

確率的情報処理としての移動体通信(2)

ターボ復号法の情報幾何的理解と改善の可能性

池田 思朗

1. はじめに

携帯電話に代表される移動体通信技術は、近年飛躍的に発達している。高品質の通信が安定して利用できるのは、ハードウェアの発達、そして理論的な要素技術の進歩による。前回¹⁾は其中で多元接続を実現するための要素技術 CDMA を扱った。本稿では第3世代移動通信方式から採用されている誤り訂正符号、ターボ符号³⁾を扱う。前回と同様に通信技術の話題だが、ターボ符号もまた興味深い数理的構造を持っている。

ターボ符号は1993年に提案されて以来、その誤り訂正能力の高さから大きな注目を集めている。その特徴は独特な繰り返し計算を用いる「ターボ復号法」にある。様々な実験を通じて有効性を示され実用化されているが、理論的には繰り返し復号法の収束性や安定性などが完全には解明されていない。さらにターボ復号が統計物理学の近似法や人工知能の手法と関係していることも示されている。これらの手法も数理的には解明されていない点が多く含まれる。したがってターボ符号は分野横断的な立場からも興味ある問題を含んでいる。本稿ではターボ符号の問題を説明し、我々が行なっている情報幾何学^{1,2)}を用いた解析⁵⁻⁷⁾を紹介する。

2. 誤り訂正符号とターボ符号

2.1 誤り訂正符号

デジタル通信では、一般に通信路にノイズが生じ、受信側では送信側と完全に同じデータを受け取ることができない。ノイズによって多少データに誤りが生じても、受け取った側で訂正する技術が誤り訂正符号である。誤りを訂正するためには、送るデータに冗長性を持たせる必要がある。



図1 検査語による誤り訂正

図1は検査語を用いた誤り訂正の全体図である。送信したい情報(情報語)を x と書く。本稿では x は2値のベクトル、 $x = (x_1, \dots, x_N)^T (x_i \in \{-1, +1\})$ とする。図中の $y = (y_1, \dots, y_L)^T (y_i \in \{-1, +1\})$ は検査語と呼ばれる。これは x の関数であり、必要であれば $y(x)$ と表現する。この2つのベクトル(送信語)を送信する(図2)。 (x, y) は $N+L$ の長さを持つが y が x の関数であることから 2^N の値しかとらない。したがって送信語は 2^{N+L} の空間の中に疎らにしか存在せず、冗長である。

(x, y) が通信路を通る際、送信された情報には通信路のノイズによる誤りが生じ、受信語は (\tilde{x}, \tilde{y}) となるとする $(\tilde{x} = (\tilde{x}_1, \dots, \tilde{x}_N)^T, \tilde{y} =$

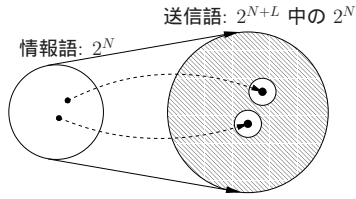


図2 送信語: 情報語と検査語

$(\tilde{y}_1, \dots, \tilde{y}_L)^T$. 通信路の性質により (\tilde{x}, \tilde{y}) は実

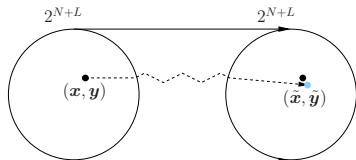


図3 送信語と受信語

ベクトルとなる場合もあるが, ここでは簡単のため $\tilde{x}_i, \tilde{y}_j \in \{-1, +1\}$ の場合を考える. (\tilde{x}, \tilde{y}) は 2^{N+L} の値を取り得る (図3). 誤り訂正符号の目的は (\tilde{x}, \tilde{y}) から x を求めることである.

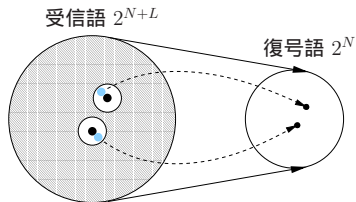


図4 復号: 受信語から情報語を推測する

受信語が何らかの意味で送信語と“近い”ことが期待できるならば, 図4のように, 2^{N+L} のベクトルの中に疎らに存在している送信語の中から最も近いものを選び, 対応する情報語を復号結果として推論するのが適切であろう. これが基本的な復号の考え方である. この“近さ”は, 通信路の性質から定まる. L を大きくとれば一般には送信語はより疎らになり, ノイズに対して頑強となると考えられる. しかし送信語の単位長さあたりに含まれる情報量は減る. L を小さくとり, 高い誤り訂正能力を得るのが理想である. Shannon はこの問題に対して理論的な限界を示した. 証明では, ランダムに構成された符号のなかにこの限界を達成できるものがあることを示しているが, こ

のような符号では 2^N の候補から最適な x を効率的に選ぶ復号法が存在しない. 一方, ターボ復号は符号長 N に対して N の多項式オーダーの計算量で実現可能でありながら, この限界に大変近い誤り訂正能力を示すことが実験によって確かめられている.

2.2 MPM 復号

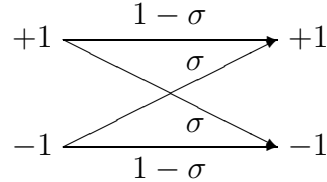


図5 2元対称通信路

通信路のモデルには様々なものがあるが, ここでは簡単のため記憶のない2元対称通信路 (binary symmetric channel: BSC) を考える. 記憶の無い通信路というのは, ノイズが各ビット独立なことである. BSC では各ビットが反対の符号に一定の確率 σ で変わることを仮定する (図5). このように通信路のモデルを用いると $p(\tilde{x}, \tilde{y}|x)$ は簡単に計算できる. 通信路に記憶がないことから

$$p(\tilde{x}, \tilde{y}|x) = p(\tilde{x}|x)p(\tilde{y}|x).$$

送信語, 受信語の各々のビットが $\{-1, +1\}$ であることを用いると, それぞれの分布は

$$\begin{aligned} p(\tilde{x}|x) &= \exp(\beta \tilde{x} \cdot x - N\psi(\beta)) \\ p(\tilde{y}|x) &= \exp(\beta \tilde{y} \cdot \mathbf{y}(x) - L\psi(\beta)), \\ \psi(\beta) &= \ln(e^{-\beta} + e^{\beta}) \end{aligned}$$

と書ける. “ \cdot ” は内積, β は正の実数であり通信路のビットの誤り率 σ との間には $\sigma = (1 - \tanh \beta)/2$ の関係がある. $\mathbf{h} = \beta \tilde{x}$, $c(x) = \beta \tilde{y} \cdot \mathbf{y}(x)$ と置くと,

$$p(\tilde{x}, \tilde{y}|x) = \exp(\mathbf{h} \cdot \mathbf{x} + c(x) - (N + L)\psi(\beta))$$

となる. x の事前分布として一様分布 $p(x) = 1/2^N$ を考えれば x の事後分布は次のようになる

$$p(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) = \frac{p(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}|\mathbf{x})}{\sum_{\mathbf{x}} p(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}|\mathbf{x})} = C \exp(\mathbf{h} \cdot \mathbf{x} + c(\mathbf{x})). \quad (1)$$

この分布から情報語の推論を行う．一つの考え方は $p(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$ を最大にする \mathbf{x} を復号語とする MAP (maximum a posteriori) 推定であるが，ターボ符号の場合は計算量が多く現実的ではない．ターボ符号では MPM (maximum posterior marginal) 復号を目指す．これは $p(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$ から

$$\boldsymbol{\eta} = \sum_{\mathbf{x}} \mathbf{x} p(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}}), \quad \boldsymbol{\eta} = (\eta_1, \dots, \eta_N)^T$$

によって \mathbf{x} の平均をとり η_i の符号によって x_i を復号結果とする．この結果各ビットの誤り率は最小となる．ターボ復号では MPM 復号を効率的に求めることを目的とする．

2.3 ターボ符号

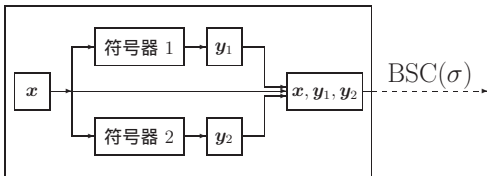


図 6 ターボ符号器の概要

図 6 にターボ符号器の概要を示す．ターボ符号はひとつの符号語に対して 2 つの符号器を用いて 2 つの検査語を作成することが大きな特徴である．それぞれを $\mathbf{y}_1 = (y_{11}, \dots, y_{1L})^T$, $\mathbf{y}_2 = (y_{21}, \dots, y_{2L})^T$, $y_{1j}, y_{2j} \in \{-1, +1\}$ とする． \mathbf{y}_r , $r = 1, 2$ は \mathbf{x} の関数である．それぞれの符号器は同等だが，符号器の入力となる \mathbf{x} のビット列の順番をインターリーバによって入れ換えている．したがって \mathbf{y}_1 と \mathbf{y}_2 とは一致しない．

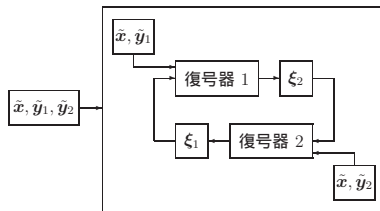


図 7 ターボ復号器の概要

$(\mathbf{x}, \mathbf{y}_1, \mathbf{y}_2)$ を通信路によって送信すると，これらは $(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2)$, $\tilde{x}_i, \tilde{y}_{1j}, \tilde{y}_{2j} \in \{-1, +1\}$ として受信される．この受信語に基づき復号する (図 7)．ターボ復号では 2 つの復号器を交互に用いて復号を行なう^{*1)}．確率分布 $p(\tilde{\mathbf{x}}|\mathbf{x})$, $p(\tilde{\mathbf{y}}_r|\mathbf{x})$, $r = 1, 2$ ，さらに以下の変数と関数を定義する．

$$l x_i = \frac{1}{2} \ln \frac{\sum_{\{\mathbf{x}: x_i = +1\}} p(\tilde{\mathbf{x}}|\mathbf{x})}{\sum_{\{\mathbf{x}: x_i = -1\}} p(\tilde{\mathbf{x}}|\mathbf{x})} = \frac{1}{2} \ln \frac{p(\tilde{x}_i|x_i = +1)}{p(\tilde{x}_i|x_i = -1)},$$

$$l y_{rj} = \frac{1}{2} \ln \frac{\sum_{\{\mathbf{x}: y_{rj} = +1\}} p(\tilde{\mathbf{y}}_r|\mathbf{x})}{\sum_{\{\mathbf{x}: y_{rj} = -1\}} p(\tilde{\mathbf{y}}_r|\mathbf{x})} = \frac{1}{2} \ln \frac{p(\tilde{y}_{rj}|y_{rj} = +1)}{p(\tilde{y}_{rj}|y_{rj} = -1)},$$

$$L_r \mathbf{x} = \mathbf{F}(l\mathbf{x}, l\mathbf{y}_r) = (F_1(l\mathbf{x}, l\mathbf{y}_r), \dots, F_N(l\mathbf{x}, l\mathbf{y}_r))^T,$$

$$F_i(l\mathbf{x}, l\mathbf{y}_r) = \frac{1}{2} \ln \frac{\sum_{\{\mathbf{x}: x_i = +1\}} p(\tilde{\mathbf{x}}|\mathbf{x}) p(\tilde{\mathbf{y}}_r|\mathbf{x})}{\sum_{\{\mathbf{x}: x_i = -1\}} p(\tilde{\mathbf{x}}|\mathbf{x}) p(\tilde{\mathbf{y}}_r|\mathbf{x})}.$$

通常は 1/2 を係数とせず定義するが，後の議論との整合性のため係数をつける．これらを用い，ターボ復号アルゴリズムは次のように定義される．

ターボ復号

1. $t = 0$ に対し $\boldsymbol{\xi}_1^t = 0$ とおき， $t = 1$ と置く．
2. $L_1 \mathbf{x}^{(t)} = \mathbf{F}((l\mathbf{x} + \boldsymbol{\xi}_1^t), l\mathbf{y}_1)$ を計算し， $\boldsymbol{\xi}_2$ を次のように更新する

$$\boldsymbol{\xi}_2^t = L_1 \mathbf{x}^{(t)} - (l\mathbf{x} + \boldsymbol{\xi}_1^t). \quad (2)$$

3. $L_2 \mathbf{x}^{(t)} = \mathbf{F}((l\mathbf{x} + \boldsymbol{\xi}_2^t), l\mathbf{y}_2)$ を計算し， $\boldsymbol{\xi}_1^{t+1}$ を次のように更新する

$$\boldsymbol{\xi}_1^{t+1} = L_2 \mathbf{x}^{(t)} - (l\mathbf{x} + \boldsymbol{\xi}_2^t). \quad (3)$$

4. t を 1 ずつ増しながら 2, 3 を $L_1 \mathbf{x}^{(t)} = L_2 \mathbf{x}^{(t)}$ が満たされるまで繰り返す．
5. 収束したならば， $L_r \mathbf{x}^*$ の各成分の符号を復号結果とする．

このアルゴリズムは必ずしも収束しないため，実

*1) この部分がターボと呼ばれる所以のようだ

際には数回から十数回程度の繰り返し回数をあらかじめ決めておき、その回数のみ繰り返す。

ここで、なぜ2つの検査語 y_1, y_2 とを分ける必要があるのかという疑問が生じる。ターボ符号ではこれらの検査語をひとつの長い検査語とすると、復号のための計算量が多くなってしまい、実現不可能となる。一方、ひとつの検査語のみを用いて F を計算する際に必要な計算量は N のオーダーであり、効率良く復号できる。したがってこのような複雑な復号法が必要となる。また、ターボ復号は MPM 復号の近似手法であり、真の MPM 復号の結果とは必ずしも一致しない。

このようにターボ復号は必ずしも収束せず、復号結果も MPM 復号と厳密には一致しない。しかしそれでも実際に適用してみると、誤り訂正能力に優れた現実的な符号である。

3. ターボ符号の情報幾何

我々はこの不思議な誤り訂正符号であるターボ符号を理解するため、情報幾何学を用いた解析を行ってきた⁵⁻⁷⁾。以下でその概略を示す。

3.1 情報幾何の準備

情報幾何学とは、微分幾何学を用い、統計的な推定、検定などの様々な問題を新たな幾何的視点から考える学問である。ターボ符号に対しても、情報幾何学を用いて直感的な表現を与え、解析のための数理的枠組みを作ることができる。

本節では情報幾何の準備を行なう。 x の確率分布の族 S を考える。これは 2^N 個の要素に対する多項分布の多様体である。和が1であるという制約から $(2^N - 1)$ 次元の自由度を持つ。

$$S = \left\{ p(x) \mid p(x) > 0, x \in \{-1, +1\}^N, \sum_x p(x) = 1 \right\}.$$

次に S に含まれる e -平坦, m -平坦な部分多様体を定義する。

e -平坦な部分多様体: 部分多様体 $M \subset S$ は全ての $q(x), p(x) \in M$ に対し、次式で定義され

る $r(x; t)$ が M に含まれるとき, e -平坦である。

$$\ln r(x; t) = (1-t) \ln q(x) + t \ln p(x) + c(t) \\ t \in \mathfrak{R}.$$

$c(t)$ は規格化のための関数である。定義より指数型分布族は e -平坦な部分多様体を構成する。
 m -平坦な部分多様体: 部分多様体 $M \subset S$ は全ての $q(x), p(x) \in M$ に対し、次式で定義される $r(x; t)$ が M に含まれるとき, m -平坦である。

$$r(x; t) = (1-t)q(x) + tp(x), \quad t \in [0, 1].$$

混合分布は m -平坦な部分多様体を構成する。

次に $q(x) \in S$ から e -平坦な部分多様体 M への m -射影を定義する。

定義 1. M を S の e -平坦な部分多様体とする。 $q(x) \in S$ から M への m -射影は, M の確率分布で, $q(x)$ から M への Kullback-Leibler ($K-L$) 情報量を最小にするものである。すなわち

$$\Pi_{M \circ q}(x) = \operatorname{argmin}_{p(x) \in M} D[q(x); p(x)].$$

$K-L$ 情報量 $D[\cdot; \cdot]$ は次のように定義される。

$$D[q(x); p(x)] = \sum_x q(x) \ln \frac{q(x)}{p(x)}.$$

$K-L$ 情報量は $D[q(x); p(x)] \geq 0$ を満たし, 全ての x に対して $q(x) = p(x)$ が成り立つ場合に限り $D[q(x); p(x)] = 0$ である。

m -射影に関しては以下の結果が知られている¹⁾。

定理 1. $q(x) \in S$ から S の e -平坦な部分多様体 M への m -射影 $\Pi_{M \circ q}(x)$ は一意に定まる。

これらの定義を用いてターボ復号アルゴリズムを表現する。まず S の中に各成分が独立である分布から成る部分多様体 M_0 を考える。定義は次の通りである。

$$M_0 = \left\{ p_0(x; \theta) = \exp(\mathbf{h} \cdot \mathbf{x} + \theta \cdot \mathbf{x} - \psi_0(\theta)) \mid \theta = (\theta_1, \dots, \theta_N)^T \in \mathfrak{R}^N \right\}.$$

$p_0(\mathbf{x}; \boldsymbol{\theta}) = \prod_i \exp((\beta \tilde{x}_i + \theta_i)x_i - \psi_{0i}(\theta_i))$ とかけることから各 x_i が独立な分布となることがわかる．確率分布を定めるパラメータ $\boldsymbol{\theta}$ は自然パラメータと呼ばれ, $\psi_0(\boldsymbol{\theta})$ は規格化関数である． M_0 は e -平坦な部分多様体である²⁾．この多様体に含まれる確率分布では各 x_i が独立であることから $\eta_0(\boldsymbol{\theta}) = \sum_{\mathbf{x}} \mathbf{x} p_0(\mathbf{x}; \boldsymbol{\theta})$ が簡単に求まる．

さて, MPM 復号では $\boldsymbol{\eta} = \sum_{\mathbf{x}} \mathbf{x} p(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2)$ を求めたいのだが $\boldsymbol{\theta}$ から $\eta_0(\boldsymbol{\theta})$ への変換は簡単であることから $\eta_0(\boldsymbol{\theta}) = \boldsymbol{\eta}$ を満たす $\boldsymbol{\theta}$ が求まればただちに復号ができる．この $\boldsymbol{\theta}$ を $\hat{\boldsymbol{\theta}}$ とする． $p_0(\mathbf{x}; \hat{\boldsymbol{\theta}})$ は $p(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2)$ から M_0 への m -射影となっている．簡単に示しておく．

$$\hat{\boldsymbol{\theta}} = \underset{\boldsymbol{\theta}}{\operatorname{argmin}} D[p(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2); p_0(\mathbf{x}; \boldsymbol{\theta})]$$

$$\left. \frac{\partial D}{\partial \boldsymbol{\theta}} \right|_{\boldsymbol{\theta}=\hat{\boldsymbol{\theta}}} = \mathbf{0}$$

より

$$\sum_{\mathbf{x}} \mathbf{x} p(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2) = \sum_{\mathbf{x}} \mathbf{x} p_0(\mathbf{x}; \hat{\boldsymbol{\theta}}).$$

よって $\eta_0(\hat{\boldsymbol{\theta}}) = \boldsymbol{\eta}$ である． $D[p; p_0]$ の 2 階微分は $p_0(\mathbf{x}; \boldsymbol{\theta})$ の Fisher 情報量行列となることから, 正定値行列である．したがってこれが最小値となることもわかる．これより MPM 復号は M_0 への m -射影 $p_0(\mathbf{x}; \hat{\boldsymbol{\theta}})$ を求めればただちに得られる⁵⁾．

3.2 ターボ復号の情報幾何的表現

ターボ復号では, $p(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2)$ として, 2 つのパーティ検査語を同時に用いるのではなく, $\tilde{\mathbf{x}}$ とひとつのパーティ検査語のみを考慮した $p(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1|\mathbf{x})$, $p(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_2|\mathbf{x})$ を用いて復号を行なう．BSC の通信路を考える場合, $p(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_r|\mathbf{x})$, $r = 1, 2$ は次のように書ける．

$$p(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_r|\mathbf{x})$$

$$= \exp(\mathbf{h} \cdot \mathbf{x} + c_r(\mathbf{x}) - (N + L)\psi(\beta)).$$

ここで $c_r(\mathbf{x}) = \beta \tilde{\mathbf{y}}_r \cdot \mathbf{y}_r(\mathbf{x})$, $r = 1, 2$ と定義した．これらの条件付き分布に加え $\omega(\mathbf{x}; \boldsymbol{\xi}) = \exp(\boldsymbol{\xi} \cdot \mathbf{x} - \psi(\boldsymbol{\xi}))$ を \mathbf{x} の事前分布としてベイズ則から \mathbf{x} の事後分布を考える． $\omega(\mathbf{x}; \boldsymbol{\xi})$ は各 x_i が独立であるような任意の分布を表現できる．事

後分布は以下ようになる

$$p_r(\mathbf{x}; \boldsymbol{\xi}) = p_r(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_r; \boldsymbol{\xi})$$

$$= \frac{p_r(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_r|\mathbf{x})\omega(\mathbf{x}; \boldsymbol{\xi})}{\sum_{\mathbf{x}} p_r(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_r|\mathbf{x})\omega(\mathbf{x}; \boldsymbol{\xi})}$$

$$= \exp(\mathbf{h} \cdot \mathbf{x} + c_r(\mathbf{x}) + \boldsymbol{\xi} \cdot \mathbf{x} - \varphi_r(\boldsymbol{\xi})).$$

$\varphi_r(\boldsymbol{\xi})$ は規格化関数である． $\boldsymbol{\xi}$ は各 p_r に対して異なるので 2 つのベクトルを用意し $p_1(\mathbf{x}; \boldsymbol{\xi}_2)$, $p_2(\mathbf{x}; \boldsymbol{\xi}_1)$ として定義する．添え字が互いに逆になっているのはターボ復号の仕組みから後に明らかになる．この $p_r(\mathbf{x}; \boldsymbol{\xi}_s)$ による \mathbf{x} の平均を $\eta_r(\boldsymbol{\xi}_s)$ とおく．ターボ復号では全ての $\boldsymbol{\xi}_s \in \mathbb{R}^N$ に対して $\eta_r(\boldsymbol{\xi}_s)$ が計算可能だとする．その上で $\boldsymbol{\xi}_s$ 繰り返しアルゴリズムによって調整し $\eta_1(\boldsymbol{\xi}_2)$ と $\eta_2(\boldsymbol{\xi}_1)$ が等しくなるようにし, $p(\mathbf{x}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2)$ の m -射影を近似する．

ターボ復号の情報幾何的な解釈を考えよう．まずターボ符号で重要な 3 つの多様体を定義する．

$$M_0 = \left\{ p_0(\mathbf{x}; \boldsymbol{\theta}) \mid \boldsymbol{\theta} \in \mathbb{R}^N \right\},$$

$$M_1 = \left\{ p_1(\mathbf{x}; \boldsymbol{\xi}_2) \mid \boldsymbol{\xi}_2 \in \mathbb{R}^N \right\},$$

$$M_2 = \left\{ p_2(\mathbf{x}; \boldsymbol{\xi}_1) \mid \boldsymbol{\xi}_1 \in \mathbb{R}^N \right\}.$$

$\boldsymbol{\theta}$ 及び $\boldsymbol{\xi}_s$ は各多様体の座標系を与える．次にオペレータ π_{M_0} を任意の $q(\mathbf{x}) \in S$ から M_0 への m -射影となる座標 $\boldsymbol{\theta}$ として定義する．

$$\pi_{M_0} \circ q(\mathbf{x}) = \underset{\boldsymbol{\theta} \in \mathbb{R}^N}{\operatorname{argmin}} D[q(\mathbf{x}); p_0(\mathbf{x}; \boldsymbol{\theta})].$$

この π_{M_0} を用いると, ターボ復号は次のように書ける．

ターボ復号の情報幾何的表現

1. $t = 0$ に対し $\boldsymbol{\xi}_1^t = \mathbf{0}$ とおき, $t = 1$ とする．
2. $p_2(\mathbf{x}; \boldsymbol{\xi}_1^t)$ から M_0 への射影 $\pi_{M_0} \circ p_2(\mathbf{x}; \boldsymbol{\xi}_1^t)$ を求め, $\boldsymbol{\xi}_2^t$ を次のように更新する．

$$\boldsymbol{\xi}_2^t = \pi_{M_0} \circ p_2(\mathbf{x}; \boldsymbol{\xi}_1^t) - \boldsymbol{\xi}_1^t. \quad (4)$$

3. $p_1(\mathbf{x}; \boldsymbol{\xi}_2^t)$ から M_0 への射影 $\pi_{M_0} \circ p_1(\mathbf{x}; \boldsymbol{\xi}_2^t)$ を求め, $\boldsymbol{\xi}_1^{t+1}$ を次のように更新する．

$$\boldsymbol{\xi}_1^{t+1} = \pi_{M_0} \circ p_1(\mathbf{x}; \boldsymbol{\xi}_2^t) - \boldsymbol{\xi}_2^t. \quad (5)$$

4. $\pi_{M_0} \circ p_1(x; \xi_2^t)$ と $\pi_{M_0} \circ p_2(x; \xi_1^{t+1})$ が一致しなければ step 2 へ戻る.
5. 収束した時点の ξ_1, ξ_2 を ξ_1^*, ξ_2^* とする. $\eta_1(\xi_2^*) = \eta_2(\xi_1^*)$ の各成分の符号をもって復号結果とする.

(2), (3) 式中の $L_1 x^{(t)}, L_2 x^{(t)}$, すなわち, $F((lx + \xi_1^t), ly_1), F((lx + \xi_2^t), ly_2)$ は (4), (5) 式中の $\pi_{M_0} \circ p_2(x; \xi_1^t), \pi_{M_0} \circ p_1(x; \xi_2^t)$ に対応している. また, (2), (3) 式中の ξ_1^t, ξ_2^{t+1} は (4), (5) 式中の ξ_1^t, ξ_2^{t+1} と一致する⁷⁾.

3.3 ターボ復号の解が持つ性質

ターボ復号が収束したならば $\pi_{M_0} \circ p_1(x; \xi_2^*) = \pi_{M_0} \circ p_2(x; \xi_1^*)$ が満たされている. これを θ^* とする. それぞれの復号器の結果が一致すること, そして $\pi_{M_0} \circ p_1(x; \xi_2^*) = \pi_{M_0} \circ p_2(x; \xi_1^*) = \theta^*$ であることとアルゴリズムのステップ 2, 3 より次の 2 つの条件が成り立つ.

1. $\eta_0(\theta^*) = \eta_1(\xi_2^*) = \eta_2(\xi_1^*)$,
2. $\theta^* = \xi_1^* + \xi_2^*$.

さらに $p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2) (= p)$, $p_0(x; \theta^*) (= p_0^*)$, $p_1(x; \xi_2^*) (= p_1^*)$, $p_2(x; \xi_1^*) (= p_2^*)$ を比較してみると, それぞれ以下のような形をしている.

$$p = \exp(\mathbf{h} \cdot \mathbf{x} + c_1(\mathbf{x}) + c_2(\mathbf{x}) - \ln C)$$

$$p_0^* = \exp(\mathbf{h} \cdot \mathbf{x} + \xi_1^* \cdot \mathbf{x} + \xi_2^* \cdot \mathbf{x} - \varphi_0(\theta^*))$$

$$p_1^* = \exp(\mathbf{h} \cdot \mathbf{x} + c_1(\mathbf{x}) + \xi_2^* \cdot \mathbf{x} - \varphi_1(\xi_2^*))$$

$$p_2^* = \exp(\mathbf{h} \cdot \mathbf{x} + \xi_1^* \cdot \mathbf{x} + c_2(\mathbf{x}) - \varphi_2(\xi_1^*))$$

となる. これを見ると直観的には $\xi_1^* \cdot \mathbf{x}$ によって $c_1(\mathbf{x})$ を, $\xi_2^* \cdot \mathbf{x}$ によって $c_2(\mathbf{x})$ を置き換え, それぞれの影響を表現しようとしていることが分る. また, $p_1(x; \xi_2^*), p_2(x; \xi_1^*)$ と添字を互いに逆にした理由も理解できるだろう. しかし $c_r(\mathbf{x})$ は x_i の非線形な項によって構成されているので, このような近似の意味は明らかではない.

このターボ復号によって求めた分布のもつ性質について, 我々が情報幾何の枠組みによって得た結果を示す. そのために, 以下の 2 つの多様体を定義する. まずは多様体上の全ての分布で x の期

待値が同じである等平均多様体 $M(\theta)$ を定義する.

$$M(\theta) = \left\{ p(x) \mid \sum_x xp(x) = \eta_0(\theta) \right\}$$

$M(\theta)$ に $p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$ が含まれていれば, $p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$ による x の平均 η と $\eta_0(\theta)$ が一致することから, その θ が正しい MPM 解となる. しかし一般にターボ復号の解ではこれは成り立たない. 次に新たな多様体を定義する.

$$E^* = \left\{ p = Cp_0^{*t_0} p_1^{*t_1} p_2^{*t_2} \mid \sum_{r=0}^2 t_r = 1 \right\}.$$

この多様体は定義より, 明らかに $p_0(x; \theta^*), p_1(x; \xi_2^*), p_2(x; \xi_1^*)$ を含んでいる. これら 2 つの多様体とターボ復号の収束した分布の間には次の関係が成り立つ.

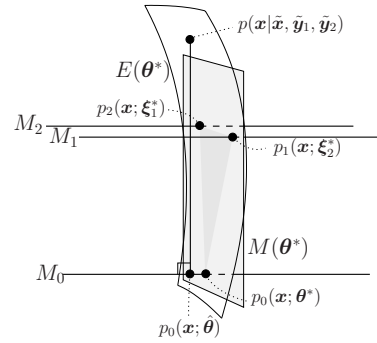


図 8 ターボ符号の情報幾何的な解釈

定理 2. 収束したならば, $p_0(x; \theta^*), p_1(x; \xi_2^*), p_2(x; \xi_1^*)$ の 3 つの分布が $M(\theta^*)$ に含まれ, $p_0(x; \theta^*), p_1(x; \xi_2^*), p_2(x; \xi_1^*), p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$ の 4 つが E^* に含まれる (図 8).

証明. $p_0(x; \theta^*), p_1(x; \xi_2^*), p_2(x; \xi_1^*)$ が $M(\theta^*), E^*$ に含まれることはその定義から t_0, t_1, t_2 それぞれを 1 に, 他を 0 とすることで確かめられる. $p_0(x; \theta^*), p_1(x; \xi_2^*), p_2(x; \xi_1^*), p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$ の 4 つが E^* に含まれることは $t_0 = -1, t_1 = t_2 = 1$ と置き, $\theta^* = \xi_1^* + \xi_2^*$ を用い

$$C \frac{p_1(x; \xi_2^*) p_2(x; \xi_1^*)}{p_0(x; \theta^*)}$$

$$= C \exp(\mathbf{h} \cdot \mathbf{x} + c_1(\mathbf{x}) + c_2(\mathbf{x}))$$

$$= p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$$

となることから，確かめられる． □

図 8 の中で， $\hat{\theta}$ は真の MPM 復号解であり， $p(x|\hat{x}, \hat{y}_1, \hat{y}_2)$ を直接 M_0 に m -射影することにより求まる．真の MPM 復号解 $\hat{\theta}$ とターボ復号解 θ^* との間には差がある．この差は図 8 から分るように E^* と $M(\theta^*)$ との差から生じる．我々はこの差を摂動展開により計算し，その主要項が多様体の曲率に関係していることを示した^{5, 6)}，

4. まとめ

本稿では最新の移動体通信に用いられている誤り訂正符号であるターボ符号について情報幾何学に基づく解釈を行ない，アルゴリズムの新たな表現，復号誤差の直感的な理解を与えられることを示した．本稿に含めなかったが，アルゴリズムの局所的な安定性，ターボ復号解の安定性についても初歩的な結果が得られている⁵⁻⁸⁾．これは既に情報理論の枠組で得られている結果と一致している¹⁰⁾．我々は情報幾何学に基づき，ターボ符号の解析のための数理的枠組を確立したいと考えているが，見通しは明るい．

この情報幾何学的な構造はターボ復号アルゴリズムだけでなく，より一般的に確率分布の周辺分布を近似する問題として捉えることができる．同様の構造は低密度パリティ検査符号^{4, 9)}，統計物理の Bethe 近似，ループのあるベイジアンネットワークの確率伝搬法にも存在する．アルゴリズムの詳細については多少の差があり，解の安定性などについては全く同じ結果は得られないが，2つの多様体の差が結果の誤差を生じさせる，などの直観的な結果は他の手法においても同様に成り立つ⁸⁾．低密度パリティ検査符号に対する復号問題の情報幾何学的構造に関しては，本論文で述べたターボ復号問題の幾何学的構造との関連も含めて我々が解析を行なっている⁷⁾．

今後は情報幾何学に基づく解釈を各分野の手法に対して適用し，見通しの良い数理的解析手法を与えるべく，本研究を発展させていきたい．

参考文献

- 1) 甘利俊一，長岡浩司．情報幾何の方法．岩波講座 応用数学 [対象 12]．岩波書店，1993．
- 2) S. Amari and H. Nagaoka. *Methods of Information Geometry*. AMS and Oxford University Press, 2000.
- 3) C. Berrou, A. Glavieux, and P. Thitimajshima. "Near Shannon limit error-correcting coding and decoding: Turbo-codes," *Proc. IEEE Int. Conf. Commun.*, pp. 1064–1070, Geneva, Switzerland, 1993.
- 4) R. G. Gallager. "Low density parity check codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 21–28, 1962.
- 5) 池田思朗，田中利幸，甘利俊一．「ターボ復号の情報幾何」，電子情報通信学会論文誌，vol. J85-D-II, no. 5, pp. 758–765, 2002.
- 6) S. Ikeda, T. Tanaka, and S. Amari. "Information geometrical framework for analyzing belief propagation decoder," *Advances in Neural Information Processing Systems*, vol. 14, pp. 407–414. MIT Press, 2002.
- 7) S. Ikeda, T. Tanaka, and S. Amari. "Information geometry of turbo and low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 50, no. 6, pp. 1097–1114, 2004.
- 8) S. Ikeda, T. Tanaka, and S. Amari. "Stochastic reasoning, free energy, and information geometry," *Neural Computation*, vol. 16, no. 9, pp. 1779–1810, 2004.
- 9) D. J. C. MacKay. "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 399–431, 1999.
- 10) T. J. Richardson. "The geometry of turbo-decoding dynamics," *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 9–23, 2000.
- 11) 田中利幸．リレー連載「確率の情報処理と統計力学」第 2 回，数理科学，vol. 42, no. 12, 2004.

(いけだ・しろう，統計数理研究所)