

ターボ復号法の情報幾何的理解と改善の可能性

九州工業大学 大学院 生命体工学研究科 池田 思朗¹
東京都立大学 大学院 工学研究科 田中 利幸²
理化学研究所 脳科学総合研究センター 甘利 俊一³

1 はじめに

近年, 携帯電話に代表される移動体通信技術は飛躍的に発展している. 様々な環境で用いられる移動体通信が可能となったのは, 集積回路などのハードウェア, そして理論的な基礎技術の進歩によるところが大きい. 基礎技術の進歩は現在も継続しており, 携帯端末はさらに小型化し, 高速に高品質のデータ通信が可能となっていくだろう. ここで紹介する話題は, 移動体通信の発展を支えている最新の理論的基礎技術のひとつ, ターボ符号と呼ばれる誤り訂正符号 [3] である.

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, 第 3 世代移動通信方式から実際に採用されている. 独特な復号法 (ターボ復号法) を用いるターボ符号は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, 理論的には未知の部分も多い. 既存の解析技術では全貌を把握できないのだ. 我々はこの問題に対して, 情報幾何学 [1, 2] を用いた解析を行ない, ターボ復号法の持つ謎に迫りたいと考えている [5, 6].

最近の研究から, このターボ復号法が人工知能や統計物理の手法と密接に関係していることが分かってきており [7, 9], 分野間のつながりが密接になりつつある. その中であって, 情報幾何学によりどのような立場で何を明らかにしようとするのか, 本稿で説明したい.

2 誤り訂正符号

2.1 誤り訂正符号とシャノンの限界

デジタルの信号を送る際, 通信路にはノイズが生じ, 受信側では送信側と完全に同じ信号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いても, 受け取った側でその情報を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, 送りたいデータに冗長性を持たせる必要がある. この冗長性により, 誤りを含んだデータを復元することができる. 図 1 を用いて説明する.

¹E-mail: shiro@brain.kyutech.ac.jp

²E-mail: tanaka@eei.metro-u.ac.jp

³E-mail: amari@brain.riken.go.jp

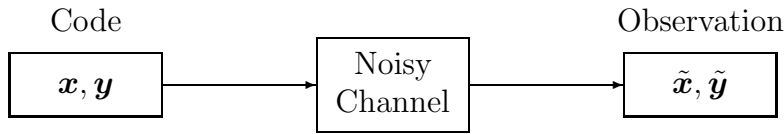


図 1: 検査語による誤り訂正

送信したい情報 (送信語) を x と書く．ここではデジタルの情報と考え x は 2 値のベクトル， $x = (x_1, \dots, x_N)^T$ である．便利のため $\{0, 1\}$ ではなく $\{-1, +1\}$ を用いる．

$$x_i \in \{-1, +1\}, \quad i = 1, \dots, N.$$

図中の $y = (y_1, \dots, y_L)^T$ 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．検査語は x から一意的に計算できるという意味で冗長な情報である．これら 2 つのベクトル (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．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．

冗長性を大きくとればノイズに対してより頑強となるが，限られた長さで送ることのできる情報の量は減る．したがって，できるだけ短い符号で高い誤り訂正能力を得たい．この問題に対し，シャノンは理論的な限界 (シャノン限界) を示した．しかし，シャノン限界が示されてから 50 年以上が経った今も，シャノン限界を達成する実用的な符号は存在していない．

シャノン限界を示した通信路符号化定理の証明は，ランダム的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．しかし，ランダム的に構成した符号を用いると復号の際に問題が生じる．復号とは前に述べたように， (\tilde{x}, \tilde{y}) から最適な x を探すことである．ランダム的に構成された符号では x の取り得る 2^N の候補から最適な x を選ぶ効率的な計算法が一般に存在しない．したがって，総当たりで選ぶ以外の方法がないため計算量が指数的に増えてしまい，長い符号に対しては実現不可能である．ターボ復号は符号長に対して多項式オーダーの計算量で実現可能で，シャノン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．これがターボ符号が一躍注目を集めた理由である．

2.2 MPM 復号

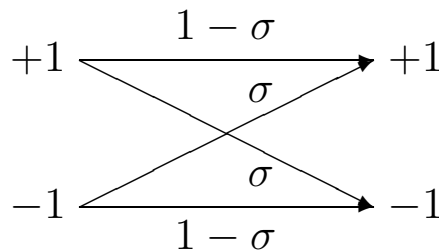


図 2: 2 元対象通信路

通信路は確率分布を用いて表現される．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, 以下 BSC) を考えることにする。これは、各ビットが通信路によって反対の符号に一定の確率で変わってしまうというものである。図 2 ではその確率が σ となっている。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

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

となる。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

$$p(\tilde{x}|x) = \exp(\beta \tilde{x} \cdot x - N\psi(\beta))$$

$$p(\tilde{y}|x) = \exp(\beta \tilde{y} \cdot y(x) - L\psi(\beta)), \quad \psi(\beta) = \ln(e^{-\beta} + e^{\beta})$$

と書ける。ここで β は正の実数で、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。 $c_0(x) = \beta \tilde{x} \cdot x$, $c_1(x) = \beta \tilde{y} \cdot y$, と置くと、 $p(\tilde{x}, \tilde{y}|x)$ は

$$p(\tilde{x}, \tilde{y}|x) = \exp(c_0(x) + c_1(x) - (N + L)\psi(\beta))$$

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

$$p(x|\tilde{x}, \tilde{y}) = \frac{p(\tilde{x}, \tilde{y}|x)}{\sum_x p(\tilde{x}, \tilde{y}|x)} = C \exp(c_0(x) + c_1(x)). \quad (1)$$

すなわち $p(x|\tilde{x}, \tilde{y}) \propto p(\tilde{x}, \tilde{y}|x)$ となる。この分布から情報語を推測するのだが、ターボ符号では MPM (maximum posterior marginal) 復号を目指す。これは $p(x|\tilde{x}, \tilde{y})$ から各成分の周辺分布 $p(x_i|\tilde{x}, \tilde{y})$, $i = 1, \dots, N$ を求め、各分布を最大にする $x_i \in \{-1, +1\}$ を復号結果とするものである。別の表現をすれば、

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

によって 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とと等しい。

2.3 ターボ符号

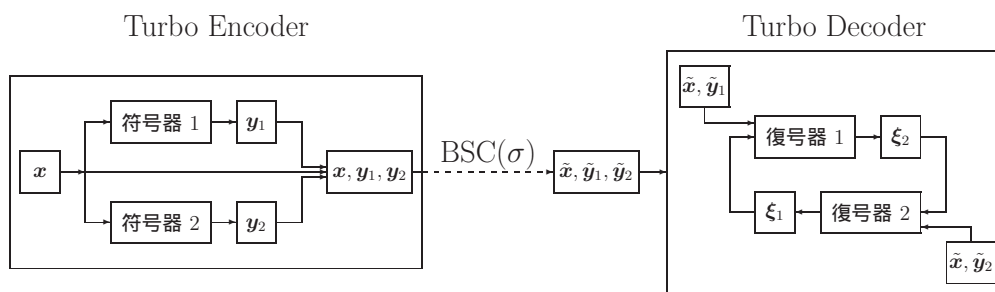


図 3: ターボ符号の概要

図 3 にターボ符号の概要を示す。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 $y_1 = (y_{11}, \dots, y_{1L})^T$, $y_2 = (y_{21}, \dots, y_{2L})^T$,

$y_{1j}, y_{2j} \in \{-1, +1\}$ とする． $y_r, r = 1, 2$ は x の関数である．それぞれの符号器は同等のものだが，符号器の入力となる x のビット列の順番をインターリーバーによって入れ換えている．したがって y_1 と y_2 とは一致しない．

(x, y_1, y_2) を通信路によって送信すると，これらは $(\tilde{x}, \tilde{y}_1, \tilde{y}_2), \tilde{x}_i, \tilde{y}_{1j}, \tilde{y}_{2j} \in \{-1, +1\}$ として受信される．この受信語に基づき復号する．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．確率分布 $p(\tilde{x}|\mathbf{x}), p(\tilde{y}_r|\mathbf{x}), r = 1, 2$ ，さらに次の変数と関数 F を定義する．

$$l_{x_i} \stackrel{\text{def}}{=} \ln \frac{\sum_{\{\mathbf{x}:x_i=+1\}} p(\tilde{\mathbf{x}}|\mathbf{x})}{\sum_{\{\mathbf{x}:x_i=-1\}} p(\tilde{\mathbf{x}}|\mathbf{x})} = \ln \frac{p(\tilde{x}_i|x_i=+1)}{p(\tilde{x}_i|x_i=-1)},$$

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

$$L_r \mathbf{x} \stackrel{\text{def}}{=} F(l_{\mathbf{x}}, l_{\mathbf{y}_r}) = \left\{ \ln \frac{\sum_{\{\mathbf{x}:x_i=+1\}} p(\tilde{\mathbf{x}}|\mathbf{x}) p(\tilde{\mathbf{y}}_r|\mathbf{x})}{\sum_{\{\mathbf{x}:x_i=-1\}} p(\tilde{\mathbf{x}}|\mathbf{x}) p(\tilde{\mathbf{y}}_r|\mathbf{x})} \right\}.$$

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 (図3)．

ターボ復号

1. $\xi_1 = 0, t = 1$ と置く．

2. $L_1 \mathbf{x}^{(t)} = F((l_{\mathbf{x}} + \xi_1), l_{\mathbf{y}_1})$ を計算し， ξ_2 を次のように更新する

$$\xi_2 = L_1 \mathbf{x}^{(t)} - (l_{\mathbf{x}} + \xi_1). \quad (2)$$

3. $L_2 \mathbf{x}^{(t)} = F((l_{\mathbf{x}} + \xi_2), l_{\mathbf{y}_2})$ を計算し， ξ_1 を次のように更新する

$$\xi_1 = L_2 \mathbf{x}^{(t)} - (l_{\mathbf{x}} + \xi_2). \quad (3)$$

4. t を1つつ増しながら2, 3を $L_1 \mathbf{x}^{(t)} = L_2 \mathbf{x}^{(t)} = L_1 \mathbf{x}^{(t+1)} = L_2 \mathbf{x}^{(t+1)}$ が満たされるまで繰り返す．

このアルゴリズムは必ずしも収束しないため，実際には数回から10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．

ここで疑問が生じる．なぜ y_1, y_2 とを分ける必要があるのかという点である．これら2つの検査語を組み合わせ，ひとつの長い検査語とすれば，何も複雑なことはしないですむように思える．しかし，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，復号の計算が実現不可能になってしまう．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，ターボ復号の結果が本当にMPM復号の結果と一致するのかという疑問も生じるだろう．ターボ復号はMPM復号の近似手法であり，結果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．しかしそれでも誤り訂正能力に優れた現実的な符号である．我々は情報幾何学を用いて，この謎を明らかにしたいと考えている．

3 ターボ符号の情報幾何

3.1 情報幾何の準備

情報幾何学とは、確率密度関数に対して微分幾何学を用い、新たな視点から統計的な推定、検定などを考える学問である。新たな視点に基づき確率分布間の距離や確率モデルによる多様体を考えることで、様々な問題において直感的に分り易い表現が得られている。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ようというのが本研究の目的のひとつである。

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。

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

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: 多様体 $M \in S$ は、全ての $q(\mathbf{x}), p(\mathbf{x}) \in M$ に対し、次の式で定義される $r(\mathbf{x}; t)$ が M に含まれるとき、 e -平坦である。

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

c は規格化定数である。定義より指数分布族の確率分布は e -平坦な多様体を作る。

m -平坦: 多様体 $M \in S$ は、全ての $q(\mathbf{x}), p(\mathbf{x}) \in M$ に対し、次の式で定義される $r(\mathbf{x}; t)$ が M に含まれるとき、 m -平坦である。

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

混合分布は m -平坦な多様体を構成する。

次に確率分布から多様体への射影, m -射影について定義する。

定義 1. M を S の e -平坦な部分多様体とする。 $q(\mathbf{x}) \in S$ から M への m -射影は、 M 上の点で、 $q(\mathbf{x})$ から M への Kullback-Leibler (K-L) 情報量を最小にする点であり、次のように定義する。

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

なお $q(\mathbf{x}) \in S$ から S の e -平坦な部分多様体 M への m -射影 $\Pi_M \circ q(\mathbf{x})$ は 1 点に定まる。

K-L 情報量 $D[\cdot; \cdot]$ は次のように定義される

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

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

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ことを考える。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_D を考える。定義は次の通りである。

$$M_D = \left\{ p(\mathbf{x}; \boldsymbol{\theta}) = \exp(\boldsymbol{\theta} \cdot \mathbf{x} - \psi(\boldsymbol{\theta})) \mid \boldsymbol{\theta} \in \mathcal{R}^N \right\}.$$

確率分布を定めるパラメータ θ は自然パラメータと呼ばれ, 多様体 M_D の座標系を与える. また $\psi(\theta)$ は規格化関数であり, 次のように定義される.

$$\psi(\theta) = \ln \sum_x \exp(\theta \cdot x) = \sum_i \ln(e^{-\theta_i} + e^{\theta_i}).$$

M_D 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は各ビットの確率分布が独立であることから $\sum_x xp(x; \theta)$ は簡単に求まる. 証明は省くが, 任意の x の確率分布によって x の平均をとる操作は M_D への m -射影を求めることと等しい [5].

3.2 ターボ復号の情報幾何的表現

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

$$p(\tilde{x}, \tilde{y}_r|x) = \exp(c_0(x) + c_r(x) - (N + L)\psi(\beta)), \quad r = 1, 2.$$

ここで $c_r(x) = \beta \tilde{y}_r \cdot y(x)$, $r = 1, 2$ と定義した. これらの分布に $\omega(x; \xi) \in M_D$ を x の事前分布として x の事後分布を考えると以下のようなになる

$$p_r(x; \xi) = p_r(x|\tilde{x}, \tilde{y}_r; \xi) = \frac{p_r(\tilde{x}, \tilde{y}_r|x)\omega(x; \xi)}{\sum_x p_r(\tilde{x}, \tilde{y}_r|x)\omega(x; \xi)} = \exp(c_0(x) + c_r(x) + \xi \cdot x - \varphi_r(\xi)).$$

$\varphi_r(\xi)$ は規格化関数である. ターボ符号では, この $p_r(x; \xi)$, $r = 1, 2$ を基にした x の平均操作, すなわち M_D への m -射影の計算が実現可能である. その上で ξ を繰り返しアルゴリズムによって変化させ, 最終的に $p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$ 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.

$$M_0 = \left\{ p_0(x; \xi) = \exp(c_0(x) + \xi \cdot x - \varphi_0(\xi)) \mid \xi \in \mathcal{R}^N \right\}$$

$$M_1 = \left\{ p_1(x; \xi) \mid \xi \in \mathcal{R}^N \right\}, M_2 = \left\{ p_2(x; \xi) \mid \xi \in \mathcal{R}^N \right\}.$$

ξ は各多様体の座標系を与える. $c_0(x) = \beta \tilde{x} \cdot x$ であるので, $\theta' = \theta + \beta \tilde{x}$ と置くと, $p(x; \theta') = p_0(x; \theta)$ となる. したがって M_0 は M_D と等しい.

$q(x)$ から M_0 への m -射影によって求まる座標 ξ を $\pi_{M_0} \circ q(x)$ とする.

$$\pi_{M_0} \circ q(x) = \operatorname{argmin}_{\xi \in \mathcal{R}^N} D[q(x); p_0(x; \xi)].$$

なお, $\pi_{M_0} \circ q(x) = \pi_{M_D} \circ q(x) + \beta \tilde{x}$ が成り立つ. 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 $\xi_1^t = 0$ とおき, $t = 1$ とする.
2. $p_2(x; \xi_1^t)$ から M_0 への射影 $\pi_{M_0} \circ p_2(x; \xi_1^t)$ を求め, ξ_2^{t+1} を次のように計算する.

$$\xi_2^{t+1} = \pi_{M_0} \circ p_2(x; \xi_1^t) - \xi_1^t. \quad (4)$$

3. $p_1(\mathbf{x}; \xi_2^{t+1})$ から M_0 への射影 $\pi_{M_0 \circ p_1}(\mathbf{x}; \xi_2^{t+1})$ を求め, ξ_1^{t+1} を次のように計算する.

$$\xi_1^{t+1} = \pi_{M_0 \circ p_1}(\mathbf{x}; \xi_2^{t+1}) - \xi_2^{t+1}. \quad (5)$$

4. $\pi_{M_0 \circ p_1}(\mathbf{x}; \xi_2^{t+1})$ と $\pi_{M_0 \circ p_2}(\mathbf{x}; \xi_1^{t+1})$ が一致しなければ step 2 へ戻る.

(2), (3) 式中の $L_1 \mathbf{x}^{(t)}$, $L_2 \mathbf{x}^{(t)}$, すなわち, $F((l\mathbf{x} + \xi_1), l\mathbf{y}_1)$, $F((l\mathbf{x} + \xi_2), l\mathbf{y}_2)$ は (4), (5) 式中の $\pi_{M_0 \circ p_2}(\mathbf{x}; \xi_1^t)$, $\pi_{M_0 \circ p_1}(\mathbf{x}; \xi_2^{t+1})$ に対応している. また, (2), (3) 式中の ξ_1 , ξ_2 は (4), (5) 式中の ξ_1^t , ξ_2^{t+1} と対応している.

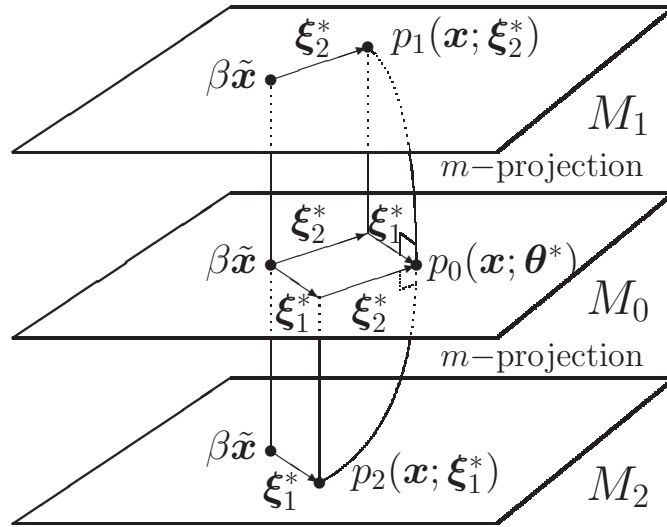


図 4: ターボ復号の情報幾何的表現

3.3 ターボ復号の解が持つ性質

ターボ復号の収束点を ξ_1^* , ξ_2^* とする. 最終的な結果は $\pi_{M_0 \circ p_1}(\mathbf{x}; \xi_2^*) = \pi_{M_0 \circ p_2}(\mathbf{x}; \xi_1^*)$ となる M_0 の座標である. 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 $\pi_{M_0 \circ p_1}(\mathbf{x}; \xi_2^*) = \pi_{M_0 \circ p_2}(\mathbf{x}; \xi_1^*) = \theta^*$ 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. $\sum_{\mathbf{x}} \mathbf{x} p_0(\mathbf{x}; \theta^*) = \sum_{\mathbf{x}} \mathbf{x} p_1(\mathbf{x}; \xi_2^*) = \sum_{\mathbf{x}} \mathbf{x} p_2(\mathbf{x}; \xi_1^*)$
2. $\theta^* = \xi_1^* + \xi_2^*$

が成り立つ. すなわちターボ復号では, 真の MPM 復号の結果を $\theta^* = \xi_1^* + \xi_2^*$ として近似している. $p_0(\mathbf{x}; \theta^*)$ と $p(\mathbf{x} | \tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2)$ とを比べてみると,

$$p(\mathbf{x} | \tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1, \tilde{\mathbf{y}}_2) = \exp(c_0(\mathbf{x}) + c_1(\mathbf{x}) + c_2(\mathbf{x}) - \ln C)$$

$$p_0(\mathbf{x}; \theta^*) = \exp(c_0(\mathbf{x}) + \xi_1^* \cdot \mathbf{x} + \xi_2^* \cdot \mathbf{x} - \varphi_0(\theta^*)).$$

となる．これを見ると直観的には $\xi_1^* \cdot x$ によって $c_1(x)$ を， $\xi_2^* \cdot x$ によって $c_2(x)$ 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．

このターボ復号によって求まった点がどのような性質を持っているか，特に復号誤差についての結果を示す．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．

$$M(\theta) = \left\{ p(x) \mid \sum_x p(x) = \sum_x p_0(x; \theta) \right\}$$

$M(\theta)$ 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 の平均と $p_0(x; \theta)$ の平均が一致することから，その θ が正しい MPM 解となる．次に新たな多様体を定義する．

$$E(\theta^*) = \left\{ p = C p_0(x; \theta^*)^{t_0} p_1(x; \xi_2^*)^{t_1} p_2(x; \xi_1^*)^{t_2} \mid \sum_{r=0}^2 t_r = 1 \right\}.$$

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点の間には次の関係が成り立つ．

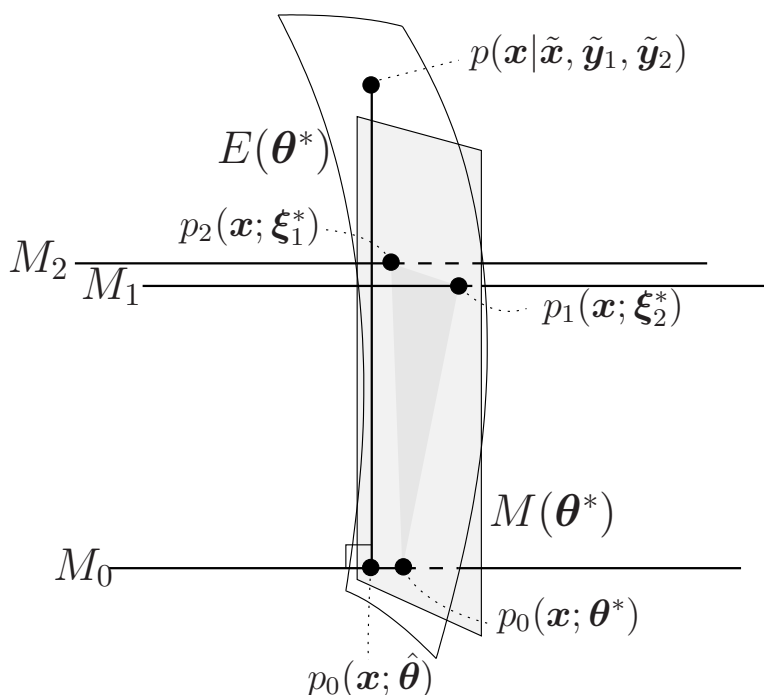


図 5: ターボ符号の情報幾何的な解釈

定理 1. 停留点では， $p_0(x; \theta^*)$ ， $p_1(x; \xi_2^*)$ ， $p_2(x; \xi_1^*)$ 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 $E(\theta^*)$ に含まれる (図 5)．

証明. $p_0(x; \theta^*)$ ， $p_1(x; \xi_2^*)$ ， $p_2(x; \xi_1^*)$ が $M(\theta^*)$ ， $E(\theta^*)$ 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 $E(\theta^*)$ 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

$$C \frac{p_1(x; \xi_2^*) p_2(x; \xi_1^*)}{p_0(x; \theta^*)} = C \exp(c_0(x) + c_1(x) + c_2(x)) = p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$$

となることから，確かめられる．

□

図 5 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 5 から分るように $E(\theta^*)$ と $M(\theta^*)$ との差から生じる．我々はこの差を近似的に計算することができ，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, 6]．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, 8]，統計物理の Bethé 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．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．

今後は情報幾何学に基づく解釈を分野横断的に様々なアルゴリズムに対して適用し，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．岩波講座 応用数学「情報幾何の方法」，岩波書店，1993.
- [2] S. Amari and H. Nagaoka. “Methods of Information Geometry”, AMS, 2000.
- [3] C. Berrou, A. Glavieux, and P. Thitimajshima. *Proceedings of IEEE International Conf. on Commun.* (1993), 1064.
- [4] R. G. Gallager. *IRE Trans. Inform. Theory* (**IT-8**) (1962), 21.
- [5] 池田思朗，田中利幸，甘利俊一．電子情報通信学会論文誌，(**J85-D-II**) (2002)，759.
- [6] S. Ikeda, T. Tanaka, and S. Amari. The MIT Press, In *Advances in Neural Information Processing Systems 14*, 2002.

- [7] Y. Kabashima and D. Saad. The MIT Press, “Advanced Mean Field Methods – Theory and Practice”, (2001) 65.
- [8] D. J. C. MacKay. *IEEE Trans. Inform. Theory*, **45** (2000), 399.
- [9] R. J. McEliece, D. J. C. MacKay, and J.-F. Cheng. *IEEE J. Select. Areas in Commun.* **16** (1998), 140.
- [10] T. J. Richardson. *IEEE Trans. Inform. Theory* **46** (2000), 9.