数理解析研究所講究録
第 333 巻 1978 年 221-235

Z_qの上の線型フィードバック・シフトレジスタについて

日本電気(株) 中央研究所 中村勝洋

[1] まえがき

誤り訂正符号(*Error Correcting Codes*)その他に種々の工学的応用を持つ線型フィードバック・シフトレジスタ(*Linear Feedback Shift Register*；以後<u>LFSR</u>と略す。)については既に多くの研究がなされ、その諸性質はよく知られている。[1]〜[7]

しかしながら、従来考察の対象とされてきたものは、一般には<u>有限体$GF(q)$</u>($q=p^m$；pは素数，mは自然数)の上のLFSRであり，qを法とする<u>整数剰余環Z_q</u>(*the ring of integers modulo* q，Z_q)の上のLFSRに関する研究は筆者の知る限り今迄あまりなされていない様に思われる。

Z_qの上のLFSRについて論じることは、結局のところZ_qの拡大環(*extension ring*)の具体的な構造あるいは性質を論じることにつながるが，このZ_qの拡大環に関する具体的な性質に関しても，*Blake*[8]が指摘したように、あまり考察され

てはいない。

また、実用的な面からいえば、最近のディジタル通信技術の分野で，Z_4あるいはZ_8の上のごく簡単なLFSRが、一部、プリコーダとして応用されてはいるものの、LFSR自体の一般的な性質の解明は殆んどなされていない。

一方、筆者は先に衛星通信への応用に適した誤り訂正符号として、Z_q $(q=2^m)$ の上の誤り訂正符号の新しい構成法について論じたが[9],[10]，その過程において，Z_qの上のLFSRの諸性質を明らかにしなければならなかった。

そこで、本稿は，その際の結果も含め，このZ_qの上のLFSRに対して更に考察を加え、その諸性質を整理し、あわせて未解決な一命題をも提示しようとするものである。

本稿によって、Z_qの上のLFSRの基本的な諸性質は、だいたい明らかになったものと考えられる。

[2] Z_qの上のLFSRの諸性質

図1に Z_q $(q=p^m)$ の上のLFSR（以後LFSR(Z_q)と略す。）を示す。LFSR(Z_q)としては他のタイプも考えられるが、結局のところ図1のタイプに話は還元できるので、本稿では、図1のタイプに限って話を進める。

定義1　図1において、特性多項式$f(x)$並びに縮約特性多

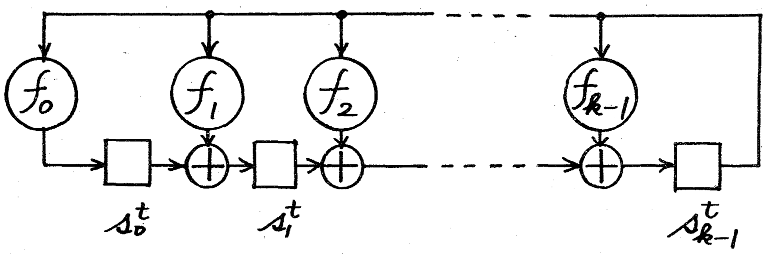
項式 $rf(x)$ を次のように定義する。

$$f(x)=x^k-f_{k-1}x^{k-1}-\cdots\cdots-f_1x-f_0 \qquad (1)$$

$$rf(x)=x^k-rf_{k-1}x^{k-1}-\cdots\cdots-rf_1x-rf_0 \qquad (2)$$

但し，$rf_i\equiv f_i \pmod{r=p^l\ (1\leqq l\leqq m)}$ (3)

であって，$0\leqq rf_i<r\quad(i=0,1,\cdots,k-1)$ (4)



$f_i,\ s_i^t\in Z_q\quad(i=0,1,\cdots,k-1)$

□ ： q 値レジスタ（遅延素子）

(f_i) ： f_i 倍の乗算器 $(\bmod q)$; ⊕ ：加算器 $(\bmod q)$

$S^t=\{s_0^t,s_1^t,\cdots,s_{k-1}^t\}$ ：時刻 t での状態ベクトル

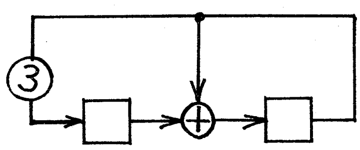
図 1　Z_q の上の LFSR

(2-1)　状態ベクトル(列)の分類

定義 2　LFSR (Z_q) の状態ベクトル $S^t=\{s_0^t,s_1^t,\cdots,s_{k-1}^t\}$ が，レベル j $(0\leqq j\leqq m-1)$ にあるとは，次の事をいう。即ち、任意の i $(0\leqq i\leqq k-1)$ に対し s_i^t が p^j で割り切れ，かつ少なくとも一つの i に対し s_i^t が p^{j+1} で割り切れない事である。また便宜上，零ベクトルはレベル m にあると定義する。

例 1　図 2 において、集合 A_j に属する状態ベクトルは、すべ

て、レベル j にある。なお $q=4=2^2$ より $m=2$ である。



A_2:

	1	x
s^0	(0, 0)	

A_1:

	1	x
s^0	(2, 0)	
s^1	(0, 2)	
s^2	(2, 2)	

A_0:

	1 x	1 x
s^0	(1, 0)	(1, 2)
s^1	(0, 1)	(2, 3)
s^2	(3, 1)	(1, 1)
s^3	(3, 0)	(3, 2)
s^4	(0, 3)	(2, 1)
s^5	(1, 3)	(3, 3)

図2. Z_4 の上のLFSRと状態ベクトル列の一例

次に、状態ベクトル列 $\{s^t\}$ もレベルという概念で分類する。そのために、まず次の性質1および性質2を導いておこう。

性質1　LFSR(Z_q)の任意の状態ベクトル列 $\{s^t\}$ が周期系列となるための条件は、$pf_0 \neq 0$ が成立することである。

(略証)　状態ベクトルの数が有限であること、および $s^t = s^{t-1}\cdot T$ (Tは Z_q 上のある行列)と表わせることから、求むる条件は、行列式 $|T| = f_0$ が零因子とならないことである。(3)

性質2　LFSR(Z_q)において、$pf_0 \neq 0$ が成立するならば、各状態ベクトル列 $\{s^t\}$ は、それぞれ、同一のレベルにある状態ベクトルから成る。

(略証)　s^t がレベル j にあるとし、その要素 a^t_{k-1} が p^j で割り切れる場合と、そうでない場合とに分けて考え、$pf_0 \neq 0$ の条件をあとの場合について用いれば、s^t と s^{t+1} とが同一のレベルにあることは容易に導ける。(3)

以後特に断わらない限り，${}_p f_0 \neq 0$ とする。

定義3　状態ベクトル列 $\{S^t\}$ がレベル j にあるとは，$\{S^t\}$ に属する任意の状態ベクトルが，レベル j にあることをいう。

次に，LFSR (Z_q) と LFSR (Z_r) （但し，$q=p^m$, $r=p^{m-i}$）との関係について触れておこう。証明は明らかなので略す。

性質3　LFSR (Z_q) $(q=p^m)$ の状態ベクトル列 $\{S^t\}$ が，レベル j $(i \leqq j \leqq m)$ にあるならば，系列 $\{p^{-i}S^t\}$ は，${}_r f(x)$ $(r=p^{m-i})$ を特性多項式とする LFSR (Z_r) のレベル $(j-i)$ にある系列である。また，その逆も成り立つ。

(2-2) 状態ベクトル列（または特性多項式）の周期

本節以降では，簡明な話とするために，LFSR (Z_q) の縮約特性多項式 ${}_p f(x)$ は，Z_p つまり $GF(p)$ の上の既約多項式であるものとする。他の場合についても本節の結果をもとに議論できるが，ここでは省略する。

なお，${}_p f(x)$ の（最小）周期を $M({}_p f)$ とする。$M({}_p f)$ の値が，p^k-1 またはその約数に等しいことは，よく知られている。[1]

性質4　LFSR (Z_q) において，2つの相異なる状態ベクトル列が同一のレベルにあるならば，両系列は同一の周期を持つ。但し，逆は一般には成立しない。

（略証）両系列を $\{U^t\}$, $\{S^t\}$ とし，$U^0=(1,0,\cdots,0)$, $S^0=(s_0^0, s_1^0, \cdots, s_{k-1}^0)$ で，S^0 はレベル0にある任意の状態ベクトルとしても一般性

は失なわれない(性質3参照)。次に(3),(4)式の場合と同様の意味で、記号 ${}_rU^t, {}_rS^t, {}_rs_i^t$ を定義し(省略), 証明は帰納法を用いて行なう。まず系列 $\{{}_pU^t\}, \{{}_pS^t\}$ の周期が共に $M({}_pf)$ に等しいことは明らか。次に系列 $\{{}_{p^\ell}U^t\}, \{{}_{p^\ell}S^t\}$ の周期が相等しいものとし,その周期を N_ℓ とする。このとき

$$\begin{cases} {}_{p^{\ell+1}}U^{N_\ell} = (1,0,\cdots,0) + (\eta_0^0, \eta_1^0, \cdots, \eta_{k-1}^0) \quad , \quad \eta_i \in \{0, p^\ell\} & (5) \\ {}_{p^{\ell+1}}S^{N_\ell} = ({}_{p^{\ell+1}}s_0^0, {}_{p^{\ell+1}}s_1^0, \cdots, {}_{p^{\ell+1}}s_{k-1}^0) + \sum_{i=0}^{k-1} {}_ps_i^0 \eta^i & (6) \end{cases}$$

(但し, $\{\eta^i\}$ は $\eta^0 = (\eta_0^0, \eta_1^0, \cdots, \eta_{k-1}^0)$ を初期状態とする系列)

と表わせることは容易に導ける。但し, $1 \leqq \ell \leqq m-1$ である。

(5),(6)式より, $\eta^0 = \mathbf{0}$ ならば, 系列 $\{{}_{p^{\ell+1}}U^t\}, \{{}_{p^{\ell+1}}S^t\}$ の周期は共に N_ℓ に等しい。また $\eta^0 \neq \mathbf{0}$ ならば, ${}_ps_i^0$ の中の少なくとも一つが p で割り切れないことおよび ${}_pf(x)$ が Z_p 上の既約多項式であることから $\sum_{i=0}^{k-1} {}_ps_i^0 \eta^i$ が零ベクトルになり得ないことが導ける。これより、系列 $\{{}_{p^{\ell+1}}S^t\}$ の周期は,系列 $\{{}_{p^{\ell+1}}U^t\}$ と同じく $p{\cdot}N_\ell$ に等しいことが導ける。以上により、同一レベルにある2つの系列の周期は相等しい。

なお, 逆が成立しないことは、例えば図2の LFSR を Z_8 上の LFSR とみなし, その状態ベクトル列を調べると分る。(3)

次に、状態ベクトル列の各レベルに応じた周期を定義する。

<u>定義4</u> Z_g の上の多項式 $f(x)$ を特性多項式とする $LFSR(Z_g)$ において, レベル j にある状態ベクトル列 $\{S^t\}$ の(最小)周期

を、LFSR(Z_q) の j レベル(最小)周期と定義し，$N(j\,;{}_qf)$ あるいは略して単に $N(j)$ で表わす。

|
|---|
| <u>性質5</u>　$N(j\,;{}_qf)$ は，Z_q 上の多項式 $f(x)$ で割り切れる多項式 $p^j(x^i-1)$ の次数 $i\ (\geqq 1)$ の中で最小のものに等しい。 |

(略証)　$x^i\ (\mathrm{mod}\ f(x))$ と状態ベクトル S^i とを対応させれば明らか。

<u>定義5</u>　$N(j\,;{}_qf)$ を Z_q 上の多項式 $f(x)$ の j レベル周期とも呼ぶ。

j レベル周期 $N(j\,;{}_qf)$ は、更に次の様に表わせる。

|
|---|
| <u>性質6</u>　$\begin{cases} N(j\,;{}_qf) = p^{C(j\,;{}_qf)}\cdot M({}_pf) & (0 \leqq j \leqq m-1) \quad (7) \\ N(j\,;{}_qf) = 1 & (j = m) \quad (8) \end{cases}$
但し，$C(j\,;{}_qf)$ は，$j,\ q(=p^m)$ 及び $f(x)$ に依存して定まる、ある整定数で，かつ　$0 \leqq C(j\,;{}_qf) \leqq m-j-1$　(9) |

(略証)　(5)式より，系列 $\{{}_{p^{\ell+1}}U^t\}$ の周期が N_ℓ 又は $p\cdot N_\ell$ となることが導けるので性質6は明らか。

<u>例2</u>　Z_8 上の多項式 $f(x) = x^2 - x - 3$ に対しては，$M({}_2f) = 3$，$N(0) = 6$，$N(1) = 6$，$N(2) = 3$，$N(3) = 1$ である。

<u>定義6</u>　j レベル周期 $N(j\,;{}_qf)$ が、任意の $j\ (0 \leqq j \leqq m-1)$ の値に対し次式で与えられる時，$Z_q\ (q = p^m)$ の上の多項式 $f(x)$ は、<u>最大のレベル周期</u>をもつと定義する。

$$N(j\,;{}_qf) = p^{m-j-1} M({}_pf) \qquad (10)$$

さて，例2で示した様に，Z_8 上の多項式 $f(x) = x^2 - x - 3$ は，最大のレベル周期を持たない。しかし，$f(x)$ を Z_4 上の多項

式とみなせば，Z_4 上の多項式 $f(x)$ は，最大のレベル周期をもつ。このことを更に一般的な形でまとめたのが，次の性質7である。

> 性質7　(イ) p を奇素数とした時，Z_{p^2} 上の多項式 $f(x)$ が，最大のレベル周期をもつならば，任意の自然数 i に対し，Z_{p^i} の上の多項式とみなした $f(x)$ もまた最大のレベル周期をもつ。
>
> (ロ) Z_{2^3} の上の多項式 $f(x)$ が最大のレベル周期をもつならば，任意の自然数 i に対し，Z_{2^i} の上の多項式とみなした $f(x)$ もまた，最大のレベル周期をもつ。
>
> (ハ) Z_{2^3} の上の多項式 $f(x)$ が，最大のレベル周期をもつための必要十分条件は，$x^{M(2f)} \not\equiv \pm 1 \pmod{{}_4 f(x)}$　(11)
> が成立することである。

(略証) (イ) 性質4の略証で用いた記号を使う。条件より，$N_2 = pN_1$ であるから，性質3，4および5より，$N_{\ell+1} \neq N_\ell$（つまり，$N_{\ell+1} = pN_\ell$）と仮定した時，$N_{\ell+2} \neq N_{\ell+1}$（つまり，$N_{\ell+2} = pN_{\ell+1}$）となる事を，系列 $\{U^t\}$ について示せば十分。その為には，まず，

$$\begin{cases} p^{\ell+2}U^{N_\ell} = (1, 0, \cdots, 0) + \xi^0 & (12) \\ p^{\ell+2}U^{N_{\ell+1}} = (1, 0, \cdots, 0) + p\xi^0 + \frac{p(p-1)}{2}\tilde{\xi} & (13) \end{cases}$$

但し，ξ^0 はレベル ℓ に，$\tilde{\xi}$ はレベル $(\ell+1)$ 又はレベル $(\ell+2)$ にある状態ベクトルで，$\xi^{N_\ell} = \xi^0 + \tilde{\xi}$　(14)

を導き，ついで　$p\xi^0 + \frac{p(p-1)}{2}\tilde{\xi} \neq 0$　(15)

を示せばよい。(15)式は，p が奇素数であること，および ξ^0 が

レベルℓにあることから容易に導ける。

(ロ) 条件より、$p=2$で, $N_3=2N_2=4N_1$である。これより$\tilde{\xi}=\mathbf{0}$が導け，(15)式が成立する。

(ハ) (15)式の条件、つまり$2\xi^0+\tilde{\xi}\neq\mathbf{0}$は，$\ell=1$のとき(11)式の条件と等価であることは，容易に導ける。(11)式が成立すれば，$\ell\geqq 2$のとき，$2\xi^0+\tilde{\xi}=2\xi^0\neq\mathbf{0}$となる。(3)

さて，次に問題となるのは、最大のレベル周期をもつ多項式を直接得るにはどうしたらいいかという問題である。この問に対しては，次の仮説1が役立つ。

<u>仮説1</u>　Z_qの上の2次以上の多項式$f(x)$に対し，$f(x)={}_{p}{}^{f(x)}$が成立するならば，$f(x)$は最大のレベル周期をもつ

仮説1は，Z_p上の既約多項式表がいくつかの文献[2],[5]で知られていることから重要な仮説ではあるが、筆者自身，未だ完全な証明には至っていない。ただ筆者は，$p=2$の場合につき、16次までのすべての既約多項式$f(x)$に対し、仮説1が成立することを、性質7の(ハ)を用いて検証済である。また，17次以上の既約多項式についても未だ反例となるものには出会っていない。この最大のレベル周期をもつ多項式は，誤り訂正符号への応用にとって重要である。

なお，万一仮説1が成立しなくても，次の性質8を用いれば，任意の次数について、最大のレベル周期をもつ多項式を

割合簡単に求めることができる。証明は $f(x)$ の相反多項式に着目して導けるが、スペースの都合上ここでは省略する。

<u>性質8</u>　Z_q $(q=p^m)$ の上の多項式 $f(x)$ は最大のレベル周期を持たないものとする。このとき、ある適当な係数 f_i $(0 \leqq i \leqq k-1)$ を $f_i+p \pmod q$ に変更することによって，新しい Z_q 上の多項式 $f(x)$ が最大のレベル周期を持つようにすることができる。

(2-3)　状態ベクトル列の総数

状態ベクトルの総数を各レベルについて求め、それを各レベル周期で割り，更にその総和を求めれば，次の性質9が導かれる。

<u>性質9</u>　Z_q $(q=p^m)$ の上の k 次の多項式 $f(x)$ が、最大のレベル周期をもつ時，レベル j にあって相異なる状態ベクトル列の総数 $V(j)$ および，すべての相異なる状態ベクトル列の総数 W は、次式で与えられる。但し，$0 \leqq j \leqq m-1$，$k \geqq 2$.

$$\begin{cases} V(j)=p^{(m-j-1)(k-1)}\cdot(p^k-1)/M(pf) & (16) \\ W=\{(p^{m(k-1)}-1)/(p^{k-1}-1)\}\cdot\{(p^k-1)/M(pf)\}+1 & (17) \end{cases}$$

なお，ここでは，互いにシフトした関係にある状態ベクトル列は，同一の系列とみなして数え上げてある。

(2-4) 状態ベクトル列間の関係

応用上有用と思われる，いくつかの状態ベクトル列間の関係を，次の性質10にまとめる。証明はスペースの都合上略す。

<u>性質10</u> (イ) LFSR(Z_{2^m})の特性多項式$f(x)$が最大のレベル周期をもつならば，レベルが$(m-2)$以下にある状態ベクトル列$\{S^t\}$と$\{-S^t\}$とは相異なる系列で，単にシフトした関係にはない。

(ロ) LFSR(Z_{p^m}) $(p\neq 2)$の縮約特性多項式${}_pf(x)$が，Z_pつまり$GF(p)$上の原始多項式であるならば，状態ベクトル列$\{S^t\}$と$\{-S^t\}$とは単にシフトした関係にある同一の系列である。

(ハ) LFSR(Z_q)の特性多項式$f(x)$は最大のレベル周期をもつものとする。このとき，レベルが$(m-2)$以下の状態ベクトル列$\{S^t\}=\{(s_0^t, s_1^t, \cdots, s_{k-1}^t)\}$に対し，間隔$u$でサンプリングして得られる系列$\{\tilde{s}_i^t\}\triangleq\{s_i^{ut}\}$は，間隔$u$をどのように選んでも，系列$\{s_i^t\}$とは相異なる系列で，単にシフトしたり，あるいは，定数$(\in Z_q)$倍した関係にある系列ではない。

(2-5) 状態ベクトル間の関係、構造

<u>定義7</u> LFSR(Z_q)においてjレベルにある状態ベクトル$S=(s_0, s_1, \cdots, s_{k-1})$に対し，多項式$S(x)=\sum_{i=0}^{k-1} s_i x^i$を対応づけ，$S(x)$をそのLFSR($Z_q$)の<u>$j$レベルにある状態多項式</u>と呼ぶ。

次に，状態多項式間の演算を導入し，状態ベクトルの集合のもつ構造について記す。証明は容易に導けるので略す。

<u>性質11</u> (イ) $f(x)$を特性多項式とするLFSR(Z_q)において，$S_i(x)$ $(i=1,2,\cdots,u)$をレベルj_iにあるZ_q $(q=p^m)$の上の状態多項式とする。このとき$\prod_{i=1}^{u} S_i(x)\equiv 0 \pmod{f(x)}$が成立するの

は，$\sum_{i=1}^{u} j_i \geq m$ のとき，その時に限る。また $\sum_{i=1}^{u} j_i < m$ ならば，$\sum_{i=1}^{u} j_i$ は，状態多項式 $\prod_{i=1}^{u} S_i(x) \pmod{f(x)}$ のレベルに等しい。

(ロ) $LFSR(Z_q)$ において，A_j をレベル j にある状態多項式 $S_i(x)$（これは，$p^j \widetilde{S_i}(x)$ と表わせる）の全集合とする。このとき，$\widetilde{A_j} = \{\widetilde{S_i}(x)\}$ は，$p^{m-j} f(x)$ を特性多項式とする $LFSR(Z_{p^{m-j}})$ のレベル 0 の状態多項式の全集合に等しい．また $\widetilde{A_j}$ は，mod $p^{m-j} f(x)$ の演算のもとに可換な乗法群を構成する。

(ハ) 状態ベクトル列 $\{S^t\}$ はレベル j にあるとする．この時，

$$\sum_{t=0}^{N(j;q,f)-1} S^t(x) \equiv 0 \pmod{f(x)} \tag{18}$$

〔3〕 あとがき

Z_q の上の $LFSR$ のもつ基本的な諸性質を明らかにし，あわせて未解決な一命題をも提示した。後半はスペースの都合上説明不足となったが、性質 10 および 11 とも，誤り訂正符号への応用上重要な性質である。更に詳しい解析・応用等については別途報告したい。本稿で得られた結果は、他のディジタル通信技術や計算機技術へも応用されることが期待される．

末筆ながら，日頃御指導・御討論頂く関係各位に深謝する次第である。

文献

[1] S. W. Golomb : 'Shift Register Sequences' (Holden Day Inc., San Francisco, 1967), Part I, II, pp. 1–108

[2] W. W. Peterson and E. J. Weldon : 'Error Correcting Codes', 2nd Edition (The M.I.T. Press, Cambridge, Mass., 1972), chap. 7 pp. 170–205

[3] N. Zierler : "Linear Recurring Sequences", SIAM Journal, Vol. 7, Mar. 1959, pp. 31–48

[4] W. H. Kautz (ed.) : 'Linear Sequential Switching Circuits', [Holden-Day, San Francisco, 1965] pp. 1–234

[5] 宮川 他 : '符号理論' (昭晃堂, 1973), pp. 112–137, pp. 527–567

[6] G. ホフマン・ド・ヴィスメ (伊理正夫・由美 訳) : '2値系列' (共立出版, 1977) pp. 1–168.

[7] 佐藤, 中村 : '擬似ランダム系列(4), (5)', **bit** (共立出版) 1975, 2月号, 3月号.

[8] I. F. Blake : "Codes over Integer Residue Rings", Inf. and Control, 1975, 29, pp. 295–300

[9] 中村 : "差動符号化を併用する誤り訂正符号の一構成法", 電子通信学会部門別全国大会, No. 13, 1976, 9月.

[10] 中村 : "差動符号化に適した誤り訂正符号の一理論", 電子通信学会総合全国大会, No. S9-5, 1977, 3月.

付　記

研究集会終了後、相模工業大学の坂田省二郎先生より、以下の貴重な文献を紹介して頂いた。この文面を借り、深く感謝致します。

[11] M. Magidin and A. Gill, "Singular shift registers over residue class rings," Mathematical Systems Theory, Vol. 9, No. 4, 1976

[12] M. Hall, "An isomorphism between linear recurring sequences and algebraic rings," Trans. Amer. Math. Soc., vol. 40 (1938) pp. 196−218.

本稿との関連について述べれば、文献[11]は、性質1で述べた条件 $pf_0 \neq 0$ が成立しない場合について、過渡的な状態ベクトル列の性質を詳しく調べている。これは本稿の対象外としたことである。

文献[12]は、種々の言いまわしの違いや、再帰系列に対応するLFSRの違いはあるものの、基本的に本稿で述べた結果を含むものが幾つかある。これは筆者の勉強不足に帰する。

まず、文献[12]では、特性多項式 $f(x)$ を、本稿の場合より広い形で、$f(x) = (h(x))^e$ （$h(x)$ は GF(p) 上で既約）とし、その周期パターンをⅢ節において調べている。そして、その過程において導かれた Theorem 4.2 は、基本的に本稿の性質6

を含み，またTheorem 4.3 も性質7の(イ)および(ロ)をその特別な場合として含む。

しかしながら，本稿では特に $e=1$ としたために導かれた性質4とか性質8以降の性質などに，文献12は注意を向けておらず，また最大のレベル周期に関連した特別の話もない。

その代り，文献12では，初期状態に依存した周期のありようを，グラフのある領域内で表現することに成功している。

なお文献12では，Ⅱ節において，再帰系列と多項式環との対応づけをⅣ節では，numeric という概念と零系列との関係を（numeric とは，系列 $\{u_n\}$ に対し，$u_{n+\tau}\equiv u_n \pmod m$ $n\geqq n(m)$ を満たす最小数 $n(m)$ のことである。但し τ は，この系列の周期である。），Ⅴ節では，系列内の各 integer の分布に関する問題を取り扱っている。

いずれにしろ，文献12は，一つの古典ともなるべき貴重な文献であり，筆者は，この文献を媒介として更に検討を続ける予定である。

なお，本稿の結果を利用した誤り訂正符号の構成法については，下記に発表する予定である。

[13] 中村，"Z_{2^m} の上のリー誤り訂正符号の一クラスについて"，電子通信学会オートマトンと言語研究会，1977，11月（予定）