

交代式符号の代数的な構造と最小距離復号法に関する考察

三 浦 晋 示

中 村 勝 洋

日本電気株式会社 C & C 情報研究所

交代式符号は、Reed-Solomon 符号 (RS 符号)、一般化 Reed-Solomon 符号、更にはそれら Maximum Distance Separable 符号の部分体部分符号として得られる BCH 符号、Goppa 符号・・・などの広範囲な符号群からなる符号 (の総称) である。本稿では、この交代式符号、特に Reed-Solomon 符号、BCH 符号の代数的構造について調べ、その復号法における代数的諸量 (予想する誤り多項式、シンドローム多項式、拡張シンドローム、誤り位置多項式、誤り評価多項式など) の諸関係について新たに整理し直し、従来の代数的復号アルゴリズムを見通しよく整理し位置づける。更にこれらの代数的諸量が満たすべき条件を、最小距離復号の観点からいくつか与え、復号時におけるその有用性について述べる。

Notes on the algebraic structure of alternant codes
and their minimum distance decoding algorithms

Shinji Miura

Katsuhiro Nakamura

C & C Information Technology Research Laboratories, NEC Corporation
4-1-1, Miyazaki, Miyamae-ku, Kawasaki City, 213, Japan

Alternant codes are known as a large and powerful family of codes, such as BCH codes, Goppa codes, Reed-Solomon codes and generalized Reed-Solomon codes. In this paper, we investigate the algebraic structure of alternant codes (especially, Reed-Solomon codes and BCH codes) and give some relations among such algebraic quantities as error polynomials, syndrome polynomials, generalized syndromes, error location polynomials and error evaluation polynomials. We also derive some useful "necessary and sufficient" conditions on these algebraic quantities which give an insight of the algebraic structure of alternant codes from the viewpoint of minimum distance decoding.

1. はじめに 交代式符号はReed-Solomon符号、一般化Reed-Solomon符号、更にはそれらMDS (Maximum Distance Separable)符号の部分体部分符号として得られるBCH符号、Goppa符号・・・などの広範囲な符号群からなる符号 (の総称) である ([2])。

本稿ではこの交代式符号の代数的構造について、特に、その復号法における代数的諸量 (予想する誤り多項式、シンδροーム多項式、拡張シンδροーム、誤り位置多項式、誤り評価多項式など) の構造、諸関係について整理し直し、最小距離復号の観点から、これらの諸量が満たすべき必要十分条件を与える。それによって、従来の代数的復号アルゴリズムを見通しよく整理し位置づける。この観点からBCH符号の良く知られている代数的復号アルゴリズムを眺めたとき、このアルゴリズムは、いまやBCH符号のために独立に開発されたものと考えられるよりも、それを部分体部分符号として含むReed-Solomon符号 (以下RS符号と記す) における復号アルゴリズムをそのまま適用したものと考えべきであり、当然BCH符号の構造も、基礎体を固定したままで符号長を伸ばすことを目的に考え出された部分体部分符号との見方が最も自然である。それは必要な符号長に応じた定義を持つあるRS符号の部分符号、すなわちRS符号の受信語空間において基礎体の固定のために受信語空間自体に制限を加えることに伴って必然的に符号語が限定された符号、としての構造を持つ ([2])。それゆえにこの見地からBCH符号の従来からある復号アルゴリズムを解析するなら、目的・必要に応じては一部の機能は省略されることはあるものの、受信語に対する復号処理それ自体は本質的にはRS符号の復号アルゴリズムに全く一致するものであることが云える。同様な議論はGoppa符号などの一般の交代式符号の現在知られている復号アルゴリズムについても云え、それらはそれを部分体部分符号として含むある一般化RS符号における代数的復号アルゴリズムをそのまま適用するものである。また、この一般化RS符号は適当な線形変換によってRS符号とみなせるのでそれらの復号アルゴリズムも容易に類推される ([2], p365)。そこで本稿では紙面の都合上、まずはRS符号に関して考察を進め、上記代数的諸量の構造、諸関係について新たに整理し直し、次いでその部分体部分符号として得られるBCH符号に関する結果をRS符号での結果を踏まえた上で展開することにとどめる。

ところで受信者が、一般的に真に発生した誤りを受信語 $u(X)$ のみから推定することは如何なる符号化によっても勿論不可能である。そこで本稿では、受信語空間のそれぞれの受信語 $u(X)$ に対して “最小距離復号の意味の誤り (以下ではこれを “予想する誤り” と呼ぶ)” に対応する “誤り多項式 $E(X)$ ” を集合

$\{E(X) : E(X) \text{ は受信語多項式 } u(X) \text{ に対し、}$

条件 “ $u(X) - E(X)$ は符号語多項式”、のもとでHamming重みを最小とするもの}

に含まれる要素として明確に定義し、この集合の元 $E(X)$ を、与えられた受信語多項式 $u(X)$ から効率良く導き出すことを最終の目標とする。

なお、本稿では、多項式 $\sigma(X), \eta(X) \in GF(q^n)[X]$ の任意の組 $(\sigma(X), \eta(X))$ に対して同値関係 $(\sigma_1(X), \eta_1(X)) \sim (\sigma_2(X), \eta_2(X))$ を、 $\exists \lambda (\neq 0) \in GF(q^n), \sigma_1(X) = \lambda \cdot \sigma_2(X)$ かつ $\eta_1(X) = \lambda \cdot \eta_2(X)$ で定義し、以後この関係により多項式の組としての等号を表すこととする。また記述の簡素化のため多項式の組 $(\sigma(X), \eta(X))$ に対して、その次数を、 $\deg(\sigma(X), \eta(X)) = \max\{\deg \sigma(X), \deg \eta(X) + 1\}$ で定義し、集合 Γ に対して $\#\Gamma$ は元の個数を表すとする。

2. Reed-Solomon符号 有限体 $GF(q^n)$ の元 $\alpha \neq 0$ を固定し、乗法群 $GF(q^n)^* = GF(q^n) \setminus \{0\}$ の元としての α の位数を n と置くと、符号長 n のReed-Solomon符号 (RS符号) は、次の様にして定義される。

$GF(q^n)[X] / ((X^n - 1) \cdot GF(q^n)[X])$ を受信語空間とする巡回符号で、
 $g(X) = (X - \alpha^1) \cdot (X - \alpha^{r+1}) \cdots (X - \alpha^{r+d-2}) \in GF(q^n)[X]$ をその生成多項式とする符号。定義終了。

RS符号は $GF(q^n)$ 上の $(n, n-d+1, d)$ -MD S符号をなす ([2])。

従来の復号手順の明確化 さて、受信語空間の元である受信語 $u(X)$ を一つ任意に固定したとき、

“予想する誤り” に対応する誤り多項式 $E(X)$ の一つを、 $E(X) = e_{j1}X^{j1} + e_{j2}X^{j2} + \cdots + e_{jk}X^{jk}$ とする。

このとき、 $E(X)$ を使って $GF(q^n)[X]$ に含まれる二つの多項式を

$$\sigma(X) = \prod_{i=1}^k (1 - \alpha^{ji} X) \quad , \quad \eta(X) = \sum_{i=1}^k e_{ji} \alpha^{r+ji} \prod_{s=1}^k (1 - \alpha^{js} X)$$

として定義し、これらをそれぞれ “予想する誤り” に対応して定まる誤り位置多項式、誤り評価多項式と呼ぶ。

さて逆に、ここで定義された多項式の組 $(\sigma(X), \eta(X))$ が、ある何等かの手順 (如何なる方法でも良い) によって導き出されたとするなら。

$$\text{“予想する誤り”} : E(X) = e_{j1}X^{j1} + e_{j2}X^{j2} + \cdots + e_{jk}X^{jk}$$

は、容易に確かめられるように

$$\sigma(X) = 0 \text{ の } GF(q^n) \text{ の解 } \alpha^{-ji}, i = 1, \dots, k \text{ を使って、 } e_{ji} = -\alpha^{(1-r) \cdot ji} \eta(\alpha^{-ji}) / \sigma'(\alpha^{-ji})$$

と再現される。ただし、ここで $\sigma'(X)$ は $\sigma(X)$ の形式的微分を表す。

この事実、“予想する誤り” $E(X)$ を決定することすなわち復号が、多項式の組 $(\sigma(X), \eta(X))$ を導き出すことに帰着されることを示している。

それ故、任意に多項式の組 $(\sigma(X), \eta(X))$ が与えられたとき、それが求める “予想する誤り” $E(X)$ に対応して定まる誤り位置多項式と誤り評価多項式の組に一致するか否かを判定するための必要十分条件 (必要条件は従来から良く知られている) を、直接 $E(X)$ を経由しない表現で提示しておく事は重要な意味を持つ。そこで、まずこれを実行し、その結果として従来の復号手順を見通しよく整理しなおす。そこでは従来、不明確にされていた、受信語がどの符号語の訂正可能勢力圏内 (設計距離=最小距離で保証される半径 $[(d-1)/2]$ 以内) にも含まれていない場合の判定すなわち、“誤り検出”の方法を与え、更にこれを一歩進めて、その場合にも最小距離復号を実行する復号手順も与える。

さて、“予想する誤り” に対応して定まる誤り位置多項式 $\sigma(X)$ と誤り評価多項式 $\eta(X)$ の特定問題に戻るが、そのためにそれらと受信語多項式 $u(X)$ との仲立ちの役割をするSyndrome多項式を次のように定義する。

$$S(X) = S_0 + S_1 X + S_2 X^2 + \cdots + S_{d-2} X^{d-2}$$

$$S_0 = u(\alpha^1), \quad S_1 = u(\alpha^{r+1}), \quad \dots, \quad S_{d-2} = u(\alpha^{r+d-2})$$

ここで特に注意すべきことは、後で述べるように、“予想する誤り” に対応する誤り多項式 $E(X)$ を決定するための情報のすべては、受信語多項式から導かれるこの $d-2$ 次のSyndrome多項式 $S(X)$ に過不足なく受け継が

れているということである。この事実から、“予想する誤り”に対応する誤り位置多項式 $\sigma(X)$ と誤り評価多項式 $\eta(X)$ は Syndrome 多項式 $S(X)$ にのみ依存して特徴付けられ、それは次のように定式化される（十分条件でもあることに注意、証明略）。

定理 1 多項式の組 $(\sigma(X), \eta(X)) \in (GF(q^n)[X]) \times (GF(q^n)[X])$ がそれぞれ “予想する誤り” に対応する誤り位置・誤り評価多項式であるための必要十分条件は

- I $\sigma(X) \cdot S(X) \equiv \eta(X) \pmod{X^{d-1}}$.
- II $\Gamma = \{\alpha^{-i} \in GF(q^n) : \sigma(\alpha^{-i}) = 0\}$ と置くと、 $\#\Gamma = \deg \sigma(X)$ 、すなわち、 $\sigma(X) = 0$ は $GF(q^n)^*$ で一次因子に分解し、重根を持たない。
- III $\deg \sigma(X) > \deg \eta(X)$ 。
- IV 上の I、II、III を満たす多項式の組全体の中で $\deg \sigma(X)$ が最小。 \square

“予想する誤り” が一意に定まらない場合には、当然 $(\sigma(X), \eta(X))$ も一意には定まらない、その場合には $(\sigma(X), \eta(X))$ の全体は複数の要素からなる集合をなす。

さて、定理によって “予想する誤り” に対応して定まる誤り位置多項式と誤り評価多項式の組 $(\sigma(X), \eta(X))$ は明確に定式化されたので、これらを効率的に求めるためのアルゴリズムの具体的な構成が次の課題となろうが、これに関連しては Berlekamp-Massey algorithm と Euclid algorithm と呼ばれる二つの代表的なアルゴリズムが既によく知られている。以下ではこれらを復号の目的と一旦切り離して単にアルゴリズムとして見たとき、いったい何を実行するものであるかと云うことを見る。本稿では、つぎの二つのアルゴリズムを引用する。

これらは共に任意に $k-1$ 次の多項式 $S(X) \in GF(q^n)[X]$ を入力すると、それぞれに次の条件を満たす多項式の組 $(\sigma(X), \eta(X)) \in (GF(q^n)[X]) \times (GF(q^n)[X])$ を出力する。

任意に与えられた多項式 $S(X) \in GF(q^n)[X]$ (実質的には $\deg S(X) \leq k-1$ の部分) に対して、

Berlekamp-Massey algorithm ([3], p124. 注: [1], p184. とは本質的に異なる部分がある) は

次の条件を満たす、ある二つの多項式の組 $(\sigma_B(X), \eta_B(X))$ を導き出す ([5] など)

- I $\sigma_B(X) \cdot S(X) \equiv \eta_B(X) \pmod{X^k}$
 - II $\sigma_B(0) \neq 0$ ($\sigma_B(0) = 1$)
 - III I、II を満たす多項式全体の中で $\deg(\sigma_B(X), \eta_B(X))$ が最小
- Euclid algorithm ([4]) は、前もって定める $0 \leq t \leq k-1$ に対して
- 次の条件を満たす、唯一に定まる多項式の組 $(\sigma_E(X), \eta_E(X))$ を導き出す ([4])
- I $\sigma_E(X) \cdot S(X) \equiv \eta_E(X) \pmod{X^k}$
 - II $\sigma_E(X) \neq 0$ ($\sigma_E(X)$ は monic)、 $\deg \sigma_E(X) \leq t$ 、 $\deg \eta_E(X) \leq k-t-1$
 - III g.c.d($\sigma_E(X), \omega(X)$) = 1、ただし $\omega(X)$ は $\sigma_E(X) \cdot S(X) = \eta_E(X) + \omega(X) \cdot X^k$

ここで、 $k = d-1$ 、 $t = \lfloor (d-1)/2 \rfloor$ とおくと、よく知られているように

定理 2 ([1], [2]) 予想する誤りに対応する誤り多項式 $E(X)$ の Hamming 重みが $\lfloor (d-1)/2 \rfloor$ 以内のときには (無論、真に発生した誤りの Hamming 重みが $\lfloor (d-1)/2 \rfloor$ 以内のときを含む)、 $E(X)$ とそれに対応する誤り位置多項式 $\sigma(X)$ 、誤り評価多項式 $\eta(X)$ は共に一意に定まり、

$$(\sigma_B(X), \eta_B(X)) = (\sigma(X), \eta(X))$$

$$(\sigma_E(X), \eta_E(X)) = (\sigma(X), \eta(X)) \quad \text{が成立する。} \quad \square$$

この事実から、どちらのアルゴリズムを使用してもランダムな $\lfloor (d-1)/2 \rfloor$ シンボル以内の誤りまでは、誤りの訂正は完全に保証されたことになる。次の段階の問題は、 $\lfloor (d-1)/2 \rfloor$ を超えた誤りが発生したときにそれを旨く判定する条件を求め、さらにはその場合にも最小距離復号を実行する手順を与えることである ([1], 231. [6])。

その前に、任意に与えられた入力多項式 $S(X) \in GF(q^n)[X]$ に対して Berlekamp-Massey algorithm、Euclid algorithm のそれぞれの出力結果を $(\sigma_B(X), \eta_B(X))$ 、 $(\sigma_E(X), \eta_E(X))$ とするとき、それらの間の関係を与えておく。

$d = 2 \cdot t_1 + 1$ の場合。 $k = d-1 = 2 \cdot t_1$ 、 $t = t_1$ としてアルゴリズムを作動する。

定理 3 次の三つの条件は同値である

- 1. $(\sigma_B(X), \eta_B(X)) \neq (\sigma_E(X), \eta_E(X))$
- 2. $\deg(\sigma_B(X), \eta_B(X)) > t_1$
- 3. $\sigma_E(0) = 0$

(証明略) \square

$d = 2 \cdot t_1 + 2$ の場合。 $k = d-1 = 2 \cdot t_1 + 1$ とする。 $t = t_1$ 、 $t = t_1 + 1$ としたときの Euclid algorithm の出力をそれぞれ $(\sigma_{E1}(X), \eta_{E1}(X))$ 、 $(\sigma_{E2}(X), \eta_{E2}(X))$ とおく。

定理 4

$\deg(\sigma_B(X), \eta_B(X)) \leq t_1$ ならば、 $(\sigma_B(X), \eta_B(X)) = (\sigma_{E1}(X), \eta_{E1}(X)) = (\sigma_{E2}(X), \eta_{E2}(X))$ 。

$\deg(\sigma_B(X), \eta_B(X)) = t_1 + 1$ ならば、

$$\deg(\sigma_{E1}(X), \eta_{E1}(X)) = \deg(\sigma_{E2}(X), \eta_{E2}(X)) = t_1 + 1.$$

か、または $(\sigma_{E1}(X), \eta_{E1}(X)) = (\sigma_{E2}(X), \eta_{E2}(X))$ 、 $\deg(\sigma_{E1}(X), \eta_{E1}(X)) \leq t_1$ 、 $\sigma_{E1}(0) = \sigma_{E2}(0) = 0$ 。

$\deg(\sigma_B(X), \eta_B(X)) > t_1 + 1$ ならば、 $\sigma_{E1}(0) = \sigma_{E2}(0) = 0$ 。

(証明略) \square

定理 3、定理 4 の諸関係は、 t_1 を超える “予想する誤り” の検出にも利用できる。

RS 符号の構造解析と、それに伴う最小距離復号の実現。

さて、RS 符号の (巡回符号としての) 構造は、次の短完全系列により特徴付けられる。

$$0 \longrightarrow (g(X) \cdot GF(q^n)[X]) / ((X^n - 1) \cdot GF(q^n)[X]) \longrightarrow GF(q^n)[X] / ((X^n - 1) \cdot GF(q^n)[X]) \longrightarrow$$

$$v(X) \longmapsto \longrightarrow v(X), u(X) \longmapsto \longrightarrow$$

$$\longrightarrow GF(q^n)[X] / (g(X) \cdot GF(q^n)[X]) \longrightarrow 0 \quad (\text{exact}).$$

$$\longrightarrow u(X) \pmod{g(X)}$$

ここで $(g(X) \cdot GF(q^n)[X]) / ((X^n-1) \cdot GF(q^n)[X])$: 符号語空間
 $GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X])$: 受信語空間、エラー空間
 $GF(q^n)[X] / (g(X) \cdot GF(q^n)[X])$: (巡回符号としての) シンドローム空間

であり、この自然に定義された短完全系列は、“予想する誤り”に対応する誤り多項式 $E(X)$ を決定するための情報のすべてを、受信語多項式 $u(X)$ から導かれるこの $d-2$ 次の巡回符号としてのシンドローム多項式 $u(X) \bmod g(X)$ に過不足なく受け継ぐことを示す。

さて、 $u(X) \in GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X])$: 受信語多項式
 $e(X) \in GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X])$: エラー多項式
 $E(X) \in GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X])$: 予想するエラー多項式
 $v(X) \in (g(X) \cdot GF(q^n)[X]) / ((X^n-1) \cdot GF(q^n)[X])$: 送信語多項式
 $V(X) \in (g(X) \cdot GF(q^n)[X]) / ((X^n-1) \cdot GF(q^n)[X])$: 予想する符号語多項式
 に関して、 $u(X) = e(X) + v(X)$ 、 $u(X) = E(X) + V(X)$ であり、

エラー空間に関する以下の有限体上の離散フーリエ変換、

$$\begin{aligned} GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X]) &\xrightarrow{\quad} \prod_{i=0}^{n-1} GF(q^n)[X] / ((X - \alpha^{r+i}) \cdot GF(q^n)[X]) \\ e(X) &\xrightarrow{\quad} (e(\alpha^r), \dots, e(\alpha^{r+n-1})) \\ &\xrightarrow{\quad} GF(q^n)^n \\ &\xrightarrow{\quad} (e(\alpha^r), e(\alpha^{r+1}), \dots, e(\alpha^{r+n-1})) \\ &\xrightarrow{\quad} GF(q^n)[X] / (X^n \cdot GF(q^n)[X]) \\ &\xrightarrow{\quad} a(X) = e(\alpha^r) + e(\alpha^{r+1})X + \dots + e(\alpha^{r+n-1})X^{n-1} \end{aligned}$$

は中国人の剰余定理から同型写像となる。この同型対応からエラー多項式 $e(X)$ に対して

$e(\alpha^{r+i}) = a_i$, ($i = 0, 1, \dots, n-1$) と置くと

$e(X) = a_0 + a_1X + a_2X^2 + \dots + a_{n-1}X^{n-1}$

は一対一に対応することが示される。これから、 $e(X)$ を決定するためには a_0, a_1, \dots, a_{n-1} はそのすべてを決定する必要があることが分かる。すなわち、そのどれが欠けても $e(X)$ の決定に自由度が残る。この $a(X)$ を、拡張シンドロームと呼ぶ。また、つぎの同型写像によってシンドローム多項式 $S(X)$ と、シンドローム空間 $GF(q^n)[X] / (X^{d-1} \cdot GF(q^n)[X])$ が定義される。

$$\begin{aligned} GF(q^n)[X] / (g(X) \cdot GF(q^n)[X]) &\xrightarrow{\quad} \prod_{i=0}^{d-2} GF(q^n)[X] / ((X - \alpha^{r+i}) \cdot GF(q^n)[X]) \\ u(X) \bmod g(X) &\xrightarrow{\quad} (u(\alpha^r), \dots, u(\alpha^{r+d-2})) \\ &\xrightarrow{\quad} GF(q^n)^{d-1} \\ &\xrightarrow{\quad} (u(\alpha^r), u(\alpha^{r+1}), \dots, u(\alpha^{r+d-2})) \\ &\xrightarrow{\quad} GF(q^n)[X] / (X^{d-1} \cdot GF(q^n)[X]) \\ &\xrightarrow{\quad} S(X) = u(\alpha^r) + u(\alpha^{r+1})X + \dots + u(\alpha^{r+d-2})X^{d-2} \end{aligned}$$

これは受信語多項式 $u(X)$ に対する巡回符号としてのシンドローム $u(X) \bmod g(X)$ とシンドローム多項式 $S(X)$ とのあいだの同型対応を与える。

さらに、受信語多項式 $u(X)$ 、エラー多項式 $e(X)$ 、拡張シンドローム $e(\alpha^r) + e(\alpha^{r+1})X + \dots + e(\alpha^{r+n-1})X^{n-1}$ 、巡回符号としてのシンドローム $u(X) \bmod g(X)$ とシンドローム多項式 $u(\alpha^r) + u(\alpha^{r+1})X + \dots + u(\alpha^{r+d-2})X^{d-2}$ の間で成り立つ、つぎの完全系列は可換な図式をなし、自然な対応関係を与える。

$$\begin{array}{ccccc} GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X]) & \xrightarrow{\quad} & GF(q^n)[X] / (g(X) \cdot GF(q^n)[X]) & \xrightarrow{\quad} & 0 \quad \text{exact} \\ \downarrow & & \downarrow & & \\ GF(q^n)[X] / (X^n \cdot GF(q^n)[X]) & \xrightarrow{\quad} & GF(q^n)[X] / (X^{d-1} \cdot GF(q^n)[X]) & \xrightarrow{\quad} & 0 \quad \text{exact} \end{array}$$

$$\begin{array}{ccc} u(X) = e(X) + v(X) & \xrightarrow{\quad} & u(X) \bmod g(X) = e(X) \bmod g(X) \\ e(X) & \xrightarrow{\quad} & e(X) \bmod g(X) \\ \downarrow & & \downarrow \\ e(\alpha^r) + e(\alpha^{r+1})X + \dots + e(\alpha^{r+n-1})X^{n-1} & \xrightarrow{\quad} & e(\alpha^r) + e(\alpha^{r+1})X + \dots + e(\alpha^{r+d-2})X^{d-2} \\ & & = u(\alpha^r) + u(\alpha^{r+1})X + \dots + u(\alpha^{r+d-2})X^{d-2} \end{array}$$

さてここで、任意の $e(X) = e_{j1}X^{j1} + e_{j2}X^{j2} + \dots + e_{jk}X^{jk} \in GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X])$ に対して $GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X])$ に属する二つの多項式を

$$\sigma(X) = \prod_{i=1}^k (1 - \alpha^{ji}X) \quad , \quad \eta(X) = \sum_{i=1}^k e_{ji} \alpha^{r-ji} \prod_{s \neq i} (1 - \alpha^{js}X)$$

として定義して、 (σ, η) 多項式と呼ぶ。

ここで、集合 $\mathcal{E} \subset (GF(q^n)[X]) \times (GF(q^n)[X])$

を、次の二つの条件を満たす多項式の組 $(\sigma(X), \eta(X))$ の全体として定義する

$$I \quad \Gamma = \{\alpha^{-i} \in GF(q^n) : \sigma(\alpha^{-i}) = 0\} \text{ と置くととき、} \# \Gamma = \deg \sigma(X), \quad \prod \deg \sigma(X) > \deg \eta(X), \quad (n \geq \deg \sigma(X))$$

すると、上の $e(X)$ から $(\sigma(X), \eta(X))$ への対応は、エラー空間 $GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X])$ から

(σ, η) 多項式空間 \mathcal{E} への全単射であることが示される。その逆写像は

$\sigma(X) = 0$ の $GF(q^n)$ 上の解 $\Gamma = \{\alpha^{-j1}, \alpha^{-j2}, \dots, \alpha^{-jk}\}$ を使って

$$e_{ji} = -\alpha^{(1-r)-ji} \eta(\alpha^{-ji}) / \sigma'(\alpha^{-ji}) \quad , \quad e(X) = e_{j1}X^{j1} + e_{j2}X^{j2} + \dots + e_{jk}X^{jk}$$

で与えられる。

さてここで、受信語多項式 $u(X)$ を一つ固定する。すると、上のエラー多項式、 (σ, η) 多項式、拡張シンδροームはそれらの空間の中で、それぞれに次のような制限を受ける。

① エラー多項式

$e(X) \in GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X])$ としては、 $u(X) = e(X) + v(X)$
 $v(X) \in (g(X) \cdot GF(q^n)[X]) / ((X^n-1) \cdot GF(q^n)[X])$ 、と表されるものだけ。

② 対応する (σ, η) 多項式は

$\sigma(X) \cdot S(X) \equiv \eta(X) \pmod{X^{d-1}}$ 、を満たす $(\sigma(X), \eta(X)) \in \mathcal{E}$ だけ。

③ 対応する拡張シンδροームは

$a(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} \in GF(q^n)[X] / (X^n \cdot GF(q^n)[X])$

としては、 $a_0 = S_0, a_1 = S_1, \dots, a_{d-2} = S_{d-2}$ を満たすもの。

この定式化により受信語 $u(X)$ が確定したときの誤り多項式 $e(X)$ の不確定度が明確になり、敢えて誤りの発生確率を考慮に入れないならば、 $e(X)$ は $GF(q^n)$ 上に $n-d-1$ 次の自由度があることも再確認できた。それ故、勿論真に発生した誤りを受信語 $u(X)$ のみから完全に導き出す事は不可能となる。

そこでその代わりとして、誤りの発生確率を考慮に入れて $e(X)$ に一致する可能性の最も高いものの候補として、最小距離復号の意味で決定される“予想する誤り” $E(X)$ を、受信語空間のおおのの受信語 $u(X)$ に対して明確に定義したのである。さて、このとき $E(X)$ に対応するものは、次の様に特徴付けられる。

① “予想する誤り” のエラー多項式

$E(X) \in GF(q^n)[X] / ((X^n-1) \cdot GF(q^n)[X])$ の中で、 $u(X) = E(X) + v(X)$ 、

$v(X) \in (g(X) \cdot GF(q^n)[X]) / ((X^n-1) \cdot GF(q^n)[X])$ と表され、 $E(X)$ の重みが最小なもの。

② 対応する (σ, η) 多項式は

$\sigma(X) \cdot S(X) \equiv \eta(X) \pmod{X^{d-1}}$ を満たす $(\sigma(X), \eta(X)) \in \mathcal{E}$ の中で、 $\deg \sigma(X)$ の最小なもの。

③ 対応する拡張シンδροーム

$a(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} \in GF(q^n)[X] / (X^n \cdot GF(q^n)[X])$ の中で、

$a_0 = S_0, a_1 = S_1, \dots, a_{d-2} = S_{d-2}$ を満たし、 $a_{d-1}, a_d, a_{d+1}, \dots, a_{n-1}$ は、

条件②で決定される $(\sigma(X), \eta(X)) \in \mathcal{E}$ に対して $\sigma(X) \cdot a(X) \equiv \eta(X) \pmod{X^n}$ を満たすもの。

ここに至って、我々は $[(d-1)/2]$ を超えた誤りが発生したときにそれを判定し、最小距離復号を実行する手順を与えることができる。

まず $[(d-1)/2] = t_1, k = d-1, t = t_1$ として、シンδροーム多項式 $S(X)$ を入力とした Berlekamp-Massey algorithm と Euclid algorithm の出力結果をそれぞれ $(\sigma_B(X), \eta_B(X))$ 、 $(\sigma_E(X), \eta_E(X))$ とおく、このとき、これらが予想する誤りに対応する誤り位置多項式、誤り評価多項式の組 $(\sigma(X), \eta(X))$ に一致するか否かに関して

定理 5 つぎの二つの条件は同値である (証明略)

1. $(\sigma_B(X), \eta_B(X)) = (\sigma(X), \eta(X))$ 2. $\deg(\sigma_B(X), \eta_B(X)) = \# \Gamma, \Gamma = \{\beta \in GF(q^n) : \sigma_B(\beta) = 0, \beta \neq 0\}$ □

同様に

定理 6 つぎの二つの条件は同値である (証明略)

1. $(\sigma_E(X), \eta_E(X)) = (\sigma(X), \eta(X))$ 2. $\deg(\sigma_E(X), \eta_E(X)) = \# \Gamma, \Gamma = \{\beta \in GF(q^n) : \sigma_E(\beta) = 0, \beta \neq 0\}$ □

が成り立つ。すなわち、どちらのアルゴリズムを使用した場合でも定理 5、定理 6 の条件の 2. の判定により、予想する誤りに対応する誤り多項式を、その出力された多項式の組から再現することが可能であるか、或は不可能であるかが判断できる。尚、この判定は従来の復号手順の中に自然に組み込める。

それは、集合 $\Gamma = \{\beta \in GF(q^n) : \sigma(\beta) = 0, \beta \neq 0\}$ を

Chien search により求めた時点でその個数を $\deg(\sigma(X), \eta(X))$ と比較すればよい。

つぎに、 t_1 を超える誤りが発生した場合にも最小距離復号を実行する方法を与える。

それには、 a_{d-1} を、 $GF(q^n)$ の変数として変化させ、シンδροーム多項式を $s_0 + s_1X + \dots + s_{d-2}X^{d-2} + a_{d-1}X^{d-1}$ に拡張して Berlekamp-Massey 或は Euclid のいずれかのアルゴリズムに入力して、その出力結果に定理 5、定理 6 の条件の 2. の判定を施して誤り多項式の再現を試みればよい。

それでも駄目な場合には a_{d-1}, a_d を変数としてシンδροーム多項式を $s_0 + s_1X + \dots + s_{d-2}X^{d-2} + a_{d-1}X^{d-1} + a_dX^d$ に拡張してアルゴリズムを作動してその出力結果にやはり定理 5、定理 6 の条件の 2. の判定を施して誤り多項式の再現を試みる。なおそれでも駄目な場合には a_{d-1}, a_d, a_{d+1} を変数として \dots 、以上の動作を続けるならば必ずいつかは最小距離復号が実現される。

3. BCH 符号

$n \mid (q^m-1)$ として n を固定するとき、自然数 i を含み q, n に付随する (q, n) サイクル Π_i を

$\Pi_i := \{i \cdot q^j \pmod n : j \in \mathbb{N}\}$ で定義する。このとき、 $\alpha \in GF(q^m)$ を位数が n の元とすると、つぎはよく知られている。

I α^k の $GF(q)[X]$ での最小多項式を $h_k(X)$ と置くと
 $h_k(X) = \prod_{j \in \Pi_k} (X - \alpha^j)$ 。このとき $\# \Pi_k = \deg h_k(X)$ で、これは m の約数となる。

II 任意の整数 i, j に対して $\Pi_i = \Pi_j$ である事と、
 α^i と α^j の $GF(q)[X]$ 上での最小多項式が一致することは同値である。

III α の $GF(q)[X]$ での最小多項式を $h(X)$ と置くと、 $n \mid (q^s-1)$ を満たす最小の自然数 s に対して
 $GF(q)[X] / (h(X) \cdot GF(q)[X]) \cong GF(q^s) \subset GF(q^m)$

重要なのは α が原始元 (すなわち $n = q^m - 1$) の場合であるので、今後はこれを仮定し α に付随する原始多項式を $f(X) \in GF(q)[X]$ とおく。

IV α^k の $GF(q)[X]$ での最小多項式を $h_k(X)$ と置き、
 $\deg h_k(X) = \# \Pi_k = s$ とするとき、自然な埋め込み写像が以下のように定義される。

このとき、 $s = m$ でない限りこの埋め込み写像は全射でないことを注意しておく。

さて、つづいてBCH符号をRS符号の部分体部分符号として定義する。BCH符号の受信語空間は、RS符号としての定義体 $GF(q^n)$ に対して基礎体を $GF(q)$ に落とすためにRS符号の受信語空間を

そして、これに伴って符号語空間も限定され、 $GF(q)[X] / ((X^n - 1) \cdot GF(q)[X])$ が単項 id 環を成すことから $(g(X) \cdot GF(q^m)[X]) / ((X^n - 1) \cdot GF(q^m)[X]) \cap GF(q)[X] / ((X^n - 1) \cdot GF(q)[X]) = (h(X) \cdot GF(q)[X]) / ((X^n - 1) \cdot GF(q)[X])$ となり巡回符号を成す。ただし、 $h(X)$ は $g(X) = (X - \alpha^r) \cdot (X - \alpha^{r+1}) \cdots (X - \alpha^{r+d-2}) \in GF(q^m)[X]$ に対応する $\alpha^r, \alpha^{r+1}, \dots, \alpha^{r+d-2}$ に関しての $GF(q)[X]$ での最小多項式 $h(X) = \prod_{j \in J} (X - \alpha^j)$ である (ここで、 $J = \bigcup_{i=0}^{d-2} J_i + r$)。

$$\Gamma = \{c(r), c(r+1), \dots, c(r+d-2)\} \subset \mathbb{Z}_n, \quad h(X) = \prod_{k \in \Gamma} h_k(X),$$

ここで	$(h(X) \cdot GF(q)[X]) / ((X^n - 1) \cdot GF(q)[X])$: 符号語空間
	$GF(q)[X] / ((X^n - 1) \cdot GF(q)[X])$: 受信語空間、エラー空間
	$GF(q)[X] / (h(X) \cdot GF(q)[X])$: (巡回符号としての本来の) シンドローム空間。
さて、	$u(X) \in GF(q)[X] / ((X^n - 1) \cdot GF(q)[X])$: 受信語多項式
	$e(X) \in GF(q)[X] / ((X^n - 1) \cdot GF(q)[X])$: エラー多項式
	$E(X) \in GF(q)[X] / ((X^n - 1) \cdot GF(q)[X])$: 予想するエラー多項式
	$v(X) \in (g(X) \cdot GF(q)[X]) / ((X^n - 1) \cdot GF(q)[X])$: 送信語多項式
	$V(X) \in (g(X) \cdot GF(q)[X]) / ((X^n - 1) \cdot GF(q)[X])$: 予想する符号語多項式

$S(X) = S_0 + S_1 X + S_2 X^2 + \cdots + S_{d-2} X^{d-2}$ で定義される。

$$\begin{aligned} e(X) \in \text{GF}(q)[X] / \langle (X^n - 1) \cdot \text{GF}(q)[X] \rangle &\xrightarrow{\quad} \text{GF}(q^n)[X] / \langle (X^n - 1) \cdot \text{GF}(q^n)[X] \rangle \\ &\xrightarrow{\quad} \prod_{i=0}^{n-1} \text{GF}(q^n)[X] / \langle (X - \alpha^{r+i}) \cdot \text{GF}(q^n)[X] \rangle \\ &\xrightarrow{\quad} \text{GF}(q^n)^n \\ &\xrightarrow{\quad} \text{GF}(q^n)[X] / \langle (X^n \cdot \text{GF}(q^n)[X]) \rangle \end{aligned}$$

それは、つぎの、包含写像とRS符号での同型写像から求められる。

《 6 》

$$\xrightarrow{\quad} \Pi_{i=0}^{d-2} GF(q^n)[X] / ((X - \alpha^{r+i}) \cdot GF(q^n)[X])$$

$$\xrightarrow{\quad} (u(X) \bmod (X - \alpha^r), \dots, u(X) \bmod (X - \alpha^{r+d-2}))$$

$$\xrightarrow{\quad} GF(q^n)^{d-1}$$

$$\xrightarrow{\quad} (u(\alpha^r), u(\alpha^{r+1}), \dots, u(\alpha^{r+d-2}))$$

$$\xrightarrow{\quad} GF(q^n)[X] / (X^{d-1} \cdot GF(q^n)[X])$$

$$\xrightarrow{\quad} S(X) = u(\alpha^r) + u(\alpha^{r+1})X + \dots + u(\alpha^{r+d-2})X^{d-2}$$

すなわち $GF(q^n)[X] / (X^{d-1} \cdot GF(q^n)[X])$ の任意の元が、実際にある受信語多項式 $u(X)$ から導かれるシンドロームに一致するための必要十分条件はその係数、 S_0, S_1, \dots, S_{d-2} を使って次のように与えられる。

I S_i と S_j に関して、 $\Pi(r+i) = \Pi(r+j)$ のときは $r+i = (r+j) \cdot q^k + n \cdot t$ ($k, t \in \mathbb{Z}$) と書くとき $(S_j)^{q^k} = S_i$ を満たす。

II S_i の i に関して $\Pi(r+i) = s$ と置くと、 S_i は $GF(q^n)$ の部分体 $GF(q^s)$ を動くのみ。

ただし、ここでの $GF(q^s)$ は $GF(q)$ ($\subset GF(q^n)$) 上 α^{r+i} で生成される体。

以上のことから BCH 符号のシンドロームを表現する空間は $GF(q^n)[X] / (X^{d-1} \cdot GF(q^n)[X])$ であるものの、その自由度は $GF(q)$ 上に d^* となることがその構造と共に確認された。

更にまた RS 符号のときと同様に、 $e(X) = e_{j1}X^{j1} + e_{j2}X^{j2} + \dots + e_{jk}X^{jk} \in GF(q)[X] / ((X^n-1) \cdot GF(q)[X])$ に対して $GF(q^n)[X]$ に属する二つの多項式を

$\sigma(X) = \prod_{i=1}^k (1 - \alpha^{ji}X)$ 、 $\eta(X) = \sum_{i=1}^k e_{ji} \alpha^{r+ji} \prod_{s \neq i} (1 - \alpha^{js}X)$

として定義して、やはり (σ, η) 多項式と呼ぶ。

ここで、集合

$\mathcal{E}_B \subset (GF(q^n)[X]) \times (GF(q^n)[X])$

を、次の三つの条件を満たす多項式の組 $(\sigma(X), \eta(X))$ の全体として定義する

I $\Gamma = \{\alpha^{-i} \in GF(q^n) : \sigma(\alpha^{-i}) = 0\}$ と置くと $\#\Gamma = \deg \sigma(X)$ 、II $\deg \sigma(X) > \deg \eta(X)$, ($n \geq \deg \sigma(X)$)

III $\sigma(X) = 0$ の解 $\Gamma = \{\alpha^{-j1}, \alpha^{-j2}, \dots, \alpha^{-jk}\}$ に対して、 $e_{ji} = -\alpha^{(1-r) \cdot ji} \eta(\alpha^{-ji}) / \sigma'(\alpha^{-ji})$ を導くとき $e_{ji} \in GF(q)$

すると、上の $e(X)$ から $(\sigma(X), \eta(X))$ への対応は、エラー空間 $GF(q)[X] / ((X^n-1) \cdot GF(q)[X])$ から

\mathcal{E}_B への全単射であることが示され、その逆写像は $\sigma(X) = 0$ の $GF(q^n)^*$ 上の解 $\Gamma = \{\alpha^{-j1}, \alpha^{-j2}, \dots, \alpha^{-jk}\}$ を使って $e_{ji} = -\alpha^{(1-r) \cdot ji} \eta(\alpha^{-ji}) / \sigma'(\alpha^{-ji})$ 、

$e(X) = e_{j1}X^{j1} + e_{j2}X^{j2} + \dots + e_{jk}X^{jk} \in GF(q)[X] / ((X^n-1) \cdot GF(q)[X])$ で与えられる。

尚、上の条件 III は、次の条件 III' に置き換えてもよい

III' $A(X) = \eta(X) / \sigma(X) \bmod X^n$ と置くと、 $A(X) \in \mathbb{F}$

さてここで、RS 符号のときと同様に“予想する誤り” $E(X)$ を一つ固定する。すると、以上の三つはそれらの空間の中で、それぞれに次の様な制限を受ける。

① エラー多項式

$e(X) \in GF(q)[X] / ((X^n-1) \cdot GF(q)[X])$ としては、 $u(X) = e(X) + v(X)$ 、 $v(X) \in (h(X) \cdot GF(q)[X]) / ((X^n-1) \cdot GF(q)[X])$ と、表されるものだけ。

② (σ, η) 多項式は

$\sigma(X) \cdot S(X) \equiv \eta(X) \bmod X^{d-1}$ 、を満たす $(\sigma(X), \eta(X)) \in \mathcal{E}_B$ だけ。

③ 拡張シンドローム

$a(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} \in GF(q^n)[X] / (X^n \cdot GF(q^n)[X])$

としては、 $a_0 = S_0, a_1 = S_1, \dots, a_{d-2} = S_{d-2}$ で、さらに、 $a(X) \in \mathbb{F}$ を満たすもの。

さて、RS 符号の場合と同様に“予想する誤り” $E(X)$ が定義されるが、

BCH 符号の場合の $E(X)$ の特徴付けは次の様になる

① エラー多項式

$E(X) \in GF(q)[X] / ((X^n-1) \cdot GF(q)[X])$ としては $u(X) = E(X) + v(X)$ 、

$v(X) \in (h(X) \cdot GF(q)[X]) / ((X^n-1) \cdot GF(q)[X])$ と表され、 $E(X)$ の重みが最小なもの。

② (σ, η) 多項式は

$\sigma(X) \cdot S(X) \equiv \eta(X) \bmod X^{d-1}$ 、を満たす $(\sigma(X), \eta(X)) \in \mathcal{E}_B$ の中で、 $\deg \sigma(X)$ の最小なもの。

③ 拡張シンドローム

$a(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} \in GF(q^n)[X] / (X^n \cdot GF(q^n)[X])$

としては、 $a_0 = S_0, a_1 = S_1, \dots, a_{d-2} = S_{d-2}$ を満たし、かつ、 $a(X) \in \mathbb{F}$ 。

更に、 $a_{d-1}, a_d, a_{d+1}, \dots, a_{n-1}$ は条件②の (σ, η) に対して $\sigma(X) \cdot a(X) \equiv \eta(X) \bmod X^n$ を満たす。

特に、条件②からは RS 符号の場合と同様に“予想する誤り”に対応する誤り位置多項式 $\sigma(X)$ と誤り評価多項式 $\eta(X)$ の組が、Syndrome 多項式 $S(X)$ にのみ依存して特徴付けられるという次の定理を得る。ここで、注意しなければならないことはエラー空間の違いから RS 符号の場合と BCH 符号の場合では当然、予想する誤りが異なるということである。

定理 7 多項式の組 $(\sigma(X), \eta(X)) \in GF(q^n)[X] \times GF(q^n)[X]$ がそれぞれ“予想する誤り”に対応する誤り位置・誤り評価多項式であるための必要十分条件は (証明略、 $S(X)$ と (σ, η) 多項式の定義が異なるが部分的に [6] 参照)

I $\sigma(X) \cdot S(X) \equiv \eta(X) \bmod X^{d-1}$

II $\Gamma = \{\alpha^{-i} \in GF(q^n) : \sigma(\alpha^{-i}) = 0\}$ と置くと、 $\#\Gamma = \deg \sigma(X)$

III $\deg \sigma(X) > \deg \eta(X)$

IV $\sigma(X)=0$ のゼロ以外の解 $\Gamma = \{\alpha^{-j_1}, \alpha^{-j_2}, \dots, \alpha^{-j_k}\}$ に対して
 $e_{ji} = -\alpha^{(1-r) \cdot j_i} \eta(\alpha^{-j_i}) / \sigma'(\alpha^{-j_i})$ を導くとき、 $e_{ji} \in GF(q)$

V 上のI、II、III、IVを満たす多項式の組全体の中で $\deg \sigma(X)$ が最小。□

この定理に基づいて、設計距離 d に対してBCH符号の場合にも $[(d-1)/2]$ を超えた誤りの発生を判定し、その場合にも最小距離復号を実行する手順を与えることができる。但し、この手順は文献[1],[6]に記された手順とは異なる。まず $[(d-1)/2] = t_1$, $k = d-1$, $t = t_1$ として、シンドローム多項式 $S(X)$ を入力としたBerlekamp-Massey algorithmとEuclid algorithmの出力結果をそれぞれ $(\sigma_B(X), \eta_B(X))$, $(\sigma_E(X), \eta_E(X))$ とおく、このとき、これらが予想する誤りに対応する誤り位置多項式、誤り評価多項式の組 $(\sigma(X), \eta(X))$ に一致するか否かに関して、つぎの二つの定理が成り立つ。(証明略)

定理 8 つぎの二つの条件は同値である

1. $(\sigma_B(X), \eta_B(X)) = (\sigma(X), \eta(X))$
2. I $\deg(\sigma_B(X), \eta_B(X)) = \#\Gamma$, $\Gamma = \{\beta \in GF(q^m) : \sigma_B(\beta) = 0, \beta \neq 0\}$
 II $\Gamma = \{\alpha^{-j_1}, \alpha^{-j_2}, \dots, \alpha^{-j_k}\}$ に対して $e_{ji} = -\alpha^{(1-r) \cdot j_i} \eta_B(\alpha^{-j_i}) / \sigma'_B(\alpha^{-j_i})$ となると
 $e_{ji} \in GF(q)$ □

同様に

定理 9 つぎの二つの条件は同値である

1. $(\sigma_E(X), \eta_E(X)) = (\sigma(X), \eta(X))$
2. I $\deg(\sigma_E(X), \eta_E(X)) = \#\Gamma$, $\Gamma = \{\beta \in GF(q^m) : \sigma_E(\beta) = 0, \beta \neq 0\}$
 II $\Gamma = \{\alpha^{-j_1}, \alpha^{-j_2}, \dots, \alpha^{-j_k}\}$ に対して $e_{ji} = -\alpha^{(1-r) \cdot j_i} \eta_E(\alpha^{-j_i}) / \sigma'_E(\alpha^{-j_i})$ となると
 $e_{ji} \in GF(q)$ □

すなわち、どちらのアルゴリズムを使用した場合でも条件の2. の判定により、予想する誤りに対応する誤り多項式、その出力された多項式の組から再現することが可能であるか、或は不可能であるかが判断できる。

それは、集合 $\Gamma = \{\beta \in GF(q^m) : \sigma(\beta) = 0, \beta \neq 0\}$ をChien searchにより求めた時点でその個数を $\deg(\sigma(X), \eta(X))$ と比較し、さらに $\Gamma = \{\alpha^{-j_1}, \alpha^{-j_2}, \dots, \alpha^{-j_k}\}$ に対して

$$e_{ji} = -\alpha^{(1-r) \cdot j_i} \eta(\alpha^{-j_i}) / \sigma'(\alpha^{-j_i}) \text{を計算して、}$$

$e_{ji} \in GF(q)$ を満たすか否かを判定すればよい。

つぎに、 t_1 を超える誤りが発生した場合にも最小距離復号を実行する方法を与える。

RS符号の場合には $S(X) = S_0 + S_1X + S_2X^2 + \dots + S_{d-2}X^{d-2} + A_{d-1}X^{d-1} + A_dX^d + \dots + A_{n-1}X^{n-1}$ を拡張シンドロームとすると $A_{d-1}, A_d, A_{d+1}, \dots, A_{n-1}$ を自由変数として復号手順を構成したが、BCH符号では $S(X)$ が \mathbb{A} に含まれていなければならないことから、 $\{c(r), c(r+1), \dots, c(n-1), c(0), c(1), \dots, c(r-1)\}$ をコセツトリダーの集合として、これから $\{c(r), c(r+1), \dots, c(r+d-2)\}$ を除いた集合を K とおくとき、 A_k ($k \in K$)だけが変数となり得る。ただし、 A_k ($k \in K$)が全て $GF(q^m)$ 上の自由変数となるのではなく、つぎの制約も受ける。 A_k は、 $\# \Pi_{r+k}$ を s とおくとき $GF(q^s)$ 上の自由変数である。ただし $GF(q^s)$ は $GF(q)$ 上に α^{r+k} で生成される $GF(q^m)$ の部分体。

RS符号の復号手順との違いは、拡張シンドロームは \mathbb{A} に含まれるものに限られるとの束縛条件が加わったことと(これにより手順は簡単になる)、定理8、定理9の判定条件の2. に条件IIが加わったこと、すなわち、 (σ, η) 多項式が、 \mathbb{A} にではなく \mathbb{B} に含まれるものに限ることを要求することに尽きる(これにより手順は複雑になる)。

以上に注意すると、誤りの検出と最小距離復号の実現手段は容易に構成される。

なお特にbinary-BCH符号の場合で、 $0 \in \{r, r+1, \dots, r+d-2\}$ のときは、

$$\Gamma = \{\alpha^{-j_1}, \alpha^{-j_2}, \dots, \alpha^{-j_k}\} \text{ に対して}$$

$$e_{ji} = -\alpha^{(1-r) \cdot j_i} \eta_B(\alpha^{-j_i}) / \sigma'_B(\alpha^{-j_i}) \quad (e_{ji} = -\alpha^{(1-r) \cdot j_i} \eta_E(\alpha^{-j_i}) / \sigma'_E(\alpha^{-j_i}) \text{ に関して}) \text{を算出すると必ず } e_{ji} = 1 \quad (1 \in GF(2)) \text{ が満たされることが示され、面倒な定理8および定理9の2. IIの条件は必要ない。}$$

謝辞 末筆ながら日頃ご指導、ご討論いただく関係各位に感謝する。

参考文献

- [1] E.R.Berlekamp, Algebraic Coding Theory. New York: McGraw-Hill, 1968.
- [2] F.J.MacWilliams and Sloane, The Theory of Error-Correcting Codes. Amsterdam: North-Holland, 1977.
- [3] J.L.Massey, "Shift-register synthesis and BCH decoding", IEEE Trans. Inform. Theory, vol. IT-15, pp. 122-127, Jan. 1969.
- [4] Y.Sugiyama, "An Algorithm for Solving Discrete-Time Wiener-Hopf Equations Based upon Euclid's Algorithm", IEEE Trans. Inform. Theory, vol. IT-32, NO. 3, pp. 394-409, MAY 1986.
- [5] K.Imamura, W.Yoshida, "A Simple Derivation of the Berlekamp-Massey Algorithm and Some Applications", IEEE Trans. Inform. Theory, vol. IT-33, pp. 146-150, Jan 1987.
- [6] C.R.P.Hartmann, "Decoding Beyond the BCH Bound", IEEE Trans. Inform. Theory, vol. IT-18, pp. 441-444, May 1972.
- [7] 日本数学会編集, 岩波 数学辞典 第3版。