ISSN 1561-2430 (Print)
ISSN 2524-2415 (Online)
УДК 519.118
https://doi.org/10.29235/1561-2430-2023-59-2-130-135

Поступила в редакцию 31.01.2023
Received 31.01.2023

С. В. Агиевич

НИИ прикладных проблем математики и информатики,
Белорусский государственный университет, Минск, Республика Беларусь

ОЦЕНКА СВЕРХУ ЧИСЛА БЕНТ-ФУНКЦИЙ С ПОМОЩЬЮ 2-СТРОЧНЫХ БЕНТ-ПРЯМОУГОЛЬНИКОВ

Аннотация. С помощью представления бент-функций (максимально нелинейных функций) бент-прямоугольниками (специальными матрицами с ограничениями на строки и столбцы) получена оценка сверху для числа бент-функций, которая улучшает ранее известные оценки в практическом диапазоне размерностей. Используется следующий факт, основанный на недавнем наблюдении В. Потапова (arXiv:2107.14583): 2-строчный бент-прямоугольник полностью определяется одной из своих строк и оставшимися значениями в немногим более половине столбцов.

Ключевые слова: бент-функция, бент-прямоугольник, почти-бент-функция, число бент-функций, спектр Уолша – Адамара

Для цитирования. Агиевич, С. В. Оценка сверху числа бент-функций с помощью 2-строчных бент-прямоугольников / С. В. Агиевич // Вес. Нац. акад. навук Беларусі. Сер. фіз.-мат. навук. – 2023. – Т. 59, № 2. – С. 130–135. https://doi.org/10.29235/1561-2430-2023-59-2-130-135

Sergey V. Agievich

Research Institute for Applied Problems of Mathematics and Informatics,
Belarusian State University, Minsk, Republic of Belarus

UPPER BOUNDING THE NUMBER OF BENT FUNCTIONS USING 2-ROW BENT RECTANGLES

Abstract. Using the representation of bent functions (maximum nonlinear functions) by bent rectangles, that is, special matrices with restrictions on columns and rows, we obtain herein an upper bound on the number of bent functions that improves the previously known bounds in a practical range of dimensions. The core of our method is the following fact based on the recent observation by V. Potapov (arXiv:2107.14583): a 2-row bent rectangle is completely determined by one of its rows and the remaining values in slightly more than half of the columns.

Keywords: bent function, bent rectangle, near-bent function, number of bent functions, Walsh – Hadamard spectrum

For citation. Agievich S. V. Upper bounding the number of bent functions using 2-row bent rectangles. *Vestsi Natsyyanal'nai akademii navuk Belarusi. Seryya fizika-matematychnykh navuk = Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics series*, 2023, vol. 59, no. 2, pp. 130–135 (in Russian). https://doi.org/10.29235/1561-2430-2023-59-2-130-135

1. Результаты. Пусть $\mathbb{F}_2$ – поле из двух элементов: 0 и 1. Булева функция $f:\mathbb{F}_2^n\to\mathbb{F}_2$ от четного числа переменных n называется *бент-функцией*, если $|\hat{f}(\mathbf{u})|=2^{n/2}$ для всех $\mathbf{u}\in\mathbb{F}_2^n$. Здесь $\hat{f}$ – *спектр* Уолша – Адамара функции f:

$$\hat{f}(\mathbf{u})=\sum_{x\in\mathbb{F}_2^n}\chi\bigl(f(\mathbf{x})+\mathbf{x}\cdot\mathbf{u}\bigr).$$

Символ χ под знаком суммы – это нетривиальный аддитивный характер $\mathbb{F}_2$: $\chi(a)=(-1)^a$, точка обозначает скалярное произведение векторов. Множество всех бент-функций от n переменных обозначим через $\mathcal{B}_n$. Очевидно, $\mathcal{B}_n$ непусто, только если n нечетно.

Бент-функции являются идеальными объектами в некоторых контекстах теории кодирования, криптографии и комбинаторики. Несмотря на интенсивные исследования, существует множество открытых проблем, связанных с бент-функциями. Одна из них – оценка $|\mathcal{B}_n|$ сверху и снизу (см. обсуждение в [1–3]). В настоящей работе нас интересуют оценки сверху.

Обозначим $B(n,d)=2^{\sum_{i=0}^{d}\binom{n}{i}}$ и напомним, что булева функция f однозначно представляется многочленом факторкольца $\mathbb{F}_2[x_1,\ldots,x_n]/\left(x_1^2-x_1,\ldots,x_n^2-x_n\right)$, который называется *алгебраической нормальной формой f* (или *многочленом Жегалкина* в русскоязычном контексте). Пусть $\deg f$ – степень многочлена.

Наивная оценка сверху (так она названа в работе [4]) для $|\mathcal{B}_n|$ основана на следующем факте, установленном в [5]: если $n\geq 4$ и $f\in\mathcal{B}_n$, то $\deg f\leq n/2$. Оценка имеет следующий вид:

$$|\mathcal{B}_n|\leq B(n,n/2)=2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}.$$

Оценка может быть немного усилена: следует учесть условие $2\leq\deg f$ и вычесть из правой части 2^{n+1} – число аффинных функций.

В [4] найдено более серьезное усиление

$$|\mathcal{B}_n|\leq\frac{B(n,n/2)}{2^{2^{n/2}-n/2-1}}(1+\varepsilon_n)+B(n,n/2-1),\qquad \varepsilon_n=\frac{1}{2^{\binom{n-1}{n/2-1}-2}},$$

справедливое при $n\geq 6$. При оценивании учитывается не только ограничение на $\deg f$, но и спектральное строение бент-функций.

В [6] для оценивания числа бент-функций предложено использовать их представление бент-прямоугольниками – специальными матрицами с ограничениями на строки и столбцы [7, 8]. Согласно [6], число бент-функций равняется числу 2-строчных бент-прямоугольников и, следовательно, не превосходит произведения (a) числа способов выбора одной из строк прямоугольника на (b) максимум числа способов доопределения бент-прямоугольника с фиксированной строкой. Полученная в [6] оценка лишь незначительно опережает оценку [4].

В работе [9] В. Потапов доказал, что число $|\mathcal{B}_n|$ ограничено сверху величиной, которая имеет асимптотическую форму

$$2^{3\cdot 2^{n-3}(1+o(1))},\qquad n\to\infty. \tag{1}$$

На самом деле В. Потапов нашел еще более точную оценку

$$2^{\alpha\cdot 2^{n-3}(1+o(1))},\quad \alpha=2+\frac{3}{8}\log_2 6\approx 2{,}96, \tag{2}$$

и упростил ее в самом конце своей работы. Оценка Потапова асимптотически намного опережает предыдущие, имеющие вид $2^{2^{n-1}(1+o(1))}$.

В настоящей работе нам удалось значительно усилить метод работы [6], применяя одну из идей работы [9]: оказывается, что на этапе (b) достаточно учитывать число способов доопределения не всех столбцов бент-прямоугольника, а немногим более их половины.

Мы получили следующий результат.

Т е о р е м а. *При четном $n\geq 6$ справедлива оценка*

$$|\mathcal{B}_n|\leq\sqrt{B(n-1,n/2)}\left(\frac{B(n-1,n/2)-B(n-1,n/2-1)}{2^{2^{n/2-1}-n/2+1}}+B(n-1,n/2-1)\right).$$

В таблице оценка теоремы проиллюстрирована для малых n. Точные значения $|\mathcal{B}_6|$ и $|\mathcal{B}_8|$, представленные в таблице, найдены соответственно в работах [10] и [11].

Оценки сверху для числа бент-функций от *n* переменных

Upper bounds on the number of bent functions in *n* variables

n	$\lvert\mathcal{B}_n\rvert$	Оценки сверху для $\lvert\mathcal{B}_n\rvert$		
		наивная	[4]	настоящая работа
2	8	–	–	–
4	896	2016	–	–
6	$5425430528 \approx 2^{32,3}$	2^{42}	2^{38}	2^{37}
8	$99270589265934370305785861242880 \approx 2^{106,3}$	2^{163}	2^{152}	$2^{143,5}$
10	Неизвестно	2^{638}	2^{612}	2^{561}
12	Неизвестно	2^{2510}	2^{2453}	2^{2202}

Оценка теоремы имеет форму (1) и, таким образом, асимптотически проигрывает оценке Потапова (2). Впрочем, дополнительный анализ, проведенный за пределами настоящей работы, показывает, что асимптотическое преимущество последней оценки начинает сказываться только при непрактично больших n (по крайней мере не меньших 5000).

В разделе 2 мы приводим необходимые факты о бент-прямоугольниках, а в разделе 3 доказываем теорему.

2. Бент-прямоугольники. Пусть n – четное число, записанное в виде $n = m + k$, где m и k – неотрицательные целые. Пусть f – булева функция от n переменных. Разобьем ее переменные на две части: $\mathbf{u} \in \mathbb{F}_2^m$ и $\mathbf{y} \in \mathbb{F}_2^k$. Фиксируя первую часть переменных всевозможными способами, получаем функции $f_{\mathbf{u}}(\mathbf{y}) = f(\mathbf{u},\mathbf{y})$. Применим к ним преобразование Уолша – Адамара и получим функцию

$$\overset{\square}{f}(\mathbf{u},\mathbf{v}) = \hat{f}_{\mathbf{u}}(\mathbf{v}), \qquad \mathbf{v} \in \mathbb{F}_2^k.$$

Она называется *прямоугольником f*. Сужение $\overset{\square}{f}(\mathbf{u},\mathbf{v})$ на $\mathbf{v}$ называется *строкой* $\overset{\square}{f}$, сужение на $\mathbf{u}$ при $\mathbf{v} = \mathbf{b}$ – *столбцом* (с номером $\mathbf{b}$). Строки и столбцы удобно задавать векторами своих значений, а весь прямоугольник $\overset{\square}{f}$ интерпретировать как матрицу.

По построению строки $\overset{\square}{f}$ являются спектрами функций от k переменных. Прямоугольник $\overset{\square}{f}$ называется *бент-прямоугольником*, если дополнительно столбцы $\overset{\square}{f}$, домноженные на $2^{(m-k)/2}$, являются спектрами функций от m переменных. В [7] доказано, что f – бент-функция тогда и только тогда, когда $\overset{\square}{f}$ – бент-прямоугольник.

Пусть $\overset{\square}{\mathcal{B}}_{m,k}$ – множество всех $m \times n$ бент-прямоугольников. Для вектора $\mathbf{v}$ через $\mathrm{wt}(\mathbf{v})$ обозначим его вес Хемминга, т. е. число ненулевых координат.

Лемма 1. *Бент-прямоуольник из* $\overset{\square}{\mathcal{B}}_{m,k}$ *однозначно определяется своими значениями в столбцах с номерами из множества* $\left\{\mathbf{v} \in \mathbb{F}_2^k : \mathrm{wt}(\mathbf{v}) \le n/2\right\}$.

Доказательство. Пусть $\overset{\square}{f} \in \overset{\square}{\mathcal{B}}_{m,k}$ и в $\overset{\square}{f}$ определены столбцы с указанными номерами. Изменим размеры $\overset{\square}{f}$ – перейдем к прямоугольнику $\overset{\square}{f}' \in \overset{\square}{\mathcal{B}}_{0,n}$. Правила изменения размеров описаны в [8]. Согласно им по известным столбцам $\overset{\square}{f}$ однозначно определяются столбцы $\overset{\square}{f}$ с номерами $\mathbf{v}' \in \mathbb{F}_2^n$ такими, что $\mathrm{wt}(\mathbf{v}') \le n/2$.

Прямоугольник $\overset{\square}{f}'$ – это спектральная функция $\hat{f}$. Она принимает значения из множества $\{\pm 2^{n/2}\}$. Пусть g – дуальная к f бент-функция: $\chi\big(g(\mathbf{x})\big) = 2^{-n/2}\hat{f}(\mathbf{x})$, $\mathbf{x} \in \mathbb{F}_2^n$. По построению значения g известны для всех $\mathbf{x}$ таких, что $\mathrm{wt}(\mathbf{x}) \le n/2$. Остается доказать, что g однозначно определяется этими значениями. Для этого повторим рассуждения работы [9].

Для двоичных векторов $\mathbf{x} = (x_1,\ldots,x_n)$, $\mathbf{u} = (u_1,\ldots,u_n)$ через $\mathbf{x}^{\mathbf{u}}$ обозначим произведение $\prod_i x_i^{u_i}$, в котором $0^0 = 1^1 = 1^0 = 1$, $0^1 = 0$. Запись $\mathbf{x} \le \mathbf{u}$ означает, что $x_i \le u_i$ для всех $i = 1,\ldots,n$. Алгебраическая нормальная форма g имеет следующий вид:

$$g(\mathbf{x}) = \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathrm{ANF}[g](\mathbf{u})\mathbf{x}^{\mathbf{u}}.$$

Здесь $\mathrm{ANF}[g](\mathbf{u})$ – булева функция коэффициентов. Поскольку $\deg f \le n/2$, $\mathrm{ANF}[g](\mathbf{u}) = 0$ для всех $\mathbf{u}$ таких, что $\mathrm{wt}(\mathbf{u}) > n/2$. Остальные коэффициенты определяются по g с помощью преобразования Мёбиуса:

$$\mathrm{ANF}[g](\mathbf{u}) = \sum_{\mathbf{x}\le\mathbf{u}} g(\mathbf{x}), \quad \mathrm{wt}(\mathbf{u}) \le n/2.$$

В правой части последней формулы используются только значения $\{g(\mathbf{x}) : \mathrm{wt}(\mathbf{x}) \le n/2\}$. Они однозначно определяют функцию ANF[g], которая, в свою очередь, однозначно определяет все остальные значения g. Это и требовалось доказать.

Пусть G – множество, составленное из булевых функций g от $n-1$ переменных таких, что $\hat{g}(\mathbf{v}) \in \{0, \pm 2^{n/2}\}$ для всех $\mathbf{v} \in \mathbb{F}_2^{n-1}$. Такие функции названы в [12] *почти-бент-функциями*. В [13] доказано (в более широком контексте платовидных функций), что если $g \in G$, то $\deg g \le n/2$.

При $m = 1$ бент-прямоугольник $\overset{\square}{f} \in \overset{\square}{\mathcal{B}}_{m,k} = \overset{\square}{\mathcal{B}}_{1,n-1}$ состоит из двух строк. Если $\hat{g}$ – некоторая из них, то $g \in G$. Действительно, $\overset{\square}{f}$ – бент-прямоугольник, и его столбцы (в виде векторов значений) принимают одну из следующих форм: $(0, \pm 2^{n/2})$, $(\pm 2^{n/2}, 0)$.

Оценку сверху для $|G|$ дает

Л е м м а 2. *При $n \ge 6$ в прямоугольнике из $\overset{\square}{\mathcal{B}}_{1,n-1}$ строку можно выбрать не более чем*

$$\frac{B(n/2, n-1) - B(n/2-1, n-1)}{2^{2^{n/2}-n/2+1}} + B(n/2-1, n-1)$$

способами.

Д о к а з а т е л ь с т в о. Следует из теоремы 4.3 работы [4]. Теорема дает оценку сверху для числа функций g от $n-1$ переменных таких, что $\deg g \le n/2$, и все спектральные коэффициенты $\hat{g}(\mathbf{v})$ делятся на $2^{n/2}$. Все такие функции входят в G. Лемма 2 доказана.

3. Доказательство теоремы. Разобьем G на 3 части: G_1, G_2 и G_3. Разбиение выполняется в зависимости от числа нулей среди значений $\{g(\mathbf{v}) : \mathbf{v} \in \mathbb{F}_2^{n-1}, \mathrm{wt}(\mathbf{v}) \le n/2\}$: у функций $g \in G_1$ нулевых значений меньше половины, у функций $g \in G_3$ – больше половины, у функций $g \in G_2$ нулевых и ненулевых значений поровну. Пусть $\widehat{G}_i = \{\hat{g} : g \in G_i\}$.

Докажем, что $|G_1| = |G_3|$. Рассмотрим произвольную функцию $g \in G_1$. Пусть $\mathbf{b}$ – вектор $\mathbb{F}_2^{n-1}$ из всех единиц и $h(\mathbf{y}) = g(\mathbf{y}) + \mathbf{y}\cdot\mathbf{b}$, $\mathbf{y} \in \mathbb{F}_2^{n-1}$. Тогда $\hat{h}(\mathbf{v}) = \hat{g}(\mathbf{v}+\mathbf{b})$ и среди значений

$$\{\hat{h}(\mathbf{v}) : \mathrm{wt}(\mathbf{v}) \ge n/2 - 1\} = \{\hat{g}(\mathbf{v}) : \mathrm{wt}(\mathbf{v}) \le n/2\}$$

менее половины нулевых. Но тогда среди значений $\{\hat{h}(\mathbf{v}) : \mathrm{wt}(\mathbf{v}) \le n/2\}$ более половины нулевых. Это действительно так, ведь $\hat{h}$, будучи спектром почти-бент-функции, принимает нулевые значения ровно в половине случаев. Сказанное означает, что $h \in G_3$ и, таким образом, построено биективное отображение $G_1 \to G_3 : g \mapsto h$. Наличие биекции означает равномощность G_1 и G_3.

Число прямоугольников $\overset{\square}{f} \in \overset{\square}{\mathcal{B}}_{1,n-1}$, первая строка $\hat{g}$ которых лежит в $\widehat{G}_1$, не превосходит величины

$$|G_1| \sqrt{B(n-1, n/2)}.$$

Здесь $|G_1|$ – число способов выбора $\hat{g}$, $\sqrt{B(n-1,n/2)}$ – оценка сверху числа способов определения знаков ненулевых элементов второй строки после выбора $\hat{g}$ в качестве первой. По лемме 1 достаточно определить знаки в столбцах с номерами из множества $\left\{\mathbf{v} \in \mathbb{F}_2^{n-1} : \hat{g}(\mathbf{v}) = 0, \mathrm{wt}(\mathbf{v}) \le n/2\right\}$.

Поскольку $g \in G_1$, задействовано менее половины номеров $\left\{\mathbf{v} \in \mathbb{F}_2^{n-1} : \mathrm{wt}(\mathbf{v}) \le n/2\right\}$ и имеется менее $\sqrt{B(n-1, n/2)}$ способов расстановки знаков.

Число прямоугольников $\overset{\square}{f} \in \overset{\square}{\mathcal{B}}_{1,n-1}$, первая строка которых лежит в $\widehat{G}_3$, также не превосходит указанной величины. Действительно, справедливы те же рассуждения. Только теперь $\hat{g}$ – это вторая строка, а знаки расставляются в первой.

Повторяя рассуждения еще раз, устанавливаем, что число прямоугольников, первая строка которых лежит в $\widehat{G}_2$, не превосходит величины

$$|G_2|\sqrt{B(n-1, n/2)}.$$

Собирая оценки и учитывая равенство $|G_1| = |G_3|$, получаем

$$|\mathcal{B}_n| = |\overset{\square}{\mathcal{B}}_{1,n-1}| \le (|G_1| + |G_2| + |G_1|)\sqrt{B(n-1, n/2)} =$$
$$= (|G_1| + |G_2| + |G_3|)\sqrt{B(n-1, n/2)} = |G|\sqrt{B(n-1, n/2)}.$$

Окончательный результат получается применением оценки сверху для $|G|$ из леммы 2.

Список использованных источников

1. Carlet, C. Boolean Functions for Cryptography and Coding Theory / C. Carlet. – Cambridge: Cambridge University Press, 2021. – 562 p. https://doi.org/10.1017/9781108606806

2. Mesnager, S. Bent Functions: Fundamentals and Results / S. Mesnager. – Cham: Springer, 2016. – 544 p. https://doi.org/10.1007/978-3-319-32595-8

3. Tokareva, N. Bent Functions: Results and Applications to Cryptography / N. Tokareva. – London; San Diego: Academic Press, 2015. – 202 p. https://doi.org/10.1016/C2014-0-02922-X

4. Carlet, C. Upper bounds on the numbers of resilient functions and of bent functions / C. Carlet, A. Klapper // Proceedings of the 23rd Symposium on Information Theory in the Benelux, Louvain-La-Neuve, Belgium, 2002. – [S. l.], 2002. – P. 307–314.

5. Rothhaus, O. On "bent" functions / O. Rothhaus // J. Comb. Theory, Ser. A. – 1976. – Vol. 20, № 3. – P. 300–305. https://doi.org/10.1016/0097-3165(76)90024-8

6. Агиевич, С. О продолжении до бент-функций и оценке сверху их числа / С. Агиевич // Прикладная дискретная математика. Приложение. – 2020. – Вып. 13. – С. 18–21. https://doi.org/10.17223/2226308X/13/4

7. Agievich, S. On the representation of bent functions by bent rectangles / S. Agievich // Probabilistic Methods in Discrete Mathematics: Fifth International Conference (Petrozavodsk, Russia, June 1–6, 2000). – Utrecht; Boston, 2002. – P. 121–135. https://doi.org/10.1515/9783112314104-013

8. Agievich, S. Bent rectangles / S. Agievich // Proceedings of the NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Moscow, September 8–18, 2007). – Amsterdam, 2008. – P. 3–22. https://doi.org/10.3233/978-1-58603-878-6-3

9. Potapov, V. An upper bound on the number of bent functions / V. Potapov // Arxiv [Preprint]. – 2021. – Mode of access: https://arxiv.org/abs/2107.14583. https://doi.org/10.48550/arxiv.2107.14583

10. Propagation characteristics of Boolean functions / B. Preneel [et al.] // Advances in Cryptology: Proceedings of EUROCRYPT'90. – Berlin; Heidelberg: Springer, 1991. – P. 161–173. – (Lecture Notes in Computer Science. Vol. 473). https://doi.org/10.1007/3-540-46877-3_14

11. Langevin, P. Counting all bent functions in dimension eight 99270589265934370305785861242880 / P. Langevin, G. Leander // Des. Codes Cryptogr. – 2011. – Vol. 59, № 1–3. – P. 193–205. https://doi.org/10.1007/s10623-010-9455-z

12. Leander, G. Construction of bent functions from near-bent functions / G. Leander, G. McGuire // J. Comb. Theory, Ser. A. – 2009. – Vol. 116, № 4. – P. 960–970. https://doi.org/10.1016/j.jcta.2008.12.004

13. Zheng, Y. Plateaued Functions / Y. Zheng, X.-M. Zhang // Information and Communication Security. ICICS 1999. – Berlin, Heidelberg: Springer, 1999. – P. 284–300. – (Lecture Notes in Computer Science. Vol. 1726). https://doi.org/10.1007/978-3-540-47942-0_24

References

1. Carlet C. *Boolean Functions for Cryptography and Coding Theory*. Cambridge, Cambridge University Press, 2021. 562 p. https://doi.org/10.1017/9781108606806

2. Mesnager S. *Bent Functions: Fundamentals and Results*. Cham, Springer, 2016. 544 p. https://doi.org/10.1007/978-3-319-32595-8.

3. Tokareva N. *Bent Functions: Results and Applications to Cryptography*. London, San Diego, Academic Press, 2015. 202 p. https://doi.org/10.1016/C2014-0-02922-X

4. Carlet C., Klapper A. Upper bounds on the numbers of resilient functions and of bent functions. *Proceedings of the 23rd Symposium on Information Theory in the Benelux*, Louvain-La-Neuve, Belgium, 2002, pp. 307–314.

5. Rothhaus O. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 1976, vol. 20, no. 3, pp. 300–305. https://doi.org/10.1016/0097-3165(76)90024-8

6. Agievich S. On the continuation to bent functions and upper bounds on their number. *Prikladnaya Diskretnaya Matematika. Supplement*, 2020, iss. 13, pp. 18–21 (in Russian). https://doi.org/10.17223/2226308X/13/4

7. Agievich S. On the representation of bent functions by bent rectangles. *Probabilistic Methods in Discrete Mathematics: Fifth International Conference (Petrozavodsk, Russia, June 1–6, 2000)*. Utrecht, Boston, 2002, pp. 121–135. https://doi.org/10.1515/9783112314104-013

8. Agievich S. Bent rectangles. *Proceedings of the NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Moscow, September 8–18, 2007)*. Amsterdam, 2008, pp. 3–22. https://doi.org/10.3233/978-1-58603-878-6-3

9. Potapov V. An upper bound on the number of bent functions. *Arxiv* [Preprint], 2021. Available at: https://arxiv.org/abs/2107.14583. https://doi.org/10.48550/arxiv.2107.14583

10. Preneel B., Van Leekwijck W., Van Linden L., Goevarts R., Vanderwalle J. Propagation characteristics of Boolean functions. *Advances in Cryptology: Proceedings of EUROCRYPT'90. Lecture Notes in Computer Science, vol. 473*. Berlin, Heidelberg, 1991, pp. 161–173. https://doi.org/10.1007/3-540-46877-3_14

11. Langevin P., Leander G. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Designs, Codes and Cryptography*, 2011, vol. 59, no. 1–3, pp. 193–205. https://doi.org/10.1007/s10623-010-9455-z

12. Leander G., McGuire G. Construction of bent functions from near-bent functions. *Journal of Combinatorial Theory, Series A*, 2009, vol. 116, no. 4, pp. 960–970. https://doi.org/10.1016/j.jcta.2008.12.004

13. Zheng Y., Zhang X.-M. Plateaued Functions. *Information and Communication Security. ICICS 1999. Lecture Notes in Computer Science, vol. 1726*. Berlin, Heidelberg, 1999, pp. 284–300. https://doi.org/10.1007/978-3-540-47942-0_24

Информация об авторе

Агиевич Сергей Валерьевич – кандидат физико-математических наук, заведующий научно-исследовательской лабораторией, НИИ прикладных проблем математики и информатики, Белорусский государственный университет (пр. Независимости, 4-802, 220030, Минск, Республика Беларусь). E-mail: agievich@bsu.by

Information about the author

Sergey V. Agievich – Ph. D. (Physics and Mathematics), Head of a Research Laboratory, Research Institute for Applied Problems of Mathematics and Informatics, Belarusian State University (4, Nezavisimosti Ave., 220030, Minsk, Republic of Belarus). E-mail: agievich@bsu.by