Литература

1. *Якубович, В.А.* Линейные дифференциальные уравнения с периодическими коэффициентами / В.А. Якубович, В.М. Старжинский. – М.: Наука, 1972. – 720 с.
2. *Маркеев, А. П.* Точки либрации в небесной механике и космодинамике/ А. П. Маркеев. – М.: Наука, 1978. – 312 с.
3. *Гребеников, Е.А.* Методы компьютерной алгебры в проблеме многих тел / Е.А. Гребеников, Д. Козак-Сковородкина, М. Якубяк. – 2-е изд., перераб. и доп. – М.: Изд-во РУДН, 2002. – 209 с.
4. *Budzko, D.A.* Computing the stability boundaries for the Hill's equation / D.A. Budzko // Computer algebra in scientific computing: proc. of the international conference of young scientists CYS CASC'2006, Chisinau, Moldova, Sept. 11–15, 2006 / Technical university of Moldova; Eds.: E.A. Grebenikov [and others]. – Chisinau, 2006. – P. 15–20.
5. *Budzko, D.A.* Determination of the stability boundaries for the fourth order Hamiltonian system / D.A. Budzko // Computer Algebra Systems in Teaching and Research: proc. of the 4th International Workshop CASTR'2007, Siedlce, Poland, Jan. 31 – Feb. 3, 2007 / University of Podlasie; Eds.: L. Gadomski [and others]. – Siedlce, 2007. – P. 30–33.
6. *Wolfram, S.* The Mathematica book / S. Wolfram. – Wolfram Media/Cambridge University Press, 1999. – 1470 p.
7. *Прокопеня, А.Н.* Об одном методе символьных вычислений характеристических показателей линейной системы дифференциальных уравнений с периодическими коэффициентами / А.Н. Прокопеня // Сб. науч. тр. / Ин-т системного анализа РАН. – Москва, 2005. – Вып. 9(2): Динамика неоднородных систем. – С. 73-87.

ИССЛЕДОВАНИЕ ПЕРИОДИЧЕСКИХ СВОЙСТВ ПОСЛЕДОВАТЕЛЬНОСТИ СОСТОЯНИЙ ОДНОГО КЛАССА АВТОНОМНЫХ АВТОМАТОВ

Валуева Т.А.

ННИЦ ППМИ, Белорусский государственный университет, г. Минск

Введение

Рассмотрим автономный автомат, реализующий генератор, который состоит из нескольких регистров сдвига и блока управления движением регистров. По набору текущих состояний регистров блок управления определяет, на сколько шагов должен продвинуться каждый из регистров за один такт работы генератора.

В работе [

1] была рассмотрена математическая модель данного автомата, согласно которой функционирование автомата описывается случайным блужданием на окружности или торе. При этом шаги, на которые сдвигаются регистры, принимают значения из множества $\{1,2,\ldots,K\}$, $K \in N$. В работе [

1] получена вероятность того, что случайно выбранное состояние лежит на цикле длины n. В данной работе рассмотрен случай, когда каждый из регистров сдвига сдвигается на k или d шагов, $k, d \in N$, $k \neq d$, найдено среднее время возвращения автомата в начальное состояние, и длина наиболее вероятного цикла, в случае, когда $d = k + 1$.

Вероятность появления цикла длины *n*

Рассмотрим автономный автомат U, реализующий генератор, состоящий из m линейных регистров сдвига $LFSR_i$, минимальные полиномы которых являются примитивными полиномами степеней n_i, $i=\overline{1,m}$ (см. [2]). Обозначим через $Z=\{0,1\}$ множество выходов автомата U, через $S=S_1\times S_2\times\ldots\times S_m$ — множество состояний, где S_i — множество ненулевых состояний регистра LFSRi, $S_i(t)$ — состояние i-того регистра сдвига в момент времени t, $s(t)=(S_1(t),S_2(t),\ldots,S_m(t))$ — состояние автомата в момент времени t, $t\geq 1$. Функция переходов состояний имеет следующий вид:

$$S_i(t+1)=S_i(t)\cdot A_i^{\overline{v}_i(t)},\ i=\overline{1,m},$$

где $\overline{v}_i(1),\overline{v}_i(2),\ldots,\overline{v}_i(t),\ldots$ — реализация независимых в совокупности случайных величин $v_i(1),v_i(2),\ldots,v_i(t),\ldots$ с равномерным на множестве $\{k,d\}$ распределением, A_i — характеристическая матрица минимального полинома LFSRi. Отметим, что данная модель задает класс автоматов мощности $2^{m(2^{n_1}-1)\cdot\ldots\cdot(2^{n_m}-1)}$, каждый автомат которого определяется реализацией случайных величин $\{v_i(t)\}_{t=1}^{2^{m(2^{n_1}-1)\ldots(2^{n_m}-1)}}$, $i=\overline{1,m}$.

Пусть $C(n)$ — множество циклических точек автомата U, лежащих на циклах длины n. Обозначим через $L=\max\{k,d\}$, $n_q=\max_{1\leq i\leq m} n_i$ — степень минимального полинома регистра максимальной длины, $B(n,r)=n!/(2^n x_1!(n-x_1)!)$, где $x_1=(r-nd)/(k-d)$. Положим $B(n,r)=0$ в случае, когда $x_1\notin N$ или $n\leq x_1$.

Теорема 1. Пусть $s(1)$ — случайное начальное состояние автомата U, равномерно распределенное на множестве S, тогда

$$P\{s(1)\in C(n)\}\leq\prod_{i=1}^{m}\left(\sum_{\substack{(k+d-L)n/(2^{n_i}-1)\leq d_i\leq\\ Ln/(2^{n_i}-1)}} B(n,d_i(2^{n_i}-1))\right),\ n\geq 1. \qquad (1)$$

В случае $1\leq n<2\max_{1\leq i\leq m}\{(2^{n_i}-1)/L\}$ в (1) имеет место равенство.

Замечание 1. Доказательство данной теоремы почти полностью повторяет доказательство теоремы 1[
1].

Следствие 1. При $d=k+1$ и выполнении одного из условий:

1) $k>0$ и $\max_{1\leq i\leq m}\{2^{n_i}-1\}/(k+1)\leq n<\min_{1\leq i\leq m}\{2^{n_i}-1\}/k$,

2) $k=0$ и $\max_{1\leq i\leq m}\{2^{n_i}-1\}<n<2\min_{1\leq i\leq m}\{2^{n_i}-1\}$,

соотношение (1) имеет вид:

$$P\{s(1)\in C(n)\}=\frac{1}{2^{mn}}\prod_{i=1}^{m}\left(\frac{n!}{((k+1)n-2^{n_i}+1)!(2^{n_i}-1-nk)!}\right). \qquad (2)$$

Замечание 2. В случае, когда $\{v_i(t)\}_{t=1}^{2^{m(2^{n_1}-1)\ldots(2^{n_m}-1)}}$, $i=\overline{1,m}$ независимые в совокупности случайные величины с распределением $P\{v_i(t)=k\}=p$, $P\{v_i(t)=k+1\}=1-p$, а n удовлетворяет ограничениям следствия 1, формула (2) имеет вид:

$$P\{s(1)\in C(n)\}=\prod_{i=1}^{m}\left(\frac{n!p^{(k+1)n-2^{n_i}+1}(1-p)^{2^{n_i}-1-nk}}{((k+1)n-2^{n_i}+1)!(2^{n_i}-1-nk)!}\right). \qquad (3)$$

Длина наиболее вероятного цикла есть $\arg\max_n P\{s(1)\in C(n)\}$. В случае, когда $d=k+1$ и $n_1=n_2=...=n_m$, для некоторых значений $p=P\{v_i(t)=k\}$ приведем длину наиболее вероятного цикла. Обозначим через $K=2^{n_1}-1=2^{n_2}-1=...=2^{n_m}-1$. Поскольку максимум вероятностей, определенных в (2) и (3), доставляет вещественное число, а длина цикла — натуральное число, то в таблице 1 приведены нижние и верхние границы промежутка $[n_*,n^*]$, в котором содержится длина наиболее вероятного цикла, максимум берется по всем $n\in[N_1,N_2[$.

Таблица 1. *Длина наиболее вероятного цикла*

p	k	d	$n\in[N_1,N_2[$	n_*	n^*
½	1	2	$n\in[K/2,K[$	$\lfloor 2K/3-5/9\rfloor$	$\lceil 2K/3-1/3\rceil$
¼	1	2	$n\in[K/2,K[$	$\lfloor 4K/7-33/49\rfloor$	$\lceil 4K/7-3/7\rceil$
½	0	1	$n\in[K,2K[$	$2K-1$	$2K-1$
¼	0	1	$n\in[K,2K[$	$\lfloor 4K/3-1\rfloor$	$\lceil 4K/3-1\rceil$

Среднее время возвращения автомата в начальное состояние

Отметим, что в данном разделе, говоря о состоянии автомата, будем иметь в виду только те состояния, которые являются циклическими вершинами соответствующего автоматного графа. Тогда в качестве начального момента времени считаем тот момент, когда автомат попал в одно из вышеописанных состояний.

Теорема 2. Время T_i, через которое регистр LFSRi вернется в начальное состояние, представимо в виде:

$$\sum_{j=1}^{T_i}\overline{v_i}(j)=(2^{n_i}-1)\cdot h_i,\ h_i\in\{1,2,...,\frac{|S|}{2^{n_i}-1}\},\text{ и }\forall t<T_i,\ \sum_{j=1}^{t}v_i(j)<(2^{n_i}-1)\cdot h_i. \quad (4)$$

В случае, когда $k=0,d=1$, $h_i=1$.

Из теоремы 2 следует, что T_i+1 есть значение процесса восстановления $\eta(t)$ в точке $t=(2^{n_i}-1)h_i$, причем в случае $k=0,d=1$ данный процесс является непрерывным сверху (см. [3]).

Теорема 3. Пусть $k=0,d=1$, тогда среднее время, через которое регистр LFSRi вернется в начальное состояние

$$E\{T_i\}=\frac{2^{n_i}-1}{1-p}-1,\ p=P\{v_i(1)=0\}.$$

В случае, когда значения k,d не равны 0,1, h_i принимает значение из множества $\{1,2,...,|S|/(2^{n_i}-1)\}$. Обозначим через $T_i(h_i)$ время, через которое регистр LFSRi вернулся в начальное состояние только после h_i проходов своего периода. В данном случае момент первого возвращения регистра LFSRi в начальное состояние есть $T_i(h_i)=\eta((2^{n_i}-1)h_i)-1$.

Теорема 4. Если все $\{v_i(j)\}$, $j=1,2,...$ одинаково распределены и $E\{v_i^2(j)<\infty\}$, то для математического ожидания времени возвращения LFSRi в начальное состояние справедлива следующая оценка:

$$E\{T_i(h_i)\} = \frac{2^{n_i}-1}{pk+(1-p)d} h_i - 1 + \frac{p(k^2+k)+(1-p)(d^2+d)}{2(pk+(1-p)d)^2} + o(1) \qquad (5).$$

Замечание 3. Период последовательности состояний автомата U есть такое число T, для которого выполняются равенства (4) при всех $i=\overline{1,m}$. Очевидно, что в этом случае $h_q = \min_{1\le i\le m}\{h_i\}$. Поскольку для T справедливо представление (4), то период последовательности состояний автомата есть $\eta(2^{n_q}-1)h_q - 1$, где $h_q \in \{1,2,...,|S|/(2^{n_q}-1)\}$. Тогда, если $k=0, d=1$, то $E\{T(h_q)\} = (2^{n_q}-1)h_q/(1-p)-1$. В других случаях для математического ожидания периода автомата U справедлива оценка (5).

В таблице 2 приведен сравнительный анализ результатов, полученных при изучении периодических свойств последовательности состояний автомата U. Отметим, что $E\{T(1)\}$ ($LFSR_q$ — регистр сдвига наибольшей длины, вернулся в начальное состояние после первого прохода своего периода), близко к длине наиболее вероятного цикла из промежутка $[K/(k+1), K/k[$, если $k>0$, и $[K,2K[$, в случае $k=0$.

Таблица 2. *Средний и наиболее вероятный период*

p	k	d	$n\in[N_1,N_2[$	n_*	n^*	$E\{T\}$
½	1	2	$n\in[K/2,K[$	$\lfloor 2K/3-5/9\rfloor$	$\lceil 2K/3-1/3\rceil$	$2K/3-1/9+o(1)$
¼	1	2	$n\in[K/2,K[$	$\lfloor 4K/7-33/49\rfloor$	$\lceil 4K/7-3/7\rceil$	$4K/7-13/49+o(1)$
½	0	1	$n\in[K,2K[$	$2K-1$	$2K-1$	$2K-1$
¼	0	1	$n\in[K,2K[$	$\lfloor 4K/3-1\rfloor$	$\lceil 4K/3-1\rceil$	$4K/3-1$

Литература

1. Михайлов В.Г. //Труды по дискретной математике. 2002. Т. 5. С. 167.
2. Лидл Р., Нидеррайтер Г. Конечные поля: В 2т. М., 1988. - Т.2. С. 495.
3. Боровков А. А. Теория вероятностей. - М., 2003.

СХОДИМОСТЬ В ГИЛЬБЕРТОВОМ ПРОСТРАНСТВЕ ИТЕРАЦИОННОЙ ПРОЦЕДУРЫ РЕШЕНИЯ НЕКОРРЕКТНЫХ ЗАДАЧ С ПРАВИЛОМ ОСТАНОВА ПО НЕВЯЗКЕ

Василькович С.И., Савчук В.Ф.
Брестский государственный университет им. А.С. Пушкина, г. Брест

Для решения операторного уравнения $Ax=y$ в гильбертовом пространстве H с положительным самосопряженным ограниченным оператором A предлагается итерационный метод

$$x_{n+1} = (E-\alpha A)^2 x_n + A^{-1}\left[E-(E-\alpha A)^2\right]y, x_0 = 0. \qquad (1)$$

Здесь нуль не является собственным значением оператора A, поэтому решение единственно. Однако $0\in SpA$ и, значит, рассматриваемая задача неустойчива, т.е. некорректна. Предполагается, что при точной правой части уравнения y существует точное решение x.

Обычно правая часть уравнения известна с некоторой погрешностью δ, т.е. известен y_δ, для которого $\|y-y_\delta\|\le\delta$. Поэтому вместо (1) приходится рассматривать приближения

$$x_{n+1,\delta} = (E-\alpha A)^2 x_{n,\delta} + A^{-1}\left[E-(E-\alpha A)^2\right]y_\delta, x_{0,\delta} = 0. \qquad (2)$$