Math-Net.Ru

Общероссийский математический портал

А. Б. Шишков, О бент-функциях на группе $\mathbb{Z}_{p^n}$, *Матем. вопр. криптогр.*, 2015, том 6, выпуск 4, 127–138

DOI: <https://doi.org/10.4213/mvk171>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.27.143

26 апреля 2023 г., 16:50:49

УДК: 519.719

О бент-функциях на группе $\mathbb{Z}_{p^n}$

А. Б. Шишков

ООО «Центр сертификационных исследований», Москва

Получено 20.IV.2015

Показано, что бент-функции на группе $\mathbb{Z}_{p^n}$ (p — простое) существуют только в случаях $n = 2$ при $p = 2$ и $n = 1, 2$ при $p > 2$.

Ключевые слова: бент-функции на абелевых группах, суммы характеров, алгебраические числа

On bent-functions on the group $\mathbb{Z}_{p^n}$

A. B. Shishkov

LLC “Certification Research Center”, Moscow

Abstract. It is shown that a bent-function on the group $\mathbb{Z}_{p^n}$ (p prime) exists only if $n = 2$ for $p = 2$ or $n = 1, 2$ for $p > 2$.

Key words: bent-function on abelian groups, character sums, algebraic numbers

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 4, pp. 127–138 (Russian).

© 2015 А. Б. Шишков

Вначале для полноты изложения приведем краткую сводку результатов теории характеров конечных абелевых групп (см., например, [2]), являющейся эффективным инструментом изучения свойств дискретных отображений.

Как хорошо известно, любая конечная абелева группа раскладывается в прямую сумму циклических групп, порядки которых являются степенями простых чисел. Рассмотрим группу G :

$$G = \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \dots \oplus \mathbb{Z}_{p_s^{k_s}},$$

где p_i — простые (не обязательно различные), а k_i — натуральные числа. Любой элемент $g \in G$ имеет вид $g = (g_1, \dots, g_s)$, $g_i \in \{0, \dots, p_i^{k_i} - 1\}$. Характером группы G , соответствующим элементу g , назовем отображение $\chi_g : G \rightarrow \mathbb{C}^*$, определяемое следующим правилом:

$$\text{если } x = (x_1, \dots, x_s) \in G, \text{ то } \chi_g(x) = \prod_{j=1}^s \exp \left\{ \frac{2\pi i}{p_j^{k_j}} x_j g_j \right\}.$$

Характеры являются гомоморфизмами группы $(G, +)$ в группу $(\mathbb{C}^*, \cdot)$. При этом множество всех характеров совпадает со множеством таких гомоморфизмов. Одним из важных свойств характеров является *соотношение ортогональности*:

$$\frac{1}{|G|} \sum_{x \in G} \chi_a(x) \overline{\chi_b(x)} = \delta_{ab} \text{ для любых } a, b \in G.$$

Здесь верхняя черта — знак комплексного сопряжения, а δ_{ab} — символ Кронекера. Из этого соотношения, в частности, следует, что множество характеров $\{\chi_g\}_{g \in G}$ образует базис линейного пространства функций из G в $\mathbb{C}$ над полем $\mathbb{C}$.

Пусть теперь H также конечная абелева группа. Характер группы H , соответствующий элементу h , будем обозначать η_h .

Пусть $f : G \rightarrow H$ — произвольное отображение G в H . В дальнейшем термины «функция» и «отображение» используются как синонимы.

Композиция $\eta_h \circ f$ функции f и характера η_h является, очевидно, отображением группы G в $\mathbb{C}^*$ и, следовательно, однозначно раскладывается в линейную комбинацию характеров группы G :

$$\eta_h \circ f = \sum_{g \in G} C_g^{(h, f)} \chi_g.$$

Такое представление будем называть *разложением Фурье*, а коэффициенты $C_g^{(h,f)}$ — *коэффициентами Фурье функции f* , соответствующими элементам $h \in H, g \in G$.

Коэффициенты Фурье являются элементами поля комплексных чисел и обладают следующими свойствами [4]:

- $C_g^{(h,f)} = \frac{1}{|G|} \sum_{x \in G} \eta_h(f(x)) \overline{\chi_g(x)}$;
- $\sum_{g \in G} |C_g^{(h,f)}|^2 = 1$ для всех $h \in H$ (равенство Парсеваля);
- $\max_{g \in G} |C_g^{(h,f)}| \geq \frac{1}{\sqrt{|G|}}$.

С учетом изложенного, следуя работе [4]¹, можно дать определение бент-функции на абелевой группе.

Определение 1. Функцию $f : G \rightarrow H$ будем называть *бент-функцией*, если для любых $g \in G$ и $h \in H \setminus \{0\}$ выполняется равенство

$$|C_g^{(h,f)}| = \frac{1}{\sqrt{|G|}}.$$

Следующая теорема (см. [4]) описывает необходимое и достаточное условие того, что f является бент-функцией (свойство *абсолютной негомоморфности*).

Теорема 1. Функция $f : G \rightarrow H$ является бент-функцией тогда и только тогда, когда функция $\Delta_\omega f(x) = f(x + \omega) - f(x)$ является уравновешенной для любого $\omega \in G \setminus \{0\}$ (т. е. для всех $h \in H$ прообразы $[\Delta_\omega f]^{-1}(h)$ равномогутны).

Отметим, что эта теорема является обобщением результата работы [1], в которой рассматривались функции на аддитивных группах конечных полей.

Впервые определение бент-функции было дано для булевых функций [11], т. е. при $G = (\mathbb{Z}_2)^n$ и $H = \mathbb{Z}_2$. Известно, что булевы бент-функции существуют тогда и только тогда, когда n четно. При этом класс бент-функций совпадает с классом функций, максимально удаленных от класса аффинных функций в смысле метрики Хэмминга (свойство *минимальности* [4]).

¹Строго говоря, вид определения в работе [4] несколько иной, однако эквивалентность двух определений сразу следует из равенства Парсеваля.

Впоследствии бент-функции изучались довольно интенсивно, рассматривались различные их обобщения (к теме нашего исследования ближе всего результаты работ [9, 10]). Наиболее полный обзор известных результатов по бент-тематике приведен в [6]. Естественный криптографический интерес при изучении этих объектов вызывают указанные свойства абсолютной негомоморфности и минимальности. Вместе с тем описание свойств этого класса дискретных функций далеко от завершения, в частности, полностью не описаны даже булевы бент-функции.

В [5] подробно рассмотрен случай так называемых *p-примарных функций*, т. е. функций из группы G в группу H , когда $G = (\mathbb{Z}_p)^n$, $H = (\mathbb{Z}_p)^m$. В частности, получены необходимые и достаточные условия существования бент-функций:

Множество бент-функций из группы $(\mathbb{Z}_p)^n$ в группу $(\mathbb{Z}_p)^m$ непусто тогда и только тогда, когда выполняется одно из двух условий:

$$\begin{aligned} p = 2, \quad 2|n \text{ и } n \geq 2m, \\ p \geq 3 \text{ и } n \geq m. \end{aligned}$$

В настоящей работе рассматривается другой случай, когда группа G является циклической группой порядка p^n , $G = \mathbb{Z}_{p^n}$. Как будет показано, в этом случае необходимые условия существования бент-функций гораздо более жесткие, а именно, бент-функции существуют только при $n = 1, 2$.

Пусть f — бент-функция из группы $G = \mathbb{Z}_{p^n}$ в группу H . Из теоремы 1 следует, что порядок H равен p^m , $m \leq n$. Из результатов работ [4, 5] вытекает, что если $f : G \rightarrow H$ — бент-функция, то для любого гомоморфизма $\psi : H \rightarrow \mathbb{Z}_p$ композиция $\psi \circ f$ является бент-функцией из G в $\mathbb{Z}_p$. Поэтому вначале рассмотрим условия существования бент-функций в случае, когда $G = \mathbb{Z}_{p^n}$ и $H = \mathbb{Z}_p$.

Ниже будем использовать обозначение $N = p^n$. Характеры группы G имеют в нашем случае вид $\chi_k(x) = \xi^{kx}$, $k \in \{0, \dots, N-1\}$, где ξ — некоторый фиксированный примитивный корень степени N из единицы, например: $\xi = \exp\{\frac{2\pi i}{N}\}$. Характеры группы H имеют вид $\eta_m(y) = \zeta^{my}$, $m \in \{0, \dots, p-1\}$, где ζ — некоторый фиксированный примитивный корень степени p из единицы, который можно представить следующим образом: $\zeta = \xi^{p^{n-1}}$. Тогда коэффициенты Фурье вычисляются по формуле

$$C_k^{(m,f)} = \frac{1}{N} \sum_{x=0}^{N-1} \zeta^{mf(x)} \xi^{kx} = \frac{1}{N} \sum_{x=0}^{N-1} \xi^{mf(x)p^{n-1}+kx}. \quad (1)$$

Рассмотрим расширение поля $\mathbb{Q}(\xi)$ рациональных чисел корнем ξ . Минимальным многочленом этого элемента над полем $\mathbb{Q}$ является так называемый круговой многочлен

$$Q_N(x) = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \dots + x^{p^{n-1}} + 1,$$

множество корней которого совпадает со множеством всех примитивных корней степени N из единицы: $\{\xi^s \mid s \in \{1, \dots, N\}, (s, p) = 1\}$. Степень $Q_N(x)$ равна $\varphi(N)$, где φ — функция Эйлера. Любой элемент $\mathbb{Q}(\xi)$ может быть однозначно представлен в виде $c_0 + c_1\xi + \dots + c_{\varphi(N)-1}\xi^{\varphi(N)-1}$, $c_i \in \mathbb{Q}$. Рассмотрим подмножество $\mathbb{Z}[\xi]$ поля $\mathbb{Q}(\xi)$, состоящее из всевозможных таких линейных комбинаций, коэффициенты которых являются целыми числами. Несложно видеть, что $\mathbb{Z}[\xi]$ является подкольцом в $\mathbb{Q}(\xi)$.¹ Нам также понадобится рассматривать автоморфизмы поля $\mathbb{Q}(\xi)$ над $\mathbb{Q}$. Множество всех этих автоморфизмов состоит из отображений σ_s , $s \in \{1, \dots, N\}$, $(s, p) = 1$, однозначно определяемых своим действием на элемент ξ : $\sigma_s(\xi) = \xi^s$.

Лемма 2. Пусть f — бент-функция из группы $\mathbb{Z}_{p^n}$ в группу $\mathbb{Z}_p$. Тогда

$$\prod_{s \in \{1, \dots, N\}, (s, p) = 1} \left(C_s^{(s \bmod p, f)} \cdot C_0^{(s \bmod p, f)} \right) = \pm p^{-n\varphi(N)}.$$

Доказательство. Из определения бент-функции следует равенство

$$\left| \prod_{s \in \{1, \dots, N\}, (s, p) = 1} \left(C_s^{(s \bmod p, f)} \cdot C_0^{(s \bmod p, f)} \right) \right| = p^{-n\varphi(N)}.$$

Остается показать, что данное произведение коэффициентов Фурье является действительным числом. Рассмотрим коэффициенты

$$C_1^{(1, f)} = \frac{1}{N} \sum_{x=0}^{N-1} \xi^{f(x)p^{n-1}+x} \text{ и } C_0^{(1, f)} = \frac{1}{N} \sum_{x=0}^{N-1} \xi^{f(x)p^{n-1}}.$$

Их образы при действии автоморфизма σ_s имеют вид

$$\sigma_s(C_1^{(1, f)}) = \frac{1}{N} \sum_{x=0}^{N-1} \sigma_s(\xi^{f(x)p^{n-1}+x}) = \frac{1}{N} \sum_{x=0}^{N-1} \xi^{(s \bmod p)f(x)p^{n-1}+sx} = C_s^{(s \bmod p, f)}$$

¹На самом деле символом $\mathbb{Z}[\xi]$ обозначают множество элементов поля $\mathbb{Q}(\xi)$, являющихся корнями унитарных многочленов с целыми коэффициентами, однако в нашем случае эти множества совпадают.

и

$$\sigma_s(C_0^{(1,f)}) = \frac{1}{N} \sum_{x=0}^{N-1} \xi^{(s \bmod p)f(x)p^{n-1}} = C_0^{((s \bmod p),f)},$$

где $s \bmod p$ — остаток от деления s на p . Для любого элемента $a \in \mathbb{Q}(\xi)$ произведение $\prod_{s \in \{1, \dots, N\}, (s,p)=1} \sigma_s(a)$ является действительным (точнее, рациональным) числом и называется нормой элемента a (см. [3]). Таким образом, в левой части равенства из формулировки леммы стоит произведение норм элементов $C_1^{(1,f)}$ и $C_0^{(1,f)}$, т. е. действительное число. Лемма доказана. $\square$

Лемма 3. *Справедливо равенство $p = (1 - \xi)^{\varphi(N)} \cdot u$, где u — обратимый элемент кольца $\mathbb{Z}[\xi]$.*

Доказательство. Как было отмечено выше,

$$Q_N(x) = \prod_{s \in \{1, \dots, N\}, (s,p)=1} (x - \xi^s).$$

Подставляя в последнее равенство 1 вместо x , имеем

$$Q_N(1) = p = \prod_{s \in \{1, \dots, N\}, (s,p)=1} (1 - \xi^s) = (1 - \xi)^{\varphi(N)} \prod_{s \in \{1, \dots, N\}, (s,p)=1} \frac{1 - \xi^s}{1 - \xi}.$$

Покажем, что числа $\frac{1 - \xi^s}{1 - \xi}$ являются обратимыми элементами кольца $\mathbb{Z}[\xi]$. Поскольку числа s и N взаимно просты, для любого s найдется такое натуральное a_s , что $sa_s \equiv 1 \pmod{N}$. Число $1 - \xi^s$ в кольце $\mathbb{Z}[\xi]$, очевидно, делит число $1 - \xi^{sa_s}$. Но $1 - \xi^{sa_s} = 1 - \xi$, следовательно, число $\frac{1 - \xi}{1 - \xi^s}$ лежит в $\mathbb{Z}[\xi]$ и $\frac{1 - \xi^s}{1 - \xi}$ — обратимый элемент этого кольца. $\square$

Известно (см. [3, IV, § 1, теорема 1, с. 81]), что идеал (λ) кольца $\mathbb{Z}[\xi]$, порожденный элементом $\lambda = 1 - \xi$, простой. Используя этот факт, докажем следующую лемму.

Лемма 4. *Пусть f — бент-функция из группы $\mathbb{Z}_{p^n}$ в группу $\mathbb{Z}_p$. Тогда любой элемент C из множества*

$$M = \{N \cdot C_s^{(s \bmod p, f)}, N \cdot C_0^{(s \bmod p, f)} \mid s \in \{1, \dots, N\}, (s, p) = 1\}$$

представим в виде

$$C = \lambda^t v,$$

где $t \in \mathbb{N}_0$, а v — обратимый элемент кольца $\mathbb{Z}[\xi]$.

Доказательство. Заметим вначале, что

$$N \cdot C_s^{(s \bmod p, f)} = \sum_{x=0}^{N-1} \xi^{(s \bmod p)f(x)p^{n-1}+sx},$$

$$N \cdot C_0^{(s \bmod p, f)} = \sum_{x=0}^{N-1} \xi^{(s \bmod p)f(x)p^{n-1}},$$

т. е. $C \in \mathbb{Z}[\xi]$ для любого элемента C из множества M , определенного в условии леммы. Из лемм 2 и 3 следуют равенства

$$\begin{aligned} \prod_{s \in \{1, \dots, N\}, (s, p)=1} \left(N \cdot C_s^{(s \bmod p, f)} N \cdot C_0^{(s \bmod p, f)} \right) &= \pm N^{\varphi(N)} = \\ &= \pm p^{n\varphi(N)} = \pm (\lambda^{\varphi(N)} \cdot u)^{n\varphi(N)} = \lambda^{n\varphi(N)^2} \cdot \tilde{u}, \end{aligned} \quad (2)$$

где u и $\tilde{u}$ — обратимые элементы кольца $\mathbb{Z}[\xi]$, и, следовательно, произведение

$$\prod_{s \in \{1, \dots, N\}, (s, p)=1} \left(N \cdot C_s^{(s \bmod p, f)} \cdot N \cdot C_0^{(s \bmod p, f)} \right)$$

всех элементов C множества M лежит в идеале (λ) . Так как этот идеал простой, то λ делит какое-то из чисел C в кольце $\mathbb{Z}[\xi]$. Сократим обе части равенства на λ (это возможно в силу отсутствия делителей нуля) и повторим эту процедуру $n\varphi(N)^2$ раз. В результате в левой части равенства останется $\tilde{u}$, следовательно, в правой части равенства будет находиться произведение обратимых элементов, «оставшихся» от входивших в произведение чисел C после выполненных сокращений. Таким образом, для любого $C \in M$ справедливо равенство $C = \lambda^t v$, где $t \in \mathbb{N}_0$, а v — обратимый элемент кольца $\mathbb{Z}[\xi]$. $\square$

Из общих результатов теории алгебраических чисел (см. [3]) можно получить следующее утверждение (его доказательство приводится, например, в [9]).

Утверждение 5. Пусть α — элемент кольца $\mathbb{Z}[\xi]$, модуль которого равен единице. Тогда α — корень некоторой степени из единицы.

Известно (см. также [3]), что если ω_t и ω_s — корни степеней t и s из единицы соответственно, где t и s взаимно просты, то $\mathbb{Q}(\omega_t) \cap \mathbb{Q}(\omega_s) = \mathbb{Q}$. Отсюда следует, что в $\mathbb{Z}[\xi]$ лежат только корни степеней p^m , $m \leq n$.

Лемма 6. Пусть f — бент-функция из группы $\mathbb{Z}_{p^n}$ в группу $\mathbb{Z}_p$. Тогда найдется такое $l \in \{1, \dots, N-1\}$, что $\xi^l C_0^{(1,f)} = C_1^{(1,f)}$.

Доказательство. Ясно, что числа $N \cdot C_0^{(1,f)}$, $N \cdot C_1^{(1,f)}$ являются элементами множества M из леммы 4 и, значит,

$$N \cdot C_0^{(1,f)} = \lambda^{t_0} v_0, \quad N \cdot C_1^{(1,f)} = \lambda^{t_1} v_1,$$

где $t_0, t_1 \in \mathbb{N}_0$, а v_0, v_1 — обратимые элементы кольца $\mathbb{Z}[\xi]$. Предположим, что $t_0 \leq t_1$. Тогда

$$C_1^{(1,f)} \cdot (C_0^{(1,f)})^{-1} = N C_1^{(1,f)} \cdot (N C_0^{(1,f)})^{-1} = \lambda^{t_1-t_0} v_1 v_0^{-1} \in \mathbb{Z}[\xi].$$

Поскольку f — бент-функция, то

$$|C_1^{(1,f)} \cdot (C_0^{(1,f)})^{-1}| = |C_1^{(1,f)}| \cdot |C_0^{(1,f)}|^{-1} = 1.$$

Для завершения доказательства остается воспользоваться утверждением 5 и замечанием после него.

В случае $t_0 > t_1$ доказательство аналогично. $\square$

Теперь получим необходимое условие существования бент-функции.

Утверждение 7. Если существует бент-функция из группы $\mathbb{Z}_{p^n}$ в группу $\mathbb{Z}_p$, то $n \leq 2$.

Доказательство. Из леммы 6 следует, что для некоторого l выполняется равенство

$$\sum_{x=0}^{N-1} \xi^{f(x)p^{n-1}+x} = \sum_{x=0}^{N-1} \xi^{f(x)p^{n-1}+l}. \quad (3)$$

Разделим l с остатком на p^{n-1} : $l = l_1 p^{n-1} + l_0$, $l_0 \in \{0, \dots, p-1\}$. Тогда правую часть равенства (3) можно привести к виду

$$\sum_{x=0}^{N-1} \xi^{f(x)p^{n-1}+l} = \sum_{x=0}^{N-1} \xi^{(f(x)+l_1)p^{n-1}+l_0} = \xi^{l_0} \sum_{x=0}^{N-1} \zeta^{f(x)+l_1}, \quad (4)$$

где $\zeta = \xi^{p^{n-1}}$ — примитивный корень степени p из единицы.

Левую часть равенства (3) перепишем следующим образом:

$$\sum_{x=0}^{N-1} \xi^{f(x)p^{n-1}+x} = \sum_{y=0}^{p^{n-1}-1} \sum_{x \in [y]_{p^{n-1}}} \xi^{f(x)p^{n-1}+x} =$$

$$\begin{aligned}
&= \sum_{y=0}^{p^{n-1}-1} \sum_{k=0}^{p-1} \zeta^{f(y+kp^{n-1} \bmod p^n)p^{n-1}+y+kp^{n-1}} = \\
&= \sum_{y=0}^{p^{n-1}-1} \zeta^y \sum_{k=0}^{p-1} \zeta^{(f(y+kp^{n-1} \bmod p^n)+k)p^{n-1}} = \\
&= \sum_{y=0}^{p^{n-1}-1} \zeta^y \sum_{k=0}^{p-1} \zeta^{f(y+kp^{n-1} \bmod p^n)+k}. \tag{5}
\end{aligned}$$

Здесь через $[y]_{p^{n-1}}$ обозначен класс вычетов по модулю p^{n-1} , содержащий число y .

Покажем, что элементы поля $\mathbb{Q}(\xi)$, равные $1, \xi, \xi^2, \dots, \xi^{p^{n-1}-1}$, образуют базис этого поля над полем $\mathbb{Q}(\zeta)$. Действительно, как было отмечено выше, степень расширения поля $\mathbb{Q}(\xi)$ над $\mathbb{Q}$ равна $\varphi(p^n) = (p-1)p^{n-1}$, а степень расширения поля $\mathbb{Q}(\zeta)$ над $\mathbb{Q}$ равна $p-1$. Тогда, по теореме о башне полей, степень расширения $\mathbb{Q}(\xi)$ над $\mathbb{Q}(\zeta)$ равна p^{n-1} . С другой стороны, очевидно, что любой элемент поля $\mathbb{Q}(\xi)$ можно представить линейной комбинацией элементов $1, \xi, \xi^2, \dots, \xi^{p^{n-1}-1}$ с коэффициентами из $\mathbb{Q}(\zeta)$. Следовательно, это базис $\mathbb{Q}(\xi)$ над $\mathbb{Q}(\zeta)$.

В силу единственности разложения по базису из равенств (3)–(5) следуют равенства

$$\sum_{k=0}^{p-1} \zeta^{f(l_0+kp^{n-1} \bmod p^n)+k} = \sum_{x=0}^{N-1} \zeta^{f(x)+l_1}, \tag{6}$$

$$\sum_{k=0}^{p-1} \zeta^{f(t+kp^{n-1} \bmod p^n)+k} = 0, \quad t \in \{0, \dots, p^{n-1}-1\} \setminus \{l_0\}. \tag{7}$$

Обозначим через $A_m(t)$ мощность множества

$$\{k \in \{0, \dots, p-1\} \mid f(t+kp^{n-1} \bmod p^n) + k \equiv m \pmod{p}\}, \quad m \in \{0, \dots, p-1\}.$$

Тогда из равенства (6) получаем

$$\sum_{m=0}^{p-1} A_m(l_0) \zeta^m = \sum_{x=0}^{N-1} \zeta^{f(x)+l_1}. \tag{8}$$

Так как f — бент-функция, то модуль правой части последнего равенства равен $p^{\frac{n}{2}}$. С другой стороны,

$$\left| \sum_{m=0}^{p-1} A_m(l_0) \zeta^m \right| \leq \sum_{m=0}^{p-1} |A_m(l_0) \zeta^m| = \sum_{m=0}^{p-1} A_m(l_0) = p. \quad (9)$$

Следовательно, $p^{\frac{n}{2}} \leq p$ и $n \leq 2$. $\square$

При $n = 1$, как известно, не существует бент-функций из $\mathbb{Z}_2$ в $\mathbb{Z}_2$. В случае $p > 2$ бент-функции из группы $\mathbb{Z}_p$ в группу $\mathbb{Z}_p$ описывает следующее утверждение.

Утверждение 8. Пусть $p > 2$. Для того чтобы функция $f(x)$ из группы $\mathbb{Z}_p$ в группу $\mathbb{Z}_p$ являлась бент-функцией, необходимо и достаточно, чтобы f представлялась многочленом $ax^2 + bx + c \in \mathbb{Z}_p[x]$, $a \neq 0$.

Доказательство. Доказательство состоит из ссылок на известные результаты.

В первую очередь пользуемся теоремой 1. Теперь достаточность проверяется непосредственно:

$$f(x + w) - f(x) = 2awx + aw^2 + bw,$$

и, поскольку $2aw \neq 0$, функция $f(x + w) - f(x)$ уравновешена, т. е. f — бент-функция.

Необходимость условия $f(x) = ax^2 + bx + c$ для уравновешенности функции $f(x + w) - f(x)$ доказана в [8]. Заметим, что существенной частью этого доказательства является, в свою очередь, ссылка на результат работы [7], где описаны квадратичные суммы Гаусса, модуль которых равен $\sqrt{p}$. $\square$

Рассмотрим случай $n = 2$. Приводимое ниже следствие определяет необходимое условие на бент-функцию.

Следствие 1. Пусть f — бент-функция из группы $\mathbb{Z}_{p^2}$ в группу $\mathbb{Z}_p$. Для каждого t из $\mathbb{Z}_p$ определим отображение $g_t : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ следующим образом:

$$\forall x \in \mathbb{Z}_p \quad g_t(x) = f(t + xp \bmod p^2) + x \bmod p.$$

Тогда существует единственное значение t , для которого g_t является константой, для всех остальных значений t отображение g_t является подстановкой на $\mathbb{Z}_p$.

Доказательство. Так как f — бент-функция, то неравенство в цепочке (9) обращается в равенство. Из элементарных свойств комплексных чисел следует, что такое равенство возможно лишь тогда, когда только одно слагаемое из соответствующей суммы отлично от нуля. Таким образом, существует такое $m_0 \in \{0, \dots, p-1\}$, для которого $A_{m_0}(l_0) = p$, и $A_m(l_0) = 0$ для остальных m . Следовательно, $g_{l_0}(x)$ — константа m_0 .

Пусть теперь $t \neq l_0$. Из равенств (7) следует, что $\sum_{m=0}^{p-1} A_m(t)\zeta^m = 0$. Известно, что $\sum_{m=0}^{p-1} \zeta^m = 0$, поэтому

$$\sum_{m=1}^{p-1} (A_m(t) - A_0(t))\zeta^m = 0.$$

Но числа $\zeta, \dots, \zeta^{p-1}$ образуют базис поля $\mathbb{Q}(\zeta)$ над $\mathbb{Q}$, следовательно, $A_0(t) = A_1(t) = \dots = A_{p-1}(t)$ и функция g_t — подстановка на $\mathbb{Z}_p$. $\square$

Следующее утверждение описывает класс функций из группы $\mathbb{Z}_{p^2}$ в группу $\mathbb{Z}_p$, являющихся бент-функциями.

Утверждение 9. Пусть $a_0, \dots, a_{p-1}$ — произвольные элементы $\mathbb{Z}_p$, p — простое число, $(i_0, \dots, i_{p-1})$ — произвольная перестановка множества $\{0, \dots, p-1\}$. Функцию $f: \mathbb{Z}_{p^2} \rightarrow \mathbb{Z}_p$ определим следующим образом. Пусть $x \in \mathbb{Z}_{p^2}$ и $x = x_0 + x_1p$, где $x_0, x_1 \in \{0, \dots, p-1\}$. Положим

$$f(x) = a_{x_0} + x_1 i_{x_0} \pmod{p}.$$

Тогда f — бент-функция.

Доказательство. Рассмотрим произвольный коэффициент Фурье функции f :

$$\begin{aligned} C_k^{(m,f)} &= \frac{1}{p^2} \sum_{x=0}^{p^2-1} \xi^{mf(x)p+kx} = \frac{1}{p^2} \sum_{x=0}^{p^2-1} \xi^{m(a_{x_0} + x_1 i_{x_0})p + k(x_1 p + x_0)} = \\ &= \frac{1}{p^2} \sum_{x_0=0}^{p-1} \xi^{ma_{x_0}p + kx_0} \sum_{x_1=0}^{p-1} \xi^{(mi_{x_0} + k)x_1}. \end{aligned}$$

Внутренняя сумма обращается в 0 при всех значениях x_0 , за исключением того, для которого выполнено сравнение $mi_{x_0} + k \equiv 0 \pmod{p}$. Такое значение x_0 , очевидно, единственно, и в этом случае сумма равна p . Таким образом, $C_k^{(m,f)} = \frac{1}{p} \xi^{ma_{x_0}p + kx_0}$ для указанного значения x_0 , следовательно, $|C_k^{(m,f)}| = \frac{1}{p}$ и f является бент-функцией. $\square$

Компьютерная проверка показала, что для $p = 2, 3, 5$ функции, описанные в последнем утверждении, исчерпывают все бент-функции из группы $\mathbb{Z}_{p^2}$ в группу $\mathbb{Z}_p$. Для других значений p существование бент-функций, отличных от описанных, является предметом дальнейшего исследования.

В итоге сформулируем основной результат работы в виде теоремы.

Теорема 10. *Необходимым для существования бент-функции из $\mathbb{Z}_{p^n}$ в нетривиальную конечную абелеву группу H является следующее условие:*

$$|H| = p^m, \quad m \leq 2, \quad n = \begin{cases} 2 & \text{при } p = 2 \\ 1, 2 & \text{при } p \geq 3. \end{cases}$$

При $m = 1$ это условие является и достаточным.

Автору пока не удалось построить пример бент-функции для случая $m = n = 2$ (т. е. $H = \mathbb{Z}_{p^2}$ или $H = (\mathbb{Z}_p)^2$). Компьютерный перебор показал отсутствие таких функций для $p = 2, 3$.

В заключение автор выражает глубокую признательность Виктору Игоревичу Солодовникову за ценные замечания и советы, позволившие повысить качество этой работы.

Список литературы

- [1] Амбросимов А. С., “Свойства бент-функций q -значной логики над конечными полями”, *Дискрет. матем.*, **14**:3 (1994), 50–60.
- [2] Кэртис Ч., Райнер И., *Теория представлений конечных групп и ассоциативных алгебр*, М.: Наука, 1969, 668 с.
- [3] Ленг С., *Алгебраические числа*, М.: Мир, 1966, 230 с.
- [4] Солодовников В. И., “Бент-функции из конечной абелевой группы в конечную абелеву группу”, *Дискрет. матем.*, **14**:1 (2002), 99–113.
- [5] Солодовников В. И., “О совпадении класса бент-функций с классом функций, минимально близких к линейным”, *Пробл. дискретн. матем.*, 2012, № 3, 25–33.
- [6] Токарева Н. Н., *Нелинейные булевы функции: бент-функции и их обобщения*, Saarbrücken, Germany : LAP LAMBERT Acad. Publ., 2011, 180 с.
- [7] Cavior S., “Exponential sums related to polynomials over $GF(p)$ ”, *Proc. Amer. Math. Soc.*, **15** (1964), 175–178.
- [8] Gluck D., “A note on permutation polynomials and finite geometries”, *Discrete Mathematics*, **80** (1990), 97–100.
- [9] Kumar P. V., Scholtz R. A., Welch L. R., “Generalized bent functions and their properties”, *J. Combin. Theory Ser. A*, **40**:1 (1985), 90–107.
- [10] Nyberg K., “Construction of bent functions and difference sets”, *EUROCRYPT’90, Lect. Notes Comput. Sci.*, **473** (1991), 151–160.
- [11] Rothaus O. S., “On “bent” functions”, *J. Combin. Theory (A)*, **20** (1976), 300–305.