ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 1**

УДК 621.391.1 : 519.7

© 2020 г. **А.Р. Васин**

КУСОЧНО-ПОЛИНОМИАЛЬНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ НАД КОЛЬЦОМ ГАЛУА

Описывается построение кусочно-полиномиального генератора над кольцом Галуа, доказывается критерий его полноцикловости. Приводится оценка отклонения выходных последовательностей рассматриваемого генератора. Показывается, что полученная оценка асимптотически эквивалентна известным оценкам для частных случаев кусочно-полиномиального генератора, а в некоторых случаях является асимптотически более точной.

Ключевые слова: кусочно-полиномиальные последовательности, кольцо Галуа, распределение элементов в последовательности, отклонение, тригонометрические суммы.

DOI: 10.31857/S0555292320010088

§ 1. Введение

В настоящее время актуальной математической задачей является задача построения псевдослучайных последовательностей (ПСП), удовлетворяющих некоторым заданным свойствам. Одним из важных свойств ПСП с практической точки зрения является “хорошее” распределение ее элементов. Для решения некоторых задач, возникающих, например, в методе Монте-Карло, имитационном моделировании и криптографии, требуются последовательности, распределение которых близко к равномерному.

Широкое распространение получили различные ПСП над кольцами Галуа, такие как, например, линейные рекуррентные последовательности (ЛРП) и последовательности, вырабатываемые полиномиальными генераторами, поскольку, во-первых, они строятся с помощью стандартных кольцевых операций и, во-вторых, являются достаточно легко реализуемыми. Существенным недостатком ЛРП является небольшая глубина линейной зависимости элементов последовательности от предыдущих, что не позволяет использовать их в чистом виде в криптографических приложениях. Последовательности, вырабатываемые полиномиальными генераторами, с другой стороны, как правило, лишены этой проблемы, поэтому представляют интересную альтернативу ЛРП.

В работе [1] была исследована цикловая структура полиномиальных генераторов над кольцами Галуа. В частности, было показано, что транзитивных полиномов (задающих полноцикловые подстановки) над кольцами Галуа R, отличными от конечных полей $GF(q)$ из q элементов и примарных колец вычетов $\mathbb{Z}_{p^n}$ по модулю p^n, не существует.

В работе [2] был предложен способ построения генератора над кольцами Галуа максимального периода $|R|$, названного инверсным, который представляет собой попеременное действие инверсной функции и некоторой подстановки на множестве

делителей нуля кольца R. Также в [2,3] исследовалась величина, называемая отклонением. В нестрогом смысле, который далее будет формализован, эта величина дает количественную оценку отклонения распределения отрезка исследуемой последовательности от равномерного распределения. В этих работах были получены оценки отклонения D_ℓ^* отрезка длины ℓ его выходных последовательностей и отклонение последовательности пар элементов на всем периоде.

В настоящей статье предлагается способ построения генератора максимального периода над произвольным кольцом Галуа R, который обобщает инверсный генератор. Этот генератор назван кусочно-полиномиальным. Как и в случае полиномиального, кусочно-полиномиальный генератор реализуется с помощью стандартных кольцевых операций, однако его преимуществом над полиномиальным является длина периода, которая равна $|R|$, тогда как для полиномиальных генераторов над кольцами Галуа, отличными от конечных полей и примарных колец вычетов, такая величина длины периода не достижима.

Так же как и инверсный, кусочно-полиномиальный генератор представляет собой попеременное действие полинома и некоторой подстановки на множестве делителей нуля кольца R. Исследуются длина периода и статистические свойства рассматриваемого генератора, доказывается критерий полноцикловости и приводится оценка отклонения D_ℓ^* отрезка длины ℓ его выходных последовательностей. Полученные новые результаты сравниваются с известными оценками отклонения для частных случаев кусочно-полиномиального генератора над различными алгебраическими структурами. В частности, если длина отрезка последовательности $\ell = O(T)$, степень многочлена $d = O(T)$ при мощности кольца $T \to \infty$, то отклонение отрезка кусочно-полиномиальной последовательности

$$D_\ell^* = O\big(d^{\frac{1}{2}}\ell^{-\frac{1}{2}}T^{\frac{1}{2}}\log T\big),$$

а при достаточно больших ℓ справедлива асимптотически более точная оценка

$$D_\ell^* = O\big(d^{\frac{1}{4}}\ell^{-\frac{1}{4}}T^{\frac{1}{4}}\log T\big).$$

Полученная асимптотика при определенных значениях соответствует аналогичной асимптотике для последовательностей, вырабатываемых полиномиальными генераторами над кольцами вычетов $\mathbb{Z}_M$ и простыми полями $GF(p)$. Также при определенных значениях оценка отклонения кусочно-полиномиальных последовательностей, полученная в данной статье, является асимптотически более точной, чем оценка отклонения кусочно-инверсных последовательностей из работы [2].

§ 2. Основные определения и обозначения

Рассмотрим кольцо Галуа $R = GR(p^{tn}, p^n)$ характеристики p^n с $p^{tn} = q^n$ элементами (см. [4,5]). Пусть R^* – множество обратимых элементов кольца R. Обозначим через ξ элемент кольца R, порождающий множество Тейхмюллера

$$\Gamma(R) = \{0, e, \xi, \xi^2, \ldots, \xi^{p^t-2}\} = \{x \in R \mid x^q = x\}.$$

Пусть

$$\Gamma(R)^* = \Gamma(R) \setminus \{0\}.$$

Произвольный элемент x кольца R можно однозначно представить в виде

$$x = x_0 + px_1 + \ldots + p^{n-1}x_{n-1}, \tag{1}$$

где $x_0, x_1, \ldots, x_{n-1} \in \Gamma(R)$. С другой стороны, рассматривая R как модуль над кольцом $\mathbb{Z}_{p^n}$ вычетов по модулю p^n, произвольный элемент y кольца R можно предста-

вить в виде

$$y = a_0 + a_1\xi + \ldots + a_{t-1}\xi^{p^t-1}, \tag{2}$$

где $a_0, \ldots, a_{t-1} \in \mathbb{Z}_{p^n}$. Рассмотрим автоморфизм Фробениуса σ, действующий на каждый элемент x, определенный равенством (1), по правилу

$$\sigma(x) = x_0^p + px_1^p + \ldots + p^{n-1}x_{n-1}^p,$$

а на многочлен $f(s) = f_0 + f_1 s + \ldots + f_d s^d \in R[s]$ – по правилу

$$\sigma(f(s)) = \sigma(f_0) + \sigma(f_1)s^p + \ldots + \sigma(f_d)s^{dp},$$

и функцию следа Tr:

$$\mathrm{Tr}(x) = \sum_{j=0}^{t-1} \sigma^j(x).$$

Здесь e – единица кольца R, а $R_0 = \{0, e, \ldots, (p^n-1)e\}$ – подкольцо кольца R, изоморфное $\mathbb{Z}_{p^n}$.

Будем говорить, что элемент $x \in R$ сравним с элементом $y \in R$ по модулю идеала p^iR, $0 \leqslant i \leqslant n$, и обозначать $x \equiv y\ (p^iR)$, если $x - y \in p^iR$.

Рассмотрим произвольный многочлен $f(s) \in R[s]$. Назовем многочлен $f(s)$ невырожденным, если $f(s) \neq \sigma(g(s)) - g(s) + \theta$ для произвольных $g(s) \in R[s]$, $\theta \in R$ (см. [6]). Используя представление (1) элементов кольца, представим $f(s)$ в следующем виде:

$$f(s) = f_0(s) + pf_1(s) + \ldots + p^{n-1}f_{n-1}(s),$$

где $f_i(s)$ – многочлен с коэффициентами из $\Gamma(R)$ для всех $0 \leqslant i \leqslant n-1$. Пусть степень каждого $f_i(s)$ равна d_i. Назовем число

$$D_f = \max\{d_0p^{n-1}, \ldots, d_{n-2}p, d_{n-1}\}$$

взвешенной степенью многочлена $f(s)$.

Пусть χ_e – канонический аддитивный характер кольца R:

$$\chi_e(x) = e^{2\pi i\frac{\mathrm{Tr}(x)}{p^n}}.$$

Произвольный аддитивный характер χ кольца R можно представить в виде $\chi(x) = \chi_e(\alpha x)$ для некоторого элемента α из R. Если $\alpha \neq 0$, то характер χ называется нетривиальным.

§ 3. Построение кусочно-полиномиальной функции над кольцом Галуа

Представим произвольный элемент x кольца R в виде $x = p^\ell\widehat{x}$, где $\widehat{x} \in R^*$, $0 \leqslant \ell \leqslant n$. Элемент кольца может быть записан в таком виде многими способами, однако в двух таких представлениях $x = p^\ell\widehat{x} = p^\ell\widetilde{x}$ элементы $\widehat{x}$ и $\widetilde{x}$ сравнимы по модулю $p^{n-\ell}R$. Для некоторого числа $d \geqslant 1$ и многочлена $F(s) = f_0 + f_1 s + \ldots + f_d s^d$ из $R[s]$, где $f_0, \ldots, f_{d-1} \in R$, $f_d \in R\backslash\{0\}$, определим функцию $\varphi_F\colon R \to R$ по правилу

$$\varphi_F(x) = \varphi_F(p^\ell\widehat{x}) = f_0 + p^\ell(f_1\widehat{x} + \ldots + f_d\widehat{x}^d).$$

Такое задание корректно, поскольку если $x = p^\ell\widehat{x} = p^\ell\widetilde{x}$, то $\widehat{x} \equiv \widetilde{x}\ (p^{n-\ell}R)$, поэтому $f_1\widehat{x} + \ldots + f_d\widehat{x}^d \equiv f_1\widetilde{x} + \ldots + f_d\widetilde{x}^d\ (p^{n-\ell}R)$, следовательно, $p^\ell(f_1\widehat{x} + \ldots + f_d\widehat{x}^d) = p^\ell(f_1\widetilde{x} + \ldots + f_d\widetilde{x}^d)$, откуда $\varphi_F(p^\ell\widehat{x}) = \varphi_F(p^\ell\widetilde{x})$.

Введем следующие обозначения: $\varphi_F^1 = \varphi_F$, $\varphi_F^{k+1} = \varphi_F^k \circ \varphi_F$, $k \geqslant 1$.

По функции φ_F определим функцию $\varphi_0 \colon GF(p^t) \to GF(p^t)$ следующим образом. Пусть $\bar{f}_0, \ldots, \bar{f}_d$ – образы элементов $f_0, \ldots, f_d$ при действии естественного эпиморфизма из R на $R/pR = GF(p^t)$. Тогда

$$\varphi_0(z) = \bar{f}_0 + \bar{f}_1 z + \ldots + \bar{f}_d z^d,$$

где сложение выполняется в $GF(p^t)$.

Пусть $\varphi_0'(z) = \bar{f}_1 + 2\bar{f}_2 z + \ldots + d\bar{f}_d z^{d-1}$ – производная многочлена φ_0 (см. [7]).

Предложение 1. *Отображение φ_F является подстановкой на R тогда и только тогда, когда выполнены условия*

$$\begin{cases} \varphi_0 \text{ – подстановка на } GF(p^t), \\ \varphi_0' \text{ не имеет ненулевых корней в } GF(p^t). \end{cases} \tag{3}$$

Доказательство. Необходимость. Поскольку φ_F инъективно, то для любых различных элементов x, y из кольца R справедливо неравенство $\varphi_F(x) \neq \varphi_F(y)$. Рассмотрим такие x, y, что $x = p^{n-1}x_0$, $y = p^{n-1}y_0$, где x_0, y_0 – произвольные элементы из $\Gamma(R)$, $x_0 \neq y_0$. Получаем, что поскольку $\varphi_F(x) \neq \varphi_F(y)$, то $p^{n-1}(f_1 x_0 + \ldots + f_d x_0^d) \neq p^{n-1}(f_1 y_0 + \ldots + f_d y_0^d)$, откуда $\overline{f_1 x_0 + \ldots + f_d x_0^d} \neq \overline{f_1 y_0 + \ldots + f_d y_0^d}$. Отсюда $\varphi_0(\bar{x}_0) \neq \varphi_0(\bar{y}_0)$ для любых $x_0, y_0 \in \Gamma(R)$. В силу произвольности выбора элементов x_0, y_0 получаем, что $\varphi_0(z_1) \neq \varphi_0(z_2)$ для любых различных $z_1, z_2 \in GF(p^t)$, следовательно, φ_0 инъективно, поэтому является подстановкой на $GF(p^t)$.

Рассмотрим элементы x, y вида $x = p^{n-2}(z + px_1)$, $y = p^{n-2}(z + py_1)$, где $x_1, y_1 \in \in \Gamma(R)$, $x_1 \neq y_1$, $z \in \Gamma(R) \setminus \{0\}$. Из условия $\varphi_F(x) \neq \varphi_F(y)$ получаем, что

$$p^{n-2}\big(f_1(z + px_1) + \ldots + f_d(z + px_1)^d\big) \neq p^{n-2}\big(f_1(z + py_1) + \ldots + f_d(z + py_1)^d\big),$$

поэтому

$$p^{n-2}\big(f_1(z + px_1) + f_2(z^2 + 2pzx_1 + p^2x_1^2) + \ldots + f_d(z^d + dpz^{d-1}x_1 + p^2 r_1)\big) \neq$$
$$\neq p^{n-2}(f_1(z + py_1) + f_2(z^2 + 2pzy_1 + p^2y_1^2) + \ldots + f_d(z^d + dpz^{d-1}y_1 + p^2 r_2))$$

для некоторых $r_1, r_2 \in R$. Отсюда следует, что

$$f_1(z + px_1) + f_2(z^2 + 2pzx_1) + \ldots + f_d(z^d + dpz^{d-1}x_1) \not\equiv$$
$$\not\equiv f_1(z + py_1) + f_2(z^2 + 2pzy_1) + \ldots + f_d(z^d + dpz^{d-1}y_1) \pmod{p^2R},$$

откуда

$$(x_1 - y_1)p(f_1 + 2f_2 z + \ldots + df_d z^{d-1}) \not\equiv 0 \pmod{p^2R},$$

следовательно, $f_1 + 2f_2 z + \ldots + df_d z^{d-1} \not\equiv 0 \pmod{pR}$, поэтому

$$\overline{f_1 + 2f_2 z + \ldots + df_d z^{d-1}} \neq 0,$$

откуда $\varphi_0'(\bar{z}) \neq 0$ для любого $z \in \Gamma(R) \setminus \{0\}$. В силу произвольности выбора элемента z получаем, что для любого элемента $z' \in GF(p^t) \setminus \{0\}$ справедливо неравенство $\varphi_0'(z') \neq 0$.

Достаточность. Покажем, что при выполнении условия (3) отображение φ_F является подстановкой на R. Для этого достаточно доказать, что для любых элементов $y_1 \neq y_2$ из R справедливо неравенство $\varphi_F(y_1) \neq \varphi_F(y_2)$. Пусть $y_1 = p^{\ell_1}x_1$, $y_2 = p^{\ell_2}x_2$, $x_i \in R^*$, $i = 1, 2$.

Рассмотрим случай, когда $\ell_1 \neq \ell_2$. Пусть, не ограничивая общности, $\ell_1 < \ell_2$. Заметим, что если $\overline{f_1 x_1 + \ldots + f_d x_1^d} = \bar{0}$, то $\varphi_0(\bar{x}_1) = \bar{f}_0 = \varphi_0(\bar{0})$, откуда $\bar{x}_1 = \bar{0}$

в силу инъективности подстановки φ_0, поэтому $x_1 \notin R^*$ – противоречие. Поэтому $\overline{f_1x_1 + \ldots + f_dx_1^d} \neq 0$. Тогда в p-адическом разложении $\varphi_F(y_2) = f_0 + p^{\ell_2}(f_1x_2 + \ldots + f_dx_2^d)$ слагаемое при p^{ℓ_1} равно p^{ℓ_1}-му разряду элемента f_0, а в p-адическом разложении $\varphi_F(y_1) = f_0 + p^{\ell_1}(f_1x_1 + \ldots + f_dx_1^d)$ слагаемое при p^{ℓ_1} не равно p^{ℓ_1}-му разряду элемента f_0, поэтому $\varphi_F(y_1) \neq \varphi_F(y_2)$.

Рассмотрим случай, когда $\ell_1 = \ell_2 = \ell$. Предположим, что $\varphi_F(y_1) = \varphi_F(y_2)$. Тогда

$$\varphi_F(y_1) - \varphi_F(y_2) = p^{\ell}\big(f_1(x_1 - x_2) + \ldots + f_d(x_1^d - x_2^d)\big) = 0.$$

Поскольку $x_1 = x_2 + p^ic$, $\bar{c} \neq \bar{0}$, $0 \leqslant i \leqslant n - \ell - 1$, получаем

$$p^{\ell}\big(f_1(x_2 - x_2 + p^ic) + f_2((x_2 + p^ic)^2 - x_2^2) + \ldots + f_d((x_2 + p^ic)^d - x_2^d)\big) = 0,$$

откуда

$$p^{\ell}\big(f_1p^ic + 2f_2x_2p^ic + (p^ic)^2 + \ldots + df_dx_2^{d-1}p^ic + \ldots\big) = 0,$$

поэтому

$$p^{\ell}\big(p^i(f_1c + 2f_2x_2c + \ldots + df_dx_2^{d-1}c) + p^{i+1}r\big) = 0,$$

где $r \in R$. Получаем, что коэффициент при $p^{\ell+i}$ равен

$$\overline{c(f_1 + 2f_2x_2 + \ldots + df_dx_2^{d-1})} = \bar{c}(\bar{f}_1 + 2\bar{f}_2\bar{x}_2 + \ldots + d\bar{f}_d\bar{x}_2^{d-1}) = \bar{c}\varphi_0'(\bar{x}_2).$$

Поскольку $\bar{c} \neq \bar{0}$, $\varphi_0'(\bar{x}_2) \neq \bar{0}$, то $\bar{c}(\bar{f}_1 + 2\bar{f}_2\bar{x}_2 + \ldots + d\bar{f}_d\bar{x}_2^{d-1}) \neq \bar{0}$ – противоречие. Таким образом, φ_F инъективно, и следовательно, является подстановкой на R. ▲

Всюду далее будем предполагать, что отображение φ_F является подстановкой на R. Рассмотрим последовательность $(z_i)_{i=0}^{\infty}$, где $z_i = \varphi_0^i(z_0)$, $i \in \mathbb{N}$, $z_0 \in GF(p^t)$. Заметим, что если φ_0 – полноцикловая подстановка на $GF(p^t)$, то последовательность $x_0 = 0$, $x_1 = \varphi_F(x_0)$, …, $x_{m+1} = \varphi_F(x_m)$, … пробегает элементы R, p-адическое разложение которых имеет вид

$$x_m = x_0^{(m)} + px_1^{(m)} + \ldots + p^{n-1}x_{n-1}^{(m)},$$

где $\bar{x}_m = \bar{x}_0^{(m)} = z_m$. Поэтому $x_0^{(m)}$ пробегает $\Gamma(R)$, когда $m = 0, 1, \ldots, p^t - 1$.

Пусть всюду далее φ_0 – полноцикловая подстановка на $GF(p^t)$. Пусть $\mathcal{B}(\varphi_F) = x_0^{(p^t-1)} + pR$. Для любого элемента $x' \in pR$ определим множество

$$\mathrm{Orb}(x') = \big\{x', \varphi_F(x'), \ldots, \varphi_F^{p^t-1}(x')\big\}.$$

Заметим, что когда i пробегает значения от 0 до $p^t - 1$, младшие разряды элементов $\varphi_F^i(x')$ пробегают множество $\Gamma(R)$. Таким образом, для любого элемента $x \in R$ существует единственный элемент $x' \in pR$, такой что $x \in \mathrm{Orb}(x')$.

О п р е д е л е н и е. Пусть φ_F – подстановка на R, соответствующая ей функция φ_0 – полноцикловая подстановка на $GF(p^t)$, x – произвольный элемент из R, и пусть $x \in \mathrm{Orb}(x')$ для некоторого $x' \in pR$. Пусть π – некоторая полноцикловая подстановка на множестве pR. Определим функцию $\Phi_{F,\pi}\colon GR(p^{tn}, p^n) \to GR(p^{tn}, p^n)$ следующим образом:

$$\Phi(x) = \Phi_{F,\pi}(x) = \begin{cases} \varphi_F(x), & \text{если } x \notin \mathcal{B}(\varphi_F), \\ \pi(x'), & \text{если } x \in \mathcal{B}(\varphi_F). \end{cases}$$

Функции $\Phi_{F,\pi}$ такого вида будем называть кусочно-полиномиальными.

П р е д л о ж е н и е 2. *Функция $\Phi_{F,\pi}$ – полноцикловая подстановка на R.*

Доказательство. Покажем, что для любых $y_1 \neq y_2$ из кольца R выполняется неравенство $\Phi(y_1) \neq \Phi(y_2)$. Пусть $y_1 \in \mathrm{Orb}(y_1')$, $y_2 \in \mathrm{Orb}(y_2')$, $y_1', y_2' \in pR$. Если $y_1, y_2 \in \mathcal{B}(\varphi_F)$, то $y_1' \neq y_2'$, поэтому $\Phi(y_1) = \pi(y_1') \neq \pi(y_2') = \Phi(y_2)$. Если $y_1 \in \mathcal{B}(\varphi_F)$, $y_2 \notin \mathcal{B}(\varphi_F)$, то $\Phi(y_2) = \varphi_F(y_2) \notin pR$, поэтому $\Phi(y_1) \neq \Phi(y_2)$, поскольку $\Phi(y_1) = \pi(y_1') \in pR$. Если $y_1, y_2 \notin \mathcal{B}(\varphi_F)$, то $\Phi(y_1) = \varphi_F(y_1) \neq \varphi_F(y_2) = \Phi(y_2)$, поскольку φ_F – подстановка. Таким образом, Φ инъективно, и следовательно, является подстановкой на R.

Полноцикловость подстановки Φ следует из того, что для каждого элемента $x' \in pR$ элементы множества $\mathrm{Orb}(x')$ лежат на одном цикле подстановки φ_F, а подстановка π является полноцикловой на множестве делителей нуля pR. ▲

Класс кусочно-полиномиальных функций не является пустым, а также нетривиально обобщает класс кусочно-инверсных функций из работы [2]. В качестве примера рассмотрим подкласс кусочно-полиномиальных функций – класс кусочно-степенных функций, задаваемых отображением $\varphi_F(p^\ell x) = ap^l x^d + b$, где $a \in R \setminus \{0\}$, $b \in R$, $d \in \mathbb{N}$. Пусть $\varphi_0(s) = \bar{a}s^d + \bar{b}$ – полноцикловый (транзитивный) многочлен над полем $GF(p^t)$. Тогда, поскольку производная $\varphi_0'(s) = d\bar{a}s^{d-1}$ может быть равна нулю только в точке $s = 0$, по предложению 1 функция φ_F является подстановкой над R, поэтому корректно задана кусочно-полиномиальная функция $\Phi_{F,\pi}$ с произвольной полноцикловой на множестве pR подстановкой π. Приведем пример таких функций.

Пример 1. Рассмотрим кольцо

$$R = GR(3^4, 3^2) = \{A\alpha + B : \ A, B \in \mathbb{Z}_9\} = \mathbb{Z}_9[\alpha]/D,$$
$$GF(3^2) = \{0, 1, \beta, \beta^2, \beta^3, 2, \beta^5, \beta^6, \beta^7\},$$

где $D \in \mathbb{Z}_9[\alpha]$ – некоторый многочлен Галуа степени 2, т.е. неприводимый по модулю 3 многочлен степени 2 из $\mathbb{Z}_9$. Положим $a = 2\alpha + r_0$, $r_0 \in pR$, $b = r_1 + r_2$, где $r_1 \in \{1, 2\alpha+1, 8, \alpha+2\}$, $r_2 \in pR$. Пусть $F(s) = as^7 + b$. Тогда $\bar{F}(s) = \varphi_0(s) = \beta^5 s^7 + b'$, где $b' \in \{1, \beta^3, 2, \beta^7\}$, и преобразование φ_0 является полноцикловой подстановкой над полем $GF(3^2)$.

Поскольку по предложению 1 преобразование φ_F является подстановкой, то корректно задана кусочно-степенная функция $\Phi_{F,\pi}$ для некоторой подстановки π, полноцикловой на множестве pR.

Заметим, что такое преобразование отлично от кусочно-инверсного, задаваемого функцией $\varphi_F(p^\ell x) = ap^\ell x^{23} + b$.

Кусочно-полиномиальные функции не ограничиваются кусочно-степенными, как показывают следующие примеры.

Пример 2. В обозначениях примера 1 рассмотрим многочлен

$$F(s) = s^5 + (8\alpha + 8)s + \alpha.$$

Тогда $\bar{F}(s) = \varphi_0(s) = s^5 + \beta^6 s + \beta$ является транзитивным многочленом над $GR(3^2)$, а производная $\varphi_0'(s) = 2s^4 + \beta^6$ не имеет корней. Поэтому по предложению 1 преобразование

$$\varphi_F(p^\ell x) = p^\ell x^5 + (8\alpha + 8)p^\ell x + \alpha$$

является подстановкой, и корректно задана кусочно-полиномиальная функция $\Phi_{F,\pi}$ для некоторой подстановки π, полноцикловой на множестве pR.

Пример 3. Рассмотрим кольцо

$$R = GR(2^6, 2^2) = \{A\alpha^2 + B\alpha + C : \ A, B, C \in \mathbb{Z}_4\} = \mathbb{Z}_4[\alpha]/D,$$
$$GF(2^3) = \{0, 1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6\},$$

где $D \in \mathbb{Z}_4[\alpha]$ – некоторый многочлен Галуа степени 3. Рассмотрим многочлен

$$F(s) = (3\alpha^2 + 2\alpha + 2)s^7 + s^6 + (\alpha + 1)s^4 + s^3 + \alpha s^2 + s + 1.$$

Тогда $\bar{F}(s) = \varphi_0(s) = \beta^2 s^7 + s^6 + \beta^3 s^4 + s^3 + \beta s^2 + s + 1$ является транзитивным многочленом над $GR(2^3)$, а производная $\varphi_0'(s) = \beta^2 s^6 + s^2 + 1$ не имеет корней. Поэтому по предложению 1 преобразование

$$\varphi_F(p^\ell x) = p^\ell\big((3\alpha^2 + 2\alpha + 2)x^7 + x^6 + (\alpha + 1)x^4 + x^3 + \alpha x^2 + x\big) + 1$$

является подстановкой, и корректно задана кусочно-полиномиальная функция $\Phi_{F,\pi}$ для некоторой подстановки π, полноцикловой на множестве pR.

§ 4. Оценка тригонометрической суммы

Пусть $\Phi = \Phi_{F,\pi}$ – произвольная кусочно-полиномиальная функция над кольцом Галуа $GR(p^{tn}, p^n)$, $T = p^{tn}$, $1 \leqslant \ell \leqslant T$. Пусть задана последовательность

$$x_0,\ x_1 = \Phi(x_0),\ \ldots,\ x_{\ell-1} = \Phi^{\ell-1}(x_0).$$

В данном параграфе приводится оценка тригонометрической суммы

$$|S_\ell(\Phi)| = \left|\sum_{m=0}^{\ell-1} \chi(x_m)\right|$$

методом, предложенным в работе [8] для оценки отклонения выходных последовательностей полиномиальных генераторов над конечными простыми полями. Над кольцами Галуа он был впервые применен в работах [2, 3] для получения оценок отклонения выходных последовательностей инверсных генераторов над кольцами Галуа, а в работе [9] – для получения оценок отклонения линейных рекуррентных последовательностей над кольцами Галуа.

Нам понадобится следующая

Лемма 1 [6, теорема 2]. *Пусть $f(s) \in R[s]$ – невырожденный многочлен со взвешенной степенью D_f. Тогда для нетривиального аддитивного характера χ справедливо неравенство*

$$\left|\sum_{x \in \Gamma(R)} \chi(f(x))\right| \leqslant (D_f - 1)\sqrt{p^t}.$$

Лемма 2. *Пусть $\Phi = \Phi_{F,\pi}$ – произвольная кусочно-полиномиальная функция над кольцом Галуа $GR(p^{tn}, p^n)$, $d = \deg F(s)$, $T = p^{tn}$. Пусть задана последовательность x_0, $x_1 = \Phi(x_0)$, $\ldots$, $x_{\ell-1} = \Phi(x_{\ell-2})$, $1 \leqslant \ell \leqslant T$. Тогда если $F(s) \neq s + a$, $a \in R$, $d \geqslant 3p^{\frac{t}{2}-n-1}$, $(d, p) = 1$, то*

$$|S_\ell(\Phi)| = \left|\sum_{m=0}^{\ell-1} \chi(x_m)\right| <$$
$$< \ell^{1/2}\left(\sqrt{\frac{4}{3}\ell p^{t(n-1)}K} + p^{t(n-1)}\left(\frac{2K}{3} - p^{t/2} + 2\right)\right)^{1/2} + \sqrt{\frac{3\ell}{4p^{t(n-1)}K}} + \frac{1}{2},$$

где $K = dp^{n+\frac{t}{2}-1} + 2$.

Доказательство. Для любого целого k справедливо

$$\left|S_\ell(\Phi) - \sum_{m=0}^{\ell-1} \chi(x_{m+k})\right| \leqslant 2|k|. \tag{4}$$

Для натурального числа Q определим множество $C(Q) = \left\{k \in \mathbb{Z} \,\middle|\, -\frac{Q}{2} < k \leqslant \frac{Q}{2}\right\}$. Тогда

$$\sum_{k\in C(Q)} |k| \leqslant \frac{Q^2}{4}.$$

Суммируя неравенство (4) по всем $k \in C(Q)$, получаем

$$Q|S_\ell(\Phi)| \leqslant V + \frac{Q^2}{2}, \tag{5}$$

где

$$V = \left|\sum_{m=0}^{\ell-1} \sum_{k\in C(Q)} \chi(x_{m+k})\right| \leqslant \sum_{m=0}^{\ell-1} \left|\sum_{k\in C(Q)} \chi(\Phi^k(x_m))\right|.$$

Из неравенства Коши – Буняковского – Шварца следует, что

$$\begin{aligned}
V^2 &\leqslant \ell \sum_{m=0}^{\ell-1} \left|\sum_{k\in C(Q)} \chi(\Phi^k(x_m))\right|^2 \leqslant \ell \sum_{m=0}^{T-1} \left|\sum_{k\in C(Q)} \chi(\Phi^k(x_m))\right|^2 = \\
&= \ell \sum_{m=0}^{T-1} \sum_{k_1,k_2\in C(Q)} \chi\big(\Phi^{k_1}(x_m) - \Phi^{k_2}(x_m)\big) = \ell \sum_{k_1,k_2} \sum_{m=0}^{T-1} \chi\big(\Phi^{k_1}(x_m) - \Phi^{k_2}(x_m)\big) = \\
&= \ell \sum_{k_1,k_2} \sum_{x\in R} \chi\big(\Phi^{k_1}(x) - \Phi^{k_2}(x)\big) = Q\ell^2 + \ell \sum_{k_1\neq k_2} \sum_{x\in R} \chi\big(\Phi^{k_1}(x) - \Phi^{k_2}(x)\big) \leqslant \\
&\leqslant Q\ell^2 + 2\ell \sum_{k_2<k_1} \left|\sum_{x\in R} \chi(\Phi^{k_1-k_2}(x) - x)\right|.
\end{aligned}$$

Получаем

$$V^2 \leqslant Q\ell^2 + 2\ell \sum_{k=1}^{Q-1} (Q-k) \left|\sum_{x\in R} \chi(\Phi^k(x) - x)\right|. \tag{6}$$

Положим $Q = \left[\sqrt{\frac{3\ell}{p^{t(n-1)}K}}\right] + 1$. Такое Q удовлетворяет условиям $1 \leqslant Q \leqslant T$ при $1 \leqslant \ell \leqslant T$. Из условия $d \geqslant 3p^{\frac{t}{2}-n-1}$ следует, что $K > 3p^{t-2}$, поэтому

$$\frac{1}{3}p^{t(n-1)+2}K > p^{tn}.$$

Поскольку $\ell \leqslant p^{tn}$, получаем

$$\ell < \frac{1}{3}p^{t(n-1)+2}K,$$

откуда

$$\frac{3\ell}{p^{t(n-1)}K} < p^2,$$

поэтому $Q - 1 < p$. Заметим, что

$$\left|\sum_{x\in R}\chi(\Phi^k(x)-x) - \sum_{x\in R}\chi(\varphi_F^k(x)-x)\right| \leqslant 2p^{t(n-1)}k,$$

поэтому

$$\left|\sum_{x\in R}\chi(\Phi^k(x)-x)\right| \leqslant \left|\sum_{x\in R}\chi(\varphi_F^k(x)-x)\right| + 2p^{t(n-1)}k.$$

Оценим величину $\left|\sum\limits_{x\in R}\chi(\varphi_F^k(x)-x)\right|$. Пусть $F_1(s) = F(s)$, $F_k(s) = F(F_{k-1}(s))$, $k \geqslant 2$. Представив произвольный элемент x как $x_0 + c$, где $x_0 \in \Gamma(R)$, $c \in pR$, получаем

$$\left|\sum_{x\in R}\chi(\varphi_F^k(x)-x)\right| = \left|\sum_{c\in pR}\sum_{x_0\in\Gamma(R)}\chi\big(\varphi_F^k(x_0+c)-(x_0+c)\big)\right| =$$
$$= \left|\sum_{c\in pR}\left[\chi\big(\varphi_F^k(c)-c\big) + \sum_{x_0\in\Gamma(R)^*}\chi\big(F_k(x_0+c)-(x_0+c)\big)\right]\right| =$$
$$= \left|\sum_{c\in pR}\left[\chi\big(\varphi_F^k(c)-c\big) - \chi(F_k(c)-c) + \sum_{x_0\in\Gamma(R)}\chi\big(F_k(x_0+c)-(x_0+c)\big)\right]\right| \leqslant$$
$$\leqslant \sum_{c\in pR}\left[\left|\sum_{x_0\in\Gamma(R)}\chi\big(F_k(x_0+c)-(x_0+c)\big)\right| + 2\right].$$

Для элемента c из pR определим многочлен $G_{k,c}(s) = F_k(s+c) - (s+c)$. Если $d = k = 1$, то поскольку $F(s) \neq s + a$, $a \in R$, степень многочлена $G_{k,c}$ равна 1, поэтому многочлен $G_{k,c}$ невырожден. Если d и k одновременно не равны 1, то степень многочлена $G_{k,c}$ равна dk. Поскольку $(d, p) = 1$, $k \leqslant Q - 1 < p$, получаем, что $(\deg G_{k,c}, p) = 1$. Заметим, что если многочлен $g(s)$ вырожденный, то $g(s) = \sigma(h(s)) - h(s) + \theta$ для некоторых $h(s) \in R[s]$, $\theta \in R$. Пусть $h(s) = h_0 + h_1 s + \ldots + h_u s^u$. Тогда $\sigma(h(s)) = \sigma(h_0) + \sigma(h_1)s^p + \ldots + \sigma(h_u)s^{pu}$, поэтому либо $g(s)$ – константа, либо $\deg g(s) = pu$, откуда $(\deg g, p) = p$. Так как $(\deg G_{k,c}, p) = 1$, получаем, что многочлен $G_{k,c}$ невырожден. Применяя лемму 1 и учитывая, что взвешенная степень $D_{G_{k,c}} \leqslant p^{n-1}dk$, получаем

$$\left|\sum_{x\in R}\chi(\varphi_F^k(x)-x)\right| \leqslant \sum_{c\in pR}\Big[(p^{n-1}kd-1)p^{t/2}+2\Big] = p^{t(n-1)}((p^{n-1}kd-1)p^{t/2}+2),$$

поэтому

$$\left|\sum_{x\in R}\chi(\Phi^k(x)-x)\right| \leqslant p^{t(n-1)}((p^{n-1}kd-1)p^{t/2}+2) + 2p^{t(n-1)}k =$$
$$= p^{t(n-1)}((p^{n-1}kd-1)p^{t/2}+2k+2).$$

Из (6) получаем

$$V^2 \leqslant Q\ell^2 + 2\ell \sum_{k=1}^{Q-1}(Q-k)p^{t(n-1)}(kK - p^{t/2} + 2) =$$

$$= Q\ell^2 + 2\ell p^{t(n-1)} \left(Q \sum_{k=1}^{Q-1}(kK - (p^{t/2}-2)) - \sum_{k=1}^{Q-1}(k^2K - k(p^{t/2}-2)) \right) =$$

$$= Q\ell^2 + 2\ell p^{t(n-1)} \Bigg(Q^2(Q-1)\frac{K}{2} - Q(Q-1)(p^{t/2}-2) -$$

$$- K\frac{(Q-1)Q(2Q-1)}{6} + \frac{Q(Q-1)}{2}(p^{t/2}-2) \Bigg) =$$

$$= Q\ell^2 + 2\ell p^{t(n-1)} Q(Q-1) \left(K\frac{Q+1}{6} - \frac{p^{t/2}-2}{2} \right) <$$

$$< Q\ell^2 + 2\ell p^{t(n-1)} Q^2 \left(K\frac{Q+1}{6} - \frac{p^{t/2}-2}{2} \right) =$$

$$= Q^2\ell \left(\ell Q^{-1} + p^{t(n-1)} \left(K\frac{Q+1}{3} - p^{t/2} + 2 \right) \right).$$

Подставляя $Q = \left[\sqrt{\dfrac{3\ell}{p^{t(n-1)}K}} \right] + 1$ в неравенство (5), получаем

$$|S_\ell(\Phi)| < \ell^{1/2} \Bigg(\frac{\ell}{\left[\sqrt{\dfrac{3\ell}{p^{t(n-1)}K}} \right] + 1} + \left(\left[\sqrt{\frac{3\ell}{p^{t(n-1)}K}} \right] + 1 \right) \frac{p^{t(n-1)}K}{3} +$$

$$+ p^{t(n-1)} \left(\frac{K}{3} - p^{t/2} + 2 \right) \Bigg)^{1/2} + \frac{\left[\sqrt{\dfrac{3\ell}{p^{t(n-1)}K}} \right] + 1}{2} <$$

$$< \ell^{1/2} \Bigg(\ell \sqrt{\frac{p^{t(n-1)}K}{3\ell}} + \sqrt{\frac{3\ell}{p^{t(n-1)}K}} \cdot \frac{p^{t(n-1)}K}{3} +$$

$$+ p^{t(n-1)} \left(\frac{2K}{3} - p^{t/2} + 2 \right) \Bigg)^{1/2} + \frac{\sqrt{\dfrac{3\ell}{p^{t(n-1)}K}} + 1}{2} =$$

$$= \ell^{1/2} \left(\sqrt{\frac{4}{3}\ell p^{t(n-1)}K} + p^{t(n-1)} \left(\frac{2K}{3} - p^{t/2} + 2 \right) \right)^{1/2} + \sqrt{\frac{3\ell}{4p^{t(n-1)}K}} + \frac{1}{2}. \quad \blacktriangle$$

Замечание 1. Условия $F(s) \neq s + a$, $a \in R$, $\deg F(s) \geqslant 3p^{\frac{t}{2}-n-1}$, $(\deg F(s), p) = 1$ на многочлен $F(x)$ в кусочно-полиномиальной функции $\Phi_{F,\pi}$ из леммы 2 не являются вырожденными. Они выполняются, например, для многочленов из примеров 1–3.

§ 5. Оценка отклонения

Для определения того, насколько распределение последовательности близко к равномерному, вычисляется величина, которая называется отклонением (статистикой Колмогорова).

Введем обозначение $I = [0,1)$ и зафиксируем некоторое натуральное число ℓ. Отклонением D_ℓ^* (см. [10, определение 1.2]) последовательности $x_0, \ldots, x_{\ell-1}$ чисел из I называется величина

$$D_\ell^* = D_\ell^*(x_0, \ldots, x_{\ell-1}) = \sup_{0<\alpha\leqslant 1} \left| \frac{A([0,\alpha),\ell)}{\ell} - \alpha \right|,$$

где $A([0,\alpha),\ell)$ – число элементов последовательности $x_0, \ldots, x_{\ell-1}$, попадающих в полуинтервал $[0,\alpha)$.

Заметим, что величина D_ℓ^* определяет отклонение реального распределения элементов последовательности от "идеального" равномерного распределения.

Для произвольного элемента x кольца R вида (2) определим нормализующее отображение $\eta\colon R \to [0,1)$ следующим образом:

$$\eta(x) = \frac{(a_0 + a_1 p^n + \ldots + a_{t-1} p^{n(t-1)})}{p^{tn}},$$

где $a_i \in \mathbb{Z}_{p^n}$.

Нам понадобится следующая

Лемма 3 [9, утверждение 1]. *Пусть P – множество, состоящее из чисел $y_0, \ldots, y_{\ell-1}$, $y_i = \eta(x_i)$, $0 \leqslant i \leqslant \ell-1$, а $x_0, \ldots, x_{\ell-1}$ – последовательность элементов кольца $R = GR(p^{tn}, p^n)$. Тогда, если*

$$\left| \sum_{i=0}^{\ell-1} \chi(x_i) \right| \leqslant B,$$

где χ – произвольный нетривиальный аддитивный характер кольца R, а B – некоторое действительное число, не зависящее от характера χ, то

$$D_\ell^*(P) < \frac{1}{p^{tn}} + \frac{B}{\ell}\left(t\left(\frac{4}{\pi^2} n \ln p + \frac{9}{5} - \frac{1}{p^n} \right) + \frac{1-p^n}{p^n} \right).$$

Пусть задана произвольная кусочно-полиномиальная функция $\Phi_{F,\pi}$ над кольцом Галуа $R = GR(p^{tn}, p^n)$. Последовательность $(x_i)_{i=0}^\infty$ будем называть кусочно-полиномиальной последовательностью с порождающей функцией $\Phi_{F,\pi}$, если $x_i = \Phi_{F,\pi}(x_{i-1})$, $i \geqslant 1$. Пусть $y_i = \eta(x_i)$, $i \in \mathbb{N}_0$. Последовательность $(y_i)_{i=0}^\infty$ будем называть последовательностью чисел в полуинтервале $[0,1)$, порожденной кусочно-полиномиальной последовательностью над кольцом Галуа.

Теорема. *Пусть $\Phi = \Phi_{F,\pi}$ – произвольная кусочно-полиномиальная функция над кольцом Галуа R, $T = p^{tn}$. Пусть также имеется многочлен $F(s) \neq s + a$, $a \in R$, $d = \deg F(s) \geqslant 3p^{\frac{t}{2}-n-1}$, $(d,p) = 1$. Пусть P – последовательность чисел*

$$y_i, \quad 0 \leqslant i \leqslant \ell - 1,$$

в полуинтервале $[0,1)$, порожденная кусочно-полиномиальной последовательностью над кольцом Галуа с порождающей функцией Φ. Тогда для чисел ℓ, удовлетворяющих неравенству $1 \leqslant \ell \leqslant T$, справедлива оценка

$$D_\ell^*(P) < \frac{1}{p^{tn}} + C_2\left(\left(\left(\frac{4C_1}{3\ell} \right)^{1/2} + \frac{2C_1}{3\ell} - \frac{p^{t(n-1)}(p^{t/2}-2)}{\ell} \right)^{1/2} + \left(\frac{3}{4\ell C_1} \right)^{1/2} + \frac{1}{2\ell} \right),$$

где $C_1 = p^{t(n-1)}\left(dp^{n+\frac{t}{2}-1} + 2\right)$, $C_2 = t\left(\frac{4}{\pi^2} n \ln p + \frac{9}{5} - \frac{1}{p^n}\right) - \frac{p^n - 1}{p^n}$.

Доказательство. Теорема непосредственно следует из лемм 2 и 3. ▲

Замечание 2. Условия $F(s) \neq s + a$, $a \in R$, $\deg F(s) \geqslant 3p^{\frac{t}{2}-n-1}$, $(\deg F(s), p) = 1$ на многочлен $F(x)$ в кусочно-полиномиальной функции $\Phi_{F,\pi}$ из теоремы не являются вырожденными. Они выполняются, например, для многочленов из примеров 1–3.

Из теоремы следует, что если $\ell = O(T)$, $d = O(T)$ при $T \to \infty$, то

$$D_\ell^* = O\big(d^{\frac{1}{2}}\ell^{-\frac{1}{2}}T^{\frac{1}{2}}\log T\big),$$

а при достаточно больших ℓ, т.е. когда $\ell \geqslant \dfrac{4}{3}C_1$, справедлива асимптотически более точная оценка

$$D_\ell^* = O\big(d^{\frac{1}{4}}\ell^{-\frac{1}{4}}T^{\frac{1}{4}}\log T\big).$$

Отметим, что подобная асимптотика корректна, поскольку существует бесконечная последовательность многочленов возрастающих степеней, удовлетворяющих условиям теоремы. В эту последовательность входят, по крайней мере, многочлены, задающие кусочно-инверсные функции, т.е. многочлены $F(s) = as^{\exp R-1} + b$, $a \in R \setminus \{0\}$, $b \in R$, $\exp R$ – экспонента кольца R, для которых $F(s)$ является полноцикловым над полем (условие на производную при этом также выполняется). Согласно [11] такие многочлены существуют.

В работах [2, 3] для частного случая кусочно-инверсных последовательностей, когда $\varphi_F(p^\ell x) = ap^\ell x^{-1} + b$, $a, b \in \Gamma(R)$, была получена оценка отклонения $D_\ell^* = O(\ell^{-1/2}T^{1/2}\log T)$. Пусть $d = o(1)$ при $T \to \infty$. Тогда оценки являются асимптотически эквивалентными, а при $\dfrac{4}{3}C_1 \leqslant \ell < T$ оценка из теоремы является асимптотически более точной. Для колец вычетов $\mathbb{Z}_M$ с уточнением для простых полей $GF(p)$ известна следующая оценка отклонения выходных последовательностей полиномиальных генераторов (см. [12, теорема 11; 13, теорема 4.1; 14, теорема 2]): пусть $\ell = O(M)$, $M \to \infty$, тогда для любого натурального числа r

$$D_\ell^* = O\big(\ell^{-\frac{1}{2r}}M^{\frac{1}{2r}}(\log M)^{-\frac{1}{2}}\log\log M\big),$$

где константа зависит лишь от степени многочлена и числа r. Эта оценка является асимптотически более точной, чем оценка из теоремы, если $r \geqslant 2$.

СПИСОК ЛИТЕРАТУРЫ

1. *Ермилов Д.М., Козлитин О.А.* Цикловая структура полиномиального генератора над кольцом Галуа // Матем. вопр. криптогр. 2013. Т. 4. № 1. С. 27–57.
2. *Solé P., Zinoviev D.* Inversive Pseudorandom Numbers over Galois Rings // European J. Combin. 2009. V. 30. № 2. P. 458–467.
3. *Вернигора Е.В.* Инверсный конгруентный генератор над кольцом Галуа характеристики p^l // Укр. матем. вісник. 2011. Т. 8. № 4. С. 607–618.
4. *Нечаев А.А.* Код Кердока в циклической форме // Дискрет. матем. 1989. Т. 1. № 4. С. 123–139.
5. *McDonald B.R.* Finite Rings with Identity. New York: M. Dekker, 1974.
6. *Helleseth T., Kumar P.V., Shanbhag A.G.* Exponential Sums over Galois Rings and Their Applications // Finite Fields and Applications (Proc. 3rd Int. Conf. Glasgow, Scotland. July 11–14, 1995). Lond. Math. Soc. Lecture Notes Ser. V. 233. Cambridge: Cambridge Univ. Press, 1996. P. 109–128.
7. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра. Т. 1. М.: Гелиос АРВ, 2003.
8. *Niederreiter H., Shparlinski I.E.* On the Distribution and Lattice Structure of Nonlinear Congruential Pseudorandom Numbers // Finite Fields Appl. 1999. V. 5. № 3. P. 246–253.

9. *Васин А.Р.* Оценки отклонения линейных рекуррентных последовательностей над кольцами Галуа // Дискрет. матем. 2019. Т. 31. № 3. С. 17–25.
10. *Кейперс Л., Нидеррейтер Г.* Равномерное распределение последовательностей. М.: Наука, 1985.
11. *Chou W.-S.* The Period Lengths of Inversive Pseudorandom Vector Generations // Finite Fields Appl. 1995. V. 1. № 1. P. 126–132.
12. *El-Mahassni E.* Exponential Sums for Nonlinear Recurring Sequences in Residue Rings // Albanian J. Math. 2010. V. 4. № 1. P. 3–13.
13. *Topuzoğlu A., Winterhof A.* Pseudorandom Sequences // Topics in Geometry, Coding Theory and Cryptography. Dordrecht: Springer, 2007. P. 135–166.
14. *Niederreiter H., Winterhof A.* Exponential Sums for Nonlinear Recurring Sequences // Finite Fields Appl. 2008. V. 14. № 1. P. 59–64.

Васин Антон Романович
ООО "Центр сертификационных исследований", Москва
vasinantr@yandex.ru

Поступила в редакцию
21.07.2019
После доработки
05.02.2020
Принята к публикации
07.02.2020