Vol. 17 No. 90　　電波研究所季報　　May 1971
pp. 249—263

解　　説

UDC 517.5

PN系列—特にM系列について

吉　谷　清　澄*

(昭和 45, 11, 27 受理)

目　　次

まえがき

PN 系列（Pseudo-Noise Sequences*1；擬似雑音系列）の1種である M 系列（Maximum-Length Sequences；最大周期系列*2）は，その不規則性，鋭い自己相関性および発生の容易さなどの特徴により，擬似雑音，擬似乱数あるいは符号として各方面に幅広く利用されいている。

ところで，この種の系列についての解説はいくつかあるようであるが，そのほとんどが応用面を目的とした論文の一部分であるために，数学的背景を省略した簡単なものにとどまっている。

ここではそのような事情に留意し，PN 系列，そのうち特に M 系列について，その数学的側面をも含めてなるべくていねいに解説することを試みた。

内容は，一般的説明と利用面を扱った第Ⅰ部および数学的背景にふれた第Ⅱ部からなっている。

したがって，これらの系列の利用のみを目的とする読者は第Ⅰ部だけを読まれればじゅうぶんであろう。

なお，PN 系列に初めて接する方々にも理解しやすいように予備知識をほとんど仮定しないで書いてあるため，中にはくどすぎる個所もたぶんにあるが，その点読者の諒解を得たい。

*通信機器部通信方式研究室

第Ⅰ部　概　　論

1. PN 系　列[1][2]

1.1.　自己相関関数

本文全体を通して対象にする系列は，その要素が‘0’または‘1’からなるいわゆる“2元系列”（binary sequences）である。以下，文中の“系列”という言葉はすべて2元系列を意味するものとする。

まず初めに，系列の“自己相関関数”（autocorrelation function）について説明する。

いま，任意の周期 p（正の整数）をもつ任意の系列を便宜上

*1 Pseudo-Random Sequences；擬似乱数系列ともいう。
*2 直訳すれば“最大長系列”であるが，通常は本文のような表現が用いられている。

$$\{a_i\}=(a_0,a_1,\cdots,a_{p-1},a_0,a_1,\cdots),\quad a_i=0,1^{*1} \tag{1}$$

で表示する。

次に系列 $\{a_i\}$ から1周期分をとり出したものを

$$A_0=(a_0,a_1,\cdots,a_{p-1}) \tag{2}$$

で，またこの A_0 のすべての要素を左方へ任意に k 回巡回シフトして得られるものを

$$A_k=(a_k,a_{k+1},\cdots,a_{k-1}) \tag{3}$$

で，それぞれ表示する。

定義1（自己相関関数）

このとき，もとの周期系列 $\{a_i\}$ の自己相関関数 $\rho(k)$ を次式で定義する*2。

$$\rho(k)=\frac{\alpha-\beta}{\alpha+\beta}=\frac{p-2\beta}{p},\quad 0\leqq k\leqq p-1 \tag{4}$$

ただし，α, β は A_0 と A_k を各項ごとに比較した場合

$$\begin{cases}\alpha=a_i \text{ と } a_{i+k} \text{ とが一致する個所の総数}\\ \beta=a_i \text{ と } a_{i+k} \text{ とが一致しない個所の総数}\end{cases} \tag{5}$$

を意味する。

(4)式はまた次のように表わすこともできる。

$$\rho(k)=[p-2\sum_{i=0}^{p-1}(a_i\oplus a_{i+k})]/p \tag{6}$$

ただし $\oplus$ は exclusive-or すなわち mod 2 和の記号で

$$a_i\oplus a_{i+k}=\begin{cases}0, & a_i=a_{i+k}\\ 1, & a_i\neq a_{i+k}\end{cases} \tag{7}$$

である。なお(6)式における $\sum$ は通常の和を意味し，また a_i の添字 i はすべて mod p*3で考えるものとする。

（定義終り）

ところで自己相関関数 $\rho(k)$ は一般的には系列の種類や周期およびシフト回数 k の関数になるのであるが，系列によっては次式で示されるような特異な性質をもつものがある。

$$\rho(k)=\begin{cases}1, & k\equiv 0 \pmod p\\ K/p, & k\not\equiv 0 \pmod p\end{cases},\quad 0\leqq|K|\leqq p-1 \tag{8}$$

このような系列は“2値自己相関関数系列”(two-level autocorrelation function sequences) あるいは単に，“2値系列”とよばれる。

この解説の主題である PN 系列は，2値系列の1種になっている。

ところで，2値系列は実は“組合せ理論”(combinatorial theory) における“差集合”(difference sets) と等価な関係にあり，さらに実験計画法における“釣合不完備ブロック計画”(balanced incomplete block design) いわゆる“BIBD”とも密接な関係をもつ。

これらについては文献 (1)(2)(10)(17)(18) などを参照されたい。

1.2. 定義および性質

以上の準備のもとに，PN 系列の定義*4を次に述べる。

定義2（PN 系列）

次の四つの性質を満たす系列を PN 系列とよぶ。

（PN—1）周期性 (periodicity)

周期系列である。

（PN—2）均一性 (balance property)

1周期内において‘0’の出現回数と‘1’の出現回数とはたかだか1しか違わない。

（PN—3）連なり性 (run property)

1周期内において同じ要素が連続するものどおしを分類した場合，それらのうちの $1/2^k$*5 は連なり数*6 k のものである。

さらに，連なり数 k のものの中では，‘0’の k 個連なりと‘1’の k 個連なりとか半分ずつ存在する。

（PN—4）自己相関性 (autocorrelation property)

$$\begin{cases}1, & k\equiv 0 \pmod p\\ -1/p, & k\not\equiv 0 \pmod p\end{cases} \tag{9}$$

（定義終り）

ところで，上記の性質のうち（PN-1）を除く（PN-2），（PN-3）および（PN-4）は，硬貨を無作為に投げて得られる‘表’(1)，‘裏’(0) のランダム系列*7—いわゆる“Bernoulli 試行列”にふさわしい内容のものである。

すなわち，（PN-2）および（PN-3）は‘表’と‘裏’がそれぞれ 1/2 の確率で互いに独立的に出現することを規定し，さらに（PN-4）は，系列自身とそのシフト系列とがほとんど無相関であることを規定している。

---

*1 $a_i=0,1$ は，$a_i=0$ または $a_i=1$ を意味する。以下同様。

*2 $\rho(k)=\sum_{i=0}^{p-1}a_ia_{i+k}$ で定義する場合もあるが(1)，本質的な差はない。

*3 $i=mp+r$, m,r=整数，$0\leqq r\leqq p-1$ であるとき $i\equiv r \pmod p$ とすること。したがって，すべての整数は0から $p-1$ の p 個の整数値に類別される。$k\equiv 0 \pmod p$ は $k=mp$ を意味する。

*4 これらの定義がそのまま PN 系列の性質にもなっている。また，これらの性質の意味は次章2.3の例により具体的に理解される。

*5 k の値は，この値が整数値になる範囲のものである。

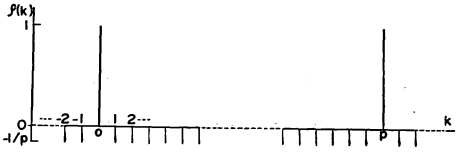
*6 “連なり数 k”とは，同じ要素が k 個連続して出現するものを意味する。

一方，(*PN*-1) はこれに反して，周期性という，真のランダム系列にはあり得ない性質を規定している。

以上の説明で示されたように，*PN* 系列には (*PN*-2)，(*PN*-3) および (*PN*-4) という“雑音的”な性質と，(*PN*-1) という“非雑音的”な性質とが共に存在しているのである。

ここで注意すべきことは，(*PN*-2)，(*PN*-3) および (*PN*-4) の三つの性質が互いに独立的であることである。

このことは 1.4 の具体例によって確かめられるであろう。なお参考までに，*PN* 系列の自己相関関数 $\rho(k)$ のだいたいの様子を第1図に示す。



第1図*2 *PN* 系列の自己相関関数 $\rho(k)$，((4)式)

これをみてもわかるように，$\rho(k)$ は $k\equiv 0 \pmod p$ のところでのみ peak 値‘1’をとり，他の k のところでは‘$-1/p$’という，p を大きくとればほとんど無相関とみなせる値になっている。

これが *PN* 系列の“鋭い（自己）相関性”とよばれるもので，*PN* 系列の（擬似）雑音性を端的に示すものである。

1.3. *PN* 系列の種類

PN 系列としてよく知られているものに次の4種類がある。

（i） *M* 系列[1)~5)]

2^n-1 の形の周期をもつ。

（これについては次章以下で詳しく説明する。）

（ii） Legendre 系列[1)2)6)7)]（平方剰余系列）

$4k-1$ 形の素数の周期をもつ。

（発生法）

$$a_i=\left(\frac{i}{p}\right)^{*3}=\begin{cases}1, & i \text{ が } \bmod p \text{ の平方剰余*4であるとき;}\\ -1, & \text{その他}\end{cases}$$

(iii) Hall 系列[1)2)8)]

$4k-1=4m^2+27$ 形の素数の周期をもつ。

これは Legendre 系列の一部である。

(iv) 双子素数系列[1)2)9)]

$q, q+2$ が共に素数であるとき $q(q+2)$ の周期をもつ。

（発生法）

$$a_i=\begin{cases}\left(\frac{i}{q}\right)\left(\frac{i}{q+2}\right)^{*3}, & (i,q)^{*5}=1\\ 1, & i\equiv 0 \pmod{q+2}\\ -1, & \text{その他}\end{cases}$$

ところで上に示した系列は‘1’および‘-1’を要素としてもっているが，これを‘0’および‘1’の系列に変換するには，‘1’→‘0’，‘-1’→‘1’なる変換を施せばよい。(1.5 参照)

また(i)~(iv) の系列は全然別種の *PN* 系列になるわけではなく，中には互いに重複し合っているものもある。

なおここで注意すべきことは，*M* 系列はすべて *PN* 系列であるが，他の系列の場合，中には *PN* 系列ではないものもあるということである。（次節(b)参照）

1.4. 例[1)]

参考までに *PN* 系列の簡単な具体例を(a)に示す。

また(b)(c)(d)は 1.2 の *PN* 系列の性質 (*PN*-2)，(*PN*-3) および (*PN*-4) が互いに独立的であることを示し，いずれも *PN* 系列ではない例である。

(a) (1110100) (*M* 系列)

(*PN*-1)~(*PN*-4) のすべてを満たす。

(b) (11011100010) (Legendre 系列)

(*PN*-1)，(*PN*-2) および (*PN*-4) を満たすが (*PN*-3) は満たさない。

(c) (1111101110010)

(*PN*-1) および (*PN*-4)*6を満たすが (*PN*-2) および (*PN*-3) は満たさない。

(d) (10110010)

(*PN*-1)，(*PN*-2) および (*PN*-3) を満たすが (*PN*-4) は満たさない。

1.5. 変換 *PN* 系列

いま第1表のような対応関係を考えるとする。

第1表 系列要素の変換表

PN 系列		変換 *PN* 系列
0	⟷	+1
1	⟷	−1
⊕	⟷	・

(但) ・印は積の記号

このとき，*PN* 系列を第1表により変換して得られる

---

*7 ランダム系列に対する統一的な定義は確立していない。

*2 $k<0$ のときは“右方”へ巡回シフトすることを意味する。なお，図では $-1/p$ の値を誇張して示してある。

*3 “Legendre の記号”

*4 互いに素な（つまり1以外の公約数をもたない）数を i,p としたとき，$x^2\equiv i \pmod p$ が解をもてば，この i を mod p の“平方剰余”(quadratic residue) であるという。

*5 二つの整数 i,q の最大公約数を表わす記号，したがって $(i,q)=1$ は i と q が互いに素であることを意味する。

*6 この場合 $\rho(k)=+1/p$ となる。

系列を，便宜上“変換 PN 系列”とよぶことにする。

ここで変換 PN 系列の自己相関関数を $\rho'(k)$ で表わすと，これは(4)式および第1表から次式のようになることがわかる。

$$\rho'(k)=\frac{1}{p}\sum_{i=0}^{p-1}a_ia_{i+k},\quad a_i=1,\ -1 \tag{10}$$

なぜなら，$a_i=a_{i+k}$ であれば $a_ia_{i+k}=1$，また $a_i\neq a_{i+k}$ であれば $a_ia_{i+k}=-1$ となり，これらの総和がちょうど(4)式の分子に等しくなるからである。

したがって変換 PN 系列の自己相関関数は PN 系列のものとまったく同一のものになり，次式が成り立つ。

$$\rho'(k)=\begin{cases}1, & k\equiv 0 \pmod p\\ -1,\ k/p, & k\not\equiv 0 \pmod p\end{cases} \tag{11}$$

1.6. *PN* 系列の *Fourier* 解析

PN 系列を Fourier 解析するために，周期 p の変換 PN 系列を次のように“インパルス列”として表示した場合を考える。

$$\sum_{i=-\infty}^{\infty}a_i\delta(t-i),\quad a_i=1,\ -1 \tag{12}$$

このとき(12)式を Fourier 級数展開すると，その Fourier 係数は次式のようになる。

$$C_n=\frac{1}{p}\sum_{l=0}^{p-1}a_le^{j2\pi nl/p},\quad j=\sqrt{-1} \tag{13}$$

この式から C_n の絶対値を計算する。

$$\begin{aligned}|C_n|^2&=\frac{1}{p^2}\sum_{l=0}^{p-1}a_le^{j2\pi nl/p}\sum_{m=0}^{p-1}a_me^{-j2\pi nm/p}\\&=\frac{1}{p^2}\sum_{l=0}^{p-1}\sum_{m=0}^{p-1}a_la_me^{j2\pi n(l-m)/p}\\&=\frac{1}{p^2}\sum_{k=0}^{p-1}\left(\sum_{m=0}^{p-1}a_ma_{m+k}\right)e^{j2\pi nk/p}\end{aligned} \tag{14}$$

ここで(10)式および(11)式を用いると

$$\begin{aligned}|C_n|^2&=\frac{1}{p}\sum_{k=0}^{p-1}\rho'(k)e^{j2\pi nk/p}\\&=\frac{1}{p}\left(1-\frac{1}{p}\sum_{k=1}^{p-1}e^{j2\pi nk/p}\right)\end{aligned} \tag{15}$$

したがって，n が p の整数倍である場合には

$$|C_n|^2=\frac{1}{p}\left(1-\frac{p-1}{p}\right)=\frac{1}{p^2},\quad n\equiv 0 \pmod p \tag{16}$$

$$|C_n|=1/p,\qquad n\equiv 0 \pmod p \tag{17}$$

一方，n が p の整数倍でない場合には

$$\sum_{k=1}^{p-1}e^{j2\pi nk/p}=-1 \tag{18}$$

となるので，(15)式は次のようになる。

$$|C_n|^2=\frac{1}{p}\left(1+\frac{1}{p}\right)=\frac{p+1}{p^2} \tag{19}$$

$$|C_n|=\frac{\sqrt{p+1}}{p} \tag{20}$$

ところで変換 PN 系列と PN 系列とは前述したように，同一の自己相関関数をもつから，(16)式～(20)式は PN 系列に対してもそのまま成り立つ。

以上の結果をまとめると次のようになる。

PN 系列の周波数スペクトル成分：

$$|C_n|=\begin{cases}1/p, & n\equiv 0 \pmod p\\ \sqrt{p+1}/p, & n\not\equiv 0 \pmod p\end{cases} \tag{21}$$

PN 系列の電力スペクトル成分：

$$|C_n|^2=\begin{cases}1/p^2, & n\equiv 0 \pmod p\\ (p+1)/p^2, & n\not\equiv 0 \pmod p\end{cases} \tag{22}$$

上記の結果をみると，PN 系列の周波数スペクトルおよび電力スペクトルは，自己相関関数の場合と同様に周期 p の高調波以外の成分において平坦な特性になっていることがわかる。

次に，変換 PN 系列を今度は次のように“パルス列”として表示した場合を考える。

$$\sum_{i=-\infty}^{\infty}a_iu(t-i),\quad a_i=1,-1 \tag{23}$$

ただし

$$u(t-i)=\begin{cases}1, & i\leqq t<i+1\\ 0, & \text{その他}\end{cases}$$

(23)式で表示されるパルス列は“PN 波形”とよばれる(2)。この場合の Fourier 解析は周知のとおり先の結果に関数形

$$\left[\frac{\sin(\pi n/p)}{\pi n/p}\right] \tag{24}$$

を乗ずるだけでよい。したがって次の結果が得られる。

PN 波形の周波数スペクトル成分：

$$|C_n|=\begin{cases}\dfrac{1}{p}, & n\equiv 0 \pmod p\\ \dfrac{\sqrt{p+1}}{p}\left[\dfrac{\sin(\pi n/p)}{\pi n/p}\right], & n\not\equiv 0 \pmod p\end{cases} \tag{25}$$

PN 波形の電力スペクトル成分：

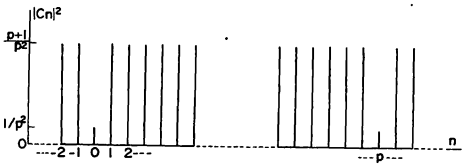
$$|C_n|^2=\begin{cases}\dfrac{1}{p^2}, & n\equiv 0 \pmod p\\ \dfrac{p+1}{p^2}\left[\dfrac{\sin(\pi n/p)}{\pi n/p}\right]^2, & n\not\equiv 0 \pmod p\end{cases} \tag{26}$$

また，*PN* 波形の自己相関関数 $\rho_w(\tau)$ は次式で表わされる。

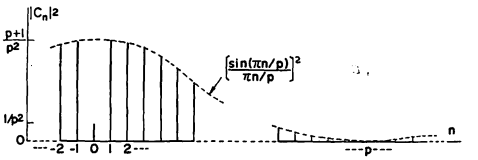
$$\rho_w(\tau)=\begin{cases}1-\dfrac{(p+1)}{p}|\tau|, & |\tau|\leqq 1\\ -\dfrac{1}{p}, & 1<|\tau|\leqq p-1\end{cases} \tag{27}$$*1

なお参考までに，*PN* 系列および *PN* 波形の電力スペクトルと，*PN* 波形の自己相関関数のだいたいの様子をそれぞれ第2図，第3図および第4図に示す。

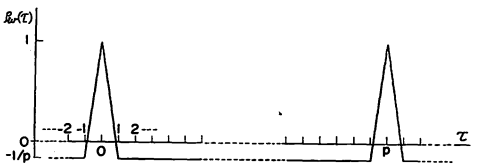
なおこれらの図においては，$1/p^2$ および $-1/p$ の値を誇張して示してあることに注意されたい。



第2図 *PN* 系列の電力スペクトル ((22)式)



第3図 *PN* 波形の電力スペクトル ((26)式)



第4図 *PN* 波形の自己相関関数 $\rho_w(\tau)$, ((27)式)

2. M 系 列[1)~5)]

2.1. 定義および性質*2

定義3 (*M* 系列)

1.2 で述べた性質 (*PN*-1)～(*PN*-4) を含む次の五つの性質 (*M*-1)～(*M*-5) を満たす系列を *M* 系列とよぶ。

(*M*-1) 周期性

$p=2^n-1$ なる形の周期をもつ*3。

(*M*-2) 均一性

1 周期内において，

'1' の出現回数 $=2^{n-1}=(p+1)/2$

'0' の出現回数 $=2^{n-1}-1=(p-1)/2$

(*M*-3) 連なり性

1周期内における連なり数 $k(\leqq n-2)$ の出現回数は 2^{n-k-1} であり，このうち '1' の連なりと '0' の連なりは半分ずつ存在する。また，連なり数 k のものの出現率は 2^{-k} である。

そのほか，連なり数 $(n-1)$ の '0' の連なり，および連なり数 n の '1' の連なりがそれぞれ1回ずつ出現する。

(*M*-4) 自己相関性

$$\rho(k)=\begin{cases}1, & k\equiv 0 \pmod p\\ -1/(2^n-1)=-1/p, & k\not\equiv 0 \pmod p\end{cases} \tag{28}$$

(*M*-5) Delay-and-Add 性

系列の1周期分 $A_0=(a_0, a_1, \cdots, a_{p-1})$ と，これを任意に k 回シフトした $A_k=(a_k, a_{k+1}, \cdots, a_{k-1})$*4 との各項ごとの mod 2 和から得られる系列は，再び A_0 の適当な巡回シフト系列になる。

すなわち，

$$\begin{aligned}A_0\oplus A_k&=(a_0\oplus a_k, a_1\oplus a_{k+1}, \cdots, a_{p-1}\oplus a_{k-1})\\ &=(a_i, a_{i+1}, \cdots, a_{i-1})\\ &=A_i, \quad 0<i<p\end{aligned} \tag{29}$$

となるような，A_0 の巡回シフト系列 A_i が存在する。

(定義終り)

ところで上記の性質のうち最後の (*M*-5) Delay-and-Add 性なるものは，他の *PN* 系列にはみられない特異なものである。この性質と (*M*-2) 均一性とを用いると，*M* 系列は誤り訂正能力*5 をもつ巡回符号の1種になり得ることがわかる。

M 系列には上記のほかに次のような性質もある[1)5)]。

いま周期 p の *M* 系列 $(a_0, a_1, \cdots, a_{p-1}, a_0, a_1, \cdots)$ があるとすると，これを逆向きに並べて得られる系列

$$(a_{p-1}, a_{p-2}, \cdots, a_1, a_0, a_{p-1}, \cdots) \tag{30}$$

---

*1 ほかの τ に関しては，1周期分の繰返しになる。(第4図参照)

*2 これらの性質の意味は 2.3 の例により具体的に理解される。また *M* 系列がこれらの性質をもつことの証明は第Ⅱ部 5.2 に示されている。

*3 n の意味は次節で明らかになる。

*4 この系列も *M* 系列になることはいうまでもない。

*5 $A_0, A_1, \cdots, A_{p-1}$ をそれぞれ符号ベクトルとみなせば，このときの符号間距離 (Hamming 距離) は 2^{n-1} になり，したがって $2^{n-2}-1$ 個以下の誤りを訂正できる。

もまた M 系列になることは容易にわかる*1。

また，周期 $p=2^n-1$ の M 系列から k 個 ($=2^l, 1\leqq l\leqq p-1$) おきにとり出して得られる系列

$$(a_0, a_k, a_{2k}, \cdots),\quad k=2^l,\quad 1\leqq l\leqq p-1 \tag{31}$$

は，再びもとの M 系列の適当なシフト系列になる。

一方，p に素で，かつ 2^l には等しくない数 k' をとるとこのときの系列

$$(a_0, a_{k'}, a_{2k'}, \cdots),\ (k', p)=1,\ k'\neq 2^l,\quad 1\leqq l\leqq p-1 \tag{32}$$

は，もとの M 系列のシフト系列にはならないが，やはり周期 $p=2^n-1$ の M 系列になる。

2.2. 発生法*2

2.2.1. 直接計算による発生

周期 $p=2^n-1$ の M 系列 $\{a_i\}=(a_0, a_1, \cdots, a_{p-1}, a_0, a_1, \cdots)$ は次に示される n 次線形回帰方程式*3 (linear recurring equation) により生成される*4。

$$a_i\equiv\sum_{l=1}^{n} c_l a_{i-l}\pmod 2,\quad i=n, n+1, \cdots \tag{33}$$*5

ただし“初期値” $(a_0, a_1, \cdots, a_{n-1})$ は，すべてが‘0’である場合（以後これを all 0 と略記する）を除けば任意に‘0’または‘1’を与えてよい。また n 個の定数 $c_0, c_1, \cdots, c_n$ は次に示されるような n 次原始多項式*6の係数である。

$$f(x)=\sum_{l=0}^{n} c_l x^l, \tag{34}$$

$$c_0=c_n=1$$

$$c_l=0, 1,\quad 0<l<n$$

ところで(33)式の $c_1, \cdots, c_n$ が一定であれば，初期値を変えて得られる M 系列どおしは互いにシフトした関係になる。（第Ⅱ部 5.3 参照）

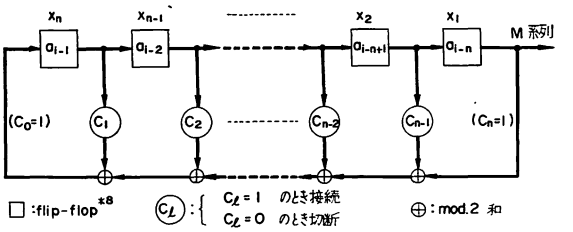
電子計算機による M 系列の発生には(33)式をそのまま用いればよい。

2.2.2. シフトレジスタによる発生

(33)式をみると，周期 2^n-1 の M 系列は第5図のようなフィードバック付 n 段シフトレジスタにより簡単に発生できることがわかる。

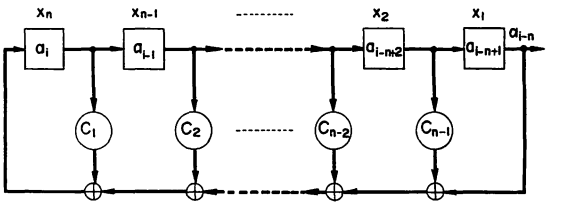
ここで第5図の回路の働きを簡単に説明する。

（i） いま，ある時刻 t_0 における n 個の flip-flop $x_n, x_{n-1}, \cdots, x_1$ の内容がそれぞれ $a_{i-1}, a_{i-2}, \cdots, a_{i-n}$ であったとする。（第5図）



第5図 M 系列発生 n 段シフトレジスタ*8

（ii） このとき次の clock*9がくると，x_n の内容 a_{i-1} が x_{n-1} に，x_{n-1} の内容 a_{i-2} が x_{n-2} に，…，x_2 の内容 a_{i-n+1} が x_1 に，それぞれ移され，x_n には $\sum_{l=1}^{n} c_l a_{i-l}\equiv a_i$(33)式）がフィードバックされる。



第6図 （第5図）の次の状態図

このとき同時に，x_1 の内容 a_{i-n} が出力される。

（iii） 上の動作が完了すると，時刻 $t_0+\Delta$(Δ=clock 間隔）におけるシフトレジスタの状態は第6図のようになる。

そこで flip-flop $x_1, x_2, \cdots, x_n$ に初期値 $a_0, a_1, \cdots, a_{n-1}$ を (all 0 を除いて) 任意に与えて，上記の (i)～(iii) の動作を繰り返えすと，その結果周期 $p=2^n-1$* の M 系列が順次出力される。

以上の説明でもわかるように，M 系列は原始多項式さえ既知であれば，回帰方程式(33)式あるいは第5図のシフトレジスタ回路のいずれを用いてもきわめて簡単に発生できる。

M 系列が PN 系列の1種として他のものよりも重要視され，各方面で活用されている最大の理由は，この“発生の容易さ”にあるといえるのである。

---

*1 一般に PN 系列の逆向き系列もまた PN 系列である。

*2 ここで述べる方法のほかに“母関数”を用いる方法もある。（第Ⅱ部 4.1 参照）

*3 n 階線形差分方程式 (linear difference equation) でもある。

*4 したがって M 系列は“回帰系列”の1種である。なお M 系列が (33)式および(34)式により生成される理由は第Ⅱ部で詳しく述べる。

*5 乗法は $0\cdot a=0$, $1\cdot 1=1$ で行なう。（第Ⅱ部 2.1 (41)式参照）

*6 第Ⅱ部 5.2 および付録Ⅰ参照。

*7 ‘0’または‘1’のどちらか一方の状態をとる回路。

*8 この回路は“有限状態オートマトン”の1種である。

*9 これにより各部の動作が開始される。

ところで M 系列発生の“鍵”ともいうべき原始多項式についてはすでに多くの研究がなされており，特に文献 (3) には $n=34$ 次（周期＝約 1.6×10^{10} の M 系列を発生）までのものが多数示されている。

この解説の付録にもすぐ利用できるように，いくつかの原始多項式を示しておいた。

なお，M 系列を高速で発生させる方法が文献 (11) に示されている。

2.3. 例

1.1, 2.1 および 2.2 で述べたことを具体的に理解するために，ごく簡単な例として4次の原始多項式により発生される周期 $15(=2^4-1)$ の M 系列をとりあげる。

2.3.1. 直接計算による発生

まず4次の原始多項式 $f(x)=\sum_{i=0}^{4} c_i x^i$ の係数は付録にあるように

$$(c_0, c_1, c_2, c_3, c_4)=(1,1,0,0,1) \tag{35}$$

であるから，(33)式を参考にするとこの場合の回帰方程式は次式になる。

$$a_i=a_{i-1}\oplus a_{i-4}, \quad i=4,5,\cdots \tag{36}$$

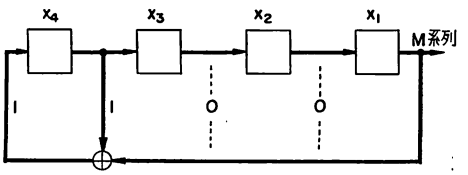
ここで初期値として便宜上 $a_0=a_1=a_2=0$, $a_3=1$ を与えると，この条件のもとで(36)式により生成される M 系列は次のようになる。

$$(\underset{\text{初期値}}{\text{‘000111101011001’}}\ 0001\cdots\cdots) \tag{37}$$

これをみると‘ ’内のものが1周期分の系列であり，周期が $2^4-1=15$ になっていることがわかる。

2.3.2. シフトレジスタによる発生

(35)式および第5図を参考にすると，この場合の M 系列発生回路は第7図のようになる。



第7図 周期 15 の M 系列発生回路

そこでこの回路において flip-flop (x_4, x_3, x_2, x_1) の初期値を 2.3.1 の場合にならって $(1,0,0,0)$ とすると，各時刻における (x_4, x_3, x_2, x_1) の状態は (2.2.2 の (i)～(iii) を参考にすれば）次のように変化していくことがわかる。

$(x_4x_3x_2x_1)$ の内容の変化

$$1000\to1100\to1110\to1111\to0111\to1011\to0101\to1010\to1101\to0110\to0011\to1001\to0100\to0010\to0001\to1000\to \tag{38}$$

→以後繰返し

これから出力系列となる x_1 の内容（… のついた部分）をとり出すと次のような M 系列が得られる。

$$(\underset{\text{初期値}}{\text{‘000111101011001’}}\ 0001\cdots) \tag{39}$$

これは当然のことながら先の結果(37)式に一致している。

なお(38)式をみると $(x_4x_3x_2x_1)$ の状態が，1周期の間にすべての可能な状態（1から15までのすべての整数の2進表示）を経過していることが確かめられる。

2.3.3. $(M\text{-}1)$～$(M\text{-}5)$ の検証

次にいま得られた(39)式の M 系列の1周期分

$$A_0=(000111101011001) \tag{40}$$

が 2.1 の性質 $(M\text{-}1)$～$(M\text{-}5)$ を実際に満たしているかどうかを調べてみる。

$(M\text{-}1)$ 周期性

周期 $p=15=2^4-1$ をもつ。

$(M\text{-}2)$ 均一性

‘1’の出現回数＝$8=2^{4-1}$

‘0’の出現回数＝$7=2^{4-1}-1$

$(M\text{-}3)$ 連なり性

連なりを分類すると次のようになる。

| 000 | 1111 | 0 | 1 | 0 | 11 | 00 | 1 |

したがって

分類数＝8

連なり数1のもの $\left\{\begin{matrix}\text{‘0’…2回}\\ \text{‘1’…2回}\end{matrix}\right\}$ 計 4回$=2^{4-1-1}$,

出現率$=\frac{4}{8}=2^{-1}$

連なり数2のもの $\left\{\begin{matrix}\text{‘00’…1回}\\ \text{‘11’…1回}\end{matrix}\right\}$ 計 2回$=2^{4-2-1}$,

出現率$=\frac{2}{8}=2^{-2}$

連なり数3のもの ‘000’ 1回 計1回

連なり数4のもの ‘1111’ 1回 計1回

*第5図の回路により発生し得る系列の最大の周期は 2^n-1 であることは容易にわかる。（なお第Ⅱ部 4.2 参照）

(M-5) Delay-and-Add 性

A_0 とこれを左方へ1回巡回シフトした系列 A_1 との mod 2 和を計算する。

$$\begin{array}{ll} & A_0=(000111101011001) \\ \oplus) & A_1=(001111010110010) \\ \hline & A_0\oplus A_1=(001000111101011) \end{array}$$

このとき右辺は A_0 を左方へ 12 回巡回シフトしたものになっているから，これは A_{12} に等しい。

$$\therefore\ A_0\oplus A_1=A_{12}$$

$$\begin{array}{ll} & A_0=(000111101011001) \\ \oplus) & A_2=(011110101100100) \\ \hline & A_0\oplus A_2=(011001000111101) \end{array}$$

$$\therefore\ A_0\oplus A_2=A_9$$

同様にして $A_0\oplus A_3,\cdots,A_0\oplus A_{15}$ について計算すると A_0 が Delay-and-Add 性を満たしていることがわかる。

(M-4) 自己相関性

(M-2) および (M-5) により任意の $k(0<k<15)$ に対して $\sum_{i=0}^{14}(a_i\oplus a_{i+k})=8,\ 0<k<15$

これと(6)式から

$$\rho(k)=(15-2\times 8)/15=-1/15$$
$$=-1/(2^4-1),\quad 0<k<15$$
$$\rho(0)=1$$

となる。

以上により(39)式が (M-1)～(M-5) をすべて満たしていることが確かめられた。

この例によって，PN 系列の性質 (PN-1)～(PN-4) および M 系列の性質 (M-1)～(M-5) を具体的に理解されたことと思う。

3. M 系列の利用

PN 系列の代表的存在である M 系列は，その発生の容易さから各方面にいろいろな形で利用されているが，その中から主なものをあげると次のように分類できる。

（i） 鋭い自己相関性を利用したもの：レーダ(2)(12)，符号(2)(3)

（ii） 雑音性を利用したもの：擬似白色雑音源(13)(14)

(iii) M 系列固有の性質を利用したもの：符号誤り率測定(15)

なお擬似乱数として利用する場合には，周期をなるべく大きくとり，そのうちの一部分を使用するほうがよいであろう。

第Ⅱ部 特 論(数学的側面)

第Ⅰ部では PN 系列および M 系列の一般的な説明を行なった。

これに対してこの第Ⅱ部では，特に M 系列についてその理論的背景にふれることを目的としている。

ところで M 系列の理論は“円分剰余類”(cyclotomic cosets)，“差集合”などの概念を用いて代数的に構成するのが，全体的な見通しもよくきくので具合がよい。しかしそれには代数学についての予備知識をある程度仮定しなければならず，この解説の初期の目的にそわなくなる。

そこで，ここでは予備知識をほとんど必要としない，線形回帰系列論を利用した説明を試みた。

4. 線形回帰系列序論(1)(5)

初めに系列の要素である‘0’および‘1’についての代数的説明をしておく。

いま，0および1の二つの元からなる集合 $\{0,1\}$ を考え，この集合の元について次のような二つの結合関係—“加法”および“乗法”—を定義する。

(加法)*1

$\dotplus$	0	1
0	0	1
1	1	0

(乗法)

$\cdot$	0	1
0	0	0
1	0	1

(41)

このとき集合 $\{0,1\}$ は“有限体”*2 (finite field) となり，通常これを $GF(2)$ で表示する。

$$GF(2)=\{0,1\} \tag{42}$$

$GF(2)$ においては(41)式から次式が成り立つ。

$$\begin{aligned} -0&=0 \\ -1&=1 \end{aligned} \tag{43}$$*3

4.1. 線形回帰系列と母関数

2.2 の(33)式にならって，次のような n 次線形回帰方

---

*1 mod 2 和である。

*2 ある適当な集合があり，この集合の各元に対していわゆる“四則算法”（加減乗除）が自由にできるとき，この集合を“体”(field) とよぶ。このとき，集合の元の個数が有限ならば有限体，そうでなければ無限体あるいは単に体とよぶ。たとえば有理数全体の集合 Q は体である。なお GF は Galoi Field（ガロア体）の頭文字である。詳しくは代数学の参考書，たとえば文献(16)など参照。

*3 $\because$ 0+0=0, 1+1=0

程式を考える。

$$a_i \equiv \sum_{l=1}^{n} c_l a_{i-l} \pmod 2, \quad i=n, n+1, \cdots \tag{44}$$

$$c_n=1, \quad c_l=0,1, \quad 1 \leqq l \leqq n-1$$

$$a_l=0,1$$

このとき初期値 $(a_0, a_1, \cdots, a_{n-1})$ を与えた場合，この式から生成される系列を“線形回帰系列”(linear recurrent sequences) とよび，これを 1.1 の(1)式にならって次式で表示する。

$$\{a_i\}=(a_0, a_1, \cdots, a_{n-1}, a_n, a_{n+1}, \cdots), \quad a_l=0,1 \tag{45}$$

また，(44)式の c_l を係数とする n 次多項式

$$f(x)=\sum_{l=0}^{n} c_l x^l, \quad c_0=c_n=1, \quad c_l=0,1, \quad 1 \leqq l \leqq n-1 \tag{46}$$

を回帰系列 $\{a_i\}$ の（n 次）“特性多項式” (characteristic polynomial) とよぶ。

さらに，(45)式の各要素を係数とするベキ級数

$$G(x)=\sum_{i=0}^{\infty} a_i x^i \tag{47}$$

を回帰系列 $\{a_i\}$ の“母関数” (generating function) とよぶ。すると回帰系列 $\{a_i\}$ と母関数 $G(x)$ とは明らかに1対1に対応づけられることになり，母関数は回帰系列を調べるうえで有効な概念となる。

ところで(44)式，(46)式および(47)式をみるとわかるように，母関数 $G(x)$ と特性多項式 $f(x)$ とは互いに密接な関係にあることが予想される。次にこの関係を明らかにする。

いま $G(x)$ の係数 a_i が(44)式により決定されるものとすると，$G(x)$ は(44)式および(47)式から次のように変形できる。

$$\begin{aligned} G(x) &= \sum_{i=0}^{n-1} a_i x^i + \sum_{i=n}^{\infty} \left(\sum_{l=1}^{n} c_l a_{i-l}\right) x^i \\ &= \sum_{i=0}^{n-1} a_i x^i + \sum_{l=1}^{n} c_l x^l \sum_{i=n}^{\infty} a_{i-l} x^{i-l} \\ &= \sum_{i=0}^{n-1} a_i x^i + \sum_{l=1}^{n} c_l x^l \sum_{k=n-l}^{\infty} a_k x^k \\ &= \sum_{i=0}^{n-1} a_i x^i + \sum_{l=1}^{n-1} c_l x^l \left[\sum_{k=0}^{\infty} a_k x^k - \sum_{k=0}^{n-l-1} a_k x^k\right] \\ &\quad + c_n x^n \sum_{k=0}^{\infty} a_k x^k \\ &= \sum_{i=0}^{n-1} a_i x^i - \sum_{l=1}^{n-1} \sum_{k=0}^{n-l-1} c_l a_k x^{l+k} + G(x) \sum_{l=1}^{n} c_l x^l \end{aligned} \tag{48}$$

ここで右辺第3項を左辺に移すと左辺は次のようになる。

$$G(x)\left[1-\sum_{l=1}^{n} c_l x^l\right]=G(x)\sum_{l=0}^{n} c_l x^l = G(x) f(x) \tag{49}$$*1

(49)式を用いると(48)式は次のようになる。

$$G(x)=\frac{h(x)}{f(x)} \tag{50}$$

ただし

$$h(x)=\sum_{i=0}^{n-1} a_i x^i + \sum_{l=1}^{n-1} \sum_{k=0}^{n-l-1} c_l a_k x^{l+k} \tag{51}$$

この(50)式が回帰系列 $\{a_i\}$ の母関数 $G(x)$ と特性多項式 $f(x)$ との関係を表わす式である。

したがって特性多項式 $f(x)$ (46)式) が決まり，初期値 $(a_0, a_1, \cdots, a_{n-1})$ が与えられれば，回帰系列 $\{a_i\}$ は(44)式の回帰方程式あるいは(50)式の母関数のいずれを用いても生成できることがわかる。

なお(51)式をみればわかるように，(50)式の分母 $f(x)$ の次数が n 次であるのに対し，分子 $h(x)$ の次数は $(n-1)$ 次以下であることに注意されたい。

4.2. 回帰系列の周期

前節で明らかにされたように，回帰系列 $\{a_i\}$ は特性多項式 $f(x)$ および初期値 $(a_0, a_1, \cdots, a_{n-1})$ が与えられれば一意に決定される。このとき(44)式または(50)式により生成される回帰系列は，その名のとおり必ず周期性をもつことが次の定理により示される。

定理1

n 次特性多項式 $f(x)$ により生成される回帰系列 $\{a_i\}$ は必ず周期性をもち，かつその周期 p はたかだか 2^n-1 である。

$$1 \leqq p \leqq 2^n-1 \tag{52}$$

(証明)

いろいろな証明法があるが，ここでは直観的にわかりやすい方法で証明する。

いま(44)式に注目すると，a_i は右辺の n 組 (n-tuple) $c_1 a_{i-1}$, $c_2 a_{i-2}$, $\cdots$, $c_n a_{i-n}$ により一意的に決定される。

*1 符号の反転は(43)式による。以下同様。

ところで，n-tuple のとり得る可能な状態の総数は 2^n であるから，係数 $(c_1, c_2, \cdots, c_n)$ が一定であれば，初期値 $(a_0, a_1, \cdots, a_{n-1})$ をどのように与えても，先の n-tuple の状態はたかだか 2^n 個の状態経過の中で必ず最初の状態にもどってしまう。このことは，とりもなおさず系列 $\{a_i\}$ が周期系列になることを示している。

ところで n-tuple が all 0 である場合（たとえば初期値が all 0）には，生成される系列は常に 0 だけからなる 0 系列（00…）となる。このようなものを除外することにすると n-tuple の可能な状態数は 2^n-1 になる。

したがって上記の回帰系列 $\{a_i\}$ は周期 p $(1 \leqq p \leqq 2^n-1)$ をもつことが結論される。

（証明終り）

定理 1 で回帰系列の周期性が示されたが，次に述べる定理 2 はその周期の値を決定するものである。

定理 2

n 次の既約[*1]な特性多項式 $f(x)$ により生成される回帰系列 $\{a_i\}$ の周期は，$f(x)$ で割り切れるような多項式 (x^p+1) の p の最小値で与えられる。

$$\{a_i\} \text{ の周期} = \inf\{p\,;\, f(x) \mid x^p+1\} \tag{53}$$[*2]

さらにこのときの周期は初期値 $(a_0, a_1, \cdots, a_{n-1})$ には依存しない。

（証明）

4.1 の記号をそのまま用いる。

（i） $\{a_i\}$ が周期 p をもつと仮定する。

$$\begin{aligned} h(x)/f(x) = G(x) &= (a_0+a_1x+\cdots+a_{p-1}x^{p-1}) \\ &\quad +x^p(a_0+a_1x+\cdots+a_{p-1}x^{p-1})+\cdots \\ &= (a_0+a_1x+\cdots+a_{p-1}x^{p-1})(1+x^p \\ &\quad +x^{2p}+\cdots) \\ &= (a_0+a_1x+\cdots+a_{p-1}x^{p-1})/(1+x^p) \end{aligned} \tag{*3}$$

したがって

$$h(x)(1+x^p)/f(x) = (a_0+a_1x+\cdots+a_{p-1}x^{p-1})$$

この式において，前節で示した $d(h) < d(f)$[*4] なることと $f(x)$ の既約性を用いると $f(x) \mid (1+x^p)$ が結論される。

（ii） $f(x) \mid (1+x^p)$ を仮定する。

$$h(x)(1+x^p)/f(x) = b_0+b_1x+\cdots+b_{p-1}x^{p-1}$$

とおくと

$$\begin{aligned} h(x)/f(x) &= (b_0+b_1x+\cdots+b_{p-1}x^{p-1})/(1+x^p) \\ &= (b_0+b_1x+\cdots+b_{p-1}x^{p-1})(1+x^p \\ &\quad +x^{2p}+\cdots) \\ &= (b_0+b_1x+\cdots+b_{p-1}x^{p-1})+x^p(b_0+b_1x \\ &\quad +\cdots+b_{p-1}x^{p-1})+\cdots \end{aligned}$$

$$\therefore\ G(x) = \sum_{i=0}^{\infty} a_ix^i = b_0+b_1x+\cdots+b_{p-1}x^{p-1} + b_0x^p+b_1x^{p+1}+\cdots$$

この式において同じ次数の係数を等しいとおくと

$$b_i = a_i = a_{i+p} = a_{i+2p} = \cdots\cdots,\quad i = 0, 1, 2, \cdots$$

となる。したがって $\{a_i\}$ は周期 p をもつことがわかり，結局 $\{a_i\}$ の周期はこのような p の最小値で与えられることが結論される。さらに，この周期 p が初期値 $(a_0, a_1, \cdots, a_{n-1})$ に依存しないことは，上記の証明の過程をみれば明らかである。（証明終り）

5. M 系 列

5.1. 原始 p 乗根

4.2 の定理 1 および定理 2 によると，n 次の既約な特性多項式を適当にとれば，それにより生成される回帰系列 $\{a_i\}$ は最大周期 2^n-1 をもち得ることがわかる。

この節および次節では，そのような特性多項式がどんな性質のものであるかについて説明する。

いま周期 $p=2^n-1$ をもつ系列 $\{a_i\}$ を生成する n 次の特性多項式 $f(x)$ が存在するものとすると，定理 2 から次式が成り立つ。

$$f(x) \mid (x^p+1), \qquad p = 2^n-1 \tag{54}$$

これは (x^p+1) を既約多項式の積に因数分解したとき，そのうちのある因子が $f(x)$ であることを示している。そこで (x^p+1) の因数分解について考えると，これは

$$x^p+1 = 0 \tag{55}$$

あるいは

$$x^p = 1 \tag{56}$$

の根がすべて求められれば可能となる。

ところが，(53)式の根は一見してわかるとおり 1 の p

---

*1 $GF(2)$ の係数をもつより低次の多項式に因数分解できない多項式のこと。なお $f(x)$ が可約（非既約）である場合の周期については文献（1）（5）を参照されたい。

*2 "inf" は "下限" を意味する記号。また，$f(x) \mid g(x)$ は，$f(x)$ が $g(x)$ を割り切ることを意味する "Landau の記号" である。

*3 $(1+x^p)(1+x^p+x^{2p}+\cdots\cdots)=1$

*4 $d(f)$ は $f(x)$ の次数（degree）を意味する記号である。

乗根であり全部で p 個存在するが，このうちで $GF(2)$ に属するものは根 '1' だけである。すなわち(55)式は $GF(2)$ の範囲だけでは完全に解くことはできない。

この制限をなくすために，$GF(2)$ に1以外のすべての1の p 乗根を追加して新しい集合をつくる。このようにして得られる集合は全部で 2^n 個*1の元を含み，これもまた有限体となる*2。これを通常 $GF(2^n)$ で表わす*3。

このようにすると(55)式は $GF(2^n)$ においてすべての根をもち，それらはよく知られているように次式で表わされる。

$$r_k=e^{j2\pi k/p}, \quad k=0,1,\cdots, p-1 \tag{57}$$

$$p=2^n-1, \quad j=\sqrt{-1}$$

次に(57)式において k が p に素である場合を考える。このような k を k' で表わすと，根 r_k'

$$r_k'=e^{2\pi jk'/p}, \quad (k',p)=1 \tag{58}$$

の p 個の累乗

$$r_k'=e^{j2\pi k'/p}, \ r_k'^2=e^{j2\pi 2k'/p}, \ \cdots,$$

$$r_k'^p=e^{j2\pi pk'/p}(=1) \tag{59}$$

は互いに相異なる p 個の，1 の p 乗根となる。

なぜなら，もし $l\neq m$, $1\leqq l,m\leqq p$ に対して

$$r_k'^l=r_k'^m$$

となったとすると，(59)式から

$$lk'/p\equiv mk'/p \pmod p$$

したがって

$$lk'\equiv mk' \pmod p$$

$$(l-m)k'\equiv 0 \pmod p$$

となる。ところが $(k', p)=1$ であるから，上式が成り立つためには

$$l-m\equiv 0 \pmod p$$

となることが必要であるが，これは先の条件のもとでは不可能である。

以上のことから次の結論が得られる。

$x^p=1$ のすべての根（(57)式）は，根

$$r_k'=e^{j2\pi k'/p}, \ (k',p)=1, \ 1\leqq k'<p, \ p=2^n-1 \tag{60}$$

の適当な累乗（(59)式）に等しくなる。

いいかえると，すべての '1 の p 乗根' は(60)式の r_k' の累乗として生成される。

また，このような根 r_k' は p 乗して初めて1に等しくなる（このことを "位数"（order）p をもつという）ことも，先の説明から容易にわかる。

このとき，(60)式で表わされるような位数 p をもつ根 r_k' を1の "原始 p 乗根"（primitive root）とよぶ。

次に，p が与えられた場合，1の原始 p 乗根がいくつ存在するかということについて調べることにする。

これは(60)式をみればわかるように，$1\leqq k'<p$ で $(k', p)=1$ すなわち p に素である整数 k' の個数に等しい。

この個数を $\varphi(p)$ とすると，これは "Euler の関数"

$$\varphi(p)=p\prod_{i=1}^{m}\left(1-\frac{1}{q_i}\right)$$

$$=\prod_{i=1}^{m}q_i^{\nu_i-1}(q_i-1) \tag{61}$$*4

ただし

$$p=\prod_{i=1}^{m}q_i^{\nu_i}, \ q_i=\text{素数}\ (p\ \text{の素因数分解})$$

により求めることができる(16)。

ここで $p=2^n-1$ の場合には次式が成り立つ(16)。

$$n\mid\varphi(2^n-1) \tag{62}$$

すなわち，1 の原始 (2^n-1) 乗根の個数は n の整数倍だけ存在する。

5.2. 原始多項式と M 系列

前節の説明によって多項式 (x^p+1) は，$\varphi(p)$ 個の原始 p 乗根と $p-\varphi(p)$ 個のその他の p 乗根（位数$<p$）をもつことがわかった。

そこで $\varphi(2^n-1)$ 個の原始 (2^n-1) 乗根のうちの n 個を根としてもち，かつ係数が $GF(2)$ であるような n 次多項式—これを "原始多項式"（primitive polynomial）とよぶ(3)—を $f(x)$ で表わすと，

$$f(x)\mid x^p+1, \quad p=2^n-1 \tag{63}$$

および

$$f(x)\mid x^{p'}+1, \quad p'<2^n-1 \tag{64}$$

---

*1 $2+p-1=2+2^n-1-1=2^n$

*2 一般に q を素数とすると，q^n 個の元をもつ集合は有限体 $GF(q^n)$ になることが証明される(16)。

*3 この $GF(2^n)$ を，x^p+1 の "分解体"（decomposition field）あるいは $GF(2)$ の "拡大体'（extension field）とよび，これに対して $GF(2)$ を "基礎体"（ground field）とよぶ。詳しくは文献(16)などを参照されたい。

*4 この式は任意の正の整数に対して成り立つ。

（例）$p=15$ のとき，15 に素な数は $\{1,2,4,7,8,11,13,14\}$ の8個，一方 $\varphi(15)=\varphi(3\cdot 5)=(3-1)(5-1)=8$

が成り立つことは容易にわかる。さらに，この $f(x)$ は既約であることも証明できる(3)(16)。

したがって，4.2 の定理2(53)式，(63)式および(64)式を用いると，n 次の原始多項式を特性多項式にすれば，これにより生成される回帰系列 $\{a_i\}$ は“最大周期 2^n-1”をもち，次節でこれが M 系列になることがわかる。

ところで，互いにシフト関係にある M 系列を同種の M 系列であるとみなすと，周期 2^n-1 の相異なる M 系列の数は，上記の結論から n 次の原始多項式の数だけであることがわかる。すなわち，この個数は(62)式により

$$\varphi(2^n-1)/n \tag{65}$$

で求められる。

以上の説明によって，M 系列が原始多項式により生成される理由についてだいたい理解されたことと思う。

5.3. M 系列の諸性質の証明

この節では，第Ⅰ部2.1で述べた (M-1)～(M-5) の性質を前節で述べた M 系列が事実もっていることについての証明をする。

前節までの説明からわかるように，周期 $p=2^n-1$ をもつ M 系列 $\{a_i\}=(a_0, a_1, \cdots, a_{p-1}, a_0, a_1, \cdots)$ があるとすると，このときの n-tuple $(a_{i-n}, a_{i-n+1}, \cdots, a_{i-1})$ の状態は，1周期の間にすべての可能な状態（1から 2^n-1 までのすべての整数を2進表示したもの）を各々1回ずつ経過する。

このことをわかりやすくするために，1周期内における n-tuple の状態を便宜上次のように行列表示する。

(n-tuple)

$$\left.\begin{array}{l} a_0a_1\cdots\cdots\cdots a_{n-1} \\ a_1a_2\cdots\cdots\cdots a_n \\ \cdots\cdots\cdots\cdots\cdots \\ a_{i-n}a_{i-n+1}\cdots\cdots a_{i-1} \\ a_{i-n+1}a_{i-n+2}\cdots\cdots a_i \\ \cdots\cdots\cdots\cdots\cdots \\ a_{p-1}a_0\cdots\cdots\cdots a_{n-2} \end{array}\right\}, \quad a_l=0,1 \tag{66}$$

すると(66)式の各行は，順序は別にして，1から 2^n-1 までのすべての2進表示を表わしている。

また(66)式の各列は M 系列 $\{a_i\}$ のシフト系列になっていることもわかる。

以下の証明はこれらの事実をもとにして行なう。

(M-1) 周期性

明らかに周期 $p=2^n-1$ をもつ。

(M-2) 均一性

各行の2進数において，いちばん左のほうを2進数の最下位とみなせば，1から 2^n-1 の間に奇数（最下位=1）は 2^{n-1} 個，偶数（最下位=0）は $2^{n-1}-1$ 個存在するから，$(a_0, a_1, \cdots, a_{p-1})$ において‘1’は 2^{n-1} 回，‘0’は $2^{n-1}-1$ 回それぞれ出現する。

(M-3) 連なり性

M 系列の1周期分 $(a_0, a_1, \cdots, a_{p-1})$ を(66)式の各行のように n-tuple ずつに区切る。このとき各行において連なり数 k のものが何回出現するかを調べる。

まず連なり数 $k(1\leqq k\leqq n-2)$ の‘1’の連なりについて調べる。これを便宜上，(66)式の n-tuple において

$$(\underbrace{011\cdots}_{k}\underbrace{10}\underbrace{XX\cdots X}_{n-k-2}), \quad 1\leqq k\leqq n-2$$

の形で勘定すると，X 印は任意にとれるから，この形のものは 2^{n-k-2} 個存在する。このことは‘0’の場合についても同様に成り立つから，結局連なり数 $k(1\leqq k\leqq n-2)$ の出現回数は次式で与えられる。

$$2^{n-k-1} \tag{67}$$

すると連なり数 k のものに含まれる‘0’および‘1’の個数は全部で

$$\sum_{k=1}^{n-2} k2^{n-k-1}=2^n-2n$$

だけある。したがって残りの部分は $2^n-1-(2^n-2n)=2n-1$ となる。このうち，連なり数 n の‘1’の連なりがあることは明らかである。すると最後の残りは連なり数 $(n-1)$ のものであるが，これは (M-2) の均一性により‘0’の連なりであることがわかる。

以上のことから，連なりの分類数は

$$\sum_{k=1}^{n-1} 2^{n-k-1}+2=2^{n-1} \tag{68}$$

であり，これと(67)式から連なり数 k の出現率は

$$2^{n-k-1}/2^{n-1}=2^{-k}, \quad 1\leqq k\leqq n-2 \tag{69}$$

となることがわかる。

(M-5) Delay-and-Add 性

前述したとおり，M 系列は特性多項式の係数 $c_1, c_2, \cdots, c_n$ が一定であれば，初期値 $(a_0, a_1, \cdots, a_{n-1})$ により一意的に決定される。そこでいま初期値 $(a_0, a_1, \cdots, a_{n-1})$ による系列を A_0 とする。このとき他の任意の初期値を考えると，これは(66)式のいずれかの行に必ず一致するはずであるから，これを $(a_k, a_{k+1}, \cdots, a_{k+n-1})$ と表示することができる。

このとき初期値 $(a_k, a_{k+1}, \cdots, a_{n+k-1})$ による系列 A_k は明らかに A_0 の k 回シフト系列になっている。

ところで A_0 および A_k は同じ回帰方程式

$$a_i \equiv \sum_{l=1}^{n} c_l a_{i-l} \pmod 2 \tag{70}$$

を満たすから当然次式が成り立つ。

$$a_n \equiv c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_n a_0 \pmod 2 \tag{71}$$

$$a_{k+n} \equiv c_1 a_{k+n-1} + c_2 a_{k+n-2} + \cdots + c_n a_k \pmod 2 \tag{72}$$

(71)(72)の両式を mod 2 加算すると

$$a_n + a_{k+n} \equiv c_1(a_{n-1} + a_{k+n-1}) + c_2(a_{n-2} + a_{k+n-2}) + \cdots + c_n(a_0 + a_k) \pmod 2 \tag{73}$$

となる。ここで n-tuple $\{a_0 \oplus a_k, a_1 \oplus a_{k+1}, \cdots, a_{n-1} \oplus a_{k+n-1}\}$ について考えると，これもやはり (66)式のいずれかの行に一致するから，これを $(a_i, a_{i+1}, \cdots, a_{i+n-1})$ で表わすことができる。

すると(73)式から次式が成り立つ。

$$a_{i+n} \equiv c_1 a_{i+n-1} + c_2 a_{i+n-2} + \cdots + c_n a_i \pmod 2 \tag{74}$$

ところで初期値 $(a_i, a_{i+1}, \cdots, a_{i+n-1})$ による系列 A_i もやはり A_0 の i 回シフト系列である。

以上のことから結局次式が得られる。

$$A_0 \oplus A_k = A_i \tag{75}$$

ここでもちろん $0 < i < p$ であり，かつ $i \neq k$ である。(∵ $i=k$ とすると A_0 は0系列になってしまう。)

(M-6) 自己相関性

自己相関関数の定義 ((6)式)，(M-2) および (M-5) により明らかである。 (証明終り)

あ と が き

第Ⅰ部においては PN 系列についての一般的説明を行なった。そのうち特に M 系列については，その発生法を具体的に述べ，付録Ⅰを用いることにより直ちに利用できるようにした。

一方第Ⅱ部においては，M 系列の数学的側面を線形回帰系列論を用いてわかりやすく説明した。そのうち M 系列と原始多項式との関係については詳しく説明した。ただし，予備知識をほとんど仮定しないという条件のために，内容がある面に限定されたことを断わっておく。

なお，この解説で述べなかったことのうちで特に重要と思われる関連事項は，だいたい次のようなことである。

- M 系列と円分剰余類 (cyclotomic cosets) との関係[1]
- M 系列と，差集合および実験計画法における BIBD との関係[1][2][10][17][18]
- M 系列の誤り訂正符号における立場[3]
- M 系列の部分系列[2]
- 行列法による M 系列の解析[4]
- 線形回帰系列詳論[1][4][5]

なお PN 系列 (M 系列も含む) についての詳しい成書としては文献(1)が，また利用面に主眼をおいたものとしては文献(2)などがあげられる。

おわりに，日ごろ指導いただく生島当研究室長ならびにこの解説を作成する際有益な意見を下さった角川通信系研究室長に深謝する。また文献(14)の存在を知らせて下さった鈴木音声研究室長にも厚くお礼申し上げる。

参 考 文 献

(1) Golomb, S. W., Shift Register Sequences, Holden-Day Inc., 1967.

(2) Golomb, S. W., ed. Digital Communications with Space Applications, Prentice-Hall Inc., 1964.

(3) Peteson, W. W., Error-Correcting Codes, MIT. Press, 1961.

(4) Elspas, B., The Theory of Autonomous Linear Sequential Networks, I. R. E. Trans. CT., **CT-6**, 1, pp. 45～60, Mar., 1959.

(5) Zieler, N., Linear Recurring Sequences, *Linear Sequential Switching Circuits*, Kauts W., ed. Holden-Day Inc., 1965.

(6) Paley, R. E. A. C., On Orthogonal Matrices, Jour. Math. Phys., 12, pp. 311～320, 1933.

(7) Plotkin, M., Binary Codes with Specified Minimum Distance, IRE. Trans. IT, **IT-6**, 4, Sept. 1960.

(8) Hall, Jr. M., A Survey of Difference Sets, Proc. American Math. Soc., 7, pp. 975～986, 1956.

(9) Brauer, A., On A New Class of Hadamard Determinants, Mathematishe Zeitschrift, 58, pp. 219～225, 1953.

(10) Gordon, B. et al., Some New Difference Sets, Canadian Jour. Math., 14, pp. 614～625, 1962,

(11) 松岡 毅，千葉信行，M 系列発生の高速化，信学論(A) **53-A**，2，p. 120，昭和45. 2.

(12) 阪本，滝，宮川ほか，符号化パルスレーダー方式，電通学誌，46，2，pp. 155～162，昭和38. 2.

(13) 相良節夫，同定問題，計測と制御，8，4，pp. 268～280，昭和44. 4.

(14) 青島伸治，五十嵐寿一，M 系列の相関を用いた音響測定，音響学誌，24，4，pp. 197～206，昭和43. 7.

(15) 笠原芳郎，笠原正雄，最大周期系列を用いた符号誤り測定の一方式，電通学誌，48，5，pp. 877～883，昭和40. 5.

(16) Van der Waerden B. L.，(銀林浩訳)，現代代数学Ⅰ，Ⅱ，東京図書，昭和35.

(17) 増山元三郎，実験計画法，岩波講座現代応用数学，岩波書店，昭和32.

(18) 山本純恭，BIBD と Coding Theory，数理科学，8，6，pp. 62～66，昭和45. 6.

なお上記の文献は本文で引用したものであって，PN 系列に関する完全なリストではない。

付録Ⅰ　原始多項式係数表

文献(3)pp. 254～270 にある，34次までの既約多項式表からいくつかの原始多項式を適当に選び出したものを次表に示す。

(表の見方)

表には，原始多項式

$$f(x)=c_nx^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0 \qquad (A.1)$$

の係数 $c_n, c_{n-1}, \cdots, c_1, c_0$ を，c_0 のほうから3桁ずつ区切り，その各々の3桁の2進数を8進数に変換したものを示してある。

(例)

10次のところにある '2157' は

2　1　5　7

010 001 101 111

$c_{10}c_9\cdots\cdots c_1c_0$

であるから，原始多項式

$$f(x)=x^{10}+x^6+x^5+x^3+x^2+x+1$$

を意味している。

8進↔2進変換表

8進数	2進数
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

なお (A.1) 式が原始多項式であれば，これらの係数を逆向きにして得られる多項式

$$g(x)=c_0x^n+c_1x^{n-1}+\cdots+c_{n-1}x+c_n \qquad (A.2)$$

もまた原始多項式である。

この $g(x)$ により生成される M 系列は，$f(x)$ による M 系列を逆向きに並べたものになる。

原　始　多　項　式　係　数　表

次数	周　期	係　数　(8 進 表 示)
3	7	13,
4	15	23,
5	31	45, 67, 75,
6	63	103, 147, 155,
7	127	203, 211, 217, 235, 277, 313, 325, 345, 367,
8	255	435, 453, 537, 543, 545, 551,
9	511	1021, 1055, 1131, 1157, 1167, 1175,
10	1023	2011, 2033, 2157, 2443, 2745, 3471,
11	2047	4005, 4445, 5023, 5263, 6211, 7363,
12	4095	10123, 11417, 12515, 13505, 14127, 15053,
13	8191	20033, 23261, 24623, 30741, 32535, 37505,
14	1.6(4*)	42103, 51761, 55753, 60153, 71147, 67401,
15	3.2(4)	100003, 110013, 120265, 133663, 142305, 164705,
16	6.3(4)	210013, 233303, 307572, 311405, 347433, 375213,
17	1.3(5)	400011, 411335, 444257, 527427, 646775, 714303,
18	2.5(5)	1000201, 1002241, 1025711, 1703601,
19	5(5)	2000047, 2020471, 2227023, 2331067, 2570103, 3610353,
20	1(6)	4000011, 4001051, 4004515, 4442235, 6000031,
21	2(6)	10000005, 10020045, 10040205, 10040315, 10103075,

22	4 (6)	20000003, 20001043, 20070217, 20401207, 20430607,
23	7.9(6)	40000041, 40000063, 40006341, 40103271, 40435651,
24	1.6(7)	100000207, 113763063, 125245661,
25	3.2(7)	200000011, 200000017, 200010031, 200402017, 201014171,
26	7.3(7)	400000107, 402365755, 426225667, 473167545,
27	1.3(8)	1000000047, 1001007071, 1020024171, 1102210617,
28	2.5(8)	2000000011, 2000025051, 2020006031, 2104210431,
29	5 (8)	4000000005, 4001040115, 4004204435, 4400000045,
30	1 (9)	10040000007, 10115131333, 10343244533, 11326212703,
31	2 (9)	20000000011, 20000000017, 20000020411, 21042104211,
32	4 (9)	40020000007, 40035532523, 40460216667, 42003247143,
33	7.9(9)	100000020001, 100020024001, 100020224401, 104000420001,
34	1.6(10)	201000000007, 201472024107, 225213433257, 227712240037,

* 約 1.6×10^4 を意味，以下同様