НАИБОЛЬШИЙ ПЕРИОД ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ, ФОРМИРУЕМОЙ ДИСКРЕТНЫМ АЛГОРИТМОМ С ЗАПАЗДЫВАНИЕМ

Беляев Р.В., Воронцов Г.М., Залогин Н.Н., Колесов В.В.

Институт радиотехники и электроники РАН
103907, Москва, ул. Моховая, 11

Для передачи сигналов с большой базой в технике связи, навигации и радиолокации, а также для криптографических целей необходимы псевдослучайные числовые последовательности большого периода. Как правило, такие последовательности генерируются с помощью компьютеров, так как техника сдвиговых регистров, используемая для генерации М-последовательностей, не позволяет получить большие значения периода. Известны алгоритмы, используемые в различных пакетах программ прикладной математики, дающие псевдослучайные последовательности чисел, равномерно распределенных в интервале [0, 1]. Они основаны на рекуррентных преобразованиях некоторого числа, взятого в качестве начального условия. При этом, для обеспечения равномерности распределения используются, как правило, операции умножения, сложения и логическая операция mod. Поскольку вычисления последовательности производятся с конечной разрядностью, т.е. на конечном множестве чисел, а алгоритм вычисления детерминированный, то длительность непериодического сегмента последовательности неизбежно ограничена.

Каждый шаг порождающего рекуррентного алгоритма генератора случайных чисел, заданного на числовом отрезке длиной M, однозначно определеляется конкретным значением d-мерного вектора начальных или текущих значений. Размерность вектора d определяет размерность геометрического пространства алгоритма и, тем самым, объем всех значений векторов, равный M^d. Каждому шагу алгоритма соответствует определенное значение вектора в пространстве размерностью d. Попадание алгоритма в одну и ту же точку d-мерного пространства означает выход последовательности на период. По условию однозначности алгоритма все циклы последовательности не должны иметь ни одной общей точки в d-мерном пространстве, в противном случае решение алгоритма на этом шаге будет неоднозначным, в то время как в реализаций последовательности могут содержаться одинаковые члены.

Значение M^d определяет максимально возможную длительность непериодической реализации последовательности. Практически длина этого сегмента может быть меньше на число начальных векторов, приводящих к циклам меньшего периода, если они существуют.

Если при численном эксперименте за разумные времена удалось обнаружить, что алгоритм генерирует C_k циклов длиной k членов и k_{max} - длина найденного цикла наибольшей длительности, тогда максимальная длина непериодического сегмента последовательности L_{max} , будет не превышать значения:

$$L_{max} = M^d - \sum_{k=1}^{k_{max}} C_k \cdot k \qquad (1)$$

Выражение (1) дает верхнюю оценку длины непериодической последовательности L_{max} , формируемой данным алгоритмом, поскольку в этой формуле не учтены циклы более высокого порядка, которые может быть существуют, но не найдены.

В [1] было предложено использовать для генерации псевдослучайной последовательности алгоритм, родившийся из математической модели генератора СВЧ-шумов – шумотрона [2]. Суть этого алгоритма состоит в том, что используется кольцевая система с запаздыванием, и вместо одного числа, подлежащего преобразованию, фигурирует d чисел, т.е. d-мерный вектор. Степенной характер зависимости в (1) позволяет надеяться на возможность существенного увеличения максимального периода, несмотря на возможное существование в системе коротких циклов. Оценке величины максимального периода в зависимости от размерности алгоритма d посвящена настоящая работа. При малых d можно пытаться выявить циклы за разумные времена перебором начальных значений. Поэтому в данной работе рассмотрение ограничивается случаем размерности d = 2 - 4.

Для выяснения характера зависимости величины максимального цикла от размерности, вычисления производились по алгоритму, формирующему псевдослучайную последовательность целых положительных чисел на интервале [0, 255] [3]. В этом случае M = 256. Размерность алгоритма d варьировалась от 2-х до 4-х. Для вычислений использовалась версия MATLAB 5.2. Начальные условия задавались с помощью генератора случайных чисел (последовательность чисел, равномерно распределенных в интервале [0, 1]) с умножением на 255 и округлением до ближайшего целого числа. Проводилось вычисление первых 16384 значений последовательности. После этого с помощью двойного БПФ осуществлялся поиск «короткого» периода. Если он оказывался безрезультатным, реализация запоминалась на диске, и вычислялись следующие 16384 значений последовательности. Корреляционный анализ первого и второго сегментов с помощью двойного БПФ позволял найти величину периода, если он не превышал 32768. Если же период не находился, второй отрезок стирался из оперативной памяти, и начиналась генерация следующего сегмента. Далее проводился корреляционный анализ вновь вычисленного сегмента, присоединенного к первому. И так до нахождения периода. В ходе вычислений обнаружилось, что не все вектора, взятые в качестве начальных условий, принадлежат циклам. Большая часть этих векторов входит в так называемые бассейны циклов. Выход на цикл

с таких начальных условий продолжался в течение большого числа итераций, зачастую превышающего период цикла. В связи с этим поиск цикла был несколько видоизменен. Сначала генерировалась некоторая длинная реализация последовательности, и запоминался конечный ее сегмент в предположении, что этот отрезок уже принадлежит самому циклу. Корреляционный анализ производился для последующих сегментов последовательности уже в сопоставлении с данным. В случае долгого отсутствия значимого уровня корреляции в качестве сегмента сравнения выбирался еще более поздний сегмент последовательности и т.д.

При исследовании алгоритма с размерностью d = 2 выявился спектр циклов:

«1», «4», «7», «22», 25», «76», «127», «382».

При этом реализации последовательности в цикле данного порядка были полностью идентичны. Исключение составил только цикл «25», в котором наблюдались реализации двух типов. Устойчивой точке 1 соответствовали начальные условия (0, 0). Размеры бассейнов, т.е. количество итераций, предшествующих выходу на цикл, как правило, превышали размеры максимального цикла. Величина максимального цикла 382 была больше количества используемых чисел M = 256, но меньше «объема» пространства 256^2.

Генерация псевдослучайных последовательностей алгоритмом размерностью d = 3 привела к существенному увеличению величины максимального цикла, в то время как количество типов циклов увеличилось незначительно. Спектр циклов в этом случае выглядел следующим образом:

«1», «5», «7», «28», «43», «117», «1313», «4566», «5292», «46894».

Наибольшим бассейном обладал цикл «4566». Он реализовывался в 60% случайно выбранного вектора начальных условий. При этом количество итераций, предшествующих выходу на цикл, составляло в среднем величину $5 \cdot 16384 = 81920$. Имела место также множественность циклов «7» (около 60 типов) и циклов «28» (2 типа). Наибольший цикл «46894» при запуске случайно выбранными тремя числами начальных условий встречался примерно в 10% случаев. Выходу на этот цикл предшествовало в среднем $2 \cdot 16382 = 32764$ итерации.

Алгоритм с размерностью d = 4 не внес в качественную картину ничего нового. Спектр циклов:

«1», «15», «13107», «17671», «978927».

Наибольший цикл встречался в 60% случаев и обладал наибольшим бассейном. Для выхода на этот цикл со случайно выбранного вектора начальных условий требовалось в среднем $50 \cdot 16384 = 819200$ итераций.

Таким образом, можно уверенно утверждать, что максимального цикла величиной, близкой к объему пространства решений в данном классе алгоритмов не существует. Этому препятствует наличие более коротких циклов, а также существование обширных бассейнов притяжения к различным циклам. Тем не менее, с увеличением размерности пространства решений с d = 2 до d = 4 имеет место существенный (степенной) рост величины максимального цикла. Проведенные расчеты позволяют оценить характер роста величины максимального цикла с увеличением размерности. Отложим на диаграмме рис.1 по оси X размерность алгоритма, а по оси Y - десятичные логарифмы величины объема фазового пространства V и десятичные логарифмы длины максимальных циклов N.

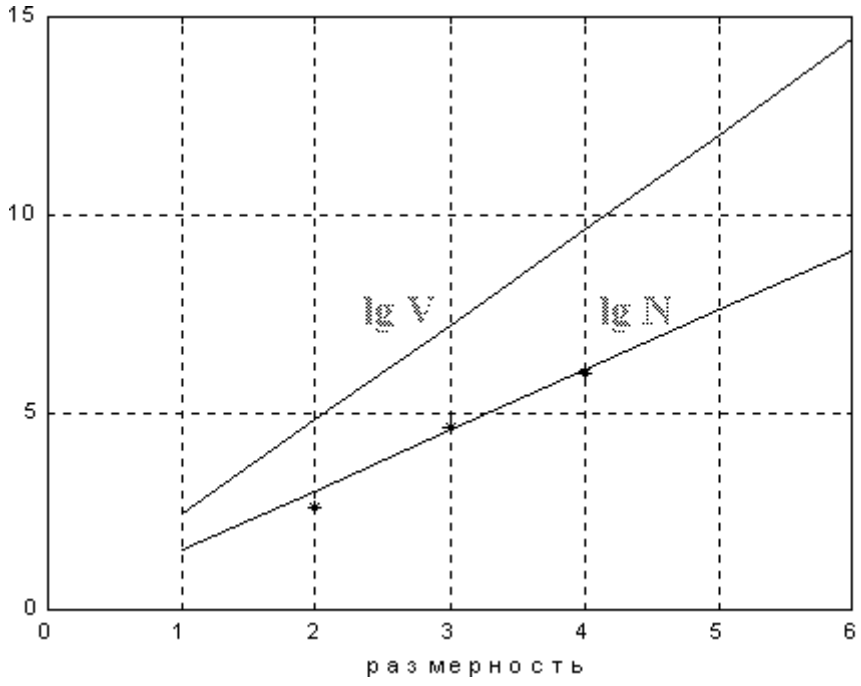

Рис.1

Как видно из графика, прямая, соответствующая длине максимальных циклов, проходит существенно ниже прямой объемов и имеет меньший наклон. Нетрудно выявить эмпирическую зависимость величины максимального цикла N_{max} от размерности алгоритма d. Зависимость выглядит как

$$N_{max} = 256^{0.63d} \tag{2}$$

Это значит, что ожидаемый максимальный цикл в 5-мерной системе составит величину порядка $4 \cdot 10^7$.

На основании полученного выражения (2) следует, что оценку величины периода последовательности, формируемой алгоритмом с запаздыванием $N = 256^d$, приведенную в работе [3], надо рассматривать как существенно завышенную.

Длительность непериодического сегмента хаотической последовательности можно увеличить по сравнению с величиной (2) за счет формирования последовательности в объеме бассейна притяжения найденных циклов. Увеличивая же размерность алгоритма, можно получить непериодический сегмент псевдослучайной последовательностям заданной длины.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проекты № 98-07-90299 и № 00-07-90147

Литература

1. Гуляев Ю.В., Кислов В.Я., Кислов В.В. Новый класс сигналов для передачи информации. Широкополосные хаотические сигналы // ДАН. 1998. т.359, № 6, С. 750-754.

2. Анисимова Ю.В., Воронцов Г.М., Залогин Н.Н., Кислов В.Я., Мясин Е.А. Шумотрон // Радиотехника. 2000. № 2. С. 19-25.

3. Беляев Р.В., Воронцов Г.М., Колесов В.В. Случайные последовательности, формируемые нелинейным алгоритмом с запаздыванием // Радиотехника и электроника. 2000. т. 45, № 8 (в печати).

———————♦———————

THE LARGEST PERIOD OF PSEUDO-RANDOM SEQUENCE FORMING BY DISCRETE ALGORITHM WITH DELAY

Belyaev R.V.,.Vorontsov G.M, Zalogin N.N., Kolesov V.V.

Institute of Radioengineering and Electronics RAS
103907, Moscow, Mokchovaya, 11

For transmitting of signals with large base in communication, navigation, radar and also for cryptography it is necessary to use pseudo-random numerical sequences with large period. Commonly such type sequences are generated by computing because the technique of shift-registers, ordinary used for obtaining M-sequences, doesn't allow to have large period. There are known the algorithms that are used in variety of applied mathematics program, forming pseudo-numerical sequences with uniform distribution on interval [0,1]. These algorithms are based on recursive transformations of some number taken as a start condition. At that for providing uniform distribution there are used the procedures of multiplication, adding and logical operations such as "*mode*". As the calculations of sequence are carried out with finite digit, i.e. on finite numerical set, and algorithm of calculations is deterministic then the length of nonperiodical realization of sequence is inevitably limited.

Every step of the generating recursive algorithm, fixed on numerical section with length M, is defined uniquely by an actual value of d-dimensional vector of start or current conditions. The dimension d of this vector defines the dimension of geometrical space of algorithm and by this the volume of all values of vectors. This volume is equal to M^d. Every step of calculation of algorithm is corresponded to a definite value of vector in d-dimensional space. If algorithm hits into the same point of d-dimensional space then it signifies that process of calculation has got on the cycle. Under the condition of algorithm's single-valuedness all cycles of sequence do not able to have two common points in d-dimensional space. In opposite case the solution of algorithm on the step will be ambiguous. But at the same time there is possible to have equal members in realization of sequence.

A value M^d defines the maximum possible length of nonperiodic realization of sequence. On practice the length of such period may be less of the shown value on the number of start vectors which are leading to cycles of less periods if ones exist.

If on a numerical experiment for reasonable time it was occurred to find that algorithm generates C_k cycles of length k and k_{max} is the length of the most longest of them than the maximal length of nonperiodic realization of sequence L_{max} will not more than value

$$L_{max} = M^d - \sum_{k=1}^{k_{max}} C_k \cdot k \tag{1}$$

The expression (1) gives the upper rating of a length of nonperiodic realization of the sequence generated by algorithm. So in expression (1) there is not taken into account the cycles of more high order which may be exists in reality but were not found.

For generating pseudo-random sequences it was proposed in [1] to use the algorithm, founded on the base of mathematical model of generator of UHF- noise named shoumotron [2]. In this algorithm it is used a ring-circuit of transformation with delay and instead of one number subjecting to transformation there are d-numbers, i.e. d-dimensional vector. The power character of dependence in relation (1) allows to hope on essential period increasing in spite of that there are possible an existence of cycles with less periods. The evaluation of maximum period in sequences generated by this algorithm in dependence of its dimension d is the object of this study.

A little value of d makes possible to find cycles for reasonable short time of calculation by means of selection of start values. Therefor this study is limited by consideration only algorithms with dimension d = 2÷4. The search of cycles was fulfilled by correlation analyses with Fast Fourier Transformation of sequence's segments with length 16384. The algorithm with dimension d =2 had the follow spectrum of cycles:

«1», «4», «7», «22», 25», «76», «127», «382».

At that realizations of sequence in the cycle were completely identical excepting the cycle «25». The size of basin, i.e. the quantity of iterations before exit on cycle, were more as a rule the size of maximal cycle.

Generation of pseudo-random sequence with d = 3 results in substantial increasing of maximal cycle value. The spectrum of cycles in this case shows as:

«1», «5», «7», «28», «43», «117», «1313», «4566», «5292», «46894».

The cycle «4546» had the most basin. It was realized in 60 % of cases of start value vectors. At that number of iterations before achievement of cycle was equal to 5·16384 = 81920 on average. There was also a number of cycles «7» (nearly of 60 types) and cycles «28» (2 types). The cycle of most length was «46894» and it was realized under the conditions of randomly selected start value for 3 numbers in 10% of sampling. Number of iterations before achievement of this cycle was equal on average 2·16382 = 32764 iterations.

Algorithm with dimension d = 4 didn't make any news in quality pattern. The spectrum of cycles has the structure:

«1», «15», «13107», «17671», «978927».

The cycle of most length was occurred in 60% of sampling and it has the most basin of attraction. To achievement of this cycle with starting from randomly selected start conditions it was needed on average 50·16384 = 819200 iterations.

So it is possible to state positively that maximal cycle with a length nearly equal to volume of space of solutions for algorithm of this class does not exist. It is opposed to this the presence of other cycles with periods of less values and existence of. basins of attraction to cycles having rather large values. Nevertheless on increasing the dimensions of solutions space from d = 2 to d = 4 there were observed substantial growth of maximal cycle's period. The calculations allow to give estimation for dependence of maximal length period on dimension d. Such empirical dependence may be shown as:

$$N_{max} = 256^{0.63d} \qquad (2)$$

This means that expected maximal length period for algorithm with dimension d=5 will be equal $4\ 10^7$.On the base of expression (2) it is followed that the evaluation of sequence period generated by algorithm with delay $N = 256^d$ given in [3] is essentially overestimated.

The nonperiodic segment of pseudo-random sequence duration may be increased in comparison with value given by (2) at the expanse of sequence forming in volume of founded cycles basin attraction. By increasing the algorithm dimension it is possible to get nonperiodical segment of pseudo-random sequence with needed length.

This study was fulfilled under the support of Russian Foundation of Basic Research, projects № 98-07-90299 and № 00-07-90147.

References

1. Gulyaev Yu.V., Kislov V.Ya., Kislov V.V. New class of signals for information transmitting. Wide band chaotic signals //Reports of RAS. 1998.V.359, № 6. P. 750-754.

2. Anisimova Yu.V., Vorontsov G.M., Zalogin N.N., Kislov V.Ya., Myasin E.A. Shoumotron // Radiotechnika. 2000. № 2. P. 19-25.

3. Belyaev R.V., Vorontsov G.M., Kolesov V.V. Random-sequences generated by nonlinear algorithm with delay // Radiotechnika i Electronika. 2000. V.45. №8 (in print).