TAP 平均場近似による誤り訂正符号の復号化

東京工業大学大学院総合理工学研究科　樺島祥介 [1]

統計モデルを用いた情報処理では最適性が理論的に示されながらもその計算量的複雑さのために実用化に至っていないアルゴリズムが少なからず存在する。他方、統計力学では専ら厳密計算が絶望的な大自由度のボルツマン分布を相手にしてきたため数多くの近似計算法を高度に発達させてきた。ならば、それらの近似計算法を計算が困難な情報処理の問題に活用することはできないだろうか？本稿では、厳密計算が困難な情報処理の一例である誤り訂正符号の復号化問題に対してスピングラスの平均場理論で開発された TAP 平均場近似が高性能な近似解法となることを示す。なお、本報告は Aston 大学 David Saad 氏、東工大総理工 村山立人氏との共同研究の結果 [5, 4, 6, 12] に基づいている。

1　誤り訂正符号

誤り訂正符号とはデジタル情報通信を行う際にノイズによる誤りを小さくするために用いられる符号化技術である。以下、簡単のため情報はビット間に相関のない N 次元 2 値ベクトル $\boldsymbol{\xi} = (\xi_1, \xi_2, \ldots, \xi_N)$、$(\xi_i = \pm 1, i = 1, \ldots, N)$ で表現されるものとし、ノイズの種類としては 2 値符号が各成分無相関に確率 p で反転する Binary Symmetric Channel (BSC) を仮定するが、Gaussian Channel でも同様である。この目的のため、通常情報 $\boldsymbol{\xi}$ を符号語と呼ばれるそれよりも長い M 次元 $(M > N)$ の 2 値ベクトル $\boldsymbol{J}^0 = (J_1^0, J_2^0, \ldots, J_M^0)$、$(J_\mu = \pm 1, \mu = 1, \ldots, M)$ に一旦変換 (**符号化**) して送信し、受け手はノイズを含む符号語 $\boldsymbol{J}$ から元情報 $\boldsymbol{\xi}$ を推定 (**復号化**) する、という手続きがなされる (図 1)。このとき符号化率 $R = N/M$ が小さい程冗長性が大きく誤り訂正能力は高くなるが、そのぶん単位時間当たりに送信できる情報量が減少する。この二つの要請を出来るだけ満足し、かつ現実的な計算資源の範囲で符号化／復号化の手続きを設計することが誤り訂正符号研究に課された研究課題である。

2　Sourlas 符号

Sourlas (1989) はこの誤り訂正符号の問題がスピングラスモデルと密接に関連していることを指摘し、以下のような符号を考察した [18, 19]。送信者は元情報から K 個の成分を選び、その積により符号語

[1]E-mail: kaba@dis.titech.ac.jp

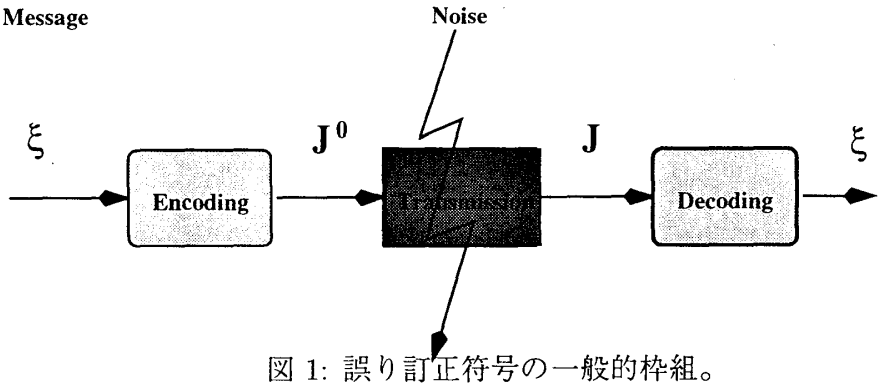

図 1: 誤り訂正符号の一般的枠組。

$$J_\mu^0 = \xi_{l_{\mu,1}} \xi_{l_{\mu,2}} \cdots \xi_{l_{\mu,K}} \tag{1}$$

を構成する。ただし、$l_{\mu,i}$ は符号語の第 μ 成分 J_μ^0 を作る際に i 番目に取り出す元情報の成分 $\xi_{l_{\mu,i}}$ を指定する添字であり、これに関してはあらかじめ送信者、受信者とも既知であるとする。Sourlas はすべての積の組み合わせ $M = N!/K!(M-K)!$ を送信すると仮定したがこれでは符号語があまりにも長すぎて実用的に意味がない [18]。以下では、各符号語を構成する K 個の元情報の成分は出来るだけランダムに、なおかつ各成分はなるべく均等に KM/N 回ずつ符号語の構成に用いられるように決める、と仮定する [5, 4]。

受信者は送信中にノイズが付加された符号語 $\boldsymbol{J}$ を受け取る。Sourlas は復号化を以下のハミルトニアン

$$\mathcal{H}(\boldsymbol{S}|\boldsymbol{J}) = -\sum_{\mu=1}^{M} J_\mu S_{l_{\mu,1}} S_{l_{\mu,2}} \cdots S_{l_{\mu,K}} \tag{2}$$

によって表現されるイジングスピン系の問題と関連付けた。より具体的に言えば、西森温度 $\beta_N = (1/2)\ln[(1-p)/p]$ での各イジングスピン変数 S_l に関する磁化 $\langle S_l \rangle_{\beta_N}$ を計算し

$$\hat{\xi}_l^B = \mathrm{sign}\, \langle S_l \rangle_{\beta_N} \tag{3}$$

のように元情報 $\boldsymbol{\xi}$ の推定値を割り当てると、オーバーラップ $M = (1/N)\sum_{l=1}^{N} \xi_l \hat{\xi}_l$ の期待値はどのようなアルゴリズムによる結果よりも大きくなる [19, 13, 8]。つまり、式 (3) は元情報と復号化された情報のオーバーラップを最大にするという意味での Sourlas 符号に関する最適復号法に他ならない。

この符号の性能／限界を考えるために Shannon にならい長符号長極限 $N, M \to \infty$、$R = N/M \sim O(1)$ を考えることにする [16]。驚くべきことに上記の符号化/復号化が実現可能ならば $K \to \infty$ でこの符号は Shannon により求められた誤り訂正符号に関する限界性能を達成することも示される [18, 5]。問題はこれが現実的な計算資源で可能か否かということである。符号化に関しては各符号語を構成するのに元情報に関する K 個の要素間の積を計算するだけでよいので計算量は $O(MK)$ であり全く問題ではない。

問題となるのは復号化 (3) に必要な計算量である。磁化は各イジング変数 S_l のボルツマン分布に関する期待値

$$\langle S_l \rangle_{\beta_N} = \frac{\sum_{\boldsymbol{S}} S_l \exp\left[-\beta_N \mathcal{H}(\boldsymbol{S}|\boldsymbol{J})\right]}{\mathcal{Z}(\boldsymbol{J}, \beta_N)} \tag{4}$$

である。これは離散変数 (イジング変数) に関する和であるため求積法などで求めることは出来ない。したがって、厳密に計算するためには $\boldsymbol{S}$ に関する 2^N 個の状態すべての和が必要となる。残念ながら、これを現存する計算資源で高速に行なうことは極めて難しい。

3 平均場近似

ここで改めて困難の原因を考えよう。これは要するにボルツマン分布

$$\mathcal{P}(\boldsymbol{S}|\boldsymbol{J}) = \frac{\exp[-\beta\mathcal{H}(\boldsymbol{S}|\boldsymbol{J})]}{\mathcal{Z}(\boldsymbol{J},\beta)} \tag{5}$$

が変数間の多数の依存関係を含むためスピン S_l の期待値を計算するのに他の変数の情報が必要となり、その変数の情報を得るためにはまた他の変数の情報が必要となる、といった計算の連鎖的爆発が生じてしまうからである。逆にいうと、もし仮にボルツマン分布が

$$\prod_{l=1}^{N} \mathcal{Q}_l(S_l) \tag{6}$$

のように独立な分布の積の形で表現されていれば上で述べたような計算の爆発は生じない。

それならば、式 (6) のように変数に関して因数分解される分布の中で何らかの基準に基づいて真のボルツマン分布 (5) に "似ているもの" を選びそれを復号化に用いる、というのは自然な発想であろう。これは統計力学において平均場近似として広く知られている近似法の発想である。近似の基準として分布間の一種の距離を表す KL ダイバージェンス

$$KL(\mathcal{Q}|\mathcal{P}) = \sum_{\boldsymbol{S}} \mathcal{Q}(\boldsymbol{S}) \ln \frac{\mathcal{Q}(\boldsymbol{S})}{\mathcal{P}(\boldsymbol{S})} \tag{7}$$

を最小にする、ナイーブ平均場近似がよく知られているが、平均場近似はこれに限らず色々な種類がある [14]。

4 TAP 平均場近似による復号化

その中でこれまでの統計力学での経験と照らし合わせて最も Sourlas 符号と相性が良いと思われるのは TAP (Thouless, Anderson and Palmer) 平均場近似と呼ばれるものである [20]。TAP 平均場近似はもともと系に含まれるランダム性により特徴付けられるスピングラスモデルの研究から開発された近似手法であり、系に内在するランダムネスが従う統計性をうまく利用するように構成される。Sourlas 符号の復号化問題には符号語を構成する成分の選び方、元情報、ノイズなどハミルトニアン (2) に (凍結された) ランダムネスが存在し、その統計構造が既知であるためスピングラスモデルと類似した取り扱いが有効であることが予想されるのである。

ただし、これまでのところ TAP 法の適用は専ら SK モデル [20, 15]、Hopfield モデル [11, 17] などの全結合型のモデルに限られている。そのため、ボンド数 (符号語の和) M が

高々$O(N)$となる“希釈スピングラスモデル”であるSourlas符号には既存の手法をそのまま適用することは出来ず、原点に立ち返り改めて考察を行なう必要がある。

詳細は[4]に譲ることにして、Sourlas符号におけるTAP平均場近似ではこの系に内在する凍結されたランダムネスの性質を反映して以下の2つの要請を行う。

- ボルツマン分布はイジング変数S_lに関して因数分解可能である。
- 各イジング変数S_lに対する(有効)ボルツマンウエイトは符号語J_μに関してやはり因数分解可能である。

1番目は平均場近似の要請であるが、2番目の要請は符号語J_μはほぼ要素間で無相関になるように構成されているというSourals符号の特徴を取り入れたものでありTAP法特有の要請である。この2つの要請に基づきBethe近似[2]にならい導出される平均場分布と有効ボルツマンウエイト(あるいは空孔場(cavity field))間の自己無撞着方程式がTAP方程式である。

Sourlas符号に関して得られるTAP方程式は以下のようになる。

$$\hat{m}_{\mu l} = \tanh \beta J_\mu \prod_{k \in \mathcal{L}(\mu)/l} m_{\mu k} \tag{8}$$

$$m_{\mu l} = \tanh \left(\sum_{\nu \in \mathcal{M}(l)/\mu} \tanh^{-1} \hat{m}_{\nu l} + F \right) \tag{9}$$

ここで、$\hat{m}_{\mu l}$は符号語J_μがない系にそれが加えられたとき、スピンS_lに加えられる有効ボルツマンウエイトを

$$\mathcal{W}_{eff}(J_\mu | S_l, \{J_{\nu \neq \mu}\}) \sim \frac{1 + \hat{m}_{\mu l} S_l}{2} \tag{10}$$

により与えるパラメータであり、$\tanh^{-1} \hat{m}_{\mu l}$が空孔場(cavity field)を意味する。また、$m_{\mu l}$は符号語J_μがない系でのスピンS_lに関する周辺分布(1体分布関数)

$$\mathcal{P}(S_l | \{J_{\nu \neq \mu}\}) = \frac{1 + m_{\mu l} S_l}{2} \tag{11}$$

を与え、Fは元情報が偏って表現されている場合に導入される事前知識を表している。$\mathcal{L}(\mu)$、$\mathcal{M}(l)$はそれぞれ符号語のμ成分を構成しているスピンを表す添字の集合、l番目のスピンが関連している符号語の成分を表す添字の集合、$\mathcal{L}(\mu)/l$、$\mathcal{M}(l)/\mu$はそれぞれ$\mathcal{L}(\mu)$からlを、$\mathcal{M}(l)$からμを除いた集合を意味する。

TAP方程式(8)、(9)は適当な初期条件から反復法により解くことが出来る。復号化が可能な場合(強磁性相)は高々$O(10)$程度の繰り返しで実用的には十分な解が得られる。一回の繰り返し計算かかる計算量は高々$O(K^2 M)$程度であるので実用的に全く問題はない。ただし、パラメータ$m_{\mu l}$や$\hat{m}_{\mu l}$がそのまま磁化を表すのではないことに注意しなければならない。反復法により収束解が得られた後、磁化は

$$\langle S_l \rangle_\beta = \tanh \left(\sum_{\mu \in \mathcal{M}(l)} \tanh^{-1} \hat{m}_{\mu l} + F \right) \tag{12}$$

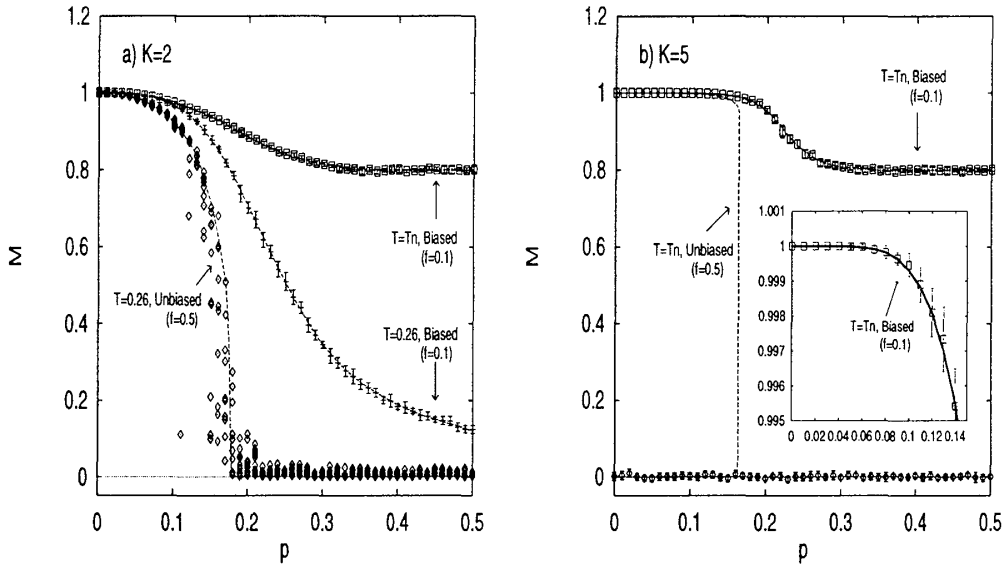

図 2: TAP 方程式を用いた復号化の実験結果。a) $K = 2$、b)$K = 5$ とも $N = 10000$、$M = 20000$ $(R = N/M = 1/2)$ の系に関して TAP 方程式を事前知識 (符号の偏り) を反映させた初期条件からそれぞれ 30 回反復させた解を用いて復号化した。マーカーは 10 回の実験での平均 (誤差棒はそれより小さい)、曲線はレプリカ法 (RS 解) による予想である。

から求められる。2 つの式 (12)、(9) の違いが Onsager 自己反跳場に対応する。全結合型のモデルと異なりこの系では 1 つ 1 つのボンド (符号語) の影響が大きいため反跳場をナイーブな平均場方程式に対する補正という形では表現できないのである。

$N = 10000$、$M = 20000$ $(R = N/M = 1/2)$ の系に関して $K = 2, 5$ の 2 つの場合に TAP 方程式による復号化の性能を調べた。その結果を図 2 に示す。横軸はチャンネルノイズ p、縦軸は元情報と復号化された情報とのオーバーラップ M を表す。ここでは元情報に偏りが存在していない場合 (unbiased) と元情報が $+1$ の出現する確率が 0.1 になるように偏って符号化されている場合 (biased) に関して調べた。また、西森温度での最良性が "近似" を行なった際にも保証されるかいなかを調べるため西森温度と低温 $T = 0.26$ での結果も比較した。さらに理論との比較を行なうためにレプリカ法 (RS 解) による予想も同時にグラフに記した。マーカーは 1 0 回の実験結果の平均値を表し、その誤差棒はマーカーより小さい。曲線はレプリカ法 (RS 解) による理論予想である。

この結果から以下のことが分かる。

$K = 2$ の場合

- 強磁性解 $(M > 0)$ は元情報に偏りがある場合、ない場合とも大きな引き込み領域を持ち、どのような初期条件からも収束する。
- 西森温度の最良性が認められる。

- ノイズの大きさに関して性能は連続的に悪化する。p を大きくした場合に $M=0$ の解に連続的につながるため強磁性解であっても M の値が $K=5$ の場合と比較して小さくなる。すなわち、誤り訂正能力が低い。
- レプリカ法による理論予想と極めて良く一致している。

$K=5$ の場合

- 元情報に偏りがない場合、常磁性解 ($M=0$) の引き込み領域が大きくそのままでは意味のある復号化が難しい。
- この問題を解決するためには元情報に偏りを持たせるバイアス符号化が有効である。
- 西森温度の最良性が認められる。
- 転移は 1 次であり強磁性解と常磁性解はつながっていない。強磁性解は比較的大きな M を保ちつつある臨界的なノイズの値で消失する。そのため、強磁性解が得られる場合は誤り訂正能力は高い。
- レプリカ法による理論予想と極めて良く一致している。

5 おわりに

統計力学における TAP 平均場近似が Sourlas 符号の復号化に有効であることを示した。最近、符号理論における ブレークスルーとされ注目されているものに Turbo 符号と呼ばれるものがある [1]。Turbo 符号も Sourlas 符号と同様スピンモデルに帰着させることが出来る。両者の大きな差異は格子構造の違いにあるが、実のところ Turbo 符号で用いられる復号化アルゴリズムは TAP 平均場近似により導かれたものと同じになる。

Sourlas 符号の性能は Turbo 符号のそれには及ばない。その理由は Turbo 符号が実質的にスピン変数に付加して通信中にノイズによる符号語のビット反転が生じたかしないかまで推定することによりフラストレーションを解消しながら復号化を行なうのに対し、Sourlas 符号ではあくまでもフラストレーションを含むハミルトニアン (2) のまま推定を行なうからである。これは利用するハミルトニアンの違いから生じる能力差であると言える。ただし、ここで述べた TAP 方程式による復号化は Sourlas 符号が潜在的に持っている復号化能力を ($N \to \infty$ で) 完全に引き出していると考えることができる一方、同じ形をしている Turbo 符号の復号化アルゴリズムはその潜在能力を完全には引き出してはいないと思われる。なぜなら、TAP 方程式 (8)、(9) は Sourlas 符号が有する**ランダム格子**の性質を反映して得られるものであるが Turbo 符号の格子には規則性があるため同じアルゴリズムが一般には厳密解を導かないからである。

それならば、Turbo 符号と同様ビット反転が生じたか否かまで推定しフラストレーションを解消しながら復号する符号で、なおかつランダム格子を有するものを構成すれば良さ

そうである。実は Gallager 符号と呼ばれる符号がこれに対応する [3, 9, 10]。不思議なことに Gallager 符号は１９６２年に提案されていながらごく最近 MacKay and Neal に再発見されるまで符号理論の世界から完全に忘れ去られていた [9]。この符号は Sourlas 符号と同様統計力学的に解析することが可能でありその詳細は [12, 6] にある。ちなみに、最近の研究成果によれば適切なランダム格子を有する Gallager 符号は Turbo 符号を抜き世界最高の誤り訂正能力を有することが報告されている [7]。

参考文献

[1] Berrou C, Glavieux A and Thitimajshima P, *in Proc. 1993 IEEE International Conference on Communications, Geneva, Switzerland*, 1064 (1993).

[2] Bethe HA, *Proc. Roy. Soc.*, **A 150**, 552 (1935).

[3] Gallager RG, *IRE Trans. Info. Theory*, **IT-8**, 21 (1962).

[4] Kabashima Y and Saad D, *Europhys. Lett.*, **44**, 668 (1998).

[5] Kabashima Y and Saad D, *Europhys. Lett.*, **45**, 97 (1999).

[6] Kabashima Y, Murayama T and Saad D, *submitted to Physical Review Letters* (1998).

[7] Kanter I and Saad D, *preprint* (1999).

[8] Iba Y, *J. Phys. A: Math. and Gen.*, **33**, 3875 (1999)

[9] MacKay DJC and Neal R, *Electronic Lett.*, **33**, 457 (1997).

[10] MacKay DJC, *IEEE Trans. IT*, **45**, 399 (1999).

[11] Mezard M, Parisi G and Virasoro MA, *Spin Glass Theory and Beyond* (*World Scientific*) (1987).

[12] 村山立人「低密度パリティ検査符号の統計力学的解析」東京工業大学修士論文 (1999); 物性研究 **72** No 6 (1999 年 9 月号) 掲載予定.

[13] Nishimori H, *J. Phys. Soc. Jpn.*, **62**, 2973 (1993).

[14] 小口武彦「磁性体の統計理論」(物理学選書１２、裳華房) (1970).

[15] Plefka T, *J. Phys. A: Math. and Gen.*, **15**, 1971 (1982).

[16] Shannon CE, *Bell Sys. Tech. J.*, **27**, 379 (1948); **27**, 623 (1948).

[17] Shiino M and Fukai T, *Phys. Rev. E*, **48**, 867 (1993).

[18] Sourlas N, *Nature*, **339** 693 (1989).

[19] Sourlas N, *Europhys. Lett.*, **25**, 159 (1994).

[20] Thouless D, Anderson PW and Palmer RG, *Phil. Mag.* **35**, 593 (1977)