ショート・ノート

高速乱数の2,3の性質について*

森山純臣** 北村正一***

1. まえがき

C. M. Rader 等の考案した乱数発生法[1]については2, 3の発表があるが[2),3)]，ここではまず，簡単に途中の2項が求められること，次に，L ビットの乱数の各ビットがすべて0である {0} やすべて1である {1} を含む数列はある性質をもつので，これらを含まない数列を求めるための方法とその一例を示している．また，いくつかの検定を行ない，特に3次元の逐次検定では特有の性質をもつことがわかった．

なお，必要な言語・記号等は文献 2) を参照されたい．

2. 発生理論

L ビットの2進乱数 X_i の発生アルゴリズムは(1)式によって示される．

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

ただし，T_p: P 桁移動 (cyclic rotation), $\oplus$: 排他的論理和，$i=0,1,2,\cdots$.

また，作用子 $D(D^k a_m = a_{m-k})$ を用いて，初期値 $X_{-2}=\{a\}$, $X_{-1}=\{b\}$ のとき(2)式のようにも示される[2)]．

$$X_i = \{B_i\}. \qquad (2)$$

ただし，

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

ここで，$L=23$, $P=1$ のとき $i=2^j-1$, 2^j-2 ($j=1,2,\cdots$) の B_i 列は表1となる．表1を用いて，任意の連続した2項，たとえば X_{22}, X_{23} は乱数列が0番から始まっているので 23 に1を加え，$24=2^4+2^3$ と分解し，まず 2^4-1, 2^4-2 を求め，これらをおのおの新しい a, b として 2^3-1, 2^3-2 を求めると，X_{22}, X_{23} となり求められる．

こうして途中の2項が知れると，周期の長い数列の検定を行なう場合に便利であろう．

3. 初期値の性質

合同法では最大周期をもつとき mod 内の数が必ず1個出現するため初期値をどのように選ぼうと構わないが，この方法では初期値 ($\{a\}$, $\{b\}$) により性質の異なった乱数列ができる．

図1(a)で {0} をさかいにしてサイクリックに桁移動 $1(\bmod L)$, $2(\bmod L)$, …とすることにより，前半の $D, D^2, D^2D^3, \cdots$ は後半の $D^0, D^0, DD^0, \cdots$ となり，桁移動 $0(\bmod L)$ では同じ数となることがわかる．

(b)図の {1} の場合も(a)図から容易につくり出すことができる．そこでこのような性質をもたない数列すなわち {0} や {1} を含まない数列を求めるためには同値類 $C_0, C_1, C_2, \cdots$ の代表を $\{a\}$, $\{b\}$ とし，これらの組合せから求めることができる．

例として，$\{a\}=\underbrace{0\cdots01}_{L}$, $\{b\}=\underbrace{0\cdots011}_{L}$ とすると，$\{bD^k\}$ は(3)式のように表わされる．

$$\{bD^{k \bmod L}\} = \{aD^{k \bmod L}\} \oplus \{aD^{k+L-1 \bmod L}\}. \qquad (3)$$

ただし，$k=0,1,\cdots,L-1$.

こうして初期値を ($\{a\}$, $\{bD^k\}$) として，このとき数列中に {0} や {1} があるかどうか，すなわち a の係数が0か $D^0 \cdot D^1 \cdot \cdots \cdot D^{L-1}$ かを計算したのが表2である．周期の長い 23 ビットではどちらかが必ず存在するが，17 ビットの $k=11$ のみ，すなわち，$(\underbrace{0\cdots01}_{17}, \underbrace{0\cdots0110\cdots0}_{9\quad 6})$, $(\underbrace{0\cdots010}_{15}, \underbrace{0\cdots0110\cdots0}_{8\quad 7})$, … 等のときのみ {0}, {1} 両方とも存在しないことがわかる．

---

* On a Few Properties of the Fast Digital Random Number, 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子工学科
*** 室蘭工業大学電子工学科

Table 1 B_i column table of 23 bit (where D^2D^3 implies $D^2 \oplus D^3$)

乱数列の番号	a 列	b 列	乱数列の番号	a 列	b 列
2^1-2	D	D	$2^{12}-2$	$D^{19}D^{12}D^{13}D^{22}D^7D^{16}D^9D^{17}D^{21}D^0$	D
2^1-1	D^2	DD^2	$2^{12}-1$	D^2	$D^{19}D^{12}D^{13}D^{22}D^7D^{16}D^9D^{17}D^{21}D^0D^2$
2^2-2	D^2D^3	D^3	$2^{13}-2$	$D^{15}DD^{21}D^{14}D^9D^{18}D^{11}D^{19}D^0$	D^3
2^2-1	D^4	$D^2D^3D^4$	$2^{13}-1$	D^4	$D^{15}DD^{21}D^{14}D^9D^{18}D^{11}D^{19}D^9D^4$
2^3-2	$D^4D^6D^7$	D^7	$2^{14}-2$	$D^0D^2D^5D^{14}D^{22}D^{13}D^{15}D^{19}$	D^7
2^3-1	D^8	$D^4D^6D^7D^8$	$2^{14}-1$	D^8	$D^0D^2D^5D^{16}D^{22}D^{13}D^{15}D^{19}D^8$
2^4-2	$D^8D^{12}D^{14}D^{15}$	D^{15}	$2^{15}-2$	$D^0D^4D^{10}D^{13}D^{21}D^3D^7$	D^{15}
2^4-1	D^{16}	$D^8D^{12}D^{14}D^{15}D^{16}$	$2^{15}-1$	D^{16}	$D^0D^4D^{10}D^{13}D^{21}D^3D^7D^{16}$
2^5-2	$D^5D^9D^{16}DD^7$	D^8	$2^{16}-2$	$D^0D^{20}D^8D^{19}D^6D^{14}$	D^6
2^5-1	D^9	$DD^8D^9D^7D^{16}$	$2^{16}-1$	D^9	$D^0D^{20}D^8D^{19}D^6D^{14}D^9$
2^6-2	$D^{10}D^{16}D^9D^2D^4D^{17}$	D^{17}	$2^{17}-2$	$D^0D^6D^{15}D^{12}D^5$	D^{17}
2^6-1	D^{18}	$D^{10}D^{16}D^9D^2D^{14}D^{17}D^{18}$	$2^{17}-1$	D^{18}	$D^9D^6D^{16}D^{12}D^5D^{16}$
2^7-2	$D^{20}D^6D^{14}D^4D^5D^{11}D^{12}$	D^{12}	$2^{18}-2$	$D^6D^9DD^{10}$	D^{12}
2^7-1	D^{13}	$D^{20}D^9D^{15}D^4D^5D^{11}D^{12}D^{13}$	$2^{18}-1$	D^{13}	$D^9D^7DD^{16}D^{13}$
2^8-2	$D^{17}D^{18}D^{13}D^8D^{10}D^{21}DD^2$	D^2	$2^{19}-2$	$D^9D^{14}D^{20}$	D^2
2^8-1	D^3	$D^{17}D^{18}D^{13}D^8D^{10}D^{22}DD^2D^3$	$2^{19}-1$	D^3	$D^9D^{14}D^{20}D^3$
2^9-2	$D^{11}D^{13}D^3D^{16}D^{20}D^{21}D^2D^4D^6$	D^6	$2^{20}-2$	D^9D^{17}	D^5
2^9-1	D^6	$D^{11}D^{13}D^3D^{16}D^{20}D^{21}D^2D^4D^5D^6$	$2^{20}-1$	D^6	$D^9D^{17}D^6$
$2^{10}-2$	$D^{22}D^8D^9D^{17}D^{19}D^4D^8D^{10}D^{11}$	D^{11}	$2^{21}-2$	D^9	D^{11}
$2^{10}-1$	D^{12}	$D^{22}D^8D^9D^{17}D^{19}D^4D^8D^{10}D^{11}D^{12}$	$2^{21}-1$	D^{12}	D^9D^{12}
$2^{11}-2$	$D^{21}D^8D^{12}D^{18}D^{11}D^{15}D^8D^{14}D^{20}D^{22}D^9$	D^9	$2^{22}-2$	0	D^9
$2^{11}-1$	D	$D^{21}D^8D^{12}D^{18}D^{11}D^{15}D^8D^{16}D^{20}D^{22}D^9D$	$2^{22}-1$	D	D

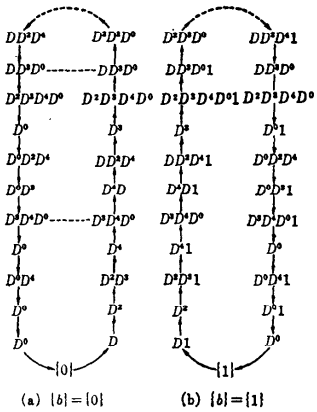

Fig. 1 B_i column of 5 bit

		ビット	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
3	15	{0}	○	○	○																				
		{1}	○	○	○																				
4	12	{0}	○	○																					
		{1}																							
5	255	{0}	○	○	○	○	○																		
		{1}	○	○	○	○	○																		
6	30	{0}	○	○																					
		{1}																							
7	63	{0}	○	○				○	○																
		{1}																							
8	24	{0}	○	○						○															
		{1}																							
9	315	{0}	○	○			○			○	○	○	○												
		{1}																							
10	510	{0}	○	○																					
		{1}																							
11	33825	{0}	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○								
		{1}	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○								
12	60	{0}	○	○																					
		{1}																							
13	159783	{0}	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○						
		{1}	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○						
14	126	{0}	○	○																					
		{1}																							
15	255	{0}	○	○																					
		{1}																							
16	48	{0}	○	○																					
		{1}																							
17	65535	{0}	○	○	○	○	○																		
		{1}						○	○	○	○	○	○	○	○	○	○	○	○						
18	630	{0}	○	○																					
		{1}																							
19	14942265	{0}	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			
		{1}	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○			
20	1020	{0}	○	○																					
		{1}																							
21	4095	{0}	○	○																					
		{1}																							
22	67650	{0}	○	○																					
		{1}																							
23	4194303	{0}	○	○			○			○			○			○			○			○			
		{1}			○			○			○			○			○			○			○		

Table 2 The existence of {0} or {1} of L bit from 3 to 23 when the initial values are ($\{a\}, \{bD^t\}$)

4. 検定

各検定で使用する記号として，$\langle U_i\rangle (=U_0, U_1, \cdots)$ は0と1の間の一様実乱数を意味し，$\langle Y_i\rangle (=\lfloor dU_i \rfloor$, ただし，$d$ は2の累乗) は0と d-1の間の一様整乱数を意味する．

(イ) 頻度検定：$\langle Y_i\rangle$ が任意の整数 $r (0 \leqq r < d)$ に等しくなる回数を数え，χ^2 検定を適用する．図2は17ビット，初期値 (1, 192) (このとき数列中に{0}や{1}がない) の場合の結果であり十分良好である．

(ロ) 逐次検定：連続した2個の乱数の組 (Y_{2i}, Y_{2i+1}) や3個の組 ($Y_{3i}, Y_{3i+1}, Y_{3i+2}$) などの頻度が一様かどうかみるのであるが，2個の場合は良好であったが，3個の場合次のことから一様性が言えないことがわかった．図3で x は0と1のどちらでもとり得るものとすると，$\langle Y_i\rangle$ は d の値により図のように分類される．いま，$d=4$ のとき $P=1$ で(1)式の演算を4-0と4-1の間で行なうと，$T_1(00x\cdots x \oplus 01x\cdots x) = x01x\cdots x$ となり，最左側桁の x が1のときは $101x\cdots x$ で4-2となり，x が0のときは $001x\cdots x$ となり4-0となる．したがって，4-1や4-3になり得ないことがわかる．次に $P=2$ とすると $T_2(00x\cdots x \oplus 01x\cdots x) = xx01x\cdots x$ となり左側2個の x は00, 01, 10, 11となり得るから $P=1$ とちがい3個の組のすべてがあらわれ得る．しかし $d=8$ とすると $P=2$ でも8-0と8-1との演算では，$T_2(000x\cdots x \oplus 001x\cdots x) = xx001x\cdots x$

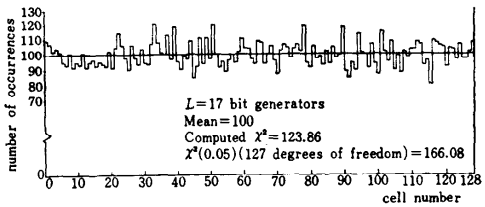

Fig. 2 Measured distribution for the Frequency test

となり，左側3桁目が0である8-0, 8-2, 8-4, 8-6のみしかならない．しかし，$d=8$ でも $P=3$ とするとやはり3個の組のすべてをとり得ることになる．こうして P はかぎられた値 ($P \simeq L/2$) であるから，一般に3次元の一様性が言えないことになる．

(ハ) 系列相関：これは乱数列の無規則性をみるため乱数相互間の依存度を評価するもので，系列相関係数 C_k は次式で示される．

$$C_k = N\sum_{i=0}^{N} U_iU_{i+k} - (U_0+U_1+\cdots+U_{N-1})^2 / N(U_0^2+U_1^2+\cdots+U_{N-1}^2) - (U_0+U_1+\cdots+U_{N-1})^2. \quad (4)$$

ただし，$k=1, 2, \cdots, N-1$.

C_k が $\mu_N - 2\sigma_N$ と $\mu_N + 2\sigma_N$ との間にあると望ましいといえる．ただし，$\mu_N = -1/(N-1)$, $\sigma_N = (1/(N-1))\cdot\sqrt{N(N-3)/(N+1)}$.

図4は $k=1$〜141 までの結果であり，十分良好であると思われる．

Table 3 Run test ($L=17$ bit)

連の長さ	期待値	初期値 (1, 192)								初期値 (98295, 49600)							
		$P=1$	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1	833.41	926	856	897	821	832	848	850	845	916	836	816	830	869	851	867	853
2	366.43	339	353	346	376	369	339	368	391	347	368	348	373	339	369	344	372
3	105.42	126	111	106	110	98	109	103	91	116	100	117	110	114	105	109	94
4	22.98	4	22	19	21	31	24	23	21	10	20	30	20	24	20	24	22
5	4.06	0	3	3	1	2	7	3	1	0	9	3	3	1	2	4	5
6	0.60	0	0	0	0	0	2	0	1	0	0	0	0	0	0	0	1
7	0.08	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
8	0.01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$X^2(0.05)$ 自由度 5	11.07	36.69	2.32	7.56	3.70	4.97	10.75	1.27	6.52	22.26	6.93	5.58	1.59	7.22	2.43	3.49	2.30

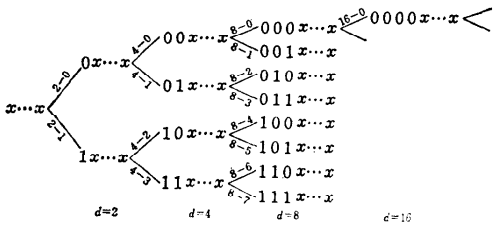

Fig. 3 The classification of the random number sequences

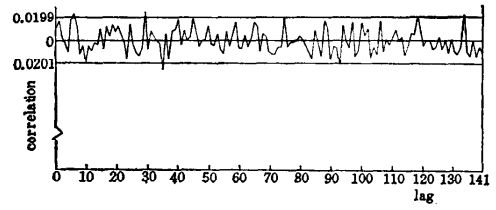

Fig. 4 Autocorrelation function of $L=17$ bit generator

(ニ) 連の検定：$\langle U_i \rangle$ があるとき，長さ r の上昇の連を $U_{i-1}>U_i<U_{i+1}<\cdots<U_{i+r}>U_{i+r+1}$ のように乱数が連続して r 回増加する場合として定義される．このとき乱数が N 個の場合の長さ r の連がおこる頻度は，

$$R=2N\cdot\frac{r^2+3r+1}{(r+3)!}-2\cdot\frac{r^3+3r^2-r-4}{(r+3)!}. \quad (5)$$

ただし，$r=1,2,\cdots,N-2$.

結果は表3であり，$P=1$ 以外は良好である．

5. あとがき

いろいろの検定を行なった結果，全体としては良好であるが，3次元の逐次検定では特有の性質をもち，$P=1$ のときの連の検定で不合格となった．したがって，これらの欠点のない拡張した発生式として $X_i=T_p(X_{i-1}\oplus X_{i-k})$，ただし，$k=2,3,\cdots$ が考えられる．($k=3$ のとき3次元の性質をもたないことが知られている．)

なお，計算機は北大大型計算機センター FACOM 230-60 を使用した．

参考文献

1) C. M. Rader et al.: Bell Syst. Tech. J., Vol. 48, pp. 2303～2310 (Nov. 1970).
2) 森山，北村：情報処理，Vol. 14, No. 1, pp.15～22 (Jan. 1973).
3) Sato: Publ. Res. Inst. Math. Sci. (Kyoto), To Appear.
4) Knuth: The Art of Computer Programming, Vol. 2, Addison Wesley, pp. 54～66 (1969).

(昭和48年12月27日受付)