

(19)日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11)特許番号

第2801150号

(45)発行日 平成10年(1998) 9月21日

(24)登録日 平成10年(1998) 7月10日

(51)Int.Cl. ⁶	識別記号	F I
G 0 6 F 7/58		G 0 6 F 7/58 A
	5 2 0	15/18 5 2 0 K
H 0 3 K 3/64		H 0 3 K 3/64

請求項の数4 (全 23 頁)

(21)出願番号	特願平6-217240	(73)特許権者	591018497 山川 烈 福岡県飯塚市大字幸袋781番地300
(22)出願日	平成6年(1994)9月12日	(72)発明者	山川 烈 福岡県飯塚市大字幸袋781番地300
(65)公開番号	特開平8-83166	(74)代理人	弁理士 吉田 研二 (外2名)
(43)公開日	平成8年(1996)3月26日	審査官	朽名 一夫
審査請求日	平成8年(1996)8月29日	(58)調査した分野(Int.Cl. ⁶ , DB名)	G06F 7/58

(54)【発明の名称】 カオス信号発生器

1

(57)【特許請求の範囲】

【請求項1】 入力デジタル信号に、デジタルテントマップを適用し、適用後の出力デジタル信号を出力するデジタルテントマッピング手段と、オフセット信号を出力するオフセットカウンタと、前記出力デジタル信号から前記オフセット信号を減算する減算手段と、前記減算後の出力デジタル信号を1クロック遅延させて、前記デジタルテントマッピング手段に、次の入力デジタル信号として供給する遅延手段と、前記オフセットカウンタがカウント動作を行った後に、前記遅延手段が最初に出力する入力デジタル信号を記憶する記憶手段と、前記記憶手段に記憶されている信号の値と、前記遅延手段が出力する入力デジタル信号の値とを比較し、一致

2

した場合に前記オフセットカウンタにクロック信号を印加し、前記オフセットカウンタにカウント動作させるコンパレータと、

を含み、前記入力デジタル信号をカオス信号として外部に出力することを特徴とするカオス信号発生器。

【請求項2】 前記請求項1記載のカオス信号発生器において、

前記オフセットカウンタは、 2^{p-1} 以上で、 $2^p - 1$ 以下の範囲の値 (p は発生されるカオス信号のビット数) の信号のみを出力することを特徴とするカオス信号発生器。

【請求項3】 前記請求項1記載のカオス信号発生器において、

前記オフセットカウンタの出力するオフセット信号を、pビットの 2^{p-1} と加算し、pビットのデジタル信号

10

(p は発生するカオス信号のビット数) に変換する加算手段、

を含み、

前記オフセットカウンタは $p - 1$ ビットのオフセット信号を出力するカウンタであり、

前記減算手段は、前記出力デジタル信号から、前記加算手段が出力する p ビットのオフセット信号を減算することを特徴とするカオス信号発生器。

【請求項 4】 p (p は 1 以上の整数) ビットの入力デジタル信号に、デジタルテントマップを適用し、適用後の p ビットの出力デジタル信号を出力するデジタルテントマッピング手段と、

$p - 1$ ビットのオフセット信号を出力するオフセット算出手段と、

前記オフセット算出手段が出力する $p - 1$ ビットのオフセット信号を、 p ビットの 2^{p-1} と加算し、 p ビットの信号に変換する加算手段と、

前記出力デジタル信号から、前記加算手段の出力信号を減算する減算手段と、

前記減算後の出力デジタル信号を 1 クロック遅延させて、前記デジタルテントマッピング手段に、次の入力デジタル信号として供給する遅延手段と、

前記オフセット算出手段が出力するオフセット信号を更新した後に、前記遅延手段が最初に出力する入力デジタル信号を記憶する記憶手段と、

前記記憶手段に記憶されている信号の値と、前記遅延手段が出力する入力デジタル信号の値とを比較し、一致した場合に前記オフセット算出手段にクロック信号を印加し、前記オフセット算出手段にオフセットの更新動作を行わせるコンパレータと、

を含み、前記入力デジタル信号をカオス信号として外部に出力することを特徴とするカオス信号発生器。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、カオス信号発生器に関する。特に、デジタル回路を用いて構成されているにもかかわらず、長い周期のカオス信号が得られるカオス信号発生器に関する。

【0002】

【従来の技術】時間的に変化する信号値の大きさが予測できない信号をカオス信号と称し、自然界に発生するカオス信号的な自然現象の解明、あるいは予測するためにこれらの現象を模擬する信号として有用であり、今後極めて重要な信号となることが予想されている。

【0003】このような予測不能なカオス信号は、更に各種の産業分野におけるランダム信号としても用いられる。例えば、布地、台紙その他の表面に施される模様パターンの製作時においては、基本的なパターンに対して前記カオス信号を付加することにより、基本パターンを予測できない方向あるいは大ききで変形させ、同一パタ

ーンの生じない模様を容易に得ることができるという利点がある。

【0004】また、このようなカオス信号は、ノイズシャワー、あるいはコンピュータシステムのテスト用として用いられるランダムベクター信号としても用いられ、これらのカオス信号は同時に複数個発生するランダムシグナルをコンピュータの入力に供給し、これによって、コンピュータシステムその他の産業機器に対して、極めて短時間でその特性の検査を行い得る。

10 【0005】従って、将来においても、このようなカオス信号は広い分野において要求される。

【0006】従来においてこの種のカオス信号を得るための最も簡単な手法の一つとして、次元写像を用いたものがある。図 27 はこの次元写像による手法を説明するグラフである。図 27 のグラフに示されているように、ここで用いられている次元写像は関数 $X_{n+1} = 4X_n(1 - X_n)$ である。尚、図 27 のグラフは横軸が X_n を表し、縦軸が X_{n+1} を表す。そして、この n は 0 以上の整数である。つまり、初期値は X_0 であり、

20 図 27 のグラフにおいては初期値 X_0 が 0.1 である場合についての値の変化の例が示されている。

【0007】図 27 に示されているように、初期値 X_0 ($= 0.1$) に対して関数 $4X_n(1 - X_n)$ を適用することにより、 X_1 ($= 0.35$) が得られる。この X_1 ($= 0.35$) に対して同じ関数を再び適用すれば X_2 が得られるが、図 27 においては、これを図示的に求められるように、 $X_{n+1} = X_n$ の直線もあわせて示している。この $X_{n+1} = X_n$ の直線は Identity Line と呼ばれる。

30 【0008】この Identity Line を用いれば、前述した X_1 ($= 0.35$) に対して上記関数を再び適用することが視覚的に容易になる。

【0009】すなわち、図 27 における X_n の軸上の所定の値の X_n から向かって上方向に (すなわち、 X_{n+1} の軸に平行に) 線をのばして上記関数 $X_{n+1} = 4X_n(1 - X_n)$ と交わった点を求めれば、その点の X_{n+1} 座標が、前記 X_n に前記関数 $X_{n+1} = 4X_n(1 - X_n)$ を適用した結果である。

40 【0010】そして、このようにして得られた X_{n+1} を、新たな X_n として、再び上記関数 $X_{n+1} = 4X_n(1 - X_n)$ を適用するためには、まず、上記交点 ($X_{n+1} = 4X_n(1 - X_n)$ 上の点) から横方向に向かつて (すなわち、 X_{n+1} の値を一定にして) 線をのばし、上述した Identity Line と交わる点を求める。この Identity Line 上は $X_n = X_{n+1}$ であるため、この求められた交点の X_n 座標は X_{n+1} と等しくなる。従って、この交点から再び関数 $X_{n+1} = 4X_n(1 - X_n)$ に向かつて縦方向の (X_{n+1} 軸と平行な) 線をのばすことにより、この線と関数

50 $X_{n+1} = 4X_n(1 - X_n)$ との交点を求める。する

と、この交点の X_{n+1} 座標が新たな値を表す点となる。

【0011】このように、関数 $X_{n+1} = 4X_n(1 - X_n)$ を繰り返し適用することにより、一連の数列 $X_0, X_1, X_2, X_3, \dots$ が得られる。

【0012】さて、関数 $X_{n+1} = 4X_n(1 - X_n)$ は、一般的に $X_{n+1} = aX_n(1 - X_n)$ と書くことができる。そして、従来からこの a の値として、4以外の値を用いた場合についても、この関数の振る舞いが調べられている。

【0013】図28には、 $X_{n+1} = aX_n(1 - X_n)$ のパラメータ a を変化させた場合のこの関数による数列 $X_0, X_1, X_2, X_3, \dots$ の挙動を表すグラフが示されている。この図28に示されているグラフは縦軸が X_n ($n = 0, 1, 2, 3, \dots$) の値であり、横軸が n の値である。このグラフには、上記パラメータ a の値を変化させた場合の複数のグラフが、各パラメータについて初期値として $X_0 = 0.1, 0.5, 0.9$ を与えた場合について示されている。例えば、 $a = 3.0$ の場合には、 X_n の値はおよそ 0.6 と 0.7 との間を振動することが理解されよう。また、 $a = 2.5$ の場合には、 X_n の値は n が大きくなるにつれて 0.6 に収束する。また、 $a = 1.5$ の場合には 0.33 ($= 1/3$) に収束し、 $a = 0.5$ の場合には 0 に収束する。

【0014】また、図29には $a = 3.8$ の場合の X_n の値の列のグラフが示されている。図29に示されているように、およそ 0.2 からおよそ 0.95 までの間で見かけ上ランダムに値が現れているように見える。

【0015】このように、関数 $X_{n+1} = aX_n(1 - X_n)$ のパラメータ a を変化させると X_n の値の列が一定の値に収束したり、ランダムな値を採り続けたりする。このパラメータ a の値と、 X_n の採りうる値との関係を表したグラフが図30に示されている。図30に示されているグラフは周期倍分岐図と呼ばれている。このグラフでは、横軸はパラメータ a であり、縦軸は X_n (n は十分大きいとしている) の採りうる値を示している。上述したように、パラメータ a がおよそ3未満の場合には X_n は一定の値に収束するが、 a が大きくなるに従って、 X_n の採りうる値の種類が増えていく。図30に示されているように、 a がほぼ3以上になると、 X_n の採りうる値の個数が2種類になり、およそ a が 3.45 以上では4種類となる。

【0016】図30に示されている周期倍分岐図のパラメータ a が 2.8 から 4.0 までの間を拡大したグラフが図31に示されている。このグラフでも横軸がパラメータ a を示し、縦軸は X_n をそれぞれ示す。図31に示されているように、パラメータ a がおよそ 3.565 を越えると X_n の採りうる値はさらに8個に増える。また、図31に示されている周期倍分岐図のパラメータ a

が 3.54 から 3.64 の間の拡大図が図32に示されている。図32に示されているように、パラメータ a が 3.57 を越えると X_n の採りうる値はさらに16個に増える。 a が4になると、 X_n の値は 0 から 1 までの間に見かけ上ランダムに分布するようになる。

【0017】このように、関数 $X_{n+1} = aX_n(1 - X_n)$ を用いて、特にパラメータ a が4の時に見かけ上ランダムなカオス信号を得ることができる。

【0018】同様のことが、他の関数を用いても実現される。単に三角形の山形の関数を用いてもカオス信号を作成することができる。例えば、次のような関数が好適である。

【0019】

$$X_{n+1} = k(X_n) \quad (0 \leq X_n < 0.5) \\ = k(-X_n + 1) \quad (0.5 \leq X_n < 1.0)$$

この関数におけるパラメータ k を 0 から 2.0 までの間で変化させた場合の周期倍分岐図が図33に示されている。図33に示されているグラフの横軸はパラメータ k であり、縦軸は X_n の値である。図33に示されているように、パラメータ k が2になると見かけ上ランダムなカオス信号が得られる。また、このような三角形の関数を用いた場合は、上述した関数 $X_{n+1} = aX_n(1 - X_n)$ と異なり、採りうる X_n の値が 0 から 1 の間で一様に分布することが知られている。

【0020】図34には、パラメータ k が 0.5 である場合の X_n の値の変化を表すグラフが示されている。図34に示されているグラフは、横軸が n を表し、縦軸が X_n の値を表す。このグラフには初期値 X_0 が 0.1 の場合と、 0.5 の場合と 0.9 の場合との3つの場合についての X_n の値の変化が示されているが、いずれの場合においてもおよそ X_1 以降においては X_n の値は 0.0 に収束している。

【0021】図35には、パラメータ k が 1.00 である場合の X_n の値の変化を表すグラフが示されている。図35に示されているグラフも横軸が n を表し、縦軸が X_n の値を表す。このグラフには初期値 X_0 が 0.1 の場合と、 0.5 の場合と 0.9 の場合との3つの場合についての X_n の値の変化が示されているが、それぞれの場合において収束する値が異なっている。つまり、初期値 X_0 が 0.1 の場合は収束する値は 0.1 である。また、初期値が 0.5 の場合もその収束する値は 0.5 である。一方、初期値 X_0 が 0.9 の場合には収束する値は 0.1 となる。

【0022】図36には、パラメータ k が 1.10 である場合の X_n の値の変化を表すグラフが示されている。図36に示されているグラフも横軸が n を表し、縦軸が X_n の値を表す。このグラフには初期値 X_0 が 0.1 の場合と、 0.5 の場合と 0.9 の場合との3つの場合についての X_n の値の変化が示されているが、いずれの場合も最終的な状態に近づく速度は異なるものの、およそ

0.5と、0.55との間を往復するような振動状態に陥る。

【0023】次に、図37には、パラメータkが1.25である場合のXnの値の変化を表すグラフが示されている。図37に示されているグラフも横軸がnを表し、縦軸がXnの値を表す。このグラフには初期値X0が0.1の場合と、0.5の場合と0.9の場合との3つの場合についてのXnの値の変化が示されているが、いずれの場合も最終的な状態に近づく速度は異なるものの、およそ0.5と、0.6との間を往復するような振動状態に陥る。

【0024】また、図38には、パラメータkが1.99である場合のXnの値の変化を表すグラフが示されている。図38に示されているグラフも横軸がnを表し、縦軸がXnの値を表す。このグラフには初期値X0が0.1の場合と、0.5の場合と0.9の場合との3つの場合についてのXnの値の変化が示されているが、いずれの場合も、およそ0.0と、1.0との間を一見するとランダム状に動くカオス信号である。

【0025】以上述べたように、所定の一次写像である所定の関数を用いてカオス信号を得る手法が、従来知られている。

【0026】

【発明が解決しようとする課題】しかしながら、上記手法はあくまでも数学理論に基づくものであり、そのため、数値は実数として取り扱う必要がある。すなわち、実際の装置として構成するにはアナログ信号による装置としなければならない。

【0027】近年、デジタル技術の進展に伴い、デジタル信号を取り扱う装置においてもランダムなカオス信号を用いる必要が生じている。このようなデジタルシステムにおいて、上記のような山形の関数を用いてカオス信号を得ようとする、例えば、図39に示されているような入出力関係を有するデジタルテントマップを用いることが第一に考えられよう。

【0028】図39に示されているのは、3ビットのデジタル信号を用いて、上述したような山形の三角形形状の関数、すなわちデジタルテントマップを表すグラフである。また、図40には、同じく4ビットの場合のデジタルテントマップを表すグラフが示されている。ここで、横軸はXnを表し、縦軸はXn+1を表すことになる。一般にデジタルテントマップを定義する式は、以下のように表される。

【0029】

$$X_{n+1} = 2(X_n) + 1 \quad (0 \leq X_n < 2^{p-1})$$

$$= 2(2^p - 1 - X_n) \quad (2^{p-1} \leq X_n < 2^p)$$

ここで、pはビット数を表し、図39に示されているグラフにおいてはpは3であり、図40に示されているグラフにおいてはpは4である。このようなデジタルテ

ントマップを用いてカオス信号を得るための構成の例が図41に示されている。図41に示されているように、デジタルテントマップを実現するデジタルテントマッピング手段(Tent Mapping)10と、1クロックの時間遅延を生じさせるディレイエレメント(Delay Element)12とを組み合わせループを形成することによって、カオス信号発生器は構成されている。図41において説明されているように、デジタルテントマッピング手段10は、3ビットのデジタルテントマップを記録したテーブル、例えばROM等により構成されており、入力されるXnを、Xn+1に変換する。一方、ディレイエレメント12は、デジタルテントマッピング手段10から出力されたXn+1を、1クロックだけ時間遅延させる。これによって、Xn+1は、次の周期においてはXnとして用いられる。

【0030】換言すれば、このディレイエレメント12は、identity lineを表したものであるとも言えよう。このディレイエレメント12によって1クロックだけ遅延された信号は、次の周期においてデジタルテントマッピング手段10に入力される。

【0031】このような、デジタルテントマップによるカオス信号の発生の様子を説明するための模式図が図42に示されている。図42に示されているように、初期値X0が「0」の場合には、デジタルテントマッピング手段によって、X1が「1」と算出される。この「1」であるX1がディレイエレメント12が実現しているidentity lineを介して、再びデジタルテントマッピング手段10に印可される。その結果、X2として、「3」が算出される。以下、同様にして、X3、X4、X5、X6が、「7」、「0」、「1」が算出される。このような繰り返し(iteration)から、容易に理解されるように、この例によるXnの値は、「0」、「1」、「3」、「7」の繰り返しとなる。この繰り返しの値は初期値によって変わり、初期値を「0」とすれば上述したシーケンスの信号が得られ、初期値を「2」とすれば「2」、「5」、「4」、「6」という順の信号が得られる。このように、3ビットの場合の最大周期は4周期である。

【0032】尚、4ビットのデジタルテントマップを使用しても同様に一定のシーケンスの信号の列が得られる。図41におけるデジタルテントマッピング手段10のデジタルテントマップとして、図40に示されている4ビットのデジタルテントマップを採用すると、得られるXnの値の列は次の4種類存在する。

【0033】

- 「0」、「1」、「3」、「7」、「15」
- 「2」、「5」、「11」、「8」、「14」
- 「4」、「9」、「12」、「6」、「13」
- 「10」、「10」、「10」、「10」、「10」

この4種類のX_nの列から容易に理解されるように、4ビットの場合の最大周期は5である。一般に任意のビット数pにおける最大周期はp + 1であることを本願発明者は実験的に確認した。

【0034】しかし、このp + 1という周期は、表現できる数からすると、極めて短い周期であると言えよう。例えば、一定のランダムな値を生成する手法としていわゆるM系列がよく知られている。

$$x_t = 0 \cdot a_{t-1} + a_{t-2} + \dots + a_{t-L} \quad (2 \text{進数表現})$$

ここで、1、2・・・、Lは互いに異なり、tに無関係な定数である。1 = 0としても一般性を失わないので、以降 1 = 0とする。

【0037】<x_t>は、<a_t>の位相を適当にずらしたものを各ビットに配置して構成される。つまり、<x_t>の各ビット位置に現れる数列は、同一の漸化式によって生成される。したがって、次の漸化式を用いることによって、<x_t>を高速に生成することができる。

【0038】

$$x_t = c_1 \cdot x_{t-1} + c_2 \cdot x_{t-2} + \dots + x_{t-p}$$

尚、上式における「+」はビット毎の繰り上がりなしの足し算を表す。これは、多くの計算機に備えられている排他的論理和 (EXOR) の演算機能を使用することにより高速に処理することができる。特に特性多項式 f が 3項式

$$f(D) = 1 + D^q + D^p \quad (q < p)$$

の場合には上記 x_t の漸化式は、

$$x_t = x_{t-q} + x_{t-p}$$

となり、1回の排他的論理和の演算によって乱数1個が生成されるので、大幅に高速化することができる。

【0039】また、このM系列を発生する装置の例が図43に示されている。図43には4段M系列シフトレジスタの回路図が示されている。この4段M系列シフトレジスタは、初段への帰還入力D₀がD₀ = Q₂ + Q₃となるように、図中の2番目及び3番目の段からEXOR (排他的論理和) 帰還を付けている。ここで「+」は、排他的論理和を表す。このレジスタの初期状態をQ₀ = 1、Q₁ = 0、Q₂ = 0、Q₃ = 0とすると、D₀ = Q₂ + Q₃ = 0 + 0となるので、次のクロックパルスが入ると、レジスタの内容はQ₀ = 0、Q₁ = 1、Q₂ = 0、Q₃ = 0となる。このようにして求めたレジスタの状態に関する完全なシーケンスが図44に示されている。図44に示されている表において、fは各状態での帰還関数である。

【0040】このシフトレジスタの状態数は、全部で15個あり、この数は、EXOR帰還を有する4段シフトレジスタの採りうる最大の状態数である。従って、これを最大周期系列、すなわちM系列と呼ぶのである。状態S₀ = 0000は、これ以上状態が変わることのないいわゆる「ロック・イン」状態であるため、シーケンスには含まれていない。このような回路に対するM系列の長

* 【0035】M系列は、0と1とから成る系列、すなわち1ビットの系列である。しかし乱数列として、通常用いられるのは、例えば合同抱乱数のように、もっと桁数の大きい数列である。そこで、M系列を基にして、L (L - 2) ビットの2進数の系列<x_t>を、次のようにして生成する。

【0036】

さLは、一般にL = 2^N - 1で、与えられる。ここで、Nは、シフトレジスタの段数である。

【0041】尚、EXOR接続されたレジスタが常にM系列を発生するわけではなく、帰還端子に依存することになる。図45には、Nの値に対して、M系列を発生し得るような帰還関数が、N = 18まで示されている。

【0042】また、EXOR関数の否定関数を帰還すれば、同じレジスタ長のままで他のM系列を発生することができ、このとき状態S₀ = 0000は、ロック・イン状態ではなくなる。以上述べたこれらの回路は、周期性があるが、出力シーケンスの数字が明らかに不規則性を有するため、疑似乱数発生器として使用されている。

【0043】このように、デジタルテントマップをそのまま用いたカオス信号発生器においては得られる信号の周期は、例えばM系列などで生成した乱数列と比較して極めて短いので、実用に供することは極めて困難であった。

【0044】本発明は、上記従来の課題に鑑みなされたものであり、その目的は、デジタルテントマップを用いたカオス発生器であって、長い周期の信号を発生させることが可能なカオス信号発生器を提供することである。

【0045】

【課題を解決するための手段】上記目的を達成するために、第一の本発明は、入力デジタル信号に、デジタルテントマップを適用し、適用後の出力デジタル信号を出力するデジタルテントマッピング手段と、オフセット信号を出力するオフセットカウンタと、前記出力デジタル信号から前記オフセット信号を減算する減算手段と、前記減算後の出力デジタル信号を1クロック遅延させて、前記デジタルテントマッピング手段に、次のクロックの入力デジタル信号として供給する遅延手段と、前記オフセットカウンタがカウント動作を行った後に、前記遅延手段が最初に出力する入力デジタル信号を記憶する記憶手段と、前記記憶手段に記憶されている信号の値と、前記遅延手段が出力する入力デジタル信号の値とを比較し、一致した場合に前記オフセットカウンタにクロック信号を印加し、前記オフセットカウンタにカウント動作させるコンパレータと、を含み、前記入力デジタル信号をカオス信号として外部に出力することを特徴とするカオス信号発生器である。

*

10

20

30

40

50

【 0 0 4 6 】上記目的を達成するために、第二の本発明は、前記第一の本発明のカオス信号発生器において、前記オフセットカウンタは、 2^{p-1} 以上で、 $2^p - 1$ 以下の範囲の値（ p は発生されるカオス信号のビット数）の信号のみを出力することを特徴とするカオス信号発生器である。

【 0 0 4 7 】上記目的を達成するために、第三の本発明は、第一の本発明のカオス信号発生器において、前記オフセットカウンタの出力するオフセット信号を、 p ビットの 2^{p-1} と加算し、 p ビットのデジタル信号（ p は発生するカオス信号のビット数）に変換する加算手段、
10 を含み、前記オフセットカウンタは $p - 1$ ビットのオフセット信号を出力するカウンタであり、前記減算手段は、前記出力デジタル信号から、前記加算手段が出力する p ビットのオフセット信号を減算することを特徴とするカオス信号発生器である。

【 0 0 4 8 】上記目的を達成するために、第四の本発明は、 p （ p は1以上の整数）のビットの入力デジタル信号に、デジタルテントマップを適用し、適用後の p ビットの出力デジタル信号を出力するデジタルテントマッピング手段と、 $p - 1$ ビットのオフセット信号を出力するオフセット算出手段と、前記オフセット算出手段が出力する $p - 1$ ビットのオフセット信号を、 p ビットの 2^{p-1} と加算し、 p ビットの信号に変換する加算手段と、前記出力デジタル信号から、前記加算手段の出力信号を減算する減算手段と、前記減算後の出力デジタル信号を1クロック遅延させて、前記デジタルテントマッピング手段に、次のクロックの入力デジタル信号として供給する遅延手段と、前記オフセット算出手段が出力するオフセット信号を更新した後に、前記遅延手段が最初に出力する入力デジタル信号を記憶する記憶手段と、前記記憶手段に記憶されている信号の値と、前記遅延手段が出力する入力デジタル信号の値とを比較し、一致した場合に前記オフセット算出手段にクロック信号を印加し、前記オフセット算出手段にオフセットの更新動作を行わせるコンパレータと、を含み、前記入力デジタル信号をカオス信号として外部に出力することを特徴とするカオス信号発生器である。

【 0 0 4 9 】

【作用】本発明によれば、デジタルテントマッピング
40 手段の出力信号から、所定のオフセット信号を減算し、且つ、同じ値のカオス信号が出力される度にオフセットを更新したので、長い周期を有するカオス信号が得られる。

【 0 0 5 0 】また、オフセットカウンタの出力するオフセットの値を $2^{p-1} \sim 2^p - 1$ の範囲に制限したので、長い周期を有しつつ、且つ、一様性をも満足しうるカオス信号が得られる。このオフセットの範囲は実験により見出したものである。

【 0 0 5 1 】また、一様性を満足するために、オフセッ
50

トの値の範囲を上記範囲に制限することは、 $p - 1$ ビットのカウンタと、 p ビットの 2^{p-1} と前記カウンタの出力信号とを加算する加算手段とを用いれば容易に実現可能である。

【 0 0 5 2 】また、上記カオス信号発生器によれば、オフセットは順にカウンタにより所定の値を加算又は減算することにより更新されるが、このオフセット信号をカオス信号発生器により発生させることも好適であり、上記のカオス信号発生器に比べて、よりランダムな信号を得ることが可能である。

【 0 0 5 3 】

【実施例】以下、図面に基づき本発明の好適な実施例を説明する。

【 0 0 5 4 】上述したように、通常のデジタルテントマップから生成される時系列は周期が極めて短い。

【 0 0 5 5 】写像関数から所定のカオス信号を出力する手法においては、この写像関数の高さを変えることによって、異なる時系列データが得られることが知られている。このことを表す説明図が図1に示されている。図1の（a）は、放物線の関数の高さを変化させた場合の変化の様子を示す説明図であり、図1の（b）は、三角型の関数の山の高さを変化させた場合の変化の様子を示す説明図である。

【 0 0 5 6 】従って、適当なタイミングで写像関数の高さを変化させることにより、異なる時系列データを発生させ、時系列データ全体としての周期を長くすることも考えられるが、ハードウェアが複雑になるため、現実的とは言えない。すなわち、写像関数の高さを変えるには、乗算等を使用しなければならず、ハードウェア規模及び実行速度の点から見て、実際的ではない。

【 0 0 5 7 】そこで、本実施例においては、写像関数を上下に移動（シフト）させることによって、異なる時系列データを発生させている。このように、写像関数を上下にシフトさせた場合の関数のグラフの形状の変化が図2に示されている。すなわち、写像関数に所定のオフセットを加えるのである。これは、図3に示されているように、identity lineを上下に動かすことと等価である。つまり、写像関数の形を変えずに、identity lineを変化させるのである。これはもちろん、図4に示されているように、identity lineの前に所定のオフセットを挿入する手段（オフセット関数）を設けることによっても等価な回路を実現可能である。図4においては、写像関数と、identity lineと、新たに設けた所定のオフセット関数との3つの関数のグラフが示されている。

【 0 0 5 8 】本実施例において特徴的なことはこのように写像関数を適宜変化させることにより、得られる時系列データの周期を長くしたことである。このように、写像関数をいわば「動かす」ことによって、短い周期でデータが繰り返して発生することを防止し、長周期の時系

列データを得ようとするものである。本実施例においては、このように写像関数のパラメータを変化させながら、時系列データの生成を繰り返すので、パラメトリック・イタレーションと呼ぶ。

【0059】本実施例においては、パラメータとして、写像関数に加えられるオフセットを変化させた例を示す。また、このオフセットを変化させる手法として大きく2種類の手法について説明する。本実施例においては、この2種類の手法をそれぞれType 1、Type 2と呼ぶ。

【0060】1.1 Type 1のカオス信号発生器
このType 1のカオス信号発生器においては、上記オフセットは0、1、2、3のように順番に1つずつ増やされていくのである。本実施例においては、このオフセットを加えることは、減算器により実現している。この減算器は、デジタルテントマッピング手段とディレイエレメントとの間に挿入されている。

【0061】図5には、本実施例に係るカオス信号発生器の構成ブロック図が示されている。図5に示されているように、このカオス信号発生器は、ROM等を用いて構成されているデジタルテントマッピング手段100と、ディレイエレメント102と、減算器104とを含んでいる。そして、デジタルテントマッピング手段100の出力信号が減算器104の一方の入力端子に供給されており、この減算器104の出力信号はディレイエレメント102の入力端子に供給されている。そして、このディレイエレメント102の出力信号は、デジタルテントマッピング手段100の入力端子に供給されている。

【0062】本実施例において特徴的なことは、デジタルテントマッピング手段100の出力信号に、減算器104において所定のオフセットが減算されることである。そして、この減算後の信号が、ディレイエレメント102に供給されるのである。この減算器104の他方の入力端子にはオフセットカウンタ106の出力信号が供給されており、デジタルテントマッピング手段100の出力信号は、このオフセットカウンタ106が出力するオフセットの分だけ減算されるのである。

【0063】ディレイエレメント102の出力信号は、前述したデジタルテントマッピング手段100に供給されるとともに、レジスタ108とコンパレータ110とも供給されている。レジスタ108は、オフセットカウンタ106がカウントアップした後、1クロック後のディレイエレメント102の出力信号を記憶保持する。すなわち、オフセットカウンタ106がインクリメントし、新たなオフセットが加えられた最初のデータが1クロック後にディレイエレメント102から出力されるが、その最初のデータがレジスタ108に記憶保持されるのである。

【0064】一方、コンパレータ110は、このレジ

タ108に記憶保持されている値と、ディレイエレメント102から出力されるデータとを常に監視しており、両データが一致した場合に一致信号を出力するのである。そして、上述したように、この一致信号が出力されると、オフセットカウンタ106がカウントアップするのである。レジスタ108に記憶保持されている値と、ディレイエレメント102から出力されるデータとが一致する場合は、オフセットカウンタ106が所定の値をオフセットとして出力した後に、ディレイエレメント102から同じ値が出力された場合である。上述したように、レジスタ108は、オフセットカウンタ106がカウントアップし、新たな値がオフセット値として出力された後の最初のデータを記憶保持する。このレジスタ108の記憶保持する値がディレイエレメント102の出力信号の値と一致するという事は、同一のオフセット値に対して同一の値がディレイエレメント102から出力されたことを意味し、このことはすなわちデジタルテントマップにおける一周期分のデータが出力されて、二周期目(つまり一周期目と同一)のデータがちょうど出力し始めていることを意味する。

【0065】尚、本実施例においては便宜上、図5に示されているように、デジタルテントマッピング手段100の出力信号を X'_{n+1} で表し、減算器104の出力信号を新たに X_{n+1} で表すことにしている。また、図5中のpは、デジタルデータのビット数を表す。

【0066】図6には、本実施例のカオス信号発生器の動作を表すフローチャートが示されている。

【0067】まず、電源投入又は外部からのリセット信号等により、本カオス信号発生器の初期設定がステップ6-1において行われる。このステップ6-1においては、初期値である X_0 の設定と、オフセット(off set)の設定と、ループ変数であるnを0にする設定とが行われる。

【0068】次にステップ6-2においては、この初期値 X_0 の値がレジスタ(register)108に記憶保持される。

【0069】ステップ6-3においては、 X_n が外部にカオス信号として出力される。

【0070】ステップ6-4においては、デジタルテントマッピング手段100において、外部に出力した X_n の値の写像が行われる。この写像の結果が X'_{n+1} である。

【0071】ステップ6-5においては、上記写像の結果得られた値 X'_{n+1} からオフセット(off set)値が減算される。この減算によって X_{n+1} が得られる。

【0072】ステップ6-6においては、ループ変数であるnがインクリメント、すなわち+1される。

【0073】次にステップ6-7において、オフセット(off set)を変えた直後か否かが検査される。す

なわち、オフセット値に対する最初のカオス信号（時系列データ）であるか否かが検査されるのである。その結果、オフセットを変えた直後である場合にはステップ6 - 8に処理が移行し、オフセットを変えた直後でない場合にはステップ6 - 9に処理が移行する。

【0074】ステップ6 - 8においては、 X_n をレジスタ(register)に記憶させる。このように、あるオフセット値における最初に出力されたカオス信号（時系列データ）をレジスタ(register)に記憶させることにより、同一のオフセット値に対して同一の X_n が出力されたか否かを検出することができるようにするものである。尚、このステップ6 - 8の処理の後には前述したステップ6 - 3に処理が移行する。

【0075】ステップ6 - 9においては、 X_n とレジスタの値が等しいか否かが検査される。これは同一のオフセット値に対してそのオフセット値に変更されてから最初の X_n と同一の値のカオス信号（時系列データ）が出力されたか否かを検査するものである。ここで、同一のデータが出力されたと判断された場合には、次のステップ6 - 10に処理が移行し、同一でないとは判断された場合には上述したステップ6 - 3に処理が移行する。

【0076】ステップ6 - 10においてはオフセット（値）がインクリメントされる。これは同一のオフセットに対して同一の X_n が出力されたので、そのオフセットに対する一周期のデータが出力され終わったことを意味する。従って、かかる場合には、本ステップにおいてオフセットを更新すべくオフセット（値）のインクリメントを行うのである。

【0077】次に、本実施例においてコンパレータ110がデータの一致を検出した場合の本カオス信号発生器の動作の例を具体的な数値に基づいて詳細に説明する。図7には、本実施例の動作についての説明図が示されている。この説明図は、上記図4と同様に、デジタルテントマップと、オフセット関数と、identity lineの関数のそれぞれのグラフが示されている。また、この説明図においては、初期値が「0」であり、オフセットが「0」である状態からの動作が説明されている。さらに、ビット数 p は3である。

【0078】まず、初期値 X_0 は「0」であるから、時系列データは、「0」、「1」、「3」、「7」、「0」と出力される。最初の初期値 X_0 の「0」という値はレジスタ108に記憶保持される。従って、 X_4 が「0」であることから、 X_4 が出力された時点で一周期が経過したことがわかる。上述したように、一周期が経過したことがコンパレータ110において検出されるとコンパレータ110は一致信号を出力する。すると、オフセットカウンタ106がカウントアップし、オフセットが「1」に更新される。このオフセットが「1」に更新されたことは、図7中のオフセット関数のグラフが（1）から（2）に変化することによって表される。

【0079】このようにして、オフセットが「1」の状態を引き続いて時系列データが出力される。オフセットが「0」の状態における最後のデータ「0」に基づいて、まずデジタルテントマッピング手段100により、この「0」は「1」に変換される。これは図7の左上のグラフに示されていることであり、デジタルテントマッピング手段100の出力信号 X'_{n+1} が「1」となることが理解されよう。次にこの「1」が図7中の（2）で示される関数に従って変更される。この結果、「1」は「0」に変化し、最終的に X_n として「0」が出力される。

【0080】すなわち、本実施例に係るカオス信号発生器においては、上述したようにまずオフセットが「0」の状態「0」、「1」、「3」、「7」、「0」と出力され、次にオフセットが「1」の状態「0」と出力される。この最後の X_5 （その値は「0」）がオフセットが「1」の状態における最初の時系列データであるので、レジスタ108に記憶保持される。

【0081】また、オフセット「1」の状態では出力される時系列データとして「0」が繰り返されるので、次の X_6 が「0」であり、先にレジスタ108に記憶保持された X_5 のデータと一致することが検出される。すると、上述したのと同様に、コンパレータ110から一致信号が出力され、オフセットカウンタ106がカウントアップする。すなわちオフセットの値が新たに「2」となるのである。このように、オフセットの値が「1」から「2」になる様子が図8に示されている。図中（2）、（3）はそれぞれオフセットの値が「1」、「2」の場合のオフセット関数である。

【0082】「0」である X_5 がデジタルテントマッピング手段100において「1」に変換され、これがオフセット関数（2）により「0」に変換され、 X_0 として現われる。オフセット関数（2）によって既に「0」が出ているのでここでオフセットを「1」から「2」に更新し、オフセット関数を（2）から（3）に変更する。次に X_6 である「0」はデジタルテントマッピング手段100において「1」に変換され、これは新しいオフセット関数（3）により「7」に変換され、ディレイエレメント102から X_7 として出力される。以下、同様にして、このオフセットの値が「2」の状態 $X_7 = 「7」、X_8 = 「6」、X_9 = 「0」、X_{10} = 「7」と時系列データが出力される。そして、この X_{10} が「7」であることがコンパレータ110によって検出された時点で再びオフセットが更新される。以下、同様にして、同一のオフセット値に対して同一の値が出力された場合に、オフセット値を更新していくことにより、極めて長い周期のカオス信号を得ることができる。$

【0083】尚、図7及び8において \wedge が挿入されているところは、その時点においてオフセット値が更新されたことを表す。以上のようにして本実施例においては順

に、「0」、「1」、「3」、「7」、「0」^
「0」、「0」^「7」、「6」、「0」、「7」^
「5」、「1」、「0」、「6」、「7」、「5」^
「0」、「5」、「0」^「4」・・・のようにカオ
ス信号（時系列データ）が出力される。本実施例に係る
カオス信号発生器によって発生したカオス信号の最初の
50個の例が図9に示されている。図9には、横軸が時間
n (Time) を表し、縦軸はカオス信号の値 (Signal
Level) を表すグラフが示されている。また、この
グラフの下部には、オフセット関数 (offset
function) のグラフの形を表す番号が示されている。尚、
本実施例に係るカオス発生器の出力するカオス信号の
周期は291周期となり、単にデジタルテントマッピン
グを用いた場合（最大周期は4）と比較して大幅に周
期を長くすることが可能となった。

【0084】このように、Type 1のカオス信号発生器
によれば長周期のカオス信号を得ることができるが、
周期は初期値によっても変化することが本願発明者によ
って確認されている。また、カオス信号（時系列デー
タ）に一様性が得られず、ビット数が多くなるほど、分
布に2つの山がでてくる傾向にある。例えば、データの
ビット幅が3ビットであって、初期値が0の場合の1周
期分のデータ（291個）のヒストグラムが図10に示さ
れている。図10に示されているヒストグラムにおいて、
縦軸は頻度 (Frequency) を表し、横軸は信号の値
(Signal Level) を表す。また、データのビット幅が8
ビットであって、初期値が3である場合の1周期分の
データ（2,433,158個）のヒストグラムが図11に示
されている。図11についても、図10と同様に、縦軸は
頻度 (Frequency) を表し、横軸は信号の値 (Signal
Level) を表す。

【0085】1.2 非一様分布の改善

オフセットの状態と時系列のヒストグラムとの関係に
ついて以下説明する。

【0086】例えば、8ビットの場合にはオフセットの
値は0~255の範囲で変化するが、この範囲を、説明
の便宜上4つの区間に分割し、各領域におけるヒストグ
ラムを上述したヒストグラムと同様に求める。

【0087】4つの区間は(a):0~63と、
(b):64~127と、(c):128~191と、
(d):192~255と、の4つの区間である。これら
4つの区間をオフセット関数のグラフ上で表すと、図
12に示されているように各区間に対応する領域として
表現される。これらの4つの区間に対するヒストグラム
が、図13から図16にそれぞれ示されている(図13:
(a)区間、図14:(b)区間、図15:(c)区間、
図16:(d)区間)。

【0088】ここで、区間(c)(d)において、つまり
オフセットが128~255の範囲においては、カオ

ス信号（時系列データ）の値はその区間において一様
に分布していることが上記図15、16から実験的に確
認される。本願発明者は、8ビット以外の他のビット
数の場合にもほぼ同様の傾向があることを確認した。

【0089】従って、カオスデータ（時系列データ）の
非一様分布の原因はオフセットの状態にあるといえる。
一様分布となることが期待されるオフセットの状態は、
図17に示されているように、 $2^{p-1} \sim 2^p - 1$
(ここで、pはビット数である)となる場合である。

【0090】このような実験結果から、カオス信号（時
系列データ）が一様分布となるような範囲内でオフセ
ットを変化させることも好適である。Type 1のカオス
信号発生器においてオフセットの変化する範囲を図17
の()の範囲でのみ動かすように制限したカオス信号
発生器の構成ブロック図が図18に示されている。

【0091】図18に示されているように、この改良さ
れたType 1のカオス信号発生器においては、オフセ
ットカウンタ206がp-1ビットで構成されていること
である。このオフセットカウンタ206の出力信号に加
算器204bにおいて 2^{p-1} を加算することにより、
減算器204aに供給される減数は $2^{p-1} \sim 2^p - 1$
の範囲の数となる。この減算器204aは、前述した図5
に示されているType 1のカオス信号発生器の減算器
204と同等の構成要素である。つまり、図18に示さ
れている構成が図5に示されている構成と異なる点は、
オフセットカウンタ206のビット数が1つ小さいこと
と、新たに加算器204bがもうけられている点であ
る。これらの構成により、 X'_{n+1} から減算される数
を $2^{p-1} \sim 2^p - 1$ の範囲の数とすることができ、得
られる信号列の一様性が確保される。

【0092】図18の構成によれば、具体的に次のよう
な結果が得られた。

【0093】ビット数が3ビットであって、初期値が2
の場合のカオス信号（時系列データ）（初期点から50
点まで、112周期）のグラフが図19に示されてい
る。図9に示されているグラフは、縦軸が信号の値
(Signal Level) を表し、横軸が X_n のn、すなわち
換言すれば時間 (Time) を表すものである。尚、この
図19も図9と同様に、その下部にオフセット関数
(offset function) の値が記載されている。

【0094】ビット数が3ビットであって、初期値が2
の場合のカオス信号（時系列データ）の一周期分
(112周期)のデータのヒストグラムが図20に示されて
いる。このヒストグラムにおいて、縦軸は頻度
(Frequency) を表し、横軸は信号の値 (Signal
Level) を表す。

【0095】ビット数が8ビットであって、初期値が0
の場合のカオス信号（時系列データ）の一周期分(1,

726, 201周期)のデータのヒストグラムが図21に示されている。このヒストグラムにおいても同様に、縦軸は頻度(Frequency)を表し、横軸は信号の値(Signal Level)を表す。

【0096】この図20及び21に示されているヒストグラムから理解されるように、この改良型のType1のカオス信号発生器によれば、一様性を有するカオス信号(時系列データ)を得ることができる。

【0097】このようにして得られたカオス信号の一様性を検証するために、²検定を行った。データ幅が8ビットであり、初期値が0の場合の100,000点のデータを16分割した場合の²検定の結果は、7.84であり²₁₅(0.05)=25.0以下となり、有意水準5パーセントで等確率性が保証された。

【0098】従って、この改良型のType1のカオス信号発生器によるカオス信号は、一様乱数として十分に使用可能である。

【0099】2. Type2のカオス信号発生器
次にType2のカオス信号発生器について説明する。

【0100】上記Type1のカオス発生器においてはオフセットを0、1、2、3のように順番に1つずつ増やしていったが、Type2のカオス発生器においては、乱数により、オフセット値を決定していく。この乱数を発生するカオス信号発生器は、上述した改良型のType1のカオス信号発生器を用いる。

【0101】このように、カオス信号発生器の出力信号をオフセットとして利用するType2のカオス信号発生器のブロック構成図が図22に示されている。ここでオフセットとして利用するのはType1のカオス信号発生器306である。

【0102】このType1のカオス信号発生器306はp-1ビットの乱数(カオス信号)をコンパレータ310から一致信号が出力される度に出力する。このType2のカオス信号発生器の周期を以下に示す。

【0103】データ幅が3ビットであり、初期値が0の場合のカオス信号(時系列データ)の周期は189となった。また、この場合の初期値から50点までの信号の値のグラフが図23に示されている。図23に示されているグラフは、図19などのグラフと同様に、縦軸が信号の値(Signal Level)を表し、横軸がX_nのn、換言すれば時間(Time)を表す。

【0104】また、データ幅が3ビットであり、初期値が0の場合の一周期分(189信号点)のカオス信号(時系列データ)のヒストグラムが図24に示されている。図24に示されているヒストグラムは、図10などのヒストグラムと同様に、縦軸が頻度(Frequency)を表し、横軸が信号の値(Signal Level)を表す。

【0105】また、データ幅が8ビットであり、初期値が0の場合の一周期分(268, 435, 456信号

点)のカオス信号(時系列データ)のヒストグラムが図25に示されている。図25に示されているヒストグラムは、図24のヒストグラムと同様に、縦軸が頻度(Frequency)を表し、横軸が信号の値(Signal Level)を表す。

【0106】また、データ幅が8ビットであり、初期値が0の場合の1000, 000点のデータを16分割した場合の²検定の結果は10.80で²₁₅(0.05)=25.0以下となり、有意水準5パーセントで、等確立性が保証された。従って、このType2のカオス信号発生器の出力信号を一様乱数として種々の利用に供することが可能である。

【0107】3. 最大周期の比較

以上述べたように、本実施例によれば、通常のデジタル点とマップを用いた方法と比較して極めて長い周期の信号を出力することができる。そこで、本実施例で述べたパラメトリック・イタレーションのType1及びType2と、M系列乱数と、デジタルテントマップを用いた数列と、における最大周期を比較する。この比較はパラメータとしてビット数(Bits)を横軸にとり、縦軸が最大周期(Maximum Period)を表すグラフを作成することにより行った。このグラフが図26に示されている。このグラフから理解されるように、一般的な乱数の生成に頻繁に用いられるM系列(M-Sequence)と比較して、本発明であるパラメトリック・イタレーション(Parametric Iteration)のType1及びType2は極めて長い周期を実現できる。尚、グラフ中にはデジタルテントマッピング(Digital Tent Mapping)による周期も示されているが、従来の技術において述べたように、デジタルテントマッピングによる数列の周期は極めて短いので、実用には適しない。

【0108】

【発明の効果】以上説明したように本発明によれば、デジタルテントマッピングを用いつつ、極めて周期の長いカオス信号を得られるという効果を奏する。

【0109】また、オフセットの所定の範囲に制限すれば一様性を満足するカオス信号の発生器が得られるという効果を奏する。

【0110】特に、オフセットを所定の範囲に制限することは、p-1ビットのカウンタと、所定の加算手段とを用いれば簡易な構成で実現可能であり、安価なカオス信号発生器が得られるという効果を奏する。ここで、pは1以上の整数であり、カオス信号のビット数である。

【0111】さらに、カオス信号発生器を、オフセットを得る手段として利用することも好適である。これによって、よりランダムなカオス信号を得ることが可能なカオス信号発生器が得られるという効果を奏する。

【図面の簡単な説明】

【図1】写像関数の高さを変えることによって、異なる

時系列データが得られることを説明する説明図である。

【図 2】写像関数を上下にシフトした場合のグラフの形状の変化を説明する説明図である。

【図 3】Identity Line を上下に変化させることを説明する説明図である。

【図 4】Identity Line の前に所定のオフセットを挿入することを説明する説明図である。

【図 5】本実施例に係るカオス信号発生器の構成ブロック図である。

【図 6】図 5 のカオス信号発生器の動作を表すフローチャートである。

【図 7】図 5 のカオス信号発生器の動作の説明図である。

【図 8】図 5 のカオス信号発生器の動作を説明図である。

【図 9】図 5 のカオス信号発生器による最初の 50 個の X_n のグラフを示す説明図である。

【図 10】データ幅が 3 ビットである場合であって、初期値が 0 のときの 1 周期分のデータ (291 個) のヒストグラムである。

【図 11】データ幅が 8 ビットである場合であって、初期値が 3 のときの 1 周期分のデータ (2, 433, 158 個) のヒストグラムである。

【図 12】4 つの区間を、オフセット関数上で表したグラフである。

【図 13】図 12 に示されている区間 (a) に対するヒストグラムである。

【図 14】図 12 に示されている区間 (b) に対するヒストグラムである。

【図 15】図 12 に示されている区間 (c) に対するヒストグラムである。

【図 16】図 12 に示されている区間 (d) に対するヒストグラムである。

【図 17】時系列データが一様分布となるようなオフセットの範囲を表すグラフである。

【図 18】オフセットの変化させる時系列データが一様分布となるようなオフセットの範囲でのみオフセットが変化するように構成したカオス信号発生器の構成ブロック図である。

【図 19】ビット幅が 3 ビットであって、初期値が 2 の場合のカオス信号 (最初の 50 点) のグラフを示す図である。

【図 20】ビット幅が 3 ビットであって、初期値が 2 の場合のカオス信号 (一周期分、112 点) のグラフを示す図である。

【図 21】ビット幅が 8 ビットであって、初期値が 0 の場合のカオス信号 (一周期分、1, 726, 201 点) のヒストグラムを示す図である。

【図 22】本実施例に係る他の種類のカオス信号発生器の構成ブロック図である。

【図 23】ビット幅が 3 ビットであって、初期値が 0 の場合のカオス信号 (最初の 50 点) のグラフを示す図である。

【図 24】ビット幅が 3 ビットであって、初期値が 0 の場合のカオス信号 (一周期分、189 点) のヒストグラムを示す図である。

【図 25】ビット幅が 8 ビットであって、初期値が 0 の場合のカオス信号 (一周期分、268, 435, 456 点) のヒストグラムを示す図である。

【図 26】各種の方式による信号の最大周期を比較するグラフである。

【図 27】一次写像関数 $X_{n+1} = aX_n(1 - X_n)$ によるカオス信号の発生原理を説明する説明図である。

【図 28】関数 $X_{n+1} = aX_n(1 - X_n)$ におけるパラメータ a を変化させた場合の X_n の値の列のグラフを示す図である。

【図 29】関数 $X_{n+1} = aX_n(1 - X_n)$ におけるパラメータ a を 3.8 に設定した場合の X_n の値の列のグラフを示す図である。

【図 30】関数 $X_{n+1} = aX_n(1 - X_n)$ を用いた場合の周期倍分岐図である。

【図 31】パラメータ a が 2.8 から 4.0 までである場合の周期倍分岐図の拡大図である。

【図 32】パラメータ a が 3.54 から 3.64 までである場合の周期倍分岐図の拡大図である。

【図 33】三角形の山形の関数を利用した場合の周期倍分岐図である。

【図 34】パラメータ k が 0.50 である場合の X_n の値の変化を表すグラフを示す図である。

【図 35】パラメータ k が 1.00 である場合の X_n の値の変化を表すグラフを示す図である。

【図 36】パラメータ k が 1.10 である場合の X_n の値の変化を表すグラフを示す図である。

【図 37】パラメータ k が 1.25 である場合の X_n の値の変化を表すグラフを示す図である。

【図 38】パラメータ k が 1.99 である場合の X_n の値の変化を表すグラフを示す図である。

【図 39】3 ビットのデジタルテントマップを表すグラフを示す図である。

【図 40】4 ビットのデジタルテントマップを表すグラフを示す図である。

【図 41】デジタルテントマップを用いてカオス信号を得るための構成のブロック図である。

【図 42】デジタルテントマップによるカオス信号の発生の様子を表す模式図である。

【図 43】従来の 4 段 M 系列シフトレジスタを用いたカオス信号発生器の説明図である。

【図 44】従来の 4 段シフトレジスタの M 系列の表を示す説明図である。

【図 45】従来の 4 段シフトレジスタの最大周期系列を

達成する帰還関数の説明図である。

【符号の説明】

- 100 デジタルテントマッピング手段
- 102 デレイエレメント

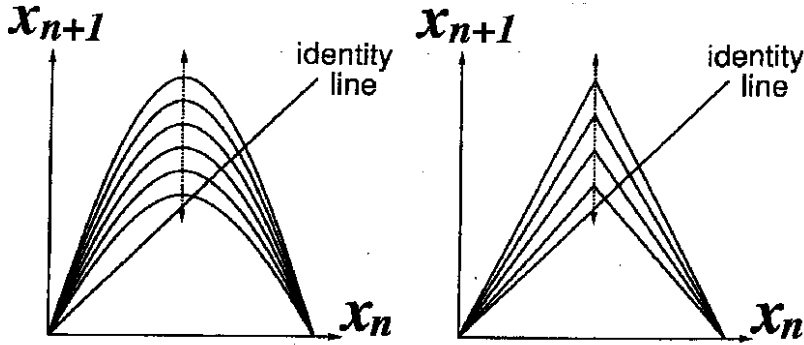
* 104 減算器

106 オフセットカウンタ

108 レジスタ

* 110 コンパレータ

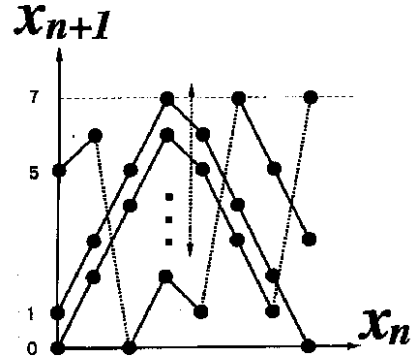
【図1】



(a)

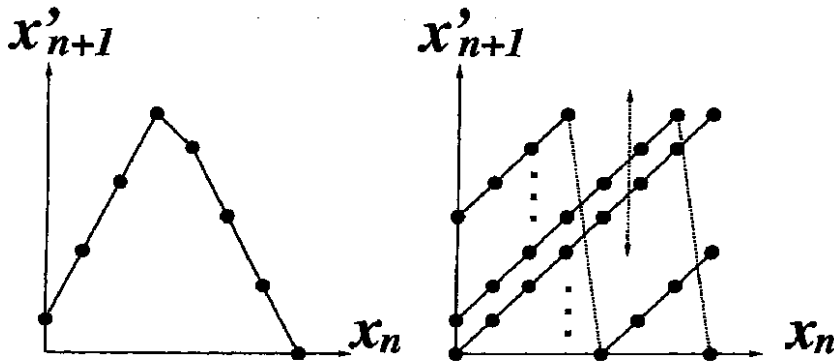
(b)

【図2】

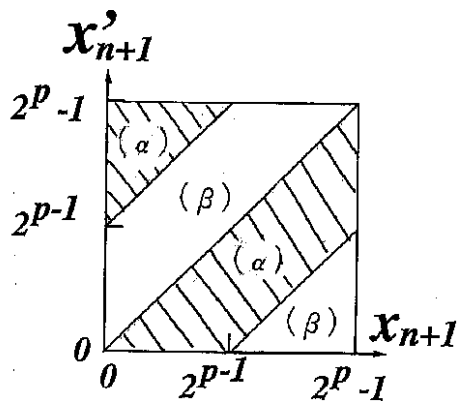
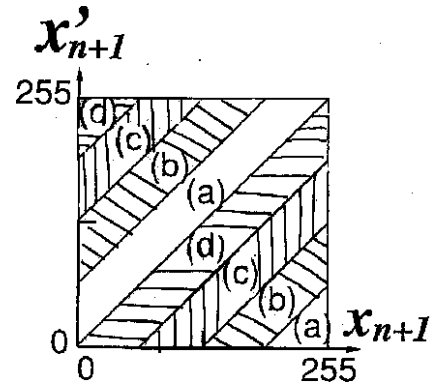


【図12】

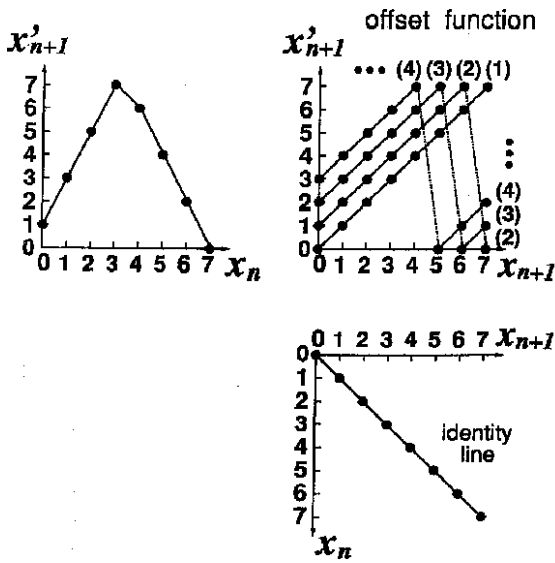
【図3】



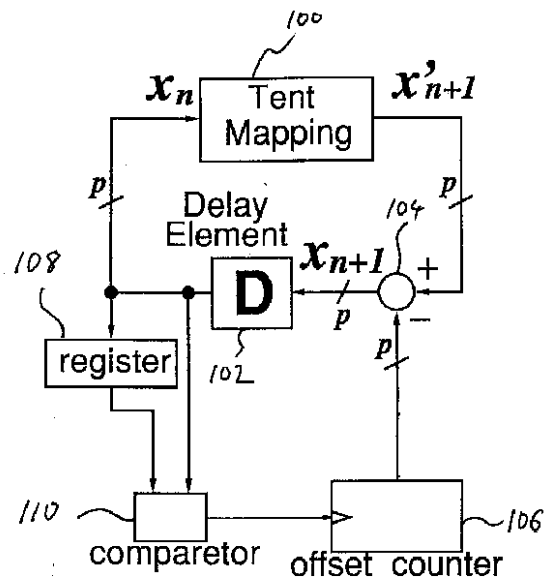
【図17】



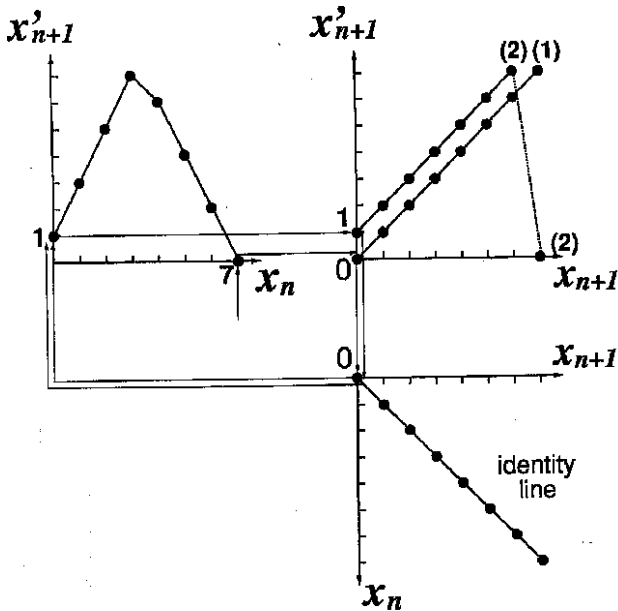
【図4】



【図5】

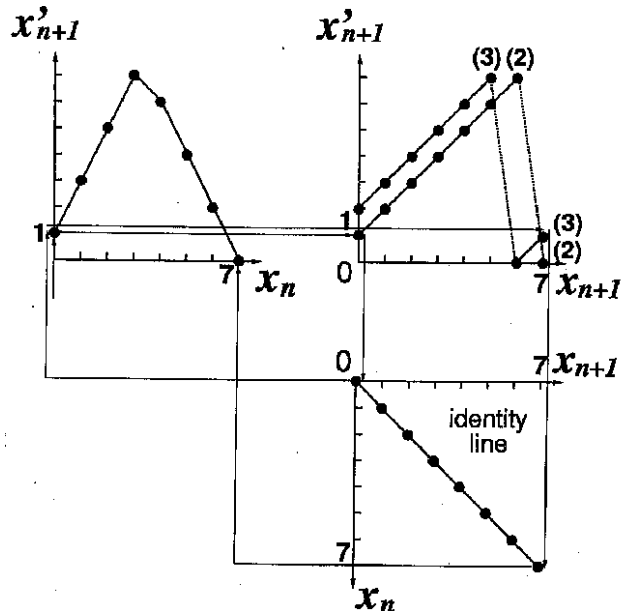


【図7】



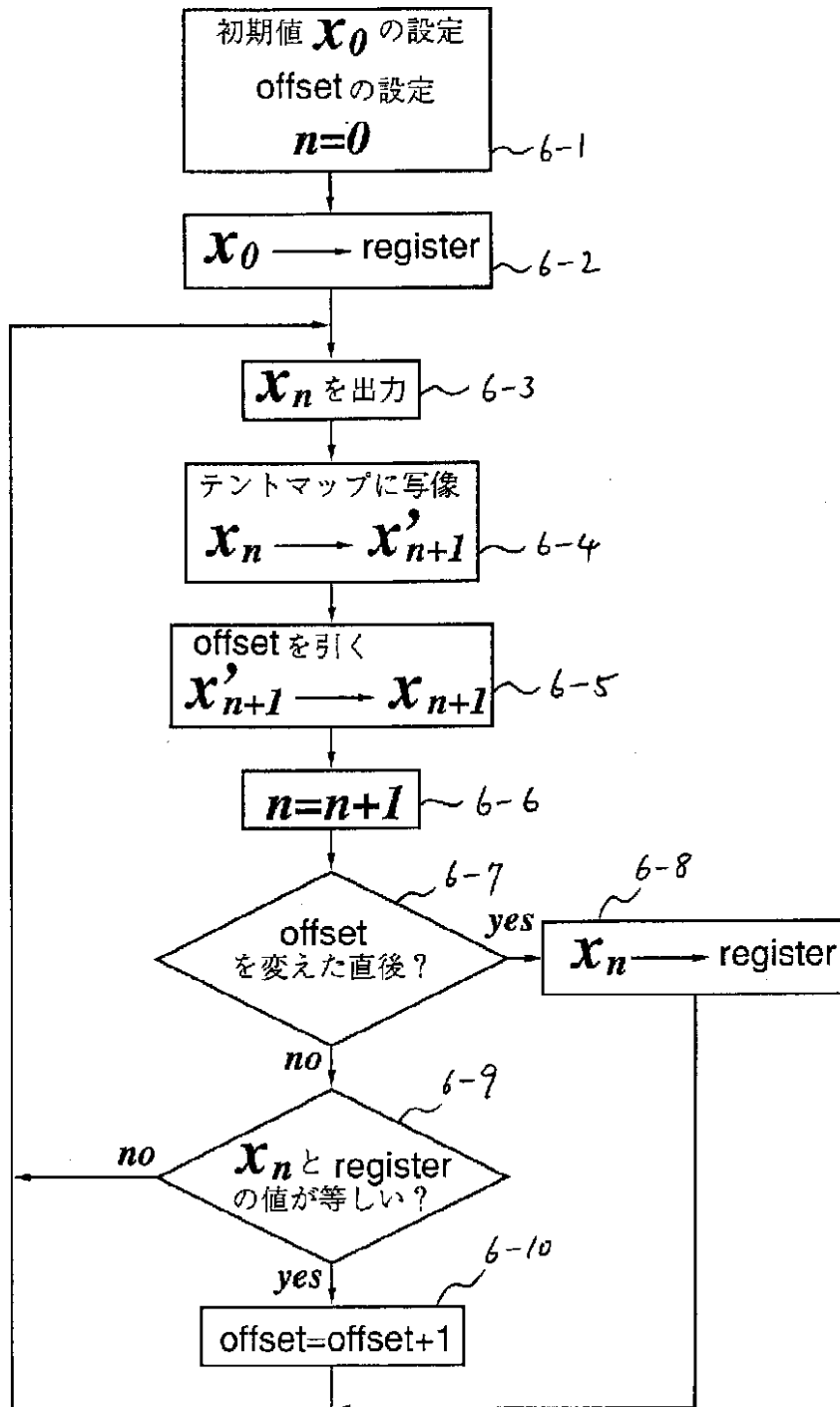
0 1 3 7 0 ^ 0 0 ^ 7 6 0 7 ^

【図8】

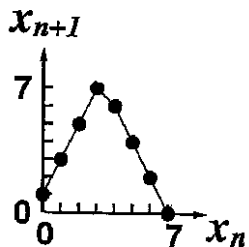


0 1 3 7 0 ^ 0 0 ^ 7 6 0 7 ^ 5

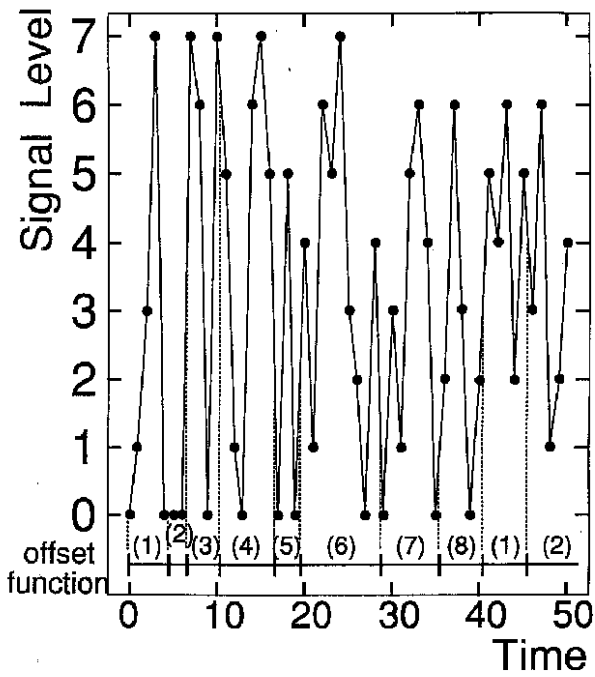
【図6】



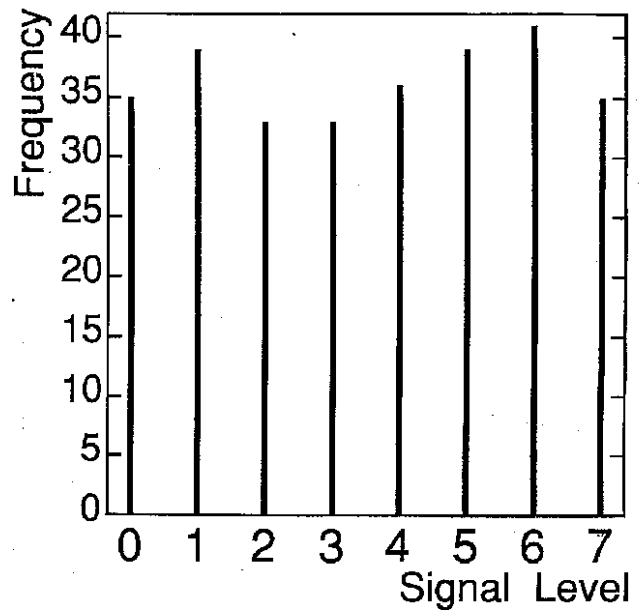
【図39】



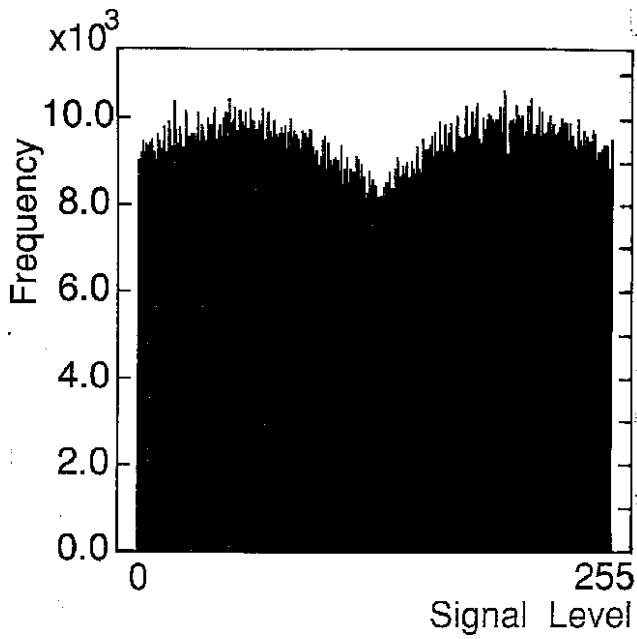
【図9】



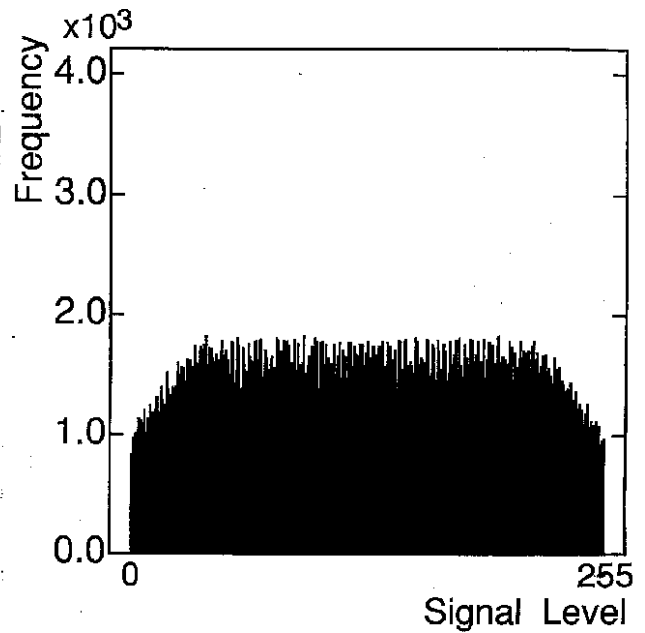
【図10】



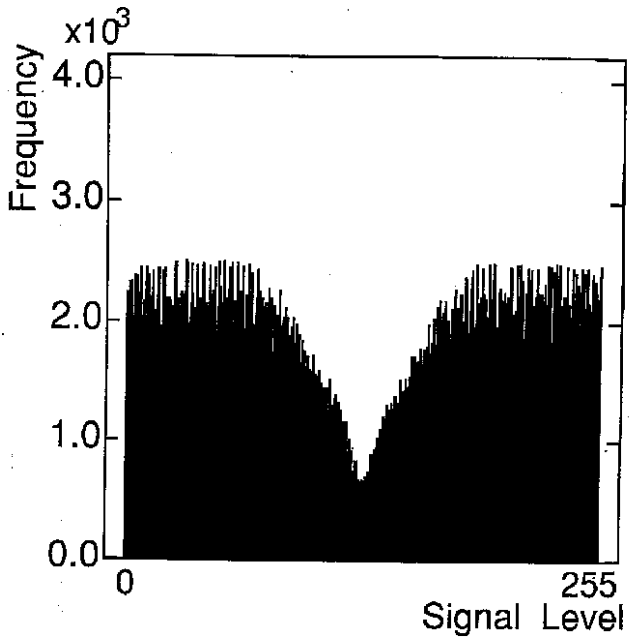
【図11】



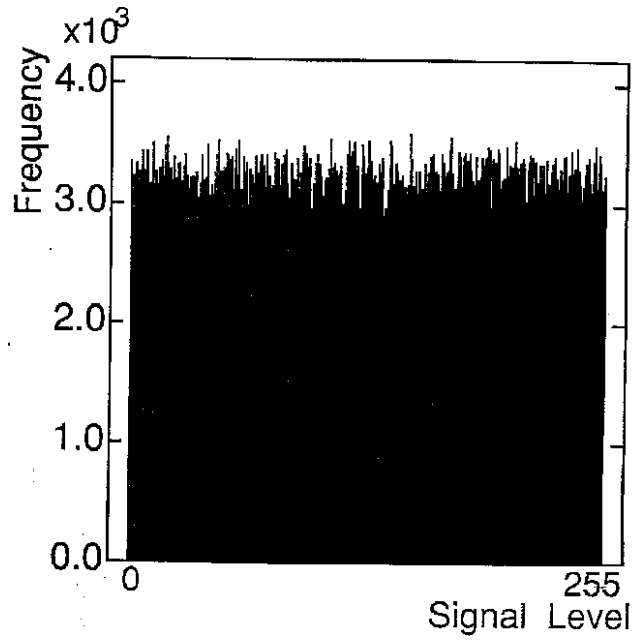
【図13】



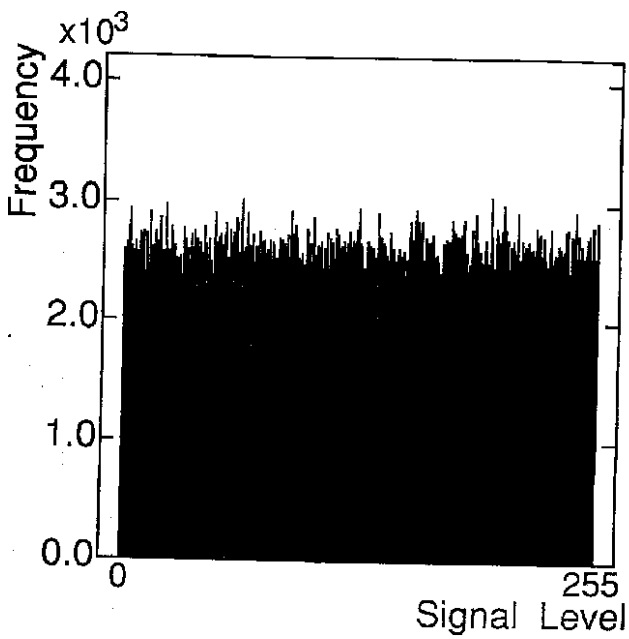
【図14】



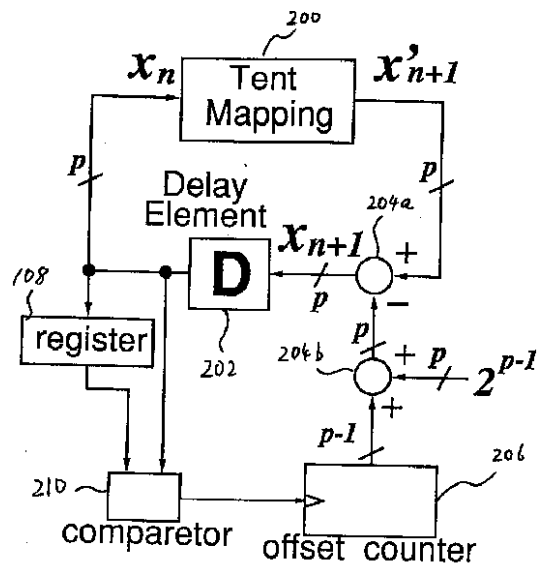
【図15】



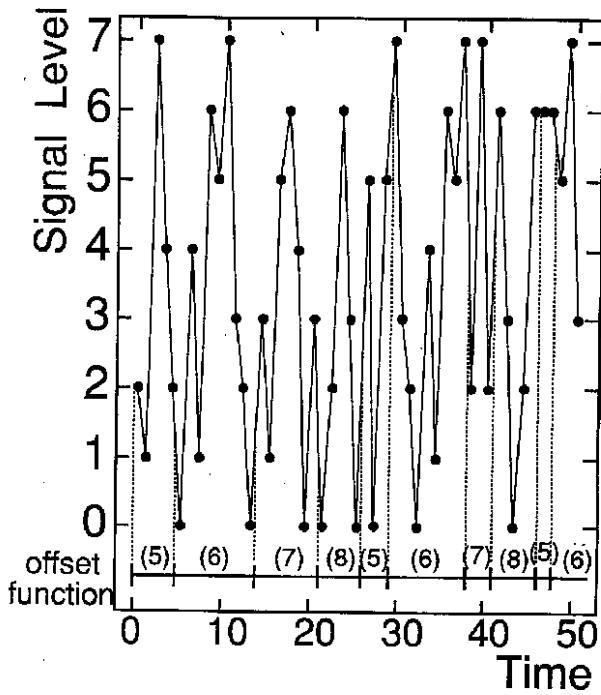
【図16】



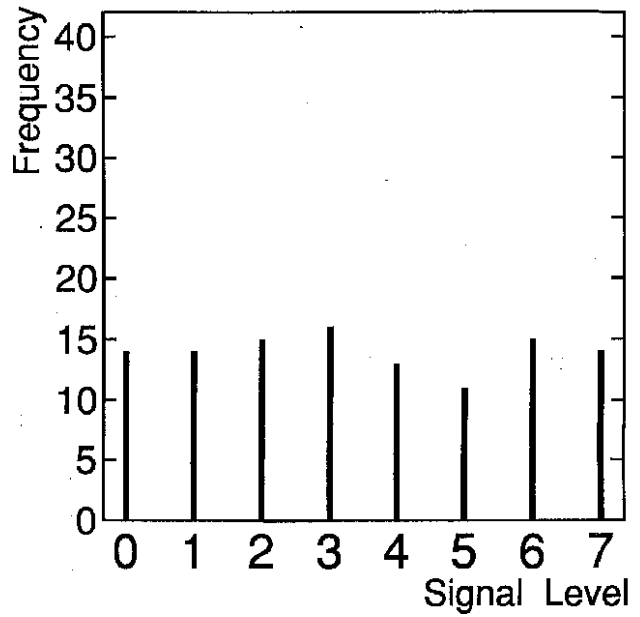
【図18】



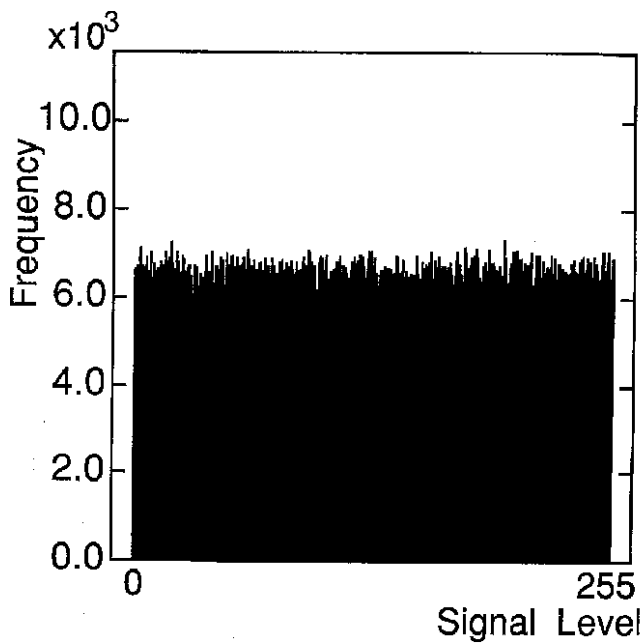
【図19】



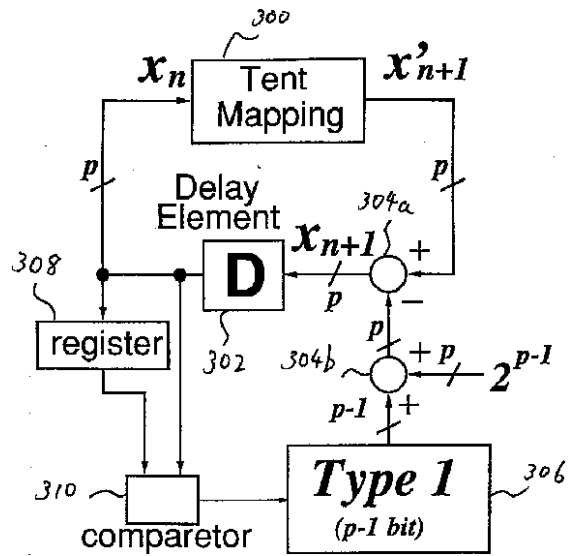
【図20】



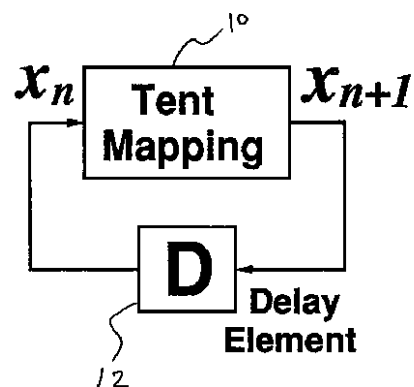
【図21】



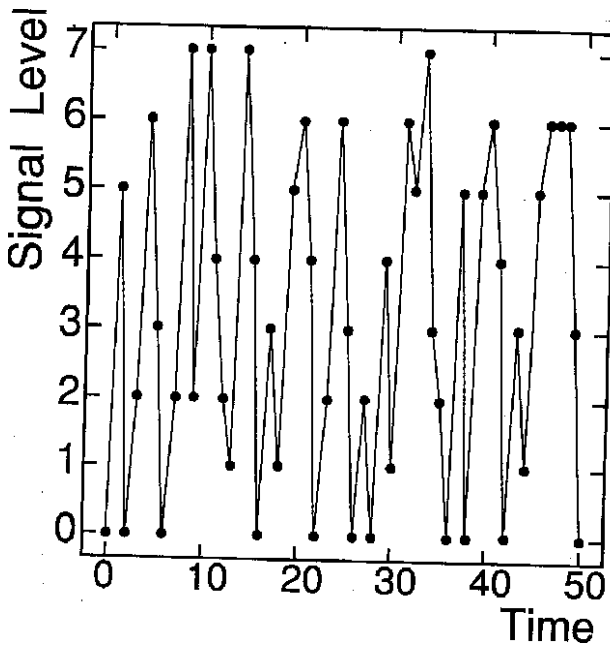
【図22】



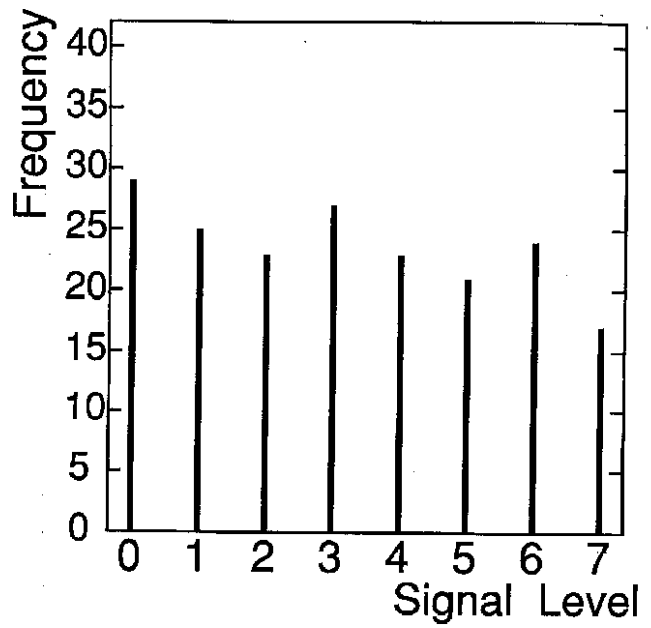
【図41】



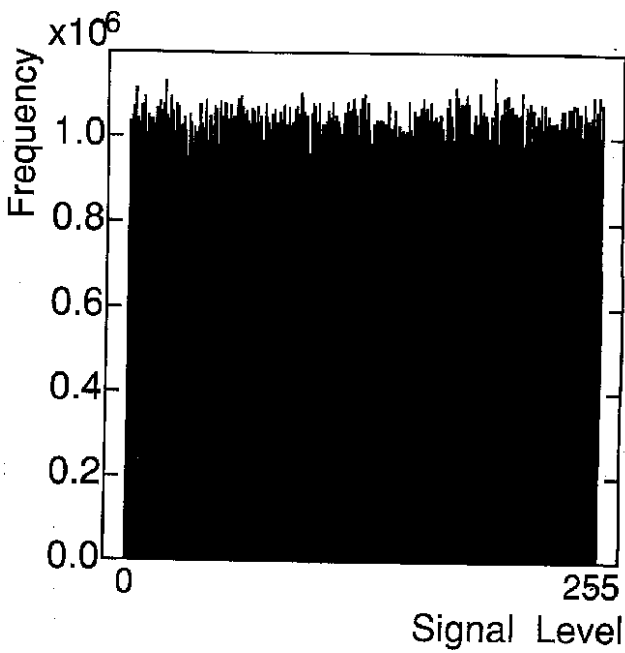
【図 23】



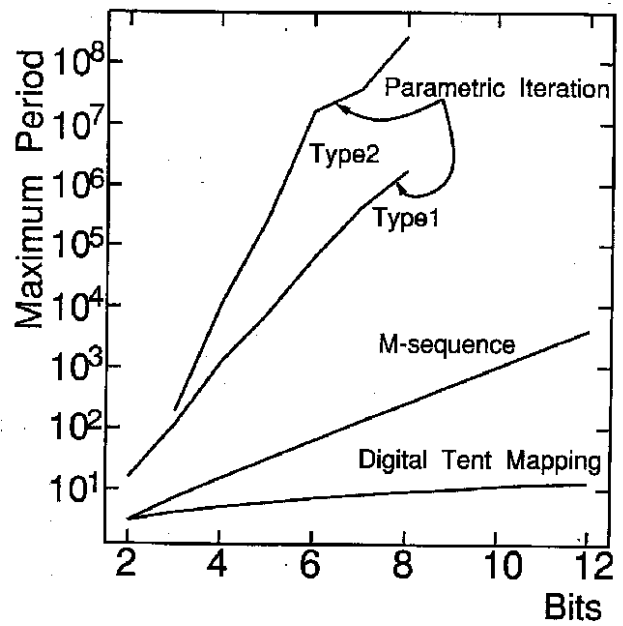
【図 24】



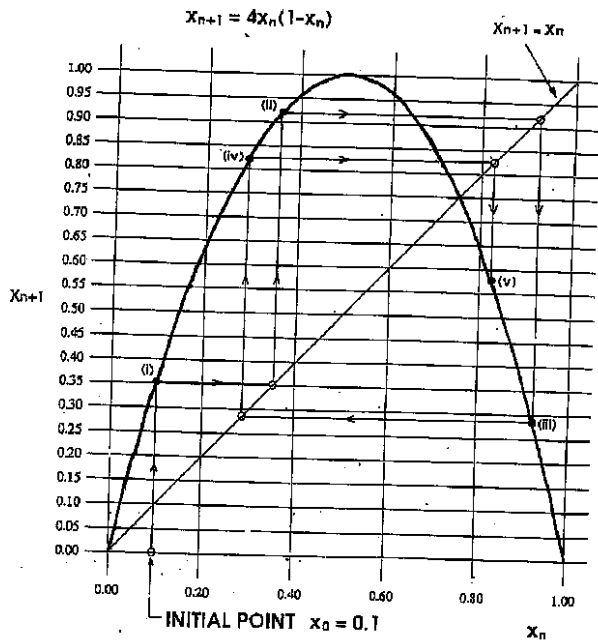
【図 25】



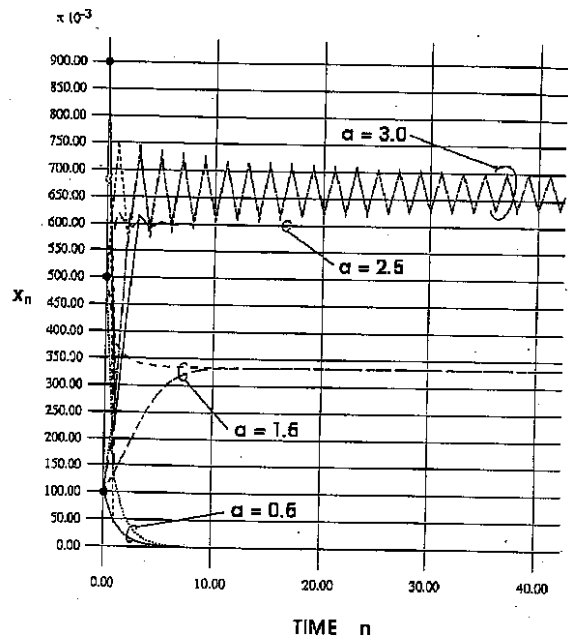
【図 26】



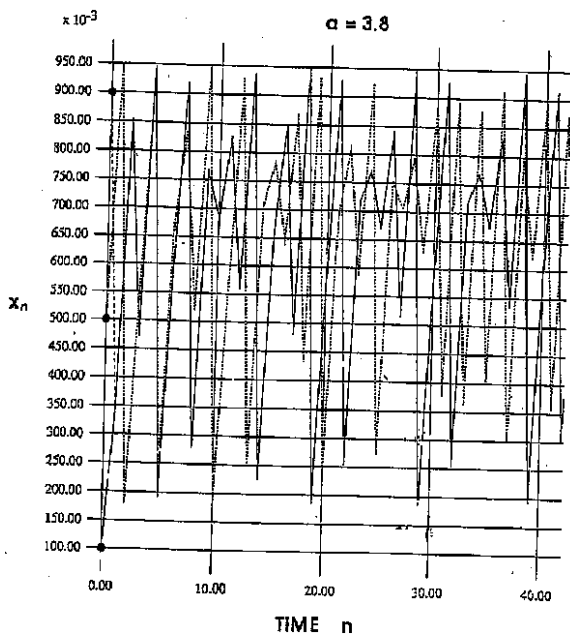
【図 27】



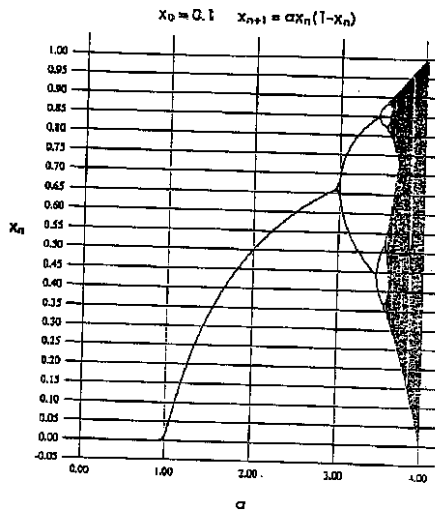
【図 28】



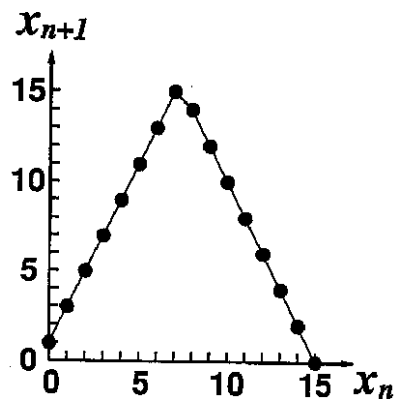
【図 29】



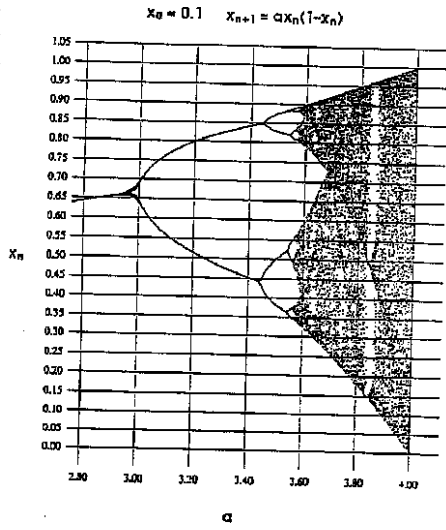
【図 30】



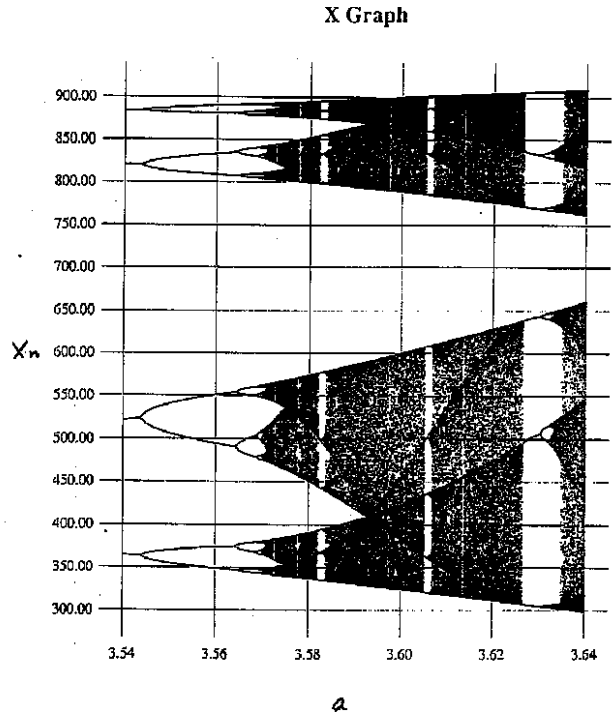
【図 40】



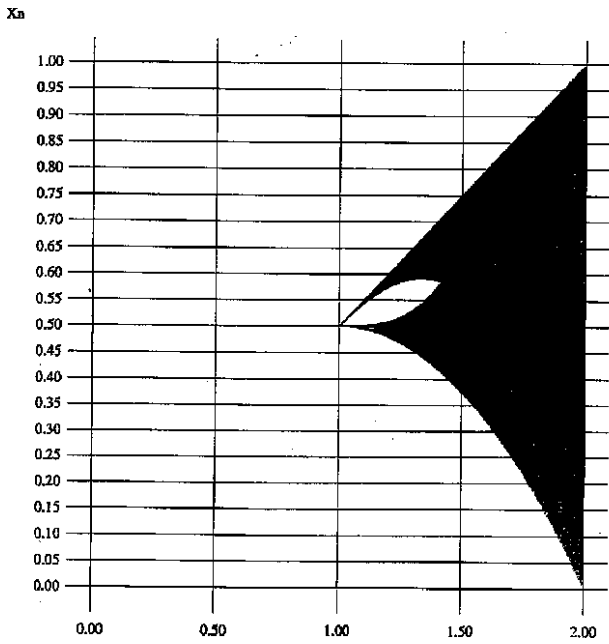
【図 3 1】



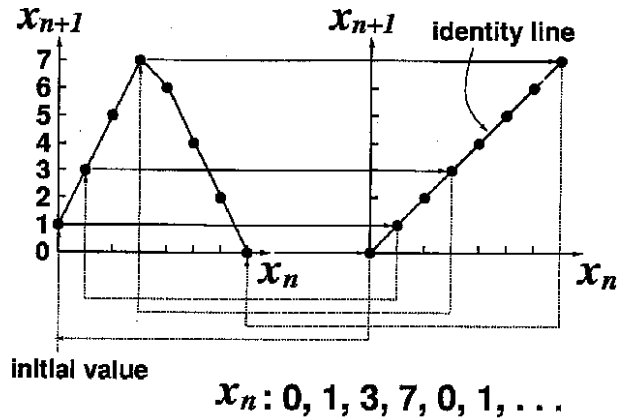
【図 3 2】



【図 3 3】



【図 4 2】

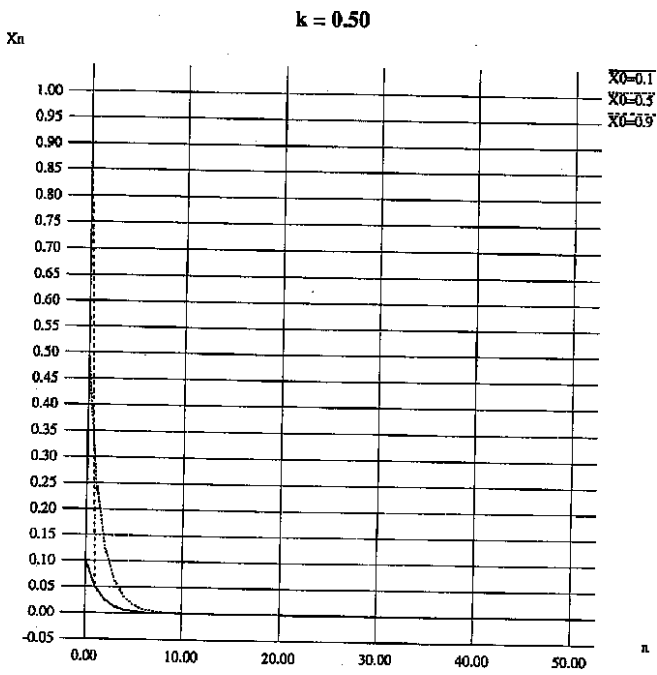


【図 4 5】

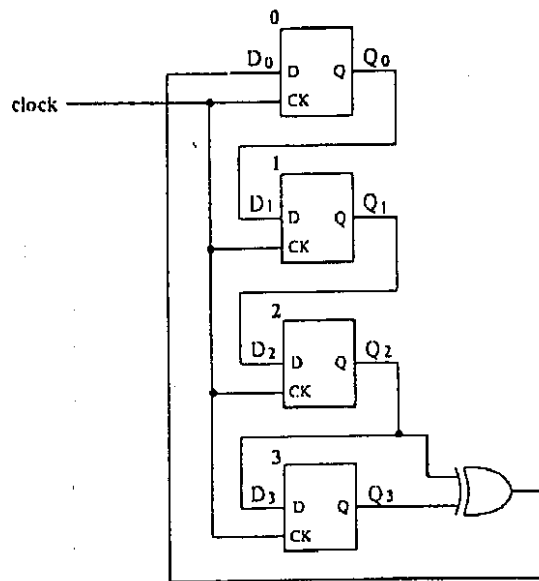
段数 N	相遷方程式	段数 N	相遷方程式
1	Q_0	10	$Q_6 \oplus Q_9$
2	$Q_0 \oplus Q_1$	11	$Q_5 \oplus Q_{10}$
3	$Q_1 \oplus Q_2$	12	$Q_5 \oplus Q_7 \oplus Q_{10} \oplus Q_{11}$
4	$Q_2 \oplus Q_3$	13	$Q_8 \oplus Q_{11} \oplus Q_{11} \oplus Q_{12}$
5	$Q_2 \oplus Q_4$	14	$Q_3 \oplus Q_7 \oplus Q_{12} \oplus Q_{13}$
6	$Q_4 \oplus Q_5$	15	$Q_{13} \oplus Q_{14}$
7	$Q_5 \oplus Q_6$	16	$Q_3 \oplus Q_{12} \oplus Q_{13} \oplus Q_{15}$
8	$Q_3 \oplus Q_4 \oplus Q_5 \oplus Q_7$	17	$Q_{13} \oplus Q_{16}$
9	$Q_5 \oplus Q_8$	18	$Q_{10} \oplus Q_{17}$

最大開期系列の相遷関数

【図 3 4】

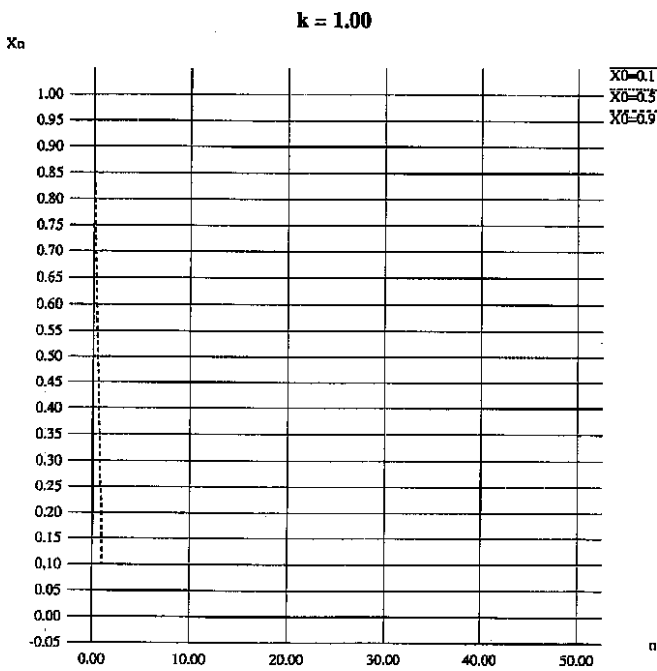


【図 4 3】



4 段 M 系列シフト・レジスタ発生器

【図 3 5】



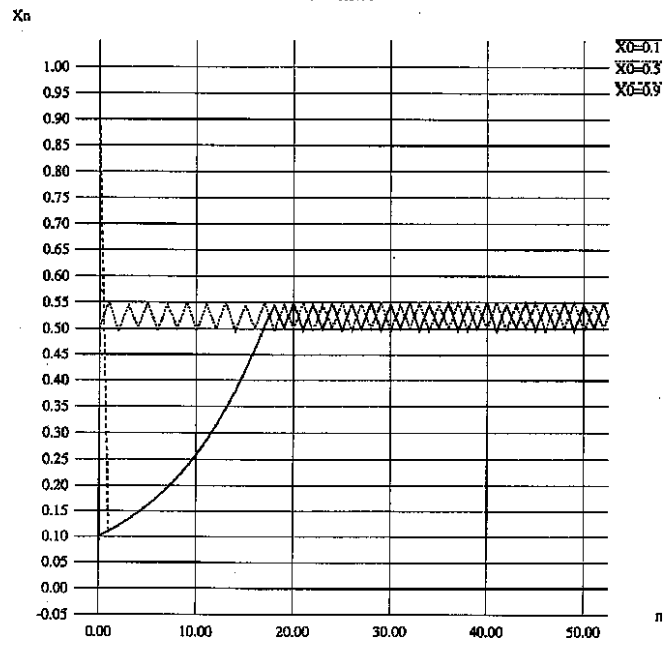
【図 4 4】

<i>s</i>	D	C	B	A	f
S_1	0	0	0	1	0
S_2	0	0	1	0	0
S_4	0	1	0	0	1
S_9	1	0	0	1	1
S_3	0	0	1	1	0
S_6	0	1	1	0	1
S_{13}	1	1	0	1	0
S_{10}	1	0	1	0	1
S_5	0	1	0	1	1
S_{11}	1	0	1	1	1
S_7	0	1	1	1	1
S_{15}	1	1	1	1	0
S_{14}	1	1	1	0	0
S_{12}	1	1	0	0	0
S_8	1	0	0	0	1

4 段シフト・レジスタの M 系列

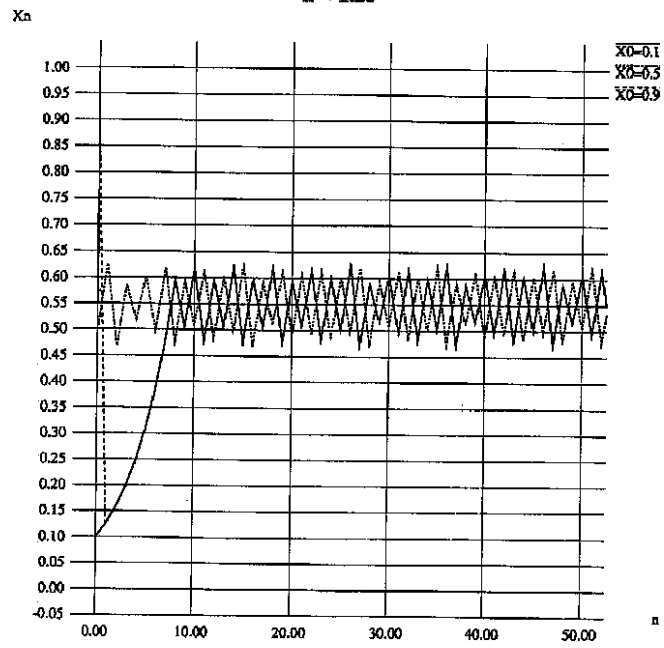
【図 3 6】

$k = 1.10$



【図 3 7】

$k = 1.25$



【図 3 8】

