Московский физико-технический институт
(государственный университет)

Л. Ю. Бараш

ДИПЛОМНАЯ РАБОТА

Гиперболические автоморфизмы тора и генераторы псевдослучайных чисел

научный руководитель
д. ф.-м. н., проф.
Л. Н. Щур

Черноголовка – 2004 г.

Аннотация

Предложен метод построения генераторов псевдослучайных чисел высокого качества. В его основе лежит использование ансамбля гиперболических автоморфизмов единичного двумерного тора («преобразований кошки») и скрытие части информации. Скрытые переменные вводятся для того, чтобы избавиться от корреляций. Отображения вида «преобразования кошки» приводят к свойствам эргодичности, стохастичности, гиперболичности, которые необходимы для хороших генераторов. Проведен анализ генератора псевдослучайных чисел, на основе результатов теории Percival и Vivaldi, в слегка обобщенном виде. Вычислен период генератора и исследованы полезные свойства генератора. Теория была численно проверена. Кроме этого, проведен набор стандартных статистических тестов, в ходе которых не обнаружено корреляций. Некоторые корреляции, однако, найдены при помощи критерия направленного случайного блуждания. Мы нашли природу этих корреляций и указали способ их минимизации.

Содержание

1 Введение

Методы Монте-Карло исследования явлений из различных областей физики получили широкое распространение с появлением мощных компьютеров. Необходимой задачей для широкомасштабных численных экспериментов методом Монте-Карло является эффективная и машинонезависимая генерация равномерно распределенных случайных чисел. Наиболее широко используются генераторы случайных чисел (Random Number Generators). Конечно, RNG – это простая программа, которая выдает некоторую последовательность чисел. Эта последовательность выглядит как независимые реализации случайной величины, имеющей равномерное распределенные, а также обладает важными свойствами случайной последовательности, но на самом деле произведена детерминистским способом и является псевдослучайной. В течении последних десятилетий произошел большой прогресс в изучении алгоритмов для генераторов случайных чисел.

Имеется ряд общепринятых требований для генератора случайных чисел и его реализации в библиотеках подпрограмм.

- *Статистическая устойчивость.* Значения на выходе идеального RNG должны быть равномерно распределены, корреляции должны отсутствовать. Другими словами, все подпоследовательности любой фиксированной длины должны иметь одну и ту же вероятность попадания в последовательность на выходе генератора. С практической точки зрения, последовательность псевдослучайных чисел должна пройти набор статистических тестов на равномерное распределение и независимость.

- *Непредсказуемость.* В основном это свойство важно для криптографических алгоритмов. Должно быть сложно надежно предсказать a_{n+1} из $(a_0, \ldots, a_n)$ при помощи какого-либо полиномиального алгоритма. Здесь a_n – значение на выходе генератора.

- *Длинный период.* Период должен быть достаточно длинным, чтобы не быть исчерпанным за месяцы компьютерного времени. Численный эксперимент на суперкомпьютере может задействовать 10^9 случайных чисел в секунду в течение многих часов (или месяцев в случае, например, вычислений КХД), поэтому $10^{13} - 10^{16}$ случайных чисел могут вносить вклад в результат эксперимента. Для большинства генераторов использование небольшой части периода T предпочтительнее с точки зрения статистических свойств, чем использование периода целиком. Хорошим правилом является использовать не более $\sqrt{T}$ чисел.

- *Эффективность.* Должна существовать эффективная реализация RNG с точки зрения скорости и использования оперативной памяти.

- *Наличие теории.* Свойства генератора, такие как длина периода, часто могут быть вычислены в точном виде. Для RNG чрезвычайно желательно понимать поведение генератора, а не рассчитывать только на эмпирические тесты. Другими словами, хороший генератор должен быть основательно проанализирован теоретически и, кроме того, пройти статистические тесты.

- *Повторяемость.* Часто полезно повторить ту же самую последовательность псевдослучайных чисел, что возникла в предыдущем запуске приложения. Большинство генераторов псевдослучайных чисел повторяемы, в отличие от последовательностей, генерируемых физическими устройствами. Например, случайный бит можно получить, приготовив кубит $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ и спроектировав его на $\{|0\rangle, |1\rangle\}$, однако последовательность таких случайных битов не будет повторяема.

- *Переносимость* – это возможность генерировать одну и ту же последовательность псевдослучайных чисел на разных платформах.

- *Пропуск кусков.* Для любого большого r должна быть возможность быстро вычислить s_{n+r} напрямую из s_n, не генерируя промежуточные состояния. Здесь s_n – состояние генератора.

- *Правильная инициализация.* Важно, чтобы короткие последовательности, выдаваемые RNG, не имели корреляций; этого не так просто добиться для генераторов с большим объемом информации о состоянии генератора.

В настоящее время используется несколько классов RNG.

- Линейно-конгруэнтные генераторы (LCG) – наиболее известный и, все еще, наиболее широко распространенный в настоящее время класс генераторов. Существует два основных недостатка этого метода. Во-первых, максимальная длина периода мультипликативного LCG с модулем 2^{32} может быть исчерпана за несколько секунд на современной рабочей станции. Во-вторых, LCG не следует использовать в приложениях, имеющих дело со случайными векторами в нескольких размерностях, из-за того, что все точки на выходе LCG будут лежать в пространстве меньшей размерности.

- Генераторы, основанные на сдвиговом регистре, широко используются во многих областях вычислительной физики. Эти RNG быстрые и обладают гигантским периодом при условии правильного выбора примитивных триномов, лежащих в основе таких генераторов [11]. Поэтому они особенно хорошо подходят для приложений, требующих большое количество случайных чисел. Однако, имеются наблюдения корреляций, которые могут привести к систематическим ошибкам в вычислениях Монте-Карло [12, 13, 14, 15, 16].

- Другие генераторы не столь широко распространены, и их свойства исследуются [8, 17].

Кроме того, многие генераторы, используемые сегодня, сравнительно легко поддаются расшифровке.

Мы рассматриваем задачу использования простых нелинейных динамических систем для построения RNG. Конечно, большинство динамических систем не подойдут для этой цели. К примеру, двоичный сдвиг Бернулли $x_{n+1} = 2x_n \pmod 1$, являющийся основным элементом в преобразовании Пекаря, является хаотическим отображением. Он выдаст

последовательность случайных чисел, если начальное значение будет случайным иррациональным числом. Конечно, в реальных вычислениях числа имеют конечное число бит, так что на каждом шагу число оставшихся бит будет уменьшаться, так что такая схема бесполезна для RNG.

Квадратичное (логистическое) отображение также не годится для RNG. Дело в том, что вычисления с вещественными числами постоянной точности приведут к существенным ошибкам на длинных орбитах. Кроме того, последовательность чисел на выходе логистического отображения не имеет равномерного распределения, поскольку инвариантная плотность не является константой.

Следующий класс нелинейных динамических систем – диффеоморфизмы Аносова единичного двумерного тора, которые активно исследовались в контексте эргодической теории. Системы Аносова обладают следующими стохастическими свойствами: эргодичность, перемешивание, экспоненциальная расходимость близких траекторий (которая следует из положительности показателя Ляпунова). Эти свойства напоминают определенные свойства случайности. Каждый диффеоморфизм Аносова тора топологически сопряжен гиперболическому автоморфизму, который является полностью хаотической динамической системой. Гиперболический автоморфизм определяется матрицей 2×2 с целыми числами, единичным детерминантом и вещественными собственными значениями. Часто гиперболические автоморфизмы единичного двумерного тора называют «отображениями кошки», поскольку хаотические свойства этих отображений в литературе традиционно иллюстрируют, рисуя образ изображения кошки [2]. Отметим, что отображения кошки – гамильтоновы системы. В самом деле, действие отображения (1) при $k = \mathrm{Tr}(M) > 2$ на вектор $\binom{p}{q}$ соответствует движению, определяемому гамильтонианом $H(p,q) = \frac{\mathrm{arcsh}(\sqrt{k^2-4}/2)}{\sqrt{k^2-4}}(m_{12}p^2 - m_{21}q^2 + (m_{11} - m_{22})pq)$, где p и q берется по модулю 1 при каждом наблюдении, проводимом в целочисленные моменты времени. Преобразование кошки сохраняет площадь, в силу того, что у него единичный детерминант. Это важное свойство, очевидно, оно имеется у всех гамильтоновых систем, поскольку теорема Лиувилля гарантирует сохранение фазового объема во временной эволюции системы.

Эмпирические исследования показали, что использования одного преобразования кошки недостаточно для построения хорошего RNG из-за наличия существенных корреляций на выходе генератора. Мы увидим, что использование ансамбля гиперболических автоморфизмов тора и частичное скрытие информации позволяет существенно уменьшить корреляции и создать хороший RNG.

В разделе 2 представлен RNG, основанный на этой идее. В разделе 3 мы исследуем свойства генератора. В частности, предложен метод вычисления периода генератора для произвольных параметров отображения и решетки. Этот метод основан на работе Персиваля и Вивальди [3], в которой показано, как задача изучения периодических орбит преобразований кошки может быть сведена к проблемам арифметики алгебраических чисел (фактически к вычислениям в кольцах квадратичных чисел). Как показано в разделе 3, типичная длина периода генератора равна $T_m = 3 \times 2^{m-3}$ для решетки $2^m \times 2^m$. Кроме того, в разделе 4 будет показано, что последовательность на выходе RNG проходит набор стандартных статистических тестов на равномерное распределение и на независимость.

2 Генератор

Рассмотрим гиперболические автоморфизмы единичного двумерного тора (квадрата $(0,1]\times(0,1]$ с отождествленными противоположными сторонами). Действие автоморфизма определяется матрицей

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \in SL_2(\mathbb{Z}). \tag{1}$$

Элементы матрицы M – целые числа, кроме того $\det M = 1$ и $|\mathrm{Tr}(M)| > 2$. Отображение кошки действует в два этапа. На первом этапе отображение M действует на вектор $\binom{p}{q}$, на втором этапе берется дробная часть обоих координат p и q в фазовом пространстве.

Легко показать, что все периодические орбиты гиперболического автоморфизма тора состоят из точек с рациональными координатами. Поэтому естественно рассмотреть множество точек с координатами, имеющими один и тот же знаменатель g. Для RNG, имеющего эффективную реализацию на компьютере, естественно ограничиться случаем $g = 2^m$.

Состояние генератора случайных чисел включает в себя s точек, лежащих на решетке $2^m \times 2^m$ на торе:

$$\binom{x_i^{(0)}/2^m}{y_i^{(0)}/2^m}, i = 0, 1, \ldots, (s-1). \tag{2}$$

Здесь $x_i^{(0)}, y_i^{(0)} \in \{0, 1, \ldots, 2^m - 1\}$.

На каждом шаге эти точки преобразуются при помощи отображения M:

$$\binom{x_i^{(n)}/2^m}{y_i^{(n)}/2^m} = M\binom{x_i^{(n-1)}/2^m}{y_i^{(n-1)}/2^m} \pmod 1, i = 0, 1, \ldots, (s-1). \tag{3}$$

Здесь операция $\bmod\ 1$ означает взятие дробной части вещественного числа. По-другому действие преобразования кошки можно записать следующим образом:

$$\binom{x_i^{(n)}}{y_i^{(n)}} = M\binom{x_i^{(n-1)}}{y_i^{(n-1)}} \pmod{2^m}, i = 0, 1, \ldots, (s-1). \tag{4}$$

Осталось определить последовательность $\{a^{(n)}\}$, которая будет на выходе генератора. Пусть $\alpha_i^{(n)}$ – первый бит $x_i^{(n)}$: $\alpha_i^{(n)} = [x_i^{(n)}/2^{m-1}]$. Тогда искомое число на выходе генератора будет следующим: $a^{(n)} = \sum_{i=0}^{s-1} \alpha_i^{(n)} \cdot 2^n$. Другими словами, $a^{(n)}$ – это s-битовое целое число, которое состоит из первых битов чисел $x_0^{(n)}, x_1^{(n)}, \ldots, x_{s-1}^{(n)}$.

Мы видим, что построенный RNG содержит много скрытой информации. Именно, все биты точек $\binom{x_i^{(n)}}{y_i^{(n)}}$, которые не участвуют в построении значения $a^{(n)}$ являются скрытыми переменными.

Таким образом, основными ингредиентами предложенного метода является применение хаотических свойств движения Аносова и рассмотрение ансамбля систем с частичным скрытием информации. Преобразования кошки приводят к свойствам эргодичности,

стохастичности, гиперболичности, которые необходимы для хороших генераторов. Скрытые переменные уменьшают корреляции и существенно усложняют задачу расшифровки RNG.

Заметим, что для последовательности на сдвиговом регистре, которая широко используется в качестве RNG высокого качества, процедуру генерации можно написать явно в виде динамической системамы. Пусть в некоторый момент состояние регистра – $\mathbf{v_{n-1}} = (a_{n-r}, a_{n-r+1}, \ldots, a_{n-1})$. В следующий момент состоянием сдвигового регистра будет $\mathbf{v_n} = (a_{n-r+1}, a_{n-r+2}, \ldots, a_n)$, где $a_n = c_r a_{n-r} + c_s a_{n-s} \pmod 2$. Другими словами, $\mathbf{v_{n+1}} = A\mathbf{v_n} \pmod 2$, где A – некоторая $r \times r$-матрица. Простейшие случаи можно описать матрицами 2×2. Например, последовательность Фибоначчи $a_n = a_{n-1}+a_{n-2} \pmod 2$ можно записать как $\binom{a_n}{a_{n-1}} = A\binom{a_{n-1}}{a_{n-2}}$, где $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Заметим, что $A^2 \in SL_2(\mathbb{Z})$ является преобразованием кошки.

Действие линейно-конгруэнтных генераторов часто тоже можно записать в виде действия гиперболического автоморфизма двумерного единичного тора. Действительно, рассмотрим генератор $x_{t+1} = cx_t \pmod p$, где p – простое число. Пусть g – примитивный элемент в группе $\mathbb{Z}_p^*$, т.е. g – натуральное число и наименьшее число s такое что $g^s \equiv 1 \pmod p$ – это $s = p-1$. Обычно существует матрица $M \in SL_2(\mathbb{Z})$ такая, что

$$M\begin{pmatrix} g^k \\ g^{k+l} \end{pmatrix} \equiv \begin{pmatrix} g^{k+1} \\ g^{k+l+1} \end{pmatrix} \pmod p. \tag{5}$$

Здесь l выбрано так, чтобы $bg^l + a - g \equiv 0 \pmod p$, а условия, при помощи которых можно найти матрицу, следующие: $M \in SL_2(\mathbb{Z})$, $\exists q : q^2 \equiv Tr(M)^2 - 4 \pmod p$, $2g \equiv Tr(M) \pm q \pmod p$. Это позволяет сформулировать при помощи преобразования кошки модель «генератора» $x_{t+1} = gx_t \pmod p$, и, следовательно, генератора $x_{t+1} = cx_t \pmod p$. Детальное описание этой модели может быть найдено в [18].

Отметим также, что даже небольшие отклонения от схемы RNG, представленной в этом разделе (например, конструирование $a^{(n)}$ из различных или не старших битов $x_0^{(n)}, x_1^{(n)}, \ldots, x_{s-1}^{(n)}$), приводят к появлению корреляций и ухудшению свойств RNG. Это было получено эмпирически.

3 Периодические орбиты преобразования кошки на решетке $2^n \times 2^n$ и период генератора

В этом разделе приведен обзор основных арифметических методов изучения периодов орбит, которые предложены в [3]. Результаты о периодах орбит на решетке $2^n \times 2^n$ обобщены. На этой основе проведено исследование периода генератора из раздела 2.

3.1 Динамика гиперболических автоморфизмов и кольца квадратичных целых чисел

Действие автоморфизма единичного двумерного тора определяется матрицей (1). Элементы матрицы M – целые числа, ее детерминант равен единице. Кроме того, собственные числа матрицы M, равные $\lambda = \frac{k \pm \sqrt{k^2-4}}{2}$, где $k = \mathrm{Tr}(M)$, должны быть вещественны (известно, что для комплексных λ отображение тора M не является даже эргодичным). Поэтому дополнительное условие гиперболичности отображения заключается в том, что $|k| > 2$.

Обычно из всех матриц со следом k выделяют одну матрицу, такую, для которой связь между свойствами орбит автоморфизма тора и арифметикой квадратичных целых чисел наиболее прозрачна. А именно, элементы матрицы (1) выбираются так, чтобы

$$\begin{cases} \lambda &= m_{11} + \tau m_{21} \\ \lambda\tau &= m_{12} + \tau m_{22} \end{cases} \tag{6}$$

Здесь τ – базисный элемент кольца квадратичных целых $R_D = \{a + b\tau : a, b \in \mathbb{Z}\}$, в котором лежит λ. Это означает, что $k^2 - 4 = n^2 D$, где целое число D свободно от квадратов и

$$\begin{cases} \tau = \sqrt{D} & \text{при } D \not\equiv 1 \pmod 4 \text{ (это может быть только для четных } k); \\ \tau = \frac{1}{2}(1 + \sqrt{D}) & \text{при } D \equiv 1 \pmod 4. \end{cases}$$

Легко проверить, что если элементы матрицы выбрать по правилу (6), то для любых целых x, y, x', y' равенство $x' + y'\tau = \lambda(x + y\tau)$ равносильно равенству $\binom{x'}{y'} = M\binom{x}{y}$. В самом деле, $\lambda(x + y\tau) = \lambda x + (\lambda\tau)y = (m_{11}x + m_{12}y) + (m_{21}x + m_{22}y)\tau = x' + y'\tau$. Таким образом, действие автоморфизма M соответствует умножению на квадратичное число λ, действие же автоморфизма M^{-1} соответствует умножению на λ^{-1}, поэтому для длины орбиты неважно, какое из двух собственных чисел $\lambda_{1,2} = \frac{k \pm \sqrt{k^2-4}}{2}$ выбирать. Для определенности, можно всегда выбирать большее из них.

Вообще говоря, существует бесконечно много матриц в $SL_2(\mathbb{Z})$, имеющих один и тот же след k. Вопрос о том, верно ли, что они все обладают одними и теми же свойствами орбит, окончательно не решен, однако рассуждения, приведенные в [3] свидетельствуют о том, что скорее всего это верно.

3.2 Инвариантные подрешетки на торе и разложение на множители квадратичных идеалов

Итак, каждому элементу R_D соответствует некоторая точка на целочисленной решетке. Пусть $\langle g \rangle = \{ag + bg\tau : a, b \in \mathbb{Z}\}$ – принципиальный квадратичный идеал, порожденный числом g. Он соответствует точкам целочисленной решетки, координаты которых делятся на g. Определим сравнение по модулю идеала A как $\xi \equiv \eta \pmod A \Leftrightarrow (\xi - \eta) \in A$. Тогда периодом точки тора $\binom{x/g}{y/g}$ при отображении M является наименьшее T, такое что $\lambda^T z \equiv z \pmod{\langle g \rangle}$, где $z = x + y\tau$.

Каждый квадратичный идеал A соответствует некоторой подрешетке на $\mathbb{Z}^2$. При этом поскольку λ имеет единичную норму, то $\lambda A = A$, т.е. эта подрешетка инвариантна относительно умножения на λ. Для задачи классификации орбит интересны подрешетки $\mathbb{Z}^2$, которые не меняются при сдвиге на любой элемент $\binom{ag}{bg}$, где $a, b \in \mathbb{Z}$. Их можно считать подрешетками тора, а не просто подрешетками $\mathbb{Z}^2$. Такие подрешетки соответствуют лишь тем идеалам A, которые делят $\langle g \rangle$. Итак, разложение $\langle g \rangle$ на простые идеалы предоставляет нам полную информацию об инвариантных подрешетках тора.

3.3 Классификация простых идеалов и периоды орбит для решетки $2^n \times 2^n$

Для наших целей достаточно разложить на простые множители идеал $\langle 2^s \rangle = \langle 2 \rangle^s$. Это сводится к разложению на простые множители идеала $\langle 2 \rangle$. Напомним, что идеал $\langle 2 \rangle$ называется инертным, если $\langle 2 \rangle$ простой идеал; расщепленным, если $\langle 2 \rangle = P_1 P_2$, где P_1 и P_2 – простые идеалы; разветвленным, если $\langle 2 \rangle = P_1^2$, где P_1 – простой идеал. Инертным, расщепленным и разветвленным случаями исчерпывается задача разложения $\langle 2 \rangle$ на простые идеалы. $\langle 2 \rangle$ инертен, если $D \equiv 5 \pmod 8$; расщеплен, если $D \equiv 1 \pmod 8$; разветвлен, если $D \not\equiv 1 \pmod 4$.

Таким образом, если k нечетно, то $k^2 - 4 \equiv 5 \pmod 8 \Rightarrow D \equiv 5 \pmod 8$, т.е. $\langle 2 \rangle$ инертен. Если $k \equiv 0 \pmod 4$, то найдется некоторое $n_1 \in \mathbb{Z}$, такое что $\frac{k^2-4}{4} = n_1^2 D \equiv 3 \pmod 4 \Rightarrow D \equiv 3 \pmod 4$, т.е. $\langle 2 \rangle$ разветвлен. Если $k \equiv 2 \pmod 4$, то найдется $n_1 \in \mathbb{Z}$, такое что $\frac{k^2-4}{4} = n_1^2 D \equiv 0 \pmod 4$, т.е. никаких ограничений на D отсюда не следует, $\langle 2 \rangle$ может быть как инертен, так и расщеплен или разветвлен.

Введем обозначения: T_n – период свободных орбит при $g = 2^n$, T'_n – период тех идеальных орбит при $g = 2^n$, которые не лежат целиком на подрешетке $\frac{g}{2} \times \frac{g}{2}$. Напомним, что идеальная орбита – это орбита, лежащая в подрешетке, соответствующей некоторому идеалу, который делит $\langle g \rangle$, но отличен от $\langle 1 \rangle$. Свободная орбита – это любая другая орбита.

Из утверждений, доказанных в [3], следует поведение орбит на решетке 2×2. А именно

- если $\langle 2 \rangle$ инертен, то либо $T_1 = 3$, либо $T_1 = 1$, все орбиты свободны.
- если $\langle 2 \rangle$ расщеплен, то $T_1 = T'_1 = 1$, одна свободная орбита и две идеальных.
- если $\langle 2 \rangle$ разветвлен, то $T_1 = 2, T'_1 = 1$, одна свободная орбита и одна идеальная (возможно также, что $T_1 = 1, T'_1 = 1$, две свободные орбиты и одна идеальная).

Чтобы лучше понять, как устроены орбиты на решетке $2^n \times 2^n$, мы доказали следующее утверждение.

Теорема.

1. $\forall n$: либо $T_{n+1} = 2T_n$, либо $T_{n+1} = T_n$
2. $\forall n$: либо $T'_n = T_n$, либо $T'_n = T_{n-1}$
3. $\forall n \geq 3$: $T_n \neq T_{n-1} \Rightarrow T_{n+1} \neq T_n$

4. Пусть $n \geq 3$ и $T_n = 2T_{n-1}$. Тогда $T'_n = T_n/a \Rightarrow T'_{n+1} = T_{n+1}/a$ (здесь $a = 1$ или $a = 2$)

Более того, в расщепленном случае (т.е. если идеал $\langle 2 \rangle$ расщеплен) всегда выполняется $T'_n = T_n$, а в инертном случае вводить T'_n нет никакой необходимости, поскольку все идеальные орбиты лежат на подрешетке $\frac{q}{2} \times \frac{q}{2}$.

Эта теорема является обобщением теорем C_1 и C_2 статьи [3]. Доказательство приведено ниже, в приложении А.

Таким образом, зная T_n и T'_n для очень небольших n, применяя теорему, мы знаем периоды всех орбит на решетке $2^n \times 2^n$ для любого n. При этом всегда найдутся n_1, n_2, n_3, такие что $T_n = T_1 2^{n-n_1}$, $T'_n = T_1 2^{n-n_2}$ для всех $n \geq n_3$.

Заметим, что в случае, когда $\langle 2 \rangle$ инертен, все идеалы (идеалы-делители $\langle 2^n \rangle = \langle 2 \rangle^n$) сами имеют вид $\langle 2 \rangle^r$, поэтому каждая идеальная орбита – это просто орбита, полностью лежащая на подрешетке $2^{n-1} \times 2^{n-1}$. Т.е. идеальная орбита является свободной орбитой для некоторой решетки $2^r \times 2^r$, где $r < n$ (и наоборот, любая орбита решетки $2^{n-1} \times 2^{n-1}$, для решетки $2^n \times 2^n$ будет идеальной орбитой). Найдем количество свободных орбит в этом случае. Всего для орбит предназначено $2^{2n} - 1$ точек. Идеальные орбиты состоят из $2^{2n-2} - 1$ точек. Следовательно, число свободных орбит: $(2^{2n} - 2^{2n-2})/T_n = 3 \cdot 2^{2n-2}/T_n$.

Отсюда видно, как фазовое пространство поделено на области в характерном инертном случае $T_n = 3 \cdot 2^{n-3}$. Именно,

- 2^{n+1} траекторий имеют период T_n и заметают $3/4$ фазового пространства (а именно, заметаются все точки, не лежащие на подрешетке $2^{n-1} \times 2^{n-1}$).
- 2^n траекторий имеют период $T_{n-1} = T_n/2$ и заметают $3/16$ фазового пространства.
- 2^{n-1} траекторий имеют период $T_{n-2} = T_{n-1}/2$ и заметают $3/64$ фазового пространства.
- можно продолжать далее, это справедливо вплоть до траекторий, содержащих лишь несколько точек.

3.4 Период генератора

Вернемся к изучению периода генератора псевдослучайных чисел. Итак, мы задаем начальные условия: $x_i^{(0)}, y_i^{(0)}$, $i = 0, 1, \ldots, (s-1)$, где $x_i^{(0)}, y_i^{(0)}$ – целые числа от 0 до $2^m - 1$, которые задают рациональную точку $\binom{x_i^{(0)}/2^m}{y_i^{(0)}/2^m}$ на единичном торе. Мы определяем $\binom{x_i^{(n)}}{y_i^{(n)}}$ при помощи выражения (4), где M – заданный заранее автоморфизм тора. Мы хотим определить период в последовательности $\{a^{(i)}\}$, где s-битное число $a^{(i)}$ состоит из первых битов чисел $x_0^{(i)}, x_1^{(i)}, \ldots, x_{s-1}^{(i)}$.

Для подавляющего большинства начальных условий период последовательности $\{a^{(i)}\}$ будет равен периоду T_m свободных орбит заданного автоморфизма тора. Действительно, если хотя бы одна из точек $\binom{x_b^{(0)}}{y_b^{(0)}}$ лежит на свободной орбите (вероятность этой ситуации в инертном случае равна $(1 - 4^{-s})$), то период вряд ли будет меньше, чем период свободных орбит T_m.

Более аккуратно: он будет не меньше, чем период последовательности первых битов чисел $x_b^{(i)}, i = 0, 1, 2, \ldots$. Возникает вопрос, равен ли период последовательности из первых битов точек орбиты периоду T_m самой орбиты. Конечно, для подавляющего большинства орбит это именно так (лишь для очень коротких орбит можно обнаружить отдельные случаи, когда это не так).

С другой стороны, период каждой орбиты на торе делит T_m, поэтому период последовательности $\{a^{(i)}\}$ не может быть больше, чем T_m.

В характерном примере инертного случая $M = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$ имеем $T_m = 3 \times 2^{m-3}$.

Экспериментальная численная проверка полностью подтвердила этот факт для указанного инертного случая ($M = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$). А именно, при $m = s = 14$, программа 1000 раз случайным образом задавала начальные условия, и каждый раз период последовательности $\{a^{(i)}\}$ оказывался равным $6144 = 3 \times 2^{11}$. Тонкий вопрос в алгоритме этой программы заключался в том, как правильно определить, в какой момент достигнут период. Он был решен аккуратно (чтобы период был равен T, нужно чтобы состояние генератора (все точки, а не только $\{a^{(i)}\}$) в момент T полностью совпало с состоянием в начальный момент времени и, кроме того, чтобы не существовало меньшего периода, являющегося делителем T).

Итак, мы получили, что период генератора псевдослучайных чисел совпадает с периодом свободных орбит автоморфизма тора, выяснили интересные свойства этих орбит и указали простой способ нахождения периода в каждом случае.

4 Статистические тесты

Для сравнения, все результаты представлены сразу для двух генераторов: генератора, реализованного функцией `random()` в системе `FreeBSD` (слева) и генератора, основанного на автоморфизме тора $\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$ с фиксированными (но выбранными наугад) начальными значениями (справа). Параметры: сетка на единичном торе $g \times g$, где $g = 2^m = 2^{28} = 268435456$, период генератора совпадает с периодом свободных орбит автоморфизма тора и равен $T_m = 3 \cdot 2^{m-3} = 100663296$. На выходе генератора 28-битное число (т.е. $k = m = 28$).

4.1 Критерий равномерности

На рис. 1 представлена эмпирическая функция распределения 500 полученных последовательно значений генератора. Видно, что гипотеза о равномерном распределении значений вполне правдоподобна. Значения K_{500}^+ и K_{500}^- показывают, что тест КС по этим 500 значениям пройден.

Более убедительно гипотезу о равномерном распределении подтверждают результаты, приведенные на рис. 2 и рис. 3. Было проведено 20 проверок по КС, в каждой из которых

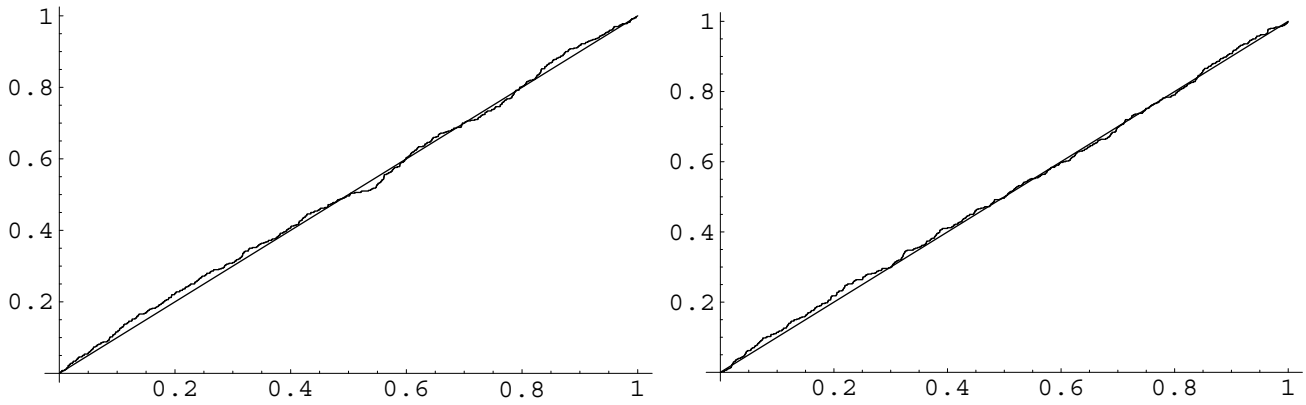


Рис. 1: Эмпирическая функция распределения 500 последовательных значений генератора.

участвовало 10^6 значений генератора, и были вычислены K^+ и K^-. На рис. 2 и рис. 3 приведены эмпирические функции распределения двадцати величин $P(K^+)$ и $P(K^-)$ соответственно, где $P(x)$ – теоретическая функция распределения величин K^+ и K^- (формула (25) параграфа 3.3.1 Кнута [8]). Из рис. 2 и рис. 3 следует, что все 20 тестов КС успешно пройдены (более того, значения K^+ и K^- на выходе этих тестов распределены согласно теоретической функции распределения).

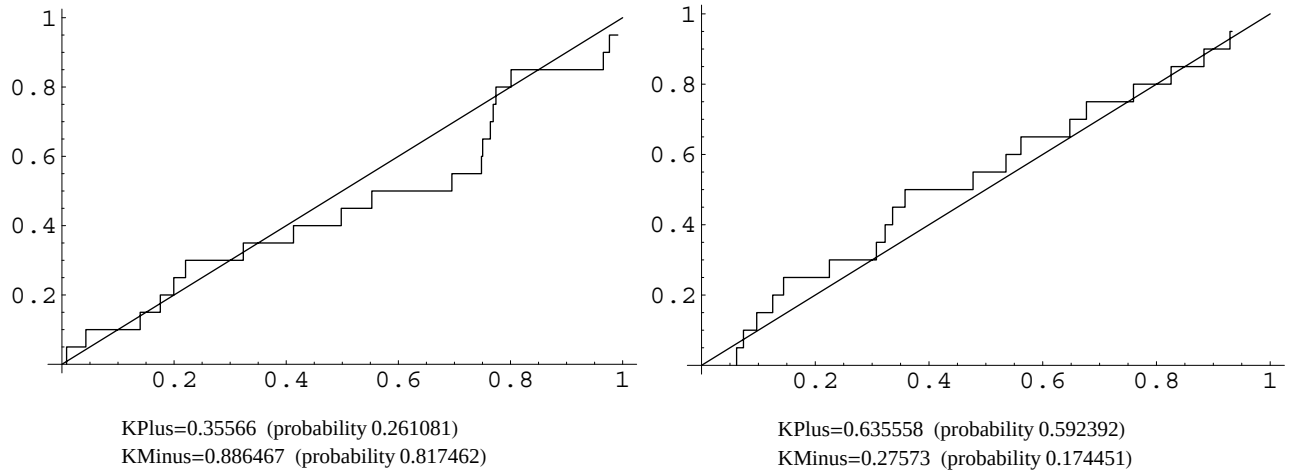
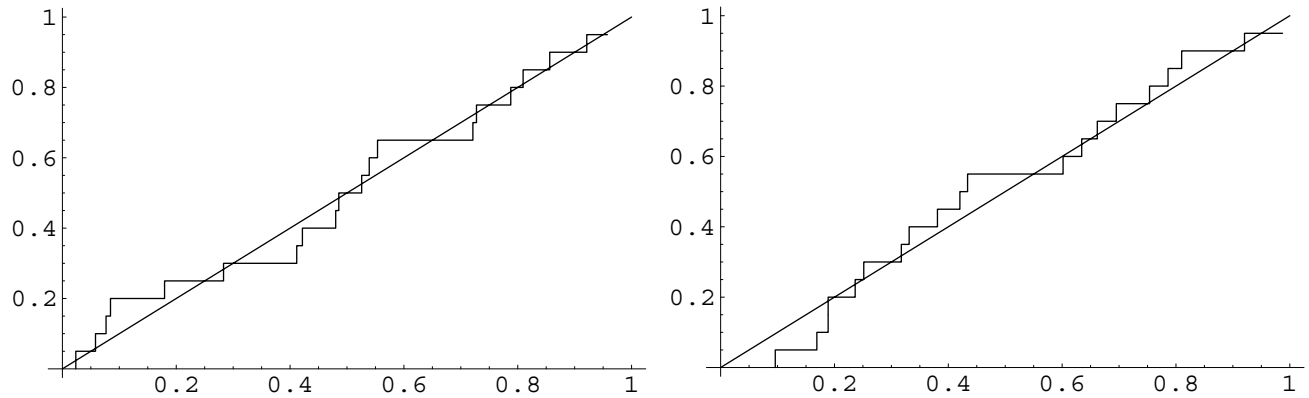


Рис. 2: Критерий равномерности: распределение величин $P(K^+)$.

4.2 Критерий серий

Произведено 20 χ^2-проверок по критерию серий, так, как указано в [8]. Параметры: $d = 8 \;\Rightarrow\; \nu = d^2 - 1 = 63$. В каждой проверке участвовало $n = 10^6$ значений гене-

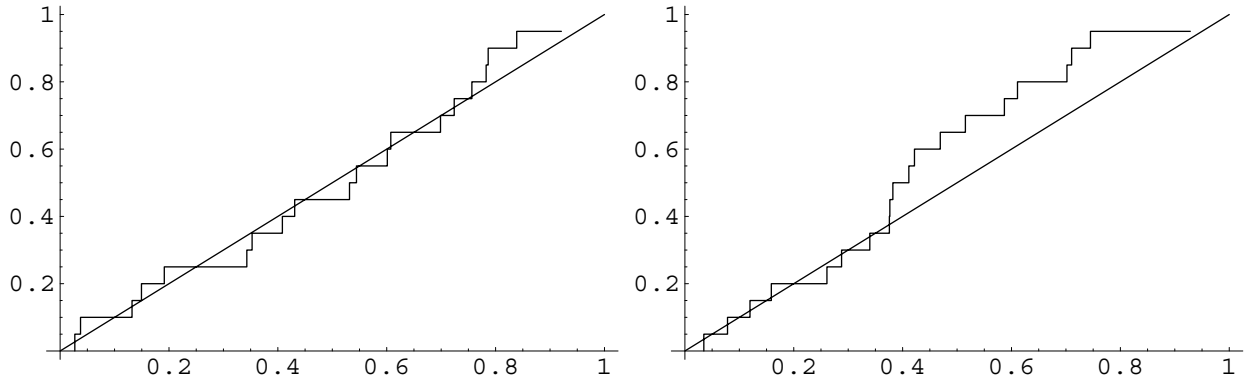


KPlus=0.516603 (probability 0.454412)
KMinus=0.499551 (probability 0.433859)

KPlus=0.519385 (probability 0.457758)
KMinus=0.532399 (probability 0.473379)

Рис. 3: Критерий равномерности: распределение величин $P(K^-)$.

ратора. На рис. 4 изображена эмпирическая функция распределения двадцати величин $P(V_i)$, где $V_i, i = 1, \ldots, 20$ – результаты χ^2-статистики для каждого теста (формула (6) параграфа 3.3.1 Кнута [8]), $P(x)$ – теоретическое распределение величины V (формула (22) параграфа 3.3.1 Кнута [8]). Как видим, все 20 тестов успешно пройдены (более того, значения V_i на выходе этих тестов распределены согласно теоретической функции распределения).



KPlus=0.508209 (probability 0.444301)
KMinus=0.415837 (probability 0.333075)

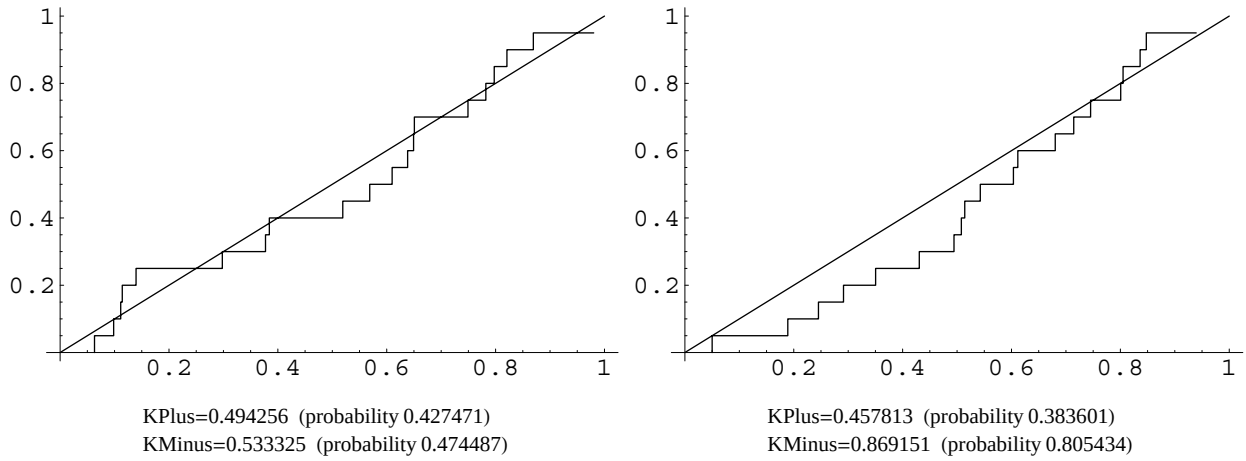
KPlus=0.916551 (probability 0.837112)
KMinus=0.272519 (probability 0.17128)

Рис. 4: Критерий серий.

4.3 Критерий монотонности

Произведено 20 χ^2-проверок по критерию монотонности так, как указано в [8]. (параграф 3.3.2 и упр.14 к нему). Параметры: $\nu = 5$, т.е. отслеживаются восходящии серии длин

1,2,3,4,5, а также длины $\geqslant 6$. Как обычно, $n = 10^6$. Все тесты пройдены. Результаты χ^2-проверок изображены на рис. 5 по тому же принципу, что и результаты критерия серий.



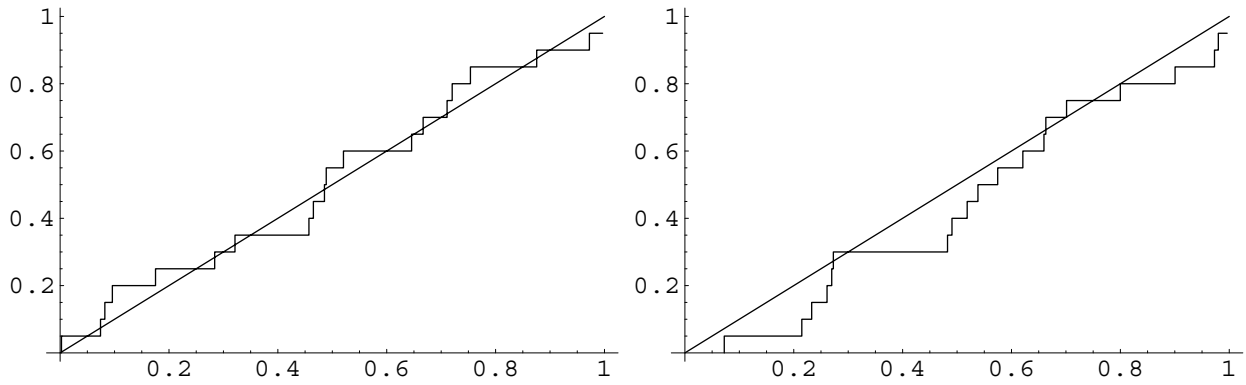
KPlus=0.494256 (probability 0.427471)
KMinus=0.533325 (probability 0.474487)

KPlus=0.457813 (probability 0.383601)
KMinus=0.869151 (probability 0.805434)

Рис. 5: Критерий монотонности.

4.4 Критерий «максимум-t»

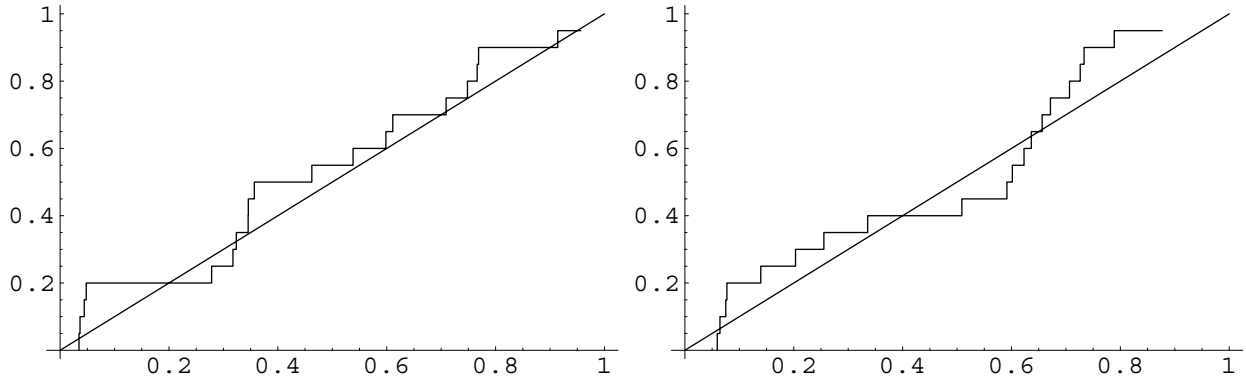
Произведено 20 КС-проверок по критерию "максимум-t" так, как указано в [8]. Параметры: $t = 5$, $n = 10^6$. Тесты пройдены. Результаты КС-проверок изображены на рис. 6 и рис. 7 по тому же принципу, что и результаты критерия равномерности.



KPlus=0.465303 (probability 0.392589)
KMinus=0.478867 (probability 0.408911)

KPlus=0.218477 (probability 0.120912)
KMinus=0.816017 (probability 0.765201)

Рис. 6: Критерий "максимум-t": распределение величин $P(K^+)$.



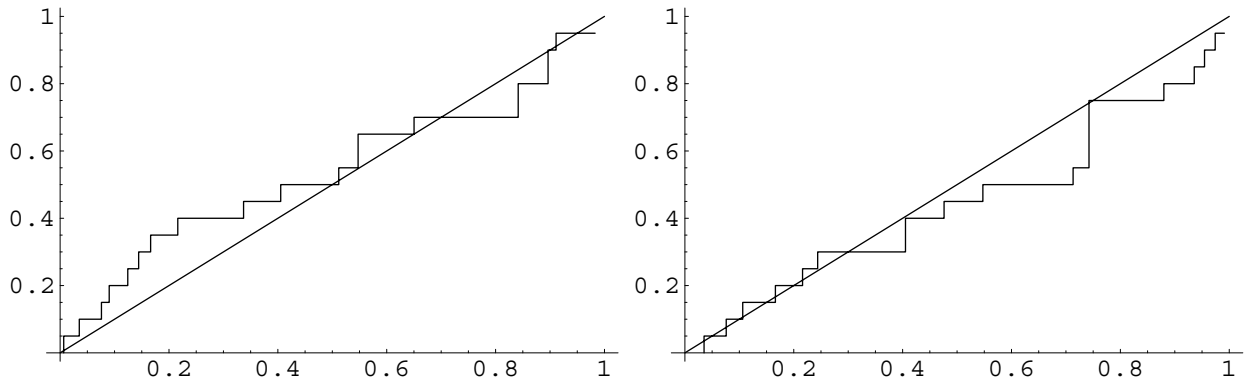
KPlus=0.68002 (probability 0.639652)
KMinus=0.350276 (probability 0.254841)

KPlus=0.745532 (probability 0.704026)
KMinus=0.633102 (probability 0.589702)

Рис. 7: Критерий "максимум-t": распределение величин $P(K^-)$.

4.5 Критерий конфликтов

Произведено 20 проверок по критерию конфликтов так, как указано в [8]. Параметры: $m = 2^{20}$, $n = 2^{14}$. В каждой проверке вычисляется число конфликтов c, а также теоретическая вероятность того, что число конфликтов $\leqslant c$. На рис. 8 приведена эмпирическая функция этих двадцати вероятностей. Как видим, все тесты пройдены.



KPlus=0.822216 (probability 0.770155)
KMinus=0.632883 (probability 0.589462)

KPlus=0.250797 (probability 0.150537)
KMinus=0.953218 (probability 0.858955)

Рис. 8: Критерий конфликтов.

5 Критерий направленного случайного блуждания

5.1 Описание теста

Тест на случайное блуждание оказывается одним из наиболее мощных и чувствительных тестов на наличие корреляций в генераторах случайных чисел. В частности, тест с использованием идеи случайного блуждания был одним из тестов, выявивших корреляции в генераторах случайных чисел типа «сдвиговый регистр» [13]. Другой тест на случайное блуждание позволил объяснить природу этих корреляций [10]. Некоторые тесты на случайное блуждание достаточно просты для теоретического анализа и позволяют достичь ясной картины механизма корреляций в генераторах случайных чисел.

Существует несколько вариаций теста на случайное блуждание, в различном количестве измерений [9]. Мы рассмотрим одномерную модель направленного случайного блуждания [10]: однонаправленное блуждание начинается в некотором узле одномерной решетки и, при дискретных значениях времени i, или происходит шаг длины 1 с вероятностью μ, или блуждание останавливается с вероятностью $1-\mu$. В последнем случае начинается новое блуждание. Вероятность блуждания длиной n равна $P(n) = \mu^{n-1}(1-\mu)$, а средняя длина блуждания равна $\langle n \rangle = 1/(1-\mu)$. Отметим, что эта модель представляет собой эффективный метод Вольфа для одномерной модели Изинга [10]. Это можно увидеть из того, что средний размер кластера в методе Вольфа равен средней длине блуждания для $\mu = \tanh(J/k_BT)$, где J – константа связи спинов.

5.2 χ^2-проверки

Произведено 20 χ^2-проверок по критерию направленного случайного блуждания с $\mu = 1/2$. Используется "Алгоритм P" случайного блуждания, т.е. при $r < \mu$ мы совершаем шаг вправо, при $r \geqslant \mu$ останавливаемся, где $r \in [0,1)$ – случайное число, порожденное генератором. Таким образом, $\mu = 1/2$ означает, что в проверках участвует лишь один бит генератора. Параметры χ^2-критерия: $\nu = 6$, т.е. отслеживаются блуждания, покрывающие 1,2,3,4,5,6 узлов, а также $\geqslant 7$ узлов. Результаты для $n = 10^6$ приведены на рисунке 9. Мы видим, что для генератора, основанного на автоморфизме тора, распределение величин V_i на выходе тестов существенно отличается от χ^2-распределения, хоть каждый из двадцати тестов и пройден в том смысле, что имеет вполне приемлимое значение V_i на выходе (с точки зрения того же χ^2-распределения).

Чтобы получить более полную картину, мы провели дополнительные проверки

- сменив алгоритм P на алгоритм N случайного блуждания
- перед каждым новым тестом выставляя начальные значения генератора случайным образом (чтобы они не обязательно совпадали с конечными значениями предыдущего теста)
- взяв $g = 2^{31}$, чтобы период генератора был существенно больше n
- экспериментировали с различными значениями n

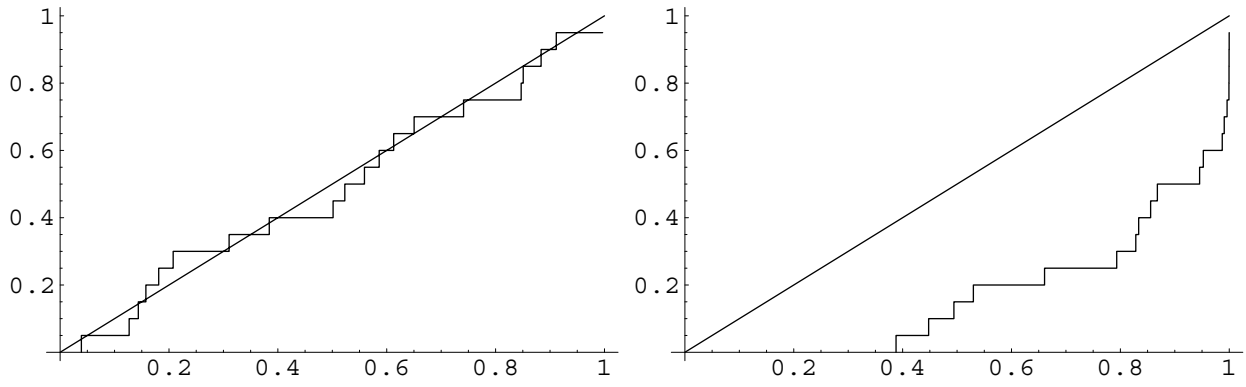


Рис. 9: Результаты двадцати χ^2-проверок по критерию направленного случайного блуждания. $n = 10^6$. Слева – генератор random() системы FreeBSD, справа – генератор на автоморфизме тора

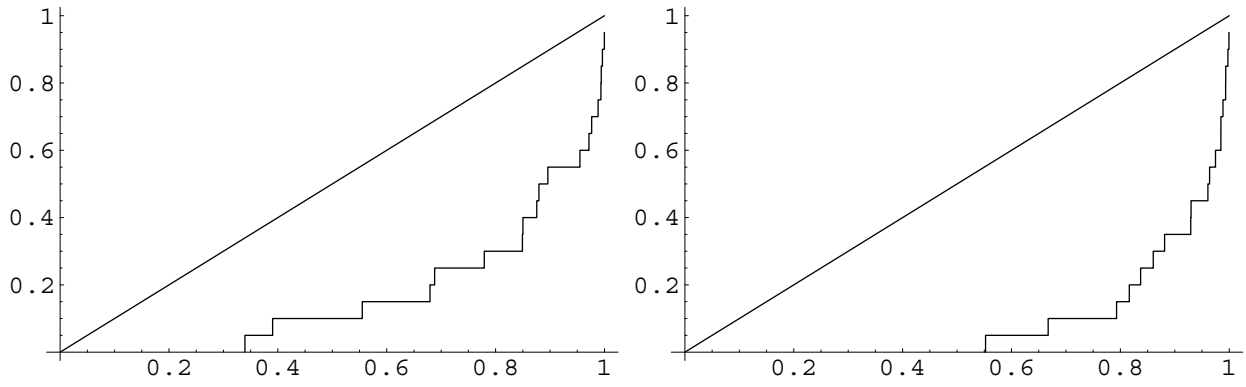
Результаты представлены на рис. 10,11,12 и свидетельствуют, что корреляции, обнаруженные при помощи критерия случайного блуждания, существенны. Природа этих корреляций выявлена в следующем разделе.

5.3 Природа корреляций в тесте на случайное блуждание

Детальные результаты теста на случайное блуждание представлены на рисунке 13. Проведено 100 χ^2-проверок, каждая из которых включала в себя $n = 10^7$ случайных блужданий с $\mu = 1/2$. Таким образом, использовался лишь первый бит генератора с $M = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$. После каждой χ^2-проверки подсчитывалось значение $\delta P_s = (Y_s - np_s)/(np_s)$ для всех $s \leq 7$. Здесь s – длина блуждания, а p_s – теоретическая вероятность блуждания длины s, в предположении, что случайные числа не имеют корреляций, Y_s – число блужданий длины s. Заметим, что корреляции можно обнаружить только собрав статистику по достаточно большому числу случайных блужданий. Например, для $n = 10^5$ корреляции обнаружены не были.

Таким образом, тест на случайное блуждание выявляет существенные корреляции. Из рисунка 13 видно, что на выходе генератора псевдослучайных чисел некоторые последовательности из пяти бит появляются с частотой, отличной от 1/32, т.е. не все последовательности из пяти бит равноправны.

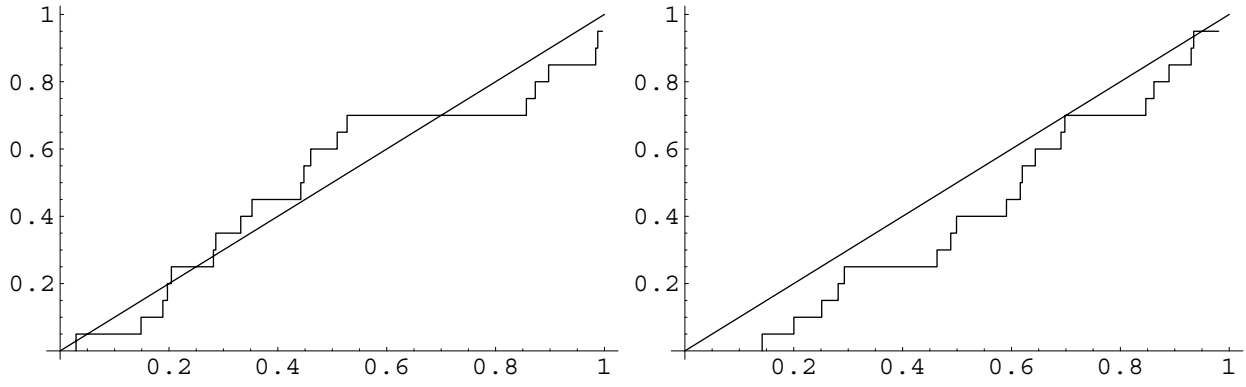
Этот эффект можно объяснить следующим образом. Пусть $X = (0, \frac{1}{2}] \times (0, 1]$; $Y = (\frac{1}{2}, 1] \times (0, 1]$, т.е. X и Y – это левая и правая половины тора. Рассмотрим произвольную подпоследовательность длины 5, например 10011. Пусть x – начальная точка $\binom{x_0^{(0)}}{y_0^{(0)}}$ генератора. Для того, чтобы первые пять бит генератора совпали с нашей последовательностью 10011, необходимо и достаточно, чтобы $x \in Z_{10011} = Y \cap M^{-1}(X) \cap M^{-2}(X) \cap M^{-3}(Y) \cap M^{-4}(Y)$. Множество Z_{10011} состоит из многоугольников, причем точные дан-



KPlus=0.000201246 (probability 0.0000450385)
KMinus=2.45632 (probability 0.999998)

KPlus=0.000800512 (probability 0.00017961)
KMinus=3.09919 (probability 1.)

Рис. 10: Результаты двадцати χ^2-проверок по критерию направленного случайного блуждания, $n = 10^6$, генератор на автоморфизме тора, каждый следующий тест начинается со случайных начальных точек. Справа: то же, но вместо "алгоритма P" используется "алгоритм N" случайного блуждания.



KPlus=0.773094 (probability 0.728994)
KMinus=0.700064 (probability 0.660054)

KPlus=0.0871888 (probability 0.0281365)
KMinus=0.953303 (probability 0.859003)

Рис. 11: Результаты двадцати χ^2-проверок по критерию направленного случайного блуждания, генератор на автоморфизме тора. Слева $n = 10^4$, справа $n = 10^5$.

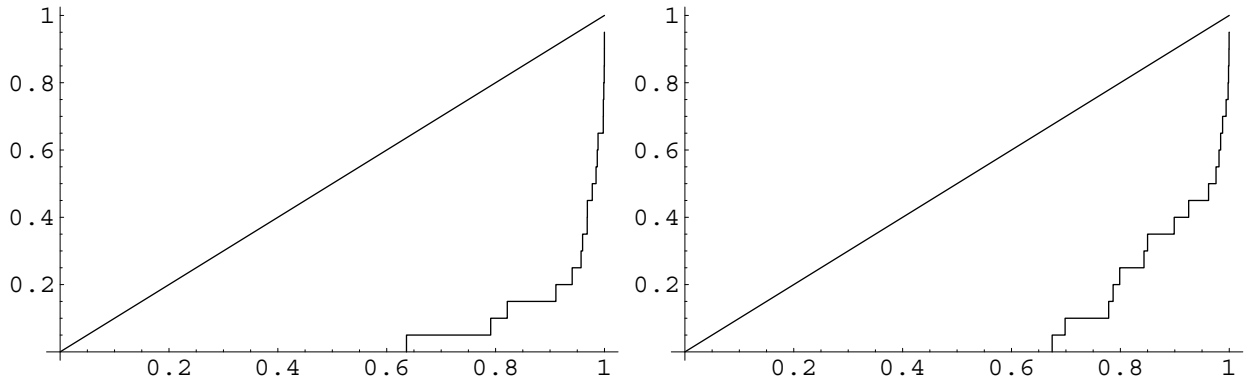


Рис. 12: Результаты двадцати χ^2-проверок по критерию направленного случайного блуждания, генератор на автоморфизме тора. Здесь $g = 2^{31}$. Справа каждый следующий тест начинается со случайных начальных точек.

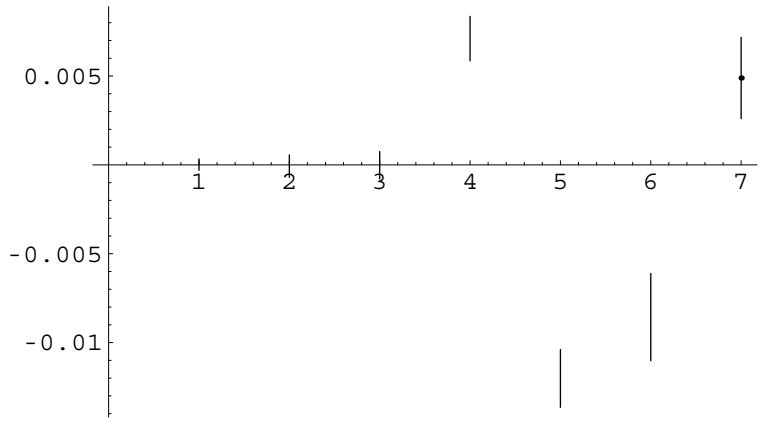


Рис. 13: Отклонения δP_s вероятности блуждания длиной s от нескоррелированного значения в зависимости от длины блуждания s. Изображены средние значения и дисперсии δP_s для 100 численных χ^2-проверок.

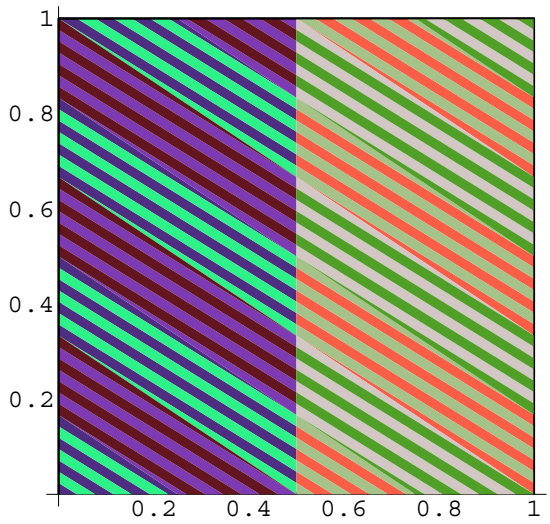


Рис. 14: Геометрическая структура.

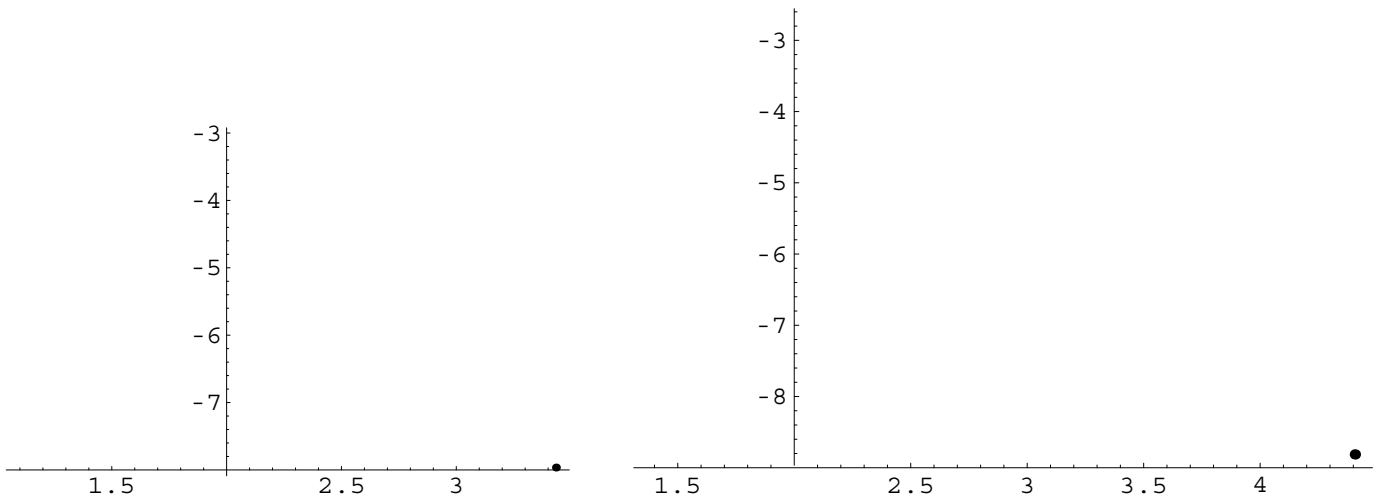


Рис. 15: Слева: зависимость $\log(P(00000)/P_0 - 1)$ от $\log k$ для нечетных k. Справа: зависимость $\log(P(0000)/P_0 - 1)$ от $\log k$ для четных k.

Таблица 1: Вероятности подпоследовательностей для различных преобразований кошки.

Trace	$P(0000)/P_0$	Trace	$P(00000)/P_0$
4	16/15	3	22/21
6	36/35	5	70/69
8	64/63	7	142/141
10	100/99	9	238/237
12	144/143	11	358/357
14	196/195	13	502/501
16	256/255	15	670/669
18	324/323	17	862/861
20	400/399	19	1078/1077
22	484/483	21	1318/1317
24	576/575	23	1582/1581
26	676/675	25	1870/1869
28	784/783	27	2182/2181
30	900/899	29	605880602550401842/605639978894389635
32	1024/1023	31	850271435234332343/849975990375949500
34	1156/1155		
36	1296/1295		
38	1444/1443		
40	1600/1599		
42	1764/1763		
44	1936/1935		
46	2116/2115		
48	2304/2303		
50	2500/2499		
52	2704/2703		
54	2916/2915		
56	3136/3135		
58	3364/3363		
60	3880443680/3879365699		
62	3844/3843		
64	11433681067/11430889470		
66	4356/4355		
68	1939164492226513/1938745080012510		
70	4900/4899		
72	3539214127440373/3538531321884720		
74	341659702/341597295		
76	1084269727936919/1084081980961980		
78	30460702637/30455695270		
80	103417494448271/103401332918520		
82	43473310937/43466843862		

ные для каждого из этих многоугольников можно посчитать. Площадь $S(Z_{10011})$ равна искомой вероятности того, что первые пять бит генератора – это 10011. Итак, мы видим, что природа корреляций лежит в геометрических свойствах преобразования кошки.

На рисунке 14 представлены многоугольники подпоследовательностей длины 3. Каждое множество многоугольников, например $X \cap M^{-1}(Y) \cap M^{-2}(X)$, закрашено своим цветом.

Мы посчитали точные площади $S(Z_{00000}), \ldots, S(Z_{11111})$ для всевозможных автоморфизмов тора. Результаты следующие. Если след k отображения является нечетным числом, то все подпоследовательности длины 4 имеют одну и ту же вероятность $P_0 = 1/16$. Если же k четно, то только подпоследовательности длины 3 равновероятны. Вероятности подпоследовательностей длины 5 для нечетных k и вероятности подпоследовательностей длины 4 для четных k представлены в таблице 1. Заметим, что для нечетных k идеал $\langle 2 \rangle$ инертен, а отображения с инертным $\langle 2 \rangle$ наиболее перспективны для генераторов случайных чисел. Кроме того, можно легко показать аналитически, что вне зависимости от преобразования кошки все подпоследовательности длины 2 равновероятны.

Из рисунка 15 видно, что вероятности ведут себя как $P/P_0 - 1 = Bk^{-2}$ для больших k, где $P_0 = 2^{-n}$ для подпоследовательностей длины n. Таким образом, отклонения, найденные при помощи теста на случайное блуждание, стремятся к нулю при увеличении следа k.

A Доказательство теоремы

Приводим доказательство теоремы из раздела 3.3.

Утверждение 1. T_n – наименьшее целое число, такое, что $\lambda^{T_n} \equiv 1 \pmod{\langle 2^n \rangle}$. В частности, периоды всех свободных орбит равны.

Доказательство. Произвольный z, который лежит на орбите, период которой равен T, удовлетворяет условию $\lambda^T z \equiv z \pmod{\langle 2^n \rangle} \Rightarrow z(\lambda^T - 1) \in \langle 2^n \rangle$. Если орбита свободна, то для любого идеала $P | \langle 2^n \rangle$, $P \neq \langle 1 \rangle$, выполняется $z \notin P$. Следовательно, $(\lambda^T - 1) \in \langle 2^n \rangle$, ч.т.д.

Утверждение 2. $T_n | T_{n+1}$.

Доказательство. Действительно, $\lambda^{T_{n+1}} \equiv 1 \pmod{\langle 2^{n+1} \rangle} \Rightarrow \lambda^{T_{n+1}} \equiv 1 \pmod{\langle 2^n \rangle} \Rightarrow T_{n+1} = mT_n$, где $m \in \mathbb{N}$.

Утверждение 3. $\forall n$: либо $T_{n+1} = 2T_n$, либо $T_{n+1} = T_n$

Доказательство. Действительно, поскольку $(\lambda^{T_n} - 1) \in \langle 2^n \rangle$, то $(\lambda^{T_n} + 1) = (\lambda^{T_n} - 1) + 2 \in \langle 2 \rangle$. Следовательно, $\lambda^{2T_n} - 1 = (\lambda^{T_n} - 1)(\lambda^{T_n} + 1) \in \langle 2^{n+1} \rangle$, т.е. либо $T_{n+1} = 2T_n$, либо $T_{n+1} = T_n$.

Утверждение 4. Если $n \geq 3$ и $T_n \neq T_{n-1}$, то $T_{n+1} \neq T_n$.

Доказательство. Итак, $T_n = 2T_{n-1}$. Следовательно, $\begin{cases} \lambda^{T_{n-1}} \equiv 1 \pmod{\langle 2^{n-1} \rangle} \\ \lambda^{T_{n-1}} \not\equiv 1 \pmod{\langle 2^n \rangle} \end{cases} \Rightarrow$ $\lambda^{T_{n-1}} = 1 + z \cdot 2^{n-1}$, где $z \notin \langle 2 \rangle$. Возведем в квадрат: $\lambda^{2T_{n-1}} = 1 + z \cdot 2^n + z^2 \cdot 2^{2n-2} \equiv 1 + z \cdot 2^n \pmod{\langle 2^{n+1} \rangle}$ при $n \geq 3$. Следовательно, $\lambda^{2T_{n-1}} \not\equiv 1 \pmod{\langle 2^{n+1} \rangle} \Rightarrow T_{n+1} \neq T_n$, ч.т.д.

Утверждение 5. Если $\langle 2\rangle$ расщеплен, то $\forall n : T'_n = T_n$. В частности, периоды всех орбит, не лежащих на подрешетке $2^{n-1} \times 2^{n-1}$, равны.

Доказательство. Поскольку $\langle 2\rangle$ расщеплен, то $\langle 2\rangle = P_1P_2$. Пусть S и T – периоды орбит, лежащих в P_1^n и P_2^n, т.е. T и S – наименьшие целые числа, такие что $\lambda^T \equiv 1 \pmod{P_1^n}$, $\lambda^S \equiv 1 \pmod{P_2^n}$. Заметим, что P_1 и P_2 сопряжены, т.е. $P_1 = P_2^*$. Пусть $T = S + R$, $R \geq 0$. Тогда равенством, сопряженным к равенству $\lambda^S \equiv 1 \pmod{P_2^n}$, будет $\lambda^{*S} \equiv 1 \pmod{P_1^n}$, где $\lambda^* = \lambda^{-1}$. Следовательно, $\lambda^S\lambda^{*S}\lambda^R \equiv \lambda^T \equiv 1 \pmod{P_1^n} \Rightarrow \lambda^R \equiv 1 \pmod{P_1^n}$, т.е. $R = lT$ для некоторого целого $l \geq 0$. Таким образом $T = S + lT$, что возможно только при $l = 0$. Итак, $T = S$.

Пусть z лежит на идеальной орбите, период которой равен T'_n, причем $z \in P_2^k$, $z \notin P_2^{k+1}$, где $k \in \{1, 2, \ldots, n\}$. Тогда T'_n и T_n – наименьшие целые числа, такие что $\lambda^{T'_n} \equiv 1 \pmod{P_1^nP_2^{n-k}}$ и $\lambda^{T_n} \equiv 1 \pmod{P_1^nP_2^n}$. Следовательно, $T'_n|T_n$. С другой стороны, $\lambda^{T'_n} \equiv 1 \pmod{P_1^n} \Rightarrow \lambda^{T'_n} \equiv 1 \pmod{P_2^n} \Rightarrow \lambda^{T'_n} \equiv 1 \pmod{P_1^nP_2^n}$, т.е. $T_n|T'_n$. Таким образом, $T'_n = T_n$.

Утверждение 6. Если $\langle 2\rangle$ разветвлен, то $\forall n$: либо $T'_n = T_n$, либо $T'_n = T_{n-1}$

Доказательство. Поскольку $\langle 2\rangle$ разветвлен, то $\langle 2\rangle = P^2$. Орбита лежит в P, требуется показать, что ее период равен либо T_n, либо T_{n-1}.

$$\begin{cases} \lambda^{T_{n-1}} \equiv 1 \pmod{\langle 2^{n-1}\rangle} \\ \lambda^{T'_n} \equiv 1 \pmod{\langle 2^{n-1}\rangle P} \\ \lambda^{T_n} \equiv 1 \pmod{\langle 2^n\rangle} \end{cases} \Rightarrow T_{n-1}|T'_n|T_n.$$

Отсюда и из утверждения 3 сразу следует требуемое.

Утверждение 7. Пусть $\langle 2\rangle$ разветвлен, $n \geq 3$ и $T_n = 2T_{n-1}$. Тогда $T'_{n+1} = 2T'_n$.

Доказательство. Пусть $T = T_{n-1}$, тогда

$$\begin{cases} \lambda^T \equiv 1 \pmod{A} \\ \lambda^T \not\equiv 1 \pmod{AP} \end{cases} \tag{7}$$

Здесь $A = \langle 2^{n-1}\rangle$ если $T'_n = T_n$; $A = \langle 2^{n-1}\rangle P$ если $T'_n = T_{n-1}$. В любом случае $\langle 2^{n-1}\rangle|A$, $AP|\langle 2^n\rangle$. Из (7) следует, что $\lambda^T = 1 + z$, где $z \in A$, $z \notin AP$, поэтому $\lambda^{2T} = 1 + 2z + z^2$, где $2z \in (\langle 2\rangle A)$, $2z \notin (\langle 2\rangle AP)$, кроме того при $n \geq 3$ выполняется $z^2 \in \langle 2^{n+1}\rangle \Rightarrow z^2 \in (\langle 2\rangle AP)$. Следовательно,

$$\begin{cases} \lambda^{2T} \equiv 1 \pmod{\langle 2\rangle A} \\ \lambda^{2T} \not\equiv 1 \pmod{\langle 2\rangle AP} \end{cases} \tag{8}$$

В случае $T'_n = T_n$ это означает, что $T'_{n+1} \neq T_n \Rightarrow T'_{n+1} = T_{n+1}$. В случае $T'_n = T_{n-1}$ это означает, что $T'_{n+1} = T_n$. В любом случае $T'_{n+1} = 2T'_n$.

Список литературы

[1] V. I. Arnol'd, *Mathematical Methods of Classical Mechanics*, Springer, New York (1978)

[2] V. I. Arnol'd, A. Avez, *Ergodic Problems of Classical Mechanics*, Nenjamin, New York (1968)

[3] I. C. Percival, F. Vivaldi, *Arithmetical Properties of Strongly Chaotic Motions*, Physica 25D, 105-130 (1987)

[4] J. P. Keating, *Asymptotic properties of the periodic orbits of the cat maps*, Nonlinearity 4, 277-307 (1991)

[5] J. H. Hannay, M. V. Berry, Physica 1D, 267-290 (1980)

[6] H. Cohn, *A Second Course in Number Theory*, Wiley, New York (1962). [Reprinted by Dover, New York with the title *Advanced Number Theory* (1980)]

[7] R. Chapman, *Notes on Algebraic Numbers*, http://www.maths.ex.ac.uk/~rjc/notes/algn.ps (1995, 2002)

[8] D. E. Knuth, *The art of Computer Programming*, Vol.2, Addison-Wesley, Cambridge (1981)

[9] K. Binder, D. W. Heermann, *Monte Carlo Simulation in Statistical Physics* (Springer-Verlag, Berlin, 1992)

[10] L. N. Shchur, J. R. Heringa, H. W. J. Blöte, Physica A241, 579 (1997)

[11] S. W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco (1967)

[12] A. M. Ferrenberg, D. P. Landau, Y. J. Wong, Phys.Rev.Lett. 69, 3382 (1992)

[13] I. Vattulainen, T. Ala-Nissila, K. Kankaala, Phys.Rev.Lett.73, 2513 (1994)

[14] F. Schmid, N. B. Wilding, Int.J.Mod.Phys. C 6, 781 (1995)

[15] L. N. Shchur, H. W. J. Blöte, Phys.Rev.E 55, R4905 (1997)

[16] P. Grassberger, Phys. Lett. 181, 43 (1993)

[17] P. L'ecuyer, Uniform Random Number Generation

[18] A. Bonelli, S. Ruffo, Int. J. Mod. Phys. C, Vol.9 (1998)