Math-Net.Ru

Общероссийский математический портал

О. В. Камловский, В. В. Мизеров, Свойства последовательностей, вырабатываемых комбинирующими генераторами над конечными полями, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 4, 23–47

DOI: <https://doi.org/10.4213/mvk338>

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: 54.162.85.209

26 апреля 2023 г., 17:05:47

**Свойства последовательностей, вырабатываемых
комбинирующими генераторами
над конечными полями**

О. В. Камловский, В. В. Мизеров

ООО «Центр сертификационных исследований», Москва

Получено 15.V.2020

Аннотация. Изучаются частотные характеристики и периодические свойства выходных последовательностей комбинирующих генераторов над произвольными конечными полями. Указывается строение графа автоматной модели комбинирующего генератора.

Ключевые слова: конечные поля, линейные рекуррентные последовательности, линейные регистры сдвига, комбинирующие генераторы

Properties of the output sequences of a combination generators over finite fields

O. V. Kamlovskii, V. V. Mizerov

LLC «Sertification Research Center», Moscow

Abstract. We investigate frequency characteristics and periodic properties of the output sequences of a combination generators over finite fields. Some new properties of the state graph of combination generators are described.

Keywords: finite fields, linear recurrent sequences, linear feedback shift registers, combination generators

Введение

Пусть $P = GF(q)$ — конечное поле из q элементов, $F_1(x), \dots, F_k(x)$ — многочлены над полем P , имеющие степени $m_1, \dots, m_k$ соответственно. Всюду в дальнейшем будем считать, что $F_1(x), \dots, F_k(x)$ — реверсивные многочлены (см. [1]), т. е. $F_1(0) \neq 0, \dots, F_k(0) \neq 0$. Для каждого отображения $\varphi : P^k \rightarrow P$ рассмотрим выходную последовательность v комбинирующего генератора (см. [2–4]), элементы которой имеют вид

$$v(i) = \varphi(u_1(i), u_2(i), \dots, u_k(i)), \quad i \geq 0, \quad (1)$$

где u_j — ненулевая линейная рекуррентная последовательность (ЛРП) над полем P с характеристическим многочленом $F_j(x)$ для всех $j \in \{1, 2, \dots, k\}$. В силу реверсивности многочленов каждая из ЛРП $u_1, \dots, u_k$ будет чисто периодической последовательностью (см., например, [1, 5]). Отсюда следует, что v является чисто периодической последовательностью.

Комбинирующие генераторы, выходные последовательности которых являются усложнениями ЛРП с помощью нелинейных функций, применяются для получения последовательностей с требуемыми криптографическими свойствами. Примеры поточных шифрсистем, построенных с использованием комбинирующих генераторов, приведены в [4, 6, 7].

Достаточно хорошо изучены ранги (линейные сложности) выходных последовательностей v (см., например, [2, 4]). Нижние и верхние оценки периодов таких последовательностей получены в [3, 4, 8]. Обзор первых работ о периодических свойствах и рангах выходных последовательностей комбинирующих генераторов представлен в [4]. В [3] и [9] получены точные формулы для частот появлений элементов на циклах последовательностей v в случае поля $P = GF(2)$ и примитивных многочленов $F_1(x), \dots, F_k(x)$, имеющих попарно взаимно простые степени. Эти результаты обобщены в [10] на случай r -грамм. Оценки частот появлений элементов на цикле последовательности v над полем $P = GF(q)$ в случае, когда φ — линейная функция, получены в [11]. Некоторые свойства выходных последовательностей комбинирующих генераторов над произвольными конечными полями приводятся в [12]. Частотные характеристики последовательностей v в ситуации, когда $\varphi(x_1, \dots, x_k) = x_1 \oplus \dots \oplus x_k$, а начальные отрезки ЛРП $u_1, \dots, u_k$ выбираются случайно и равновероятно из множества всех двоичных векторов соответствующих длин, изучались в [13]. Случай, когда начальные отрезки ЛРП $u_1, \dots, u_k$ выбираются неравновероятно, изучался в [14].

Данная работа продолжает исследования свойств последовательностей, вырабатываемых комбинирующими генераторами над произвольными конечными полями. В разделе 1 изучаются свойства графа автоматной модели комбинирующего генератора. В разделе 2 приводятся нижние оценки количества различных векторов, поступающих на вход функции φ при заданном числе l тактов работы комбинирующего генератора. В разделе 3 получены нижние оценки числа l , при котором на входе функции φ появляются все возможные векторы. В разделе 4 доказываются нижние и верхние оценки числа появлений элементов поля на цикле последовательности v . Результаты раздела 1 используются в разделе 5 для вычисления точных значений частот появлений нулевого вектора на цикле последовательности векторов $(u_1(i), \dots, u_k(i))$, $i \geq 0$. В разделе 6 указываются значения периода последовательности v в случае, когда функция φ задается над полем P многочленом, свободным от квадратов. В разделе 7 приводятся оценки частот появлений элементов на отрезках последовательности v при условии, что функция φ биективна по каждой из своих переменных.

1. Свойства графа комбинирующего генератора

Для описания свойств графа комбинирующего генератора нам понадобится понятие мультипликатора многочлена и ЛРП [15, 16]. Пусть $F(x)$ — реверсивный многочлен над полем $P = GF(q)$ степени $\deg F(x) = m$, $P^* = P \setminus \{0\}$. Существуют такие элемент $a \in P^*$ и натуральное число k (см. [1, 5]), что

$$F(x) \mid x^k - a. \quad (2)$$

Наименьшее число $k \in \mathbb{N}$, при котором существует элемент $a \in P^*$, удовлетворяющий соотношению (2), назовем редуцированным периодом многочлена $F(x)$ и обозначим $T_{red}(F)$. Элемент $a \in P^*$, для которого найдется такое число $k \in \mathbb{N}$, что выполнено соотношение (2), назовем мультипликатором многочлена $F(x)$. Множество всех мультипликаторов многочлена $F(x)$ обозначим через $\text{Mult}(F)$.

Укажем свойства множества $\text{Mult}(F)$, которые можно найти в [15–18].

Теорема 1. Пусть $F(x)$ — реверсивный многочлен степени m над полем $P = GF(q)$ и выполнено соотношение

$$F(x) \mid x^{T_{red}(F)} - b.$$

Тогда:

- 1) если выполнено соотношение (2), то $T_{red}(F) \mid k$ и $a \in \langle b \rangle$, где $\langle b \rangle$ — циклическая группа, порожденная элементом b ,
- 2) $Mult(F) = \langle b \rangle$,
- 3) $T_{red}(F) \cdot |Mult(F)| = T(F)$, где $T(F)$ — период многочлена $F(x)$,
- 4) если $F(x)$ — неприводимый многочлен над полем P , то

$$T_{red}(F) = \frac{T(F)}{(T(F), q-1)}, \quad |Mult(F)| = (T(F), q-1),$$

- 5) если $F(x)$ — примитивный многочлен над полем P , то

$$T_{red}(F) = \frac{q^m - 1}{q - 1}, \quad Mult(F) = P^*, \quad b = F(0).$$

Пусть u — ЛРП над полем P с минимальным многочленом $M_u(x) = F(x)$. Существуют такие натуральное число k и элемент $a \in P^*$, что

$$u(i+k) = au(i), \quad i \geq 0. \quad (3)$$

Наименьшее такое число $k \in \mathbb{N}$, что равенство (3) выполнено для некоторого $a \in P$, назовем редуцированным периодом ЛРП u и обозначим $T_{red}(u)$ (см. [15]). Каждый элемент $a \in P^*$, удовлетворяющий соотношению (3) при некотором $k \in \mathbb{N}$, назовем мультипликатором ЛРП u . Множество всех мультипликаторов ЛРП u обозначим через $Mult(u)$.

Заметим, что для элементов $k \in \mathbb{N}$ и $a \in P^*$ соотношение $u(i+k) = au(i)$, $i \geq 0$, равносильно тому, что $F(x) \mid x^k - a$. Таким образом,

$$T_{red}(u) = T_{red}(F), \quad Mult(u) = Mult(F) = \langle b \rangle. \quad (4)$$

Отрезок $(u(0), u(1), \dots, u(T(F) - 1))$ ЛРП u записывается следующим образом:

$$(u(0), u(1), \dots, u(t-1), bu(0), bu(1), \dots, bu(t-1), b^2u(0), b^2u(1), \dots, \\ b^2u(t-1), \dots, b^{d-1}u(0), b^{d-1}u(1), \dots, b^{d-1}u(t-1)),$$

где $t = T_{red}(F)$, $d = |Mult(F)|$.

Пусть $P = GF(q)$, $F_1(x), \dots, F_k(x)$ — примитивные многочлены над полем P степеней $m_1, \dots, m_k$. Будем считать, что числа $m_1, \dots, m_k$ попарно взаимно просты. Пусть v — последовательность, построенная по правилу (1). В рассматриваемом случае последовательности $u_1, \dots, u_k$ являются ЛРП максимальных периодов $q^{m_1} - 1, \dots, q^{m_k} - 1$ соответственно.

Рассмотрим автоматную модель комбинирующего генератора. Будем изучать автономный автомат $A = (S, P, h, f)$ с алфавитом состояний

$$S = (P^{m_1} \setminus \{\vec{0}\}) \times (P^{m_2} \setminus \{\vec{0}\}) \times \dots \times (P^{m_k} \setminus \{\vec{0}\}),$$

выходным алфавитом P , функцией переходов $h : S \rightarrow S$ и функцией выходов $f : S \rightarrow P$, определенных равенствами

$$\begin{aligned} & h(s_{11}, s_{12}, \dots, s_{1m_1}, \dots, s_{k1}, s_{k2}, \dots, s_{km_k}) \\ &= (s_{12}, \dots, s_{1m_1}, \sum_{i=1}^{m_1} a_{1i} s_{1i}, \dots, s_{k2}, \dots, s_{km_k}, \sum_{i=1}^{m_k} a_{ki} s_{ki}), \\ & f(s_{11}, \dots, s_{1m_1}, \dots, s_{k1}, \dots, s_{km_k}) = \varphi(s_{11}, \dots, s_{k1}), \end{aligned}$$

где $s_{ij} \in P, i = 1, \dots, k, j = 1, \dots, m_i, F_1(x) = x^{m_1} - a_{1m_1}x^{m_1-1} - \dots - a_{11}, \dots, F_k(x) = x^{m_k} - a_{km_k}x^{m_k-1} - \dots - a_{k1}$.

Начальное состояние

$$\vec{\alpha}_0 = (u_1(0), \dots, u_1(m_1 - 1), \dots, u_k(0), \dots, u_k(m_k - 1))$$

автомата A выбирается из множества S . Тогда в i -й такт, где $i \geq 0$, получим состояние

$$\vec{\alpha}_i = (u_1(i), \dots, u_1(i + m_1 - 1), \dots, u_k(i), \dots, u_k(i + m_k - 1)) \in S.$$

Последовательность $(\vec{\alpha}_i)_{i=0}^\infty$ является чисто периодической последовательностью периода T , который ввиду того, что $(q^{m_i} - 1, q^{m_j} - 1) = q - 1$ для всех $i \neq j$, равен

$$T = [T(u_1), \dots, T(u_k)] = \frac{(q^{m_1} - 1) \dots (q^{m_k} - 1)}{(q - 1)^{k-1}}.$$

Таким образом, каждое состояние $\vec{\alpha}_i \in S$ лежит на цикле длины T в графе автомата A и все состояния расположены на $(q - 1)^{k-1}$ различных циклах длины T .

Получим достаточное условие принадлежности векторов из S различным циклам. Каждый вектор $\vec{\alpha} \in S$ запишем в виде $\vec{\alpha} = (\vec{\alpha}(1), \vec{\alpha}(2), \dots, \vec{\alpha}(k))$, где $\vec{\alpha}(j) \in P^{m_j} \setminus \{\vec{0}\}$, для всех $j = 1, 2, \dots, k$. Зададим на множестве S бинарное отношение $\sim$: если $\vec{\alpha}, \vec{\beta} \in S$, то $\vec{\alpha} \sim \vec{\beta}$ тогда и только тогда, когда существуют такие элементы $c_1, c_2, \dots, c_k \in P^*$, что $\vec{\alpha}(j) = c_j \vec{\beta}(j)$ для всех $j = 1, 2, \dots, k$. Это отношение является отношением эквивалентности на множестве S .

Пусть θ_j — корень многочлена $F_j(x)$ в расширении $GF(q^{m_j})$ поля P , где $j = 1, 2, \dots, k$. Тогда из п. 5 теоремы 1 следует, что элемент

$$b_j = \theta_j^{\frac{q^{m_j}-1}{q-1}} = \theta_j^{T_{red}(F_j)}, \quad j = 1, 2, \dots, k,$$

является мультипликатором многочлена $F_j(x)$. Пусть $m = m_1 m_2 \cdots m_k$. Зададим на множестве S еще одно бинарное отношение $\overset{\text{red}}{\sim}$: если $\vec{\alpha}, \vec{\beta} \in S$, то $\vec{\alpha} \overset{\text{red}}{\sim} \vec{\beta}$ тогда и только тогда, когда существует такое $s \in \{0, 1, \dots, q-2\}$, что $\vec{\alpha}(j) = b_j^{\frac{m_j}{m}s} \vec{\beta}(j)$ для всех $j = 1, 2, \dots, k$. Данное отношение является отношением эквивалентности на множестве S . Так как числа $m/m_1, m/m_2, \dots, m/m_k$ взаимно просты в совокупности, то для каждого вектора из S существует ровно $q-1$ векторов из S , находящихся с ним в отношении $\overset{\text{red}}{\sim}$.

Теорема 2. Пусть векторы $\vec{\alpha}$ и $\vec{\beta} \in S$ находятся в отношении $\sim$ и не находятся в отношении $\overset{\text{red}}{\sim}$. Тогда $\vec{\alpha}$ и $\vec{\beta}$ принадлежат различным циклам в графе автомата A .

Доказательство. Допустим противное: векторы $\vec{\alpha}$ и $\vec{\beta}$ принадлежат одному циклу. По условию существуют такие элементы $c_1, c_2, \dots, c_k \in P^*$, что $\vec{\alpha}(j) = c_j \vec{\beta}(j)$ для всех $j = 1, 2, \dots, k$. Пусть $u_j, j = 1, 2, \dots, k$, — ЛРП над полем P с характеристическим многочленом $F_j(x)$ и начальным вектором $\vec{\beta}(j)$. Так как векторы $\vec{\alpha}$ и $\vec{\beta}$ принадлежат одному циклу в графе переходов автомата A , то

$$\vec{\alpha} = (u_1(t), \dots, u_1(t + m_1 - 1), \dots, u_k(t), \dots, u_k(t + m_k - 1))$$

для некоторого $t \in \mathbb{N}$. Так как последовательность $c_j u_j$ и последовательность $x^t u_j$, полученная из u_j сдвигом на t шагов, являются ЛРП с характеристическим многочленом $F_j(x)$ и имеют равные начальные векторы, то $c_j u_j = x^t u_j$ для всех $j = 1, 2, \dots, k$. Следовательно,

$$c_1 u_1(i) = u_1(i + t), c_2 u_2(i) = u_2(i + t), \dots, c_k u_k(i) = u_k(i + t), \quad i \geq 0.$$

Из равенств (4) и теоремы 1 имеем $T_{red}(F_j) \mid t$ для всех $j = 1, 2, \dots, k$. Отсюда ввиду попарной взаимной простоты чисел $m_1, \dots, m_k$ получаем

$$t = \frac{(q^{m_1} - 1) \cdots (q^{m_k} - 1)d}{(q - 1)^k}, \quad (5)$$

где $d \in \mathbb{N}$. По выбору элементов $b_1, \dots, b_k$ справедливы равенства

$$u_1(i + t) = b_1^{\frac{t}{T_{red}(F_1)}} u_1(i), \dots, u_k(i + t) = b_k^{\frac{t}{T_{red}(F_k)}} u_k(i), \quad i \geq 0.$$

Заметим, что $q \equiv 1 \pmod{q-1}$, а значит,

$$\frac{q^{m_j} - 1}{q - 1} = 1 + q + \dots + q^{m_j-1} \equiv m_j \pmod{q-1}, \quad j = 1, 2, \dots, k.$$

Отсюда, из равенств для мультипликативных порядков $\text{ord } b_1 = \dots = \text{ord } b_k = q - 1$ элементов $b_1, \dots, b_k$ поля P и соотношения (5) следует, что

$$u_1(i+t) = b_1^{\frac{m}{m_1}d} u_1(i), \dots, u_k(i+t) = b_k^{\frac{m}{m_k}d} u_k(i), \quad i \geq 0, \quad (6)$$

а значит,

$$\vec{\alpha} = (b_1^{\frac{m}{m_1}d} \vec{\beta}(1), \dots, b_k^{\frac{m}{m_k}d} \vec{\beta}(k))$$

и $\vec{\alpha} \stackrel{\text{red}}{\sim} \vec{\beta}$, что противоречит условию. $\square$

Предложим способ построения $(q-1)^{k-1}$ векторов, принадлежащих всем различным циклам графа автомата A . Рассмотрим внешнюю прямую сумму

$$G = \underbrace{\mathbb{Z}_{q-1} \oplus \dots \oplus \mathbb{Z}_{q-1}}_k,$$

k экземпляров аддитивной группы $\mathbb{Z}_{q-1} = \{0, 1, \dots, q-2\}$ кольца вычетов по модулю $q-1$. Пусть $H = \langle (\frac{m}{m_1}, \dots, \frac{m}{m_k}) \rangle$ — подгруппа группы G , порожденная элементом $(\frac{m}{m_1}, \dots, \frac{m}{m_k})$. Так как числа $m/m_1, \dots, m/m_k$ взаимно просты в совокупности, то $|H| = q-1$ и разложение группы G в смежные классы по подгруппе H имеет вид

$$G = \bigcup_{(i_1, \dots, i_k) \in I} (H + (i_1, \dots, i_k)), \quad (7)$$

где $I \subset G$ и $|I| = (q-1)^{k-1}$.

Следствие 1. Пусть $\vec{\alpha} = (\vec{\alpha}(1), \dots, \vec{\alpha}(k))$ — произвольный вектор из множества S и выполнено равенство (7). Тогда векторы

$$(b_1^{i_1} \vec{\alpha}(1), \dots, b_k^{i_k} \vec{\alpha}(k)), \quad (i_1, \dots, i_k) \in I$$

принадлежат различным циклам в графе автомата A .

Доказательство. Согласно теореме 2 достаточно доказать, что любые два из рассматриваемых векторов не находятся в отношении $\stackrel{\text{red}}{\sim}$. Допустим противное: существуют различные элементы $(i_1, \dots, i_k), (j_1, \dots, j_k) \in I$, для которых

$$(b_1^{i_1} \vec{\alpha}(1), \dots, b_k^{i_k} \vec{\alpha}(k)) \stackrel{\text{red}}{\sim} (b_1^{j_1} \vec{\alpha}(1), \dots, b_k^{j_k} \vec{\alpha}(k)).$$

Тогда существует такое $d \in \{0, 1, \dots, q-2\}$, что $b_1^{j_1} = b_1^{i_1 + \frac{m}{m_1}d}, \dots, b_k^{j_k} = b_k^{i_k + \frac{m}{m_k}d}$. Значит, $(j_1 - i_1, \dots, j_k - i_k) \in H$, что противоречит равенству (7). □

2. Число различных векторов, поступающих на вход функции усложнения

Определим множество

$$M(u_1, \dots, u_k) = \{(u_1(i), \dots, u_k(i)) : i \geq 0\}$$

всех различных векторов, поступающих на вход функции φ , и множество

$$M_l(u_1, \dots, u_k) = \{(u_1(i), \dots, u_k(i)) : i \in \overline{0, l-1}\}$$

всех различных векторов, поступающих на вход φ на первых l тактах работы комбинирующего генератора. Оценим снизу величины $|M(u_1, \dots, u_k)|$ и $|M_l(u_1, \dots, u_k)|$.

Теорема 3. Пусть $P = GF(q)$, $q = p^t$, где p — простое число, $t \in \mathbb{N}$, $F_1(x), \dots, F_k(x)$ — реверсивные многочлены над полем P , $F(x) = [F_1(x), \dots, F_k(x)]$ — наименьшее общее кратное многочленов $F_1(x), \dots, F_k(x)$, $\deg F(x) = m$, $u_1, \dots, u_k$ — ЛРП над полем P с минимальными многочленами $F_1(x), \dots, F_k(x)$ соответственно. Тогда:

1) при всех таких l , что $m \leq l \leq [T(F_1), \dots, T(F_k)]$, выполнено неравенство

$$|M_l(u_1, \dots, u_k)| \geq (l - m + 1)^{\frac{1}{m}},$$

2) $|M(u_1, \dots, u_k)| \geq ([T(F_1), \dots, T(F_k)] - m + 1)^{\frac{1}{m}}$,

3) если $F_1(x), \dots, F_k(x)$ — сепарабельные многочлены (не имеющие кратных корней в своих полях разложения), то

$$|M_l(u_1, \dots, u_k)| \geq \min \left\{ |M(u_1, \dots, u_k)|, \frac{l^{\frac{1}{1+p \log_p m}}}{p} \right\}.$$

Доказательство. Докажем неравенство, сформулированное в п. 1. Покажем, что $m \leq [T(F_1), \dots, T(F_k)]$, т. е. п. 1 является содержательным. По определению периода многочлена

$$F_s(x) \mid x^{T(F_s)} - e \mid x^{[T(F_1), \dots, T(F_k)]} - e$$

для всех $s = 1, \dots, k$. Значит, $F(x) \mid x^{[T(F_1), \dots, T(F_k)]} - e$ и $m \leq [T(F_1), \dots, T(F_k)]$. Рассмотрим расширение $Q = GF(q^k)$ поля P . Пусть $\alpha_1, \dots, \alpha_k$ — базис векторного пространства Q_P , ω — последовательность над полем Q с элементами

$$\omega(i) = \alpha_1 u_1(i) + \dots + \alpha_k u_k(i), \quad i \geq 0.$$

Многочлен $F(x)$ является характеристическим многочленом последовательности ω . Ее минимальный многочлен $M(x) \in Q[x]$ делит $F(x)$, а значит, $\deg M(x) = d \leq m$. Ясно, что ω — чисто периодическая последовательность периода $[T(u_1), \dots, T(u_k)]$, а так как $T(u_s) = T(F_s)$ для всех $s = 1, \dots, k$ (см., например, [1, 5]), то

$$T(\omega) = [T(F_1), \dots, T(F_k)].$$

Очевидно, что $|M_l(\omega)| = |M_l(u_1, \dots, u_k)|$. Согласно [19, теорема 3] при всех таких l , что $d \leq l \leq T(\omega) + d - 1$,

$$|M_l(\omega)| \geq (l - d + 1)^{\frac{1}{d}},$$

поэтому

$$|M_l(u_1, \dots, u_k)| = |M_l(\omega)| \geq (l - m + 1)^{\frac{1}{m}}.$$

Для доказательства неравенства из п. 2 достаточно подставить в полученное соотношение значение $l = [T(F_1), \dots, T(F_k)]$, которое совпадает с периодом последовательности векторов $(u_1(i), \dots, u_k(i))$, $i \geq 0$. Как показано в [19, теорема 2], для ЛРП ω с реверсивным сепарабельным характеристическим многочленом

$$|M_l(\omega)| \geq \min \left\{ |M(\omega)|, \frac{l^{\frac{1}{1+p \log_p d}}}{p} \right\}.$$

Отсюда и из равенства $|M(\omega)| = |M(u_1, \dots, u_k)|$ непосредственно следует утверждение п. 3. $\square$

3. Число тактов, при котором на вход функции усложнения поступают все возможные векторы

В данном разделе получены оценки длины l отрезка последовательности, для которого имеет место равенство $M_l(u_1, \dots, u_k) = M(u_1, \dots, u_k)$. В частности, для таких l выполнено соотношение $M_l(v) = M(v)$.

Нам понадобятся вспомогательные факты о рангах ЛРП. Пусть $P = GF(q)$, $k \geq 2$, $F_1(x), \dots, F_k(x) \in P[x]$ — сепарабельные многочлены. Пусть Q — поле разложения рассматриваемых многочленов и $F_i(x) = (x - \alpha_{i1}) \cdots (x - \alpha_{im_i})$, где $m_i = \deg F_i(x)$, $i = 1, 2, \dots, k$. Определим так называемый дизъюнктивный многочлен (см., например, [5]) по правилу

$$F_1(x) \vee \dots \vee F_k(x) = [\{(x - \alpha_{1j_1} \cdots \alpha_{kj_k}) : 1 \leq j_1 \leq m_1, \dots, 1 \leq j_k \leq m_k\}]. \quad (8)$$

Ясно, что $F_1(x) \vee \dots \vee F_k(x)$ является сепарабельным многочленом над полем Q . На самом деле это многочлен из $P[x]$. Имеет место следующее утверждение.

Лемма 1 ([5]). Пусть $P = GF(q)$, $k \geq 2$, $u_1, \dots, u_k$ — ЛРП над P с сепарабельными характеристическими многочленами $F_1(x), \dots, F_k(x) \in P[x]$ соответственно, $\omega = u_1 \cdots u_k$. Тогда ω — ЛРП с характеристическим многочленом $F_1(x) \vee \dots \vee F_k(x)$, и для ее ранга справедливо соотношение

$$\text{rank } \omega \leq \text{rank } u_1 \cdots \text{rank } u_k.$$

Лемма 2 ([20]). Пусть $P = GF(q)$, $q = p^t$, где p — простое число, $t \in \mathbb{N}$, $F(x) \in P[x]$ — сепарабельный многочлен, $\deg F(x) = m$, u — ЛРП над P с характеристическим многочленом $F(x)$. Тогда, если p -ичное разложение числа $s \in \{0, \dots, q-1\}$ имеет вид $s = \delta_0(s) + p\delta_1(s) + \dots + p^{t-1}\delta_{t-1}(s)$, где $\delta_0(s), \dots, \delta_{t-1}(s) \in \{0, \dots, p-1\}$, то для ранга последовательности $u^s = \underbrace{u \cdots u}_s$ справедливо соотношение

$$\text{rank } u^s \leq \prod_{r=0}^{t-1} \binom{m + \delta_r(s) - 1}{\delta_r(s)}.$$

Следующее утверждение уточняет результаты из [21, теорема 4].

Теорема 4. Пусть $P = GF(q)$, $q = p^t$, где p — простое число, $t \in \mathbb{N}$, $F_1(x), \dots, F_k(x) \in P[x]$ — реверсивные сепарабельные многочлены степеней $m_1, \dots, m_k$ соответственно, $u_1, \dots, u_k$ — ЛРП над полем P с характеристическими многочленами $F_1(x), \dots, F_k(x)$ соответственно. Тогда, если

$$l \geq \prod_{j=1}^k \binom{m_j + p - 1}{p - 1}^t, \quad (9)$$

то $M_l(u_1, \dots, u_k) = M(u_1, \dots, u_k)$.

Доказательство. Допустим противное: справедливо неравенство (9) и существует вектор $\vec{z} = (z_1, \dots, z_k)$, принадлежащий множеству $M(u_1, \dots, u_k) \setminus M_l(u_1, \dots, u_k)$. Рассмотрим многочлен $a(\vec{x}) \in P[\vec{x}]$, где $\vec{x} = (x_1, \dots, x_k)$, вида

$$a(\vec{x}) = (e - (x_1 - z_1)^{q-1}) \cdots (e - (x_k - z_k)^{q-1}).$$

Пусть ω — последовательность над полем P , элементы которой равны

$$\omega(i) = (e - (u_1(i) - z_1)^{q-1}) \cdots (e - (u_k(i) - z_k)^{q-1}), \quad i \geq 0.$$

Так как $\vec{z} \in M(u_1, \dots, u_k)$, то существует такое число $s \in \mathbb{N}_0$, что $u_1(s) = z_1, \dots, u_k(s) = z_k$. Тогда $\omega(s) = e$ и ω — ненулевая последовательность. В силу того что $\vec{z} \notin M_l(u_1, \dots, u_k)$, выполнены равенства $\omega(0) = 0, \dots, \omega(l-1) = 0$. Следовательно,

$$\text{rank } \omega \geq l + 1. \quad (10)$$

Пусть при всех $j = 1, \dots, k$

$$\omega_j(i) = (e - (u_j(i) - z_j)^{q-1}) = a_0^{(j)} + a_1^{(j)} u_j(i) + \dots + a_{q-1}^{(j)} u_j(i)^{q-1}, \quad i \geq 0,$$

для некоторых элементов $a_0^{(j)}, \dots, a_{q-1}^{(j)} \in P$. Тогда $\omega = \omega_1 \cdots \omega_k$. Согласно лемме 2

$$\text{rank } u_j^s \leq \prod_{r=0}^{t-1} \binom{m_j + \delta_r(s) - 1}{\delta_r(s)},$$

тогда

$$\begin{aligned} \text{rank } \omega_j &\leq \sum_{s=0}^{q-1} \prod_{r=0}^{t-1} \binom{m_j + \delta_r(s) - 1}{\delta_r(s)} \\ &= \left(\sum_{s_0=0}^{p-1} \binom{m_j + s_0 - 1}{s_0} \right) \cdots \left(\sum_{s_{t-1}=0}^{p-1} \binom{m_j + s_{t-1} - 1}{s_{t-1}} \right) = \binom{m_j + p - 1}{p - 1}^t. \end{aligned}$$

Последовательность ω_j является ЛРП с характеристическим многочленом

$$[x - e, F_j, F_j \vee F_j, \dots, \underbrace{F_j \vee \dots \vee F_j}_{q-1}],$$

который в силу сепарабельности многочлена $F_j(x)$ является сепарабельным, поэтому по лемме 1

$$\text{rank } \omega \leq \prod_{j=1}^k \text{rank } \omega_j \leq \prod_{j=1}^k \binom{m_j + p - 1}{p - 1}^t. \quad (11)$$

Соотношения (10) и (11) противоречат выбору l . □

Заметим, что при фиксированном p и $m_j \rightarrow \infty$

$$\binom{m_j + p - 1}{p - 1} \sim \frac{m_j^{p-1}}{(p-1)!}.$$

Таким образом, из теоремы 4 следует, что при фиксированных параметрах p, q, k соотношение $M_l(u_1, \dots, u_k) = M(u_1, \dots, u_k)$ имеет место при

$$l = O((m_1 \cdots m_k)^{(p-1)t}),$$

где $m_1 \rightarrow \infty, \dots, m_k \rightarrow \infty$.

Приведем более простую оценку.

Следствие 2. В условиях теоремы 4 при

$$l \geq (m_1 + 1)^{pt} \cdots (m_k + 1)^{pt}$$

имеет место равенство $M_l(u_1, \dots, u_k) = M(u_1, \dots, u_k)$.

Доказательство. Достаточно воспользоваться неравенством

$$\binom{m + p - 2}{p - 1} \leq m^p, \tag{12}$$

справедливым для любого натурального числа m и простого числа p . □

4. Оценки частот появлений векторов на входе функции усложнения

Пусть $P = GF(q)$, $u_1, \dots, u_k$ — ЛРП максимальных периодов $T(u_1) = q^{m_1} - 1, \dots, T(u_k) = q^{m_k} - 1$. Будем считать, что числа $m_1, \dots, m_k$ попарно взаимно просты. Пусть

$$T = [q^{m_1} - 1, \dots, q^{m_k} - 1] = \frac{(q^{m_1} - 1) \cdots (q^{m_k} - 1)}{(q - 1)^{k-1}}.$$

Изучим величину $N(\vec{z}, u_1, \dots, u_k)$, равную количеству появлений вектора $\vec{z} \in P^k$ среди векторов $(u_1(i), \dots, u_k(i))$, $i = 0, 1, \dots, T - 1$. В дальнейшем понадобятся следующие вспомогательные утверждения.

Лемма 3 ([5, следствие 8.83]). Пусть δ — ЛРП порядка m с характеристическим многочленом $G(x)$ степени m , тогда для числа $N(z, \delta)$ появлений элемента $z \in P$ среди элементов $\delta(0), \dots, \delta(T(\delta) - 1)$ справедливы оценки

$$\frac{T(\delta)}{q} - (q-1)q^{\frac{m}{2}-1} \leq N(z, \delta) \leq \frac{T(\delta)}{q} + (q-1)q^{\frac{m}{2}-1}.$$

Лемма 4. Пусть δ — ЛРП порядка m , $m \geq 3$, над полем $P = GF(q)$ с неприводимым минимальным многочленом периода $r = \frac{q^m-1}{q-1}$. Тогда в последовательности δ появляется каждый элемент поля P .

Доказательство. Согласно лемме 3

$$N(z, \delta) \geq \frac{r}{q} - (q-1)q^{\frac{m}{2}-1} = \frac{1}{(q-1)q} (q^m - 1 - (q-1)^2 q^{\frac{m}{2}}).$$

Заметим, что $(q-1)^2 q^{\frac{m}{2}} < q^{\frac{m}{2}+2} - 1$, поэтому при $m \geq 4$ имеем $q^m - 1 > (q-1)^2 q^{\frac{m}{2}}$, а значит, $N(z, \delta) > 0$. Остается рассмотреть случай $m = 3$. Из [5, теорема 8.84]

$$N(0, \delta) \geq \frac{(q^2-1)r}{q^3-1} - \frac{q-1}{q} \left(\frac{r}{h} - \frac{r}{q^3-1} \right) q^{\frac{3}{2}},$$

где $h = [r, q-1]$. Тогда

$$N(0, \delta) \geq q+1 - (q-1) \left(\frac{(q^3-1)}{(q-1)[(q^3-1)/(q-1), q-1]} - \frac{1}{q-1} \right) q^{\frac{1}{2}}.$$

Заметим, что

$$[(q^3-1)/(q-1), q-1] = \frac{(q^2+q+1)(q-1)}{(q^2+q+1, q-1)} = \frac{(q^2+q+1)(q-1)}{(3, q-1)}.$$

Если 3 не делит $q-1$, то $N(0, \delta) \geq q+1 > 0$. Если 3 делит $q-1$, то справедливы неравенства

$$N(0, \delta) \geq q+1 - 2q^{\frac{1}{2}} = (\sqrt{q}-1)^2 > 0.$$

Значит, $N(0, \delta) > 0$. Пусть теперь $z \in P \setminus \{0\}$, тогда согласно [5, теорема 8.84]

$$N(z, \delta) \geq \frac{q^2}{q-1} - \left(\frac{r}{h} - \frac{r}{q^3-1} + \frac{h-r}{h} \sqrt{q} \right) q^{\frac{1}{2}}.$$

Если 3 не делит $q - 1$, то

$$N(z, \delta) \geq \frac{q^2}{q-1} - \frac{(q-2)q}{q-1} = \frac{2q}{q-1} > 0.$$

Если 3 делит $q - 1$, то

$$N(z, \delta) \geq \frac{q^2}{q-1} - \left(\frac{2}{q-1} + \frac{(q-4)\sqrt{q}}{q-1} \right) \sqrt{q} = \frac{4q - 2\sqrt{q}}{q-1} > 0.$$

Таким образом, $N(z, \delta) > 0$ при всех $z \in P$. $\square$

Теорема 5. Пусть $P = GF(q)$, $u_1, \dots, u_k$ — ЛРП максимальных периодов $T(u_1) = q^{m_1} - 1, \dots, T(u_k) = q^{m_k} - 1$ над полем P , числа $m_1, \dots, m_k$ попарно взаимно просты и больше 1. Тогда:

- 1) $M(u_1, \dots, u_k) = P^k$,
- 2) для каждого $\vec{z} \in P^k$

$$\frac{q^{m_1-1} - 1}{q^{k-1}(q-1)^{k-1}} \prod_{i=2}^k (q^{m_i} - 1 - (q-1)^2 q^{\frac{m_i}{2}}) \leq N(\vec{z}, u_1, \dots, u_k),$$

$$N(\vec{z}, u_1, \dots, u_k) \leq \frac{q^{m_1-k}}{(q-1)^{k-1}} \prod_{i=2}^k (q^{m_i} - 1 + (q-1)^2 q^{\frac{m_i}{2}}).$$

Доказательство. Без ограничения общности будем считать, что $m_1 < \dots < m_k$. Докажем п. 1 теоремы методом математической индукции по параметру k . При $k = 1$ согласно [1, глава 25, теорема 30] и [18, теорема 8] имеем $N(z_1, u_1) = q^{m_1-1} - 1$, если $z_1 = 0$, и $N(z_1, u_1) = q^{m_1-1}$, если $z_1 \neq 0$. Таким образом, $N(z_1, u_1) > 0$ при любом $z_1 \in P$. Допустим, что $M(u_1, \dots, u_{k-1}) = P^{k-1}$, т. е. среди векторов

$$(u_1(i), \dots, u_{k-1}(i)), \quad i = 0, 1, \dots, \bar{r} - 1,$$

где $\bar{r} = (q^{m_1} - 1) \dots (q^{m_{k-1}} - 1) / (q - 1)^{k-2}$, появляются все векторы

$$(z_1, \dots, z_{k-1}) \in P^{k-1}.$$

Заметим, что $\bar{r}$ является периодом последовательности векторов $(u_1(i), \dots, u_{k-1}(i))$, $i \geq 0$. Возьмем любой вектор $(z_1, \dots, z_k) \in P^k$. По предположению индукции найдется такое число i_0 , $0 \leq i_0 < \bar{r}$, что

$$(u_1(i_0), \dots, u_{k-1}(i_0)) = (z_1, \dots, z_{k-1}).$$

Рассмотрим векторы

$$(u_1(i_0 + \bar{r}j), \dots, u_k(i_0 + \bar{r}j)), \quad j = 0, 1, \dots$$

Они имеют вид

$$(z_1, \dots, z_{k-1}, u_k(i_0 + \bar{r}j)).$$

Пусть δ — последовательность с элементами $\delta(j) = u_k(i_0 + \bar{r}j)$, $j \geq 0$. Представим ЛРП u_k с использованием функции «след» (см. [1, 5])

$$u_k(i) = \text{Tr}_P^Q(c\theta_k^i), \quad i \geq 0,$$

где c — ненулевой элемент поля $Q = GF(q^{m_k})$, θ_k — корень многочлена $F_k(x)$ в поле Q . Тогда

$$\delta(j) = \text{Tr}_P^Q(c\theta_k^{i_0 + \bar{r}j}) = \text{Tr}_P^Q(b\beta^j), \quad j \geq 0,$$

где $b = c\theta_k^{i_0}$, $\beta = \theta_k^{\bar{r}}$. Пусть $H(x)$ — минимальный многочлен элемента β над полем P . Тогда период $T(H)$ многочлена $H(x)$ и порядок $\text{ord } \beta$ элемента β в мультипликативной группе поля Q связаны соотношениями

$$\begin{aligned} T(H) = \text{ord } \beta &= \frac{\text{ord } \theta_k}{(\text{ord } \theta_k, \bar{r})} = \frac{q^{m_k} - 1}{(q^{m_k} - 1, (q^{m_1} - 1) \dots (q^{m_{k-1}} - 1)/(q - 1)^{k-2})} \\ &= \frac{q^{m_k} - 1}{(q - 1)((q^{m_k} - 1)/(q - 1), (q^{m_1} - 1) \dots (q^{m_{k-1}} - 1)/(q - 1)^{k-1})} \\ &= \frac{q^{m_k} - 1}{q - 1} > q^{m_k-1} - 1. \end{aligned}$$

Значит, δ ненулевая ЛРП порядка m_k с минимальным многочленом $H(x)$, $T(\delta) = T(H) = (q^{m_k} - 1)/(q - 1)$ и $m_k > m_1 \geq 2$. Остается заметить, что по лемме 4 существует такое $j_0 \in \mathbb{N}$, что $\delta(j_0) = u_k(i_0 + \bar{r}j_0) = z_k$.

Докажем п. 2. Согласно рассуждениям, проведенным при доказательстве п. 1, если $\vec{a} = (z_1, \dots, z_{k-1}) \in P^{k-1}$ и $i_0 \in \{0, 1, \dots, \bar{r} - 1\}$ таковы, что

$$(u_1(i_0), \dots, u_{k-1}(i_0)) = \vec{a},$$

то среди чисел $i_0 + \bar{r}j$, где $j = 0, 1, \dots, (q^{m_k} - 1)/(q - 1) - 1$, имеется $N(z_k, \delta)$ значений j , удовлетворяющих соотношению

$$(u_1(i_0 + \bar{r}j), \dots, u_{k-1}(i_0 + \bar{r}j)) = (z_1, \dots, z_{k-1}, z_k),$$

где $\delta = \delta(i_0, \bar{r})$ — ЛРП, зависящая от i_0 и $\bar{r}$. Значит,

$$N(\vec{z}, u_1, \dots, u_k) = \sum_{i_0 \in \{0, \dots, \bar{r}-1\}: (u_1(i_0), \dots, u_{k-1}(i_0)) = \vec{a}} N(z_k, \delta(i_0, \bar{r})).$$

Используя лемму 3, находим, что

$$\frac{N(\vec{a}, u_1, \dots, u_{k-1})}{q(q-1)} (q^{m_k} - 1 - (q-1)^2 q^{\frac{m_k}{2}}) \leq N(\vec{z}, u_1, \dots, u_k),$$

$$N(\vec{z}, u_1, \dots, u_k) \leq \frac{N(\vec{a}, u_1, \dots, u_{k-1})}{q(q-1)} (q^{m_k} - 1 + (q-1)^2 q^{\frac{m_k}{2}}).$$

Поэтому

$$\frac{N(z_1, u_1)}{q^{k-1}(q-1)^{k-1}} \prod_{i=2}^k (q^{m_i} - 1 - (q-1)^2 q^{\frac{m_i}{2}}) \leq N(\vec{z}, u_1, \dots, u_k),$$

$$N(\vec{z}, u_1, \dots, u_k) \leq \frac{N(z_1, u_1)}{q^{k-1}(q-1)^{k-1}} \prod_{i=2}^k (q^{m_i} - 1 + (q-1)^2 q^{\frac{m_i}{2}}).$$

Остается воспользоваться неравенствами $q^{m_1-1} - 1 \leq N(z_1, u_1) \leq q^{m_1}$. □

Получим естественные выводы из доказанных результатов.

Следствие 3. Если выполнены условия теоремы 5 и отображение φ сюръективно, то в последовательности v , построенной по правилу (1), появляются все элементы поля P , т. е. $M(v) = P$.

Следствие 4. Если выполнены условия теоремы 5, то для частоты $N(z, v)$ появления элемента $z \in P$ среди элементов $v(0), \dots, v(T-1)$ справедливы оценки

$$\frac{(q^{m_1-1} - 1)|\varphi^{-1}(z)|}{q^{k-1}(q-1)^{k-1}} \prod_{i=2}^k (q^{m_i} - 1 - (q-1)^2 q^{\frac{m_i}{2}}) \leq N(z, v),$$

$$N(z, v) \leq \frac{q^{m_1-k}|\varphi^{-1}(z)|}{(q-1)^{k-1}} \prod_{i=2}^k (q^{m_i} - 1 + (q-1)^2 q^{\frac{m_i}{2}}).$$

Следствие 4 устанавливает единственную известную авторам оценку числа появлений элементов на циклах последовательности v в случае произвольного поля P и произвольной функции φ . Ранее в [3, теорема 18.2] и [9, теоремы 4, 5, 6] были получены нижние и верхние оценки для исследуемых частот при $q = 2$. В [11] получены оценки частот $N(z, v)$ при произвольном q и функции $\varphi(x_1, \dots, x_k) = x_1 + \dots + x_k$.

5. Количество появлений нулевого вектора на входе функции усложнения

В условиях теоремы 5 удастся найти величину $N(\vec{0}, u_1, \dots, u_k)$.

Теорема 6. Пусть $P = GF(q)$, $u_1, \dots, u_k$ — ЛРП над P максимальных периодов $T(u_1) = q^{m_1} - 1, \dots, T(u_k) = q^{m_k} - 1$, числа $m_1, \dots, m_k$ попарно взаимно просты. Тогда

$$N(\vec{0}, u_1, \dots, u_k) = \frac{(q^{m_1-1} - 1) \cdots (q^{m_k-1} - 1)}{(q - 1)^{k-1}}.$$

Доказательство. Рассмотрим автомат $A = (S, P, h, f)$, описанный в разделе 1, где

$$S = (P^{m_1} \setminus \{\vec{0}\}) \times (P^{m_2} \setminus \{\vec{0}\}) \times \cdots \times (P^{m_k} \setminus \{\vec{0}\}).$$

Выберем начальное состояние

$$\vec{\alpha}_0 = (u_1(0), \dots, u_1(m_1 - 1), \dots, u_k(0), \dots, u_k(m_k - 1))$$

из множества S . Тогда в i -й момент времени, $i \geq 0$, получим состояние

$$\vec{\alpha}_i = (u_1(i), \dots, u_1(i + m_1 - 1), \dots, u_k(i), \dots, u_k(i + m_k - 1)) \in S.$$

Последовательность $(\vec{\alpha}_i)_{i=0}^\infty$ — чисто периодическая с периодом

$$T = \frac{(q^{m_1} - 1) \cdots (q^{m_k} - 1)}{(q - 1)^{k-1}}.$$

Каждое состояние лежит на цикле длины T и все состояния из множества S расположены на $(q-1)^{k-1}$ различных циклах длины T . Как было показано в следствии 1, существует такое множество I , состоящее из $(q-1)^{k-1}$ векторов $(c_1, \dots, c_k) \in (P \setminus \{0\})^k$, что имеет место следующее разбиение множества S :

$$\bigcup_{(c_1, \dots, c_k) \in I} \bigcup_{i=0}^{T-1} \{(c_1 u_1(i), \dots, c_1 u_1(i + m_1 - 1), \dots, c_k u_k(i), \dots, c_k u_k(i + m_k - 1))\}.$$

Тогда величина

$$\sum_{(c_1, \dots, c_k) \in I} N(\vec{0}, c_1 u_1, \dots, c_k u_k) = (q - 1)^{k-1} N(\vec{0}, u_1, \dots, u_k)$$

равна количеству всех векторов из S вида

$$(0, \underbrace{*, \dots, *}_{m_1-1}, 0, \underbrace{*, \dots, *}_{m_2-1}, \dots, 0, \underbrace{*, \dots, *}_{m_k-1}),$$

где на местах, обозначенных символом $*$, стоят произвольные элементы поля P . Число таких векторов равно

$$(q^{m_1-1} - 1)(q^{m_2-1} - 1) \dots (q^{m_k-1} - 1),$$

поэтому

$$N(\vec{0}, u_1, \dots, u_k) = \frac{(q^{m_1-1} - 1) \dots (q^{m_k-1} - 1)}{(q - 1)^{k-1}}.$$

□

6. Периоды выходных последовательностей комбинирующих генераторов

Оценим период последовательности v , построенной по правилу (1) с использованием функции усложнения φ специального вида.

Теорема 7. Пусть $P = GF(q)$, $F_1(x), \dots, F_k(x)$ — примитивные многочлены над полем P попарно взаимно простых степеней $m_1, \dots, m_k$ соответственно, функция φ задается над полем P многочленом, свободным от квадратов:

$$\varphi(x_1, \dots, x_k) = c_0 + \sum_{s=1}^k \sum_{1 \leq j_1 < j_2 < \dots < j_s \leq k} c_{j_1 j_2 \dots j_s} x_{j_1} x_{j_2} \dots x_{j_s},$$

и существенно зависит от всех своих аргументов. Тогда существует такой делитель d числа $q - 1$, что

$$T(v) = \frac{(q^{m_1} - 1) \dots (q^{m_k} - 1)d}{(q - 1)^k}.$$

Доказательство. Период последовательности векторов

$$(u_1(i), \dots, u_1(i + m_1 - 1), \dots, u_k(i), \dots, u_k(i + m_k - 1)), \quad i \geq 0,$$

равен

$$T = [T(u_1), \dots, T(u_k)] = \frac{(q^{m_1} - 1) \dots (q^{m_k} - 1)}{(q - 1)^{k-1}}.$$

Значит, $T(v) \mid T$. Период последовательности v не зависит от выбора элемента c_0 , поэтому будем считать, что $c_0 = 0$. Для последовательности v имеем

$$v = \sum_{s=1}^k \sum_{(j_1, \dots, j_s) \in I_s} c_{j_1 \dots j_s} u_{j_1} \dots u_{j_s}, \quad (13)$$

где $I_s = \{(j_1, \dots, j_s) : c_{j_1 \dots j_s} \neq 0\}$, $s = 1, \dots, k$. Известно (см., например, [4]), что $c_{j_1 \dots j_s} u_{j_1} \dots u_{j_s}$ является ненулевой ЛРП с неприводимым над полем P минимальным многочленом степени $m_{j_1} \dots m_{j_s}$. Если $(j_1, \dots, j_s)$ и $(j'_1, \dots, j'_s)$ — различные наборы из I_s , то минимальные многочлены ЛРП $c_{j_1 \dots j_s} u_{j_1} \dots u_{j_s}$ и $c_{j'_1 \dots j'_s} u_{j'_1} \dots u_{j'_s}$ различны, так как имеют разные степени. Если $(j_1, \dots, j_s) \in I_s$, $(i_1, \dots, i_r) \in I_r$, где $s \neq r$, то по этим же причинам минимальные многочлены ЛРП $c_{j_1 \dots j_s} u_{j_1} \dots u_{j_s}$ и $c_{i_1 \dots i_r} u_{i_1} \dots u_{i_r}$ различны. Последовательность v является суммой ЛРП с попарно взаимно простыми характеристическими многочленами и согласно [1, глава 25, утверждение 22]

$$T(v) = [T(u_{j_1} \dots u_{j_s}) : (j_1, \dots, j_s) \in I_s, s = 1, \dots, k]. \quad (14)$$

Рассмотрим $T(u_{j_1} \dots u_{j_s})$. Минимальный многочлен ЛРП $u_{j_1} \dots u_{j_s}$ — это многочлен $F_{j_1}(x) \vee \dots \vee F_{j_s}(x)$ (см. [4]), который является неприводимым многочленом над полем P . Его корень — элемент $\theta_{j_1} \dots \theta_{j_s}$, где θ_{j_l} — корень $F_{j_l}(x)$ в поле $GF(q^{m_{j_l}})$, $l = 1, \dots, s$. Из равенства $T(F_{j_1} \vee \dots \vee F_{j_s}) = \text{ord}(\theta_{j_1} \dots \theta_{j_s})$ и из соотношения (14) получаем

$$T(v) = [\text{ord}(\theta_{j_1} \dots \theta_{j_s}) : (j_1, \dots, j_s) \in I_s, s = 1, \dots, k]. \quad (15)$$

Пусть $t = \text{ord}(\theta_{j_1} \dots \theta_{j_s})$. Ясно, что

$$t \mid [q^{m_{j_1}} - 1, \dots, q^{m_{j_s}} - 1] = \frac{(q^{m_{j_1}} - 1) \dots (q^{m_{j_s}} - 1)}{(q - 1)^{s-1}}. \quad (16)$$

Справедливо равенство $\theta_{j_1}^t \dots \theta_{j_s}^t = e$. Так как

$$\theta_{j_1}^t \in GF(q^{m_{j_1}}), \theta_{j_2}^t \dots \theta_{j_s}^t \in GF(q^{m_{j_2} \dots m_{j_s}}),$$

$$GF(q^{m_{j_1}}) \cap GF(q^{m_{j_2} \dots m_{j_s}}) = GF(q),$$

то $T_{\text{red}}(F_{j_1}) = (q^{m_{j_1}} - 1)/(q - 1) \mid t$ и $\theta_{j_2}^t \dots \theta_{j_s}^t \in GF(q)$. Аналогичными рассуждениями в силу попарной взаимной простоты чисел $T_{\text{red}}(F_{j_1}), \dots, T_{\text{red}}(F_{j_s})$ показываем, что

$$T_{\text{red}}(F_{j_1}) \dots T_{\text{red}}(F_{j_s}) \mid t,$$

а значит, учитывая (16),

$$\text{ord}(\theta_{j_1} \dots \theta_{j_s}) = T_{\text{red}}(F_{j_1}) \dots T_{\text{red}}(F_{j_s}) d_{j_1 \dots j_s},$$

где $d_{j_1 \dots j_s}$ — некоторый делитель числа $q - 1$. Следовательно, имеем

$$T(v) = [T_{\text{red}}(F_{j_1}) \dots T_{\text{red}}(F_{j_s}) d_{j_1 \dots j_s} : (j_1, \dots, j_s) \in I_s, s = 1, \dots, k].$$

Таким образом, учитывая, что φ существенно зависит от всех своих переменных, получим $T_{\text{red}}(F_1) \dots T_{\text{red}}(F_k) \mid T(v)$. $\square$

Отметим, что при $q = 2$ каждая функция φ имеет вид, указанный в теореме 7. В этом случае из теоремы 7 следует точное равенство для периода:

$$T(v) = (2^{m_1} - 1) \dots (2^{m_k} - 1).$$

Этот результат был ранее доказан в [3, теорема 18.2]. В [9] показано, что если при $q = 2$ в формулировке теоремы 7 условие примитивности многочленов заменить на неприводимость над полем P , то будет справедливо равенство

$$T(v) = T(u_1) \dots T(u_k).$$

Согласно результатам работы [4] в условиях теоремы 7 и при дополнительном ограничении $c_0 = 0$ для ранга последовательности v справедливо равенство

$$\text{rank } v = \sum_{s=1}^k \sum_{(j_1, \dots, j_s) \in I_s} m_{j_1} \dots m_{j_s}.$$

7. Частотные характеристики отрезков выходных последовательностей комбинирующих генераторов

Рассмотрим последовательность v , построенную по правилу (1). Пусть l — натуральное число, z — элемент поля P . В этом разделе изучим число $N_l(z, v)$ появлений элемента z среди знаков $v(0), v(1), \dots, v(l-1)$ в одном частном случае выбора функции φ .

Будем говорить, что функция $\varphi(x_1, \dots, x_k)$ биективна по первой переменной, если для любых элементов $a_2, \dots, a_k \in P$ отображение $\varphi_{a_2, \dots, a_k} : P \rightarrow P$, осуществляемое по правилу $\varphi_{a_2, \dots, a_k}(a_1) =$

$\varphi(a_1, a_2, \dots, a_k)$, $a_1 \in P$, является биективным. Аналогично определяется понятие биективности функции φ по i -й переменной, где $i = 1, \dots, k$. Рассмотрим функции φ , которые биективны по каждой из своих переменных. Такие функции называются $(k-1)$ -устойчивыми (см. [22]) или k -арными квазигруппами (см. [23]).

Теорема 8. Пусть $u_1, \dots, u_k$ — ЛРП над полем $P = GF(q)$ с попарно взаимно простыми минимальными многочленами $F_1(x), \dots, F_k(x)$, $\deg F_1(x) = m_1, \dots, \deg F_k(x) = m_k$, $T = [T(F_1), \dots, T(F_k)]$, функция $\varphi(x_1, \dots, x_k)$ биективна по каждой из своих переменных, $z \in P$. Тогда:

1) если $l = T$, то

$$\left| N_l(z, v) - \frac{T}{q} \right| \leq \frac{(q-1)^{\frac{k}{2}+1}}{q} (q^{m_1+\dots+m_k} - T)^{\frac{1}{2}},$$

2) если $l < T$, то

$$\left| N_l(z, v) - \frac{l}{q} \right| \leq \frac{(q-1)^{\frac{k}{2}+1}}{q} \left(\frac{4}{\pi^2} \ln T + \frac{9}{5} \right) q^{\frac{m_1+\dots+m_k}{2}}.$$

Доказательство. Рассмотрим канонический аддитивный характер χ поля $P = GF(q)$ (см. [5]), определенный равенством

$$\chi(x) = e^{2\pi i \frac{\text{Tr}_{P_0}^P(x)}{p}}, \quad x \in P, \quad (17)$$

где i — мнимая комплексная единица, $\text{Tr}_{P_0}^P$ — функция «след» из поля P в простое подполе $P_0 = GF(p)$. Справедливы соотношения (см., например, [5])

$$\sum_{c \in P} \chi(cx) = \begin{cases} q, & \text{если } x = 0, \\ 0, & \text{если } x \in P^*. \end{cases}$$

Тогда

$$N_l(z, v) = \frac{1}{q} \sum_{i=0}^{l-1} \sum_{c \in P} \chi(c(v(i) - z)) = \frac{1}{q} \sum_{c \in P} \chi(-cz) \sum_{i=0}^{l-1} \chi(cv(i)),$$

и следовательно,

$$N_l(z, v) = \frac{l}{q} + \frac{1}{q} \sum_{c \in P^*} \chi(-cz) \sum_{i=0}^{l-1} \chi(cv(i)).$$

Для каждого $c \in P^*$ рассмотрим отображение ψ_c , действующее по праву

$$\psi_c(x_1, \dots, x_k) = \chi(c\varphi(x_1, \dots, x_k)), \quad x_1, \dots, x_k \in P. \quad (18)$$

Получим равенство

$$N_l(z, v) = \frac{l}{q} + \frac{1}{q} \sum_{c \in P^*} \chi(-cz) \sum_{i=0}^{l-1} \psi_c(u_1(i), \dots, u_k(i)).$$

Разложим отображение ψ_c по базису характеров группы $(P^k, +)$ (см., например, [24–26])

$$\psi_c(x_1, \dots, x_k) = \sum_{\vec{a}=(a_1, \dots, a_k) \in P^k} \nu_{\psi_c}(\vec{a}) \chi(a_1 x_1 + \dots + a_k x_k), \quad (19)$$

где для всех $\vec{a} \in P^k$ комплексные числа $\nu_{\psi_c}(\vec{a})$ (спектральные коэффициенты) определяются равенствами

$$\nu_{\psi_c}(\vec{a}) = \frac{1}{q^k} \sum_{\vec{b}=(b_1, \dots, b_k) \in P^k} \psi_c(\vec{b}) \chi(-a_1 b_1 - \dots - a_k b_k). \quad (20)$$

Согласно равенству (19)

$$N_l(z, v) = \frac{l}{q} + \frac{1}{q} \sum_{c \in P^*} \chi(-cz) \sum_{i=0}^{l-1} \sum_{\vec{a} \in P^k} \nu_{\psi_c}(\vec{a}) \chi(a_1 u_1(i) + \dots + a_k u_k(i)).$$

Обозначим через $\|\vec{a}\|$ вес вектора $\vec{a} = (a_1, \dots, a_k) \in P^k$, равный количеству ненулевых элементов среди $a_1, \dots, a_k$. Биективность функции φ по каждой из переменных согласно [22] равносильна тому, что $\nu_{\psi_c}(\vec{a}) = 0$ для всех таких $\vec{a} \in P^k$, что $\|\vec{a}\| < k$. Следовательно,

$$\begin{aligned} & \left| N_l(z, v) - \frac{l}{q} \right| \\ & \leq \frac{1}{q} \sum_{c \in P^*} \sum_{\vec{a} \in P^k, \|\vec{a}\|=k} |\nu_{\psi_c}(\vec{a})| \max_{\vec{a} \in P^k, \|\vec{a}\|=k} \left| \sum_{i=0}^{l-1} \chi(a_1 u_1(i) + \dots + a_k u_k(i)) \right|. \end{aligned} \quad (21)$$

Используя неравенство Коши и равенство Парсеваля (см. [1, 24, 26]), получим

$$\sum_{\vec{a} \in P^k, \|\vec{a}\|=k} |\nu_{\psi_c}(\vec{a})| \leq (q-1)^{\frac{k}{2}} \left(\sum_{\vec{a} \in P^k, \|\vec{a}\|=k} |\nu_{\psi_c}(\vec{a})|^2 \right)^{\frac{1}{2}} = (q-1)^{\frac{k}{2}}. \quad (22)$$

Последовательность $a_1u_1 + \dots + a_ku_k$ при каждом таком векторе $\vec{a} \in P^k$, что $\|\vec{a}\| = k$, является ЛРП с минимальным многочленом $F(x) = F_1(x) \cdots F_k(x)$, при этом ее период равен $T = T(F) = [T(F_1), \dots, T(F_k)]$ (см. [1, 5]). Согласно [5, задача 8.66] при $l = T$

$$\left| \sum_{i=0}^{l-1} \chi(a_1u_1(i) + \dots + a_ku_k(i)) \right| \leq (q^{m_1+\dots+m_k} - T)^{\frac{1}{2}}, \quad (23)$$

а при $l < T$ (см., например, [25])

$$\left| \sum_{i=0}^{l-1} \chi(a_1u_1(i) + \dots + a_ku_k(i)) \right| \leq \left(\frac{4}{\pi^2} \ln T + \frac{9}{5} \right) q^{\frac{m_1+\dots+m_k}{2}}. \quad (24)$$

Для завершения доказательства остается воспользоваться неравенствами (21)–(24). $\square$

Заметим, что если в условиях теоремы 8 числа $T(F_1), \dots, T(F_k)$ попарно взаимно просты, то согласно результатам [8]

$$T(v) = T = T(F_1) \cdots T(F_k).$$

Приведем один класс функций φ , удовлетворяющих условиям теоремы 8. Пусть $g_1, \dots, g_{k+1}$ — произвольные подстановки на множестве P . Рассмотрим функцию φ вида

$$\varphi(x_1, \dots, x_k) = g_{k+1}(g_1(x_1) + \dots + g_k(x_k)), \quad x_1, \dots, x_k \in P.$$

Несложно заметить, что так заданная функция φ биективна по каждой из своих переменных.

Отметим, что функции φ , удовлетворяющие одновременно условиям теорем 7 и 8, имеют следующий вид:

$$\varphi(x_1, \dots, x_k) = c_0 + c_1x_1 + \dots + c_kx_k,$$

где $c_1, \dots, c_k$ — ненулевые элементы поля P .

Вопрос о возможности получения нетривиальных оценок частот $N_l(z, v)$ для других классов функций усложнения φ пока остается открытым.

Список литературы

- [1] Глухов М.М., Елизаров В.П., Нечаев А.А., *Алгебра: Учебник*, СПб.: Лань, 2015, 608 с.
- [2] Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В., *Основы криптографии*, М.: Гелиос АРВ, 2001, 480 с.
- [3] Фомичев В.М., *Методы дискретной математики в криптологии*, М.: Диалог-МИФИ, 2010, 424 с.
- [4] Rueppel R.A., *Analysis and design of stream ciphers*, Springer-Verlag, 1986, 244 pp.
- [5] Лидл Р., Нидеррайтер Г., *Конечные поля*, **1, 2**, М.: Мир, 1988, 822 с.
- [6] Gammel B.M., Gottfert R., Kniffler O., “The Achterbahn stream cipher. eSTREAM, ECRYPT stream cipher project”, report 2005/002, 2005.
- [7] Lot N.H., Zawawi A., Seman K., Zaizi N.J.M., “A new proposed design of a stream cipher algorithm: Modified Grain-128”, *Int. J. Computer and Inf. Technology*, **3**:5 (2014), 902–908.
- [8] Фомичев В.М., “О периодах усложненных последовательностей”, *Математические вопросы кибернетики*, 2004, № 13, 37–40.
- [9] Бияляк И.Б., Камловский О.В., “Частотные характеристики циклов выходных последовательностей комбинирующих генераторов над полем из двух элементов”, *Прикладная дискретная математика*, 2015, № 3(29), 17–31.
- [10] Камловский О.В., “Количество появлений векторов на циклах выходных последовательностей двоичных комбинирующих генераторов”, *Проблемы передачи информации*, **53**:1 (2017), 92–100.
- [11] Niederreiter H., “Weights of cyclic codes.”, *Inf. and control*, **34** (1977), 130–140.
- [12] Aulet R. Rodriguez, “Some properties of the output sequences of combined generator over finite fields”, *Prikl. Diskr. Mat. Suppl*, 2019, № 12, 151–154.
- [13] Меженная Н.М., Михайлов В.Г., “О распределении числа единиц в выходной последовательности генератора Пола над полем $GF(2)$ ”, *Математические вопросы криптографии*, **4**:4 (2013), 95–107.
- [14] Меженная Н.М., “О распределении числа единиц в двоичной мультициклической последовательности”, *Прикладная дискретная математика*, 2015, № 1(27), 69–77.
- [15] Нечаев А.А., Кузьмин А.С., Куракин В.Л., “Структурные, аналитические и статистические свойства линейных и полилинейных рекуррент”, *Труды по дискретной математике*, **3** (2000), 155–194.
- [16] Михайлов Д.А., “Унитарные полилинейные регистры и их периоды”, *Дискретная математика*, **14**:1 (2002), 30–59.
- [17] Hall M., “Equidistribution of residues in sequences”, *Duke Math. J.*, **4**:4 (1938), 691–695.
- [18] Цирлер Н., “Линейные возвратные последовательности”, *Кибернетический сборник*, 1963, № 6, 55–79.
- [19] Mullen G.L., Shparlinski I.E., “Values of linear recurring sequences of vectors over finite fields”, *Acta Arith.*, **65**:3 (1993), 221–226.
- [20] Herlestam T., “On functions of linear shift register sequences”, *Lect. Notes Comput. Sci.*, **219**, 1986, 119–129.
- [21] Шпарлинский И.Е., “О распределении значений рекуррентных последовательностей”, *Проблемы передачи информации*, **25**:2 (1989), 46–53.
- [22] Camion P., Canteaut A., “Generalization of Siegenthaler inequality and Schnorr-Vaundenay multipermutation”, *Lect. Notes Comput. Sci.*, 1996, 372–386.
- [23] Черемушкин А.В., *Декомпозиция и классификация дискретных функций*, М.: Курс, 2018, 288 с.

- [24] Солодовников В.И., “Бент-функции из конечной абелевой группы в конечную абелеву группу”, *Дискретная математика*, **14**:1 (2002), 99–113.
- [25] Камловский О.В., “Количество появлений элементов в выходных последовательностях фильтрующих генераторов”, *Прикладная дискретная математика*, 2013, №3(21), 11–25.
- [26] Камловский О.В., “Спектральный метод оценки числа решений систем нелинейных уравнений с линейными рекуррентными аргументами”, *Дискретная математика*, **28**:2 (2016.), 27–43.