Український математичний вісник
Том 8 **(2011)**, № 4, 607 – 618

Инверсный конгруентный генератор над кольцом Галуа характеристики p^l

Елена В. Вернигора

(*Представлена И. В. Протасовым*)

Аннотация. Рассматривается конструкция инверсного конгруентного генератора над кольцом Галуа нечетной характеристики p^l, которая была предложена Соле и Зиновьевым для $p = 2$. С помощью оценок тригонометрических сумм на последовательностях псевдослучайных чисел получена оценка дискрипантной функции, порождаемой последовательности псевдослучайных чисел и ассоциированной с ней последовательности двумерных "перекрывающихся" точек.

2010 MSC. 11K45.

Ключевые слова и фразы. Дискрипанция, псевдослучайные числа, конгруентный генератор, кольца Галуа.

Введение

Последовательности псевдослучайных чисел широко применяются в задачах имитирования случайных процессов, а также при использовании метода Монте Карло для вычисления интегралов. В последние годы псевдослучайные числа используются в криптографии. Среди нелинейных конгруентных генераторов, порождающих непредсказуемые последовательности псевдослучайных чисел, наиболее хорошо изученными являются инверсные конгруентные генераторы (см. [2–4])

$$y_{n+1} = ay_n^{-1} + b, \quad n = 0, 1, \ldots,$$

где параметры a, b и инициальное значение y_0 берутся из конечного поля F_q, причем y_n^{-1} есть обратное к y_n в поле F_q, если $y_n \neq 0$, а для $y_n = 0$ берем (условно) $y_n^{-1} = 0$.

Статья поступила в редакцию 25.07.2011

В работе P. Sole и D. Zinoviev [8] рассматривается обобщение инверсного конгруентного генератора на случай кольца Галуа $R(l,m)$ характеристики 2^l. Этими авторами предложена конструкция генератора над $R(l,m)$, порождающего последовательность псевдослучайных чисел отрезка $[0,1)$.

В настоящей работе мы рассматриваем инверсный конгруентный генератор над кольцом Галуа характеристики p^l, где $p>2$ — простое число, и показываем, что соответствующая последовательность псевдослучайных чисел проходит двумерный сериальный тест на статистическую независимость (непредсказуемость).

На протяжении всей статьи мы используем следующие обозначения:

p всегда обозначает простое число больше 2;

$e_q(x) := e^{2\pi i\frac{x}{q}}$ для натурального q и вещественного x;

Z_q — кольцо классов вычетов по модулю q;

F_q — поле из q элементов.

1. Основные определения и вспомогательные утверждения

Пусть $g(x)$ — фундаментально примитивный многочлен степени m из кольца $Z_{p^l}[x]$, то есть старший коэффициент $g(x)$ равен 1 и многочлен $\tilde{g}(x)$, получаемый из $g(x)$ заменой его коэффициентов $a_i \in Z_{p^l}$ вычетами по модулю p, является примитивным многочленом степени m над полем Z_p. Через $R(l,m)$ мы обозначим фактор-кольцо $Z_{p^l}[x]/(g(x))$. Ясно, что $R(l,m)$ — это кольцо Галуа характеристики p^l. Пусть ξ — примитивный элемент в $R(l,m)$, который порождает тейхмюллерово множество $\Xi \subset R(l,m)$, $\Xi = \left\{0,1,\xi,\ldots,\xi^{p^m-2}\right\}$, так что каждое $x \in R(l,m)$ допускает p-адическое представление (разложение).

$$\begin{gathered} x = x^{(0)} + px^{(1)} + p^2x^{(2)} + \cdots + p^{l-1}x^{(l-1)}, \\ x^{(i)} \in \Xi,\ i = 0,\ldots,l-1. \end{gathered} \tag{1.1}$$

Для x, представленного в форме (1.1), задаем автоморфизм Фробениуса

$$F(x) = (x^{(0)})^p + p(x^{(1)})^p + \cdots + p^{l-1}(x^{(l-1)})^p \in R(l,m).$$

Обозначим $Tr(x) = \sum_{j=0}^{m-1} F^j(x)$, где $F^j(x) = F(F^{j-1}(x))$. Очевидно, $Tr(x) \in Z_{p^l}$.

Поскольку каждое $x^{(i)} \in \Xi$ допускает единственное представление через базис $1, \xi, \xi^2, \ldots, \xi^{m-1}$, то из (1.1) получаем альтернативное представление

$$x = a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1}, \quad a_i \in Z_{p^l}. \tag{1.2}$$

Обозначим:

$$R_s(l,m) = \left\{ x \in R(l,m) |\ \ x^{(0)}, \ldots, x^{(s-1)} = 0; x^{(s)} \neq 0 \right\} \tag{1.3}$$

$$R_*(l,m) = \left\{ x \in R(l,m) |\ \ x^{(0)} \neq 0 \right\}. \tag{1.4}$$

Следовательно,

$$R_s(l,m) = p^s R_*(l,m).$$

Ясно, что

$$R(l,m) = \bigcup_{s=0}^{l} R_s(l,m).$$

Обозначим:

$$B_s(x) = x + R_s(l,m) = \{x + y |\ y \in R_s(l,m)\}; \quad B_1(x) := B(x).$$

Очевидно, $B_s(x+y) = B_s(x)$ для $\forall\, y \in R_s(l,m)$. Кроме того, имеем дизъюнктивное разложение

$$R(l,m) = \bigcup_{x \in \Xi} B(x).$$

Для $x \in R(l,m)$ обозначим $\bar{x} \in \Xi$ такое, что $x \equiv \bar{x} (mod\ p)$, то есть $\bar{x} = x^{(0)}$ (см. (1.1)).

Покажем, что каждое $x \in R_*(l,m)$ обратимо в $R(l,m)$. Действительно, если $x = x^{(0)} + px^{(1)} + \cdots + p^{l-1}x^{(l-1)}$, то

$$x^{-1} = y = y^{(0)} + py^{(1)} + \cdots + p^{l-1}y^{(l-1)},$$

где

$$\begin{gathered} y_0 = \begin{cases} 1, & \text{если } x^{(0)} = 1 \\ \xi^{k_0}, & \text{если } x^{(0)} = \xi^{p^m - 1 - k_0}, \end{cases} \\ y_1 = -x_1^{(1)} y_0^2 = \xi^{\frac{1}{2}(p^m-1)} x_1^{(1)} y_0^2, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ y_j = -y_0^{(0)}(x^{(j)}y^{(0)} + x^{(j-1)}y^{(1)} + \cdots + x^{(1)}y^{(j-1)}), \\ j = 1, 2, \ldots, l-1. \end{gathered} \tag{1.5}$$

Рассмотрим отображение $R(l,m)$ в F_{p^m}, которое получается из представления (1.2) заменой коэффициентов a_i их вычетами по mod p и отождествлением ξ с примитивным элементом поля F_{p^m}:

$$R(l,m) \ni \overline{x} = \overline{a}_0 + \overline{a}_1\xi + \cdots + \overline{a}_{m-1}\xi^{m-1} \in F_{p^m},$$

где $\overline{a}_i \equiv a_i (mod\ p),\ 0 \le a_i < p$.

Обобщим определение обратимости на случай $x \in R_s(l,m)$. Пусть $x = p^s y, y \in R_*(l,m)$, тогда обобщенное обратное определяется так: $x^{-1}_{\text{об.}} = p^s y^{-1}$, где y^{-1} определено выше для $y \in R_*(l,m)$.

Над полем F_{p^m} определим отображение $\varphi_0 : F_{p^m} \to F_{p^m}$

$$\varphi_0(t) = \begin{cases} a_0 t^{-1} + b_0, & \text{если } t \neq 0, \\ b_0, & \text{если } t = 0; \end{cases} \tag{1.6}$$

(здесь a_0, b_0 — фиксированные из F_{p^m}). Рассмотрим рекурсию: $t_{n+1} = a_0\varphi_0(t_n) + b_0,\ n = 0,1,\ldots,\ (a_0, b_0, t_0 \in F_{p^m})$.

Таким образом, мы имеем последовательность $t_0, t_1, \ldots$. Эта последовательность вполне определяется однозначно параметрами $a_0, b_0, t_0 \in F_{p^m}$.

Известно (см., например, [1, 4, 7]), что существует непустое множество M_{p^m} наборов $(a_0, b_0) \in F^2_{p^m}$ таких, что наименьший период последовательности $\{t_n\}$ равен p^m, т.е. элементы $t_0, t_1, \ldots$ пробегают все поле F_{p^m}, а потому t_0 можно брать равным 0.

Определим функцию $\varphi : R(l,m) \to R(l,m)$. Зафиксируем $a, b \in \left\{1, \xi, \ldots, \xi^{p^m-2}\right\} = \Xi \setminus \{0\} := \Xi_*$.

$$\varphi(x) = \begin{cases} b & \text{если } x = 0, \\ p^s a x_*^{-1} + b, & \text{если } x = p^s x_*,\ x_* = R_*(l,m). \end{cases} \tag{1.7}$$

В дальнейшем мы будем считать, что для $a, b \in \Xi_*$ имеем $\overline{a} = a_0,\ \overline{b} = b_0,\ (a_0, b_0) \in M_{p^m}$. Тогда последовательность $x_0, x_1, \ldots$, определяемая как $x_0 = 0, x_{n+1} = \varphi(x_n),\ n = 0, 1, \ldots$, имеет -адическое представление

$$x_n = x_n^{(0)} + p x_n^{(1)} + \cdots + p^{l-1} x_n^{(l-1)}, \quad \overline{x}_n = x_n^{(0)} = t_n. \tag{1.8}$$

Учитывая длину периода этой последовательности $\tau = p^m$, получаем, что $x_n^{(0)}$ пробегает всё $\Xi = F_{p^m}$, а потому имеем

$$R(l,m) = \bigcup_{n=0}^{p^m-1} (x_n^{(0)} + pR(l,m)) = \bigcup_{n=0}^{p^m-1} B(x_n^{(0)}).$$

Обозначим $B = B(x^{(0)}_{p^m-1})$. Для $x \in R(l,m)$ определяем множество:

$$Orb(x) := \left\{x, \varphi(x), \ldots, \varphi^{p^m-1}(x)\right\}, \quad \varphi^k(x) = \varphi(\varphi^{k-1}(x)).$$

Мы также имеем

$$R(l,m) = \bigcup_{x \in pR(l,m)} Orb(x).$$

Следовательно, для каждого $x \in R(l,m)$ найдётся $x' \in pR_*(l,m)$ такое, что $x \in Orb(x')$.

Зафиксируем некоторую транзитивную подстановку на множестве $pR(l,m)$. Число элементов в $pR(l,m)$ равно $p^{m(l-1)}$.

Определим функцию $\Phi : R(l,m) \to R(l,m)$ так:

$$\Phi(x) = \begin{cases} \varphi(x), & \text{если } x \notin B, \\ \pi(x'), & \text{если } x \in B \text{ и } x \in Orb(x'). \end{cases} \tag{1.9}$$

Это определение корректно, так как $x' \in pR$ определено однозначно для каждого $x \in R(l,m)$.

Заметим, что функция Φ определяет взаимно однозначное отображение, так как если $y = \Phi(x)$, то

$$x = \begin{cases} \Phi^{-1}(y) = a(y-b)^{-1}, & \text{если } y \neq b, \\ 0 = \Phi^{-1}(b), & \text{если } y = b. \end{cases} \tag{1.10}$$

Таким образом, Φ действует как транзитивная подстановка на кольце R. Случай $p = 2$ исследован в [8], случай произвольного простого рассматривается аналогично.

Пусть теперь $f(x) \in R(l,m)[x]$. Представим $f(x)$ в виде

$$f(x) = F_0(x) + pF_1(x) + \cdots + p^{l-1}F_{l-1}(x), \quad F_j(x) \in \Xi[x].$$

Пусть $D_f = \max[d_0 p^{l-1}, \ldots, d_{l-2}p, d_{l-1}]$, $d_j =$ степень $F_j(x)$. Тогда справедливы утверждения.

Лемма 1.1. *Пусть f — невырожденный многочлен над $R(l,m)$. Тогда для $(c,p) = 1$ имеем:*

$$\left| \sum_{x \in \Xi} e_{p^l}(c \cdot Tr(f(x))) \right| \leq (D_f - 1)p^{\frac{m}{2}}.$$

Доказательство см. [6, теор. 1]

Лемма 1.2. *Пусть $f_1(x), f_2(x) \in R(l,m)[x]$, причем f_1, f_2 одновременно невырождены. Тогда для $(c_1, c_2, p) = 1$ имеем*

$$\left| \sum_{x \in \Xi_*} e_{p^l}(c_1 Tr(f_1(x)) + c_2 Tr(f_2(x^{-1}))) \right| \leq (D_{f_1} + D_{f_2})p^{\frac{m}{2}}.$$

Доказательство см. [5].

2. Тригонометрические суммы на последовательности псевдослучайных чисел

Рассмотрим последовательность x_n элементов из $R(l,m)$, определенную рекурсией

$$x_{n+1} = \Phi(x_n) = \Phi^{n+1}(x_0), \quad n = 0, 1, \ldots \tag{2.1}$$

Из предыдущего следует, что период этой последовательности равен p^{ml}. Представляя x_n в форме (1.2) определим нормализованное отображение $R(l,m) \to [0,1)$:

$$R \ni y = a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1} \to \eta(y) = \frac{a_0 + a_1 p + \cdots + a_{m-1}p^{m-1}}{p^{ml}} \in [0,1).$$

Таким образом, последовательность $\{x_n\}$ периода p^{ml} порождает последовательность $\eta(x_n) \in [0,1)$, которую мы назовём инверсной конгруентной последовательностью псевдослучайных чисел. Но чтобы оправдать название псевдослучайной последовательности, мы должны показать, что $\{\eta(x_n)\}$ равномерно распределена на $[0,1)$ и непредсказуема.

Для этого нам понадобятся оценки некоторых специальных сумм.

Теорема 2.1. *Пусть последовательность $\{x_n\}$, порожденная рекурсией (1.5), имеет период $\tau = p^{ml}$. Тогда для любого $N \le \tau$ и любого ненулевого по mod p вектора $h \in Z^m$, справедлива оценка:*

$$\left| \sum_{n=0}^{N-1} e_{p^m}(h \cdot x_n) \right| \le (3Np^{lm-\frac{m}{2}+l-1})^{1/2},$$

здесь запись $h \cdot x_n$ означает скалярное произведение векторов $h = (h_0, \ldots, h_{m-1})$ и $x_n = (x^{(0)}, x^{(1)}, \ldots, x^{(m-1)})$.

Доказательство. Обозначим $S_N(h) = \sum_{n=0}^{N-1} e_q(h \cdot x_n)$. Поскольку $x_n = \Phi^n(x_0),\ n = 0, 1, \ldots$, то мы имеем для любого целого k

$$\left| S_N(h) - \sum_{n=0}^{N-1} e_q(h \cdot x_{n+k}) \right| \le 2\,|k|\,. \tag{2.2}$$

Для целого $K \ge 1$ обозначим через $R(K)$ множество целых $k \in Z$, для которых

$$-\frac{K-1}{2} \le k \le \frac{K-1}{2},$$

если K — нечетное;

$$-\frac{K}{2}+1\le k\le\frac{K}{2},$$

если K — четное. Очевидно, $\sum_{k\in R(k)}|k|\le\frac{1}{4}K^2$.

Применяя неравенство (2.2) для всех $k\in R(K)$ и складывая эти неравенства, получим

$$K\,|S_N(h)|\le W+\frac{1}{2}K^2, \tag{2.3}$$

где

$$W=\Big|\sum_{n=0}^{N-1}\sum_{k\in R(K)}e_q(h\cdot x_{n+k})\Big|\le\sum_{n=0}^{N-1}\Big|\sum_{k\in R(K)}e_q(h\cdot\Phi^k(x_n))\Big|.$$

Теперь, в силу неравенства Коши–Шварца, находим

$$\begin{aligned}
W^2&\le N\sum_{n=0}^{N-1}\Big|\sum_{k\in R(K)}e_q(h\cdot\Phi^k(x_n))\Big|^2\\
&\le N\sum_{n=0}^{\tau-1}\Big|\sum_{k\in R(K)}e_q(h\cdot\Phi^k(x_n))\Big|^2=N\sum_{x\in R(l,m)}\Big|\sum_{k\in R(K)}e_q(h\cdot\Phi^k(x))\Big|^2\\
&\le N\sum_{k_1,k_2\in R(K)}\Big|\sum_{x\in R(l,m)}e_q(h(\Phi^{k_1}(x)-\Phi^{k_2(x)}))\Big|\\
&=KNp^{lm}+2N\sum_{\substack{k_1,k_2\in R(K)\\k_1>k_2}}\Big|\sum_{x\in R(l,m)}e_q(h\cdot(\Phi^{k_1-k_2}(\Phi^{k_2}(x))-\Phi^{k_2}(x))\Big|\\
&=KNp^{lm}+2N\sum_{\substack{k_1,k_2\in R(K)\\k_1>k_2}}\Big|\sum_{x\in R(l,m)}e_q(h\cdot(\Phi^{k_1-k_2}(x)-x))\Big|.
\end{aligned}\tag{2.4}$$

Пусть $\alpha_0,\alpha_1,\dots,\alpha_{m-1}$ — базис $R(l,m)$ над Z_{p^l}, двойственный к базису $\{1,\xi,\xi^2,\dots,\xi^{m-1}\}:=\Xi_*$. Тогда для каждого $x\in R(l,m)$, $x=x^{(0)}+x^{(1)}\xi+\dots+x^{(m-1)}\xi^{m-1}$, по определению двойственного базиса имеем:

$$x^{(i)}=Tr(\alpha_i x),\quad i=0,1,\dots,m-1,$$

где $Tr(\alpha_i x)$ означает функцию следа из $R(l,m)$ в Z_{p^l}.

Поэтому, в силу линейности Tr над Z_{p^l}, получаем, обозначая $\Phi^{k_1-k_2}(x)=y$, $x=(x^{(0)},\dots,x^{(m-1)})$, $y=(y^{(0)},\dots,y^{(m-1)})$:

$$\sum_{x\in R(l,m)} e_q(h\cdot(\Phi^{k_1-k_2}(x)-x))$$

$$= \sum_{x\in R(l,m)} e_q\Big(\sum_{j=0}^{m-1} h_j(y^{(j)}-x^{(j)})\Big)$$

$$= \sum_{x\in R(l,m)} e_q\Big(\sum_{j=0}^{m-1} h_j Tr(\alpha_j(y-x))\Big)$$

$$= \sum_{x\in R(l,m)} e_q\Big(\sum_{j=0}^{m-1} Tr(h_j\alpha_j(y-x))\Big)$$

$$= \sum_{x\in R(l,m)} e_q(Tr(\beta y-\beta x)) := S(\beta),$$

где $\beta=\sum_{j=0}^{m-1} h_j\alpha_j \in R(l,m)$.

Далее, так как $y=\Phi^{k_1-k_2}(x)$, то применяя индукцию по k и используя рекурсию (1.5), мы легко получаем, что $\Phi^k(x)$ имеет один из трёх следующих видов:

$$\begin{cases} (i) & \frac{A(k)x+B(k)}{C(k)x+D(x)}, & A(k),B(k),C(k),D(k)\in Z_{p^l};\\ & & (A(k),B(k),p)=(C(k),D(k),p)=1;\\ & & 0\le s<l-1;\\ (ii) & A(k)x+B(k), & A(k)\neq 0;\\ (iii) & B(k) & \end{cases} \tag{2.5}$$

Каждый элемент из $R(l,m)$ можно однозначно представить в виде $x+c$, где $x\in\Xi,\ c\in pR(l,m)=B(0)$.

Теперь учтём, что в представлении (2.5)(i) элемента $x\in R(l,m)$ знаменатель обращается в нуль (для каждого k) не более $(rk-1)$ раз. Поэтому имеем:

$$|S(\beta)|\le \sum_{c\in pR(l,m)}\Big(\Big|\sum_{x\in\Xi_*} e_q(\beta_1 x+\beta_2 x^{-1})\Big|+2k-1\Big),$$

где β_1,β_2 линейно выражаются через β и одновременно не обращаются в нуль.

Сумму по $x\in\Xi_*$ можно оценить по лемме 1.1, если $\beta_2=0$ или по лемме 1.2, если $\beta_2\neq 0$. Поэтому имеем(учитывая, что $|pR(l,m)|=p^{m(l-1)}$):

$$W^2\le KNp^{lm}+2N\sum_{k=1}^{K-1}(K-k)p^{m(l-1)}(2p^l\cdot p^{\frac{m}{2}}+2k-1)$$

$$\le KNp^{lm} + 2Np^{m(l-1)}\Big(2p^{l-1}\cdot p^{\frac{m}{2}}\cdot\frac{K(K-1)}{2} + \frac{K(K-1)(2K-1)}{6}\Big)$$
$$< KNp^{lm} + (K-1)KN(2p^{l+\frac{m}{2}-1} + \frac{K}{3})p^{m(l-1)}$$
$$= K^2N\Big(p^{lm}(1-2p^{-\frac{m}{2}+l-1})K^{-1} + 2p^{lm-\frac{m}{2}+l-1} + \frac{2}{3}K\Big). \quad (2.6)$$

при условии, что $K \le \tau$. Положим

$$K = \Big[\Big(\frac{3}{2}\Big)^{1/2} p^{\frac{lm}{2}-1}\big|1-2p^{-\frac{m}{2}+l}\big|^{1/2}\Big] + 1. \quad (2.7)$$

Будем считать, что $\tau \ge N > 2p^{\frac{lm}{2}}$. Тогда условие $K \le \tau$ удовлетворяется. При таком выборе К имеем:

$$p^{lm}\big|1-2p^{-\frac{m}{2}+l-1}\big|K^{-1} + 2p^{lm-\frac{m}{2}+l-1} + \frac{2}{3}K \le \Big(\Big(\frac{8}{3}\Big)^{1/2} + 2\Big)p^{lm-\frac{m}{2}+l-1}. \quad (2.8)$$

Следовательно, из (2.2)–(2.8) находим:

$$|S_N(h)| < \Big(\Big(\frac{8}{3}\Big)^{1/2} + 2\Big)^{1/2} N^{1/2}\cdot p^{\frac{lm}{2}-\frac{m}{4}+\frac{l}{2}-\frac{1}{2}}.$$

Отсюда уже следует утверждение теоремы 1.1. □

Следствие 2.1. *Пусть последовательность x_n порождена рекурсией (1.5) и имеет максимальный период $\tau = p^{ml}$, причем $m > 2l$. Тогда для ненулевого по mod p вектора $h \in Z^m$ справедливо равенство $|S_\tau(h)| = 0$.*

Действительно, мы имеем

$$S_\tau(h) = \sum_{n=0}^{\tau-1} e_q(h\cdot x_n) = \sum_{x\in R(l,m)} e_q(h\cdot x)$$
$$= \sum_{x^{(0)},\dots,x^{(m-1)}=0}^{q-1} e_q\Big(\sum_{j=0}^{m-1} h_j x^{(j)}\Big) = \prod_{j=0}^{m-1}\sum_{x^{(j)}=0}^{q-1} e^{2\pi i\frac{h_j x^{(j)}}{q}} = 0, \quad (2.9)$$

так как хотя бы одно $h_j \not\equiv 0\ (mod\ p)$.

Пусть последовательность $\{x_n\}$, порожденная рекурсией (1.5), имеет период τ. Положим

$$S_\tau(h_1,h_2) := \sum_{n=0}^{\tau-1} e_q(h_1x_n + h_2x_{n+r}), \quad (2.10)$$

где r — натуральное, $r < \tau$, $h_1, h_2 \in Z_q^m$.

Теорема 2.2. *Пусть* $\{x_n\}$ — *последовательность максимального периода, то есть* $\tau = p^{ml}$, *и пусть* h_1, h_2 — *ненулевые по mod p векторы. Тогда*

$$|S_\tau(h_1, h_2)| \le 3p^{ml-\frac{m}{2}+l-1}.$$

Доказательство. Поскольку функция Φ есть подстановка на $R(l,m)$, то $\Phi(x_{n+r}) = \Phi^r(x_n)$, а потому

$$S_\tau(h_1, h_2) = \sum_{n=0}^{\tau} e_q(h_1 \cdot x_n + h_2 \cdot x_{n+r}) = \sum_{x \in R(l,m)} e_q(h_1 \cdot x + h_2 \cdot \Phi^r(x)).$$

Теперь, как и при доказательстве теоремы 2.1, мы получаем:

$$\left| \sum_{x \in R(l,m)} e_q(h_1 \cdot x + h_2 \cdot \Phi^r(x)) \right| = \left| \sum_{x \in R(l,m)} e_q(Tr(\beta_1 x + \beta_2 x^{-1})) \right|$$
$$\le \sum_{c \in pR(l,m)} \left(2m + \left| \sum_{x \in \Xi_*} e_q(Tr(\beta_1 x + \beta_2 x^{-1})) \right| \right), \quad (2.11)$$

где $\beta_1, \beta_2 \in R(l,m), \beta_1, \beta_2$ одновременно не равны нулю. А потому

$$|S_\tau(h_1, h_2)| \le p^{m(l-1)}(2m + 2p^{l-1}p^{\frac{m}{2}}) \le 3p^{ml-\frac{m}{2}+l-1}.$$

Теорема доказана. □

Замечание 2.1. Полученные оценки сумм $S_N(h)$ и $S_\tau(h_1, h_2)$ равномерны по векторам $h_1, h_2 \not\equiv 0 \ (mod\ p^l)$. Эти оценки мы будем использовать для анализа на равнораспределенность и непредсказуемость последовательности $\{\eta(x_n)\}$, описанной в начале этого пункта.

3. Дискрипанция

Пусть $\{X_n\}$ — последовательность k-мерных точек из гиперкуба $[0,1)^k$. Дискрипанция этой последовательности $\{x_n\}$ определяется величиной

$$D_N^{(k)}(X_0, X_1, \ldots, X_{N-1}) = \sup_{\Delta \subset [0,1)^k} \left| \frac{A_N(\Delta)}{N} - |\Delta| \right|,$$

где супремум берется по всем параллелепипедам Δ из гиперкуба $[0,1)^k$ со сторонами, параллельными координатным осям, $|\Delta|$ — объём параллелепипеда Δ, $A_N(\Delta)$ — количество точек x_j, $j = 0, 1, \ldots, N-1$, попавших в Δ. Ясно, что $0 \le \Delta \le 1$.

Если $D_N^{(k)} \to 0$ при $N \to \infty$, то распределение точек x_n в $[0,1)^k$ "практически" равномерное. Для периодических последовательностей D_N не может стремиться к нулю. Но считается, что чем меньше $D_N^{(k)}$ при больших N, тем "лучше" равнораспределены точки в $[0,1)^k$.

Из одномерной последовательности точек $\{U_n\}$ можно строить различные последовательности k-мерных точек. Для изучения непредсказуемости одномерной последовательности обычно рассматривают следующую последовательность k-мерных точек:

$$X_n^{(k)} = (x_n, x_{n+1}, \ldots, x_{n+k-1}). \tag{3.1}$$

Сериальный тест на непредсказуемость одномерной последовательности $\{x_n\}$ утверждает, что если k-мерные точки типа (20) равномерно распределены, $k = 1,2,3,4,5$, то последовательность $\{U_n\}$ "практически" непредсказуема. В нашем случае, применение лемм 3.12 и 3.13 из работы Х. Нидеррайтера [7], а также равномерность по векторам $h, h_1, h_2 \in Z_q^m$ оценок тригонометрических сумм $S_N(h)$, $S_\tau(h_1, h_2)$, приводят к следующим неравенствам:

$$D_N^{(1)} \le \frac{1}{p^{ml}} + \left(\frac{2}{\pi}\log p^{ml} + \frac{7}{5}m - \frac{m-1}{p^l}\right)\left(3N^{-1}p^{lm-\frac{m}{2}+l-1}\right)^{1/2} \tag{3.2}$$

$$D_\tau^{(2)} \le 1 - \left(1 - \frac{1}{p^{ml}}\right)^2 + 3\left(\frac{2}{\pi}\log p^{ml} + \frac{7}{5}m - \frac{m-1}{p^l}\right)^2 p^{-\frac{m}{2}+l-1}. \tag{3.3}$$

Таким образом, при $m > 2(l-1)$ и $N > p^{lm(1+\epsilon)-\frac{m}{2}+l-1}$, $\epsilon > 0$ — произвольно малая постоянная, последовательность $\{\eta(x_n)\}$ проходит двумерный сериальный тест на псевдослучайность.

В заключение заметим, что результат теоремы 2.2 в случае $p = 2$ был получен в работе [8].

Литература

[1] W.-S. Chou, *The Period Lengths of Inversive Pseudorandom Vector Generations* // Finite Fields and Their Applications, **1** (1995), 126–132.

[2] J. Eichenauer-Herrmann, H. Grothe, *A new inversive congruential pseudorandom numbers generator with power of two modulus* // ACM Trans. Modeling and Comp. Simulation, **2(1)** (1992), 1–11.

[3] J. Eichenauer, J. Lehn, *A non-linear congruential pseudorandom numbers generator* // Statist. Heftc, **27** (1986), 315–326.

[4] M. Flahive, H. Niederreiter, *On inversive congruential generators for pseudorandom numbers* in: Finite Fields, Coding Theory, and Advances in Communications and Computing, G. L. Mullen and P. J.-S. Shines (eds.), Marsel Dekker, N-Y, 1992, 75-80.

[5] T. Helleseth, P. V. Kumar, A. G. Shanbhag, *Exponential sums over Galois rings and their applications, Finite Fields and Applications* // Lond. Math. Soc., Lecture Notes Ser., **233** (1996), 109–128.

[6] P. V. Kumar, T. Helleseth, A. R. Calderbank, *An upper bound for Weil exponential sums over Galois rings and applications* // IEEE Trans. Inform. Theory, IT-**41** (1995), 456–468.

[7] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[8] P. Sole, D. Zinoviev, *Inversive Congruential Pseudorandom Numbers over Galois Rings*, IITP RAS, Moscow, Russia, CNRS-13S, Sophia Antipolis, FRANCE.

Сведения об авторах

Елена Викторовна Вернигора
Институт математики, экономики и механики
Одесский национальный университет им. И. И. Мечникова
ул. Дворянская, 2,
Одеса, 65082
Украина
E-Mail: verlin@ukr.net