Math-Net.Ru

Общероссийский математический портал

О. А. Логачев, А. А. Сальников, В. В. Ященко, Бент-
функции на конечной абелевой группе, *Дискрет. матем.*,
1997, том 9, выпуск 4, 3–20

DOI: <https://doi.org/10.4213/dm498>

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: 54.92.164.108

26 апреля 2023 г., 11:50:49

Бент-функции на конечной абелевой группе

© 1997 г. О. А. Логачев, А. А. Сальников, В. В. Яценко

Вводится понятие бент-функции на конечной абелевой группе, которое в случае элементарной абелевой 2-группы совпадает с хорошо известным понятием булевой бент-функции. С помощью аппарата теории характеров и коммутативного гармонического анализа получен ряд свойств бент-функций, обобщающих свойства булевых бент-функций. Построены некоторые классы бент-функций.

Работа последним из авторов выполнялась при поддержке Российского фонда фундаментальных исследований, проект 96-01-00931.

1. Введение

Понятие булевых бент-функций было введено в [1–4]. В [1] исследованы некоторые их свойства и приведены два класса бент-функций. В [2] указана связь бент-функций и такого комбинаторного объекта, как разностные множества. Исходя из методов построения разностных множеств, в [3, 4] приведены два достаточно больших класса бент-функций: M и PS . Причем последний из них состоит из задаваемых неявно подклассов PS^+ и PS^- , и явно задаваемого класса функций $PS_{a,p}$. Дальнейшие исследования в этом направлении [5] привели к рассмотрению новых классов бент-функций D и C . В этой же работе введено понятие полноты класса бент-функций и показано, что классы D и C не входят в ранее известные классы M и PS , а также показано, что классы M и PS не полны. Существенное продвижение в исследовании бент-функций получено в [6]. В этой работе рассмотрено так называемое геометрическое представление бент-функций и введен класс GPS бент-функций, задаваемых с помощью этого представления. Получен ряд свойств бент-функций из этого класса, продемонстрирована эффективность этого подхода при построении новых бент-функций (см. также [7]). В заключение высказана гипотеза о возможности представления (характеризации) бент-функций в виде суммы (в поле рациональных чисел) характеристических функций подпространств специального вида. Эта гипотеза была доказана в [8].

Достаточно широкие приложения бент-функций в теории кодирования (см. [9], где бент-функции названы максимально-нелинейными функциями), в теории связи [10–14], в других областях, породили направления исследований, изучающие бент-функции с дополнительными условиями [15], а также функции, близкие по своим свойствам к бент-функциям [16].

Одновременно с изучением булевых бент-функций развивались различные обобщения этого понятия. Здесь следует отметить работы [17, 18]. В них введены бент-функции, определенные на прямом произведении конечного числа одинаковых циклических групп, со значениями в этой циклической группе. Иное обобщение понятия бент-функции приведено в [19]. В этой статье рассмотрены бент-функции, определенные на векторном пространстве над конечным полем, со значениями в этом конечном поле. Изложение ведется на языке случайных величин и характеристических функций. Более подробный обзор результатов о свойствах булевых бент-функций (максимально-нелинейных функций) содержится в [20].

В настоящей работе введено понятие бент-функции на произвольной конечной абелевой группе, причем это понятие совпадает с понятием булевой бент-функции, если рассматриваемая группа является элементарной абелевой 2-группой. Для бент-функций получены многие из свойств, известных для булева случая.

2. Определения, обозначения и результаты

В обозначениях и исходных результатах мы будем следовать двум монографиям, по абстрактному гармоническому анализу [21] и по теории кодирования [9], а также статье [22], в которой с целью обобщения кодов Рид-Маллера получен ряд свойств функций на конечной абелевой группе.

Пусть G — конечная абелева группа в мультипликативной записи, порядок G равен n , экспонента G (максимальный порядок элементов из G) равна m , e — единица G . Пусть T — группа вращений окружности, то есть

$$T = \{e^{2\pi ix}, 0 \leq x < 1\},$$

T_m — подгруппа T , состоящая из корней степени m из единицы. Как обычно, через T^G обозначим множество функций на G со значениями в T . Если зафиксировать некоторую нумерацию элементов G , то множество T^G можно отождествить с множеством T^n и представлять его как множество векторов длины n с координатами из T . Множество T^G является подмножеством n -мерного линейного пространства $\mathbb{C}^G$ всех комплекснозначных функций на G . На $\mathbb{C}^G$ обычным образом вводится скалярное произведение

$$(f_1, f_2) = \sum_{x \in G} f_1(x) \bar{f}_2(x),$$

где $\bar{f}_2(x)$ — число, комплексно сопряженное числу $f_2(x)$. Отметим, что если $f \in T^G$, то $(f, f) = n$.

Множество $T_m^G \subset T^G$ функций на G со значениями в T_m является конечной абелевой группой относительно покомпонентного умножения функций, порядок T_m^G равен m^n , экспонента равна m . Подчеркнем, что в настоящей работе в разных ситуациях используются как функции из T^G , так и функции из T_m^G . Подгруппой группы T_m^G является группа $\hat{G}$, группа характеров группы G , то есть гомоморфизмов $\chi: G \rightarrow T_m$. Группа $\hat{G}$ изоморфна группе G . Зафиксируем некоторый изоморфизм и будем считать, что все характеры $\chi_\alpha \in \hat{G}$ занумерованы элементами $\alpha \in G$. Характеры удовлетворяют соотношениям ортогональности

$$(\chi_\alpha, \chi_\beta) = \begin{cases} 0, & \text{если } \alpha \neq \beta, \\ n, & \text{если } \alpha = \beta. \end{cases}$$

Удобно ввести в рассмотрение квадратную матрицу $H(G)$ размера $n \times n$

$$H(G) = \|\chi_\alpha(x)\|.$$

Строка матрицы $H(G)$ с номером $\alpha \in G$ — это вектор значений характера $\chi_\alpha \in \hat{G}$. В случае, когда G — элементарная абелева 2-группа порядка 2^k , матрица $H(G)$ является хорошо известной матрицей Адамара [9]. Соотношения ортогональности эквивалентны матричному равенству

$$H(G)H^*(G) = nE,$$

где E — единичная матрица размера $n \times n$, $H^*(G)$ — транспонированная и комплексно-сопряженная к $H(G)$ матрица. Матрица $H(G)$ задает преобразование Фурье $f(x) \rightarrow \hat{f}(\alpha)$ функций из $\mathbb{C}^G$ равенством

$$\hat{f}(\alpha) = \sum_{x \in G} f(x) \bar{\chi}_\alpha(x).$$

Обратное преобразование задается равенством

$$f(x) = \frac{1}{n} \sum_{\alpha \in G} \hat{f}(\alpha) \chi_\alpha(x).$$

Функцию $f \in T^G$, для которой при всех $\alpha \in G$

$$|\hat{f}(\alpha)|^2 = n,$$

будем называть бент-функцией, здесь $|\hat{f}(\alpha)|$ — модуль комплексного числа $\hat{f}(\alpha)$. Множество всех бент-функций на группе G обозначим через $BF(G)$.

Нам понадобятся еще некоторые свойства функций $f \in T^G$ и их преобразований Фурье.

Преобразование Фурье произведения двух функций $\widehat{f\varphi}(\alpha)$ равно свертке преобразований Фурье $(\hat{f} * \hat{\varphi})(\alpha)$, которая определяется равенством

$$\frac{1}{n} \sum_{\beta \in G} \hat{f}(\beta) \hat{\varphi}(\alpha\beta^{-1}) = (\hat{f} * \hat{\varphi})(\alpha) = \widehat{f\varphi}(\alpha).$$

Применив преобразование Фурье к обеим частям тождества

$$f(x)\bar{f}(x) = 1,$$

получим соотношения ортогональности для коэффициентов Фурье любой функции $f \in T^G$:

$$\sum_{\alpha \in G} \hat{f}(\alpha) \bar{\hat{f}}(\alpha\beta^{-1}) = \begin{cases} 0, & \text{если } \beta \neq e, \\ n^2, & \text{если } \beta = e. \end{cases}$$

При этом мы воспользовались легко проверяемым тождеством

$$\hat{f}(\alpha) = \bar{\hat{f}}(\alpha^{-1}).$$

Соотношения ортогональности накладывают достаточно сильные ограничения на возможные значения коэффициентов Фурье $\hat{f}(\alpha)$ для функций $f \in T^G$ и являются

необходимыми и достаточными условиями того, что для данной функции $F(\alpha) \in \mathbb{C}^G$ найдется такая функция $f(x) \in T^G$, для которой $\hat{f}(\alpha) = F(\alpha)$.

В различных ситуациях возникает множество функций, выделяемых условием

$$\hat{f}(\mathbf{e}) = \sum_{x \in G} f(x) = 0.$$

Обозначим это множество через $UF(G)$ и будем называть функции из этого множества уравновешенными функциями. Другими словами, уравновешенными будем называть те функции из T^G , для которых в разложение по характерам не входит тривиальный характер $\chi_{\mathbf{e}}(x)$.

Для функций из $UF(G) \cap T_m^G$ можно получить более простое описание, поскольку в этом случае $\hat{f}(\mathbf{e})$ выражается через частоты значений из T_m , принимаемых функцией $f \in T_m^G$:

$$\hat{f}(\mathbf{e}) = \sum_{\xi \in T_m} b^{(f)}(\xi)\xi,$$

где

$$b^{(f)}(\xi) = |\{x \in G: f(x) = \xi\}|.$$

Теперь зафиксируем некоторую образующую $\eta \in T_m$ циклической группы T_m , положим

$$b_k^{(f)} = b^{(f)}(\eta^k), \quad k = 0, 1, \dots, m-1,$$

и рассмотрим многочлен

$$p^{(f)}(z) = \sum_{k=0}^{m-1} b_k^{(f)} z^k.$$

По построению

$$\hat{f}(\mathbf{e}) = p^{(f)}(\eta)$$

и, значит, $f \in UF(G) \cap T_m^G$ тогда и только тогда, когда η — корень многочлена $p^{(f)}(z)$. Но все элементы $\xi \in T_m$ являются корнями уравнения

$$z^m - 1 = 0$$

и, значит, если $f \in UF(G) \cap T_m^G$, то многочлены $p^{(f)}(z)$ и $z^m - 1 = 0$ имеют общий нетривиальный делитель. Простейшим примером являются такие функции, для которых $p^{(f)}(z)$ делится на $\sum_{k=0}^{m-1} z^k$, то есть функции, для которых $b^{(f)}(\xi)$ — постоянная, не зависящая от ξ , и тем самым равная n/m . Такие функции обычно называют равновероятными или функциями, сохраняющими равномерное распределение.

Полезно также заметить, что если для функции $f \in T^G$ выполнено условие

$$\hat{f}(\beta) = 0,$$

то

$$\bar{\chi}_\beta(x)f(x) \in UF(G).$$

Обозначим через S_G симметрическую группу всех перестановок элементов G . Назовем аффинной группой преобразований группы G следующую группу:

$$A(G) = \{\pi \in S_G: x^\pi = \mathbf{e}^\pi x^\omega, \omega \in \text{Aut}(G)\}.$$

Действие $A(G)$ на функциях $f \in T^G$ определяется естественным образом:

$$f^\pi(x) = f(x^\pi),$$

где x^π — образ элемента $x \in G$ при перестановке $\pi \in A(G)$.

Теперь все множество T^G разбивается на орбиты относительно действия группы $A(G)$, которые мы будем называть аффинными классами по аналогии с соответствующим понятием для булевых функций. Функции из одной орбиты мы будем называть аффинно эквивалентными (или просто эквивалентными). Такие характеристики функций, которые постоянны на орбите, то есть которые равны для аффинно эквивалентных функций, мы будем называть аффинными инвариантами.

Очевидно, что множества $BF(G)$ и $UF(G)$ замкнуты относительно действия $A(G)$, то есть состоят из какого-то количества аффинных классов.

Производная $df(x)/d\sigma$ функции $f \in T^G$ по направлению $\sigma \in G$ введена в [22] с помощью равенства

$$\frac{df}{d\sigma}(x) = \bar{f}(x)f(\sigma x), \quad x \in G.$$

Коды $RM_r(G)$ типа Рида–Маллера порядка r , $r = 0, 1, \dots$, на группе G определены в работе [22] рекуррентным образом:

$$\begin{aligned} RM_r(G) &= \{f \in T_m^G : df/d\sigma \in RM_{r-1}(G), \sigma \in G\}, \\ RM_{-1}(G) &= \{f \in T_m^G : f(x) \equiv 1\}. \end{aligned}$$

При этом функции из $RM_1(G)$ — это аффинные функции на G , так как они получаются из характеров (линейных функций) умножением на константу: $f \in RM_1(G)$ тогда и только тогда, когда $f(x) = f(e)\chi_\alpha(x)$ для некоторого $\alpha \in G$ при всех $x \in G$. Функции из $RM_2(G)$ — это квадратичные функции на G , так как любая их производная — аффинная функция.

3. Основные свойства бент-функций

Теорема 1. *Справедливо равенство*

$$BF(G) = \{f \in T^G : df/d\sigma \in UF(G), \sigma \in G \setminus e\}.$$

Доказательство. Вычислим преобразование Фурье функции $df/d\sigma$ и приведем его к более удобному виду

$$\begin{aligned} \widehat{\frac{df}{d\sigma}}(\alpha) &= \sum_{x \in G} \bar{f}(x)f(\sigma x)\bar{\chi}_\alpha(x) \\ &= \sum_{x \in G} \frac{1}{n} \sum_{\beta \in G} \bar{\hat{f}}(\beta)\bar{\chi}_\beta(x) \frac{1}{n} \sum_{\gamma \in G} \hat{f}(\gamma)\chi_\gamma(\sigma x)\bar{\chi}_\alpha(x) \\ &= \frac{1}{n^2} \sum_{\beta, \gamma \in G} \bar{\hat{f}}(\beta)\hat{f}(\gamma)\chi_\gamma(\sigma) \sum_{x \in G} \bar{\chi}_\beta(x)\chi_\gamma(x)\bar{\chi}_\alpha(x) \\ &= \frac{1}{n} \sum_{\beta \in G} \bar{\hat{f}}(\beta)\hat{f}(\beta\alpha)\chi_{\beta\alpha}(\sigma). \end{aligned}$$

Отсюда получаем, что при всех $\sigma \in G$

$$\widehat{\frac{df}{d\sigma}}(\mathbf{e}) = \frac{1}{n} \sum_{\beta \in G} |\hat{f}(\beta)|^2 \chi_{\beta}(\sigma).$$

Теперь достаточно воспользоваться свойствами системы характеров и получить, что условие $|\hat{f}(\beta)|^2 = n$ для всех $\beta \in G$ эквивалентно условию

$$\widehat{\frac{df}{d\sigma}}(\mathbf{e}) = 0$$

для всех $\sigma \in G$, $\sigma \neq \mathbf{e}$.

Полученный в теореме 1 критерий для случая булевых бент-функций известен как критерий Ротхауза; он установлен Ротхаузом в [1]. На случай элементарной абелевой p -группы критерий Ротхауза обобщен в [19].

Еще одну форму этого критерия можно получить, рассмотрев следующую числовую характеристику функций из T^G :

$$\Delta^2 f = \sum_{\sigma \neq \mathbf{e}} \left| \widehat{\frac{df}{d\sigma}}(\mathbf{e}) \right|^2.$$

Очевидно, что $\Delta^2 f$ является аффинным инвариантом. Из линейной системы, полученной в теореме 1, легко получить систему

$$\begin{aligned} \widehat{\frac{df}{d\sigma}}(\mathbf{e}) &= \frac{1}{n} \sum_{\beta \in G} \left(|\hat{f}(\beta)|^2 - n \right) \chi_{\beta}(\sigma), \quad \sigma \neq \mathbf{e}, \\ 0 &= \frac{1}{n} \sum_{\beta \in G} \left(|\hat{f}(\beta)|^2 - n \right). \end{aligned}$$

В силу ортогональности матрицы $\|\chi_{\beta}(\sigma)\|$ отсюда следует, что

$$\sum_{\sigma \neq \mathbf{e}} \left| \widehat{\frac{df}{d\sigma}}(\mathbf{e}) \right|^2 = \frac{1}{n} \sum_{\beta \in G} \left(|\hat{f}(\beta)|^2 - n \right)^2.$$

Следствие 1. *Справедливо равенство*

$$BF(G) = \{f \in T^G : \Delta^2 f = 0\}.$$

Таким образом, аффинный инвариант $\Delta^2 f$ можно рассматривать как меру удаленности функции $f \in T^G$ от множества $BF(G)$.

Легко видеть, что для любых $c \in T$, $\sigma \in G$, $\chi \in \hat{G}$, $f \in T^G$ выполнено равенство

$$\widehat{\frac{d(c\chi f)}{d\sigma}}(\mathbf{e}) = \chi(\sigma) \widehat{\frac{df}{d\sigma}}(\mathbf{e})$$

и поэтому

$$\Delta^2(c\chi f) = \Delta^2 f.$$

В частности, отсюда вытекает, что для всех $f \in BF(G)$ функции $c\chi f$ также являются бент-функциями.

Теорема 2. Функция $f \in T^G$ является бент-функцией тогда и только тогда, когда система из n функций

$$b_\sigma(x) = \frac{df}{d\sigma}(x), \quad \sigma \in G,$$

образует ортогональный базис в $\mathbb{C}^G$.

Доказательство. Легко видеть, что условия ортогональности

$$(b_\sigma, b_\omega) = 0, \quad \sigma, \omega \in G, \quad \sigma \neq \omega,$$

эквивалентны условию

$$\sum_{x \in G} \frac{df}{d\sigma}(x) = 0, \quad \sigma \in G, \quad \sigma \neq e,$$

которое в силу теоремы 1 выполнено только для бент-функций.

Базисы в $\mathbb{C}^G$, выделяемые теоремой 2, имеют специальный вид. Для их описания введем следующее понятие. Систему из n функций $b_\sigma(x)$, $\sigma \in G$, назовем бент-базисом, если она удовлетворяет следующим условиям:

- (1) $(b_\sigma, b_\omega) = n$ при $\sigma = \omega$ и $(b_\sigma, b_\omega) = 0$ при $\sigma \neq \omega$,
 - (2) $S_\sigma b_\omega = \bar{b}_\sigma b_{\sigma\omega}$ при $\sigma, \omega \in G$, где $S_\sigma: \mathbb{C}^G \rightarrow \mathbb{C}^G$ — оператор сдвига
- $$(S_\sigma f)(x) = f(\sigma x), \quad \sigma, x \in G.$$

Из определения легко получить также следующие свойства любого бент-базиса:

- (а) $b_e(x) \equiv 1$, для доказательства достаточно в (2) положить $\sigma = e$;
- (б) из (1) с учетом (а) следует, что

$$\sum_{x \in G} b_\sigma(x) = \begin{cases} 0, & \text{если } \sigma \neq e, \\ n, & \text{если } \sigma = e; \end{cases}$$

- (с) $b_\sigma(x) \in T^G$ при всех $\sigma \in G$, для доказательства достаточно в (2) положить $\omega = e$ и воспользоваться (а);
- (д) при всех $x \in G$

$$\left| \sum_{\sigma \in G} b_\sigma(x) \right|^2 = n,$$

для доказательства достаточно провести следующие простые выкладки с учетом свойств (2) и (б):

$$\begin{aligned} \sum_{\sigma \in G} \bar{b}_\sigma(x) \sum_{\tau \in G} b_\tau(x) &= \sum_{\sigma, \tau \in G} \bar{b}_\sigma(x) b_\tau(x) \\ &= \sum_{\omega \in G} \sum_{\sigma \in G} \bar{b}_\sigma(x) b_{\sigma\omega}(x) \\ &= \sum_{\omega \in G} \sum_{\sigma \in G} S_\sigma b_\omega(x) \\ &= \sum_{\omega \in G} \sum_{y \in G} b_\omega(y) = n. \end{aligned}$$

Возвращаясь теперь к теореме 2, отметим, что один ортогональный базис вида $df(x)/d\sigma$, $\sigma \in G$, соответствует не единственной бент-функции, он не меняется при умножении функции f на любую константу из T . Чтобы исключить эту неоднозначность, введем условие нормировки $f(e) = 1$.

Теорема 3. Взаимнообратные отображения

$$f(x) \rightarrow b_\sigma(x) = \frac{df}{d\sigma}(x), \quad \forall \sigma \in G,$$

и

$$b_\sigma(x), \quad \forall \sigma \in G, \rightarrow f(x) = b_x(e)$$

устанавливают взаимно однозначное соответствие между множеством бент-базисов в C^G и множеством бент-функций с условием нормировки $f(e) = 1$.

Доказательство. Пусть $f \in BF(G)$. В соответствии с теоремой 2 система функций $b_\sigma(x) = df(x)/d\sigma$, $\sigma \in G$, образует ортогональный базис в C^G , то есть выполнено условие (1) в определении бент-базиса. Условие (2) проверяется непосредственно. Действительно,

$$\begin{aligned} (S_\sigma b_\omega)(x) &= S_\sigma(\bar{f}(x)f(\omega x)) = \bar{f}(\sigma x)f(\sigma\omega x) \\ &= (f(x)\bar{f}(\sigma x))(\bar{f}(x)f(\sigma\omega x)) = (\bar{b}_\sigma b_{\sigma\omega})(x). \end{aligned}$$

Пусть $b_\sigma(x)$, $\sigma \in G$, — некоторый бент-базис. Положим

$$f(x) = b_x(e).$$

Тогда $f \in T^G$, $f(e) = 1$ в силу свойств (а) и (с) бент-базиса. Покажем, что $df(x)/d\sigma = b_\sigma(x)$. Действительно, для всех $\sigma, x \in G$

$$\frac{df}{d\sigma}(x) = \bar{f}(x)f(\sigma x) = \bar{b}_x(e)b_{\sigma x}(e) = (S_x b_\sigma)(e) = b_\sigma(x).$$

В силу свойства (1) бент-базиса и теоремы 2 функция $f(x)$ является бент-функцией.

Зафиксируем какую-нибудь бент-функцию f на группе G . Теперь любую функцию из C^G можно разложить по базису из производных $df(x)d\sigma$, $\sigma \in G$, при этом естественно возникает понятие бент-преобразования, задаваемого матрицей

$$D_f(G) = \left\| \frac{df}{d\sigma}(x) \right\|$$

аналогично преобразованию Фурье, задаваемому матрицей $H(G)$. В силу теоремы 2 функция $f(x)$ принадлежит $BF(G)$ тогда и только тогда, когда

$$D_f(G)D_f^*(G) = nE,$$

то есть, тогда и только тогда, когда для матрицы $D_f(G)$ при $f \in BF(G)$ выполнено такое же соотношение ортогональности, что и для матрицы $H(G)$. Естественно, для произвольных бент-преобразований справедливы все результаты теории преобразования Фурье, которые используют только ортогональность матрицы $H(G)$.

Для примера приведем простейшие факты о бент-преобразовании $\varphi(x) \rightarrow \check{\varphi}(\sigma)$, заданном с помощью матрицы $D_f(G)$, $f \in BF(G)$:

$$\begin{aligned}\check{\varphi}(\sigma) &= \sum_{x \in G} \varphi(x) \overline{\frac{df}{d\sigma}}(x), & \sigma \in G, \\ \varphi(x) &= \frac{1}{n} \sum_{\sigma \in G} \check{\varphi}(\sigma) \frac{df}{d\sigma}(x), & x \in G, \\ \sum_{\sigma \in G} |\check{\varphi}(\sigma)|^2 &= n^2.\end{aligned}$$

В связи с теоремой 1 естественно для произвольной функции $f \in T^G$ ввести множество

$$PC(f) = \{\sigma \in G: df/d\sigma \in UF(G)\}.$$

Обозначение $PC(f)$ связано с тем, что в булевом случае принято говорить, что функция f удовлетворяет критерию распространения (propagation criterion) относительно элемента $\sigma \in PC(f)$ (см., например, [23]). При таких обозначениях утверждение теоремы 1 можно записать следующим образом:

$$BF(G) = \{f \in T^G: PC(f) = G \setminus \mathbf{e}\}.$$

Из рассуждений, связанных с теоремой 1, легко получить следующий результат.

Следствие 2. *Справедливо равенство*

$$PC(f) = \left\{ \sigma \in G: \sum_{\beta \in G} |\hat{f}(\beta)|^2 \chi_{\beta}(\sigma) = 0 \right\}.$$

В булевом случае следствие 2 совпадает с теоремой 2 работы [24].

С помощью условий на $PC(f)$ можно вводить различные множества функций и естественно ожидать, что чем больше множество $PC(f)$, тем ближе в определенном смысле функция f к множеству бент-функций. Приведем описание двух естественных множеств функций, рассмотренных в булевом случае в [24].

Пусть $Q < G$ — подгруппа группы G . Через $Q^{\perp}$ обозначим дуальную к Q подгруппу (в другой терминологии — аннулятор подгруппы Q):

$$Q^{\perp} = \{\alpha \in G: \chi_{\alpha}(x) = 1, x \in Q\}.$$

Как обычно, G/Q — это фактор-группа группы G по подгруппе Q .

Теорема 4. *Пусть $Q < G$. Для функции $f \in T^G$ выполнено включение $Q \setminus \mathbf{e} \subseteq PC(f)$ тогда и только тогда, когда коэффициенты Фурье функции f удовлетворяют системе линейных уравнений*

$$\sum_{\alpha \in Q^{\perp}} |\hat{f}(\alpha\gamma)|^2 = \frac{n^2}{|Q|}, \quad \gamma \in G/Q^{\perp}.$$

Доказательство. В силу следствия 2 коэффициенты Фурье любой функции $f \in T^G$ удовлетворяют системе линейных уравнений

$$\sum_{\beta \in G} |\hat{f}(\beta)|^2 \chi_{\beta}(\sigma) = 0, \quad \sigma \in PC(f).$$

Разложив G на смежные классы по $Q^{\perp}$, представим эти уравнения в виде

$$\sum_{\gamma \in G/Q^{\perp}} \sum_{\alpha \in Q^{\perp}} |\hat{f}(\alpha\gamma)|^2 \chi_{\alpha\gamma}(\sigma) = 0, \quad \sigma \in PC(f).$$

Поскольку $Q \setminus e \subseteq PC(f)$ и $\chi_{\alpha}(\sigma) = 1$ для всех $\alpha \in Q^{\perp}$, $\sigma \in Q$, получаем, что

$$\sum_{\gamma \in G/Q^{\perp}} \chi_{\gamma}(\sigma) \sum_{\alpha \in Q^{\perp}} |\hat{f}(\alpha\gamma)|^2 = 0, \quad \sigma \in Q \setminus e.$$

Добавляя теперь равенство Парсеваля, получаем следующую невырожденную систему из $|Q|$ уравнений относительно $|Q|$ неизвестных $\sum_{\alpha \in Q^{\perp}} |\hat{f}(\alpha\gamma)|^2$, $\gamma \in G/Q^{\perp}$:

$$\begin{aligned} \sum_{\gamma \in G/Q^{\perp}} \chi_{\gamma}(\sigma) \left(\sum_{\alpha \in Q^{\perp}} |\hat{f}(\alpha\gamma)|^2 \right) &= 0, \quad \sigma \in Q \setminus e, \\ \sum_{\gamma \in G/Q^{\perp}} \left(\sum_{\alpha \in Q^{\perp}} |\hat{f}(\alpha\gamma)|^2 \right) &= n^2. \end{aligned}$$

Эта система имеет единственное решение

$$\sum_{\alpha \in Q^{\perp}} |\hat{f}(\alpha\gamma)|^2 = \frac{n^2}{|Q|}, \quad \gamma \in G/Q^{\perp}.$$

Обратное утверждение теоремы очевидно.

Аналогично теореме 4 доказывается следующее утверждение.

Теорема 5. Пусть $Q < G$, $\sigma_0 \in G/Q$, $\sigma_0 \neq e$. Для функции $f \in T^G$ выполнено включение $PC(f) \supseteq \sigma_0 Q$ тогда и только тогда, когда коэффициенты Фурье функции f удовлетворяют системе линейных уравнений

$$\sum_{\alpha \in Q^{\perp}} |\hat{f}(\alpha\gamma)|^2 \chi_{\alpha}(\sigma_0) = 0, \quad \gamma \in G/Q^{\perp}.$$

Группой линейности L_f функции $f \in T^G$ называется подгруппа группы G

$$L_f = \left\{ \sigma \in G : \frac{df}{d\sigma}(x) \equiv c \right\},$$

где c — постоянная. В булевом случае элементы $\sigma \in L_f$ называют также линейной структурой функции f . Теперь очевиден следующий результат.

Лемма 1. Для любой бент-функции f группа линейности тривиальна, то есть $L_f = \{e\}$.

Рассмотрим теперь функции из $RM_2(G)$, для них любая производная является сдвигом или тривиального, или нетривиального характера, поэтому вся группа распадается на две части:

$$G = L_f \cup PC(f).$$

Отсюда вытекает следующий результат.

Лемма 2. *Функция $f \in RM_2(G)$ является бент-функцией тогда и только тогда, когда ее группа линейности тривиальна.*

Булевы функции, удовлетворяющие условиям леммы 2, невырожденные квадратичные формы, были первыми примерами бент-функций. Для случая $G = \mathbf{Z}_p$, где p — простое число, лемма 2 утверждает, что все функции из $RM_2(G) \setminus RM_1(G)$ являются бент-функциями.

Интересной особенностью бент-функций является то, что для них можно определить понятие дуальной функции, которая задает преобразование Фурье исходной функции. Пусть $f \in BF(G)$, тогда $|\hat{f}(\alpha)|^2 = n$ для всех $\alpha \in G$ и дуальная функция $\hat{f}(\alpha) \in T^G$ определяется равенством

$$\sqrt{n}\hat{f}(\alpha) = \hat{f}(\alpha), \quad \alpha \in G.$$

Теорема 6. *Пусть $f \in BF(G)$, тогда $\tilde{f}$ также является бент-функцией, причем*

$$\tilde{\tilde{f}}(x) = f(x^{-1}), \quad x \in G.$$

Доказательство. Утверждение теоремы вытекает из определения дуальной бент-функции и известного свойства преобразования Фурье

$$\hat{\hat{f}}(x) = nf(x^{-1}).$$

Важный пример явного выражения дуальной бент-функции приведен ниже.

Естественно теперь ввести следующее понятие. Зафиксируем некоторую константу $\varepsilon \in T$. Функцию $f \in BF(G)$ назовем ε -самодуальной, если

$$\tilde{f}(\alpha) = \varepsilon f(\alpha), \quad \alpha \in G.$$

Функции, являющиеся ε -самодуальными, — это собственные векторы матрицы $H(G)$ с собственным значением $\varepsilon\sqrt{n}$. В силу теоремы 6 для ε -самодуальной бент-функции f выполнены тождества

$$\varepsilon^2 f(x) = f(x^{-1}), \quad \varepsilon^4 = 1.$$

Определим множество обобщенных бент-функций $OBF(G) \subset \mathbf{C}^G$, отказавшись в определении бент-функции от ограничения $f \in T^G$ и рассматривая все функции из $\mathbf{C}^G$, так что

$$OBF(G) = \{f \in \mathbf{C}^G : |\hat{f}(\alpha)| = \sqrt{n}, \alpha \in G\}.$$

Для любой обобщенной бент-функции определена дуальная функция из T^G , причем очевидны следующие утверждения.

Лемма 3. *Переход к дуальной функции устанавливает взаимно однозначное соответствие между множествами функций $OBF(G)$ и T^G .*

Теорема 7. *Обобщенная бент-функция $f(x)$ является бент-функцией тогда и только тогда, когда дуальная функция $\tilde{f}(\alpha)$ удовлетворяет соотношениям ортогональности*

$$\sum_{\alpha \in G} \tilde{f}(\alpha) \tilde{f}(\alpha\beta^{-1}) = \begin{cases} 0, & \text{если } \beta \neq e, \\ n, & \text{если } \beta = e. \end{cases}$$

В условиях теоремы 7 дуальная функция $\tilde{f}(\alpha)$ также является бент-функцией (в силу теоремы 6) и поэтому теорема 7 дает другой вариант доказательства теоремы 1.

Функция $f \in T^G$ называется разложимой, если для некоторого представления группы G в виде прямого произведения $G = U \times V$ функция f имеет вид

$$f(u, v) = \varphi(u)\psi(v), \quad (u, v) \in G, \quad \varphi \in T^U, \quad \psi \in T^V,$$

то есть представляется в виде произведения функций-компонент, определенных на U и V соответственно. Например, характеры группы G являются разложимыми функциями для любого представления G в виде $G = U \times V$. Очевидно, что любая производная разложимой функции есть произведение производных компонент и преобразование Фурье разложимой функции есть произведение преобразований Фурье компонент. Отсюда вытекает следующее утверждение.

Теорема 8. *Если $f \in T^G$ — разложимая функция и $f(u, v) = \varphi(u)\psi(v)$, то $f \in UF(G)$ тогда и только тогда, когда или $\varphi \in UF(U)$, или $\psi \in UF(V)$, и $f \in BF(G)$ тогда и только тогда, когда и $\varphi \in BF(U)$, и $\psi \in BF(V)$.*

4. Кусочно-аффинные функции

При использовании аппарата гармонического анализа проще всего работать с функциями, составленными каким-нибудь образом из характеров группы и характеристических функций подгрупп. В этом случае легко находится преобразование Фурье и упрощается анализ функций. Широкий класс таких функций составляют кусочно-линейные и кусочно-аффинные функции. Пусть

$$G = U \times V, \quad \nu: V \rightarrow U, \quad \varphi \in T^V.$$

Функцию $f \in T^G$, представимую в виде

$$f(y, z) = \chi_{\nu(z)}(y), \quad y \in U, \quad z \in V,$$

будем называть кусочно-линейной, а представимую в виде

$$f(y, z) = \varphi(z)\chi_{\nu(z)}(y), \quad y \in U, \quad z \in V,$$

будем называть кусочно-аффинной. Для данной функции $f \in T^G$ может быть несколько различных представлений в кусочно-линейной или кусочно-аффинной форме. При любом фиксировании $z = z_0 \in V$ функция $f(y, z_0)$ аффинна.

Для работы с преобразованиями Фурье кусочно-аффинных функций удобно ввести еще одно понятие, неполное преобразование Фурье. Для $M \subseteq G$, $f \in T^G$ неполным преобразованием Фурье $\hat{f}_M$ функции f по множеству M будем называть следующие суммы:

$$\hat{f}_M(\alpha) = \sum_{x \in M} f(x) \bar{\chi}_\alpha(x), \quad \alpha \in G.$$

Простейшие свойства $\hat{f}_M$ очевидны:

$$\begin{aligned}\hat{f}_G(\alpha) &= \hat{f}(\alpha), & \alpha \in G, \\ \hat{f}_{\{x_0\}}(\alpha) &= f(x_0)\bar{\chi}_\alpha(x_0), & \alpha, x_0 \in G, \\ \hat{f}_\emptyset(\alpha) &= 0, & \alpha \in G, \\ \hat{f}_M(\alpha) &= \hat{f}_{M_1}(\alpha) + \hat{f}_{M_2}(\alpha), & \alpha \in G,\end{aligned}$$

где $M = M_1 \cup M_2$, $M_1 \cap M_2 = \emptyset$.

Лемма 4. Пусть $f(y, z) = \varphi(z)\chi_{\nu(z)}(y) \in T^G$. Тогда для всех $\alpha \in U$, $\beta \in V$

$$\hat{f}(\alpha, \beta) = |U|\hat{\varphi}_{\nu^{-1}(\alpha)}(\beta),$$

Доказательство. Пользуясь тем, что в условиях леммы

$$\chi_{(\alpha, \beta)}(y, z) = \chi_\alpha(y)\chi_\beta(z),$$

путем простых преобразований получаем, что

$$\begin{aligned}\hat{f}(\alpha, \beta) &= \sum_{(y, z) \in G} \varphi(z)\chi_{\nu(z)}(y)\bar{\chi}_{(\alpha, \beta)}(y, z) \\ &= \sum_{z \in V} \varphi(z)\bar{\chi}_\beta(z) \sum_{y \in U} \chi_{\nu(z)}(y)\bar{\chi}_\alpha(y) \\ &= |U| \sum_{z \in V, \nu(z) = \alpha} \varphi(z)\bar{\chi}_\beta(z) = |U|\hat{\varphi}_{\nu^{-1}(\alpha)}(\beta).\end{aligned}$$

Отметим следующее полезное наблюдение. Если отображение ν не сюръективно, то многие коэффициенты Фурье $\hat{f}(\alpha, \beta)$ обращаются в нуль: $\hat{f}(\alpha_0, \beta) = 0$ для всех $\beta \in V$ и $\alpha \in U$ таких, что $\nu^{-1}(\alpha) = \emptyset$.

Теорема 9. Включение $f(y, z) = \varphi(z)\chi_{\nu(z)}(y) \in BF(G)$ справедливо тогда и только тогда, когда

- (1) $|\nu^{-1}(\alpha)| = |V|/|U|$ для всех $\alpha \in U$;
- (2) $|\hat{\varphi}_{\nu^{-1}(\alpha)}(\beta)| = \sqrt{|V|/|U|}$ для всех $\alpha \in U$, $\beta \in V$.

Доказательство. Пусть $f(y, z) \in BF(G)$. Вычислим

$$\widehat{\frac{df}{d(u, \mathbf{e})}}(\mathbf{e}, \mathbf{e}), \quad u \in U, \quad u \neq \mathbf{e}.$$

Ясно, что

$$\frac{df}{d(u, \mathbf{e})}(y, z) = \bar{\varphi}(z)\bar{\chi}_{\nu(z)}(y)\varphi(z)\chi_{\nu(z)}(uy) = \chi_{\nu(z)}(u),$$

поэтому

$$\widehat{\frac{df}{d(u, \mathbf{e})}}(\mathbf{e}, \mathbf{e}) = |U| \sum_{z \in V} \chi_{\nu(z)}(u) = |U| \sum_{\alpha \in U} |\nu^{-1}(\alpha)|\chi_\alpha(u).$$

Теперь достаточно воспользоваться свойствами системы характеров и получить, что из условия

$$\widehat{\frac{df}{d(u, e)}}(e, e) = 0, \quad u \in U, \quad u \neq e$$

вытекает условие

$$|\nu^{-1}(\alpha)| = \frac{|V|}{|U|}, \quad \alpha \in U.$$

Теперь воспользуемся леммой 4 и из условия $|\hat{f}(\alpha, \beta)| = \sqrt{|U||V|}$ получим, что $|\hat{\varphi}_{\nu^{-1}(\alpha)}(\beta)| = \sqrt{|V|/|U|}$. Обратное утверждение теоремы очевидным образом следует из леммы 4.

В белевом случае теорема 9 доказана в работе [24].

Следствие 3. Пусть $f(y, z) = \varphi(z)\chi_{\nu(z)}(y) \in BF(G)$, а $\pi: U \rightarrow U$ — взаимно однозначное отображение. Тогда

$$F(y, z) = \varphi(z)\chi_{\pi\nu(z)}(y) \in BF(G).$$

Доказательство. Условия (1) и (2) теоремы 9 выполнены для функции $F(y, z)$, поскольку они выполнены для функции $f(y, z)$, а взаимно однозначное отображение π переставляет все блоки $\nu^{-1}(\alpha)$:

$$(\pi\nu)^{-1}(\alpha) = \nu^{-1}(\pi^{-1}\alpha).$$

Следствие 3 позволяет из одной кусочно-аффинной бент-функции получать достаточно большой класс бент-функций за счет свободы выбора произвольного взаимно однозначного отображения $\pi: U \rightarrow U$.

Два частных случая теоремы 9 представляют особый интерес.

Следствие 4. Включение $f(y, z) = \chi_{\nu(z)}(y) \in BF(G)$ справедливо тогда и только тогда, когда отображение ν взаимно однозначно.

Доказательство. При $\varphi(z) \equiv 1$ условие (2) теоремы 9 может выполняться только при $|V|/|U| = 1$.

Следствие 5. Пусть $|G| = k^2$, $|U| = k$, $\nu: V \rightarrow U$ — взаимно однозначное отображение. Тогда $f(y, z) = \varphi(z)\chi_{\nu(z)}(y) \in BF(G)$ для любой функции $\varphi \in T^V$. Дуальная к f функция имеет вид

$$\tilde{f}(y, z) = \varphi(\nu^{-1}(y))\chi_{\nu^{-1}(y)}(z^{-1}).$$

Доказательство. При $|\nu^{-1}(\alpha)| = 1$ условие (2) теоремы 9 выполняется для любой функции $y \in T^V$, при этом в соответствии с леммой 4

$$\hat{f}(\alpha, \beta) = \sqrt{|G|}\varphi(\nu^{-1}(\alpha))\bar{\chi}_{\beta}(\nu^{-1}(\alpha)), \quad (\alpha, \beta) \in G.$$

Отсюда получается требуемое выражение для дуальной функции.

В булевом случае класс бент-функций, описанный следствием 4, был введен впервые в работе [1] и назван классом $\mathbf{M}$ бент-функций. Этот класс достаточно большой за счет свободы выбора произвольного взаимно однозначного отображения $\nu: V \rightarrow U$ и произвольной функции $\varphi \in T^V$.

Из следствия 5 легко также увидеть, что самодуальными среди таких бент-функций являются только некоторые квадратичные бент-функции.

В силу условия (2) теоремы 9 функцию $\varphi \in T^V$ естественно назвать частичной бент-функцией на множествах $\nu^{-1}(\alpha)$, $\alpha \in U$. В таких терминах теорему 9 можно сформулировать следующим образом: функция $f(y, z) = \varphi(z)\chi_{\nu(z)}(y)$ является бент-функцией тогда и только тогда, когда все прообразы $\nu^{-1}(\alpha)$, $\alpha \in U$, равномощны и функция φ на каждом из них является частичной бент-функцией. Для частичных бент-функций можно получить аналог теоремы 1. Положим

$$\widehat{\frac{d\varphi}{d\sigma}}(\mathbf{e})|_M = \sum_{x \in M: \sigma x \in M} \bar{\varphi}(x)\varphi(\sigma x).$$

Получим для неполного преобразования Фурье некоторые полезные тождества, например, аналог равенства Парсеваля.

Лемма 5. Для любых $M \subseteq G$, $\varphi \in T^G$ имеют место следующие тождества:

$$\begin{aligned} \sum_{\alpha \in G} |\hat{\varphi}_M(\alpha)|^2 &= n|M|, \\ \sum_{\sigma \neq \mathbf{e}} \left| \widehat{\frac{d\varphi}{d\sigma}}(\mathbf{e})|_M \right|^2 &= \frac{1}{n} \sum_{\alpha \in G} (|\hat{\varphi}_M(\alpha)|^2 - |M|)^2. \end{aligned}$$

Доказательство. Из определения неполного преобразования Фурье следует, что

$$\begin{aligned} |\hat{\varphi}_M(\alpha)|^2 &= \sum_{x \in M} \varphi(x) \bar{\chi}_\alpha(x) \sum_{y \in M} \bar{\varphi}(y) \chi_\alpha(y) \\ &= \sum_{x, y \in M} \varphi(x) \bar{\varphi}(y) \chi_\alpha(x^{-1}y). \end{aligned}$$

Суммируя по всем $\alpha \in G$ и пользуясь соотношением ортогональности для характеров, приходим к первому тождеству:

$$\begin{aligned} \sum_{\alpha \in G} |\hat{\varphi}_M(\alpha)|^2 &= \sum_{x, y \in M} \varphi(x) \bar{\varphi}(y) \sum_{\alpha \in G} \chi_\alpha(x^{-1}y) \\ &= n \sum_{x \in M} \varphi(x) \bar{\varphi}(x) = n|M|. \end{aligned}$$

Аналогичными приемами получим вспомогательное тождество

$$\begin{aligned} \sum_{\alpha \in G} |\hat{\varphi}_M(\alpha)|^4 &= \sum_{x, y, u, v \in M} \varphi(x) \bar{\varphi}(y) \varphi(v) \bar{\varphi}(u) \sum_{\alpha \in G} \chi_\alpha(x^{-1}y v^{-1}u) \\ &= n \sum_{\sigma \in G} \sum_{x, \sigma x, u, \sigma u \in M} \varphi(x) \bar{\varphi}(\sigma x) \bar{\varphi}(u) \varphi(\sigma u) \\ &= n|M|^2 + n \sum_{\sigma \neq \mathbf{e}} \sum_{x, \sigma x, u, \sigma u \in M} \varphi(x) \bar{\varphi}(\sigma x) \bar{\varphi}(u) \varphi(\sigma u). \end{aligned}$$

Теперь легко увидеть, что второе слагаемое в последней сумме равно

$$n \sum_{\sigma \neq e} \left| \widehat{\frac{d\varphi}{d\sigma}}(e)|_M \right|^2.$$

Объединяя полученные соотношения, приходим ко второму тождеству:

$$\begin{aligned} \sum_{\alpha \in G} (|\hat{\varphi}_M(\alpha)|^2 - |M|)^2 &= \sum_{\alpha \in G} (|\hat{\varphi}_M(\alpha)|^4 - 2|M||\hat{\varphi}_M(\alpha)|^2 + |M|^2) \\ &= \sum_{\alpha \in G} |\hat{\varphi}_M(\alpha)|^4 - 2|M| \sum_{\alpha \in G} |\hat{\varphi}_M(\alpha)|^2 + n|M|^2 \\ &= n|M|^2 + n \sum_{\sigma \neq e} \left| \widehat{\frac{d\varphi}{d\sigma}}(e)|_M \right|^2 - 2n|M|^2 + n|M|^2. \end{aligned}$$

Из леммы 5 очевидно вытекает аналог теоремы 1.

Теорема 10. Функция $\varphi \in T^G$ является частичной бент-функцией на множестве $M \subseteq G$ тогда и только тогда, когда

$$\widehat{\frac{d\varphi}{d\sigma}}(e)|_M = 0, \quad \sigma \in G \setminus e.$$

Большие классы бент-функций можно строить, используя уже известные бент-функции. Уникальными в этом смысле являются квадратичные бент-функции, их значение уже отмечалось при рассмотрении бент-базисов, а также в лемме 2. Поскольку производные квадратичной бент-функции — все характеры, возможно с некоторыми константами, то легко получать бент-функции, умножая некоторые функции на квадратичные бент-функции.

Теорема 11. Пусть $q(x) \in RM_2(G) \cap BF(G)$, причем

$$\frac{dq}{d\sigma}(x) = c_\sigma \bar{\chi}_{\nu(\sigma)}(x)$$

с некоторой константой $c_\sigma \in T_m$ и некоторым взаимно однозначным отображением $\nu: G \rightarrow G$. Функция $q(x)f(x)$ является бент-функцией тогда и только тогда, когда

$$\widehat{\frac{df}{d\sigma}}(\nu(\sigma)) = 0, \quad \sigma \in G, \quad \sigma \neq e.$$

Доказательство. Ясно, что

$$\frac{d(qf)}{d\sigma}(x) = \frac{dq}{d\sigma}(x) \frac{df}{d\sigma}(x) = c_\sigma \bar{\chi}_{\nu(\sigma)}(x) \frac{df}{d\sigma}(x),$$

а эта функция является уравновешенной при $\sigma \neq e$ тогда и только тогда, когда

$$\widehat{\frac{df}{d\sigma}}(\nu(\sigma)) = 0, \quad \sigma \in G, \quad \sigma \neq e.$$

Список литературы

1. Rothaus O. S. On "bent" functions. *J. Comb. Theory*, Ser. A (1976) **20**, №3, 300–305.
2. McFarland R. A family of difference sets in noncyclic groups. *J. Comb. Theory*, Ser. A (1973) **15**, №1, 1–10.
3. Dillon J. F. A survey of bent functions. *The NSA Technical J.* (1972), 191–215.
4. Dillon J. F. Elementary Hadamard difference sets, *Ph. D. Dissertation*. Univ. Maryland, (1974).
5. Carlet C. Two new classes of bent functions, *Advances in Cryptology, Proc. EURO-CRYPT'93, Lect. Notes Computer Sci.* (1994) **765**, 77–101.
6. Carlet C. Generalized partial spreads, *IEEE Trans. Inform. Theory* (1995) **41**, №5, 1482–1487.
7. Carlet C. A construction of bent functions. *Proc. Seventh Joint Swedish-Russian Intern. Workshop Inform. Theory*. St.-Petersburg, Russia, 1995, 57–59.
8. Carlet C., Guillot Ph. A characterization of binary bent functions. *Proc. Fifth Intern. Workshop*. Sozopol, Bulgaria, 1996, 86–92.
9. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. *Теория кодов, исправляющих ошибки*. Связь, Москва, 1979.
10. Carlet C., Seberry J., Zhang X. M. Comments on "Generating and counting binary bent sequences". *IEEE Trans. Inform. Theory* (1994) **40**, №2, 600.
11. Gold R. Optimal binary sequences for spread-spectrum multiplexing. *IEEE Trans. Inform. Theory* (1967) **13**, №4, 619–621.
12. Lempel A., Cohn M. Maximal families of bent sequences. *IEEE Trans. Inform. Theory* (1982) **IT-28**, №6, 865–868.
13. Olsen J. D., Scholtz R. A., Welch L. R. Bent-function sequences. *IEEE Trans. Inform. Theory* (1982) **IT-28**, №6, 858–864.
14. Yarlagadda R., Hershey J. E. Analysis and synthesis of bent sequences. *IEE Proc.* (1989) **136**, N 2.
15. Carlet C. Hyper-bent functions. *Proc. PRAGOCRYPT'96*, CTU, GC UCMP, 145–155.
16. Carlet C. Partially-bent functions. *Advances in Cryptology, Proc. CRYPTO'92, Lect. Notes Computer Sci.* (1993) **740**, 280–291.
17. Chung H., Kumar P. V. A new general construction for generalized bent functions. *IEEE Trans. Inform. Theory* (1989) **35**, №1, 206–209.
18. Kumar P. V., Scholtz R. A., Welch L. R. Generalized bent functions and their properties. *J. Comb. Theory*, Ser. A, (1985) **40**, 90–107.
19. Амбросимов А. С. Свойства бент-функций q -значной логики над конечными полями. *Дискретная математика* (1994) **6**, №3, 50–60.
20. Кузнецов Ю. В., Шкарин С. А. Коды Риды–Маллера (обзор публикаций). *Матем. вопросы кибернетики*. (1996) **6**, 5–50.
21. Хьюитт Э., Росс К. *Абстрактный гармонический анализ*, том 1. Наука, Москва, 1975, том 2. Мир, Москва, 1975.
22. Логачев О. А., Ященко В. В. Коды типа Риды–Маллера на конечной абелевой группе. *Синтез и сложность управляющих систем*. Нижегородский госуниверситет, Нижний Новгород, 1996.

23. Seberry J., Zhang X. M., Zheng Y. Structures of cryptographic functions with strong avalanche characteristics. *Advances in Cryptology, Proc. ASIACRYPT'94, Lect. Notes Computer Sci.* (1995) **864**, 96–106.
24. Яценко В. В. О критерии распространения для булевых функций и бент-функциях. *Пробл. передачи информации* (1997) **33**, №1, 52–63.