Math-Net.Ru

Общероссийский математический портал

О. В. Камловский, Расстояние между двоичными представлениями линейных рекуррент над полем $GF(2^k)$ и кольцом $\mathbb{Z}_{2^n}$, *Матем. вопр. криптогр.*, 2016, том 7, выпуск 1, 71–82

DOI: <https://doi.org/10.4213/mvk175>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.91.87.62

26 апреля 2023 г., 18:34:12

**Расстояние между двоичными представлениями
линейных рекуррент над полем $GF(2^k)$ и кольцом $\mathbb{Z}_{2^n}$**

О. В. Камловский

ООО «Центр сертификационных исследований», Москва

Получено 20.IV.2015

Рассматриваются линейные рекуррентные последовательности над полем $GF(2^k)$ и над кольцом $\mathbb{Z}_{2^n}$ со взаимосвязанными законами рекурсии. Оценивается расстояние Хэмминга между циклами последовательностей, полученных из исходных заменой каждого их знака его образом при действии произвольных отображений в поле из двух элементов.

Работа выполнена при финансовой поддержке Академии криптографии Российской Федерации.

Ключевые слова: линейные рекуррентные последовательности, двоичные представления последовательностей, конечные поля, кросс-корреляционная функция

**On the Hamming distance between binary representations of linear
recurrent sequences over field $GF(2^k)$ and ring $\mathbb{Z}_{2^n}$**

O. V. Kamlovskiy

Sertification Research Center, LLC, Moscow

Abstract. Linear recurrent sequences over the field $GF(2^k)$ and over the ring $\mathbb{Z}_{2^n}$ with dependent recurrent relations are considered. We establish the bounds for the Hamming distance between two binary sequences obtained from the initial sequences by replacing each element by its image under the action of arbitrary maps into the field of two elements.

Keywords: linear recurrent sequences, binary representations of sequences, finite fields, cross-correlation function

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 1, pp. 71–82 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

1. Введение

Пусть $Q = GF(2^k)$ есть конечное поле из 2^k элементов, $R = \mathbb{Z}_{2^n}$ — кольцо вычетов по модулю 2^n , $P = \mathbb{Z}_2 = \{0, 1\}$, u — линейная рекуррентная последовательность (ЛРП) над полем Q , v — ЛРП над кольцом R . Рассмотрим отображения $f : Q \rightarrow P$, $\psi : R \rightarrow P$ и двоичные последовательности $\omega_1 = f(u)$, $\omega_2 = \psi(v)$, знаки которых определены равенствами

$$\omega_1(i) = f(u(i)), \quad \omega_2(i) = \psi(v(i)), \quad i = 0, 1, 2, \dots \quad (1)$$

Последовательности ω_1 и ω_2 называются *двоичными представлениями* ЛРП u и v соответственно и используются как псевдослучайные последовательности (см., например, [1], [2]).

Целью данной работы является установление нетривиальных оценок расстояния Хэмминга между отрезками $\bar{\omega}_1 = (\omega_1(0), \omega_1(1), \dots, \omega_1(T-1))$ и $\bar{\omega}_2 = (\omega_2(0), \omega_2(1), \dots, \omega_2(T-1))$, где T — общий период последовательностей ω_1 и ω_2 .

Пусть $\alpha_1, \alpha_2, \dots, \alpha_k$ — базис линейного пространства Q_P . Последовательности $u_s = \{u_s(i)\}_{i=0}^\infty$ ($s = 1, 2, \dots, k$) над полем P , знаки которых заданы равенствами

$$u(i) = \alpha_1 u_1(i) + \alpha_2 u_2(i) + \dots + \alpha_k u_k(i), \quad i = 0, 1, 2, \dots,$$

называются *координатными последовательностями* ЛРП u (см. [3]). Согласно результатам работы [3] $u_1, u_2, \dots, u_k$ являются ЛРП с общим характеристическим многочленом $F(x) \in P[x]$. Пусть φ — булева функция от k переменных, удовлетворяющая равенству

$$\varphi(x_1, x_2, \dots, x_k) = f(\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_k x_k), \quad x_1, x_2, \dots, x_k \in P.$$

Тогда

$$\omega_1(i) = \varphi(u_1(i), u_2(i), \dots, u_k(i)), \quad i = 0, 1, 2, \dots \quad (2)$$

Для такой последовательности будем ниже использовать обозначение $\omega_1 = \varphi(u_1, u_2, \dots, u_k)$. Всюду в дальнейшем будем рассматривать более общую ситуацию, когда $u_1, u_2, \dots, u_k$ — произвольные ЛРП с общим характеристическим многочленом $F(x)$ (не обязательно координатные последовательности одной ЛРП). Если $u_1, u_2, \dots, u_k$ являются сдвигами одной ЛРП, то последовательность $\varphi(u_1, u_2, \dots, u_k)$ является выходной последовательностью двоичного фильтрующего генератора с фильтрующей функцией φ .

Пусть $G(x) \in R[x]$ — характеристический многочлен ЛРП v , а $\bar{G}(x)$ — многочлен над полем P , полученный из $G(x)$ приведением всех его коэффициентов по модулю 2. В данной работе сформулированная выше задача решается при следующих ограничениях: $F(x)$ неприводим над полем P и $\bar{G}(x) = F(x)$.

Отдельно рассматриваются частные случаи, когда $\omega_1 = \varphi(u_1, u_2, \dots, u_k)$, $\omega_2 = \omega$ — ЛРП над полем P с характеристическим многочленом $F(x)$ (раздел 4) и $\omega_1 = \omega$, $\omega_2 = \psi(v)$ (раздел 5). В разделе 6 полученные результаты применяются к построению (с использованием линейного регистра над кольцом R) булевых функций, гарантированно удаленных от класса всех аффинных функций.

2. Кросс-корреляционная функция и расстояние между последовательностями

Пусть ω_1 и ω_2 — произвольные двоичные периодические последовательности с периодами $T(\omega_1)$ и $T(\omega_2)$ соответственно, а T — некоторое общее кратное этих чисел. Назовем *кросс-корреляционной функцией* последовательностей ω_1 и ω_2 (см., например, [4]) функцию

$$C_{\omega_1, \omega_2}(t) = \sum_{i=0}^{T-1} (-1)^{\omega_1(i) \oplus \omega_2(i+t)}, \quad t=0, 1, \dots, T-1. \quad (3)$$

В случае когда $\omega_1 = \omega_2$ и $T = T(\omega_1) = T(\omega_2)$, кросс-корреляционную функцию называют *автокорреляционной функцией* последовательности ω_1 .

Величина $C_{\omega_1, \omega_2}(t)$ характеризует «близость» последовательностей ω_1 и сдвига $x^t \omega_2 = (\omega_2(t), \omega_2(t+1), \dots)$ последовательности ω_2 на t шагов. Действительно, пусть $\rho(\omega_1, x^t \omega_2)$ — расстояние Хэмминга между векторами $(\omega_1(0), \omega_1(1), \dots, \omega_1(T-1))$ и $(\omega_2(t), \omega_2(t+1), \dots, \omega_2(T+t-1))$. Тогда

$$\begin{aligned} C_{\omega_1, \omega_2}(t) &= |\{i \in \{0, 1, \dots, T-1\} : \omega_1(i) = \omega_2(i+t)\}| - \\ &\quad - |\{i \in \{0, 1, \dots, T-1\} : \omega_1(i) \neq \omega_2(i+t)\}| = \\ &= T - 2\rho(\omega_1, x^t \omega_2), \end{aligned}$$

а, значит,

$$\rho(\omega_1, x^t \omega_2) = \frac{1}{2} (T - C_{\omega_1, \omega_2}(t)). \quad (4)$$

Таким образом, чем меньше величина $|C_{\omega_1, \omega_2}(t)|$, тем ближе исследуемое расстояние к числу $T/2$.

Заметим, что функция C_{ω_1, ω_2} , определенная равенством (3), зависит от выбора параметра T . В основном приложения относятся к ситуации, когда $T = T(\omega_1) = T(\omega_2)$.

3. Расстояние между $\varphi(u_1, \dots, u_k)$ и $\psi(v)$

Пусть $u_1, u_2, \dots, u_k$ — ЛРП над полем $P = \mathbb{Z}_2$ с неприводимым над P характеристическим многочленом $F(x) \in P[x]$ степени $\deg F(x) = m$, v — ЛРП над $R = \mathbb{Z}_{2^n}$ с таким характеристическим многочленом $G(x) \in R[x]$, что $\overline{G}(x) = F(x)$. В этом случае для периодов $T(F)$ и $T(G)$ многочленов $F(x)$ и $G(x)$ справедливы равенства

$$T(F) = \frac{2^m - 1}{d}, \quad T(G) = 2^\nu T(F),$$

где d — некоторый делитель числа $2^m - 1$, а ν — целое число, удовлетворяющее неравенствам $0 \leq \nu \leq n - 1$ (см. [5]).

Обозначим $\bar{v}$ двоичную последовательность, полученную из v приведением каждого ее элемента по модулю 2. Она является ЛРП с характеристическим многочленом $F(x)$. Всюду в дальнейшем будем рассматривать случай, когда среди элементов $v(0), v(1), \dots, v(m-1)$ начального отрезка ЛРП v есть хотя бы один обратимый элемент кольца R , т. е. $\bar{v}$ является ненулевой последовательностью. Назовем отображение ψ *сбалансированным* (см. [6]), если уравнение $\psi(x) = 1$ имеет ровно 2^{n-1} решений относительно неизвестного $x \in R$.

Теорема 1. Пусть $\omega_1 = \varphi(u_1, u_2, \dots, u_k)$, $\omega_2 = \psi(v)$, где ψ — сбалансированное отображение. Тогда если $x^t \bar{v}$ линейно не выражается через систему $u_1, u_2, \dots, u_k$, то для кросс-корреляционной функции C_{ω_1, ω_2} , определенной равенством (3) при $T = T(G)$, справедливо неравенство

$$\left| C_{\omega_1, \omega_2}(t) + \frac{2^\nu}{d} (-1)^{\varphi(\bar{0}) + \psi(0)} \right| \leq \frac{2^\nu (d 2^{n-1} - 1)}{d} 2^{(m+k+n)/2}.$$

Доказательство. Из определений (1)–(3) следует соотношение

$$C_{\omega_1, \omega_2}(t) = \sum_{i=0}^{T-1} (-1)^{\varphi(u_1(i), u_2(i), \dots, u_k(i)) \oplus \psi(v(i+t))}.$$

Применяя разложение по базису характеров (см., например, [7, с. 77]), получаем

$$(-1)^{\varphi(u_1(i), u_2(i), \dots, u_k(i))} = \frac{1}{2^k} \sum_{\vec{a}=(a_1, \dots, a_k) \in P^k} W_\varphi(\vec{a}) (-1)^{a_1 u_1(i) \oplus \dots \oplus a_k u_k(i)}, \quad (5)$$

где $W_\varphi(\vec{a})$ — коэффициенты Уолша–Адамара булевой функции φ , определенные равенством

$$W_\varphi(\vec{a}) = \sum_{\vec{b}=(b_1, b_2, \dots, b_k) \in P^k} (-1)^{\varphi(b_1, b_2, \dots, b_k) \oplus a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_k b_k}.$$

Введем обозначение

$$\sigma(\varphi) = \sum_{\vec{a} \in P^k} |W_\varphi(\vec{a})|. \quad (6)$$

В [8, утверждение 2] показано, что

$$\sigma(\varphi) \leq 2^{3k/2}. \quad (7)$$

Согласно результатам работы [9, предложение 1] справедливо следующее разложение по базису характеров группы $\mathbb{Z}_{2^n}$:

$$(-1)^{\psi(v(i))} = \sum_{c \in R} \mu_c \chi(cv(i)), \quad (8)$$

где

$$\mu_c = \frac{1}{2^n} \sum_{b \in R} (-1)^{\psi(b)} \chi(-cb), \quad (9)$$

а

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

Введем обозначение

$$\sigma(\psi) = \sum_{c \in R} |\mu_c|. \quad (10)$$

Как показано в [9, предложение 1],

$$\sigma(\psi) \leq 2^{n/2}. \quad (11)$$

Согласно (5) и (8)

$$C_{\omega_1, \omega_2}(t) = \frac{1}{2^k} \left(\sum_{\vec{a} \in P^k} W_\varphi(\vec{a}) (-1)^{a_1 u_1(i) \oplus \dots \oplus a_k u_k(i)} \right) \left(\sum_{c \in R} \mu_c \chi(cv(i+t)) \right).$$

Изменяя порядок суммирования и используя равенство $(-1)^x = \chi(2^{n-1}x)$, $x \in P$, получаем

$$C_{\omega_1, \omega_2}(t) = \frac{1}{2^k} \sum_{\vec{a} \in P^k, c \in R} W_\varphi(\vec{a}) \mu_c \sum_{i=0}^{T-1} \chi(\delta_{a_1, a_2, \dots, a_k, c}(i)), \quad (12)$$

где $\{\delta_{a_1, a_2, \dots, a_k, c}(i)\}_{i=0}^{\infty}$ — последовательность над кольцом R , общий член которой имеет вид

$$\delta_{a_1, \dots, a_k, c}(i) = 2^{n-1} a_1 u_1(i) + 2^{n-1} a_2 u_2(i) + \dots + 2^{n-1} a_k u_k(i) + c v(i+t).$$

Из равенства $\overline{G}(x) = F(x)$ следует, что $\delta_{a_1, a_2, \dots, a_k, c}$ является ЛРП с характеристическим многочленом $G(x)$. Покажем, что она ненулевая при всех $c \in R \setminus \{0\}$ и $(a_1, a_2, \dots, a_k) \in P^k$. Действительно, если бы она была нулевой, то из $\bar{v} \neq (\bar{0})$ имели бы $c = 2^{n-1}$, а значит, $x^t \bar{v} = a_1 u_1 \oplus a_1 u_1 \oplus \dots \oplus a_k u_k$, что противоречит условию. Преобразовав равенство (12), получим

$$C_{\omega_1, \omega_2}(t) + \varkappa = \frac{1}{2^k} \sum_{\vec{a} \in P^k, c \in R} W_{\varphi}(\vec{a}) \mu_c \left(\sum_{i=0}^{T-1} \chi(\delta_{a_1, a_2, \dots, a_k, c}(i)) + \frac{2^\nu}{d} \right),$$

где

$$\varkappa = \frac{2^\nu}{2^k d} \sum_{\vec{a} \in P^k, c \in R} W_{\varphi}(\vec{a}) \mu_c.$$

Найдем значение $\varkappa$. Согласно (5) и (8)

$$\varkappa = \frac{2^\nu}{2^k d} \left(\sum_{\vec{a} \in P^k} W_{\varphi}(\vec{a}) \right) \left(\sum_{c \in R} \mu_c \right) = \frac{2^\nu}{d} (-1)^{\varphi(\vec{0}) \oplus \psi(0)}.$$

Значит,

$$\begin{aligned} C_{\omega_1, \omega_2}(t) + \frac{2^\nu}{d} (-1)^{\varphi(\vec{0}) \oplus \psi(0)} &= \\ &= \frac{1}{2^k} \sum_{\vec{a} \in P^k, c \in R} W_{\varphi}(\vec{a}) \mu_c \left(\sum_{i=0}^{T-1} \chi(\delta_{a_1, a_2, \dots, a_k, c}(i)) + \frac{2^\nu}{d} \right). \end{aligned} \quad (13)$$

По условию ψ — сбалансированное отображение, поэтому, с учетом равенства (9), имеем $\mu_0 = 0$. В (13) для кросс-корреляционной функции достаточно ограничиться суммированием по всем $c \neq 0$. Переходя к исследованию абсолютных величин, получаем

$$\begin{aligned} \left| C_{\omega_1, \omega_2}(t) + \frac{2^\nu}{d} (-1)^{\varphi(\vec{0}) \oplus \psi(0)} \right| &\leq \\ &\leq \frac{1}{2^k} \sigma(\varphi) \sigma(\psi) \max_{\vec{a} \in P^k, c \neq 0} \left| \sum_{i=0}^{T-1} \chi(\delta_{a_1, a_2, \dots, a_k, c}(i)) + \frac{2^\nu}{d} \right|. \end{aligned}$$

В [10, теорема 2.1] показано, что для каждой ненулевой ЛРП δ с характеристическим многочленом $G(x)$ над кольцом R имеет место соотношение

$$\left| \sum_{i=0}^{T-1} \chi(\delta(i)) + \frac{2^\nu}{d} \right| \leq \frac{2^\nu (d 2^{n-1} - 1)}{d} 2^{m/2}.$$

Таким образом,

$$\left| C_{\omega_1, \omega_2}(t) + \frac{2^\nu}{d} (-1)^{\varphi(\vec{0}) \oplus \psi(0)} \right| \leq \frac{1}{2^k} \sigma(\varphi) \sigma(\psi) \frac{2^\nu (d2^{n-1} - 1)}{d} 2^{m/2}. \quad (14)$$

Для завершения доказательства остается воспользоваться неравенствами (7) и (11). $\square$

Отметим, что если параметры $\sigma(\varphi)$ и $\sigma(\psi)$ вычислены или для них известны более точные оценки, чем (7) и (11), то предпочтительнее использовать неравенство (14).

Согласно равенству (3) для всех t справедлива тривиальная оценка $|C_{\omega_1, \omega_2}(t)| \leq T$. Правая часть оценки из теоремы будет меньше T при условии

$$T \geq 2^{(3n+m+k)/2-1}.$$

Если $T = 2^m - 1$, то последнее неравенство справедливо для всех m таких, что $m \geq 3n + k$.

Следующая теорема описывает свойства расстояния $\rho(\omega_1, x^t \omega_2)$.

Теорема 2. В условиях теоремы 1 для расстояния Хэмминга справедливы оценка

$$\left| \rho(\omega_1, x^t \omega_2) - \frac{T}{2} - \frac{2^{\nu-1}}{d} (-1)^{\varphi(\vec{0}) \oplus \psi(0)} \right| \leq \sigma(\varphi) \sigma(\psi) \frac{d2^{n-1} - 1}{d} 2^{m/2 + \nu - k - 1}$$

и более простая, но менее точная оценка

$$\left| \rho(\omega_1, x^t \omega_2) - \frac{T}{2} - \frac{2^{\nu-1}}{d} (-1)^{\varphi(\vec{0}) \oplus \psi(0)} \right| \leq \frac{d2^{n-1} - 1}{d} 2^{(m+k+n)/2 + \nu - 1}.$$

Доказательство. Достаточно воспользоваться теоремой 1 и равенством (4). $\square$

4. Расстояние между $\varphi(u_1, u_2, \dots, u_k)$ и ω

Пусть $u_1, u_2, \dots, u_k$ — ЛРП над полем $P = \mathbb{Z}_2$ с неприводимым над P характеристическим многочленом $F(x) \in P[x]$ степени $\deg F(x) = m$, а ω — ЛРП над $R = \mathbb{Z}_2$ с характеристическим многочленом $F(x)$,

$$T = T(F) = \frac{2^m - 1}{d},$$

где d — некоторый делитель числа $2^m - 1$.

Рассмотрим случай $\omega_1 = \varphi(u_1, u_2, \dots, u_k)$ и $\omega_2 = \omega$.

Теорема 3. Пусть $x^t \omega$ линейно не выражается через систему ЛРП $u_1, u_2, \dots, u_k$. Тогда справедливы оценки

$$\left| \rho(\omega_1, x^t \omega_2) - \frac{T}{2} - \frac{(-1)^{\varphi(\vec{0})}}{2d} \right| \leq \sigma(\varphi) \frac{d-1}{d} 2^{m/2-k-1},$$

$$\left| \rho(\omega_1, x^t \omega_2) - \frac{T}{2} - \frac{(-1)^{\varphi(\vec{0})}}{2d} \right| \leq \frac{d-1}{d} 2^{(m+k)/2-1}.$$

Доказательство. В условиях теоремы 2 положим $n = 1$, $v = \omega$, $\psi(x) = x$, $x \in \{0, 1\}$. Тогда по условию v будет ненулевой последовательностью, $\sigma(\psi) = |\mu_0| + |\mu_1| = 1$, и первое из неравенств доказано. Для доказательства второго неравенства достаточно в первом неравенстве воспользоваться оценкой (7). $\square$

Достижимость каждой из полученных оценок устанавливается следующим практически важным результатом, получающимся при $d = 1$.

Следствие 1. Пусть выполнены условия теоремы 3 и $F(x)$ — многочлен максимального периода $T(F) = 2^m - 1$. Тогда

$$\rho(\omega_1, x^t \omega_2) = \begin{cases} 2^{m-1} - 1, & \text{если } \varphi(\vec{0}) = 1, \\ 2^{m-1}, & \text{если } \varphi(\vec{0}) = 0. \end{cases}$$

Таким образом, усложненная последовательность $\varphi(u_1, u_2, \dots, u_k)$ отличается от $x^t \omega$ примерно половиной знаков.

5. Расстояние между ω и $\psi(v)$

Пусть $\omega_1 = \omega$ есть ненулевая ЛРП над полем $P = \mathbb{Z}_2$ с неприводимым над P характеристическим многочленом $F(x) \in P[x]$ степени $\deg F(x) = m$, $\omega_2 = \psi(v)$, где v — ЛРП над $R = \mathbb{Z}_{2^n}$ с таким характеристическим многочленом $G(x) \in R[x]$, что $\bar{G}(x) = F(x)$, причем $\bar{v}$ — ненулевая последовательность. Выберем $T = T(G) = 2^\nu T(F)$.

Теорема 4. Пусть $x^t \bar{v} \neq \omega$. Тогда

$$\left| \rho(\omega_1, x^t \omega_2) - \frac{T}{2} - \frac{2^{\nu-1}}{d} (-1)^{\psi(0)} \right| \leq \sigma(\psi) \frac{d2^{n-1}-1}{d} 2^{m/2+\nu-1},$$

$$\left| \rho(\omega_1, x^t \omega_2) - \frac{T}{2} - \frac{2^{\nu-1}}{d} (-1)^{\psi(0)} \right| \leq \frac{d2^{n-1}-1}{d} 2^{(m+n)/2+\nu-1}.$$

Доказательство. Рассмотрим в условиях теоремы 1 случай $k = 1$, $u_1 = \omega$, $\varphi(x) = x$, $x \in \{0, 1\}$. Тогда $W_\varphi(0) = 0$, $W_\varphi(1) = 2$ и равенство (13) принимает вид

$$C_{\omega_1, \omega_2}(t) + \frac{2^\nu}{d}(-1)^{\psi(0)} = \sum_{c \in R} \mu_c \left(\sum_{i=0}^{T-1} \chi(\delta_{1,c}(i)) + \frac{2^\nu}{d} \right),$$

где $\{\delta_{1,c}(i)\}_{i=0}^\infty$ — последовательность над R , общий член которой имеет вид

$$\delta_{1,c}(i) = 2^{n-1}\omega(i) + cv(i+t).$$

Из соотношения $x^t \bar{v} \neq \omega$ получим, что $\delta_{1,c}$ является ненулевой последовательностью при всех $c \in R$. Отсюда

$$\left| C_{\omega_1, \omega_2}(t) + \frac{2^\nu}{d}(-1)^{\psi(0)} \right| \leq \sigma(\psi) \frac{2^\nu(d2^{n-1}-1)}{d} 2^{m/2}.$$

Для доказательства первой оценки теоремы остается воспользоваться равенством (4). Вторая оценка следует из первой и из неравенства (11). $\square$

Заметим, что в условиях теоремы 4 не требуется сбалансированности отображения ψ , которая использовалась в теореме 1.

6. Класс булевых функций

Пусть $R = \mathbb{Z}_{2^n}$, $P = \mathbb{Z}_2$, многочлен $F(x) \in P[x]$ имеет степень m и максимальный период, а $G(x) \in R[x]$ есть соответствующий ему *отмеченный многочлен* (см. [5]), т. е. $\bar{G}(x) = F(x)$ и $T = T(G) = T(F) = 2^m - 1$. Такой многочлен $G(x)$ единственный, причем существует достаточно простой рекурсивный способ его построения по $F(x)$ (см. [5]). Пусть v — такая ЛРП над кольцом R с характеристическим многочленом $G(x)$, что $\bar{v}$ — ненулевая последовательность. Рассмотрим булеву функцию $g = g_{v, \psi}$ от m переменных, определенную по правилу: $g(0, 0, \dots, 0) = \psi(0)$ и для всех $i = 0, 1, \dots, 2^m - 2$

$$g(\bar{v}(i), \bar{v}(i+1), \dots, \bar{v}(i+m-1)) = \psi(v(i)). \quad (15)$$

Заметим, что $\bar{v}$ является ЛРП максимального периода $T(\bar{v}) = 2^m - 1$, поэтому среди элементов $(\bar{v}(i), \bar{v}(i+1), \dots, \bar{v}(i+m-1))$, $i = 0, 1, \dots, 2^m - 2$, появляются по одному разу все ненулевые двоичные векторы длины m . Таким образом, правило (15) однозначно задает булеву функцию g . Таблицу данной функции легко построить с использованием регистра сдвига над кольцом R .

Всюду в дальнейшем будем считать, что отображение ψ линейно по старшему биту, т. е. для каждого $a \in R$ с двоичным представлением

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

выполнено равенство

$$\psi(a) = a_{n-1} \oplus \eta(a_0, a_1, \dots, a_{n-2}), \quad (16)$$

где $\eta: P^{n-1} \rightarrow P$ — произвольное отображение. Отметим, что каждое такое отображение ψ является сбалансированным.

Пусть $\text{nl}(g)$ — коэффициент нелинейности (см., например, [7, с. 82]) функции g , определенный равенством

$$\text{nl}(g) = 2^{m-1} - \frac{1}{2} \max_{\vec{a} \in P^m} |W_g(\vec{a})|. \quad (17)$$

Величина $\text{nl}(g)$ равна расстоянию Хэмминга от функции g до класса всех аффинных булевых функций от m переменных.

Теорема 5. Пусть $n > 1$ и булева функция g построена по правилу (15), где ψ задается равенством (16). Тогда

$$\begin{aligned} \text{nl}(g) &\geq 2^{m-1} - \sigma(\psi) (2^{n-1} - 1) 2^{m/2-1} \geq \\ &\geq 2^{m-1} - (2^{n-1} - 1) 2^{(m+n-3)/2}. \end{aligned}$$

Доказательство. Для коэффициента Уолша – Адамара булевой функции g получим

$$\begin{aligned} W_g(\vec{a}) &= \sum_{\vec{b} \in P^m} (-1)^{g(\vec{b}) \oplus a_1 b_1 \oplus \dots \oplus a_m b_m} = \\ &= (-1)^{\psi(0)} + \sum_{i=0}^{T-1} (-1)^{g(\bar{v}(i), \bar{v}(i+1), \dots, \bar{v}(i+m-1)) \oplus a_1 \bar{v}(i) \oplus a_2 \bar{v}(i+1) \oplus \dots \oplus a_m \bar{v}(i+m-1)} = \\ &= (-1)^{\psi(0)} + C_{\omega_1, \omega_2}(0), \end{aligned}$$

где $\{\omega_1(i)\}_{i=0}^{\infty}$ и $\{\omega_2(i)\}_{i=0}^{\infty}$ — последовательности, общие члены которых имеют вид

$$\begin{aligned} \omega_1(i) &= a_1 \bar{v}(i) \oplus a_2 \bar{v}(i+1) \oplus \dots \oplus a_m \bar{v}(i+m-1), \\ \omega_2(i) &= \psi(v(i)). \end{aligned}$$

По аналогии с доказательством теоремы 1 получим

$$W_g(\vec{a}) = \sum_{c \in R} \mu_c \left(\sum_{i=0}^{T-1} \chi(\delta_{a_1, a_2, \dots, a_m, c}(i)) + 1 \right),$$

где $\{\delta_{a_1, a_2, \dots, a_m, c}(i)\}_{i=0}^{\infty}$ — последовательность над кольцом R , общий член которой имеет вид

$$\delta_{a_1, a_2, \dots, a_m, c}(i) = 2^{n-1} a_1 \bar{v}(i) \oplus 2^{n-1} a_2 \bar{v}(i+1) \oplus \dots \oplus 2^{n-1} a_m \bar{v}(i+m-1) + c v(i).$$

Все коэффициенты μ_c отображения ψ , соответствующие необратимым элементам c в кольце R , равны 0 (см. [9, предложение 2]). Поэтому достаточно ограничиться суммированием по всем обратимым элементам c . Учитывая, что $n > 1$ и $\bar{v}$ — ненулевая последовательность, при всех таких c последовательность $\delta_{a_1, \dots, a_m, c}$ будет ненулевой ЛРП с характеристическим многочленом $G(x)$. Таким образом, по аналогии с доказательством теоремы 1 приходим к неравенству

$$|W_g(\vec{a})| \leq \left(\sum_{c \in R} |\mu_c| \right) (2^{n-1} - 1) 2^{m/2} = \sigma(\psi) (2^{n-1} - 1) 2^{m/2}.$$

Первое из доказываемых неравенств следует теперь из (17). Второе неравенство вытекает из соотношения $\sigma(\psi) \leq 2^{(n-1)/2}$, полученного в [9, предложение 2] для всех отображений ψ вида (16). $\square$

Рассмотрим важный с практической точки зрения случай, когда в равенстве (16) функция η тождественно равна 0.

Следствие 2. Пусть выполнены условия теоремы 5 и $\psi(a) = a_{n-1}$. Тогда

$$\text{nl}(g) \geq 2^{m-1} - \left(\frac{2}{\pi} \ln 2^{n-1} + 1 \right) (2^{n-1} - 1) 2^{m/2-1}.$$

Доказательство. Утверждение непосредственно следует из оценки

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

доказанной в [11, теорема 1]. $\square$

Результат, приведенный в следствии 2, ранее был сформулирован в [12]. Там же отмечалось, что булева функция g , соответствующая отображению $\psi(a) = a_{n-1}$, $a \in \mathbb{Z}_{2^n}$, при условии $m > 2^n$ имеет степень нелинейности (степень многочлена Жегалкина), равную 2^{n-1} .

Полученные результаты и возможность простого построения функций с использованием линейных регистров сдвига свидетельствуют о важности дальнейшего исследования рассматриваемого класса булевых функций.

Список литературы

- [1] Кузьмин А. С., Куракин В. Л., Нечаев А. А., “Псевдослучайные и полилинейные последовательности”, *Труды по дискретной математике*, **1** (1997), 139–202.
- [2] Nawaz Y., Gong G., “WG: a family of stream ciphers with designed randomness properties”, *Inform. Sci.*, **178**:7 (2008), 1903–1916.
- [3] Гольтваница М. А., Зайцев С. Н., Нечаев А. А., “Скрученные линейные рекурренты максимального периода над кольцами Галуа”, *Фундам. и прикл. матем.*, **17**:3 (2012), 5–23.
- [4] Golomb S. W., Gong G., *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge etc.: Cambridge Univ. Press, 2005, 438 pp.
- [5] Нечаев А. А., “Цикловые типы линейных подстановок над конечными коммутативными кольцами”, *Матем. сб.*, **184**:3 (1993), 21–56.
- [6] *Словарь криптографических терминов*, /под общ. ред. Б. А. Погорелова, В. Н. Сачкова, М.: МЦНМО, 2006, 92 с.
- [7] Логачев О. А., Сальников А. А., Яценко В. В., *Булевы функции в теории кодирования и криптологии*, М.: МЦНМО, 2012, 584 с.
- [8] Камловский О. В., “Количество появлений элементов в выходных последовательностях фильтрующих генераторов”, *Прикладная дискретная математика*, № 3(21) (2013), 11–25.
- [9] Камловский О. В., “Равномерные последовательности над простыми полями, построенные из одного класса линейных рекуррент над кольцами вычетов”, *Проблемы передачи информации*, **50**:2 (2014), 60–76.
- [10] Камловский О. В., Кузьмин А. С., “Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа”, *Фундам. и прикл. матем.*, **6**:4 (2000), 1083–1094.
- [11] Камловский О. В., “Метод тригонометрических сумм для исследования частот t -грамм в старших координатных последовательностях линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$ ”, *Математические вопросы криптографии*, **1**:4 (2010), 33–62.
- [12] Былков Д. Н., “Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент”, *Прикладная дискретная математика. Приложение*, **7** (2014), 59–60.