ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь–декабрь 2019. Т. 26, № 4. С. 121–131

УДК 519.7 DOI 10.33048/daio.2019.26.649

СВЯЗЬ ОДНОРОДНЫХ БЕНТ-ФУНКЦИЙ И ГРАФОВ НЭГИ *)

А. С. Шапоренко[1,2]

[1] Новосибирский гос. университет,
ул. Пирогова, 2, 630090, Новосибирск, Россия

[2] JetBrains Research,
ул. Пирогова, 1, 630090, Новосибирск, Россия

E-mail: shaporenko.alexandr@gmail.com

Аннотация. Исследуется связь однородных бент-функций и графов пересечений специального вида, которые называются графами Нэги и обозначаются через $\Gamma_{(n,k)}$. Граф $\Gamma_{(n,k)}$ — граф, вершины которого соответствуют $\binom{n}{k}$ неупорядоченным подмножествам размера k множества $\{1,\ldots,n\}$. Две вершины такого графа соединены ребром в том и только том случае, если рассматриваемые подмножества размера k имеют в точности один общий элемент. Были выделены те значения n и k, при которых в графе $\Gamma_{(n,k)}$ клики размера $k+1$ максимальны. Получена формула для числа клик размера $k+1$ в графе $\Gamma_{(n,k)}$ для $n = \frac{(k+1)k}{2}$. Доказано, что однородные булевы функции от 10 и 28 переменных, полученные путём взятия дополнения к кликам максимального размера в графах $\Gamma_{(10,4)}$ и $\Gamma_{(28,7)}$ соответственно, не являются бент-функциями. Табл. 3, ил. 2, библиогр. 9.

Ключевые слова: граф пересечений, граф Нэги, однородная бент-функция, клика максимального размера.

Введение

В настоящей работе исследуется связь однородных бент-функций и графов пересечений специального вида, которые называются графами Нэги и обозначаются через $\Gamma_{(n,k)}$.

Бент-функции — класс булевых функций, обладающих экстремальными свойствами нелинейности [1]. Свойство линейности функции, как

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект № 18–07–01394) и Министерства образования и науки РФ (задание № 1.13559.2019/13.1 и Программа 5–100).

правило, является источником информации о многих других её свойствах, а также свидетельствует о простой структуре этой функции, поэтому мера нелинейности — одна из важнейших характеристик булевой функции в криптографии. Бент-функции используются в создании блочных и поточных шифров для повышения стойкости этих шифров к методам линейного и дифференциального криптоанализа.

Однородные бент-функции — это подкласс бент-функций, который был выделен авторами [2] как состоящий из функций с относительно простой алгебраической нормальной формой. Вопрос о классификации однородных бент-функций до сих пор остаётся открытым.

В [3] было показано, как с помощью дополнения к кликам графа Нэги $\Gamma_{(6,3)}$ можно определять однородные бент-функции от шести переменных степени три.

В данной работе исследуются максимальные клики в графах $\Gamma_{(n,k)}$, а именно, мы ищем размер максимальных клик и их количество для некоторых n и k. Также докажем, что однородные булевы функции от 10 и 28 переменных, полученные путём взятия дополнения к кликам максимального размера в графах $\Gamma_{(10,4)}$ и $\Gamma_{(28,7)}$ соответственно, не являются бент-функциями.

Определение 1. Пусть $\mathbb{Z}_2 = \{0, 1\}$. Векторное пространство двоичных векторов длины n обозначается через $\mathbb{Z}_2^n$. Произвольная функция, действующая из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2$, называется *булевой функцией* от n переменных.

Определение 2. Пусть $\oplus$ обозначает сложение по модулю 2. Каждая булева функция однозначно может быть задана своей *алгебраической нормальной формой* (АНФ), а именно, представлена единственным образом в виде

$$f(v) = \left(\bigoplus_{k=1}^{n} \bigoplus_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} v_{i_1} \ldots v_{i_k} \right) \oplus a_0,$$

где при каждом k индексы $i_1, \ldots, i_k$ различны и в совокупности пробегают все k-элементные подмножества $\{1, \ldots, n\}$. Коэффициенты $a_{i_1}, \ldots, a_{i_k}, a_0$ принимают значения 0 или 1.

Определение 3. *Расстояние Хэмминга* $\mathrm{dist}(f, g)$ между булевыми функциями f и g — это число координат, в которых различаются векторы их значений.

Определение 4. *Степенью нелинейности* $\deg(f)$ булевой функции f называется число переменных в самом длинном слагаемом её АНФ. Функция называется *аффинной*, если её степень не больше 1.

Определение 5. *Бент-функцией* называется булева функция от n переменных (n чётно) такая, что расстояние Хэмминга N_f от данной функции до множества всех аффинных функций является максимально возможным.

Определение 6. Булева функция называется *однородной*, если все одночлены её АНФ имеют одинаковые степени.

1. Исследование бент-функций с помощью графов

В данном разделе представлены примеры использования различных графов для исследования и классификации бент-функций.

В [4] был предложен способ классификации бент-функций с помощью сильно регулярных графов.

Определение 7. Через $\mathrm{supp}(f)$ обозначим *носитель* булевой функции f, т. е. множество всех двоичных векторов длины n, на которых функция f принимает значение 1.

Рассмотрим *граф Кэли* G_f булевой функции f. Вершинами графа являются все двоичные векторы длины n. Две вершины x и y соединены ребром, если вектор $x \oplus y$ принадлежит $\mathrm{supp}(f)$.

Определение 8. Регулярный граф G называется *сильно регулярным*, если существуют неотрицательные целые числа λ и μ такие, что для любых двух вершин x и y число общих смежных им вершин равно λ или μ в зависимости от того, соединены вершины x, y ребром или нет.

В [5] было доказано, что булева функция f является бент-функцией тогда и только тогда, когда граф G_f сильно регулярный, причём $\lambda = \mu$.

Рассмотрим граф GB_n, вершинами которого являются бент-функции от n переменных, где рёбрами соединены функции, находящиеся на минимально возможном расстоянии $2^{n/2}$ друг от друга. В [6] доказано, что число бент-функций, которые находятся на расстоянии $2^{n/2}$ от f, где f — бент-функция от n переменных, не больше чем $2^{n/2} \prod_{i=1}^{n/2} (2^i+1)$. Оценка достигается тогда и только тогда, когда f — квадратичная бент-функция. В [7] доказано, что GB_n связный для $n = 2, 4, 6$.

Графами квадратичных бент-функций от шести переменных называются графы на шести вершинах, каждая из которых соответствует одной из шести переменных функции. Если две вершины соединены ребром, то в АНФ функции есть произведение соответствующих переменных. В 2013 г. Е. П. Корсаковой была получена классификация таких графов [8]: существует ровно 45 графов неэквивалентных бент-функций и 37 различных типов графов (тип определяется списком степеней вершин).

2. Графы Нэги

Определение 9. В [3] был определён *граф Нэги* $\Gamma_{(n,k)}$, вершины которого соответствуют $\binom{n}{k}$ неупорядоченным подмножествам размера k множества $\{1,\ldots,n\}$. Две вершины такого графа соединены ребром в том и только том случае, если рассматриваемые подмножества размера k имеют в точности один общий элемент.

Определение 10. Будем называть *дополнением* к клике графа $\Gamma_{(n,k)}$ множество всех вершин этого графа, которые не входят в рассматриваемую клику.

Пример 1. Рассмотрим случай $n = 6$, $k = 3$. В графе $\Gamma_{(6,3)}$ 20 вершин вида $\{a, b, c\}$, где $a, b, c \in \{1,\ldots,6\}$ различны. В этом графе были выделены клики размера $4 = k + 1$, и, как указано в [3], такой размер клики является максимальным. Всего в графе $\Gamma_{(6,3)}$ насчитывается 30 таких клик.

В графе $\Gamma_{(6,3)}$ дополнением к клике C (рис. 1) с вершинами $\{1,3,6\}$, $\{1,4,5\}$, $\{2,3,5\}$ и $\{2,4,6\}$ будет множество, состоящее из 16 вершин (всех вершин $\Gamma_{(6,3)}$, кроме указанных четырёх). Если будем сопоставлять вершине $\{\ell, m, s\}$ одночлен $x_\ell x_m x_s$, где $\ell, m, s = 1,\ldots,6$, то 16 вершин из дополнения к клике C будут соответствовать 16 одночленам алгебраической нормальной формы однородной бент-функции от 6 переменных степени 3 [2]. Поскольку таких клик 30 (равно как и однородных бент-

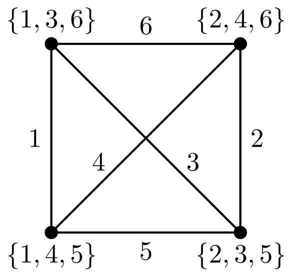

Рис. 1. Клика размера 4 в графе $\Gamma_{(6,3)}$

функций от 6 переменных степени 3 [2]), справедливо, что 30 однородных бент-функций от 6 переменных находятся во взаимно однозначном соответствии с дополнениями клик (максимальных) C_i графа $\Gamma_{(6,3)}$, где $i = 1,\ldots,30$.

Возникает вопрос о возможности классификации однородных бент-функций от большего числа переменных с помощью выделения некоторого подмножества множества вершин графа $\Gamma_{(n,k)}$.

Замечание 1. В качестве такого подмножества, как и в случае графа $\Gamma_{(6,3)}$, будем рассматривать дополнение к клике максимального размера.

3. Клики максимального размера в графе $\Gamma_{(n,k)}$

В графе $\Gamma_{(6,3)}$ максимальными будут клики размера $k+1$. Всегда ли в графе $\Gamma_{(n,k)}$ существует клика размера $k+1$, и если такая клика найдётся, будет ли она максимальной?

Утверждение 1. *В графе $\Gamma_{(n,k)}$, где n и k — положительные целые числа, не всегда найдётся клика размера $k+1$.*

Доказательство. Рассмотрим граф $\Gamma_{(12,5)}$. Пусть в графе существует клика размера $k+1$. Пронумеруем все вершины клики и введём обозначение a_i для числа элементов i-й вершины, которые не являются общими ни для одной из предыдущих $i-1$ вершин. Так, a_1 будет равно пяти, а a_2 — четырём. Для третьей вершины это число будет равно трём, если общие элементы этой вершины с первой и второй не равны, и четырём в противном случае. Остальные значения a_i приведены в табл. 1.

Таблица 1

i	a_i	i	a_i
1	5	4	$\geqslant 2$
2	4	5	$\geqslant 1$
3	$\geqslant 3$	6	$\geqslant 0$

Сумма всех a_i не должна превосходить $n = 12$. В нашем случае

$$\sum_{i=1}^{6} a_i \geqslant 15,$$

следовательно, клики размера $k+1$ в графе $\Gamma_{12,5}$ не существует. Утверждение 1 доказано.

Пример 2. Рассмотрим граф $\Gamma_{(8,3)}$. В этом графе существует клика размера 7 (рис. 2). Значит, если в графе $\Gamma_{(n,k)}$ существует клика размера $k+1$, она не всегда будет максимальной.

Теорема 1. *Пусть $n = \frac{(k+1)k}{2}$, где $k > 1$. Тогда максимальный размер клики в графе $\Gamma_{(n,k)}$ равен $k+1$.*

Доказательство. Найдём клику размера $k+1$ явно, тем самым покажем, что клика такого размера существует в графе $\Gamma_{(n,k)}$. Пронумеруем и поместим все $k+1$ вершин в табл. 2. Пусть a_i — число элементов i-й вершины, которые не являются общими ни для одной из предыдущих $i-1$ вершин.

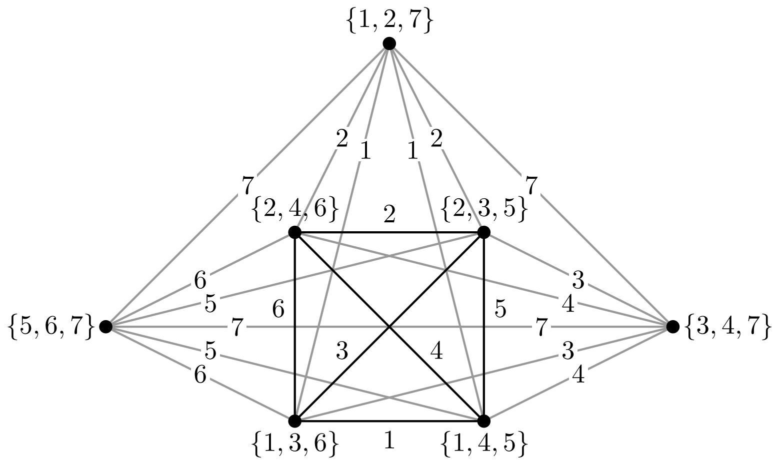

Рис. 2. Клика размера 7 в графе $\Gamma_{(8,3)}$

Таблица 2

i	i-я вершина	a_i
1	$\{1, 2, 3, \ldots, k\}$	k
2	$\{1, k+1, k+2, \ldots, 2k-1\}$	$k-1$
3	$\{2, k+1, 2k, 2k+1, \ldots, 3k-3\}$	$k-2$
4	$\{3, k+2, 2k, 3k-2, 3k-1, \ldots, 4k-6\}$	$k-3$
$\ldots$	$\ldots$	$\ldots$
ℓ	$\{\ell-1, k+\ell-2, 2k+\ell-4, \ldots, \ell k-1-2-\cdots-\ell+1\}$	$k-\ell+1$
$\ldots$	$\ldots$	$\ldots$
$k+1$	$\{k, 2k-1, 3k-3, \ldots, (k+1)k-1-2-\cdots-k\}$	0

Сумма всех a_i не должна превышать n. Пользуясь формулой суммы первых k элементов арифметической прогрессии, получаем

$$k + (k-1) + \cdots + 2 + 1 = \frac{(k+1)k}{2} = n. \tag{1}$$

Также нужно убедиться, что все элементы каждой вершины действительно являются элементами множества $\{1, \ldots, n\}$. В приведённой клике каждый элемент вершины i больше или равен (в случае, если этот элемент общий) всех элементов предыдущих $i-1$ вершин. Кроме того, элементы любой вершины упорядочены по возрастанию. Следовательно, достаточно проверить, что последний элемент $(k+1)$-й вершины не превосходит n. Используя формулу (1), получаем, что последний элемент $(k+1)$-й вершины равен n.

Теперь покажем, что клики большего размера в графе $\Gamma_{(n,k)}$ быть не может. Предположим, напротив, что в графе $\Gamma_{(n,k)}$ существует клика размера $k+2$. Тогда любая вершина должна иметь общие элементы с $k+1$ вершинами. Каждая вершина содержит только k элементов, следовательно, есть две другие вершины, которые имеют с ней один и тот же общий элемент.

Как и в случае клики размера $k+1$, пронумеруем все вершины. Без ограничения общности в качестве первых трёх вершин возьмём указанные в табл. 3.

Таблица 3

i	i-я вершина	a_i
1	$\{1, 2, 3, \ldots, k\}$	k
2	$\{1, k+1, k+2, \ldots, 2k-1\}$	$k-1$
3	$\{1, 2k, 2k+1, \ldots, 3k-2\}$	$k-1$
$\ldots$	$\ldots$	$\ldots$

Так как $a_3 > k-2$, а все остальные a_i не меньше, чем в случае клики размера $k+1$, сумма всех a_i будет превосходить n. Стало быть, клики размера $k+2$ в графе $\Gamma_{(n,k)}$ не существует. Теорема 1 доказана.

Следствие 1. *При $n = \frac{(k+1)k}{2}$, где $k > 1$, клики максимального размера не содержат более двух вершин, которые имеют один и тот же общий элемент.*

Замечание 2. $\Gamma_{(6,3)}$ принадлежит к числу тех графов $\Gamma_{(n,k)}$, для которых справедливо равенство $n = \frac{(k+1)k}{2}$.

При n, равном $\frac{(k+1)k}{2}$, количество рёбер в клике размера $k+1$ будет равно n. Кроме того, если будем помечать каждое ребро значением элемента, который является общим для двух вершин, между которыми это ребро проведено, то (как видно на рис. 1) согласно следствию 1 в кликах не будет рёбер, помеченных одинаковыми значениями. Таким образом, рёбра помечаются значениями от 1 до n.

Теорема 2. *Пусть $n = \frac{(k+1)k}{2}$, где $k > 1$. Тогда в графе $\Gamma_{(n,k)}$ число клик размера $k+1$ равно $\frac{n!}{(k+1)!}$.*

Доказательство. Пусть d — число всех клик графа $\Gamma_{(n,k)}$, содержащих одну конкретную вершину. Заметим, что это число не зависит от выбора вершины. Определить общее количество клик размера $k+1$ в графе $\Gamma_{(n,k)}$ можно с помощью формулы $\frac{C_n^k \cdot d}{k+1}$.

Рассмотрим клику размера $k+1$. Без ограничения общности будем считать, что одной из вершин этой клики будет множество $\{1, \ldots, k\}$. Эта вершина соединена с другими k вершинами рёбрами, каждое из которых помечено одним из k элементов множества, соответствующего первой вершине. Остальные $n-k$ рёбер будут помечены значениями из множества $\{k+1,\ldots,n\}$. Все различные клики размера $k+1$, содержащие вершину $\{1,\ldots,k\}$, будут отличаться между собой значениями, которыми помечены упомянутые выше $n-k$ рёбер. Эти $n-k$ рёбер могут быть помечены $n-k$ оставшимися значениями в любом порядке, поэтому общее число способов пометить эти рёбра, а следовательно, количество клик графа $\Gamma_{(n,k)}$, содержащих одну конкретную вершину, равно $(n-k)!$. Таким образом, в графе $\Gamma_{(n,k)}$, где $n=\frac{(k+1)k}{2}$, число всех клик размера $k+1$ равно

$$\frac{C_n^k\cdot d}{k+1}=\frac{\frac{n!}{k!(n-k)!}\cdot(n-k)!}{k+1}=\frac{n!}{k!(k+1)}=\frac{n!}{(k+1)!}.$$

Теорема 2 доказана.

4. Однородные булевы функции от 10 и 28 переменных

Рассмотрим граф $\Gamma_{(10,4)}$. Условие $n=\frac{(k+1)k}{2}$ выполнено, следовательно, максимальный размер клики в этом графе равен 5. Построим однородную булеву функцию от 10 переменных и проверим, является ли она бент-функцией. Для этого исключаем из множества всех вершин графа $\Gamma_{(10,4)}$ пять, которые являются вершинами заранее выбранной клики. Далее нужно составить функцию, соответствующую множеству оставшихся вершин. Делается это следующим образом: каждой вершине $\{\ell,m,r,s\}$ сопоставляем одночлен $x_\ell x_m x_r x_s$, где $\ell,m,r,s=1,\ldots,n$, затем все одночлены суммируются по модулю два. Полученная функция будет являться алгебраической нормальной формой булевой функции.

Была выбрана клика с вершинами $\{1,2,3,4\}$, $\{1,5,6,7\}$, $\{2,5,8,9\}$, $\{3,6,8,10\}$ и $\{4,7,9,10\}$. Граф $\Gamma_{(10,4)}$ имеет 210 вершин, следовательно, АНФ нашей функции будет состоять из 205 одночленов. Для того чтобы проверить, будет ли эта функция бент-функцией, было рассмотрено преобразование Уолша — Адамара:

$$W_f(v)=\sum_{u\in\mathbb{Z}_2^n}(-1)^{\langle u,v\rangle\oplus f(u)}.$$

Для бент-функций модуль каждого коэффициента Уолша — Адамара (для любого вектора $v\in\mathbb{Z}_2^n$) должен быть равен $2^{\frac{n}{2}}$ [9]. Однако для полученной функции $W_f(\mathbf{0})=-232$. Поскольку $W_f(\mathbf{0})\neq 32$, заключаем, что полученная нами функция не является бент-функцией.

Компьютерные вычисления также показали, что булева функция от 28 переменных степени 7, полученная исключением из графа $\Gamma_{(28,7)}$ клики размера 8, также не будет бент-функцией.

Следующим шагом может быть рассмотрение таких графов $\Gamma_{(n,k)}$, где $n = \frac{(k+1)k}{2}$ чётно и больше 28. Однако проверить, будут ли однородные булевы функции, которые могут быть получены из таких графов описанным выше образом, бент-функциями — сложная в вычислительном смысле задача. Также имеет смысл рассмотреть большие значения n, при которых максимальный размер клики превосходит $k + 1$.

ЛИТЕРАТУРА

1. **Rothaus O. S.** On “bent” functions // J. Comb. Theory., Ser. A. 1976. Vol. 20, No. 3. P. 300–305.
2. **Qu C., Seberry J., Pieprzyk J.** Homogeneous bent functions // Discrete Appl. Math. 2000. Vol. 102, No. 1–2. P. 133–139.
3. **Charnes C., Rotteler M., Beth T.** Homogeneous bent functions, invariants, and designs // Des., Codes Cryptogr. 2002. Vol. 26, No. 1–2. P. 139–154.
4. **Bernasconi A, Codenotti B.** Spectral analysis of Boolean functions as a graph eigenvalue problem // IEEE Trans. Comput. 1999. Vol. 48, No. 3. P. 345–351.
5. **Bernasconi A., Codenotti B., Vanderkam J. M.** A characterization of bent functions in terms of strongly regular graphs // IEEE Trans. Comput. 2001. Vol. 50, No. 9. P. 984–985.
6. **Коломеец Н. А.** Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикл. дискрет. математика. 2014. № 3. С. 28–39.
7. **Коломеец Н. А.** О связности графа минимальных расстояний множества бент-функций // Прикл. дискрет. математика. Прил. 2015. № 8. С. 33–34.
8. **Корсакова Е. П.** Классификация графов квадратичных бент-функций от шести переменных // Дискрет. анализ и исслед. операций. 2013. Т. 20, № 5. С. 45–47.
9. **Tokareva N. N.** Bent functions: results and applications to cryptography. Amsterdam: Acad. Press, 2015. 220 p.

Шапоренко Александр Сергеевич

Статья поступила
25 февраля 2019 г.

После доработки —
1 августа 2019 г.

Принята к публикации
28 августа 2019 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
October–December 2019. Vol. 26, No. 4. P. 121–131

UDC 519.7 DOI 10.33048/daio.2019.26.649

RELATIONSHIP BETWEEN HOMOGENEOUS BENT FUNCTIONS AND NAGY GRAPHS *)

A. S. Shaporenko [1,2]

[1] Novosibirsk State University,
2 Pirogov Street, 630090, Novosibirsk, Russia

[2] JetBrains Research,
1 Pirogov Street, 630090, Novosibirsk, Russia

E-mail: shaporenko.alexandr@gmail.com

Abstract. We study the relationship between homogeneous bent functions and some intersection graphs of a special type that are called Nagy graphs and denoted by $\Gamma_{(n,k)}$. The graph $\Gamma_{(n,k)}$ is the graph whose vertices correspond to $\binom{n}{k}$ unordered subsets of size k of the set $\{1,\ldots,n\}$. Two vertices of $\Gamma_{(n,k)}$ are joined by an edge whenever the corresponding k-sets have exactly one common element. Those n and k for which the cliques of size $k+1$ are maximal in $\Gamma_{(n,k)}$ are identified. We obtain a formula for the number of cliques of size $k+1$ in $\Gamma_{(n,k)}$ for $n=(k+1)k/2$. We prove that homogeneous Boolean functions of 10 and 28 variables obtained by taking the complement to the cliques of maximal size in $\Gamma_{(10,4)}$ and $\Gamma_{(28,7)}$ respectively are not bent functions. Tab. 3, illustr. 2, bibliogr. 9.

Keywords: intersection graph, Nagy graph, homogeneous bent function, maximal clique.

REFERENCES

1. **O. S. Rothaus,** On “bent” functions, *J. Comb. Theory , Ser. A* **20** (3), 300–305 (1976).
2. **C. Qu, J. Seberry,** and **J. Pieprzyk,** Homogeneous bent functions, *Discrete Appl. Math.* **102** (1–2), 133–139 (2000).
3. **C. Charnes, M. Rotteler,** and **T. Beth,** Homogeneous bent functions, invariants, and designs, *Des. Codes Cryptogr.* **26** (1–2), 139–154 (2002).

*) This research is supported by the Russian Foundation for Basic Research (Project 18–07–01394) and the Ministry of Science and Higher Education of Russian Federation (Contract No. 1.13559.2019/13.1 and the Programme 5–100).

4. **A. Bernasconi** and **B. Codenotti,** Spectral analysis of Boolean functions as a graph eigenvalue problem, *IEEE Trans. Comput.* **48** (3), 345–351 (1999).
5. **A. Bernasconi, B. Codenotti,** and **J. M. Vanderkam,** A characterization of bent functions in terms of strongly regular graphs, *IEEE Trans. Comput.* **50** (9), 984–985 (2001).
6. **N. A. Kolomeec,** An upper bound for the number of bent functions at distance 2^k from an arbitrary bent function of $2k$ variables, *Prikl. Diskretn. Mat.,* No. 3, 28–39 (2014) [Russian].
7. **N. A. Kolomeec,** On connectivity of the minimal distance graph for the set of bent functions, *Prikl. Diskretn. Mat., Suppl.,* No. 8, 33–34 (2015) [Russian].
8. **E. P. Korsakova,** Some classification of the graphs for quadratic bent functions of 6 variables, *Diskretn. Anal. Issled. Oper.* **20** (5), 45–47 (2013) [Russian].
9. **N. Tokareva,** *Bent Functions: Results and Applications to Cryptography* (Acad. Press, Amsterdam, 2015).

Aleksandr S. Shaporenko

Received February 25, 2019
Revised August 1, 2019
Accepted August 28, 2019