EDN: FHQCGI

УДК 621.391 *2.2.13*

ДИСКРЕТНЫЕ ГЕОМЕТРИЧЕСКИЕ ИНВАРИАНТЫ В АНАЛИЗЕ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Р.Р. Нигматуллин, С.С. Логинов

Казанский национальный исследовательский технический университет
им. А.Н. Туполева-КАИ
Российская Федерация, 420111, г. Казань, ул. К. Маркса, 10

Аннотация. В работе представлены результаты анализа наиболее известных генераторов псевдослучайных чисел методом дискретных геометрических инвариантов (ДГИ). Показано, что данный метод позволяет сопоставлять различные типы генераторов псевдослучайных чисел, классифицировать генераторы по временным реализациям псевдослучайных последовательностей и найти их различия друг с другом (в рамках параметров ДГИ), которые обусловлены их малыми физическими различиями (на уровне их приборных реализаций).

Ключевые слова: генератор псевдослучайных чисел, тестирование последовательностей на случайность, дискретные геометрические инварианты, генератор Мерсенна Твистера.

Введение

Генерация случайных и псевдослучайных чисел широко используется в различных областях, таких как, математическое моделирование, криптография, информационная безопасность, тестирование программного обеспечения. В настоящее время существует большое количество генераторов случайных чисел, а также наборов псевдослучайных чисел
[1-3], полученных на их основе.

Для тестирования генераторов случайных чисел используются различные виды тестов. Основные виды тестов применяются для *двоичных* последовательностей. Среди них особую известность приобрели статистические тесты FIPS, NIST, тесты Дональда Кнута, DIEHARD, TESTU01, Crypt-XS [4-6]. Кроме того, известны графические тесты, которые позволяют отобразить в удобной форме их различные статистические свойства. Графическое отображение гистограмм последовательностей чисел, автокорреляционных функций, спектров Фурье позволяет наглядно сравнивать различные генераторы случайных чисел [7]. В этом ключе невозможно не обратить внимание на оценки случайности различных видов энтропий, в частности Шеннона, Tsallisa [8]. Также известны методы фрактального анализа в виде использования спектра показателей Реньи, включающих оценку информационной энтропии [8,9].

Идеальным тестом генераторов случайных чисел мог бы стать некий обобщенный тест, который выдавал бы на выходе одно из двух возможных решений: последовательность случайная или последовательность не является случайной. Однако в настоящее время *не* представляется возможным найти такую функцию, которая выдавала бы подобный результат. Поэтому все упомянутые тесты представляют собой набор из десятков частных тестов, которые принимаются или опровергаются стандартными методами: на основе порогового значения; на основе оценки доверительного интервала, оцениваемого с соответствующей доверительной вероятностью.

Несмотря на широкое применение различных генераторов (псевдо) случайных чисел (ГСЧ) вопрос о критериях надежной оценки меры "случайности" по-прежнему остается интересным и открытым для исследователей.

Целью данной работы является сопоставительный анализ генераторов псевдослучайных последовательностей с использованием метода дискретных геометрических инвариантов (ДГИ).

1. Исследуемые генераторы псевдослучайных чисел

Благодаря воспроизводимости статистических характеристик псевдослучайные числа находят более широкое применение, так как позволяют исследователям сопоставлять результаты, полученные с использованием идентичных последовательностей. Поэтому в данной работе мы решили использовать в качестве объекта исследований ряд наиболее часто используемых генераторов псевдослучайных чисел (ПСЧ), представленных в [10].

Наиболее исследованным генератором псевдослучайных чисел, используемым в качестве хрестоматийного примера, является генератор М-последовательности, описываемый выражением

$$x_{n+p} = c_{p-1} \cdot x_{n+p-1} + c_{p-2} \cdot x_{n+p-2} + ... + c_1 \cdot x_{n+1} + x_n \left(mod\, 2\right), n = 1, 2, 3\ldots \quad (1)$$

где c_p– коэффициенты порождающего полинома.

Схема типового генератора М-последовательности, представлена на рис. 1.

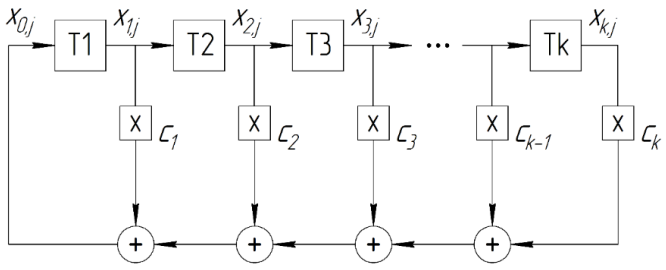

Рис. 1. Блок-схема генератора на основе метода М-последовательности

В схеме Т1, Т2, Т3…Tk – сдвиговые регистры; c1, c2, c3…ck – коэффициенты, определяемые порождающим полиномом; x0,j, x1,j, x2,j, x3,j… xk,j – символы на входе соответствующих сдвиговых регистров; k – кол-во сдвиговых регистров.

Пятипараметрический метод использует характеристический полином из 5 членов и позволяет генерировать последовательности w-битовых двоичных целых чисел в соответствии с рекуррентным выражением

$$X_{n+p} = X_{n+q1} + X_{n+q2} + X_{n+q3} + X_n \left(mod\, 2\right), n = 1, 2, 3\ldots \quad (2)$$

Генератор псевдослучайных чисел на основе метода Таусворта использует рекуррентную формулу

$$X_n = x_{nt} x_{nt+1} \ldots x_{nt+w-1}\ , n = 0, 1, 2\ldots \quad (3)$$

где $x_{n+p} = x_{n+q} + x_n \left(mod\, 2\right), n = 0, 1, 2\ldots$. Выбранные параметры генератора на основе метода Таусворта, использованные в данной работе равны: $p = 16; q = 7; w = 16; t = 19$.

Комбинированный метод Таусворта представляет собой комбинацию нескольких простых последовательностей Таусворта с одной и той же длиной слова w и определяется формулой

$$X_n = X_n^{(1)} + X_n^{(2)} + \ldots + X_n^{(J)} \left(mod\, 2\right), n = 0,1,2\ldots \tag{4}$$

Генератор на основе комбинированного метода Таусворта разрабатывался при помощи 3-х простых последовательностей с параметрами: $p = 16; w = 16; t = 19$.

Метод Мерсенна Твистера позволяет генерировать последовательность двоичных псевдослучайных w-битовых чисел по рекуррентной формуле

$$X_{n+p} = X_{n+q} + (X_n \mid X_{n+1})^{(r)} A\left(mod\, 2\right), n = 1,2,3\ldots, \tag{5}$$

где $(X_n^{(f)} \mid X_{n+1}^{(1)})^{(r)}$ – двоичное число, полученное конкатенацией чисел X_n и X_{n+1}, когда первые $\left(w-r\right)$ битов взяты из X_n, а последние r битов – из X_{n+1}; A – матрица, состоящая из нулей и единиц, и определенная посредством a.

Принцип построения генератора формирования псевдослучайных чисел на основе метода Мерсенна Твистера представлен на рис. 2.

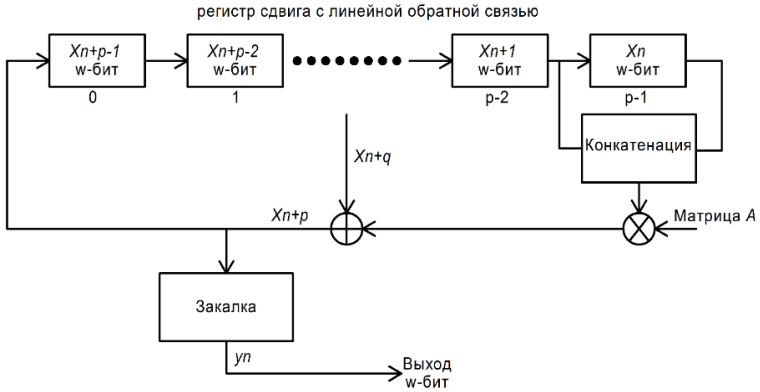

Рис. 2. Блок-схема генератора на основе метода Мерсенна Твистера

Для улучшения рандомизации полученного ряда применяется метод закалки, определяемый по выражениям

$$1) y1_n = X_{n+p}$$
$$2) y2_n = (y1_n + (y1_n >> u))$$
$$3) y3_n = (y2_n + (y2_n << s) \cdot b)$$
$$4) y4_n = (y3_n + (y3_n << t) \cdot c)$$
$$5) y5_n = (y4_n + (y4_n >> l))$$
$$6) y_n = y5_n$$

Для реализации генератора на основе метода Мерсенна Твистера выбраны следующие параметры: $p = 12; q = 4; w = 16; r = 8; u = 11; s = 7; t = 15; l = 18$.

Все приведенные генераторы были реализованы в программной среде Matlab. На основе формируемых ими двоичных псевдослучайных последовательностей сформированы 16-битные целые числа. Длина целочисленных последовательностей для анализа составила не менее 12000 элементов. Длины двоичных последовательностей обычно составляют не менее 20000 двоичных элементов, в данной работе длина

целочисленных последовательностей, если их представить в двоичном виде несколько выше. Указанная длина последовательностей, по-нашему мнению, позволит выявить индивидуальные свойства последовательностей, необходимые для их различения между собой.

2. Изложение метод ДГИ четвертого порядка

Для выявления различий между последовательностями ПСЧ, предварительно переведенных в обычное десятичное представление, применим метод ДГИ 4-го порядка.

1. *Параметры пространства признаков ДГИ 4-го порядка.*

В этом теоретическом разделе мы можем расширить возможности предыдущей теории, изложенной в статье [11], и дать полную форму 3D-ДГИ 4-го порядка вместе с полным набором параметров, которые могут быть полезны во многих приложениях. Полезно выписать полную форму четвертого порядка

$$\begin{aligned}
L_k^{(4)} &= A_{400}\left(X-\Delta x_k\right)^4 + A_{040}\left(Y-\Delta y_k\right)^4 + A_{004}\left(Z-\Delta z_k\right)^4 \\
&-\frac{1}{2}A_{310}\left(X-\Delta x_k\right)^3\left(Y-\Delta y_k\right) - \frac{1}{2}A_{130}\left(X-\Delta x_k\right)\left(Y-\Delta y_k\right)^3 - \\
&-\frac{1}{2}A_{301}\left(X-\Delta x_k\right)^3\left(Z-\Delta z_k\right) - \frac{1}{2}A_{103}\left(X-\Delta x_k\right)\left(Z-\Delta z_k\right)^3 - \\
&-\frac{1}{2}A_{031}\left(Y-\Delta y_k\right)^3\left(Z-\Delta z_k\right) - \frac{1}{2}A_{013}\left(Y-\Delta y_k\right)\left(Z-\Delta z_k\right)^3 - \\
&-A_{220}\left(X-\Delta x_k\right)^2\left(Y-\Delta y_k\right)^2 - A_{202}\left(X-\Delta x_k\right)^2\left(Z-\Delta z_k\right)^2 - \\
&-A_{022}\left(Y-\Delta y_k\right)^2\left(Z-\Delta z_k\right)^2 - A_{211}\left(X-\Delta x_k\right)^2\left(Y-\Delta y_k\right)\left(Z-\Delta z_k\right) - \\
&-A_{121}\left(X-\Delta x_k\right)\left(Y-\Delta y_k\right)^2\left(Z-\Delta z_k\right) - A_{112}\left(X-\Delta x_k\right)\left(Y-\Delta y_k\right)\left(Z-\Delta z_k\right)^2 .
\end{aligned} \tag{6}$$

Здесь параметры $A_{\alpha\beta\gamma}$ определяют соответствующие степенные показатели в разложении формы четвертого порядка. Индекс $k=\overline{1,N}$ определяет соответствующий набор данных, формирующий трехмерный вектор $\boldsymbol{r}_k=F(x_k,y_k,z_k)$. Индекс Δ означает, что из любой вектор-последовательности r_k следует вычесть среднее значение $\langle\boldsymbol{r}\rangle$. Любой текущий вектор $\boldsymbol{r}(x,y,z)$, определяющий трехмерную поверхность, получается из условия

$$\frac{1}{N}\sum_{k=1}^{N} L_k^{(4)} = II_4 . \tag{7}$$

Подставляя форму (6) в (7) и приравнивая линейные части нулю, можно получить следующую систему линейных уравнений для корреляторов третьего порядка

$$\begin{aligned}
&\frac{1}{2}A\left(3Q_{210}+3Q_{201}+Q_{030}+Q_{003}\right)+2B\left(Q_{120}+Q_{102}\right)+C\left(2Q_{111}+Q_{021}+Q_{012}\right)=4Q_{300} \\
&\frac{1}{2}A\left(3Q_{120}+3Q_{021}+Q_{300}+Q_{003}\right)+2B\left(Q_{210}+Q_{012}\right)+C\left(2Q_{111}+Q_{201}+Q_{102}\right)=4Q_{030} . \\
&\frac{1}{2}A\left(3Q_{102}+3Q_{012}+Q_{300}+Q_{030}\right)+2B\left(Q_{201}+Q_{021}\right)+C\left(2Q_{111}+Q_{210}+Q_{120}\right)=4Q_{003}
\end{aligned} \tag{8}$$

Можно уменьшить число переменных, введя следующие обозначения

$$
\begin{aligned}
&A_{400} = A_{040} = A_{004} = E,\\
&\frac{A_{310}}{E} = \frac{A_{130}}{E} = \frac{A_{301}}{E} = \frac{A_{103}}{E} = \frac{A_{031}}{E} = \frac{A_{013}}{E} = A,\\
&\frac{A_{220}}{E} = \frac{A_{202}}{E} = \frac{A_{022}}{E} = B,\\
&\frac{A_{211}}{E} = \frac{A_{121}}{E} = \frac{A_{112}}{E} = C.
\end{aligned}
\tag{9}
$$

Для моментов и их взаимных корреляций, фигурирующих в (8) можно ввести следующие компактные обозначения

$$
\begin{aligned}
&Q_{\alpha\beta\gamma} = \frac{1}{N}\sum_{k=1}^{N}\left(\left(\Delta x_k\right)^{\alpha}\left(\Delta y_k\right)^{\beta}\left(\Delta z_k\right)^{\gamma}\right),\\
&\alpha+\beta+\gamma = 3,\ 0 \le \alpha,\beta,\gamma \le 3.
\end{aligned}
\tag{10}
$$

Эти компактные обозначения будут использованы для оценки парных корреляций ($\alpha+\beta+\gamma=2$) и для корреляций четвертого порядка ($\alpha+\beta+\gamma=4$). Знаки в четвертой форме (6) были выбраны таким образом, чтобы все знаки в линейной системе уравнений (8) были положительными.

После некоторых алгебраических преобразований требование (7) принимает форму

$$
\begin{aligned}
&K_4 - K_2 = II_4\\
&K_4 = X^4 + Y^4 + Z^4 - \frac{A}{2}\left(X^3Y + XY^3 + X^3Z + XZ^3 + Y^3Z + YZ^3\right) -\\
&-B\left(X^2Y^2 + X^2Z^2 + Y^2Z^2\right) - C\left(X^2YZ + Y^2XZ + XYZ^2\right)\\
&K_2 = M_{200}X^2 + M_{020}Y^2 + M_{002}Z^2 + M_{110}XY + M_{101}XZ + M_{011}YZ
\end{aligned}
\quad . \tag{11}
$$

Искомые параметры $M_{\alpha\beta\gamma}$ ($\alpha+\beta+\gamma=2$) определяются следующими выражениями

$$
\begin{aligned}
M_{200} &= \frac{3}{2}A\left(Q_{110}+Q_{101}\right) + B\left(Q_{020}+Q_{002}\right) + CQ_{011} - 6Q_{200}\\
M_{020} &= \frac{3}{2}A\left(Q_{110}+Q_{011}\right) + B\left(Q_{200}+Q_{002}\right) + CQ_{101} - 6Q_{020}\\
M_{002} &= \frac{3}{2}A\left(Q_{101}+Q_{011}\right) + B\left(Q_{200}+Q_{020}\right) + CQ_{110} - 6Q_{002}\\
M_{110} &= \frac{3}{2}A\left(Q_{200}+Q_{020}\right) + 4BQ_{110} + C\left(2Q_{101}+2Q_{011}+Q_{002}\right)\\
M_{101} &= \frac{3}{2}A\left(Q_{002}+Q_{200}\right) + 4BQ_{101} + C\left(2Q_{110}+2Q_{011}+Q_{020}\right)\\
M_{011} &= \frac{3}{2}A\left(Q_{020}+Q_{002}\right) + 4BQ_{011} + C\left(2Q_{110}+2Q_{101}+Q_{200}\right)
\end{aligned}
\quad . \tag{12}
$$

Константа II_4 в (2.2) определяется через корреляторы 4-го порядка и имеет вид

$$
\begin{aligned}
II_4 &= \frac{A}{2}\left(Q_{310}+Q_{130}+Q_{103}+Q_{301}+Q_{013}+Q_{031}\right) +\\
&+B\left(Q_{220}+Q_{202}+Q_{022}\right) + C\left(Q_{211}+Q_{121}+Q_{112}\right) -\\
&-\left(Q_{400}+Q_{040}+Q_{004}\right)
\end{aligned}
\quad . \tag{13}
$$

Полученная форма 4-го порядка может быть разрешена в сферической системе координат. Если предположить

$$\begin{aligned} x &= < x > + X(\theta,\varphi) = < x > + R(\theta,\varphi)\cos(\varphi)\sin(\theta), \\ y &= < y > + Y(\theta,\varphi) = < y > + R(\theta,\varphi)\sin(\varphi)\sin(\theta), \\ z &= < z > + Z(\theta,\varphi) = < z > + R(\theta,\varphi)\cos(\theta), \end{aligned} \tag{14}$$

то подстановка выражений (14) в (6) приводит к биквадратному уравнению относительно положительного радиуса-вектора $R(\theta,\varphi)$

$$R^4(\theta,\varphi)P_4(\theta,\varphi) - R^2(\theta,\varphi)P_2(\theta,\varphi) = II_4\,, \tag{15}$$

с соответствующим решением

$$R(\theta,\varphi) = \left(\frac{P_2\left(\theta,\varphi\right) + \sqrt{P_2^2\left(\theta,\varphi\right) + 4II_4P_4\left(\theta,\varphi\right)}}{2P_4\left(\theta,\varphi\right)} \right)^{1/2}. \tag{16}$$

Вследствие положительности радиуса вектора $R(\theta,\varphi)$ в последнем выражении выбран только положительный корень. Полиномы $P_{2,4}(\theta,\varphi)$, входящие в это выражение определяются следующими выражениями

$$\begin{aligned} &P_4\left(\theta,\varphi\right) = P^{(4)}\left(\theta,\varphi\right) - P^{(3,1)}\left(\theta,\varphi\right) - P^{(2,2)}\left(\theta,\varphi\right) - P^{(2,1,1)}\left(\theta,\varphi\right) \\ &P^{(4)}\left(\theta,\varphi\right) = \cos^4\left(\varphi\right)\sin^4(\theta) + \sin^4\left(\varphi\right)\sin^4(\theta) + \cos^4(\theta), \\ &P^{(3,1)}\left(\theta,\varphi\right) = \frac{A}{2}\left(\cos^3(\varphi)\sin(\varphi)\sin^4(\theta) + \cos^3(\varphi)\sin^3(\theta)\cos(\theta) + \sin^3(\varphi)\sin^3(\theta)\cos(\theta)\right) + \\ &+ \frac{A}{2}\left(\sin^3(\varphi)\cos(\varphi)\sin^4(\theta) + \cos(\varphi)\sin(\theta)\cos^3(\theta) + \sin(\varphi)\sin(\theta)\cos^3(\theta)\right), \\ &P^{(2,2)}\left(\theta,\varphi\right) = B\left(\cos^2(\varphi)\sin^2(\varphi)\sin^4(\theta) + \cos^2(\varphi)\sin^2(\theta)\cos^2(\theta) + \sin^2(\varphi)\sin^2(\theta)\cos^2(\theta)\right), \\ &P^{(2,1,1)}(\theta,\varphi) = C\left(\cos^2(\varphi)\sin(\varphi)\sin^2(\theta)\cos(\theta) + \cos(\varphi)\sin^2(\varphi)\sin^3(\theta)\cos(\theta) + \sin(\varphi)\cos(\varphi)\cos^2(\theta)\right). \end{aligned} \tag{17}$$

$$\begin{aligned} &P_2(\theta,\varphi) = P^{(2,0)}(\theta,\varphi) + P^{(1,1)}(\theta,\varphi) \\ &P^{(2,0)}(\theta,\varphi) = M_{200}\cos^2(\varphi)\sin^2(\theta) + M_{020}\sin^2(\varphi)\sin^2(\theta) + M_{002}\cos^2(\theta), \\ &P^{(1,1)}(\theta,\varphi) = M_{110}\cos(\varphi)\sin(\varphi)\sin^2(\theta) + M_{101}\cos(\varphi)\sin(\theta)\cos(\theta) + M_{011}\sin(\varphi)\sin(\theta)\cos(\theta) \end{aligned} \tag{18}$$

Выражения (14) -(17) определяет поверхность для формы 4-го порядка, которая определяется (3(1)+6(2)+3(*A*,*B*,*C*)+1(4))=13-ю параметрами, определяющим её вид в декартовой системе координат (x,y,z). Однако, более детальный анализ показывает, что полный набор корреляционных параметров определяется 3(1)+6(2)+10(3)+15(4) = 34-мя *независимыми* параметрами. Эта комбинация, в свою очередь, образуется из 3 независимых параметров как (*A*, *B*, *C*) +6 параметров из (12) и одного параметра из выражения (13).

Поэтому полное число параметров образующих пространство признаков, для 3D-ДГИ четвертого порядка содержит в целом (34+10) = 44 параметра. Подчеркнем, что это максимально возможное сжатие 3-х последовательностей, каждая из которых содержит $j = \overline{1, N}$ дискретных точек. Это обстоятельство связано с тем, что не существует форм более

высоких порядков, допускающих разделение переменных вида (15), может быть за исключением специальных случаев.

Можно поставить следующий вопрос: к каким задачам применима теория ДГИ разработанная выше и что можно ожидать в результате от её применения? Как видно из теории ДГИ, этот метод в состоянии оценить все корреляции до 4-го порядка включительно, которые скрыты внутри 3 последовательностей, сформированных изначально из $3N$ точек данных. Она может быть применена для рассмотрения волн, которые распространяются по 3 независимым осям OX, OY, OZ, а также для любых трех последовательностей $x(t)$, $y(t)$, $z(t)$ т.е. к вектору (x, y, z), определяющему траекторию в трехмерном пространстве (например, странный аттрактор) или может совпадать с пространственным вектором электромагнитного поля. Эта теория сокращает количество больших наборов данных, сформированных из $3N$ точек данных, и позволяет рассмотреть специфический "корреляционный каркас или скелет" в пространстве признаков с размерностью $d=44 << N$. Очевидно, что полный корреляционный анализ изначально скрыт от глаз обработчика исходных данных, но тем не менее может дать окончательный набор параметров (равный 44), вполне достаточный для дальнейших количественных оценок. Заканчивая этот раздел, мы хотим также ответить на вопрос: что должен делать читатель, когда у него есть только одна случайная последовательность? В этом случае рекомендуется использовать процедуру сокращения до 3 инвариантных (стабильных) точек. Это означает, что на данном отрезке, имеющем число точек, совпадающем с его диной b, можно выбрать только три точки, таких как b_{max}, b_{mean} и b_{min}, которые являются инвариантными относительно перестановок всех других точек, образующих отрезок длины b. Другими словами, предложенная теория применима и для одиночной случайной последовательности. Если две последовательности тесно связаны друг с другом, то для этого случая рекомендуется теория ДГИ для плоского пространства, разработанная в статьях [12], [13], [14].

3. Данные ПСЧ генераторов. Их отбор и применение теории ДГИ 4-го порядка

Как уже упоминалось в первом разделе, мы подготовили для анализа "лучший" из доступных наборов данных ПСЧ, который предварительно был протестирован как полностью "хаотичные" в двоичной системе счисления. Чтобы четко увидеть их разницу, необходимо выполнить следующие предварительные шаги:

Ш-1. Преобразуем эти двоичные последовательности в десятичную систему счисления.

Ш-2. Если последовательность одинарная, то применяем процедуру приведения к трем инвариантным точкам (из минимального множества b=5).

Ш-3. Применяем интегрирование сжатой последовательности по методу трапеций относительно ее среднего значения.

После выполнения этих 3 предварительных шагов применяется теория, рассмотренная выше, и получается вектор, содержащий 44 количественных параметра, состоящий из всех корреляций (1-4) порядков включительно.

Имеет смысл пояснить эти шаги рядом рисунков. В статье рассмотрены данные файла (gsch_rezObshiy_14,txt), состоящие из 14 независимых столбцов и имеющих N=12286 строк. Используя процедуру сжатия данных с b=5, мы получим три последовательности без тренда.

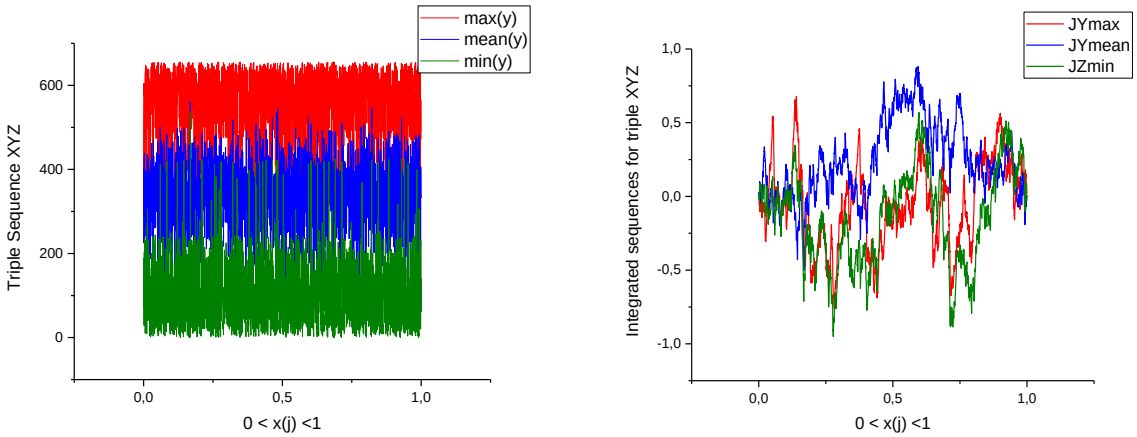

Рис.1 (*a, b*). На левом рисунке мы показываем три расщепленных БТП, имеющих уже редуцированную длину N/b=2457, полученных с помощью процедуры сжатия (b=5). На правом рисунке (*b*) мы показываем 3 проинтегрированные БТП, полученные с помощью метода трапеций. Полученные тренды имеют туже окраску, что и на левом рисунке

Рисунок 1(*b*) подготовлен для применения метода 3D-ДГИ.

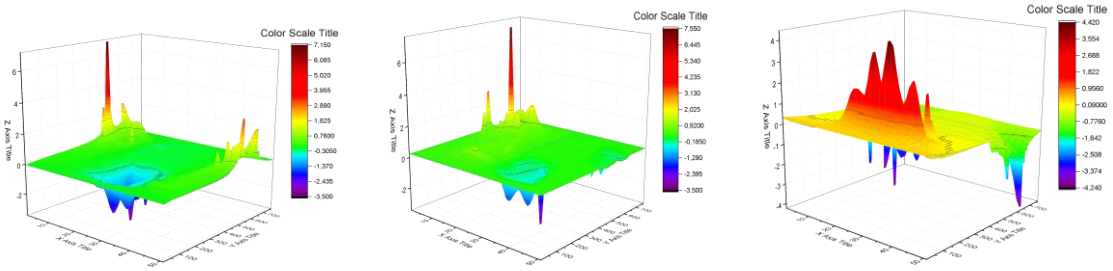

Рис.2 (*a, b, c*). На этих рисунках (слева направо) мы показываем 3D-поверхности для $x(\varphi,\theta)$, $y(\varphi,\theta)$, $z(\varphi,\theta)$, полученных с помощью выражения (14)

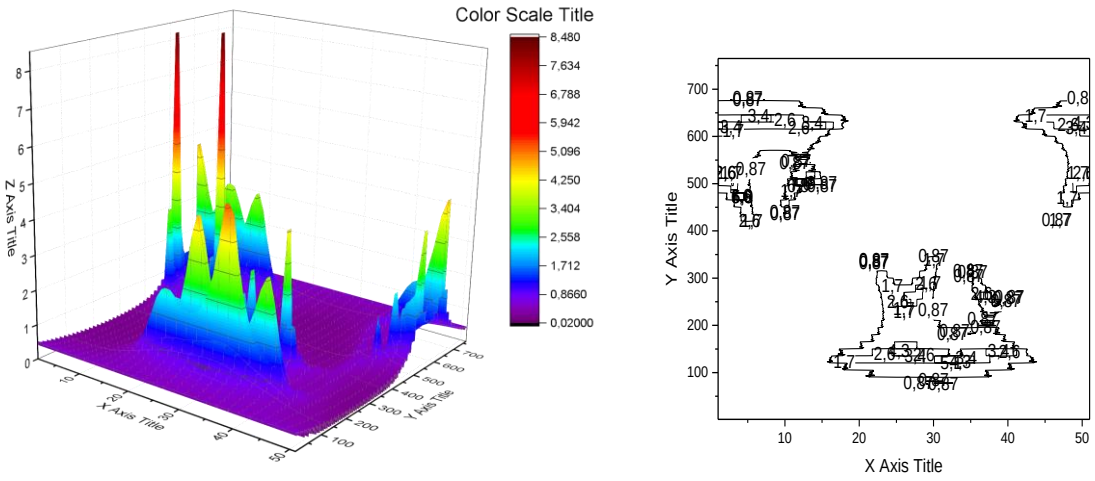

Рис. 3 (*a, b*). На этих двух рисунках мы показываем зависимость $R(\theta,\varphi)$: Левый рисунок (*a*) рассчитан с помощью выражения (16). Поперечные сечения этой поверхности показаны на правом рисунке (*b*)

Следовательно, в результате этих манипуляций по приведенным выше формулам, мы получаем компактные вектора, имеющих длину 44 точки в пространстве признаков. Аналогично можно получить 13 компактных векторов от других генераторов ПСЧ для их сравнения между собой. Для того, чтобы подчеркнуть их чисто визуальные различия между собой, мы покажем только 3D-поверхность для $R(\theta,\varphi)$ и его поперечное сечение для второй колонки из того же файла (gsch_rezObshiy_14.txt)

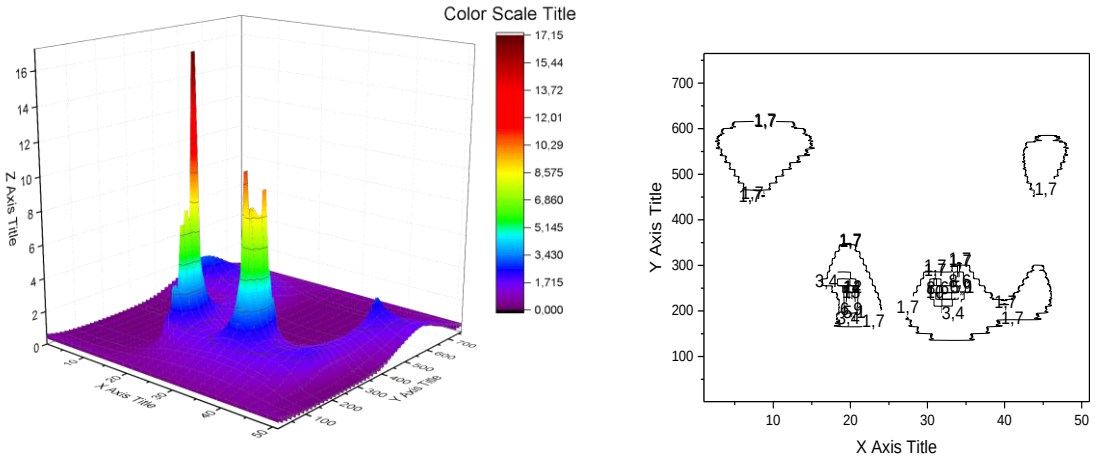

Рис. 4 (*a, b*). На этих двух рисунках мы показываем зависимость $R(\theta,\varphi)$ для второй колонки данных. Левый рисунок (*a*) также рассчитан с помощью выражения (2.11). Поперечные сечения этой поверхности показаны на правом рисунке (*b*). Если сравнить эти два рисунка 3 и 4, то можно заметить их различие даже визуально

В итоге этих расчетов получаем матрицу с количеством строк 44 и столбцов 14. Чтобы увидеть разницу между ними, мы применяем процедуру деления матрицы на саму себя. Можно взять матрицу Mt ("тестовую"), содержащую Prm=44 строки ×14 столбцов, и разделить на ту же матрицу Mr ("эталонную") = 44×14. За неимением эталонных генераторов ПСЧ мы вынуждены отождествить тестовую и эталонную матрицы между собой. Ввиду важности такого выбора, мы вернемся к обсуждению этого вопроса в заключительном разделе. Эта процедура деления матриц возможна потому, что две матрицы содержат одинаковое количество строк 44, и мы предполагаем, что элементы матрицы Mr не равны нулю. Математически эта процедура деления может быть записана в виде

$$D_{ij}(k) = \frac{Mt_{k,i}}{Mr_{k,j}},\ i = 1,2,...,I;\ j = 1,2,...,J,$$
$$k = 1,2...,K,\ K = 44,\ I = J = 14. \qquad (19)$$

В результате этой процедуры получается новая матрица, содержащая в общей сложности I строк и J столбцов. Следует также отметить, что элементы этой трехмерной матрицы, разделенной на части, являются векторами (имеющими длину K). Каждый разделенный элемент имеет следующую структуру Di,j(k). В нашем случае K=44, I=14, J=14. Заключительный этап предлагаемой процедуры обработки связан с выбором доверительного интервала, который может быть выбран в качестве критерия желаемого сходства этих двух матриц между собой. Действительно, давайте предположим, что

пределы значений в матрицах числителя и знаменателя, соответственно, известны и являются следующими:

$$\min(Mt) \le Mt \le \max(Mt),\ \min(Mr) \le Mr \le \max(Mr),$$
$$\left(\frac{\min(Mt)}{\max(Mr)}\right) \le \left(\frac{Mt}{Mr}\right) \le \frac{\max(Mt)}{\min(Mr)}, \quad (20)$$

Рассмотрение предельного случая (приведенного во второй строке (20), когда разделенные матрицы статистически идентичны друг другу, позволяет предложить следующий критериальный интервал подобия для двух сравниваемых матриц

$$-1 \le \left(\frac{Mt}{Mr}\right) \le 1. \quad (21)$$

Соотношение (21) включает в себя два важных интервала корреляций: (а) (-1,0) интервал антикорреляций и (б) (0,1) интервал истинных корреляции.

Таблица 1. Результат деления матрицы Mt на саму себя и выбора элементов, удовлетворяющих критерию (21)

	Cl	C2	C3	C4	C5	C6	C7	C8	C9	C10	Cl1	C12	C13	C14
C1	**44**	28	28	13	24	29	11	25	20	42	31	11	22	6
C2	18	**44**	18	5	12	16	12	18	5	18	17	4	11	2
C3	18	28	**44**	12	24	23	15	27	18	18	23	10	25	4
C4	33	41	34	**44**	39	37	30	39	32	33	42	18	36	11
C5	22	34	22	7	**44**	25	19	28	14	22	24	5	18	3
C6	21	22	35	26	37	**44**	30	33	29	25	30	19	27	12
C7	35	34	31	16	27	31	**44**	37	24	35	37	13	28	5
C8	21	28	19	7	18	17	9	**44**	11	21	22	3	17	0
C9	26	41	28	14	32	34	22	35	**44**	26	37	12	29	4
C10	43	28	28	13	24	29	11	25	20	**44**	31	11	22	6
C11	15	29	23	4	22	26	9	24	9	15	**44**	5	28	0
C12	35	42	36	28	41	39	33	43	34	35	41	**44**	38	15
C13	24	35	21	10	28	27	18	29	17	24	18	8	**44**	6
C14	40	43	42	35	43	43	41	42	42	40	43	31	40	**44**

Комментарии к таблице 1. В этой таблице показано количество элементов, входящих в интервал (21), полученных в результате деления матриц друг на друга. Следует отметить, что данная матрица является асимметричной, поскольку количество элементов рассчитывается в соответствии с (21) в соотношении col(x)/cols(y) ≠ col(y)/cols(x). Следует также отметить, что на главной диагонали этой матрицы количество элементов достигает максимального значения, равного 44.

В таблице 1 C1 – C5 соответствуют уравнениям (1) – (5) с одним вариантом порождающего полинома, C6 – C10 с другим вариантом порождающего полинома. Матрицы C11 – C14 соответствуют генераторам псевдослучайных чисел Matlab, Python, Mathcad, C++. При анализе таблицы примем две градации 29 и 39 в качестве критерия близости матриц. Соответственно, данные градации выделены в таблице 1 светло-серым и темно-серым цветом. В таблице 1 наибольшим числом 12 превышений значения 39 обладает строка C14, далее идет строка C12 с 5 превышениями значения 39, и строка C3 с 3 превышениями. Строка C14 имеет общие черты со всеми оцененными в работе матрицами

генераторов, оставшиеся 2 значения в ней превышают 29. В С12 имеется 7 значений, превышающих 29, в строке С4 таких значений 9, в строке С6 таких значений 5, в строке С7 – 7. Из анализа таблицы 1 следует, что наиболее близким ко всем генераторам С1-С13 является генератор С14 пакета С++. Чуть менее универсальным генератором является С12, встроенный Python, а также генератор, представляющий комбинированный метод Таусворта.

4. Основные результаты и их анализ

В заключение этой работы, необходимо вкратце перечислить основные результаты и подчеркнуть их значимость.

1. *Все* генераторы ПСЧ, полученные на *физических* носителях, отличаются между собой. Чтобы выявить эти отличия, необходимо совершить три последовательных шага, отмеченные в работе и сравнивать уже их проинтегрированные последовательности методом 3D-ДГИ в пространстве признаков, имеющих максимальную размерность по их моментам и корреляциям, с размерностью равной 44.

2. Отличия всех физических генераторов кроются в малых несовершенствах, порождаемых уже его физической структурой. Каждый структурный элемент генератора имеет свои собственные шумы. Эти шумы (случайные флуктуации) отличаются между собой по используемым материалам, по структуре элементной базы и пр. Иными словами, эти генераторы порождают свои "уникальные" шумы и каждый из этих шумов имеет собственный "отпечаток пальца".

3. А существуют ли эталонные шумы, которые не имеют физических недостатков? Один из авторов этой работы смог найти положительный ответ на этот вопрос, ответ на который изложен в статье [15]. Ответ очень простой и одновременно не очень. Любая бесконечная последовательность, получаемая как корень из простого число может служить идеальным генератором ПСЧ, свободным от физической структуры генератора. Как этот факт можно использовать для целей криптографии? Достаточно детальный ответ дан в работе [15] одного из авторов.

4. Само собой разумеется, что метод ДГИ можно применить к универсально классификации все известных странных аттракторов и сравнить их между собой в рамках единой платформы. Авторы этой статьи предполагают использовать этот метод в этом перспективном направлении.

Информация о конфликте интересов. В данной статье отсутствует реальный конфликт интересов.

Список литературы

1. Petrie C. S. A noise-based IC random number generator for applications in cryptography / C. S. Petrie and J. A. Connelly // IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications. – 2000, май. – Vol. 47, no. 5. – P. 615-621, doi: 10.1109/81.847868.
2. Devi D. I. Hardware Random Number Generator Using FPGA / D. I. Devi, S. Chithra and M. Sethumadhavan // Journal of Cyber Security and Mobility, October, 2019. – Vol. 8, no. 4. – P. 409-418, doi: 10.13052/jcsm2245-1439.841.
3. Гавришев, А. А. Оценка свойств хаотических сигналов, влияющих на надежность передачи данных / А. А. Гавришев, Д. Л. Осипов // Научное приборостроение. – 2025. – Т. 35, № 1. – С. 122-128. – EDN PHUZDX.

4. FIPS 140-1, Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-1. U.S. Department of Commerce/NIST, National TechnicalInformation Service, Springfield, VA, 1994. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf (Дата обращения 01.02.2026)
5. Susanti B. H. Evaluation with NIST Statistical Test on Pseudorandom Number Generators based on DMP-80 and DMP-128 / B. H. Susanti, J. Jimmy, M. W. Ardyani // 2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 2022. – P. 166-171, doi: 10.1109/ISRITI56927.2022.10053041.
6. Тестирование на «случайность» генераторов псевдослучайных чисел для стендов полунатурного моделирования асинхронных радиоэлектронных систем / Р. Р. Раупов, С. С. Логинов, И. Н. Фролов, Ю. Р. Буткевич // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. – 2024. – № 4(64). – С. 68-77. – DOI 10.25686/2306-2819.2024.4.68. – EDN TYWPLM.
7. Лавданский, А. А. Оценка статистических свойств последовательностей на выходе комбинационного генератора с помощью графических тестов / А. А. Лавданский, Э. В. Фауре // Системные исследования и информационные технологии. – 2015. – № 2. – С. 39-50. – EDN VEDQWD.
8. Lacković A.V. Local Shannon, Rényi, and Tsallis Entropy for Useful Content Extraction from Choi-Williams and Zhao-Atlas-Marks Time-Frequency Distributions / A.V. Lacković, J. Lerga and M. Tomić // 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Maldives, Maldives, 2022. - P. 1-5, doi: 10.1109/ICECCME55909.2022.9988560.
9. Liu W. Correntropy: Properties and Applications in Non-Gaussian Signal Processing / W. Liu, P. P. Pokharel and J. C. Principe // in IEEE Transactions on Signal Processing. – Vol. 55, no. 11. - P. 5286-5298, Nov. 2007, doi: 10.1109/TSP.2007.896065.
10. ГОСТ Р ИСО 28640-2012. Статистические методы. Генерация случайных чисел.
11. Nigmatullin R.R. Discrete Geometrical Invariants in 3D Space: How Three Random Sequences Can Be Compared in Terms of “Universal” Statistical Parameters /Frontiers Physics // V.8. – P.76, doi: 10.3389/fphy.2020.00076.
12. Nigmatullin R.R. Discrete Geometrical Invariants: How to Differentiate the Pattern Sequences from the Tested Ones? – Published in the Proceedings of the ICFDA conference / R.R. Nigmatullin and A.S. Vorobev // Springer Proceedings in Mathematics & Statistics, January 2019.
13. Nigmatullin, R.R. The "universal" Set of Quantitative Parameters for Reading of the Trendless Sequences / R.R. Nigmatullin, A.S. Vorobev // Fluctuation and Noise Letters. – 2019. – Vol. 18. – No. 4. – 1950023 (19 pages), World Scientific Publishing Company, DOI: 10.1142/S0219477519500238 (SCOPUS).
14. Nigmatullin, R.R. Advanced and sensitive method by discrete geometrical invariants for detection of differences between complex fluids / Nigmatullin, R.R., Vorobev, A.S., Nasybullin et al. // Commun Nonlinear Sci Numer Simulat. - 73 (2019). – P.265–274. – https://doi.org/10.1016/j.cnsns.2019.02.012 , 1007-5704/© 2019 Elsevier
15. Нигматуллин Р. Р. Способ создания дополнительного канала связи, основанного на временных азбуках Морзе / Р.Р. Нигматуллин // Электроника, фотоника и киберфизические системы. - 2023. - Т.3. - №4. – С.80-96.

DISCRETE GEOMETRIC INVARIANTS IN THE ANALYSIS OF PSEUDORANDOM NUMBER GENERATORS

R.R. Nigmatullin, S.S. Loginov

Kazan National Research Technical University named after A.N. Tupolev-KAI
10, K. Marx St., Kazan, 420111, Russian Federation

Abstract. The paper presents the results of the analysis of the most famous pseudorandom number generators by the method of discrete geometric invariants (DGI). It is shown that this method makes it possible to compare different types of pseudorandom number generators, classify generators by time realizations of pseudorandom sequences and find their differences with each other (within the parameters of the DG), which are due to their small physical differences (at the level of their instrument implementations).

Keywords: pseudorandom number generator, randomness testing of sequences, discrete geometric invariants, Mersenne Twister generator.

Статья представлена в редакцию 25.02.2026