論　文

Matrix-reduction法を用いた受信シンドロームを生成するLFSRのタップ多項式導出法

藤田　悠[†a)]　杉村　立夫[†b)]　柴田　孝基[††c)]

A Deriving Method for Tap Polynomials of LFSR Generating Syndromes Using Matrix-Reduction Algorithm

Yutaka FUJITA[†a)], Tatsuo SUGIMURA[†b)], and Koki SHIBATA[††c)]

あらまし　代数的誤り訂正において，受信シンドローム多項式，誤り位置多項式，及び誤り評価多項式間の多項式の合同関係であるKey Equationを解き，受信シンドロームを生成する最短長のLFSRのタップ多項式として誤り位置多項式を導出する方法としてBerlekamp-Massey法が知られている．しかし，Berlekamp-Massey法は計算過程の複雑さからほとんど用いられていない．そこで，本論文ではMatrix-reduction法を用いた受信シンドロームを生成するLFSRのタップ多項式導出法を与える．Matrix-reduction法により得られたすべてのタップ多項式が誤り位置多項式を因数多項式としてもち，その因数多項式が誤り位置多項式として一意に得られることを明らかにする．また，Matrix-reduction法が誤り位置多項式導出法として処理時間において特に有利であることを示す．

キーワード　母関数，Matrix-reduction法，単純型Linear Feedback Shift-Register，Key Equation

1. まえがき

代数的誤り訂正に必要な値は，誤り位置と誤り値である．このうち，誤り位置を組織的に導出するために，誤り位置多項式なる概念がPeterson [1]によって導入され，Peterson法[1]によって誤り位置多項式を代数的に導出することが可能になった．しかし，Peterson法は，誤り個数を決定するために用いられる，行列の正則性を検査する作業に多くの手間を必要とするため，誤り訂正可能個数が大きい符号の誤り位置導出法として用いられることは少ない．一方，Berlekamp法[2]の一解釈であるBerlekamp-Massey [3], [5]法は，受信シンドロームを導出するLinear Feedback Shift-Register (LFSR)の最短のタップ係数を導出するための方法であるが，計算過程の複雑さなどの理由から，ほとんど用いられていない．しかし，Berlekamp-Massey法が与えた，受信シンドロームを生成するタップは，誤りシンドロームを生成可能なタップであり，誤りシンドローム多項式を逆フーリエ変換することで，誤り多項式そのものを直接得ることができる．誤りシンドローム多項式を逆フーリエ変換することによって誤り多項式を得る復号手法を用いるとき，個々の誤り位置と誤り値を導出する必要がなく，誤りシンドロームを発生するLFSRのタップが得られれば十分であり，最短長のタップ係数をもつ誤り位置多項式を導出する必要はない．

本論文では，$2t$個の連続する受信シンドロームからt個以下の誤りを訂正する代数的誤り訂正について考える．誤り発生個数が$w(\leq t)$のとき，Key Equation [2]は$2t$次未満の多項式の合同関係を示すものである．しかしながら，誤り評価多項式の次数がw次未満であることから，実際に合同をとる範囲は，w次未満であることに注目する．

誤り発生個数が不明のとき，誤り訂正可能個数t個

† 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
b) E-mail: tsugimu@gipwc.shinshu-u.ac.jp
c) E-mail: shibata@lab.jrc.co.jp

以下の誤りを訂正するために，t 次以下の誤り位置多項式の候補となる多項式を考える．このとき，誤り評価多項式は t 次未満であることから，Key Equation は t 次未満の多項式の合同関係と等価である．したがって，Key Equation により誤り評価多項式と合同となる，受信シンドローム多項式と誤り位置多項式の候補となる多項式の積は，t 次から $2t-1$ 次の係数がゼロでなければならない．このことから，t 個の連立方程式が与えられる．

本論文では，t 個の連立方程式は t 個の線形再帰関係に対応することから，誤り位置多項式の候補となる多項式を，レジスタ長を t とする単純型 LFSR のタップ多項式であるととらえ，与えられた t 個の連立方程式を Matrix-reduction 法によって解く．このとき，Matrix-reduction 法は，受信シンドロームを生成する長さ t 以下，w 以上のタップ長をもつ単純型 LFSR のタップをすべて導出することを示す．

また，これらすべてのタップ多項式が誤り位置多項式を因数多項式にもつことを示し，最短のタップ長 w をもつタップと，タップ長が t 以下 $w+1$ 以上となるタップを与える部分を区別した形で与えるために必要な，Matrix-reduction 法を施す行列に対する一定の規則を与える．

最後に，Matrix-reduction 法の演算は，行列の独立した列処理の繰返しであることから，並列処理が可能であることを示す．並列処理を行うことで処理時間の短縮が可能であることを従来法と比較し，その優位性を明確にする．また，従来法と比較して，Matrix-reduction 法の総計算量や装置量は多くなる傾向があるが，誤り訂正可能個数が比較的小さな範囲においては，総計算量，装置量ともに低く抑えられることも示す．

2. 基礎的準備

代数的誤り訂正で用いられる種々の多項式を定義し，線形再帰関係を扱う際に重要な役割を果たす単純型 LFSR を定義する．また，本論文では，符号語を時間領域にあるベクトルとし，誤り訂正を周波数領域における操作とする．それぞれの領域の多項式を不定元 x，Z を用いて表すこととし，時間領域，周波数領域の間の関係を表すフーリエ変換について，母関数を用いたフーリエ変換を示す．

2.1 巡回符号

q を素数または素数のべき乗とする．本論文で用いる符号を，その生成多項式が

$$\alpha^{m_0}, \alpha^{m_0+1}, \alpha^{m_0+2}, \cdots, \alpha^{m_0+2t-1}$$

の $2t$ 個の零点の連なりをもつ長さ n の $GF(q^m)$ の上の巡回符号とする．ただし，α は $GF(q^m)$ の位数 n の元である．本論文では，BCH 限界で定められる誤り訂正可能個数 t 個以下の誤りを訂正するものとする．

誤り個数が $w(\leq t)$ のとき，誤り多項式を

$$e(x) = e_{j_1}x^{j_1} + e_{j_2}x^{j_2} + \cdots + e_{j_w}x^{j_w} \qquad (1)$$

と表現する．ただし，$0 \leq j_i \leq n-1$，$e_{j_i} \in GF(q^m) - \{0\}$ $(i = 1, 2, \cdots, w)$，$j_i \neq j_k$ $(i \neq k)$ とする．

誤り多項式のフーリエ変換は

$$E(Z) = E_0 + E_1Z^1 + \cdots + E_{n-1}Z^{n-1} \qquad (2)$$

で表される．ただし，$E_i = e(\alpha^i)$，$e_i = \frac{1}{n}E(\alpha^{-i})$ $(0 \leq i \leq n-1)$ である．

受信語 $r(x)$ は，符号語を $c(x)$ としたとき

$$r(x) = c(x) + e(x) \qquad (3)$$

と表現できるため，受信語 $r(x)$ に連続する零点を代入すると符号語の項はゼロになり，誤り多項式の固有の値，受信シンドロームが導出される．これら受信シンドロームを係数にもつ多項式を受信シンドローム多項式と呼ぶことにし，次に定義する．

[定義 1] 受信語より得られる受信シンドローム $r(\alpha^{m_0+i}) = e(\alpha^{m_0+i}) = E_{m_0+i} = S_{m_0+i}$ $(i = 0, 1, \cdots, 2t-1)$ を係数にもつ多項式

$$S(Z) = S_{m_0} + S_{m_0+1}Z^1 + \cdots + S_{m_0+2t-1}Z^{2t-1} \qquad (4)$$

を受信シンドローム多項式と定義する． □

誤り位置を組織的に導出するために，式 (1) で表されている誤り位置 j_i と 1 対 1 対応させた誤りロケータ α^{j_i} を用いて，誤り位置多項式を定義する．

[定義 2] 誤り位置 j_i に 1 対 1 対応させた誤りロケータ α^{j_i} の逆元を零点にもつ多項式

$$\Lambda(Z) = \prod_{i=1}^{w}(1 - \alpha^{j_i}Z) = 1 + \Lambda_1Z^1 + \Lambda_2Z^2 + \cdots + \Lambda_wZ^w \qquad (5)$$

を誤り位置多項式と定義する． □

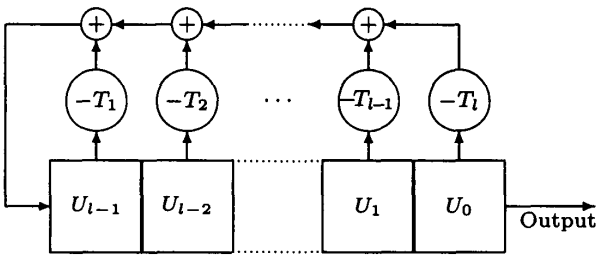

図 1 単純型 LFSR の初期状態
Fig. 1 Initial state of simple type LFSR.

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 3] タップ多項式を

$$T(Z) = 1 + T_1 Z^1 + T_2 Z^2 + \cdots + T_l Z^l \qquad (6)$$

として出力側に高次係数がくるように係数を配置し，出力側を低次係数とした初期値多項式を

$$U(Z) = U_0 + U_1 Z^1 + U_2 Z^2 + \cdots + U_{l-1} Z^{l-1} \qquad (7)$$

としたとき，図 1 のレジスタ回路を単純型 LFSR と呼ぶ．

ただし $U_i \in GF(q^m)$ $(0 \le i \le l-1)$, $T_i \in GF(q^m)$ $(1 \le i \le l)$ とする． □

レジスタの個数を LFSR の長さとし，レジスタ長と呼び，タップ多項式の次数をタップの長さとし，タップ長と呼ぶ．レジスタ長を l とし，タップ長を v としたときタップ長 v は $v \le l$ でなければならない．

i 回シフト時の出力を $O_i \in GF(q^m)$ としたとき，単純型 LFSR の出力は式 (8)，(9) で表される．

$$O_i = U_i \qquad (0 \le i \le l-1) \qquad (8)$$

$$O_i = -\sum_{j=1}^{l} T_j O_{i-j} \quad (l \le i) \qquad (9)$$

単純型 LFSR は，線形再帰関係式（式 (9)）を忠実に表すものであり，出力 O_i $(0 \le i)$ は $T(Z) \mid 1 - Z^L$ を満たす最小の正整数である指数 L の約数となる周期をもつ [1]．

2.3 母関数を用いたフーリエ変換・逆フーリエ変換

$GF(q^m)$ の要素 a_i $(0 \le i \le n-1)$ を係数にもつ多項式 $a(x) = \sum_{i=0}^{n-1} a_i x^i$ をフーリエ変換することによって得られる多項式 $A(Z) = \sum_{i=0}^{n-1} A_i Z^i$ は $A_i = a(\alpha^i)$ $(0 \le i \le n-1)$ となる係数をもつ．また，$A(Z)$ の逆フーリエ変換により $a(x)$ が得られ，$a_i = \frac{1}{n} A(\alpha^{-i})$ $(0 \le i \le n-1)$ なる関係をもつ．$a(x)$ のフーリエ変換 $A(Z)$ は半無限周期系列を係数にもつ母関数表現を用いることで

$$A(Z) = (1 - Z^n) \sum_{i=0}^{n-1} \frac{a_i}{1 - (\alpha^i) Z} \qquad (10)$$

と表すことができる．また，$A(Z)$ の逆変換 $a(x)$ は $A(Z)$ の係数 A_i $(0 \le i \le n-1)$ を用いて

$$a(x) = \frac{1}{n}(1 - x^n) \sum_{i=0}^{n-1} \frac{A_i}{1 - (\alpha^{-i}) x} \qquad (11)$$

と表すことができる [7]．

3. 母関数を用いた線形再帰関係の導出

3.1 Key Equation と誤り評価多項式

式 (1) で表現される誤り多項式のフーリエ変換は母関数を用いて

$$E(Z) = (1 - Z^n) \sum_{i=1}^{w} \frac{e_{j_i}}{1 - \alpha^{j_i} Z} \qquad (12)$$

と表されることから，$E(Z)$ の係数を低次方向に m_0 だけ巡回シフトした多項式は

$$[E(Z) Z^{n-m_0}]_n = (1 - Z^n) \sum_{i=1}^{w} \frac{e_{j_i} (\alpha^{j_i})^{m_0}}{1 - \alpha^{j_i} Z} \qquad (13)$$

と表される．ただし，$[f(y)]_n$ は，$f(y) \bmod (1 - y^n)$ を表すものとする．式 (13) は受信シンドロームを 0 次から $2t-1$ 次の係数にもち，誤り多項式をフーリエ変換したすべての係数を有していることから，誤りシンドローム多項式と呼び，誤りシンドローム多項式の係数が表す系列を誤りシンドロームと呼ぶ．

式 (13) の係数を周期的に繰り返す半無限周期系列を係数にもつ母関数は

$$\frac{[E(Z) Z^{n-m_0}]_n}{(1 - Z^n)} = \sum_{i=1}^{w} \frac{e_{j_i} (\alpha^{j_i})^{m_0}}{1 - \alpha^{j_i} Z} \qquad (14)$$

と表すことができる．ここで，式 (14) の母関数の 0 次から $2t-1$ 次までの部分は受信シンドローム多項式

$S(Z)$ に一致することから

$$\sum_{i=1}^{w} \frac{e_{j_i}(\alpha^{j_i})^{m_0}}{1-\alpha^{j_i}Z} \equiv S(Z) \bmod Z^{2t} \tag{15}$$

なる多項式の合同関係が得られる．この両辺に $\Lambda(Z)$ を乗じることにより得られる

$$\Omega(Z) \equiv S(Z)\Lambda(Z) \bmod Z^{2t} \tag{16}$$

は Key Equation として知られている [2]．ここで $\Omega(Z)$ は

$$\begin{aligned}\Omega(Z) &= \Lambda(Z)\sum_{i=1}^{w} \frac{e_{j_i}(\alpha^{j_i})^{m_0}}{1-\alpha^{j_i}Z} \\ &= \sum_{i=1}^{w} e_{j_i}(\alpha^{j_i})^{m_0} \prod_{\substack{k=1 \\ k\neq i}}^{w} (1-\alpha^{j_k}Z)\end{aligned} \tag{17}$$

で示される $w-1$ 次以下の多項式であり，誤り評価多項式と呼ばれる．

Key Equation と誤り評価多項式の関係から次の定理が与えられる．

[定理 1]　w 重誤りが発生したとき，受信シンドローム多項式と誤り位置多項式の積 $S(Z)\Lambda(Z)$ の w 次から $2t-1$ 次までの係数は 0 である．　□

(証明)　式 (16) の合同式において，誤り評価多項式 $\Omega(Z)$ が式 (17) で表されることから，$S(Z)\Lambda(Z)$ と誤り評価多項式 $\Omega(Z)$ が $2t$ 次未満で多項式の合同関係をもつためには $S(Z)\Lambda(Z)$ の w 次から $2t-1$ 次係数は 0 でなければならない．　□

定理 1 は，Key Equation が受信シンドローム多項式全体を包含する $2t$ 次未満の多項式の合同関係を示しているのに対し，w 次未満での多項式の合同関係

$$\Omega(Z) \equiv S(Z)\Lambda(Z) \bmod Z^{w} \tag{18}$$

と等価であることに起因しているが，式 (18) は，w 重誤り発生時の線形再帰関係を表す単純型 LFSR の初期値 $S(Z)$ から，単純型 LFSR と同じ出力を発生するモジュラー型 LFSR の初期値 $\Omega(Z)$ への初期値変換 [8] と等しい．したがって，定理 1 は，Key Equation（式 (16)）と，その中に含まれている初期値変換（式 (18)）の間にある関係を示しているという解釈もできる．

誤り発生個数 w が判明することで，$2t-w$ 個の Λ_i $(1 \le i \le w)$ に関する連立方程式が得られ，その連立方程式を解くことで誤り位置多項式 $\Lambda(Z)$ が導出できる．しかし，誤り発生個数が不明であるとき，訂正可能個数以下の誤りに対し，次の系 1.1 が成立する．

[系 1.1]　$\Lambda(Z)$ を因数多項式にもつ 0 次係数が 1 である t 次以下の多項式と $S(Z)$ の積は t 次から $2t-1$ 次までの係数が 0 となり，このような，$\Lambda(Z)$ を因数多項式にもつ多項式は $(q^m)^{t-w}$ 個存在する．　□

(証明)　誤り位置多項式を因数多項式にもつ多項式は $\Lambda(Z)B(Z)$ と表される．ただし $B(Z) = 1+\sum_{i=1}^{t-w} B_i Z^i$，$B_i \in GF(q^m)$ $(1 \le i \le t-w)$ とする．式 (15) の両辺に $\Lambda(Z)B(Z)$ を乗じることによって

$$\begin{aligned}&S(Z)\Lambda(Z)B(Z) \\ &\quad\equiv \Lambda(Z)B(Z)\sum_{i=1}^{w} \frac{e_{j_i}(\alpha^{j_i})^{m_0}}{1-\alpha^{j_i}Z} \bmod Z^{2t} \\ &\quad\equiv B(Z)\Omega(Z) \bmod Z^{2t}\end{aligned} \tag{19}$$

が得られる．式 (19) 右辺の次数は $t-1$ 次以下であることから，多項式の合同関係より $S(Z)\Lambda(Z)B(Z)$ の t 次から $2t-1$ 次までの係数はゼロでなければならない．また，$\Lambda(Z)$ を因数多項式にもつ $\Lambda(Z)B(Z)$ は $B(Z)$ がとり得る係数分の自由度を有する．したがって，$t-w$ 個の係数それぞれが $GF(q^m)$ の係数をもち得ることから，$\Lambda(Z)B(Z)$ は $(q^m)^{t-w}$ 個存在する．　□

3.2　限界内の誤りに対する線形再帰関係

ここで，誤り発生個数 w が未知であるとき，$S(Z)P(Z)$ の t 次から $2t-1$ 次の係数がゼロになる多項式 $P(Z) = 1+\sum_{i=1}^{t} P_i Z^i$ の条件を考える．ただし，$P_i \in GF(q^m)$ $(1 \le i \le t)$ である．

このとき，$S(Z)P(Z)$ の t 次係数がゼロになることから

$$S_{m_0+t} + S_{m_0+t-1}P_1 + \cdots + S_{m_0}P_t = 0 \tag{20}$$

と表される関係式が得られる．同様に，$t+1$ 次から $2t-1$ 次係数がゼロになることから $t-1$ 個の関係式が得られ，合わせて t 個の関係式からなる連立方程式

$$\begin{aligned}
S_{m_0+t} &+ S_{m_0+t-1}P_1 + \cdots + S_{m_0}P_t &&= 0 \\
S_{m_0+t+1} &+ S_{m_0+t}P_1 + \cdots + S_{m_0+1}P_t &&= 0 \\
&\vdots \\
S_{m_0+2t-1} &+ S_{m_0+2t-2}P_1 + \cdots + S_{m_0+t-1}P_t &&= 0
\end{aligned} \tag{21}$$

が得られる．$P(Z)$ は式 (21) を満たす係数をもつ．式

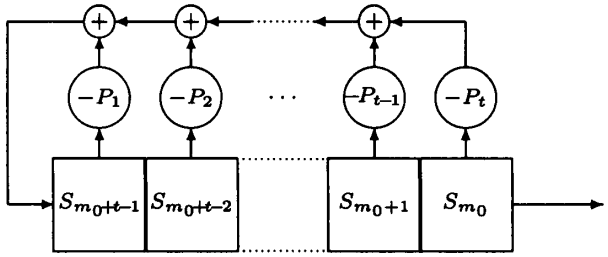

図 2 $P(Z)$ による $S(Z)$ 導出単純型 LFSR の初期状態
Fig. 2 Initial state of simple type LFSR derivating $S(Z)$ by $P(Z)$.

(21) の連立方程式はタップ多項式を $P(Z)$，初期値多項式を $S(Z)$ とした単純型 LFSR によって与えられる線形再帰関係と等価であり，図 2 に対応している．

式 (21) の連立方程式の各式に対応する受信シンドロームによって構成される係数のベクトル

$$\begin{matrix}(S_{m_0+t} & S_{m_0+t-1} & \cdots & S_{m_0} &) \\ (S_{m_0+t+1} & S_{m_0+t} & \cdots & S_{m_0+1} &) \\ & & \vdots & & \\ (S_{m_0+2t-1} & S_{m_0+2t-2} & \cdots & S_{m_0+t-1} &)\end{matrix} \quad (22)$$

がすべて一次独立である場合，受信シンドロームを導出するタップ多項式 $P(Z)$ は，ただ一つ導出される．一方，式 (22) の一次独立なベクトルの数が $w(<t)$ であるときは，最短のタップ長 w を決定した上で連立方程式を再構成しなければ，複数の解が導出される．そこで，Matrix-reduction 法を用いて式 (21) の連立方程式を解くことによって，最短のタップ長 w をもつタップと，タップ長が t 以下 $w+1$ 以上となるタップを与える部分を区別した形で与え，t 以下 w 以上の任意の長さのタップを構築できる一般解の導出法を次章で与える．

4. タップ多項式導出法

式 (21) を満足し，図 2 に対応する LFSR のタップ多項式 $P(Z)$ を求めるために，Matrix-reduction 法を用いる．

4.1 Matrix-reduction 法の適用

式 (21) の連立方程式を Matrix-reduction 法により解くために，式 (21) を行列表現へ置き換える必要があるが，$P(Z)$ の係数を中心にした並べ方を考えると降順と昇順の 2 通りある．

$P(Z)$ の係数を降順 $(P_t, P_{t-1}, \cdots, P_1)$ に並べた場合と，昇順 $(P_1, P_2, \cdots, P_t)$ と並べた場合では，ともに同じ $P(Z)$ の解集合を与えるが，本節では最短のタップ長のタップ多項式である，誤り位置多項式の導出を念頭におき，線形再帰関係を満たす最小次数のタップを一意に導出するために，降順を用いることとする．

$P_i(1 \le i \le t)$ の並びを降順とした場合，式 (21) は

$$\begin{pmatrix} P_t \\ P_{t-1} \\ \vdots \\ P_1 \end{pmatrix}^T \begin{pmatrix} S_{m_0} & S_{m_0+1} \cdots S_{m_0+t-1} \\ S_{m_0+1} & S_{m_0+2} \cdots S_{m_0+t} \\ & \vdots \\ S_{m_0+t-1} & S_{m_0+t} \cdots S_{m_0+2t-2} \end{pmatrix}$$
$$= (\ -S_{m_0+t}\ -S_{m_0+t+1} \cdots -S_{m_0+2t-1}\ ) \quad (23)$$

と表現できる．ただし，$\mathbf{A}^T$ は行列 $\mathbf{A}$ の転置を表すものとする．また，次の表記が式 (23) に対応するものとする．

$$(\mathbf{P})(\mathbf{S}) = (\mathbf{U}) \quad (24)$$

ただし，

$$\mathbf{P} = (P_t\ P_{t-1} \cdots P_1) \quad (25)$$

$$\mathbf{S} = \begin{pmatrix} S_{m_0} & S_{m_0+1} \cdots S_{m_0+t-1} \\ S_{m_0+1} & S_{m_0+2} \cdots S_{m_0+t} \\ & \vdots \\ S_{m_0+t-1} & S_{m_0+t} \cdots S_{m_0+2t-2} \end{pmatrix} \quad (26)$$

$$\mathbf{U} = (-S_{m_0+t}\ -S_{m_0+t+1} \cdots -S_{m_0+2t-1}) \quad (27)$$

である．

式 (26) で表される $\mathbf{S}$ は Peterson 法において誤り発生個数を決定する初期時の行列に等しい．誤り発生個数が t 個のとき，$\mathrm{rank}\,\mathbf{S} = w = t$ であるため，誤り位置多項式の各係数が一意に決定できる．しかし，誤りが t 個未満の w 個発生している場合，$\mathrm{rank}\,\mathbf{S} = w < t$ であるため複数の解が存在する．そこで，Peterson 法では，$\mathbf{S}$ の行列式が非ゼロになる $w \times w$ 行列になるまで $\mathbf{S}$ を縮小することで誤り発生個数を導出していた．$\mathrm{rank}\,\mathbf{S}$ を導出することは誤り発生個数を導出することと等価であり，誤り発生個数を導出することは，代数的誤り訂正の導出目的の一つである．Matrix-reduction 法を用いたタップ導出法において，誤り発生個数 w と一致する最短のタップ長 w は受信シンドロームを発生するすべてのタップの導出と同時に判明する値である．

式 (23) の右辺にある要素をすべて左辺に移項することによって，$\mathbf{P}$ 部分に要素 -1 が付け加えられ

$$\begin{pmatrix} P_t \\ P_{t-1} \\ \vdots \\ \hline P_1 \\ -1 \end{pmatrix}^T \begin{pmatrix} S_{m_0} & S_{m_0+1} & \cdots S_{m_0+t-1} \\ S_{m_0+1} & S_{m_0+2} & \cdots S_{m_0+t} \\ & & \vdots \\ \hline S_{m_0+t-1} & S_{m_0+t} & \cdots S_{m_0+2t-2} \\ -S_{m_0+t} & -S_{m_0+t+1} & \cdots -S_{m_0+2t-1} \end{pmatrix}$$
$$= (0\ 0 \cdots 0) \tag{28}$$

のようになり，次の表記が対応する．

$$\left(\mathbf{P}\middle|-1\right)\left(\frac{\mathbf{S}}{\mathbf{U}}\right) = (\mathbf{0}) \tag{29}$$

式 (29) の $\left(\frac{\mathbf{S}}{\mathbf{U}}\right)$ の行列に対して，行列 $\mathbf{S}$ が reduced triangular idempotent form [2] をとるように Matrix-reduction 法（付録 **1.** 参照）を施すことで式 (30) を得る．

$$\left(\frac{\mathbf{S}'}{\mathbf{U}'}\right) = \begin{pmatrix} S_{1,1} & S_{1,2} & \cdots & S_{1,t} \\ S_{2,1} & S_{2,2} & \cdots & S_{2,t} \\ & & \ddots & \vdots \\ S_{t-1,1} & & S_{t-1,t-1} & S_{t-1,t} \\ \hline S_{t,1} & S_{t,2} & \cdots & S_{t,t} \\ u_t & u_{t-1} & \cdots & u_1 \end{pmatrix} \tag{30}$$

ここで，$S_{i,j}$ $(1 \le i, j \le t)$ は Matrix-reduction 法による処理後の行列の i 行 j 列要素，u_i $(1 \le i \le t)$ は $t+1$ 行 $t-i+1$ 列要素を表す．式 (30) の行列 $\mathbf{S}'$ は reduced triangular idempotent form をとることから，$S_{i,j} = 0$ $(i > j)$ であり，対角要素である $S_{i,i}$ $(1 \le i \le t)$ は，0 若しくは 1 であり，0 のとき，その列の要素はすべて 0 となり，1 のとき，その行のほかの要素はすべて 0 となっている．

連立方程式の解は，式 (30) における $(t \times t)$ の行列である $\mathbf{S}'$ から，t 次単位行列 $\mathbf{I}_t$ を引くことで得られ，次のようになる．

$$\left(\frac{\mathbf{S}' - \mathbf{I}_t}{\mathbf{U}'}\right) = \begin{pmatrix} S_{1,1}-1 & S_{1,2} & \cdots & S_{1,t} \\ S_{2,1} & S_{2,2}-1 & \cdots & S_{2,t} \\ & & \ddots & \vdots \\ S_{t-1,1} & & S_{t-1,t-1}-1 & S_{t-1,t} \\ \hline S_{t,1} & S_{t,2} & & S_{t,t}-1 \\ u_t & u_{t-1} & \cdots & u_1 \end{pmatrix} \tag{31}$$

以上の方法によって導出された式 (31) は以下のような対応関係

$$\begin{pmatrix} S_{1,1}-1 & S_{1,2} & \cdots & S_{1,t} \\ S_{2,1} & S_{2,2}-1 & \cdots & S_{2,t} \\ & & \ddots & \vdots \\ S_{t-1,1} & & S_{t-1,t-1}-1 & S_{t-1,t} \\ \hline S_{t,1} & S_{t,2} & & S_{t,t}-1 \\ u_t & u_{t-1} & \cdots & u_1 \end{pmatrix} = \begin{pmatrix} \mathbf{p}^{[1]} \\ \mathbf{p}^{[2]} \\ \vdots \\ \mathbf{p}^{[t-1]} \\ \hline \mathbf{p}^{[t]} \\ \mathbf{U}' \end{pmatrix} \tag{32}$$

をもつ行ベクトルで表されるとする．式 (32) で表される行ベクトル $\mathbf{U}'$ と行ベクトル $\mathbf{p}^{[i]}$ $(1 \le i \le t)$ の一次結合は式 (23) を満たす $\mathbf{P}$ の解であり次の式で表される．

$$\mathbf{P} = \mathbf{U}' + \sum_{i=1}^{t} k_i \mathbf{p}^{[i]} \tag{33}$$

ただし，k_i $(1 \le i \le t)$ は $GF(q^m)$ の元をとる一次結合係数である．以上の結果を多項式表現を用いて表す．第 i $(1 \le i \le t)$ 行の行ベクトル表現

$$\mathbf{p}^{[i]} = (S_{i,1}, \cdots, S_{i,i-1}, S_{i,i}-1, S_{i,i+1}, \cdots, S_{i,t}) \tag{34}$$

は，多項式

$$\mathbf{p}^{[i]}(Z) = S_{i,1}Z^t + \cdots + S_{i,i-1}Z^{t-i+2} + (S_{i,i}-1)Z^{t-i+1} + S_{i,i+1}Z^{t-i}$$

$$+\cdots+S_{i,t}Z^1 \tag{35}$$

に対応し

$$\mathbf{U}'=(u_t,u_{t-1},\cdots,u_1) \tag{36}$$

は，多項式

$$\mathbf{U}'(Z)=u_tZ^t+u_{t-1}Z^{t-1}+\cdots+u_1Z^1 \tag{37}$$

に対応する．式 (33) によって $P(Z)$ の P_1 から P_t 次までの係数が決定できることから，$P(Z)$ は $\mathbf{p}^{[i]}(Z)$ $(1\le i\le t)$ の一次結合と $\mathbf{U}'(Z)$ 及び 0 次係数の 1 によって次の式 (38) で表される．

$$P(Z)=\mathbf{U}'(Z)+\sum_{i=1}^{t}k_i\mathbf{p}^{[i]}(Z)+1 \tag{38}$$

式 (38) は Matrix-reduction 法を用いた一般的な連立方程式の解である．

4.2 すべてのタップと最短長のタップの決定

$w=t$ であるときは，$\mathrm{rank}\,\mathbf{S}=t$ であることから，Matrix-reduction 法によって導出された行列 $\mathbf{S}'$ は t 次単位行列となる．したがって，式 (38) の一般解を与える $\mathbf{p}^{[i]}(Z)$ $(1\le i\le t)$ がすべてゼロ多項式になるため，Matrix-reduction 法による結果は一意な解を与え，受信シンドロームを生成するタップ多項式の導出が完了する．一方，$w(<t)$ 個の誤りが発生したとき，$\mathrm{rank}\,\mathbf{S}=w$ であることから，Matrix-reduction 法の操作後に reduced triangular idempotent form をとる行列 $\mathbf{S}'$ は，対角要素の 1 を唯一の非ゼロ要素としてもつ w 個の行と，列のすべての要素が 0 をもつ $t-w$ 個の列をもつ．Matrix-reduction 法の操作後の行列 $\mathbf{S}'$ から t 次単位行列を引く操作によって，対角要素に 1 をもつ w 個の行は，すべて 0 を要素にもつ行となる．したがって，多項式表現された $\mathbf{p}^{[i]}(Z)$ $(1\le i\le t)$ のうち w 個がゼロ多項式となるため，式 (38) は

$$P(Z)=\mathbf{U}'(Z)+\sum_{r=1}^{t-w}k_{i_r}\mathbf{p}^{[i_r]}(Z)+1 \tag{39}$$

とまとめられる．ただし，$\mathbf{p}^{[i_r]}(Z)$ $(1\le i_r\le t,\ 1\le r\le t-w)$ は非ゼロ多項式，$k_{i_r}\in GF(q^m)$ とする．

式 (39) によって表される連立方程式の解に対して次の定理 2 が与えられる．

[定理 2] 誤り発生個数 $w(\le t)$ のとき，$S(Z)P(Z)$ の t 次から $2t-1$ 次までの係数をゼロにする多項式

$$P(Z)=1+\sum_{i=1}^{t}P_iZ^i \quad (P_i\in GF(q^m)) \tag{40}$$

は最短のタップ多項式である誤り位置多項式 $\Lambda(Z)$ を因数多項式にもつ． □

(証明) $P(Z)$ が誤り位置多項式を因数多項式としてもつことが，$P(Z)$ と受信シンドローム多項式 $S(Z)$ の積の t 次から $2t-1$ 次までの係数がゼロになるための必要十分条件であることを示す．

系 1.1 より，誤り位置多項式 $\Lambda(Z)$ を因数多項式にもつ t 次以下で 0 次係数が 1 である多項式 $B(Z)\Lambda(Z)$ と受信シンドローム多項式 $S(Z)$ の積は t 次から $2t-1$ 次までの係数が 0 である．したがって，$P(Z)$ が $\Lambda(Z)$ を因数多項式にもつことは，$P(Z)S(Z)$ の t 次から $2t-1$ 次の係数が 0 になるための十分条件である．

一方，必要条件について考える必要があるが，十分条件において，誤り位置多項式 $\Lambda(Z)$ を因数多項式にもつ t 次以下で 0 次係数が 1 である多項式の数 $(q^m)^{t-w}$ は，式 (39) より表される受信シンドローム多項式との積の t 次から $2t-1$ 次係数をゼロにする $P(Z)$ のとり得る解の個数 $(q^m)^{t-w}$ と等しい．それぞれの条件を満たす個数が等しい多項式集合に対して十分条件が成り立つことから，$P(Z)$ が誤り位置多項式 $\Lambda(Z)$ を因数多項式にもっていることと，$P(Z)$ と受信シンドローム多項式 $S(Z)$ の積の t 次から $2t-1$ 係数が 0 になることは同値である．したがって，$P(Z)S(Z)$ の t 次から $2t-1$ 次の係数が 0 になることは，$P(Z)$ が誤り位置多項式 $\Lambda(Z)$ を因数多項式にもつための必要条件となる．結果として，式 (39) によって表される Matrix-reduction 法によって導出された解 $P(Z)$ は $\Lambda(Z)$ を因数多項式にもつことが示された． □

また，定理 2 より，$\Lambda(Z)\mid P(Z)$ であることから次の系 2.1 が与えられる．

[系 2.1]

$$\Lambda(Z)\mid\mathbf{U}'(Z)+1 \tag{41}$$

であり，一般解を与える非ゼロ多項式それぞれについて

$$\Lambda(Z)\mid\mathbf{p}^{[i_r]}(Z)\quad(1\le i_r\le t,\ 1\le r\le t-w) \tag{42}$$

が成立する． □

(証明) 式 (39) の $P(Z)$ において定理 2 が成立することから，一次結合係数 k_{i_r} $(1 \leq i_r \leq t,\ 1 \leq r \leq t-w)$ をすべてゼロにしたとき，$\Lambda(Z) \mid \mathbf{U}'(Z)+1$ が得られる．次に，ある一次結合係数 k_{i_j} $(\in \{k_{i_r} \mid 1 \leq i_r \leq t,\ 1 \leq r \leq t-w\})$ が唯一の非ゼロ一次結合係数であるとき，$\Lambda(Z) \mid \mathbf{U}'(Z)+k_{i_j}\mathbf{p}^{[i_j]}(Z)+1$ が成立するためには，$\Lambda(Z) \mid \mathbf{U}'(Z)+1$ であることから $\Lambda(Z) \mid k_{i_j}\mathbf{p}^{[i_j]}(Z)$ でなければならない．したがって，$\Lambda(Z) \mid \mathbf{p}^{[i_r]}(Z)$ $(1 \leq i_r \leq t,\ 1 \leq r \leq t-w)$ が成立する． □

また，最短のタップである誤り位置多項式を一意に導出するためには次の系 2.2 が重要である．

[系 2.2] $P(Z)$ の係数が降順になるように並べることにより，Matrix-reduction 法は $t+1$ 行目に最小次数の解である誤り位置多項式 $\Lambda(Z)=\mathbf{U}'(Z)+1$ に対応するベクトル $\mathbf{U}'$ を与える． □

(証明) $\operatorname{rank}\mathbf{S}=w(<t)$ であるとき，$P(Z)$ の係数が降順になるように並べることによって，Matrix-reduction 法の処理によって得られる行列は，w 次単位行列を有する式 (43) の形をした行列になる．

$$\left(\begin{array}{c|c} \mathbf{0}_{t-w} & \check{\mathbf{S}} \\ \hline \mathbf{0}_{w\times(t-w)} & \mathbf{I}_w \\ \hline 0\cdots 0 & u_w\cdots u_1 \end{array}\right) \tag{43}$$

この行列から，$\mathbf{I}_t$ を引くことで，

$$\left(\begin{array}{c|c} -\mathbf{I}_{t-w} & \check{\mathbf{S}} \\ \hline \mathbf{0}_{w\times(t-w)} & \mathbf{0}_w \\ \hline 0\cdots 0 & u_w\cdots u_1 \end{array}\right) \tag{44}$$

となる．ただし，$\mathbf{0}_i$ は i 次ゼロ行列，$\mathbf{0}_{i\times j}$ は $(i\times j)$ ゼロ行列，$\mathbf{I}_i$ は i 次単位行列，$\check{\mathbf{S}}$ は $S_{i,j}$ $(1 \leq i \leq t-w,\ t-w+1 \leq j \leq t)$ の値をもつ部分行列である．式 (44) の各行ベクトルに対応する非ゼロ多項式は

$$\mathbf{p}^{[i]}(Z) = -Z^{t-i+1} + \sum_{j=1}^{w} S_{i,t-j+1}Z^j \quad (1 \leq i \leq t-w) \tag{45}$$

と表される．したがって，系 2.1 及び系 2.2 より

$$\deg(\mathbf{U}'(Z)+1) < \deg\mathbf{p}^{[i]}(Z) \quad (1 \leq i \leq t-w) \tag{46}$$

なる関係が成立する．結果として，$t+1$ 行目に最小次数の解となる誤り位置多項式 $\Lambda(Z)=\mathbf{U}'(Z)+1$ に対応するベクトル $\mathbf{U}'$ を与える． □

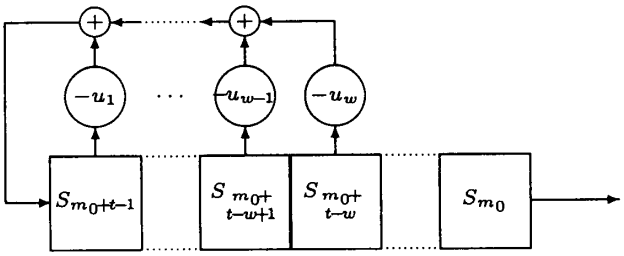

図 3 $\Lambda(Z)$ によるレジスタ長 t の $S(Z)$ 導出単純型 LFSR の初期状態

Fig. 3 Initial state of simple type LFSR derivating $S(Z)$ by $\Lambda(Z)$ register langth t.

$P(Z)$ の係数が降順になるように並べることで $P(Z)$ に含まれる最小次数の解である誤り位置多項式 $\Lambda(Z)$ が一意に導出できるが，$P(Z)$ の係数が昇順になるように並べたとき，$\mathbf{U}'(Z)+1$ は $P(Z)$ に含まれる最小次数の解とならない．このとき，導出された $P(Z)$ に含まれる最小次数の解である誤り位置多項式 $\Lambda(Z)$ を導出するための手順を，$P(Z)$ の係数を降順に並べたときの誤り位置多項式導出手順と併せて付録 **2.** に示す．

系 2.2 により与えられる最低次数の解 $\Lambda(Z)=\mathbf{U}'(Z)+1$ をタップ多項式とする，受信シンドロームを発生するレジスタ長 t，タップ長 w のレジスタ回路は図 3 のようになる．図 3 は，レジスタ長とタップ長が一致せず，S_{m_0} から $S_{m_0+t-w-1}$ は，再帰関係に関連することなく出力されている．これは $P(Z)$ を図 2 に関連するレジスタ長 t のタップとして導出したため，誤り発生個数が t 個未満であるときは，式 (21) で与えられる連立方程式に含まれない線形再帰関係をもつ受信シンドロームの部分が存在することを意味している．S_{m_0+w} から S_{m_0+t-1} までを導出する線形再帰関係は，誤り発生個数 w が判明したときに得られる $2t-w$ 個の連立方程式のうち，S_{m_0+t} から S_{m_0+2t-1} を導出する t 個の連立方程式（式 (21)）を除いた $t-w$ 個の連立方程式によって表される．したがって，S_{m_0} から S_{m_0+w-1} を初期値，タップ多項式 $\mathbf{U}'(Z)+1$ とする，レジスタ長 w，タップ長 w の単純型 LFSR を構築することも可能である．

また，系 2.2 より，式 (39) は式 (45) によって表される非ゼロ多項式の一次結合によって

$$P(Z) = \mathbf{U}'(Z) + \sum_{i=1}^{t-w} k_i\mathbf{p}^{[i]}(Z) + 1 \tag{47}$$

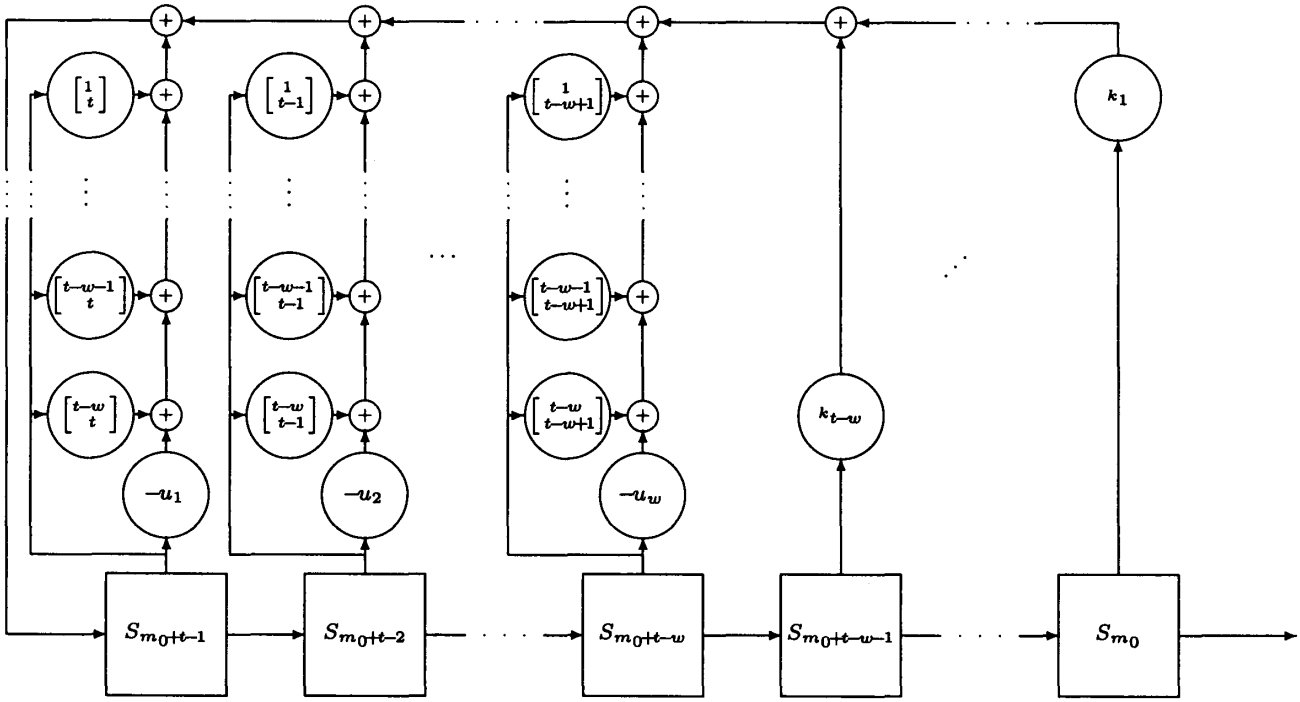

図 4 $S(Z)$ 導出一般形単純型 LFSR の初期状態
Fig. 4 Generalized initial state of simple type LFSR derivating $S(Z)$.

と表される．$2t$ 個の受信シンドロームを導出可能なタップ長 t 以下 w 以上の単純型 LFSR のタップは，式 (47) における k_i $(1 \leq i \leq t-w)$ を任意に指定することで任意のタップが構築できる．任意のタップを構成する要素はベクトル表現を用いて

$$\begin{pmatrix} -k_1 & 0 & 0 \cdots 0 & 0 & k_1 S_{1,t-w+1} & \cdots & k_1 S_{1,t} \\ 0 & -k_2 & 0 \cdots 0 & 0 & k_2 S_{2,t-w+1} & \cdots & k_2 S_{2,t} \\ & & \ddots & & & \vdots & \\ 0 & 0 & 0 \cdots 0 & -k_{t-w} & k_{t-w} S_{t-w,t-w+1} & \cdots & k_{t-w} S_{t-w,t} \\ 0 & 0 & 0 \cdots 0 & 0 & u_w & \cdots & u_1 \end{pmatrix} \tag{48}$$

と表すことができ，これらのベクトルの和をタップとする単純型 LFSR（図 4）が構築できる．ただし，$\begin{bmatrix} i \\ j \end{bmatrix}$ は $-k_i S_{i,j}$ を表すものとする．

5. 検　　討

Matrix-reduction 法を用いた誤り位置多項式導出法を処理時間，総計算量，装置量に関して評価するのに先立って，Matrix-reduction 法における並列処理を明確にする．並列処理は，各列処理を一度に行うことにより実現され，処理時間の短縮を図ることができる．$S_{i,j}$ を i 行 j 列要素とする $((t+1) \times t)$ 行列において第 1 列目要素の定数倍をある一つの第 i $(2 \leq i \leq t)$

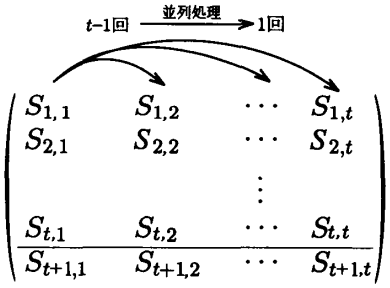

図 5 列の並列処理
Fig. 5 Column parallel processing.

列から引く操作は式 (49) に示したような t 次多項式を t 次多項式で割り，$t-1$ 次以下の剰余多項式を得る操作と等価である．これを第 2 列から第 t 列それぞれに行う操作（図 5）は，それぞれ独立しているため，同時に行うことができる．この並列処理によって，通常は $O(t^2)$ の処理時間を必要とする各列処理を，$O(t)$ の時間で処理することができる．

$$\begin{array}{r} Q_1 \\ \hline S_{1,1}S_{2,1}\cdots S_{t+1,1} \overline{)\, S_{1,i} \quad S_{2,i} \quad \cdots S_{t,i}} \\ \underline{S_{1,1}Q_1 \; S_{2,1}Q_1 \cdots S_{t+1,1}Q_1} \\ R_2 \quad \cdots \quad R_{t+1} \end{array} \tag{49}$$

この並列処理を施した Matrix-reduction 法におけ

る列処理と，ユークリッド法における除算操作を比較する．ユークリッド法における多項式の除算処理の繰返しのうち，最終段階で生じる可能性のある，$t+1$ 次多項式を t 次多項式で割り，$t-1$ 次以下の剰余多項式を得る操作は，除算の商多項式が一次多項式であるとしたとき，Matrix-reduction 法において行列のある 2 列を列操作することに相当する．しかし，この 2 列の操作に相当するユークリッド法における一次多項式の二つの係数を導出する操作は，同時に行うことができないので，Matrix-reduction 法で用いた並列処理ができない．したがって，ユークリッド法のすべての除算操作において一次の商多項式が導出されるとしたとき，Matrix-reduction 法を用いた誤り位置多項式導出法の倍の時間を要する．これら二つの誤り位置多項式導出法と比較して，Berlekamp-Massey 法に要する処理時間は，$2t$ 回のすべてのステップにおいて discrepancy を導出する必要があることと，導出された discrepancy に応じてそのステップにおける新たなタップの構築をするかどうかによって決まるが，t 回構築されるとしたとき，合計 $3t$ の時間を要する．Matrix-reduction 法の処理時間を 1 とした場合の各誤り位置多項式導出法の相対処理時間を図 6 に示す．

次に総計算量について検討する．誤り訂正可能個数だけの誤りが発生している場合を想定し，各誤り位置多項式導出法における総計算量（元の積，和，逆元の導出回数）をそれぞれ図 7，図 8 及び図 9 に示す．ユークリッド法と Berlekamp-Massey 法では Berlekamp-Massey 法の総計算量が少ないが，ともに $O(t^2)$ である（付録 **3.1** 参照）．一方，図 7，図 8 に比べて図 9 を比較すると，Matrix-reduction 法は $O(t^3)$ の計算を必要とするため，誤り訂正可能個数の増加に伴い急激に総計算量が増加するものの，$t \leq 4$ では Matrix-reduction 法はユークリッド法よりも総計算量が少なく，$t \leq 2$ では，Matrix-reduction 法の総計算量が最も少ない．

最後に，装置量について検討する．誤り位置多項式を導出するために必要なシンドロームの格納，また，計算過程において保存しておかなければならない値の格納に必要なレジスタの量を表す．一つの元を格納するためには，拡大次数分の 0，1 を格納するレジス

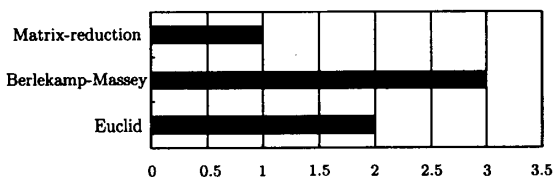

図 6　相対処理時間
Fig. 6　Relative processing time.

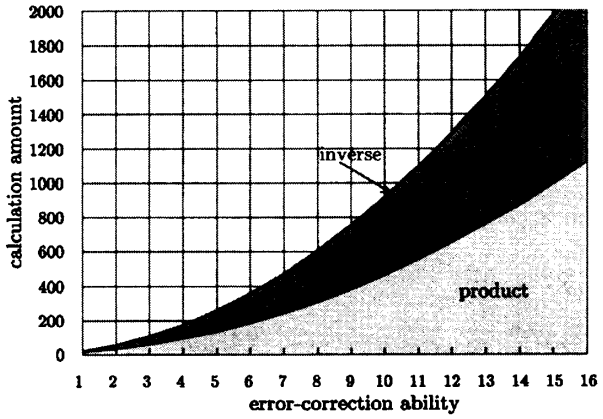

図 7　総計算量（ユークリッド法）
Fig. 7　All calculation amount of Euclid algorithm.

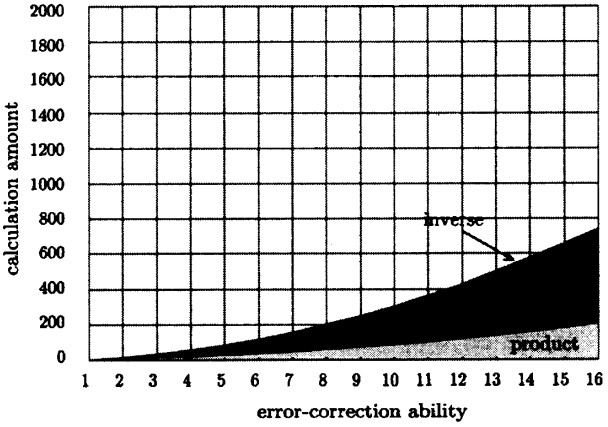

図 8　総計算量（Berlekamp-Massey 法）
Fig. 8　All calculation amount of Berlekamp-Massey algorithm.

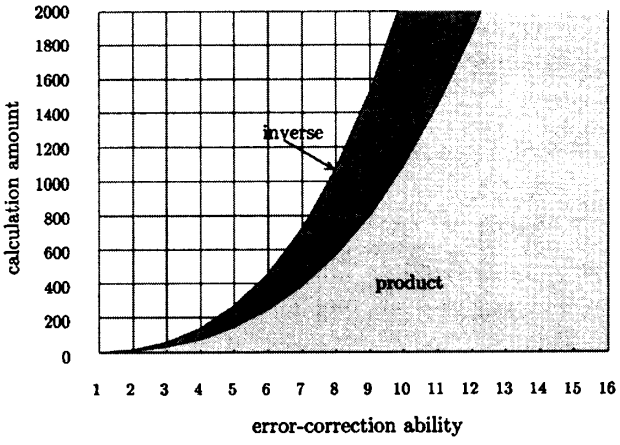

図 9　総計算量（Matrix-reduction 法）
Fig. 9　All calculation amount of Matrix-reduction algorithm.

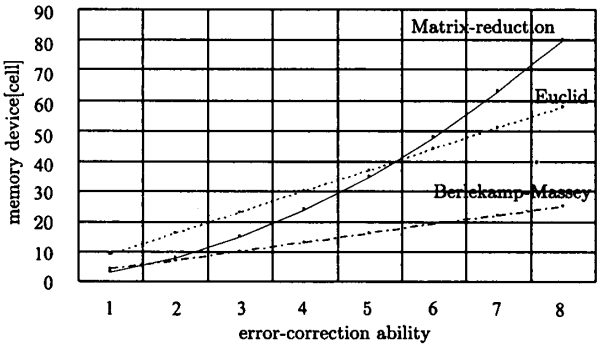

図 10 装 置 量
Fig. 10 Devices amount.

タを必要とするが，ここでは，一つの元を格納するためのレジスタを 1 [cell] と考える．このとき，ユークリッド法においては，除算処理に用いられるシンドローム系列を格納できる長さのレジスタ二つのほかに，商多項式の格納のためのレジスタ，また，商多項式から誤り位置多項式を導出するためのレジスタが必要である（付録 **3. 2. 1**）．Berlekamp-Massey 法では，discrepancy の導出にシフトレジスタを用意し，discrepancy が非零であるときの新たなタップの構築に用いる過去のタップを保存するためのレジスタを必要とする（付録 **3. 2. 2**）．Matrix-reduction 法では，シンドロームを保存する $((t+1)\times t)$ の行列分のレジスタを必要とする（付録 **3. 2. 3**）．誤り訂正可能個数の増大に伴う各誤り位置多項式導出法におけるレジスタ量を図 10 に示す．図 10 より，$t \leq 5$ の範囲では，Matrix-reduction 法はユークリッド法よりも少ないレジスタで構成することが可能であることが分かる．

6. 考　　察

Matrix-reduction 法が行列処理による誤り位置多項式導出法であることは，処理時間において大きな効果をもたらす．このことは，多項式の除算処理における商多項式の各次数の係数の導出が同時に行えないことに対して，行列の列処理の並列操作が可能であることに起因している．結果として，Matrix-reduction 法は，ユークリッド法，Berlekamp-Massey 法の 1/2, 1/3 の処理時間で誤り位置多項式を導出することが可能である．

受信シンドローム多項式と誤り位置多項式の候補の積の t 次から $2t-1$ 次の係数がゼロになる関係から，t 個の連立方程式が与えられ，その解法として Matrix-reduction 法を用いることで誤り位置多項式が得られることは Berlekamp によっても示唆されていた．しかし，Berlekamp は総計算量と装置量の多さから，Matrix-reduction 法を用いた誤り位置多項式導出法を実用のものとせず，Berlekamp 法に優位性があるという結論に至っている．Matrix-reduction 法の総計算量，装置量に関しては $O(t^3)$ であることから，誤り訂正可能個数が大きくなるにつれて増加量が顕著になるが，$t \leq 5$ 程度では，ユークリッド法や Berlekamp-Massey 法に比べて優位となる．また，ユークリッド法や Berlekamp-Massey 法と比べて，Matrix-reduction 法は装置量の総数は多くなるが，行列要素を格納するレジスタとそれに付随する演算素子を規則的に並べることで回路を組むことができるので，総量的には少ないユークリッド法などに比べても，高集積化を図りやすい構造を有している．

本論文において，誤り位置多項式を導出する手法として Matrix-reduction 法をとらえると，図 3 のようなタップを導出するだけでよいため，次数を大きくする自由度を与える部分は必要としない．しかし，誤り位置多項式を因数多項式とする誤り発生個数以上の次数となる多項式が得られることは，誤り位置多項式を直接導出することが困難でありながら，誤り位置多項式を因数多項式に含む多項式を導出できる誤り位置導出法の研究に寄与する．その一つとして，Feng ら [6] が示した，連続する二つのシンドローム系列を用いた，設計誤り訂正可能個数以上の誤りに対する誤り位置導出法が挙げられる．Feng らは，設計最小距離と真の最小距離の異なる符号に対して，連続している二つのシンドロームを連結し，Fundamental Iterative 法を用いて多項式を導出する．その多項式を連結した分の補正を行うことで誤り位置多項式を因数多項式に含む，誤り発生個数以上の次数である多項式を導出している．Matrix-reduction 法を用いることで，Feng らが示した誤り位置多項式を因数多項式に含む多項式を直接導出することが可能であり，Matrix-reduction 法が最小次数の解を因数多項式に含む解を導出する性質を用いて結果づけることができる．

7. む　す　び

本論文では，誤り評価多項式を与える Key Equation が示す多項式の合同関係と誤り評価多項式の次数関係から分かる多項式の合同関係の違いに注目し，その差異が与える連立方程式を単純型 LFSR が示す線形再帰関係であるととらえ，受信シンドロームを導出する

タップ多項式を Matrix-reduction 法を用いて与えることができることを示した．

Matrix-reduction 法が与えるあらゆる解は，与えられた受信シンドロームを出力する単純型 LFSR のタップとなり得る．したがって，最短長のタップか否かにかかわらず誤りシンドロームを導出するタップとなる．

また，線形再帰関係を満たす最小次数の解を導出することを目的としたとき，導出するタップ多項式の係数が降順に導出されるように，受信シンドロームによって構成される行列を構築し，Matrix-reduction 法を施すことで，線形再帰関係を満たすタップ係数の集合は最小次数を与える解と一般解を与える部分に区別された状態で与えられる．Matrix-reduction 法によって導出された複数の解はすべて与えられた受信シンドロームを出力する単純型 LFSR のタップ多項式となり，最小次数の解は同じ系列を与える最短レジスタ長のタップ係数である．結果として，Matrix-reduction 法は誤り位置多項式を一意に与えることができることを示した．

実際に，Matrix-reduction 法を誤り位置多項式導出法として用いる際に問題となる処理時間，総計算量，装置量に関して，誤り訂正可能個数に応じた値を示した．Matrix-reduction 法を並列処理することで，従来法よりも少ない時間で処理することが可能である．デメリットとして挙げられることが多い総計算量と装置量については，誤り訂正可能個数の大きな範囲では大きくなる傾向があるが，小さな範囲では従来法よりも抑えられる傾向があることも示した．

本論文で与えた結果は，Berlekamp が言及するに至らなかった，Matrix-reduction 法が与える一般解に対する検討として，すべての解が誤り位置多項式を因数多項式にもつことを示し，誤り位置多項式を一意に導出するために，導出する多項式の係数を降順に並べることを示した．

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] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "A method for solving key equation for decoding Goppa codes," Inf. Control, vol.27, pp.87–99, 1975.

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

[6] G.L. Feng and K.K. Tzeng, "Decoding cyclic and BCH codes up to actual minimum distance using nonrecurrent syndrome dependence relations," IEEE Trans. Inf. Theory, vol.37, no.6, pp.1716–1723, June 1991.

[7] 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.

[8] 藤田　悠，杉村立夫，柴田孝基，"2 種類の LFSR の等価性と初期値変換，" 信学論（A），vol.J87-A, no.7, pp.1086–1089, July 2004.

付　録

1. Matrix-reduction 法 [2]

$(t \times t)$ 列の正方行列に対して，次の操作を行う．

（1） $(1,1)$ 要素が非ゼロであれば，何もしない．$(1,1)$ 要素がゼロであれば，他の列と交換する．交換する対象は，第 1 行目の要素が非ゼロでかつ対角要素がゼロである列．それがなければ，第 1 行目の要素が非ゼロでかつ対角要素が非ゼロの列と交換する．もし，第 1 行目の要素がすべてゼロである場合は，何もしない．

（2） $(1,1)$ 要素が 1 になるように第 1 列目の各要素を正規化する．もし，$(1,1)$ 要素がゼロである場合は，何もしない．

（3） 第 1 列目を各対象列の第 1 行要素倍した値を，その対象列から引き，$(1,1)$ 要素以外の第 1 行目の要素をゼロにする．

（4） 行転回，列転回する．

この（1）から（4）までの一連の操作を t 回繰り返す．

□

Matrix-reduction 法を用いて連立方程式を解くとき，t 個の連立方程式から与えられる $((t+1) \times t)$ 列の行列に対して操作を行う．このとき，増加した $t+1$ 行目は行転回の操作から除外されることを注意しておく．

2. 誤り位置多項式導出手順の例

符号長 255，$GF(2^8)$ 上の 5 重誤り訂正リードソロモン符号を考える．発生した誤りに対応する誤り多項式を

$$e(x) = \alpha^{101}x^{223} + \alpha^{218}x^2 \qquad \text{(A·1)}$$

とする．このときの誤り位置多項式は

$$\begin{aligned}\Lambda(Z) &= (1-\alpha^{223}Z)(1-\alpha^2 Z) \\ &= \alpha^{225}Z^2 + \alpha^{104}Z^1 + 1\end{aligned} \qquad \text{(A·2)}$$

と表される．受信語より得られる受信シンドロームは

$$\begin{aligned} S_1 &= \alpha^{247} \quad S_6 = \alpha^{194} \\ S_2 &= \alpha^{31} \quad S_7 = \alpha^{136} \\ S_3 &= \alpha^{194} \quad S_8 = \alpha^{22} \\ S_4 &= \alpha^{21} \quad S_9 = \alpha^{148} \\ S_5 &= \alpha^{231} \quad S_{10} = \alpha^{130} \end{aligned} \tag{A·3}$$

である．$P(Z)$ の係数を降順に並べたときと昇順に並べたとき，それぞれの誤り位置多項式導出手順を示す．

2.1 降順に並べたとき

誤り位置多項式の候補となる多項式 $P(Z)$ の未知である係数が降順になるように行列を構成すると

$$\left(\begin{array}{c} P_5 \\ P_4 \\ P_3 \\ P_2 \\ P_1 \\ \hline -1 \end{array}\right)^T \left(\begin{array}{ccccc} S_1 & S_2 & S_3 & S_4 & S_5 \\ S_2 & S_3 & S_4 & S_5 & S_6 \\ S_3 & S_4 & S_5 & S_6 & S_7 \\ S_4 & S_5 & S_6 & S_7 & S_8 \\ S_5 & S_6 & S_7 & S_8 & S_9 \\ \hline S_6 & S_6 & S_8 & S_9 & S_{10} \end{array}\right) = \left(\begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{array}\right)^T \tag{A·4}$$

となる．受信シンドロームによって構成される行列に実際に得られた値を代入し，Matrix-reduction 法の処理を施し，単位行列を減じた行列は

$$\left(\begin{array}{ccccc} 1 & 0 & 0 & \alpha^{147} & \alpha^{111} \\ 0 & 1 & 0 & \alpha^{81} & \alpha^{164} \\ 0 & 0 & 1 & \alpha^{134} & \alpha^{30} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \alpha^{225} & \alpha^{104} \end{array}\right) \tag{A·5}$$

となる．式 (A·5) より得られる連立方程式の一般解は

$$\begin{aligned} P(Z) = {} & \alpha^{225}Z^2 + \alpha^{104}Z^1 + 1 \\ & + k_1(Z^5 + \alpha^{147}Z^2 + \alpha^{111}Z^1) \\ & + k_2(Z^4 + \alpha^{81}Z^2 + \alpha^{164}Z^1) \\ & + k_3(Z^3 + \alpha^{134}Z^2 + \alpha^{30}Z^1) \end{aligned} \tag{A·6}$$

となる．一次結合係数 k_1，k_2，k_3 をゼロにすることで，誤り位置多項式 $\Lambda(Z)$ が得られる．

2.2 昇順に並べたとき

誤り位置多項式の候補となる多項式 $P(Z)$ の未知である係数が昇順になるように行列を構成すると

$$\left(\begin{array}{c} P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \\ \hline -1 \end{array}\right)^T \left(\begin{array}{ccccc} S_5 & S_6 & S_7 & S_8 & S_9 \\ S_4 & S_5 & S_6 & S_7 & S_8 \\ S_3 & S_4 & S_5 & S_6 & S_7 \\ S_2 & S_3 & S_4 & S_5 & S_6 \\ S_1 & S_2 & S_3 & S_4 & S_5 \\ \hline S_6 & S_5 & S_8 & S_9 & S_{10} \end{array}\right) = \left(\begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{array}\right)^T \tag{A·7}$$

となる．受信シンドロームによって構成される行列に実際に得られた値を代入し，Matrix-reduction 法の処理を施し，単位行列を減じた行列は

$$\left(\begin{array}{ccccc} 1 & 0 & 0 & \alpha^{57} & \alpha^{246} \\ 0 & 1 & 0 & \alpha^{21} & \alpha^{74} \\ 0 & 0 & 1 & \alpha^{104} & \alpha^{225} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \alpha^{76} & \alpha^{27} \end{array}\right) \tag{A·8}$$

となる．式 (A·8) より得られる連立方程式の一般解は

$$\begin{aligned} P(Z) = {} & 1 + \alpha^{76}Z^4 + \alpha^{27}Z^5 \\ & + k_1(Z^1 + \alpha^{57}Z^4 + \alpha^{246}Z^5) \\ & + k_2(Z^2 + \alpha^{21}Z^4 + \alpha^{74}Z^5) \\ & + k_3(Z^3 + \alpha^{104}Z^4 + \alpha^{225}Z^5) \end{aligned} \tag{A·9}$$

となる．式 (A·9) によって表される $P(Z)$ から誤り位置多項式を導出するために，$P(Z)$ が与える最小次数の多項式を与える一次結合係数を決定する．$P(Z)$ が与える最小のタップ長は 2 であるので，$P(Z)$ の三次以上の係数がゼロになることから与えられる連立方程式

$$\begin{aligned} & k_1\alpha^{246} + k_2\alpha^{74} + \alpha^{27} = 0 \\ & k_1\alpha^{57} + k_2\alpha^{21} + \alpha^{76} = 0 \\ & k_3 = 0 \end{aligned} \tag{A·10}$$

が得られ．この連立方程式を解くことで，$k_1 = \alpha^{104}$，$k_2 = \alpha^{225}$，$k_3 = 0$ が得られ，誤り位置多項式 $\Lambda(Z)$ を導出できる．

3. 総計算量・装置量の見積り

3.1 各誤り位置多項式導出法の総計算量

3.1.1 ユークリッド法の総計算量

拡張ユークリッドの互除法において，多項式の除算操作が最多の t 回，かつ t 回の各除算操作では一次多

項式が商多項式として導出されるとする．一次の商多項式を導出する際には，除多項式の最高次係数の逆元と被除多項式の最高次係数の積を各 2 回必要とするため，t 回の多項式の除算操作において

$$2 \times t \quad [回] \tag{A·11}$$

の積と逆元の演算を必要とする．それぞれの除算操作において，一次の商多項式の一つの係数の導出後，被除多項式から，除多項式を商多項式の係数倍したものを減じるために，除多項式の係数の個数分の積と和の演算が生じる．除多項式は $2t-1$ 次から t 次まで降下していくため

$$\sum_{i=0}^{t-1} 2 \times (2t-i) = 3t^2 + t \quad [回] \tag{A·12}$$

の積と和の演算を必要とする．

1 回の多項式の除算操作が終了後，誤り位置多項式を導出するための多項式積に

$$\sum_{i=1}^{t+1} 2 \times i = t^2 + 3t + 2 \quad [回] \tag{A·13}$$

の積と和の演算を必要とする．これらの合計から次の表 A·1 に表される総計算量が得られる．

3.1.2 Berlekamp-Massey 法の総計算量

discrepancy が $2t$ 回導出され，対象となる系列の長さが，1 から t まで増加する．しかし，増加率は一様でないため，平均値 $\frac{1+t}{2}$ を系列の長さとする．したがって，積は $t(t+1)$ 回，和は $t(t-1)$ 回必要となる．discrepancy の結果から新たなタップを構築するが，補正を行う元のタップを t 次未満の多項式としたとき，$\frac{1+(t+1)}{2}$ を次数の平均値とする．discrepancy が非零である回数を t 回としたとき，積は $\frac{1+(t+1)}{2} \times t$ 回，和は $(t+1)t$ 回となる．これらの合計から表 A·2 が得られる．

3.1.3 Matrix-reduction 法の総計算量

第 1 列を $(1,1)$ 要素で正規化した列ベクトルに第 2 列から第 t 列の各列ベクトルの 1 行目の要素を乗じ，各列ベクトルの $t+1$ 行に加算操作する．これを t 回繰り返すことで，$(t-1) \times (t+1) \times t$ 回の積及び和の演算を必要とする．したがって，これらの合計から表 A·3 に表される総計算量が得られる．

表 A·1 ユークリッド法における総計算量
Table A·1 Calculation amount of Euclid algorithm.

演算	計算量 [回]
積	$4t^2+6t+2$
和	$4t^2+4t+2$
逆元	$2t$

3.2 各誤り位置多項式導出法の装置量

3.2.1 ユークリッド法の装置量

除多項式，被除多項式及び商多項式の格納に必要なレジスタは，それぞれ $2t$, $2t+1$, t [cells] であり，商多項式から誤り位置多項式を導出するために，商多項式及び累積される多項式の格納にぞれぞれ t, $t+1$ [cells] のレジスタを必要とする．したがって，

$$7t+2 \quad [\text{cells}] \tag{A·14}$$

の装置量を必要とする．

3.2.2 Berlekamp-Massey 法の装置量 [3]

discrepancy の導出のために，レジスタ長 $t+1$ のシフトレジスタを用意しておく必要がある．したがって，シンドローム格納のための $t+1$ [cells]，及びタップ値格納のための t [cells] のレジスタを必要とする．また，新しいタップを構築するために必要な過去のタップの保存に t [cells] のレジスタを必要とする．合計で

$$3t+1 \quad [\text{cells}] \tag{A·15}$$

の装置量を必要とする．

3.2.3 Matrix-reduction 法の装置量

シンドロームを格納するための $((t+1) \times t)$ の行列分のレジスタのほかに，Matrix-reduction 法における行と列の転回をせず，ポインタを移動させることで同様の処理が可能であることから，変化させた位置の情報を保存しておく t [cells] のレジスタを必要とする．

表 A·2 Berlekamp-Massey 法における総計算量
Table A·2 Calculation amount of Berlekamp-Massey algorithm.

演算	計算量 [回]
積	$\frac{3}{2}t^2+2t$
和	$2t^2$
逆元	t

表 A·3 Matrix-reduction 法における総計算量
Table A·3 Calculation amount of Matrix-reduction algorithm.

演算	計算量 [回]
積	t^3+t^2-t
和	t^3-t
逆元	t

したがって

$$t^2 + 2t \quad [\text{cells}] \qquad \text{(A·16)}$$

の装置量を必要とする．

（平成 16 年 10 月 8 日受付，17 年 4 月 12 日再受付，
6 月 21 日最終原稿受付）

藤田　悠　（学生員）

平 13 信州大・工・電気電子卒．平 15 同大大学院工学系研究科前期課程了．同年同大学院工学系研究科後期課程入学．誤り訂正符号に関する研究に従事．

杉村　立夫　（正員）

昭 51 阪大・工・通信卒．昭 57 同大大学院博士後期課程了．工博．同年松下電器産業（株）入社．昭 60 福岡工大助教授．平 3 信州大・工・電気電子工学科助教授，現在教授．誤り訂正符号の構成及びその応用，有限体理論，情報セキュリティに関する研究に従事．情報理論とその応用学会，IEEE 各会員．

柴田　孝基　（正員）

平 5 信州大・工・電気電子卒．平 7 同大大学院博士前期課程了．同年日本無線（株）入社．平 8 信州大・大学院博士後期課程入学．平 11 同大大学院博士後期課程了．工博．現在，日本無線（株）研究開発部モバイル研究グループ勤務．地上ディジタル放送波中継 SFN 回り込みキャンセラ，及び同一チャネル干渉除去装置，並びに誤り訂正符号に関する研究に従事．