СТРУКТУРНЫЕ СВОЙСТВА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ФОРМРУЕМЫХ ДИСКРЕТНЫМ АЛГОРИТМОМ С ЗАПАЗДЫВАНИЕМ

Рябенков В.И., Колесов В.В., Беляев Р.В., Попов А.М.

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

Последовательности случайных чисел широко используются в научных и прикладных применениях. Это прежде всего методы статистического моделирования (методы Монте-Карло) и обширные области технических применений: телекоммуникация, криптография и цифровая техника [1, 2]. В последнее время развиваются новые применения случайных последовательностей как широкополосных шумовых сигналов, например, сверхширокополосная шумовая радиолокация.

Применение таких последовательности требует разработки способов их формирования, то есть создания специальных генераторов. Особое место в связи с расширением использования цифровой техники занимают методы формирования целочисленных последовательностей, определенных на ограниченном интервале множества целых числе. Одним из основных направлений цифровой техники является использование бинарных последовательностей, что обеспечивает значительные удобства с точки зрения унификации методов обработки потоков данных в различных технических устройствах, а также позволяет эффективно решать проблемы помехозащищенности, электромагнитной совместимости и ряд других специфических проблем в телекоммуникационных системах.

Будучи заданными на ограниченном множестве целых чисел алгоритмы в процессе формирования числовых последовательностей неизбежно выходят на период, являющийся аналогом предельного цикла динамических систем, определенных на непрерывном числовом множестве. Поэтому формируемые ими последовательности, обладающие статистическими свойствами последовательностей истинно случайных чисел, на интервале до достижения периода принято называть псевдослучайными последовательностями (ПСП).

В настоящее время разработаны обширные классы алгоритмических генераторов таких ПСП и тем не менее разработка и создание новых алгоритмов продолжается в связи с особенностями и разнообразием требований к их применению в различных технических областях. Одновременно постоянно развиваются и методы анализа, позволяющие определять и сопоставлять статистические свойства ПСП.

Известно множество методов анализа статистических характеристик ПСП. И тем не менее продолжается поиск новых подходов к такому анализу. В докладе с целью получения некоторой количественной характеристики структурных свойств выполнен анализ нескольких бинарных ПСП, формируемых различными алгоритмами.

При этом подходе учитывалось, что в технических применениях информационное содержание передается с использованием некоторых числовых блоков, каждый из которых тем или иным методом кодирует информацию. В современных системах телекоммуникации такой блок символов (последовательность нулей и единиц) принято называть базой (В). Таким образом информационный поток представляет собой последовательность блоков из таких бинарных импульсов. При заданном размере базы полное число различных вариантов бинарных блоков (полный код) составляет 2^B .

При анализе структурных свойств ПСП использовалась следующая процедура. Последовательно задавалось значение базы В и определялся соответствующий ей набор блоков, составляющих полный код. Каждый блок имел длину, равную базе. Также фиксировалась длина реализации ПСП (N_0), полученной с использованием того или иного алгоритма генерации. Поочередно для всех блоков полного кода с номерами j от j=1 до j=2^B определялось сколько раз такой блок встречается в анализируемой ПСП. При этом на каждом следующем шаге такого сопоставления новый анализируемый блок, также имевший длину равную базе В, формировался путем смещения на один символ в последовательности символов исследуемой ПСП. Таким образом при длине реализации ПСП - N_0 и заданном размере базы В для каждого блока из полного кода с номером j производилось сопоставление с выделяемыми из реализации блоками начиная с номера i=1 до i= N_0-B+1. Здесь N_0-B+1 это число блоков длиной В, которое можно выделить из анализируемой последовательности, сдвигаясь каждый раз на один символ от начала ПСП к ее концу. Определялось сколько раз (n_j) j-блок встречается в анализируемой реализации ПСП. Далее аналогичное сопоставление производилось для следующего блока из полного кода с номером j+1 и т.д. Далее размер базы увеличивался на единицу. При этом возрастала длина блока Соответственно изменялось число блоков полного кода. Затем выполнялась аналогичная процедура сопоставления блоков из полного кода и из реализации ПСП.

В результате определялось распределение повторяемости всех возможных вариантов блоков в анализируемой реализации ПСП.

Следует указать, что конечно совершенно не обязательно, что в конкретной реализации ПСП будут представлены все блоки полного кода , соответствующего данной базе. Это особенно может проявиться в случае большой базы, когда соответствующее число блоков полного кода велико.

С точки зрения статистики такая процедура имеет смысл лишь до тех пор пока в анализируемой реализации ПСП длины N_0 для данной базы можно выделить достаточное число блоков полного кода. Для базы B число различных блоков полного кода $2^{B.}$. Число блоков, выделяемых из ПСП при данной базе B, равно (N_0-B+1). Тогда среднее число выделяемых из ПСП блоков, приходящееся на один блок полного кода $n_0 = (N_0 - B+1)/ 2^B$, должно по крайней мере удовлетворять соотношению $n_0>100$. Так для базы B=10 и длины реализации N_0 должно выполняться соотношение $N_0>102400$, а для B=16 должно быть $N_0 > 6553600$. Эти оценки указывают на трудность такого анализа для алгоритмов с длинными корреляционными связями.

Для получения хорошей оценки свойств структуры реализации, формируемой тем или иным алгоритмом, длина базы должна быть больше, чем время корреляции процессов в реализации ПСП. Другими словами на больших временах должно происходить забывание и реализация ПСП должна быть ближе к истинно случайному процессу с независимыми выборками. Это соображение следует учитывать при проведении оценок с использованием описанной методики.

Естественно считать, что для идеального случайного процесса с независимыми выборками из реализации блоков, имеющих одинаковые равные длины B, такие блоки должны встречаться в реализации одинаково часто с вероятностью $P \sim 1/2^B$ [3].

Однако, если процесс формирования последовательности не является случайным, а включает некоторые операции, связанные с памятью о прошлом, другими словами если последовательные выборки нельзя считать полностью независящими от предыдущих шагов вычисления, то это должно каким-то образом проявиться в структуре последовательности, а значит и в распределении плотности по полным кодам для данной базы. Так в алгоритмах с запаздыванием (к которым, например, относятся алгоритмы типа Фибоначчи) таким временем может быть время запаздывания. Наличие такой памяти должно проявиться в появлении неравномерности в функции распределения. Естественно, что сопоставление структурных свойств ПСП , формируемых разными алгоритмами можно проводить только при одинаковой базе для выбираемых кодов.

Для выполнения описанной процедуры исследования структуры были использованы ПСП, формируемые несколькими алгоритмами. В качестве одного из таких алгоритмов использовался алгоритм типа Фибоначчи

$$X_{N+1}=X_N +X_{N-Nz} ,$$

с множеством целых чисел из интервала определения [1, M], M=256 . Запаздывающий член X_{N-Nz} определяется значением Nz=16. Алгоритм дополняется условием, что при выходе нового члена последовательности X_{N+1} за пределы указанного интервала определения производится операция сдвига, переводящая его значение в указанный интервал по правилу:

$$\text{если } X_{N+1} > M, \text{ то } X_{N+1} = X_{N+1} - M$$

Приведенные условия возврата играют определяющую роль в механизме перемешивания, которое в сочетании с запаздыванием обеспечивает хаотизацию генерируемой последовательности с длинным циклом при правильно выбранных начальных условиях.

Другим использованным алгоритмом являлся алгоритм генерации последовательности случайных чисел RND из программного пакета Maple 7 [4]. Для обоих алгоритмов. определенных на множествах из интервалов [1, M], для перевода в бинарную последовательность применялась операция клипирования по уровню M/2.

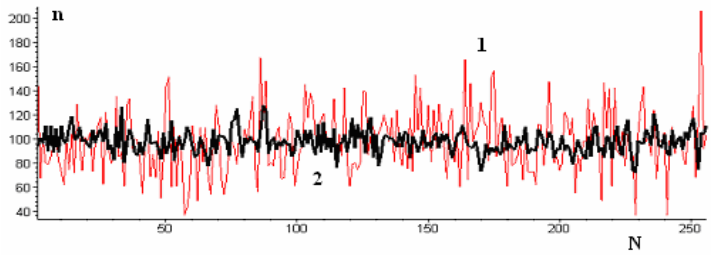

Рис.1 Распределение числа блоков в реализациях ПСП, формируемых алгоритмами типа Фибоначчи (1) и Maple 7 (2), в зависимости от номера блока полного кода для базы B=8.

На рис.1, для примера, показано распределение числа блоков в реализациях ПСП, формируемых алгоритмами типа Фибоначчи (1) и Maple 7 (2), в зависимости от номера блока полного кода для базы B=8. Длина реализации для кривой (1) специально была выбрана равной нескольким периодам, чтобы подчеркнуть отличие в распределениях.

Для характеристики структуры ПСП, анализируемой по приведенной методике, представляет-ся удобным использовать выборочную дисперсию, вычисляемую как среднеквадратичное отклонение распределения плотностей по блокам полного кода с базой B от ожидаемого среднего значения для идеальной случайной последовательности с независимыми последовательными выборками:

$$\sigma^2 = \sum_{j=1}^{2^B} (n_0 - n_j)^2 \Big/ 2^B ,$$

Типичная зависимость σ^2 от базы для трех различных ПСП показана на рис.2

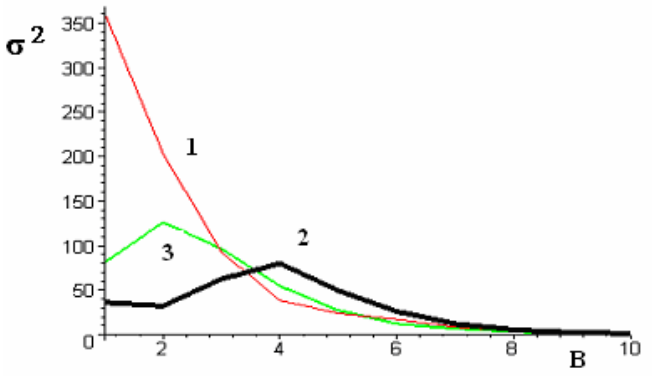

Рис.2 Зависимость дисперсии от базы для ПСП алгоритма Фибоначчи-1, алгоритма Maple7-2 и М-последовательности длиной 8191 со степенью соответствующего многочлена m=13 -3.

Для характеристики структуры ПСП можно ввести коэффициент структурной сложности K_{cc} , которому для нормировки и устранения бесконечности для идеального случайного процесса для которого в пределе при $N_0 \to \infty$ дисперсия $\sigma \to 0$ удобно придать такую форму:

$$K_{CC} = 1/\left(1+\sigma^2\right),$$

Здесь дисперсия определяется при использовании изложенной процедуры.

В таблице 1 представлены распределения средних дисперсии и K_{cc} по 5 выбранным случайным образом последовательностям для алгоритмов RND Maple7, Фибоначчи и М-последовательности в зависимости от базы B для последовательностей длиной 6400 .

Коэффициент K_{cc} при любой длине базы для М-последовательности существенно превышает аналогичные величины для других алгоритмов, причем для RND он больше , чем для алгоритма Фибоначчи. Это обусловлено тем, что длина 6400 существенно превышает период для алгоритма Фибоначчи, составляющий 1920.

Таблица 1

База B		2	4	6	8	10
Алгоритм RND Maple7	σ^2	1225,10	240,78	114,32	28,54	6,54
	K_{cc}	$8{,}9\ 10^{-4}$	$4{,}2\ 10^{-3}$	0,0087	0,034	0,13
Алгоритм Фибоначчи M=256, Nz=4	σ^2	2227,40	1240,23	1819,58	419,86	74,60
	K_{cc}	$4{,}8\ 10^{-4}$	$8{,}1\ 10^{-4}$	$5{,}5\ 10^{-4}$	0,0024	0,013
М-последовательность m=13	σ^2	139,60	58,73	18,49	4,68	1,31
	K_{cc}	0,011	0,018	0,052	0,176	0,433

Оценки показывают, что для последовательностей, состоящих из одних только «0» или «1», при изменении B от 3 до 8 коэффициент K_{cc} изменяется от $0{,}9\ 10^{-5}$ до $2{,}6\ 10^{-4}$. Аналогично для последовательности типа “меандр“ из чередующихся «0» и «1» при тех же значениях B от 3 до 8 коэффициент K_{cc} изменяется $1{,}6\ 10^{-5}$ до $2{,}6\ 10^{-4}$, а для последовательностей, сформированных RND Maple 7 и алгоритмов типа Фибоначчи $K_{cc} \approx 0{,}03 \ldots 0{,}15$, что существенно больше.

Представленные на рис.3. зависимости *Kcc* от базы показывают, что начиная с базы B=3 *Kcc* для рассматриваемой М-последовательности постоянно превышает *Kcc* других алгоритмов.

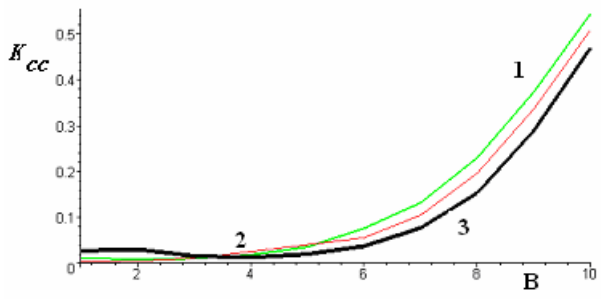

Рис. 3 Зависимость коэффициента *Kcc* от базы для ПСП М-последовательности-1, алгоритма Фибоначчи-2 и алгоритма Mapple 7-3.

Предложенный метод позволяет сопоставить для ПСП некоторой длины одно число (коэффициент структурной сложности), которое характеризует внутреннюю структуру ПСП и позволяет проводить сравнение с ПСП, формируемыми другими алгоритмами.

Описанная методика вычисления K_{cc} очевидно применима к инвертированной ПСП т.е. с заменой 0 на 1 и наоборот) и дает тот же результат, что представляется абсолютно справедливым.

Представляет интерес применение рассмотренной процедуры к ПСП с использованием других наборов блоков, например, циклические перестановки коротких М-последовательностей, искусственно созданные сложные сигналы .

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований проекты 03-07-90133, 04-07-90161 и 04-07-08013.

Литература

1. Скляр Б. Цифровая связь. Теоретические основы и практические применения. Пер. с англ.- М.: Изд. дом “Вильямс”, 2003. С.1099.
2. Аграновский А.В., Хади Р.А.. Практическая криптография. М.: Солон-Пресс. 2002. С.255
3. Беляев Р.В., Воронцов Г.М., Кислов В.В., Колесов В.В., Попов А.М., Рябенков В.И. Спектр периодов псевдослучайных последовательностей, формируемых дискретным алгоритмом с запаздыванием. Радиотехника и электроника 2004. Т.49. №3 . С.325-332.
4. В.Дьяконов. Maple 7: учебный курс. – СПб.: Питер, 2002 . -672 с.