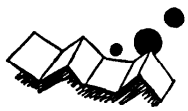
解　説

誤り検出・訂正符号の最近の動向†

——情報通信システムへの応用——



今　井　秀　樹††

1. まえがき

本稿は，昭和59年7月号本誌に掲載された同名の解説[1]の続編である．前回の解説では，誤り検出・訂正符号の理論（符号理論）の基礎として，誤りの検出・訂正の原理及び応用上重要な基本的誤り検出・訂正符号について述べ，次いで，計算機に応用されている符号を，主記憶などの高速記憶装置のためのものと，磁気テープや磁気ディスクなどの低速記憶装置のためのものとに分けて論じた．また，誤り検出・訂正符号の応用の今後の動向について概観した．

今回の解説は，前回の解説を受けて，誤り検出・訂正符号の計算機システムへの応用について，更に深く論じるとともに，関連他分野への応用にも言及する．まず，前回その重要性を指摘した **Reed-Solomon 符号**（**RS 符号**と略す）及び**畳込み符号**について解説し，次いで，通信及びオーディオ・ビデオ（**AV** と略す）の分野への誤り検出・訂正符号の応用について概説する．

なお，前回と同様，誤り検出符号と誤り訂正符号を総称して **ECC** と略称する．

2. RS 符号

RS 符号は応用上最も重要な符号であり，既にさまざまな分野で用いられているし，その応用範囲を更に拡大しつつある．これは，この符号が，後に述べるような意味で，効率が非常に良い符号であること，符号化・復号が半導体技術の進歩によって，比較的容易に行えるようになってきたことなどによる．

本章では，まず RS 符号による誤り訂正の原理とその復号法について，できるだけ直観的な説明を行い，次いで RS 符号の計算機への応用について述べる．

2.1 Galois 体[2),3)]

RS 符号を理解するには，**Galois 体**についてのある程度の知識が必要である．ここでは，ごく簡単に Galois 体について述べておこう．

Galois 体は体（field）の一種であるが，体そのものは，われわれにむしろ馴染み深いものである．というのは，加減乗除の四則演算がふつうに行えるのが体だからである．たとえば，実数全体の集合は体をなす．しかし，Galois 体は，そのような無限な元を持つ体ではなくて，有限個の元しか持たない体なのである．

元の数が q 個の Galois 体を GF(q) で表す．GF(q) は任意の q に対して存在するわけではなく，q が素数のべき乗のとき，またそのときに限って存在する．

応用上重要な Galois 体は GF(2^b)（b：正整数）である．以下，このような体について述べよう．

まず，GF(2) は，0, 1 に対し mod 2 の演算を行えばよい．つまり整数として演算し，結果が2以上になれば，2で割って余りをとるのである．

$b \geqq 2$ に対し，GF(2^b) は，GF(2) の元を係数とする b-1 次以下のすべての多項式を考え，元とする集合と考え，この多項式間の演算は mod $P(x)$ で演算すればよい．ただし，$P(x)$ は GF(2) の元を係数とする**既約多項式**（それ以上因数分解できない多項式）である．

一例として GF(2^2) を考えよう．この体の元は，0, 1, x, $x+1$ の四つであり，演算は2次の既約多項式 x^2+x+1 で mod をとって行えばよい．たとえば，$x\cdot(x+1)=x^2+x$ は x^2+x+1 で割って余りをとれば1となるから，$x\cdot(x+1)=1$ である．また，この結果は $x^{-1}=x+1$, $(x+1)^{-1}=x$ となることを意味している．これを用いれば除算も行える．

なお，GF(2^b) の元は，その多項式の係数だけを並べた長さ b の 0, 1 の系列で表すことがある．たとえば，0, 1, x, $x+1$ はそれぞれ 00, 01, 10, 11 のように表すのである．

† A Survey of Error-Detecting and Error-Correcting Codes with Emphasis on Their Applications to Information Systems by Hideki IMAI (Faculty of Engineering, Yokohama National University).

†† 横浜国立大学工学部電子情報工学科

2.2 RS 符号による誤り訂正の原理

α をある体 F に含まれ，n 乗するとはじめて1になる元とする．このような元を**1の原始 n 乗根と呼ぶ**．この α を用い，F の元からなる長さ n の系列 $\boldsymbol{w}=(w_0, w_1, \cdots, w_{n-1})$ に対し，

$$\tilde{w}_i=\sum_{j=0}^{n-1} w_j\alpha^{ij} \quad i=0, 1, \cdots, n-1 \qquad (1)$$

という $\boldsymbol{w}$ から $\tilde{\boldsymbol{w}}=(\tilde{w}_0, \tilde{w}_1, \cdots, \tilde{w}_{n-1})$ への変換を考えよう．このような変換を，一般に**フーリエ変換**と呼び，$\tilde{\boldsymbol{w}}$ を $\boldsymbol{w}$ の**スペクトル**という．

たとえば，F を複素数体とし，$\alpha=\exp(-2\pi i/n)$ とおけば，α は F における1の原始 n 乗根であり，(1)式の変換は，離数フーリエ変換となる．この場合，$\tilde{\boldsymbol{w}}$ は $\boldsymbol{w}$ の周波数スペクトルを与える．

どのような体 F においても，スペクトル $\tilde{\boldsymbol{w}}$ から

$$w_j=n^{-1}\sum_{i=0}^{n-1} \tilde{w}_i\alpha^{-ji} \quad j=0, 1, \cdots, n-1 \qquad (2)$$

によって，$\boldsymbol{w}=(w_0, w_1, \cdots, w_{n-1})$ を復元することができる．これを**フーリエ逆変換**という．

さて，ここで，**図-1**(a)に示すように，スペクトル $\tilde{\boldsymbol{w}}$ の r 個の成分 $\tilde{w}_0, \cdots, \tilde{w}_{r-1}$ までが0となるような $\boldsymbol{w}$ のみを用いて通信を行うという場合を考えよう．いわば，低周波成分は0として，高周波成分だけで通信を行おうというのである．

このとき，通信路で誤り（雑音）$\boldsymbol{e}=(e_0, e_1, \cdots, e_{n-1})$ が加わり，$\boldsymbol{y}=\boldsymbol{w}+\boldsymbol{e}$ が受信されるものとする．この誤りパターン $\boldsymbol{e}$ のスペクトルは，たとえば**図-1**(b)のようになっているであろう．

ここで，受信語 $\boldsymbol{y}$ のスペクトル $\tilde{\boldsymbol{y}}$ を求めれば，$\boldsymbol{w}$ のスペクトル $\tilde{\boldsymbol{w}}$ と $\boldsymbol{e}$ のスペクトル $\tilde{\boldsymbol{e}}$ が重なって，**図-1**(c)のようになるであろう．ところが，$\tilde{\boldsymbol{w}}$ は $i=0, \cdots, r-1$ の部分で0であるから，$\tilde{\boldsymbol{y}}$ の $i=0, \cdots, r-1$ の部分には，$\tilde{\boldsymbol{e}}$ のその部分がそのまま現れることになる．すなわち，

$$\tilde{y}_i=\tilde{e}_i=\sum_{j=0}^{n-1} e_j\alpha^{ij} \quad i=0, 1, \cdots, r-1 \qquad (3)$$

となる．このように，誤りパターンのスペクトルの一部は，受信語をフーリエ変換することにより得られるのである．

誤りパターンとして任意のものを考えるとすれば，誤りパターンのスペクトルの一部 $\tilde{e}_0, \cdots, \tilde{e}_{r-1}$ が得られても，それから誤りパターンを推定することはできない．しかし，誤りパターン $\boldsymbol{e}=(e_0, \cdots, e_{n-1})$ の非ゼロの成分が t 個以下であり，

$$2t \leqq r \qquad (4)$$

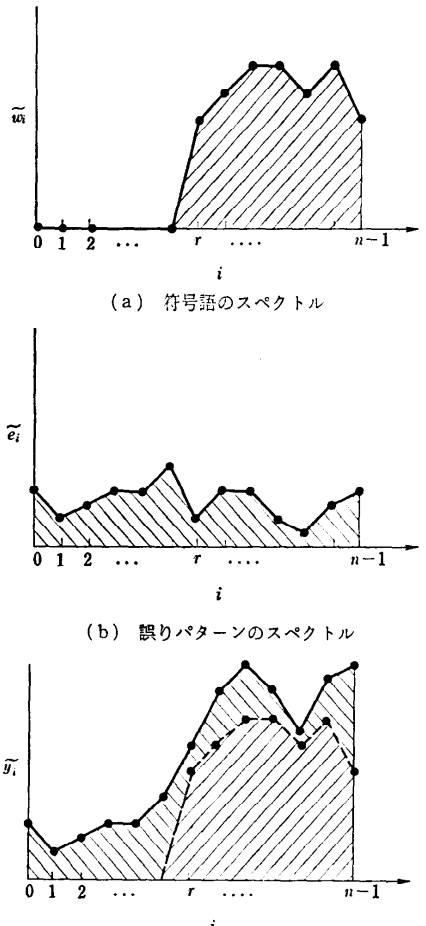


図-1 各種のスペクトル

が満たされるなら，$\tilde{e}_0, \cdots, \tilde{e}_{r-1}$ から誤りパターン $\boldsymbol{e}$ が一意に定まることが証明できる．

このことは，誤りの個数が $r/2$ 以下なら，受信語のスペクトルの一部 $\tilde{y}_0, \cdots, \tilde{y}_{r-1}$ から，誤りパターン $\boldsymbol{e}$ を推定でき，それによって誤りの訂正が行えることを意味している．なお，r が奇数の場合，$(r+1)/2$ 個の誤りは訂正はできないが，検出は可能である．

RS 符号は，以上のような原理に基づいて誤り訂正を行う符号である．以上の議論において，体 F は1の原始 n 乗根が存在しさえすればなんでもよい．しかし実用上重要であるのは，F が Galois 体，特に GF (2^s) の場合である．

GF(2^s) で定義された RS 符号の符号長 n は，GF(2^s) に1の原始 n 乗根が存在するように選ばねばならな

い．このためには，n が 2^b-1 の約数であることが必要十分であるが，通常は $n=2^b-1$ とする．

また，RS 符号の符号化は，原理的には，まず符号語 $\boldsymbol{w}$ のスペクトル $\tilde{\boldsymbol{w}}$ を，符号化すべき情報に従って定めることにより行える．$\tilde{\boldsymbol{w}}$ の r 個の成分 $\tilde{w}_0, \cdots, \tilde{w}_{r-1}$ は常に 0 としなければならないが，残りの $\tilde{w}_r, \cdots, \tilde{w}_{n-1}$ は任意である．そこで，この $n-r$ 個の成分を情報記号とすればよい．このように $\tilde{\boldsymbol{w}}$ を定め，それをフーリエ逆変換すれば，符号語 $\boldsymbol{w}$ が得られることになる．したがって，RS 符号の情報記号数は $n-r$，検査記号数は r である．

RS 符号は，同一の符号長と誤り訂正能力をもつ線形符号の中で，検査記号数が最小になるという意味で，きわめて効率の良い符号である．ただし，誤り訂正能力と検査記号数を同一に保ったままで，符号長を伸ばすことは可能である．どのような場合でも，少なくとも 2 だけは符号長を伸ばせる．このように符号長を伸ばした RS 符号を**拡大 RS 符号**と呼ぶ．

さて，GF(2^b) 上の RS 符号の符号語の各成分 w_i は GF(2^b) の元であるが，これを前節で述べたようにして，長さ b の 0, 1 の系列で表し，2 元符号として用いるのがふつうである．このとき，RS 符号は長さ b のバイト単位の誤りを訂正できる符号となる．前回の解説の表-2 は，拡大 RS 符号をこのように用いる場合について示したものである．

2.3 RS 符号の復号

RS 符号の復号は，受信語 $\boldsymbol{y}$ のスペクトル $\tilde{\boldsymbol{y}}$ の r 個の成分 $\tilde{y}_0, \cdots, \tilde{y}_{r-1}$ から誤りパターン $\boldsymbol{e}=(e_0, e_1, \cdots, e_{n-1})$ を推定するという過程で行われる．RS 符号の場合，$\tilde{y}_0, \cdots, \tilde{y}_{r-1}$ が**シンドローム**となるのである．

しかし，このシンドロームから直接 $\boldsymbol{e}$ を推定するのは難しい．そこで，$2l \leqq r$ となる l に対し，

$$\begin{bmatrix} \tilde{y}_{2l-2} & \tilde{y}_{2l-3} \cdots \tilde{y}_{l-1} \\ \tilde{y}_{2l-3} & \tilde{y}_{2l-4} \cdots \tilde{y}_{l-2} \\ \vdots & \vdots \\ \tilde{y}_{l-1} & \tilde{y}_{l-2} \cdots \tilde{y}_0 \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_l \end{bmatrix} = \begin{bmatrix} \tilde{y}_{2l-1} \\ \tilde{y}_{2l-2} \\ \vdots \\ \tilde{y}_l \end{bmatrix} \qquad (5)$$

を満たす $\sigma_1, \sigma_2, \cdots, \sigma_l$ を求める．もし，誤りの個数 t が，$2t \leqq r$ を満たすなら，$l=t$ のとき，この式は一意的な解を持ち，$l>t$ では一意的な解は持たない．したがって，l を $[r/2]$ から順次小さくしていって，この式を解いてみれば，$2t \leqq r$ である限り，一意的な解を求めることができる．なお，(5)式は **Yule-Walker 方程式**の形をしている．この方程式は信号処理の分野でも重要な役割を演ずる式であり，ECC と信号処理の間の関連を示すものとして興味深い．

さて，$\sigma_1, \sigma_2, \cdots, \sigma_t$ が求まったら

$$\sigma_1\alpha^{-j}+\sigma_2\alpha^{-2j}+\cdots+\sigma_t\alpha^{-tj}=1 \qquad (6)$$

を満たすすべての $j(0 \leqq j \leqq n-1)$ を求める．これはちょうど t 個存在し，誤りの位置を与える．これを $j_1, j_2, \cdots, j_t$ とおこう．

誤りの位置が判れば，それぞれの位置における誤りの値 $e_{j_1}, e_{j_2}, \cdots, e_{j_t}$ を求めるのは難しいことではない．このとき，シンドロームは

$$\tilde{y}_i=\sum_{l=1}^{t} e_{j_l}\alpha^{ij_l} \quad i=0, 1, \cdots, r-1 \qquad (7)$$

となっているはずである．これは $e_{j_1}, \cdots, e_{j_t}$ について一意的な解をもつ連立方程式であり，これを解けば $e_{j_1}, \cdots, e_{j_t}$ が求まる．これで，誤りパターン $\boldsymbol{e}$ が完全に定まるから，受信語を訂正できる．

以上は RS 符号の復号の原理を示したものである．実際の復号法は，誤り訂正能力によってかなり異なったものとなる．単一誤り訂正 RS 符号では，通常シンドロームから直接的に誤りの値と位置を求めてしまう．これについては，前回の解説の **2.4** 節で詳しく述べた．2〜3 重誤り訂正 RS 符号の場合は，Yule-Walker 方程式を数式的に解いておいて，シンドロームをその式に代入し $\sigma_1, \cdots, \sigma_t$ を求めることが多い．

しかし，誤り訂正能力の高い RS 符号の場合には，そのような方法は式が複雑になり過ぎて難しい．このため，シンドロームを求めた後，Yule-Walker 方程式を解いて $\sigma_1, \cdots, \sigma_t$ を求めることになる．その効率の良い解法として **Berlekamp-Massey アルゴリズム**（**BM アルゴリズム**と略す）や **Euclid の互除法**による方法が知られている[4]．これらの解法によって $\sigma_1, \cdots, \sigma_t$ を求める場合の計算量は t^2 に比例する．すなわち $O(t^2)$ である．これに対し，BM アルゴリズムや Euclid の互除法による復号法を改善し，計算量を $O(t \log^2 t)$ とした方法も提案されている[5),6)]．しかし，このような改善が有効となるためには，t はかなり大きくなくてはならない．実際的な t の範囲（数十以下）では，現在のところ，BM アルゴリズムが最も効率が良いようである．

なお，BM アルゴリズムや Euclid の互除法による復号法を実際に実現するには，さまざまな方法があり得る．その中で最近関心を集めているものに，シストリックアレイを用いて Euclid 互除法による復号を行おうという試みがある[7),8)]．この方法によれば，ハードウェア量はかなり大きくなるが，任意の誤り訂正能力をもつ GF(2^8) 上の RS 符号の復号を，10 Mbps 程度なら無理なく実現できるようである．

2.4 RS 符号の計算機システムへの応用

高速記憶装置用の ECC は，前回の解説で述べたように，符号化・復号の高速性などに対する要求が厳しく，ごく簡単なものしか使えない．このため，従来 RS 符号はあまり用いられなかったが，複数ビット（バイト）単位で生じる誤りに対する必要から，単一誤り訂正・2重誤り検出 (SEC/DED) RS 符号から構成された単一バイト誤り訂正・2重バイト誤り検出 (SbEC/DbED) 符号が用いられるようになってきた．現在用いられている符号は，GF(2^4) 上の SEC/DED-RS 符号から作られている．したがって，1バイト＝4ビットの SbEC/DbED 符号が得られる．ただし，RS 符号をそのまま用いたのでは，情報ビット数が最大48までしかとれないので，RS 符号をやや変形して (80, 64) SbEC/DbED 符号を導いている[9]．

このような SbEC/DbED 符号の実用例はまだ少ない．しかし，今後，半導体メモリの高集積化が更に進むにつれて，バイト誤り対策は一層重要性を増すと考えられるから，やがては，このような符号が，現在の SEC/DED 符号と同様に用いられるようになるであろう．

低速記憶装置には，最近 RS 符号から構成されるバイト誤り訂正符号が盛んに用いられるようになってきた．これについては，前回かなり詳しく述べたので重複を避け，ここではごく最近製品化された CD-ROM への応用についてみておこう．

CD-ROM はディジタルオーディオ用の CD（コンパクトディスク）を ROM（読出し専用記憶）として用いたものであり，片面 500 M バイト（1バイト＝8ビット）以上の記憶容量をもっている．

オーディオ用 CD には，**CIRC** (Cross Interleaved Reed-Solomon Code) と呼ばれる誤り訂正方式が用いられている[10]．これは，GF(2^8) 上の (28, 24) 及び (32, 28) の二つの（短縮化）RS 符号を用いる方式である．情報は，まず (28, 24) RS 符号に符号化される．次に，バースト誤りに対処するために，記号の順序を入れ替えた後，(32, 28) RS 符号に符号化される．このとき，冗長度は全体で 25% となる．

オーディオ用としては，CIRC は十分な誤り訂正能力を持っている．たとえば，CD のビット誤り率を 10^{-3} とすると，誤った訂正（誤訂正）を行う確率は約 10^{-13}，訂正はできないが検出は可能な誤りの生じる確率は約 10^{-6} である．ディジタルオーディオの場合，誤りを訂正できなくても，検出さえできれば，後に述べる補正という方法によって，音質を十分保ち得る場合が多い．したがって，まず問題となるのは，誤訂正の確率であるが，10^{-13} というのは，1日24時間用いて数年間で1回発生するかしないかの確率である．また，CD のビット誤り率も 10^{-3} までになることは滅多にないので，CIRC はオーディオ用としては，十分過ぎる程十分な能力をもつ方式である．

しかし，計算機用としては，その誤り訂正能力は十分ではない．そこで，CD-ROM では，CIRC で符号化した結果に，誤り検出のための CRC による検査ビットを付け，更にそれを GF(2^8) 上の (26, 24) 及び (45, 43) の二つの単一誤り訂正（短縮化）RS 符号によって2重に符号化を行っている．したがって結局，RS 符号で4重に符号化していることになる．(CRC も含めれば5重符号化を行っている．) この結果，誤り訂正のための冗長度は約 34% となるが，誤りを訂正できない確率はきわめて小さくなり，CD のビット誤り率が 10^{-3} のとき 10^{-20} 程度になると考えられている[11]．(全体として符号の構造がきわめて複雑となるので厳密な評価は難しい．)

この CD-ROM のように，訂正能力の低い RS 符号を，**多重符号化**して用いるという符号化法は，装置化が比較的簡単で，訂正能力の高い符号化が行えるという点で実用上優れた方式であり，今後も広く使われていくであろう．しかし，この方式は，効率という面では必ずしも良いとは言えない．誤りの性質によって事情が異なってくるので一概には言えないが，多くの場合，多重符号化を行うよりも，符号長が長く誤り訂正能力の高い一つの符号を用いる方が，小さい冗長度で同等の復号特性を得ることができる．訂正能力の高い RS 符号の復号には，BM アルゴリズムなどを用いねばならず装置化は複雑となるが，通信やオーディオの分野ではそのような符号が採用され始めており，やがては計算機の低速記憶装置にも用いられると思われる．

3. 畳込み符号

前回の解説で述べたように，畳込み符号は，ランダム誤りの訂正に関し，ブロック符号よりも優れた性質を示す．本章では，この符号について概説し，計算機システムへの応用の可能性について論じる．

3.1 畳込み符号の基礎概念[12]

畳込み符号を扱う場合には，系列 $x_0x_1x_2\cdots$ を

$$X(D)=x_0+x_1D+x_2D^2+\cdots \qquad (8)$$

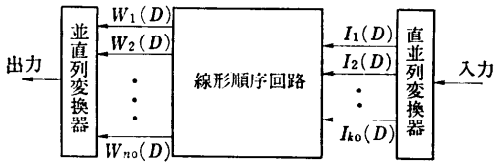


図-2 畳込み符号器

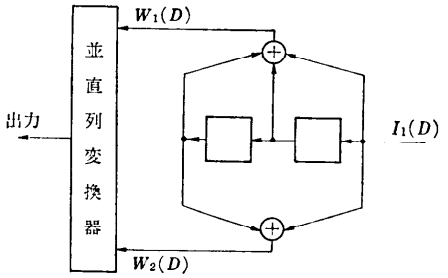


図-3 畳込み符号器の例

のように D の多項式で表すと便利である．D は1単位時間のずれを表すと考えられるから，**遅延演算子**と呼ばれる．

畳込み符号の符号器は，**図-2** に示すように，k_0 個の情報系列 $I_1(D), \cdots, I_{k_0}(D)$ を n_0 個の符号系列 $W_1(D), \cdots, W_{n_0}(D)$ に変換する回路が中心となっている．この回路は記憶を持ち，線形である．すなわち，線形順序回路である．この回路は，もし記憶がなければ，ブロック符号の並列符号器にほかならないが，畳込み符号の場合，ブロック長 n_0 はきわめて小さく，2, 4 ないし8程度である．なお，ブロック符号の場合と同様，k_0/n_0 を**情報率**と呼ぶ．

ここで，**図-3** に示す畳込み符号器を考えよう．これは，情報率 1/2 の畳込み符号の符号器である．この符号器で符号化される符号系列は

$$\left.\begin{aligned} W_1(D) &= G_{11}(D)I_1(D) \\ W_2(D) &= G_{12}(D)I_1(D) \end{aligned}\right\} \qquad (9)$$

と表せる．ここに

$$\left.\begin{aligned} G_{11}(D) &= 1+D+D^2 \\ G_{12}(D) &= 1+D^2 \end{aligned}\right\} \qquad (10)$$

であり，これらは**生成多項式**と呼ばれる．

一般には，情報率 k_0/n_0 の畳込み符号の符号系列は生成多項式 $\{G_{ij}(D) | i=1, \cdots, k_0,\ j=1, \cdots, n_0\}$ を用いて，次のように表せる．

$$W_j(D) = \sum_{i=0}^{k_0} G_{ij}(D)I_i(D) \quad j=1, \cdots, n_0 \qquad (11)$$

畳込み符号器は，線形順序回路であるから，その動作を**状態図**を用いて表すことができる．例として，

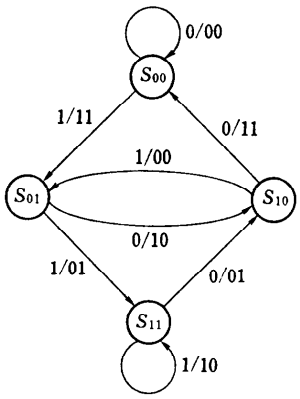


図-4 畳込み符号器の状態図の例

図-3の符号器の状態図を示せば，**図-4** のようになる．この図は，たとえば S_{00} という状態についてみると，この状態で入力0であれば00を出力し，同じ状態に留まり，入力が1であれば11を出力し，状態 S_{01} に遷移するということを表している．

さて，畳込み符号の重要なパラメータとして**拘束長** (constraint length) がある．これは，さまざまな定義があり，かなり混乱して用いられているが，ここでは，1ブロックの k_0 個の情報ビットが直接影響を及ぼし得るブロックの数と定義しておこう．生成多項式を用いて言えば，$G_{ij}(D)$ の中で次数が最大なものの次数 +1 が拘束長ということになる．図-3 の畳込み符号では，拘束長は3となる．

拘束長を K とすれば，畳込み符号器に含まれる記憶素子の数は（符号器が無駄なく設計されているなら），$(K-1)k_0$ 以下であるが，たいていの場合，ちょうど $(K-1)k_0$ である．このとき，状態図の状態の数は $2^{(K-1)k_0}$ となる．

また，並直列変換された後の符号系列について言えば，一つのブロックの情報ビットは n_0K ビットに影響を与えることになる．符号器の装置化の複雑さという観点から見ると，この n_0K がブロック符号の符号長に相当するものと考えてよい．そこで，これらを同一にし，更に情報率も一致させて，畳込み符号とブロック符号を比較すると，畳込み符号の方が数倍高い誤り訂正能力を持つことが知られている．しかも，畳込み符号の場合，次節で述べる Viterbi 復号などの優れた復号法を適用できるため，その差は更に開く．

3.2 畳込み符号の復号

畳込み符号は，ブロック符号とは異なり，符号の構

造ではなく，復号法によって分類するのが適当である．畳込み符号の復号法としては，しきい値復号法，シンドロームパターンによる復号法，Viterbi 復号法，逐次復号法の四つがある．

しきい値復号法は，非常に簡単な復号法であるが，これが適用可能な符号は効率があまり良くない．

シンドロームパターンによる復号法は，ごく簡単なランダム誤り訂正符号，あるいはバースト誤り訂正符号に用いられる．これも装置化は容易である．

Viterbi 復号法は，拘束長が短ければ，どのような畳込み符号にも適用できる．また，ランダム誤りに対しては，正しく復号できる確率を最大にするという意味で**最適な復号法**である．(ただし，厳密な意味で最適なのは，情報系列が0,1を等確率で含むランダムな系列の場合である．) 加えて，**軟判定復号**という方法を用いることにより，復号特性を更に向上させることができる．

通信路の出力は本来アナログ波形であるが，通常はこれを0か1のいずれかに硬判定してから復号を行う．これに対し，軟判定復号では，アナログ的な情報を残し，それを利用して，より確度の高い復号を行うのである．ブロック符号では，軟判定復号を行うのはかなり難しいが，畳込み符号の Viterbi 復号では，これが比較的容易に実現できる．

しかし，Viterbi 復号法は，受信系列に最も近い系列を，状態図の中で探索していくという方法で行われるので，状態数 $2^{(K-1)k_0}$ があまり大きくなると実現不可能となってくる．実際上，$(K-1)k_0$ が10以下でなければ装置化は難しい．現在よく用いられているのは，$(K-1)k_0=6$ のものである．

このように制約はあるが，Viterbi 復号はきわめて強力な復号法であるし，$(K-1)k_0=6$ 程度の場合には，かなり高速な復号 (10 Mbps 以上) が行えるので，通信の分野では盛んに用いられている．

逐次復号 (sequential decoding) は，同一の畳込み符号では Viterbi 復号よりも復号特性はやや劣化するが，拘束長のより長い符号に適用できる．ただし，装置化はそう簡単ではないし，高速な復号も難しい．

3.3 畳込み符号の計算機システムへの応用

前述のように，畳込み符号，特に，Viterbi 復号による畳込み符号は，通信には盛んに用いられているが，計算機への応用はほとんどないようである．

畳込み符号は，並列処理には向かないから，高速記憶装置への応用は考えにくい．しかし，低速記憶装置へは，十分応用可能であると思われる．

これまで，低速記憶装置にも応用されなかったのは，畳込み符号はデータ長が短い場合には十分にその能力を発揮できないこと，通信で用いられている畳込み符号の多くは情報率が 1/2 であり，これは記憶装置ではやや低いこと，Viterbi 復号はバースト誤りに対処しにくいこと，などによるのであろう．しかし，データ長が数百ビット以上であれば，畳込み符号は十分その力を発揮する．また，最近では，情報率 3/4 以上の高情報率畳込み符号も実用化されようとしているし[13]，そのような符号の復号の簡単化法も見出されている[14),15]．バースト誤りに対しても，交錯法をうまく利用すれば，十分対処し得るであろう．更に，Viterbi 復号は，変調方式と一体化して考えることが可能であり，誤り訂正方式と変調方式の総合的最適化を図り得る可能性がある．特に，多値伝送，多値記録の場合に威力を発揮する[16]．

以上のような点から，畳込み符号の Viterbi 復号は，計算機の記憶装置にも，今後の高密度記録の誤り訂正方式として採用される可能性が十分あると思われる．

4. ECC の通信への応用[17)~22)]

本章では，はじめの2節で，ECC の通信への応用に特徴的な問題について論じ，次いで**4.3** で ECC の応用が特に顕著な分野について述べる．

4.1 ARQ と FEC

通信では，帰還通信路を利用できることが多い．この場合，誤り検出符号を用い，誤りを検出したら帰還通信路を通して再送を要求するという **ARQ** (Automatic Repeat Request) 方式を用い得る．従来，通信における誤り制御としては，この方式が主流であったし，今後も，この方式が重要であることは変りない．

しかし，かつては装置化が複雑になり過ぎるとしてあまり用いられることのなかった，誤り訂正符号を用い受信側で誤りの訂正を行う **FEC** (Forward Error Correction) 方式が，LSI 技術の進歩とともに，広く利用されるようになってきた．

FEC は，送信側に符号器，受信側に復号器を置きさえすればよいわけだから，システムの制御という面では，ARQ より簡単であるし，遅延も少ない．しかし，達成し得る信頼度という点では，ARQ に一歩譲る．

したがって，もとの情報が音声や画像などで，ある

程度の誤りが許容されるような場合には FEC を用い，計算機通信など高い信頼性を要求される場合には ARQ を用いるのが適当であろう．しかし，後者の場合でも，まず FEC を用いて誤り率を軽減し，そのうえで ARQ を適用するのが最近の傾向である．更に，FEC と ARQ を一体化したハイブリッド方式も検討されている．

4.2 通信ネットワークと ECC

最近では，一つの通信ネットワーク内のさまざまな部分に ECC が用られるようになってきた．この場合，用いられる部分に適した ECC を設計する必要がある．

たとえば，ECC をネットワークのノード間のリンクに用いる場合，その符号器，復号器は変復調器と同じ場所に置かれることが多い．この場合は，軟判定復号を用い得る．また，変復調と誤り訂正を一体化して考えることもできる．このような点を考慮して ECC を選択すべきであろう．

これに対し，ユーザ間 (end to end) で ECC を用いる場合には，軟判定復号の適用は難しい．しかし，一方，ユーザ間の合意によって，それぞれのアプリケーションに要求される通信品質を確保するような ECC を選択することができる．

しかし，通信ネットワークの中で ECC をどのように用いるべきかという問題は，まだ十分な検討は行われてはいない．今後の重要な課題と言えよう．

4.3 FEC の応用例

ARQ の通信への応用は枚挙にいとまがない．ここでは，最近急速に拡大しつつある FEC のいくつかの応用例について簡単に述べておこう．

(a) 衛 星 通 信

衛星通信では，往復の遅延がかなり大きいから，ARQ を用いるのは難しく，FEC が比較的古くから用いられていた．

衛星通信では，ランダム誤りが主体であるので，ランダム誤り訂正符号が用いられる．また，衛星の送信電力や搭載するアンテナの大きさに制限があるために，通信路の誤り率は比較的高く，訂正能力の高い符号を用いることが望ましい．更に，衛星通信の場合，データ伝送速度が非常に高いことが多いので，符号化，復号が高速に行える必要がある．

このような点から衛星通信には，大きな訂正能力の得られる情報率 1/2，拘束長 $K=7$ 程度の畳込み符号を用い Viterbi 復号を行う方式が採用されることが多い．しかし，最近では，衛星通信の周波数帯域もかなり制約されるようになってきた．このため，より情報率の高い畳込み符号や BCH 符号なども用いられている．

(b) 放送への応用

放送では，通常帰還通信路は存在しないから，誤り制御のためには FEC を用いざるを得ない．現在実用化されているディジタル放送としては，テレビジョンの文字放送，衛星放送の音声などがあり，これらにはいずれも FEC が用いられている．

放送の場合，誤りは，ランダム誤りと比較的短いバースト誤りが主体である．また，復号器は家庭内の受像機に組み込まれるから，できるだけ簡単なものでなければならない．

このような点から，Hamming 符号や符号長の短い 2 重誤り訂正 BCH 符号などが用いられているが，我が国の文字放送には，(272, 190) 差集合巡回符号が採用された[23]．この符号は 8 個の誤りをすべて訂正し，9 個の誤りのほとんどを訂正する強力な符号であるが，復号は簡単で，既に LSI 化されている．

(c) 移動通信への応用

ディジタル移動通信においては，通常 ARQ などの誤り制御方式も用い得るが，一般に通信路のビット誤り率が非常に高いので，ARQ だけでは再送ばかり繰り返され，効率が著しく悪い．このため，なんらかの FEC が併用される．

移動通信において問題となる誤りは，フェージングによって引き起こされるバースト誤りである．また，周波数帯域がかなり厳しく制限されているので，情報率も高いことが望ましい．更に，符号器，復号器は移動体に搭載するので，小型軽量でなければならない．

現在，ディジタル移動通信には，バースト誤り訂正畳込み符号やバースト誤り訂正巡回符号が用いられているが，まだ ECC 応用の初期段階にある．しかし，ディジタル移動通信は，将来大きな発展が予想される分野であり，いずれは ECC の最大の応用分野の一つになると思われる．

5. ECC の AV 機器への応用[10),17),18),24)]

AV の分野において，**PCM** (Pulse Code Modulation) によるディジタル方式が採用されるようになったのは比較的最近のことである．しかし，その後の発展は目覚しく，ディジタルオーディオ機器である CD プレーヤは，既に従来のアナログプレーヤを上まわる

売上げ高を示している.

この分野においては, ECC の応用が, その当初から考えられていた. はじめは計算機の低速記憶装置の技術を導入していたのであるが, その後独自の発展を遂げ, 現在では逆に, この分野で開発されたものが計算機に用いられるようになってきている.

5.1 オーディオへの応用

ディジタルオーディオ機器にはさまざまなものがあるが, ECC 応用の主たる対象となるのは, 記録機器である.

ディジタルオーディオ用記録機器には, 一般に記録密度が高く, このため誤り率も高いものが多い. したがって, 訂正能力の高い符号を用いる必要がある. ただし, オーディオデータの場合, すべての誤りを訂正するという必要はない. 隣接するデータの間の相関が強いので, 誤りを検出したとき, それが訂正できなくても, 前後のデータからかなり正確に推定できるからである. このような方式を**誤り補正**という.

前後に正しいデータがあれば, 誤り補正を行っても聴感上ほとんど問題とならない. しかし, 連続したデータに誤りが生じた場合, それをすべて補正で回復するのは不可能である. したがって, ある程度は誤り訂正を行い, 補正の対象となるデータが連続しないようにする必要がある.

一方, あまり無理をして訂正を行うと, 誤訂正の確率が高くなる. 誤訂正が生じると, クリック音が発生し, 音質を著しく劣化させる. したがって, 誤訂正の可能性が高い場合には, 誤り検出に止め, 補正を行う方がよい.

このように, ECC のオーディオ機器への応用においては, 誤り訂正と補正の兼合いをどのようにするかが重要な問題となる.

また, オーディオ機器においては, ランダム誤りとバースト誤りがともに発生するものが多い. このため, オーディオ機器の誤り制御としては, RS 符号系の符号を交錯して用いる方式が主流となっている. 更に, 高い誤り訂正能力を得るため, 2重に符号化することが多い. 2.4節で述べた CD 用の CIRC は, その例である. また, **DAT** (ディジタルオーディオテープ) の実験仕様に用いられている符号もそうである. DAT では, CD の場合よりも訂正能力の高い4重誤り訂正 RS 符号が採用されている. これは, 今後の一つの方向を示すものであろう.

5.2 ビデオへの応用

ECC の応用の対象となるビデオ機器としては, ディジタル VTR がある. これに対する ECC の応用は, ディジタルオーディオ機器への応用と同様の特徴を持っている. オーディオの場合と異なる点は, 誤訂正や補正の確率に対する条件が緩いこと, 符号化, 復号がきわめて高速でなければならないことである.

このため, 現在のところ, あまり誤り訂正能力の高い符号は使えないが, やはり, RS 符号を2重符号化して用いる方式が主流となりつつある.

6. むすび

前回の解説に引き続き, 計算機を中心とする情報通信システムへの ECC の最近の応用について論じた. 特に, 応用上最も重要と考えられる RS 符号及び今後計算機への応用が期待される畳込み符号については, かなり詳しく述べた.

前回と今回の解説を通し, ECC の応用すべてを語り尽したわけではない. 特に, 誤り検出・訂正の効果の評価の問題は重要であるが, ほとんど触れることができなかった. もっとも, この問題は, 例外的な場合を除いて非常に難しい問題であり, 完成した理論があるわけではない.

しかし, 前回と今回の解説によって, 情報通信システムへの応用という観点から見たときの, 現在の ECC 研究開発の主要な流れをつかんでいただけたのではないかと思う. ECC は, その重要性の割には, あまり知られていない面が多い. 本稿が, ECC への理解を少しでも拡げることになれば筆者として最大の喜びとするところである.

参考文献

1) 今井秀樹：誤り検出・訂正符号の最近の動向—計算機への応用を中心として, 情報処理, Vol. 25, No. 27, p. 688 (1984).
2) 今井秀樹：情報数学, 昭晃堂 (1982).
3) 今井秀樹：コンパクトディスクとガロア, SUT Bulletin, Vol. 2, No. 8, p. 7 (1985).
4) 杉山康夫：ユークリッド整除法を用いたテプリッツシステムの解法 その1, 信学技報 IT 84-13 (1984).
5) Justesen, J: On the Complexity of Decoding Reed-Solomon Codes, IEEE Trans. Inf. Theory, Vol. IT-22, No. 2, p. 237 (1976).
6) Blahut, R.E: Theory and Practice of Error Control Codes, Addison-Wesley (1983).
7) Brent, R.P. and Kung, H.T.: Systolic VLSI

Arrays for Polynomial GDC Computation, IEEE Trans. Comput., Vol. C-33, No. 8, p. 731 (1984).
8) 木村，今井，土肥：シストリックアルゴリズムに基づく Reed-Solomon 符号の復号器の構成法，信学技報 AL 84-76 (1985).
9) Kaneda, S. and Fujiwara, E.: Single Byte Error Correcting-Double Byte Error Detecting Codes for Memory Systems, IEEE Trans. Comput. Vol. C-31, No. 7, p. 596 (1982).
10) 土井，伊賀：ディジタルオーディオ，ラジオ技術社 (1982).
11) 佐古，鈴木，古谷，古川：CD-ROM のデータクオリティについて，信学技報 IT 85-31 (1985).
12) Viterbi, A. J. and Omura, J. K.: Principle of Digital Communication and Coding, McGraw-Hill (1979).
13) 平田，高畑，安永，安田：国際ビジネス衛星通信用 TDMA システムに関する考察，信学技報 SAT 84-4 (1984).
14) 安田，平田，小川：ヴィタビ復号の容易な高符号化率たたみ込み符号とその諸性質，信学論(B)，Vol. J 64-B, No. 7, p. 573 (1981).
15) 山田，原島，宮川：トレリスを用いた高符号化率畳込み符号の新しい最尤復号法，信学論(A)，Vol. J 66-A, No. 7, p. 611 (1983).
16) Ungerboeck, G.: Channel Coding with Multi-Level/Phase Signals, IEEE Trans. Inf. Theory, Vol. IT-28, No. 1, p. 55 (1982).
17) 今井秀樹：誤り訂正符号化技術の応用，信学誌，Vol. 67, No. 10, p. 1094 (1984).
18) 今井秀樹監修：誤り訂正符号化技術の要点，日本工業技術センター (1986).
19) Wiggert, D.: Error-Control Coding and Applications, Artech House (1978).
20) Clark, Jr. G. C. and Cain, J. B.: Error-Correction Coding for Digital Communications, Plenum Press (1981).
21) Lin, S. and Costello, Jr. D. J.: Error-Control Coding, Prentice-Hall (1983).
22) Michelson, A. M. and Levesque, A. H.: Error-Control Techniques for Digital Communication, John Wisley & Sons (1985).
23) 山田 幸：符号化伝送方式文字放送誤り訂正符号，信学論(B)，Vol. J 67-B, No. 4, p. 439 (1984).
24) 平野，江藤：ディジタル VTR の誤り訂正，修整方式，テレビ誌，Vol. 35, No. 7, p. 549 (1981).

(昭和 60 年 8 月 26 日受付)