

1 第一回

1.1 符号理論とは

通信や記録を行う情報に冗長性を付け加えることで、通信伝達や記録装置で生じた誤りを検出あるいは訂正し、信頼性を高める方法について研究する学問。

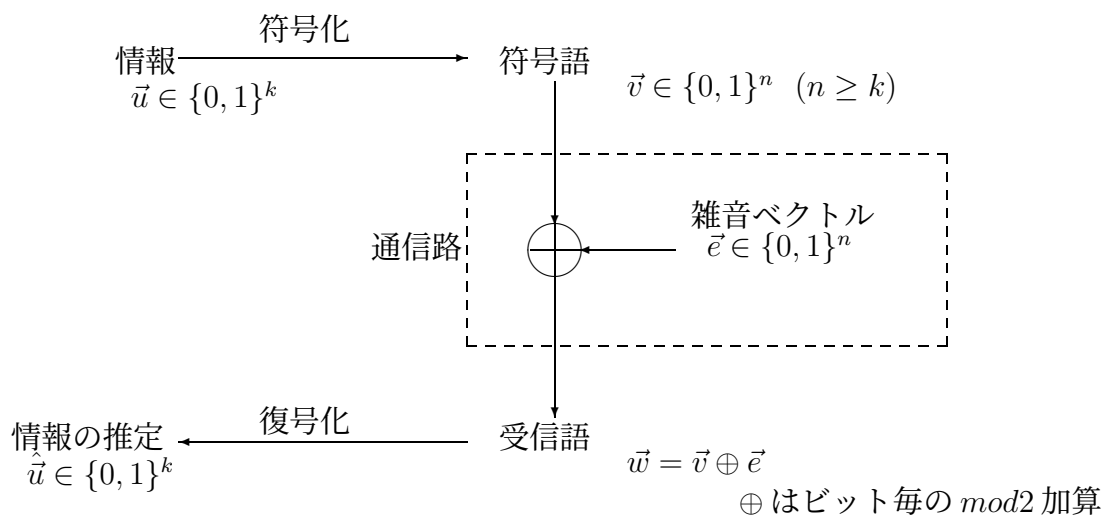
1.2 符号理論の歴史

単一誤りを訂正できる	1950 年	ハミング符号 (唯一個の誤りを訂正できる符号)
複数個の誤りを訂正できる	1959 年	BCH(Bose-Chaudhuri-Hocquenghem) 符号
	1960 年	RS(Reed-Solomon) 符号
衛星通信への応用	1971 年	Mariner 9 号 (火星探査衛星) 双直交符号
	1975 年	Viking(火星探査衛星) 双直交符号
	1977 年	Voyager(太陽系探査衛星)
		RS 符号+たたみ込み符号 (NASA の標準技術)
民生機への応用	1980 年	音楽 CD RS 符号
	1985 年	TV 文字放送 差集合巡回符号 (NHK)
	1992 年	MD
	1993 年	ディジタル携帯電話
	1996 年	CS ディジタル放送
	1996 年	DVD
	⋮	

1.3 情報伝送のモデル

ほとんど全てのデジタル情報について誤り訂正符号が用いられている。

情報に冗長性を付け加える操作 : 符号化
 誤りの検出/訂正を行ない元の情報を取り出す操作 : 復号化



1.4 簡単な誤り訂正符号の例

- 単一パリティ検査符号

情報 $\vec{u} = (u_1, u_2, \dots, u_k)$ $\xleftrightarrow{k \text{ ビット}}$	$\xrightarrow{\text{符号化}}$	符号語 $\vec{v} = (u_1, \dots, u_k, \sum_{i=1}^k u_i)$ $\xleftrightarrow{n = k + 1 \text{ ビット}}$
$\vec{u} = (1, 1, 0)$	$\longrightarrow$	$\vec{v} = (1, 1, 0, 1 + 1 + 0)$ $\quad \quad \quad \underline{\vec{u}}$ $\quad \quad \quad = (1, 1, 0, 0)$
$\vec{u} = (1, 0, 0)$	$\longrightarrow$	$\vec{v} = (1, 0, 0, 1 + 0 + 0)$ $\quad \quad \quad = (1, 0, 0, 1)$

符号語 $\vec{v} = (1, 0, 0, 1)$ に誤りベクトル $\vec{e} = (1, 0, 0, 0)$ が加わって受信語

$$\mathbf{w} = \mathbf{v} + \mathbf{e} = (1 + 1, 0, 0, 1) = (0, 0, 0, 1)$$

を得る。このとき1の個数は奇数なので誤りが生じたことが分かる。
受信側では誤りを検出したら送信側に同一符号語の再送を要求する。そして、正しく受信できるまで再送を繰り返すことで、信頼の高い通信が行える。(例 TCP)

1.5 線形符号の導入

$\mathbf{v} = (u_1, u_2, \dots, u_k, \sum_{i=1}^k u_i)$: 単一パリティ検査符号の符号語

ここで行列 H を $H = \begin{bmatrix} 1 & 1 & \dots & 1 \end{bmatrix}$ によって定めると

$$\begin{aligned} \mathbf{v}H^T &= (u_1, u_2, \dots, u_k, \sum_{i=1}^k u_i) \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \\ &= u_1 + u_2 + \dots + u_k + \sum_{i=1}^k u_i \\ &= \sum_{i=1}^k u_i + \sum_{i=1}^k u_i \\ &= 0 \end{aligned}$$

ただし H^T は H の転置行列を表す。また、逆に $\mathbf{w}H^T = 0$ をみたすベクトル $\mathbf{w} \in \{0, 1\}^{k+1}$ は

$$0 = \mathbf{w}H^T = (w_1, w_2, \dots, w_{k+1}) \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \sum_{i=1}^k w_i + w_{k+1}$$

すなわち

$$w_{k+1} = \sum_{i=1}^k w_i$$

を満足する。このことから

$\mathbf{v}$ が単一パリティ検査符号の符号語 $\uparrow$ 必要十分 $\mathbf{v}H^T = 0$ をみたすベクトル $\mathbf{v}$
--

このような行列 H をその符号のパリティ検査行列と呼ぶ。

一般にパリティ検査行列 H を用いて

$$C = \{\mathbf{v} \in \{0, 1\}^n : \mathbf{v}H^T = \mathbf{0}\}$$

として特徴付けられる符号 C を線形符号と呼ぶ。

線形符号では、 v_1 と v_2 が符号語ならば、 $v_1 + v_2$ もまた符号語である。なぜならば、

$$(v_1 + v_2)H^T = v_1H^T + v_2H^T = \mathbf{0} + \mathbf{0} = \mathbf{0}$$

であるからである。

1.6 ハミング符号

符号長 $n = 2^m - 1$, (パラメータ : $m = 2, 3, 4, \dots$)

$m = 3$ の場合

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

H は長さ 3 の非零の列ベクトルを全て並べて得られるもの。

ハミング符号の符号語の例

$$\begin{aligned} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} H^T &= \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \\ &= \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

行列の基本変形 $\begin{cases} \text{行を入れ換える} \\ \text{ある行を他の行に加える} \end{cases}$

このような操作によっても行列 H の行空間は変化しない。

行空間 : 行ベクトルの線形結合によって得られる線形空間

H の後ろ 3 行 3 列を単位行列になるように変形

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

$$\xrightarrow{\text{1行目を3行目に加える}} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\xrightarrow{\text{2行目を3行目に加える}} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{\text{3行目を1行目と2行目に加える}} \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} = \hat{H}$$

このとき、 $\boldsymbol{v}H^T = \mathbf{0} \iff \boldsymbol{v}\hat{H}^T = \mathbf{0}$ が成り立つ。

$$\text{なぜならば、} H^T = \begin{bmatrix} \boldsymbol{w}_1 \\ \boldsymbol{w}_2 \\ \boldsymbol{w}_3 \end{bmatrix} \text{ とすれば、}$$

$$\boldsymbol{v}H^T = \mathbf{0} \iff \boldsymbol{v}\boldsymbol{w}_1^T = \boldsymbol{v}\boldsymbol{w}_2^T = \boldsymbol{v}\boldsymbol{w}_3 = 0$$

$$\text{他方、} \hat{H} = \begin{bmatrix} \boldsymbol{w}_2 + \boldsymbol{w}_3 \\ \boldsymbol{w}_1 + \boldsymbol{w}_3 \\ \boldsymbol{w}_1 + \boldsymbol{w}_2 + \boldsymbol{w}_3 \end{bmatrix} \text{ と書けるので}$$

$$\begin{aligned} \boldsymbol{v}(\boldsymbol{w}_2 + \boldsymbol{w}_3)^T &= \boldsymbol{v}(\boldsymbol{w}_1 + \boldsymbol{w}_3)^T = \boldsymbol{v}(\boldsymbol{w}_1 + \boldsymbol{w}_2 + \boldsymbol{w}_3)^T = 0 \\ &\quad \updownarrow \\ \boldsymbol{v}\hat{H}^T &= \mathbf{0} \end{aligned}$$

となるからである。

以上のことからハミング符号の符号語を $\boldsymbol{v} = (v_1, v_2, \dots, v_7)$ とすれば、 $\boldsymbol{v}\hat{H}^T = \mathbf{0}$ から

$$\begin{aligned} \mathbf{0} &= \boldsymbol{v}\hat{H}^T \\ &= (v_1, \dots, v_7) \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}^T \\ &= (v_2 + v_3 + v_4 + \underline{v_5}, v_1 + v_3 + v_4 + \underline{v_6}, v_1 + v_2 + v_4 + \underline{v_7}) \end{aligned}$$

従って、

$$v_5 = v_2 + v_3 + v_4$$

$$v_6 = v_1 + v_3 + v_4$$

$$v_7 = v_1 + v_2 + v_4$$

情報ベクトル

$(v_1, v_2, v_3, v_4) \in \{0, 1\}^4$ 符号化 $(v_1, v_2, v_3, v_4, v_2 + v_3 + v_4, v_1 + v_3 + v_4, v_1 + v_2 + v_4)$
この符号化は

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right]$$

を用いて、

$$(v_1, v_2, \dots, v_7) = (v_1, v_2, v_3, v_4)G$$

と書ける。このような行列 G を生成行列と呼ぶ。生成行列の各行ベクトルは符号語であり、各行ベクトルの線形結合 (行ベクトルのつくる線形空間) が符号語の集合となる。

1.7 ハミング符号の復号法

符号語 : $\mathbf{v} = (0110011)$ を送信

誤りベクトル : $\mathbf{e} = (0010000)$ が加わり

受信語 : $\mathbf{w} = \mathbf{v} + \mathbf{e} = (0100011)$

復号には、まず $\mathbf{w}H^T$ を計算する。

$$\mathbf{w}H^T = (0100011) \left[\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{array} \right] = (110)$$

(110) はパリティ検査行列 H の 3 列目の転置に等しいので 3 番目の成分に誤りがあったと判定する。なぜなら、

$$\mathbf{w}H^T = (\mathbf{v} + \mathbf{e})H^T = \mathbf{v}H^T + \mathbf{e}H^T = \mathbf{0} + \mathbf{e}H^T = \mathbf{e}H^T$$

となり、 wH^T は誤りベクトル e にのみ依存するからである。特に、 eH^T はシンドロームと呼ばれている。