第 9 章
LDPC 符号と sum-product 復号法

9.1 時をこえた符号の話

訂正無し。

9.2 消失誤り訂正と LDPC 符号

補題 9.1 (単一検査による消失誤り訂正) 変更なし。

定義 9.2 $c_1, c_2, \cdots \in \{0, 1, *\}$ に対し，関数 $\mathrm{SUM}, \mathrm{PROD} : \{0, 1, *\}$ 上の系列全体 $\to \{0, 1, *\}$ を次で定義する：

$$\mathrm{SUM}(c_1, c_2, \cdots, c_n) := \begin{cases} c_1 + \cdots + c_n & (c_{n_0} \neq *(1 \leqq n_0 \leqq n)) \\ * & (\text{その他}) \end{cases}$$

$$\mathrm{PROD}(c_1, c_2, \cdots, c_n) := \begin{cases} 0 & (N(0\,|\,c) > N(1\,|\,c)) \\ 1 & (N(0\,|\,c) < N(1\,|\,c)) \\ * & (\text{その他}) \end{cases}$$

ここで，$N(x|c) := N(x|c_1, c_2, \cdots, c_n)$，$N(\ |\ )$ は登場回数 (定義 6.6 参照)，$x \in \{0, 1\}$ を表す.

記号の書き方として，$\mathrm{SUM}(c_1, c_2, \cdots, c_n)$ の代わりに

$$\mathrm{SUM}(\{c_{n_0} \mid n_0 \in \{1, 2, \cdots, n\}\})$$

のように表すなど，意味が明らかにわかるよう，表記を工夫する．

定義 9.3 (**添字の集合**)　訂正無し。

注意 9.4　訂正無し。

定義 9.5 (**消失通信路上の sum-product 復号法**)　訂正無し。

例 9.6　二元体上の行列 H を以下で定義しよう：

$$H := \begin{pmatrix} 0_{\mathbb{F}} & 0_{\mathbb{F}} & 0_{\mathbb{F}} & 1_{\mathbb{F}} & 1_{\mathbb{F}} & 1_{\mathbb{F}} & 0_{\mathbb{F}} & 0_{\mathbb{F}} & 0_{\mathbb{F}} \\ 1_{\mathbb{F}} & 0_{\mathbb{F}} & 0_{\mathbb{F}} & 1_{\mathbb{F}} & 0_{\mathbb{F}} & 0_{\mathbb{F}} & 0_{\mathbb{F}} & 1_{\mathbb{F}} & 0_{\mathbb{F}} \\ 1_{\mathbb{F}} & 1_{\mathbb{F}} & 1_{\mathbb{F}} & 0_{\mathbb{F}} & 1_{\mathbb{F}} & 0_{\mathbb{F}} & 1_{\mathbb{F}} & 1_{\mathbb{F}} & 1_{\mathbb{F}} \end{pmatrix}.$$

系列 y を $y := (*, 0_{\mathbb{F}}, 1_{\mathbb{F}}, *, 0_{\mathbb{F}}, 1_{\mathbb{F}}, 0_{\mathbb{F}}, 0_{\mathbb{F}}, *)$ とし，$l_{\max} := 20$ としよう．

1. において，行列 H の列数と系列 y の長さを比較する．今回はどちらも 9 であるから，次の手順へ進む．

2. において，正整数 l を $l := 1$ と定義する．さらに，行列 β を以下で定義する．ただし，空白記号 b を空白で表している．

$$\beta := \begin{pmatrix} & & & * & 0_{\mathbb{F}} & 1_{\mathbb{F}} & & & \\ * & & & * & & & & 0_{\mathbb{F}} & \\ * & 0_{\mathbb{F}} & 1_{\mathbb{F}} & & 0_{\mathbb{F}} & & 0_{\mathbb{F}} & 0_{\mathbb{F}} & * \end{pmatrix}$$

3. において，行列 α の各成分に対して行処理を行う．例を計算しよう．

- 各行列の $(1,1)$ 成分に注目して計算する．パリティ検査行列 H の $(1,1)$ 成分は $0_{\mathbb{F}}$ であるから，3. に従い行処理を行わない．
- $(2,1)$ 成分に注目して計算する．H の $(2,1)$ 成分は $1_{\mathbb{F}}$ である．そこで，3. に従い行処理を行う．

$$\alpha_{2,1} := \mathrm{SUM}(\beta_{2,4}, \beta_{2,8}) = \mathrm{SUM}(*, 0_{\mathbb{F}}) = *$$

- $(1,4)$ 成分に注目して計算する．H の $(1,4)$ 成分は $1_{\mathbb{F}}$ である．そこで，3. に従い行処理を行う．

$$\alpha_{1,4} := \mathrm{SUM}(\beta_{1,5}, \beta_{1,6}) = \mathrm{SUM}(0_{\mathbb{F}}, 1_{\mathbb{F}}) = 0_{\mathbb{F}} + 1_{\mathbb{F}} = 1_{\mathbb{F}}$$

- $(3,8)$ 成分に注目して計算する．H の $(3,8)$ 成分は $1_{\mathbb{F}}$ である．そこで，3. に従い処理を行う．

$$\begin{aligned}\alpha_{3,8} &:= \mathrm{SUM}(\beta_{3,1}, \beta_{3,2}, \beta_{3,3}, \beta_{3,5}, \beta_{3,7}, \beta_{3,9}) \\ &= \mathrm{SUM}(*, 0_{\mathbb{F}}, 1_{\mathbb{F}}, 0_{\mathbb{F}}, 0_{\mathbb{F}}, *) = *\end{aligned}$$

これらの操作をすべての成分に対して施す．行列 α は以下となる：

$$\alpha = \begin{pmatrix} & & 1_{\mathbb{F}} & * & * & & & \\ * & & & * & & & * & \\ * & * & * & & * & & * & * & * \end{pmatrix}.$$

4. において，β の各成分に対して列処理を行う．例を計算しよう．

- $(1,1)$ 成分に注目して計算する．H の $(1,1)$ 成分は $0_{\mathbb{F}}$ であるから，4. に従い行処理を行わない．
- $(2,1)$ 成分に注目して計算する．H の $(2,1)$ 成分は $1_{\mathbb{F}}$ である．そこで，4. に従い行処理を行う．第 1 列には，$(2,1)$ 成分以外では $\mathbb{F}_2$ の元は登場しない．よって，$(2,1)$ 成分を $*$ とする．
- $(1,4)$ 成分に注目して計算する．H の $(1,4)$ 成分は $1_{\mathbb{F}}$ である．そこで，4. に従い行処理を行う．

$$\beta_{1,4} := \mathrm{PROD}(y_4, \alpha_{2,4}) = \mathrm{PROD}(*, *) = *$$

- $(2,4)$ 成分に注目して計算する．H の $(2,4)$ 成分は $1_{\mathbb{F}}$ である．そこで，4. に従い行処理を行う．

$$\beta_{2,4} := \mathrm{PROD}(y_4, \alpha_{1,4}) = \mathrm{PROD}(*, 1_{\mathbb{F}}) = 1_{\mathbb{F}}$$

この操作により，行列 β は以下となる：

$$\beta = \begin{pmatrix} & & & * & 0_{\mathbb{F}} & 1_{\mathbb{F}} & & & \\ * & & & 1_{\mathbb{F}} & & & & 0_{\mathbb{F}} & \\ * & 0_{\mathbb{F}} & 1_{\mathbb{F}} & & 0_{\mathbb{F}} & & 0_{\mathbb{F}} & 0_{\mathbb{F}} & * \end{pmatrix}.$$

5. において，系列 c を定義する．例として，第 $1, 2, 4$ 成分を計算する．

- 第 1 成分 $c_1 := \mathrm{PROD}(y_1, \alpha_{2,1}, \alpha_{3,1}) = \mathrm{PROD}(*, *, *) = *$.
- 第 2 成分 $c_2 := \mathrm{PROD}(y_2, \alpha_{3,2}) = \mathrm{PROD}(0_{\mathbb{F}}, *) = 0_{\mathbb{F}}$.
- 第 4 成分 $c_4 := \mathrm{PROD}(y_4, \alpha_{1,4}, \alpha_{2,4}) = \mathrm{PROD}(*, 1_{\mathbb{F}}, *) = 1_{\mathbb{F}}$.

系列 c のすべての成分を求めれば，以下を得る：

$$c = (*, 0_{\mathbb{F}}, 1_{\mathbb{F}}, 1_{\mathbb{F}}, 0_{\mathbb{F}}, 1_{\mathbb{F}}, 0_{\mathbb{F}}, 0_{\mathbb{F}}, *).$$

6. において，c に $*$ が含まれるため，次の手順へ進む．

7. において，$l = 1, l_{\max} = 20$ であるから，不等式 $l > l_{\max}$ は成立しない．次の手順へ進む．

8. において，$l = 2$ に更新され，3. へ移る．

以下，各手順の計算結果を述べる．

3. において，行列 α が更新された結果は以下となる：

$$\alpha = \begin{pmatrix} & & & 1_{\mathbb{F}} & * & * & & & \\ 1_{\mathbb{F}} & & & * & & & * & & \\ * & * & * & & * & & * & * & * \end{pmatrix}.$$

4. において，行列 β が更新された結果は以下となる：

$$\beta = \begin{pmatrix} & & & 1_{\mathbb{F}} & 0_{\mathbb{F}} & 1_{\mathbb{F}} & & & \\ * & & & 1_{\mathbb{F}} & & & & 0_{\mathbb{F}} & \\ 1_{\mathbb{F}} & 0_{\mathbb{F}} & 1_{\mathbb{F}} & & 0_{\mathbb{F}} & & 0_{\mathbb{F}} & 0_{\mathbb{F}} & * \end{pmatrix}.$$

5. において，系列 c は以下となる：

$$c = (1_{\mathbb{F}}, 0_{\mathbb{F}}, 1_{\mathbb{F}}, 1_{\mathbb{F}}, 0_{\mathbb{F}}, 1_{\mathbb{F}}, 0_{\mathbb{F}}, 0_{\mathbb{F}}, *).$$

6. において，c に $*$ が含まれるため次の手順へ進む．

7. において，$l = 2, l_{\max} = 20$ であるから不等式 $l > l_{\max}$ は成立しない．次

の手順へ進む.

8. において，$l = 3$ に更新され，3. へ移る．

3. において，行列 α が更新された結果は以下となる：

$$\alpha = \begin{pmatrix} & & & 1_{\mathbb{F}} & 0_{\mathbb{F}} & 1_{\mathbb{F}} & & & \\ 1_{\mathbb{F}} & & & * & & & * & & \\ * & * & * & & * & & * & * & 0_{\mathbb{F}} \end{pmatrix}.$$

4. において，行列 β が更新された結果は以下となる：

$$\beta = \begin{pmatrix} & & & * & 0_{\mathbb{F}} & 1_{\mathbb{F}} & & & \\ * & & & 1_{\mathbb{F}} & & & & 0_{\mathbb{F}} & \\ 1_{\mathbb{F}} & 0_{\mathbb{F}} & 1_{\mathbb{F}} & & 0_{\mathbb{F}} & & 0_{\mathbb{F}} & 0_{\mathbb{F}} & * \end{pmatrix}.$$

5. において，系列 c の結果は以下となる：

$$c = (1_{\mathbb{F}}, 0_{\mathbb{F}}, 1_{\mathbb{F}}, 1_{\mathbb{F}}, 0_{\mathbb{F}}, 1_{\mathbb{F}}, 0_{\mathbb{F}}, 0_{\mathbb{F}}, 0_{\mathbb{F}}).$$

6. において，c に $*$ が含まれないのでシンドロームを計算する．実際に計算すれば，$Hc^T = \mathbf{0}$ の成立が確かめられる．よって，$c = (1_{\mathbb{F}}, 0_{\mathbb{F}}, 1_{\mathbb{F}}, 1_{\mathbb{F}}, 0_{\mathbb{F}}, 1_{\mathbb{F}}, 0_{\mathbb{F}}, 0_{\mathbb{F}}, 0_{\mathbb{F}}, 0_{\mathbb{F}})$ を出力し，停止する．

定義 9.7 (**最大反復回数，反復**)　訂正無し。

注意 9.8　訂正無し。

注意 9.9　訂正無し。

注意 9.10　訂正無し。

定義 9.11 (**疎行列，LDPC 符号**)　訂正無し。

9.3 消失通信路に対する密度発展法

注意 9.12 訂正無し。

定義 9.13 ((λ, ρ) **正則 LDPC 符号，設計符号化率**) 訂正無し。

いよいよ密度発展法の説明に入る．整数 m_0, n_0 をパリティ検査行列 H の (m_0, n_0) 成分 h_{m_0,n_0} に関して $h_{m_0,n_0} = 1$ が従う整数の組みとする．sum-product 復号で登場した行列 α, β の (m_0, n_0) 成分に着目しよう．

行列 H と消失誤り率 p が与えられたとし，sum-product 復号において，成分 $\alpha_{m_0,n_0}, \beta_{m_0,n_0}$ が $\alpha_{m_0,n_0} = *$ もしくは $\beta_{m_0,n_0} = *$ となる確率を考察し，sum-product 復号における反復ごとの考察も行おう．

- 受信語の考察：まず，受信語 y の第 n_0 成分 y_{n_0} に関して $y_{n_0} = *$ となる確率を求めよう．元来の符号語によらず，受信語の第 n_0 成分 y_{n_0} が記号 $*$ である確率は，通信路の消失誤り率 $p_0 := p$ と等しい．
- 初期化：sum-product 復号の定義から，成分 β_{m_0,n_0} は y_{n_0} そのものとして定義される．よって，$\beta_{m_0,n_0} = *$ となる確率は p と等しい．
- 最初の行処理：行処理の定義により，

  $$\alpha_{m_0,n_0} := \mathrm{SUM}(\{\beta_{m_0,n_1} \mid n_1 \in V(m_0) \setminus \{m_0\}\})$$

  が従う．行処理の結果，$\alpha_{m_0,n_0} = *$ であるか否かは $\{\beta_{m_0,n_1} \mid n_1 \in V(m_0) \setminus \{n_0\}\}$ に依存する．それら $\rho - 1$ 個の成分中に 1 つでも $*$ があれば，$\alpha_{m_0,n_0} = *$ が従う．1 つもなければ $\alpha_{m_0,n_0} \neq *$ が従う．

  行列 β において，特定の成分が $*$ である確率は p であるから，$\alpha_{m_0,n_0} \neq *$ の確率は

  $$(1 - \text{「成分が } * \text{ である確率」})^{(m_0,n_0) \text{ 成分以外の成分数}} = (1-p)^{\rho-1}$$

  と表せる．一方で成分 α_{m_0,n_0} は $*$ か $\mathbb{F}_2$ のどちらかであるから，$\alpha_{m_0,n_0} = *$ となる確率は次で表せる：

  $$1 - (1-p)^{\rho-1}.$$

- 最初の列処理：列処理の定義により，

$$\beta_{m_0,n_0} := \mathrm{PROD}(y_{n_0}, \{\alpha_{m_1,n_0} \mid m_1 \in F(n_0) \setminus \{m_0\}\})$$

が従う．列処理の結果，$\beta_{m_0,n_0} = *$ であるか否かは y_{n_0}，および，$\{\alpha_{m_1,n_0} \mid m_1 \in F(n_0) \setminus \{m_0\}\}$ に依存する．それらすべてが $*$ であるとき，かつ，そのときに限り $\beta_{m_0,n_0} = *$ が従う．そして，y_{n_0} が $*$ である確率は受信語の考察で見た通りに p である．

その他の $\lambda - 1$ 個の成分に関して，それぞれが $*$ である確率は $1-(1-p)^{\rho-1}$ である．よって，$\lambda - 1$ 個の成分すべてが $*$ である確率は $(1-(1-p)^{\rho-1})^{\lambda-1}$ である．

これらの考察から，$\beta_{m_0,n_0} = *$ である確率をおおざっぱに計算すれば，

$$p(1-(1-p)^{\rho-1})^{\lambda-1}$$

と表せる [1)]．この値を p_1 と書くことにする．

- l 回目の行処理 ($l \geqq 2$)：最初の行処理と同じ考え方で計算すれば，$\beta_{m_0,n_0} = *$ の確率は次で表せる：

$$1-(1-p_{l-1})^{\rho-1}.$$

- l 回目の列処理：最初の列処理と同じ考え方で計算すれば，$\alpha_{m_0,n_0} = *$ の確率は

$$p(1-(1-p_{l-1})^{\rho-1})^{\lambda-1}$$

と表せる．この値を p_l と書くことにする．

以上から，l 回目の反復時に $\beta_{m_0,n_0} = *$ となる確率 p_l がおおざっぱに得られた．具体的には以下である．

$$p_l = \begin{cases} p & (l=0) \\ p(1-(1-p_{l-1})^{\rho-1})^{\lambda-1} & (l \geqq 1) \end{cases} \tag{9.2}$$

上の計算を**密度発展法**とよぶ．

[1)] 実際にはこの計算は正しい値を与えない．各行の相関を考慮していないためである．

例 9.14 訂正無し。

例 9.15 訂正無し。

注意 9.16 訂正無し。

9.4 正則 LDPC 符号の構成法

補題 9.17 訂正無し。

例 9.18 (シャッフルを用いた構成) 訂正無し。

例 9.19 訂正無し。

定義 9.20 (置換行列) 訂正無し。

例 9.21 (置換行列を用いた構成) 訂正無し。

定義 9.22 (巡回置換行列) 訂正無し。

例 9.23 (巡回置換行列を用いた構成) 正則 LDPC 符号を構成する方法として，成分がすべて 1 の行列に対し，その 1 を置換行列に置き換える方法を述べた (例 9.21)．特に，その置換行列がいずれも巡回置換行列であるときに，その符号を**準巡回 LDPC 符号**とよぶ．

$(2,5)$ 正則 LDPC 符号を準巡回 LDPC 符号として構成しよう．ここでは，巡回置換行列のサイズを 4×4 とする．

$$\begin{pmatrix}
\bar{\mathbf{1}} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \bar{\mathbf{1}} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \bar{\mathbf{1}} & 0 \\
0 & \bar{\mathbf{1}} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \bar{\mathbf{1}} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \bar{\mathbf{1}} \\
0 & 0 & \bar{\mathbf{1}} & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \bar{\mathbf{1}} & 0 & 0 & 0 & 0 & 1 & \bar{\mathbf{1}} & 0 & 0 & 0 \\
0 & 0 & 0 & \bar{\mathbf{1}} & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \bar{\mathbf{1}} & 1 & 0 & 0 & 0 & 0 & \bar{\mathbf{1}} & 0 & 0 \\
0 & 0 & 1 & 0 & \bar{\mathbf{1}} & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \bar{\mathbf{1}} & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & \bar{\mathbf{1}} & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \bar{\mathbf{1}} & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & \bar{\mathbf{1}} & 0 & 0 & 1 & 0 & 0 & \bar{\mathbf{1}} & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & \bar{\mathbf{1}} & 0 & 0 & 1 & 0 & 0 & \bar{\mathbf{1}} & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

巡回置換行列を表す先の記法 $I(a)$ の a によって，上の行列を表現すれば

$$\begin{pmatrix}
0 & 2 & 0 & 1 & 2 \\
2 & 0 & 3 & 2 & 0
\end{pmatrix}$$

と特徴付けられる．このように，置き換えに用いる巡回置換行列のパラメータ a を列挙した行列を**モデル行列**とよぶ．

注意 9.24　訂正無し。

例 9.25　訂正無し。

9.5　タナーグラフ

定義 9.26 (**二部グラフ**)　訂正無し。

定義 9.27 (**タナーグラフ**)　訂正無し。

定義 9.28 (**頂点集合，辺集合，チェックノード，変数ノード，辺**)　訂正無し。

定義 9.29 (**タナーグラフの図示**)　訂正無し。

例 9.30 訂正無し。

注意 9.31 訂正無し。

定義 9.32 (次数) 訂正無し。

定義 9.33 (連結，経路) 訂正無し。

定義 9.34 (サイクル) 訂正無し。

例 9.35 訂正無し。

定義 9.36 (最小内径) 訂正無し。

注意 9.37 訂正無し。

9.6 木と周辺事後確率計算

定義 9.38 (木) 訂正無し。

注意 9.39 訂正無し。

定義 9.40 (事後確率, 受信可能系列) $W : \mathcal{Y} \times \mathcal{X} \to \mathbb{R}$ を通信路，n を正整数，P を $\mathcal{X}^n$ 上の分布とする．

系列 $y \in \mathcal{Y}^n$ と通信路 W と分布 P に対し，関数 $P^W(\,|y) : \mathcal{X}^n \to \mathbb{R}$ を分母が 0 でないときに限り，以下で定義する：

$$P^W(x|y) := \frac{P(x)W(y|x)}{\sum_{x' \in \mathcal{X}^n} P(x')W(y|x')}. \qquad (x \in \mathcal{X}^n)$$

上の式の分母が 0 とならない系列 y を**受信可能系列**とよび，それら全体を

$\mathcal{Y}_r^n$ で表す．y を固定すれば，$P^W(\,|y)$ は $\mathcal{X}^n$ 上の分布になる．$P^W(\,|y)$ を W と y に対する**事後確率分布**とよぶ．

例 9.41 $W : \{0,1\} \times \{0,1\} \to \mathbb{R}$ を二元対称通信路，$P : \{0,1\} \to \mathbb{R}$ を一様分布とする．$x, y \in \{0,1\}$ に対して P^W は以下のようになる：

$$P^W(x|y) = \begin{cases} 1-p & (x = y) \\ p & (x \neq y) \end{cases}$$

例 9.42 $W : \{0,1\} \times \{0,1,*\} \to \mathbb{R}$ を二元消失通信路，$P : \{0,1\} \to \mathbb{R}$ を一様分布とする．$x \in \{0,1\}$ と $y \in \{0,1,*\}$ に対して P^W は以下のようになる：

$$P^W(x|y) = \begin{cases} \frac{1}{2} & (y = *) \\ 1 & (y \neq *, x = y) \\ 0 & (y \neq *, x \neq y) \end{cases}$$

例 9.43 $C \subset \mathcal{X}^n$ を部分集合とし，$\mathcal{X}^n$ 上の分布 $P^{(C)}$ を

$$P^{(C)}(x) := \begin{cases} \frac{1}{|C|} & (x \in C) \\ 0 & (x \notin C) \end{cases} \tag{9.3}$$

としよう．このとき，事後確率分布は

$$P^{(C)W}(x|y) = \begin{cases} \frac{W(y|x)}{\sum_{c \in C} W(y|c)} & (x \in C) \\ 0 & (x \notin C) \end{cases} \tag{9.4}$$

と表せる．以降，集合 C に対して $P^{(C)}$ を上記の意味で用いる．

定義 9.44 (最大事後確率復号 (MAP 復号)) $W : \mathcal{Y} \times \mathcal{X} \to \mathbb{R}$ を通信路，(f, ϕ_{MAP}) を W 上の通信路符号，n を (f, ϕ_{MAP}) の符号長，$\mathcal{M}$ を (f, ϕ_{MAP})

のメッセージ集合，$P : \mathcal{X}^n \to \mathbb{R}$ を分布とする．

復号写像 ϕ_{MAP} が**最大事後確率 (maximum a posteriori probability) 復号**であるとは，次の条件を満たすことをいう．

条件：任意の受信可能系列 $y \in \mathcal{Y}_r^n$ に対して次の等式を満たす：

$$P^W(f(\phi_{MAP}(y))|y) = \max_{M \in \mathcal{M}} P^W(f(M)|y).$$

補題 9.45 符号語の生起確率が一様分布に従うとき，最大事後確率復号は最尤復号である．

証明 最大事後確率復号の定義は事後確率を最大にするメッセージを出力する復号である．そこで，事後確率の定義に注目する．符号語の生起確率が一様分布であるなら，例 9.4.3 の式 (9,4) より，

$$P^{(C)W}(x|y) = \begin{cases} \dfrac{W^n(y|x)}{\sum\limits_{c \in C} W^n(y|c)} & (x \in C) \\ 0 & (x \notin C) \end{cases}$$

が従う．系列 y が与えられたとき，分母は定数であることに注意しよう．よって，事後確率を最大にすることは，分子を最大にすることと同値である．そしてこの分子を最大にする復号は，最尤復号の定義そのものである． □

補題 9.46 $\mathbb{F}_2$ を二元体，$\mathcal{Y}$ を有限集合，$W : \mathcal{Y} \times \mathbb{F}_2 \to \mathbb{R}$ を通信路，H をサイズ $m \times n$ の $\mathbb{F}_2$ 上の行列，C を H が与える線型符号とする．

このとき，任意の系列 $x \in \mathbb{F}_2^n$, 任意の受信可能系列 $y \in \mathcal{Y}_r^n$ に対する事後確率 $P^{(C)W}(\,|y)$ に関して，以下が従う：

$$P^{(C)W}(x|y) = K\left(\prod_{m_0=1}^{m} \delta\left[\sum_{\nu \in V(m_0)} x_\nu = 0\right]\right)\left(\prod_{n_1=1}^{n} W(y_{n_1}|x_{n_1})\right).$$

ただし，K は $\sum\limits_{x \in \mathbb{F}_2^n} P^{(C)W}(x|y) = 1$ を満たすように正規化する定数を表し，$\delta[\,]$ は $[\,]$ 内の等式が成立するときに実数 1 を与え，不成立のときに実数 0 を

与える関数とする．

証明　例 9.4.3 の式 (9,4) より，事後確率は

$$P^{(C)W}(x|y) = \begin{cases} \dfrac{W(y|x)}{\sum\limits_{c\in C} W(y|c)} & (x \in C) \\ 0 & (x \notin C) \end{cases}$$

と表せた．正規化する定数を K で表し，通信路の独立性に注目することで，上の式は

$$P^{(C)W}(x|y) = \begin{cases} KW(y|x) = K\prod\limits_{n_1=1}^{n} W(y_{n_1}|x_{n_1}) & (x \in C) \\ 0 & (x \notin C) \end{cases}$$

と表せる．ただし，$x = (x_1, x_2, \cdots, x_n), y = (y_1, y_2, \cdots, y_n)$ を表す．ここで，主張の式と右辺を見比べれば，右辺が主張の式と一致するためには

$$\prod_{m_0=1}^{m} \delta\left[\sum_{\nu\in V(m_0)} x_\nu = 0\right] = \begin{cases} 1 & (x \in C) \\ 0 & (x \notin C) \end{cases}$$

が従えばよい．ところで，$\prod\limits_{m_0=1}^{m} \delta\left[\sum\limits_{\nu\in V(m_0)} x_\nu = 0\right]$ は Hx^T のすべての成分が 0 であるとき，そして，そのときに限り 1 である．言い換えれば $x \in C$ であるとき，そして，そのときに限り 1 をとる．

以上から主張を得た．　□

定義 9.47 (**周辺事後確率**)　n を正整数，$W : \mathcal{Y} \times \mathcal{X} \to \mathbb{R}$ を通信路，$P : \mathcal{X} \to \mathbb{R}$ を分布，$y \in \mathcal{Y}_r^n$ を受信可能系列とし，$P^W(\,|y) : \mathcal{X}^n \to \mathbb{R}$ を W と y に関する事後確率分布とする．

事後確率分布 $P^W(\,|y)$ と正整数 $1 \leqq n_0 \leqq n$ に対して，分布 $P_{n_0}^W(\,|y) : \mathcal{X} \to \mathbb{R}$ を以下で定義する：

$$P_{n_0}^W(x_{n_0}|y) := \sum_{x/[n]\setminus\{n_0\}} P^W(x|y). \qquad (x_{n_0} \in \mathcal{X})$$

ただし，

$$\sum_{x/[n]\setminus\{n_0\}} := \sum_{x_1\in\mathcal{X}} \cdots \sum_{x_{n_0-1}\in\mathcal{X}} \sum_{x_{n_0+1}\in\mathcal{X}} \cdots \sum_{x_n\in\mathcal{X}}$$

を表す．つまり，x_{n_0} を除いた範囲で和を計算する．

分布 $P_{n_0}^W(\,|y)$ を (事後確率分布 P と系列 y と第 n_0 成分に関する) **周辺事後確率分布**とよぶ．

定義 9.48 (**周辺事後確率復号 (MPM(maximum posterior marginal) 復号)**) W を通信路，(f,ϕ_{MPM}) を W 上の通信路符号，n を (f,ϕ_{MPM}) の符号長，$P:\mathcal{X}\to\mathbb{R}$ を分布，$\mathcal{M}$ を (f,ϕ_{MPM}) のメッセージ集合，$\mathcal{Y}$ を (f,ϕ_{MPM}) の受信アルファベットとする．

復号写像 ϕ_{MPM} が**周辺事後確率復号**であるとは，次の条件を満たすことをいう．

条件：任意の受信可能系列 $y\in\mathcal{Y}_r^n$ と任意の正整数 $1\leqq n_0\leqq n$ に対して，次の等式を満たす：

$$P_{n_0}^W(c_{n_0}|y)=\max_{x\in\mathcal{X}} P_{n_0}^W(x|y).$$

ただし，$f(\phi_{MPM}(y))=(c_1,c_2,\cdots,c_n)$ を表す．

以下，数式 $\delta\left[\sum_{\nu\in V(m_0)} x_\nu=0\right]$ を簡略化して $\delta[x/V(m_0)]$ と表すことにする．

定理 9.49 (**一時推定の正当化**) $\mathbb{F}_2$ を二元体，H をサイズ $m\times n$ の $\mathbb{F}_2$ 上の行列であってそのタナーグラフが木であるとする．$W:\mathcal{Y}\times\mathbb{F}_2\to\mathbb{R}$ を通信路，C を H の定める線型符号，$P^{(C)}:\mathbb{F}_2^n\to\mathbb{R}$ を例 9.4.3 で定めた分布，y を $\mathcal{Y}$ 上の長さ n の受信可能系列，n_0 を条件 $1\leqq n_0\leqq n$ を満たす正整数，$P_{n_0}^W(\,|y):\mathbb{F}_2\to\mathbb{R}$ を第 n_0 成分に関する周辺事後確率分布とする．

正整数 $1\leqq m_0\leqq m$ と n_0 に対して，関数 $\alpha_{m_0,n_0}:\mathbb{F}_2\to\mathbb{R}$ を以下で定義する：

$$\alpha_{m_0,n_0}(x_{n_0}) := \sum_{x/V(m_0,n_0)\setminus\{n_0\}} \left(W(y/V(m_0,n_0)\setminus\{n_0\}|x/V(m_0,n_0)\setminus\{n_0\}) \times \prod_{m_0^*\in F(m_0,n_0)} \delta[x/V(m_0^*)] \right)$$

ただし，右辺の $\sum$ の右側にある式の変数は $x/V(m_0,n_0)$ とし，$V(m_0,n_0)$ の定義はやや複雑なため，証明中に記載している．

このとき，以下が従う：

$$P_{n_0}^{(C)W}(x_{n_0}|y) = KW(y_{n_0}|x_{n_0}) \prod_{m_0\in F(n_0)} \alpha_{m_0,n_0}(x_{n_0}).$$

ただし，K は補題 9.46 の K であり，次の右辺と一致する．

$$K := 1/\left(W(y_{n_0}|0) \prod_{m_1\in F(n_0)} \alpha_{m_1,n_0}(0) + W(y_{n_0}|1) \prod_{m_1\in F(n_0)} \alpha_{m_1,n_0}(1) \right)$$

証明　周辺事後確率の定義に従い

$$P_{n_0}^{(C)W}(x_{n_0}|y) := \sum_{x/[n]\setminus\{n_0\}} P^{(C)W}(x|y)$$

と表す．パリティ検査行列が与える線型符号では，事後確率をいくつかの条件の積で表せる (補題 9.46) ことに着目し，右辺を変形すれば

$$P_{n_0}^{(C)W}(x_{n_0}|y) = K \sum_{x/[n]\setminus\{n_0\}} W(y_{[n]}|x_{[n]}) \prod_{m_0=1}^{m} \delta[x/V(m_0)]$$

が従う．和が x_{n_0} 以外の変数に関して動くことから

$$P_{n_0}^{(C)W}(x_{n_0}|y) = KW(y_{n_0}|x_{n_0}) \times \sum_{x/[n]\setminus\{n_0\}} W(y_{[n]\setminus\{n_0\}}|x_{[n]\setminus\{n_0\}}) \prod_{m_0=1}^{m} \delta[x/V(m_0)]$$

と表せる．

ところで，タナーグラフが木であることを仮定している．木の性質を利用してチェックノードの集合の分割を与える．この分割は，図 9.7 を参照しながら考えるとわかりやすい．タナーグラフから，変数ノード v_{n_0} および (f, v_{n_0}) と表される辺をすべて取り除いた状況を考える．すると，新しくできるタナー

グラフは「v_{n_0} の次数個の連結したグラフ」となる．図 9.7 でいえば，最上段の頂点およびそこから伸びている辺を除くことで，2 段目以降が残るという意味である．このとき，各連結したグラフは $F(n_0)$ の元を 1 つずつもつとして特徴付けられる．そこで，各元 $f_{m_0} \in F(n_0)$ に対して，f_{m_0} を含むタナーグラフのチェックノード全体を $F(m_0, n_0)$ と表す．また，そのタナーグラフの変数ノード全体および v_{n_0} からなる集合を $V(m_0, n_0)$ と表そう．図では最上段に注目しているが，そうでなくともこのような定義は可能である．実際，図では $F(m_1, n_1)$ を含む領域を与えている．

さて，このような分割の下で

$$\prod_{m_0=1}^{m} = \prod_{m_0 \in F(n_0)} \prod_{m_0^* \in F(m_0, n_0)}$$

と表せる．この事実に注目して，先の右辺を変形すれば

$$\begin{aligned} P_{n_0}^W(x_{n_0}|y) = KW(y_{n_0}|x_{n_0}) \\ \times \sum_{x/[n]\setminus\{n_0\}} W(y_{[n]\setminus\{n_0\}}|x_{[n]\setminus\{n_0\}}) \\ \times \prod_{m_0 \in F(n_0)} \prod_{m_0^* \in F(m_0, n_0)} \delta[x/V(m_0^*)] \end{aligned}$$

が従う．タナーグラフが木であることを仮定しているから，

$$[n] \setminus \{n_0\} = \bigsqcup_{m_0 \in F(n_0)} (V(m_0, n_0) \setminus \{n_0\})$$

と分割できる．この事実に注目して，右辺の和と積の順序および和の範囲を変更すれば

$$\begin{aligned} & P_{n_0}^W(x_{n_0}|y) \\ & \quad = KW(y_{n_0}|x_{n_0}) \\ & \qquad \times \prod_{m_0 \in F(n_0)} \left(\sum_{x/V(m_0, n_0)\setminus\{n_0\}} W(y/V(m_0, n_0) \setminus \{n_0\}|x/V(m_0, n_0) \setminus \{n_0\}) \right. \\ & \qquad\qquad \left. \times \prod_{m_0^* \in F(m_0, n_0)} \delta[x/V(m_0^*)] \right) \end{aligned}$$

が従う．関数 α_{m_0,n_0} の定義から

$$P_{n_0}^W(x_{n_0}|y) = KW(y_{n_0}|x_{n_0}) \prod_{m_0 \in F(n_0)} \alpha_{m_0,n_0}(x_{n_0})$$

を得た． □

定理 9.50 (**列処理および行処理の正当化**) 補題と同じ記号のもと，関数 $\beta_{m_0,n_0} : \mathbb{F}_2 \to \mathbb{R}$ を以下で定義する：

$$\beta_{m_0,n_0}(x_{n_0}) := W(y_{n_0}|x_{n_0}) \prod_{m_1 \in F(n_1)\setminus\{m_0\}} \alpha_{m_1,n_0}(x_{n_0}).$$

このとき，以下が従う：

$$\alpha_{m_0,n_0}(x_{n_0}) = \sum_{x/V(m_0)\setminus\{n_0\}} \delta[x/V(m_0)] \prod_{n_1 \in V(m_0)\setminus\{n_0\}} \beta_{m_0,n_1}(x_{n_1}).$$

証明 タナーグラフが木という仮定から

$$F(m_0,n_0)\setminus\{m_0\} = \bigsqcup_{n_1 \in V(m_0)\setminus\{n_0\}} \bigsqcup_{m_1 \in F(n_1)\setminus\{m_0\}} F(m_1,n_1)$$

と分割できることに注意しよう．この事実に注意して，関数 α_{m_0,n_0} の定義を変形すれば

$$\begin{aligned}
&\alpha_{m_0,n_0}(x_{n_0}) \\
&\quad = \sum_{x/V(m_0,n_0)\setminus\{n_0\}} \delta[x/V(m_0)] W(y/V(m_0,n_0)\setminus\{n_0\}|x/V(m_0,n_0)\setminus\{n_0\}) \\
&\qquad \times \prod_{n_1 \in V(m_0)\setminus\{n_0\}} \prod_{m_1 \in F(n_1)\setminus\{m_0\}} \prod_{m_1^* \in F(m_1,n_1)} \delta[x/V(m_1^*)]
\end{aligned}$$

が従う．右辺の $W(y/V(m_0,n_0)\setminus\{n_0\}|x/V(m_0,n_0)\setminus\{n_0\})$ を分割すれば

$$\begin{aligned}
\alpha_{m_0,n_0}(x_{n_0}) = &\sum_{x/V(m_0,n_0)\setminus\{n_0\}} \delta[x/V(m_0)] \prod_{n_1 \in V(m_0)\setminus\{n_0\}} W(y_{n_1}|x_{n_1}) \\
&\times \prod_{m_1 \in F(n_1)\setminus\{m_0\}} W(y/V(m_1,n_1)\setminus\{n_1\}|x/V(m_1,n_1)\setminus\{n_1\}) \\
&\times \prod_{m_1^* \in F(m_1,n_1)} \delta[x/V(m_1^*)]
\end{aligned}$$

が従う.

分配法則によって $\sum, \prod$ を交換すれば,

$$\begin{aligned}
&\alpha_{m_0,n_0}(x_{n_0}) \\
&\quad = \sum_{x/V(m_0)\setminus\{n_0\}} \delta[x/V(m_0)] \prod_{n_1\in V(m_0)\setminus\{n_0\}} W(y_{n_1}|x_{n_1}) \\
&\qquad \times \prod_{m_1\in F(n_1)\setminus\{m_0\}} \left(\sum_{x/V(m_1,n_1)\setminus\{n_1\}} \delta[x/V(m_1)] \right. \\
&\qquad\qquad \left. \times W(y/V(m_1,n_1)\setminus\{n_1\}|x/V(m_1,n_1)\setminus\{n_1\}) \right) \\
&\qquad \times \prod_{m_1^*\in F(m_1,n_1)} \delta[x/V(m_1^*)] \\
&\quad = \sum_{x/V(m_0)\setminus\{n_0\}} \delta[x/V(m_0)] \prod_{n_1\in V(m_0)\setminus\{n_0\}} W(y_{n_1}|x_{n_1}) \\
&\qquad \times \prod_{m_1\in F(n_1)\setminus\{m_0\}} \alpha_{m_1,n_1}(x_{n_1})
\end{aligned}$$

となる. ここで, $\beta_{m_0,n_1}(x_{n_1})$ を用いて右辺を変形すれば

$$\alpha_{m_0,n_0}(x_{n_0}) = \sum_{x/V(m_0)\setminus\{n_0\}} \delta[x/V(m_0)] \prod_{n_1\in V(m_0)\setminus\{n_0\}} \beta_{m_0,n_1}(x_{n_1})$$

を得た. □

9.7 確率領域 sum-product 復号法

定義 9.51 (**(確率領域) sum-product 復号法**)

* 入力： $\mathbb{F}_2$ 上の行列 $H=(h_{m_0,n_0})$，通信路 $W:\mathcal{Y}\times\mathbb{F}_2\to\mathbb{R}$，$\mathcal{Y}$ 上の系列 y，整数 $l_{\max}$.
* 出力： H が与える線型符号 C の符号語 c もしくは記号 ?.

1. H の列数と y の長さが異なれば停止する．以降，行列 H のサイズを $m\times n$ とする．
2. 初期化：$h_{m_0,n_0}=1$ を満たすすべての組 (m_0,n_0) に対して，実数 $\beta_{m_0,n_0}(0),\beta_{m_0,n_0}(1)$ を以下で定義する：
$$\beta_{m_0,n_0}(x):=W(y_{n_0}|x).$$
ただし，$x\in\{0,1\}$．また，(反復回数のカウンタとして) $l:=1$ と定義する．
3. 行処理：$h_{m_0,n_0}=1$ を満たすすべての組 (m_0,n_0) に対して，実数 $\alpha_{m_0,n_0}(0),\alpha_{m_0,n_0}(1)$ を定義する．
$$\alpha_{m_0,n_0}(x):=K\sum_{c/V(m_0)\setminus\{n_0\}}\delta\left[\sum_{\nu\in V(m_0)\setminus\{n_0\}}c_\nu=x\right]\times\prod_{n_1\in V(m_0)\setminus\{n_0\}}\beta_{m_0,n_1}(c_{n_1})$$
ここで，$x\in\{0,1\}$，定数 K は $\alpha_{m_0,n_0}(0)+\alpha_{m_0,n_0}(1)=1$ を満たすよう定める．
4. 列処理：$h_{m_0,n_0}=1$ を満たすすべての組 (m_0,n_0) に対して，改めて $\beta_{m_0,n_0}(0)$ と $\beta_{m_0,n_0}(1)$ を定義する．
$$\beta_{m_0,n_0}(x):=K'W(y_{n_0}|x)\prod_{m_1\in F(n_0)\setminus\{m_0\}}\alpha_{m_1,n_0}(x)$$
ここで，$x\in\{0,1\}$，定数 K' は $\beta_{m_0,n_0}(0)+\beta_{m_0,n_0}(1)=1$ を満たすように定める．

5. 一時推定：各整数 $1\leqq n_0\leqq n$ に対して，実数 $\gamma_{n_0}(0),\gamma_{n_0}(1)$ を
$$\gamma_{n_0}(x):=W(y_{n_0}|x)\prod_{m_1\in F(n_0)}\alpha_{m_1,n_0}(x)$$
と定義する．ただし $x\in\{0,1\}$ とする．そして，$\gamma_{n_0}(0)\geqq\gamma_{n_0}(1)$ のとき，二元体 $\mathbb{F}_2$ の元 $\hat{c}_{n_0}$ を $\hat{c}_{n_0}:=0$，それ以外のときは $\hat{c}_{n_0}:=1$ と定義する．
6. パリティ検査：等式 $H(\hat{c}_1,\hat{c}_2,\cdots,\hat{c}_{n_0})^T=0$ を満たせば $c:=(\hat{c}_1,\hat{c}_2,\cdots,\hat{c}_{n_0})$ を出力する．そうでなければ 7. へ，
7. $l\geqq l_{max}$ ならば，? を出力して停止する．
8. もし $l<l_{max}$ ならば，変数 l の値 1 つ増やして 3. (行処理) へ．

9.8 対数領域 sum-product 復号法

定義 9.52 (対数領域 sum-product 復号法)

* 入力： $\mathbb{F}_2$ 上の行列 $H = (h_{m_0,n_0})$，通信路 $W : \mathcal{Y} \times \mathbb{F}_2 \to \mathbb{R}$，$\mathcal{Y}$ 上の系列 y，整数 $l_{\max}$.
* 出力： H が与える線型符号 C の符号語 c もしくは記号 ?.

1. H の列数と y の長さが異なれば停止する．以降，行列 H のサイズを $m \times n$ とする.
2. 初期化：各 $1 \leqq n_0 \leqq n$ に対して，実数 λ_{n_0} を次で定義する：

$$\lambda_{n_0} := \log_2 \frac{W(y_{n_0}|0)}{W(y_{n_0}|1)}.$$

そして，$h_{m_0,n_0} = 1$ を満たすすべての組 (m_0, n_0) に対して，$\beta_{m_0,n_0} := \lambda_{n_0}$ と定義する．また，反復回数のカウンタとして $l := 1$ と定義する．

3. 行処理：$h_{m_0,n_0} = 1$ を満たすすべての組 (m_0, n_0) に対して，実数 α_{m_0,n_0} を次で定義する：

$$\alpha_{m_0,n_0} := \left(\prod_{n_1 \in V(m_0)\setminus\{n_0\}} \mathrm{sgn}(\beta_{m_0,n_1})\right) \mathrm{GA}\left(\sum_{n_1 \in V(m_0)\setminus\{n_0\}} \mathrm{GA}(|\beta_{m_0,n_1}|)\right)$$

ただし $\mathrm{sgn}(a) := 1 (a \in \mathbb{R}$ かつ $a \geqq 0$ が従うとき)，もしくは，$\mathrm{sgn}(a) := -1$ (その他) を表す．さらに，$\mathrm{GA}(a)$ は次の実数を表す：

$$\mathrm{GA}(a) := \log_2 \frac{\exp_2(a) + 1}{\exp_2(a) - 1}.$$

4. 列処理：$h_{m_0,n_0} = 1$ を満たすすべての組 (m_0, n_0) に対して，β_{m_0,n_0} を改めて定義する：

$$\beta_{m_0,n_0} := \lambda_{n_0} + \sum_{m_1 \in F(n_0)\setminus\{m_0\}} \alpha_{m_1,n_0}.$$

5. 一時推定：各 $1 \leqq n_0 \leqq n$ に対して

$$\gamma_{n_0} := \lambda_{n_0} + \sum_{m_1 \in F(n_0)} \alpha_{m_1,n_0}$$

と定義する．そして，$\gamma_{n_0} \geqq 0$ のとき，二元体 $\mathbb{F}_2$ の元 $\hat{c}_{n_0}$ を $\hat{c}_{n_0} := 0$ と，それ以外のときには $\hat{c}_n := 1$ と定義する．

6. パリティ検査：等式 $H(\hat{c}_1, \hat{c}_2, \cdots, \hat{c}_{n_0})^T = 0$ を満たせば，$c := (\hat{c}_1, \hat{c}_2, \cdots, \hat{c}_{n_0})$ を出力する．そうでなければ 7. へ．
7. $l \geqq l_{max}$ ならば，? を出力して停止する．
8. もし $l < l_{max}$ ならば，変数 l の値 1 つ増やして 3. (行処理) へ．

注意 9.53 訂正無し。