ЗАО АВТЭКС Санкт-Петербург тел/факс: 567-72-02 info@autex.spb.ru

ОЦЕНКА СТРУКТУРНОЙ СЛОЖНОСТИ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ЦЕЛЫХ ЧИСЕЛ

Колесов В.В.

Институт радиотехники и электроники РАН
125009, Москва, центр, ГСП-9, ул. Моховая, д.11, корп. 7

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 разработка критериев объективной оценки их структурной сложности является достаточно актуальной задачей.

В качестве тестируемого алгоритма рассмотрим алгоритм с запаздыванием, формирующий псевдослучайную последовательность (ПСП) целых чисел $\{x_n\}$, определенный на конечном замкнутом интервале [1, M], M>1 с «отражающими границами»:

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

Здесь Nz - параметр запаздывания, а параметр Kz≠Nz выбирается из интервала запаздывания (x_{n-1}, x_{n-2},… x_{n-Nz}). В (1) основным является отображение типа Фибоначчи [1]:

$$x_n = x_{n-1} \pm x_{n-Nz} \qquad (2)$$

только теперь, в отличие от работы [1], знак перед запаздывающим членом изменяется не случайным независимым образом, а определяется внутренней динамикой системы.

Поскольку фазовое пространство (ФП) отображения Фибоначчи не ограничено, в алгоритм введена дополнительная операция преобразования числового интервала [1, M] самого в себя, которая играет важную роль в механизме хаотического поведения данной динамической системы (ДС). Во-первых, эта операция ограничивает объем ФП, делая его конечным, а, во-вторых, обеспечивает дополнительное перемешивание траекторий в фазовом пространстве. Необходимо отметить, что одного преобразования числового интервала самого в себя недостаточно для эффективного перемешивания траекторий в ФП. Определенный механизм хаотизации должен уже содержаться в функции отображения. В данном случае это обеспечивается свойствами генератора случайных чисел Фибоначчи. Эти два условия– ограниченность объема ФП и наличие мощного механизма перемешивания– являются необходимыми условиями хаотического поведения любой динамической системы.

Фазовое пространство алгоритма (1) размерности Nz имеет ограниченный объем и состоит из M^{Nz} точек состояния данной дискретной динамической системы (ДДС). В зависимости от выбора начального вектора $R_0(x_{-1}, x_{-2}, \ldots x_{-Nz})$, радиус-вектор $R_n(x_{-n-1}, x_{-n-2}, \ldots x_{-n-Nz})$ описывает в ФП ту или иную траекторию, представляющую собой последовательные дискретные переходы из одной точки состояния динамической системы в другую по случайному закону. Эти «траектории» движения ДДС в ФП из-за ограниченности объема ФП образуют замкнутые циклы, которые, вследствие однозначности преобразования (1), не пересекаются и не имеют общих точек. Все точки ФП принадлежат только одному какому-либо циклу.

В зависимости от значений параметров Nz≥3 и M в фазовом пространстве алгоритма существует только одна изолированная точка с координатами (M,M,… M) и целый ряд циклов различного периода, из которых каждому длинному циклу до его замыкания соответствует непериодическая ПСП с практически равномерным распределением генерируемых чисел. И нас будут интересовать процессы только до замыкания циклов, т.е. непериодический сегмент формируемой алгоритмом ПСП. Этот сегмент может быть любой длины (сколь угодно большой) при соответствующем выборе параметров алгоритма и начальных условий.

Множество точек в ФП, объединенных в цикл, мы будем называть псевдослучайным циклом (ПСЦ), если формируемый алгоритмом непериодический процесс до замыкания цикла имеет случайный, хаотический характер, в отличие от регулярного цикла, которому до замыкания соответствует регулярный процесс. Очевидно, что псевдослучайному циклу соответствует нерегулярное движение в фазовом пространстве, а регулярному циклу– регулярное. Конечно, в том и другом случае поведение ДС на цикле полностью детерминировано.

ПСЦ представляет собой детерминированное хаотическое множество последовательных точек во всем объеме фазового пространства, в отличие от притягивающего множества– странного аттрактора непрерывной динамической системы, аналогом которого для дискретной ДС он, по сути дела, является,

Для характеристики фрактальных свойств хаотического множества точек на ПСЦ ограничимся анализом геометрической (эвклидовой) и корреляционной размерностей [2, 3]. Численный эксперимент проводился для малых значениях параметров алгоритма Nz=4, Kz=2, M=11, длине исследуемой ПСП N=500 чисел, начальном векторе $R_0(8,6,7,1)$, что имеет принципиальное значение для оценки мажоритарных свойств ПСЦ. При увеличении размерности алгоритма характер поведения ДДС существенно усложняется и улучшаются статистические характеристики формируемых ПСП. Вычисление корреляционного интеграла $C(l)$ путем определения расстояний l между всеми парами векторов состояний на цикле в ФП и построение зависимости $\log(C(l))=f(\log(l))$, показанной на Рис.1 (кривая 1), позволяют с помощью вычисления локального углового коэффициента [3] дать следующую оценку корреляционной размерности исследуемого ПСЦ: $D_2=3.3$. Полученное значение согласуется с геометрической размерностью $D_0=4$, $D_2/D_0=0.83$. Величина последнего отношения может служить характеристикой степени однородности заполнения точками цикла полного объема ФП. Как показывает 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.

Кривая 2 на Рис.1 соответствует логарифму корреляционного интеграла для ПСЦ с $R_0(1,6,6,7)$ тестируемого алгоритма №2 на основе отображения Фибоначчи $x_n=x_{n-1}+x_{n-Nz}$, дополненного тем же, что и в (1), преобразованием отображения интервала [1, M] само в себя [4]. Nz=4, M=11, N=500. Графики 1 и 2 функции $\log(C(l)) = f(\log(l))$ на Рис.1 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 (1) и (2) соответствуют ПСП с хорошими статистическими и корреляционными свойствами, особенно при увеличении запаздывания Nz больше 5.

Алгоритм на основе отображения Фибоначчи с операцией отражения от границ интервала [1, M] типа «отражения от стенки бильярдного шара»:

$$\begin{aligned} \tilde{x}_n &= x_{n-1} + x_{n-Nz}, \quad x_n \in [1,\ M] \\ x_n &= \tilde{x}_n, \quad \text{если} \quad \tilde{x}_n \in [1,\ M] \\ x_n &= 2M - \tilde{x}_n, \quad \text{если} \quad M < \tilde{x}_n < 2M \\ x_n &= \tilde{x}_n + 2, \quad \text{если} \quad \tilde{x}_n = 2M \end{aligned} \qquad (3)$$

имеет неравномерное распределение с уменьшением вероятности генерации малых чисел из интервала области определения. При Nz=4, M=17, N=500, для цикла с начальным радиус-вектором $R_0(7,14,6,15)$ и имеющим период T=613 зависимость $\log(C(l))=f(\log(l))$ (кривая 3 на рис.1) не имеет четко выраженного прямолинейного участка. Это означает, что у корреляционного интеграла существенные отклонения от закона $C(l)\sim l^{-D}$ и, следовательно, точки данного ПСЦ расположены в ФП неравномерно.

Для оценки степени сложности хаотического процесса, формируемого алгоритмом, необходимо определить однородность аттрактора в ФП на всех масштабах дискретного времени. Определение корреляционной размерности аттракторов требует большого объема вычислительных ресурсов особенно в случае ДС высокой размерности, поэтому имеет смысл исследовать структурные свойства реализации псевдослучайного процесса, являющегося проекцией траектории движения ДС в ФП на одно из направлений в этом пространстве,

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 ($D_0=1$) хаотическому массиву из N=1000 чисел ПСП, сформированному алгоритмами (1)÷(4) при параметрах Nz=16, M=21 дало следующие результаты. Для всех тестируемых алгоритмов значение корреляционной размерности находится в пределах $D_2=D_2/D_0=0.91\div0.96$, в том числе для генератора RND(Maple) (алгоритм №5, M=21) и алгоритма №4, отличающегося от (1) тем, что для него параметр Kz=Nz , что существенно сказывается на форме распределения условной вероятности первого порядка $p(i+1,\ x_m \mid i,\ x_n)$, в котором появляются запретные переходы для четных, либо нечетных чисел в зависимости от четности числа на предыдущем шаге.

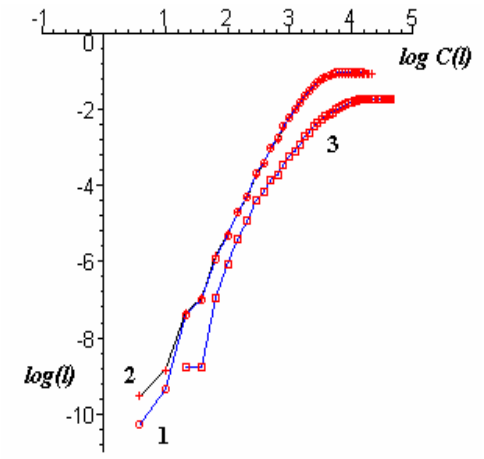

Рис.1.

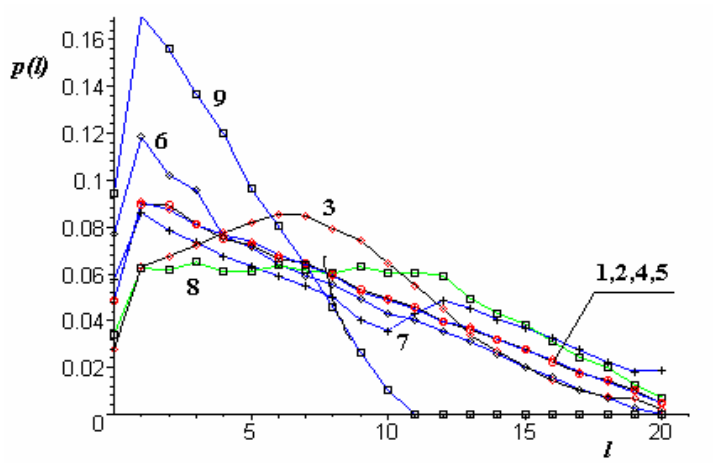

Рис.2.

Полученные значения отношения D_2/D_0 свидетельствует о достаточно хорошей однородности заполнения интервала [1, M] генерируемыми числами. Это подтверждается анализом одномерного распределения вероятностей чисел в последовательности. Но на основе этих данных ничего нельзя сказать о структурной сложности ПСП и, главное, насколько она близка к последовательности независимых случайных событий, что можно рассматривать как эталон хаотического поведения. С этой целью исследуем локальную структуру ПСП на основе анализа фрактальной геометрии [5].

Случайную последовательность целых чисел можно рассматривать как дискретную топологию сложного геометрического рельефа («береговой линии»). Для оценки геометрической структурной сложности исследуем изменения расстояния последовательно между соседними точками такого рельефа в окне заданного масштаба. Другими словами, на основе данных реализации ПСП длиной N перейдем к анализу алгебраической последовательности

$$\{y_n=|x_n-x_{n+1}|\},\ n=1,2\ldots (N-1),\ y_n\in[0,(M-1)]. \qquad (4)$$

Следуя методике вычисления корреляционного интеграла, подсчитаем число $N(l)$ наступления одинаковых событий $y_n=l$, l=0, 1, 2,… (M–1) в последовательности из (N–1) членов и построим график частоты наступления таких событий $p(l)=N(l)/(N-1)$ в зависимости от l (Рис.2). Расчеты выполнены для ПСП длиной N=50000. Кривая 1 соответствует алгоритму (1) с параметрами Nz=16, Kz=9, M=21. Этот график почти в точности повторяет соответствующую теоретическую зависимость для последовательности статистически независимых равновероятных чисел– $p_Э(l)$, которую мы принимаем за эталонную. В качестве последней можно использовать и экспериментально полученные значения $p(l)$ для ПСП в случае близости их к теоретическим, например, для ПСП, формируемой генератором RND или алгоритмом (1). Обратную величину $S=1/(s+1)$ суммарного модуля отклонений значений $p_i=p(l_i)$, полученных для анализируемого процесса, от эталонных $s=\Sigma|p_i-p_{Эi}|$ можно принять за меру структурной сложности этого процесса $\{x_n\}$. Кривые 2, 4 и 5, полученные при анализе алгоритмов (2), (4) с той же большой размерностью ФП (Nz=16, M=21) и генератора RND(Maple) с M=21, также мало отличаются от эталонного графика. Кривая 3 соответствует алгоритму (3) с неравномерным распределением генерируемых чисел $p(x)$. Графики 6, 7, 8 и 9 построены для модифицированных ПСП алгоритма (1) с целью моделирования дискретных процессов с разным видом функции распределения чисел $p(x)$ (среднее значение $x_{ср}$, среднеквадратичное отклонение σ, коэффициенты асимметрии γ_1 и эксцесса γ_2) и интервала автокорреляции $\tau_{кор}$. Кривые 3, 6, 7, 8 и 9 заметно отличаются от эталонной, что свидетельствует о высокой информативности предложенного метода оценки структурной сложности алгоритмов путем построения графика относительной частоты наблюдения величины разности соседних чисел в реализации ПСП $p(l)=f(l)$. Данный метод не требует больших объемов вычислительных ресурсов по сравнению с методами статистического, корреляционного и фрактального анализа. В Таблицу сведены результаты численного эксперимента.

Из приведенных данных видно, что все три алгоритма (1), (2) и (4) на основе отображения Фибоначчи, так же как и генератор 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.

Таблица

Номер графика на Рис.1	Алгоритм	p(x) тестируемой ПСП				$\tau_{кор}$	Отличие p(l)=f (l) от эталона	
		$x_{ср}$	σ	γ_1	γ_2		s	**S**
1	(1)	10.9	6.07	$1.08 \cdot 10^{-2}$	-1.21	1	$4.50 \cdot 10^{-2}$	0.96
2	(2)	11.0	6.07	$1.85 \cdot 10^{-2}$	-1.25	1	$4.80 \cdot 10^{-2}$	0.96
3	(3)	8.29	5.04	-1.21	-0.40	1	0.22	0.82
4	(4)	11.0	6.05	$-1.97 \cdot 10^{-3}$	-1.20	1	$4.70 \cdot 10^{-2}$	0.96
5	RND	11.0	6.06	$1.0 \cdot 10^{-3}$	-1.20	1	$4.40 \cdot 10^{-2}$	0.96
6	(1) модиф.	11.0	5.55	$8.79 \cdot 10^{-2}$	-1.21	2	$1.85 \cdot 10^{-1}$	0.85
7	(1) модиф.	11.0	6.81	$-1.02 \cdot 10^{-2}$	-1.43	1	$2.12 \cdot 10^{-1}$	0.83
8	(1) модиф.	7.32	5.85	0.86	-0.43	–	$1.46 \cdot 10^{-2}$	0.87
9	(1) модиф.	11.1	5.26	$-2.14 \cdot 10^{-2}$	-0.88	10	0.63	0.62

Параметры алгоритмов Nz=16, M=21, длина реализаций N=50000.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проекты № 03-07-90133, № 04-07-90161, № 04-07-08013.

Литература

1. Hayes Brian. The Vibonacci Numbers. //American Scientist: Computing Science: July-August 1999.
2. Кузнецов С.П. Динамический хаос. – М.: Издат-во физ.-мат. литературы, 2001.
3. Мун Ф. Хаотические колебания. – М.: Мир, 1990.
4. Беляев Р.В. и др. // Радиотехника и электроника, 2004, т.49, №3, с.325-332.
5. Потапов А.А. Фракталы в радиофизике и радиолокации. - М.: Логос, 2002.