УДК 621.391.1:004.7

ЧАСТОТНЫЕ ХАРАКТЕРИСТИКИ ЦИКЛОВ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ КОМБИНИРУЮЩИХ ГЕНЕРАТОРОВ НАД ПОЛЕМ ИЗ ДВУХ ЭЛЕМЕНТОВ

И. Б. Биляк, О. В. Камловский

г. Москва, Россия

Приводятся формулы для подсчёта числа элементов на циклах выходных последовательностей комбинирующих генераторов над полем из двух элементов. Из этих формул выводятся некоторые оценки рассматриваемых частот. Получены формулы для вычисления автокорреляционных функций выходных последовательностей и расстояний Хемминга между отрезками последовательностей.

Ключевые слова: *комбинирующий генератор, линейные рекуррентные последовательности, статистические свойства рекуррент, псевдослучайные последовательности.*

DOI 10.17223/20710410/29/2

FREQUENCY CHARACTERISTICS OF CYCLES IN OUTPUT SEQUENCES GENERATED BY COMBINING GENERATORS OVER THE FIELD OF TWO ELEMENTS

I. B. Bilyak, O. V. Kamlovskii

Moscow, Russia

E-mail: bil-ib@mail.ru, ov-kam@yandex.ru

Some formulas are given for counting the number of elements in the cycles of output sequences generated by combining generators over the field of two elements. From these formulas, some estimates of the considered frequencies appear. Also, formulas for calculation of the autocorrelation functions and Hamming distances between the line segments of these sequences are obtained.

Keywords: *combining generator, linear recurrent sequences, distribution properties of recurrent, a pseudo-random sequence.*

Введение

Пусть $P = \mathrm{GF}(2)$, $F_1(x), \ldots, F_k(x)$ — многочлены над полем P, имеющие степени $m_1, \ldots, m_k$ соответственно. Для каждой булевой функции $\varphi(x_1, \ldots, x_k)$ от k переменных комбинирующий генератор (см. [1, с. 272; 2, с. 311; 3, с. 92]) вырабатывает выходную последовательность v, элементы которой имеют вид

$$v(i) = \varphi(u_1(i), u_2(i), \ldots, u_k(i)), \quad i \geqslant 0, \tag{1}$$

где u_j — ненулевая линейная рекуррентная последовательность (ЛРП) над полем P с характеристическим многочленом $F_j(x)$ для всех $j \in \{1, 2, \ldots, k\}$.

Наибольший интерес к исследованию комбинирующих генераторов отмечался с 1966 по 1986 г. Подробный обзор зарубежных публикаций за этот период представлен в работе [3, с. 92–93]. Там же приводятся все основные результаты о рангах (линейной сложности) последовательностей v, построенных по правилу (1) и основы корреляционной атаки на начальные отрезки ЛРП, приводящей к необходимости выбора корреляционно-иммунных функций усложнения φ [3, с. 93–141].

Вопрос о частотных характеристиках последовательностей v, построенных по правилу (1), оказался менее изученным. Авторам не известны результаты о распределении элементов в последовательностях v. Исключение составляет работа [2], где В. М. Фомичев для случая $P = \mathrm{GF}(2)$ получил точные формулы для вычисления частот появлений элементов на циклах последовательностей v и привёл оценки рассматриваемых частот.

Данная работа продолжает эти исследования. Предлагается другая формула для вычисления частот появлений элементов на циклах, основанная на знании коэффициентов Уолша — Адамара булевой функции φ. С использованием этой формулы приводятся оценки рассматриваемых частот в ситуации, когда φ — корреляционно-иммунная булева функция. Кроме того, приводится формула для вычисления автокорреляционной функции последовательности v, что позволяет находить расстояния Хемминга между отрезками выходных последовательностей комбинирующих генераторов, полученных на различных ключах.

1. Периоды и ранги выходных последовательностей

Последовательность v, определённая равенством (1), является периодической. Её минимально возможный период $T(v)$ делит наименьшее общее кратное чисел $T(u_1), T(u_2), \ldots, T(u_k)$. В частности, v является ЛРП над полем P [4, утверждение 10, с. 319]. Приведём результат [1, теорема 4, с. 273; 3, corollary 5.15], позволяющий достаточно просто находить ранг последовательности v, который определяется как наименьшая из всех возможных степеней характеристических многочленов последовательности v.

Теорема 1. Пусть $P = \mathrm{GF}(2)$, $F_1(x), \ldots, F_k(x)$ — неприводимые многочлены над полем P попарно взаимно простых степеней $m_1, \ldots, m_k$ соответственно. Тогда если многочлен Жегалкина функции φ имеет вид

$$\varphi(x_1, \ldots, x_k) = \sum_{s=1}^{k} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant k} c_{i_1 i_2 \ldots i_s} x_{i_1} x_{i_2} \ldots x_{i_s},$$

то

$$\operatorname{rank} v = \sum_{s=1}^{k} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant k} c_{i_1 i_2 \ldots i_s} m_{i_1} m_{i_2} \ldots m_{i_s}.$$

В процессе доказательства этой теоремы получено следующее утверждение.

Утверждение 1 [3, lemma 5.12]. В условиях теоремы 1 для всех чисел i_1, i_2, …, i_s, таких, что $1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant k$, последовательность $u_{i_1} u_{i_2} \ldots u_{i_s}$ с элементами

$$u_{i_1} u_{i_2} \ldots u_{i_s}(i) = u_{i_1}(i) u_{i_2}(i) \ldots u_{i_s}(i), \quad i \geqslant 0,$$

является ЛРП над полем P с неприводимым характеристическим многочленом степени $m_{i_1} m_{i_2} \cdots m_{i_s}$.

Утверждение 1 позволяет найти период $T(v)$ последовательности v.

Теорема 2. Пусть в условиях теоремы 1 функция φ существенно зависит от всех своих переменных. Тогда $T(v) = T(u_1)T(u_2)\cdots T(u_k)$.

Доказательство. Последовательность v задается следующим образом:

$$v = \sum_{s=1}^{k} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant k} c_{i_1 i_2 \ldots i_s} u_{i_1} u_{i_2} \ldots u_{i_s}.$$

Согласно утверждению 1, все ненулевые ЛРП, входящие в рассматриваемую сумму, имеют неприводимые характеристические многочлены различных степеней. В работе [4, утверждение 11, с. 321] показано, что для ЛРП ω_1, ω_2, …, ω_l, у которых указаны взаимно простые характеристические многочлены, выполнено равенство

$$T(\omega_1 + \omega_2 + \ldots + \omega_l) = [T(\omega_1), T(\omega_2), \ldots, T(\omega_l)].$$

Поэтому $T(v)$ равен наименьшему общему кратному чисел $T(u_{i_1} u_{i_2} \ldots u_{i_s})$, рассматриваемых для тех наборов i_1, i_2, …, i_s, при которых $c_{i_1 i_2 \ldots i_s} = 1$.

В работе [5, теорема 8.70] показано, что для ненулевых ЛРП ω_1, ω_2, …, ω_l, имеющих попарно взаимно простые периоды, выполнено равенство

$$T(\omega_1 \omega_2 \cdots \omega_l) = T(\omega_1)T(\omega_2)\cdots T(\omega_l).$$

Числа $T(u_1), \ldots, T(u_k)$ являются делителями чисел $2^{m_1} - 1, \ldots, 2^{m_k} - 1$ соответственно. В силу попарной взаимной простоты чисел $m_1, \ldots, m_k$ для всех $i \neq j$, $i, j \in \{1, 2, \ldots, k\}$, получим равенство $(2^{m_i} - 1, 2^{m_j} - 1) = 1$, а значит, $(T(u_i), T(u_j)) = 1$. Таким образом,

$$T(u_{i_1} u_{i_2} \ldots u_{i_s}) = T(u_{i_1})T(u_{i_2})\cdots T(u_{i_s})$$

и $T(v)$ равен наименьшему общему кратному чисел $T(u_{i_1}), T(u_{i_2}), \ldots, T(u_{i_s})$, рассматриваемых для тех наборов $i_1, i_2, \ldots, i_s$, при которых $c_{i_1 i_2 \ldots i_s} = 1$. Учитывая, что булева функция φ существенно зависит от всех своих переменных, получим $T(v) = T(u_1)T(u_2)\cdots T(u_k)$. ■

Отметим, что ранее теорема 2 была доказана в частном случае, когда все многочлены $F_1(x)$, …, $F_k(x)$ являются примитивными многочленами, т. е. многочленами максимально возможных периодов $2^{m_1} - 1$, …, $2^{m_k} - 1$ соответственно [2, теорема 18.2].

В условиях теоремы 1 последовательность v является чисто периодической, так как все последовательности $u_1, \ldots, u_k$ являются чисто периодическими.

Некоторые нижние оценки периода последовательности v (не обязательно двоичной), полученной в результате усложнения последовательностей u_1, …, u_k с использованием функции φ, приводятся в работе [6, теорема 1].

2. Формулы В. М. Фомичева

Изучим частотные характеристики последовательности v, определённой равенством (1). Исследуем величину $N(z, v)$, равную количеству появлений элемента $z \in P$ среди элементов $v(0), v(1), \ldots, v(T(v) - 1)$. Приведём вспомогательный результат из работы [2], представляющий и самостоятельный интерес. Этот результат формулируется как очевидный (см. [2, доказательство теоремы 18.2]). Для полноты изложения приведём его доказательство.

Утверждение 2. Пусть $P = \mathrm{GF}(2)$, $F_1(x), \ldots, F_k(x) \in P[x]$ — примитивные многочлены попарно взаимно простых степеней $m_1, \ldots, m_k$ соответственно, $z_j \in P$, u_j —

ЛРП максимального периода с характеристическим многочленом $F_j(x)$, $j \in \{1, 2, \ldots, k\}$, $T = (2^{m_1} - 1) \cdots (2^{m_k} - 1)$. Тогда для числа $N(z_1, \ldots, z_k, u_1, \ldots, u_k)$ решений системы уравнений

$$\begin{cases} u_1(i) = z_1, \\ u_2(i) = z_2, \\ \quad \ldots \\ u_k(i) = z_k \end{cases}$$

относительно неизвестного $i \in \{0, 1, \ldots, T-1\}$ справедливо равенство

$$N(z_1, \ldots, z_k, u_1, \ldots, u_k) = (2^{m_1-1} - 1 + z_1)(2^{m_2-1} - 1 + z_2) \cdots (2^{m_k-1} - 1 + z_k).$$

Доказательство. Рассмотрим упорядоченные наборы

$$\alpha_i = (u_1(i), \ldots, u_1(i + m_1 - 1), u_2(i), \ldots, u_2(i + m_2 - 1), \ldots, u_k(i), \ldots, u_k(i + m_k - 1)),$$

где $i \in \{0, 1, \ldots, T-1\}$. Заметим, что равенство $\alpha_i = \alpha_j$ влечёт соотношения $T(u_1) \,|\, i-j$, …, $T(u_k) \,|\, i - j$, а значит, $T(u_1) \cdots T(u_k) = T \,|\, i - j$. Отсюда следует, что все рассматриваемые векторы α_i попарно различны. Тогда

$$\{\alpha_i : i = 0, 1, \ldots, T-1\} = (P^{m_1} \backslash \{\mathbf{0}\}) \times \ldots \times (P^{m_k} \backslash \{\mathbf{0}\})$$

и число $N(z_1, \ldots, z_k, u_1, \ldots, u_k)$ равно количеству наборов из множества $(P^{m_1} \backslash \{\mathbf{0}\}) \times \ldots \times (P^{m_k} \backslash \{\mathbf{0}\})$, имеющих следующий вид:

$$(z_1, \underbrace{*, \ldots, *}_{m_1-1}, z_2, \underbrace{*, \ldots, *}_{m_2-1}, \ldots, z_k, \underbrace{*, \ldots, *}_{m_k-1}),$$

где на местах, обозначенных символом $*$, стоят произвольные элементы поля P. Число таких наборов равно $(2^{m_1-1} - 1 + z_1)(2^{m_2-1} - 1 + z_2) \cdots (2^{m_k-1} - 1 + z_k)$. ■

Заметим, что число решений не зависит от выбора ненулевых ЛРП $u_1, \ldots, u_k$.

Утверждение 2 описывает строение графа переходов автоматной модели комбинирующего генератора. При выборе произвольного начального состояния α_0 из множества $(P^{m_1} \backslash \{\mathbf{0}\}) \times \ldots \times (P^{m_k} \backslash \{\mathbf{0}\})$ в моменты времени $i = 0, 1, \ldots, T-1$ автомат проходит последовательность состояний $\alpha_0, \ldots, \alpha_{T-1}$ и все элементы множества $(P^{m_1} \backslash \{\mathbf{0}\}) \times \ldots \times (P^{m_k} \backslash \{\mathbf{0}\})$ расположены на одном цикле длины T.

Заметим, что, согласно теореме 2, в условиях утверждения 2 имеет место равенство $T(v) = T(u_1) \cdots T(u_k) = (2^{m_1} - 1) \cdots (2^{m_k} - 1) = T$ для каждой функции φ, существенно зависящей от всех своих переменных. Таким образом, справедлива

Теорема 3 [2]. Пусть в условиях утверждения 2 функция φ существенно зависит от всех своих переменных. Тогда

$$N(z, v) = \sum_{\mathbf{z}=(z_1,\ldots,z_k) \in P^k, \varphi(\mathbf{z})=z} (2^{m_1-1} - 1 + z_1)(2^{m_2-1} - 1 + z_2) \cdots (2^{m_k-1} - 1 + z_k).$$

Таким образом, в наиболее интересном с практической точки зрения случае теорема 3 позволяет найти точное значение частот $N(z, v)$.

3. Спектральный подход к исследованию частотных характеристик

Предложим альтернативный подход к исследованию частот $N(z, v)$. Пусть функция $\varphi(x_1, \ldots, x_k)$ имеет коэффициенты Уолша — Адамара [7, с. 76]

$$W_\varphi(\mathbf{a}) = \sum_{x_1,\ldots,x_k \in P} (-1)^{\varphi(x_1,\ldots,x_k) \oplus a_1 x_1 \oplus \ldots \oplus a_k x_k},$$

где $\mathbf{a} = (a_1, \ldots, a_k)$. Тогда

$$(-1)^{\varphi(x_1,\ldots,x_k)} = \frac{1}{2^k} \sum_{\mathbf{a} \in P^k} W_\varphi(\mathbf{a}) (-1)^{a_1 x_1 \oplus \ldots \oplus a_k x_k},$$

и из равенства (1) получим

$$(-1)^{v(i)} = (-1)^{\varphi(u_1(i),\ldots,u_k(i))} = \frac{1}{2^k} \sum_{\mathbf{a} \in P^k} W_\varphi(\mathbf{a}) (-1)^{a_1 u_1(i) \oplus \ldots \oplus a_k u_k(i)}. \tag{2}$$

Следующее утверждение сводит исследование частот $N(z, v)$ к исследованию коэффициентов Уолша — Адамара функции φ и некоторой суммы, зависящей только от знаков ЛРП.

Утверждение 3. Для последовательности v, построенной по правилу (1), справедливы равенства

$$N(0, v) = T(v) \left(1 - \frac{\|\varphi\|}{2^k}\right) + \frac{1}{2^{k+1}} \sum_{\mathbf{a} \in P^k \setminus \{\mathbf{0}\}} W_\varphi(\mathbf{a}) \sigma(\mathbf{a}, u_1, \ldots, u_k),$$

$$N(1, v) = \frac{T(v)\|\varphi\|}{2^k} - \frac{1}{2^{k+1}} \sum_{\mathbf{a} \in P^k \setminus \{\mathbf{0}\}} W_\varphi(\mathbf{a}) \sigma(\mathbf{a}, u_1, \ldots, u_k),$$

где $\|\varphi\|$ — вес функции φ, а величина $\sigma(\mathbf{a}, u_1, \ldots, u_k)$ определена равенством

$$\sigma(\mathbf{a}, u_1, \ldots, u_k) = \sum_{i=0}^{T(v)-1} (-1)^{a_1 u_1(i) \oplus \ldots \oplus a_k u_k(i)}.$$

Доказательство. Заметим, что справедливы соотношения

$$N(z, v) = \frac{1}{2} \sum_{i=0}^{T(v)} (1 + (-1)^{v(i) \oplus z}) = \frac{T(v)}{2} + \frac{1}{2}(-1)^z \sum_{i=0}^{T(v)-1} (-1)^{v(i)}.$$

Подставляя равенство (2), будем иметь

$$N(z, v) = \frac{T(v)}{2} + \frac{1}{2}(-1)^z \sum_{i=0}^{T(v)-1} \frac{1}{2^k} \sum_{\mathbf{a} \in P^k} W_\varphi(\mathbf{a}) (-1)^{a_1 u_1(i) \oplus \ldots \oplus a_k u_k(i)} =$$

$$= \frac{T(v)}{2} + \frac{1}{2^{k+1}}(-1)^z \sum_{\mathbf{a} \in P^k} W_\varphi(\mathbf{a}) \sum_{i=0}^{T(v)-1} (-1)^{a_1 u_1(i) \oplus \ldots \oplus a_k u_k(i)} =$$

$$= \frac{T(v)}{2} + \frac{1}{2^{k+1}}(-1)^z W_\varphi(\mathbf{0}) T(v) + \frac{1}{2^{k+1}}(-1)^z \sum_{\mathbf{a} \in P^k \setminus \{\mathbf{0}\}} W_\varphi(\mathbf{a}) \sum_{i=0}^{T(v)-1} (-1)^{a_1 u_1(i) \oplus \ldots \oplus a_k u_k(i)}.$$

Для завершения доказательства остаётся воспользоваться равенством $W_\varphi(\mathbf{0}) = 2^k - 2\|\varphi\|$. ■

Значения величины $\sigma(\mathbf{a}, u_1, \ldots, u_k)$ в некоторых случаях удаётся точно подсчитать.

Утверждение 4. Пусть $P = \mathrm{GF}(2)$, $\mathbf{a} = (a_1, \ldots, a_k) \in P^k$, u_j — ЛРП максимального периода $2^{m_j} - 1$ с примитивным характеристическим многочленом $F_j(x)$, где $j \in \{1, 2, \ldots, k\}$; $T = (2^{m_1} - 1) \cdots (2^{m_k} - 1)$. Тогда если числа $m_1, \ldots, m_k$ попарно взаимно просты, то

$$\sigma(\mathbf{a}, u_1, \ldots, u_k) = \frac{(-1)^{\|\mathbf{a}\|} T}{(2^{m_1} - 1)^{a_1} (2^{m_2} - 1)^{a_2} \ldots (2^{m_k} - 1)^{a_k}},$$

где $\|\mathbf{a}\|$ — вес вектора $\mathbf{a}$.

Доказательство. Если вектор $\mathbf{a}$ нулевой, то равенство выполнено. Пусть $\|\mathbf{a}\| = s$, $s \in \mathbb{N}$, и $a_{j_1}, \ldots, a_{j_s}$ — все ненулевые координаты вектора $\mathbf{a}$, где $1 \leqslant j_1 < \ldots < j_s \leqslant k$. Тогда

$$\sigma(\mathbf{a}, u_1, \ldots, u_k) = \sum_{i=0}^{T-1} (-1)^{u_{j_1}(i) \oplus \ldots \oplus u_{j_s}(i)}.$$

Введём обозначение $v_t = u_{j_t}$, где $t \in \{1, 2, \ldots, s\}$. Тогда

$$\sigma(\mathbf{a}, u_1, \ldots, u_k) = \sum_{i=0}^{T-1} (-1)^{v_1(i)} \ldots (-1)^{v_s(i)}. \tag{3}$$

Представим каждую ЛРП v_t с использованием функции след:

$$v_t(i) = \mathrm{tr}_P^{Q_t}(a_t \alpha_t^i), \quad i \geqslant 0,$$

где $Q_t = \mathrm{GF}(2^{m_{j_t}})$; α_t — корень многочлена $F_{j_t}(x)$ в поле Q_t; a_t — ненулевой элемент поля Q_t. С использованием [5, равенство (5.17)] получим

$$(-1)^{v_t(i)} = (-1)^{\mathrm{tr}_P^{Q_t}(a_t \alpha_t^i)} = \chi_t(a_t \alpha_t^i) = \frac{1}{2^{m_{j_t}} - 1} \sum_{\psi_t} G(\bar{\psi}_t, \chi_t) \psi_t(a_t \alpha_t^i),$$

где χ_t — аддитивный характер поля Q_t, определённый равенством $\chi_t(x) = (-1)^{\mathrm{tr}_P^{Q_t}(x)}$, $x \in Q_t$, суммирование осуществляется по всем мультипликативным характерам ψ_t поля Q_t; $G(\bar{\psi}_t, \chi_t)$ — сумма Гаусса. Тогда из равенства (3) будем иметь

$$\sigma(\mathbf{a}, u_1, \ldots, u_k) = \frac{1}{(2^{m_{j_1}} - 1) \cdots (2^{m_{j_s}} - 1)} \sum_{\psi_1, \ldots, \psi_s} \prod_{t=1}^{s} G(\bar{\psi}_t, \chi_t) \psi_t(a_t) \sum_{i=0}^{T-1} (\psi_1(\alpha_1) \cdots \psi_s(\alpha_s))^i.$$

Заметим, что

$$\sum_{i=0}^{T-1} (\psi_1(\alpha_1) \cdots \psi_s(\alpha_s))^i = \begin{cases} \dfrac{(\psi_1(\alpha_1) \cdots \psi_s(\alpha_s))^T - 1}{\psi_1(\alpha_1) \ldots \psi_s(\alpha_s) - 1}, & \text{если } \psi_1(\alpha_1) \cdots \psi_s(\alpha_s) \neq 1, \\ T, & \text{если } \psi_1(\alpha_1) \cdots \psi_s(\alpha_s) = 1, \end{cases}$$

а так как $(\psi_1(\alpha_1) \cdots \psi_s(\alpha_s))^T = \psi_1(\alpha_1^T) \cdots \psi_s(\alpha_s^T) = \psi_1(e) \cdots \psi_s(e) = 1$, то

$$\sum_{i=0}^{T-1} (\psi_1(\alpha_1) \ldots \psi_s(\alpha_s))^i = \begin{cases} 0, & \text{если } \psi_1(\alpha_1) \cdots \psi_s(\alpha_s) \neq 1, \\ T, & \text{если } \psi_1(\alpha_1) \cdots \psi_s(\alpha_s) = 1. \end{cases}$$

В силу того, что $\psi_t(\alpha_t)$ является корнем степени $2^{m_{j_t}} - 1$ из единицы для всех $t \in \{1, 2, \ldots, s\}$, а числа $2^{m_{j_1}} - 1, \ldots, 2^{m_{j_s}} - 1$ попарно взаимно просты, соотношение $\psi_1(\alpha_1) \cdots \psi_s(\alpha_s) = 1$ выполнено только в случае, когда $\psi_1(\alpha_1) = \ldots = \psi_s(\alpha_s) = 1$.

Другими словами, каждый из характеров $\psi_1, \ldots, \psi_s$ должен быть тривиальным. Значит,

$$\sigma(\mathbf{a}, u_1, \ldots, u_k) = \frac{T}{(2^{m_{j_1}} - 1) \cdots (2^{m_{j_s}} - 1)} G(\psi_0^{(1)}, \chi_1) \cdots G(\psi_0^{(s)}, \chi_s),$$

где $\psi_0^{(1)}, \ldots, \psi_0^{(s)}$ — тривиальные мультипликативные характеры полей $Q_1, \ldots, Q_s$ соответственно. Согласно [5, равенство (5.14)], для всех $j \in \{1, 2, \ldots, k\}$ выполнено $G(\psi_0^{(j)}, \chi_1) = -1$. Таким образом, получим

$$\sigma(\mathbf{a}, u_1, \ldots, u_k) = \frac{(-1)^s T}{(2^{m_{j_1}} - 1)(2^{m_{j_2}} - 1) \ldots (2^{m_{j_s}} - 1)} = \frac{(-1)^{\|\mathbf{a}\|} T}{(2^{m_1} - 1)^{a_1} (2^{m_2} - 1)^{a_2} \ldots (2^{m_k} - 1)^{a_k}}.$$

Утверждение доказано. ■

Непосредственно из утверждений 3 и 4 получим основной результат этого пункта.

Теорема 4. Пусть $P = \mathrm{GF}(2)$, $u_1, \ldots, u_k$ — ЛРП максимального периода над полем P, имеющие периоды $2^{m_1} - 1, \ldots, 2^{m_k} - 1$ соответственно, причём числа $m_1, \ldots, m_k$ попарно взаимно просты, $T = (2^{m_1} - 1) \cdots (2^{m_k} - 1)$. Тогда для последовательности v, определённой равенством (1), где функция φ существенно зависит от всех своих переменных, справедливы следующие соотношения:

$$N(0, v) = T - \frac{T\|\varphi\|}{2^k} + \frac{T}{2^{k+1}} \sum_{\mathbf{a} \in P^k \setminus \{\mathbf{0}\}} \frac{(-1)^{\|\mathbf{a}\|} W_\varphi(\mathbf{a})}{(2^{m_1} - 1)^{a_1} (2^{m_2} - 1)^{a_2} \cdots (2^{m_k} - 1)^{a_k}},$$

$$N(1, v) = \frac{T\|\varphi\|}{2^k} - \frac{T}{2^{k+1}} \sum_{\mathbf{a} \in P^k \setminus \{\mathbf{0}\}} \frac{(-1)^{\|\mathbf{a}\|} W_\varphi(\mathbf{a})}{(2^{m_1} - 1)^{a_1} (2^{m_2} - 1)^{a_2} \cdots (2^{m_k} - 1)^{a_k}}.$$

Отметим, что по столбцу значений булевой функции $\varphi(x_1, \ldots, x_k)$ достаточно просто находится набор $W_\varphi(\mathbf{a})$, $\mathbf{a} \in P^k \setminus \{\mathbf{0}\}$, её коэффициентов Уолша — Адамара, а также набор $\tilde{W}_\varphi(\mathbf{a}) = -W_\varphi(\mathbf{a})/2$, $\mathbf{a} \in P^k \setminus \{\mathbf{0}\}$, её коэффициентов Фурье. Таким образом, теорема 4 позволяет в наиболее интересном случае вычислить частоты $N(z, v)$.

4. Примеры

Рассмотрим некоторые примеры использования теорем 3 и 4. Во всех примерах функция φ существенно зависит от всех своих переменных, поэтому, согласно теореме 2, период $T(v)$ последовательности v, построенной по правилу (1), равен $T = (2^{m_1} - 1) \cdots (2^{m_k} - 1)$.

Утверждение 5. Пусть $\varphi(x_1, \ldots, x_k) = x_1 \oplus \ldots \oplus x_k \oplus \varepsilon$, где $\varepsilon \in \{0, 1\}$. Тогда

$$N(0, v) = \frac{T + (-1)^{k+\varepsilon}}{2}, \quad N(1, v) = \frac{T - (-1)^{k+\varepsilon}}{2}, \quad \operatorname{rank} v = m_1 + \ldots + m_k.$$

Доказательство. Для булевой функции $\varphi(x_1, \ldots, x_k) = x_1 \oplus \ldots \oplus x_k \oplus \varepsilon$ имеем

$$W_\varphi(1, \ldots, 1) = (-1)^\varepsilon 2^k, \quad W_\varphi(\mathbf{a}) = 0 \quad \text{для всех} \quad \mathbf{a} \neq (1, \ldots, 1).$$

Тогда с использованием теоремы 4 получим

$$N(0, v) = T \left(1 - \frac{\|\varphi\|}{2^k}\right) + \frac{(-1)^{k+\varepsilon}}{2} = \frac{T + (-1)^{k+\varepsilon}}{2},$$

$$N(1, v) = \frac{T\|\varphi\|}{2^k} - \frac{(-1)^{k+\varepsilon}}{2} = \frac{T - (-1)^{k+\varepsilon}}{2}.$$

Равенство для $\operatorname{rank} v$ непосредственно следует из теоремы 1. ■

Отметим, что формулы для частот из утверждения 5 были ранее получены в работе [8, с. 133].

Утверждение 6. Пусть $\varphi(x_1, \ldots, x_k) = x_1^{\alpha_1} \cdots x_k^{\alpha_k}$, где $\alpha_1, \ldots, \alpha_k \in \{0, 1\}$ (считаем, что $x_i^0 = \bar{x}_i$, $x_i^1 = x_i$, $i = 1, \ldots, k$). Тогда

$$N(0, v) = T - (2^{m_1 - 1} - 1 + \alpha_1) \cdots (2^{m_k - 1} - 1 + \alpha_k),$$
$$N(1, v) = (2^{m_1 - 1} - 1 + \alpha_1) \cdots (2^{m_k - 1} - 1 + \alpha_k),$$
$$\operatorname{rank} v = (m_1 + \bar{\alpha}_1) \cdots (m_k + \bar{\alpha}_k).$$

Доказательство. С использованием утверждения 2 получим

$$N(1, v) = N(\alpha_1, \ldots, \alpha_k, u_1, \ldots, u_k) = (2^{m_1 - 1} - 1 + \alpha_1) \cdots (2^{m_k - 1} - 1 + \alpha_k),$$
$$N(0, v) = T - N(1, v) = T - (2^{m_1 - 1} - 1 + \alpha_1) \cdots (2^{m_k - 1} - 1 + \alpha_k).$$

Равенство для $\operatorname{rank} v$ непосредственно следует из теоремы 1 и равносильности формул $x_i^{\alpha_i} \equiv x_i \oplus \bar{\alpha}_i$, $i = 1, 2, \ldots, k$. ■

Утверждение 7. Пусть $\varphi(x_1, \ldots, x_k) = x_1 \oplus x_2 x_3 \cdots x_k$. Тогда

$$N(0, v) = (2^{m_1 - 1} - 1)(2^{m_2} - 1) \cdots (2^{m_k} - 1) + 2^{m_2 + \ldots + m_k - k + 1},$$
$$N(1, v) = 2^{m_1 - 1}(2^{m_2} - 1) \cdots (2^{m_k} - 1) - 2^{m_2 + \ldots + m_k - k + 1},$$
$$\operatorname{rank} v = m_1 + m_2 m_3 \cdots m_k.$$

Доказательство. Обозначим через v' последовательность $u_2 \cdots u_k$. С использованием теоремы 3 и утверждения 6 получим

$$N(1, v) = \sum_{\substack{\mathbf{z} = (z_1, \ldots, z_k) \in P^k, \\ \varphi(\mathbf{z}) = 1}} (2^{m_1 - 1} - 1 + z_1)(2^{m_2 - 1} - 1 + z_2) \cdots (2^{m_k - 1} - 1 + z_k) =$$
$$= 2^{m_1 - 1} \sum_{(z_2, \ldots, z_k) \neq (1, \ldots, 1)} (2^{m_2 - 1} - 1 + z_2) \cdots (2^{m_k - 1} - 1 + z_k) + (2^{m_1 - 1} - 1) 2^{m_2 + \cdots + m_k - k + 1} =$$
$$= 2^{m_1 - 1} N(0, v') + (2^{m_1 - 1} - 1) 2^{m_2 + \cdots + m_k - k + 1} =$$
$$= 2^{m_1 - 1}((2^{m_2} - 1) \cdots (2^{m_k} - 1) - 2^{m_2 + \cdots + m_k - k + 1}) + (2^{m_1 - 1} - 1) 2^{m_2 + \cdots + m_k - k + 1} =$$
$$= 2^{m_1 - 1}(2^{m_2} - 1) \cdots (2^{m_k} - 1) - 2^{m_2 + \ldots + m_k - k + 1},$$
$$N(0, v) = T - N(1, v) = (2^{m_1 - 1} - 1)(2^{m_2} - 1) \cdots (2^{m_k} - 1) + 2^{m_2 + \ldots + m_k - k + 1}.$$

Равенство для $\operatorname{rank} v$ непосредственно следует из теоремы 1. ■

Отметим, что в утверждении 7 для подсчёта частот можно воспользоваться теоремой 4, если учесть, что справедливы равенства

$$W_\varphi(\mathbf{a}) = \begin{cases} 0, & \text{если } \mathbf{a} = (0, a_2, \ldots, a_k), (a_2, \ldots, a_k) \in P^{k-1}, \\ 2^k - 4, & \text{если } \mathbf{a} = (1, 0, \ldots, 0), \\ 4(-1)^{\|\mathbf{a}\|}, & \text{если } \mathbf{a} = (1, a_2, \ldots, a_k), (a_2, \ldots, a_k) \neq \mathbf{0}. \end{cases}$$

Утверждение 8. Пусть $\varphi(x_1, \ldots, x_k) = x_1 \oplus \cdots \oplus x_{k-2} \oplus x_{k-1} x_k$. Тогда для каждого $z \in \{0, 1\}$

$$N(z, v) = \frac{T}{2} + \frac{(-1)^{k+z}}{2}(2^{m_{k-1} + m_k - 1} - 2^{m_{k-1}} - 2^{m_k} + 1),$$
$$\operatorname{rank} v = m_1 + \cdots + m_{k-2} + m_{k-1} m_k.$$

Доказательство. Заметим, что справедливы равенства

$$W_\varphi(\mathbf{a}) = \begin{cases} 0, & \text{если } (a_1,\ldots,a_{k-2}) \neq (1,\ldots,1), \\ 2^{k-1}, & \text{если } (a_1,\ldots,a_{k-2}) = (1,\ldots,1), (a_{k-1},a_k) \neq (1,1), \\ -2^{k-1}, & \text{если } \mathbf{a} = (1,1,\ldots,1). \end{cases}$$

Тогда, согласно теореме 4,

$$N(z,v) = \frac{T}{2} + \frac{(-1)^{k+z}}{4}\left((2^{m_{k-1}}-1)(2^{m_k}-1) - (2^{m_k}-1) - (2^{m_{k-1}}-1) - 1\right) = \\ = \frac{T}{2} + \frac{(-1)^{k+z}}{2}(2^{m_{k-1}+m_k-1} - 2^{m_{k-1}} - 2^{m_k} + 1).$$

Равенство для $\operatorname{rank} v$ непосредственно следует из теоремы 1. ■

5. Оценки частот

Использование формул из теорем 3 и 4 не всегда удобно ввиду большого числа слагаемых в них. Представляет интерес получение оценок частот $N(z,v)$. Приведём оценку, полученную по аналогии с доказательством из работы [2, теорема 18.2].

Теорема 5. Пусть $P = \mathrm{GF}(2)$, $z \in P$, $u_1,\ldots,u_k$ — ЛРП максимального периода над полем P, имеющие периоды $2^{m_1}-1,\ldots,2^{m_k}-1$ соответственно, причём числа $m_1,\ldots,m_k$ попарно взаимно просты и $m_1 < m_2 < \ldots < m_k$. Тогда для последовательности v, определённой равенством (1) с функцией φ, существенно зависящей от всех своих переменных, справедливы неравенства

$$2^{m_1+\ldots+m_k-k}(1 - 2^{2-m_1} + 2^{2-m_1-k})|\varphi^{-1}(z)| \leqslant N(z,v) \leqslant 2^{m_1+\ldots+m_k-k}|\varphi^{-1}(z)|,$$

где $\varphi^{-1}(z) = \{\mathbf{a} \in P^k : \varphi(\mathbf{a}) = z\}$.

Доказательство. Верхняя оценка вытекает из теоремы 3 и неравенства

$$(2^{m_1-1}-1+z_1)(2^{m_2-1}-1+z_2)\cdots(2^{m_k-1}-1+z_k) \leqslant 2^{m_1+\ldots+m_k-k},$$

справедливого для всех $z_1,z_2,\ldots,z_k \in P$. Докажем справедливость нижней оценки. Методом математической индукции по параметру k нетрудно показать, что для всех неотрицательных действительных чисел $a_1,\ldots,a_k$ верно неравенство $(1-a_1)\cdots\times$ $\times(1-a_k) \geqslant 1 - a_1 - \ldots - a_k$. Тогда с использованием теоремы 3 получаем

$$N(z,v) = \sum_{\mathbf{z}\in\varphi^{-1}(z)} 2^{m_1+\ldots+m_k-k}\left(1-\frac{1-z_1}{2^{m_1-1}}\right)\ldots\left(1-\frac{1-z_k}{2^{m_k-1}}\right) \geqslant \\ \geqslant 2^{m_1+\ldots+m_k-k}|\varphi^{-1}(z)|\left(1-\frac{1}{2^{m_1-1}}\right)\ldots\left(1-\frac{1}{2^{m_k-1}}\right) \geqslant \\ \geqslant 2^{m_1+\ldots+m_k-k}|\varphi^{-1}(z)|\left(1-\frac{1}{2^{m_1-1}}-\ldots-\frac{1}{2^{m_k-1}}\right) \geqslant \\ \geqslant 2^{m_1+\ldots+m_k-k}|\varphi^{-1}(z)|\left(1-\frac{1}{2^{m_1-1}}-\frac{1}{2^{m_1}}-\ldots-\frac{1}{2^{m_1+k-2}}\right) = \\ = 2^{m_1+\ldots+m_k-k}|\varphi^{-1}(z)|(1-2^{2-m_1}+2^{2-m_1-k}).$$

Теорема доказана. ■

Верхняя оценка из теоремы 5 доказана в [2, теорема 18.2]. В этой же работе приводится нижняя оценка, которая в условиях теоремы 5 имеет следующий вид:

$$N(1,v) > 2^{m_1+\ldots+m_k-k}(1-2^{1-m_1})|\varphi^{-1}(z)|.$$

Доказательство этой оценки ошибочно и сама оценка не верна. Приведём соответствующий пример. Пусть $k \geqslant 2$, $\varphi(x_1,x_2,\ldots,x_k) = \bar{x}_1\bar{x}_2\cdots\bar{x}_k$. Тогда, согласно утверждению 6,

$$N(1,v) = (2^{m_1-1}-1)(2^{m_2-1}-1)\cdots(2^{m_k-1}-1) < (2^{m_1-1}-1)2^{m_2+\ldots+m_k-k+1},$$

а рассматриваемая оценка имеет вид

$$N(1,v) > 2^{m_1+\ldots+m_k-k} - 2^{m_2+\ldots+m_k-k+1},$$

что не верно.

Получение общих оценок с использованием теоремы 4 представляется затруднительным. Применим эти результаты для важного класса функций усложнения φ, называемых корреляционно-иммунными [3, § 5.3; 7, гл. 7].

Теорема 6. Пусть, в условиях теоремы 5, $T = (2^{m_1}-1)\cdots(2^{m_k}-1)$ и φ является корреляционно-иммунной порядка d функцией. Тогда

$$|N(z,v) - \delta(z)| \leqslant (2^{m_{d+2}}-1)\cdots(2^{m_k}-1)\frac{|M(\varphi)\backslash\{\mathbf{0}\}|^{1/2}}{2},$$

где $M(\varphi) = \{\mathbf{a} \in P^k : W_\varphi(\mathbf{a}) \neq 0\}$, а величина $\delta(z)$ определена равенствами

$$\delta(z) = \begin{cases} T\dfrac{\|\varphi\|}{2^k}, & \text{если } z = 1, \\ T\left(1 - \dfrac{\|\varphi\|}{2^k}\right), & \text{если } z = 0. \end{cases}$$

Доказательство. Из теоремы 4 имеем

$$|N(z,v) - \delta(z)| = \frac{T}{2^{k+1}}\left|\sum_{\mathbf{a}\in P^k\backslash\{\mathbf{0}\}} \frac{(-1)^{\|\mathbf{a}\|}W_\varphi(\mathbf{a})}{(2^{m_1}-1)^{a_1}\cdots(2^{m_k}-1)^{a_k}}\right|.$$

Отсюда получим неравенство

$$|N(z,v) - \delta(z)| \leqslant \frac{T}{2^{k+1}}\sum_{\mathbf{a}\in P^k\backslash\{\mathbf{0}\}} \frac{|W_\varphi(\mathbf{a})|}{(2^{m_1}-1)^{a_1}\cdots(2^{m_k}-1)^{a_k}}.$$

Согласно [7, теорема 7.10], $W_\varphi(\mathbf{a}) = 0$ для всех векторов $\mathbf{a} \in P^k$ веса $1 \leqslant \|\mathbf{a}\| \leqslant d$. Следовательно,

$$|N(z,v) - \delta(z)| \leqslant \frac{T}{2^{k+1}(2^{m_1}-1)\ldots(2^{m_{d+1}}-1)}\sum_{\mathbf{a}\in P^k\backslash\{\mathbf{0}\}} |W_\varphi(\mathbf{a})|. \tag{4}$$

Воспользуемся неравенством Коши [4, с. 131] и равенством Парсеваля [7, с. 80] для получения оценки сверху суммы модулей коэффициентов Уолша — Адамара. Тогда

$$\sum_{\mathbf{a}\in P^k\setminus\{\mathbf{0}\}} |W_\varphi(\mathbf{a})| = \sum_{\mathbf{a}\in M(\varphi)\setminus\{\mathbf{0}\}} |W_\varphi(\mathbf{a})| \leqslant |M(\varphi)\setminus\{\mathbf{0}\}|^{1/2} \left(\sum_{\mathbf{a}\in M(\varphi)\setminus\{\mathbf{0}\}} |W_\varphi(\mathbf{a})|^2 \right)^{1/2} \leqslant$$

$$\leqslant |M(\varphi)\setminus\{\mathbf{0}\}|^{1/2} \left(\sum_{\mathbf{a}\in M(\varphi)} |W_\varphi(\mathbf{a})|^2 \right)^{1/2} = |M(\varphi)\setminus\{\mathbf{0}\}|^{1/2} 2^k.$$

Подставив полученную оценку в неравенство (4), получим

$$|N(z,v) - \delta(z)| \leqslant (2^{m_{d+2}} - 1)\cdots(2^{m_k} - 1)\frac{|M(\varphi)\setminus\{\mathbf{0}\}|^{1/2}}{2}.$$

Теорема доказана. ■

Для сбалансированных корреляционно-иммунных порядка d функций (d-устойчивых функций) получаем следующий результат.

Следствие 1. Пусть, в условиях теоремы 5, функция φ является d-устойчивой. Тогда

$$\left| N(z,v) - \frac{T}{2} \right| \leqslant (2^{m_{d+2}} - 1)\cdots(2^{m_k} - 1)\frac{|M(\varphi)\setminus\{\mathbf{0}\}|^{1/2}}{2}.$$

Приведём оценку, не зависящую от величины $M(\varphi)$.

Следствие 2. Пусть, в условиях теоремы 5, φ является корреляционно-иммунной порядка d функцией. Тогда

$$|N(z,v) - \delta(z)| \leqslant (2^{m_{d+2}} - 1)\cdots(2^{m_k} - 1)\frac{(2^k - s(k,d))^{1/2}}{2},$$

где

$$s(k,d) = \binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \ldots + \binom{k}{d}.$$

Доказательство. Используя равенство $W_\varphi(\mathbf{a}) = 0$, справедливое для всех векторов $\mathbf{a} \in P^k$ веса $1 \leqslant \|\mathbf{a}\| \leqslant d$ [7, теорема 7.10], получим

$$|M(\varphi)| \leqslant 2^k - \binom{k}{1} - \binom{k}{2} - \ldots - \binom{k}{d}.$$

Если функция φ не является сбалансированной, то $W_\varphi(\mathbf{0}) \neq 0$ и $\mathbf{0} \in M(\varphi)$. Если функция φ является сбалансированной, то $W_\varphi(\mathbf{0}) = 0$ и $\mathbf{0} \notin M(\varphi)$. Таким образом,

$$|M(\varphi)\setminus\{\mathbf{0}\}| \leqslant 2^k - \binom{k}{0} - \binom{k}{1} - \binom{k}{2} - \ldots - \binom{k}{d} = 2^k - s(k,d),$$

и остаётся воспользоваться оценкой из теоремы 6. ■

Оценки из теоремы 6, следствий 1 и 2 обращаются в равенства для каждой из $(k-1)$-устойчивых функций $\varphi(x_1,\ldots,x_k) = x_1 \oplus \cdots \oplus x_k$ и $\varphi(x_1,\ldots,x_k) = x_1 \oplus \cdots \oplus x_k \oplus 1$ (см. утверждение 5).

6. Автокорреляционная функция и расстояние между отрезками выходных последовательностей

Рассмотрим случай, когда $F_1(x), \ldots, F_k(x)$ — примитивные многочлены над полем $P = \mathrm{GF}(2)$ попарно взаимно простых степеней $m_1, \ldots, m_k$ соответственно, φ — булева функция, существенно зависящая от всех своих переменных, а начальное состояние

$$\alpha_0 = (u_1(0), u_1(1), \ldots, u_1(m_1 - 1), \ldots, u_k(0), u_k(1), \ldots, u_k(m_k - 1))$$

комбинирующего генератора выбирается из множества $(P^{m_1}\backslash\{\mathbf{0}\})\times\ldots\times(P^{m_k}\backslash\{\mathbf{0}\})$, т. е. все ЛРП $u_1, \ldots, u_k$ являются ненулевыми. Пусть $T = (2^{m_1} - 1)\cdots(2^{m_k} - 1)$. Согласно теореме 2, каждая выходная последовательность v комбинирующего генератора, построенная по правилу (1), имеет период $T(v) = T$. Как показано в утверждении 2, состояния

$$\alpha_i = (u_1(i), u_1(i + 1), \ldots, u_1(i + m_1 - 1), \ldots, u_k(i), u_k(i + 1), \ldots, u_k(i + m_k - 1))$$

комбинирующего генератора в моменты времени $i = 0, 1, \ldots, T - 1$ пробегают все множество $(P^{m_1}\backslash\{\mathbf{0}\}) \times \ldots \times (P^{m_k}\backslash\{\mathbf{0}\})$ и лежат на одном цикле.

Для каждого $r \in \mathbb{N}_0$ обозначим через $x^r v$ сдвиг последовательности v на r шагов, т. е. последовательность вида $x^r v = (v(r), v(r + 1), \ldots)$. Заметим, что множество всех последовательностей над полем P образует модуль над кольцом многочленов $P[x]$ [4, с. 297], и введённое обозначение согласуется с внешней операцией умножения последовательности на многочлен. Последовательность $x^t v$, $t = 0, 1, \ldots, T - 1$, вырабатывается на начальном состоянии α_t, и в рассматриваемом случае все выходные последовательности генератора являются сдвигами друг друга. В силу равенства $T(v) = T$ последовательности $v, xv, \ldots, x^{T-1}v$ попарно различны.

Нас интересует вопрос о расстоянии Хэмминга $\rho(v, x^t v)$, $t = 0, 1, \ldots, T - 1$, между векторами $(v(0), v(1), \ldots, v(T-1))$ и $(v(t), v(t+1), \ldots, v(t+T-1))$, т. е. между циклами последовательностей v и $x^t v$.

Рассмотрим автокорреляционную функцию последовательности v [5; 9, с. 123], определённую равенством

$$C_v(t) = \sum_{i=0}^{T-1} (-1)^{v(i)\oplus v(i+t)}, \quad i = 0, 1, \ldots, T - 1. \tag{5}$$

Из равенства $C_v(t) = T - 2\rho(v, v_t)$ получим

$$\rho(v, x^t v) = (T - C_v(t))/2. \tag{6}$$

Всюду в дальнейшем изучается ситуация, когда для всех $j = 1, 2, \ldots, k$ выполнено

$$(u_j(0), u_j(1), \ldots, u_j(m_j - 1)) \neq (u_j(t), u_j(t + 1), \ldots, u_j(t + m_j - 1)), \tag{7}$$

т. е. при выработке v и $x^t v$ все соответствующие начальные заполнения регистров сдвига различны.

Лемма 1. Условие (7) равносильно тому, что t не кратно каждому из чисел $2^{m_1} - 1, \ldots, 2^{m_k} - 1$.

Доказательство. При каждом $j = 1, 2, \ldots, k$ соотношение

$$(u_j(0), u_j(1), \ldots, u_j(m_j - 1)) = (u_j(t), u_j(t + 1), \ldots, u_j(t + m_j - 1))$$

означает, что $u_j = x^t u_j$, т. е. $(x^t - 1)u_j = (0)$. Это равносильно тому, что $T(u_j) = 2^{m_j} - 1$ делит t. ■

Теорема 7. Пусть $P = \mathrm{GF}(2)$, $F_1(x), \ldots, F_k(x)$ — примитивные многочлены над полем P попарно взаимно простых степеней $m_1, \ldots, m_k$ соответственно, $u_1, \ldots, u_k$ — ненулевые ЛРП, $T = (2^{m_1} - 1) \cdots (2^{m_k} - 1)$, функция φ существенно зависит от всех своих переменных. Тогда для всех t, не кратных каждому из чисел $2^{m_1} - 1$, …, $2^{m_k} - 1$,

$$C_v(t) = T\left(1 - \frac{\|\varphi\|}{2^{k-1}}\right)^2 + \frac{T}{2^{k-1}}\left(1 - \frac{\|\varphi\|}{2^{k-1}}\right) \sum_{\mathbf{a} \in P^k \setminus \{\mathbf{0}\}} \frac{(-1)^{\|\mathbf{a}\|} W_\varphi(\mathbf{a})}{(2^{m_1} - 1)^{a_1} \ldots (2^{m_k} - 1)^{a_k}} + \\ + \frac{T}{2^k} \sum_{\substack{\mathbf{a} = (a_1, \ldots, a_k), \\ \mathbf{b} = (b_1, \ldots, b_k) \in P^k \setminus \{\mathbf{0}\}}} \frac{(-1)^{\|(a_1 \vee b_1, \ldots, a_k \vee b_k)\|} W_\varphi(\mathbf{a}) W_\varphi(\mathbf{b})}{(2^{m_1} - 1)^{a_1 \vee b_1} \ldots (2^{m_k} - 1)^{a_k \vee b_k}}.$$

Доказательство. Из равенств (2) и (5) имеем

$$C_v(t) = \sum_{i=0}^{T-1} (-1)^{v(i)} (-1)^{v(i+t)} = \frac{1}{2^{2k}} \sum_{\mathbf{a}, \mathbf{b} \in P^k} W_\varphi(\mathbf{a}) W_\varphi(\mathbf{b}) \sum_{i=0}^{T-1} (-1)^{\omega_1(i) \oplus \cdots \oplus \omega_k(i)},$$

где для каждого $j = 1, 2, \ldots, k$ последовательность ω_j определена равенством $\omega_j = (b_j x^t + a_j) u_j$. Последовательность ω_j является ЛРП с характеристическим многочленом $F_j(x)$, причём она нулевая тогда и только тогда, когда $F_j(x)$ делит $b_j x^t + a_j$. По выбору числа t это выполнено только при условии $a_j = b_j = 0$. Отсюда с использованием утверждения 4 получаем следующее равенство:

$$\sum_{i=0}^{T-1} (-1)^{\omega_1(i) \oplus \cdots \oplus \omega_k(i)} = \frac{(-1)^{\|(a_1 \vee b_1, \ldots, a_k \vee b_k)\|} T}{(2^{m_1} - 1)^{a_1 \vee b_1} \ldots (2^{m_k} - 1)^{a_k \vee b_k}}.$$

Значит,

$$C_v(t) = \frac{T}{2^{2k}} \sum_{\mathbf{a}, \mathbf{b} \in P^k} W_\varphi(\mathbf{a}) W_\varphi(\mathbf{b}) \frac{(-1)^{\|(a_1 \vee b_1, \ldots, a_k \vee b_k)\|} T}{(2^{m_1} - 1)^{a_1 \vee b_1} \ldots (2^{m_k} - 1)^{a_k \vee b_k}}.$$

Выделяя отдельно случаи $\mathbf{a} = \mathbf{b} = \mathbf{0}$; $\mathbf{a} = \mathbf{0}$, $\mathbf{b} \in P^k \setminus \{\mathbf{0}\}$; $\mathbf{b} = \mathbf{0}$, $\mathbf{a} \in P^k \setminus \{\mathbf{0}\}$ и используя равенство $W_\varphi(\mathbf{0}) = 2^k - 2\|\varphi\|$, получим нужную формулу. ■

Теорема 7 и равенство (6) позволяют найти точные значения для расстояний Хэмминга $\rho(v, x^t v)$. Например, пусть, в условиях теоремы 7, $\varphi(x_1, \ldots, x_k) = x_1 \oplus \cdots \oplus x_k \oplus \varepsilon$, где $\varepsilon \in \{0, 1\}$. Тогда (см. утверждение 5)

$$C_v(t) = \frac{T(-1)^k W_\varphi(1, \ldots, 1)^2}{2^{2k}(2^{m_1} - 1) \cdots (2^{m_k} - 1)} = (-1)^k, \quad \rho(v, x^t v) = \frac{T + (-1)^{k-1}}{2}.$$

В этом случае рассматриваемые векторы отличаются примерно в половине координат.

Рассмотрим ещё один пример. Пусть, в условиях теоремы 7, $\varphi(x_1, \ldots, x_k) = x_1 \oplus \oplus \cdots \oplus x_{k-2} \oplus x_{k-1} x_k$. Тогда (см. утверждение 8)

$$C_v(t) = \frac{T}{2^{2k}} \sum_{\mathbf{a}, \mathbf{b} \in \{(1\ldots100), (1\ldots101), (1\ldots110), (1\ldots1)\}} \frac{(-1)^{(-1)^{\|(a_1 \vee b_1, \ldots, a_k \vee b_k)\|}} W_\varphi(\mathbf{a}) W_\varphi(\mathbf{b})}{(2^{m_1} - 1)^{a_1 \vee b_1} \ldots (2^{m_k} - 1)^{a_k \vee b_k}}.$$

Отсюда нетрудно получить равенства

$$C_v(t) = (-1)^k (2^{m_{k-1} + m_k - 2} - 2^{m_{k-1}} - 2^{m_k} + 1),$$
$$\rho(v, x^t v) = (T + (-1)^{k-1} (2^{m_{k-1} + m_k - 2} - 2^{m_{k-1}} - 2^{m_k} + 1))/2.$$

Установим оценку сверху величины $C_v(t)$ для корреляционно-иммунных функций усложнения.

Следствие 3. Пусть, в условиях теоремы 7, $m_1 < m_2 < \ldots < m_k$ и φ является корреляционно-иммунной порядка d функцией. Тогда

$$\left|C_v(t) - T\left(1 - \frac{\|\varphi\|}{2^{k-1}}\right)\right| \leqslant (2^{m_{d+2}}-1)\cdots(2^{m_k}-1)|M(\varphi)\backslash\{\mathbf{0}\}|^{1/2}\left(2 - \frac{\|\varphi\|}{2^{k-2}} + |M(\varphi)\backslash\{\mathbf{0}\}|^{1/2}\right).$$

Доказательство. Из теоремы 7 получим

$$\left|C_v(t) - T\left(1 - \frac{\|\varphi\|}{2^{k-1}}\right)^2\right| \leqslant \frac{T}{2^{k-1}}\left(1 - \frac{\|\varphi\|}{2^{k-1}}\right)\sum_{\mathbf{a}\in P^k\backslash\{\mathbf{0}\}}\frac{|W_\varphi(\mathbf{a})|}{(2^{m_1}-1)^{a_1}\ldots(2^{m_k}-1)^{a_k}} + \\ + \frac{T}{2^{2k}}\sum_{\substack{\mathbf{a}=(a_1,\ldots,a_k),\\ \mathbf{b}=(b_1,\ldots,b_k)\in P^k\backslash\{\mathbf{0}\}}}\frac{|W_\varphi(\mathbf{a})||W_\varphi(\mathbf{b})|}{(2^{m_1}-1)^{a_1\vee b_1}\ldots(2^{m_k}-1)^{a_k\vee b_k}}.$$

Так как $W_\varphi(\mathbf{a}) = 0$ для всех векторов $\mathbf{a} \in P^k$ веса $1 \leqslant \|\mathbf{a}\| \leqslant d$ [7, теорема 7.10], то

$$\left|C_v(t) - T\left(1 - \frac{\|\varphi\|}{2^{k-1}}\right)^2\right| \leqslant \frac{(2^{m_{d+2}}-1)\cdots(2^{m_k}-1)(2^k - 2\|\varphi\|)}{2^{2k-1}}\sum_{\mathbf{a}\in P^k\backslash\{\mathbf{0}\}}|W_\varphi(\mathbf{a})| + \\ + \frac{(2^{m_{d+2}}-1)\cdots(2^{m_k}-1)}{2^{2k}}\left(\sum_{\mathbf{a}\in P^k\backslash\{\mathbf{0}\}}|W_\varphi(\mathbf{a})|\right)^2.$$

Для завершения доказательства остаётся воспользоваться неравенством

$$\sum_{\mathbf{a}\in P^k\backslash\mathbf{0}}|W_\varphi(\mathbf{a})| \leqslant |M(\varphi)\backslash\{\mathbf{0}\}|^{1/2}2^k,$$

полученным при доказательстве теоремы 6. ■

Следствие 4. Пусть, в условиях теоремы 7, $m_1 < m_2 < \ldots < m_k$ и φ является d-устойчивой булевой функцией. Тогда

$$|C_v(t)| \leqslant (2^{m_{d+2}}-1)\cdots(2^{m_k}-1)|M(\varphi)\backslash\{\mathbf{0}\}| \leqslant (2^{m_{d+2}}-1)\cdots(2^{m_k}-1)(2^k - s(k,d)),$$
$$\left|\rho(v, x^t v) - \frac{T}{2}\right| \leqslant (2^{m_{d+2}}-1)\cdots(2^{m_k}-1)\frac{|M(\varphi)\backslash\{\mathbf{0}\}|}{2} \leqslant (2^{m_{d+2}}-1)\cdots(2^{m_k}-1)\frac{2^k - s(k,d)}{2}.$$

Доказательство. Достаточно воспользоваться оценкой $|M(\varphi)\backslash\{\mathbf{0}\}| \leqslant 2^k - s(k,d)$, полученной при доказательстве следствия 2, и равенством (6). ■

Оценки из следствий 3 и 4 достижимы для булевой функции $\varphi(x_1,\ldots,x_k) = x_1 \oplus x_2 \oplus \cdots \oplus x_k \oplus \varepsilon$, где $\varepsilon \in \{0,1\}$.

ЛИТЕРАТУРА

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001. 480 с.
2. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
3. *Rueppel R. A.* Analysis and Design of Stream Ciphers. Springer Verlag, 1986. 244 p.
4. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Т. 2. М.: Гелиос АРВ, 2003. 416 с.
5. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988. Т. 1, 2. 822 с.

6. *Фомичев В. М.* О периодах усложненных последовательностей // Математические вопросы кибернетики. Вып. 13. М.: Физматлит, 2004. С. 37–40.
7. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012. 584 с.
8. *Niederreiter H.* Weights of cyclic codes // Information and Control. 1977. V. 34. P. 130–140.
9. *Golomb S. W. and Gong G.* Signal Design for Good Correlation. Cambridge, 2005. 438 p.

REFERENCES

1. *Alferov A. P., Zubov A. Yu., Kuz'min A. S., Cheremushkin A. V.* Osnovy kriptografii [Basics of Cryptography]. Moscow, Gelios ARV Publ., 2001. 480 p. (in Russian)
2. *Fomichev V. M.* Metody diskretnoy matematiki v kriptologii. Moscow, Dialog-MIFI Publ., 2010. 424 p. (in Russian)
3. *Rueppel R. A.* Analysis and Design of Stream Ciphers. Springer Verlag, 1986. 244 p.
4. *Glukhov M. M., Elizarov V. P., Nechaev A. A.* Algebra. V. 2. Moscow, Gelios ARV Publ., 2003. 416 p. (in Russian)
5. *Lidl R., Niderrayter G.* Konechnye polya [Finite Fields]. Moscow, Mir Publ., 1988, vol. 1, 2. 822 p. (in Russian)
6. *Fomichev V. M.* O periodakh uslozhnennykh posledovatel'nostey [On periods of complicated sequences]. Matematicheskie Voprosy Kibernetiki, iss. 13. Moscow, Fizmatlit Publ., 2004, pp. 37–40. (in Russian)
7. *Logachev O. A., Sal'nikov A. A., Smyshlyaev S. V., Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2012. 584 p. (in Russian)
8. *Niederreiter H.* Weights of cyclic codes. Information and Control, 1977, vol. 34, pp. 130–140.
9. *Golomb S. W. and Gong G.* Signal Design for Good Correlation. Cambridge, 2005. 438 p.