高速乱数発生法について†

森山純臣†† 北村正一†††

Abstract

C. M. Rader, L. R. Rabiner and R. W. Schaffer have proposed a fast method of generating digital random numbers using arithmetic operations of an L bit exclusive-or and a cyclic rotation.

In this paper, some properties of this pseudorandom numbers are presented as follows: (a) An equation of the ith random number is derived by means of the delay operator method. (b) There are special relations between the shorter periods and the initial values. (c) There are some sub-periods in the word lengths of 5, 11, 13 and 19 that have unreasonable randomness.

1. まえがき

乱数発生法には中央2乗法・合同法・相加法などがあるが，現在ほとんど全ては mod 演算を用いて発生させる合同法が使われている．しかし，この方法では1個の乱数を発生させるのに少なくとも1回の加算・乗算が必要のため，演算時間が相当に長いものとなる．そこで，1970年 C. M. Rader 等が従来の方法よりもはるかに高速で，質の良い乱数発生法を報告した[1]．ここでは Rader の論文でまだ明らかにされていない 2, 3 の性質について述べている．すなわち，任意の i 番目の乱数を表わす式が示されていること，初期値の選び方によりいろいろな周期が存在すること，また副周期（と名づける）が存在し乱数の無規則性に好ましくないことなどである．

2. 理　論

発生アルゴリズムは，L ビットの2進数乱数 X_i が前2つの同じ長さの X_{i-1} と X_{i-2} との各ビット毎の排他的論理和演算と適当な桁移動とを行うことによって得られることである．すなわち，

$$X_i = T_p(X_{i-1} \oplus X_{i-2}). \qquad (1)$$

但し，T_p: p 桁移動 (cyclic rotation),

$\oplus$: 排地的論理和,

$i=0, 1, 2, \cdots$

と示される．こうして，次々と新しい乱数 X_i が発生されるが，ここで初期値 X_{-2} と X_{-1} とが連続して再び現われるまでが周期であり，周期が最大となるのは p と L とが互に素なときである．次にいま，L ビットの初期値を $X_{-2}=(a_0, a_1, \cdots, a_{L-1})$, $X_{-1}=(b_0, b_1, \cdots, b_{L-1})$ と表わすと，$D^0 a_K = a_K$, $Da_K = a_{K-1}$, $D^2 a_K = a_{K-2}$, $\cdots$ となるような作用子 D を用いて次のようにも表わされる．

$$X_{-2}=(D^{L-1}a_{L-1}, D^{L-2}a_{L-1}, \cdots, Da_{L-1}, a_{L-1}),$$

$$X_{-1}=(D^{L-1}b_{L-1}, D^{L-2}b_{L-1}, \cdots, Db_{L-1}, b_{L-1}),$$

ここで，$X_{-2}=\{a_{L-1}\}$, $X_{-1}=\{b_{L-1}\}$ とすると，最右側桁が Da_{L-1}, D^2a_{L-1}, $\cdots$; Db_{L-1}, D^2b_{L-1}, $\cdots$; である乱数は各々次のように表わされる．

$$\{Da_{L-1}\}=(a_{L-1}, D^{L-1}a_{L-1}, \cdots, D^2a_{L-1}, Da_{L-1}),$$

$$\{D^2a_{L-1}\}=(Da_{L-1}, a_{L-1}, \cdots, D^3a_{L-1}, D^2a_{L-1}),$$

$$\cdots\cdots\cdots\cdots,$$

$$\{Db_{L-1}\}=(b_{L-1}, D^{L-1}b_{L-1}, \cdots, D^2b_{L-1}, Db_{L-1}),$$

$$\{D^2b_{L-1}\}=(Db_{L-1}, b_{L-1}, \cdots, D^3b_{L-1}, D^2b_{L-1}),$$

$$\cdots\cdots\cdots\cdots.$$

Table 1 The arithmetic process of L bit random numbers with $p=1$ using an operator D.

乱数列	各桁の演算過程			
X_{-2}	$D^{L-1}a$	$D^{L-2}a$	⋯	a
X_{-1}	$D^{L-1}b$	$D^{L-2}b$	⋯	b
X_0	$a\oplus b$	$D^{L-1}(a\oplus b)$	⋯	$D(a\oplus b)$
X_1	$b\oplus D(a\oplus b)$	$D^{L-1}b\oplus a\oplus b$	⋯	$Db\oplus D^2(a\oplus b)$
X_2	$Da\oplus D^2(a\oplus b)$	$a\oplus D(a\oplus b)$	⋯	$D^3a\oplus D^3(a\oplus b)$
X_3	$Db\oplus D^2b\oplus D^3(a\oplus b)$	$b\oplus Db\oplus D^2(a\oplus b)$	⋯	$D^2b\oplus D^3b\oplus D^4(a\oplus b)$

† On a fast method of generating digital random numbers, by Yoshitomi Moriyama (Kushiro Technical College) and Shoichi Kitamura (Faculty of Engineering, Muroran Institute of Technology)

†† 釧路工業高等専門学校電気工学科
††† 室蘭工業大学電子工学科

Table 2 The arithmetic process of the most right hand bit of random numbers with $p=1$ using an operator D.

乱数列の番号 i	最右側桁の演算過程	
-2	a	
-1	b	
0	aD	$\oplus bD$
1	aD^2	$\oplus b(D\oplus D^2)$
2	$a(D^2\oplus D^3)$	$\oplus b(2D^2\oplus D^3)$
3	$a(2D^3\oplus D^4)$	$\oplus b(D^3\oplus 3D^3\oplus D^4)$
4	$a(D^3\oplus 3D^4\oplus D^5)$	$\oplus b(3D^3\oplus 4D^4\oplus D^5)$
5	$a(3D^4\oplus 4D^5\oplus D^6)$	$\oplus b(D^3\oplus 6D^4\oplus 5D^5\oplus D^6)$
6	$a(D^4\oplus 6D^5\oplus 5D^6\oplus D^7)$	$\oplus b(4D^4\oplus 10D^5\oplus 6D^6\oplus D^7)$
7	$a(4D^5\oplus 10D^6\oplus D^7\oplus D^8)$	$\oplus b(D^4\oplus 10D^5\oplus 15D^6\oplus 7D^7\oplus D^8)$
8	$a(D^5\oplus 10D^6\oplus 15D^7\oplus 7D^8\oplus D^9)$	$\oplus b(5D^5\oplus 20D^6\oplus 21D^7\oplus 8D^8\oplus D^9)$
9	$a(5D^6\oplus 20D^7\oplus 21D^8\oplus 8D^9\oplus D^{10})$	$\oplus b(D^5\oplus 15D^6\oplus 35D^7\oplus 30D^8\oplus 9D^9\oplus D^{10})$

(2)

但し，D の指数は $\bmod L$ とする．

いま，右へ1桁移動する（本論文では以後 $p=1$ とする）場合，(1) 式の演算を次々に行うと第1表のようになる．第1表において，$a_{L-1}=a$，$b_{L-1}=b$ および D と a，D と b とはそれぞれ可換であるものとする．ここで，L ビットの乱数列 $X_0, X_1, X_2, \cdots$ は最右側桁がわかると，それに $D, D^2, \cdots, D^{L-1}$ を乗ずることによって他の桁が導き出される．そこでいま，最右側桁だけの演算過程を求めると，第2表のようになる　ここで作用子Dの係数に注目すると，一般に最右側桁の i 番目 ($i=0, 1, 2, \cdots$) の値 B_i は (3) 式で示される．(第2表において係数に mod 2 の演算を行うと，偶係数は 0，奇係数は1となる．)

$$B_i=\sum_{K=1}^{\left\lceil\frac{i+1}{2}\right\rceil} a\binom{i+1-K}{i+1-(2K-1)}\bmod 2 \times D^{i+1-(K-1)\bmod L} \oplus \sum_{K=1}^{\left\lfloor\frac{i+1}{2}\right\rfloor+1} b\binom{i+1-(K-1)}{i+1-2(K-1)}\bmod 2. \times D^{i+1-(K-1)\bmod L} \quad (3)$$

但し，$\binom{m}{l}$：2項係数　$m\geq l\geq 0$，

$\lceil x\rceil$：x より大きい最小の整数，

$\lfloor x\rfloor$：x より小さい最大の整数．

B_i が求められると，L ビットの i 番目の乱数 X_i は (4) 式のように示される．

$$X_i=\{B_i\}. \quad (4)$$

例として，$L=5$，$X_{-2}=\{a\}=00011$，$X_{-1}=\{b\}=01101$ のとき X_4 を求めるとすると，(3) 式から

$$B_4=\sum_{K=1}^{3} a\binom{5-K}{5-(2K-1)}\bmod 2 \times D^{5-(K-1)\bmod 5} \oplus \sum_{K=1}^{3} b\binom{5-(K-1)}{5-2(K-1)}\bmod 2 \times D^{5-(K-1)\bmod 5} \quad (5)$$

となる．ここで (2) 式を用いると，$\{aD^0\}\oplus\{aD^4\}\oplus\{aD^3\}=0001\oplus 00110\oplus 01100=01001$，　$\{bD^0\}\oplus\{bD^3\}=01101\oplus 10101=11000$，ゆえに $X_4=\{B_4\}=01001\oplus 11000=10001$ となる．

なお，L ビットの乱数列が周期 n をもつとすると，$\{B_{n+i}\}=\{B_i\}$ が成り立つことがわかる．

3. 初期値の類別による周期

この乱数発生法では2つの初期値が必要であるが，一方はビット内全てが0である $\{0\}$ とし，他方は任意の数 $\{b\}$ をとることにする．($\{0\}$ をとる理由は乱数列中に $\{0\}$ が来ると，その前2つの乱数は同じものであり，乱数列として好ましくないからである．なお，

Table 3 The random number sequences for the starting values of ($\{0\}$, $\{b\}$), ($\{0\}$, $\{bD\}$),…

乱数列 ＼ 初期値	$\{0\}$, $\{b\}$	$\{0\}$, $\{bD\}$	$\{0\}$, $\{bD^2\}$	$\{0\}$, $\{bD^3\}$
X_0	$\{bD\}$	$\{bD^2\}$	$\{bD^3\}$	$\{bD^4\}$
X_1	$\{bD\}\oplus\{bD^2\}$	$\{bD^2\}\oplus\{bD^3\}$	$\{bD^3\}\oplus\{bD^4\}$	$\{bD^4\}\oplus\{bD^5\}$
X_2	$\{bD^3\}$	$\{bD^4\}$	$\{bD^5\}$	$\{bD^6\}$
X_3	$\{bD^3\}\oplus\{bD^3\}\oplus\{bD^4\}$	$\{bD^3\}\oplus\{bD^4\}\oplus\{bD^5\}$	$\{bD^4\}\oplus\{bD^5\}\oplus\{bD^6\}$	$\{bD^5\}\oplus\{bD^6\}\oplus\{bD^7\}$

後に述べる副周期をもつ $L=5, 11, 13, 19$ ビット以外の L ビット ($L\leq 25$) では初期値 (0, 1) のときには {0} が途中現われないことが確かめられている.) このとき $\{b\}$ を桁移動してできる $\{bD\}$, $\{bD^2\}$, … などを初期値とした L ビットの乱数列は第3表で表わされる.

第8表で, 初期値 ($\{0\}$, $\{bD\}$), ($\{0\}$, $\{bD^2\}$), … などの乱数列は初期値 ($\{0\}$, $\{b\}$) の乱数列にそれぞれ D, D^2, … を乗じたものであり, 本質的な違いがないことがわかる. すなわち, $\{b\}$ は $\{bD\}$, $\{bD^2\}$, … などの代表と考えてよい. そこでいま, L ビットで表わされる全ての数, すなわち $0, 1, 2, \cdots, 2^L-1$ の数の集合を桁移動しても本質的に変らない(例えば, 0011 と 0110 とは単に桁移動だけのちがいであり, 本質的に変らないものと考える) 同値類に分割し, その同値類の代表を $\{b\}$ とすることにより, 同値類の個数だけ互に無縁な乱数列ができる. 同値類をつくるには次の通りである. まず1から 2^L-2 までの整数 (ここで0と 2^L-1 とを $\{b\}$ にとるのは無意味であるから除く) のうち, $1, 2, 4, \cdots, 2^{L-1}$ は L 個の元をもった部分群を形成するので, これに 2^L-1 を法として他の元を乗ずることによって剰余類をつくることができる. この剰余類がここでの同値類に一致する. 例として, $L=4$ のとき 0001, 0011, 0111, 0101 を代表とする同値類 C_0, C_1, C_2, C_3 はそれぞれ

C_0: 1　2　4　8
C_1: 3　6　12　9
C_2: 7　14　11　13
C_3: 5　10

となるが, これはまず $2^4-1=15$ を法として C_0 に C_0 にない数3を乗じて C_1 をつくり, 次に C_0 に C_0, C_1 にない数7を乗じて C_2 を, C_0 に C_0, C_1, C_2 にない数5を乗じて C_3 を各々つくる. こうして4ビットの場合の同値類がつくられる (他のビットの場合も同様にしてつくることができる) が, 同じ同値類に属する全ての数は桁移動することによって互に同値になることがわかる. 次に, これらの同値類をつくるのに, その個数がいくらあるのかが知られていると便利である. そこで, 同値類の個数 (すなわち, 互に無縁な乱数列の個数) $Z(q)$ は $2^L-1=q$ の関数として次式で与えられる[2].

$$Z(q)=\frac{1}{L}\sum_{i=1}^{L}\left[2^{(i,L)}-1\right]-1$$
$$=\left[\frac{1}{L}\sum_{d\backslash L}\phi(d)2^{L/d}\right]-2. \qquad (6)$$

Table 4 The number of equivalence classes as a functionof q.

L	q	$Z(q)$
2	2	1
3	7	2
4	15	4
5	31	6
6	63	12
7	127	18
8	255	34
9	511	58
10	1023	106
11	2047	186
12	4095	350
13	8191	630
14	16383	1180
15	32767	2190

但し, (i, L) は i と L との最大公約数,
$d\backslash L$ は d が L の約数,
$\phi(d)$ はオイラー関数.

これを第4表に表わす.

なお, 同値類に属するどの数をとっても代表になりうるが, 第5表では初期値 $\{b\}$ として, その中の最小値を代表 (2進数パターンを示すため8進数を使っている) とし, そのときの周期 (10進数) を L が2ビットから11ビットまでのものについて表わしている. 第5表の中にはいろいろな短周期が存在しているが, その短周期の発生する条件について例をあげて説明する.

例1　5ビット, 11 ビットには2種類の周期がある.

いま, 奇, 偶は L ビットのうち1の状態のビットの個数がそれぞれ奇数個, 偶数個を意味するものとする. このとき5ビットの周期が85と11ビットの周期が11275となる初期値は偶と偶とのときである. すなわち,

$\{a\}\oplus\{aD\}\oplus\cdots\oplus\{aD^{L-1}\}=\{0\}$,
$\{b\}\oplus\{bD\}\oplus\cdots\oplus\{bD^{L-1}\}=\{0\}$.

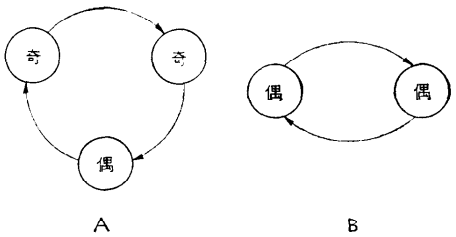

Fig. 1 The properties of the random number sequences

Table 5 The period for the representatives of the equivalence class of L bit from 2 to 11

初期値(8進)		周期(10進)	初期値(8進)	周期(10進)	初期値(8進)	周期(10進)	初期値(8進)	周期(10進)	初期値(8進)	周期(10進)
2 bit	1	6	35	24	137	315	127	510	667	510
3 bit	1	15	37	24	147	315	131	510	677	170
	3	15	45	24	153	63	133	510	737	510
4 bit	1	12	47	24	155	315	135	510	757	85
	3	12	53	24	157	315	137	170	777	510
	5	6	55	24	165	315	143	85		
	7	12	57	24	167	63	145	510	11 bit 1	33825
5 bit	1	255	63	12	173	315	147	510	3	11275
	3	85	65	24	175	315	151	170	5	11275
	5	85	67	24	177	315	153	510	7	33825
	7	255	73	24	253	315	155	510	11	11275
	13	255	75	24	257	63	157	510	13	33825
	17	85	77	24	267	315	163	510	15	33825
6 bit	1	30	125	6	277	315	165	510	17	11275
	3	30	127	24	327	315	167	170	21	11275
	5	30	133	24	333	15	171	510	23	33825
	7	30	137	24	337	63	173	510	25	33825
	11	15	157	24	357	315	175	170	27	11275
	13	30	167	12	377	315	177	510	31	33825
	15	30	177	24			223	170	33	11275
	17	30			10 bit 1	510	225	510	35	11275
	25	6	9 bit 1	315	3	510	227	510	37	33825
	27	30	3	315	5	170	233	510	41	11275
	33	15	5	315	7	510	235	510	43	33825
	37	30	7	63	11	510	245	85	45	33825
7 bit	1	63	11	63	13	510	247	510	47	11275
	3	63	13	315	15	510	253	510	51	33825
	5	63	15	315	17	170	255	510	53	11275
	7	63	17	315	21	170	257	170	55	11275
	11	63	21	315	23	510	263	510	57	33825
	13	63	23	315	25	510	265	510	61	33825
	15	21	25	63	27	510	267	510	63	11275
	17	63	27	315	31	510	275	510	65	11275
	25	63	31	315	33	170	277	510	67	33825
	27	7	33	63	35	510	315	510	71	11275
	31	63	35	315	37	510	317	510	73	33825
	33	63	37	315	41	255	325	510	75	33825
	35	63	43	63	43	510	327	170	77	11275
	37	63	45	315	45	510	331	510	103	33825
	53	63	47	315	47	170	333	510	105	33825
	57	63	51	315	51	510	335	170	107	11275
	67	63	53	315	53	510	337	510	111	33825
	77	63	55	63	55	170	347	255	113	11275
8 bit	1	24	57	315	57	510	353	170	115	11275
	3	24	63	315	61	510	355	510	117	33825
	5	24	65	315	63	170	357	510	121	11275
	7	24	67	315	65	510	365	170	123	11275
	11	24	71	315	67	510	367	510	125	11275
	13	24	73	315	71	170	371	510	127	33825
	15	24	75	315	73	510	373	510	131	11275
	17	24	77	63	75	510	375	510	133	33825
	21	12	111	15	77	510	377	170	135	33825
	23	24	113	315	105	510	525	6	137	11275
	25	24	115	315	107	510	527	510	143	11275
	27	24	117	63	111	510	537	510	145	11275
	31	24	123	63	113	170	553	255	147	33825
	33	24	125	315	115	510	557	510	151	11275
			127	315	117	510	567	510	153	33825
			133	315	123	510	573	510	155	33825
			135	63	125	170	577	510	157	11275

Table 5 (Cont'd). The period for the representatives of equivalence class of L bit from 2 to 11.

初期値 (8進)	周期 (10進)	初期値 (8進)	周期 (10進)	初期値 (8進)	周期 (10進)	初期値 (8進)	周期 (10進)	初期値 (8進)	周期 (10進)
161	11275	265	33825	371	11275	557	33825	757	11275
163	33825	267	11275	373	33825	563	11275	765	33825
165	33825	271	33825	375	33825	565	11275	767	11275
167	11275	273	11275	377	11275	567	33825	773	11275
171	33825	275	11275	445	11275	573	33825	775	11275
173	11275	277	33825	447	33825	575	33825	777	33825
175	11175	307	33825	453	33825	577	11275	1253	11275
177	33825	311	11275	455	33825	633	11275	1257	33825
211	33825	313	33825	457	11275	635	11275	1267	33825
213	11275	315	33825	463	33825	637	33825	1273	33825
215	11275	317	11275	465	33825	647	11275	1277	11275
217	33825	323	33825	467	11275	653	11275	1333	33825
223	11275	325	33825	473	11275	655	11275	1337	11275
225	11275	327	11275	475	11275	657	33825	1357	11275
227	33825	331	33825	477	33825	665	11275	1367	11275
231	11275	333	11275	513	33825	667	33825	1373	11275
233	33825	335	11275	515	33825	672	33825	1377	33825
235	33825	337	33825	517	11275	675	33825	1557	11275
237	11275	345	33825	523	33825	677	11275	1567	11275
243	11275	347	11275	525	33825	717	33825	1577	33825
245	11275	351	33825	527	11275	725	11275	1677	33825
247	33825	353	11275	533	11275	727	33825	1737	33825
251	11275	355	11275	535	11275	733	33825	1777	11275
253	33825	357	33825	537	33825	735	33825		
255	33825	363	11275	547	11275	737	11275		
257	11275	365	11275	553	11275	753	33825		
263	33825	367	33825	555	11275	755	33825		

が成り立つときである．なお，乱数列の性質として初期値に偶と偶とをとると，発生される乱数は第1図のBのように常に偶となる．また，他の場合はAのような構成の乱数列となる．このことは L ビットにおいて次のように証明される．

[証明] 1ビットの場合の⊕演算の全ての組合せは 0⊕0, 0⊕1, 1⊕0, 1⊕1 の4通りであり，L ビットのときはこれらの集合からなるが，結果が1となるのは {0⊕1, 1⊕0} の演算の場合のみによる．いま，L ビットにおいて偶と偶との⊕演算では {1⊕1} の演算回数が偶数でも奇数でも，{0⊕1, 1⊕0} の演算回数は偶数であるから偶となることがわかる．同様に，偶と奇または奇と奇との⊕演算では {1⊕1} の演算回数が偶数・奇数のいずれでも，前者は奇となり，後者は偶となる．ここで第1図のAとBとを比較してみると，Aの方がBよりも乱数列を構成する数が全てにわたっている理由で好ましいと言える．

例 2 L が偶数のときには周期=6 がある．

一般に $\{B_{6+i}\}=\{B_i\}$ を満足する条件を求めると，a, b ともに $D^K=D^{K+2}=D^{K+4}=\cdots$．但し，$K=0$, 1 となり，これらを満足する $\{a\}$, $\{b\}$ の初期値のとき周期は6となる．

例 3 L が9ビットのときに周期=15 がある．いま，$\{a\}$, $\{b\}$ を mi 桁とすると，

$$\{a\}=((D^{(m-1)i+i-1}a,\ D^{(m-1)i+i-2}a,\ \cdots,\ D^{(m-1)i}a),\ (D^{(m-2)i+i-1}a,\ D^{(m-2)i+i-2}a,\ \cdots,\ D^{(m-2)i}a),\ \cdots,\ (D^{i-1}a,\ D^{i-2}a,\ \cdots,\ D^0a)), \quad (7)$$

但し，$a=a_{(m-1)i+i-1}$

となる．ここで $D^Ka=D^{i+K}a=\cdots=D^{(m-1)i+K}a$，但し，$K=0, 1, 2, \cdots, i-1$ を満足するとき，これは m 重対称と言われる[2]．

このとき $\{a\}=((D^{i-1}, a\,D^{i-2}a, \cdots D^0a), (D^{i-1}a, D^{i-2}a, \cdots, D^0a), \cdots, (D^{i-1}a, D^{i-2}a, \cdots, D^0a))$ となる．（$\{b\}$ は $\{a\}$ と全く同様に成り立つものとする．）明らかに，mi 桁の初期値 ($\{a\}$, $\{b\}$) の周期は i 桁の初期値 $((D^{i-1}a, D^{i-2}a, \cdots, D^0a), (D^{i-1}b, D^{i-2}b, \cdots, D^0b))$ の周期に一致する．9ビットの初期値 $(0, 111_8)$ は3重対称であり，3ビットの初期値 $(0, 1_8)$ の周期 (=15) に等しいことがわかる．

例 4 9ビットのときの周期=63 となるのは $\{B_{63+i}\}=\{B_i\}$ より，a, b ともに次式を満足するときである．

$$D^K(D^0\oplus D^2\oplus D^3\oplus D^5\oplus D^6\oplus D^8)=0. \quad (8)$$

但し，$K=0, 1, 2$.

例 5 7ビットのときの周期=7 となるのは $\{B_{7+i}\}=\{B_i\}$ より，a，b ともに次式を満足するときである．

$$D^K(D^0\oplus D^4\oplus D^6)=0. \qquad (9)$$

但し，$K=0, 1, \cdots, 6$.

例 6 10ビットにおける周期=170 となるのは $\{B_{170+i}\}=\{B_i\}$ より，a，b ともに

$$\begin{cases} D^0\oplus D\oplus D^2\oplus D^3\oplus D^4\oplus D^5 \\ \quad\oplus D^6\oplus D^7\oplus D^8\oplus D^9=0, \\ D^K(D^0\oplus D^2\oplus D^4\oplus D^6\oplus D^8)=0, \end{cases} \qquad (10)$$

但し，$K=0, 1$

の両式を満足するときである．

4. 副 周 期

第6表に 25 ビットまでの最大周期と副周期とを表わしているが，ここでいう副周期とは普通の周期のように全く同じ数がくりかえし出現することではなくて，適当な桁移動を行うと互に同値となるような相関性をもった周期のことである．

25ビットまでには 5, 11, 13, 19 の各ビットにそれぞれビット数と同じ回数だけの副周期が1周期内にある．10, 22ビットにも副周期はあるが，これはそれぞれ 5, 11 ビットの副周期の2倍になっているもので，桁が2倍になると周期も2倍になるという性質による

Table 6 The maximum periods and the sub-periods of $L=2$ to 25.

L	最 大 周 期	副 周 期 A (B)
2	6	6
2	15	15
4	12	12
5	255	51 (17)
6	30	30
7	63	64
8	24	24
9	315	315
10	510	102 (34)
11	33825	3075 (1025)
12	60	60
13	159783	12291 (4097)
14	126	126
15	255	255
16	48	48
17	65535	65535
18	630	630
19	14942265	786435 (262165)
20	1020	204 (68)
21	4095	4095
22	67650	6150 (2050)
23	4194303	4194303
24	120	120
25	17825775	17825775

($L\leq 25$)．その他の場合，副周期は最大周期に一致する．

副周期の例として，5ビットの場合には第7表のようにして周期を完了する．

Table 7 The random number sequences of 5 bit having the sub-periods of 17 and 51

乱数列の番号 i	5 ビ ッ ト の 乱 数 列
−2	$\{a\}$
−1	$\{b\}$
15	$\{aD\}\oplus\{b\}\oplus\{bD\}\oplus\{bD^2\}\oplus\{bD^3\}\oplus\{bD^4\}$
16	$\{a\}\oplus\{aD\}\oplus\{aD^2\}\oplus\{aD^3\}\oplus\{aD^4\}\oplus\{b\}\oplus\{bD^2\}\oplus\{bD^3\}\oplus\{bD^4\}$
32	$\{a\}\oplus\{aD\}\oplus\{aD^3\}\oplus\{aD^4\}\oplus\{b\}\oplus\{bD\}\oplus\{bD^2\}\oplus\{bD^3\}\oplus\{bD^4\}$
33	$\{a\}\oplus\{aD\}\oplus\{aD^2\}\oplus\{aD^3\}\oplus\{aD^4\}\oplus\{bD^2\}$
49	$\{aD^3\}$
50	$\{bD^3\}$
66	$\{aD^4\}\oplus\{b\}\oplus\{bD\}\oplus\{bD^2\}\oplus\{bD^3\}\oplus\{bD^4\}$
67	$\{a\}\oplus\{aD\}\oplus\{aD^2\}\oplus\{aD^3\}\oplus\{aD^4\}\oplus\{b\}\oplus\{bD\}\oplus\{bD^2\}\oplus\{bD^3\}$
83	$\{aD\}\oplus\{aD^2\}\oplus\{aD^3\}\oplus\{aD^4\}\oplus\{b\}\oplus\{bD\}\oplus\{bD^2\}\oplus\{bD^3\}\oplus\{bD^4\}$
84	$\{a\}\oplus\{aD\}\oplus\{aD^2\}\oplus\{aD^3\}\oplus\{aD^4\}\oplus\{b\}$
100	$\{aD\}$
101	$\{bD\}$
151	$\{aD^4\}$
152	$\{bD^4\}$
202	$\{aD^2\}$
203	$\{bD^2\}$
253	$\{a\}$
254	$\{b\}$

第7表において，$\{a\}\oplus\{aD\}\oplus\cdots\oplus\{aD^4\}=\{0\}$，$\{b\}\oplus\{aD\}\oplus\cdots\oplus\{bD^4\}=\{0\}$ のとき，すなわち，第1図のBの場合のみ副周期は 17 であり，Aの場合には副周期は 51 であることがわかる．また，副周期をもつ 11, 13, 19 の各ビットの場合にも副周期 (n') はAの場合 $\{B_{n'+i}\}=\{D^3B_i\}$，Bの場合 $\{B_{n'+i}\}=\{DB_i\}$ を満足したものであることが確かめられる．なお，副周期をもつ L ビットにおいて周期は初期値 (0, 0) と $(0, 2^L-1)$ のとき（周期はそれぞれ 1, 3 である）を除くと，2通りだけである．（但し，$L\leq 25$.）

［証明］ 一般に L ビットにおいて，

$$\sum_{K=0}^{\left[\frac{L}{2}\right]}\binom{L}{2K}=\sum_{K=0}^{\left[\frac{L-1}{2}\right]}\binom{L}{2K+1} \qquad (11)$$

が成立する．すなわち，偶と奇との個数が等しい．そこで，例えば5ビットの場合における2つの数の可能な組は初期値が (0, 0) と $(0, 2^5-1)$ の場合を除けば $2^5\times 2^5-4=1020$ である．次に，初期値の一方を 0，他方を 1, 2, …, 2^5-2 の数をとると，(0, 偶) の周期は 85，(0, 奇) の周期は 255 で各々周期内に5回の副周期があるから，(0, 偶) を初期値とした場合に使われる組は全部で $\frac{2^5-2}{2}\cdot\frac{85}{5}=255$ であり，(0, 奇) では $\frac{2^5-2}{2}\cdot\frac{255}{5}=765$ となり，合わせて 1020 となるので，5ビットの場合には周期が 85 と 255 以外ないことがわかる．他の副周期をもつ 11, 13, 19 の各ビットの場合も同様に確かめられる．次に，この副周期間の相関図を書く．

整乱数列 $\{X_0, X_1, \cdots\}$ と $\{X_{n'+0}, X_{n'+1}, \cdots\}$ とをそれぞれ実乱数列 $\{x_0, x_1, \cdots\}$ と $\{y_0, y_1, \cdots\}$ に変換し，さらに正規化して $\left\{\frac{x_0}{m}, \frac{x_1}{m}, \cdots\right\}$ と $\left\{\frac{y_0}{m}, \frac{y_1}{m}, \cdots\right\}$ との相関関係を第2図に示す．但し，$m=2^L$ である．第2図で座標 $\left(\frac{x_i}{m}, \frac{y_i}{m}\right)$ が直線上のみにあり，相関性がみられるので副周期と名づけたのである．従って，副周期の存在する乱数を用いることは好ましくないと思われる．

5. あとがき

以上，高速乱数発生法についての 2, 3 の性質について述べてきたが，乱数として採用できるのは周期の比較的長い 11, 13, 17, 19, 22, 23, 25 の各ビットであり，このうち副周期をもつ 11, 13, 19 の各ビットのうち 19 ビットは十分長い副周期をもつので好ましいが，11, 13 の両ビットは副周期が短いので，好ましくないと思われる．残りの 17, 22, 23, 25 の各ビットについては，いまのところ性質がはっきりしないが，25 ビットには5重対称となる初期値があるので気をつける必要がある．次に，ここでは乱数の検定について述べられなかったが，文献 1) では自己及び相互相関関数，$\chi 2$ 乗検定などを行い，十分良好であると報告しているが，11, 13 ビット（副周期をもつ）や 17 ビットについてだけなので，他のビットについて検定する必要がある．今後の問題としては，周期の理論式を求めること，無縁な乱数列の特徴を調べること，またビットが2倍になると周期が2倍になる証明など未解決のものがある．なお，この発生法が普通の方法と比較して高速な点は発生アルゴリズムにのっと

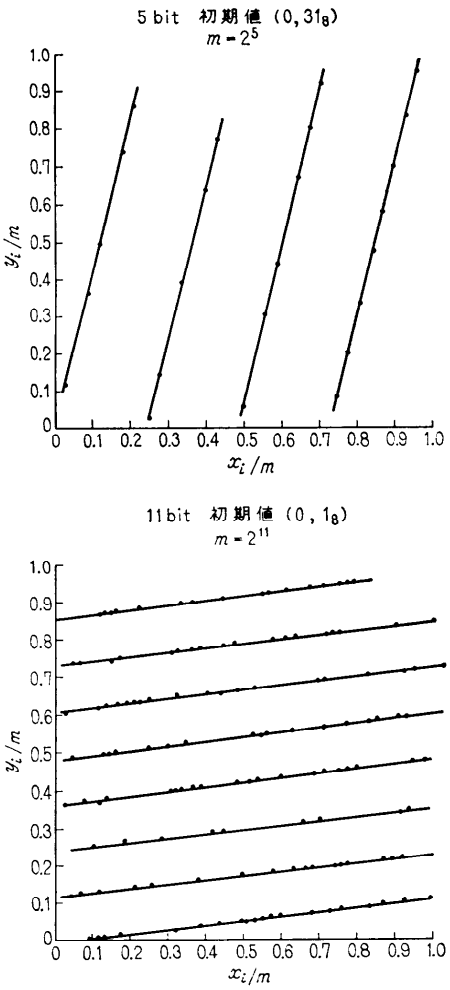

Fig. 2 Correlation diagram

ってハード上で実さいに回路をつくることにある．従って，ソフトウェア上で普通の方法と比較しても，それほど高速にはならない．（釧路高専 NEAC-3200 アセンブラーでワードサイズで mod をとった混合合同法とこの方法との 1 個の乱数発生時間は前者は 32.0 μs，後者は 16.8 μs である．）

終りに，当研究は著者の一人が室蘭工大で文部省の昭 46 年度情報処理関係内地研究員として留学中に行われたもので，これに関して便宜を下された釧路高専坂元義男校長に対して深く感謝する．また，研究の便宜を戴いた室蘭工大電子工学科，プログラム上で助言を下された山本伸宣技官に深く感謝する．なお，計算機は北海道大学大型計算機センター FACOM 230-60 および室蘭工大電子工学科 FACOM 270-20 を使用した．

参考文献

1) C. M. Rader, L. R. Rabiner and S. W. Scwafer: A fast method of generationg digital random number. Bell System Tech. J. Vol. 148, Nov. 1970, pp. 2303～2310.
2) Golomb, S. W.: Shift Register Sequences. Holden-Day, San Francisco, 1967.
3) Knuth: The art of Computer Programming. Vol. 12, Seminumerical algorithms. Addison Wesley, 1969.
4) 森山・北村・山本：電気四学会北海道支部連合大会 昭和 46.

(昭和 47 年 4 月 26 日 受付)
(昭和 47 年 7 月 14 日 再受付)