А. Д. Бугров, Кросс-корреляционная функция усложнений линейных рекуррент, *Дискрет. матем.*, 2016, том 28, выпуск 4, 38–49

DOI: 10.4213/dm1391

Дискретная математика

том 28 выпуск 4 * 2016

УДК 512.547+512.552 DOI 10.4213/dm1391

Кросс-корреляционная функция усложнений линейных рекуррент

© 2016 г. А. Д. Бугров*

Рассматриваются усложнения линейных рекуррентных последовательностей над полем $GF(q)$ и кольцом $GR(q^n, p^n)$ с взаимосвязанными законами рекурсии. Оценивается кросс-корреляционная функция между циклами данных последовательностей.

Ключевые слова:линейные рекуррентные последовательности, усложнение последовательности, конечные поля, кольцо Галуа, кросс-корреляционная функция

Введение

Пусть p — простое число, $q = p^s$, где s — натуральное число, $P = GF(q)$ — конечное поле из q элементов, $R = GR(q^n, p^n)$ — кольцо Галуа из q^n элементов характеристики p^n. Обозначим через $u_1, u_2, \ldots, u_k$ линейные рекуррентные последовательности (ЛРП) над P с общим характеристическим многочленом $F(x) \in P[x]$ степени $\deg F(x) = m$, а через v ЛРП над R с характеристическим многочленом $G(x) \in R[x]$. Рассмотрим произвольные отображения $\varphi : P^k \to P$, $\psi : R \to P$ и последовательности $\omega_1 = \varphi(u_1, u_2, \ldots, u_k)$, $\omega_2 = \psi(v)$ знаки которых определены равенствами

$$\omega_1(i) = \varphi(u_1(i), u_2(i), \ldots, u_k(i)), \quad \omega_2(i) = \psi(v(i)), \quad i \in \mathbb{N}_0, \tag{1}$$

где $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ — множество целых неотрицательных чисел. Последовательности ω_1 и ω_2 будем называть усложнениями исходных ЛРП $u_1, u_2, \ldots, u_k$ и v соответственно. В [1] и [2] такие последовательности рассматриваются и используются как псевдослучайные последовательности. Заметим, что если u_1, u_2, …, u_k являются сдвигами одной ЛРП, то последовательность $\varphi(u_1, u_2, \ldots, u_k)$ является выходной последовательностью фильтрующего генератора с фильтрующей функцией φ.

Здесь решается задача получения нетривиальных оценок значения кросс-корреляционной функции отрезков

$$(\omega_1(0), \omega_1(1), \ldots, \omega_1(T-1)), (\omega_2(0), \omega_2(1), \ldots, \omega_2(T-1)),$$

*Место работы: ООО «Центр сертификационных исследований»,
e-mail: bugrovalexey1@ya.ru

где T — общий период последовательностей ω_1 и ω_2. В [3] эта задача была решена в частном случае $P = GF(2)$, $R = \mathbb{Z}_{2^n}$. В настоящей работе оценки кросс-корреляционной функции получены в случае, когда $F(x)$ неприводим над полем P и $\bar{G}(x) = F(x)$, т. е. $G(x)$ — многочлен Галуа.

Для кольца Галуа $R = GR(q^n, p^n)$ характеристики p^n поле $\bar{R} = R/pR$ называется его полем вычетов. Известно, что $\bar{R}$ — поле из q элементов. Далее для удобства изложения будем считать, что $\bar{R} = P$, а операции сложения в R и $\bar{R}$ будем обозначать одним символом $+$. Образ элемента $a \in R$ при действии естественного эпиморфизма колец $R \to \bar{R}$ обозначим через $\bar{a}$. Естественный эпиморфизм колец $R \to \bar{R}$ индуцирует эпиморфизм колец многочленов $R[x] \to \bar{R}[x]$. Образ многочлена $A(x) = \sum a_i x^i \in R[x]$ при этом эпиморфизме будем обозначать через $\bar{A}(x)$, где $\bar{A}(x) = \sum \bar{a}_i x^i \in \bar{R}[x]$.

1. Кросс-корреляционная функция последовательностей

Пусть ω_1 и ω_2 — произвольные периодические последовательности над P с периодами $T(\omega_1)$ и $T(\omega_2)$ соответственно, T — некоторое общее кратное этих чисел. Через $\mathrm{tr}_{P_0}^{P}$ будем обозначать функцию след из поля P в простое подполе P_0, задаваемую равенством

$$\mathrm{tr}_{P_0}^{P}(x) = x + x^p + \ldots + x^{p^{s-1}}, \quad x \in P.$$

Для любого $b \in P$ через χ_b будем обозначать аддитивный характер поля P

$$\chi_b(x) = \exp\left\{2\pi i \frac{\mathrm{tr}_{P_0}^{P}(bx)}{p}\right\}, \quad x \in P.$$

Назовем кросс-корреляционной функцией последовательностей ω_1 и ω_2 (см., например, [4]) функцию

$$C_{b,\omega_1,\omega_2}(t) = \sum_{i=0}^{T-1} \chi_b(\omega_1(i) - \omega_2(i+t)), \quad t \in \overline{0, T-1}, \tag{2}$$

где $\overline{0, T-1} = \{0, 1, \ldots, T-1\}$. При нулевом b всегда верно равенство $C_{b,\omega_1,\omega_2}(t) = T$, поэтому всюду далее будем исследовать кросс-корреляционную функцию последовательностей только при ненулевом b. В случае когда $\omega_1 = \omega_2$, кросс-корреляционную функцию называют автокорреляционной функцией последовательности ω_1. Введем обозначение

$$C_{\omega_1,\omega_2}(t) = \max_{b \in P \setminus \{0\}} |C_{b,\omega_1,\omega_2}(t)|.$$

Величина $C_{\omega_1,\omega_2}(t)$ характеризует «близость» последовательности ω_1 и сдвига $x^t\omega_2 \stackrel{\text{def}}{=} (\omega_2(t), \omega_2(t+1), \ldots)$ последовательности ω_2 на t шагов. Чем меньше значение $C_{\omega_1,\omega_2}(t)$, тем больше отличаются друг от друга рассматриваемые последовательности. Известно (см., например, [5]), что $C_{\omega_1,\omega_2}(t) = 0$ тогда и только тогда,

когда среди элементов $\omega_1(i) - \omega_2(i+t), i \in \overline{0, T-1}$, все элементы из P появляются одинаковое количество раз. Если $p = q$, то можно считать, не ограничивая общности, что $P = \mathbb{Z}_p$. Будем говорить, что последовательность ω над кольцом целых чисел равномерно распределена по модулю p (см. [6, глава 5]), если

$$\lim_{N\to\infty} \frac{A(j,p,N)}{N} = \frac{1}{p}, \quad j \in \overline{1,p},$$

где $A(j,p,N)$ — число элементов среди $\omega(0), \omega(1), \ldots, \omega(N-1)$, удовлетворяющих сравнению $\omega(i) \equiv j \pmod p$. Если последовательности ω_1, ω_2 — чисто периодические, то верно равенство

$$\lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{N} \exp\left\{2\pi i \frac{b(\omega_1(j) - \omega_2(j+t))}{p}\right\} = \frac{C_{b,\omega_1,\omega_2}(t)}{T},$$

следовательно, по критерию Вейля [6, теорема 1.2, глава 5] $C_{\omega_1,\omega_2}(t) = 0$ тогда и только тогда, когда последовательность с элементами

$$\omega_1(i) - \omega_2(i+t), i \in \mathbb{N}_0,$$

равномерно распределена по модулю p. Если ω_1 и ω_2 — двоичные последовательности, то верно равенство

$$T - 2\rho(\omega_1, x^t\omega_2) = C_{\omega_1,\omega_2}(t),$$

где $\rho(\omega_1, x^t\omega_2)$ — расстояние Хемминга между начальными отрезками последовательностей ω_1 и $x^t\omega_2$ длины T (см. [3]).

Пусть отрезки последовательностей

$$(\omega_1(0), \ldots, \omega_1(T-1)), (\omega_2(t), \ldots, \omega_2(t+T-1))$$

— это вектор-строки значений функций $f, g : P^n \to P$ соответственно при некотором расположении аргументов. Тогда значение кросс-корреляционной функции последовательностей ω_1 и ω_2 совпадает со значением коэффициента кросс-корреляции между функциями f и g:

$$C_{b,\omega_1,\omega_2}(t) = C_b(f,g).$$

Подробнее коэффициенты кросс-корреляции между функциями рассматриваются в [5]. Заметим, что функция $C_{b,\omega_1,\omega_2}(t)$, определенная равенством (2), зависит от выбора параметра T. В основном приложения относятся только к ситуации когда $T = T(\omega_1) = T(\omega_2)$, где $T(\omega_1)$, $T(\omega_2)$ — минимальные периоды последовательностей.

2. Оценка кросс-корреляционной функции

Пусть $u_1, \ldots, u_k$ — ЛРП над полем $P = GF(q)$ с неприводимым над P характеристическим многочленом $F(x) \in P[x]$ степени $\deg F(x) = m$, а v — ЛРП над

$R = GR(q^n, p^n)$ с характеристическим многочленом $G(x) \in R[x]$, удовлетворяющим условию $\bar{G}(x) = F(x)$. Заметим, что $\deg G(x) = m$. В этом случае для периодов $T(F)$ и $T(G)$ многочленов $F(x)$ и $G(x)$ справедливы равенства

$$T(F) = \frac{q^m - 1}{d}, \quad T(G) = p^\nu T(F), \tag{3}$$

где d — некоторый делитель числа $q^m - 1$, а ν — целое число, удовлетворяющее неравенствам $0 \leqslant \nu \leqslant n-1$ (см. [7, утверждение 4.1]).

Обозначим через $\bar{v}$ последовательность, полученную из v действием естественного эпиморфизма $R \to \bar{R}$ на каждый ее элемент. Она является ЛРП с характеристическим многочленом $F(x)$ (см. [7]). Всюду в дальнейшем мы будем рассматривать случай, когда среди элементов $v(0)$, $v(1)$, …, $v(m-1)$ начального отрезка ЛРП v есть хотя бы один обратимый элемент кольца R, т. е. $\bar{v}$ — ненулевая последовательность. Назовем отображение $\psi : R \to P$ сбалансированным (см. [8]), если при каждом $a \in P$ уравнение $\psi(x) = a$ имеет ровно $|R|/|P| = q^{n-1}$ решений относительно неизвестного $x \in R$.

Пусть χ — канонический аддитивный характер поля P, т. е.

$$\chi(x) = \exp\left\{2\pi i \frac{\mathrm{tr}_{P_0}^{P}(x)}{p}\right\}, \quad x \in P.$$

Группа характеров группы $(\underbrace{P \oplus \ldots \oplus P}_{k}, +)$ состоит из отображений вида $\chi(a_1x_1 + \ldots + a_kx_k), a_1, \ldots, a_k \in P$. Применяя разложение композиции $\chi_b \circ \varphi \colon P^k \to \mathbb{C}^*$ отображений χ_b и φ по базису характеров группы $(\underbrace{P \oplus \ldots \oplus P}_{k}, +)$ (см., например, [9, равенство 12]), получим

$$\chi_b\Big(\varphi(u_1(i), u_2(i), \ldots, u_k(i))\Big) = \sum_{\vec{a}=(a_1,\ldots,a_k)\in P^k} W_{\chi_b\circ\varphi}(\vec{a})\chi(a_1u_1(i)+\ldots+a_ku_k(i)), \tag{4}$$

где $W_{\chi_b\circ\varphi}(\vec{a})$ — спектральные коэффициенты, которые определяются равенством

$$W_{\chi_b\circ\varphi}(\vec{a}) = \frac{1}{q^k} \sum_{\vec{y}=(y_1,\ldots,y_k)\in P^k} (\chi_b \circ \varphi)(\vec{y})\chi(-a_1y_1 - \ldots - a_ky_k).$$

Введем обозначение

$$\sigma_1(\chi_b \circ \varphi) = \sum_{\vec{a}\in P^k} |W_{\chi_b\circ\varphi}(\vec{a})|.$$

Приведем некоторые обозначения и результаты из теории колец Галуа (см. [10, §§ 2, 3]). Введем p-адическое множество $\Gamma(R) = \{\alpha \in R | \alpha^q = \alpha\}$. Каждый элемент x кольца R может быть единственным образом представлен в виде p-адического разложения

$$x = \gamma_0(x) + p\gamma_1(x) + \ldots + p^{n-1}\gamma_{n-1}(x),$$

где $\gamma_j \colon R \to \Gamma(R), j \in \overline{0, n-1}$, — разрядные функции кольца R. Обозначим через R_0 множество, состоящее из элементов $0, e, 2e, \ldots, (p^n - 1)e$, где e — единица кольца R.

Множество R_0 является подкольцом кольца R, изоморфным кольцу $\mathbb{Z}_{p^n}$. Через $\mathrm{Aut}(R/R_0)$ обозначим множество всех автоморфизмов кольца R, оставляющих на месте каждый элемент кольца R_0. Группа $(\mathrm{Aut}(R/R_0), \circ)$ — циклическая группа порядка t, порожденная автоморфизмом σ_0, который действует на каждый элемент $x \in R$, имеющий p-адическое разложение $x = \gamma_0(x) + p\gamma_1(x) + ... + p^{n-1}\gamma_{n-1}(x)$, следующим образом:

$$\sigma_0(x) = \gamma_0(x)^p + p\gamma_1(x)^p + ... + p^{n-1}\gamma_{n-1}(x)^p.$$

Функция след $\mathrm{Tr}_{R_0}^R$ из кольца R в кольцо R_0 определяется равенством

$$\mathrm{Tr}_{R_0}^R(x) = \sum_{\sigma \in \mathrm{Aut}(R/R_0)} \sigma(x).$$

Для любого элемента $c \in R$ отображение $\hat{\chi}_c : R \to \mathbb{C}^*$,

$$\hat{\chi}_c(x) = \exp\left\{2\pi i \mathrm{Tr}_{R_0}^R(cx)/p^n\right\}$$

является характером аддитивной группы кольца R, причем если a и b — различные элементы кольца R, то $\hat{\chi}_a \neq \hat{\chi}_b$. Других характеров аддитивной группы кольца R нет (см. [11, §3]). В дальнейшем будем использовать обозначение $\hat{\chi}_e = \hat{\chi}$.

Имеет место следующее разложение композиции $\chi_{-b} \circ \psi : R \to \mathbb{C}^*$ отображений χ_{-b} и ψ по базису характеров группы $(R, +)$ (см., например, [9, равенство (12)]):

$$\chi_b\Big(-\psi(v(i))\Big) = \chi_{-b}\Big(\psi(v(i))\Big) = \sum_{r \in R} \mu_{r,-b}\hat{\chi}(rv(i)), \tag{5}$$

где

$$\mu_{r,-b} = \frac{1}{q^n}\sum_{s \in R} \chi_{-b}(\psi(s))\hat{\chi}(-rs). \tag{6}$$

Введем обозначение

$$\sigma_2(\chi_{-b} \circ \psi) = \sum_{r \in R} |\mu_{r,-b}|.$$

Зададим операцию $\oplus : \Gamma(R) \times \Gamma(R) \to \Gamma(R)$ правилом $\alpha \oplus \beta = \gamma_0(\alpha + \beta)$. Известно, что $(\Gamma(R), \oplus, \cdot)$ — поле из q элементов. Определим отображение $\tau : (P, +, \cdot) \to (\Gamma(R), \oplus, \cdot)$, являющееся изоморфизмом полей, правилом $\tau(\bar{r}) = \gamma_0(r)$. Определение τ корректно, так как все представители одного класса вычетов факторкольца R/pR имеют одинаковые нулевые разряды в p-адическом представлении.

Заметим, что естественный эпиморфизм колец $R \to \bar{R}$ задается правилом $\bar{r} = [\gamma_0(r)]$. Следовательно, композиция естественного эпиморфизма колец $R \to \bar{R} = P$ и изоморфизма $\tau : P \to \Gamma(R)$ является тождественным преобразованием на P:

$$\overline{\tau(\bar{r})} = \overline{\gamma_0(r)} = [\gamma_0(\gamma_0(r))] = [\gamma_0(r)] = \bar{r}. \tag{7}$$

Несложно видеть, что для любого $r \in R$ верно равенство

$$p^{n-1}r = p^{n-1}\tau(\bar{r}),$$

которое будет использоваться далее.

Теорема 1. *Пусть* $\omega_1 = \varphi(u_1, \dots, u_k)$, $\omega_2 = \psi(v)$, *где* ψ — *сбалансированное отображение. Тогда, если* $x^t\bar{v}$ *линейно не выражается через систему* u_1, u_2, …, u_k, *то для кросс-корреляционной функции* $C_{b,\omega_1,\omega_2}(t)$, *определенной равенством* (2) *при* $T = T(G)$, *справедливо неравенство*

$$\left| C_{b,\omega_1,\omega_2}(t) + \frac{p^\nu}{d}\chi_b(\varphi(\vec{0}) - \psi(0)) \right| \leqslant \sigma_1(\chi_b \circ \varphi)\sigma_2(\chi_{-b} \circ \psi)\frac{p^\nu(dp^{n-1} - 1)}{d} q^{\frac{m}{2}}.$$

Доказательство. Из равенств (1), (2) следует соотношение

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

С использованием равенств (4) и (5) будем иметь

$$C_{b,\omega_1,\omega_2}(t) = \sum_{i=0}^{T-1} \left(\sum_{\vec{a}\in P^k} W_{\chi_b\circ\varphi}(\vec{a})\chi(a_1u_1(i) + \ldots + a_ku_k(i)) \right) \left(\sum_{r\in R} \mu_{r,-b}\hat{\chi}(rv(i+t)) \right). \tag{8}$$

Пусть $x \in P$, тогда $\tau(x)$ представим в виде

$$\tau(x) = \gamma_0(\tau(x)).$$

Используя результаты [10, §§2, 3], получим равенства

$$\mathrm{Tr}_{R_0}^R(p^{n-1}\tau(x)) = \sum_{\sigma\in Aut(R/R_0)} \sigma\left(p^{n-1}\gamma_0(\tau(x))\right) =$$

$$= \sum_{i=0}^{t-1} \sigma_0^i\left(p^{n-1}\gamma_0(\tau(x))\right) = \sum_{i=0}^{t-1} p^{n-1}\gamma_0(\tau(x))^{p^i} = \sum_{i=0}^{t-1} p^{n-1}\tau(x)^{p^i} =$$

$$= p^{n-1}\sum_{i=0}^{t-1} \oplus\tau(x)^{p^i} = p^{n-1}\tau\left(\sum_{i=0}^{t-1} x^{p^i}\right) = p^{n-1}\tau(\mathrm{tr}_{P_0}^P(x)) = p^{n-1}\,\mathrm{tr}_{P_0}^P(x).$$

Следовательно,

$$\chi(x) = e^{2\pi i\frac{\mathrm{tr}_{P_0}^P(x)}{p}} = e^{2\pi i\frac{\mathrm{Tr}_{R_0}^R(p^{n-1}\tau(x))}{p^n}} = \hat{\chi}(p^{n-1}\tau(x)). \tag{9}$$

Используя равенства (8), (9), получим

$$C_{b,\omega_1,\omega_2}(t) = \sum_{\vec{a}\in P^k, r\in R} W_{\chi_b\circ\varphi}(\vec{a})\mu_{r,-b}\sum_{i=0}^{T-1}\hat{\chi}\Big(u_{a_1,\dots,a_k,r}(i)\Big), \tag{10}$$

где $u_{a_1,\dots,a_k,r}$ — последовательность над кольцом R, элементы которой определены равенством

$$u_{a_1,\dots,a_k,r}(i) = p^{n-1}\tau(a_1u_1(i)) + \ldots + p^{n-1}\tau(a_ku_k(i)) + rv(i+t), \quad i \in \mathbb{N}_0.$$

Покажем, что $u_{a_1,\ldots,a_k,r}$ — ЛРП с характеристическим многочленом $G(x)$. Для этого достаточно показать, что последовательность с элементами $p^{n-1}\tau(a_ju_j(i))$, $i \in \mathbb{N}_0$, для любого $j \in \overline{1,k}$ является ЛРП с характеристическим многочленом $G(x)$. В терминах работы [12, глава XXV, §2] это значит, что верно равенство $p^{n-1}G(x)\tau(a_ju_j) = (0)$, которое равносильно равенству $\overline{G(x)\tau(a_ju_j)} = (\bar{0})$, где $(0) = (0,0,\ldots,0,\ldots), 0 \in R$, $(\bar{0}) = (\bar{0},\bar{0},\ldots,\bar{0},\ldots), \bar{0} \in R/pR$. Пусть $G(x) = \sum_{i=0}^{m} g_ix^i$, следовательно, $\overline{G(x)} = F(x) = \sum_{i=0}^{m} \bar{g}_ix^i = \sum_{i=0}^{m} f_ix^i$. Поэтому, учитывая равенство (7), получим

$$\overline{G(x)\tau(a_ju_j)} = \overline{\sum_{i=0}^{m} g_ix^i\tau(a_ju_j)} = \sum_{i=0}^{m} f_i\overline{\tau(a_jx^iu_j)} =$$

$$= \sum_{i=0}^{m} f_ia_jx^iu_j = a_jF(x)u_j = (\bar{0}).$$

Покажем, что последовательность $u_{a_1,\ldots,a_k,r}$ ненулевая при всех $r \in R\backslash\{0\}$ и $(a_1,\ldots,a_k) \in P^k$. Действительно, если бы она была нулевой, то из $\bar{v} \neq (\bar{0})$ имели бы $r \in p^{n-1}R\backslash\{0\}$, что равносильно $r = ap^{n-1}$, где a — обратимый элемент кольца R. Тогда

$$p^{n-1}(av(i+t) + \tau(a_1u_1(i)) + \ldots + \tau(a_ku_k(i))) = 0,$$

из чего следует равенство

$$\overline{av(i+t)} + \overline{\tau(a_1u_1(i))} + \ldots + \overline{\tau(a_ku_k(i))} = \bar{a}\bar{v}(i+t) + a_1u_1(i) + \ldots + a_ku_k(i) = \bar{0},$$

противоречащее условию $\bar{a} \neq \bar{0}$.

Преобразовав равенство (10), имеем

$$C_{b,\omega_1,\omega_2}(t) + \varkappa = \sum_{\vec{a}\in P^k, r\in R} W_{\chi_b\circ\varphi}(\vec{a})\mu_{r,-b}\Big(\sum_{i=0}^{T-1}\hat{\chi}(u_{a_1,\ldots,a_k,r}(i)) + \frac{p^\nu}{d}\Big)\Big),$$

где

$$\varkappa = \frac{p^\nu}{d}\sum_{\vec{a}\in P^k, r\in R} W_{\chi_b\circ\varphi}(\vec{a})\mu_{r,-b}.$$

Найдем значение $\varkappa$. Согласно (4) и (5)

$$\varkappa = \frac{p^\nu}{d}\left(\sum_{\vec{a}\in P^k} W_{\chi_b\circ\varphi}(\vec{a})\right)\left(\sum_{r\in R}\mu_{r,-b}\right) = \frac{p^\nu}{d}\chi_b(\varphi(\vec{0}) - \psi(0)).$$

Значит

$$C_{b,\omega_1,\omega_2}(t) + \frac{p^\nu}{d}\chi_b(\varphi(\vec{0}) - \psi(0)) = \sum_{\vec{a}\in P^k, r\in R} W_{\chi_b\circ\varphi}(\vec{a})\mu_{r,-b}\left(\sum_{i=0}^{T-1}\hat{\chi}(u_{a_1,\ldots,a_k,r}(i)) + \frac{p^\nu}{d}\right). \tag{11}$$

По условию отображение ψ сбалансировано, и из (6) следует равенство $\mu_{0,-b} = 0$, поэтому в равенстве (11) достаточно ограничиться суммированием по всем $r \neq 0$. Переходя к абсолютным величинам, получим

$$\left|C_{b,\omega_1,\omega_2}(t)+\frac{p^\nu}{d}\chi_b(\varphi(\vec{0})-\psi(0))\right| \leqslant \sigma_1(\chi_b\circ\varphi)\sigma_2(\chi_{-b}\circ\psi)\max_{\vec{a}\in P^k, r\neq 0}\left|\sum_{i=0}^{T-1}\hat{\chi}(u_{a_1,\ldots,a_k,r}(i))+\frac{p^\nu}{d}\right|.$$

Пусть $u(i)$ — такая ЛРП над R с характеристическим многочленом $G(x)$, что $\bar{u} \neq (0)$. Рассмотрим подробнее значение величины $\hat{\chi}(u(i))$, где $\hat{\chi}$ — аддитивный характер кольца R, этот факт будем отображать в обозначении $\hat{\chi}_R$. Из [10, теорема 8] следует, что $u(i) = \mathrm{Tr}_R^S(b\alpha^i)$, где $S = GR(q^{mn}, p^n)$ — расширение Галуа кольца R, $b \in S$, α — корень многочлена $G(x)$ в кольце S, $i \in \overline{0, T-1}$. Поэтому, учитывая транзитивность функции след, получим

$$\hat{\chi}_R(u(i)) = \exp\left\{2\pi i\,\mathrm{Tr}_{R_0}^R(u(i))/p^n\right\} = \exp\left\{2\pi i\,\mathrm{Tr}_{R_0}^R(\mathrm{Tr}_R^S(b\alpha^i))/p^n\right\} =$$

$$= \exp\left\{2\pi i\,\mathrm{Tr}_{R_0}^S(b\alpha^i)/p^n\right\} = \hat{\chi}_S(b\alpha^i).$$

Несложно проверить, что элемент b обратим в кольце S, так как это равносильно условию $\bar{u} \neq (0)$. Следовательно, $\mathrm{ord}\,\alpha = T(G)$. Также заметим, что $\bar{u}_{a_1,\ldots,a_k,r} \neq (0)$. Это позволяет применить теорему 2 из работы [13] к ЛРП $u_{a_1,\ldots,a_k,r}$:

$$\left|\sum_{i=0}^{T-1}\hat{\chi}_R(u_{a_1,\ldots,a_k,r}(i)) + \frac{p^\nu}{d}\right| \leqslant \frac{p^\nu(dp^{n-1}-1)}{d}q^{\frac{m}{2}}. \tag{12}$$

Таким образом

$$\left|C_{b,\omega_1,\omega_2}(t) + \frac{p^\nu}{d}\chi_b(\varphi(\vec{0}) - \psi(0))\right| \leqslant \sigma_1(\chi_b\circ\varphi)\sigma_2(\chi_{-b}\circ\psi)\frac{p^\nu(dp^{n-1}-1)}{d}q^{\frac{m}{2}}. \quad \square \tag{13}$$

Следствие 1. *В условиях теоремы* 1 *верно неравенство*

$$\left|C_{b,\omega_1,\omega_2}(t) + \frac{p^\nu}{d}\chi_b(\varphi(\vec{0}) - \psi(0))\right| \leqslant \frac{p^\nu(dp^{n-1}-1)}{d}q^{\frac{m+n+k}{2}}.$$

Доказательство. Учитывая нормировку в определении величины $W_{\chi_b\circ\varphi}(\vec{a})$, из п.4 утверждения 2 в [14] следует, что

$$\sigma_1(\chi_b\circ\varphi) \leqslant q^{\frac{k}{2}}, \tag{14}$$

а в [15, теорема 1] показано, что

$$\sigma_2(\chi_{-b}\circ\psi) \leqslant q^{\frac{n}{2}}. \quad \square \tag{15}$$

Отметим, что если параметры $\sigma_1(\chi_b\circ\varphi)$ и $\sigma_2(\chi_{-b}\circ\psi)$ вычислены или для них известны более точные оценки, чем (14) и (15), то в этих случаях предпочтительнее использовать неравенство (13).

Введем понятие, обобщающее p-адическое множество $\Gamma(R)$. Разрядным множеством кольца R называется любое его подмножество $K = \{k_0, k_1, \ldots, k_{q-1}\}$ такое,

что все его элементы попарно не сравнимы по идеалу pR (см., например, [13], [16]). Если K — разрядное множество кольца R, то каждый элемент $a \in R$ однозначно представим в виде

$$a = a_0 + pa_1 + \ldots + p^{n-1}a_{n-1}, \tag{16}$$

где $a_i \in K, i \in \overline{0, n-1}$. Равенство (16) называется разрядным представлением элемента a в множестве K, а элемент a_i, где $i \in \overline{0, n-1}$, называется i-м разрядом элемента a в множестве K. При этом элемент a_{n-1} называется старшим разрядом. Для каждого $t \in \overline{0, n-1}$ зададим разрядное отображение $\varkappa_t^K(a) = a_t$.

Рассмотрим разрядное множество $K = \{k_0, k_1, ..., k_{p-1}\}$ кольца $R = \mathbb{Z}_{p^n}$. Будем говорить, что K образует арифметическую прогрессию, если

$$K = \{a, a+d, a+2d, ..., a+(p-1)d\}$$

для некоторых элементов $a, d \in R, a \equiv 0 \,(\mathrm{mod}\, p), (d, p) = 1$. В этом случае будем использовать обозначение $K = K_{a,d}$. Важным примером разрядного множества, образующего арифметическую прогрессию, является p-ичное разрядное множество $K_{0,1} = \{0, 1, ..., p-1\}$.

Следствие 2. *Пусть $R = \mathbb{Z}_{p^n}$, $n \geqslant 2$, разрядное множество $K = K_{a,d}$ образует арифметическую прогрессию, $\psi(x) = \alpha\varkappa_{n-1}^K(x), \alpha \in P\backslash\{0\}$, тогда в условиях теоремы 1 верно неравенство*

$$\left| C_{b,\omega_1,\omega_2}(t) + \frac{p^\nu}{d}\chi_b(\varphi(\vec{0}))\right| \leqslant \sigma_1(\chi_b \circ \varphi)\left(\frac{2}{\pi}\ln(p^{n-1}) + \frac{13}{40}p + \frac{7}{20}\right)\frac{p^\nu(dp^{n-1}-1)}{d}q^{\frac{m}{2}}.$$

Доказательство. Заметим, что $\psi(0) = 0$ и верна оценка

$$\sigma_2(\chi_{-b} \circ \psi) \leqslant \frac{2}{\pi}\ln(p^{n-1}) + \frac{13}{40}p + \frac{7}{20}, \tag{17}$$

доказанная в работе [13, § 6] для случая $\alpha = 1$, но верная и для случая $\alpha \in P^*$, так как $\sigma_2(\chi_{-b} \circ \psi) = \sigma(\chi_{-b} \circ \frac{\psi}{\alpha})$, где $\frac{\psi}{\alpha}(x) = \frac{\psi(x)}{\alpha}$. $\square$

Согласно равенству (2) для всех t справедлива простая оценка $|C_{b,\omega_1,\omega_2}(t)| \leqslant T$.

Следствие 3. *Пусть*

$$T \geqslant q^{\frac{n+m+k}{2}}p^{\nu+n-1}.$$

Тогда в условиях теоремы 1 верна нетривиальная оценка $|C_{b,\omega_1,\omega_2}(t)| < T$.

Доказательство. В силу следствия 1

$$|C_{b,\omega_1,\omega_2}(t)| \leqslant \frac{p^\nu(dp^{n-1}-1)}{d}q^{\frac{m+n+k}{2}} + \frac{p^\nu}{d} < p^{\nu+n-1}q^{\frac{m+n+k}{2}},$$

т. е. при

$$T \geqslant q^{\frac{n+m+k}{2}}p^{\nu+n-1}$$

получим требуемый результат. Если $T = q^m - 1$, то последнее неравенство справедливо для всех таких m, что $m > n + k + \frac{2\nu+2n-2}{5}$.

Следствие 4. *Оценка* $|C_{b,\omega_1,\omega_2}(t)| < T$ *для некоторого класса параметров* $(\varphi, u_1, u_2, \ldots, u_k, \psi, v)$ *означает, что комбинирующие генераторы с выходной последовательностью* $\omega_1 = \varphi(u_1, u_2, \ldots, u_k)$, *совпадающей с последовательностью* $\omega_2 = \psi(v)$, *не существуют.*

Рассмотрим подробнее случай, когда $n = 1, R = P$, $\psi(x) = x$, т. е. ω_2 — ЛРП над P с характеристическим многочленом $F(x)$.

Утверждение 1. *Пусть* $x^t\omega_2$ *линейно не выражается через систему ЛРП* u_1, u_2, $\ldots$, u_k. *Тогда справедливы соотношения*

$$\left| C_b(\omega_1, \omega_2, t) + \frac{\chi_b(\varphi(\vec{0}))}{d} \right| \leqslant \sigma_1(\chi_b \circ \varphi)\frac{d-1}{d} q^{\frac{m}{2}},$$

$$\left| C_b(\omega_1, \omega_2, t) + \frac{\chi_b(\varphi(\vec{0}))}{d} \right| \leqslant \frac{d-1}{d} q^{\frac{m+k}{2}}.$$

Доказательство. Найдем точное значение $\sigma_2(\chi_{-b} \circ \psi)$:

$$\sigma_2(\chi_{-b} \circ \psi) = \sum_{r \in P} |\mu_{r,-b}|,$$

$$\mu_{r,-b} = \frac{1}{q} \sum_{s \in P} \chi_{-b}(s)\hat{\chi}(-rs).$$

Заметим, что при $n = 1$ верно равенство $\chi = \hat{\chi}$, тогда

$$\mu_{r,-b} = \frac{1}{q} \sum_{s \in P} \chi_s(-b - r) = \delta_{r,-b},$$

$$\sigma_2(\chi_{-b} \circ \psi) = 1$$

(здесь и всюду далее $\delta_{r,-b}$ — символ Кронекера), отсюда следует первое неравенство. Верно также равенство

$$\psi(0) = 0.$$

Теперь доказываемое утверждение следует из теоремы 1 и следствия 1. □

Достижимость каждой из полученных оценок устанавливает следующий практически важный результат, получающийся при $d = 1$.

Следствие 5. *Если в условиях утверждения* 1 *многочлен* $F(x)$ *имеет максимальный период* $T(F) = q^m - 1$, *то*

$$C_b(\omega_1, \omega_2, t) = -\chi_b(\varphi(\vec{0})).$$

Доказательство. Учитывая равенство $d = 1$, получим

$$\left| C_b(\omega_1, \omega_2, t) + \chi_b(\varphi(\vec{0})) \right| \leqslant 0.$$

Следовательно, знак неравенства можно заменить знаком равенства. □

Рассмотрим подробнее случай, когда $k = 1$, $\varphi(x) = x$, т. е. $\omega_1 = u_1$.

Утверждение 2. *Пусть $x^t\bar{v}$ линейно не выражается через ω_1. Тогда*

$$\left|C_{b,\omega_1,\omega_2}(t)+\frac{p^\nu}{d}\chi_b(\psi(0))\right|\leqslant\sigma_2(\chi_{-b}\circ\psi)\frac{p^\nu(dp^{n-1}-1)}{d}q^{\frac{m}{2}},$$

$$\left|C_{b,\omega_1,\omega_2}(t)+\frac{p^\nu}{d}\chi_b(\psi(0))\right|\leqslant\frac{p^\nu(dp^{n-1}-1)}{d}q^{\frac{m+n}{2}}.$$

Доказательство. Так как $W_{\chi_b\circ\varphi}(a)=\delta_{a,b}$, то равенство (11) из теоремы 1 принимает вид

$$C_{b,\omega_1,\omega_2}(t)+\frac{p^\nu}{d}\chi_b(\psi(0))=\sum_{r\in R}\mu_{r,-b}\left(\sum_{i=0}^{T-1}\hat{\chi}(u_{b,r}(i))+\frac{p^\nu}{d}\right),$$

где $u_{b,r}$ — последовательность над R с элементами

$$u_{b,r}(i)=p^{n-1}\tau(b\,\omega_1(i))+rv(i+t),\quad i\in\mathbb{N}_0.$$

По условию утверждения $x^t\bar{v}$ линейно не выражается через ω_1. Следовательно, как и в доказательстве теоремы 1, получим, что $\delta_{b,r}$ является ненулевой последовательностью при всех $r\in R$. Значит,

$$\left|C_{b,\omega_1,\omega_2}(t)+\frac{p^\nu}{d}\chi_b(\psi(0))\right|\leqslant\sigma_2(\chi_{-b}\circ\psi)\frac{p^\nu(dp^{n-1}-1)}{d}q^{\frac{m}{2}}.$$

Второе неравенство следует из первого и из соотношения (15). □

Заметим, что в условиях утверждения 2 не требуется сбалансированность отображения ψ, которая использовалась в теореме 1.

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", *Information Sciences*, **178.**:7 (2008), 1903–1916.
3. Камловский О.В., "Расстояние между двоичными представлениями линейных рекуррент над полем $GF(2^k)$ и кольцом $\mathbb{Z}_{2^n}$", *Математические вопросы криптографии*, **7**:1 (2016), 73–84.
4. Golomb S.W., Gong G., "Signal design for good correlation", 2005, 458 pp.
5. Бугров А.Д., "Кусочно-аффинные подстановки конечных полей", *Прикладная дискретная математика*, 2015, №4(30), 5–23.
6. Kuipers L., Niederreiter H., *Uniform distribution of sequences*, Wiley, New York, 1974, 390 pp.; пер. с англ.: Кейперс Л., Нидеррайтер Г., *Равномерное распределение последовательностей*, 1985, 408 с.
7. Нечаев А.А., "Цикловые типы линейных подстановок над конечными коммутативными кольцами", *Мат. сборник*, **184**:3 (1993), 21–56; англ. пер.: A. A. Nechaev, "Cycle types of linear substitutions over finite commutative rings", *Russian Acad. Sci. Sb. Math.*, **78**:2 (1994), 283–311.
8. *Словарь криптографических терминов*, Под ред. Б.А. Погорелова и В.Н. Сачкова, М.: МЦНМО, 2006, 92 с.

9. Солодовников В. И., “Бент-функции из конечной абелевой группы в конечную абелеву группу”, *Дискретная математика*, **14**:1 (2000), 99–113; англ. пер.: . Solodovnikov V. I, “Bent functions from a finite abelian group into a finite abelian group”, *Discrete Math. Appl.*, **12**:2 (2002), 111–126.
10. Нечаев А.А., “Код Кердока в циклической форме”, *Дискретная математика*, **1**:4 (1989), 123–139; англ. пер.: Nechaev A.A., “Kerdock code in a cyclic form”, *Discrete Math. Appl.*, **1**:4 (1991), 365–384.
11. О. В. Камловский, “Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа”, *Матем. сб.*, **200**:4 (2009), 31–52; англ. пер.: O. V. Kamlovskiy, “Frequency characteristics of linear recurrence sequences over Galois rings”, *Sb. Math.*, **200**:4 (2009), 499–519.
12. Глухов М.М., Елизаров В.П., Нечаев А.А., *Алгебра. Учебник в 2-х томах*, М.: Гелиос АРВ, 2003, 336 с.
13. О. В. Камловский, “Частотные характеристики разрядных последовательностей линейных рекуррент над кольцами Галуа”, *Изв. РАН. Сер. матем.*, **77**:6 (2013), 71–96; англ. пер.: Kamlovskiy O. V., “Frequency characteristics of coordinate sequences of linear recurrences over Galois rings”, *Izv. Math.*, **77**:6 (2013), 1130–1154.
14. Камловский О.В., “Количество появлений элементов в выходных последовательностях фильтрующих генераторов”, *Прикладная дискретная математика*, 2013, № 3(21), 11–25.
15. Камловский О.В., “Спектральный метод для оценки числа решений систем нелинейных уравнений с линейными рекуррентными аргументами” (в печати).
16. Кузьмин А.С., Нечаев А.А., “Линейные рекуррентные последовательности над кольцами Галуа”, *Алгебра и логика*, **34**:2 (1995), 169–189; англ. пер.: Kuzmin A.S., Nechaev A.A., “Linear recurring sequences over Galois rings”, *Algebra and Logic*, **34**:2 (1995), 87–100.

Статья поступила 02.06.2016.
Переработанный вариант поступил 12.11.2016.