2. *Крылов А. Н.* О некоторых дифференциальных уравнениях математической физики, имеющих приложения в технических вопросах. Л. : ГИТТЛ, 1950. 368 с.

3. *Корнев В. В., Хромов А. П.* Резольвентный подход в методе Фурье для волнового уравнения в несамосопряженном случае // Ж. вычисл. матем. и матем. физ. 2015. Т. 55, № 7. С. 1156–1167.

4. *Чернятин В. А.* Обоснование метода Фурье в смешанной задаче для уравнений в частных производных. М. : Изд-во Моск. ун-та, 1991. 112 с.

УДК 519.651

НЕКОТОРЫЕ СВОЙСТВА АФФИННОЙ ЭКВИВАЛЕНТНОСТИ ГИПЕР–БЕНТ–ФУНКЦИЙ

М. К. Датиев, А. В. Иванов (Москва, РФ)
mkdat05@rambler.ru

В прикладных областях криптографии значительную роль играют булевы функции. Гипер-бент-функции (ГБФ) — это специальный класс булевых функций, впервые описанный в работе [1]. Данный класс функций обладает рядом полезных свойств, что позволяет использовать класс гипер-бент-функций во многих областях криптографии.

При решении задач анализа криптографических алгоритмов, построенных с использованием преобразований конечных полей, часто возникает следующая проблема: найти эффективное приближение некоторой функции, заданной на конечном поле, в определенном множестве функций — классе приближений [2].

Многими авторами изучался вопрос нахождения лучшего приближения произвольной булевой функции в классе аффинных функций. Как известно, вероятность совпадения значений любой булевой функции от n переменных со значениями ее лучшей аффинной аппроксимации не меньше величины $\frac{1}{2} + 2^{-\frac{n}{2}-1}$ [2]. Функции, для которых эта оценка обращается в равенство, были названы «бент-функциями» [3].

Для исследования свойств булевых функций от n переменных, возможно рассмотрение их представлений в виде многочленов от одной переменной над полем $\mathrm{GF}(2^n)$. Данный факт позволяет использовать соответствующий алгебраический аппарат [4]. В работе [5] для одного из таких специальных представлений используется термин «приведенное представление в базисе векторного пространства $\mathrm{GF}(2^n)_{\mathrm{GF}(2)}$». В том же исследовании [5] изучался класс, так называемых, собственных мономиальных функций, заданных приведенными представлениями в базисе пространства $\mathrm{GF}(2^n)_{\mathrm{GF}(2)}$, двойственном к некоторому полиномиальному базису. Показано, что в данном классе для бент-функций от n переменных степени нелинейности не выше $\frac{n}{2} - 1$ существует более точное приближение, чем в классе линейных функций [5]. В работе [1] Йозефом и Гонгом построен такой класс отображений из поля $\mathrm{GF}(2^n)$ в поле $\mathrm{GF}(2)$, который наихудшим образом приближается как линейными функциями, так и собственными мономиальными функциями. Такие отображения получили название «гипер-бент-функции» [1, 5].

Введем следующее обозначение. Пусть $\mathcal{F}_n$ — множество всех отображений из поля $\mathrm{GF}(2^n)$ в поле $\mathrm{GF}(2)$. Для того чтобы определить, является ли $F \in \mathcal{F}_n$ гипер-бент-функцией, необходимо найти коэффициенты расширенного преобразования Уолша – Адамара, т. е. посчитать расстояние до множества функций вида $\mathrm{tr}_1^n(ax^\delta)$, где $a \in Q$, $(\delta, 2^n - 1) = 1$. Для наиболее эффективного нахождения коэффициентов расширенного преобразования Уолша – Адамара для любого δ : $(\delta, 2^n - 1) = 1$ был разработан соответствующий алгоритм:

Алгоритм 1.

1. Для заданного $\delta : (\delta, 2^n - 1) = 1$ найти с помощью расширенного алгоритма Евклида соответствующее значение $\sigma : \sigma \cdot \delta \equiv 1(\mathrm{mod} 2^n - 1)$.
2. Вычислить значения функции $F_\sigma(x) = F(x^\sigma)$.
3. С помощью быстрого преобразования Фурье найти коэффициенты Фурье для функции $F_\sigma(x)$.
4. Так как соответствующие коэффициенты Фурье для функции связаны известным соотношением с коэффициентами Уолша – Адамара для функции, то мы можем определить соответствующие коэффициенты преобразования Уолша – Адамара для функции F.

Найденные при помощи алгоритма 1 коэффициенты будут равны соответствующим коэффициентам расширенного преобразования Уолша – Адамара для функции $F \in \mathcal{F}_n$.

Если выполняется условие, что для всех $\delta : (\delta, 2^n - 1) = 1$ соответствующие коэффициенты расширенного преобразования Уолша – Адамара по абсолютной величине все будут равны $2^{\frac{n}{2}}$, тогда функция $F \in \mathcal{F}_n$ является гипер-бент-функцией.

Ротхаусом было экспериментально установлено, что любая булева функция φ от $n = 6$ переменных $\deg\varphi = 3$, являющаяся бент-функцией, эквивалентна с точностью до невырожденных аффинных замен переменных и добавления произвольных аффинных функций одной из следующих трех функций [3]:

$$f_1 = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6, \tag{1}$$

$$f_2 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5, \tag{2}$$

$$\begin{gathered} f_3 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4 \oplus x_2x_6 \oplus \\ \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6, \end{gathered} \tag{3}$$

Авторами работы исследовался вопрос, бент-функциям какого из этих классов соответствуют в различных базисах бент-функции, являющиеся гипер-бент-функциями. В результате проведенного анализа был получен результат, показывающий, что только в третьем классе существуют бент-функции, соответствующие в некотором базисе гипер-бент-функциям.

На основании проведенных исследований было доказано утверждение, которое описывает новые свойства отображений из множества $\mathcal{F}_n$, соответствующих одной булевой функции, в специальным образом подобранных базисах.

Утверждение. Пусть $\varphi(x_0, x_1, \dots, x_{n-1})$ — булева функция от n переменных. Пусть в векторном пространстве Q_P базис $\overrightarrow{\varepsilon} = (\varepsilon_0, \dots, \varepsilon_{n-1})$ — двойственный базису $\overrightarrow{\theta} = (1, \theta, \theta^2, \dots, \theta^{n-1})$, где θ — примитивный элемент поля Q, а базис $\overrightarrow{\varepsilon^*} = (\varepsilon_0^*, \dots, \varepsilon_{n-1}^*)$ — двойственный базису $\overrightarrow{\theta^d} = (1, \theta^d, \theta^{2d}, \dots, \theta^{(n-1)d})$, где $d = 2^k (k \geq 1)$. Пусть $\varphi(x_0, x_1, \dots, x_{n-1})$ соответствует в базисе $\overrightarrow{\varepsilon}$ отображению $F(x)$, а в базисе $\overrightarrow{\varepsilon^*}$ отображению $F^*(x)$. Тогда $F(x)$ — гипер-бент-функция тогда и только тогда, когда $F^*(x)$ гипер-бент-функция.

СПИСОК ЛИТЕРАТУРЫ

1. *Youssef A., Gong G.* Hyper-bent-functions // Advances in Cryptology. Proc. Of Eurocrypt'2001 // Lecture Notes in Computer Science. 2001. Vol. 2045. P. 406–419.

2. *Амбросимов А. С.* О приближении функций k-значной логики функциями из заданной системы // Фундаментальная и прикладная математика. 1997. Т. 3, вып. 3. С. 653–674.

3. *Rothaus O. S.* On "Bent"Functions // Journal of Combinatorial Theory (A). 1976. Vol. 20. № 3. P. 300–305.

4. *Лидл Р., Нидеррайтер Г.* Конечные поля : в 2 т. Т. 1, 2. М.: Мир, 1988.

5. *Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б.* Приближение булевых функций мономиальными // Дискрет. матем. 2006. Т. 18, № 1. С. 9–29.

УДК 517.51

ПРОИЗВОДЯЩИЕ ФУНКЦИИ КЛАССИЧЕСКИХ ПОЛИНОМИАЛЬНЫХ ОПЕРАТОРОВ И ИХ ОБОБЩЕНИЙ

А. Б. Дикмен (Стамбул, Турция),
А. Л. Лукашов (Саратов, РФ)
LukashovAL@info.sgu.ru

Для построения и исследования аппроксимационных свойств многих классических линейных положительных операторов применяется метод производящих функций. В. С. Виденским был построен обширный класс обладающих хорошими аппроксимативными свойствами операторов, значения которых являются рациональными функциями с фикси-