1997年度日本オペレーションズ・リサーチ学会
春季研究発表会

数理計画法による乱数生成算法の設計

01501020　東京大学　伏見　正則　　FUSHIMI Masanori
01604870　東京大学　諸星　穂積　　MOROHOSI Hozumi

1　はじめに

擬似乱数は確率的シミュレーションの基本的道具であり，多数の生成法が提案されているが，大部分の利用者にとっては，それはブラック・ボックスであろう．一方，「乱数とは何か？」という根源的な問いに対する答えを与えようとする研究も，Kolmogorov や Chaitin 等によって精力的に行われた．有名な Knuth の本 [2] には，乱数の定義（をしようとする試み）が多数掲載されている．数学の教科書ならば，一つの概念に対する定義はふつう一つだけであるのと対照的である．これは，乱数生成が数学ではなくて，Knuth の本の題名のとおり，まさに Art であることの反映であろう．

乱数の定義と，現実的な乱数の生成アルゴリズム (を設計しようとする立場) との間には大きな隔たりがあるが，これを少しでも縮める努力も必要であろう．種々の定義や概念の中で，この目的のために重要と思われるのは，多次元均等分布 (equidistribution) と von Mises によるコレクティーフ (Collective) である．Kolmogorov[3] は，コレクティーフの概念に基づく有限乱数列（乱数表）の存在の問題に対して一つの解答を与えているが，それをどのようにして構成するかは，まったく別の問題である．

Fushimi[1] は，Kolmogorov[3] の例示した部分列抽出規則の中で最も単純なもの（以下では抽出規則 S と略称することにし，その詳細は以節で述べる）だけを考えた場合に，多次元均等分布の意味で良い乱数列を，M系列を基にして生成するアルゴリズムを設計する方法を提案している．一方，M系列を基にして生成する乱数列に関しては，Tootill 等 [4] が asymptotically random sequence という概念を提案し，そのような系列を一つ偶然に見つけたことを報告している．ただし，部分列抽出規則のことはまったく考慮していない．

本論文の目的は，抽出規則 S を考慮した上で，asymptotically random という性質 (a.r. 性) を近似的に満たす乱数列を生成するアルゴリズムを設計する方法を提案することである．

2　基本的事項

部分列選出規則 S：与えられた数列 $\{x_t : t = 1,2,3,\cdots\}$ から等間隔に抽出する規則のこと．間隔を n とすると，得られる数列は
$\{x_{nt} : t = 1,2,3,\cdots\}$ となる．

k 次均等分布：周期が T の l ビットの 2 進数の数列 $\{x_t : t = 1,2,\cdots,T\}$ が与えられた場合に，k 次元ベクトル $(x_t, x_{t+1}, \cdots, x_{t+k-1})$ の 1 周期 $(1 \le t \le T)$ にわたる頻度分布が，2^{kl} 個の値上の一様分布であるならば，もとの数列 $\{x_t\}$ は k 次均等分布をするという．

M系列：ガロア体 GF(2) 上の原始多項式

$$f(z) = 1 + c_1 z + c_2 z^2 + \cdots + c_p z^p, \qquad c_p = 1$$

を特性多項式とする漸化式

$$a_t = c_1 a_{t-1} + c_2 a_{t-2} + \cdots + c_p a_{t-p} \pmod 2$$

と非零の初期値 $(a_1, a_2, \cdots, a_p)$ を用いて生成される数列 $\{a_t\}$ のことを (p 次の) M系列という．これは周期が $2^p - 1$ の周期列である．

Tausworthe 列：M系列から次のようにして構成される l ビットの 2 進数の系列 $\{x_t\}$ のこと．

$$x_t = 0.a_{\sigma t+1} a_{\sigma t+2} \cdots a_{\sigma t+l}$$

ただし，σ は $2^p - 1$ と互いに素な自然数である．

Tausworthe 列の k 次均等分布：
Tausworthe 列が k 次均等分布をするための必要十分条件は，$\{x_t : 1 \le t \le k\}$ に含まれるM系列の kl 個の要素が線形独立であることである．ここで‘線形独立’というのは，下記の重みベクトルの線形独立性のことである．

M系列の任意の要素は，漸化式を繰り返し適用することによって $e_1a_1 + e_2a_2 + \cdots + e_pa_p$ の形に書くことができる．すなわち，M系列の各要素には唯一の重みベクトル $(e_1, e_2, \cdots, e_p)$ が対応する．

一般化 Tausworthe 列： Tausworthe 列の均等分布の最大次数は，$m = \lfloor p/l \rfloor$ である．そして，たとえば $\sigma = l$ と選べば，この最大次数が達成できる．しかし，このように選んでも，部分列選出規則Sを適用して得られる数列 $\{x_{nt}\}$ も m 次の均等分布をするという保証はない．そこで，x_t のビットを入れ換えて

$$x'_t = 0.a_{\sigma t+j(1)}a_{\sigma t+j(2)}\cdots a_{\sigma t+j(l)}$$

（ただし，$\{j(1), j(2), \cdots, j(l)\}$ は $\{1, 2, \cdots, l\}$ の順列）と表現される一般化 Tausworthe 列 $\{x'_t\}$ を構成し，この数列の上位 l' ビットだけに注目すれば，選出規則Sを適用しても m 次均等分布が保証されるようにすることを考える．l' は大きいほど好ましいことはいうまでもない．

3 0-1 整数計画問題

選出規則Sを適用するときの抽出間隔 n の集合を $\mathbf{N}$ とする．（これは，$2^p - 1$ と互いに素な自然数のうちで小さいものをいくつか集めた集合とするのが常識的であろう．）f, σ, l はすでに選ばれているものとする．われわれの目標は，下記の l' を最大にする順列 $\{j(1), j(2), \cdots, j(l)\}$ を見つけることである：すべての数列 $\{x'_{nt}\}, n \in \mathbf{N}$, が上位の l' ビットに注目すると m 次均等分布をする．

この目標を達成するためには，まずビット間の従属関係を見つける必要がある．すなわち，各 $n \in \mathbf{N}$ について，$\{x_{nt} : 1 \le t \le m\}$ に含まれるすべてのM系列の要素の間の極小な従属関係をすべて求める．各従属関係に対応して，l 次元 0-1 ベクトル $\mathbf{g}$ を次のように定める：従属関係にあるM系列の要素が $x'_{nt}, 1 \le t \le m$, の $j_1, j_2, \cdots, j_\nu$ ビット目にあるならば $g_{j_1} = g_{j_2} = \cdots = g_{j_\nu} = 1$ とし，他の成分は 0 とおく．このようにして得られた行ベクトル $\mathbf{g}$ をすべて並べて得られる行列を G とし，
$\mathbf{z} = (z(1), z(2), \cdots, z(l))$ を l 次元 0-1 列ベクトルとして，われわれの問題は次の 0-1 整数計画問題として定式化できる．

$$\begin{aligned} \text{ILP:} \quad & \min \quad z_0 = \textstyle\sum_{j=1}^{l} z(j) \\ & \text{s.t.} \quad G\mathbf{z} \ge \mathbf{1} \end{aligned}$$

これは集合被覆問題であり，l が大きいときには厳密解を得ることが困難であるが，近似解を得る方法は種々知られている．近似解において $z_0 = l - l'$ となったものとする．$z(j) = 0$ となった j が $j_1, j_2, \cdots, j_{l'}$ だったとすると，これらが順列 $\{j(1), j(2), \cdots, j(l)\}$ の最初の l' 個の要素であれば，$\{x'_{nt}\}, n \in \mathbf{N}$, は l' ビットの精度で m 次均等分布をする [1].

4 Asymptotically random sequence

選出規則Sを適用しても a.r. 性を厳密に満たす数列を構成することは，きわめて困難であると思われる．しかし，前節で述べた方法を次のように反復適用すれば，近似的に a.r. 性を満たす数列を作ることは可能である．

まず，ILP を解く．つぎに，l' をあらたな l とし，$\lfloor p/l' \rfloor$ をあらたな m として，$\{x'_{nt}\}$ についてふたたび ILP を解く．以下同様にして $l' = 1$ となるまで繰り返す．

5 数値列

当日示す．

参考文献

[1] M. Fushimi(1988): Designing a uniform random number generator whose subsequences are k-distributed. *SIAM J.Comput.* **17**, 89-99.

[2] D. E. Knuth(1981): *The Art of Computer Programming, Vol.2: Seminumerical Algorithms,* 2nd Ed. Addison-Wesley, Reading, Mass.

[3] A. N. Kolmogorov(1963): On tables of random numbers. *Sankhya* **A25**, 369-376.

[4] J. P. R. Tootill et al.(1973): An asymptotically random Tausworthe sequence. *J.ACM* **20**, 469-481.