

12 リード・ソロモン符号

この節では、理論的にも実用上も重要なリード・ソロモン符号を解説し、その2重誤り復号法を説明する。

12.1 リード・ソロモン符号の構成

以下で、 $F = F_q$ とし、 F の要素を $F = \{\alpha_0, \alpha_1, \dots, \alpha_{q-1}\}$ と記述する。 $i = 0, 1, \dots, q-1$ について、ベクトル $\mathbf{w}^{(i)} \in F^q$ を

$$\mathbf{w}^{(i)} = (\alpha_0^i, \alpha_1^i, \dots, \alpha_{q-1}^i)$$

と定義する。ただし、 $0^0 = 1$ と見なす。よって、特に $\mathbf{w}^{(0)} = (1, 1, \dots, 1)$ となる。各 k ($1 \leq k \leq q-1$) に対して、線型符号 $C(q, k)$ を

$$C(q, k) = \langle \mathbf{w}^{(0)}, \mathbf{w}^{(1)}, \dots, \mathbf{w}^{(k-1)} \rangle \quad (12.1)$$

と定義する。つまり、 $C(q, k) = \{c_0\mathbf{w}^{(0)} + c_1\mathbf{w}^{(1)} + \dots + c_{k-1}\mathbf{w}^{(k-1)} \mid c_i \in F\}$ である。そこで、 $f(x) = c_0 + c_1x + \dots + c_{k-1}x^{k-1}$ とおくと

$$c_0\mathbf{w}^{(0)} + c_1\mathbf{w}^{(1)} + \dots + c_{k-1}\mathbf{w}^{(k-1)} = (f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{q-1})) \quad (12.2)$$

となる。 $\mathbf{w}^{(0)}, \mathbf{w}^{(1)}, \dots, \mathbf{w}^{(k-1)}$ が F 上で1次独立であることを示そう。上のベクトルが $\mathbf{0} = (0, \dots, 0)$ と仮定する。このとき

$$f(\alpha_0) = f(\alpha_1) = \dots = f(\alpha_{q-1}) = 0$$

となるが、 $\deg f \leq k-1 < q$ より $f = 0$ がわかる。つまり、 $c_0 = c_1 = \dots = c_{q-1} = 0$ となって、1次独立性が言える。したがって、(12.1) で定義された $C(q, k)$ は q 元 (q, k) 符号となる。 $C(q, k)$ を (拡張) リード・ソロモン符号と呼ぶ。

例. $q = 7, k = 3$ のとき、 $F = F_7$ について $\alpha_i = i$ とおくと、

$$C(7, 3) = \langle (1, 1, 1, 1, 1, 1, 1), (0, 1, 2, 3, 4, 5, 6), (0, 1, 4, 2, 2, 4, 1) \rangle$$

は7元 $(7, 3)$ 符号で、符号語の個数は $7^3 = 343$ である。

12.2 リード・ソロモン符号の最小距離

リード・ソロモン符号 $C = C(q, k)$ は (12.2) の表示より

$$C = \{(f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{q-1})) \mid f(x) \in F[x], \deg f \leq k-1\}$$

と書ける．一般に，符号語 $w = (f(\alpha_0), \dots, f(\alpha_{q-1}))$ について，

$$d(w, 0) = |\{\alpha \in F \mid f(\alpha) \neq 0\}| = q - |\{\alpha \in F \mid f(\alpha) = 0\}|.$$

$|\{\alpha \in F \mid f(\alpha) = 0\}|$ は $f(x) = 0$ の解の個数に等しいので， $\deg f$ 以下である．よって，

$$d(w, 0) \geq q - \deg f \geq q - (k - 1) = q - k + 1$$

が言える．一方， $f(x) = (x - \alpha_0)(x - \alpha_1) \cdots (x - \alpha_{k-2})$ のとき， $\deg f = k - 1$ で $d(w, 0) = q - (k - 1)$ である．したがって，

命題 1. リード・ソロモン符号 $C = C(q, k)$ について， $d(C) = q - k + 1$.

例. $q = 7, k = 3$ のとき， $d(C) = 7 - 3 + 1 = 5$ である．よって， $C = C(7, 3)$ は 2 個の誤りを訂正できる． $q = 8, k = 4$ のときも， $d(C) = 8 - 4 + 1 = 5$ となる．

12.3 リード・ソロモン符号のシンドローム

補題. $F = F_q = \{\alpha_0, \dots, \alpha_{q-1}\}$ について，次が成立する．

$$\alpha_0^h + \alpha_1^h + \dots + \alpha_{q-1}^h = \begin{cases} 0 & (0 \leq h \leq q-2), \\ q-1 & (h = q-1). \end{cases} \quad (12.3)$$

証明. $h = 0$ のとき，和は q で F において 0 に等しい． $0^{q-1} = 0$ ， $\alpha^{q-1} = 1$ ($\alpha \neq 0$) だから， $h = q - 1$ のとき和は $q - 1$ となる． F の原始元を β とすれば

$$\{\alpha_0, \alpha_1, \dots, \alpha_{q-1}\} = \{0, 1, \beta, \beta^2, \dots, \beta^{q-2}\}$$

と書けるから， $1 \leq h \leq q - 2$ のとき， $\beta^h \neq 1$ であって

$$\alpha_0^h + \dots + \alpha_{q-1}^h = 1 + \beta^h + \dots + \beta^{h(q-2)} = \frac{1 - \beta^{h(q-1)}}{1 - \beta^h} = 0.$$

これより，式 (12.3) がわかる．

$C(q, k)$ の符号語 w を (12.2) のように $w = (f(\alpha_0), \dots, f(\alpha_{q-1}))$ と表示する． $0 \leq j \leq q - k - 1$ のとき， $0 \leq j + k - 1 \leq q - 2$ だから補題より，内積 $(w, w^{(j)})$ は

$$\sum_{i=0}^{q-1} \alpha_i^j f(\alpha_i) = \sum_{i=0}^{q-1} \alpha_i^j (c_0 + c_1 \alpha_i + \dots + c_{k-1} \alpha_i^{k-1}) = \sum_{l=0}^{k-1} c_l \sum_{i=0}^{q-1} \alpha_i^{j+l} = 0. \quad (12.4)$$

一般に, $\mathbf{y} = (y_0, y_1, \dots, y_{q-1}) \in F^q$ に対して

$$S_j(\mathbf{y}) = (\mathbf{y}, \mathbf{w}^{(j)}) = \sum_{i=0}^{q-1} \alpha_i^j y_i = \alpha_0^j y_0 + \alpha_1^j y_1 + \dots + \alpha_{q-1}^j y_{q-1} \quad (12.5)$$

と定義する. (12.4) より次が成立する.

命題 2. $w \in C(q, k)$ ならば $S_0(w) = S_1(w) = \dots = S_{q-k-1}(w) = 0$ が成り立つ.

さて, $C = C(q, k)$ のある符号語 $w \in C$ が送信され, $\mathbf{y} \in F^q$ として受信されたとする. 受信語 \mathbf{y} を

$$\mathbf{y} = \mathbf{w} + \mathbf{e}, \quad \mathbf{e} = (e_0, e_1, \dots, e_{q-1})$$

と誤りベクトル $\mathbf{e} = \mathbf{y} - \mathbf{w}$ を用いて記述する. 定義 (12.5) と命題 2 より

$$S_j(\mathbf{y}) = S_j(\mathbf{w}) + S_j(\mathbf{e}) = S_j(\mathbf{e}) \quad (0 \leq j \leq q - k - 1) \quad (12.6)$$

が成り立つ. この $S_0(\mathbf{y}), S_1(\mathbf{y}), \dots, S_{q-k-1}(\mathbf{y})$ を受信語 \mathbf{y} のシンドロームという.

12.4 2重誤り復号法

$C = C(q, k)$ について, $d(C) \geq 5$ と仮定する. $q - k - 1 \geq 3$ だから, 受信語 \mathbf{y} からシンドローム $S_0(\mathbf{y}), S_1(\mathbf{y}), S_2(\mathbf{y}), S_3(\mathbf{y})$ が計算できる.

(a) $d(\mathbf{w}, \mathbf{y}) = 0$ つまり $\mathbf{e} = \mathbf{0}$ のとき, (12.6) より $S_j(\mathbf{y}) = 0$ ($0 \leq j \leq 3$).

(b) $d(\mathbf{w}, \mathbf{y}) = 1$, $\mathbf{e} = (0, \dots, e_s, \dots, 0)$, $e_s \neq 0$ のとき, $S_j(\mathbf{y}) = S_j(\mathbf{e}) = \alpha_s^j e_s$ より,

$$\begin{cases} S_1(\mathbf{y}) - \alpha_s S_0(\mathbf{y}) = 0, \\ S_2(\mathbf{y}) - \alpha_s S_1(\mathbf{y}) = 0. \end{cases} \quad (12.7)$$

(c) $d(\mathbf{w}, \mathbf{y}) = 2$, $\mathbf{e} = (0, \dots, e_s, \dots, e_t, \dots, 0)$, $e_s, e_t \neq 0$ ならば,

$$S_j(\mathbf{y}) = S_j(\mathbf{e}) = \alpha_s^j e_s + \alpha_t^j e_t \quad (12.8)$$

となる. この場合, 簡単な計算で次が言える.

$$\begin{cases} S_2(\mathbf{y}) - (\alpha_s + \alpha_t) S_1(\mathbf{y}) + \alpha_s \alpha_t S_0(\mathbf{y}) = 0, \\ S_3(\mathbf{y}) - (\alpha_s + \alpha_t) S_2(\mathbf{y}) + \alpha_s \alpha_t S_1(\mathbf{y}) = 0. \end{cases} \quad (12.9)$$

そこで, 復号法は次のようにする.

(1) 受信語 \mathbf{y} からシンドローム $S_0(\mathbf{y}), S_1(\mathbf{y}), S_2(\mathbf{y}), S_3(\mathbf{y})$ を計算する . これがすべて 0 であれば , 誤りはないと判断する .

(2) 0 でないシンドロームがあれば , 未知数 u_0, u_1, u_2 について連立方程式

$$\begin{cases} S_2(\mathbf{y})u_2 + S_1(\mathbf{y})u_1 + S_0(\mathbf{y})u_0 = 0, \\ S_3(\mathbf{y})u_2 + S_2(\mathbf{y})u_1 + S_1(\mathbf{y})u_0 = 0 \end{cases} \quad (12.10)$$

を F において解く . ただし , $u_2 = 1$ または $u_2 = 0, u_1 = 1$ とする .

(3) $u_2 = 0, u_1 = 1$ として (12.10) が解ければ , 誤りは 1 個と判断し , (12.7) より誤り位置を $\alpha_s = -u_0$, 誤り値を $e_s = S_0(\mathbf{y})$ と推定する .

(4) $u_2 = 1$ として (12.10) が解ければ , 誤りは 2 個と判断する . (12.9) より

$$x^2 + u_1x + u_0 = x^2 - (\alpha_s + \alpha_t)x + \alpha_s\alpha_t = (x - \alpha_s)(x - \alpha_t)$$

と分解して誤り位置 α_s, α_t を推定し , (12.8) より

$$\alpha_t S_0(\mathbf{y}) - S_1(\mathbf{y}) = (\alpha_t - \alpha_s)e_s, \quad \alpha_s S_0(\mathbf{y}) - S_1(\mathbf{y}) = (\alpha_s - \alpha_t)e_t$$

として誤り値 e_s, e_t を計算する .

例. 前例の $C(7, 3)$ の符号語 \mathbf{w} について , その受信語を $\mathbf{y} = (1, 2, 0, 2, 4, 3, 0)$ とする . この受信語のシンドロームは

$$S_0(\mathbf{y}) = 5, \quad S_1(\mathbf{y}) = 4, \quad S_2(\mathbf{y}) = 5, \quad S_3(\mathbf{y}) = 1$$

と計算できる . $5u_2 + 4u_1 + 5u_0 = u_2 + 5u_1 + 4u_0 = 0$ を解くと , $u_2 = 1, u_1 = 4, u_0 = 0$ となる . $x^2 + 4x = x(x + 4) = x(x - 3)$ より誤り位置 0, 3 を得る . 誤り値は

$$(3 - 0)e_0 = 3S_0(\mathbf{y}) - S_1(\mathbf{y}) = 4, \quad (0 - 3)e_3 = 0S_0(\mathbf{y}) - S_1(\mathbf{y}) = 3$$

より $e_0 = 6, e_3 = 6$ となる . よって , $\mathbf{e} = (6, 0, 0, 6, 0, 0, 0)$ が分かり

$$\mathbf{w} = \mathbf{y} - \mathbf{e} = (1, 2, 0, 2, 4, 3, 0) - (6, 0, 0, 6, 0, 0, 0) = (2, 2, 0, 3, 4, 3, 0)$$

と復号される .

問題 12.1 例と同じ設定の下で , $\mathbf{w} \in C(7, 3)$ の受信語 $\mathbf{y} = (4, 1, 3, 6, 2, 0, 6)$ を復号せよ .