ЛИТЕРАТУРА

1. *Kumar P. V., Scholtz R. A., and Welch L. R.* Generalized bent functions and their properties // J. Combin. Theory. Ser. A40. 1985. P. 90–107.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press, 2015.

УДК 621.391:519.7 DOI 10.17223/2226308X/12/23

КЛАСС БУЛЕВЫХ ФУНКЦИЙ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ДВОИЧНЫХ РАЗРЯДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛИНЕЙНЫХ РЕКУРРЕНТ НАД КОЛЬЦОМ $\mathbb{Z}_{2^n}$

Д. У. Эрнандес Пилото

Рассматривается класс булевых функций, построенных на основе двоичных разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$ с отмеченным характеристическим многочленом максимального периода. Для этого класса изучаются веса функций, степень нелинейности функций, расстояние между функциями. Кроме того, рассматривается расстояние между функциями из разных классов.

Ключевые слова: *булевы функции, линейные рекуррентные последовательности, двоичные разрядные последовательности.*

Введение

Пусть $R = \mathbb{Z}_{2^n}$ — кольцо вычетов по модулю 2^n, $F(x)$ — отмеченный многочлен степени m максимального периода $T(F) = 2^m - 1$ над кольцом R [1]. Введём обозначения: $P = \mathbb{Z}_2$; $\bar{F}(x)$ — многочлен, полученный из $F(x)$ приведением всех его коэффициентов по модулю 2. Тогда $T(\bar{F}) = 2^m - 1$ и $\bar{F}(x)$ является примитивным многочленом над полем P. Пусть $\omega_1, \ldots, \omega_m$ — линейно независимая система линейных рекуррентных последовательностей (ЛРП) над полем P с характеристическим многочленом $\bar{F}(x)$. Обозначим через $L_R(F)^*$ множество всех ЛРП u над кольцом R, у которых среди элементов $u(0), \ldots, u(m-1)$ есть хотя бы один обратимый элемент кольца R. Рассмотрим функцию $\psi : R \longrightarrow P$, действующую на каждый элемент $a \in R$ с двоичным представлением

$$a = a_0 + 2a_1 + 2^2a_2 + \ldots + 2^{n-1}a_{n-1}, \quad a_0, a_1, \ldots a_{n-1} \in P$$

по правилу

$$\psi(a) = a_{n-1} \oplus a_{n-2}a_{n-3} \ldots a_{n-k}, \tag{1}$$

где $n \geqslant 3$; $k \in \{3, \ldots, n\}$. Для каждой ЛРП $u \in L_R(F)^*$ рассмотрим булеву функцию $f(x_1, \ldots, x_m) = f_{u,\psi}(x_1, \ldots, x_m)$, определённую по следующему правилу: $f(0, \ldots, 0) = \psi(0)$ и для всех $i \in \{0, \ldots, 2^m - 2\}$

$$f(\omega_1(i), \ldots, \omega_m(i)) = \psi(u(i)). \tag{2}$$

Пусть $\chi : R \longrightarrow \mathbb{C}^*$ — аддитивный характер кольца R, определённый равенством

$$\chi(x) = e^{2\pi i x/2^n}, \ x \in R.$$

Группа всех аддитивных характеров кольца R имеет вид $\{\chi(ax) : a \in R\}$. Множество всех отображений из R в $\mathbb{C}^*$ образует унитарное пространство со скалярным произведением, определённым для отображений g и h по правилу

$$\langle g, h \rangle = \sum_{x \in R} g(x)\bar{h}(x).$$

Система функций $\chi(ax)$, $a \in R$, образует ортогональный базис рассматриваемого пространства, поэтому найдутся однозначно определённые числа $\nu_j = \nu_j(\psi) \in \mathbb{C}$, такие, что

$$(-1)^{\psi(x)} = \sum_{j \in R} \nu_j \chi(jx),\ x \in R.$$

Они однозначно вычисляются по формуле

$$\nu_j = \frac{1}{2^n} \sum_{a \in R} (-1)^{\psi(a)} \chi(-aj).$$

Введём обозначение $\sigma(\psi) = \sum\limits_{j \in R} |\nu_j|$.

1. Свойства функций нового класса

Для суммы модулей чисел ν_j получим следующую оценку:

Теорема 1. Пусть отображение ψ задано равенством (1) и $k = 3$, тогда

$$\sigma(\psi) \leqslant \frac{2}{\pi} \ln(2^{n-1}) + 1.$$

Эта оценка позволяет доказать теорему:

Теорема 2. Пусть f — функция, определённая равенством (2) и $k = 3$, тогда

1) вес f удовлетворяет неравенствам

$$2^{m-1} - \left(\frac{2}{\pi} \ln(2^{n-1}) + 1\right)(2^{n-1} - 1)2^{m/2-1} \leqslant \|f\| \leqslant$$
$$\leqslant 2^{m-1} + \left(\frac{2}{\pi} \ln(2^{n-1}) + 1\right)(2^{n-1} - 1)2^{m/2-1};$$

2) если $f = f_{u,\psi}$, $g = f_{v,\psi}$ и ЛРП u, v не пропорциональны в R^*, то расстояние Хэмминга $\rho(f, g)$ между столбцами значений рассматриваемых функций удовлетворяет соотношениям

$$2^{m-1} - \left(\frac{2}{\pi} \ln(2^{n-1}) + 1\right)^2 (2^{n-1} - 1)2^{m/2-1} \leqslant \rho(f, g) \leqslant$$
$$\leqslant 2^{m-1} + \left(\frac{2}{\pi} \ln(2^{n-1}) + 1\right)^2 (2^{n-1} - 1)2^{m/2-1};$$

3) для нелинейности $\mathrm{nl}(f)$ верна оценка

$$\mathrm{nl}(f) \geqslant 2^{m-1} - \left(\frac{2}{\pi} \ln(2^{n-1}) + 1\right)(2^{n-1} - 1)2^{m/2-1}.$$

Для произвольных значений k аналогичные результаты получить не удаётся. В общем виде справедливо

Утверждение 1. Пусть

$$\begin{aligned} \psi_1(a) &= a_{n-1} \oplus a_{n-2} \ldots a_{n-k}, \\ \psi_2(a) &= a_{n-1} \oplus a_{n-2} \ldots a_{n-k} a_{n-k-1}, \end{aligned}$$

где $k \in \{3, \ldots, n-1\}$. Тогда для $|\nu_j(\psi_2)|$ верна оценка

$$|\nu_j(\psi_2)| \leqslant \frac{1 + 2^{n-1} \sin(\pi j / 2^n) |\nu_j(\psi_1)|}{2^n \sin(\pi j / 2^n) |\cos(\pi j / 2^{k+1})|}.$$

Это утверждение позволяет оценить модули чисел $\nu_j(\psi_2)$, зная аналогичные коэффициенты для отображения ψ_1.

2. Расстояние Хэмминга между функциями

Изучим теперь для двух функций f и g из разных классов величину $\rho(f, g)$.

Утверждение 2. Пусть отображение ψ_1 задано равенством (1) и $\psi_2(a) = a_{n-1}$, $f = f_{u,\psi_1}$, $g = f_{u,\psi_2}$. Тогда

$$2^{m-k+1} - \frac{(2^n-1)(2^{n-1}-1)}{3}2^{m/2-k+2} \leqslant \rho(f,g) \leqslant 2^{m-k+1} + \frac{(2^n-1)(2^{n-1}-1)}{3}2^{m/2-k+2}.$$

Обозначим через ε_1, ε_2 соответственно левую и правую части неравенства из утверждения 2.

Утверждение 3. Пусть отображение ψ_1 задано равенством (1), $\psi_2(a) = a_{n-1} \oplus \oplus a_{n-2} \oplus a_{n-3} \oplus \ldots \oplus a_{n-k}$, где $k \in \{3, \ldots, n\}$, $f = f_{u,\psi_1}$, $g = f_{u,\psi_2}$. Тогда

$$\begin{array}{ll} (2^{k-2}+1)\varepsilon_1 \leqslant \rho(f,g) \leqslant (2^{k-2}+1)\varepsilon_2 & \text{для нечётного } k; \\ (2^{k-2}-1)\varepsilon_1 \leqslant \rho(f,g) \leqslant (2^{k-2}-1)\varepsilon_2 & \text{для чётного } k. \end{array}$$

Заключение

В данной работе для класса булевых функций, построенных на основе двоичных разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$, получены оценки для веса функций, нелинейности и расстояний между функциями. Отметим, что ранее в работах [2–4] аналогичные вопросы были рассмотрены только для случая, когда ψ — линейное отображение по всем двоичным разрядам.

ЛИТЕРАТУРА

1. *Нечаев А. А.* Цикловые типы линейных подстановок над конечными коммутативными кольцами // Математический сборник. 1993. Т. 184. № 3. С. 21–56.
2. *Быльков Д. Н., Камловский О. В.* Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент // Математические вопросы криптографии. 2012. Т. 3. № 4. С. 25–53.
3. *Камловский О. В.* Нелинейность одного класса булевых функций, построенных с использованием двоичных разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$ // Математические вопросы криптографии. 2016. Т. 7. № 3. С. 29–46.
4. *Быльков Д. Н.* Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент // Прикладная дискретная математика. Приложение. 2014. № 7. С. 59–60.

UDC 519.7 DOI 10.17223/2226308X/12/24

PROPERTIES OF ASSOCIATED BOOLEAN FUNCTIONS OF QUADRATIC APN FUNCTIONS[1]

A. A. Gorodilova

For a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, it is defined the associated Boolean function γ_F in $2n$ variables as follows: $\gamma_F(a, b) = 1$ if $a \neq \mathbf{0}$ and equation $F(x) + F(x + a) = b$ has solutions. A vectorial Boolean function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is called almost perfect nonlinear (APN) if equation $F(x) + F(x + a) = b$ has at most 2 solutions for all vectors $a, b \in \mathbb{F}_2^n$, where a is nonzero. In case when F is a quadratic APN function its associated function has the form $\gamma_F(a, b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1$ for appropriate

[1]The work is supported by RFBR, projects no. 18-31-00479 and 18-07-01394.