единицей 1, и пусть $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$. Обозначим через ζ образующий элемент группы $\mathbb{F}_q^*$. Поле $\mathbb{F}_q$ является векторным пространством размерности n над полем $\mathbb{F}_2$, а каждый его элемент $x \in \mathbb{F}_q$ задаётся вектором $\mathbf{x} = (x_0, \dots, x_{n-1}) \in V_n$, таким, что $x = \sum_{i=0}^{n-1} x_i \zeta^i$.

Если $a \in V_n$ — фиксированный вектор и $\mathbf{x} \in V_n$, то $(a, \mathbf{x})$ — линейная функция на V_n . Значит, существует однозначно определённый элемент $\alpha \in \mathbb{F}_q$, такой, что $(a, \mathbf{x}) = \text{Tr}(\alpha x)$, где $\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_2$ — функция абсолютного следа элементов поля $\mathbb{F}_q$ [3, теорема 2.24]. Данное наблюдение и свойство линейности функции следа позволяют для показателя нелинейности отображения $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ получить формулу

$$N_F = 2^{n-1} - \Delta_F,$$

где

$$\Delta_F = \frac{1}{2} \max_{\alpha \in \mathbb{F}_q} \max_{\beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F|, \quad U_{\alpha, \beta}^F = \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(\alpha x + \beta F(x))}.$$

В данной работе исследуется параметр N_F подстановок из класса подстановок группы $(\mathbb{F}_q, +)$, взятого из [4], являющихся при выполнении одного условия ортоморфизмами. Дадим определение.

Пусть $(G, \cdot)$ — конечная группа с единицей e . Подстановка τ из симметрической группы $S(G)$ подстановок на множестве G называется *орторморфизмом* группы G [4, 5], если отображение $\tau' : G \rightarrow G$, определяемое условием

$$\tau'(g) = g^{-1} \tau(g) \text{ для всех } g \in G,$$

является подстановкой из $S(G)$.

Известно, что ортоморфизмы существуют для любой группы нечётного порядка [4, theorem 1.22]. Ортоморфизмами групп $(\mathbb{Z}_3, +)$ и $(\mathbb{Z}_5, +)$ являются, например, следующие подстановки:

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \end{pmatrix}.$$

Примером ортоморфизма группы $(G, \cdot)$, $|G| = m$, является отображение $\varphi : G \rightarrow G$, $\varphi(g) = g^k$ для всех $g \in G$, где $k \in \mathbb{N}$, $(k, m) = (k - 1, m) = 1$.

Для ортоморфизмов могут находиться применения, например при построении систем ортогональных латинских квадратов [6].

1. Определение кусочно-линейного преобразования конечного поля

Пусть $H < \mathbb{F}_q^*$ — подгруппа порядка l мультипликативной группы поля $\mathbb{F}_q$, $0 < l \leq q - 1$, $q - 1 = l \cdot r$, где $r \in \mathbb{N}$. Группа $\mathbb{F}_q^*$ раскладывается в объединение смежных классов по подгруппе H :

$$\mathbb{F}_q^* = \bigcup_{j=0}^{r-1} H_j, \quad H_j = \zeta^j H, \quad j = 0, \dots, r - 1.$$

Рассмотрим кусочно-линейное отображение $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$, $F(0) = 0$, ограничение которого на каждый смежный класс H_j имеет вид

$$x \mapsto A_j x \quad \text{для всех } x \in H_j,$$

где $A_j \in \mathbb{F}_q^*$, $j = 0, \dots, r - 1$ (отображения такого вида изучаются в [4, chapter 3]). Заметим, что существуют однозначно определённые числа $a_j \in \{0, \dots, q - 2\}$, $j = 0, \dots, r - 1$, при которых $A_j = \zeta^{a_j}$.

Отображение F переводит смежные классы по подгруппе H в смежные классы по подгруппе H . Значит, F биективно в том и только в том случае, когда F осуществляет перестановку указанных смежных классов. Это выполняется тогда и только тогда, когда набор чисел $a_0, a_1 + 1, \dots, a_{r-1} + r - 1$ образует полную систему вычетов по модулю r , то есть тогда и только тогда, когда отображение $\pi : \mathbb{Z}_r \rightarrow \mathbb{Z}_r$,

$$\pi(j) = (a_j + j) \bmod r, \quad j = 0, \dots, r - 1, \quad (1)$$

является биективным.

Подстановка F указанного вида является ортоморфизмом группы $(\mathbb{F}_{2^n}, +)$ в том и только в том случае, если $A_j \neq 1$ для всех $j = 0, \dots, r - 1$ и отображение $\pi' : \mathbb{Z}_r \rightarrow \mathbb{Z}_r$,

$$\pi'(j) = (\log_\zeta(A_j + 1) + j) \bmod r, \quad j = 0, \dots, r - 1,$$

является биективным, где функция $\log_\zeta : \mathbb{F}_q^* \rightarrow \{0, \dots, q - 2\}$ определяется условием: для любых $\gamma \in \mathbb{F}_q^*$, $c \in \{0, \dots, q - 2\}$ равенство $\log_\zeta(\gamma) = c$ имеет место в том и только в том случае, когда $\zeta^c = \gamma$.

2. Оценка показателя нелинейности кусочно-линейного преобразования поля характеристики 2

Теорема 1. Пусть $n, r, l \in \mathbb{N}$, $q = 2^n$, $q - 1 = rl$, $3 \leq r \leq \sqrt{q} + 1$, ζ — примитивный элемент поля $\mathbb{F}_q$, $H = \langle \zeta^r \rangle$ — подгруппа группы $\mathbb{F}_q^*$ порядка l , числа $a_j \in \{0, \dots, q - 2\}$,

$j = 0, \dots, r-1$, попарно различные и такие, что отображение (1) является биективным, и отображение $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ имеет вид

$$F(x) = \begin{cases} 0, & x = 0, \\ \zeta^{a_j} x, & x \in \zeta^j H, \quad j = 0, \dots, r-1. \end{cases}$$

Тогда выполнено неравенство

$$N_F \geq \frac{\sqrt{q}(r-1)(\sqrt{q}-r+1)}{2r}.$$

Доказательство. Для произвольных $\alpha \in \mathbb{F}_q$, $\beta \in \mathbb{F}_q^*$ имеем равенство

$$U_{\alpha,\beta}^F = \sum_{x \in \mathbb{F}_q} \chi(\alpha x + \beta F(x)),$$

где функция χ — канонический аддитивный характер поля $\mathbb{F}_q$, определяемый равенством

$$\chi(y) = (-1)^{\text{Tr}(y)} \text{ для всех } y \in \mathbb{F}_q.$$

Получим далее

$$U_{\alpha,\beta}^F = 1 + \sum_{j=0}^{r-1} \sum_{x \in H_j} \chi(\alpha x + \beta F(x)),$$

или

$$U_{\alpha,\beta}^F = 1 + \sum_{j=0}^{r-1} \sum_{x \in H} \chi(\gamma_j \zeta^j x), \quad (2)$$

где $\gamma_j = \alpha + \beta A_j = \alpha + \beta \zeta^{a_j}$, $j = 0, \dots, r-1$.

Заметим, что по условию теоремы числа $a_0, a_1, \dots, a_{r-1}$ попарно различны. Поэтому при фиксированных элементах $\alpha \in \mathbb{F}_q$, $\beta \in \mathbb{F}_q^*$ элементы $\gamma_0, \gamma_1, \dots, \gamma_{r-1}$ попарно различны, и возможен один из двух случаев:

- а) $\gamma_j \neq 0$ для всех $j \in \{0, \dots, r-1\}$;
- б) $\gamma_{j_0} = 0$ для некоторого $j_0 \in \{0, \dots, r-1\}$ и $\gamma_j \neq 0$ для всех $j \in \{0, \dots, r-1\} \setminus \{j_0\}$.

1. Пусть имеет место случай «а». Воспользуемся разложением аддитивного характера χ по мультипликативным характерам поля $\mathbb{F}_q$ [3]:

$$\chi(y) = \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi) \psi(y) \text{ для всех } y \in \mathbb{F}_q^*,$$

где сумма берётся по всем мультипликативным характерам поля $\mathbb{F}_q$; $\bar{\psi}$ — характер, сопряжённый для характера ψ ; $G(\psi, \chi)$ — сумма Гаусса, определяемая равенством

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c) \chi(c).$$

Из (2) получим

$$U_{\alpha,\beta}^F = 1 + \sum_{j=0}^{r-1} \sum_{x \in H} \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi) \psi(\gamma_j \zeta^j x) = 1 + \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi) \sum_{j=0}^{r-1} \psi(\gamma_j \zeta^j) \sum_{x \in H} \psi(x).$$

Учитывая равенство

$$\sum_{x \in H} \psi(x) = \begin{cases} |H|, & \psi \in \text{Ann}(H), \\ 0, & \psi \notin \text{Ann}(H), \end{cases}$$

получим

$$U_{\alpha,\beta}^F = 1 + \frac{l}{q-1} \sum_{\psi \in \text{Ann}(H)} G(\bar{\psi}, \chi) \sum_{j=0}^{r-1} \psi(\gamma_j \zeta^j).$$

Здесь $\text{Ann}(H)$ — аннулятор группы $H = \langle \zeta^r \rangle$, состоящий из всех мультипликативных характеров ψ поля $\mathbb{F}_q$, для которых $\psi(\zeta^r) = 1$.

Пусть ψ_0 — тривиальный мультипликативный характер, тогда, учитывая равенство $lr = q - 1$, получим

$$U_{\alpha,\beta}^F = 1 + \frac{l}{q-1} \sum_{\psi \in \text{Ann}(H) \setminus \{\psi_0\}} G(\bar{\psi}, \chi) \sum_{j=0}^{r-1} \psi(\gamma_j \zeta^j) + G(\psi_0, \chi).$$

Так как $G(\psi_0, \chi) = -1$, то

$$U_{\alpha,\beta}^F = \frac{l}{q-1} \sum_{\psi \in \text{Ann}(H) \setminus \{\psi_0\}} G(\bar{\psi}, \chi) \sum_{j=0}^{r-1} \psi(\gamma_j \zeta^j).$$

Учитывая неравенство $\left| \sum_{j=0}^{r-1} \psi(\gamma_j \zeta^j) \right| \leq r$ и равенство $|G(\psi, \chi)| = \sqrt{q}$, справедливое для всех $\psi \neq \psi_0$ и всех χ , получим

$$|U_{\alpha,\beta}^F| \leq \frac{l}{q-1} \sum_{\psi \in \text{Ann}(H) \setminus \{\psi_0\}} |G(\bar{\psi}, \chi)| \cdot r = (|\text{Ann}(H)| - 1) \sqrt{q}.$$

Так как $|\text{Ann}(H)| = r$ [3, теорема 5.6], получим неравенство

$$|U_{\alpha,\beta}^F| \leq (r-1) \sqrt{q}. \quad (3)$$

2. Пусть теперь имеет место случай «б», т. е. $\gamma_{j_0} = 0$ для некоторого индекса $j_0 \in \{0, \dots, r-1\}$ и $\gamma_j \neq 0$ для всех $j \in \{0, \dots, r-1\} \setminus \{j_0\}$. Учитывая равенство $\chi(0) = 1$, из (2) получим

$$U_{\alpha,\beta}^F = 1 + |H| + \sum_{j \in \{0, \dots, r-1\} \setminus \{j_0\}} \sum_{x \in H} \chi(\gamma_j \zeta^j x).$$

Воспользовавшись разложением аддитивного характера χ по мультипликативным характерам поля $\mathbb{F}_q$ и осуществив преобразования, аналогичные сделанным в п. 1, найдём

$$\begin{aligned} U_{\alpha,\beta}^F &= 1 + |H| + \sum_{j \in \{0, \dots, r-1\} \setminus \{j_0\}} \sum_{x \in H} \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi) \psi(\gamma_j \zeta^j x) = \\ &= 1 + |H| + \frac{l}{q-1} \sum_{\psi \in \text{Ann}(H)} G(\bar{\psi}, \chi) \sum_{j \in \{0, \dots, r-1\} \setminus \{j_0\}} \psi(\gamma_j \zeta^j) = \\ &= 1 + |H| + \frac{l(r-1)}{q-1} G(\psi_0, \chi) + \frac{l}{q-1} \sum_{\psi \in \text{Ann}(H) \setminus \{\psi_0\}} G(\bar{\psi}, \chi) \sum_{j \in \{0, \dots, r-1\} \setminus \{j_0\}} \psi(\gamma_j \zeta^j). \end{aligned}$$

Так как $G(\psi_0, \chi) = -1$, $|H| = l$ и $lr = q - 1$, то

$$U_{\alpha,\beta}^F = \frac{q}{r} + \frac{1}{r} \sum_{\psi \in \text{Ann}(H) \setminus \{\psi_0\}} G(\bar{\psi}, \chi) \sum_{j \in \{0, \dots, r-1\} \setminus \{j_0\}} \psi(\gamma_j \zeta^j). \quad (4)$$

Учитывая неравенство $\left| \sum_{j \in \{0, \dots, r-1\} \setminus \{j_0\}} \psi(\gamma_j \zeta^j) \right| \leq r-1$ и равенство $|G(\psi, \chi)| = \sqrt{q}$, справедливое для всех $\psi \neq \psi_0$ и всех χ , получим неравенство

$$\left| U_{\alpha, \beta}^F - \frac{q}{r} \right| \leq \frac{(r-1)}{r} (|\text{Ann}(H)| - 1) \sqrt{q},$$

которое равносильно

$$\left| U_{\alpha, \beta}^F - \frac{q}{r} \right| \leq \frac{(r-1)^2}{r} \sqrt{q}. \quad (5)$$

Объединяя оба случая, из (3) и (5) получим

$$\max_{\alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| \leq \max \left\{ (r-1)\sqrt{q}, \quad \frac{q}{r} + \frac{(r-1)^2}{r} \sqrt{q} \right\}.$$

Заметим, что неравенство $(r-1)\sqrt{q} \leq \frac{q}{r} + \frac{(r-1)^2}{r} \sqrt{q}$ выполняется тогда и только тогда, когда $r \leq \sqrt{q} + 1$. Последнее выполняется по условию, значит,

$$\max_{\alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| \leq \frac{q}{r} + \frac{(r-1)^2}{r} \sqrt{q}.$$

Таким образом, имеем неравенство $N_F \geq \frac{\sqrt{q}(r-1)(\sqrt{q}-r-1)}{2r}$. ■

Замечание 1. Если в условии теоремы 1 неравенство $r < \sqrt{q} + 1$ заменить на $r \geq \sqrt{q} + 1$, то получится оценка $N_F \geq 0$, которая является тривиальной.

3. Спектр показателя нелинейности кусочно-линейного преобразования поля характеристики 2 в частных случаях

В некоторых случаях для отображения F можно находить точные значения показателя нелинейности.

Теорема 2. Пусть $n \in \mathbb{N}$ — чётное число, $q = 2^n$, ζ — примитивный элемент поля $\mathbb{F}_q$, $H = \langle \zeta^3 \rangle$ — подгруппа группы $\mathbb{F}_q^*$ порядка $(q-1)/3$, числа $a_0, a_1, a_2 \in \{0, \dots, q-2\}$ попарно различные и такие, что отображение

$$\pi : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3, \quad \pi(j) = (a_j + j) \bmod 3, \quad j = 0, 1, 2,$$

является подстановкой группы $\mathbb{Z}_3$, и отображение $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ имеет вид

$$F(x) = \begin{cases} 0, & x = 0, \\ \zeta^{a_j} x, & x \in \zeta^j H, \quad j = 0, 1, 2. \end{cases}$$

Тогда если $n \equiv 0 \pmod{4}$, то

$$N_F = \sqrt{q}(\sqrt{q}-1)/3,$$

а если $n \equiv 2 \pmod{4}$, то

$$N_F \in \{\sqrt{q}(2\sqrt{q}-1)/6, \sqrt{q}(\sqrt{q}-2)/3\}.$$

При этом в случае $n \equiv 2 \pmod{4}$ равенство $N_F = \sqrt{q}(2\sqrt{q} - 1)/6$ имеет место тогда и только тогда, когда

$$c_{(j+1) \bmod 3} \not\equiv c_j + 1 \pmod{3}, \quad j = 0, 1, 2,$$

где

$$c_j = (\log_{\zeta}(\zeta^{a_{(j+1) \bmod 3} - a_j} + 1) + a_j) \bmod 3, \quad j = 0, 1, 2.$$

Доказательство. Так как при $r = 3$ и $n \geq 2$ справедливо равенство

$$\max \left\{ (r-1)\sqrt{q}, \frac{q + (r-1)^2\sqrt{q}}{r} \right\} = \frac{q + (r-1)^2\sqrt{q}}{r},$$

то (как следует из доказательства теоремы 1) для нахождения N_F достаточно рассмотреть случай «б»: элементы $\alpha \in \mathbb{F}_q$, $\beta \in \mathbb{F}_q^*$ — произвольные такие, что $\gamma_{j_0} = 0$ для некоторого индекса $j_0 \in \{0, 1, 2\}$ и $\gamma_j \neq 0$ для всех $j \in \{0, 1, 2\} \setminus \{j_0\}$.

Обозначим $\{0, 1, 2\} \setminus \{j_0\} = \{j_1, j_2\}$. Так как $\text{Ann}(H) = \{\psi_0, \psi, \psi^2\}$, где ψ_0 — тривиальный мультипликативный характер; ψ — мультипликативный характер порядка 3 поля $\mathbb{F}_q$ и $G(\psi, \chi) = G(\psi^2, \chi)$, то из (4) получим

$$U_{\alpha, \beta}^F = \frac{q}{3} + \frac{1}{3}G(\psi, \chi) (\sigma(\gamma_{j_1}\zeta^{j_1}) + \sigma(\gamma_{j_2}\zeta^{j_2})),$$

где $\sigma : \mathbb{F}_q^* \rightarrow \mathbb{C}^*$, $\sigma(\zeta^u) = \psi(\zeta^u) + \psi^2(\zeta^u)$ для всех $u \in \{0, \dots, q-2\}$.

Известно [7, 8], что если ψ — мультипликативный характер порядка 3 поля $\mathbb{F}_{2^n}$, χ — канонический аддитивный характер поля $\mathbb{F}_{2^n}$, то

$$G(\psi, \chi) = (-1)^{(n-2)/2} \cdot 2^{n/2}.$$

Поэтому

$$\begin{aligned} U_{\alpha, \beta}^F &= \frac{q}{3} + \frac{1}{3}(-1)^{(n-2)/2}\sqrt{q} (\sigma(\gamma_{j_1}\zeta^{j_1}) + \sigma(\gamma_{j_2}\zeta^{j_2})) = \\ &= \frac{q}{3} + \frac{1}{3}(-1)^{(n-2)/2}\sqrt{q} (\sigma((\alpha + \beta\zeta^{a_{j_1}})\zeta^{j_1}) + \sigma((\alpha + \beta\zeta^{a_{j_2}})\zeta^{j_2})). \end{aligned}$$

Так как в рассматриваемом случае $\alpha + \beta\zeta^{a_{j_0}} = 0$, то

$$U_{\alpha, \beta}^F = \frac{q}{3} + \frac{1}{3}(-1)^{(n-2)/2}\sqrt{q} (\sigma(\alpha\zeta^{u_1}) + \sigma(\alpha\zeta^{u_2})),$$

где $\zeta^{u_1} = (\zeta^{a_{j_1} - a_{j_0}} + 1)\zeta^{j_1}$; $\zeta^{u_2} = (\zeta^{a_{j_2} - a_{j_0}} + 1)\zeta^{j_2}$; $u_1, u_2 \in \{0, \dots, q-2\}$.

Заметим, что если $\beta \neq 0$ и выполняется равенство $\alpha + \beta\zeta^{a_{j_0}} = 0$, то $\alpha \neq 0$. Заметим далее, что так как $\sigma(\zeta^u) = e^{2\pi i u/3} + e^{4\pi i u/3}$ для всех $u \in \{0, \dots, q-2\}$, то

$$\sigma(\zeta^u) = \begin{cases} 2, & u \equiv 0 \pmod{3}, \\ -1 & \text{иначе,} \end{cases} \quad \text{т. е.} \quad \sigma(\zeta^u) = \begin{cases} 2, & \zeta^u \in H, \\ -1 & \text{иначе.} \end{cases}$$

Поэтому если $u_1 \equiv u_2 \pmod{3}$, то найдётся элемент $\alpha \in \mathbb{F}_q^*$, для которого $\alpha\zeta^{u_1} \in H$, $\alpha\zeta^{u_2} \in H$, и найдётся элемент $\alpha' \in \mathbb{F}_q^*$, для которого $\alpha'\zeta^{u_1} \notin H$, $\alpha'\zeta^{u_2} \notin H$. Значит, если $u_1 \equiv u_2 \pmod{3}$, то

$$\max_{\alpha \in \mathbb{F}_q^*} (\sigma(\alpha\zeta^{u_1}) + \sigma(\alpha\zeta^{u_2})) = 4, \quad \min_{\alpha \in \mathbb{F}_q^*} (\sigma(\alpha\zeta^{u_1}) + \sigma(\alpha\zeta^{u_2})) = -2.$$

Если же $u_1 \not\equiv u_2 \pmod{3}$, то найдутся элементы $\alpha, \alpha' \in \mathbb{F}_q^*$, для которых $\alpha\zeta^{u_1} \in H$, $\alpha\zeta^{u_2} \notin H$ и $\alpha'\zeta^{u_1} \notin H$, $\alpha'\zeta^{u_2} \in H$, но не найдётся элемента $\alpha'' \in \mathbb{F}_q^*$, для которого $\alpha''\zeta^{u_1} \in H$, $\alpha''\zeta^{u_2} \in H$. Значит, в этом случае

$$\max_{\alpha \in \mathbb{F}_q^*} (\sigma(\alpha\zeta^{u_1}) + \sigma(\alpha\zeta^{u_2})) = 1, \quad \min_{\alpha \in \mathbb{F}_q^*} (\sigma(\alpha\zeta^{u_1}) + \sigma(\alpha\zeta^{u_2})) = -2.$$

Таким образом, если $n \equiv 0 \pmod{4}$, то

$$\max_{\alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| = (q + 2\sqrt{q})/3,$$

а если $n \equiv 2 \pmod{4}$, то

$$\max_{\alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| \in \{(q + \sqrt{q})/3, (q + 4\sqrt{q})/3\}.$$

При этом в случае $n \equiv 2 \pmod{4}$ равенство $\max_{\alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| = (q + \sqrt{q})/3$ выполняется тогда и только тогда, когда для любого $j_0 \in \{0, 1, 2\}$ верно условие

$$u_1 \not\equiv u_2 \pmod{3}. \quad (6)$$

Так как $\zeta^{u_1} = (\zeta^{a_{j_1} - a_{j_0}} + 1)\zeta^{j_1}$, $\zeta^{u_2} = (\zeta^{a_{j_2} - a_{j_0}} + 1)\zeta^{j_2}$, $u_1, u_2 \in \{0, \dots, q-2\}$, то выполнение условия (6) для всех $j_0 \in \{0, 1, 2\}$ означает, что имеет место система

$$\begin{cases} \log_{\zeta}(\zeta^{a_1 - a_0} + 1) \not\equiv \log_{\zeta}(\zeta^{a_2 - a_0} + 1) + 1 \pmod{3}, \\ \log_{\zeta}(\zeta^{a_0 - a_1} + 1) \not\equiv \log_{\zeta}(\zeta^{a_2 - a_1} + 1) + 2 \pmod{3}, \\ \log_{\zeta}(\zeta^{a_0 - a_2} + 1) \not\equiv \log_{\zeta}(\zeta^{a_1 - a_2} + 1) + 1 \pmod{3}, \end{cases}$$

которая равносильна системе

$$c_{(j+1) \bmod 3} \not\equiv c_j + 1 \pmod{3}, \quad j = 0, 1, 2,$$

где $c_j = (\log_{\zeta}(\zeta^{a_{(j+1) \bmod 3} - a_j} + 1) + a_j) \bmod 3$, $j = 0, 1, 2$. ■

Следствие 1. В случае $n \equiv 2 \pmod{4}$ при $r = 3$ оценка из теоремы 1 является достижимой.

Доказательство. В условиях теоремы 2 в случае $n \equiv 2 \pmod{4}$ существует отображение F рассматриваемого вида, для которого имеет место равенство

$$\max_{\alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| = (q + 4\sqrt{q})/3.$$

Действительно, данное равенство выполнено, если, например,

$$\log_{\zeta}(\zeta^{a_2 - a_1} + 1) + a_1 \equiv \log_{\zeta}(\zeta^{a_1 - a_0} + 1) + a_0 + 1 \pmod{3}.$$

Ясно, что для любого значения в правой части последнего сравнения найдётся такое $a_2 \in \{0, \dots, q-2\}$, что сравнение будет справедливо. ■

Как и в случае мультипликативного характера порядка 3, сумма Гаусса для любого мультипликативного характера порядка 5 и канонического аддитивного характера поля $\mathbb{F}_q$ принимает одно и то же действительное значение.

Лемма 1. Пусть $n, m \in \mathbb{N}$, $n = 4m$, $q = 2^n$. Если ψ' — мультипликативный характер порядка 5 поля $\mathbb{F}_q$, χ' — канонический аддитивный характер этого поля, то

$$G(\psi', \chi') = (-1)^{m-1} \sqrt{q}.$$

Доказательство. Пусть ζ — примитивный элемент поля $\mathbb{F}_q$. Тогда $\eta = \zeta^{(q-1)/15}$ — примитивный элемент поля $\mathbb{F}_{16}$, и мультипликативный характер ψ поля $\mathbb{F}_{16}$, определяемый равенством

$$\psi(\eta) = \psi'(\zeta),$$

имеет порядок 5.

Пусть χ — канонический аддитивный характер поля $\mathbb{F}_{16}$. Для характера ψ поля $\mathbb{F}_{16} = \mathbb{F}_{4^2}$ выполняются условия теоремы Штикельбергера [3, теорема 5.16], и по этой теореме получим равенство $G(\psi, \chi) = 4$ (которое можно проверить и непосредственным вычислением). Так как χ' и ψ' — поднятия до поля $\mathbb{F}_q$ характеров χ и ψ поля $\mathbb{F}_{16}$ соответственно и $[\mathbb{F}_q : \mathbb{F}_{16}] = m$, то по теореме Дэвенпорта — Хассе [3, теорема 5.14] получим $G(\psi', \chi') = (-1)^{m-1} G(\psi, \chi)^m = (-1)^{m-1} \sqrt{q}$. ■

Теорема 3. Пусть $n, m \in \mathbb{N}$, $n = 4m$, $q = 2^n$, ζ — примитивный элемент поля $\mathbb{F}_q$, $H = \langle \zeta^5 \rangle$ — подгруппа группы $\mathbb{F}_q^*$ порядка $(q-1)/5$, числа $a_j \in \{0, \dots, q-2\}$, $j = 0, \dots, 4$, — попарно различные и такие, что отображение

$$\pi : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5, \quad \pi(j) = (a_j + j) \bmod 5, \quad j = 0, \dots, 4,$$

является биективным, и отображение $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ имеет вид

$$F(x) = \begin{cases} 0, & x = 0, \\ \zeta^{a_j} x, & x \in \zeta^j H, \quad j = 0, \dots, 4. \end{cases}$$

Тогда если $n \equiv 0 \pmod{8}$, то

$$N_F = 2\sqrt{q}(\sqrt{q} - 1)/5,$$

а если $n \equiv 4 \pmod{8}$, то

$$N_F \in \{\sqrt{q}(4\sqrt{q} - t)/10 : t = 1, 6, 11, 16\}.$$

Доказательство. Так как при $r = 5$ и $n \geq 4$ справедливо равенство

$$\max \left\{ (r-1)\sqrt{q}, \frac{q + (r-1)^2 \sqrt{q}}{r} \right\} = \frac{q + (r-1)^2 \sqrt{q}}{r},$$

то (как следует из доказательства теоремы 1) для нахождения N_F достаточно рассмотреть случай «б»: элементы $\alpha \in \mathbb{F}_q$, $\beta \in \mathbb{F}_q^*$ — произвольные такие, что $\gamma_{j_0} = 0$ для некоторого индекса $j_0 \in \{0, \dots, 4\}$ и $\gamma_j \neq 0$ для всех $j \in \{0, \dots, 4\} \setminus \{j_0\}$.

Обозначим $\{0, \dots, 4\} \setminus \{j_0\} = \{j_1, j_2, j_3, j_4\}$ и пусть $l = (q-1)/5$. Если ψ — произвольный мультипликативный характер поля $\mathbb{F}_q$ порядка 5, χ — канонический аддитивный характер поля $\mathbb{F}_q$, то по лемме 1 имеем $G(\psi, \chi) = (-1)^{m-1} \sqrt{q}$. Тогда из (4) получим

$$U_{\alpha, \beta}^F = \frac{q}{5} + \frac{1}{5} (-1)^{m-1} \sqrt{q} \sum_{k=1}^4 \sigma(\gamma_{j_k} \zeta^{j_k}),$$

где $\sigma : \mathbb{F}_q^* \rightarrow \mathbb{C}^*$, $\sigma(\zeta^u) = \sum_{s=1}^4 \psi^s(\zeta^u)$ для всех $u \in \{0, \dots, q-2\}$; $\gamma_{j_k} = \alpha + \beta\zeta^{a_{j_k}}$, $k = 1, \dots, 4$. Так как в рассматриваемом случае $\alpha + \beta\zeta^{a_{j_0}} = 0$, то

$$U_{\alpha, \beta}^F = \frac{q}{5} + \frac{1}{5}(-1)^{m-1}\sqrt{q} \sum_{k=1}^4 \sigma(\alpha\zeta^{u_k}),$$

где $\zeta^{u_k} = (\zeta^{a_{j_k} - a_{j_0}} + 1)\zeta^{j_k}$, $u_k \in \{0, \dots, q-2\}$, $k = 1, \dots, 4$. Заметим, что если $\beta \neq 0$ и выполняется равенство $\alpha + \beta\zeta^{a_{j_0}} = 0$, то $\alpha \neq 0$. Заметим далее, что так как

$$\sigma(\zeta^u) = \sum_{s=1}^4 e^{2\pi i s u / 5},$$

то

$$\sigma(\zeta^u) = \begin{cases} 4, & u \equiv 0 \pmod{5}, \\ -1 & \text{иначе,} \end{cases} \quad \text{т. е. } \sigma(\zeta^u) = \begin{cases} 4, & \zeta^u \in H, \\ -1 & \text{иначе.} \end{cases}$$

Какие бы ни были числа $u_k \in \{0, \dots, q-2\}$, $k = 1, \dots, 4$, найдётся элемент $\alpha \in \mathbb{F}_q^*$, для которого $\alpha\zeta^{u_k} \notin H$ для всех $k \in \{1, \dots, 4\}$. Следовательно,

$$\min_{\alpha \in \mathbb{F}_q^*} \left(\sum_{k=1}^4 \sigma(\alpha\zeta^{u_k}) \right) = -4,$$

и при $n \equiv 0 \pmod{8}$ получим $\max_{\alpha \in \mathbb{F}_q^*, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| = (q + 4\sqrt{q})/5$.

Пусть теперь $n \equiv 4 \pmod{8}$.

С л у ч а й 1. Если $u_1 \equiv u_2 \equiv u_3 \equiv u_4 \pmod{5}$, то найдётся элемент $\alpha \in \mathbb{F}_q^*$, для которого $\alpha\zeta^{u_k} \in H$ для всех $k \in \{1, \dots, 4\}$. Тогда $\max_{\alpha \in \mathbb{F}_q^*} \left(\sum_{k=1}^4 \sigma(\alpha\zeta^{u_k}) \right) = 16$, откуда получим

$$\max_{\alpha \in \mathbb{F}_q^*, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| = (q + 16\sqrt{q})/5.$$

С л у ч а й 2. Если $u_{k_1} \not\equiv u_{k_2} \equiv u_{k_3} \equiv u_{k_4} \pmod{5}$, где $\{k_1, k_2, k_3, k_4\} = \{1, \dots, 4\}$, то возможны три подслучая:

- 2.1. $\exists \alpha \in \mathbb{F}_q^* (\alpha\zeta^{u_{k_1}} \notin H, \alpha\zeta^{u_{k_2}}, \alpha\zeta^{u_{k_3}}, \alpha\zeta^{u_{k_4}} \in H)$;
- 2.2. $\exists \alpha' \in \mathbb{F}_q^* (\alpha'\zeta^{u_{k_1}} \in H, \alpha'\zeta^{u_{k_2}}, \alpha'\zeta^{u_{k_3}}, \alpha'\zeta^{u_{k_4}} \notin H)$;
- 2.3. $\exists \alpha'' \in \mathbb{F}_q^* (\alpha''\zeta^{u_{k_1}}, \alpha''\zeta^{u_{k_2}}, \alpha''\zeta^{u_{k_3}}, \alpha''\zeta^{u_{k_4}} \notin H)$.

Так как $\sum_{k=1}^4 \sigma(\alpha\zeta^{u_k}) = 11$, $\sum_{k=1}^4 \sigma(\alpha'\zeta^{u_k}) = 1$, $\sum_{k=1}^4 \sigma(\alpha''\zeta^{u_k}) = -4$, в случае 2 получим $\max_{\alpha \in \mathbb{F}_q^*} \left(\sum_{k=1}^4 \sigma(\alpha\zeta^{u_k}) \right) = 11$, следовательно, $\max_{\alpha \in \mathbb{F}_q^*, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| = (q + 11\sqrt{q})/5$.

Аналогично получим следующее.

С л у ч а й 3. Если $u_{k_1} \not\equiv u_{k_2} \equiv u_{k_3} \not\equiv u_{k_4} \pmod{5}$, $u_{k_1} \not\equiv u_{k_4} \pmod{5}$, где $\{k_1, k_2, k_3, k_4\} = \{1, \dots, 4\}$, то $\max_{\alpha \in \mathbb{F}_q^*} \left(\sum_{k=1}^4 \sigma(\alpha\zeta^{u_k}) \right) = 6$, следовательно,

$$\max_{\alpha \in \mathbb{F}_q^*, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| = (q + 6\sqrt{q})/5.$$

С л у ч а й 4. Если $u_{k_1} \not\equiv u_{k_2} \pmod{5}$ для всех $k_1, k_2 \in \{1, \dots, 4\}$, $k_1 \neq k_2$, то $\max_{\alpha \in \mathbb{F}_q^*} \left(\sum_{k=1}^4 \sigma(\alpha \zeta^{u_k}) \right) = 1$, следовательно, $\max_{\alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q^*} |U_{\alpha, \beta}^F| = (q + \sqrt{q})/5$.

Теорема доказана. ■

Автор признателен О. В. Камловскому за полезные рекомендации и обсуждения в ходе выполнения работы.

ЛИТЕРАТУРА

1. *Логачёв О. А., Сальников А. А., Смышляев С. В., Яценко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд., доп. М.: МЦНМО, 2012. 584 с.
2. *Nyberg K.* On the construction of highly nonlinear permutations // EUROCRYPT'92. LNCS. 1993. V. 658. P. 92–98.
3. *Лидл Р., Нидеррайтер Г.* Конечные поля: в 2-х т.: пер. с. англ. М.: Мир, 1988. 822 с.
4. *Evans A. B.* Orthomorphisms Graphs and Groups. Berlin: Springer Verlag, 1992.
5. *Paige L. J.* Complete mappings of finite groups // Pacific J. Math. 1955. V. 1. P. 111–116.
6. *Глухов М. М.* О методах построения систем ортогональных квазигрупп с использованием групп // Математические вопросы криптографии. 2011. Т. 2. № 4. С. 5–24.
7. *Ding C.* Cyclotomic linear codes of order 3 // IEEE Trans. Inf. Theory. 2007. V. 53. No. 6. P. 2274–2277.
8. *McEliece R. J.* Irreducible cyclic codes and Gauss sums // Combinatorics / eds. M. Hall and J. H. van Lint. Amsterdam: Math. Centre, 1975. P. 185–202.

REFERENCES

1. *Logachev O. A., Sal'nikov A. A., Smyshlyaev S. V., Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2012. 584 p. (in Russian)
2. *Nyberg K.* On the construction of highly nonlinear permutations. EUROCRYPT'92, LNCS, 1993, vol. 658, pp. 92–98.
3. *Lidl R., Niederreiter G.* Konechnye polya [Finite Fields]. Moscow, Mir Publ., 1988, vol. 1, 2. 822 p. (in Russian)
4. *Evans A. B.* Orthomorphisms Graphs and Groups. Berlin, Springer Verlag, 1992.
5. *Paige L. J.* Complete mappings of finite groups. Pacific J. Math., 1955, vol. 1, pp. 111–116.
6. *Gluhov M. M.* O metodakh postroeniya sistem ortogonal'nykh kvazigrupp s ispol'zovaniem grupp [On a method of construction of orthogonal quasigroup systems by means of groups]. Mat. Vopr. Kriptogr., 2011, vol. 2, iss. 4, pp. 5–24. (in Russian)
7. *Ding C.* Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory, 2007, vol. 53, no. 6, pp. 2274–2277.
8. *McEliece R. J.* Irreducible cyclic codes and Gauss sums. Combinatorics (eds. M. Hall and J. H. van Lint). Amsterdam, Math. Centre, 1975, pp. 185–202.