ЭФФЕКТИВНОСТЬ ЗАПОЛНЕНИЯ ФАЗОВОГО ПРОСТРАНСТВА КОДИРУЮЩЕГО ДИСКРЕТНОГО АЛГОРИТМА С ЗАПАЗДЫВАНИЕМ

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

Институт радиотехники и электроники РАН, Москва

Для обеспечения эффективного кодирования цифровой информации требуются псевдослучайные последовательности со сколь угодно большим периодом. Синтез и исследование свойств алгоритмов, порождающих последовательности с такими свойствами, является целью настоящей работы.

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 [1]. 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}, 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}. В [2] приводится усредненная оценка периода цикла $N=M^{0.645Nz}$, полученная на основе численного эксперимента по поиску периода генерируемой алгоритмом последовательности при M=256 и небольших значениях параметра запаздывания Nz=2÷5. Но без тщательного изучения структуры фазового пространства нельзя получить однозначный ответ на вопрос, является ли данная оценка верхней границей размера непериодического сегмента генерируемой последовательности или же нет.

При больших значениях M и Nz исследование структуры фазового пространства системы прямым перебором его 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, $M^{Nz} \le 10^7$) 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. Т.о., если система находится в одной из подобных точек, то через некоторое определенное число шагов система выйдет на соответствующий цикл.

Таким образом, траектории движения системы в фазовом пространстве представляют собой отдельные замкнутые циклы, количество которых и величина их периодов зависят от параметров системы. В качестве примера приведем спектры периодов (т.е. периоды циклов, существующих в фазовом пространстве, и их количество) для случая Nz=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)

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

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: $T\sim M^{Nz}$. 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.1 показаны результаты численного эксперимента по определению трех наибольших периодов циклов (кривые 1, 2, 3) для разных значений M 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 $T(M)=M^{0.645\,Nz}$ при Nz=3 (кривая 5).

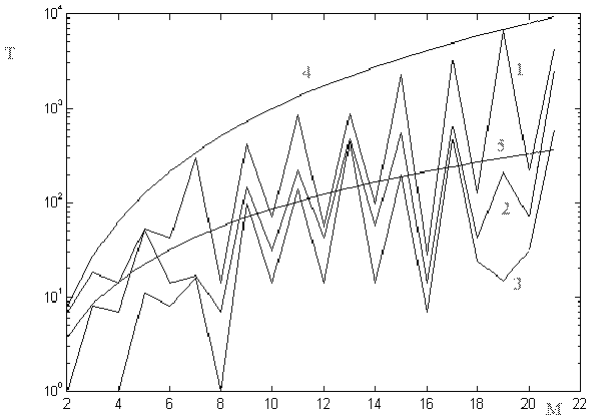

Рис.1

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÷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 мы имеем 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.1 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.

Работа выполнялась при финансовой поддержке РФФИ (проекты 00-07-90147 и 01-07-90349)

Литература

1. Беляев Р.В., Воронцов Г.М., Колесов В.В. Случайные последовательности, формируемые нелинейным алгоритмом с запаздыванием // Радиотехника и электроника. 2000. т. 45, № 8, С.954-960.

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 .

EFFICIENCY OF FILLING IN THE PHASE SPACE OF CODING DISCRET ALGORITH WITH DELAY

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

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

For providing the effective coding of digital information there are requirement of pseudo-random sequences with arbitrarily match period. Syntheses and investigation of an algorithms forming sequences with properties of such kind is an object of this report.

There was examined the phase space of algorithm with delay generating pseudo-random sequences of integer numbers $\{x_n\}$. This algorithm have been created on the basis of modeling processes in ring self-oscillating system with chaotic dynamics [1]. It was supposed that this algorithm have been defined on the manifold M of natural scale's integer numbers. The other one algorithm's parameter have been the value of delay Nz defining number of a sequences' terms

(x_{n-1}, x_{n-2}, x_{n-3}…x_{n-Nz}), which were necessary for calculating next term. of the sequence.

It was an object to find a generated by algorithm realization with the overall length N, filling up the most part of a volume of phase space M^{Nz}. Early with calculating experiment with value M=256 and delay Nz = 2÷5 there have been found an average evaluation of this one - $M^{0,645\ Nz}$ [2]. But without careful study phase space's structure it is impossible to get an single-valued answer on this question whether these one is the sufficient estimator of upper bound for an investigated sequences. When the values of M and Nz are too big such an investigation becomes too difficult. For this reason the investigation of phase space have been realized in conditions of not too much phase space's values such as $10^6 \div 10^7$.

The investigations have revealed that trajectories of a system's state in phase space constitute separated closed cycles with different periods. For examined cases there have been made the tables of the period's spectrums with deferent shown values of the system's parameters. These tables are included an information about spectrum periods and also their numbers in the phase space.

In addition the sequences with a big periods have been investigated on their non-periodic segments in accordance with a well-known statistical criterions. It have been established that their function of distribution on the manifold of definition is uniform with a root-mean square error less then 0,7%. On the basis of a monotonic changing of cycle's period with increasing system's parameters (M and Nz) they may consider the early made evaluation for maximum period of cycles in the phase space as a more likely nearer to the lower bound value.

References

1. Belyaev R.V., Vorontsov G.M., Kolesov V.V. //The Random Sequences Formed by Nonlinear Algorithm with Delay. // Journ. of Communications Technology and Electronics. 2000. V.45. N 8. P. 954-960.

2. Belyaev R.V., Vorontsov G.M., Zalogin N.N., Kolesov V.V. //The Length of a Nonperiodic Segments of a Pseudorandom Sequence Formed by a Discrete Algorithm with Delay .// Journ. of Communications Technology and Electronics. 2002. V.47. N 4. P. 429-432.