M系列を用いた三値の疑似乱数発生のための アルゴリズム

川崎医科大学　物理学教室
高田和郎・國末　浩

(昭和61年9月16日受理)

A Generating Algorithm for 3-valued Pseudo-random Numbers by Maximum Length Sequence Method

Kazuo Takata and Hiroshi Kunisue

Department of Physics, Kawasaki Medical School
Kurashiki 701–01, *Japan*

(*Received on Sep.* 16, 1986)

概　　要

最大周期系列法を用いた三値の疑似乱数を二値のコンピューターのプログラミングで発生させるためのアルゴリズムを提案した。ここで，三値データーの二値表現にはシフトの高速性を考えて，二線式を採用した。

手順中，必要な三値一桁の mod 3 積の演算を論理式で代行する方法を見出した。この手法はコンピューターの論理演算が各桁とも同じ演算を同時に行うという性質を利用したもので，この手順を用いれば各桁の mod 3 積の演算を各桁同時に，並列して実行するため，特に多数桁，長周期の三値疑似乱数を発生させる場合の高速化が期待できる。

Abstract

This paper presents an algorithm which generate the 3-volued pseudo-random numbers by maximum lenght sequence method using 2-line 3-volued logic.

In this algorithm, several logical operations are used instead of many arithmetic operations and moving instructions.

All bits of a byte are given same operations at logical instrucions, therefore modulo–3 multpilications of every digit are excuted parallel by the algorithm.

For above reason it is expected to speed up the generation of 3-valued pseudo-ramdom numbers for long period and many digits.

§1. 緒　　言

一般に乱数列は統計的な手法を用いての現象解明や問題解決のための入力として不可欠のものである。この乱数列には純粋な乱数列と疑似乱数列とがある。このうち純粋な乱数列とは数

が相互に関連がなく，不規則に並んで周期の無いものをいい，またこの条件は満たさないが乱数列に類似のもので一つ以上の乱雑さに対するテストを満たすものを疑似乱数列という。

乱数を使用する場合には，ディジタルな系の検査などのように再現性のあるものが必要な場合も多く，また目的によっては，十分に長い周期であればほとんど周期性なしとみなせて，使用に際しては疑似乱数でも実用上問題のない場合がほとんどである。このため厳密には純粋な乱数とはいえないが比較的高速発生が可能で，しかも再現性があり，非常に長周期で不規則な数列とみまがうものすなわち，疑似乱数が多く使用されている。そのうえ，ほとんどの疑似乱数は再現性を確保できるので，その乱数の性質をくわしく検査でき，目的にあった疑似乱数を選択することができる。

現在，これら疑似乱数の発生には乗算型合同法，混合型合同法，最大周期系列法，全周期系列法などの手法が用いられている。[1),2)]

筆者は以前，最大周期系列法（M系列法）を用いた三値の疑似乱数列の発生器を試作したが[3)]，今回はこれをソフトで構成し，三値の乱数を高速で発生させるために若干の工夫をしたのでここに報告する。

§2．最大周期系列法を用いる疑似乱数の発生手順

最大周期系列を用いる方法でD進級の疑似乱数を回路で発生させる場合にはフィードバック回路を伴ったシフト・レジスター回路を用いる。ソフトで製作する場合にも類似の手順となるので，図1にm桁の場合の回路ブロック図を示した。

図中，$X_n, X_{n-1}, X_{n-2}, \cdots, X_{n-m+1}$の部分はその内容が同時に左に1桁分づつ移動できるので，全体でm桁のシフト・レジスターと呼ばれ，初めにD進m桁の非零の任意定数が初期値として代入されている。$C_0, C_1, C_2, \cdots, C_{m-1}$の部分はD進m桁定数の格納場所で特定の定数のうちの1組が設定されている。このほかに，Dを法とした2変数1桁の mod 積を計算する回路がm個あって，これらの回路はXとCの各桁ごとに$X_{n-1} \cdot C_1 \bmod D$の値を算出する。この回路

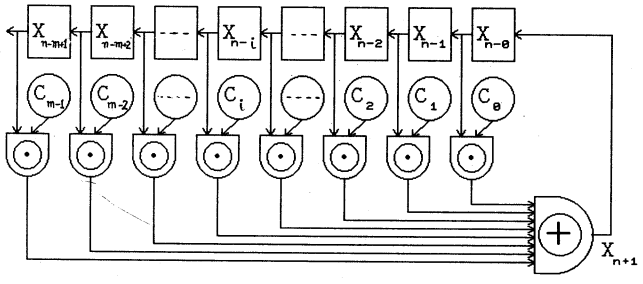


図1　最大周期系列法を用いる疑似乱数発生機構のブロック図

で算出されたデータ群は多入力の mod 和回路に入り，Dを法とした和が求められる。すなわち，

$$X_{n+1} = (\Sigma X_{n-1} \cdot C_1 \bmod D) \bmod D$$
$$= (X_n \cdot C_0 + X_{n-1} \cdot C_1 + \cdots + X_{n-m+1} \cdot C_{m-1}) \bmod D \quad (1)$$

と計算される。このX_{n+1}がD進乱数列の新しい1桁分として創生されたものである。

この値は，全体を左に1桁シフトされたレジスターの最右端に入れられ，新しいD進m桁の数がシフト・レジスターに出現する。上記手順のうちの後半が繰り返し実行されると，Cと新しいXとで式(1)の計算を毎回実行するのでつぎつぎと乱数が作りだされる。こうして得られる乱数列はシフト・レジスターの値が再び初期値と同じ値になった時から以後は最初と同じ乱数をつぎつぎと産みだす。すなわち周期性が現われてくる。

定数C_0，C_1，…，C_{m-1}の組合せを適当なものに選べば，D種類m列から作られる順列のうち，0…0を除いたすべての可能な順列が1回だけ必ず現われるようにすることができる。この場合が，この仕方で得られる最大周期のもので，D^n-1の周期を持つことがわかる。すなわち，1周期のうちにシフト・レジスターには1からD^n-1までのすべての数が必ず1回だけ現われる。

一例としてD＝3，m＝16（3値16桁）とすれば周期Nは$N=3^{16}-1=4304,6720$となる。

またこの間の0，1，2の出現確率は$3^{16}-1$回中それぞれ$3^{15}-1$回，3^{15}回，3^{15}回とほとんど均等であり，00,01,02,10,11,12,20,21,22なる2連の出現回数もまた$3^{14}-1$，3^{14}，3^{14}，…，3^{14}でほぼ一様であり，また000，001，…，222なる3連の乱数の出現回数も$3^{13}-1$，3^{13}，…，3^{13}となる。一般にi連の出現回数もシフト・レジスターの最高位の桁からi番目のまでを毎回の3進i連の乱数として採用すれば，$3^{16-i}-1$，3^{16-i}，…，3^{16-i}とほとんど均等に生ずるという特徴をもつ。

次にプログラムでM系列を発生させる場合について考察する。この場合にもほぼ上述の手順で作られ，図2がその手順の大まかな流れ図である。ただ，この図はサブルーチンとして製作する場合のものを示した。

Dが2の場合，すなわち2進級を用いてM系列の乱数を発生させるプログラムを作る場合には mod 2積のプログラム化には論理積命令を，mod 2和にはパリティー・チェック命令を利用すれば全桁の演算を一度に並列させて実行することができる。

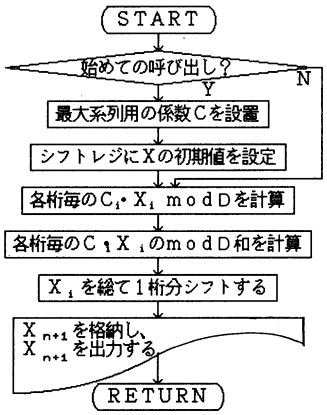


図2　D値疑似乱数発生のための流れ図

しかし，Dとして3，すなわち3進数を用いる場合には簡単でなく，3値を2値で表現するための表現法自体にもいく通りかが考えられ，mod 3積や mod 3和のプログラムもそれにしたがって異なったものになり，それに伴って乱数発生の速度も異なってくる。

§3．三進多数桁の表現法

シフト・レジスターに入れるべき3進m桁の数を2値の電子計算機で表現させるにはいくつかの方式が考えられる。

第一の方式は3進1桁の記憶に1ワードまたは1バイトを用いる方法で，このうち1ワードを用いるのは整数型の配列変数をm個用いてシフト・レジスターの記憶機能を代行させるもので BASIC や FORTRAN などのコンパイラー言語でプログラムを作る場合に便利である。また1バイトを用いるのはアセンブラ言語でプログラムを行う場合で，しかも論理命令やシフト命令を用いずに，MOV 命令でシフトの代行をし，算術演算でフィードバック部の演算を行う場合に便利であろう。著者等はM系列を満たす係数をさがすためのプログラムをこの方式で BASIC 言語でのものと機械語を用いたものの二つを別々に製作し，作動させ，桁数が3から8までのものについては全部の係数を見出した。表1に得られた結果の一部を示す。

第二の方式はいわゆる3線式3値の表現を用いるもので，3バイト分の記憶場所または3個分のレジスターを使って3進m桁を一度に表現する方式である。ここでは各バイトを0のバイト，1のバイト，2のバイトと命名し，例えば上位からi桁目の値が2の場合には，2のバイトのiビット目を1にし，0と1のバイトのiビット目は共に0にすることによりi桁目の2を表現する。以下同じ。

第三の方式は2線式3値表現とでもいうべきもので，1のバイトと2のバイトと称する2バイト分を用いて3進m桁をまとめて表わす。たとえば，上位からi桁目が2であるような3進数を表現する場合には2のバイトの上位からiビット目を1にし，1のバイトのiビット目は0にすることで3値の2を表現させる。1を表わすには上記の逆，すなわち2のバイトは0，1のバイトを1にする。また0を表現するには両方のバイトのiビット目を共に0とすることで表わす。

ここではプログラムを高速作動させる目的でこの2線式を採用した。

§4．三値一桁の三を法とする積の並列演算

フィード・バック部の演算に対応するところの3を法とした X_{m-1} と C_1 との積は2値の場合のように各桁を同時に演算できれば高速作動が期待できる。そこで，この部分の並列処理の可能性について考えてみる。

表2は3を法とする2変数XとCの積に対する3値の真理値表である。本研究では被乗数Xと乗数Cおよび両者の mod 3積Sの表現に2線式3値を用いることにする。XとCとSの2のバイトと1のバイトのi桁目の情報をそれぞれX2，X1，C2，C1，S2，S1とする

表1　M系列を満足する係数

	C_2	C_1	C_0
例　1	2	0	1
例　2	2	1	0
例　3	2	1	2
例　4	2	2	1

a）3桁の場合のすべての係数

	C_3	C_2	C_1	C_0
例　1	1	0	0	1
例　2	1	0	0	2
例　3	1	1	0	0
例　4	1	1	1	2
例　5	1	1	2	2
例　6	1	2	0	0
例　7	1	2	1	1
例　8	1	2	2	1

b）4桁の場合のすべての係数

	C_6	C_5	C_4	C_3	C_2	C_1	C_0
例　1	2	0	0	0	0	1	0
例　2	2	0	0	0	0	2	1
例　3	2	0	0	0	1	1	1
例　4	2	0	0	0	1	1	2
⋮				⋮			
例　156	2	2	2	2	2	1	0

e）7桁の場合の係数例

	C_4	C_3	C_2	C_1	C_0
例　1	2	0	0	0	1
例　2	2	0	0	1	2
例　3	2	0	1	1	2
例　4	2	0	1	2	0
例　5	2	0	2	0	2
例　6	2	0	2	1	0
例　7	2	0	2	1	1
例　8	2	1	0	0	0
例　9	2	1	0	0	2
例　10	2	1	0	1	1
例　11	2	1	1	0	1
例　12	2	1	1	2	0
例　13	2	1	2	2	2
例　14	2	2	0	0	1
例　15	2	2	0	2	0
例　16	2	2	0	2	2
例　17	2	2	1	0	0
例　18	2	2	1	1	0
例　19	2	2	1	2	2
例　20	2	2	2	0	2
例　21	2	2	2	1	2
例　22	2	2	2	2	1

c）5桁の場合のすべての係数

	C_5	C_4	C_3	C_2	C_1	C_0
例　1	1	0	0	0	0	1
例　2	1	0	0	0	0	2
例　3	1	0	0	1	0	1
例　4	1	0	0	2	0	2
⋮				⋮		
例　48	1	2	2	2	2	2

d）6桁の場合の係数例

	C_7	C_6	C_5	C_4	C_3	C_2	C_1	C_0
例　1	1	0	0	0	0	1	0	0
例　2	1	0	0	0	0	2	0	0
例　3	1	0	0	0	1	1	0	2
例　4	1	0	0	0	1	1	1	2
例　5	1	0	0	0	1	1	2	1
例　6	1	0	0	0	1	2	0	1
例　7	1	0	0	0	1	2	1	1
例　8	1	0	0	0	1	2	2	2
⋮				⋮				
例　320	1	2	2	2	2	2	2	1

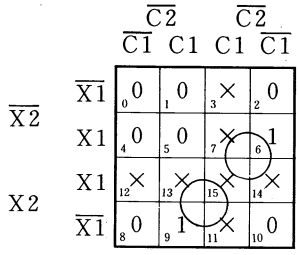
f）8桁の場合の係数例

表2　3値2変数の3を法とする積の真理値表

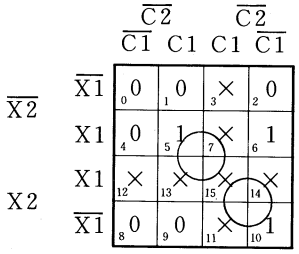
		C		
		0	1	2
X	0	0	0	0
	1	0	1	2
	2	0	2	1

表3　3を法とする2変数の積に対する2値の真理値表

被乗数		乗　数		結　果	
X2	X1	C2	C1	S2	S1
0	0	0	0	0	0
0	0	0	1	0	0
0	0	1	0	0	0
0	0	1	1	×	×
0	1	0	0	0	0
0	1	0	1	0	1
0	1	1	0	1	0
0	1	1	1	×	×
1	0	0	0	0	0
1	0	0	1	1	0
1	0	1	0	0	1
1	0	1	1	×	×
1	1	0	0	×	×
1	1	0	1	×	×
1	1	1	0	×	×
1	1	1	1	×	×



a）S2 の Veitch 図表



b）S1 の Veitch 図表

図3　mod 3 積の並列演算のための Veitch 図表

と，表2を参考にして，3を法とする2変数XとCの積Sに対する2値の真理値数は表3となる。

ここで表中の×印は少なくとも被乗数か乗数が3となる場合で，3値の演算ではこれは現実には出現しないのであるから演算結果は0としても1としてもよい。すなわち冗長な情報の部分である。

これらをS2，S1，について Veitch 図表に描けば図3が得られる。この図からS2とS1はそれぞれ簡略化された論理式で表現できて

$$S2 = C2 \cdot X1 + C1 \cdot X2$$
$$S1 = C1 \cdot X1 + C2 \cdot X2$$

となる。したがって，プログラム上でも上式をそのままプログラム化すれば論理積4回，論理和2回の演算で実際上16桁分の $X_{n-1} \cdot C_1 \bmod 3$ の演算を並列して同時に処理してしまうことができる。

§5. 結　　言

M系列の係数をさがし出すためのプログラムを BASIC と機械語を用いて製作し，3桁から8桁までのすべての係数を見出だした。

つぎに最大周期系列法を用いてコンピューターで3値の疑似乱数を発生させる手順について考察し，3値m桁の数を2バイトで表現するところのいわゆる2線式表現法を用いた場合のプログラム手法について検討した。その中で必要な3値2変数の3を法とする積の演算手法として，新しく論理積と論理和を用いる方法を見出した。この手法はコンピューターの論理演算が各桁とも同じ演算を同時に行うという性質を利用したもので，各桁の3を法とした積の演算を個別にではなく，同時に並列して行うため，特に多数桁，長周期の3値疑似乱数の高速発生に役立つものと思われる。ただし，この手法を完成させるには3値1桁で多変数の mod 3 和の並列処理的な手順を見出すことが残されている。

文　　献

1）津田孝夫：モンテカルロ法とシミュレーション，培風館
2）G. Hoffmann de Visme 著：伊理正夫，伊理由美 訳：2値系列，共立出版
3）高田和郎：M系列を用いた三値疑似乱数発生器，川崎医学会誌一般教養編，4：1～10（1973）