ГЕНЕРАТОР LSFR-CNS: АНАЛИТИЧЕСКОЕ ИССЛЕДОВАНИЕ РАВНОМЕРНОСТИ РАСПРЕДЕЛЕНИЯ

А.Н. Калугин[1,2]
[1]*Институт систем обработки изображений РАН, Самара, Россия,*
[2]*Самарский государственный аэрокосмический университет им. С.П. Королева, Самара, Россия*

Аннотация

В работе предлагается метод аналитического исследования качества равномерного распределения многомерной псевдослучайной последовательности на выходе генератора LFSR-CNS, даны асимптотические оценки отклонения генерируемого распределения от равномерного на неполном периоде генератора.

Введение

Одной из основных областей применения генераторов псевдослучайных последовательностей является численное интегрирование по методу Монте-Карло [11], [3], [12]. Многие практические задачи, могут быть сведены к вычислению многомерного интеграла.

Несмотря на то, что эмпирическое исследование генерируемой последовательности в реальных задачах имеет принципиальное значение [13], [5], [12], [15], аналитические оценки равномерности являются одним из главных критериев, принимаемых в расчет при выборе генератора [3], [14], так как позволяют для определенных классов функций «предсказать» погрешность численного интегрирования.

Генератор LFSR-CNS, предложенный в [1], является естественно многомерным генератором, позволяющим генерацию естественно многомерных последовательностей точек. Данный генератор был исследован экспериментально в ряде работ [2], [6]. В данной работе описывается метод аналитического исследования «качества равномерности», генерируемой последовательности на неполном периоде генератора.

1. Схема генерации LFSR-CNS

Введем необходимые обозначения.

Определение 1. Рассмотрим конечное поле $\mathbf{GF}(q)$ из q элементов (q - простое). Последовательность $\{y(n)\}$, удовлетворяющая линейному рекуррентному соотношению порядка s:

$$y(n) = -b_{s-1}y(n-1) - \ldots - b_0 y(n-s) \in \mathbf{GF}(q), \qquad (1)$$

где $b_0,\ldots,b_{s-1} \in \mathbf{GF}(q), \quad b_0 \neq 0,$

$$\vec{Y}(n) = (y(n),\ldots,y(n+s-1)),$$

называется линейной рекуррентной последовательностью.

Определение 2. Последовательность

$$\{\vec{Y}(n)\} = \{\vec{Y}(0),\vec{Y}(1),\ldots\}, \qquad (2)$$

называется «*гусеницей последовательности* (1)»

Последовательность (2) может быть записана в матричном виде

$$\vec{Y}(n) = [\mathbf{G}^n\vec{Y}(0)]_{\mathbf{GF}(q)},$$

где все арифметические операции выполняются в поле $\mathbf{GF}(q)$, матрица $\mathbf{G} \in \mathbf{GF}(q)$ - сопровождающая матрица характеристического многочлена [10] рекуррентного соотношения (1).

Замечание 1. Для удобства вычислений, считаем, что $\vec{Y}(n) \in [0,q)^s \cap \mathbb{Z}^s$, причем соответствие между элементами $\mathbf{GF}(q)$ и первыми q целыми неотрицательными числами: установлено «тривиально»: $0_{\mathbf{GF}(q)} \to 0_{\mathbb{R}}$, $1_{\mathbf{GF}(q)} \to 1_{\mathbb{R}}$, …, $(q-1)_{\mathbf{GF}(q)} \to (q-1)_{\mathbb{R}}$.

***Определение 3* [*10*].** Последовательность (1) максимального периода q^s-1 называется m-последовательностью.

Справедливы следующие леммы.

***Лемма 1* [*10*].** Период гусеницы m-последовательности периода q^s-1 также равен q^s-1.

***Лемма 2* [*4*].** Пусть $y(n)$ - рекуррентная функция (8.7) в поле $\mathbf{GF}(q)$ с ненулевыми начальными значениями $\vec{Y}(0) = (y(0),\ldots,y(s-1))$ и периодом, равным q^s-1, Ψ - неглавный характер [10] аддитивной группы поля $\mathbf{GF}(q)$. Пусть далее $S_\tau(N)$ задано соотношением:

$$S_\tau(N) = \sum_{n=0}^{N-1}\Psi\big(y(n)\big)\exp\left\{\frac{2\pi i}{T}\tau n\right\}, \quad N \le T.$$

Тогда справедливы оценки:

$$\left|S_\tau(N)\right| \le \begin{cases} p^{\frac{s}{2}}, & \text{при } N = T; \\ p^{\frac{s}{2}}\big(1+s\ln p\big), & \text{при } N < T, \tau = 0. \end{cases} \qquad (3)$$

***Определение 4* [*7*].** Пусть $\mathbf{M} \in \mathbb{Z}^{k\times k}$ - матрица, все собственные числа которой больше единицы по абсолютной величине.

Пусть далее множество D представляет собой полную систему вычетов $(\operatorname{mod}\mathbf{M})$, содержащую нуль.

$$\mathbb{Z}^n \supseteq D =$$
$$= \{a\vec{e} \mid e = (1,0,0,\ldots,0) \in \mathbb{Z}^n, a = 0,1,\ldots,q-1\}.$$

Пара $(\mathbf{M}, D)$ называется канонической системой счисления (КСС) в $\mathbb{Z}^k$, если для каждого элемента $\vec{z} \in \mathbb{Z}^k$ существует единственное представление вида

$$\vec{z} = \sum_{j=0}^{l(\vec{z})} \mathbf{M}^j \vec{a}_j \text{, где } \vec{a}_j \in D. \tag{5}$$

Матрица $\mathbf{M}$ называется основанием КСС, множество D - множеством цифр.

Таким образом, каждому элементу $\vec{z} \in \mathbb{Z}^k$ с использованием КСС ставится в соответствие вектор цифр

$$(\zeta_0, \zeta_1, \zeta_2, ...) ,\ \vec{a}_j = \zeta_j \vec{e} \in D. \tag{6}$$

Для любого $k \geq 2$ q-ичные канонические системы счисления существуют [7]-[9].

Схема генератора LFSR-CNS состоит из 2-х этапов.

Этап 1. Выберем рекуррентное соотношение (1), порядка $s = tk$, $t \in \mathbb{N}$, $k -$ требуемая размерность генератора, порождающее m-последовательность и ненулевые начальные условия $\vec{Y}(0) \neq (0,0,...,0)$. Вычислим элементы $\vec{Y}(n)$, $n = 0,1,2,...$ последовательности-гусеницы (2), соответствующей выбранной рекуррентной последовательности. Векторы $\vec{Y}(n) \in \mathbb{Z}^s$ (см. Замечание 1) называются состояниями генератора LFSR-CNS.

Этап 2. Выберем в $\mathbb{Z}^k$ q-ичную каноническую систему счисления $(\mathbf{M}, D)$.

Каждое состояние $\vec{Y}(n)$ генератора LFSR-CNS интерпретируем как вектор цифр (6) представления элемента $\mathbb{Z}^k$ в q-ичной канонической системе счисления.

$$\tilde{u}_i = \sum_{j=0}^{s-1} \vec{Y}(i)_j (\mathbf{M}^j \vec{e}) = \tilde{\mathbf{H}}[\mathbf{G}^i \vec{Y}(0)]_{\mathbf{GF}(q)}, \tag{7}$$

где $\tilde{\mathbf{H}} \in \mathbb{Z}^{k \times s}$, $\tilde{\mathbf{H}} = (\mathbf{M}^0 \vec{e}, \mathbf{M}^1 \vec{e}, ..., \mathbf{M}^{s-1} \vec{e})$.

Таким образом, согласно (7), каждому вектору состояния (2) $\vec{Y}(i)$ поставлен в соответствие элемент $\tilde{u}_i \in \mathbb{Z}^k$.

Заметим, что вследствие единственности представления (5), различным состояниям генератора $\vec{Y}(i)$ соответствуют различные элементы $\tilde{u}_i \in \mathbb{Z}^k$.

2. Показатели качества равномерности многомерной последовательности на выходе генератора псевдо-случайных точек

Для большинства приложений, использующих псевдослучайные последовательности и множества точек, предполагается [12], [3], [14], что элементы рассматриваемой последовательности принадлежат единичному кубу $\overline{I}^k = \prod_{j=0}^{k-1} [0,1)$.

«Качество равномерности» распределения последовательности точек единичного куба оценивается с использованием большого количества [3], [12] различных критериев, называемых отклонениями.

Определение 5. Рассмотрим множество S точек единичного куба $S = \{\vec{x}_1, \vec{x}_2, ..., \vec{x}_P\}$, $x_i \in \overline{I}^k$.

Для произвольного подмножества B единичного куба $\overline{I}^k$ определим величину

$$N(B;S) = \sum_{n=1}^{N} c_B(\vec{x}_n),\ c_B(\vec{x}) = \begin{cases} 1, & \vec{x} \in B; \\ 0, & \vec{x} \notin B. \end{cases}$$

Если Ξ - непустое семейство измеримых по Лебегу подмножеств $\overline{I}^k$, тогда отклонение (в общем случае) определяется соотношением:

$$D_N(\Xi; P) = \sup_{B \in \Xi} \left| \frac{N(B;S)}{P} - \lambda_k(B) \right|, \tag{8}$$

где λ_k - k-мерная мера Лебега в $\mathbb{R}^k$.

Наиболее часто используются [3], [11], [12] отклонения $D_P(S)$, $D_P^*(S)$, задаваемые соотношениями

$$D_P(S) = D_P(\mathrm{I}; S) \text{, где } \mathrm{I} = \left\{ B \mid B = \prod\nolimits_{j=0}^{k-1} [u_j, v_j) \right\} \tag{9}$$

$$D_P^*(S) = D_P(\mathrm{I}^*; S) \text{, где } I^* = \left\{ B \mid B = \prod\nolimits_{j=0}^{k-1} [0, u_j) \right\} \tag{10}$$

В данной работе, мы будем рассматривать аналог $D_P^*(S)$.

3. Особенности фундаментальной области генератора LFSR-CNS. Аналог $D_P^*(S)$

***Определение 6* [2].** Назовем *фундаментальной областью U генератора* LFSR-CNS множество точек $\mathbb{Z}^k$, соответствующих всем возможным состояниям генератора (2), дополненное точкой $\vec{0} = (0,0,...,0)$.

На рис. 1. приведен пример фундаментальной области генератора LFSR-CNS, соответствующей одной из КСС в трехмерном пространстве.

Так как множество точек на выходе генератора LFSR-CNS представляет собой нерегулярную, «фрактальную» область в $\mathbb{Z}^k$, для оценки качества равномерности генерируемой последовательности, неприменимы определения отклонения (9) и (10).

Определим аналог отклонения (10), ассоциированный с аналогом многомерного куба $\overline{I}^k$, в качестве которого выступает множество, называемое фундаментальной областью канонической системы счисления. Фундаментальная область генератора LFSR-CNS тесно связана с фундаментальной областью используемой КСС.

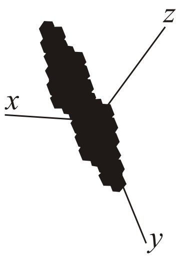

Рис. 1. Пример фундаментальной области

В силу свойств канонических систем счисления [7], если в $\mathbb{Z}^k$ задана система счисления $(\mathbf{M}, D)$, любой элемент $\vec{z} \in \mathbb{R}^k$ представим в виде:

$$\vec{z} = \vec{\rho} + \vec{\sigma}; \vec{\rho} = \sum_{j=0}^{h(z)} \mathbf{M}^j \vec{a}_j; \qquad \vec{\sigma} = \sum_{j=1}^{\infty} \mathbf{M}^{-j} \vec{a}_{-j}, \ \vec{a}_j \in D. \tag{12}$$

Слагаемое $\vec{\rho}$ в сумме (12) назовем регулярной частью $\vec{z}$, слагаемое $\vec{\sigma}$ – сингулярной.

***Определение 7* [7].** Множество всех точек

$$F = \left[\sum_{j \geq 1} \mathbf{M}^{-j} \vec{a}_j \mid \vec{a}_j \in D \right] \subseteq \mathbb{R}^k, \tag{13}$$

называется фундаментальной областью канонической системы счисления.

Из определений 6, 7, а также схемы генератора LFSR-CNS следует, что

$$U \subseteq \mathbf{M}^s F. \tag{14}$$

Замечание. Фундаментальная область F канонической системы счисления является аналогом отрезка $[0,1)$, если вместо сингулярных частей $\vec{\sigma}$ в КСС-представлении элементов $\mathbb{R}^k$ рассматривать представление дробной части чисел в традиционных системах счисления. Можно также считать, что область F^k является аналогом многомерного единичного куба $[0,1)^k$.

Следуя подходу работы [4], определим на фундаментальности области системы счисления F меру, аналогичную мере Лебега, для отрезка $[0,1)$.

***Определение 8*.** Множество чисел

$$\Theta = \left\{ \vec{z} \mid \vec{z} = \sum_{j=1}^{n} \mathbf{M}^{-j} \vec{a}_j + \sum_{j=n+1}^{\infty} \mathbf{M}^{-j} \vec{a}_j \right\},$$

где $\vec{a}_j \in D$, у которых первые n цифр фиксированы, назовем *элементарно-цилиндрическим множеством*. Конечное объединение элементарно-цилиндрических множеств назовем *цилиндрическим множеством*.

Цилиндрические множества образуют алгебру и любое цилиндрическое множество есть объединение конечного числа непересекающихся элементарно-цилиндрических множеств.

Положим значение меры на элементарно-цилиндрическом множестве Θ, у которого фиксированы первые n цифр равным

$$\hat{\mu}(\Theta) = q^{-n}, \ \operatorname{card} D = |\det \mathbf{M}| = q.$$

Меру цилиндрического множества определим как сумму мер непересекающихся элементарно-цилиндрических множеств, его составляющих.

По известной теореме теории меры, введенная выше мера $\hat{\mu}$ однозначно продолжается на наименьшую σ-алгебру, содержащую алгебру цилиндрических множеств и порождает на этой алгебре меру μ.

На множестве элементов фундаментальной области F введем *лексикографический порядок.*

Определение 9. Пусть $\vec{h}, \vec{z} \in F$

$$\vec{z} = \sum_{j=1}^{\infty} \mathbf{M}^{-j} z_j \vec{e}, \quad \vec{h} = \sum_{j=1}^{\infty} \mathbf{M}^{-j} h_j \vec{e}.$$

Будем говорить, что элемент $\vec{h}$ *предшествует* элементу $\vec{z}$, и обозначим $\vec{h} \prec \vec{z}$, если существует такое целое $n \geq 1$, что выполняются соотношения:

$$h_1 = z_1, ..., h_{n-1} = z_{n-1}; \quad h_{n-1} < z_{n-1}.$$

Определение 10. Множество всех предшественников элемента $\vec{z}$ будем называть *углом* Γ, а элемент $\vec{z}$ - *вершиной угла.*

$$\Gamma_{\vec{z}} = \{\vec{h} \mid \vec{h} \prec \vec{z}\}$$

Для угла Γ с вершиной $\vec{z}$ через Γ_n будем обозначать угол с вершиной

$$\vec{z}^{(n)} = \sum_{j=1}^{n} \mathbf{M} z_j \vec{e}.$$

Определение 11. Аналогично (10), для множества $S \subseteq F$ определим КСС-отклонение следующим образом.

$$D_P^{CNS}(S) = \sup_{\Gamma \in I^{CNS}} \left| \frac{N(\Gamma; S)}{P} - \mu(\Gamma) \right|, \tag{15}$$

где I^{CNS} - множество всех углов отвечающих рассматриваемой КСС.

4. Основная теорема

Проведем анализ равномерности последовательности на неполном периоде выхода генератора LFSR-CNS. Заметим, что анализ равномерности на полном периоде представляет собой несложное упражнение по комбинаторике.

Рассмотрим множество S в (15) на выходе генератора LFSR-CNS на участке периода генератора $P < T = q^s - 1$, масштабированное в фундаментальную область F используемой канонической системы счисления.

$$S = \left\{ \tilde{s}_i \mid \tilde{s}_i = \mathbf{M}^{-s} \sum_{j=0}^{s-1} Y(i)_j (\mathbf{M}^j \vec{e}) \right\} \qquad (16)$$

Теорема. Справедлива следующая асимптотическая оценка КСС отклонения для последовательности на выходе генератора LFSR-CNS.

$$D_P^{CNS}(S) = O\left(\frac{s^2 \sqrt{T}}{P} \right).$$

Доказательство.

Рассмотрим произвольный угол Γ с вершиной

$$\vec{z} = \sum_{j \ge 1} z_j \mathbf{M}^{-j} \vec{e}\ .$$

Покажем, что

$$N(\Gamma; S) = \mu(\Gamma) P + O\left(s^2 q^{s/2} \right).$$

Пусть для $\alpha \in \{0,1,...,q-1\}$ функция $\delta_q(\alpha)$ определена равенством:

$$\delta_q(\alpha) = \begin{cases} 1, \text{ при } a = 0 \\ 0, \text{ при } a \ne 0 \end{cases} = q^{-1} \sum_{g \in \mathbf{GF}(q)} \Omega(ag)\ ,$$

где Ω - характер [10], [4] аддитивной группы поля $\mathbf{GF}(q)$, $\mathbb{Z} \ni \alpha \leftrightarrow a \in \mathbf{GF}(q)$ в соответствии с Замечанием 1. Ниже данное отображение будет подразумеваться.

Пусть далее символ $\sum_{\mathrm{B}_s}$ означает суммирование по всем тем $b_1,...,b_s \in \{0,1,...,q-1\}$, для которых

$$\left(\sum_{j=1}^{s} \mathbf{M}^{-j} b_j \vec{e} \right) \prec \left(\sum_{j=1}^{s} \mathbf{M}^{-j} z_j \vec{e} \right),$$

то есть, по всем элементам угла Γ_s с вершиной $\sum_{j=1}^{s} \mathbf{M}^{-j} z_j \vec{e}$. Тогда имеем:

$$N_\Gamma(P) = \sum_{\mathrm{B}_s} \sum_{t=0}^{P-1} \delta_q\left(y(t+s-1) - b_1 \right) \ldots \delta_q\left(y(t) - b_s \right) + O(1). \qquad (17)$$

На основании свойств характеров аддитивных групп конечного поля сумму в (17) можно переписать в виде:

$$\sum_{\mathrm{B}_s} \sum_{t=0}^{P-1} \delta_q\left(y(t+s-1) - b_1 \right) \ldots \delta_q\left(y(t) - b_s \right) =$$
$$= \sum_{\mathrm{B}_s} \sum_{t=0}^{P-1} \left(\sum_{a_1 \in \mathbf{GF}(q)} \Omega\left(a_1 \left(y(t+s-1) - b_1 \right) \right) \ldots \right.$$
$$\left. \ldots \sum_{a_s \in \mathbf{GF}(q)} \Omega\left(a_s \left(y(t) - b_s \right) \right) \right).$$

Выделяя слагаемое с $a_1 = ... = a_s = 0 \in \mathbf{GF}(q)$, получаем

$$N(\Gamma; S) = \mu(\Gamma_s) P + R + O(1), \qquad (18)$$

где

$$R = q^{-s} \sum_{a_1,...,a_s \in \mathbf{GF}(q)}^{(*)} \left(\sum_{\mathrm{B}_s} \Omega(-a_1 b_1) \ldots \Omega(-a_s b_s) \cdot \right.$$
$$\left. \cdot \sum_{t=0}^{P-1} \Omega\left(a_1 y(t+s-1) \right) \ldots \Omega\left(a_s y(t) \right) \right) =$$
$$= q^{-s} \sum_{a_1,...,a_s \in \mathbf{GF}(q)}^{(*)} \left(\sum_{\mathrm{B}_s} \Omega(-a_1 b_1) \ldots \Omega(-a_s b_s) \cdot \right.$$
$$\left. \cdot \sum_{t=0}^{P-1} \Omega\left(a_1 y(t+s-1) + ... + a_s y(t) \right) \right). \qquad (19)$$

В последнем равенстве знак (*) в суммировании означает пропуск слагаемого с $a_1 = ... = a_s = 0 \in \mathbf{GF}(q)$. Заметим, что условие включения углов $\mathrm{B}_s \subset \Gamma_s$ равносильно системе условий

$$\begin{cases} b_1 = z_1, ..., b_{j-1} = z_{j-1}, b_j < z_j \\ j = 1, 2, ..., s. \end{cases} \qquad (20)$$

Поэтому

$$\left| \sum_{\mathrm{B}_s} \Omega(-a_1 b_1) \ldots \Omega(-a_s b_s) \right| =$$
$$= \left| \sum_{j=1}^{s} \sum_{b_j=0}^{z_j - 1} \Omega(a_j b_j) \sum_{b_{j+1},...,b_s \in \mathbf{GF}(q)} \Omega(a_{j+1} b_{j+1}) \ldots \Omega(a_s b_s) \right| =$$
$$= \left| \sum_{j=1}^{s} q^{s-j} \sum_{b_j=0}^{z_j - 1} \Omega(a_j b_j) \delta_q(a_{j+1}) \ldots \delta_q(a_s) \right| \le$$
$$\le q^{s+1} \left| \sum_{j=1}^{s} q^{-j} \delta_q(a_{j+1}) \ldots \delta_q(a_s) \right|.$$

Но тогда из (19) следует, что

$$|R| \le q^{-s} \sum_{a_1,...,a_s \in \mathbf{GF}(q)}^{(*)} \sum_{j=1}^{s} q^{-j} \delta_q(a_{j+1}) \ldots \delta_q(a_s) \cdot$$
$$\cdot \left| \sum_{t=0}^{P-1} \Omega(a_1 y(t+s-1) + ... + a_s y(t)) \right| \Big)$$
$$= \sum_{j=1}^{s} q^{1-j} \sum_{a_1,...,a_s \in \mathbf{GF}(q)}^{(*)} \left| \sum_{t=0}^{P-1} \Omega\left(a_1 y(t+s+1) + ... + a_s y(t) \right) \right|. \qquad (21)$$

Так как при всех $(a_1,...,a_s) \ne (0,...,0)$ функция $\phi(t) = a_1 y(t+s-1) + ... + a_{s-1} y(t+1) + a_s y(t)$ удовлетворяет линейному рекуррентному соотношению порядка s (см. [10]) порождающему m-последовательность, то при всех $(a_1,...,a_s) \ne (0,...,0)$ является m-последовательностью.

Поэтому, согласно Лемме 2, справедливо неравенство

$$\left| \sum_{t=0}^{P-1} \Omega\left(a_1 y(t+s-1) + ... + a_s y(t) \right) \right| \le$$
$$\le q^{s/2} (1 + s \ln q),$$

а, следовательно, и неравенство

$$\left|R\right| \le \sum_{j=1}^{s} q^{1-j} \sum_{a_1,\dots,a_s \in \mathbf{GF}(q)}^{(*)} q^{s/2}\left(1+s\ln q\right) = O\left(s^2 q^{s/2}\right).$$

Пользуясь последней оценкой, получаем

$$N(\Gamma;S;) = \mu\left(\Gamma_k\right)P + O\left(s^2 q^{s/2}\right), \tag{22}$$

а с учетом $\mu\left(\Gamma\right)P = \mu\left(\Gamma_s\right)P + O\left(q^{-s}\right)$, $T = q^s - 1$ - в форме

$$N(\Gamma;S) = \mu\left(\Gamma\right)P + O\left(s^2\sqrt{T}\right). \tag{23}$$

Из (23) и определения $D^{CNS}(S)$ следует, что

$$D_P^{CNS}(S) = O\left(\frac{s^2\sqrt{T}}{P}\right).$$

Теорема доказана.

Заключение

В данной работе предложен метод аналитической оценки качества равномерного распределения на выходе генератора LFSR-CNS, дополняющий эмпирические тесты генератора, рассмотренные в [1], [2], [6].

Заметим, несмотря на то, что в формулировке основной теоремы указано ограничение $P < T$, предлагаемые оценки приведены в асимптотической форме. Получение явного выражения для констант в используемых асимптотических выражениях $O(\cdot)$ представляет собой предмет дальнейшего исследования.

Благодарности

Работа выполнена при поддержке Российского фонда фундаментальных исследований (гранты №06-01-00722 и №07-07-97603-р_офи).

Литература

1. Калугин А.Н. Модификация многомерных псевдослучайных последовательностей с использованием пары двойственных LFSR-CNS генераторов // Компьютерная оптика - 2006. - №28.
2. Калугин А.Н. Трехмерное обобщение генератора LFSR случайных точек // Компьютерная оптика.- 2005. - №27. – С. 131-134.
3. Кейперс Л., Нидеррейтер Г. Равномерное распределение последовательностей. – М.: Наука, Гл. ред. физ.-мат. лит. 1985. – 408 с.
4. Chernov V.M. Fast uniform distribution of sequences for fractal sets // Proceedings of International Conference on Computer Vision and Graphics, 2004. September 22-24, 2004, Warsaw, Poland, Computational IMAGING AND VISION SERIES, Kluwer Academic Press.
5. Ferrenberg A.M., Landau D.P. and Wong Y.J. Monte Carlo simulations: Hidden errors from "good" random number generators // Phys. Rev. Lett. 69. P. 3382 (1992).
6. Kalouguine A.N., Chernov V.M. 3D generalization for LFSR random point Generator // Proceedings of the Second IASTED Int. Multi-Conference "Signal and Image Processing" June 20-24, 2005, Novosibirsk, Russia. 2005. P. 122-125.
7. Kátai I. Generalized Number Systems in Euclidean Spaces // Mathematical and Computer Modeling. 38. 2003. P. 883-892.
8. Kovács A., Generalized binary number systems, Annales Univ. Sci. Budapest, Sect. Comp. 20. 2001. P.195-206.
9. Kovács A. On number expansions in lattices, Proc. 5th International Conference on Applied Informatics, Eger, Hungary, 2001.
10. Lidl R., Niederreiter H., Finite Fields (Addison-Wesley, Reading, Massachussets, 1983).
11. Niederreiter H. Random Number Generation and Quasi-Monte Carlo Methods, volume 63 of SIAM CBMS-NF Regional Conference Series in Applied Mathematics. SIAM, Philadelphia, 1992.
12. Random and Quasi-Random Point Sets, P. Hellekalek, G. Larcher, Eds, Lecture notes in statistics, 138, Springer, 1998.
13. Vattulainen I. Framework for testing random numbers in parallel calculations // Phys. Rev. E. 59. **6**. P.7200 (1999).
14. Coddington P. Random Number Generators for Parallel Computers, NHSE Review, Second Issue, Northeast Parallel Architectures Center, 1996 . [http://nhse.cs.rice.edu/NHSEreview/RNG/].
15. Hellekalek P. Don’t trust parallel Monte-Carlo. [http://random.mat.sbg.ac.at/].

AN LSFR-CNS GENERATOR: ANALYTICAL STUDY OF DISTRIBUTION UNIFORMITY

A.N. Kalouguine[1,2]
[1]*Image Processing Systems Institute of the RAS, Samara, Russia,*
[2]*Samara State Aerospace University (SSAU), Samara, Russia*

Abstract:

This paper proposes a method of quality analytical study of distribution uniformity of a multidimensional pseudorandom sequence at outlet of an LFSR-CNS generator. Asymptotic estimates are given to deviation of generated distribution from uniform distribution in off-peak period of the generator.
Keywords: distribution uniformity, asymptotic estimates, pseudorandom sequence generator
Citation: Kalouguine AN. An LSFR-CNS generator: analytic study of distribution uniformity [In Russian]. Computer Optics 2007; 31(1): 58-62.
Acknowledgements: The work was supported by the Russian Foundation for Basic Research (grants No. 06-01-00722 and No. 07-07-97603-r_ofi).

References:

[1] Kalouguine AN. Modification of multidimensional pseudorandom sequences using a pair of dual LFSR-CNS generators [In Russian]. Computer Optics 2006; 28: 112-118.
[2] Kalouguine AN. 3D generalization for the LFSR random point generator [In Russian]. Computer Optics 2005; 27: 131-134.
[3] Kuipers L, Niederreiter H. Uniform distribution of sequences [Russian translation]. Moscow: “Nauka” Publisher, 1985: 408 p.
[4] Chernov VM. Fast uniform distribution of sequences for fractal sets. Proceedings of International Conference on Computer Vision and Graphics. Warsaw, Poland, Computational Imaging And Vision Series, Kluwer Academic Press, 2004.
[5] Ferrenberg AM, Landau DP, Wong YJ. Monte Carlo simulations: Hidden errors from "good" random number generators. Phys. Rev. Lett. 1992; 69: 3382.
[6] Kalouguine AN, Chernov VM. 3D generalization for LFSR random point Generator. Proceedings of the Second IASTED Int. Multi-Conference "Signal and Image Processing" June 20-24. Novosibirsk, Russia, 2005; 122-125.
[7] Kátai I. Generalized Number Systems in Euclidean Spaces. Mathematical and Computer Modeling 2003; 38: 883- 892.
[8] Kovács A. Generalized binary number systems. Annales Univ. Sci. Budapest, Sect. Comp. 2001; 20: 195-206.
[9] Kovács A. On number expansions in lattices, Proc. 5th Internation Conference on Applied Informatics, Eger, Hungary, 2001.
[10] Lidl R, Niederreiter H. Finite Fields. Addison-Wesley, Reading, Massachussets, 1983.
[11] Niederreiter H. Random Number Generation and Quasi Monte Carlo Methods. SIAM CBMS-NF Regional Conference Series in Applied Mathematics. SIAM, Philadelphia, 1992.
[12] Hellekalek P, Larcher G. Random and Quasi-Random Point Sets. Lecture notes in statistics 1998; 138.
[13] Vattulainen I. Framework for testing random numbers in parallel calculations. Phys. Rev. E 1999; 59(6): 7200.
[14] Coddington P. Random Number Generators for Parallel Computers. NHSE Review, Second Issue, Northeast Parallel Architectures Center, 1996. http://nhse.cs.rice.edu/ NHSEreview/RNG/.
[15] Hellekalek P. Don’t trust parallel Monte-Carlo. http://random.mat.sbg.ac.at/