

ターボ符号の情報幾何

Information geometry of turbo code

池田 思朗*[‡]

Shiro Ikeda

田中 利幸[†]

Toshiyuki Tanaka

甘利 俊一[‡]

Shun-ichi Amari

Abstract: Since the turbo code was proposed early in 90's, it is known that the turbo code gives a practical and powerful method for error correction. The properties of the code have been investigated intensively mainly through experiments. Although those results strongly support the high ability of the turbo code, there is no satisfactory theoretical results. In this paper, we elucidate the idea of turbo code through information geometrical viewpoint. From our study, we obtained the stability condition, characteristics of the equilibrium, convergence property, and approximation ability. Recently it is pointed out that another error correcting code, the Gallager code has the similar structure with the turbo code. Also Bethé approximation in statistical physics, and belief propagation for Bayesian net with loops have very good similarities with the turbo code. Therefore, we believe our results will give a new perspective for these family of iterative methods.

Keywords: Turbo code, MPM decoding, Information Geometry.

1 まえがき

ターボ符号は、復号アルゴリズム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 [2], 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 [6] 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、ターボ符号と他の手法との関連が指摘されている。Gallager 符号との数理的構造の共通性 [4] や、統計物理における Bethé 近似との共通性 [3], また、ループのあるベイジアンネットへの Belief Propagation 法がターボ復号の計算法と一致することが示されている [5]。当然これらの手法の理論的解析にも未知の部分が多い。したがってターボ符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。

理論的解析のために重要なのは、これらの手法を解析する枠組を与えることであり、本稿では、情報幾何 [1] を用いてターボ符号の解析のための数理的枠組を与え、その枠組のもとで、ターボ復号の収束性、解の安定性、真の解からのターボ解のずれを示す。

2 ターボ符号の情報幾何

2.1 ターボ符号

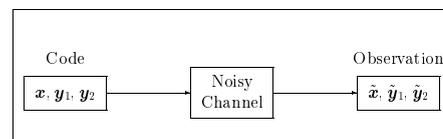


図 1: ターボ符号

情報ブロック $\mathbf{x} = (x_1, \dots, x_N)^T$, $x_i \in \{-1, +1\}$ 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。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 [5, 6]。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 $\mathbf{y}_1 = (y_{11}, \dots, y_{1L})^T$, $\mathbf{y}_2 = (y_{21}, \dots, y_{2L})^T$, $y_{1j}, y_{2j} \in \{-1, +1\}$ とする。 $(\mathbf{x}, \mathbf{y}_1, \mathbf{y}_2)$ を通信路によって

*九工大 & 科技団, 〒 808-0196 福岡県 北九州市 若松区 ひびきの 1-1, Tel & Fax. 093-695-3492, e-mail shiro@brain.kyutech.ac.jp, Kyushu Institute of Technology & JST, 1-1 Hibikino, Wakamatsu, Kitakyushu, Fukuoka 8080196, Japan.

[†] 東京都立大学, 〒 192-0397 東京都 八王子市 南大沢 1-1, e-mail tanaka@eei.metro-u.ac.jp, Tokyo Metropolitan University, 1-1 Minami Oosawa, Hachioji, Tokyo, 1920397 Japan.

[‡] 理研 脳総研, 〒 351-0198 埼玉県 和光市 広沢 2-1, RIKEN, BSI, 2-1 Hirosawa, Wako, Saitama, 3510198, Japan.

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 $p(\tilde{x}|\mathbf{x})$, $p(\tilde{y}_r|\mathbf{x})$, $(r = 1, 2)$, さらに次の変数と関数 F を定義する。

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

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

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

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2)。

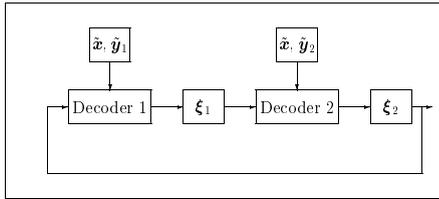


図2: ターボ復号

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

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

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

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

4. t を1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。

この繰り返しは本来収束するまで続けるべきだが、実際は数回から10回程程度の回数に決められ、その回数のみ行なわれる。

2.2 MPM 復号

ターボ符号の真の目的は、MPM (maximum posterior marginal) 復号を求めることである。MPM 復号で

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

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

となる。それぞれの分布は、

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

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

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

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 f_n は $f_n = (1 - \tanh \beta)/2$ と表される。 $c_0(\mathbf{x}) = \beta \tilde{x} \cdot \mathbf{x}$, $c_1(\mathbf{x}) = \beta \tilde{y}_1 \cdot \mathbf{y}_1$, $c_2(\mathbf{x}) = \beta \tilde{y}_2 \cdot \mathbf{y}_2$ と置くと、 $p(\tilde{x}, \tilde{y}_1, \tilde{y}_2|\mathbf{x})$ は

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

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

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

$$= C \exp(c_0(\mathbf{x}) + c_1(\mathbf{x}) + c_2(\mathbf{x})). \quad (1)$$

周辺化のオペレータを Π と置く

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

MPM 復号は次のように定義できる。

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

ターボ復号では、この MPM 復号を真の目的とするが、周辺化の計算が現実的な時間では不可能な場合を扱う。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

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

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 $q(x), p(x) \in M$ 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.

定理 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 への次の Kullback-Leibler ($K-L$) 情報量を最小にする点であり, 次のように定義される.

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

この m -射影は 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

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

$K-L$ 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の多様体を考える. これを M_D とする. これは指数分布族であり, e -平坦な多様体である. 定義は次の通りである.

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

$$\psi(\theta) = \sum_i \psi(\theta_i) = \sum_i \log(e^{-\theta_i} + e^{\theta_i}).$$

パラメータ θ 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, η を次のように定義する.

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

θ と η の間には次の 1 対 1 の関係が成り立つ.

$$\eta = \partial_\theta \psi(\theta) \quad (2)$$

定理 2. 確率分布 $q(x)$ の周辺化 $I_{M_D \circ} q(x)$ 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 θ で微分する. (2) 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 η 座標を η^* 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. □

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 つのパーティ検査語を同時に用いるのではなく, \tilde{x} と 1 つのパー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. ターボ符号はこの $p_r(x; \xi)$, ($r = 1, 2$) から M_D への m -射影が可能な場合を考える. 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.

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.

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

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

ξ は各多様体の座標系を定義する. $c_0(x) = \beta \tilde{x} \cdot x$ であるので, $\theta = \xi + \beta \tilde{x}$ と置くと, $p(x; \theta) = p_0(x; \xi)$ 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.

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

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, ξ_1^{t+1} を次のように計算する.

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

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

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 ξ_1^* , ξ_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 θ^* 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 $\theta^* = \pi_{M_0 \circ p_1}(x; \xi_2^*) = \pi_{M_0 \circ p_2}(x; \xi_1^*)$ 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.

$$p_0(x; \theta^*) = \exp(c_0(x) + \xi_1^* \cdot x + \xi_2^* \cdot x - \varphi_0(\theta^*)). \quad (3)$$

直観的にはステップ 2 で (3) 式の ξ_2 を $c_2(x)$ で置き換え, ξ_2^* を求め, ターボ復号のステップ 3 では (3) 式の ξ_1 を $c_1(x)$ で置き換え, ξ_1^* を求めている. したがって, ξ_1^* によって $c_1(x)$ の, ξ_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 ξ_1, ξ_2 をそれぞれ $\xi_1(\theta), \xi_2(\theta)$ とする.

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

$p_0(x; \theta), p_1(x; \xi_2(\theta)), p_2(x; \xi_1(\theta))$ 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.

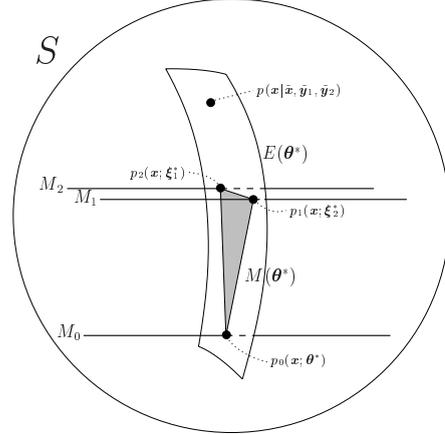


図 3: ターボ符号の情報幾何的な解釈

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 3).

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

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

となることから, 確かめられる. □

真の MPM 復号では, $p(x|\tilde{x}, \tilde{y}_1, \tilde{y}_2)$ が $M(\theta)$ に含まれるが, ターボ復号では $E(\theta)$ のみに含まれる. 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.

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 ($*$ = 0, 1, 2)

$$G_*(\theta) = \partial_{\theta\theta'} \varphi_*(\theta) = \partial_{\theta} \eta_*(\theta).$$

が成り立つ. 安定性を調べるため ξ_1^* に十分小さなベクトル δ 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 ξ_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についても考えると、

$$\delta' = T\delta$$

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

定理4. T の固有値を λ_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 [6] 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 ξ_1^*, ξ_2^* は \mathcal{F} の臨界点である。

証明. 直接微分すると、

$$\begin{aligned} \partial_{\xi_1}\mathcal{F} &= \partial_{\theta}\varphi_0(\theta) - \partial_{\xi_1}\varphi_2(\xi_1) = \eta_0(\theta) - \eta_2(\xi_1) \\ \partial_{\xi_2}\mathcal{F} &= \partial_{\theta}\varphi_0(\theta) - \partial_{\xi_2}\varphi_1(\xi_2) = \eta_0(\theta) - \eta_1(\xi_2). \end{aligned}$$

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、 $\mathbf{u} = (u_1, \dots, u_N)^T$ 、 $\mathbf{v} = (v_1, v_2)^T$ と $\mathbf{c}(\mathbf{x}) \stackrel{\text{def}}{=} (c_1(\mathbf{x}), c_2(\mathbf{x}))^T$ を用い、次のように定義する。

$$p(\mathbf{x}; \mathbf{u}, \mathbf{v}) = \exp(c_0(\mathbf{x}) + \mathbf{x} \cdot \mathbf{u} + \mathbf{c}(\mathbf{x}) \cdot \mathbf{v} - \varphi(\mathbf{u}, \mathbf{v}))$$

$$\varphi(\mathbf{u}, \mathbf{v}) = \log \sum_{\mathbf{x}} \exp(c_0(\mathbf{x}) + \mathbf{x} \cdot \mathbf{u} + \mathbf{c}(\mathbf{x}) \cdot \mathbf{v}),$$

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

$$\mathbf{e}_1 = (1, 0)^T, \quad \mathbf{e}_2 = (0, 1)^T,$$

である。期待値パラメータ $\eta(\mathbf{u}, \mathbf{v})$ を定義する。

$$\eta(\mathbf{u}, \mathbf{v}) = \partial_{\mathbf{u}}\varphi(\mathbf{u}, \mathbf{v}) = \sum_{\mathbf{x}} p(\mathbf{x}; \mathbf{u}, \mathbf{v})\mathbf{x}.$$

ここで、すべての分布の期待値パラメータが等しくなるような部分多様体 $M(\mathbf{u}_0)$ を定義する。すなわち $\eta(\mathbf{u}, \mathbf{v}) = \eta(\mathbf{u}_0)$ が成り立つような分布の集合である。ここで $\eta(\mathbf{u}_0) \stackrel{\text{def}}{=} \eta(\mathbf{u}_0, \mathbf{0})$ である。Taylor 展開すると、

$$\begin{aligned} \eta_i(\mathbf{u}, \mathbf{v}) &= \eta_i(\mathbf{u}_0) + \sum_j \partial_j \eta_i(\mathbf{u}_0) \Delta u_j + \sum_r \partial_r \eta_i(\mathbf{u}_0) v_r \\ &+ \frac{1}{2} \sum_{r,s} \partial_r \partial_s \eta_i(\hat{\theta}) v_r v_s + \sum_{j,r} \partial_r \partial_j \eta_i(\hat{\theta}) v_r \Delta u_j \\ &+ \frac{1}{2} \sum_{k,l} \partial_k \partial_l \eta_i(\hat{\theta}) \Delta u_k \Delta u_l \\ &+ O(\|\mathbf{v}\|^3) + O(\|\Delta \mathbf{u}\|^3), \end{aligned} \quad (4)$$

となる。ここで $\{i, j, k, l\}$ は \mathbf{u} の、 $\{r, s\}$ は \mathbf{v} の添え字、また $\Delta \mathbf{u} \stackrel{\text{def}}{=} \mathbf{u} - \mathbf{u}_0$ である。 $\eta_i(\mathbf{u}, \mathbf{v}) = \eta_i(\mathbf{u}_0)$ であること、また $\{g_{ij}\}$ を $p(\mathbf{x}; \mathbf{u}_0, \mathbf{0})$ の Fisher 情報行列とする。これは対角行列である。上の式は次のように書き

直せる ,

$$\begin{aligned} \Delta u_i = & -g^{ii} \left[\sum_r \partial_r \eta_i(\mathbf{u}_0) v_r - \frac{1}{2} \sum_{r,s} \partial_r \partial_s \eta_i(\mathbf{u}_0) v_r v_s \right. \\ & \left. - \frac{1}{2} \sum_{k,l} \partial_k \partial_l \eta_i(\mathbf{u}_0) \Delta u_k \Delta u_l - \sum_{k,r} \partial_r \partial_k \eta_i(\mathbf{u}_0) v_r \Delta u_k \right] \\ & + O(\|\mathbf{v}\|^3) + O(\|\Delta \mathbf{u}\|^3), \end{aligned}$$

ここで $g^{ii} = 1/g_{ii}$ である . Δu_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 ,

$$\begin{aligned} \Delta u_i \simeq & -g^{ii} \sum_r A_r^i v_r - \frac{g^{ii}}{2} \times \\ & \sum_{r,s} \left(\partial_r - \sum_k g^{kk} A_r^k \partial_k \right) \left(\partial_s - \sum_j g^{jj} A_s^j \partial_j \right) \eta_i(\mathbf{u}_0) v_r v_s. \end{aligned} \quad (5)$$

とかける . ただし

$$A_r^i = \partial_r \eta_i(\mathbf{u}_0).$$

である . 次の分布を考える .

$$p(\mathbf{x}; \mathbf{u}_0, \mathbf{o}) = \exp(c_0(\mathbf{x}) + \mathbf{x} \cdot \mathbf{u}_0 - \varphi(\mathbf{u}_0, \mathbf{o}))$$

$$p(\mathbf{x}; \mathbf{u}_r, \delta \mathbf{e}_r) =$$

$$\exp(c_0(\mathbf{x}) + \mathbf{x} \cdot \mathbf{u}_r + \delta c_r(\mathbf{x}) - \varphi(\mathbf{u}_r, \delta \mathbf{e}_r))$$

$$p(\mathbf{x}; \mathbf{u}_*, \delta \sum_r \mathbf{e}_r) =$$

$$\exp\left(c_0(\mathbf{x}) + \mathbf{x} \cdot \mathbf{u}_* + \delta \sum_r c_r(\mathbf{x}) - \varphi(\mathbf{u}_*, \delta \sum_r \mathbf{e}_r)\right),$$

これらのうち $p(\mathbf{x}; \mathbf{u}_0, \mathbf{o})$, $p(\mathbf{x}; \mathbf{u}_r, \delta \mathbf{e}_r)$, $r = 1, 2$ が $M(\mathbf{u}_0)$ に含まれるとし , \mathbf{u}_* は次式を満たすものとする

$$(\mathbf{u}_* - \mathbf{u}_0) = \sum_r (\mathbf{u}_r - \mathbf{u}_0).$$

ここで $\delta = 1$, とすれば , $\mathbf{u}_0 = \boldsymbol{\theta}^*$, となり , ターボ復号の収束点と一致する . (4) 式と (5) 式の結果から , $\eta_i(\mathbf{u}_*, \delta \sum_r \mathbf{e}_r)$ を δ の 2 次までの項で表すと ,

$$\begin{aligned} \eta_i(\mathbf{u}_*, \delta \sum_r \mathbf{e}_r) \simeq & \eta_i(\mathbf{u}_0) \\ & + \frac{1}{2} \sum_{r \neq s} \left(\partial_r - \sum_k g^{kk} A_r^k \partial_k \right) \left(\partial_s - \sum_j g^{jj} A_s^j \partial_j \right) \eta_i(\mathbf{u}_0) \delta^2. \end{aligned}$$

$\mathbf{u}_0 = \boldsymbol{\theta}^*$, $\delta = 1$ とおくと , 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 $\eta_{*,i}$, MPM 復号解によるものを η_i とおくと , その差は次の通りである .

$$\begin{aligned} \eta_{*,i} - \eta_i \simeq & \\ & \frac{1}{2} \sum_{r \neq s} \left(\partial_r - \sum_k g^{kk} A_r^k \partial_k \right) \left(\partial_s - \sum_j g^{jj} A_s^j \partial_j \right) \eta_i(\boldsymbol{\theta}^*). \end{aligned}$$

□

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

4 まとめ

我々は情報幾何に基づき , 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 , さらに多くの性質を明らかにできると考える .

この問題はターボ符号だけでなく , より一般的に , (1) 式のような構造を持つ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 Gallager 符号 , 統計物理の Bethé 近似 , ループのあるベイジアンネットの belief propagation 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 , 解の安定性については全く同じ結果は得られないが , コスト関数の定義に基づく同様の解析は有効である .

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 . したがって , それぞれの問題に対し , 定理 6 と同等の結果を導くことができる . 我々は既にターボ符号と Gallager 符号に関しては結果を得ている . さらに Bethé 近似 , belief propagation アルゴリズムについても同様の解析を行なっていきたい .

参考文献

- [1] S. Amari and H. Nagaoka. *Methods of Information Geometry*. AMS and Oxford Univ. Press, 2000.
- [2] C. Berrou and A. Glavieux. Near optimum error correcting coding and decoding: Turbo-codes. *IEEE Trans. Comm.*, 44(10):1261–1271, 1996.
- [3] Y. Kabashima and D. Saad. The TAP approach to intensive and extensive connectivity systems. In M. Opper and D. Saad, eds., *Advanced Mean Field Theory – Theory and Practice*, pages 65–84. MIT Press, 2001.
- [4] D. J. C. MacKay. Good error-correcting codes based on very sparse matrices. *IEEE Trans. IT*, 45(2):399–431, 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. SAC*, 16(2):140–152, 1998.
- [6] T. Richardson. The geometry of turbo-decoding dynamics. *IEEE Trans. IT*, 46(1):9–23, 2000.