индекс 3624

ЕРЕВАНСКИЙ ФИЗИЧЕСКИЙ ИНСТИТУТ

Preprint YERPHI-1094(57)-88

ԵՐԵՎԱՆԻ ՖԻԶԻԿԱՅԻ ԻՆՍՏԻՏՈՒՏ
ЕРЕВАНСКИЙ ФИЗИЧЕСКИЙ ИНСТИТУТ
YEREVAN PHYSICS INSTITUTE

P. S. OVNANYAN

PERIODS OF MATRIX GENERATORS OF PSEUDORANDOM NUMBERS

ЦНИИатоминформ
ЕРЕВАН—1988

Նախնական ԵՖԻ-1094(57)-88

Պ.Ս. ՀՈՎՀԱՆՆԻՍՅԱՆ

ՆԵՂ ՊԱՏԱՀԱԿԱՆ ԹՎԻՆԵՐԻ ՄԱՏՐԻՑԱՅԻՆ ԳԵՆԵՐԱՏՈՐՆԵՐԻ ՊԱՐԲԵՐՈՒԹՅՈՒՆՆԵՐԸ

Քննարկվում են $X_i = AX_{i-1}$ (mod. L) գեներատորներ, որտեղ A-ն մատրից է, իսկ X_i-ը՝ d-չափանի վեկտոր: Տարբեր A մատրիցների և L-երի համար հաշվված են գեներատորների պարբերությունները: Ցույց է տրված, որ տարածության չափողականությունը թույլ է ազդում գեներացիայի պարբերության վրա, եթե զերխորանարդի կողմը՝ L = 1, իսկ վեկտորի բաղադրիչները ամնորդական կոտորակներ են: ,,Պրիմիտիվ,, մատրիցները, որոնց DET.A≠1 և (DET.A,L)=1, ունեն հնարավոր առավելագույն պարբերություն:

Երևանի Ֆիզիկայի Ինստիտուտ
Երևան 1988

Препринт ЕФИ-1094(57)-88

П.С.ОВНАНЯН

ПЕРИОДЫ МАТРИЧНЫХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Рассмотрены генераторы $X_i = A X_{i-1}$ (мод.L), где A - матрица, X_i - d-мерный вектор. Вычислены периоды генерации для разных L и матриц A. Показано, что размерность пространства слабо влияет на период генерации, если сторона гиперкуба L = I, а компоненты вектора являются десятичными дробями. Максимально возможный период генерируют "примитивные" матрицы с DET.A = I и (DET.A, L)=I.

Ереванский физический институт
Ереван 1988

Preprint YERPHI-1094(57)-88

P.S. OVNANYAN

PERIODS OF MATRIX GENERATORS OF PSEUDORANDOM NUMBERS

Generators $X_i = AX_{i-1}$ (mod. L) are considered, where A is matrix, X_i is d-dimensional vector. Generation periods for different L and A matrices are calculated. The space dimension is shown to affect weakly the generation period, if the edge of hypercube L=1, and components of the vectors are decimal fractions. The "primitive" matrices with DET.A $\neq$ 1 and (DET.A,L) = 1 generate the maximum possible period.

Yerevan Physics Institute
Yerevan 1988

The present-day generators of pseudorandom numbers are in fact determinate nonlinear dynamical systems with pseudochaotic trajectories. Matrix generators were originally proposed in 1958 by Gross and Johnson [1] ; however, periods of these generators were estimated incorrectly. Jansson made a wrong conclusion that the action of matrix generator is identical to linear recursion relation:

$$X_{n+1} = \sum_{k=0}^{j} a_k X_{n-k} \qquad (1)$$

and attributed the periods of this generator to the matrix one [2] .

Statistical properties of matrix generators were studied in Refs.[3,4] , where were found χ^2 distributions [5] for matrices with determinant 1 and dimensions 2,3,4,6,12. Ibidem were mentioned somewhat better statistical properties of these generators compared to multiplicative generators.

We'll consider a sequence

$$X_{n+1} = AX_n \qquad (\text{mod.}L) \qquad (2)$$

where X_n is a d-dimensional integer vector, and a d-dimensional hypercube with an edge L is a "phase space". The number of various vectors in it is L^d, the zero vector being immovable. In order to turn to the usual case of a unit hypercube as a "phase space", it is necessary to divide all terms of the sequence by L.

For the trajectory unambiguity, sufficient is the condition $(D,L) = 1$, i.e. L and determinant D have no common factors. Then we can readily show that there exists an integer inverse matrix and the trajectory is a closed line. Otherwise, the system never returns to its initial state, and the trajectory has a form of a loop with a tail.

Let us prove 3 theorems which allow to determine for the given matrix periods of sequence (2) at different L.

The whole set of $L^d - 1$ points of "phase space" is divided into, generally speaking, somewhat cyclic groups.

Denote by T(L) a maximal period of sequence generated by matrix (A_{ij}) modulo L.

Theorem 1. A period $T(p^{k+1}) = p \cdot T(p^k)$, where p is a prime number.

For some point X_0 we have

$$A^{T(p^k)} X_0 = X_0 + p^k \cdot \alpha \,, \tag{3}$$

where α is some vector, generally speaking, not multiple of p. If α is multiple of p, then $T(p^{k+1}) = T(p^k)$. A repeated action of matrix $A^{T(p^k)}$ on (3) gives:

$$A^{2T(p^k)} X_0 = X_0 + 2p^k \alpha + p^{2k} \beta \tag{4}$$

The third term of this expression $= 0 \pmod{p^{k+1}}$. Hence:

$$A^{nT(p^k)} X_0 = X_0 + np^k \alpha + p^{k+1} \gamma \tag{5}$$

whence at $n = p$ we obtain:

$$A^{pT(p^k)} X_0 = X_0 + p^{k+1} \alpha \,. \tag{6}$$

Taking $\pmod{p^{k+1}}$ from both sides of equality (6), we'll obtain the statement of theorem 1.

Theorem 2. Period of sequence the vectors multiple of p^l belong to $\pmod{p^{k+l}}$ are equal to period $T(p^k)$. Multiplying the equality

$$A^{T(p^k)} X_0 = X_0 + p^k \alpha \tag{7}$$

by p^l we'll obtain:

$$A^{T(p^k)} (X_0 p^l) = (X_0 \cdot p^l) + p^{k+l} \cdot \alpha \tag{8}$$

whence the theorem statement follows.

Theorem 3. A maximal period of sequence (2) in compound module $P_1 \cdot P_2$ is equal to

$$T(P_1 \cdot P_2) = \frac{T(P_1) \cdot T(P_2)}{(T(P_1), T(P_2))} \tag{9}$$

We have

$$A^{k \cdot T(P_1)} X_0 = X_0 + P_1 \cdot \alpha_k \,, \tag{10}$$

$$A^{l \cdot T(P_2)} X_0 = X_0 + P_2 \cdot \beta_l \tag{11}$$

Let

$$H = K \cdot T(P_1) = \ell \cdot T(P_2) = \frac{T(P_1) \cdot T(P_2)}{(T(P_1), T(P_2))} , \qquad (12)$$

then

$$A^H X_0 = X_0 + P_1 \alpha_K = X_0 + P_2 \beta_\ell \qquad (13)$$

Insofar as the medium part $= X_0 \pmod{P_1}$, and the right-hand side $= X_0 \pmod{P_2}$, then

$$A^H X_0 = X_0 \quad (\mathrm{mod} \cdot P_1 \cdot P_2) \qquad (14)$$

Elucidate theorems 1 and 2 on the example of two-dimensional transformation. If we successively divide the square into P, P^2, P^3, etc. parts, then maximal period grows in proportion to P. Let S from the primary P^2 vectors belong to a maximal period $T(P)$ (clearly, S is multiple of $T(P)$), and (P^2-S-1) vectors belong to a less period $t(P)$ (if $3 \neq P^2-1$). Then $S \cdot P^2$ vectors belong to maximal period $T(P^2) = P \cdot T(P)$, and $S \cdot P^4$ vectors - to $T(P^3) = P^2 T(P)$, respectively, and so on. The square $P^K \times P^K$ contains vectors which belong to the whole set of periods $t(P)$, $T(P)$, $Pt(P)$, $PT(P)$, ...

Among P^{2K} vectors there are

1	immovable vector	
P^2-S-1	vectors with period	$t(P)$
S	" - " - " - "	$T(P)$

(15)

$(P^2-S-1) \cdot P^2$	" — " — " — "	$Pt(P)$
$S \cdot P^2$	" — " — " — "	$PT(P)$
— — — — — — — — — — — — —		
$(P^2-S-1) \cdot P^{2(K-1)}$	" — " — " — "	$P^{K-1} t(P)$
$S \cdot P^{2(K-1)}$	" — " — " — "	$P^{K-1} T(P)$

Knowing the spectrum of $T(P)$ for each concrete matrix by theorems 1-3, one can determine a period of any point in any compound module. For example, for a matrix $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ $T(2)=3$, $T(5)=20$ and hence

$$\begin{aligned} T(2^K) &= 3 \cdot 2^{K-1} \\ T(5^K) &= 20 \cdot 5^{K-1} \\ T(10) &= 60 \\ T(100) &= 300 \\ T(10^K) &= 15 \cdot 10^{K-1} \end{aligned} \qquad (16)$$

at $K \geq 3$

Thus, if the number of decimal position of the computer processor is equal to K, then the period of generator equals $1.5 \cdot 10^K$.

The increase of matrix dimension does not change strongly the period.

So, for the matrix $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ $T(10^K) = 217 \cdot 10^{K-1}$,

and for the matrix $\begin{pmatrix} 2111 \\ 1211 \\ 2221 \\ 1111 \end{pmatrix}$ $T(10^K) = 186\ 10^{K-1}$.

We can see that irrespective of space dimension, the period, roughly speaking, is equal to the number of computer-distinguishable points on a section (0,1).

Before going on, let us give some definitions from theory of numbers [7] .

Consider a comparison $a^z = 1$ (mod. m). The least z satisfying this comparison is called an exponent the number a modulo m belongs to.

The number of a number series 1,2,3,... (n-1) mutually prime with n is denoted by $\varphi(n)$ and called Euler function. At prime $n=p$, $\varphi(p)=p-1$. Numbers a belonging to exponent $\varphi(m)$ are called primitive roots modulo m .

A question arises whether it is possible to introduce a notion of primitive root for matrices? In the case of matrices a complete system of modulo p residues is formed by p^d vectors one of which is zero. Hence, the primitive matrix can be defined as follows:

$$A^{p^d-1} = E \quad (\text{mod. } p) , \tag{17}$$

where p is prime, d is matrix dimension, E is unit matrix. Computer calculations have shown that there do not exist two-dimensional primitive matrices with determinant $D=1$ modulo p less than 61. Apparently, this statement is valid for all p and d .

At $D \neq 1$ a set of matrices are found that are primitive by different moduli.

Thus matrix $\begin{pmatrix} 31 \\ 11 \end{pmatrix}$ is primitive modulo 3,5,11,13,19,37,etc. And matrix $\begin{pmatrix} 211 \\ 331 \\ 111 \end{pmatrix}$ is primitive at $p = 13,19,37,...$

The existence of primitive matrices means that for some

$$T(p) = p^d - 1 \tag{18}$$

Matrix $\begin{pmatrix} 31 \\ 11 \end{pmatrix}$ is primitive modulo $p = 787,797,1121,1171$. These values are chosen among others for the reasons that the greatest common divisors in all pairs $T(p_i), T(p_k)$ $i,k = 1-4$ would be the least. Then the period generated by this matrix mod. $L = P_1 \cdot P_2 \cdot P_3 \cdot P_4$ of their product is, according to theorem 3, $T = 10^{21}$. Recall that, as shown above, the same matrix (mod. 1) generates a sequence with period $T=10^{12}$, i.e. by 9 orders as less. If one succeeded in finding a prime number of the order of 10^{12}, modulo which the given matrix is primitive, then its generated sequence would have, according to (18), a period $T=10^{24}$. However, the finding of primitive matrices modulo $> 10^4$ and with dimension > 4 requires much computer time.

We can show that by varying in a certain way the primitive matrix in the generation process, we can achieve a period of sequence

$$T = (p^d - 1) \cdot \varphi(p^d - 1) \sim p^{2d} \tag{19}$$

A particular study is undoubtedly required for statistical properties of generators that use primitive matrices with $D \neq 1$ ($(D,L)=1$), as it was done for unimodular matrices [3,4] . The results of these studies will be published eslewhere.

The author would like to express his sincere gratitude to G.K. Savvidy for the fruitful discussions.

REFERENCES

1. Gross O., Johnson S. Additive generation of pseudorandom numbers. - RAND Corp. Res. Mem., 1958, p.2132.
2. Jansson Birger. Random number generators, Stockholm, 1966.
3. Саввиди Г.К., Тер-Арутюнян-Саввиди Н.Г. К проблеме Монте-Карло-моделирования физических систем.Препринт ЕФИ-865(I6)-86, Ереван, I986.
4. Акопов Н.З., Саввиди Г.Г., Тер-Арутюнян-Саввиди Н.Г. Матричный генератор псевдослучайных чисел. Препринт ЕФИ-867(I8)--86, Ереван,I986.
5. Ермаков С.М., Михайлов Г.А. Курс статистического моделирования. М.: Наука, I976.
6. Зельдович Я.Б., Соколов Д.Д. Фрактали, подобие, промежуточная асимптотика. УФН, I985, т.I46, вып.3.
7. Виноградов И.М. Основы теории чисел. ОНТИ НКТП СССР Москва, I936.

The manuscript was received 5 May 1988