

## ターボ復号の情報幾何

池田 思朗<sup>†</sup> 田中 利幸<sup>††</sup> 甘利 俊一<sup>†††</sup>

Information Geometry of Turbo Decoding

Shiro IKEDA<sup>†</sup>, Toshiyuki TANAKA<sup>††</sup>, and Shun-ichi AMARI<sup>†††</sup>

あらまし ターボ符号は高い誤り訂正能力を持ち、かつ効率の良い復号法を持つ誤り訂正符号として知られている。繰り返しアルゴリズムを用いる復号法の特性については、様々な数値実験を通じて細かく調べられ、有効性が示されているが、理論的な結果は十分には得られていない。本論文では情報幾何学的観点からこの問題を扱う。その結果、ターボ符号を解析するための数学的枠組を与え、その枠組の下でターボ復号解の持つ幾つかの基本的性質を明らかにする。本論文ではターボ符号に対する情報幾何を特に扱うが、近年、ターボ復号アルゴリズムが低密度パリティ検査符号の復号アルゴリズム、また統計物理における Bethé 近似の計算法、さらにはベイジアンネットワークの確率伝播アルゴリズムと対応づけられることが指摘されている。本研究の結果はこれらの広いクラスの反復計算手法に対しても有効であり、したがって新たな解析手法となる。

キーワード ターボ符号, MPM 復号, 情報幾何

## 1. ま え が き

ターボ符号は、その復号に繰り返しアルゴリズムを用いる誤り訂正符号である。1993年に提案されて以来 [1]、ターボ符号がシャノン限界に近い信頼性を与え、かつ現実的な手法であることが様々な数値実験を通じて明らかになっている。一方、理論的な結果については、いくつかの結果が報告されているものの [2] 十分ではなく、アルゴリズムの持つ基本的な性質についても未解決な部分は多い。

一方で、ターボ復号と他の手法との関連が指摘されている。ターボ復号の繰り返しアルゴリズムと低密度パリティ検査符号 [3] の復号で用いられる繰り返しアルゴリズムとの数理的構造の共通性が明らかにされ [4]、さらに、これらの誤り訂正符号の復号の問題がベイジアンネットワークにおける推論の問題として定式化でき、復号に用いられる繰り返しアルゴリズムがそのべ

イジアンネットワークに対する確率伝播法と呼ばれる計算法と一致することも明らかになった [5]。また、間接的にはあるが、統計物理における Bethé 近似の計算手法との共通性も示されている [6]。当然これらの手法についても、理論的に未知の部分は多い。したがってターボ復号の数理的構造を解明すれば、これらの繰り返し手法の仕組みも同時に明らかになる。

このような手法の理論的解析のために最も重要なのは、数理的枠組を与えることである。本稿では、情報幾何 [7], [8] を用いてターボ復号を表現し、解析のための数理的枠組を与える。さらに、その枠組のもとでターボ復号の基本的な数理的性質について明らかにする。まず、ターボ復号の解の持つ幾何的構造を明らかにし、局所的な解の安定性の条件を示す。さらに、ターボ復号において重要となるコスト関数を示し、ターボ復号の持つ復号誤差について示す。本論文の結果は前に示したクラスの繰り返しアルゴリズムに対しても有効である。

## 2. ターボ符号の情報幾何

## 2.1 ターボ符号

情報ブロック  $x = (x_1, \dots, x_N)^T, x_i \in \{-1, +1\}$  を記憶のない二元対称通信路 (BSC: binary symmetric channel) を介して送ることを考える。本論文では

<sup>†</sup>九州工業大学 & 科学技術振興事業団, 北九州市  
Kyushu Institute of Technology & JST, 2-4 Hibikino, Wakamatsu, Kitakyushu, Fukuoka, 808-0196

<sup>††</sup>東京都立大学工学部, 八王子市  
Tokyo Metropolitan University, 1-1 Minami Oosawa, Hachioji, Tokyo, 192-0397

<sup>†††</sup>理化学研究所, 和光市  
RIKEN BSI, 2-1 Hirosawa, Wako, Saitama, 351-0198

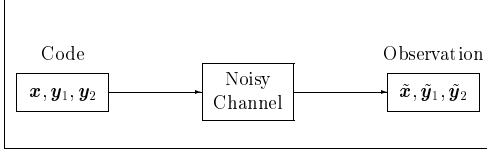


図 1 ターボ符号  
Fig. 1 Turbo codes.

確率分布の構造を簡単にし、見通しの良い議論をするため BSC を考えるが、本論文の結果得られる情報幾何の枠組自体はガウス通信路などに対しても拡張可能である。ターボ符号は一つの情報ブロックに対して畳み込み符号として実装されるが、これは符号長を大きくするためのもので本質ではない。本稿ではブロック符号として扱う [2], [5]。ターボ符号は一つの符号語に対して 2 つのエンコーダを用いて 2 つのパリティ検査語を作成する。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。 $(x, y_1, y_2)$  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。 $y_r, r = 1, 2$  は  $x$  の関数であるので、必要があれば  $y_r(x)$  と明示する。この受信語に基づき、符号語を  $\hat{x}$  として推定する。

まず、ターボ復号アルゴリズムについて示す。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  $p(\tilde{x}|x)$ ,  $p(\tilde{y}_r|x)$ ,  $r = 1, 2$ , さらに次の変数と関数  $F$  を定義する。

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

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

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

これらを用い、ターボ復号アルゴリズムは次のように

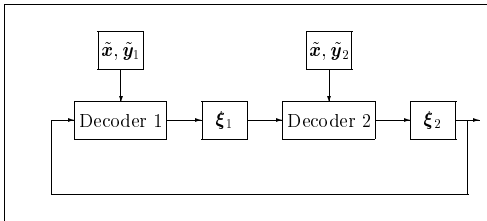


図 2 ターボ復号  
Fig. 2 Turbo decoding.

定義される (図 2)。

ターボ復号

1.  $\xi_1 = 0, t = 1$  と置く。
2.  $L_1 x^{(t)} = F((lx + \xi_1), ly_1)$  を計算し,  $\xi_2$  を次のように更新する

$$\xi_2 = L_1 x^{(t)} - (lx + \xi_1). \quad (1)$$

3.  $L_2 x^{(t)} = F((lx + \xi_2), ly_2)$  を計算し,  $\xi_1$  を次のように更新する

$$\xi_1 = L_2 x^{(t)} - (lx + \xi_2). \quad (2)$$

4.  $t$  を 1 ずつ増しながら 2, 3 を  $L_1 x^{(t)} = L_2 x^{(t)} = L_1 x^{(t+1)} = L_2 x^{(t+1)}$  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。通常、数回から 10 回程度の回数をあらかじめ決めておき、その回数のみ繰り返す。

## 2.2 MPM 復号

ターボ符号を復号する場合の目的は、MPM (maximum posterior marginal) 復号の解を求めることである。MPM 復号では  $(\tilde{x}, \tilde{y}_1, \tilde{y}_2)$  の条件付きでの  $x$  の分布  $p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$  を考え、その分布を  $x$  の各成分について周辺化し、周辺化された分布を最大にする符号を推定値とする。まず  $p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$  について考える。通信路が記憶のない BSC であることから

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

となる。それぞれの分布は、

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

$$p(\tilde{y}_r|x) = \exp(\beta \tilde{y}_r \cdot y_r(x) - L\psi(\beta)), \quad r = 1, 2$$

$$\psi(\beta) = \ln(e^{-\beta} + e^{\beta})$$

と書ける。ここで  $\beta$  は正の実数で、通信路のビットの誤り率  $f_n$  は  $f_n = (1 - \tanh \beta)/2$  と表される。 $c_0(x) = \beta \tilde{x} \cdot x$ ,  $c_1(x) = \beta \tilde{y}_1 \cdot y_1$ ,  $c_2(x) = \beta \tilde{y}_2 \cdot y_2$  と置くと、 $p(\tilde{x}, \tilde{y}_1, \tilde{y}_2|x)$  は

$$p(\tilde{x}, \tilde{y}_1, \tilde{y}_2|x) = \exp(c_0(x) + c_1(x) + c_2(x) - (N + 2L)\psi(\beta))$$

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

$$\begin{aligned} p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2) &= \frac{p(\tilde{x}, \tilde{y}_1, \tilde{y}_2|x)}{\sum_x p(\tilde{x}, \tilde{y}_1, \tilde{y}_2|x)} \\ &= C \exp(c_0(x) + c_1(x) + c_2(x)). \end{aligned} \quad (3)$$

周辺化のオペレータを  $\Pi$  と置く

$$\Pi p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2) \stackrel{\text{def}}{=} \prod_{i=1}^N p_i(x_i|\tilde{x}, \tilde{y}_1, \tilde{y}_2).$$

MPM 復号は次のように定義できる.

$$\hat{x} = \underset{x}{\operatorname{argmax}} \Pi p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2).$$

ターボ復号ではこの MPM 復号を真の目的とするが, 周辺化の計算が指数オーダーになる場合を扱う. ターボ復号アルゴリズムは MPM 復号の近似解を与える.

### 2.3 情報幾何の準備

本節では本稿で必要となる情報幾何について述べる.  $x$  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.  $(2^N - 1)$  次元の自由度を持ち, 指数分布族である

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

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

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

$c$  は規格化定数である.

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

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

次に  $m$ -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.  $q(x) \in S$  から  $M$  への  $m$ -射影は,  $M$  上の点で,  $q(x)$  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.

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

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 1 点に定まる.  $\square$

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.

ターボ復号アルゴリズムの理解のため,  $S$  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.

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

$\psi(\theta)$  は規格化関数であり, 次のように定義される.

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

$M_D$  は定義より指数分布族であり, 指数分布族は  $e$ -平坦であることから,  $M_D$  は  $e$ -平坦な部分多様体である [8]. パラメータ  $\theta$  は多様体  $M_D$  の座標系を与え, 自然パラメータと呼ぶ. 一方, 期待値パラメータと呼ばれる別の座標系,  $\eta$  を次のように定義する.

$$\eta = \sum_x p(x; \theta) x$$

$\theta$  と  $\eta$  の間には次の 1 対 1 の関係が成り立つ.

$$\eta = \partial_\theta \psi(\theta) \quad (4)$$

定理 2. 確率分布  $q(x)$  の周辺化  $\Pi_{M \circ} q(x)$  は  $q(x)$  から  $M_D$  への  $m$ -射影である.

証明.  $q(x)$  から  $M_D$  への  $m$ -射影を考える. 定理 1 より  $D[q(x); p(x; \theta)]$  を  $\theta$  で微分する. (4) の結果を用い,

$$\partial_\theta D[q(x); p(x; \theta)] = \eta - \sum_x q(x) x,$$

となる. よって,  $m$ -射影を与える  $\eta$  座標を  $\eta^*$  とすると,  $\eta^* = \sum_x q(x) x$  である. これは  $q(x)$  による  $x$  の各成分の独立な期待値によって  $m$ -射影が表されることを示しており, 周辺化と  $m$ -射影は同値である.  $\square$

さらに MPM 復号は

$$\hat{x} = \operatorname{sgn}(\eta^*),$$

と書ける. ここで  $\operatorname{sgn}(\cdot)$  は各ビットに独立に作用するものとする.

## 2.4 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1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.  $p(\tilde{x}, \tilde{y}_r|x)$ ,  $r=1, 2$  は次のように書ける.

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

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になる

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

$\varphi_r(\xi)$  は規格化関数である. ターボ符号はこの  $p_r(x; \xi)$ ,  $r=1, 2$  から  $M_D$  への  $m$ -射影の計算が多項式時間で実現可能な場合を考える. その上で  $\xi$  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.

本節では, ターボ復号の情報幾何的な解釈を与える. まずターボ符号で重要な3つの多様体を定義する.

$$\begin{aligned} M_0 &= \{p_0(x; \xi) = \exp(c_0(x) + \xi \cdot x - \varphi_0(\xi)) \mid \xi \in \mathcal{R}^N\} \\ M_1 &= \{p_1(x; \xi) \mid \xi \in \mathcal{R}^N\}, M_2 = \{p_2(x; \xi) \mid \xi \in \mathcal{R}^N\}. \end{aligned}$$

$\xi$  は各多様体の座標系を定義する.  $c_0(x) = \beta \tilde{x} \cdot x$  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  $\xi$  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  $\pi_{M_0}$  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,  $\xi_2^{t+1}$  を次のように計算する.

$$\xi_2^{t+1} = \pi_{M_0} \circ p_2(x; \xi_1^t) - \xi_1^t. \quad (5)$$

3.  $p_1(x; \xi_2^{t+1})$  から  $M_0$  への射影  $\pi_{M_0} \circ p_1(x; \xi_2^{t+1})$  を求め,  $\xi_1^{t+1}$  を次のように計算する.

$$\xi_1^{t+1} = \pi_{M_0} \circ p_1(x; \xi_2^{t+1}) - \xi_2^{t+1}. \quad (6)$$

4.  $\pi_{M_0} \circ p_1(x; \xi_2^{t+1})$  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.

(1), (2) 式中の  $L_1 x^{(t)}$ ,  $L_2 x^{(t)}$ , すなわち,  $F((lx+\xi_1), ly_1)$ ,  $F((lx+\xi_2), ly_2)$  は (5), (6) 式中の  $\pi_{M_0} \circ p_2(x; \xi_1^t)$ ,  $\pi_{M_0} \circ p_1(x; \xi_2^{t+1})$  に対応している. また, (1), (2) 式中の  $\xi_1, \xi_2$  は (5), (6) 式中の  $\xi_1^t, \xi_2^{t+1}$  と対応している.

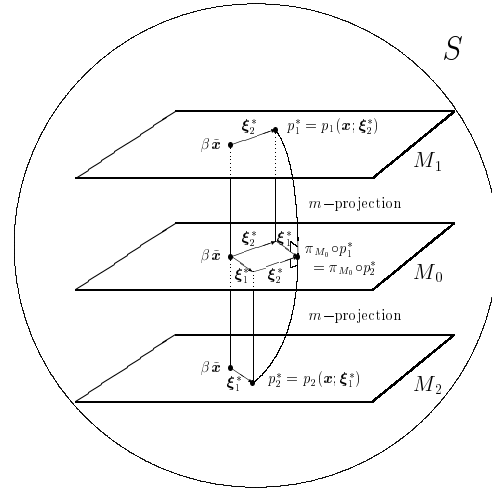


図3 ターボ復号の情報幾何

Fig. 3 Information geometry of turbo decoding.

## 3. ターボ復号の性質

### 3.1 停留点の持つ性質

ターボ復号の収束点を  $\xi_1^*$ ,  $\xi_2^*$  とする. 最終的な結果は  $\pi_{M_0} \circ p_1(x; \xi_2^*) = \pi_{M_0} \circ p_2(x; \xi_1^*)$  となる  $M_0$  の座標である. これを  $\theta^*$  とする. まず収束条件より,

$$1) \quad \Pi \circ p_1(x; \xi_2^*) = \Pi \circ p_2(x; \xi_1^*) = p_0(x; \theta^*)$$

が成り立つ. 一方  $\pi_{M_0} \circ p_1(x; \xi_2^*) = \pi_{M_0} \circ p_2(x; \xi_1^*) = \theta^*$  であることとアルゴリズムのステップ 2, 3 より,

$$2) \quad \theta^* = \xi_1^* + \xi_2^*,$$

となる. 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 .

$$p_0(x; \theta^*) = \exp(c_0(x) + \xi_1^* \cdot x + \xi_2^* \cdot x - \varphi_0(\theta^*)). \quad (7)$$

直観的にはステップ 2 で (7) 式の  $\xi_2$  を  $c_2(x)$  で置き換え,  $\xi_2^*$  を求め, ターボ復号のステップ 3 では (7) 式の  $\xi_1$  を  $c_1(x)$  で置き換え,  $\xi_1^*$  を求めている . したがって,  $\xi_1^*$  によって  $c_1(x)$  の,  $\xi_2^*$  によって  $c_2(x)$  の影響を表現したいのだが, それぞれの影響は一般に  $M_0$  上で線型に分離できない .

次の式を満す  $\xi_1, \xi_2$  をそれぞれ  $\xi_1(\theta), \xi_2(\theta)$  とする .

$$\Pi \circ p_1(x; \xi_2) = \Pi \circ p_2(x; \xi_1) = p_0(x; \theta).$$

$p_0(x; \theta), p_1(x; \xi_2(\theta)), p_2(x; \xi_1(\theta))$  を結ぶ  $m$ -平坦な多様体を  $M(\theta)$ ,  $e$ -平坦な多様体を  $E(\theta)$  とする .

$$M(\theta) = \left\{ p(x) = t_0 p_0 + t_1 p_1 + t_2 p_2 \mid t_r \geq 0, \sum_{r=0}^2 t_r = 1 \right\}$$

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

$M(\theta)$  に含まれる全ての分布の  $M_0$  への  $m$ -射影はすべて  $p_0(x; \theta)$  となる .

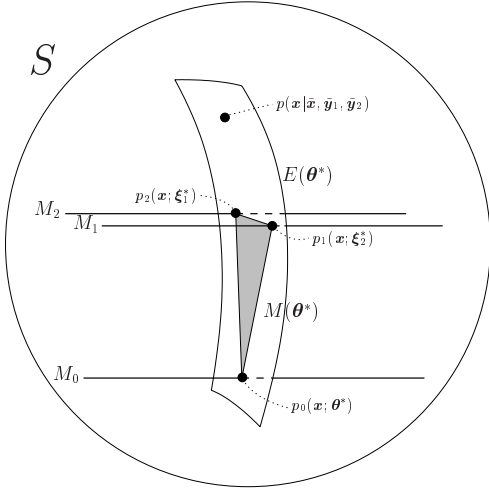


図 4 ターボ符号の情報幾何的な解釈  
Fig. 4 Information geometrical view of turbo codes.

**定理 3.** 停留点では,  $p_0^*, p_1^*, p_2^*$  の 3 つの分布が  $M(\theta^*)$  に含まれ,  $p_0^*, p_1^*, p_2^*, p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$  の 4 つが  $E(\theta^*)$  に含まれる (図 4) .

証明.  $p_0^*, p_1^*, p_2^*$  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 にすることで確かめられる .  $p_0^*, p_1^*, p_2^*, p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$  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

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

となることから, 確かめられる .  $\square$

真の MPM 復号の解が  $\theta_{MPM}^*$  として求まったとすると,  $M(\theta_{MPM}^*)$  は  $p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$  を含む . しかし, 一般にターボ復号の解  $\theta^*$  と  $\theta_{MPM}^*$  は一致しない . したがって  $p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$  は  $M(\theta^*)$  には含まれないが, 代わりに  $E(\theta^*)$  に含まれる .  $e$ -平坦性と  $m$ -平坦性とは一般に一致しないため, 多様体  $E(\theta^*)$  と多様体  $M(\theta^*)$  とはずれる . 前者で後者を代用する点がターボ符号の近似となる . 同様の構造は統計物理の他の手法にも存在している [9] ~ [12] .

### 3.2 停留点の安定性

ターボ復号の収束点を  $\xi_1^*, \xi_2^*, \theta^* = \xi_1^* + \xi_2^*$  とする .  $p_0(x; \theta), p_1(x; \xi), p_2(x; \xi)$  の Fisher 情報量行列をそれぞれ  $G_0(\theta), G_1(\xi), G_2(\xi)$  と置き,  $I_N$  を単位行列とし, それぞれの分布の期待値パラメータを  $\eta_0(\theta), \eta_1(\xi), \eta_2(\xi)$  とすると, 収束点では

$$\eta_0(\theta^*) = \eta_1(\xi_2^*) = \eta_2(\xi_1^*).$$

が成り立つ . また, それぞれに対し ( $r = 0, 1, 2$ )

$$G_r(\theta) = \partial_{\theta} \varphi_r(\theta) = \partial_{\theta} \eta_r(\theta).$$

が成り立つ . 安定性を調べるため  $\xi_1^*$  に十分小さなベクトル  $\delta$  を加えた  $\xi_1 = \xi_1^* + \delta$  をアルゴリズムの初期値とし, ターボ復号アルゴリズムを 1 回適用する . ターボ復号を 1 回行った後のパラメータを  $\xi_1' = \xi_1^* + \delta'$  と置いて線形安定性解析を行う . ステップ 2 より,  $\theta^* + \Delta\theta = \pi_{M_0} \circ p_2(x; \xi_1' + \delta)$

$$\eta_0(\theta^* + \Delta\theta) = \eta_2(\xi_1' + \delta).$$

が成り立つ . 展開すると次のようになる

$$\begin{aligned} \eta_0(\theta^*) + G_0(\theta^*) \Delta\theta &= \eta_1(\xi_2^*) + G_2(\xi_1^*) \delta \\ \Delta\theta &= G_0(\theta^*)^{-1} G_2(\xi_1^*) \delta. \end{aligned}$$

ステップ 2 における  $\xi_2$  は,

$$\xi_2 = \xi_2^* + (G_0(\theta^*)^{-1}G_2(\xi_1^*) - I_N) \delta.$$

同様にステップ 3 についても考える．その結果，ターボ符号の 1 サイクルを線形化して近似すると， $\delta$  は

$$\delta' = T\delta$$

$$T = (G_0(\theta^*)^{-1}G_1(\xi_2^*) - I_N) (G_0(\theta^*)^{-1}G_2(\xi_1^*) - I_N)$$

として更新されることになる．

定理 4.  $T$  の固有値を  $\lambda_i$  とする． $|\lambda_i| < 1$  が全ての  $i$  について成り立てば，停留点は安定である．  $\square$

この結果は [2] の結果と一致する．

### 3.3 コスト関数と停留点の性質

$\theta = \xi_1 + \xi_2$  と置き，次の関数を考える．

$$\mathcal{F}(\xi_1, \xi_2) = \varphi_0(\theta) - \varphi_1(\xi_2) - \varphi_2(\xi_1).$$

定理 5. ターボ復号の停留点  $\xi_1^*, \xi_2^*$  は  $\mathcal{F}$  の臨界点である．

証明. 直接微分すると，

$$\partial_{\xi_1} \mathcal{F} = \partial_{\theta} \varphi_0(\theta) - \partial_{\xi_1} \varphi_2(\xi_1) = \eta_0(\theta) - \eta_2(\xi_1)$$

$$\partial_{\xi_2} \mathcal{F} = \partial_{\theta} \varphi_0(\theta) - \partial_{\xi_2} \varphi_1(\xi_2) = \eta_0(\theta) - \eta_1(\xi_2).$$

平衡点では， $\eta_0(\theta^*) = \eta_2(\xi_1^*) = \eta_1(\xi_2^*)$  であることから，上の微分は 0 となる．  $\square$

ターボ復号のアルゴリズムはパラメータの更新量が微小なとき，

$$\begin{pmatrix} \xi_1^{t+1} \\ \xi_2^{t+1} \end{pmatrix} - \begin{pmatrix} \xi_1^t \\ \xi_2^t \end{pmatrix} \simeq \begin{pmatrix} O & G_0(\theta)^{-1} \\ G_0(\theta)^{-1} & O \end{pmatrix} \begin{pmatrix} \partial_{\xi_1} \mathcal{F} \\ \partial_{\xi_2} \mathcal{F} \end{pmatrix}.$$

と近似できる．しかし，この式からでは停留点の性質は明らかにはならない． $\mathcal{F}$  の Hessian を計算する

$$\mathcal{H} = \begin{pmatrix} \partial_{\xi_1 \xi_1} \mathcal{F} & \partial_{\xi_1 \xi_2} \mathcal{F} \\ \partial_{\xi_2 \xi_1} \mathcal{F} & \partial_{\xi_2 \xi_2} \mathcal{F} \end{pmatrix} = \begin{pmatrix} G_0 - G_1 & G_0 \\ G_0 & G_0 - G_2 \end{pmatrix}$$

ここで， $\theta = \xi_1 + \xi_2$ ， $\nu = \xi_1 - \xi_2$  と変数変換を行うと，

$$\begin{pmatrix} \partial_{\theta\theta} \mathcal{F} & \partial_{\theta\nu} \mathcal{F} \\ \partial_{\nu\theta} \mathcal{F} & \partial_{\nu\nu} \mathcal{F} \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 4G_0(\theta) - (G_1 + G_2) & (G_1 - G_2) \\ (G_1 - G_2) & -(G_1 + G_2) \end{pmatrix}$$

より， $\partial_{\theta\theta} \mathcal{F}$  は恐らく正定値であるが， $\partial_{\nu\nu} \mathcal{F}$  は常に負値であることが分る．したがってターボ符号の停留点は多くの場合鞍点であると考えられる．

### 3.4 真の MPM 解からのずれ

定理 3 より，MPM 復号とターボ復号の差は  $M(\theta)$  と  $E(\theta)$  の差であることがわかった．この結果を用い，ここでは真の MPM 解とターボ復号解との差を摂動法によって計算する．まず， $\theta = (\theta^1, \dots, \theta^N)^T$ ， $v = (v^1, v^2)^T$  と  $c(x) \stackrel{\text{def}}{=} (c_1(x), c_2(x))^T$  を用い  $p(x; \theta, v)$  を次のように定義する．

$$p(x; \theta, v) = \exp(c_0(x) + \theta \cdot x + v \cdot c(x) - \varphi(\theta, v))$$

$$\varphi(\theta, v) = \ln \sum_x \exp(c_0(x) + \theta \cdot x + v \cdot c(x)),$$

この分布は  $p_0(x; \theta)$  ( $v = 0$ )， $p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$  ( $\theta = 0$ )， $v = (1, 1)^T$ )， $p_r(x; \xi)$  ( $\theta = \xi$ ， $v = e_r$ ) をそれぞれ含んでいる．ただし， $e_r$  は

$$e_1 = (1, 0)^T, \quad e_2 = (0, 1)^T,$$

である．期待値パラメータ  $\eta(\theta, v)$  を定義する．

$$\eta(\theta, v) = \partial_{\theta} \varphi(\theta, v) = \sum_x p(x; \theta, v) x.$$

ここで，すべての分布の期待値パラメータが  $\eta(\theta^*)$  と等しくなるような部分多様体  $M(\theta^*)$  を定義する．すなわち  $\eta(\theta, v) = \eta(\theta^*)$  が成り立つような分布の集合である．なお， $\eta(\theta) \stackrel{\text{def}}{=} \eta(\theta, 0)$  である．以下， $\eta^* \stackrel{\text{def}}{=} \eta(\theta^*)$  とする．

以下では，摂動法を用いて  $p(x; \theta, v)$  が  $M(\theta^*)$  上にあるという拘束条件の下で  $\theta$  が  $v$  にどのように依存するかを考える．摂動法では  $\{v^r c_r(x)\}$  から  $p(x; \theta, v)$  への寄与は小さいとして  $p(x; \theta, v)$  を  $\{v^r\}$  によって Taylor 展開し， $O(\|v\|^2)$  の項まで残した上で  $v$  の高次の項を切り捨て， $\{v^r c_r(x)\}$  の影響を評価する．Taylor 展開すると，

$$\begin{aligned} \eta_i(\theta, v) &= \eta_i^* + \sum_j \partial_j \eta_i^* \Delta \theta^j + \sum_r \partial_r \eta_i^* v^r \\ &+ \frac{1}{2} \sum_{r,s} \partial_r \partial_s \eta_i^* v^r v^s + \sum_{j,r} \partial_r \partial_j \eta_i^* v^r \Delta \theta^j \\ &+ \frac{1}{2} \sum_{k,l} \partial_k \partial_l \eta_i^* \Delta \theta^k \Delta \theta^l + O(\|v\|^3) + O(\|\Delta \theta\|^3), \end{aligned}$$

となる．ここで  $\{i, j, k, l\}$  は  $\theta$  の， $\{r, s\}$  は  $v$  の添え字，また  $\Delta \theta \stackrel{\text{def}}{=} \theta - \theta^*$  である．分布が  $M(\theta^*)$  上にあるという拘束条件のもとでは  $\eta_i(\theta, v) = \eta_i^*$  である．また  $\{g_{ij}\}$  を  $p(x; \theta^*, 0)$  の Fisher 情報行列とする．これは対角行列である．これらを使うと，以下の式が

導かれる．

$$\begin{aligned} \Delta\theta^i &= -g^{ii} \left[ \sum_r \partial_r \eta_i^* v^r - \frac{1}{2} \sum_{r,s} \partial_r \partial_s \eta_i^* v^r v^s \right. \\ &\quad \left. - \frac{1}{2} \sum_{k,l} \partial_k \partial_l \eta_i^* \Delta\theta^k \Delta\theta^l - \sum_{k,r} \partial_r \partial_k \eta_i^* v^r \Delta\theta^k \right] \\ &\quad + O(\|v\|^3) + O(\|\Delta\theta\|^3), \end{aligned}$$

なお  $g^{ii} = 1/g_{ii}$  である． $\Delta\theta^i$  を  $v^r$  の 2 次までの項を用いて書き直し，3 次以上の項を無視すると，

$$\begin{aligned} \Delta\theta^i &\simeq -g^{ii} \sum_r A_{ir} v^r - \frac{g^{ii}}{2} \times \\ &\quad \sum_{r,s} (\partial_r - \sum_k g^{kk} A_{kr} \partial_k) (\partial_s - \sum_j g^{jj} A_{js} \partial_j) \eta_i^* v^r v^s. \end{aligned} \quad (8)$$

とかける．ただし

$$A_{ir} = \partial_r \eta_i^*.$$

である．

ここで  $v = e_1$  とおくと， $p(x; \theta, v)$  が  $M(\theta^*)$  に拘束されていることから  $\theta = \xi_2^*$  であり， $\Delta\theta = \xi_2^* - \theta^* = -\xi_1^*$ ，となる． $v = e_2$  のときは，同様の議論から  $\Delta\theta = -\xi_2^*$  である．(8) 式を用いると，これらが以下のように表現できる．

$$\begin{aligned} -\xi_r^{i,*} &\simeq -g^{ii} A_{ir} \\ &\quad - \frac{g^{ii}}{2} (\partial_r - \sum_k g^{kk} A_{kr} \partial_k) (\partial_r - \sum_j g^{jj} A_{jr} \partial_j) \eta_i^*. \end{aligned} \quad (9)$$

一方  $v = \sum_r e_r$  とし  $p(x; \theta, v)$  を  $M(\theta^*)$  に拘束する．このとき，拘束条件を満たすパラメータ  $\theta$  を  $\bar{\theta}$  と定義する．一般に  $\bar{\theta}$  は  $\mathfrak{o}$  とはならない．これは  $p(x|\bar{x}, \bar{y}_1, \bar{y}_2)$  が必ずしも  $M(\theta^*)$  に含まれないことを示している．(8) 式より，

$$\begin{aligned} \bar{\theta}^i - \theta^{i,*} &\simeq -g^{ii} \sum_r A_{ir} \\ &\quad - \frac{g^{ii}}{2} \sum_r (\partial_r - \sum_k g^{kk} A_{kr} \partial_k) (\partial_r - \sum_j g^{jj} A_{jr} \partial_j) \eta_i^*, \end{aligned}$$

となる． $\theta^{i,*} = \xi_1^{i,*} + \xi_2^{i,*}$  と (9) 式の結果から，

$$\begin{aligned} \bar{\theta}^i &\simeq \\ &\quad - \frac{g^{ii}}{2} \sum_{r \neq s} (\partial_r - \sum_k g^{kk} A_{kr} \partial_k) (\partial_s - \sum_j g^{jj} A_{js} \partial_j) \eta_i^*, \end{aligned}$$

となる． $M_0$  上でこのパラメータの差を評価すると，ターボ解と MPM 解との差が評価できる．MPM 解を  $\eta_{MPM}^*$  と書くことにすると，

$$\begin{aligned} \eta_{i,MPM}^* &\simeq \eta_i^* \\ &\quad + \frac{1}{2} \sum_{r \neq s} (\partial_r - \sum_k g^{kk} A_{kr} \partial_k) (\partial_s - \sum_j g^{jj} A_{js} \partial_j) \eta_i^*. \end{aligned}$$

となる．この結果から次の定理が得られる．

**定理 6.** ターボ復号の解による  $x_i$  の期待値を  $\eta^*$ ，MPM 復号解によるものを  $\eta_{MPM}^*$  とおくと，その差は次の通りである．

$$\begin{aligned} \eta_{MPM}^* - \eta^* &\simeq \\ &\quad \frac{1}{2} \sum_{r \neq s} (\partial_r - \sum_k g^{kk} A_{kr} \partial_k) (\partial_s - \sum_j g^{jj} A_{js} \partial_j) \eta^*. \end{aligned}$$

□

上式で与えられる復号誤差は，多様体  $E(\theta)$  の埋め込み  $e$ -曲率と関係している．

#### 4. まとめ

我々は，本論文において，情報幾何に基づきターボ符号の数理的構造を明らかにした．我々の結果はターボ符号の解析のための数理的枠組を与えるものであり，この枠組の中で，さらに多くの性質が明らかになると考える．

この数理的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，(3) 式のような指数分布族の構造を持つ確率分布の周辺化を近似する問題として捉えることができる．このような分布を，部分問題に分解し，それぞれの情報を繰り返しアルゴリズムで求めながら近似するという問題である．

同様の構造は低密度パリティ検査符号，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播法にも存在する．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，本論文で定義したコスト関数と同等な関数が存在し，その関数に基づく解析は有効である．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 [13]．

またそれぞれのアルゴリズムの収束点では，定理 3

と同様の構造が存在する．我々は既に低密度パリティ検査符号に関しては結果を得ている．さらに Bethé 近似，確率伝播法についても同様の解析を行なっていくたい．

#### 謝辞

本研究に対し，有益な御助言を頂いた樺島祥介氏，井坂元彦氏に感謝致します．また，二人の査読者には本論文の初稿に対する貴重な御意見を頂きました．感謝致します．

#### 文 献

- [1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," Proc. IEEE Int'l. Conf. on Commun., pp.1064–1070, Geneva, Switzerland, May 1993.
- [2] T. Richardson, "The geometry of turbo-decoding dynamics," IEEE Trans. Inform. Theory, vol.46, no.1, pp.9–23, January 2000.
- [3] R.G. Gallager, "Low density parity check codes," IRE Trans. Inform. Theory, vol.8, pp.21–28, 1962.
- [4] D.J.C. MacKay, "Good error-correcting codes based on very sparse matrices," IEEE Trans. Inform. Theory, vol.45, no.2, pp.399–431, March 1999.
- [5] R.J. McEliece, D.J.C. MacKay, and J.F. Cheng, "Turbo decoding as an instance of Pearl's "belief propagation" algorithm," IEEE J. Selec. Areas Commun., vol.16, no.2, pp.140–152, February 1998.
- [6] Y. Kabashima and D. Saad, "The TAP approach to intensive and extensive connectivity systems," in Advanced Mean Field Methods – Theory and Practice, ed. M. Oppor and D. Saad, ch. 6, pp.65–84, The MIT Press, 2001.
- [7] S. Amari, Differential-Geometrical Methods in Statistics, Lecture Notes in Statistics, vol.28, Springer-Verlag, Berlin, 1985.
- [8] S. Amari and H. Nagaoka, Methods of Information Geometry, AMS and Oxford University Press, 2000.
- [9] H.J. Kappen and W.J. Wiegierinck, "Mean field theory for graphical models," in Advanced Mean Field Methods – Theory and Practice, ed. M. Oppor and D. Saad, ch. 4, pp.37–49, The MIT Press, 2001.
- [10] S. Amari, S. Ikeda, and H. Shimokawa, "Information geometry and mean field approximation: The  $\alpha$ -projection approach," in Advanced Mean Field Methods – Theory and Practice, ed. M. Oppor and D. Saad, ch. 16, pp.241–257, The MIT Press, 2001.
- [11] T. Tanaka, "Information geometry of mean-field approximation," Neural Computation, vol.12, no.8, pp.1951–1968, August 2000.
- [12] T. Tanaka, "Information geometry of mean-field approximation," in Advanced Mean Field Methods – Theory and Practice, ed. M. Oppor and D. Saad, ch. 17, pp.259–273, The MIT Press, 2001.
- [13] S. Ikeda, T. Tanaka, and S. Amari, "Information ge-

ometry of turbo codes and low-density parity-check codes," submitted to IEEE Trans. Inform. Theory, August 2001.

(平成 13 年 8 月 17 日受付, 11 月 30 日再受付)

#### 池田 思朗 (正員)

平 8 東大大学院博士課程了 (計数工学) . 理研基礎特研, 科技団さきがけ研究員を経て, 現在九工大助教授, 理研脳総研非常勤研究員. 確率モデルの学習, 信号処理を研究.

#### 田中 利幸 (正員)

昭 63 東大・工・電子卒. 平 5 同大大学院博士課程了. 博士 (工学) . 現在, 都立大大学院工学研究科講師. 神経回路網に関する理論的研究に従事.

#### 甘利 俊一 (正員)

昭 38 東大大学院博士課程了 (数理工学) . 九大助教授, 東大助教授, 教授を経て, 現在, 理研 脳総研 領域ディレクター. 数理工学全般, 特に神経回路網理論, 情報幾何学を研究. 本会副会長, INNS 会長などを歴任. 平 7 学士院賞, 平 9 IEEE ピオー

レ賞受賞.