Секция 3

ПСЕВДОСЛУЧАЙНЫЕ ГЕНЕРАТОРЫ

УДК 519.113.6

ОБ ОДНОМ КЛАССЕ БУЛЕВЫХ ФУНКЦИЙ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ СТАРШИХ РАЗРЯДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛИНЕЙНЫХ РЕКУРРЕНТ

Д. Н. Былков

Изучается семейство булевых функций, построенных на основе старших разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$ с отмеченным характеристическим многочленом. Для данного семейства изучаются степень нелинейности функций и алгебраическая степень. Показывается, что указанное семейство содержит функции, значительно удалённые от класса всех аффинных функций.

Ключевые слова: *линейные рекуррентые последовательности, старшие разрядные последовательности, степень нелинейности булевой функции.*

В работе [1] изучались свойства булевых функций, построенных на основе последовательностей старших разрядов отмеченных линейных рекуррент над кольцом $R = \mathbb{Z}_{2^n}$. Получены результаты, описывающие веса функций, степень их нелинейности, расстояние между функциями и мощность всего семейства. А. А. Нечаевым предложен к рассмотрению ещё один класс булевых функций, построенных на основе последовательностей старших разрядов, отличающийся другим упорядочиванием вектора значений функции. В настоящей работе приводятся результаты о степени нелинейности и алгебраической степени функций из данного класса.

Пусть $F(x) \in R[x]$ — унитарный (со старшим коэффициентом 1) реверсивный многочлен степени m, такой, что его период $T(F)$ удовлетворяет условию $T(F) = T(F \bmod 2) = 2^m - 1$. В этом случае будем говорить, что $F(x)$ — отмеченный многочлен максимального периода. Обозначим $L_R(F)$ множество всех линейных рекуррентных последовательностей (ЛРП) над кольцом R с характеристическим многочленом $F(x)$ и $L_R(F)^*$ — множество всех ЛРП $u \in L_R(F)$, у которых в начальном векторе $(u(0), u(1), \ldots, u(m-1))$ есть хотя бы один обратимый элемент кольца R. Каждая последовательность $u \in L_R(F)^*$ имеет период $T(u) = T(F) = (2^m - 1)$.

Подмножество $K = \{k_0, k_1\}$ множества R назовём *разрядным множеством* кольца R (см., например, [2]), если элементы k_0 и k_1, рассматриваемые как целые числа, имеют различную чётность. Примером разрядного множества кольца R является *двоичное разрядное множество* $K = \{0, 1\}$. Если K — разрядное множество кольца R, то каждый элемент a этого кольца однозначно представим в виде

$$a = a_0 + 2a_1 + 2^2a_2 + 2^3a_3 + \ldots + 2^{n-1}a_{n-1}, \quad (1)$$

где $a_i = \varkappa_i^K(a) \in K$ для всех $i = 0, 1, \ldots, n-1$. Элемент a_i, участвующий в равенстве (1), будем называть *i-м разрядом* элемента a в разрядном множестве K.

Сопоставим каждой ЛРП $u \in L_R(F)^*$ булеву функцию $f''_{u,K}(x_1,\ldots,x_m)$ по правилу $f''_{u,K}(0,\ldots,0) = \varkappa^K_{n-1}(0) \bmod 2$,

$$f''_{u,K}(u_0(i), u_0(i+1), \ldots, u_0(i+m-1)) = \varkappa^K_{n-1}(u(i)) \bmod 2,$$

где $u_0(i) = u(i) \bmod 2$, $0 \leqslant i \leqslant 2^m - 1$. В силу выбора последовательности u вектор $(u_0(i), u_0(i+1), \ldots, u_0(i+m-1))$ принимает все возможные значения из множества $\{0,1\}^m \setminus \{(0,\ldots,0)\}$, поэтому функция определена на всех двоичных наборах $\{0,1\}^m$. Обозначим $B_n''(K,F)$ множество всех булевых функций $f''_{u,K}$, соответствующих всем ЛРП u из множества $L_R(F)^*$.

Оказывается, что для функций $f''_{u,K} \in B''_n(K,F)$ справедливы такие же оценки степени нелинейности и алгебраической степени, что и для функций из класса $B'_n(K,F)$ [1].

Теорема 1. Для коэффициентов $W_f(\mathbf{a})$ Уолша — Адамара булевой функции $f = f''_{u,K}$ при всех $n \geqslant 2$ имеет место оценка

$$|W_f(\mathbf{a})| \leqslant \left(\frac{2}{\pi}\ln(2^{n-1}) + 1\right)(2^{n-1} - 1)2^{m/2}.$$

Следствие 1. При $n = 2$ и каждом чётном m класс $B''_n(K,F)$ состоит из бент-функций, а при $n = 2$ и каждом нечётном m класс $B''_n(K,F)$ состоит из платовидных функций порядка $m - 1$.

Теорема 2. Пусть $F(x) \in R[x]$ — отмеченный многочлен степени $m > |R|$ максимального периода над кольцом R, тогда для любой функции $f \in B''_n(K,F)$ справедливо соотношение $\deg f = 2^{n-1}$.

ЛИТЕРАТУРА

1. *Былков Д. Н., Камловский О. В.* Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент // Матем. вопр. криптогр. 2012. Т. 3. № 4. С. 25–53.
2. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A.* Linear recurring sequences over rings and modules // J. Math. Sci. (New York). 1995. V. 76. No. 6. P. 2793–2915.

УДК 519.6

ОЦЕНКИ ЭКСПОНЕНТОВ ПЕРЕМЕШИВАЮЩИХ ГРАФОВ НЕКОТОРЫХ МОДИФИКАЦИЙ АДДИТИВНЫХ ГЕНЕРАТОРОВ

А. М. Дорохова

Для модификации аддитивного генератора с помощью инволютивной перестановки координат векторов исследованы условия полного перемешивания. Доказаны достаточные условия примитивности перемешивающего графа и оценки его экспонента в некоторых случаях. Полученные оценки экспонента показывают, что полное перемешивание знаков состояния генератора может быть достигнуто после числа тактов, которое существенно меньше размера состояний.

Ключевые слова: *аддитивный генератор, перемешивающий граф преобразования, экспонент графа.*