研究速報

## 2種類のLFSRの等価性と初期値変換

藤田　悠[†a)]（学生員）　杉村　立夫[†]（正員）
柴田　孝基[††]（正員）

Equivalence and Initial Value Transform between Two Types of LFSR

Yutaka FUJITA[†a)], *Student Member*, Tatsuo SUGIMURA[†], and Koki SHIBATA[††], *Members*

[†] 信州大学工学部電気電子工学科，長野市
Department of Electrical and Electronic Engineering, Faculty of Engineering, Shinshu University, 4-17-1 Wakasato, Nagano-shi, 380-8553 Japan
[††] 日本無線株式会社研究開発部モバイル研究グループ，三鷹市
Japan Radio Co., Ltd., 1-1 Shimorenjaku, 5 Chome, Mitaka-shi, 181-8510 Japan
a) E-mail: fujita@sugi.shinshu-u.ac.jp

**あらまし**　本論文では，単純型LFSRとモジュラー型LFSRの等価性を示し，同じ出力を発生するための初期値を導出する相互の初期値変換を与える．

**キーワード**　単純型LFSR，モジュラー型LFSR，初期値変換，母関数

### 1. まえがき

従来より，線形再帰関係は巡回符号を考える上で重要な役割を果たしている．単純型リニアフィードバックシフトレジスタ（Linear Feedback Shift Register：LFSR）[1],[5]は，線形再帰関係を具体的に表現するものである．Berlekamp-Massey法[2]～[4]による復号法の方針が単純型LFSRのタップ多項式導出であることは，線形再帰関係と単純型LFSRの復号における関連性を如実に表しているといえる．

一方，モジュラー型LFSRの出力や，単純型LFSRとモジュラー型LFSRの間に存在する関係[6]などは明確になっているとは言いがたい．

本論文では，単純型LFSRとモジュラー型LFSRが同じ系列を発生できることを示す．同じ系列を発生させる初期値は互いに変換可能であることを明確にし，初期値変換として与えるとともに代数的復号におけるKey Equation [2]との関係を指摘する．

### 2. 2種類のLFSR

本章では，同じ系列を出力する2種類のLFSRを定義するとともに，母関数との関係を明確にする．

#### 2.1 準　　備

$q$ を素数または素数のべき乗とする．ある正整数 $m$ に対して，$GF(q^m)$ の要素の半無限系列 $A_0, A_1, A_2, \cdots$ は次の正規べき級数

$$A(Z) = \sum_{i=0}^{\infty} A_i Z^i \tag{1}$$

で表現でき，これを母関数と呼ぶ．この系列が周期 $n$ をもつとき，最初の1周期分を母関数

$$F(Z) = \sum_{i=0}^{n-1} A_i Z^i \tag{2}$$

で表現すると，$A(Z)$ は有理型母関数として

$$A(Z) = \frac{F(Z)}{1 - Z^n} \tag{3}$$

と表される．

本論文で検討する2種類のLFSRは，ともに $l$ 個のレジスタをもつ長さ $l$ のLFSRとし，結線（タップ）の値を係数とするタップ多項式

$$T(Z) = 1 + T_1 Z^1 + T_2 Z^2 + \cdots + T_l Z^l \tag{4}$$

をもつ．ただし $T_i \in GF(q^m)(1 \le i \le l)$，$T_l \neq 0$ とする．タップ多項式 $T(Z)$ の0次係数が非ゼロであるため，$T(Z)$ は有限な値の指数 $n$ をもつ，すなわち $T(Z) \mid (1 - Z^n)$ である．

有限な値の指数 $n$ をもつ多項式 $T(Z)$ に対して

$$T_c(Z) = \frac{1 - Z^n}{T(Z)} \tag{5}$$

で定められる $n - l$ 次多項式 $T_c(Z)$ を $T(Z)$ の相補多項式と呼ぶことにする．

#### 2.2 単純型LFSR

線形再帰関係が忠実に関連づけられているレジスタ回路として，単純型LFSRを定義する．

[定義1]（単純型LFSR）　出力側に高次係数がくるようにタップ多項式 $T(Z)$ の係数を配置し，出力側を低次係数とした初期値多項式を

$$U(Z) = U_0 + U_1 Z^1 + U_2 Z^2 + \cdots + U_{l-1} Z^{l-1} \tag{6}$$

としたとき，図1のレジスタ回路を単純型LFSRと呼ぶことにする．ただし $U_i \in GF(q^m)(0 \le i \le l-1)$ とする．□

$i$ 回シフト時の出力を $O_i^{(s)} \in GF(q^m)$ としたとき，単純型LFSRの出力は式(7)，式(8)で表される．

$$O_i^{(s)} = U_i (0 \le i \le l-1) \tag{7}$$

$$O_i^{(s)} = -\sum_{j=1}^{l} T_j O_{i-j}^{(s)} (l \le i) \tag{8}$$

単純型 LFSR は，線形再帰関係式（式 (8)）を具体的に表現するものであり，出力 $O_i^{(s)}(0 \leq i)$ は周期 $n$ をもつ [1].

単純型 LFSR の出力の 1 周期分を多項式表現したものは，タップ多項式が割り切る $1-Z^n$ を法とする多項式剰余類環における，タップ多項式の相補多項式により生成されるイデアルであることは，Peterson（[1], Theorem 7.1）により示されているが，本論文における単純型シフトレジスタとは，タップ係数の置き方が異なる．すなわち，Peterson（[1], Figure 7.14）によるタップと本論文における図 1 によるタップは互いに相反な関係にある．しかし，タップ多項式の相反多項式をタップとしたとき，その出力はタップ多項式の相反多項式の相補多項式のイデアルである．したがって，本論文の定義による単純型 LFSR はタップ多項式 $T(Z)$ の相補多項式 $T_c(Z)$ のイデアルを出力することが分かる．

また，単純型 LFSR の出力の多項式表現は，出力される値を昇順に位づけした出力多項式

$$O^{(s)}(Z) = O_0^{(s)} + O_1^{(s)} Z^1 + \cdots + O_{n-1}^{(s)} Z^{n-1} \quad (9)$$

を 1 周期分とする無限大次数まで周期を繰り返す母関数によって表される．また，単純型 LFSR の初期値多項式と出力多項式の間には，式 (10) の合同関係が成立する．

$$U(Z) \equiv O^{(s)}(Z) \bmod Z^l \quad (10)$$

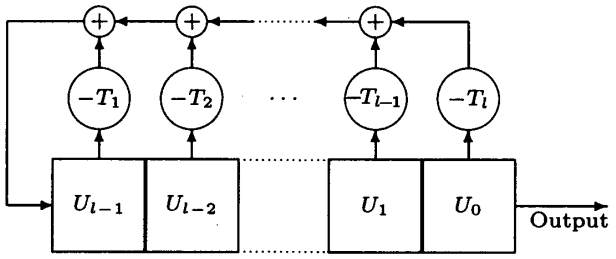


図 1 単純型 LFSR の初期状態
Fig. 1 Initial state of simple type LFSR.

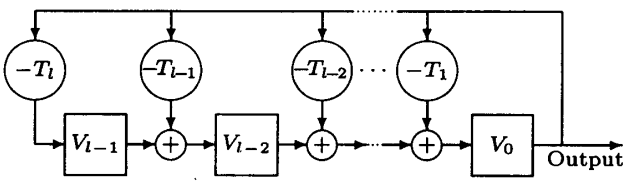


図 2 モジュラー型 LFSR の初期状態
Fig. 2 Initial state of modular type LFSR.

### 2.3 モジュラー型 LFSR

有限体上の多項式による割算器として知られる回路により構成される，モジュラー型 LFSR を定義する．

[定義 2]（モジュラー型 LFSR） 出力側に低次係数がくるようにタップ多項式 $T(Z)$ の係数を配置し，出力側を低次係数とした初期値多項式を

$$V(Z) = V_0 + V_1 Z^1 + V_2 Z^2 + \cdots + V_{l-1} Z^{l-1} \quad (11)$$

としたとき，図 2 のレジスタ回路をモジュラー型 LFSR と呼ぶことにする．ただし $V_i \in GF(q^m)(0 \leq i \leq l-1)$ とする． □

$i$ 回シフト時の出力を $O_i^{(m)} \in GF(q^m)$ としたとき，モジュラー型 LFSR の出力は式 (12)，式 (13) で表される．

$$O_i^{(m)} = V_i - \sum_{j=1}^{i} T_j O_{i-j}^{(m)} \ (0 \leq i \leq l-1) \quad (12)$$

$$O_i^{(m)} = -\sum_{j=1}^{l} T_j O_{i-j}^{(m)} \ (l \leq i) \quad (13)$$

式 (13) は単純型 LFSR の線形再帰関係式（式 (8)）と同じ線形再帰関係であり，出力 $O_i^{(m)}(0 \leq i)$ は周期 $n$ をもつ．

また，モジュラー型 LFSR の出力の多項式表現は，出力される値を昇順に位づけした出力多項式

$$O^{(m)}(Z) = O_0^{(m)} + O_1^{(m)} Z^1 + \cdots + O_{n-1}^{(m)} Z^{n-1} \quad (14)$$

を 1 周期分とする無限大次数まで周期を繰り返す母関数によって表される．

モジュラー型 LFSR の出力系列は有理型母関数を用いて補題 1 により与えられる．

[補題 1]（モジュラー型 LFSR の出力多項式） $T(Z)$ をタップ多項式，$V(Z)$ を初期値多項式とするモジュラー型 LFSR の出力多項式は

$$O^{(m)}(Z) = V(Z) T_c(Z) \quad (15)$$

により与えられる． □

（証明） 付録に掲載． □

補題 1 により以下の系 1 が得られる．

[系 1] モジュラー型 LFSR のタップ多項式 $T(Z)$，初期値多項式 $V(Z)$ 及び出力多項式 $O^{(m)}$ には，

$$\frac{V(Z)}{T(Z)} = \frac{O^{(m)}(Z)}{1-Z^n} \quad (16)$$

なる関係が成立する．ただし $\deg V(Z) < \deg T(Z)$ である． □

本論文で定義したようにモジュラー型 LFSR のタップを置くことによって，モジュラー型 LFSR が出力する半無限周期系列を，有理型母関数を用いた簡潔な表現で表すことが可能になる．

## 3. LFSR の初期値変換

単純型 LFSR とモジュラー型 LFSR は $1-Z^n$ を法とした多項式剰余類環における，タップ多項式の相補多項式 $T_c(Z)$ のイデアルを出力する．このとき，イデアルの位数は $(q^m)^l$ であり，初期値多項式（$U(Z)$ 及び $V(Z)$）の次元と一致する．したがって，2 種類の LFSR はそれぞれの初期値に対応する系列を出力し，その 2 種類の LFSR が同じ出力系列を出力するときの初期値の間に相互関係が存在する．

単純型 LFSR とモジュラー型 LFSR における初期値変換を定理 1 に示す．

[定理 1]（初期値変換） 単純型 LFSR の初期値多項式を $U(Z)$，モジュラー型 LFSR の初期値多項式を $V(Z)$，2 種類の LFSR 共通のタップ多項式を $T(Z)$ とする．二つの LFSR が同じ系列を出力するとき，初期値の間に

$$U(Z) \equiv V(Z)T_c(Z) \bmod Z^l \tag{17}$$

$$V(Z) \equiv U(Z)T(Z) \bmod Z^l \tag{18}$$

なる関係が存在し，それぞれ，モジュラー型 LFSR から単純型 LFSR への初期値変換，単純型 LFSR からモジュラー型 LFSR への初期値変換を表す． □

（証明） 単純型 LFSR の出力多項式を $O^{(s)}(Z)$，モジュラー型 LFSR の出力多項式を $O^{(m)}(Z)$ とする．2 種類の LFSR が同じ系列を出力（$O^{(s)}(Z) = O^{(m)}(Z)$）するとき，式 (10) より，

$$U(Z) \equiv O^{(m)}(Z) \bmod Z^l \tag{19}$$

が成立する．式 (19) に対し，補題 1 より

$$U(Z) \equiv V(Z)T_c(Z) \bmod Z^l \tag{20}$$

が導出される．

一方，補題 1 より，2 種類の LFSR が同じ出力（$O^{(s)}(Z) = O^{(m)}(Z)$）をもつことから

$$\frac{O^{(s)}(Z)}{T_c(Z)} = V(Z) \tag{21}$$

が成り立つ．この両辺に $1-Z^n$ を乗じることで

$$T(Z)O^{(s)}(Z) = (1-Z^n)V(Z) \tag{22}$$

が得られ，$l$ 次以下における合同関係

$$T(Z)O^{(s)}(Z) \equiv V(Z) \bmod Z^l \tag{23}$$

も成立する．式 (23) に対し，式 (10) によって

$$V(Z) \equiv U(Z)T(Z) \bmod Z^l \tag{24}$$

が得られる． □

単純型 LFSR，モジュラー型 LFSR ともに線形再帰関係によって出力を表すことが可能であり，対応した初期値を与えることで同じ出力を発生することが可能であることを示した上で，相互の初期値変換を与えた．

## 4. 考　　察

**3.** での結果は代数的誤り訂正の復号における操作と強い関連性をもつ．BCH 限界により定められる誤り訂正可能個数を $t$，誤り発生個数を $l(\leq t)$ としたとき，タップ多項式を誤り位置多項式 $\Lambda(Z)$ とし，長さ $l$ の単純型 LFSR の初期値多項式を $S(Z) \bmod Z^l$ とする．そのとき，単純型 LFSR からモジュラー型 LFSR への初期値変換は

$$S(Z)\Lambda(Z) \bmod Z^l \tag{25}$$

であることが定理 1 の結果より分かる．式 (25) は誤り評価多項式 $\Omega(Z)$ を与える．したがって

$$\Omega(Z) \equiv S(Z)\Lambda(Z) \bmod Z^l \tag{26}$$

と書き表される．式 (26) は，従来より用いられている誤り評価多項式，シンドローム多項式，誤り位置多項式の間にある関係として用いられている Key Equation

$$\Omega(Z) \equiv S(Z)\Lambda(Z) \bmod Z^{2t} \tag{27}$$

と，剰余をとる次数のみ異なる．この違いは，Key Equation がシンドローム多項式全体を含む関係として与えられることに起因する．しかし，$\Omega(Z)$ は $l-1$ 次以下の多項式であり，式 (26)，式 (27) どちらも同じ誤り評価多項式を与えている．したがって，Key Equation は単純型 LFSR からモジュラー型 LFSR への初期値変換の意味合いを含んでいるといえる．

## 5. む　す　び

単純型 LFSR とモジュラー型 LFSR の結線の値，初期値と出力の関係を明確にした．同じ系列を発生するときの初期値の関係を明らかにし，初期値変換として与えた．本論文で与えた初期値変換が実際に活用されている一例として代数的誤り訂正の復号における関係を述べた．

## 文　献


[1] W.W. Peterson and E.J. Weldon, Jr., Error-Correcting Codes, Second Edition, The MIT Press, 1972.

[2] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, 1968.

[3] J.L. Massey, "Shift-register synthesis and BCH decoding," IEEE Trans. Inf. Theory, vol.IT-15, no.1, pp.122–127, Jan. 1969.

[4] R.E. Blahut, Theory and Practice of Error-Control Codes, Addison-Wesley, Reading, Massachusetts, 1983.

[5] 中村勝洋，三浦晋示，"シフトレジスタ系列に関する一考察，" 第 9 回情報理論とその応用シンポジウム予稿集，pp.199–201, Oct. 1986.

[6] 藤田　悠，杉村立夫，"母関数を用いた Forney アルゴリズムの一解釈，" 信学技報，IT-2001-18, 2001.


## 付　録

（証明）（補題 1）　$i$ 回シフト後のレジスタ内容を，出力側を低次とみなす多項式表現を用いて，

$$R^{[i]}(Z) = R_0^{[i]} + R_1^{[i]} Z^1 + \cdots + R_{l-1}^{[i]} Z^{l-1} \tag{A·1}$$

と表す．0 回シフト後のレジスタの状態は，初期値多項式に一致することから，$R^{[0]}(Z) = V(Z)$ である．

モジュラー型 LFSR のシフトに伴うレジスタ内容の変化と出力における関係は，多項式の除算と類似するが，タップ係数の並べ方の違いから，通常の除算操作とは異なった様相を呈する．

通常の多項式の除算は除多項式，被除多項式両者の最高次係数を基準とした商を導出し，余りの次数は降下していくものである．一方，モジュラー型 LFSR が示す変化は，除多項式，被除多項式両者の最低次係数を基準として商を導出し，余りの次数は上昇していく．前者の除算が高次係数を基準とした除算とするならば，後者の除算は低次係数を基準とした除算である．

タップ多項式 $T(Z)$ をもつモジュラー型 LFSR の $i$ 回目シフト時のレジスタ内容変化（$R^{[i-1]}(Z)$ と $R^{[i]}(Z)$）とそのときの出力（$O_{i-1}^{(m)}$）が発生することは，$i$ 回目の除算操作において除多項式を $T(Z)$，被除多項式を $R^{[i-1]}(Z)Z^{i-1}$ としたとき，商が $O_{i-1}^{(m)}Z^{i-1}$，剰余多項式が $R^{[i]}(Z)Z^i$ であることに対応している．

低次係数を基準とした除算操作は式 (A·2) で表される．

$$\begin{aligned}
R^{[0]}(Z) &= O_0^{(m)}\, Z^0\, T(Z) + R^{[1]}(Z)Z^1 \\
R^{[1]}(Z)Z^1 &= O_1^{(m)}\, Z^1\, T(Z) + R^{[2]}(Z)Z^2 \\
R^{[2]}(Z)Z^2 &= O_2^{(m)}\, Z^2\, T(Z) + R^{[3]}(Z)Z^3 \\
&\vdots \\
R^{[n-2]}(Z)Z^{n-2} &= O_{n-2}^{(m)} Z^{n-2} T(Z) + R^{[n-1]}(Z)Z^{n-1} \\
R^{[n-1]}(Z)Z^{n-1} &= O_{n-1}^{(m)} Z^{n-1} T(Z) + R^{[n]}(Z)Z^n
\end{aligned} \tag{A·2}$$

式 (A·2) のうち，連続した 2 回の操作の式に共通する $R^{[i]}(Z)Z^i$ を $1 \le i \le n-1$ において消去すると式 (A·3) にまとめることができる．

$$R^{[0]}(Z) = T(Z)\sum_{i=0}^{n-1} O_i^{(m)} Z^i + R^{[n]}(Z)Z^n \tag{A·3}$$

式 (A·3) の $\sum_{i=0}^{n-1} O_i^{(m)} Z^i$ は出力多項式 $O^{(m)}(Z)$ である．また，タップ多項式 $T(Z)$ が指数 $n$ をもつことから，$V(Z) = R^{[0]}(Z) = R^{[n]}(Z)$ である．したがって，式 (A·3) は

$$V(Z) = O^{(m)}(Z)T(Z) + Z^n V(Z) \tag{A·4}$$

とまとめられる．これより，

$$\frac{V(Z)}{T(Z)} = \frac{O^{(m)}(Z)}{1 - Z^n} \tag{A·5}$$

となる．ここで，出力系列の 1 周期である $O^{(m)}(Z)$ についてまとめると式 (A·6) になる．

$$O^{(m)}(Z) = V(Z)\frac{1 - Z^n}{T(Z)} \tag{A·6}$$

$T(Z)$ とその相補多項式 $T_c(Z)$ の関係を適用することで式 (A·7) が得られる．

$$O^{(m)}(Z) = V(Z)T_c(Z) \tag{A·7}$$

□

（平成 16 年 2 月 25 日受付，3 月 15 日最終原稿受付）