DOI: 10.17725/rensit.2022.14.437

Информационные технологии на основе шумоподобных сигналов: IV. Алгоритмические генераторы псевдослучайных чисел на основе динамического хаоса

Грачев В.И., Рябенков В.И., Сургай А.В., Колесов В.В.

Институт радиотехники и электроники им. В.А. Котельникова РАН, http://www.cplire.ru/
Москва 125009, Российская Федерация

E-mail: grachev@cplire.ru, ryabenkov.vi@list.ru, ya.a1997@yandex.ru, kvv@cplire.ru

Поступила 11.12.2022, рецензирована 15.12.2022, принята 21.12.2022

Аннотация: **Численным моделированием исследованы статистические, фрактальные и структурные свойства последовательностей целых чисел, генерируемые алгоритмом с запаздыванием. Показано, что статистические свойства формируемых дискретных последовательностей, близкие к случайному процессу, обеспечивают такие порождающие кодирующие алгоритмы, у которых как одномерное распределение вероятностей, так и распределения условных вероятностей генерируемых чисел близки к равномерному. Исследована структура фазового пространства дискретного кодирующего алгоритма с запаздыванием, заданного на замкнутом интервале целых чисел. Установлено, что фазовое пространство состоит из конечного числа циклов различного периода, поведение системы на которых носит псевдослучайный характер. Обсуждается возможность создания генераторов такого типа с более сложными схемами. Показано, что при надлежащем выборе значений параметров алгоритм позволяет формировать непериодическую псевдослучайную последовательность произвольной заданной длины для кодирования информации в телекоммуникационных системах.**

Ключевые слова: **информационные технологии, хаотическая динамика, псевдослучайные последовательности, избыточные коды, шумоподобные сигналы**

УДК 621.391

Благодарности: Работа выполнена в рамках государственного задания ИРЭ им.В.А. Котельникова РАН от Минобрнауки РФ.

Для цитирования: Грачев В.И., Рябенков В.И., Сургай А.В., Колесов В.В. Информационные технологии на основе шумоподобных сигналов: IV. Алгоритмические генераторы псевдослучайных чисел на основе динамического хаоса. *РЭНСИТ: Радиоэлектроника. Наносистемы. Информационные технологии*, 2022, 14(4):437-462. DOI: 10.17725/rensit.2022.14.437.

Information Technologies Based on Noise-like Signals: IV. Algorithmic Pseudo-Random Number Generators Based on Dynamic Chaos

Vladimir I. Grachev, Viktor I. Ryabenkov, Anastasiya V. Surgay, Vladimir V. Kolesov

Kotelnikov Institute of Radioengineering and Electronics of RAS, http://www.cplire.ru/
Moscow 125009, Russian Federation

E-mail: grachev@cplire.ru, ryabenkov.vi@list.ru, ya.a1997@yandex.ru, kvv@cplire.ru

Received December 11, 2022, peer-reviewed December 15, 2022, accepted December 21, 2022

Abstract: **Numerical simulation is used to investigate the statistical, fractal and structural properties of sequences of integers generated by the algorithm with delay. It is shown that the statistical properties of the generated discrete sequences, close to a random process, are provided by such generating coding algorithms, in which both the one-dimensional probability distribution and the distributions of the conditional probabilities of the generated numbers are close to uniform. The**

structure of the phase space of a discrete coding algorithm with delay defined on a closed interval of integers is studied. It is established that the phase space consists of a finite number of cycles of different periods, the behavior of the system on which is pseudorandom. The possibility of creating generators of this type with more complex circuits is discussed. It is shown that with an appropriate choice of parameter values, the algorithm allows the formation of a non-periodic pseudo-random sequence of arbitrary given length for encoding information in telecommunication systems.

Keywords: **information technology, chaotic dynamics, pseudorandom sequences, redundant codes, noise-like signals**

UDC 621.391

Acknowledgments: The work was carried out within the framework of the state task of the Kotelnikov IRE of RAS from the Ministry of Education and Science of the Russian Federation.

For citation: Vladimir I. Grachev, Viktor I. Ryabenkov, Anastasiya V. Surgay, Vladimir V. Kolesov. Information Technologies Based on Noise-like Signals: IV. Algorithmic pseudo-random number generators based on dynamic chaos. *RENSIT: Radioelectronics. Nanosystems. Information Technologies*, 2022, 14(3):437-462e. DOI: 10.17725/rensit.2022.14.437.

Содержание

1. ВВЕДЕНИЕ

В настоящее время в целом ряде областей науки и техники в процессе решения практических задач широко используются случайные и псевдослучайные числа. К таким областям относятся математическое моделирование, криптография, защита информации в ЭВМ и телекоммуникационных сетях, а также при кодировании информации в сверхширокополосных радиотехнических системах. Для решения этих задач необходимо вырабатывать огромные массивы случайных чисел с самыми разнообразными свойствами. Наибольшее значение для практики имеют числовые последовательности с равномерным законом распределения. Проблема случайных чисел состоит в том, что пока не существует ни одного алгоритмического генератора случайных чисел. Если полученная последовательность подчиняется некоторой алгоритмической закономерности, то она по определению не является случайной.

Таким образом, основная задача такого алгоритма состоит в том, чтобы он порождал последовательность чисел, которая, не являясь случайной, была бы неотличима от случайной, не имела бы видимых закономерностей. В этом смысле алгоритмы бывают плохие и хорошие. Причем качество алгоритма, т.е. его способность генерировать числовые последовательности близкие по свойствам к случайным, может быть проверена методами математической статистики.

Одним из основных элементов в таких системах являются генераторы случайных и псевдослучайных чисел (ГСЧ и ГПСЧ), от качества и быстродействия которых существенно зависят результаты решения поставленных задач. В настоящее время ведутся интенсивные фундаментальные работы в области генерирования случайных и псевдослучайных

чисел, а также публикуется большое количество патентов и авторских свидетельств, которые говорят о все возрастающем интересе к этим областям.

Генераторы псевдослучайных последовательностей находят применение в многочисленных приложениях, где необходимы последовательности со свойствами, близкими по своим статистическим характеристикам к случайным числовым рядам. Формируемые такими генераторами последовательности чисел вычисляются с помощью детерминированных алгоритмов, что и послужило причиной назвать их псевдослучайными последовательностями (ПСП) [1].

К характеристикам этих последовательностей предъявляются разнообразные часто специфические требования, связанные с особенностями их конкретных применений. В силу этого интерес к разработке новых алгоритмов, формирующих такие псевдослучайные последовательности, не только не уменьшается, а наоборот растет. Это обусловлено также настоятельной необходимостью защиты информации в лавинообразно развивающихся в глобальном масштабе системах и сетях для обработки, хранения и передачи информации [2]. Появление новых идей в этой области, в частности, связано с развитием представлений о возможности хаотической динамики детерминированных систем даже в предположении отсутствия в них каких-либо шумов [3].

Несмотря на то, что известно довольно много алгоритмов генерации псевдослучайных последовательностей (ПСП), на практике, как правило, используется рекуррентный алгоритм. Двоичные последовательности на основе рекуррентных соотношений достаточно легко реализуются на ЭВМ в виде программ и схемотехнически на основе быстродействующих многоразрядных двоичных сдвиговых регистров. Известные классы ПСП, как линейных, так и нелинейных, обладают определенными недостатками и не удовлетворяют всем необходимым требованиям. Альтернативное решение проблемы дает применение шумоподобных сигналов (ШПС), формируемых нелинейными системами с динамическим хаосом. Такие ШПС, обладая корреляционными свойствами не хуже, чем у М-последовательностей, имеют практически неограниченный набор длин, могут образовывать ансамбли как двоичных, так и многоуровневых сигналов больших объемов и являются нелинейными, что затрудняет их распознавание в целях последующего воспроизведения при несанкционированном доступе к кодированной информации [4].

На основе математической модели кольцевой автоколебательной системы с сильной амплитудно-фазовой нелинейностью, фильтрацией и запаздыванием разработан и исследован дискретный порождающий алгоритм хаотического сигнала, относящийся к классу алгоритмов рекуррентно-параметрического типа с запаздыванием. Форма алгоритма этого класса в общем виде имеет вид дискретного функционального преобразования (отображения):

$$x_n = f(x_{n-1}, x_{n-2}, ..., x_{n-Nz}),$$

где x_n – члены формируемой псевдослучайной последовательности на n-ом шаге, Nz- параметр запаздывания, определяющий число членов последовательности на интервале запаздывания x_{n-1}, x_{n-2}, ..., x_{n-Nz}, которые полностью определяют новое значение x_n и должны быть заданы в качестве начального условия на первом шаге, а функция $f(x)$ отражает преобразования амплитуды и фазы в порождающей кольцевой автоколебательной системе в режиме хаоса. Алгоритм определен на множестве М целых чисел натурального ряда, принадлежащих замкнутому числовому интервалу [M1, M2], (M2 > M1, M = M2 – M1 + 1), и формирует практически некоррелированную псевдослучайную последовательность целых чисел с распределением вероятностей, близким к равномерному, и корреляционными характеристиками, соответствующими требованиям, предъявляемым к кодирующим сигналам. Преимущество целочисленных последовательностей состоит в том, что они идентично воспроизводятся на различных типах вычислительных устройств и при аппаратной реализации легко воспроизводятся схемотехнически [5].

Одними из простейших генераторов, формирующих псевдослучайные последовательности, являются генераторы, основанные на алгоритме Фибоначчи, которые до сих пор используются на практике [6]. В алгоритме Фибоначчи при вычислении каждого очередного члена последовательности используются несколько ранее вычисленных предыдущих членов. Это так называемый генератор с запаздывающими аргументами. Как правило, в качестве области определения фазового пространства, в котором происходит движение изображающей точки состояния системы, используется ограниченный числовой интервал. Из-за ограниченности фазового пространства, определяемого размерностью алгоритма, с учетом конечной точности представления чисел рано или поздно в результате цепочки последовательных вычислений по заданному детерминированному алгоритму должно произойти замыкание траектории системы в ее фазовом пространстве.

Это означает, что траектория выйдет на цикл, и далее результаты вычисления будут повторяться через некоторое определенное (хотя может быть и очень большое) число шагов вычисления, которое называют периодом. При разработке таких алгоритмов стремятся к поиску условий получения последовательностей чисел, имеющих возможно больший (наибольший) период повторения, и одновременно, на любом произвольном участке траектории, меньшем длины периода, обладающих характеристиками последовательности случайных числе. Достоинством класса алгоритмов с запаздыванием является то, что при большой простоте операций вычисления они позволяют исследовать закономерности формирования последовательностей с большими периодами в зависимости от характерных параметров алгоритма (интервала определения допустимых чисел {1, M}, длины запаздывания Nz). Алгоритм дополняется правилом возвращения в указанный интервал вновь вычисленного числа в случае выхода из него. Эта операция обеспечивает важный для хаотизации механизм перемешивания [7].

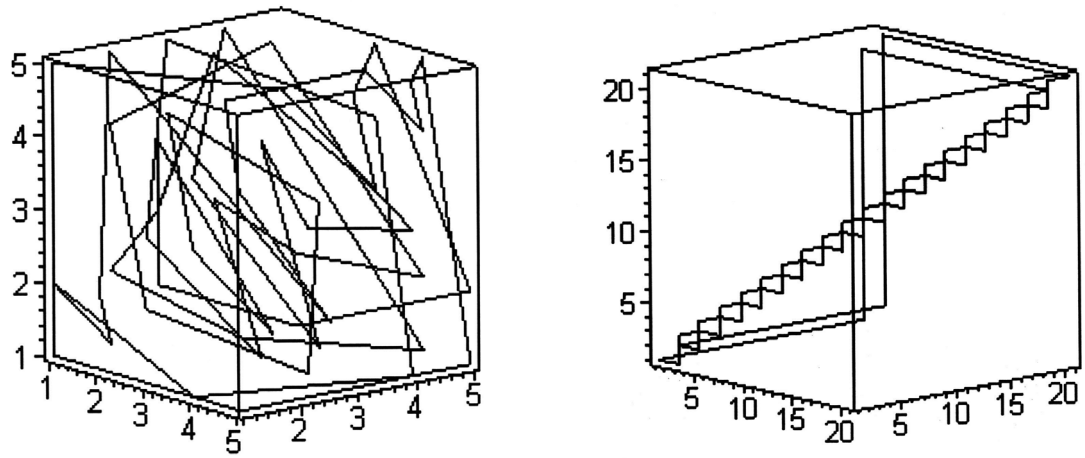
2. ПСЕВДОСЛУЧАЙНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ ЦЕЛЫХ ЧИСЕЛ, ФОРМИРУЕМАЯ АЛГОРИТМОМ С ЗАПАЗДЫВАНИЕМ, КАК МАРКОВСКИЙ ПРОЦЕСС

Проблема защиты информации в открытых информационных и компьютерных сетях от несанкционированного доступа, а также задача повышения помехоустойчивости телекоммуникационных каналов связаны с применением сложных кодирующих алгоритмов и шумоподобных сигналов с большой информационной емкостью. Поэтому разработка сложных кодирующих алгоритмов и критериев объективной оценки их статистических свойств является достаточно актуальной задачей.

В качестве тестируемого алгоритма рассмотрен алгоритм с запаздыванием на основе отображения типа Фибоначчи. Для ограничения области определения алгоритма конечным замкнутым целочисленным интервалом [1, M], M > 1 отображение дополнено операцией преобразования интервала [1, M] самого в себя с "отражающими границами":

$$\begin{aligned} &\tilde{x}_n = x_{n-1} + (-1)^{x_{n-Kz}} \cdot x_{n-Nz}, \quad Kz \in [2,\ Nz-1], \\ &x_n \in [1,\ M], \\ &x_n = \tilde{x}_n, \quad if \quad \tilde{x}_n \in [1,\ M], \\ &x_n = \tilde{x}_n - M, \quad if \quad \tilde{x}_n > M, \\ &x_n = \tilde{x}_n + M, \quad if \quad \tilde{x}_n < 1. \end{aligned} \tag{2.1}$$

Здесь Nz – параметр запаздывания, он определяет размерность фазового пространства и радиус-вектора $R_n(x_{n-1}, x_{n-2}, \ldots, x_{n-Nz})$ состояния данной дискретной динамической системы (ДДС) в этом пространстве. Число возможных состояний в ФП конечно и равно M^{Nz}. В зависимости от начальных условий $R_0(x_{-1}, x_{-2}, \ldots x_{-Nz})$ ДДС (2.1) на каждом шаге алгоритма описывает в ФП ту или иную "траекторию", представляющую собой последовательные дискретные переходы из одной точки состояния в другое по псевдослучайному закону (**Рис. 2.1**). Из-за ограниченности объема ФП эти траектории образуют замкнутые циклы, которые, вследствие однозначности преобразования (2.1), не пересекаются и не имеют общих точек. Все точки ФП принадлежат только одному какому-либо циклу, либо



а *б*

Рис. 2.1. *Фазовый портрет сигнала с замкнутым а)псевдослучайным циклом, б)регулярным циклом.*

изолированной точке с координатами (M, M, …, M). Так, например, при M = 5, Nz = 4, Kz = 3 в ФП алгоритма один 562-тактный цикл, два цикла с периодом T = 27, один 8-тактный цикл и одна особая точка. При Nz = 5, Kz = 3 и M = 13 (M^{Nz} = 371293) в ФП существуют циклы с периодами T = 332373, 21721, 7966, 4959, 3640, а при Nz = 6, Kz = 4 и M = 15 один "длинный" цикл с периодом T = 11099897 включает в себя подавляющее большинство ($0.974 \cdot M^{Nz}$) точек ФП.

Циклы алгоритма (2.1) имеют важную отличительную особенность: поведение динамической системы на цикле до его замыкания (а нас будут интересовать процессы именно до замыкания цикла) имеет случайный, хаотический характер (Рис. 2.1*а*), а порождаемая при этом алгоритмом непериодическая последовательность $\{x_n\}$ – псевдослучайного типа. Множество точек состояний динамической системы в ФП, объединенных в такой цикл, назовем псевдослучайным циклом. В отличие от регулярного цикла, которому до замыкания цикла соответствует регулярное движение в фазовом пространстве. Пример простого регулярного цикла ($x_n = x_{n-3} + 2$ с преобразования интервала [1,21] в себя) приведен на Рис. 2.1*б*. Таким образом, псевдослучайный цикл представляет собой конечное множество внешне хаотически, но строго детерминированным образом следующих одна за другой точек состояний дискретной динамической системы в фазовом пространстве алгоритма.

Для практических применений наибольший интерес представляют непериодические псевдослучайные последовательности большой длины. При надлежащем выборе параметров алгоритма (2.1) и начальных условий сегмент непериодической ПСП, формируемой алгоритмом на псевдослучайном цикле до выхода системы на период, может быть произвольно большой длины и, как показал анализ, по своим статистическим свойствам близок к последовательности с равномерным распределением вероятностей генерируемых чисел $p(x)$. Так при интервале области определения алгоритма [1,63] (M = 63) и запаздывании Nz = 3 длина непериодической ПСП равна $N = 7.8317 \cdot 10^4$ при Nz = 5, $N = 3.3174 \cdot 10^8$ при Nz = 7, $N = 1.676 \cdot 10^{12}$ при Nz = 9 длина непериодической ПСП более $5 \cdot 10^{12}$.

Отметим, что дискретная ПСП с дискретными числами $\{x_n\}$ по своему виду близка к последовательности испытаний классической теории вероятностей. Каждый переход в этой последовательности от числа x_n к следующему числу x_{n+1}, равным образом, как и к числу x_{n+s} через s шагов алгоритма, полностью определен вследствие детерминированности и однозначности процесса (2.1). Тем не менее, для внешнего наблюдателя он ничем не отличается от процесса случайных испытаний. Абстрагируясь поэтому от

детерминированности процесса (2.1), покажем, что формируемая им последовательность при должном выборе параметров алгоритма может быть очень близкой к случайной последовательности марковского типа и, более того, к случайной последовательности независимых равновероятных событий.

Как известно, марковский процесс – это процесс без вероятностного последействия, когда условная вероятность для всех $t > t_0$ однозначно определяется значением x_0, принятым в момент t_0 и не зависит от предшествующей истории [8]. Для дискретной последовательности с дискретными значениями x_n – простой цепи Маркова это означает, что существует вероятность $p(x_j, n \mid x_i, k)$ перехода от любого из значений процесса x_i при k-ом испытании к любому значению x_j при n-ом испытании ($n > k$, $i,j = 1, 2, \ldots, M$) [9]. В частном случае последовательности независимых испытаний вероятность перехода в состояние x_j совпадает с вероятность этого состояния при n-ом испытании $p(x_j, n \mid x_i, k) = p(x_j)$ независимо от результатов других испытаний. Для однородной цепи Маркова вероятности переходов зависят только от числа шагов $s = n - k$ между испытаниями $p(x_j, n \mid x_i, k) = p(x_j, \mid x_i, s) = p_{ij}(s)$. Величины $p_{ij}(s)$ образуют матрицу $\boldsymbol{\pi}_s$ вероятностей перехода за s шагов. Для однородной цепи должно выполняться соотношение (уравнение Маркова) [10]: $\boldsymbol{\pi}_s = (\boldsymbol{\pi}_1)^s$, т.е. вероятности перехода за s шагов выражаются через вероятности перехода за один шаг.

Рассмотрим алгоритм (2.1). На первый взгляд последовательность, формируемая этим алгоритмом с запаздыванием, не является процессом без последействия. Более того, каждое новое значение ПСП определяется предысторией из принятых на предыдущих этапах Nz значений запаздывания. С другой стороны, операция "преобразования числового интервала самого в себя" как бы разрывает эту связь (не нарушая однозначности процесса в прямом направлении, но делая его необратимым) при каждом выбросе нового числа за границы интервала [1,M]. Проверим, насколько справедливо соотношение $\boldsymbol{\pi}_s = (\boldsymbol{\pi}_1)^s$ для ПСП, формируемой алгоритмом (2.1). То есть, в какой степени эта последовательность отвечает уравнению Маркова. Предположение об однородности процесса $\{x_n\}$ вполне естественно, если имеется предварительная информации о близости распределения вероятности $p(x)$ к равномерному.

Для наглядности результатов численный эксперимент проведем для алгоритма (2.1) с небольшими значениями параметров, но с наличием в фазовом пространстве (ФП) псевдослучайного цикла с периодом, достаточным для генерации непериодической последовательности с числом членов N, обеспечивающим необходимый для статистической обработки массив. Положим M = 3, Nz = 9, Kz = 5, т.е. у алгоритма 9-мерное фазовое пространство и область определения из трех чисел. В этом случае в ФП существует длинный цикл с периодом T = 19677 при полном объеме ФП, равном M^{Nz} = 19683. Распределение вероятностей чисел $p(x)$ в последовательности, генерируемой алгоритмом, практически равномерное со среднеквадратичным отклонением от этого закона, равным $4.8 \cdot 10^{-5}$, и максимальным отклонением по модулю $6.8 \cdot 10^{-5}$.

На основе реализации сформированной алгоритмом ПСП длиной N = 19677 определим вероятности P(A) генерации числа x_i ($i = 1, 2, \ldots, M$) путем подсчета осуществленных наступлений события A, равного $n(x_i)$: $P(A) = n(x_i)/N$. Следуя определению условной вероятности по Колмогорову: $P(B \mid A) = P(AB)/P(A)$, где P(AB) – вероятность одновременного осуществления событий A и B. Подсчитаем в реализации из N испытаний количество $n(x_j, x_i, s)$ одновременно наступивших событий A (генерация числа x_i) и B (переход от этого числа через s шагов алгоритма к числу x_j). Тогда вероятность $P(AB) = n(x_j, x_i, s)/(N - s)$, а условная вероятность $P(B \mid A) = [n(x_j, x_i, s)/(N - s)]/[n(x_i)/N] = p_{ij}(s)$. Матрица переходов $\boldsymbol{\pi}_s = \| p_{ij}(s) \|$. Для последовательности независимых равновероятных событий все $p_{ij}(s) = 1/M$ и соответствующую матрицу вероятностей переходов обозначим через $\boldsymbol{\pi}_0$.

При анализе реализации ПСП длиной N = 19677 получены следующие матрицы перехода:

$$\pi_1 = \begin{pmatrix} 0.33335 & 0.33335 & 0.33335 \\ 0.33325 & 0.33340 & 0.33340 \\ 0.33320 & 0.33350 & 0.33320 \end{pmatrix},$$

$$\pi_2 = \begin{pmatrix} 0.33321 & 0.33352 & 0.33337 \\ 0.33326 & 0.33342 & 0.33342 \\ 0.33315 & 0.33337 & 0.33321 \end{pmatrix},\ldots,$$

$$\pi_{20} = \begin{pmatrix} 0.33321 & 0.33382 & 0.33382 \\ 0.33342 & 0.33357 & 0.33372 \\ 0.33330 & 0.33367 & 0.33376 \end{pmatrix}.$$

Установление одного этого факта, что все вероятности переходов $p_{ij}(s) = p(x_j, | x_i, s) = p(x_j, n | x_i, k)$ существуют, уже достаточно, чтобы считать этот процесс марковским [11]. Кроме того, мы видим, что все элементы матриц очень близки к равновероятному значению $p_{ij} = 1/M = 1/3$. При этом, поскольку сумма элементов каждой строки матриц π_s равны единице, то эти матрицы являются стохастическими [12]. Наибольшее отличие эвклидовых норм матриц π_s от единицы составило величину, меньшую 10^{-5}.

Оценку справедливости равенства (2.2) для исследуемой ПСП проведем на основе вычисления среднеквадратичного отклонения элементов матриц π_s и $(\pi_1)^s$:

$$\sigma_S = \sqrt{(1/M^2)\sum_{i,j=1}^{M}(p_{i,j}(s) - p_{i,j}^{(s)}(1))^2} = \\ = (1/M)\cdot\|\Delta\pi_s\|, \qquad (2.2)$$

где $\|\mathbf{\Delta\pi_s}\|$ – евклидова норма матрицы $\mathbf{\Delta\pi_s} = \mathbf{\pi_s} - \mathbf{(\pi_1)^s}$, а $p_{ij}(s)$ (1) – элементы матрицы $(\mathbf{\pi_1})^s$. Полученные числовые значения σ_s построены на графике **Рис. 2.2** (кривая 1*а*). Мы видим, что отличия элементов матриц в левой и в правой частях (2) при всех интервалах переходов $s = 1, 2, \ldots, 20$ менее $4\cdot10^{-4}$ по абсолютной величине

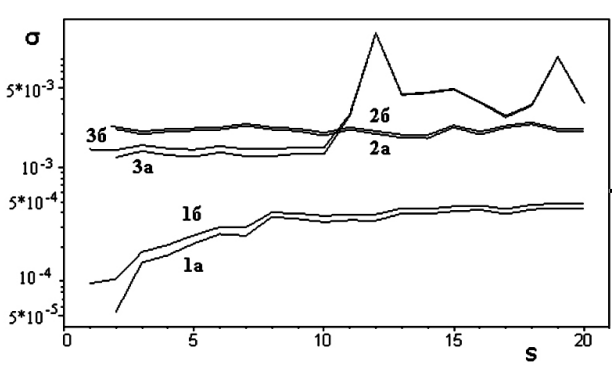


Рис. 2.2. *Среднеквадратичное отклонение элементов матриц π_s и $(\pi_1)^s$.*

или примерно 10^{-3} по относительному значению. Этот результат показывает, что тестируемую последовательность, формируемую алгоритмом (2.1) с запаздыванием, мы можем рассматривать как очень близкую к марковскому процессу. Более того, как показывает анализ близости матриц переходов $\mathbf{\pi_s}$ к матрице $\mathbf{\pi_0} = \|p_{ij} = 1/M\|$, эта последовательность при данных значениях параметров M и Nz практически не отличается от последовательности независимых равновероятных испытаний. Действительно, характеризуя отличие матриц $\mathbf{\pi_s}$ и $\mathbf{\pi_0}$ среднеквадратичным отклонением их элементов:

$$\sigma_O = \sqrt{(1/M^2)\sum_{i,j=1}^{M}(p_{i,j}(s) - 1/M)^2} = (1/M)\cdot\|\Delta\pi_0\|, \qquad (2.3)$$

где $\|\mathbf{\Delta\pi_0}\|$ – норма матрицы $\mathbf{\Delta\pi_0} = \mathbf{\pi_s} - \mathbf{\pi_0}$, полученные в численном эксперименте значения σ_0 для $s = 1, 2, \ldots, 20$ отложим на графике Рис. 2.2 (кривая 1*б*). Мы видим, что отличия элементов матриц перехода $p_{ij}(s)$ от значений 1/M при всех анализируемых переходах s не превышают уровня $5\cdot10^{-4}$ или в относительном выражении около 0.1%.

Аналогичные вычисления выполнены при анализе матриц переходов для ПСП алгоритма (2.1) с параметрами M = 9, Nz = 9, Kz = 5, т.е. с областью определения из девяти чисел и ФП объемом 387420489 точек состояний. Длина исследуемой реализации ПСП с начальным вектором $R_0(1, 1, \ldots, 1)$ выбиралась равной N = 180000. Распределение вероятностей генерируемых чисел $p(x)$ близко к равномерному со среднеквадратичным отклонением от этого закона, равным $6.42\cdot10^{-4}$, и максимальным отклонением по модулю $1.45\cdot10^{-3}$. Отличия элементов матриц переходов $\mathbf{\pi_s}$ и $(\mathbf{\pi_1})^s$, а также матриц $\mathbf{\pi_s}$ и $\mathbf{\pi_0}$ демонстрируют графики 2*а* и 2*б* на Рис. 2.2. Величины среднеквадратичного отклонения, как это следует из построенных зависимостей, находятся на уровне $\sigma = 2\cdot10^{-3}$, т.е. менее 1% по относительной величине. Это свидетельствует также в пользу принятия заключения о близости сформированного псевдослучайного процесса к цепи Маркова и к последовательности независимых равновероятных испытаний.

Кривые 3*а* и 3*б* на Рис. 2.2 относятся к случаю ПСП, сформированной алгоритмом (2.1) при следующих параметрах: M = 9, Nz = 5, Kz = 3. От предыдущего случая этот вариант отличается меньшей величиной запаздывания. В ФП алгоритма представлены циклы с периодами T = 55070, 3230, 260, 130, 50. Для численного анализа взят самый длинный псевдослучайный цикл с начальным вектором R_0(1, 1, …, 1). Длина исследуемой реализации ПСП равна N = 55070. Распределение вероятностей генерируемых чисел $p(x)$ близко к равномерному со среднеквадратичным отклонением от этого закона $7.3\cdot10^{-4}$, и максимальным отклонением по модулю $1.05\cdot10^{-3}$, что практически не отличается от степени близости к равномерному распределения генерируемых чисел в предыдущей тестируемой последовательности.

Действительно, как показали исследования, функция распределения вероятностей по мере увеличения параметра запаздывания, а значит, размерности алгоритма, имеет тенденцию к улучшению, т.е. приближению к равномерному закону, но при Nz порядка 6 и более плотность распределения $p(x)$ практически не отличается от этого закона. Как свидетельствует ход кривых 3*а* и 3*б* матрицы переходов $\boldsymbol{\pi}_s$ и $(\boldsymbol{\pi}_1)^s$, а также матрицы $\boldsymbol{\pi}_s$ и $\boldsymbol{\pi}_0$ мало отличаются на интервалах переходов s = 1, 2, …, 10, но на больших интервалах s = 12, 13, … отличия в матрицах возрастают до единиц процентов. Этот компьютерный эксперимент подтверждает, что для оценки ПСП как близкой к последовательности независимых испытаний знания о равномерности распределения вероятностей появления чисел $p(x)$ еще не достаточно. Важно, чтобы были равномерными и все распределения условных вероятностей $p(x_j,\ n \mid x_i,\ k)$. Сопоставление хода графиков 2 и 3 на Рис. 2.2 показывает, что увеличение запаздывания от значения Nz = 5 до Nz = 9 приводит к улучшению статистических характеристик формируемого алгоритмом псевдослучайного процесса, приближая их к характеристикам цепи Маркова и последовательности независимых равновероятных событий.

Заметим, что определение матриц вероятностей переходов при больших значениях параметра M требует обработки больших числовых массивов, поэтому для экспресс-анализа статистического качества формируемых ПСП вполне приемлемо, как известно, построение упрощенных матриц переходов, информирующих лишь о том, отличны от нуля вероятности перехода $p_{ij}(s)$ или же нет. Построение таких матриц возможно при анализе реализаций не обязательно большой длины. При этом не все ячейки матриц могут оказаться правильно заполненными: при больших значениях M и недостаточной длине N анализируемой ПСП ($N < s\cdot M^2$) такая матрица даже для процессов со всеми $p_{ij}(s)$ отличными от нуля имеет вид равномерно заполненного "звездного неба". Тем не менее, последовательное по номеру s рассмотрение вида матриц переходов $p_{ij}(s)$=, ≠0 дает важную информацию о качестве исследуемого дискретного процесса.

Процесс с запаздыванием – это процесс с последействием. Однако введение в алгоритм операции преобразования интервала [1,M] в себя разрывает это последействие на каждом шаге, когда число x_n выходит за границы этого интервала. При этом формируемую алгоритмом (2.1) псевдослучайную последовательность при надлежащем выборе параметров алгоритма можно рассматривать фактически как процесс без последействия, т.е. как простую однородную цепь Маркова с вероятностями переходов $p_{ij}(s) \approx 1/M$. Показано, что при соответствующем выборе параметров алгоритма и начальных условий, при которых отличие матриц переходов $\boldsymbol{\pi}_s$ и $(\boldsymbol{\pi}_1)^s$ становится заметным, статистические свойства генерируемой ПСП ухудшаются по сравнению с чисто случайным процессом, даже если при этом распределение вероятностей $p(x)$ практически равномерное.

3. КОМБИНИРОВАННЫЙ ГЕНЕРАТОР ПСП

В работе [13] предложены и исследованы характеристики псевдослучайных последовательностей, определенных на ограниченном интервале целых чисел,

формируемых простейшими алгоритмами типа алгоритма Фибоначчи. Приведены выражения, а также методика расчета максимального периода TM, Nz ПСП для стандартного генератора типа Фибоначчи, в зависимости от интервала целых чисел {1,M} и параметра запаздывания (размерности фазового пространства) Nz. Знание точного значения максимального периода TM, Nz позволяет скомбинировать два генератора, значительно улучшить статистические свойства таким образом, что период ПСП становится во много раз больше периода каждого отдельного парциального генератора. Работа каждого такого генератора производится в соответствии с алгоритмом генерации и возврата вновь вычисленного значения в область определения {1, M}

$$X_n = X_{n-1} + X_{n-Nz},$$
$$X_n = X_n - M \; for \; X_n > M. \qquad (3.1)$$

Область определения {1, M} и задержка Nz для каждого из парциальных генератора свои. Комбинированный генератор ПСП функционирует следующим образом: два парциальных генератора работают синхронно и генерируемые ими на каждом шаге числа складываются, порождая новую последовательность. Если результат сложения выходит из интервала {1, M_0}, то включается алгоритм возврата, аналогичный (3.1). Вышесказанное можно записать в виде:

$$X_{1,n} = X_{1,n-1} + X_{1,n-Nz1} \rightarrow$$
$$\rightarrow X_{1,n} = X_{1,n} - M_1 \; for \; X_{1,n} > M_1;$$
$$X_{2.n} = X_{2,n-1} + X_{2,n-Nz2} \rightarrow$$
$$\rightarrow X_{2,n} = X_{2,n} - M_2 \; for \; X_{2,n} > M_2; \qquad (3.2)$$
$$X_{0,n} = X_{1,n} + X_{2,n} \rightarrow$$
$$\rightarrow X_{0,n} = X_{0,n} - M_0 \; for \; X_{0,n} > M_0.$$

В соответствии с результатами [6] для получения максимального периода необходимо задавать начальные условия (НУ) в виде последовательности из Nz единиц. Тогда, если $Nz_1 > Nz_2$, то для 1-го генератора НУ для достижения максимального периода – последовательность из Nz_1 единиц, а 2-й генератор в качестве НУ соответственно имеет Nz_2 единиц. Недостающие для начала работы алгоритма комбинированного генератора (Nz_1 – Nz_2) числа должны сначала быть вычислены с использованием алгоритма 2-го парциального генератора. Таким образом, для комбинированного генератора НУ фактически являются Nz_1 чисел, причем первые Nz_2 из них равны 2. Следовательно, НУ для комбинированного генератора повторятся, и формируемая им последовательность выйдет на период (T_0) тогда, когда в точности (и одновременно) повторятся НУ для каждого из парциальных генераторов. Соответствующее условие запишется в виде:

$$N_1 T_{M1,Nz1} = N_2 T_{M2,Nz2} = T_0, \qquad (3.3)$$

где N_1 и N_2 – целые числа. Таким образом, T_0 должен без остатка делиться на $T_{M1,Nz1}$ и $T_{M2,Nz2}$ и, следовательно, максимальное значение для T_0 определяется произведением $(T_{M1,Nz1})(T_{M2,Nz2})$ и для достижения этого значения необходимо, чтобы $T_{M1,Nz1}$, $T_{M2,Nz2}$ не имели бы общих сомножителей и тем более являлись бы кратными числами.

Зная зависимость периода ПСП от максимального значения в области определения M и задержки Nz, можно подобрать такие M_1, Nz_1 и M_2, Nz_2, что период комбинированного генератора будет существенно превышать периоды парциальных генераторов T_{M1}, Nz_1 и T_{M2}, Nz_2. В случае небольших периодов это проверяется достаточно легко. Например, $T_{3,2}$ = 8 и $T_{4,3}$ = 14. Наименьшее число, которое делится на 8 и 14 без остатка – 56. Именно это значение получается в результате прямой генерации; $T_{15,7}$ = 97655, $T_{17,8}$ = 83520, период генерируемой последовательности чисел для комбинированного генератора – 1631229120, что много больше каждого из периодов парциальных генераторов. В качестве примера на **Рис. 3.1** приводится частотное распределение появления целых чисел в ПСП для комбинированного генератора в интервале определения {1,257}, при этом параметры парциальных генераторов таковы: M_1 = 257, Nz_1 = 11, M_2 = 253 и Nz_2 = 15. Это распределение получено для массива из 10^9 чисел, максимальное значение – 3896607, минимальное – 3885514, разность между ними составляет 11093 и разность отнесенная к

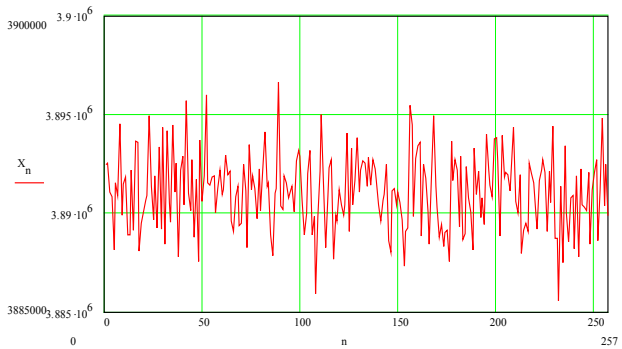


Рис. 3.1. *Распределение появления целых чисел в ПСП для комбинированного генератора в интервале определения {1,257}.*

максимальному значению – 0.0028; среднее значение ~$3.89 \cdot 10^6$; среднеквадратичное отклонение ~$1.89 \cdot 10^3$. Приведенное частотное распределение целых чисел близко к равномерному по статистическим критериям.

Предложенный алгоритм и его характеристики представляют методический интерес, т.к. для получения периода сколь угодно большой длительности число задающих генераторов может быть увеличено, а X_{0n} может быть линейной комбинацией чисел X_n с отличными от единицы весовыми коэффициентами C_n для каждого из парциальных генераторов), т.е.

$$X_{0n} = \sum_{i=1}^{N} C_{in} X_{in}. \qquad (3.4)$$

4. ХАОТИЧЕСКИЙ КОДИРУЮЩИЙ АЛГОРИТМ НА ОСНОВЕ ДВУМЕРНОГО ОТОБРАЖЕНИЯ

В качестве базового дискретного алгоритма был выбран одномерный алгоритм типа генератора случайных чисел Фибоначчи $x_n = f(x_{n-1},\ldots, x_{n-Nz}, Nz, M)$ [13]. Общий вид исследуемого двумерного алгоритма:

$$\begin{aligned} x_n &= f_1(x_{n-1},\ldots,x_{n-Nz1}, y_{n-1},\ldots,y_{n-Nz2}, Nz1, Nz2, M), \\ y_n &= f_2(y_{n-1},\ldots,y_{n-Nz2}, x_{n-1},\ldots x_{n-Nz1}, Nz1, Nz2, M). \end{aligned} \qquad (4.1)$$

Область определения алгоритма – замкнутый интервал целых чисел [1, M]. В процессе генерации последовательности при выходе чисел x_n, y_n из интервала [1, M] применялось преобразование возврата $x_n \to x_n \pm M$ и $y_n \to y_n \pm M$.

Фазовое пространство (ФП) алгоритма имеет размерность ($Nz_1 + Nz_2$). Число состояний системы в этом пространстве для алгоритма, определенного на ограниченном дискретном множестве, конечно и равно $\mathbf{M}^{(Nz1+Nz2)}$. Поскольку каждое состояние системы определено на конечном и ограниченном множестве чисел и явный вид алгоритма представляет собой однозначное отображение, то система рано или поздно попадет в первоначальное состояние и процесс станет периодическим. До выхода на период формируемая последовательность, как показывает численный эксперимент, является псевдослучайной. Появление периода в последовательности $\{\mathbf{x}_n\}$, так же как и в последовательности $\{\mathbf{y}_n\}$ реализуется в случае одновременного точного повторения полных наборов начальных условий из запаздывающих членов $(\mathbf{x}_{n-1},\ldots, \mathbf{x}_{n-Nz1})$ и $(\mathbf{y}_{n-1},\ldots, \mathbf{y}_{n-Nz2})$.

Исследование структуры ФП алгоритма было проведено в доступном для численного анализа диапазоне параметров M, Nz1, Nz_2: $M^{(Nz1+Nz2)} \le 10^6 \div 10^7$. В **Таблицах 1** и **2** приведены результаты исследования структуры ФП алгоритма при нечетном (M = 3) и четном (M = 4) значениях параметра M в сопоставлении со спектрами циклов базового одномерного алгоритма с соответствующими значениями параметров.

Таблица 1

Nz = 3	18, 8, 1	$\mathbf{M}^{Nz}$ = 27
Nz = 4	44, 29, 7, 1	$\mathbf{M}^{Nz}$ = 81
Nz = 5	118, 70, 22, 16, 13, 3, 1	$\mathbf{M}^{Nz}$ = 243
Nz = 6	457, 100, 61, 31, 28, 26, 25, 1	$\mathbf{M}^{Nz}$ = 729
Nz_1 = 4 Nz_2 = 3	1258, 351, 270, 88, 26, 1	$\mathbf{M}^{(Nz1+Nz2)}$ = 2187
Nz_1 = 5 Nz_2 = 3	3614, 862, 798, 645, 496, 70, 16, 1	$\mathbf{M}^{(Nz1+Nz2)}$ = 6561
Nz_1 = 5 Nz_2 = 4	8789, 5677, 2725, 1391, 613, 207, 39, 1	$\mathbf{M}^{(Nz1+Nz2)}$ = 19683
Nz_1 = 6 Nz_2 = 4	24844, 23261, 5908, 2781, 400, 1	$\mathbf{M}^{(Nz1+Nz2)}$ = 59049

Таблица 2

Nz = 3	14(4), 7, 1	$\mathbf{M}^{Nz}$ = 64
Nz = 4	30(8), 15, 1	$\mathbf{M}^{Nz}$ = 256
Nz = 5	42(22), 21, 14(4), 7, 6(2), 3, 1	$\mathbf{M}^{Nz}$ = 1024
Nz = 6	126(32), 63, 1	$\mathbf{M}^{Nz}$ = 4096
Nz_1 = 4 Nz_2 = 3	186(68), 93, 62(8), 31, 1	$\mathbf{M}^{(Nz1+Nz2)}$ = 16384
Nz_1 = 5 Nz_2 = 3	60(544), 30(8), 15, 1	$\mathbf{M}^{(Nz1+Nz2)}$ = 65536
Nz_1 = 5 Nz_2 = 4	465(412), 31(3), 1	$\mathbf{M}^{(Nz1+Nz2)}$ = 262144
Nz_1 = 6 Nz_2 = 4	84(1149), 42(43), 21, 14(4), 1	$\mathbf{M}^{(Nz1+Nz2)}$ = 1048576

В Таблицах 1 и 2 в круглых скобках указано количество циклов одинакового периода.

ФП исследуемого алгоритма состоит из набора циклов разной кратности и длины и одной особой изолированной точки с координатами (M, M,…, M). Из Таблицы 1 видно, что при нечетных M все циклы имеют одинарную кратность, точно также как и в ФП базового алгоритма. При этом явная закономерность между размерами циклов в ФП сопоставляемых алгоритмов не просматривается. Размер наибольшего цикла составляет ~0.5 от полного числа состояний в фазовом пространстве $\mathbf{M}^{(Nz1 + Nz2)}$.

При четных значениях M (Таблица 2) циклы в ФП, как правило, короткие и многократные, как и в случае базового алгоритма. Спектры циклов двумерного алгоритма с параметрами Nz_1 и Nz_2 не содержат циклов парциальных базовых алгоритмов с $Nz = Nz_1$ и $Nz = Nz_2$, но имеют циклы базового алгоритма с $Nz = (Nz_1 + Nz_2)/2$ с добавлением циклов удвоенного периода. При этом основные периоды циклов двумерного алгоритма отличаются в целое число раз от фундаментального периода в каждой из серий циклов: например, при $Nz_1 = 4$, $Nz_2 = 3$ спектр циклов – 31 (фундаментальный период), 62, 93, 186. Такой характер спектра циклов свойственен и одномерному алгоритму при четных значениях M.

Из Таблицы 1 видно, что размер циклов наибольшей длины двумерного алгоритма почти на два порядка превышает размер цикла соответствующего одномерного алгоритма при $Nz_1 = Nz$. Но этот выигрыш обусловлен не столько специфическими особенностями двумерного отображения по сравнению с одномерным аналогом, сколько реальным увеличением размерности ФП. Соотношение между длиной цикла максимального размера и полным числом состояний в ФП остается прежним ~0.5.

Оценку статистических характеристик надо проводить не при малых, а при реальных, т.е. относительно больших значениях параметров, соответствующих развитому хаосу и формированию длинных псевдослучайных последовательностей с хорошими корреляционными свойствами. Поэтому расчеты выполнены при параметрах M = 255, $Nz_1 = 16$, $Nz_2 = 11$. Показано, что двумерный алгоритм формирует псевдослучайную последовательность с практически равномерным распределением вероятностей $p(x) = 1/M$. Для сегмента последовательности с N = 210000 отличие от этого распределения составляет: относительное среднее отличие по модулю $\Delta\mathbf{p}_{ср} = 0.028$ при максимальном $\Delta\mathbf{p}_{макс} = 0.10$, среднеквадратичное $\boldsymbol{\sigma} = 0.002$.

Оценка корреляционных характеристик формируемых последовательностей проводилась на основе анализа неклипированных и клипированных 100 пар сегментов размером в 128 и 1024 символа, последовательно генерируемых алгоритмом без какого-либо отбора, в том числе и без отбора по сбалансированности кодов. Получено, что уровень выбросов авто- и взаимокорреляционных функций не превышал следующих значений: $(1.5\div4.8)/\sqrt{N}$ для сегментов с N = 128 и $(2.5\div4.9)/\sqrt{N}$ для сегментов с N = 1024, что согласуется с соответствующим уровнем боковых выбросов корреляционных функций чисто случайных последовательностей с равномерным распределением, так и последовательностей, генерируемых базовым алгоритмом.

Подсчет блоков из одинаковых символов на реализации клипированной последовательности из 270000 чисел показал, что вероятность появления таких блоков полностью подчиняется закону $\mathbf{p(k) = 1/2^k}$ вплоть до блока размером $\mathbf{k}$ = 12 с несущественными отличиями от этого закона для блоков из $\mathbf{k}$ = 13÷18 символов. Последние отличия обусловлены скорее недостаточностью данных для статистической обработки результатов, чем свойствами самих алгоритмов.

Оценка объема системы сигналов, формируемых двумерным и базовым алгоритмами, производилась отбором из сформированной клипированной последовательности сбалансированных кодов с заданными корреляционными свойствами. Показано, что при одинаковых длинах реализации последовательности число отбираемых кодов и скорость их отбора близки для обоих сопоставляемых алгоритмов.

Таким образом, проанализирована структура фазового пространства двумерного алгоритма. Найден спектр периодов циклических траекторий в ФП, различающихся начальными условиями. Установлено, что статистические свойства псевдослучайных последовательностей, формируемых базовым дискретным алгоритмом и алгоритмом с двумерным отображением при сопоставимых параметрах близки. Однако двумерный алгоритм имеет повышенную сложность, что значительно затрудняет его реконструкцию по реализации сформированной алгоритмом последовательности.

5. МЕТОДЫ ФРАКТАЛЬНОГО АНАЛИЗА ХАОТИЧЕСКИХ АЛГОРИТМОВ

Для эффективной реализации хаотических сигналов в радиотехнических комплексах, телекоммуникационных системах, а также для применения их в качестве информационного носителя в информационных технологиях нового поколения наряду с обычными методами исследования статистических и корреляционных характеристик необходимо разработать альтернативные методы оценки структурной сложности алгоритма и фрактальной размерности ПСП [14].

Методы фрактального анализа генераторов случайных чисел в настоящее время включают в себя определение фрактальных размерностей динамических систем, компьютерную обработку как траектории движения этих систем в фазовом пространстве (ФП), так и формируемого системой процессов в проекциях на плоскости в ФП и на координатные оси. В последнем случае речь идет об исследовании свойств непосредственно генерируемой алгоритмом последовательности.

Для эффективного применения алгоритмов фрактальной обработки необходимо представить алгебраический объект – последовательность чисел или знаков в виде графического образа. В качестве геометрических образов, характеризующих свойства хаотических алгоритмов, можно выбрать пошаговое отображение на плоскости членов рекуррентной последовательности (**Рис. 5.1***а*), двумерное сечение многомерного фазового пространства хаотического алгоритма (Рис. 5.1*б*), а также проекцию многомерного фазового пространства хаотического алгоритма на одну из координатных плоскостей с учетом или без кратности каждой точки состояния системы (Рис. 5.1*в*). Пример такой проекции ФП алгоритма с параметрами N=30000 приведен (представлен) на Рис. 5.1*в*.

Измерение фрактальных характеристик производилось по яркостному полю изображений. При измерениях по двумерному полю могут использоваться два метода. Первый – метод «скользящего окна» – позволяет получить зависимость $S = f(\delta)$, где S- измеряемый параметр, определяющий фрактальную сигнатуру, δ – размер сглаживающего окна. Второй – метод измерения локальной дисперсионной размерности, заключающийся в измерении дисперсии яркости малого участка изображения на двух масштабах. Этот метод позволяет получить спектр фрактальных размерностей по изображению [14].

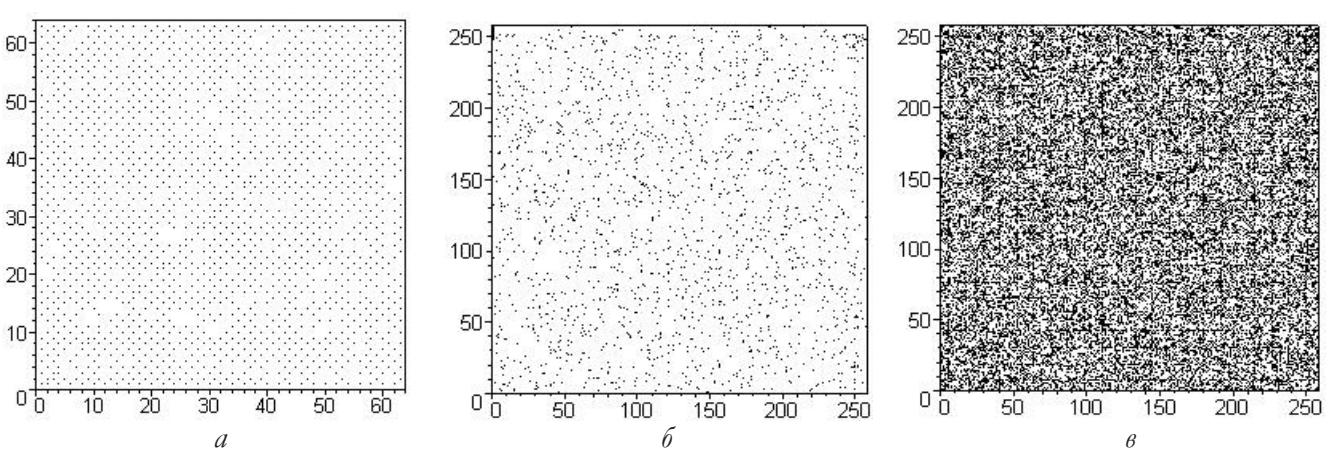


Рис. 5.1. *а) Отображение на плоскости пар членов рекуррентной хаотической последовательности, б) Двумерное сечение многомерного фазового пространства хаотического алгоритма, в) Проекция ФП хаотического алгоритма с запаздыванием.*

С этой целью анализировались простейшие алгоритмы формирования псевдослучайных последовательностей целых чисел $\{x_n\}$ с запаздыванием, использующие отображение Фибоначчи и его модификации:

$$Algorithm\ F-1 \quad \tilde{x}_n = x_{n-1} + (-1)^{x_{n-Kz}} x_{n-Nz} \quad 5(1)$$

$$Algorithm\ F-2 \quad \tilde{x}_n = x_{n-1} + (-1)^{x_{n-Nz}} x_{n-Nz} \quad 5(2)$$

$$Algorithm\ F-3 \quad \tilde{x}_n = x_{n-1} + x_{n-Nz} \quad 5(3)$$

где Nz и Kz – параметры алгоритмов, $2 \le Kz \le (Nz - 1)$. В отличие от работы [13] знак перед запаздывающим членом в F-1, F-2 изменяется не случайным независимым образом, а определяется внутренней динамикой системы. Параметр обратной связи Nz определяет размерность фазового пространства алгоритма и, соответственно, размерность радиус-вектора $R_n(x_{n-1}, x_{n-2}, ..., x_{n-Nz})$ состояния дискретной динамической системы на каждом шаге.

Объем фазового пространства (ФП) отображения Фибоначчи размерности Nz практически не ограничен. Для реального применения алгоритмов ПСП в радиотехнических системах и формирования модулирующих цифровых сигналов конечной разрядности необходимо задать область определения алгоритма на конечном множестве чисел замкнутого интервала натурального ряда [1, M], где M>1. Для этого отображения (4.1-4.3) должны быть дополнены операцией преобразования числового интервала [1, M] самого в себя, например, следующего вида:

$$\begin{aligned} &x_n = \tilde{x}_n, && if \quad \tilde{x}_n \in [1, M], \\ &x_n = \tilde{x}_n - M, && if \quad \tilde{x}_n > M, \\ &x_n = \tilde{x}_n + M, && if \quad \tilde{x}_n < 1. \end{aligned} \quad (5.4)$$

Это преобразование, соответствующее свертыванию отрезка [1, M] в кольцо, играет важную роль в механизме хаотического поведения данных динамических систем. Эта операция ограничивает объем фазового пространства, делая его конечным, равным $V_{ФП} = M^{Nz}$ точек состояний и обеспечивает дополнительное перемешивание траекторий в фазовом пространстве. Операции отображения интервала [1, M] самого в себя делают преобразования алгоритма неоднозначными, что не позволяет восстановить формулу и параметры алгоритма по известной реализации клипированного процесса.

Необходимо отметить, что одного преобразования числового интервала самого в себя недостаточно для эффективного перемешивания траекторий в фазовом пространстве. Определенный механизм хаотизации должен уже содержаться в функции отображения. В данном случае это обеспечивается свойствами отображения Фибоначчи. Эти два условия – ограниченность объема фазового пространства и наличие мощного механизма перемешивания – являются необходимыми условиями хаотического поведения любой динамической системы.

В качестве альтернативы также рассматривался алгоритм (F-4) на основе отображения Фибоначчи (5.3), но с другой операцией преобразования числового интервала [1, M] самого в себя – типа отражающей границы:

$$\begin{aligned} &x_n = \tilde{x}_n, && if \quad \tilde{x}_n \in [1, M], \\ &x_n = M, && if \quad \tilde{x}_n > 2 \cdot M, \\ &x_n = 2 \cdot M - \tilde{x}_n, && if \quad M < \tilde{x}_n < 2 \cdot M. \end{aligned} \quad (5.5)$$

В зависимости от выбора начальных условий радиус-вектор Rn описывает в фазовом пространстве алгоритма траекторию, представляющую собой последовательные дискретные переходы из одной точки состояния динамической системы (ДС) в другую по случайному закону. Эти "траектории" движения дискретной ДС в ФП из-за ограниченности объема ФП образуют замкнутые циклы, которые, вследствие однозначности преобразований, не пересекаются и не имеют общих точек. Кроме того, в ФП могут существовать бассейны циклов и изолированные точки. Циклы исследованных алгоритмов F-1, F-2, F-3, F-4 имеют важную отличительную особенность: поведение динамической системы до замыкания цикла (равным образом и на траектории бассейна, если он существует) имеет хаотический характер, а порождаемая при этом алгоритмом непериодическая последовательность – псевдослучайного типа.

Множество таких точек в ФП, объединенных в цикл, назовем псевдослучайным циклом (ПСЦ), если формируемый алгоритмом непериодический процесс до замыкания цикла имеет хаотический характер, в отличие от регулярного цикла, которому до выхода ДДС на период соответствует регулярный процесс. Псевдослучайному циклу (до его замыкания) соответствует нерегулярное движение в фазовом пространстве, а регулярному циклу- регулярное. В обоих случаях поведение динамической системы на цикле полностью детерминировано. Траектория псевдослучайного цикла представляет собой детерминированное множество хаотически следующих одна за другой точек состояний дискретной динамической системы во всем объеме фазового пространства алгоритма. Аналогом псевдослучайного цикла дискретной системы является странный аттрактор непрерывной динамической системы [15].

Различия между псевдослучайным и регулярным циклами интуитивно совершенно понятны. Периодическое движение всегда регулярно, но регулярное движение не обязательно периодическое. Таким образом ПСЦ – это такое движение дискретной динамической системы (ДДС), которое на интервалах рассмотрения, меньших периода, – случайное хаотическое, а на интервалах, больших периода (точнее $N > 2T = 2\mathrm{Np}$), поведение системы следует рассматривать уже как регулярное и периодическое.

В зависимости от значений параметров $\mathrm{Nz} \geq 3$, Kz и M в фазовом пространстве алгоритмов F-1, F-2, F-3 существует целый ряд циклов различного периода. Каждому длинному ($N \sim V_{\text{ФП}}$) циклу до его замыкания соответствует непериодическая ПСП с практически равномерным распределением $p(x) \approx 1/\mathrm{M}$ генерируемых чисел в заданном интервале области определения $p(x) \approx 1/\mathrm{M}$ и с равномерными распределениями условных вероятностей. Для характеристики фрактальных свойств хаотического множества точек на ПСЦ ограничимся анализом геометрической и корреляционной размерностей [16].

Методы фрактального анализа могут быть применены, в принципе, к любому числовому множеству. В том числе при исследовании дискретных ДС эти методы могут быть непосредственно применены к множеству точек состояний системы в n-мерном ФП, а также могут быть применены и к множеству точек проекций этих состояний на выделенные поверхности в фазовом пространстве. Методы фрактального анализа могут быть с успехом распространены также на проекции фазового пространства на координатные оси, в последнем случае мы имеем дело с исследованием фрактальных свойств непосредственно последовательностей, формируемых дискретными алгоритмами.

Для характеристики фрактальных свойств хаотического множества точек на псевдослучайном цикле в Nz-мерном ФП ограничимся анализом эвклидовой D и корреляционной размерностей D_2. Компьютерный анализ проводился для небольших значений параметров хаотического алгоритма с запаздыванием, что имеет принципиальное значение для оценки мажоритарных свойств ПСЦ. При увеличении размерности алгоритма характер поведения ДДС существенно усложняется и улучшаются статистические характеристики формируемых ПСП.

Оценку корреляционной размерности D_2 исследуемого псевдослучайного движения дискретной динамической системы по траектории в многомерном ФП можно дать на основе вычисления корреляционного интеграла C(l), заданного на множестве расстояний l между всеми парами векторов состояний ДС на цикле в ФП, построения зависимости $\lg(C(l)) = f(\lg(l))$, показанной на **Рис. 5.2**, и определения на ней углового коэффициента прямолинейного участка.

Кривая 1 на этом рисунке соответствует алгоритму с параметрами Nz = 3, Kz = 2, M = 15, ПСЦ с начальным вектором $R_0(1, 1, 1)$ и длине реализации процесса $N = 630$. С помощью вычисления локального углового коэффициента можно дать следующую оценку корреляционной размерности исследуемого цикла: $D_2 \sim 2.4$. Полученное значение

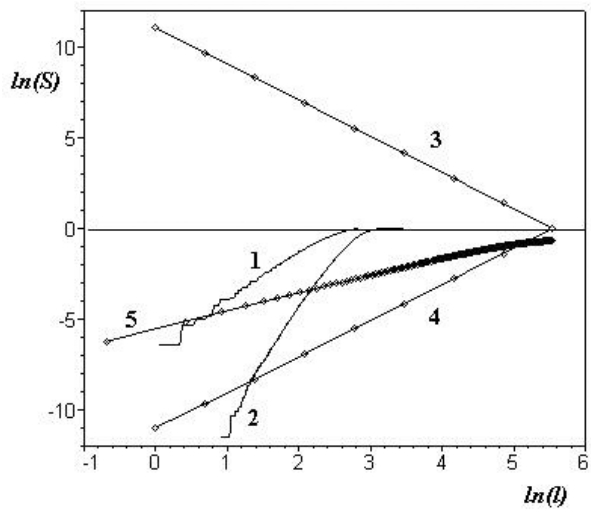


Рис. 5.2. *Фрактальные сигнатуры для определения хаусдорфовой и корреляционной размерностей.*

согласуется с эвклидовой размерностью $D = 3$, $D_2/D \sim 0.8$. Величина последнего отношения может служить характеристикой степени однородности заполнения точками цикла полного объема ФП.

Кривая 2 на Рис. 5.2 соответствует логарифму корреляционного интеграла для ПСЦ с $R_0(1, 1, ..., 1)$ алгоритма с параметрами Nz = 7, Kz = 4, M = 15, N = 630. Графики 1 и 2 функции $\ln(C(l)) = f(\ln(l))$ на Рис. 5.2 идентичны друг другу, но имеют разный наклон протяженных прямолинейных участков из-за отличия размерностей ФП. Для кривой 2 наклон соответствует корреляционной размерности анализируемого цикла $D_2 \sim 5.85$, $D = 7$, $D_2/D = 0.83$. Отметим, что длинным циклам алгоритма соответствуют ПСП с хорошими статистическими и корреляционными свойствами, особенно при увеличении запаздывания Nz больше 5.

Анализ фрактальных характеристик точек проекции состояний ДС на двумерную координатную плоскость (X_{-1}, X_{-2}) с учетом их кратности проведен методом покрытия числового множества элементарными ячейками со стороной l, подсчетом требуемого их количества $S(l)$ и последующим вычислением хаусдорфовой и корреляционной размерностей. Кривая 3 на Рис. 5.2 соответствует зависимости $\lg(C(l)) = f(\lg(l))$ проекции ПСЦ с начальным вектором $R_0(2, 2, \ldots, 2)$ алгоритма с параметрами Nz = 16, Kz = 9, M =255, длине реализации процесса N = 650000. $D_0 = 2.0$, $D = 2$, $D_0/D = 1$. Кривая 4 на рисунке получена путем подсчета логарифма сумм квадратов наблюдаемых частот появлений проекций состояний ДС в элементарных ячейках, покрывающих числовое множество, что дает следующую оценку корреляционной размерности проекции ПСЦ $D_2 = 1.989$, $D = 2$, $D_2/D = 0.994$.

Определение по стандартной методике корреляционной размерности, примененное к одномерному ($D = 1$) хаотическому массиву из N = 6500 чисел ПСП, сформированному алгоритмом с параметрами Nz = 16, Kz = 9, M = 255 (кривая 5 на Рис. 5.2) дало значение корреляционной размерности $D_2 = D_2/D = 0.988$, что свидетельствует о достаточно хорошей однородности заполнения интервала [1, M] генерируемыми числами. Это подтверждается анализом одномерного распределения вероятностей чисел в последовательности.

На **Рис. 5.3** приведены результаты компьютерного вычисления фрактальных сигнатур $\ln S = f(\ln a)$, где S – яркостная характеристика графического образа ФП хаотического алгоритма, a – сторона окна (измерительное окно квадратное, относительный размер окна a менялся от 3 до 30 пиксел).

Из рисунка видно, что все сигнатуры имеют участки с разным доминирующим наклоном, что характеризует степень статистической связи между соответствующими членами рекуррентной хаотической последовательности. Как показал численный анализ, фрактальные

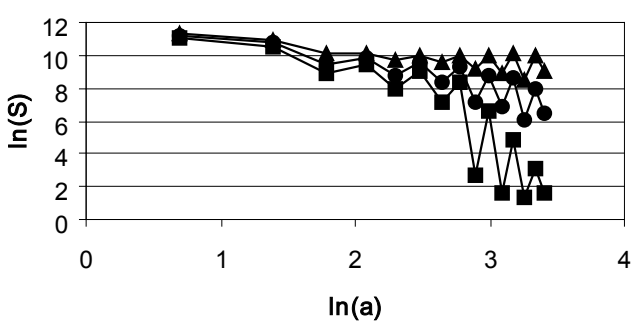


Рис. 5.3. *Фрактальные сигнатуры попарных отображений: квадрат – отображение $(x_n; x_{n+1})$, круг – $(x_n; x_{n+2})$, треугольник – $(x_n; x_{n+9})$.*

сигнатуры отображений алгоритмов с хорошим перемешиванием (слабая статистическая связь между парами членов рекуррентной хаотической последовательности) характеризуются меньшим разбросом и практически одинаковым наклоном.

Методами компьютерного анализа исследовались хаотические алгоритмы F-1, F-2, F-3, F-4 с запаздыванием с различными характеристиками (параметр запаздывания, различные механизмы перемешивания). Для алгоритма F-1 корреляционная размерность множества точек на цикле с начальным вектором $R_0(8,6,7,1)$ (кривая 1) равна $D_2 = 3.3$. Полученное значение согласуется с эвклидовой размерностью $D = 4$, $D_2/D = 0.83$. Величина последнего отношения может служить характеристикой степени однородности заполнения точками цикла полного объема ФП. Как показал анализ, исследованному циклу с начальным вектором $R_0(8,6,7,1)$ соответствует непериодическая ПСП длиной $N = 14030$ с распределением генерируемых чисел, близким к равномерному.

Линейный участок графика (кривая 2), полученного для множества точек траектории бассейна и цикла в фазовом пространстве алгоритма F-2, имеет несколько меньший наклон, которому отвечает значение корреляционной размерности около $D_2 = 3.0$. Кривая 3 на Рис. 5.3 соответствует логарифму корреляционного интеграла для псевдослучайного цикла с начальными условиями $R_0(1,6,6,7)$ тестируемого алгоритма F-3. Графики 1 и 3 функции $\log(C(l)) = f(\log(l))$ на **Рис. 5.4** почти в точности повторяют друг друга и имеют протяженный прямолинейный участок с наклоном $D_2 = 3.3$, что и позволяет получить количественную оценку однородности заполнения пространства точками состояний ДС на псевдослучайных циклах. Отметим, что алгоритмам F-1 и F-3 соответствуют ПСП с хорошими статистическими и корреляционными свойствами, особенно при увеличении запаздывания больше 5.

Для цикла алгоритма F-4 с начальным радиус-вектором $R_0(7,14,6,15)$, период T = 613, зависимость $\log(C(l)) = f(\log(l))$ (кривая 4 на Рис. 5.2) не имеет четко выраженного прямолинейного участка. Это означает, что у корреляционного интеграла существенные отклонения от закона $C(l) \sim 1 - D$ и, следовательно,

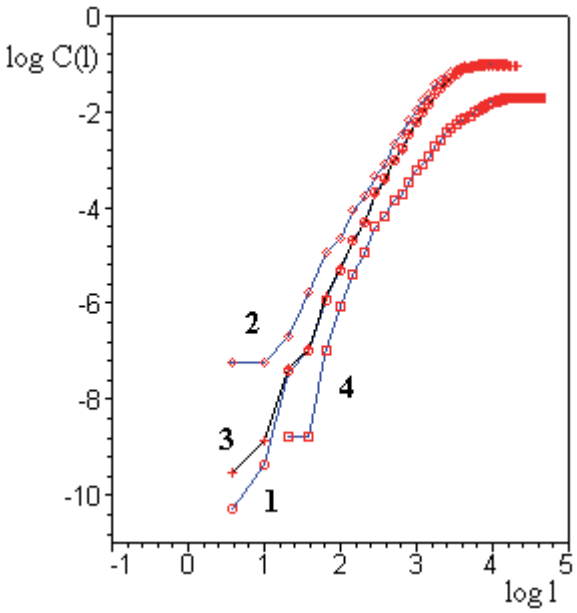


Рис. 5.4. *Зависимость $\log_2 C(l)$ от $\log_2 l$ для хаотических алгоритмов с запаздыванием и различными параметрами задержки.*

точки данного псевдослучайного цикла расположены в ФП неравномерно.

Фрактальный анализ может быть применен не только к хаотическому множеству точек в многомерном ФП, но и к одномерному множеству чисел реализации ПСП. Определение по стандартной методике корреляционной размерности, примененное к одномерному (эвклидова размерность $D = 1$) хаотическому массиву из $N = 1000$ чисел ПСП, сформированному алгоритмами F-1, F-2, F-3, F-4 при различных параметрах запаздывания дало следующие результаты. Для всех тестируемых алгоритмов значение корреляционной размерности находится в пределах $D_2 = D_2/D = 0.91 \div 0.96$, в том числе для генератора случайных чисел RND математического программного пакета Maple. Полученные значения отношения D_2/D свидетельствует о достаточно хорошей однородности заполнения области определения генерируемыми числами. Это подтверждается также анализом одномерного распределения вероятностей чисел в последовательности.

Из приведенных данных видно, что исследованные хаотические алгоритмы, так же как и сертифицированный генератор случайных чисел RND, демонстрируют достаточно

высокое структурное качество формируемых последовательностей. При изменении функции распределения генерируемых чисел $p(x)$ и коэффициента корреляции предложенная методика оценки степени структурной сложности эффективно фиксирует соответствующее изменение статистических свойств ПСП.

Таким образом, показано, что вычисление фрактальных характеристик рекуррентных хаотических последовательностей и их графических образов позволяет количественно оценить эффективность механизма перемешивания и степень статистической связи между членами хаотической последовательности, что в конечном итоге определяет сложность хаотического порождающего алгоритма.

6. СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПСЕВДОСЛУЧАЙНЫХ СИГНАЛОВ, ФОРМИРУЕМЫХ ДИСКРЕТНЫМИ АЛГОРИТМАМИ С ЗАПАЗДЫВАНИЕМ

Наиболее полную информацию о статистических свойствах дискретных последовательностей дает анализ распределений попарных условных вероятностей членов последовательности $p(i+j,\ x_n|i,\ x_k)$, $j = 1, 2, 3, \ldots, k$, $l = 1, 2, 3, \ldots, M$. Попарная условная вероятность представляет собой вероятность генерации числа x_n на $(i+j)$-том шаге алгоритма, если на i-том шаге было получено число x_k. При этом областью определения дискретного алгоритма является произвольный замкнутый целочисленный интервал [M1, M2], M = M2 – M1 + 1, $x_n \in$ [M1, M2].

Если распределение условных вероятностей при любом j практически совпадает с равномерным распределением, то отсюда следует, что все вероятности перехода $p(i+j,\ x_n|i,\ x_k) \approx 1/M$, $j = 1, 2, 3, \ldots$ при произвольном выборе i. В то же время, если распределение вероятностей генерируемых чисел $p(x_n)$ близко к равномерному, то вероятность значения xn практически также равна 1/M. Тем самым вероятности перехода в состояние x_n на j-том шаге совпадают с вероятностью этого значения на этом шаге независимо от значений последовательности на предыдущих шагах алгоритма, что характерно для случайных последовательностей при независимых испытаниях. Более того, формируемая таким алгоритмом псевдослучайная последовательность по своим вероятностным характеристикам будет близка к последовательности независимых равновероятных чисел из интервала [M1, M2] [17]. В последнем случае можно ожидать, что данная последовательность будет обладать наилучшими статистическими свойствами. Установление подобного факта подчеркивает важность исследования распределений условных вероятностей для априорного суждения о качестве формируемых псевдослучайных последовательностей.

Для характеристики условных распределений $p(x_{i+j}|x_i)$ большое значение имеет вид расположения точек $(x_{i+j},\ x_i)$ на плоскости для отображения $x_{i+j} = f(x_i)$, задаваемого дискретным алгоритмом, при соответствующих значениях $j = 1, 2, 3, \ldots$ и $i = 1, 2, 3, \ldots, N$ [18]. Получение разброса точек $(x_{i+j},\ x_i)$ и их визуализация на экране не требует больших вычислительных ресурсов по сравнению с непосредственным вычислением условных вероятностей, хотя характер этого разброса не дает непосредственно формы распределения условных вероятностей. Визуализация разброса свидетельствует о степени регулярности этих распределений, наличии функциональных связей, существовании запретных переходов, а то и целых запретных зон, что неизбежно сказывается на корреляционных и других статистических свойствах последовательности.

Рассмотрим простейшую формулу алгоритма с запаздыванием: $x_n = x_{n-1} + x_{n-Nz}$, где Nz – параметр запаздывания, дополненную операцией возврата в интервал [M1, M2] в случае выброса вновь полученного значения x_n за его пределы. В данном алгоритме перемешивание, хаотизация формируемого процесса осуществляется добавлением случайного значения запаздывающего члена последовательности и операцией клипирования получаемой суммы чисел на границе области определения M_2.

Для численного моделирования были приняты следующие значения параметров алгоритма: $M_1 = 1$, $M_2 = 255$, Nz = 16. Анализируемый алгоритм при выбранных значениях параметров и заданных начальных условиях, представляющих собой набор из 16-ти случайных чисел (вектор

запаздывания), формирует псевдослучайную последовательность с распределением вероятностей, близким к равномерному распределению $p(x) = 1/M$. Отличие от равномерного распределения характеризуется суммарным расхождением наблюдаемых в численном эксперименте частот появления в генерируемой последовательности чисел x_m и величины 1/M: $\Delta p_\Sigma = \sum_{m=1}^{M} \left| n(x_m)/N - 1/M \right|$, где $n(x_m)$ – количество чисел x_m в последовательности из N членов. Это суммарное расхождение численно совпадает с относительным средним отличием от равномерного закона $\Delta p_{ср.отн}$. Наибольшее относительное отличие частоты выпадения наблюдаемых чисел от значения 1/M: $\Delta p_{макс.отн.} = [1/(1/M)] \cdot | n(x_m)/N - 1/M |_{макс}$.

Полученные оценки распределений вероятностей и распределений условных вероятностей для последовательностей, формируемых анализируемыми в данной работе алгоритмами в сопоставлении со стандартным генератором RND, сгруппированы в **Таблице 3**:

Двумерное распределение пар точек (x_{i+j}, x_i), где $i = 1, 2, \ldots, N$ представляет собой равномерно заполненную область хаотически разбросанных точек, при любом $j = 1, 2, 3, \ldots, 16, \ldots, 32$. Такой характер равномерного, полного и случайного заполнения точками (x_{i+j}, x_i) численного интервала $[M_1, M_2]$ свидетельствует о хаотизации исследуемого процесса.

Более точные сведения о вероятностях перехода каждому из значений x_n дают построения распределений условных вероятностей. Для наглядного представления на **Рис. 6.1** построены гистограммы частот переходов только для 6-ти значений генерируемых чисел $x_k = (k - 1) \cdot 50 + 1$, $k = 1, 2, \ldots, 6$ с шагом $j = 1$. Гистограммы частот

Таблица3

Алгоритм	$p(x)$		$p(x_{i+j}\|x_i)$		
	N = 210 000		N = 52 000 000, k = 6		
	$\Delta p_{ср.отн.}$	$\Delta p_{макс.отн.}$	j	$\Delta p_{ср.отн.}$	$\Delta p_{макс.отн.}$
1	0.03	0.10	1	0.03	0.12
			16	0.031	0.12
2	0.03	0.10	1	0.997	1.12
			2	0.5	1.04
			16	0.03	0.10
RND	0.03	0.15	-	-	-

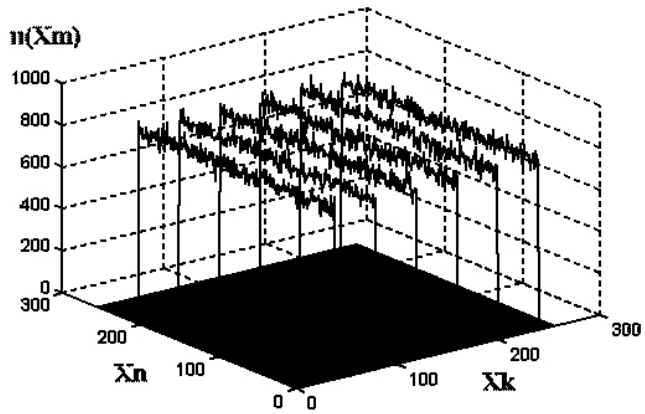


Рис. 6.1. *Гистограммы частот переходов для 6-ти значений генерируемых чисел $x_k = (k - 1) \cdot 50 + 1$, $k = 1, 2, \ldots, 6$ с шагом $j = 1$.*

рассчитаны по реализации последовательности из $5.2 \cdot 10^7$ членов. Значения $\Delta p_{ср,отн}$ и $\Delta p_{макс.отн.}$, характеризующие отличия от равномерного распределения одной из гистограмм (x_k = 251) для j = 1 и 16, приведены в Таблице 3. Из полученных данных следует, что для алгоритма №1 распределения условных вероятностей при любом j практически совпадают с равномерным распределением.

После соответствующего изменения алгоритма, при котором одномерное распределение остается равномерным, а функции распределений условных вероятностей $p(x_{i+1} | x_i) = 0$ ($j = 1$) через одно значение в зависимости от четности числа x_i на предыдущем шаге. Картина распределения точек на плоскости в этом случае носит регулярный характер (**Рис. 6.2**). Это подтверждается количественными отличиями $\Delta p_{ср.отн.}$ и $\Delta p_{макс.отн.}$ от равномерного распределения (см. Таблицу 3).

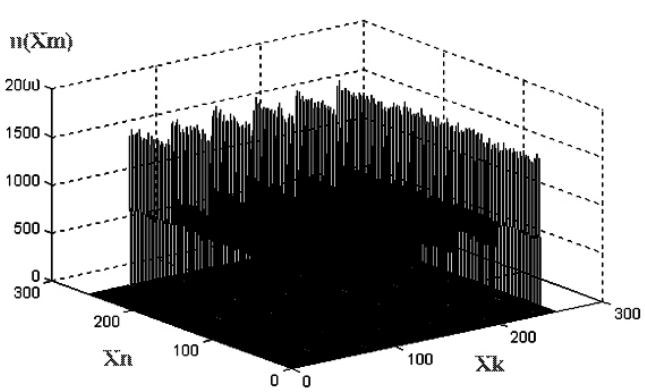


Рис. 6.2. *Распределение условных вероятностей.*

Оценка корреляционных характеристик последовательностей, сформированных алгоритмами № 1 и 2, проводилась на основе анализа клипированных и неклипированных 100 сегментов размером N = 128 и 1024 символов, последовательно генерируемых алгоритмами без какого-либо отбора. Несмотря на существенные различия в форме распределений $p(x_{i+1}|x_i)$ величина боковых выбросов АКФ и ВКФ относительно уровня $1/\sqrt{N}$ для обоих алгоритмов примерно одинакова и составляет: (1.3÷3.8) для АКФ N = 128, (1.5÷4.3) для ВКФ N = 128, (2.2÷4.8) для АКФ и ВКФ N = 1024. Эти данные свидетельствует о том, что рассмотренные выше особенности алгоритмов мало сказались на корреляционных свойствах как самих последовательностей, так и результатов их клипирования. В то же время численный эксперимент по блочной структуре на длине клипированной последовательности из $2.7\cdot10^5$ членов показал, что если алгоритм №1 генерирует последовательности с блоковой структурой, близкой к закону $p(k) = 1/2^k$ вплоть до блоков размером k = 17-18, то блоковая структура последовательностей, порождаемых алгоритмом №2, существенно отклоняется от этого закона (**Рис. 6.3**), что непосредственно связано с неравномерностью распределений вероятностей переходов даже на одном шаге $j = 1$.

Оценка объема системы сигналов, формируемых алгоритмами, производилась путем отбора из сформированной

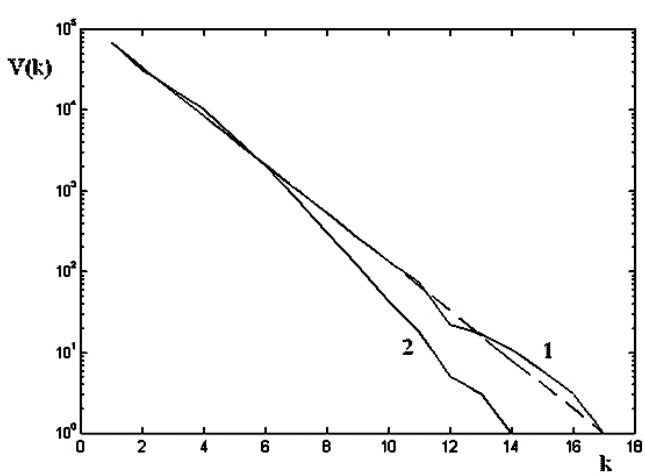


Рис. 6.3. *Блоковая структура последовательностей, порождаемых алгоритмом №2.*

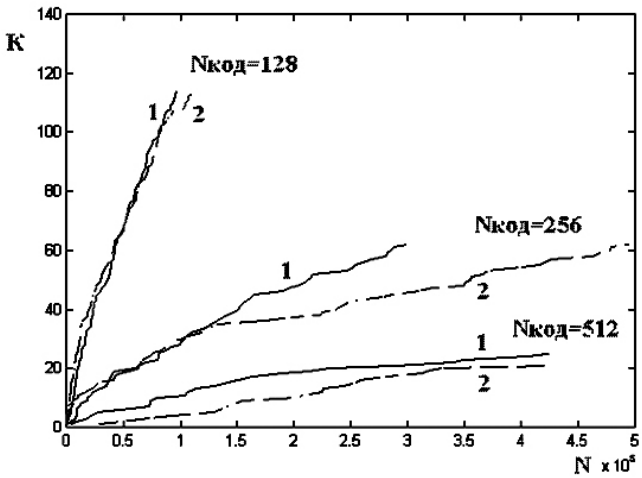


Рис. 6.4. *Количество сбалансированных кодов длиной из 128, 256 и 512 символов.*

клипированной последовательности сбалансированных кодов длиной из 128, 256 и 512 символов со следующими корреляционными свойствами: боковые выбросы апериодической автокорреляционной функции не превышают значения $R_{макс} = 2.26/\sqrt{N}_{код}$, а выбросы апериодических взаимокорреляционных функций по всему массиву отбираемых кодов меньше или равны $R_{макс} = 3.39/\sqrt{N}_{код}$. Корреляционные функции вычислялись по формуле для сбалансированных последовательностей [4].

Как показал численный эксперимент неравномерность условных распределений и существование запретных переходов сказались на скорости отбора кодов в систему сигналов по мере увеличения длительности последовательности N (**Рис. 6.4**). На этом рисунке все кривые, соответствующие алгоритму №2, проходят существенно ниже, чем у алгоритма №1.

7. МЕТОД АНАЛИЗА КОДИРУЮЩИХ ПСЕВДОСЛУЧАЙНЫХ АЛГОРИТМОВ НА ОСНОВЕ РАСПРЕДЕЛЕНИЯ КОДОВЫХ ГРУПП

Перспективным направлением развития современных радиотехнических систем связи является применение широкополосных шумоподобных сигналов [4,11]. Широкополосные системы связи имеют ряд преимуществ по сравнению с традиционными узкополосными системами. Эти преимущества связаны с ростом числа пользователей,

плотного заполнения частотного диапазона, необходимости обеспечения надежной конфиденциальной передачи информации. Необходимое для работы широкополосных систем расширение спектра передаваемого сигнала достигается применением псевдослучайных последовательностей, формируемые различными специальными алгоритмами. Эти и другие применения подобных последовательностей (избыточное кодирование информации в цифровых каналах связи, криптография, моделирование методами Монте-Карло) побуждают к поиску новых алгоритмов, в том числе с различными характеристиками и функциями распределения вероятностей. Одновременно продолжается поиск новых методов анализа статистических свойств, формируемых ими последовательностей, оценок близости их к идеальному случайному процессу [19]. Рассмотрен метод оценки статистических свойств цифровых многоуровневых псевдослучайных последовательностей путем анализа статистики распределения в них кодовых групп из полного кода для выбранной базы псевдослучайного сигнала. Развитием этого подхода является выяснение статистики интервалов между последовательными появлениями идентичных кодовых групп из полного кода. Ожидается, что этот подход позволит, в частности, анализировать структуру неизвестного алгоритма, формирующего исследуемую псевдослучайную последовательность. Проведено сопоставление указанных характеристик интервалов для последовательностей, формируемых различными алгоритмами, в том числе и применяемыми в стандартных программных пакетах.

Оценку статистических характеристик псевдослучайных последовательностей, формируемых некоторым алгоритмом, и близость к идеальной случайной последовательности можно рассматривать как процесс формирования серии шагов, результат которых на каждом шаге полностью независим от результатов на предыдущих шагах. При этом, если исследуемый алгоритм определен на множестве целых чисел, например на интервале [1, M], где M-макс. целое число, то можно считать, что соответствующая этим параметрам идеальная случайная последовательность будет формироваться в результате бросания M-мерного кубика, на каждой грани которого нанесено одно из целых чисел, входящих в указанный интервал.

Рассмотрен подход позволяющий анализировать статистические структурные особенности псевдослучайных целочисленных последовательностей. Исследуемая последовательность сравнивается с кодовой группой определенной длины и структуры. Длина группы – это число членов последовательности, равное выбранной базе псевдослучайного сигнала (B), а структура группы – это конкретный набор из B целых чисел из интервала [1, M]. Общее число всех различных кодов при этом равно числу элементов полного кода M^B [20].

Описанная процедура позволяет при многократном прохождении по выбранному участку последовательности для кодовых групп разной длины и структуры построить функции распределения вероятностей совпадения кодовых групп с текущей реализацией. Основываясь на модели идеальной случайной последовательности можно получить оценку близости к ней анализируемой последовательности для всех соответствующих функций распределения. Такие процедуры были выполнены для последовательностей, формируемых некоторыми алгоритмами. Эти последовательности имели указанные распределения, близкие к равномерным, и мало отличались по дисперсии от среднего значения дисперсии для идеальной случайной последовательности.

Установлено, что для псевдослучайных последовательностей, формируемых рядом алгоритмов (даже близких к идеальной случайной последовательности) при анализе интервалов (*K* – длина интервала) между совпадениями при смещении кодовой группы вдоль псевдослучайной последовательности обнаруживаются некоторые особенности. Для класса алгоритмов типа Фибоначчи [5] были получены близкие к равномерным распределения плотности вероятностей по всем кодовым группам для данной базы. Однако,

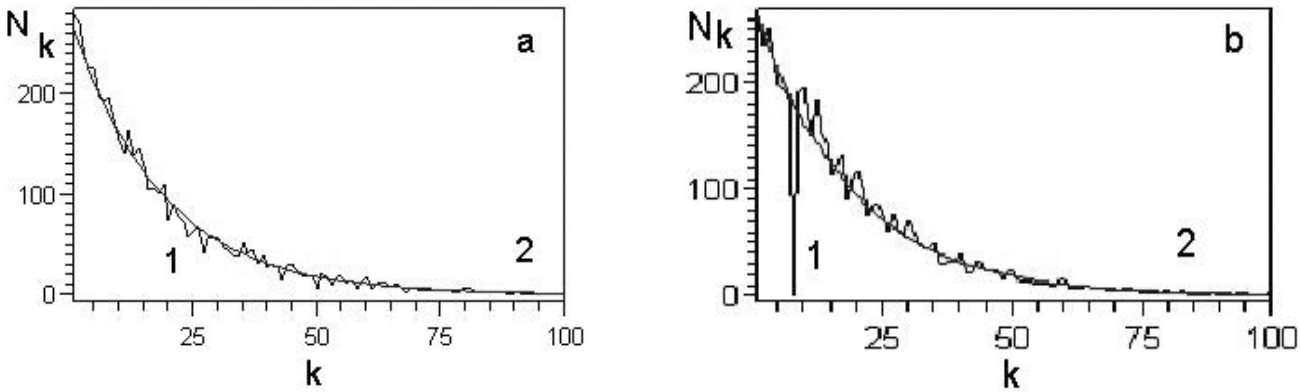


Рис. 7.1а,б. *Распределение по интервалам между появлениями идентичных кодовых групп при B = 1 для последовательности, формируемой алгоритмом типа Фибоначчи (с параметрами: M = 19, запаздывание Nz = 8; а – кривая 1 для кода 11; б – кривая 1 для кода 19; кривые 2 для идеальной случайной последовательности.*

при анализе статистики появления некоторой кодовой группы (для $B = 1$) в распределении имелся провал $N_K = 0$, где N_K – число совпадений. Этот интервал (K) равен параметру запаздывания, являющегося характеристикой анализируемого алгоритма для базы $B = 1$. Характерный вид распределений интервалов (K) для 2 разных кодовых групп (11 и 19) (параметры алгоритма M = 19, запаздывание Nz = 8) при $B = 1$, показаны на **Рис. 7.1***а,б.* Для всех других кодовых групп при данном B эта зависимость имеет идентичный вид с Рис. 7.1*а*.

Если вероятность появления кодовой группы длиной B для идеальной случайной последовательности $p = 1/M^B$, а T – число членов анализируемой последовательности, то среднее число появлений кодов T/M^B. Тогда ожидаемое число совпадений с кодовой группой длины B через интервал K в последовательности длины T равно:

$$N_K = (T / M^B) \cdot (1-p)^{K-1} p. \qquad (7.1)$$

На Рис. 7.1*а,б* эта зависимость $N_K = F(K)$ представлена для идеального случайного процесса (кривая 2). Она имеет характер близкий к экспоненте.

Для больших баз сигналов ($B > 1$) анализируемое распределение интервалов имеет более сложный вид: для интервала K, равного параметру запаздывания Nz алгоритма имеются кодовые группы для которых $N_K = 0$ и несколько кодов для которых N_K заметно превышает ожидаемый средний уровень, соответствующий модели идеального случайного процесса. Таким образом, предложенный метод анализа статистики распределения интервалов появления кодовых групп позволяет дешифровать структуру неизвестного формирующего алгоритма.

8. ЭФФЕКТИВНОСТЬ ЗАПОЛНЕНИЯ ФАЗОВОГО ПРОСТРАНСТВА КОДИРУЮЩЕГО ДИСКРЕТНОГО АЛГОРИТМА С ЗАПАЗДЫВАНИЕМ

Одним из перспективных способов формирования псевдослучайной последовательности целых чисел $\{x_n\}$ является алгоритм с запаздыванием, созданный на основе моделирования процессов в кольцевых автоколебательных системах с динамическим хаосом [13]. Дискретный вариант алгоритма определен на множестве M целых чисел натурального ряда из целочисленного отрезка $[M_1, M_2]$ ($M_2 > M_1$, $M = M_2 - M_1 + 1$). Наряду с M, основным параметром алгоритма является параметр запаздывания Nz, он определяет количество запаздывающих членов последовательности (x_{n-1}, x_{n-2}, x_{n-3}, …, x_{n-Nz}), которые необходимо знать на каждом шаге для определения нового члена x_n. Формула алгоритма дополнена операцией возврата числа x_n в интервал $[M_1, M_2]$ в случае, если принятое новое значение оказывается за его пределами.

Числа x_{n-1}, x_{n-2}, x_{n-3}, …, x_{n-Nz} являются обобщенными координатами в Nz-мерном фазовом пространстве данной динамической системы, и каждый их конкретный набор определяет радиус-вектор $R_n(x_{n-1}, x_{n-2}, \ldots, x_{n-Nz})$ и соответствующую точку состояния системы

в этом пространстве. Полное число различных векторов запаздывания и точек состояния системы в фазовом пространстве равно M^{Nz}. И каждое из этих состояний может быть принято системой хотя бы в качестве начальных условий.

При надлежащем выборе параметров алгоритма и начальных условий изменения вектора состояния, т.е. переходы из одной точки фазового пространства с координатами R_i в другую точку с координатами R_{i+1} носят псевдослучайный характер. Но только до тех пор пока вектор R_n принимает все новые и новые значения. При повторном попадании радиус-вектора в одну и ту же точку фазового пространства вследствие полной детерминированности алгоритма движение системы в фазовом пространстве в точности повторит себя, т.е. система выходит на замкнутую траекторию (цикл). Это соответствует возникновению периодичности в формируемой алгоритмом последовательности. Поскольку при заданных значениях M и Nz различных векторов в фазовом пространстве конечное число, то система рано или поздно обязательно оказывается на цикле. Задача состоит в нахождении наиболее длинной реализации N формируемой алгоритмом псевдослучайной последовательности, заполняющей весь фазовый объем M^{Nz}.

Исследование свойств алгоритмов, порождающих псевдослучайные последовательности с большим периодом, является актуальной задачей. Одним из важнейших параметров таких алгоритмов, характеризующих их качество, является степень заполнения и структура фазового пространства.

Рассмотрим дискретный алгоритм с запаздыванием типа Фибоначчи, формирующий псевдослучайную последовательность с хорошими статистическими свойствами:

$$X_n = X_{n-1} + X_{n-Nz},$$
$$X_n = X_n - M \ for \ X_n > M. \qquad (8.1)$$

Основным параметром алгоритма является параметр запаздывания Nz, определяющий число запоминаемых членов последовательности и размерность фазового пространства (ФП). Алгоритм определяется на конечном множестве целых чисел натурального ряда из замкнутого интервала [1, M]. Если вновь вычисленное число последовательности выходит за пределы этого интервала, то осуществляется линейное преобразование сдвига $\mathbf{x_n} \rightarrow \mathbf{x_n} \pm \mathbf{M}$, возвращающее это число в границы области определения. Это преобразование помимо функционального действия самого алгоритма типа Фибоначчи играет существенную роль в механизме хаотизации поведения исследуемой динамической системы [7].

Число точек состояний системы в фазовом пространстве алгоритма конечно и равно $\mathbf{M^{Nz}}$. Движение системы в ФП осуществляется путем перехода скачком из одного состояния в другое. Траектории движения системы занимают весь объем ФП, т.е. все возможные состояния. Каждая такая траектория движения системы происходит по своему замкнутому циклу, содержащему ограниченное число состояний системы. Структура ФП состоит из конечного набора циклов разного периода, поведение системы на которых носит псевдослучайный характер. Все циклы сложным образом располагаются во всем объеме ФП. Так, ФП алгоритма при Nz = 4 и M = 17 состоит из пяти циклов с периодами 73684, 3619, 2549, 2471, 529 и одной особой точки с координатами (17, 17, 17, 17). Выбор цикла определяется заданием набора начальных условий.

Псевдослучайный характер поведения системы на цикле на интервале, меньшем периода, подтверждается зависимостью изменения расстояний в ФП $\Delta R(n)$ между соседними точками на цикле, приведенной на **Рис. 8.1** для алгоритма с Nz = 3, M = 13. Это

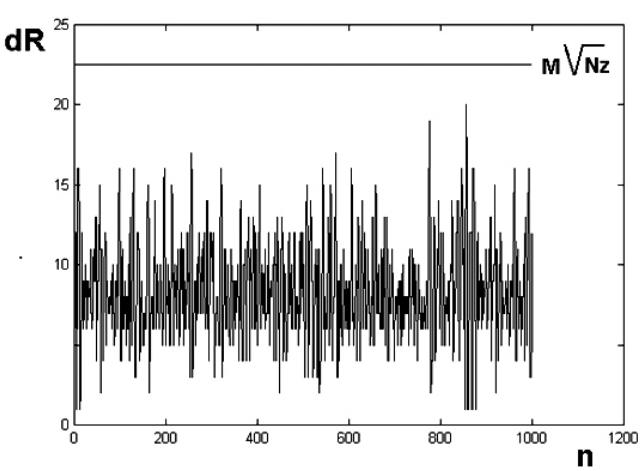


Рис. 8.1. *Расстояния в ФП между соседними точками на цикле, Nz = 3, M = 13.*

расстояние на каждом шаге алгоритма изменяется случайным образом, достигая значений, близких к наибольшим геометрическим размерам ФП.

Фазовое пространство исследуемого алгоритма при Nz > 2 состоит из одной особой точки с координатами (*M, M, …, M*) и семейства циклов разного или одного и того же периода. Каждая точка ФП принадлежит только одному конкретному циклу, при этом разные циклы не имеют ни одной общей точки.

Алгоритм выходит на тот или иной цикл в зависимости от выбора вектора начального состояния. До замыкания цикла вектор состояния описывает псевдослучайный процесс, которому соответствует непериодический сегмент формируемой алгоритмом псевдослучайной последовательности соответствующего размера.

В ансамбле фазовых пространств алгоритмов с различными параметрами *M* и Nz наблюдаются как "короткие" циклы, период которых *T* много меньше по сравнению с полным числом точек фазового пространства $\mathbf{M^{Nz}}$ ($T << \mathbf{M^{Nz}}$), так и "длинные" циклы, период которых сопоставим с последней величиной: $T \sim \mathbf{M^{Nz}}$. При четных *M* в ФП алгоритма преобладают короткие циклы, а при нечетных *M* коротких циклов вообще не существует, либо они представлены в небольшом количестве, занимая малый объем ФП, что и обеспечивает возможность существования длинного цикла. Таким образом при нечетных *M* наблюдаются наиболее длинные циклы. Период таких циклов при определенных значениях параметров алгоритма может приближаться к максимально возможной величине $\mathbf{T_{max} = M^{Nz}}$.

Численным экспериментом зафиксирован случай, когда ФП содержит только один длинный цикл и одну изолированную точку: $M = 2$, Nz = 15, $\mathbf{T/M^{Nz}} = 1.0$. Близкий результат получен при $M = 3$, Nz = 9, когда период длинного цикла $\mathbf{T/M^{Nz}} = 0.999$, а помимо него и одной изолированной точки в ФП системы существует только один пятитактный короткий цикл. Все это подтверждает, что оценкой максимального непериодического сегмента формируемой алгоритмом последовательности может служить величина $\mathbf{T_{max} = M^{Nz}}$. Следует иметь в виду, что этот максимальный период $\mathbf{T_{max}}$ может быть реализован лишь при определенных соотношениях параметров M и Nz.

Показано, что длинным циклам соответствуют распределения генерируемых чисел, близкие к равномерному. Характер изменения функций распределения генерируемых чисел при увеличении параметра Nz (для M = 255) показан на **Рис. 8.2.** Здесь: $\Delta\mathbf{p_{ср}}$, $\Delta\mathbf{p_{макс}}$, $\boldsymbol{\sigma}$ – среднее (1), максимальное (2) относительные по модулю и среднеквадратичное (3) отклонения распределений от равномерного (n = 210 000). Видно, что алгоритм формирует последовательность с практически равномерным распределением при Nz > 5. В этом случае близки к равномерному распределению и все условные вероятности $\mathbf{p(x_i|x_j)}$. Это означает, что формируемая данным алгоритмом псевдослучайная последовательность по своим вероятностным свойствам мало отличается от последовательности независимых равновероятных чисел из интервала [1, M].

При больших значениях M и Nz исследование структуры фазового пространства системы прямым перебором ее элементов весьма затруднительно. Поэтому изучение фазового портрета системы проводилось при небольших значениях "объема" фазового пространства не более $10^6 \div 10^7$. При этом, не ограничивая общность получаемых результатов, при численном анализе будем полагать, как правило, что $M_1 = 1$, $M_2 = M$.

Результаты численного изучения структуры фазового пространства при различных значениях M и Nz (M = 2÷21, Nz = 2÷18, $M^{Nz} \leq 10^7$)

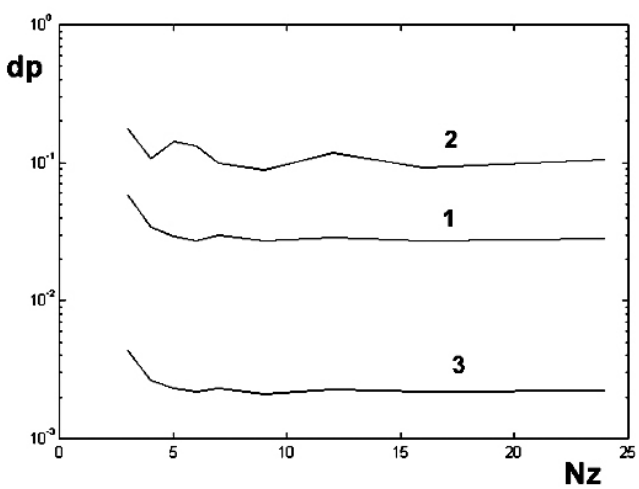


Рис. 8.2. *Отличие распределения от равномерного в зависимости от Nz (M = 255). 1 – $\Delta p_{ср}$, 2 – $\Delta p_{макс}$, 3 – σ.*

показали, что фазовое пространство алгоритма представляет собой набор конечных циклов, за исключением случаев Nz = 2 при нечетном M, когда помимо циклов в фазовом пространстве системы существуют точки, не принадлежащие ни одному циклу, а принадлежащие "бассейнам" этих циклов. Таким образом, если система находится в одной из подобных точек, то через некоторое определенное число шагов система выйдет на соответствующий цикл. При этом траектории движения системы в фазовом пространстве представляют собой отдельные замкнутые циклы, количество которых и величина их периодов зависят от параметров системы. В качестве примера можно привести спектры периодов (т.е. периоды циклов, существующих в фазовом пространстве, и их количество) для случая Nz = 4 (**Таблицы 4, 5**):

Из приведенных данных видно, что при увеличении $M = 2^k$ (k =1, 2, 3, 4), $M = 6^k$ (k = 1, 2, 3) и $M = 10^k$ (k = 1, 2) спектр циклов дополняется одним новым значением с большим периодом, причем в спектре всегда присутствуют циклы кратности 1, 15 и 30 (M > 2). При четных M > 2 и Nz = 3 в спектрах циклов всегда наблюдаются периоды 1, 7 и 14. При нечетных значениях M подобные простые закономерности в структуре спектра циклов не наблюдаются.

Полученные результаты позволяют сделать следующие выводы.

1. Траектории движения системы занимает весь объем фазового пространства, т.е. все возможные состояния, общее количество которых равно M^{Nz}.

2. Фазовое пространство алгоритма при Nz > 2 состоит из одной особой точки с координатами *R*(*M, M, …, M*) и семейства циклов разного или одного и того же периода. Каждая точка фазового пространства принадлежит только одному конкретному циклу, при этом разные циклы не имеют ни одной общей точки.

3. Система выходит на тот или иной цикл в зависимости от того, в какую точку фазового пространства попадает вектор начального состояния. До замыкания цикла вектор состояния описывает псевдослучайный процесс, т.е. циклам соответствуют сегменты псевдослучайной последовательности соответствующего размера.

4. В ансамбле фазовых пространств алгоритмов с различными параметрами M и Nz наблюдаются как "короткие" циклы, период которых *T* много меньше по сравнению с полным количеством точек фазового пространства M^{Nz} ($T << M^{Nz}$), так и "длинные" циклы, период которых сопоставим с последней величиной: T ~ MNz. При четных значениях M в фазовом пространстве алгоритма преобладают короткие циклы, а при нечетных M коротких циклов вообще не существует, либо они представлены в небольшом количестве, занимая малую область фазового пространства, что и обеспечивает возможность существования длинного цикла. Тем самым при нечетных *M* наблюдаются наиболее длинные циклы. Период таких циклов при определенных (заранее неизвестных) значениях параметров алгоритма может приближаться к максимально возможной величине $T_{max} = M^{Nz}$. На **Рис. 8.3** показаны результаты численного эксперимента по определению трех наибольших периодов циклов (кривые 1, 2, 3) для разных значений *M*

Таблица 4

M	Спектр периодов
2	1, 15
4	1, 15, 30 (8)
8	1, 15, 30 (8), 60 (64)
16	1, 15, 30(8), 60(64), 120(512)
6	1, 15(3), 30(3), 80, 90(12)
12	1, 15, 30(72), 80, 90(192), 240(5)
18	1, 15(6), 30(21), 80, 90(105), 240(27), 270(324)
10	1, 15(5), 30(10), 150(6), 312(2)
20	1, 15, 30(93), 150(918), 312(2), 1560(6)
14	1, 3(2), 15(7), 30(21), 210(168), 342(7)

Таблица 5

M	Спектр периодов
3	1, 7, 29, 44
5	1, 8, 27 (2), 562
7	1, 9, 22, 427, 653, 1289
9	1, 7, 10, 20, 22, 24, 29, 44, 75, 134, 296, 767, 5132
11	1, 21, 24, 41, 101, 173, 250, 14030
13	1, 626, 2992, 3712, 5056, 7977, 8197
15	1, 27, 44, 176, 562, 828, 1637, 4702, 7764, 11405, 11484, 11881
17	1, 529, 2471, 2549, 3619, 73684
19	1, 4182, 4219, 5067, 5408, 5916, 28778, 75061
21	1, 1289, 2833, 5228, 5401, 25900, 58208, 88633

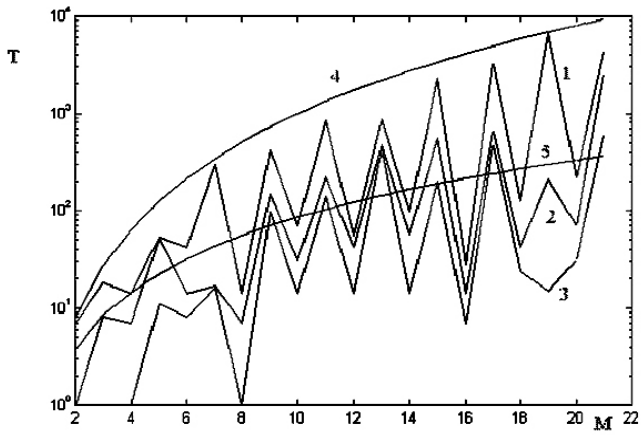


Рис. 8.3. *Периоды циклов (кривые 1, 2, 3) для разных значений M при одном и том же параметре запаздывания $N_z = 3$ в сопоставлении с полным числом точек фазового пространства – M^{N_z} (кривая 4) и оценкой максимального периода $T(M) = M^{0.645N_z}$ при $N_z = 3$ (кривая 5).*

при одном и том же параметре запаздывания Nz = 3 в сопоставлении с полным числом точек фазового пространства – M^{Nz} (кривая 4) и оценкой максимального периода $T(M) = M^{0.645Nz}$ при Nz = 3 (кривая 5).

5. При нечетном значении M все циклы имеют, как правило, разный период, т.е. представлены в единственном числе. При M-четном циклы одного периода встречаются многократно, хотя все они различны по принимаемым значениям вектора состояния.

6. При определенных значениях параметров алгоритма M и Nz период длинного цикла может быть очень близок к максимально возможной величине M^{Nz}: $T/M^{Nz} = 0.9 \div 1.0$. Более того, экспериментом зафиксирован случай, когда фазовое пространство содержит только один длинный цикл и одну изолированную точку: M = 2, Nz = 15, $T/M^{Nz} = 1.0$. Почти такой же результат можно получить при M = 3, Nz = 9: период длинного цикла $T/M^{Nz} = 0.999$, а помимо него и одной изолированной точки в фазовом пространстве системы наблюдается только один 5-ти тактный короткий цикл.

Все это свидетельствует в пользу того, что оценкой максимального периода формируемой алгоритмом последовательности может служить именно величина $T_{max} = M^{Nz}$. Следует иметь в виду, что этот максимальный период T_{max} может быть реализован лишь при определенных соотношениях параметров M и Nz. На Рис. 8.3 линию границы $T(M) = M^{0.645Nz}$ (Nz = 3) зачастую превышают не только самый длинный период, но и периоды еще двух меньших циклов, поэтому характеристику $T = M^{0.645Nz}$ следует рассматривать как усредненную величину для длинных циклов.

7. Длинным циклам соответствуют распределения генерируемых чисел, близкие к равномерному. Так для цикла с $T/M^{Nz} = 0.895$ (M = 13, Nz = 5) относительное среднее отличие по модулю от равномерного распределения равно 0.2% при относительном максимальном 0.45%, среднеквадратичное отклонение равно 0.07%. Именно такие длинные циклы могут быть использованы для формирования псевдослучайных последовательностей большой длительности с равномерным распределением вероятностей генерируемых чисел. На основе монотонности рассмотренных зависимостей, полученные результаты можно считать справедливыми при существенно больших объемах и размерностях фазового пространства.

9. ЗАКЛЮЧЕНИЕ

При соответствующем выборе параметров разработанные дискретные алгоритмы формируют длинные непериодические сегменты псевдослучайных последовательностей с равномерным распределением вероятностей, которые могут эффективно использоваться в криптографии, а также при кодировании информации в телекоммуникационных системах и компьютерных сетях [21].

ЛИТЕРАТУРА

1. Knuth DE. *The art of computer programming. Volume 2: Seminumerical Algorithms.* Third edition, Addison–Wesley, 2007, 832 p.
2. Петров АА. *Компьютерная безопасность. Криптографические методы защиты.* М., ДМК, 2000, 445 с.
3. Кузнецов СП. *Динамический хаос. Курс лекций.* М., Физматлит, 2001, 295 с.
4. Варакин ЛЕ. *Системы связи с шумоподобными сигналами.* М., Радио и связь, 1985.
5. Быков ВВ. *Цифровое моделирование в статистической радиотехнике.* М., Советское радио, 1971, 328 с.
6. Hayes Brian. The Vibonacci Numbers. American Scientist: Computing Science. July-August 1999.

7. Шустер Г. *Детерминированный хаос. Введение.* М., Мир, 1988, 240 с.
8. Булинский АВ, Ширяев АН. *Теория случайных процессов.* М., Физматлит, 2005.
9. Kemeny JG, Snell JL. *Finite Markov chains. The University Series in Undergraduate Mathematics.* Princeton, Van Nostrand, 1960.
10. Bharucha-Reid AT. *Elements of the Theory of Markov Processes and Their Applications.* New York, McGraw-Hill, 1960.
11. Рытов СМ. *Введение в статистическую радиофизику.* М., Наука, 1966.
12. Гантмахер ФР. *Теория матриц.* М., Наука. 1966.
13. Беляев РВ, Воронцов ГМ, Колесов ВВ. Случайные последовательности, формируемые нелинейным алгоритмом с запаздыванием. *Радиотехника и электроника,* 2000, 45(12):954-960.
14. Потапов АА. *Фракталы в радиофизике и радиолокации.* М., Логос, 2002.
15. Малинецкий ГГ. *Хаос. Структуры. Компьютерный эксперимент. Введение в нелинейную динамику.* М., Эдиториел УРСС, 2002.
16. Ruell D, Takens D. *Comm. Math. Phys.*, 1971, 20(3):167.
17. Вентцель ЕС. *Теория случайных процессов и ее инженерные приложения.* М., Высш. школа, 2007, 479 с.
18. Kahaner D, Moler C, Nesh S. *Numerical Methods and Software.* Prentice-Hall, Inc. A Divisioon of Simon & Shuster Englewood Cliffs. NJ, 1989.
19. Быков ВВ. *Цифровое моделирование в статистической радиотехнике.* М., Советское радио, 1971, 328 с.
20. Голенко ДИ. *Моделирование и статистический анализ псевдослучайных чисел на электронных вычислительных машинах.* М., Наука, 1965, 227 с.
21. Петров АА. *Компьютерная безопасность. Криптографические методы защиты.* М., ДМК, 2000, 445 с.

Грачев Владимир Иванович
научный сотрудник
ИРЭ им. В.А. Котельникова РАН
11/7, ул Моховая, Москва 125009, Россия
E-mail: grachev@cplire.ru

Рябенков Виктор Иванович
к.т.н., с.н.с.
ИРЭ им. В.А. Котельникова РАН
11/7, ул Моховая, Москва 125009, Россия
E-mail: ryabenkov.vi@list.ru

Сургай Анастасия Викторовна
аспирант
ИРЭ им. В.А. Котельникова РАН
11/7, ул Моховая, Москва 125009, Россия
E-mail: ya.a1997@yandex.ru

Колесов Владимир Владимирович
к.ф.-м.н., с.н.с.
ИРЭ им. В.А. Котельникова РАН
11/7, ул Моховая, Москва 125009, Россия
E-mail: kvv@cplire.ru.