GFSR 乱数の Asymptotic Randomness†

手塚 集††

最近，GFSR 乱数の k-distribution を理論的に保証する方法が確立された．ここでは，その考え方を発展させて，従来，使われてきた合同法との比較という観点から，GFSR 乱数の asymptotic randomness について述べる．さらに，実際的な場合について検討する．

1. はじめに

Monte Carlo 法等の simulation において乱数を使用するとき，その要求される精度 (resolution) は，その目的によりさまざまであり，まったく用途に依存している．したがって，任意の resolution に対し，k-distribution が保証されていることが望ましい．

通常，われわれが使う算術的な乱数は周期をもつ．その周期を M としたとき，resolution の t bits と k-distribution の間には，

$$k=\lfloor \log_2 M^{1/t} \rfloor \tag{1.1}$$

なる関係がある．たとえば $M=2^{30}, t=10$ bits とすれば $k=3$ つまり，3次元まで一様性の保証された乱数を作ることが，理論的には可能となるのである．k は t によって決まるわけだから，それぞれの t に対し，k-distribution を保証することが問題となる．

Tootill ら[9] は，以前，Tausworthe 列[8] に対して，上のような要求をみたす列を考え，asymptotially random な列と呼んだ．その後，Tausworthe 列にかわって，より簡便に発生できるよう，原始3項式を使って改良した GFSR (Generalized Feedback Shift Register) 法[6] が広く使われるようになってきている．

最近，その方法で発生される乱数列の k-distribution を理論的に保証する方法が確立された[3]．ここでは，それを発展させて，GFSR 乱数の asymptotic randomness について，従来から使われている合同法と比べながら，議論したい．

2. GFSR 乱数の Review

GF(2) 上の原始3項式を $f(D)=D^p+D^q+1\ (p>q)$ として，この式により生成される M 系列を $\{a_i\}$ で表す．また $A_i=(a_i a_{i+1}\cdots)$ として i 番目から始まる M 系列を表すことにする．

† The Asymptotic Randomness of GFSR Pseudorandom Numbers by SHU TEZUKA (Science Institute, IBM Japan Ltd.).

†† 日本アイ・ビー・エム(株)サイエンス・インスティチュート

[0, 1) 上の一様乱数 $\{u_i\}$ の上位 s bits の2進表現は，GFSR 乱数において

$$u_i=.a_{j_1+i}\ a_{j_2+i}\cdots a_{j_s+i} \tag{2.1}$$

と表すことができる．

こうすることにより，ビットごとの排他的論理和⊕を使えば，$\{u_i\}$ の生成多項式が $\{a_i\}$ の生成多項式と同じ形になり，

$$u_i=u_{i-p}\oplus u_{i-q} \tag{2.2}$$

となる．

このため，一様乱数を一つ発生するのに1回の演算(⊕)だけですむことになり，計算時間が非常に短縮される．当然，次に考えられることは，この方法により発生される列のランダム性であるが，それに関して理論的に調べたのが，文献3) である．ここでは，結果だけを簡単に述べる．

GFSR 乱数の周期は 2^p-1 であり，s bits 乱数では，

$$k=\lfloor p/s \rfloor \tag{2.3}$$

より，k-distribution まで理論的に保証できる．そのための必要十分条件が，次の式で表される行列 E の各行の線形独立性であることが証明された．

$$\begin{bmatrix} A_{j_1} \\ A_{j_1+1} \\ \vdots \\ A_{j_1+k-1} \\ A_{j_2} \\ \vdots \\ A_{j_s} \\ \vdots \\ A_{j_s+k-1} \end{bmatrix} = \begin{bmatrix} \\ \\ \boldsymbol{E} \\ \\ \\ \end{bmatrix} \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ \\ \\ \\ A_p \end{bmatrix} \tag{2.4}$$

今後，resolution の s bits を添字として E を E_s と書くことにする．また，この行列を s bits GFSR 乱数の生成行列，右辺の $(A_1, A_2, \cdots, A_p)$ をその reference と呼ぶことにする．

3. 簡単な例

(例 1) 合同法

現在でも，非常によく用いられているのが，

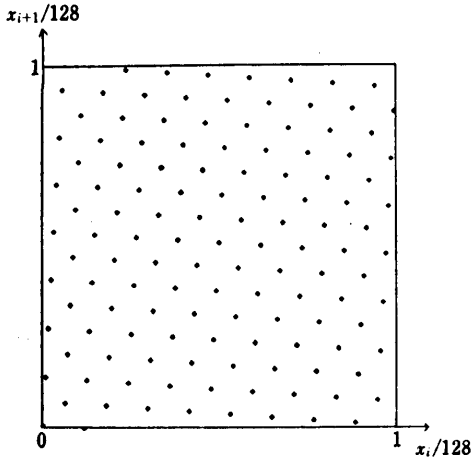

図 1 $x_{i+1}=17x_i+1 \pmod{128}$ によって生成される 2 次元の点列
Fig. 1 The points in 2-space generated by $x_{i+1}=17x_i+1 \pmod{128}$.

$$x_{i+1}=a\cdot x_i+c \pmod{M} \tag{3.1}$$

なる漸化式によって乱数を生成する合同法である．この方法は，かなり以前から理論的にその性質が調べられており[7]，よりよい性質の乱数をだすための a, c, M の値が具体的に求められている．

その方法として，代表的なのが Coveyou & MacPherson の Spectral test である[2]．$a=17$, $c=1$, $M=128$ に，この test を適用してみることにする（**図 1** 参照）．Knuth[5] に，この方法の定性的な解釈と説明があるので省略するが，これにより，合同法で発生した乱数の resolution をみることができる．実際に求めてみると

$$\log_2 \nu_2=\log_2\sqrt{128}=3.5$$
$$\log_2 \nu_3=\log_2\sqrt{6}=1.29$$
$$\log_2 \nu_4=\log_2\sqrt{4}=1$$

となる．ここで，ν_i は i 次元での accuracy である．

周期が $128=2^7$ であることから，それぞれ

$$\log_2 \nu_2 \geqq \lfloor 7/2 \rfloor=3$$
$$\log_2 \nu_3 \geqq \lfloor 7/3 \rfloor=2$$
$$\log_2 \nu_4 \geqq \lfloor 7/4 \rfloor=1$$

となることが望ましい．上の例では，3 次元に問題があるといえる．このようにして，与えられた合同法の性質を調べることができる．

（例 2） 次に，GFSR 乱数の例を二つ示す．例 1 との比較のため，周期は 1 違いの 127 となっている．例は文献 3) で用いたものである．原始 3 項式 $f(D)=D^7+D^4+1$ で生成行列は，

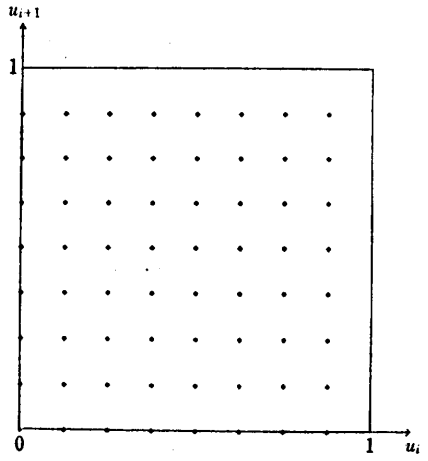

図 2 生成行列 E_3 により生成された点列
Fig. 2 The points in 2-space generated by the matrix E_3.

$$E_3=\begin{bmatrix}1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\1&0&1&0&0&0&0\\0&1&0&1&0&0&0\\1&0&0&0&1&0&0\\0&1&0&0&0&1&0\end{bmatrix} \tag{3.2}$$

となっている．E_3 は，各行線形独立なので，$\lfloor 7/3 \rfloor=2$-distribution が保証される．つまり，2 次元で resolution が 3 bits ということになる（**図 2** 参照）．

では，3 次元ではどうだろうか．$\lfloor 7/3 \rfloor=2$ より，上位 2 bits で調べると

$$E_2=\begin{bmatrix}1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&0&1&0&0&0&0\\1&0&1&0&0&0&0\\0&1&0&1&0&0&0\\0&0&1&0&1&0&0\end{bmatrix} \tag{3.3}$$

となる．見ればすぐわかるように，第 4 行目が，第 1 行目と第 3 行目の和になっている．したがって，E_2 は各行線形独立とはならない．いいかえれば，上位 2 bits では 3-distribution は成立しないわけで，resolution は 1 bit ということになる．

（例 3） 次のような生成行列を考えてみる．

$$E_7=\begin{bmatrix}1&0&0&0&0&0&0\\1&0&0&0&1&0&0\\1&0&1&0&0&0&0\\1&1&0&0&0&0&0\\1&0&0&1&0&0&0\\1&0&0&0&0&1&0\\1&0&0&0&0&0&1\end{bmatrix} \tag{3.4}$$

この行列が各行線形独立なのは容易にわかるので，$\lfloor 7/7 \rfloor = 1$-distribution がいえる．E_4, E_5, E_6 は同様なので E_3 を調べる．$\lfloor 7/3 \rfloor = 2$ より 2-distribution を調べる必要がある．

$$E_3=\begin{bmatrix}1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\1&0&0&0&1&0&0\\0&1&0&0&0&1&0\\1&0&1&0&0&0&0\\0&1&0&1&0&0&0\end{bmatrix} \tag{3.5}$$

となることから，2-distribution はいえる．E_2 は，

$$E_2=\begin{bmatrix}1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&0&1&0&0&0&0\\1&0&0&0&1&0&0\\0&1&0&0&0&1&0\\0&0&1&0&0&0&1\end{bmatrix} \tag{3.6}$$

となり，3-distribution はいえる．E_1 が各行線形独立になるのは，M系列そのものなので自明である．以上をまとめると，1次元：7 bits，2次元：3 bits，3次元：2 bits，4次元：1 bit の resolution が保証されたことになる．

初めにも述べたように，周期 M の乱数の場合，任意の t bits の resolution に対し，

$$k=\lfloor \log_2 M^{1/t} \rfloor \tag{3.7}$$

として，k-distribution をいう必要があるわけで，合同法との比較という意味でも，このことの重要性が強調されるのである．

4. 定義と応用例

(定義)

次の2条件を満たす GFSR 乱数を asymptotically random な s bits GFSR 乱数と呼ぶ．

条件1：生成行列 E_t が，任意の $t(\leqq s)$ に対し各行線形独立となる．

条件2：周期が素数となる．

1の意味は，前章の考察から明らかである．2について，付け加えれば，通常，k 次元のシミュレーションで乱数を使用する場合，一様乱数 u_i のオーバラップしない k 組 $(u_{kl}, u_{kl+1}, \cdots, u_{kl+k-1})$ を用いる．この列に対して k-distribution を保証するために必要となる[3),9)]．

前章の例3で扱ったものは，周期 2^7-1 が素数であることから，上の2条件を満たしている．したがって asymptotically random な 7 bits GFSR 乱数といえる．周期が素数となる原始3項式を**表1**にあげておく．詳しい表は 文献10),11)にある．

表 1 周期が素数となる原始3項式 $f(D)=D^p+D^q+1(p>q)$
Table 1 Primitive trinomiala whose degree is a Mersenne exponent.

p	q
7	1, 3
17	3, 5, 6
31	3, 6, 7, 13
89	38
127	1, 7, 15, 30, 63
521	32, 48, 158, 168
607	105, 147, 273

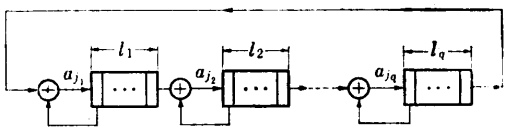

図 3 Arvillias and Maritsas の用いた toggle register
Fig. 3 Toggle register used by Arvillias and Maritsas.

4.1 Arvillias and Maritsas の方法[1)]

彼らは，$f(D)=D^p+D^q+1$ において，q が2のベキとなる，原始3項式を用い，各ビット間の位相遅れが $2^p/q$ の倍数となるような GFSR 乱数を提案した．その後，この方法の k-distribution を保証するための条件が与えられた[3)]．**図3**を使って，それを述べると $l_i \geqq \lfloor p/q \rfloor$ が条件であった．しかしこれは，q bits GFSR 乱数に対し k-distribution を述べたにすぎず，t $(<q)$bits に対する $k(=\lfloor p/t \rfloor)$-distribution つまり，asymptotic randomness は考慮されていない．以下，文献 3) で用いた例についてそれを調べてみることにする．上位 2 bits に対しては，$\lfloor 521/2 \rfloor = 260$-distribution まで理論的に保証できる可能性があるわけだが，生成行列 E_2 を求めてみると，第2位 bit を reference として，

$$E_2=\begin{bmatrix}(15)0&1&1&&(504)0\\(16)0&&1&1&(503)0\\&&\vdots&&\\(274)0&&&1&1\ (245)0\\1&(520)0&&&\\0\ \ 1&&(519)0&&\\&&\vdots&&\\(259)0&&&1&(261)0\end{bmatrix} \tag{4.1}$$

(ここで，$(n)0$ は n 個の0が続くことを示す) となる．すぐわかることは，$i=0,1,2,\cdots$ に対し

$$A_{j_1+i}=A_{j_2+16+i} \oplus A_{j_2+15+i} \tag{4.2}$$

なる関係が成立していることであり，$k>16$ では，

従属性が生じ k-distribution がいえなくなる．つまり，上位 2 bits でも 16-distribution しかいえない．同様の操作で $t \leqq 32$ に対し，調べていくと，結局すべて，16-distribution までしか成立しないことがわかる．したがって，この方法は asymptotically random ではないことになる．

4.2 Tootill ら[9]の方法

彼らは，$f(D)=D^{607}+D^{273}+1$ なる原始3項式を使い，decimation を 512 とした Tausworthe 列，つまり2進表現で表すと

$$u_i = a_{512\cdot i+1}\ a_{512\cdot i+2}\cdots a_{512\cdot i+S} \qquad (4.3)$$

なる列を考え，任意の t ($\leqq 23$)bits に対し $k(=\lfloor 607/t \rfloor)$ 個の引きつづいた列中の $t\cdot k$ bits が線形独立になることを computer search で調べた．伏見[4]によれば，$512=2^9$ であることから，この Tausworthe 列は，GFSR 乱数とみなすこともできる．

そうしてみると，上位 t (<23)bits に対し，k-distribution が成立しているわけで，条件1を満足している．また，$2^{607}-1$ は素数なので条件2をも満たす．したがって，この乱数は asymptotically random な 23 bits GFSR 乱数といえる．

5. 結　論

ここでは，GFSR 乱数の k-distribution を保証する方法を発展させて GFSR 乱数の asymptotic randomness について議論した．このことにより，同じ観点から合同法と GFSR 乱数を眺められることが示された．周期に関して付け加えれば，合同法では，その周期が計算機の語長により制限されるため，前章の GFSR 乱数と同じような周期を実現するには，多倍長整数演算が必要となる．また，GFSR 乱数でも現時点では，合同法でよりよい乗数を求める場合と同じく，asymptotically randomな生成行列を求めるには，exhaustive な computer search しかないので，このあたりが今後の課題となるであろう．

謝辞　本研究に対しご理解と励ましをいただいている音声認識/合成，金子担当に感謝いたします．

参考文献

1) Arvillias, A.C. and Maritsas, D.G.: Partitioning the Period of m-Sequences and Application to Pseudorandom Number Generation, *J. ACM*, Vol. 25, No. 4, pp. 675-686 (1978).
2) Coveyou, R.R. and MacPherson, R.D.: Fourier Analysis of Uniform Random Number Generators, *J. ACM*, Vol. 14, No. 1, pp. 100-119 (1967).
3) Fushimi, M. and Tezuka, S.: The k-Distribution of the Generalized Feedback Shift Register Pseudorandom Numbers, *Comm. ACM*, Vol. 26, No. 7, pp. 516-523 (1983).
4) 伏見正則：一様乱数の発生法，情報処理，Vol. 24, No. 4, pp. 367-371 (1983).
5) Knuth, D.E.: *The Art of Computer Programming*, Vol. 2, *Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, Mass. (1981)；渋谷政昭(訳)：準数値算法/乱数，サイエンス社，東京 (1981).
6) Lewis, T.G. and Payne, W.H.: Generalized Feedback Shift Register Pseudorandom Number Algorithms, *J. ACM*, Vol. 21, No. 3, pp. 456-468 (1973).
7) Marsaglia, G.: The Structure of Linear Congruential Sequences, in Zaremba, S.K. (ed.): *Applications of Number Theory to Numerical Analysis*, Academic Press, New York (1972).
8) Tausworthe, R.C.: Random Numbers Generated by Linear Recurrence Modulo Two, *Math. Comput.*, Vol. 19, pp. 201-209 (1965).
9) Tootill, J.P.R., Robinson, W.D. and Eagle, D.J.: An Asymptotically Random Tausworthe Sequence, *J. ACM*, Vol. 20, No. 3, pp. 469-481 (1973).
10) Zierler, N. and Brillhart, J.: On Primitive Trinomials (mod 2), *Inf. Control*, Vol. 13, No. 6, pp. 541-554 (1968).
11) Zierler, N. and Brillhart, J.: On Primitive Trinomials (mod 2) II, *Inf. Control*, Vol. 14, No. 6, pp. 556-569 (1969).

(昭和58年11月1日受付)
(昭和58年12月13日採録)