СПЕКТР ПЕРИОДОВ ПСЕВДОСЛУЧАЙНЫХ СИГНАЛОВ, ФОРМИРУЕМЫХ ЛИНЕЙНЫМ ДИСКРЕТНЫМ АЛГОРИТМОМ С ЗАПАЗДЫВАНИЕМ

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

Институт радиотехники и электроники РАН,
101999, Москва К-9, ГСП-9, Моховая 11, корп.7, ИРЭ РАН

Исследовались спектры периодов псевдослучайных последовательностей, формируемых линейным алгоритмом с запаздыванием, заданным на ограниченном интервале целых чисел, Эти исследования направлены на разработку порождающих алгоритмов, обеспечивающих повышение эффективности использования фазового пространства (ФП) путем уменьшения компонент спектра с малым периодом, увеличение объема системы сигналов, формируемых на основе таких последовательностей, и выработку "рецептов" поиска выхода алгоритма на режим максимального цикла..

Рассмотрим алгоритм формирования псевдослучайной последовательности целых чисел $\{x_n\}$ на заданном интервале [1, M] с параметром запаздывания Nz:

$$x_к = x_{к-1} + x_{к-Nz} \ ,$$

общий вид которого описан в [1]. Параметр запаздывания определяет начальные условия (НУ)- Nz чисел, принадлежащих интервалу [1, M], необходимые для начала процесса формирования последовательности, причем эти числа можно считать обобщенными координатами некого вектора $R_n(x_1, x_2, \ldots, x_{Nz})$ в Nz-мерном фазовом пространстве, однозначно определяющего состояние системы. На каждом шаге генерации место последней координаты этого вектора занимает новая, вычисленная по указанному алгоритму, а первая координата соответственно опускается. При этом конец вектора R_n перескакивает в соответствующую точку фазового пространства, объем которого, определяющий число состояний системы, равен M^{Nz}. Следовательно, при генерации случайной последовательности, конец вектора R_n будет описывать в фазовом пространстве некую фазовую "траекторию" (ФТ), которая, в силу конечности числа точек фазового объема, должна быть замкнутой. С этого момента, вследствие детерминированости алгоритма, новая ФТ обязана в точности повторить предыдущую, т.е. процесс выходит на цикл с периодом $T_{M,Nz}$, который определяется длиной ФТ при заданных M, Nz и НУ. Конечно, совершенно не обязательно, что при произвольных НУ такая траектория замкнется после похождения всех возможных точек (состояний) системы. Очевидно, с точки зрения получения максимальной непериодической последовательности псевдослучайных чисел, ФТ должна иметь как можно большую длину, при этом конфигурация ее перескоков (фазовый портрет) должна иметь "хаотичность".

Вычислительные эксперименты, выполненные для различных M ($3 \le M \le 24$), Nz ($2 \le Nz \le 16$) и НУ, показали, что в фазовом пространстве существует, как правило, несколько ФТ: две для случая M=3, Nz=2 и, например, 16 траекторий при M=20, Nz=2, при этом пять из них имеют одинаковую длину, но различную пространственную конфигурацию. Заметим, что во всех слу-чаях одна траектория является вырожденной и представляет собой одну изолированную точку, все координаты которой равны M. Все ФТ при этом нигде не пересекаются и суммирование точек по всем фазовым траекториям всегда равно объему фазового пространства. Для рас-сматриваемого алгоритма установлено, что точка, все координаты которой равны 1, при любых M и Nz всегда лежит на фазовой траектории наибольшей длины. Это заключение было сделано в результате расчета величин периодов для всех возможных начальных условиях при данных M и Nz. Отметим, что точки, все координаты которых 1 или M, являются особенными во всем фазовом пространстве: они являются как бы “полюсами” фазового объема.

Если M является не простым числом, а имеет сомножители, то фазовые траектории “наследуют” конфигурации траекторий своих сомножителей, т.е. воспроизводят их в большем масштабе. В то же время наличие большого числа ФТ с малым периодом является крайне нежелательным, т.к. они уменьшают фазовый объем, остающийся на долю длинных ФТ.

При исследовании зависимости величины наибольшего периода цикла от M и Nz НУ всегда брались одинаковыми и равными 1. Определение периода осуществлялось таким образом, что генерация псевдослучайных чисел прекращалась, когда повторялся вектор НУ. Зависимость $T_{M,Nz}$ от M при любом Nz имеет весьма сложный характер. Типичный график этой зависимости показан на рис.1 для случая Nz=4, и изменений M в диапазоне от 5 до 500. В других случаях по M удалось продвинуться до существенно меньших значений. При Nz=8, например, максимальное значение M составило 32, причем при M=29 был получен наибольший период, равный 35731886640.

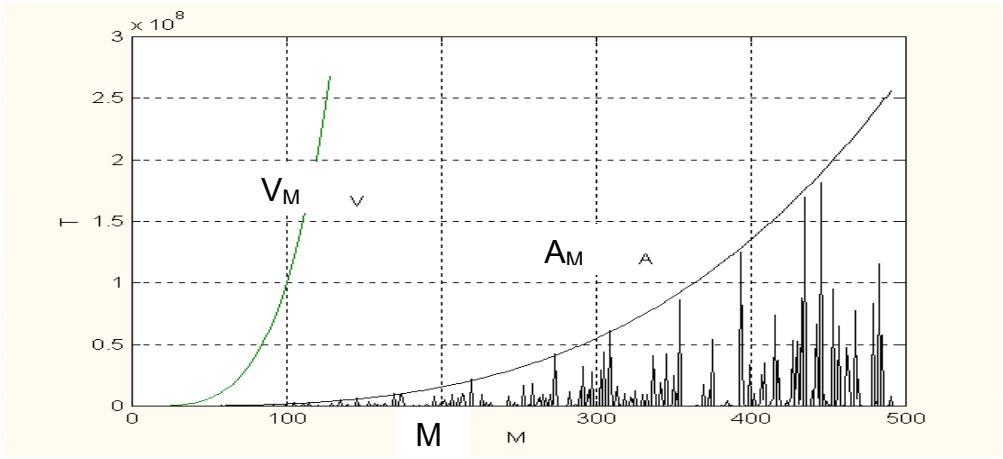

Рис.1

На рис.1 показано как ведет себя объем фазового пространства V_M, а также кривая аппроксимации наибольших периодов степенной зависимостью A_M. Как в этом, так и в других случаях указанная аппроксимация показала, что значения наибольших периодов при заданном Nz возрастают как $A_M = M^{(Nz-1)+\delta}$, где δ составляет, как правило, величину, равную 0,1÷0,25. Детальный анализ периодов показал, что с точки зрения получения последовательностей псевдослучайных чисел с максимальным периодом, четные значения M не представляют интереса, а из нечетных чисел наиболее эффективны простые числа.

Условие выхода на период можно записать в виде Nz уравнений

$$\begin{aligned} &f_n x_1+f_{n-1}x_2+\ldots+f_{n+1}x_{Nz}-\mu_1 M=x_1,\\ &f_{n+1}x_1+f_n x_2+\ldots+f_{n+2}x_{Nz}-\mu_2 M=x_2,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &f_{n+(Nz-1)}x_1+f_{n+(Nz-2)}x_2+\ldots+f_{n+Nz}x_{Nz}-\mu_{Nz}M=x_{Nz}, \end{aligned} \qquad (1)$$

где коэффициенты f_n при координатах x_n для случая Nz=2 являются классическими числами Фибоначчи (подобные алгоритмы генерации случайных чисел получили название генераторов Фибоначчи). При Nz>2 их можно назвать обобщенными числами Фибоначчи, т.к. вычисляются они с помощью следующего рекуррентного соотношения:

$$f_{n+N}=f_{n+(N-1)}+f_n. \qquad (2)$$

Члены $\mu_n M$ в (1) учитывают механизм возврата в область определения [1, M], μ_n при этом является целым числом. Используя для упрощения рекурентное соотношение (2) и пологая НУравными 1 можно определить период генерируемой последовательности $T_{M,Nz}$.

Необходимо заметить, что методика определения $T_{M,Nz}$ этим способом дает некоторый выигрыш во времени по сравнению с указанной выше и именно она использовалась при исследовании зависимости периода от размерности фазового пространства Nz.

Результаты определения зависимости $T_{M,Nz}$ от величины параметра запаздывания Nz представлены на рис.2. Расчеты выполнены для M=32, 64, 128 и 256, при этом величина Nz изменялась в пределах от 2 до 16, а НУ брались равными 1. Полученные зависимости демонстрируют рост периода $T_{M,Nz}$ при увеличении Nz, но при Nz=16 наблюдается явный провал. Ясно, что к выбору Nz надо подходить достаточно осторожно, помня при этом что зависимость периода от M куда более существенна (см. рис.1).

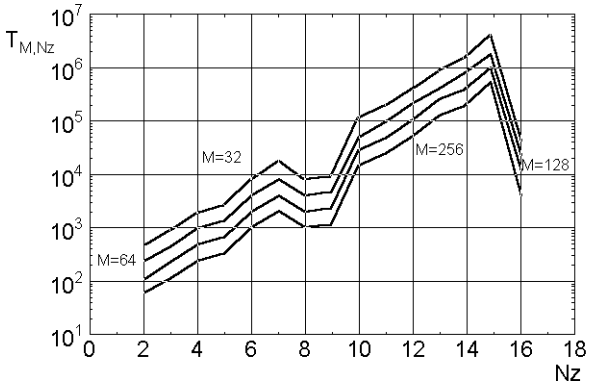

Рис.2

Оценка периода последовательности при вполне реальных значениях $M \approx 10^3$ и $Nz \approx 20$ дает величину $T \sim M^{(Nz-1)+\delta} \sim 10^{57}$, которая намного превосходит весьма осторожные оценки [2] ,если замеченная закономерность не нарушится.

Исследования проводились при финансовой поддержке Российского фонда фундаментальных исследований (проекты 00-07-90147 и 01-07-90349).

Литература

1. Каханер Д., Моулер К., Нэш С. Численные методы и программное обеспечение. –М.: Мир, 2001. С.575.
2. Беляев Р.В., Воронцов Г.М., Залогин Н.Н., Колесов В.В. Оценка длины непериодического сегмента псевдослучайной последовательности, формируемой дискретным алгоритмом с запаздыванием // Радиотехника и электроника.. 2002, т. 47, № 4, С. 477-481.

SPECTRUM'S PERIODS OF RANDOM SIGNALS FORMED BY LINEAR DISCRET ALGORITHM WITH DELAY

Ryabenkov W., Belyaev R., Vorontsov G., Kolesov V. Popov A.

The Institute of Radio-engineering and Electronics Russian Academy of Sciences, Moscow

There were investigated periods of pseudo-random sequences formed by linear algorithm with delay defined on bounded interval of integer numbers. The investigations have been directed on development of generic algorithms providing growing up the effectiveness of using the phase space by means of diminishing the spectrums components with a little periods, increasing volume of signals system forming on the basis of the such sequences and making "methods" to find modes with cycles of maximal periods.

It was considered the algorithm forming pseudo-random sequences of integer numbers $\{x_n\}$ specified on interval [1, M] with delay parameter Nz:

$$x_к = x_{к-1} + x_{к-Nz}$$

The general form of algorithms of this kind is shown in [1]. The delay parameter Nz specified starting conditions -Nz numbers out of interval [1,M]. The study was carried out for different values of M ($3<M<24$), Nz ($2<Nz<16$) and start conditions.

It was proposed a more economical method of calculation periods for this kind of algorithm
There have been given an evaluation of maximal period for specified values of M and Nz for investigated algorithm.

References

1. Kahaner D, Moler C., Nesh S. Numerical Methods and Software / Prentice-Hall, Inc.. A Divisioon of Simon & Shuster Englewood Cliffs. NJ. 1989.

2. Belyaev R.V., Vorontsov G.M., Zalogin N.N., Kolesov V.V. The Length of Nonperiodic Segments of Pseudorandom Sequence Formed by Discrete Algorithm with Delay // Journ. of Communication Technology and Electronics. 2002. V.47. N4. P.429-432.