

集中講義 応用数学特論II

## Day 4 誤り訂正符号

担当：盧 曉南 (山梨大学)

[xnlu@yamanashi.ac.jp](mailto:xnlu@yamanashi.ac.jp)

2021 年 8 月 30 日

本日の内容

本日は誤り訂正符号の基礎（線形符号，ハミング符号，シンドローム復号，完全符号，MDS 符号）について紹介する。

## 0 記号・用語

- $\Omega$ : アルファベット (alphabet)
- $\mathcal{C}$ : 符号 (code), すなわち,  $\Omega$  上の文字列 (ベクトル) の集合のこと
- $\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v}, \mathbf{w}$  (小文字太字): ベクトル; 符号語 (codeword), すなわち, 符号  $\mathcal{C}$  の要素のこと
- $\mathbb{F}_q$ : 位数  $q$  の有限体
- $\mathbb{F}_q^n$ : 長さ  $n$  の  $\mathbb{F}_q$  ベクトル全体の集合;  $n$  次元  $\mathbb{F}_q$  ベクトル空間
- $\langle \mathbf{u}, \mathbf{v} \rangle$ : ベクトル  $\mathbf{u}, \mathbf{v}$  の内積 ( $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$  のとき)
- $I_k$ :  $k \times k$  の単位行列
- $H^\top$ : 行列  $H$  の転置

## 1 符号における基本概念

**定義 1.1.** 符号語  $\mathbf{x} = (x_1, \dots, x_n)$ ,  $\mathbf{y} = (y_1, \dots, y_n)$  に対応する位置の異なる文字の数はハミング距離 (Hamming distance) といい, 次式で定義される.

$$d_H(\mathbf{x}, \mathbf{y}) = \#\{i : x_i \neq y_i, 1 \leq i \leq n\}.$$

**定義 1.2.** 符号  $\mathcal{C}$  において, 任意の 2 つの符号語間のハミング距離の最小値は  $\mathcal{C}$  の最小ハミング距離 (minimum Hamming distance) といい, 次式で定義される.

$$d_{\mathcal{C}} = \min\{d_H(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{C}\}.$$

**注 1.3.** 符号長  $n$ , 符号語数  $M$ , 最小ハミング距離  $d$  の符号は  $(n, M, d)$  符号と表記する.

## 2 線形符号

**定義 2.1.** 以下の条件が満たされるとき,  $C \subseteq \mathbb{F}_q^n$  は線形符号 (linear code) という.

- $\mathbf{v}, \mathbf{u} \in C$  に対して  $\mathbf{v} + \mathbf{u} \in C$ .
- $\mathbf{v} \in C$  と  $\alpha \in \mathbb{F}_q$  に対して  $\alpha\mathbf{v} \in C$ .

**定義 2.2.** 符号語  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$  において,  $\mathbf{x}$  に非ゼロ成分の数はそのハミング重み (Hamming weight) といい, 次式で定義される.

$$\text{wt}(\mathbf{x}) = \#\{i : x_i \neq 0, 1 \leq i \leq n\}.$$

また, 符号  $C$  において, 非ゼロ符号語の最小重みは  $C$  の最小重み (minimum weight) という.

**命題 2.3.** 線形符号の最小距離は最小重みに等しい.

**定理 2.4.**  $\mathbb{F}_q$  上の符号長  $n$  の線形符号は  $\mathbb{F}_q^n$  の線形部分空間であり, 符号語数は  $|C| = q^k$  の形である.

**注 2.5.**  $\mathbb{F}_q$  上で符号長  $n$ , 線形部分空間の次元  $k$ , 最小距離  $d$  の線形符号は  $[n, k, d]_q$  符号と表記する. また, 最小距離  $d$  が不明の場合,  $[n, k]_q$  符号と書く.

**定義 2.6.** 線形部分空間の次元が  $k$  のとき,  $[n, k]$  線形符号  $C$  から互いに線形独立な  $k$  個の符号語 (行ベクトル) を取り出し, これを  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k$  とする. このとき,

$$G = \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_k \end{bmatrix}$$

を  $C$  の生成行列 (generator matrix) という.

**注 2.7.**  $[n, k]_q$  符号の生成行列  $G$  は標準形

$$G = \begin{bmatrix} I_k & A \end{bmatrix}$$

で与えられる.

**命題 2.8.** 生成行列  $G$  において符号  $C$  は次式で生成される.

$$C = \{\mathbf{x}G : \mathbf{x} \in \mathbb{F}_q^k\}.$$

**命題 2.9.** 符号  $C$  の最小距離を  $d = 2e + 1$  とする. このとき,  $d$  文字以内の誤りを検出でき,  $e$  文字以内の誤りを正確に訂正できる. なお,  $e$  文字の誤りを正確に訂正できる符号を  $e$  誤り訂正符号といい,  $e$  を誤り訂正能力という.

**定義 2.10.**  $\mathbb{F}_q$  上の線形符号  $C$  において, 次に定義される  $C^\perp$  は  $C$  の双対符号 (dual code) という.

$$C^\perp = \{\mathbf{w} : \langle \mathbf{w}, \mathbf{v} \rangle = 0 \text{ for all } \mathbf{v} \in C\}.$$

**命題 2.11.**  $[n, k]_q$  符号  $C$  の双対符号  $C^\perp$  は  $[n, n - k]_q$  符号である.

**定理 2.12.** 生成行列  $\begin{bmatrix} I_k & A \end{bmatrix}$  を持つ線形符号  $C$  において,  $\begin{bmatrix} -A^\top & I_{n-k} \end{bmatrix}$  はその双対符号  $C^\perp$  の生成行列である.

**定義 2.13.** 線形符号  $C$  において,  $C \subseteq C^\perp$  であるとき,  $C$  は自己直交 (self-orthogonal) という. また,  $C = C^\perp$  であるとき,  $C$  は自己双対 (self-dual) という.

**定義 2.14.** 線形符号  $C$  において, 双対符号  $C^\perp$  の生成行列を  $C$  のパリティ検査行列 (parity check matrix) という. すなわち,  $GH^\top = O$ .

**定義 2.15.** 行列  $H$  を線形符号  $C$  のパリティ検査行列とする. ベクトル  $\mathbf{v} \in \mathbb{F}_q^n$  において  $S(\mathbf{v}) = H\mathbf{v}^\top$  は  $\mathbf{v}$  のシンδροーム (syndrome) という.

### 3 ハミング符号と有限射影幾何

定義 3.1.  $[n, k]_q$  符号  $\mathcal{C}$  とベクトル  $\mathbf{w} \in \mathbb{F}_q^n$  において,

$$\mathcal{C} + \mathbf{w} = \{\mathbf{x} + \mathbf{w} : \mathbf{x} \in \mathcal{C}\}.$$

は  $\mathcal{C}$  のコセット (coset) という.

命題 3.2. (1)  $\mathbf{w} \in \mathbb{F}_q^n$  に対して  $|\mathcal{C}| = |\mathcal{C} + \mathbf{w}|$ .

(2)  $\mathbf{w}, \mathbf{u} \in \mathbb{F}_q^n$  に対して  $\mathcal{C} + \mathbf{w} = \mathcal{C} + \mathbf{u}$  または  $(\mathcal{C} + \mathbf{w}) \cap (\mathcal{C} + \mathbf{u}) = \emptyset$  が成り立つ.

(3) 下式が満たされる, 互いに異なるベクトル  $\mathbf{w}_0, \dots, \mathbf{w}_{q^{n-k}-1}$  が存在する.

$$\mathbb{F}_q^n = \bigcup_{i=0}^{q^{n-k}-1} (\mathcal{C} + \mathbf{w}_i)$$

命題 3.3. 行列  $H$  を線形符号  $\mathcal{C}$  のパリティ検査行列とする.  $\mathbf{v}, \mathbf{w} \in \mathbb{F}_q^n$  において,  $S(\mathbf{v}) = S(\mathbf{w}) \iff \mathbf{v}$  と  $\mathbf{w}$  が  $\mathcal{C}$  の同じコセットに属する.

定義 3.4.  $\mathbb{F}_2$  でゼロベクトルを除く長さ  $m$  のすべての可能なパターンを列ベクトルとする  $m$  行  $2^m - 1$  列のパリティ検査行列  $H$  で定義される符号はハミング符号 (Hamming code) という. このとき, ハミング符号長は  $2^m - 1$  であり, 次元は  $2^m - m - 1$  である.

命題 3.5. ハミング符号はすべての単一誤りを訂正できる.

定義 3.6. ベクトル  $\mathbf{v}_1, \mathbf{v}_1, \dots, \mathbf{v}_n$  を有限射影幾何  $\text{PG}(m-1, \mathbb{F}_q)$  の点 ( $\mathbb{F}_q^m$  のベクトル) とする. このとき,  $\mathbf{v}_1, \mathbf{v}_1, \dots, \mathbf{v}_n$  を列ベクトルとする  $m \times n$  のパリティ検査行列  $H$  で定義される符号は  $q$  元ハミング符号という. このとき, ハミング符号長は  $n = \frac{q^m-1}{q-1}$  であり, 次元は  $\frac{q^m-1}{q-1} - m$  であり, 最小距離は 3 である.

### 4 完全符号・MDS 符号

定理 4.1 (球充填限界式). 最小重み  $2t+1$  の符号  $\mathcal{C} \subseteq \mathbb{F}_q^n$  において下式が成り立つ.

$$|\mathcal{C}| \leq \frac{q^n}{\sum_{s=0}^t \binom{n}{s} (q-1)^s}. \quad (1)$$

定義 4.2. 球充填限界式 (1) の等号が成り立つ符号は完全符号 (perfect code) と呼ぶ.

定理 4.3 (Singleton の上界式).  $(n, q^k, d)_q$  符号において下式が成り立つ.

$$d \leq n - k + 1. \quad (2)$$

定義 4.4. Singleton の上界式 (2) の等号が成り立つ符号は MDS 符号 (Maximum Distance Separable code) と呼ぶ.

予想 4.5 (MDS 予想).  $[n, k, n-k+1]_q$  MDS 符号に対して  $n \leq q+1$  が成り立つ.

### レポート課題

課題 1. 線形符号  $\mathcal{C} \subseteq \mathbb{F}_2^4$  は次の生成行列  $G$  で定義される.

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- (1)  $C$  のすべての符号語を列挙せよ.
- (2)  $C$  において, 上記の  $G$  と異なる生成行列を 1 つ求めよ.
- (3)  $C$  の双対符号  $C^\perp$  のすべての符号語を列挙せよ.
- (4)  $C^\perp$  の生成行列を 1 つ求めよ. (ヒント: 定理 2.12 を利用して良い.)
- (5)  $C^\perp$  は自己直交であるかどうかを答えよ. また, その理由を簡単に述べよ.

課題 2. (1) 符号長 15 のハミング符号のパリティ検査行列を求めよ.

- (2) (1) のパリティ検査行列を用いてベクトル (111001101101101) と (001100110011010) をそれぞれ復号せよ.

レポート提出期限: 9 月 6 日 (月) 23:59 まで

## 参考文献

- [1] S. T. Dougherty. *Combinatorics and Finite Geometry*. Springer, 2020.
- [2] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.
- [3] A. Slinko. *Algebra for Applications: Cryptography, Secret Sharing, Error-Correcting, Fingerprinting, Compression*. Springer, 2020.
- [4] 藤原良 and 神保雅一. 符号と暗号の数理. 共立出版, 1993.