# МОДИФИКАЦИЯ МНОГОМЕРНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ИСПОЛЬЗОВАНИЕМ ДВОЙСТВЕННЫХ LFSR-CNS ГЕНЕРАТОРОВ

*А.Н. Калугин*

*Институт систем обработки изображений РАН*
*Самарский государственный аэрокосмический университет имени академика С.П. Королева*

***Аннотация***

В работе рассматривается новый метод модификации многомерной псевдослучайной последовательности точек, основанный на использовании пары двойственных генераторов LFSR-CNS. Состояние генератора, восстановленное по элементу многомерной последовательности, интерпретируется как состояние двойственного генератора, что позволяет сгенерировать точку, отличную от точки исходной последовательности. Приводятся сравнительные результаты исследования исходной и модифицированной последовательности с использованием взвешенного спектрального критерия.

## *Введение*

Большинство современных методов решения задач статистической физики определенным образом используют методы Монте-Карло. Методы Монте-Карло при решении многомерных задач (физические задачи являются исходно многомерными), требуют формирования множества многомерных случайных (или псевдослучайных, квазислучайных) точек.

Для формирования многомерной псевдослучайной последовательности за редким исключением [1], [2], в большинстве случае используются последовательности случайных чисел (одна или несколько), которые [3], [4], [5] распределяются по координатам выходной многомерной последовательности. Такие методы «увеличения размерности» основаны как на разбиении одномерной псевдослучайной последовательности, так и использовании нескольких одномерных генераторов различных типов или одного типа с различными параметрами.

Иногда использование методов «увеличения размерности» одномерной последовательности обусловлено необходимостью (в виду специфики задачи или метода ее решения) использования параллельных алгоритмов обработки данных, а, следовательно, именно параллельных версий генераторов случайных точек. Однако для ряда задач [6] требуется именно многомерная последовательность псевдослучайных точек, а не параллельный способ ее формирования.

Известно [7], [8], [9], что метод «увеличения размерности» псевдослучайной последовательности чисел может привести к нежелательным результатам, а именно: к потере случайного характера итоговой последовательности, к несоответствию распределения элементов итоговой последовательности требуемому.

В данной работе предлагается схема модификации многомерной псевдослучайной последовательности, полученной методом «увеличения размерности», в целях улучшения ее многомерных свойств, основанная на использование пары двойственных LFSR-CNS генераторов. С использованием взвешенного спектрального критерия проводится анализ применимости предложенной схемы (сравнение свойств исходной и модифицированной последовательностей) на примере многомерной версии генератора Randu.

## *Предварительные сведения. Генератор LFSR-CNS*

Генератор LFSR-CNS [2] основан на использовании линейных рекуррентных последовательностей в конечных полях канонических систем счисления в решетках. Приведем основные положения этих теорий.

Пусть есть конечное поле из $q = p^s$ элементов, $p-$ простое число. Функцию, являющуюся решением линейного рекуррентного соотношения

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

где

$$b_0, \ldots, b_{s-1} \in \mathbf{GF}(q),\ b_0 \neq 0,\ \mathbf{Y} = (y(0), \ldots, y(s-1)),$$

будем называть линейной рекуррентной последовательностью порядка $s$ (или, для краткости, рекуррентной функцией) с начальными условиями (значениями) $\mathbf{Y} = (y(0), \ldots, y(s-1))$.

Рекуррентная последовательность (1) с максимально возможным периодом, равным $T = q^s - 1$, называется $m$-последовательностью (см. [10]).

Последовательность $\{\vec{Y}(n)\} = \{\vec{Y}(0), \vec{Y}(1), \ldots\}$, где

$$\vec{Y}(i) = (y(i), y(i+1), \ldots, y(i+s-1))^T \qquad (2)$$

называется *«гусеницей последовательности* (1)»

Заметим, что последовательность (2) может быть записана в матричном виде:

$$\vec{Y}(i) = [\mathbf{G}^i \vec{Y}(0)]_{\mathbf{GF}(q)} \qquad (3)$$

где все арифметические операции выполняются в поле $\mathbf{GF}(q)$.

Матрица $\mathbf{G} \in \mathbf{GF}(q)^{s \times s}$ – матрица Фробениуса, сопровождающая матрица [11] характеристического многочлена рекуррентной функции рекуррентного соотношения (1).

Пусть, далее, $\{\vec{a}_0, \vec{a}_1, \ldots, \vec{a}_{k-1}\}$ – множество линейно независимых векторов пространства $\mathbb{R}^k$. Линей-

ная оболочка с целыми коэффициентами $\Lambda$ векторов $\{\vec{a}_0,\vec{a}_1,...,\vec{a}_{k-1}\}$ называется решеткой (lattice) в $\mathbb{R}^k$ с базисом $\mathbf{a}=\{\vec{a}_0,\vec{a}_1,...,\vec{a}_{k-1}\}$.

$$\Lambda=\{\vec{\xi}\mid\vec{\xi}=\xi_0\vec{a}_0+\xi_1\vec{a}_1+...+\xi_{k-1}\vec{a}_{k-1}\},\qquad(4)$$

где $\xi_i\in\mathbb{Z}$, $i=0,1,...,k-1$.

Пусть, далее, $M$ – вложение

$M:\Lambda\to\Lambda$, $\det(M)\neq 0$,

и множество $D$ – конечное подмножество $\Lambda$, $D\subset\Lambda$, $0\in D$.

Тройка объектов $(\Lambda,M,D)$ называется *системой счисления* [12] (или, иначе, тройка $(\Lambda,M,D)$ обладает свойством *единственности представления*), если для любого элемента $\vec{\xi}\in\Lambda$ существует единственное представление

$$\vec{\xi}=\sum_{i=0}^{l(\vec{\xi})}M^i\left(\vec{a}_i\right),\qquad(5)$$

где $\vec{a}_i\in D$ и

$$l(\vec{\xi})=\max_i(\vec{a}_i\neq\vec{0}),\ l(\vec{\xi})<\infty.\qquad(6)$$

В этом случае, вложение $M$ называется *основанием системы счисления,* а $D$ *– множеством цифр.*

Далее, в качестве решетки $\Lambda$, будем рассматривать решетку $\Lambda=\mathbb{Z}^k$.

Система счисления $(\mathbb{Z}^k,M,D)$ называется канонической, если $D$ образует полную систему вычетов по модулю $M$ и

$$D=\{v\vec{e}_0,v=0,1,...,\left|\det M\right|-1\},\qquad(7)$$

где $\vec{e}_0=1\cdot\vec{a}_0+0\cdot\vec{a}_1+...+0\cdot\vec{a}_{k-1}$; $\mathbf{a}=(\vec{a}_0,\vec{a}_1,...,\vec{a}_{k-1})$ - базис $\mathbb{Z}^k$.

Если $(\mathbb{Z}^k,M,D)$ – каноническая система счисления, то для любого $\zeta\in\mathbb{Z}^k$ существует единственное представление в виде

$$\zeta=\sum_{i=0}^{l}\zeta_i\left(M^i\left(\vec{e}_0\right)\right),\ \zeta_i\in\{0,1,...,|\det M|-1\}.\qquad(8)$$

Вложения $M$ могут быть сконструированы различным способом. Рассмотрим канонические системы счисления, порождаемые многочленами с целыми коэффициентам. Рассмотрим многочлен

$$f(x)=c_kx^k+c_{k-1}x^{k-1}+...+c_0,\qquad(9)$$

где $c_k\in\mathbb{Z}$, $c_k=1$.

В работе [13] показано, что для многочленов

$$f_1=x^k+c_1x+q,\qquad(10)$$

где $-1\le c_1\le q-2$ $q\ge 2$, $q=p$;

$$f_2=x^k+px^{k-1}+px^{k-2}+...+px+p,\qquad(11)$$

где

$2\le p\in\mathbb{N}$, $q=p$.

тройка $(\mathbb{Z}^k,M_f,D)$, где $D=\{0,1,...,q-1\}$, а $M_f$ – вложение, имеющее в стандартном базисе решетки $\mathbb{Z}^k$ вид сопровождающей матрицы многочлена (9) $f$

$$\mathbf{M}_f=\begin{pmatrix}0&\dots&&-c_0\\1&0&\dots&\vdots\\0&\ddots&&\\\vdots&&&\\0&\dots&1&-c_{k-1}\end{pmatrix}.$$

Для $\mathbb{Z}^3$ многочлены (10), (11), порождающие бинарные канонические системы счисления имеют вид:

$$g_1=2+x^3,\qquad(12)$$

$$g_2=2+2x+2x^2+2x^3.\qquad(13)$$

Общая схема генератора LFSR-CNS может быть записана в следующем виде:

**Этап 1**. **Формирование гусеницы.** Генерация «гусеницы» (2) последовательности (1). Используется $m$-последовательность, заданная линейным рекуррентным соотношением (1) в конечном поле из $q$ элементов $\mathbf{GF}(q)$

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

с ненулевыми начальными условиями $\vec{Y}(0)$. Вектор $\vec{Y}(i)$ в данном случае называется вектором состояния генератора.

**Этап 2. Формирование многомерной точки.** Векторы $Y(i)$ (2) рассматриваются как цифры записи некоторого числа в $q$-ичной канонической системе счисления.

$$\tilde{u}_i=\sum_{j=1}^{s}\vec{Y}(i)_{j-1}(\mathbf{M}^{j-1}e)=\tilde{\mathbf{H}}[\mathbf{G}^i\vec{Y}(0)]_{\mathbf{GF}(q)},\qquad(14)$$

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, 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 $\tilde{u}_i\in\mathbb{Z}^k$

Для удобства практического использования далее используются генераторы с рекуррентной функцией (1) порядка

$$s=tk,\ t\in\mathbb{N}.\qquad(15)$$

Генераторы LFSR-CNS, использующие одинаковую $m$-последовательность на первом этапе, но различные системы счисления на втором этапе будем называть двойственными.

**Этап 3. Унификация.** Заметим, что в общем случае множество $U$ точек $\tilde{u}_i \in \mathbb{Z}^k$, соответствующих всем возможным состояниям генератора $\vec{Y}(i)$, имеет сложную нерегулярную форму [14], [2], однако для многочленов (10) и (11) существует взаимно однозначное инъективное вложение $U$ в единичный куб $C^k = \left([0,1)\right)^k$

$$P : U \to C^k . \tag{16}$$

*Вложение $P$ называется унификацией фундаментальной области генератора.*

Пусть

$$\tilde{P}(\tilde{u})_i = u_i ,\ i = 0,1,...,k-1 , \tag{17}$$

и $\tilde{u}_i$ – наименьший неотрицательный вычет класса $u_i \pmod{q^t}$.

Тогда унификация (16) может быть записана в виде

$$P(\tilde{u}) = \frac{1}{q^t}\tilde{P}(\tilde{u}) .$$

Обозначив $\mathbb{F}_{q^t} = \mathbb{Z}/q^t\mathbb{Z}$, общая схема генератора LFSR-CNS может быть записана в виде

$$\tilde{u}_i = \frac{1}{q^t}\left[\tilde{\mathbf{H}}[\mathbf{G}^i\vec{Y}(0)]_{\mathbf{GF}(q)}\right]_{\left(\mathbb{F}_{q^t}\right)^k} . \tag{18}$$

### *Модификация существующих схем многомерной генерации*

Сопровождающая матрица многочлена $f_1$ при $q = 2$ имеет следующий вид:

$$\mathbf{M}_{f1} = \begin{pmatrix} 0 & \dots & & -2 \\ 1 & 0 & \dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & & \\ 0 & \dots & 1 & 0 \end{pmatrix}_{k\times k} . \tag{19}$$

***Лемма 1.*** Для матрицы $\mathbf{M}_{f1}$ (19) справедливо равенство

$$\mathbf{M}_{f1}^{kt+i}e = (-2)^t\mathbf{M}_{f1}^i e ,\ i = 0,1,...,k-1 .$$

***Доказательство.*** Нетрудно видеть, что единственным отличным от нуля главным минором (любого порядка) матрицы $\mathbf{M}_{f1}$ является ее определитель, таким образом

$$S_j = \begin{cases} 0, 1 \le j < k; \\ \det\mathbf{M}_{f1}, j = k, \end{cases} \tag{20}$$

где $S_j$ – сумма главных миноров матрицы $\mathbf{M}_{f1}$ $j$-го порядка.

Используя разложение по последнему столбцу, получаем:

$$\det\mathbf{M}_{f1} = (-1)^k \cdot 2 . \tag{21}$$

Характеристическое уравнение матрицы $\mathbf{M}_{f1}$

$$(-\lambda)^k + S_1(-\lambda)^{k-1} + S_2(-\lambda)^{k-2} + ...$$

$$+S_{k-1}(-\lambda) + S_k = 0$$

с учетом (20) и (21) примет вид:

$$(-\lambda)^k + (-1)^k \cdot 2 = 0 ,$$

или

$$\lambda^k = -2 . \tag{22}$$

Применяя теорему Гамильтона-Кэли [11], из (22) получаем

$$\left(\mathbf{M}_{f1}\right)^k = (-2)\cdot\mathbf{I}_k , \tag{23}$$

где $\mathbf{I}_k$ – единичная матрица порядка $k$.

Равенство (23) доказывает утверждение леммы. ■

Таким образом, точка на выходе LFSR-CNS генератора (без учета шага 3) может быть представлена в виде

$$\tilde{u}_i = \sum_{j=0}^{kt-1} Y(i)_j(\mathbf{M}^j e) =$$

$$= \sum_{j=0}^{k-1}(\mathbf{M}^j e)\sum_{l=0}^{t-1}(-2)^l Y(i)_{kl+j} . \tag{24}$$

Равенство (24) свидетельствует, что значения по каждой из координат в базисе $(\mathbf{M}^0 e, \mathbf{M}e, \mathbf{M}^2 e, ..., \mathbf{M}^{k-1}e)$ на выходе второго этапа генератора отвечающего многочлену $f_1$ ($q = 2$) генерируются независимо.

Также из (24) следует, что элементы последовательности $\mathrm{Пр}_j\,\tilde{u}_i$ по каждой из координат получены в результате интерпретации координат вектора состояния генератора, как цифр в представлении определенного целого числа в негабинарной системе счисления: элементы последовательности $\mathrm{Пр}_j\,\tilde{u}_i$ $j = 0,1,...,k-1$ – суть элементы множества $\Sigma$

$$\Sigma = \left\{ u \,\middle|\, u = \sum_{l=0}^{t-1}(-2)^l\sigma_l ,\ \forall\sigma \in \{0,1\}^t \right\}, \tag{25}$$

где $\Sigma$ – множество целых чисел, имеющих длину представления в «негабинарной» системе счисления, не превышающую $t$.

Негабинарная система счисления, система счисления с основанием $-2$ и цифрами $\{0,1\}$, была впервые предложена Витторио Грюнвальдом в его работе [15]. Возможность единственного представления любого целого числа в негабинарной системе счисления следует, например, из существования соответствующего многочлена $f + 2 = 0$ (многочлена

типа $f_1$), порождающего бинарную систему счисления. Интересной особенностью «негабинарной» системы счисления является возможность беззнакового представления всех целых чисел. Положительные целые числа имеют нечетную длину представления в негабинарной системе счисления, отрицательные целые числа – четную [16].

Заметим, что на шаге 3 процедуры генерирования LFSR-CNS $\Sigma^k$ отображается (взаимно однозначно) в куб $C^k$, более точно на декартову степень множества $\frac{1}{q^t}\left(\mathbb{Z}\cap[0,q^t)\right)$:

$$P:\mathbb{Z}^k\to\tilde{C}^k,\ \tilde{C}^k=\left[\frac{1}{q^t}\left(\mathbb{Z}\cap[0,q^t)\right)\right]^k$$

Вид множества (25) обуславливает возможность применения пары генераторов LFSR-CNS, отвечающих многочленам $f_1$ и $f_2$ для модификации существующих схем многомерной генерации.

### *Схема модификации многомерной последовательности*

**1. Исходные данные.** Пусть произвольный многомерный генератор (или многомерная версия произвольного одномерного генератора) производит точки последовательности $\{x(i)\}$ точек многомерного куба $\tilde{C}^k$, или, после соответствующего масштабирования, точки множества $\bar{C}^k=\left[\mathbb{Z}\cap[0,q^t)\right]^k$, $x(i)\in\bar{C}^k$.

В таком случае, проекция точки $x(i)$ на каждую из координат может быть представлена в виде ее разложения в традиционной бинарной системе счисления

$$\Pr_j x(i)=\sum_{l=0}^{t-1}2^l\sigma(i)_l^{(j)},\ \ \sigma(i)^{(j)}\in\{0,1\}^t. \qquad (26)$$

**2. Конверсия в негабинарную СС.** С помощью достаточно простого алгоритма, можно перевести представление $\sigma(i)$ координат точки (26) в «негабинарную» систему счисления.

Алгоритм перевода основан на следующих фактах (27)-(30):

$$-1\cdot(-2)^i=1\cdot(-2)^{i+1}+1\cdot(-2)^i; \qquad (27)$$

$$2\cdot(-2)^i=-1\cdot(-2)^{i+1}=1\cdot(-2)^{i+2}+1\cdot(-2)^{i+1}; \qquad (28)$$

$$1\cdot(-2)^{2i}=1\cdot 2^{2i}; \qquad (29)$$

$$1\cdot 2^{2i+1}=-1\cdot(-2)^{2i+1}. \qquad (30)$$

Блок-схема алгоритма перевода из бинарной в негабинарную систему счисления представлена на рис. 1.

***Замечание.*** «Усечение» $\upsilon(\sigma)$ на последнем шаге алгоритма до $t$ бит корректно в силу единственности представления элемента в негабинарной системе счисления, а также взаимной однозначности унификации (16).

И хотя в общем случае $\upsilon(\sigma)\neq\sigma$, тем не менее, справедливо равенство:

$$\vec{x}(i)=\tilde{P}(\vec{u}(i)),$$

$$\vec{u}(i)=\left(\sum_{l=0}^{t-1}(-2)^l\upsilon(\sigma(i)^{(0)})_l,\right.$$

$$\left.\sum_{l=0}^{t-1}(-2)^l\upsilon(\sigma(i)^{(1)})_l,\ldots,\sum_{l=0}^{t-1}(-2)^l\upsilon(\sigma(i)^{(0)})_l\right)^T, \qquad (31)$$

где $\tilde{P}$ – оператор унификации.

**3. Состояние генератора.** В результате шагов 1, 2, по заданной точке $\vec{x}(i)$ выходной последовательности произвольного генератора мы получили состояние

$$Y(i)_{lk+j}=\upsilon(\sigma(i)^{(j)})_l, \qquad (32)$$

$$l=0,1,\ldots,t-1,\ \ j=0,1,\ldots,k-1$$

LFSR-CNS генератора, соответствующего многочлену $f_1$.

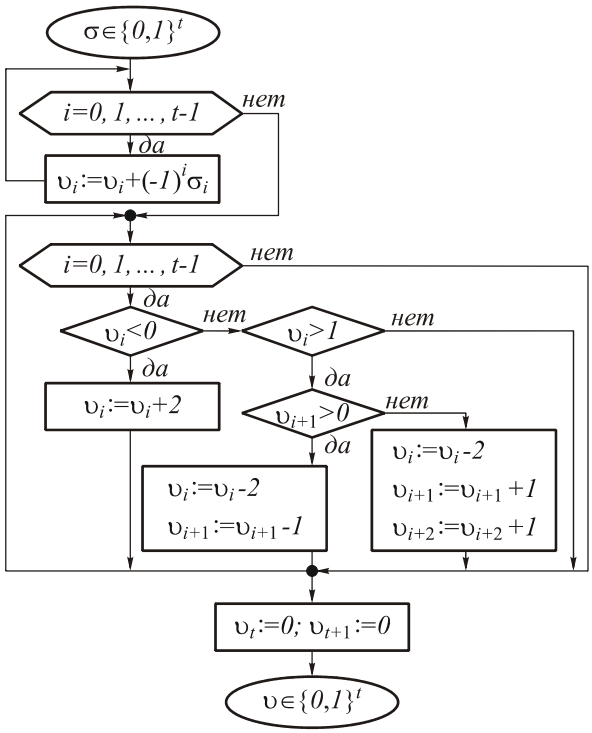


*Рис. 1. Блок-схема алгоритма перевода $\upsilon(\sigma)$ битового представления $\upsilon\in\{0,1\}^t$ числа из бинарной системы счисления в негабинарную*

**4. Интерпретация.** Интерпретируем состояние (32) как состояние LFSR-CNS генератора, соответствующего многочлену $f_2$.

**5. Вычисление модифицированной точки.** Действуя, далее, согласно второму этапу схемы генератора LFSR-CNS, по состоянию генератора (32) вычислим модифицированную точку $\tilde{x}(i) \in \overline{C}^k$, или, после соответствующего масштабирования, точку многомерного единичного куба $C^k$.

Иллюстрация предложенной схемы модификации представлена на рис. 2.

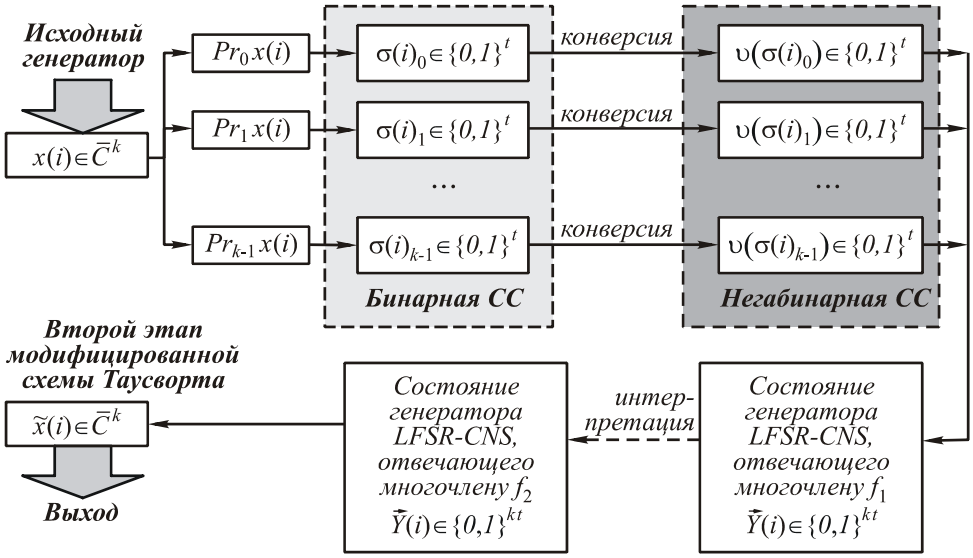


*Рис. 2. Схема модификации многомерной последовательности*

### *Сравнение свойств исходной и модифицированной многомерной последовательностей*

Покажем, что использование предложенной схемы может привести к значительному улучшению характеристик модифицированного генератора по сравнению с исходным. В качестве «теоретической» оценки качества генератора случайных чисел служит значение определенного критерия (или его оценка), которое дает некоторые основания ожидать определенных характеристик поведения генератора в реальных задачах моделирования. На практике используются различные критерии, применимость которых ограничена типом исследуемого генератора [17], [18]. Относительно недавно, в качестве универсального критерия применимого для генераторов всех типов был предложен взвешенный спектральный критерий (diaphony) [19].

Сформулируем схему исследования генератора с использованием взвешенного спектрального критерия. Пусть $\vec{h} = (h_0, ..., h_{k-1}) \in \mathbb{Z}^k$ и $\vec{x} = (x_0, ..., x_{k-1}) \in C^k$. Пусть, далее тригонометрическая функция, соответствующая мультииндексу $\vec{h}$ над $C^k$, определена равенством

$$e_{\vec{h}}(\vec{x}) = \prod_{i=0}^{k-1} e^{2\pi\sqrt{-1}h_i x_i};$$

обозначение $\sqrt{-1}$ для мнимой единицы использовано в целях избежания нежелательных совпадений с индексом произведения.

Если $\omega = (\vec{x}_n)_{n=0}^{N-1}$ – множество точек из $C^k$, тогда сумма Вейля [19] соответствующая мультииндексу $\vec{h}$ для $\omega$ имеет вид:

$$S_N(e_{\vec{h}}, \omega) = \frac{1}{N} \sum_{n=0}^{N-1} e_{\vec{h}}(\vec{x}_n), \ \vec{h} \neq \vec{0}.$$

Функционал взвешенного спектрального критерия $F_N(\omega)$ для множества точек $\omega$ задается соотношением

$$F_N(\omega) = \left( \frac{1}{(1+\pi^2/3)^k - 1} \sum_{\vec{h} \neq \vec{0}} \frac{1}{r(\vec{h})^2} \left| S_N(e_{\vec{h}}, \omega) \right|^2 \right)^{1/2},$$

где $r(\vec{h}) = \prod_{i=0}^{k-1} \max\{1, |h_i|\}$, $\vec{h} = (h_0, ..., h_{k-1}) \in \mathbb{Z}^k$.

Последовательность $\omega = (\vec{x}_n)_{n=0}^{\infty}$ распределена равномерно в $C^k$ если, и только если, $\lim_{N \to \infty} F_N(\omega) = 0$. Взвешенный спектральный критерий является мерой «нерегулярности» распределения точек последовательности $\omega$.

Существует эффективный алгоритм позволяющий вычислять значения взвешенного спектрального критерия, основанный на следующем факте (лемма 2), доказанном в [20].

***Лемма 2.*** Пусть

$$g(x) = 1 - \frac{\pi^2}{6} + \frac{\pi^2}{1}(1-2x)^2, \ x \in [0,1).$$

Пусть, далее

$$f(\vec{x}) = -1 + \prod_{i=0}^{k-1} g(x_i), \ \vec{x} = (x_0, ..., x_{k-1}) \in C^k.$$

Тогда для любого множества точек $\omega = (\vec{x}_n)_{n=0}^{N-1}$, $\vec{x}_n \in C^k$,

$$F_N^2(\omega) = \frac{1}{(1+\pi^2/3)^k - 1} \cdot$$

$$\cdot \frac{1}{N^2} \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} f(\vec{x}_n - \vec{x}_m \mod 1). \quad (33)$$

В случае если вычисление величины $F_N^2(\omega)$ в (33) аналитически связано с определенными трудностями, может быть проведено [17] численное исследование $F_N^2(\omega)$ как функции $N$. Заметим, что вычислительная сложность вычисления $F_N^2(\omega)$ по формуле (33) $O(N^2)$. Подобная асимптотика ограничивает величину $N$, которая может быть использована для исследования.

Как показано в [17], для равномерно распределенной случайной последовательности $\omega = (\vec{x}_n)_{n=0}^{\infty}$ математическое ожидание случайной величины $F_N^2(\omega)$ равно

$$\mathbf{E}\left(F_N^2(\omega)\right) = \frac{1}{N}. \quad (34)$$

Свойство (34) позволяет построить следующую схему численного исследования последовательности [17]:

**Шаг 1.** Для размерности $k$ и каждого из рассматриваемых $N$ ($N = N_1, N_2, ...N_n$) с использованием тестируемого генератора сформируем $K = 20$ упорядоченных множеств $\omega_n$, $0 \le n < K$ (каждое множество $\omega_n$ состоит из $N$ последовательных элементов $x_i$ выходной последовательности генератора).

**Шаг 2.** Для каждого из рассматриваемых $N$ ($N = N_1, N_2, ...N_n$), используя (33), вычислим значения величины

$N \cdot F_N^2(\omega_n)$, $0 \le n < K$.

Для равномерно распределенной случайной последовательности выборочное среднее $\overline{N \cdot F_N^2(\omega_n)}$ должно быть близко 1.

**Шаг 3.** Если значения $\overline{N \cdot F_N^2(\omega_n)}$ близки 1 и не наблюдается роста значения $\overline{N \cdot F_N^2(\omega_n)}$ с ростом $N = N_1, N_2, ...N_n$, качество распределения генерируемой последовательности признается **приемлемым**, иначе – **неприемлемым**.

Применим взвешенный спектральный критерий для исследования генератора Randu. Randu – линейный конгруэнтный генератор [21] со следующими параметрами: Randu= $LCG(2^{31}, 2^{16}+3 = 65539, 0, 1)$.

Пусть генератор Randu производит последовательность $\{r(i)\}$.

Многомерная последовательность $\{\vec{r}(i)\}$ для генератора Randu может быть получена по последовательности $\{r(i)\}$ методом leap-frog [22]

$$\vec{r}(i) = (r(ki), r(ki+1), ..., (ki+k-1))^T. \quad (35)$$

Значения взвешенного спектрального критерия для последовательности (35) и размерности $k = 3$ приведены в таблице 1.

*Таблица 1. Значения $\overline{N \cdot F_N^2(\omega_n)}$ для генератора Randu, $k = 3$*

| $N$ | Выборочное среднее | Максимум | Минимум |
|---|---|---|---|
| 512 | 1,02435 | 1,26149 | 0,77270 |
| 1024 | 1,04499 | 1,24142 | 0,91941 |
| 2048 | 1,03218 | 1,17598 | 0,84050 |
| 4096 | 1,07306 | 1,35123 | 0,92571 |
| 8192 | 1,07657 | 1,25191 | 0,92023 |
| 16384 | 1,13013 | 1,28906 | 0,95938 |
| 32768 | 1,26980 | 1,48367 | 1,08636 |
| 65536 | 1,57123 | 1,76214 | 1,23414 |

Можно заметить, что значения $\overline{N \cdot F_N^2(\omega_n)}$ для $\{\vec{r}(i)\}$ возрастают с ростом $N$ и имеют заметное отклонение от 1. Качество многомерной последовательности полученной с помощью генератора Randu признается [17], [18] неприемлемой в смысле взвешенного спектрального критерия.

Применив к многомерной последовательности (35), полученной на выходе генератора Randu, рассмотренную схему модификации, мы имеем следующие оценки взвешенного спектрального критерия для модифицированной последовательности (см. таблицу 2).

*Таблица 2. Значения $\overline{N \cdot F_N^2(\omega_n)}$ для модифицированной многомерной последовательности, полученной с помощью генератора Randu, $k = 3$*

| $N$ | Выборочное среднее | Максимум | Минимум |
|---|---|---|---|
| 512 | 0,99924 | 1,13273 | 0,87289 |
| 1024 | 1,02247 | 1,24364 | 0,85744 |
| 2048 | 1,00165 | 1,23207 | 0,89696 |
| 4096 | 0,97197 | 1,10564 | 0,80539 |
| 8192 | 0,98350 | 1,22752 | 0,72497 |
| 16384 | 0,98558 | 1,25042 | 0,77338 |
| 32768 | 0,99881 | 1,22190 | 0,82052 |
| 65536 | 0,98671 | 1,20719 | 0,79435 |

Можно заметить, что модифицированная последовательность обладает приемлемыми (в смысле взвешенного спектрального критерия свойствами). Значение $\overline{N \cdot F_N^2(\omega_n)}$ не превышает 1 при $N > 4096$, что свидетельствует об улучшении спектральных свойств.

Полученные экспериментальные данные (см. таблицу 2) свидетельствуют о возможности применения предложенной схемы модификации для улучшения свойств существующих схем многомерной генерации.

### *Заключение*

Предложенная схема модификации многомерной последовательности не зависит от специфики методов формирования исходной многомерной последовательности, существование генераторов LFSR-CNS отвечающих многочленам (10), (11) в пространстве любой размерности (начиная с двухмерного) позволяет модификацию практически любой многомерной псевдослучайной последовательности.

Следует отметить, что применение предложенной схемы должно сопровождаться отдельным исследованием свойств видоизмененного генератора для каждой конкретной исходной многомерной последовательности перед применением в реальных задачах.

### *Благодарности*

Работа выполнена при поддержке Министерства образования и науки РФ, правительства Самарской области (проект № 295Е2.3Д, дипломная работа), Американского фонда гражданских исследований и развития (CRDF Project SA-014-02) в рамках российско-американской программы «Фундаментальные исследования и высшее образование» (BRHE), а также при поддержке гранта Президента РФ № НШ-1007.2003.01, Российского фонда фундаментальных исследований (проекты №№ 03-01-00736, 05-01-96501).

### *Литература*

1. Wolfram S. Random sequence generation by cellular automata // Adv. Appl. Math. 7, 123 (1986).
2. Калугин А.Н. Трехмерное обобщение генератора LFSR случайных точек // Компьютерная оптика, 2005. № 27. С. 131-134
3. Coddington P., Random Number Generators for Parallel Computers, NHSE Review, Second Issue, Northeast Parallel Architectures Center, 1996. http://nhse.cs.rice.edu / NHSEreview / RNG
4. Entacher K. Parallel Streams of Linear Random Numbers in the Spectral Test // ACM Transactions on Modeling and Computer Simulation 9, 1999. № 1. С. 31-44.
5. Entacher K., Uhl A., Wegenkittl S. Parallel Random Number Generation: Long- range Correlations Among Multiple Processors // In P. Zinterhof, M. Vajteršic, and A. Uhl, editors, Parallel Computation, volume 1557 of Lecture Notes in Computer Science, Springer, New York, 1999. P. 107-116.
6. Vattulainen I. Framework for testing random numbers in parallel calculations // Phys. Rev. E, 59, 6, 7200 (1999).
7. Coddington P. Analysis of Random Number Generators Using Monte-Carlo Simulation, Int. J. Mod. Phys. 1994. С. 5. 547 p.
8. Coddington P. Tests of random number generators using Ising model simulations // Int. J. of Mod. Phys., 1996. С. 7(3). P. 295-303.
9. Ferrenberg A.M., Landau D.P. and Wong Y.J. Monte Carlo simulations: Hidden errors from good // Random number generators, Phys. Rev. Lett. 69, 3382 (1992).
10. Golomb S.W. Shift Register sequence // Holden-Day, San Francisco, 1967.
11. Гантмахер Ф.Р. Теория матриц // М.: Наука, 1988. – 552 с.
12. Kátai I., Kovács B. Canonical number systems in imaginary quadratic fields // Acta Mathematica Academiae Scientarium Hungaricae. 37 (1-3), 1981. P. 159-164.
13. Kovács A., Generalized binary number systems // Annales Univ. Sci. Budapest, Sect. Comp. 20, 2001. P. 195-206.
14. 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 (accepted for publication)
15. Vittorio Grunwald. Giornale di Matematiche di Battaglini (1885), 203-221, 367
16. Pawlek Z. and Wakulicz A. Bulletin de l'Academie Polonaise des Scienses, Classe III, 5 (1957), 233-236; Serie des sciences techniques 7 (1959), 713-721.
17. Hellekalk P., Niedderreiter H. The Weighted Spectral Test: Diaphony, ACM Trans. on Model. and Comp. Simul., 1998. Vol 8. No. 1 P. 43-60.
18. Ripley B. Stochasitc Simulation // Wiley, New York, 1987.
19. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел // М.: Мир, 1987. – 416 с.
20. Zinterhof P. Über einige Abschätzungen bei der Approximation von Funktionen met Gleivhverteilundsmethoden. Sitzungsber. Österr. Akad. Wiss. Math.-Natur. Kl. II 185, 121-132 (1976).
21. Fishman G., Moore L. An exhaustive analysis of multiplicative congruential random number generators with modulus 231-1 // SIAM J. Sci. Statist. Comput. 1986. № 7. P. 24-45.
22. Celmaster W. and Moriarty K.J.M. A method for vectorized random number generators // J. Comput. Phys. 1986. № 64. 271 p.

# Modification of multidimensional pseudo-random sequences using dual LFSR-CNS generators

*A.N. Kalugin* [1,2]
[1] *Image Processing Systems Institute of RAS*
[2] *Samara State Aerospace University named after academician S.P. Korolev*

***Abstract***

The article considers a new method for modifying a multidimensional pseudo-random sequence of points based on the use of a pair of dual LFSR-CNS generators. The generator state restored on the basis of an element of the multidimensional sequence is interpreted as the state of the dual generator, which allows to generate a point that is different from the point of the initial sequence. Comparative results of the study of the initial and the modified sequence using the weighted spectral criterion are presented.

*Keywords:* LFSR-CNS generators, pseudo-random sequence, spectral criterion.

*Citation*: Kalugin AN. Modification of multidimensional pseudo-random sequences using dual LFSR-CNS generators. Computer Optics 2005; 28: 112-118.

***References***

[1] Wolfram S. Random sequence generation by cellular automata. Adv Appl Math 1986; 7: 123.
[2] Kalugin AN. Three-dimensional generalization of the random point generator LFSR. Computer Optics 2005; 27: 131-134.
[3] Coddington P. Random number generators for parallel computers. NHSE Review. Issue 2. Northeast Parallel Architectures Center; 1996. Source: ⟨http://nhse.cs.rice.edu/NHSEreview/RNG⟩.
[4] Entacher K. Parallel streams of linear random numbers in the spectral test. ACM Trans Model Comput Simul 1999; 9(1): 31-44.
[5] Entacher K, Uhl A, Wegenkittl S. Parallel random number generation: Long-range correlations among multiple processors. In Book: Zinterhof P, Vajteršic M, Uhl A, eds. Parallel Computation. New York: Springer; 1999: 107-116.
[6] Vattulainen I. Framework for testing random numbers in parallel calculations. Phys Rev E 1999; 59(6): 7200.
[7] Coddington P. Analysis of random number generators using Monte Carlo simulation. Int J Mod Phys C 1994; 5(3): 547-560.
[8] Coddington P. Tests of random number generators using Ising model simulations. Int J Mod Phys C 1996; 7(3): 295-303.
[9] Ferrenberg AM, Landau DP, Wong YJ. Monte Carlo simulations: Hidden errors from "good" Random number generators. Phys Rev Lett 1992; 69: 3382-3384.
[10] Golomb SW. Shift register sequence. San Francisco: Holden-Day; 1967.
[11] Gantmakher FR. The theory of Matrices. 2nd ed. Providence, Rhode Islands: American Mathematical Society; 1990. ISBN: 978-0-8218-1376-8.
[12] Kátai I, Kovács B. Canonical number systems in imaginary quadratic fields. Acta Mathematica Academiae Scientiarum Hungarica 1981; 37(1-3): 159-164.
[13] Kovács A. Generalized binary number systems. Annales Univ Sci Budapest, Sect Comp 2001; 20: 195-206.
[14] Chernov VM. Fast uniform distribution of sequences for fractal sets. Proceedings of International Conference on Computer Vision and Graphics 2004; (accepted for publication).
[15] Grunwald V. Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale). Giornale di Matematiche di Battaglini 1885; 367: 203-221.
[16] Pawlak Z, Wakulicz A. Use of expansions with a negative basis in the arithmometer of a digital computer. Bulletin de l'Academie Polonaise des Scienses 1957; Classe III, 5: 233-236; Serie des Sciences Techniques 7 (1959), 713-721.
[17] Hellekalk P, Niedderreiter H. The weighted spectral test: Diaphony. ACM Trans Model Comput Simul 1998; 8(1): 43-60.
[18] Ripley B. Stochasitc simulation. New York: John Wiley and Sons; 1987.
[19] Ireland K, Rosen M. A classical introduction to modern number theory. New York: Springer-Verlag; 1990.
[20] Zinterhof P. ÜbereinigeAbschätzungenbei der Approximation von Funktionen met Gleivhverteilundsmethoden. Sitzungsber Österr Akad Wiss Math-Natur 1976; Kl. II(185): 121-132.
[21] Fishman G, Moore L. An exhaustive analysis of multiplicative congruential random number generators with modulus 231-1. SIAM J Sci Comput 1986; 7: 24-45.
[22] Celmaster W, Moriarty KJM. A method for vectorized random number generators. J Comput Phys 1986; 64(1): 271-275.