

# 代数系と符号理論 第16回板書プリント

植松友彦 2007.7.13

## 1 LDPC 符号と EG 符号

20 世紀最後の符号理論の注目を集めた符号として、ターボ符号と低密度パリティ検査符号 (Low Density Parity Check (LDPC)) 符号が知られている。これらの符号は、復号計算量が小さい (符号長の線形オーダー) にも係らず、通信路の通信路容量をほぼ達成するという高性能符号である。今回は、このうち LDPC 符号について解説する。

### 1.1 LDPC 符号

LDPC 符号とは、次のようなパリティ検査行列  $H$  を有する線形符号として、特徴付けられる。

定義 1 LDPC 符号は、次の 4 性質を有するパリティ検査行列  $H$  によって定まる 2 元線形符号である。

- (1) 各行には  $\rho$  個の 1 がある。
- (2) 各列には  $\gamma$  個の 1 がある。
- (3) 任意の 2 列の間で、同時に 1 になっている行の数  $\lambda$  は 1 か 0 である。
- (4)  $\rho$  と  $\gamma$  は符号長すなわち  $H$  の列の数に比べて十分小さい。

また、このような LDPC 符号のことを  $(\gamma, \rho)$  正規 LDPC 符号と呼ぶ。

上の定義で、(1) と (2) はパリティ検査行列  $H$  の行のハミング重みと列のハミング重みが、それぞれ全て等しいことを示している。これに対して、(3) は、もともと各列の 1 の数が少ないので、2 列で同時に 1 になっている行の数が少ないことを意味している。

以下では、パリティ検査行列の密度  $r$  を  $H$  の要素中の 1 の要素の割合によって定める。すなわち、

$$r = \rho/n = \gamma/J$$

とする。但し、 $J$  は  $H$  の行の数である。 $H$  が低密度であるとは、 $H$  が疎行列 (sparse matrix) であることを意味する。

### 例 1 パリティ検査行列

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

この行列の各行ならびに各列には 4 個の 1 があり ( $\rho = \gamma = 4$ )、どの 2 列 (どの 2 行) も同時に 1 になっている行 (列) は高々 1 つである。このパリティ検査行列  $H$  の密度は、

$$\rho = 4/15 = 0.267$$

であり、低密度である。このパリティ検査行列によって定まる線形符号は、次元 7 を有するので、 $(15, 7)$  LDPC 符号である。また、この符号は最小距離 5 を有する。尚、この符号は BCH 符号に一致する。

## 1.2 EG-LDPC 符号の構成法

ここでは、EG 符号に基づく 2 種類の LDPC 符号の構成法について述べる。

$F_{2^s}$  上の  $m$  次元のユークリッド幾何  $EG(m, 2^s)$  を考えよう。 $EG(m, 2^s)$  は、 $2^{ms}$  個の点を含み、各々の点は  $F_{2^s}$  上の  $m$  次元ベクトルとして表現される。特に、 $(0, 0, \dots, 0)$  を原点と呼ぶ。以下、 $EG(m, 2^s)$  の直線についての性質を復習する。

- $EG(m, 2^s)$  の直線は、全部で

$$J = \frac{2^{(m-1)s}(2^{ms} - 1)}{2^s - 1}$$

本あり、各々の直線は  $2^s$  個の点を含む。

- 任意の点において、

$$\gamma = \frac{2^{ms} - 1}{2^s - 1}$$

本の直線が交わっている。

- 異なる 2 直線は、平行か唯一点で交わるかのいずれかである。
- $EG(m, 2^s)$  の各直線は、それに平行な  $2^{(m-1)s} - 1$  本の直線を持ち、全体で、 $(2^{ms} - 1)/(2^s - 1)$  個の平行束があり、各々の平行束は  $2^{(m-1)s}$  本の平行線からなる。

いま、 $F_{2^{ms}}$  によって  $EG(m, 2^s)$  を表現するとする。このとき、 $F_{2^{ms}}$  の元は  $EG(m, 2^s)$  の  $2^{ms}$  個の点に対応しており、0 は原点に対応している。そこで、 $\alpha$  を  $F_{2^{ms}}$  の原始元とし、 $F_{2^{ms}}$  の非零の元、すなわち  $EG(m, 2^s)$  の原点以外の点を

$$\alpha^0 = 1, \alpha^2, \alpha^3, \dots, \alpha^{2^{ms}-2}$$

によって定める。さて、

$$v = (v_0, v_1, \dots, v_{2^{ms}-2})$$

を  $F_2$  上の  $(2^{ms} - 1)$  次元のベクトルとする。ここで、 $i$  番目の要素  $v_i$  と  $F_{2^{ms}}$  の非零元  $\alpha^i$  とが対応しているとし、 $\alpha^i$  を  $v_i$  の location number という。このとき、 $L$  を  $EG(m, 2^s)$  の直線とすると、 $F_2$  上のベクトル

$$v_L = (v_0, v_1, \dots, v_{2^{ms}-2})$$

を次のようにして定める。

$$v_i = \begin{cases} 1 & \alpha^i \text{が } L \text{ の点} \\ 0 & \text{elsewhere} \end{cases}$$

すなわち、 $v_L$  の非零要素の location number が直線  $L$  の点になっている。ベクトル  $v_L$  を直線  $L$  の生成ベクトル (incidence vector) と呼ぶ。

先に述べた、 $EG(m, 2^s)$  の性質から、 $EG(m, 2^s)$  の原点を通らない直線は、全部で

$$J_0 = \frac{(2^{(m-1)s} - 1)(2^{ms} - 1)}{2^s - 1}$$

本ある。そこで、パリティ検査行列  $H_{EG}^{(1)}$  の各行を、 $EG(m, 2^s)$  の原点を通らない  $J_0$  本の直線の生成ベクトルによって定める。すなわち、 $H_{EG}^{(1)}$  の各列は  $EG(m, 2^s)$  の原点以外の点に対応し、各行は原点を通らない直線に対応している。従って、このパリティ検査行列は次の特徴を有する。

(1) 各行はハミング重み  $\rho = 2^s$  を有する。(直線に含まれる点の数に等しい)

(2) 各列はハミング重み

$$\gamma = \frac{2^{ms} - 1}{2^s - 1} - 1$$

を有する。(ある点で交わる、原点を通過しない直線の総数に等しい)

(3) 異なる 2 列において、同時に 1 になっている行の数は高々 1 である。すなわち、 $\lambda = 0, 1$  である。(2 点を異なる直線は 1 点で交わるか、交わらないかのいずれかであることから)

(4) 異なる 2 行において、同時に 1 になっている列の数は高々 1 である。(異なる直線は 1 点で交わるか、交わらないかのいずれかであることから)

これから、 $E_{EG}^{(1)}$  の密度は、

$$r = \frac{2^s}{2^{ms} - 1}$$

であり、 $m \geq 2, s \geq 2$  のとき、 $r$  は 1 に比べて十分小さいので、 $E_{EG}^{(1)}$  は低密度行列である。

$C_{EG}^{(1)}(m, 0, s)$  によって、パリティ検査行列  $H_{EG}^{(1)}$  によって定まる線形符号を表す。このとき、 $C_{EG}^{(1)}(m, 0, s)$  は、符号長  $n = 2^{ms} - 1$  を有する LDPC 符号であり、最小距離は少なくとも

$$\gamma + 1 = \frac{2^{ms} - 1}{2^s - 1} \quad (1)$$

である。この定義から分かるように、この LDPC 符号は、 $(0, s)$  次 EG 符号に一致しており、それゆえ巡回符号である。そこでこれらの符号のことを、「 $m$  次元タイプ I 巡回  $(0, s)$  次 EG-LDPC 符号」と呼ぶ。

タイプ I 巡回  $(0, s)$  次 EG 符号の生成多項式の根について BCH 限界を用いると、最小距離の下界について

$$d_{EG}^{(1)} \geq 2^{(m-1)s} + 2^{(m-2)s+1} - 1$$

が得られ、これは、(1) よりも厳しい限界式となっている。また、タイプ I 巡回  $(0, s)$  次 EG-LDPC 符号のパリティ検査ビットの数は生成多項式の次数に等しい。

タイプ I 巡回  $(0, s)$  次 EG-LDPC 符号の特別なクラスとして、2 次元タイプ I 巡回  $(0, s)$  次 EG-LDPC 符号がある。これは、 $m = 2$  として得られる  $EG(2, 2^s)$  の直線によって構成される  $C_{EG}^{(1)}(2, 0, s)$  符号であり、次のパラメータを有する。

|            |                            |
|------------|----------------------------|
| 符号長        | $n = 2^{2s} - 1$           |
| パリティ検査ビット数 | $n - k = 3^s - 1$          |
| 次元         | $k = 2^{2s} - 3^s$         |
| 最小距離       | $d_{min} = 2^s + 1$        |
| 密度         | $r = \frac{2^s}{2^{2s}-1}$ |

$s$  を変えて得られる符号  $C_{EG}^{(1)}(2, 0, s)$  のパラメータを次の表に示す。

| $s$ | $n$   | $k$   | $d_{min}$ | $\rho$ | $\gamma$ | $r$      |
|-----|-------|-------|-----------|--------|----------|----------|
| 2   | 15    | 7     | 5         | 4      | 4        | 0.267    |
| 3   | 63    | 37    | 9         | 8      | 8        | 0.127    |
| 4   | 255   | 175   | 17        | 16     | 16       | 0.0627   |
| 5   | 1023  | 781   | 33        | 32     | 32       | 0.0313   |
| 6   | 4095  | 3367  | 65        | 64     | 64       | 0.01563  |
| 7   | 16383 | 14197 | 129       | 128    | 128      | 0.007813 |

$m$  次元タイプ I 巡回  $(0, s)$  次符号と対になる符号として、

$$H_{EG}^{(2)} = [H_{EG}^{(1)}]^T$$

をパリティ検査行列とする線形符号がある。この LDPC 符号は、符号長

$$n = J_0 = \frac{(2^{(m-1)s} - 1)(2^{ms} - 1)}{2^s - 1}$$

を有し、最小距離は少なくとも  $2^s - 1$  である。但し、この符号は巡回符号ではない。この符号のことを「 $m$  次元タイプ II 準巡回  $(0, s)$  次 EG-LDPC 符号」と呼び、 $E_{EG}^{(2)}(m, 0, s)$  と書く。

## 2 LDPC 符号の復号法

EG-LDPC 符号は様々な手法で復号することができる。ここでは、硬判定 (0 と 1 を送信して、0 か 1 を受信) を行うときの幾つかの復号法について述べる。

送信語  $v = (v_1, v_2, \dots, v_n)$  を送信し、通信路で誤り  $e = (e_1, e_2, \dots, e_n)$  が生じ受信語

$$r = (r_1, r_2, \dots, r_n) = v + e$$

を得たとする。このとき、シンドロームは、

$$s = (s_1, s_2, \dots, s_J) = rH^T = eH^T = (eh_1^T, eh_2^T, \dots, eh_n^T)$$

によって定まる。但し、 $h_j$  は  $H$  の第  $j$  行ベクトルである。尚、任意の符号語  $v$  に対し、 $vH^T = 0$  が成り立つので、シンドロームは誤りベクトル  $e$  によってのみ定まることに注意する。

## 2.1 多数決論理復号法

EG-LDPC 符号のパリティ検査符号  $H$  の性質から、任意のビット位置  $\ell$  に対して、 $\ell$  列目のビットが 1 であるような  $H$  の行ベクトルの集合

$$A_\ell = \{h_1^{(\ell)}, h_2^{(\ell)}, \dots, h_\gamma^{(\ell)}\}$$

を定義する。EG-LDPC 符号のパリティ検査符号の性質 (3) と (4) から、 $A_\ell$  に含まれるどの 2 つのベクトルも  $\ell$  番目以外のビットが同時に 1 であることはない。そこで、 $A_\ell$  に属する行ベクトルに基づいて、次のようなシンドロームの集合を考える。

$$S_\ell = \{s_j^{(\ell)} = eh_j^{(\ell)T} : h_j^{(\ell)} \in A_\ell, 1 \leq j \leq \gamma\}$$

この集合に基づき、誤りベクトルの  $\ell$  番目のビットを、この  $S_\ell$  に含まれる値  $s_j^{(\ell)}$  の多数決 (同数の場合は 0 とする) を取って得られる値であると判定することで、ハミング重み  $\lfloor \gamma/2 \rfloor$  以下の誤りベクトル  $e$  を正しく推定することができる。そして、受信語  $r$  から推定された誤りベクトル  $e$  を引くことで送信符号語を復号することができる。次の例で、実際の復号法について説明しよう。

**例 2** 例 1 のパリティ検査行列による LDPC 符号を考えよう。一番左端のビットに対応する  $A_1$  は、

$$\begin{aligned} A_1 = \{ & (100000001101000) \\ & (100010000000110) \\ & (1010001000000001) \\ & (110100010000000) \} \end{aligned}$$

となる。すると、対応するシンドロームの集合は、

$$\begin{aligned} s_1^{(1)} &= e_1 + e_9 + e_{10} + e_{12} \\ s_2^{(1)} &= e_1 + e_4 + e_{13} + e_{14} \\ s_3^{(1)} &= e_1 + e_3 + e_7 + e_{15} \\ s_4^{(1)} &= e_1 + e_2 + e_4 + e_8 \end{aligned}$$

である。受信語に  $\lfloor \gamma/2 \rfloor = 2$  個以下の誤りが生じていたとする。最初のビット  $e_1$  のみに誤りが生じていたとすれば、

$$s_1^{(1)} = s_2^{(1)} = s_3^{(1)} = s_4^{(1)} = 1$$

であるので、多数決により  $e_1 = 1$  と判定され、このビットに誤りが生じたことが分かる。他方、他の 1 ビット例えば  $e_3$  に誤りが生じたとすれば、

$$s_1^{(1)} = s_2^{(1)} = s_4^{(1)} = 0, \quad s_3^{(1)} = 1$$

となり、多数決により  $e_1 = 0$  と判定され、1 ビット目には誤りがないことが分かる。更に、 $e_1$  と  $e_2$  に誤りがあったとすると、

$$s_1^{(1)} = s_2^{(1)} = s_3^{(1)} = 1, \quad s_4^{(1)} = 0$$

からやはり、 $e_1 = 1$  と判定される。また、 $e_2$  と  $e_3$  に誤りがあったとすると、

$$s_1^{(1)} = s_2^{(1)} = 0, \quad s_3^{(1)} = s_4^{(1)} = 1$$

から、0 と 1 が同数なので  $e_1 = 0$  と判定される。

## 2.2 ビットフリッピング復号法

ビットフリッピング (Bit-flipping(BF)) 復号法では、受信語  $r$  のあるビットを反転 (0 と 1 を入れ替える) することで、シンδροーム  $\{rh_j : 1 \leq j \leq J\}$  の何個が反転するかに基づいて復号を行う方法である。

具体的には、次のステップで復号を行う。

1. シンδροームを  $s = rH^T$  によって計算し、 $s = 0$  ならば、復号を終了する。
2. 受信語  $r$  の  $i$  番目 ( $i = 1, 2, \dots, n-1$ ) のビットを反転したときに得られるシンδροームの重みを調べ、それを  $f_i$  とする。
3.  $f_i$  が最大になるビット位置  $i$  の集合  $S$  を求める。
4. 受信語中の  $S$  に属するビット位置を反転する。
5. シンδροームが 0 になるまで、1. から 4. のステップを繰り返す。または、1. から 4. のステップを一定回数繰り返したら終了する。

## 2.3 その他の復号法

軟判定 (0 と 1 を送信して、0 以上 1 以下のアナログ値を受信) に対する復号法として、「重み付き多数決論理復号法」、「重み付きビットフリッピング復号法」ならびに「Sum-Product 復号法」が知られている。これらの復号法の詳細は、例えば、

S. Lin and D. J. Costello, Jr., Error Control Coding, Prentice-Hall, 2004.

を参照にされたい。

## 2.4 LDPC 符号の性能

$m = 2, s = 5$  とするとき、2 次元タイプ I 巡回 (0,5) 次 EG-LDPC 符号は、(1023,781) 符号である。この符号の最小距離は 33 で、符号化率  $R = 0.763$  である。加法的ガウス雑音通信路に対し、2 値位相シフト変調 (PSK) にこの符号を適用したときの各種復号アルゴリズムに対する復号特性を下図に示す。但し、SPA は Sum-Product 復号法、(weighted) BF は (重み付き) ビットフリッピング復号法、MLG は多数決論理復号法を意味する。また、bit はビット誤り率を block は符号語の誤り率をそれぞれ表す。

図 1: LDPC 符号の復号誤り率特性

## 2.5 演習問題

例 1 のパリティ検査行列を持つ LDPC 符号について、受信語 (111010011010111) を多数決論理復号法で復号せよ。