M系列を用いた三値疑似乱数発生器

川崎医科大学　物理学教室
高　田　和　郎

(昭和53年9月30日受理)

3-valued pseudo random number generator by a maximum length sequence

Kazuo TAKATA
Department of Physics, Kawasaki Medical School,
Kurashiki 701-01, *Japan*
(*Received on Sep.* 30, 1978)

概　　要

改良した三安定回路を用いて $3^{10}-1=59048$ の周期をもった三レベル式のM系列三値信号発生器を試作した。このために，まず三安定回路にシフト・パルス入力用の回路を設けて，10 trit のシフト・レジスターとし，線型フィードバック・レジスターをM系列にするための係数の組合わせを電子計算機を用いて探査し，簡単に組立て得る組合わせを見出した。つぎに，フィードバック信号を得るための三値 mod 和の論理設計を行ない，これを構成するに必要な三値閾値論理回路，三値否定回路，三値論理和回路および論理積回路の設計を行った。

Abstract

This paper describes a way to construct a 3-level type 3-valued pseudo random signal generator with the improved tri-stable circuits whose period are $3^{10}-1=59048$ bit times.

In order to construct this generator a shifting register is first assembled by means of 10 tri-stable circuits and its triggering circuits. Then a suitable combination of coefficients for the general linear feedback register is detected by electronic computer to convert the feedback register to the generator. Secondly, the logical networks of mod 3 ring-sum are designed with fundamental ternary logics to generate the feedback signals for the shifting register. Lastly, the fundamental ternary logical circuirs, namely, electronic circuit implementing the ternary thershold logic, ternaly inverter, logical sum and logical product are assembled.

§1. 緒　　言

乱数はモンテカルロ法を用いた諸計算などに用いるために，色々な性質を有するものが要求され，また考案されている[1]。この中でも最も基本的な二値乱数は0と1のみで構成されている乱数で，これは高速の発生が可能であるために，二値的な系の特性の推定のような二値的な分野だけでなく，変換によっては多値の分野でも用いられている。

二値M系列は純粋な乱数ではないが，その発生器はシフト・レジスターと排他的論理和回路を組合わせた電子回路で簡単に構成でき，種々の特徴をもった[2]，再現性のある疑似乱数を生みだすことができるために多方面で利用されている。

三値乱数も二値乱数の拡張として三値ランダム信号の入力源として種々の目的に使用できるが，高速発生の目的からいえばコンピューターを用いてソフトウェアーで作るよりもハードウェアーな三値M系列の信号発生器を用いるのが簡単であろう。

この論文では試作した三値M系列の信号発生器の概要についてのべてある。すなわち，著者等はすでに三レベル式三安定回路の一部に改良をほどこして能動領域でも充分安定な回路を発表したが[3]，もし，この回路の数組に信号シフト用の付属回路を取り付ければ三値シフト・レジスターを作ることができ，これを用いればシフト・パルスにより数 trit の三値信号をシフトすることができる。また，このシフト・レジスターと適当な三値組合わせ論理回路を接続すれば目的とする三値順序論理回路を自由に構成することができる。

ここでは (1)試作したシフト・レジスターを紹介し，また (2)「三を法（mod 3）とする加算」回路，すなわち桁上げ信号不要の場合の三値半加算器の論理構成について検討し，これに必要な (3)基本の三値組合わせ論理回路を設計，製作したのち，これらを用いて三値の mod 和回路を構成し，これと試作した三値シフト・レジスターとを組合わせて三値の疑似乱数を発生するところの (4)三値M系列信号発生器を製作した。これらの原理，構成，特徴などについてのべる[4]。

§2. 三値シフト・レジスター回路

図1に前回報告したところの三レベル式三安定回路を示し，図2に今回これを用いて試作した三値シフト・レジスター回路を示す。また，本論文で用いるところの論理値と実際の回路の出力電圧との対応を表1のように定めた。シフトはシングルパルスで1シフトが行えるところのシングルパルス法を用いることができれば出力波形や高速性など種々の点で良好なのであるが，トランジスターが能動領域にある場合に生ずる中間値をシフトするための簡単な回路構成が見出せなかったので今回は図3のようなダブルパルスを用いる方法を採用した。すなわち図3の(1)のパルスですべてのレジスターを中間値にセットし，そののち信号シフト用のコンデンサーに一時的に貯えられている前段のレジスターの内容が放電や充電によって失なわない間に後続パルスによって

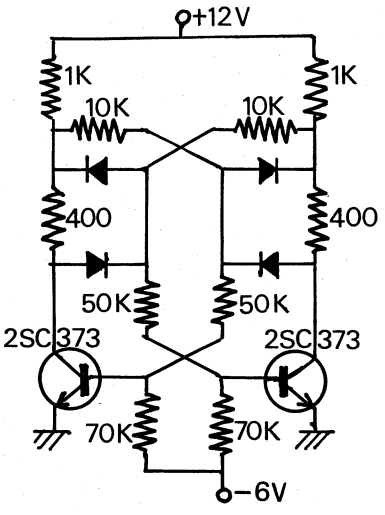


図1 三安定回路

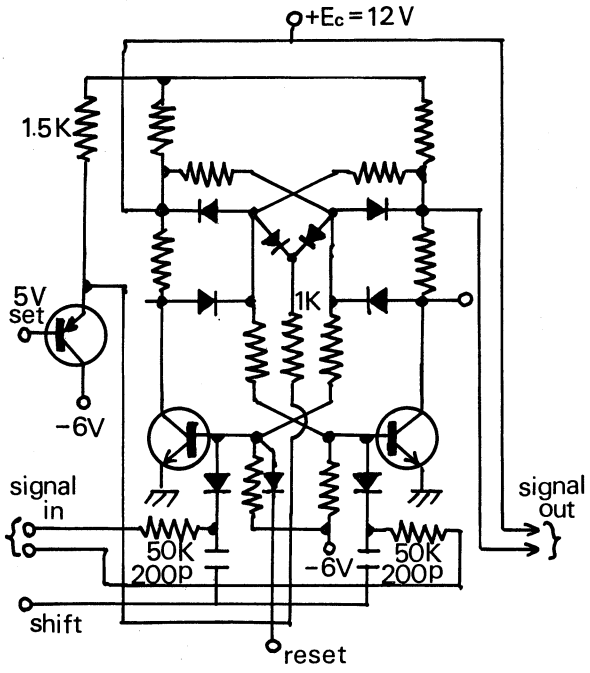


図2　1 *trit* のシフト・レジスター

表1　論理値と電圧の対応

論理値	右側のトランジスターの状態	出力電圧（ボルト）
0	導　通	0
1	能　動	5（中間値）
2	遮　断	10

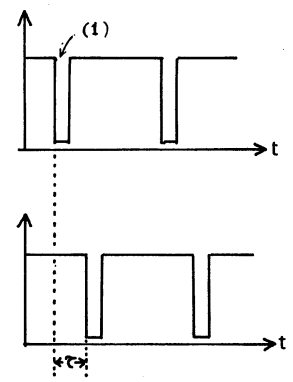


図3　パルス発生器の出力波形

その内容をその段のレジスターに移し換えるという方法をとった。ここでパルス巾は約 1 μ 秒，遅延時間 τ は約 2 μ 秒である。

回路図から判明するように中間値セットのためのトリガーはコレクター・トリガー方式であるのでトリガー端子からみた入力抵抗が小さい。このために2段ごとに1つのエミッター・フォロワーを用いて低出力抵抗のパルス源を用いた。一方信号シフト用のトリガーはベース・トリガー方式であるので試作した10個のシフト・レジスターを同じパルス源より直接供給して用いた。

§3.　M系列を構成するための係数の決定

まず二値の場合[5]を拡張した三値のM系列について説明する。ある三値の系列Sが

$$S=\{U_t,\ t=\cdots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \cdots\} \tag{1}$$

で表わされるような無限数列とする。ただし系列の要素 U_t は 0，1，2 のうちのいずれかを取るものとする。ここで D を遅延作用素とし，DS は

$$DS=\{U_{t-1}\} \tag{2}$$

を意味することとし，二つの系列の和 $S+S'$ を

$$S+S'=\{U_t+U_t'\ \mathrm{mod}\ 3\} \tag{3}$$

のように対応する各項ごとの三値一桁の加算（3を法とする和）をその項の値とする系列であ

るとする。また系列の定数 C（0，1 または 2）倍を

$$CS=\{C\cdot U_t \bmod 3\} \tag{4}$$

とする。以下の演算記号では mod 3 を省略して和，積に⊕，⊙を用いる。

ここである作用素 $P_n(D)$ を S に作用させて，それが

$$P_n(D)\ S=(X_n\odot D^n\oplus X_{n-1}\odot D^{n-1}\oplus\cdots\oplus X_1\odot D\oplus X_0)S$$
$$=X_n\odot D^nS\oplus X_{n-1}\odot D^{n-1}S\oplus\cdots\oplus X_1\odot DS\oplus X_0\odot S \tag{5}$$

で表わされるとき，この式を n 次の遅延多項式と呼ぶ。ただし，X_0, X_1, …, X_n をある三値の論理定数（0，1，2）とする。また $X_n=0$ ならば，$n-1$ 次となるので $X_n\neq 0$ と仮定し，また $X_1=0$ ならば，D で因数分解できるので，$X_1\neq 0$ と仮定する。

ここですべてが 0 とはならないような系列 S があってその S が

$$P_n(D)S=\{0\} \tag{6}$$

を満足するとき S を $P_n(D)$ の根と呼ぶ。S が $P_n(D)$ の根であれば

$$X_n\odot D^nS\oplus X_{n-1}\odot D^{n-1}S\oplus\cdots\oplus X_1\odot DS\oplus X_0\odot S=\{0\}$$

よって

$$-X_0\{X_n\odot D^nS\oplus X_{n-1}\odot D^{n-1}S\oplus\cdots\oplus X_1\odot DS\}=S \tag{7}$$

を得る。この式はこの場合の S が周期性をもっていることを表わしている。すなわち式の左辺は S の要素の n 個の過去の値にある種の一定操作をほどこしたものが S 要素の現在の値(右辺)に等しくなっていることから容易にわかる。

つぎにこの S の周期についてであるが，S の要素のうち n 個の過去の値のとり得る組合わせの数は 3^n のうちから 0，0，…，0 なる一組を除いて，たかだか 3^n-1 であるから最大周期は 3^n-1 であることがわかる。この最大周期をもつ根を M 系列（maximum length null sequence）という。

さて一般の三値線形フィードバック・レジスターとは図 4 のように三値のシフト・レジスターを構成している n 個の三値記憶素子のそれぞれの出力 U_{t-1}, U_{t-2}, …, U_{t-n} をそれぞれ X_1', X_2', …, X_n' 倍して加算した信号を初段にフィードバックしたものをいう。

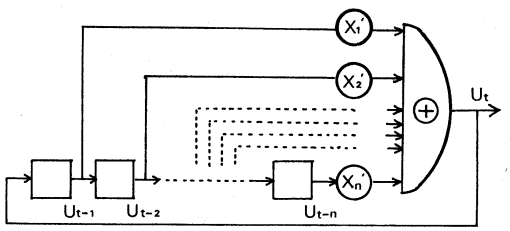


図 4 線形フィードバック・レジスター

ここで $X_i'=-X_0\odot X_i$ とみなせばこのブロック図は(7)式を回路で表現していることがわかる。したがって 3 値M系列の信号発生器の一般的な回路構成は図 4 のような形をとることがわかる。ここで X_i' にどのような値を採用すればM系列を得ることができるであろうか。M系列となるための必要条件は $P_n(D)$ が既約多項式であることはわかっているが，これは十分条件とはならない。これらM系列をとるような（X_i'）の組を系統的に見出す方法が見当たらなかったのでここでは 3 値記憶素子の数 n が10の場合についての X_i' をコンピューターでさがさせる

ことにした。このためのプログラムは一応 X_1', X_2', …, X_{10}' のすべての係数の組合わせについて順次調べていく方法を採用したが，処理のスピード化の目的で $P_n(D)$ が因数分解されることが明らかな X_i' の組合わせについては飛び起こしを行なうようにプログラムを構成した。得られた結果のうち $X_i=0$ を満足する個数の大きなものとして $X_1'=1$, $X_3'=1$, $X_{10}'=1$ 他は0というのがあったのでこれを用いてM系列の発生器を構成することにした。

§4. 三値 mod 3 和回路の論理構成

前節の結果により，$n=10$ のM系列を発生させるには $U_t=(U_{t-1}\oplus U_{t-3})\oplus U_{t-10}$ より明らかなように2入力の mod 3 和回路が二組必要である。そこでこの mod 3 和回路の論理設計を行なう。

表 2(a) 対称数系の二入力 mod 3 和の真理値表

$f=A\oplus B$		B		
		−1	0	1
A	−1	1	−1	0
	0	−1	0	1
	1	0	1	−1

表 2(b) 対称数系の二入力 mod 3 和真理値表

$f=A\oplus B$		B		
		0	1	2
A	0	2	0	1
	1	0	1	2
	2	1	2	0

まず，対称数系で表わされた三値論理変数 A と B の mod 3 和の直理値表は表2(a)のように表わせる。この真理値表の−1を0に，0を1に，1を2に変換すると表2(b)を得る。この表2(b)を用いて f を論理最小項で展開すると

$$f=A^0\cdot B^0+1\cdot A^0\cdot B^2$$
$$+1\cdot A^1\cdot B^1+A^1\cdot B^2$$
$$+1\cdot A^2\cdot B^0+A^2\cdot B^1$$

あるいは

$$f=CO_-(A)\cdot CO_-(B)$$
$$+CO_-(A)\cdot LIM\ CO_-INV(B)$$
$$+A\cdot\bar{A}\cdot B\cdot\bar{B}$$
$$+CO_+INV(A\cdot\bar{A})\cdot CO_-INV(B)$$
$$+LIM\ CO_-INV(A)\cdot CO_-(B)+CO_-INV(A)\cdot CO_+INV(B\cdot\bar{B}) \quad (8)$$

表 3 閾値論理の真理値表

	A		
	0	1	2
$A^0=CO_-(A)$	2	0	0
$CO_+(A)$	2	2	0
$A^2=CO_-INV(A)$	0	0	2
$CO_+INV(A)$	0	2	2
$LIM\ CO_-(A)$	1	0	0
$LIM\ CO_-INV(A)$	0	0	1
$A^1=CO_+INV(A\cdot\bar{A})$	0	2	0

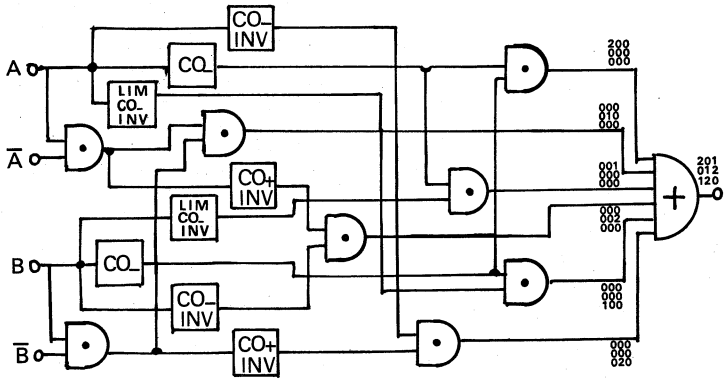


図5 論理最小項展開による mod 3 和回路

となる。ここで＋と・はそれぞれ三値の論理和と論理積を表わし，大きな1は三値論理定数であり，A^0, A^1, A^2, $CO_-(A)$, $CO_+(A)$, $CO\_INV(A)$, $CO_+INV(A)$, $LIM\ CO_-(A)$, $LIM\ CO_-INV(A)$[6] は三値一変数関数でその真理値表はそれぞれ表3に示した。

(8)式をそのままま回路化したものが図5である。しかしこれでは必要な演算素子の数が相当に多くなっている。これは最小項の和の形をそのまま用いたためで，少し変形すれば，簡略化されて図6と図7のようになる。ここで用いた簡略化の方法は系統的なものではないがその考え方の大意も図6と図7に示した。図6は否定入力が使用できる場合の例であり，図7の回路では否定入力が不要である。図7の構成のものを以下の回路に用いることにした。

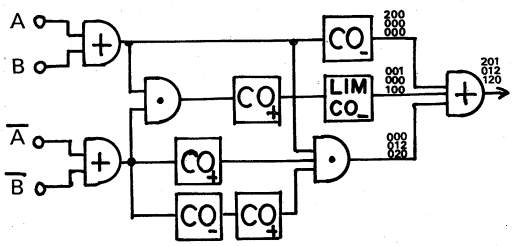


図6 否定入力が利用できる場合の mod 3 和回路

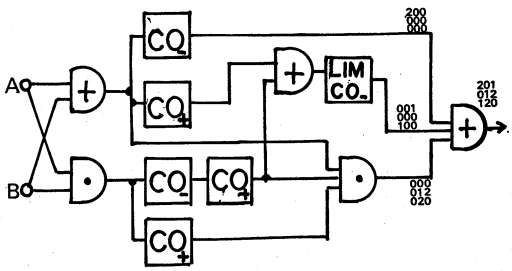


図7 試作した mod 3 和回路のブロック図

§5. 製作した三値基本論理回路の設計

(1) CO_-, $LIM\ CO_-$, CO_+, $LIM\ CO_+$ 回路

否定入力の閾値関数的な三値一変数の論理関数には表3に表わしたような CO_-, $LIM\ CO_-$, CO_+, $LIM\ CO_+$ がある。これらの回路はトランジスター1個と若干の抵抗を用いて図8のように構成できる。ここでトランジスターは 2SC-373 とし，R_L=2kΩ に選ぶと R_1, R_2, R_3 は簡単な回路解析ののち，表4のような値が算出されたのでこれを用いた。

(2)　三値インバーター回路

シフト・レジスターを働かせるには前段の信号とその否定が必要となる。初段以外では否定出力は自動的に用意されているけれども，前段がないところの初段のシフトには否定回路を設けてこれを作る必要がある。

三値インバーターの真理値表は表5のように入力が最高値の時，出力は最低値を，入力が最低値の時，出力は最高値を，入力が中央値の時，出力も中央値をとるものであるが，改良型三安定回路を参考にすると図9(a)のような回路で動作することが考えられる。すなわち三安定回路の一方の *Tr* は *E.F.* として用い，他方がインバーター

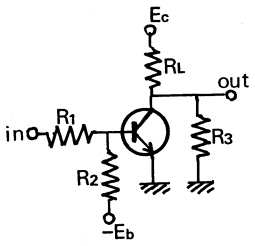


図8　否定を伴った閾値論理回路

表4　閾値論理回路

	CO_-	$LIM\ CO_-$	CO_+	$LIM\ CO_+$
R_1	25K	25K	50K	50K
R_2	70K	70K	50K	50K
R_3	10K	1.4K	10K	1.4K

表5　三値否定の真理値表

入　力	出　力
0	2
1	1
2	0

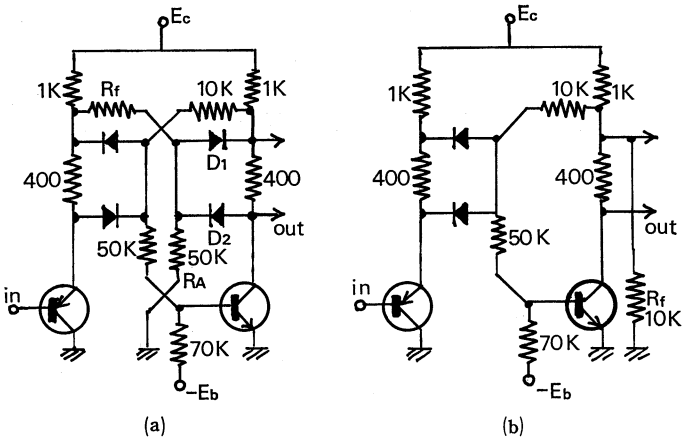


図9　三値否定回路

である。しかし，(a)回路の D_1, D_2, R_A を略し R_f を図9(b)のように用いても安定なインバーターを作り得た。(a)，(b)回路共にレベル再生機能をもっていることはいうまでもない。

(3)　三値 *AND* 回路・三値 *OR* 回路

同じく mod 3 和回路に必要な三値の *AND* と *OR* の回路はダイオード抵抗論理回路を用いて構成した。二入力の三値の *OR* と *AND* の真理値表を表6と表7に掲げる。三値の場合には

$$OR(A_1, A_2, \cdots, A_n) = max(A_1, A_2, \cdots, A_n)$$

$$AND(A_1, A_2, \cdots, A_n) = min(A_1, A_2, \cdots, A_n)$$

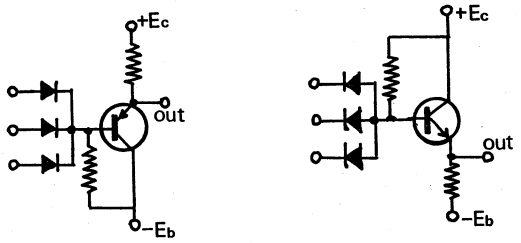
であるから，二値のダイオード *OR* や *AND* がそのまま利用できる。したがって，回路は図10

表6 三値 *OR* の真理値表

$A+B$		B		
		0	1	2
A	0	0	1	2
	1	1	1	2
	2	2	2	2

表7 三値 *AND* の真理値表

$A \cdot B$		B		
		0	1	2
A	0	0	0	0
	1	0	1	1
	2	0	1	2



(a) *OR* 回路　(b) *AND* 回路

図10 三値の *OR* と *AND* 回路

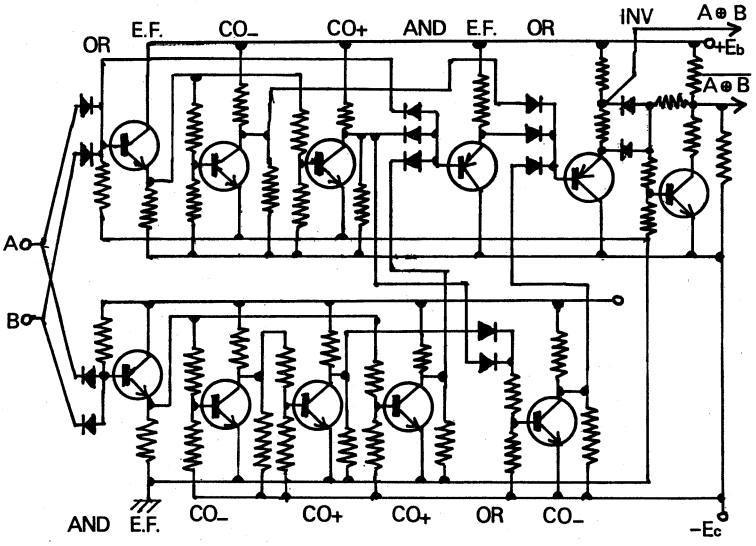


図11 2入力 mod 3 和回路

のものを用いた。これらの回路を用いて構成した否定出力付三値二入力 mod 3 和の回路を図11に表わす。

§6. 三値M系列信号発生器

前節までに説明した諸回路を図12のように接続して $n=10$ のM系列を用いた三値疑似乱数発生器を製作した。図中 *SR*-1, …, *SR*-10 はこれだけで 10 ***trit*** の シフト・レジスターを構成

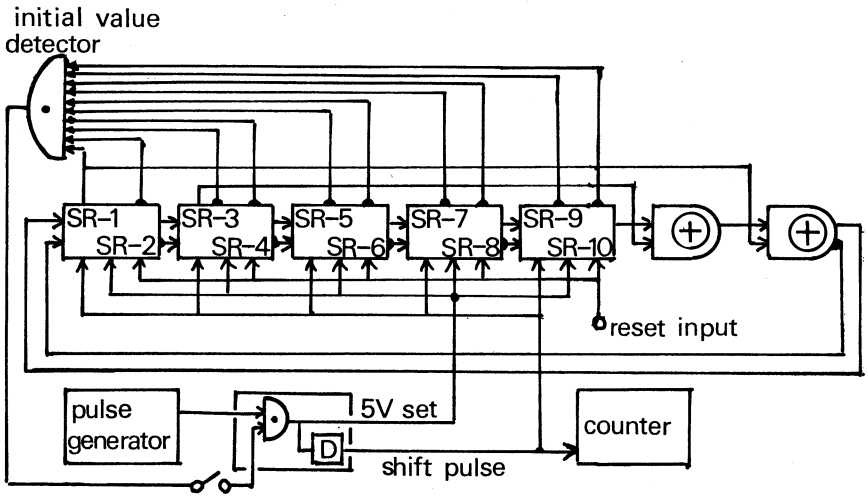


図12 試作した三値疑乱数発生器のブロック図

している。初期値検出回路と10進カウンターは装置が正常に働いているかどうかチェックするための付属回路で，レジスターの内部状態が再び初期値に達するまでのシフトパルス数を計数する。この数がM系列の周期 $3^{10}-1=59048$ であれば正常作動状態であることがわかる。

§7. 結　　言

最後にこれらの回路に関するまとめを個条書きにして示す。

(1) 製作した三値シフト・レジスターはトリガー回路が交流結合になっているのであまり高速のシフトには適さないが，パルスの繰り返し周波数が100KHz 程度までは正常に作動した。また，二組のパルスで一つのシフトを行ない，第1パルスでは常に中間値にセットするため，出力信号には刻時パルスごとに中間値を経由したのちに最終値になるので早急な情報呼び出しが出来ず，また過渡状態では不要なパルスなどが生ずるので非同期式の論理機器には使用できない。したがって高速を目的とするには今後は，直結形のトリガー回路を用い，1パルスでシフトさせる方式を開発する必要がある。

(2) 一般の線型フィード・バック・レジスターをM系列の疑似乱数発生器にするための係数 $X_i'(i=1, 2, \cdots, 10)$ の組合わせを計算機で探して，$X_i'=0$ を満足する個数が最大となるものとして $X_1'=1$, $X_3'=1$, $X_{10}'=1$ 他はすべて零という組合わせのものを得た。

(3) M系列疑似乱数発生器に必要な三値の「三を法とする加算回路を真理値表を用いて，論理最小項展開により論理設計を行ない，それを参考としてより簡略化した二組の回路を見出した。

(4) 否定入力の閾値関数的な三値一入力の論理回路および否定回路などを設計し，これらと(3)の結果を用いて「三を法とする加算回路」を製作した。

(5) 発振器，パルス成形器，および試作したシフト・レジスターと三を法とする和の回路を

用いて三値レベル式のM系列疑似乱数の発生器を構成した。正常作動をチェックする回路も設け，10数 KHz までは充分正常に動作することを確めた。今回は特に高速作動のための配慮をしていないので，この程度にとどまった。

この装置の原型においての論理設計と回路設計の討論には当時福井大学の学生であった玉置広志，藤永隆一の両君が参加した。また回路の大半は両君の作製によるものである。ここに感謝の意を表わす。

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（1969）
2）脇本和昌；乱数の知識，森北出版（1970）
3）高田和郎，國末浩；三レベル式三安定回路の改良，川医誌—般教養編 No. 2（1976）
4）昭和46年電気四学会北陸支部会にて講演
5）情報処理学会編；電子計算機ハンドブック，オーム社
6）三根，長谷川，古賀，池田，新谷；三安定回路の構成・解析及び三値フィード・バック・レジスターへの応用，信学誌 p. 443〜p. 450（1969）