# GFSR 乱数のマトロイドによる表現†

手塚 集††

GFSR 乱数と従来からよく使われている合同法を理論的に比較しようとするとき，GFSR 乱数の asymptotic randomness を考える必要がある．ここでは，asymptotically random な GFSR 乱数の生成行列を求める問題をマトロイドを用いて表現し，それがよく知られているパリティ問題の一つになることを示す．

## 1. はじめに

算術的乱数として従来から広く使われているものに合同法がある．しかし，この方法は，周期が計算機の語長に制限されるという欠点をもっている．たとえば，単精度が32ビットの計算機では，語長をフルに使った合同法で，$2^{30}$〜$2^{32}$≒数ギガ程度の周期である．ところが，いまや，スーパコンピュータでは，1 GFLOPS という声も聞かれる時代であり，このような周期では，（まったく単純に計算すると）数秒で終わってしまうことになる．といって多倍長にして周期を増やすと発生時間がかかり問題である．その点，GFSR 乱数では，周期を計算機の語長によらずに決めることができ，またさらに，発生時間の点でも，ビットごとの排他的論理和演算1回で，1個の乱数がだせるため，演算時間に関し，合同法とほとんどかわらない[8]．

しかし合同法は，Lehmer 以来，30年余りにわたって使われてきた点と，経験的にはもちろんのこと，理論的にもよく調べられているという点で優位である．合同法乱数の性質を理論的に調べる方法として，最もよく知られているものに spectral test と呼ばれるものがある[1),7)]．この test を使うことにより，合同法乱数の各次元での resolution を計算することができ，その理論的な値との比較によって，乱数としての良否を判定することができる．

当然，GFSR 乱数に対しても，各次元における resolution を調べることが必要になるわけであって，われわれは，各次元において，その resolution が，理想的な値をもった GFSR 乱数のことを asymptotically random な GFSR 乱数と呼んだ[9]．

ここでは，そのような asymptotically random な GFSR 乱数を見つける問題を，マトロイドを用いて表現し，それが，この分野でよく知られているパリティ問題の一つになっていることを示す．パリティ問題は一般的な意味で，その問題のむずかしさがわかっている問題であるため，このような観点から，よりよい性質の GFSR 乱数を発生させる問題を眺めることには，意味があると思われる．

## 2. GFSR 乱数の review

### 2.1 $M$ 系列

GF(2) 上の $p$ 次の原始多項式

$$f(D)=1+c_1D+c_2D^2+\cdots+D^p \qquad (2.1)$$

を特性多項式とする漸化式

$$a_i=c_1a_{i-1}+c_2a_{i-2}+\cdots+a_{i-p} \pmod 2$$

を任意の初期条件 $(a_1, a_2, \cdots, a_p)\neq(0, 0, \cdots, 0)$ の下に解いて得られる系列 $\{a_i\}$ を $M$ 系列という．この系列の周期は $T=2^p-1$ となることが知られている．したがって $a_{i+p}=a_i$ となる．

$A_i=(a_i\ a_{i+1}\ \cdots)$ で $a_i$ から始まる $M$ 系列を表すことにすると，次のような性質が知られている[4),5)]．

性質 1. mod 2 の termwise addition（すなわち，$A_i+A_j=(a_i\ a_{i+1}\ \cdots)+(a_j\ a_{j+1}\ \cdots)=(a_i+a_j\ a_{i+1}+a_{j+1}\cdots)$）に関して，$A_i(i=0, 1, \cdots, 2^p-1)$ は加群をなす（ここで，$A_0=(0\ 0\ \cdots)$）．

性質 2. $b_1A_1+b_2A_2+\cdots+b_pA_p=A_j$（ここで，$j(=0, 1, \cdots, 2^p-1)$ は $(b_1, b_2, \cdots, b_p)$ と1対1に対応する）

とくに，性質2は重要であり，$(b_1, b_2, \cdots, b_p)=(0, 0, \cdots, 0)$ 以外に右辺は，$A_0=(0\ 0\ \cdots)$ とならないことから，引きつづく $p$ 個の $A_i$ が線形独立であることの定義そのものになっている．

### 2.2 GFSR 乱数の $k$-distribution

定義） $k$-distribution とは，系列 $\{u_i\}$ の相続く $k$ 個を座標成分とする点 $U_i$ が（各座標成分 $l$ ビットの resolution として），単位方体内の任意の点 $U$ に関し

$$P(U_i=U)\fallingdotseq 2^{-kl}$$

となることである．ここで $P$ は1周期にわたる相対頻

† Matroid Representation 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

度である.

さて, GFSR 乱数とは, [0, 1) 上の一様乱数 $u_i$ の上位 $l$ ビットの二進表現を, 原始3項式 $f(D)=D^p+D^q+1$ により生成された $M$ 系列 $\{a_i\}$ を用いて

$$u_i=.a_{j_1+i}\ a_{j_2+i}\ \cdots\ a_{j_l+i}$$

としたものである. この $k$-distribution は, 次の行列 $G$ が各行線形独立になることが必要十分である[3].

$$\begin{bmatrix} A_{j_1} \\ A_{j_1+1} \\ \vdots \\ A_{j_1+k-1} \\ A_{j_2} \\ \vdots \\ A_{j_l} \\ \vdots \\ A_{j_l+k-1} \end{bmatrix} = \begin{bmatrix} & G & \\ (k\cdot l \text{ 行, } p \text{ 列} & & \\ \text{ただし } k=\lfloor p/l \rfloor) & & \end{bmatrix} \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ \\ \\ A_p \end{bmatrix}$$

以後, ビット数 $l$ を添字として $G$ を $G_l$ と書き, この行列のことを, GFSR 乱数の生成行列と呼ぶことにする.

### 2.3 GFSR 乱数の asymptotic randomness

GFSR 乱数の asymptotic randomness とは, $L$ ビットの GFSR 乱数の上位 $l(\leq L)$ ビットに対しても $k$-distribution (ここで $k=\lfloor p/l \rfloor$) を保証しようというものである[11]. このことは, とくに合同法との理論的比較を行う際に必要になってくる[9].

定義) 次の2条件を満たす GFSR 乱数を, asymptotically random な $L$ bits GFSR 乱数という.

条件 1. 生成行列 $G_l$ が, 任意の $l(\leq L)$ に対して各行線形独立となる.

条件 2. 周期 $2^p-1$ が素数となる.

## 3. マトロイドによる表現

### 3.1 マトロイドとパリティ問題

$E$ を有限集合として, 次の3条件を満たす独立部分集合族 $I$ が定義されているとき, $(E, I)$ を $E$ 上のマトロイドという[2].

(1) $\phi\in I$

(2) $X\in I, Y\subseteq X$ ならば $Y\in I$

(3) $X, Y\in I, |X|<|Y|$ ならば $X\cup\{y\}\in I$ であるような元 $y(\in Y-X)$ が存在する (ここで $|\cdot|$ は集合の元の数).

マトロイドの典型的なものとして, ある行列の行ベクトルの集合と, その線形独立な部分集合全体とによるマトロイドがある.

パリティ問題とは,

「マトロイド $(E, I)$ と, $E$ の $k$ 元部分集合のいくつかからなる族 $P$ とが与えられたとき,

(a) $X_i\in P$

(b) $X_i\cap X_j=\phi$ $(i\neq j)$

(c) $X_1\cup X_2\cup\cdots\cup X_l\in I$

の3条件を満たすようになるべく多くの $X_1, X_2, \cdots, X_l$ を選ぶ.」

という問題である. この問題は, 計算の手間を計る単位として, 「任意の $X(\subseteq E)$ に対して $X\in I$ か $X\notin I$ かを判定する」ことをとったとき, $k\geq 3$ において, 一般には, 多項式時間の算法は存在しないことが示されている[6].

### 3.2 GFSR 乱数のマトロイド表現

$$E=\{A_i \mid i=1, 2, \cdots, 2^p-1\}$$

その線形独立な部分集合すべてによる族を $I$ としたとき, $(E, I)$ は, マトロイドとなっている.

ここで, パリティ問題における $k$ 元部分集合を次のようにとる.

$$X_{k,i}=\{A_i, A_{i+1}, \cdots, A_{i+k-1}\}\ (i\neq 0)$$

そして, そのすべてによる族を

$$P_k=\{X_{k,i} \mid i=1, 2, \cdots, 2^p-1\}$$

とする. すると, $k$-distributed な GFSR 乱数を求める問題は, そのままパリティ問題になっていることが次のようにして示せる.

証明)

GFSR 乱数が $k$-distribution となるためには,

$$\begin{matrix} A_{j_1} & A_{j_1+1} & \cdots & A_{j_1+k-1} \\ A_{j_2} & A_{j_2+1} & \cdots & A_{j_2+k-1} \\ \vdots & & & \vdots \\ A_{j_l} & A_{j_l+1} & \cdots & A_{j_l+k-1} \end{matrix}$$

の $k\cdot l$ 個の要素がすべて線形独立になることが必要十分条件である.

$X_{k,i}$ の決め方から, 上の条件は

$$X_{k,j_1}\cup X_{k,j_2}\cup\cdots\cup X_{k,j_l}$$

が線形独立集合となり, しかもその元の総数が $k\cdot l$ 個となることである. つまり,

$$X_{k,j_m}\cap X_{k,j_n}=\phi\ \ (m\neq n)$$

という条件を加えればよい.

以上をまとめてみると, パリティ問題の条件(a), (b), (c)そのものになっていることがわかる.

(証終)

このパリティ問題は, $P_k$ のとり方のために, 自明な解が存在する. 2.1節において述べた性質2から, 引きつづく $p$ 個の $A_i$ は線形独立であることがわかっている. そこで,

$$X_{k,i}, X_{k,i+k}, \cdots, X_{k,i+(l-1)k}$$

というように $l$ 個の $k$ 元部分集合を選べば, そのまま

解になる．この解はまた，Tausworthe 列[10]に対して，$l$-distribution を保証するのに用いられた解という見方もできる．

次に asymptotically random な GFSR 乱数を求める問題をマトロイドで表現してみる．2.3節により，各 $l(\leq L)$ に対し $k$-distribution が保証されていればよいわけだから，

(問題)

すべての $k=\lfloor p/l \rfloor$ $(l=1,2,\cdots,L)$ に対し

a) $X_{k,j_m} \in P_k$

b) $X_{k,j_m} \cap X_{k,j_n} = \phi$ $(n \neq m)$

c) $X_{k,j_1} \cup X_{k,j_2} \cup \cdots \cup X_{k,j_l} \in I$

の3条件を満たす $j_1, j_2, \cdots, j_L$ を求める．

と表すことができる．

ここでは，各 $k$ に対しパリティ問題を解くことになっているが，その際 $j_1, j_2, \cdots, j_l$ を共通にして解かなければならないために，問題が複雑になっている．$p=7$ に対して一つの解が見つかっているので下に示す．

$$G_7=\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & 1 & 0 & 0 \\ * & * & 1 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & 1 \\ * & 1 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & 1 & 0 & 0 & 0 \\ * & * & * & * & * & 1 & 0 \end{bmatrix}$$

(＊は0または1のどちらでもよいことを示す)

これは，$j_1, j_2, \cdots, j_7$ に対応する行ベクトルの形で表された7ビット asymptotically random な GFSR 乱数の生成行列である．とくに，この行列の場合，$f(D)$ の形には依存せず，7次の原始多項式すべてに共通する解になっていることも一つの特長である．

また＊をすべて0とすればわかるように，Tausworthe 列のビットを置換したものも解の一つとして含まれていることがわかる．

## 4. 結　論

ここでは，よりよい性質をもつ GFSR 乱数を求める問題をマトロイドを用いて表現し，それがパリティ問題の一つになることを示した．パリティ問題自体はマトロイドの分野で研究され，その問題のむずかしさも，一般的な意味で調べられているのでそれと結びつけて考えることには意味がある．$k$-distributed な GFSR 乱数を求める問題の場合は自明な解があることを示したが，asymptotically random な GFSR 乱数を求める問題は，かなりむずかしいようである．今後，近似解法も含めて，もっと次数の高い場合についての解を求める方法を確立することが課題になると思われる．

**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) Coveyou, R. R. and MacPherson R. D.: Fourier Analysis of Uniform Random Number Generators, *J. ACM*, Vol. 14, No. 1, pp. 100-119 (1967).
2) 藤重　悟：マトロイド理論とそのシステム工学的諸問題への応用，システムと制御，Vol. 23, No. 1, pp. 11-20 (1979).
3) Fushimi, M. and Tezuka, S.: The $k$-distribution of Generalized Feedback Shift Register Pseudorandom Numbers, *Comm. ACM*, Vol. 26, No. 7, pp. 516-523 (1983).
4) Golomb, S. W.: *Shift Register Sequences*, Holden-Day, San Francisco (1967).
5) Hoffmann de Visme, G.: *Binary Sequences*; 伊理正夫・伊理由美訳：2値系列，共立出版，東京 (1977).
6) 伊理正夫：マトロイド，計算の効率化とその限界，pp. 142-145，日本評論社，東京 (1980).
7) 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).
8) Lewis, T. G. and Payne, W. H.: Generalized Feedback Shift Register Pseudorandom Number Algorithms, *J. ACM*, Vol. 21, No. 3, pp. 456-468 (1973).
9) 手塚　集：GFSR 乱数の Asymptotic Randomness, 情報処理学会論文誌，Vol. 25, No. 4, pp. 681-684 (1984).
10) Tausworthe, R. C.: Random Numbers Generated by Linear Recurrence Modulo Two, *Math. Comput.*, Vol. 19, pp. 201-209 (1965).
11) 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).

(昭和59年1月13日受付)
(昭和59年3月 6 日採録)