УДК 511.519

КОГНРУЭНЦИАЛЬНЫЕ ИНВЕРСНЫЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Рудецкий В.С., Задорожный С.А.

Одесский национальный университет им.И.И.Мечникова, Одесса, Украина

Рассматриваются инверсные генераторы псевдослучайных чисел на отрезке [0,1) и единичного круга в комплексной плоскости. С помощью неравенства Turan-Erdös-Koksma и его аналога найдены нетривиальные оценки дискрипантной функции для последовательностей псевдослучайных чисел.

КЛЮЧЕВЫЕ СЛОВА: псевдослучайные числа, генераторы чисел, инверсные генераторы, дискрипантная функция.

КОГНРУЕНЦІАЛЬНІ ІНВЕРСНІ ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Рудецький В.С., Задорожний С.А.

Розглядаються інверсні генератори псевдовипадкових чисел на відрізку [0,1) і одиничного кола в комплексній площині. За допомогою нерівності Turan-Erdös-Koksma і його аналога знайдені нетривіальні оцінки діскріпантної функції для послідовностей псевдовипадкових чисел.

КЛЮЧОВІ СЛОВА: псевдовипадкові числа, генератори чисел, інверсні генератори, діскріпантна функція.

KOGNRUENTIAL INVERSE PSEUDO RANDOM NUMBER GENERATORS

Rudetsky V.S., Zadorozhny S.A.

Inverse generators of pseudo-random numbers in the interval [0,1) and in the unit circle in the complex plane are considered. Using the Turan-Erdös-Koksma inequality and its analogue the nontrivial estimations of discrepant function for the sequences of pseudorandom numbers are found.

KEY WORDS: pseudo-random numbers, random number generator, inverse generators diskripantnaya function.

1. Введение. В различных задачах по применению метода Монте-Карло, теории и практики моделирования а также в криптографии (при формировании случайных ключей) имеется потребность в генерировании чисел «близких» к случайным. Под последовательностью случайных чисел обычно понимается всякая реализация последовательности равномерно распределённых на [0,1) и статистически независимых случайных величин.

Поскольку построение такой последовательности случайных величин весьма затруднительно, на практике пользуются «псевдослучайными» числами, то есть такими последовательностями вещественных чисел отрезка [0,1), которые по своим свойствам близки к случайным числам.

Удачное решение построения псевдослучайных чисел осуществил D. Lthmer, который в 1951 году рассмотрел рекурсию

$$y_{n+1} \equiv a y_n (\mathrm{mod}\, M) \qquad (1)$$

где a, b, y_0 и M – фиксированные целые числа, $n = 0,1,2,\ldots$.

Очевидно, что последовательность $\{y_n\}$ – периодична с периодом $\tau \le M$. Рекурсия (1) является частным случаем конгруэнтной рекурсии

$$y_{n+1} \equiv f(y_n) (\mathrm{mod}\, M), \qquad (2)$$

где $f(y)$ – целочисленная функция.

В 70-х годах прошлого столетия рядом исследователей (в частности Marsaglia, Niederreiter) показали , что линейная рекурсия (1) порождает последовательность не удовлетворяющую требованиям статистической независимости(непредсказуемости). Поэтому в последующем стали использовать нелинейные рекурсии, наиболее полные исследования относят к квадратичным ($f(x) = ax^2 + bx + c$) и инверсным ($f(x) = \frac{a}{x} + b$) рекурсиям.

На протяжении 1990–2003 годов Eichenauer, Flahive, Niederreiter, Emmerich, Grothe, Shparlinsky исследовали генератор вида

$$y_{n+1} = a y_n^{-1} + b (\mathrm{mod}\, p^m), \qquad (3)$$

который называется инверсным конгруэнтным генератором по модулю степени простого числа.

В 1995 г. Chou [1] изучил условия, при которых соответствующая последовательность $\{y_n\}$ существует (то есть y_n имеет мультипликативное обратное по модулю p^m) и ее период имеет максимально возможное значение.

Наша цель обобщить генератор (3), изучить дискрипантную функцию последовательности $\{x_n\}$ и доказать, что эта последовательность проходит сериальный тест на непредсказуемость.

В настоящей работе мы изучаем линейно-инверсный генератор

$$y_{n+1} = ay_n^{-1} + b + cy_n \pmod{p^m} \qquad (4)$$

Легко видеть, что условия $(a,p)=1,\ b \equiv c \equiv 0 \pmod p$ или $a \equiv b \equiv 0 \pmod p, (c,p)=1$ гарантируют существование $y_n^{-1}, n = 1,2,\ldots$, если брать y_0 взаимнопростым с p.

Chou [1] показал, что условия $a \equiv 0(p),\ (b,p)=1,\ c=0$ порождают последовательность $\{y_n\}$, у которой период равен 1, что не интересно для приложений.

Кроме того будем исследовать распределение точек ω_n единичного круга комплексной плоскости, порожденных инверсным генератором

$$z_{n+1} \equiv \alpha z_n + \beta \pmod{\rho^m}, (z_0, \rho) = 1 \qquad (5)$$

где $\alpha, \beta -$ целые гауссовы числа, $\rho -$ простое гауссово число, $m \ge 3, m \in \mathbb{Z}$.

Генератор (5) мы назовем комплексным генератором псевдослучайных чисел.

Для дискрипантной функции последовательности $\left\{\frac{z_n}{\rho^m}\right\}$, порожденной произвольным конгруэнтным генератором типа (5) над кольцом целых гауссовых чисел, мы строим аналог неравенства Turan-Erdös-Koksma.

В дальнейшем нам понадобятся некоторые обозначения.

Кольцо целых гауссовых чисел мы обозначим $G := \{a+bi \mid a,b \in \mathbb{Z}, i^2 = -1\}$. Греческие буквы $\alpha, \beta, \gamma, \ldots$ используются для обозначения элементов из G; $\rho -$ простое гауссово число. Для $\alpha \in G$, $N(\alpha) = |\alpha|^2$ – норма α; $\mathbb{Z}_M$ (соответственно, G_γ) – полная система остатков по модулю M (соответственно, по модулю γ); $\mathbb{Z}_M^*$, G_γ^* редуцированные системы остатков; для простых p (соответственно, $\rho \in G$) через $\nu_p(U)$ (соответственно, $\nu_\rho(V)$) обозначаем неотрицательное t такое, что $p^t \mid U$ (соответственно, $\rho^t \mid V$), но $p^{t+1} \nmid U$ (соответственно, $\rho^{t+1} \nmid V$).

2. Дополнительные результаты. Пусть $\{x_n\}$ – последовательность точек из $[0,1)$. Для любого натурального s образуем последовательность точек $X_n^{(s)} \in [0,1)^s$, де $X_n^{(s)} = (x_n, x_{n+1}, \ldots, x_{n+s-1})$.

Пусть

$$D_n^{(s)}(x_0,\ldots,x_{N-1}) = D_N^{(s)} := \sup_{\Delta \subset [0,1)} \left| \frac{A_N(\Delta)}{N} - |\Delta| \right|,$$

где $\Delta \subset [0,1)^s$ – параллелепипед, стороны которого параллельны координатным осям, $|\Delta|$ – его объем,

$$A_N(\Delta) = \sum_{\substack{x_n \in \Delta \\ n=0,\ldots,N-1}} 1,$$

супремум берется по всем $\Delta \subset [0,1)^s$.

$D_N^{(s)}$ назовем дискрипантной функцией последовательности $\{X_n^{(s)}\}$.

Показателем равномерной распределенности $\{x_n\}$ на $[0,1)$ является стремление $D_N^{(1)} = D_N$ к нулю при $N \to \infty$.

Мы будем говорить, что $\{x_n\}$ проходит s-мерный сериальный тест на статистическую независимость(непредсказуемость), если $D_N^{(1)}, \ldots, D_N^{(s)}$ стремятся к нулю при $N \to \infty$.

Для $h \in \mathbb{Z}_M$ обозначим $\overline{h} = \max(1,h)$.

Лемма 1. *Пусть $\{y_n\}$ – последовательность целых чисел из $\mathbb{Z}_M$ периода τ. Тогда для каждого $s \in \mathbb{Z}, s \ge 1$ и $0 \le N \le \tau - 1$ имеем*

$$D_N^{(s)} \le \frac{s}{M} + \frac{1}{N} \sum_{\substack{(h_0,h_1,\ldots,h_s) \in \mathbb{Z}_M^{s+1} \\ (h_0,h_1,\ldots,h_s) \ne (0,0,\ldots,0)}} \frac{1}{\overline{h}_0 \ldots \overline{h}_s} |S|,$$

где $S := \sum_{n=0}^{N-1} \exp(2\pi i (h \cdot X_n + \frac{nh_0}{\tau}))$, $h \cdot X_n$ – *скалярное произведение векторов* $h = (h_1,\ldots,h_s), X_n = (x_n, x_{n+1}, \ldots, x_{n+s-1}), x_n = \frac{y_n}{M}$.

Это утверждение является одной из форм неравенства Turan-Erdös-Koksma(док. см. [3]).

Пусть теперь $\{z_n\}$ – последовательность элементов полной системы вычетов по модулю $\gamma, \gamma \in G$. Тогда последовательность $\left\{\frac{z_n}{\gamma}\right\}$ принадлежит единичному кругу $|\omega| \le 1$.

Пусть $0 \le \xi_1 < \xi \le 1$ та $0 \le \varphi_1 < \varphi_2 < 2\pi$.

Обозначим секториальную область $S(\xi, \varphi) := \{\omega \in \mathbb{C} \mid \xi_1 < |\omega|^2 \le \xi_2, \varphi_1 < \arg\omega \le \varphi_2\}$.

$\Im$ – семейство секториальных областей единичного круга.

Для последовательности $\{\omega_n\}, \omega_n = \frac{z_n}{\gamma}$ определяем дискрипантную функцию

$\tilde{D}_N := \sup_{S(\xi,\varphi)\in\Im}\left|\frac{A_N(S)}{N}-|S|\right|$, где sup берем по всем $S\in\Im$.

Лемма 2. *Пусть $M>1$ – натуральное. Тогда для каждой последовательности точек $\{z_n\}$, $z_n\in G_M$, дискрипантная функция $\tilde{D}_N$ последовательности $\left\{\frac{z_n}{M}\right\}$ удовлетворяет неравенству*

$$\tilde{D}_N \le 2\left(1-\left(1-\frac{2\pi}{M}\right)^2\right)+\frac{2\log^2 M}{M^{5/3}}\sum_{\substack{\alpha\in G_M\\ \alpha\neq 0}}\frac{1}{N}\left|\sum_{n=0}^{N-1}e^{2\pi i\,\mathrm{Re}\left(\frac{\alpha z_n}{M}\right)}\right| \quad (6)$$

Эта лемма является обобщением неравенства Turan-Erdös-Koksma (см. Лемма 1) на случай последовательности комплексных точек единичного круга (для доказательства см.[7], Теорема 1).

Для исследования свойств последовательностей $\{x_n\}$ и $\{\omega_n\}$, порожденных генераторами (4) и (5) нам понадобятся представления элементов y_n и z_n как полиномов от индекса n и инициальных значений y_0 (соответственно, z_0).

Лемма 3. *Пусть последовательность $\{y_n\}$ порождена генератором (4), причем $(a,p)=1, b\equiv c\equiv 0\pmod p, (y_0,p)=1, m\ge 3$. Тогда имеют место представления*

$$\begin{cases} y_{2k} = kb+kacy_0^{-1}+(1-(k-1)ka^{-1}b^2)y_0-ka^{-1}by_0^2+\\ \quad +(-ka^{-1}c+k^2a^{-2}b^2)y_0^3+pF_0(k,y_0,y_0^{-1}),\\ y_{2k+1} = (k+1)b+(a-k(k+1)b^2)y_0^{-1}-kaby_0^{-2}+\\ \quad +(-ka^2c+k^2ab^2)y_0^{-3}+(k+1)y_0c+p^tG_0(k,y_0,y_0^{-1}), \end{cases} \quad (7)$$

где $k\ge 2m+1$, $t=\min(\nu_p(b^3),\nu_p(c))$.

Следствие 1. *Пусть выполнены условия Леммы 3. Тогда для всех $k, 2m+1\le k\le\frac{1}{2}\tau$, имеем*

$$\begin{cases} y_{2k} = A_0+A_1k+A_2k^2+k^3(A_3+A_4k+\ldots),\\ y_{2k+1} = B_0+B_1k+B_2k^2+k^3(B_3+B_4k+\ldots) \end{cases} \quad (8)$$

где по модулю p^α, $\alpha=\min(3\upsilon_p(b),\upsilon_p(bc))$,

$A_0\equiv y_0$,

$A_1\equiv b(1-a^{-1}y_0^2)+a^{-1}b^2y_0+acy^{-1}(1-a^{-2}y_0^4)$,

$A_2\equiv -a^{-1}b^2y_0(1-a^{-1}y_0^2)$,

$B_0\equiv b+ay_0^{-1}+cy_0$,

$B_1\equiv b(1-ay_0^{-2})-b^2y_0^2-y_0c(1-a^2y_0^{-4})$,

$B_2\equiv -b^2y_0^{-1}(1-ay_0^{-2})$,

$A_j\equiv B_j\equiv 0, j=3,4,\ldots$

(Доказательство Леммы 3 и Следствия 1 см. [5], а также [6])

Из Леммы 3 и Следствия 1 получаем следующие утверждения:

Следствие 2. *Пусть $p>2$ и $\nu_p(b)\le\frac{1}{2}m$. Последовательность $\{y_n\}$ является чисто периодической с периодом $\tau=2p^{m-l}$, где*

$l=\nu_p(b)+\nu_p(a-y_0^2)$, *если* $\nu_p(a-y_0^2)\le\nu_p(b)$;

$l=2\nu_p(b)$, *если* $\nu_p(a-y_0^2)>\nu_p(b)$.

Следствие 2`. *Пусть $p=2$, $m\ge 3$. Тогда последовательность $\{y_n\}$ из Леммы 3 является чисто периодической, период которой τ равен*

- $2^{m-2\nu+1}$, *если* $m\ge 2\nu, \nu_0>\nu$;
- $2^{m-2\nu-\beta_0}$, *если* $m\ge 2\nu, \nu_0=\nu, \beta_0=\nu_p\left(\frac{y_0^2-a}{2^{\nu_0}}+b_0\right)$;
- $2^{m-2\nu-\nu_0+1}$, *если* $m\ge\nu+\nu_0, \nu_0<\nu$,
- *где* $\nu_0=\nu_2(a-y_0^2)\ge 1$, $\nu_p(c)>\nu_p(b)=\nu$, $b_0=p^{-\nu}b$.

Лемма 4. *Пусть для генератора (4) выполнены условия*

$$a\equiv b\equiv 0(\mathrm{mod}\,p), (c,p)=1, m\ge 3 \quad (9)$$

Тогда существуют полиномы над $\mathbb{Z}$ $F(u,v), F_j(u), j=-1,1$ такие, что для всех $k\ge m+1$ по модулю p^m:

$$y_k\equiv\begin{cases} c^ky_0+b\frac{1-c^k}{1-c}+ay_0^{-1}\frac{1-c^k}{1-c}\frac{c^{1-k}}{1+c}+\\ \qquad +a^2y_0^{-3}F(k,y_0^{-1}), & \text{если } c\neq\pm 1;\\ y_0+kb+kay_0^{-1}+a^2y_0^{-3}kF_1(ay_0^{-1}), & \text{если } c=1;\\ y_0+0b-kay_0^{-1}+a^2y_0^{-3}kF_{-1}(ay_0^{-1}), & \text{если } c=-1. \end{cases}$$

Доказательство этого утверждения легко провести с помощью метода математической индукции.

Следствие 3. *Период последовательности $\{y_n\}$, порожденной генератором (4) при условии (9) равен $\tau=dp^{m-m_0}$, где*

- $m_0=1$, $d=\frac{p-1}{\delta}$, δ *–показатель, которому принадлежит c по* $\mathrm{mod}\,p$ *для* $c\neq\pm 1$;
- $m_0=\min(\nu_p(b),\nu_p(a))$, *если* $c=1$ *и* $\nu_p(b)\neq\nu_p(a)$;
- $m_0=\nu_p(a)$, *если* $c=-1$.

Это утверждение следует из вида представления y_n (см. Лемма 4).

3. Тригонометрические суммы на последовательностях псевдослучайных чисел. Пусть последовательности $\{y_n\}$ или $\{z_n\}$ сгенерированные линейно-инверсным генератором (4) или комплексно-инверсным генератором (5). Тогда последовательности $\left\{\frac{y_n}{p^m}\right\}$ (соответственно $\left\{\frac{z_n}{\rho^m}\right\}$, где ρ – простое гауссово число) мы называем последовательностями псевдослучайных чисел(ПСЧ). Для того чтобы доказать, что эти последовательности имеют свойства равномерной распределенности и статистической независимости мы оцениваем тригонометрические суммы вида

$$S(h)=\sum_{n=0}^{N-1} e^{2\pi i\frac{hy_n}{p^m}},\ h\in\mathbb{Z} \tag{10}$$

$$\tilde{S}(\hbar)=\sum_{n=0}^{N-1} e^{2\pi i\,\mathrm{Re}(\frac{\hbar z_n}{\rho^m})},\ \hbar\in G \tag{11}$$

Построение оценок для сумм $S(h)$, $\tilde{S}(\hbar)$ базируется на следующей лемме.

Лемма 5. *Пусть p – простое и $f(x)$, $g(x)$ – полиномы над $\mathbb{Z}$*

$f(x)=A_1x+A_2x^2+p(A_3x^3+\ldots)$

$g(x)=B_1x+p(B_2x^2+B_3x^3+\ldots)$,

$\nu_p(A_2)=l>0,\ \nu_p(A_j)\ge l,\ j=3,4,\ldots$

Тогда имеют место оценки

$$\left|\sum_{x\in\mathbb{Z}_{p^m}} e^{2\pi i\left(\frac{f(x)}{p^m}\right)}\right|\le\begin{cases}2p^{\frac{m+l}{2}}, & \text{если } \nu_p(A_1)\ge l\\ 0, & \text{иначе}\end{cases} \tag{12}$$

$$\left|\sum_{x\in\mathbb{Z}^*_{p^m}} e^{2\pi i\left(\frac{f(x)+g(x^{-1}))}{p^m}\right)}\right|\le\begin{cases}(Kp)^{\frac{m}{2}}, & \text{если } (B,p)=1\\ 2p^{\frac{m+l}{2}}, & \text{если } \nu_p(A_1)\ge l,\ \nu_p(B_j)\ge l,\ j=1,2,\ldots\\ 0, & \text{если } \nu_p(A_1)<l\le\nu_p(B_j),\ j=1,2,\ldots\end{cases} \tag{12'}$$

где $K=K(A_1,B_1,p)$ – количество решений сравнения $A_1-B_1u^2\equiv 0(\mathrm{mod}\,p),\ u\in\mathbb{Z}^*_p$

Эти оценки являются следствием оценок классических сумм Гаусса и Клостермана(подробнее, см. [6], Лемма3).

Теперь можно доказать теорему.

Теорема 1. *Пусть линейно-инверсный генератор (4) имеет период τ, и пусть $\nu_p(b)=\nu$, $\nu_p(a-y_0^2)=\nu_0$, $2\nu\le m$. Тогда справедливы следующие оценки*

$$|S_\tau(h)|=\begin{cases}O(m), & \text{если } p>2,\ \nu_0<\nu,\ \nu_p(h)<m-\nu-\nu_0,\\ 4\cdot 2^{\frac{m+\nu_p(h)}{2}}, & \text{если } \nu_0>\nu,\ \nu_p(h)<m-2\nu,\\ \tau, & \text{иначе.}\end{cases} \tag{13}$$

Доказательство:

Из формул (7)–(8) получаем

$$|S_\tau(h)|=\left|\sum_{n=0}^{\tau-1} e^{2\pi i\left(\frac{hy_n}{p^m}\right)}\right|\le\left|\sum_{k=0}^{\frac12\tau-1} e^{2\pi i\left(\frac{hy_{2k}}{p^m}\right)}\right|+\left|\sum_{k=0}^{\frac12\tau-1} e^{2\pi i\left(\frac{hy_{2k+1}}{p^m}\right)}\right|=$$

$$=\left|\sum_{k=2m+1}^{\frac12\tau-1} e^{2\pi i\left(\frac{hF(k)}{p^m}\right)}\right|+\left|\sum_{k=2m+1}^{\frac12\tau-1} e^{2\pi i\left(\frac{hG(k)}{p^m}\right)}\right|+O(m)=$$

$$=\left|\sum_{k=0}^{\frac12\tau-1} e^{2\pi i\left(\frac{hF(k)}{p^m}\right)}\right|+\left|\sum_{k=0}^{\frac12\tau-1} e^{2\pi i\left(\frac{hG(k)}{p^m}\right)}\right|+O(m)$$

Теперь Следствия 1 и 2, Лемма 5 сразу дают оценки

$$|S_\tau(h)|=\begin{cases}O(m), & \text{если } p>2,\nu_0>\nu,\nu_p(h)<m-\nu-\nu_0\\ O(m), & \text{если } p=2,\nu_0<\nu,\nu_2(h)<m-2\nu\\ 4p^{\frac{m+\nu_p(h)}{2}}, & \text{если } \nu_0\ge\nu,\nu_2(h)<m-2\nu\\ \tau, & \text{иначе}\end{cases}$$

Заметим, что значения в символах “О” являются константами.

Учитывая связь между полной и неполной рациональной тригонометрическими суммами, получим:

Следствие 4. *Пусть $1\le N<\tau$. Тогда в обозначениях Теоремы 1 имеем*

$$|S_\tau(h)|\le\begin{cases}N, & \text{если } \nu+\nu_p(h)\ge m\\ 4p^{\frac{m+\nu_p(h)}{2}}\log\tau, & \text{если } \nu+\nu_p(h)<m\end{cases} \tag{14}$$

Теорема 2. *Пусть a,b,c – параметры линейно-инверсного генератора (4) и пусть $(a,p)=1,\ 0<\nu=\nu_p(b)<\nu_p(c)$, $1\le N\le 2p^{m-1}$, $\nu_p(h)=p^s,\ s<m$.*

Тогда среднее значение $S_N(h)$ по всем $y_0\in\mathbb{Z}^*_{p^m}$ удовлетворяет неравенству

$$\left|\overline{S}_N(h)\right|:=\frac{1}{\varphi(p^m)}\sum_{y_0\in\mathbb{Z}^*_{p^m}}|S_N(h)|\le N^{\frac12}p^{-\frac{m}{4}}(2\varepsilon_p^{\frac{m}{4}}+4p^{\frac{\nu+s}{4}}), \tag{15}$$

где $s=\nu_p(h,p^m)$,

$$\varepsilon_p=\begin{cases}1, & \text{если } p=2\\ 1+(\frac{-a}{p}), & \text{если } p>2,((\frac{-a}{p})-\text{символ Лежандра})\end{cases}$$

Это утверждение доказывается так же, как и Теорема 2 [4].

В случае генератора (5) мы пользуемся представлением (его можно получить так же как и в рациональном случае) для $k\ge 2m+1$:

$$z_{2k} = k\beta + (1-k(k-1)\alpha^{-1}\beta^2)z_0 + (-k\alpha^{-1}\beta)z_0^2 + \\ + k^2\alpha^{-2}\beta^2 z_0^3 + \tilde{\pi}^{3\upsilon}F_0(k, z_0, z_0^{-1}), \quad (16)$$

$$z_{2k+1} = (k+1)\beta + (\alpha - k(k-1)\beta^2)z_0^{-1} + (-k\alpha\beta)z_0^{-2} + \\ + k^2\alpha\beta^2 z_0^{-3} + \tilde{\pi}^{3\upsilon}G_0(k, z_0, z_0^{-1}), \quad (17)$$

где F_0, G_0 – полиномы с коэффициентами из G, причем $F_0(0,v,w) = G_0(0,v,w) = 0$

Отсюда получим следующее утверждение:

Лемма 6. *Пусть* $\{z_n\}$ *– период последовательность, порожденная генератором (5). Ее период* τ *равен:*

- $2\tilde{p}^{m-\nu-\nu_0}$, *если* $\rho \neq 1+i, \nu_0 < \nu \le \frac{1}{2}m$
- $2\tilde{p}^{m-2\nu}$, *если* $\rho \neq 1+i, \nu_0 \ge \nu, \nu \le \frac{1}{2}m$
- $2p^{m-2\nu+1}$, *если* $\rho = 1+i, \nu_0 < \nu, 2\nu \le m$
- $2p^{m-2\nu-b_0+1}$, *если* $\rho = 1+i, \nu_0 = \nu, 2\nu \le m$
- $2p^{m-\nu-\nu_0+1}$, *если* $\rho = 1+i, \nu_0 < \nu, m \ge \nu + \nu_0$

где

$$\nu_0 = \nu_\rho(\alpha - z_0^2),\ b_0 = \upsilon_\rho\left(\frac{z_0^2-\alpha}{(1+i)\nu_0} + 2^{-\nu}\beta\right),$$

$$\tilde{p} = \begin{cases} p, & \text{если } \rho \in \mathbb{Z}, \rho = p \equiv 3 (\mathrm{mod}\, 4) \\ N(\rho), & \text{если } \rho \notin \mathbb{Z} \end{cases}$$

Так же, как Теорему 1, можно доказать теорему 1`.

Теорема 1`. *Пусть последовательность, порожденная генератором (5) имеет период* τ *и пусть* $N \le \tau$. *Тогда для любого* $\gamma \in G_{\rho^m}$, $\gamma \neq 0$, *имеем*

$$S_N(\gamma) := \sum_{n=0}^{N-1} 2^{2\pi i \mathrm{Re}(\gamma \frac{z_n}{\rho^m})} << \begin{cases} O(m), & \text{если } \rho \neq 1+i,\ \nu_0 < \nu, \\ & \nu\rho(\gamma) < m - \nu - \nu_0, \\ O(m), & \text{если } \rho = 1+i,\ \nu_0 < \nu, \\ & \nu_\rho(\gamma) < m - 2\nu, \\ \tilde{p}^{\frac{m+\nu\rho(\gamma)}{2}} \log\tau, & \text{если } \nu_0 < \nu, \\ & \nu_\rho(\gamma) < m - 2\nu, \\ \tau, & \text{иначе.} \end{cases}$$

Теперь рассмотрим генератор (4) с условиями (9).

Пусть c принадлежит по модулю p показателю δ. Тогда $c^\delta = 1 + pt$. Положим $n = \bar{n}\delta + r, 0 \le r < \delta$. Легко видеть, что только для $r = 0$ можно получить конгруэнцию $y_n = y_0 (\mathrm{mod}\, p^m)$. Пусть $n = k\delta$. Из Леммы 4 мы имеем

$$y_n = (1 + kptH_1)y_0 + (bkH_0 + a^2 k y_0^{-3} + \ldots) \quad (18)$$

где $H_1 \equiv 1 (\mathrm{mod}\, p)$, $H_0 \equiv 1 (\mathrm{mod}\, p)$, $H_{-1} \equiv 2^{-1} (\mathrm{mod}\, p)$.

Отсюда находим, что период τ последовательности $\{y_n\}$ равен δp^{m-1}, если $ty_0 + \frac{b + ay_0^{-1}}{p} \neq 0 (\mathrm{mod}\, p)$, то есть максимально возможный период $\tau = \varphi(p^m) = p^{m-1}(p-1)$ достигается, если c – первообразный корень по модулю p, $c^{p-1} = 1 + pt$, $(t, p) = 1$, $ty_0 + \frac{b + ay_0^{-1}}{p} \neq 0 (\mathrm{mod}\, p)$.

Далее, по Лемме 4 получаем

$$y_n = A(y_0, t) + k(pty_0 + b + ay_0^{-1} + \ldots) + \\ + k^2 pt(2^{-1} y_0 pt + 2^{-1} b - 3 \cdot 4 a y_0^{-1} + \ldots) + k^3 p^3 F_3(k, y_0) \quad (19)$$

(троеточие в формуле (19) означает, что неуказанные слагаемые делятся на более высокие степени, чем указанные слагаемые).

Теперь из (19) следует оценка:

Теорема 1``. *Для последовательности порожденной генератором (4) с условиями* $a \equiv b \equiv 0 (\mathrm{mod}\, p), (c, p) = 1$

$$\left|S_N(h)\right| \le 2\sqrt{\tau}\, p^{\frac{1}{2}\nu_p(h)} \log\tau$$

для каждого N, $1 \le N \le \tau$.

Теоремы 1,1`,1`` позволяют при помощи неравенства Turan-Erdös-Koksma(и его аналога, см. п.2) доказать следующие утверждения.

Теорема 3. *Для последовательности* $\{x_n\}$, *порожденной рекурсией (4) при* $(a, p) = 1$, $0 < \nu_p(b) < \nu_p(c)$, $a \equiv y_0^2 (\mathrm{mod}\, p)$ *имеем*

$$D_N \le 3N^{-1} p^{\frac{m}{2}} \log^2 p^m,\ N \le 2p^{m-1}.$$

Теорема 3`. *Пусть* ρ *– простое гауссово число,* $\rho \neq 1+i$, $\alpha, \beta, z_0 \in G$, $(\alpha, \rho) = (z_0, \rho) = 1$, $\nu_\rho(\beta) = \nu \ge 1$, $m \ge 2\nu$. *Тогда для последовательности* $\left\{\frac{z_n}{\rho^m}\right\}$ *имеем*

$$\tilde{D}_N \le \frac{9\pi}{\tilde{p}^m} + 3N^{-1}\tilde{p}^{\frac{5}{6}}(\log \tilde{p}^m)^t,$$

где $t = \begin{cases} 3, & \text{если } \alpha \neq z_0^2 (\mathrm{mod}\, \rho) \\ 4, & \text{если } \alpha \equiv z_0^2 (\mathrm{mod}\, \rho) \end{cases}$.

Теорема 3``. *Для последовательности* $\left\{\frac{y_n}{p^m}\right\}$, *порожденной генератором (4) при условии* $a \equiv b \equiv 0 (\mathrm{mod}\, p), (c, p) = 1$, $m \ge 3$ *имеем*

$$D_N \le \frac{\delta}{p^m} + 4N^{-1}\tau^{\frac{1}{2}} \log p^m,$$

где δ *– показатель с по модулю* p, *а* τ *– период последовательности* $\{y_n\}$.

Аналогичным образом можно найти оценки s-мерных псевдослучайных точек $\{x_n^{(s)}\}$,

порожденных последовательностью псевдослучайных чисел $\{x_n\}$, сгенерированных генераторами (4) и (5).

Теорема 4. *Дискрипантная функция* $D_N^{(s)}, s = 2,3,4$ *точек, порожденных генератором (4) с параметрами* a,b,c *, которые удовлетворяют условиям*

$$0 < \nu_p(b) = \nu \le \nu_p(c), \qquad (a,p) = (y_0,p) = 1,$$

$a \equiv y_0 (\mathrm{mod}\, p)$

Имеет следующую оценку

$$D_N^{(s)} \le \frac{s}{2p^{m-\nu}} + p.$$

Доказательство: Рассмотрим только случай $s = 4$. Остальные случаи доказываются аналогично.

Для $s = 4$, $h = (h_1, h_2, h_3, h_4)$ мы имеем:

$$S_N(h) = \sum_{n=0}^{N-1} e^{2\pi i \frac{h_1 y_n + h_2 y_{n+1} + h_3 y_{n+2} + h_4 y_{n+3}}{p^m}}$$

Не ограничивая общности, можно считать, что $(h_1, h_2, h_3, h_4, p) = 1$, $n = 2k$.Тогда получим(из формулы (8)):

$$S_N(h) = \sum_{n=0}^{\frac{1}{2}N-1} e^{2\pi i \frac{C_0 + C_1 k + C_2 k^2 + C_3 k^3}{p^m}}$$

где по модулю p^r, $r = \min(\upsilon_p(b^3), \upsilon_p(bc))$:

$$C_1 = b(1-a^{-1}y_0^2)[(h_1+h_3) - ay_0^{-2}(h_2+h_3)] + acy_0^{-1}[(h_1+h_3)(1-a^{-2}y_0^4) -$$
$$-(h_2+h_4)(1-a^{-2}y_0^4)] + ba^{-1}y_0[(h_1+h_3) + 2(h_2+h_4)a^2y_0^{-4}(1-a^{-1}y_0^2) +$$
$$+ba^{-1}y_0[(h_1+h_3) + 2(h_2+h_4)a^2y_0^{-4}(1-a^{-1}y_0^2) + 4(h_3+h_4)(a^2y_0^{-4} - ay_0^{-2})]$$

$$C_2 = -(1-a^{-1}y_0^2)a^{-1}y_0[(h_1+h_2) - (h_2+h_4)a^2y_0^{-4}]b^2$$

Теперь, используя оценку полной тригонометрической суммы (см. [5], Лемма 1), выводим

$$|S_\tau(h)| = \begin{cases} 0, \text{ если } (h_1+h_3) - (h_2+h_4)ay_0^2 \not\equiv 0 (\mathrm{mod}\, p) \\ Cp^{\frac{m+\nu}{2}}, \ C \le 4, \text{ иначе} \end{cases}$$

поэтому для $N < \tau$

$$|S_N(h)| = Ap^{\frac{m+\nu}{2}} \log p^m, \ A \le 5.$$

Теперь из Леммы 1 сразу находим для $M = p^m$:

$$D_N^{(s)} \le \frac{s}{p} + 5N^{-1}p^{\frac{m+\nu}{2}} (\log p^m)^{s+2}.$$

Следствие 5. *Для* $N >> p^{\frac{m+\nu}{2}+\varepsilon}$ *последовательность* $\left\{\frac{y_n}{p^m}\right\}$ *проходит s-мерный сериальный тест (s = 1,2,3,4) на непредсказуемость.*

Для двух других генераторов, рассмотренных выше, имеют место подобные оценки дискрипантной функции.

4. Выводы. Найденные результаты говорят о том, что линейно-инверсные генераторы могут быть использованы в задачах криптографии и моделировании случайных процессов.

ЛИТЕРАТУРА

1. Chou W.-S. The period lengths of inversive congruential recursions. *Acta Arith*. – 1995. – v.73(4). – P.325 – 341.
2. Kato T., Wu L.-M., Yanagihara N. On a nonlinear congruential pseudorandom number generator. *Math. Comput*. – 1996. – v.65(213). – P. 227 – 233.
3. Niederreiter H. *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM, Philadelphia, 1992.
4. Varbanets S. On inversive congruential generator for pseudorandom numbers with prime power modulus. *Ann. Univ. Sci. Budapest*, *Sect. Comput*. – 2008. – v.29. – P. 277 – 296.
5. Varbanets P., Varbanets S. Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime power modulus. *Voronoi's Impact on Modern Science.* Book 4. vol. 1. – 2008. – P. 112 – 130.
6. Varbanets P., Varbanets S. Linear – inversive congruential generator with prime power modulus *Liet. Math. I.* (to appear)
7. Варбанец П., Задорожный С. Инверсный конгруэнтный генератор комплексных псевдослучайных чисел. *Дискретная математика* (в печати).