コトの物理学——誤り訂正符号を例として——

樺島祥介 〈東京工業大学大学院総合理工学研究科知能システム科学専攻 226-8502 横浜市緑区長津田町4259 e-mail: kaba@dis.titech.ac.jp〉

誤解を恐れずに言えば，ボルツマン分布で表現される平衡統計力学とは大規模な確率分布から平均値を計算するための“ツールボックス”に他ならない．もしそうであるならば，その適用対象を自然現象に限らなければならない理由はどこにもない．本稿では，情報通信の基盤技術である誤り訂正符号へのスピングラス理論の適用を具体例として，「コト＝情報」を対象とした統計力学に関する最近の動向を紹介する．

1. はじめに

ノイズによる誤りの発生は情報通信に必ず伴う厄介な問題である．この問題を解決する誤り訂正符号は，動画や音声でデコレートされた“いわゆるIT技術”と比べると随分地味に見えるが，高度情報化社会に欠かすことのできない「縁の下の力持ち」的な存在であり，今ではハードディスクの読み書きから深宇宙通信に至るまで，高い信頼性を必要とするほとんど全ての通信用途に使われている．同時にこの技術は情報理論を支える柱の一つであるシャノンの第2定理（通信路符号化定理）と密接に関連しており，その理論の発展は通信効率の改良という実利に繋がるだけでなく，学術的観点からも特別な意味を持つ．

1980年代末，この誤り訂正符号の復号問題がスピングラスモデルの基底状態探索と数理的に類似していることが，フランスの物理学者ソウラス (N. Sourlas) により指摘された．[1] 当初，この類似性の指摘はさほど注目されていなかったが，近年スピングラス理論を応用することで，高性能な誤り訂正符号に関する新たな知見が得られることが分かってきた．[2,3] これを契機に「符号とスピングラス」，更には「コトの理論（特に情報理論）とモノの理論（特に統計力学）」との関係について，にわかに多くの関心が寄せられつつある．

このような動向を背景として，本稿では，なぜ本来関わりのない誤り訂正符号がスピングラスと関係してくるのか，また，符号研究におけるスピングラス理論，統計力学の役割ならびにコトを研究することで得られる物理サイドへのフィードバックについて，今後の可能性も含めながらなるべく前提知識を必要としない形で解説したい．

2. 誤り訂正符号と通信路符号化定理

2.1 誤り訂正符号の目的

ノイズの影響を受ける伝送路を介したデジタル情報通信を考える．情報の中身は何でも良いが，数学的には各成分（以下，ビットと呼ぶ）が全て0または1である2値ベクトルとして表現される．以下ではこれをKビット毎に小分けした$\boldsymbol{x}=(x_1, x_2, \cdots, x_K)$ $(x_{i=1,2,\cdots,K}=0, 1)$の送信を考え，ノイズ存在下で$\boldsymbol{x}$が受信者にどの程度正確に伝わるかという問題を考察する．

ノイズの原因としては熱や電気信号を伝える際に発生する電磁波，信号の減衰などが挙げられる．以下では問題を簡単化するために，各ビットが独立に確率$0<p<1/2$で反転する2値対称通信路（binary symmetric channel, 以下BSC）によってこれをモデル化する．

確率的にビット反転が起きるため，$\boldsymbol{x}$をそのまま送ったのでは信頼性の高い通信は実現できない．この問題を情報表現を冗長にすることで解決する技術が，誤り訂正符号である（図1）．

冗長性を導入することにより通信の信頼性が向上することは，例えば$\boldsymbol{x}$の各ビットを3回ずつ繰り返して送信する素朴な“符号”を考えると実感できる．受信者は繰り返しに対応する3ビット毎に0または1の多数決を取り，原情報ビットの推定値とすれば良い．同じ内容を3回繰り返して送信するので冗長である．冗長性の尺度は，通常受信した原情報の長さと実際に送信するビット系列（以下，符号語という）の長さとの比（符号化率）Rで表現される．3回繰り返しの場合には$R=1/3$である．そのまま$\boldsymbol{x}$を送った場合にはビット毎に確率pの割合で誤りが発生する．しかしながら，繰り返しを用いると復号が誤る確率は$3\times p^2(1-p)+p^3\sim O(p^2)$となり，確かに$p$より小さくなっている．また，これを一般化して，繰り返し数を3から$2r+1$ $(r=2, 3, \cdots)$に増やす（つまり，冗長性が増す）と，符号化率は$R=1/(2r+1)$で減少し通信効率は悪化するが，一方でビット当たりの復号誤り確率も$O(p^{r+1})$で減少し信頼性は向

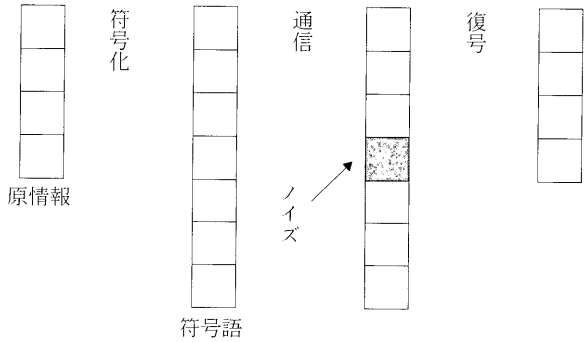

図1 誤り訂正符号を用いた通信．

上する．このことから，通信の効率と信頼性にはトレードオフの関係があることが分かる．

2.2 通信路符号化定理：最良のトレードオフ

ところで，ここで述べた繰返し符号は素朴な方法であるが，必ずしも“最も良い”符号であるとは限らない．そこで，通信の効率と信頼性に関する最良のトレードオフを与える符号はどのようなものか，ということに興味が出てくる．シャノン(C. E. Shannon)はこの問題に対する部分的な回答を，以下に述べる通信路符号化定理という形で与えた．[4] BSCに関して，この定理は次のようになる．

[通信路符号化定理]

任意の$\varepsilon>0$に対し，ビット長Kを十分大きくすると，符号化率Rが

$$R<C\equiv 1+p\log_2 p+(1-p)\log_2(1-p) \tag{1}$$

であれば，復号誤り確率がε以下となる符号が少なくとも一つ存在する．

逆に，$R>C$であれば復号誤り確率はある一定値以下にならないことも示される．つまり，式(1)は誤り確率を任意に小さくしたいという信頼性の基準に対して通信効率との最良のトレードオフを与えている．

この定理の意外性は繰返し符号のトレードオフを式(1)と比較してみれば分かる．前述の議論から$2r+1$回の繰返し送信を行うと符号化率は$R=1/(2r+1)$，復号誤り確率は$O(p^{r+1})$となる．ということは誤り確率を小さな数$\varepsilon>0$以下にするためには$r\sim(\ln\varepsilon)/(\ln p)$程度でなければならず，そのため符号化率は$R\sim(\ln p)/(\ln\varepsilon)$に従って小さくする必要がある．しかしながら，この定理は数理的な仕組み（符号化方法）を工夫するだけで，符号化率一定であっても通信容量C以下であれば任意に誤り確率を小さくできる，ということを主張しているのである．

2.3 ランダム符号と計算コスト

では，そのような符号はどうやって作ればよいのか，というと方針は分かっている．以下のようにすれば良い．まず，Kビットで表される原情報は2^K通りあるが，通信効率を高める目的から通常等確率で発生するように前処理される．この2^K個のベクトル一つ一つにランダムにNビットベクトルを割り当てこれを符号語とする．これら原情報と符号語の間の対応表（コードブックという）を前もって送信者と受信者で共有しておく．ある原情報を伝えたければ一旦それを符号語に変換して送信する．すると，ノイズによりその符号語が劣化したベクトルが受信される．ほとんどの場合，劣化したベクトルはコードブックの中には載っていない．そこで，受信者はその中から受け取ったベクトルと最も近い符号語を探し出し，それに対応する原情報を復号結果とする（図2）．K, Nを十分大きくすると，このように構成した符号はほぼ1に近い確率，正確にはある定数

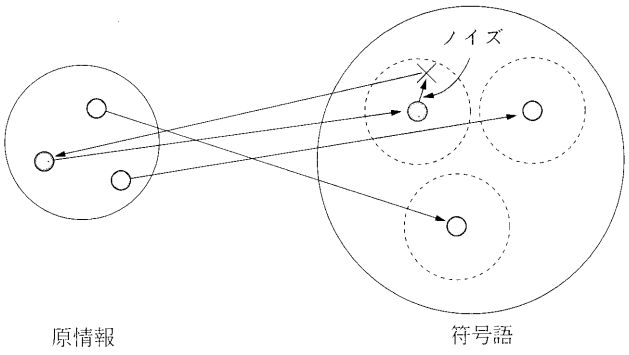

図2 誤り訂正符号の概念図．Kビットの原情報にNビットの符号語を割り当てるので隣合うベクトルの間隔が大きくなる．ランダムに符号を構成した場合，意外なことに符号語は復号誤り確率を最小化する意味でほぼ最適に配置される．符号語を送信すると伝送路ノイズにより，符号語とは異なるベクトル(×)が受信されるが，符号語の間隔が十分大きければ最も近い符号語をコードブックの中から探し，対応関係を逆に使うことで原情報を復元できる．受信語に最も近い符号語を探索することは，ウェイト（1が立っているビットの数）が最も小さなノイズベクトルを求めることに等しく，通常，後者の方が必要計算量は少ない．そのため，線形符号では受信語からのノイズベクトルの探索が復号問題の本質になる．

$a>0$を使って符号長Nに関して$1-\exp[-Na]$と表される程度の確率で，式(1)が示す限界性能を達成する．

なんだ簡単じゃないか，と納得してはいけない．問題はコードブックの大きさにある．コードブックはランダムに構成されるので短く記述し直すことができない．一方，通信路符号化定理は符号長が十分長いことを前提としている．そのため，その保持に必要な記憶容量や復号に要する時間は$O(N\times 2^K)$に比例して増大し，リアルタイムの通信にはとても使えない．

つまり，ランダムに構成した符号は，通信効率と信頼性のトレードオフという観点からは最良であるが，計算量の増大を伴うため実用的ではない．そのため，現在実用化されているほとんどの符号は，復号に関する計算量の削減を最も考慮すべき制約条件として，通信路符号化定理とは直接関係しない代数的考察に基づき構成されている．

3. スピングラスモデルとしての誤り訂正符号：西森線と最良復号

3.1 代数的符号とパリティ検査

では，代数的考察による符号とはどのようなものなのか．(7, 4)ハミング符号と呼ばれる簡単な符号を例に示そう．

(7, 4)ハミング符号では$K=4$ビットの原情報$\boldsymbol{x}=(x_1, x_2, x_3, x_4)$から3つのパリティビット

$$\begin{aligned} x_5&\equiv x_2+x_3+x_4,\\ x_6&\equiv x_1+x_3+x_4,\\ x_7&\equiv x_1+x_2+x_4 \end{aligned} \tag{2}$$

を計算し，$N=7$ビットの符号語$\boldsymbol{y}^0=(x_1, x_2, \cdots, x_7)$を構成する．ただし，特に断らない限り式(2)を含めてビット間の演算は2を法とする代数上，つまり計算結果の値は無視

し，偶奇性のみを答えとする整数演算で行うものとする．これは線形変換に他ならないので生成行列

$$G^T \equiv \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 0&1&1&1 \\ 1&0&1&1 \\ 1&1&0&1 \end{pmatrix} \tag{3}$$

を用いて $\boldsymbol{y}^0 = G^T \boldsymbol{x}$ と表すこともできる．

各ビットで反転が起これば1，そうでなければ0，とするノイズベクトルを $\boldsymbol{n}$ で表すと，送信された $\boldsymbol{y}^0$ に対し受信者はノイズにより劣化した符号語 $\boldsymbol{y} = \boldsymbol{y}^0 + \boldsymbol{n}$ を受け取ることになる．

誤りを訂正するためにはノイズベクトル $\boldsymbol{n}$ が推定できれば良い．そのためにパリティ（偶奇性）検査行列

$$A \equiv \begin{pmatrix} 0&1&1&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{pmatrix} \tag{4}$$

を定義し，生成行列との間に $AG^T = 0$ という関係式が成立することを利用する．具体的には受信された符号語に左から A を掛ける．すると $A\boldsymbol{y}^0 = A(G^T\boldsymbol{x}) = (AG^T)\boldsymbol{x} = 0$ よりノイズベクトルのみが関係するパリティ検査方程式

$$A\boldsymbol{n} = A\boldsymbol{y} \equiv \boldsymbol{z} \tag{5}$$

が得られる．右辺にあるシンドローム $\boldsymbol{z}$ は受信された符号語から分かる量である．また，求めるべきノイズベクトルは，1が立っているビットの数（ウェイトという）が多くなるほど発生確率が小さくなる．そこで式(5)を満たす $\boldsymbol{n}$ の中で最もウェイトの小さいものをノイズの推定値とすれば良さそうである．

(7, 4) ハミング符号ではシンドロームの取り得るパターン数 $2^3 = 8$ に対してウェイト0（誤りなし）のゼロベクトルとウェイト1（1ビット誤り）の7つのベクトル，合計8つのベクトルとの間にちょうど1対1対応が付くようにうまく設計されており，与えられたシンドロームからパリティ検査方程式の解を瞬時に見つけることができる．これを一般化し代数的な考察に基づいて少ない計算量でパリティ検査方程式を解くことが可能なようにパリティ検査行列 A（生成行列 G^T）を設計し，符号を構成するのが代数的符号である．

3.2 パリティ検査とハミルトニアン

さて，以上の仕組みに対してスピングラスとの類似性を最初に指摘したのがソウラスであった．[1] 彼が最初に示した対応は必ずしも上述の“線形符号”の枠組みに則ったものではないが，ここでの文脈では以下のようになる．(7, 4) ハミング符号を一般化し K ビットの原情報を N ビットの符号語に変換する線形符号を考える．$AG^T = 0$ となる $N \times K$ 生成行列 G^T は必ず $(N-K) \times N$ パリティ検査行列 A から構成できるので，これは適当な2値行列 A を定めることに他ならない．法2の代数に従うパリティ検査方程式は，同じくパリティを表現するイジングスピンを用いて書き直すことができる．具体的には式(5)において，各ノイズビット $n_l \in \{0, 1\}$ $(l = 1, 2, \cdots, N)$，シンドローム $z_\mu \in \{0, 1\}$ $(\mu = 1, 2, \cdots, N-K)$ を

$$S_l = (-1)^{n_l}, \quad J_\mu = (-1)^{z_\mu} \tag{6}$$

によって，それぞれイジングスピン S_l および ± 1 のいずれかの値を取る結合 J_μ に対応させる．この表現を用いると式(5)の $(1 \leq)\ \mu\ (\leq N-K)$ 行目に対応するパリティ検査，ウェイトの最小化はそれぞれ積 $J_\mu \prod_{l \in \mathscr{L}(\mu)} S_l$ および和 $\sum_{l=1}^N S_l$ の最大化に他ならない．ただし，$\mathscr{L}(\mu)$ は A の μ 行目にある非ゼロ要素の列添え字の集合である．ここで，シンドローム J_μ は真のノイズにより定まる固定（クェンチ）されたランダム変数であることに注意しよう．つまり，誤り訂正符号の復号問題は，$0 < F \ll \gamma$ として，ハミルトニアン

$$\mathscr{H}(S|J) = -\gamma \sum_{\mu=1}^{N-K} J_\mu \prod_{l \in \mathscr{L}(\mu)} S_l - F \sum_{l=1}^{N} S_l \tag{7}$$

で定まる k 体相互作用スピングラスモデルの基底状態探索と同じである．ここで，$0 < F \ll \gamma$ としたのは，式(5)はノイズが必ず満たさなければならない拘束条件であり，最適化を表す第2項よりも強い制約を意味するからである．

3.3 ベイズ統計と西森線

以上から，誤り訂正符号とスピングラスモデルとの対応が示されたが，ハミルトニアン(7)に不定パラメータ γ, F が含まれているのは気持ちが悪い．ソウラスの指摘から数年後，ベイズ統計の枠組みを用いるとこれらの値が自然に定まり，またそれらを用いると一般的な基準に対する最適な復号法を設計できることがルヤン (P. Rújan),[5] 西森,[6] ソウラス,[7] 伊庭[8]らによって示された．ベイズ統計とはベイズの公式（条件付確率の公式）を最大限に活用し，最適な情報処理を設計する統計学の枠組みである．パリティ検査方程式(5)に対応させてこれを示そう．

イジングスピン表現(6)を用いると，反転確率 p の BSC に対して推定すべきノイズの発生（事前）確率は

$$P(S) = \frac{\exp\left[F \sum_{l=1}^N S_l\right]}{(2\cosh F)^N} \tag{8}$$

によって与えられる．ただし，$F = (1/2)\ln[(1-p)/p]$ である．また，与えられたノイズに対しシンドロームは確定的に定まるため，この関係を表す条件付確率は

$$\begin{aligned} P(J|S) &\equiv \prod_{\mu=1}^{N-K} \delta\left(1; J_\mu \prod_{l \in \mathscr{L}(\mu)} S_l\right) \\ &= \lim_{\gamma \to \infty} \exp\left[-\gamma \sum_{\mu=1}^{N-K} \frac{1 - J_\mu \prod_{l \in \mathscr{L}(\mu)} S_l}{2}\right] \end{aligned} \tag{9}$$

となる．ベイズの公式を用いると，式(8), (9)からシンド

ロームJが与えられた後の事後分布が

$$P(S|J)=\frac{P(J|S)\,P(S)}{\mathrm{Tr}_S P(J|S)\,P(S)} \tag{10}$$

となるが，これを$\beta=1$のボルツマン分布とみなし$-\ln P(S|J)$のS依存性を取り出したものが，ハミルトニアン(7)である．こうして，“正しい”パラメータ$\gamma\to\infty$, $F=(1/2)\ln[(1-p)/p]$が演繹される．

事後分布(10)が与えられると，ベイズ統計の一般論から目的に応じた最適な復号法が導かれる．[8] 例えば，ノイズベクトルの真値と推定値が完全に一致する確率を最大化することを目的とする場合には，$P(S|J)$の最大化，すなわちハミルトニアンの基底状態探索をすることが最適な復号法であることが示される．これは真の事後確率(10)とは異なるゼロ温度のボルツマン分布での平均を意味する．一方，場合によっては真値と推定値がベクトルとして一致するのではなく，ビット毎に一致する確率を最大化したい場合もあろう．その場合には，真の事後確率である(10)を用いてスピンの平均値を計算し，ビット毎にその正負を推定値とすれば良い．

実は，この“真の事後分布”を与える条件がスピングラス理論における西森線[9]に対応する．クェンチされたランダム変数に系が支配されるスピングラス系の統計力学は，形式的にベイズ統計と類似している．ただし，統計力学では系の分布が与えられたハミルトニアンに対する逆温度βの1パラメータ族（すなわち，ボルツマン分布）で表現されるため，必ずしもその分布族でベイズ統計の意味での真の事後分布を再現できるとは限らない．その中で，ゲージ変数をここでの文脈における真のノイズに対応させると，$\pm J$模型やガウス模型はボルツマン分布の形式で逆温度パラメータをある値に設定するだけで真の事後分布を再現できる特別なモデルとなっており，その特殊性のために西森線が定まるのである．ベイズ統計では真の確率分布を用いた場合に様々な意味でパラメータ推定の効率が最大になることが知られている．スピングラス研究では何故次元にかかわらず西森線上で内部エネルギーや比熱の上限が解析的に求まるのか明確な説明を与えることは困難であったが，いくつかの性質についてはベイズ統計の文脈で自然に解釈されることが伊庭により指摘されている．[8]

4. 巨視的な解析と性能評価：レプリカ法とギャラガー形式

前節ではベイズ統計の枠組みを利用すると線形符号の復号問題が必ずスピングラス系の統計力学と類似した形式で表現できることを示した．ただし，現実には事後分布(10)に基づく計算は一般に困難であり，“厳密な計算による復号”を前提とする限りこの表現に殊更利点があるわけではない．

その一方で，復号問題をスピングラスモデルとみなし統計力学の問題として扱うことで，従来研究とは異なる発想が生まれやすくなることもまた事実である．本節と次節ではそのような視点から得られた成果について述べよう．

4.1 平均場モデルとしてのギャラガー符号

スピングラスの解析は一般に難しいが，まずは解析的取り扱いが容易な平均場モデルを構成し，その性質を解明することが統計力学として自然な接近法であろう．熱力学極限に対応させてビット長Nを大きくすると計算コストが増大するので，具体的な復号方法がやはり心配になるが，その問題は次節で論じることにして，ここでは非常に大きなNに対して“ボルツマン分布”(10)から得られる誤り訂正符号の巨視的な性質について考える．

復号問題におけるスピン間の結合はパリティ検査行列Aによって決まる．代数符号では厳密計算による復号が容易になるように規則的にAを構成するが，それではスピン間の結合がスピン添え字で定まる近傍に限定されるので平均場モデルにならない．かといって，各スピンがその他全てと結合する無限レンジモデルでは符号化率がゼロに漸近してしまい実用的な意味が希薄になる．

結論からいうと，各行，各列中にある非ゼロの要素数がそれぞれk, jになるような拘束条件の下でランダムに生成したA（のアンサンブル）が，実用的に意味のある平均場モデルになる．物理の言葉でいうと“1スピン当たりj個のボンドを持つk体相互作用ランダム格子上のスピングラスモデル”である．

驚くべきことに（というより当然とも言えるが），この平均場モデルと全く同じ符号が，今から40年あまり前に情報理論の研究者ギャラガー(R. G. Gallager)によって提案されていた[10]ことが，近年明らかにされている．ただし，この“ギャラガー符号”は当初一部の研究者には注目されたが，当時の技術的制約から実用化は困難と判断され，その後最近になるまでほぼ忘れ去られた存在となっていた．ところが，1990年代後半，その性能が現存する符号の中でほぼ最高であることを実験的に示す研究成果が発表されたため，[11] 現在最も精力的に研究が進められている符号の一つとなっている．

4.2 レプリカ法による性能評価

さて，符号の巨視的な性質として最も重要なものは，その性能を表す復号誤り確率であろう．復号誤り確率にはベクトルとして一致するか否かを問うブロック誤り確率p_{B}と，ビットとして一致するか否かで判断するビット誤り確率p_{b}の2種類が主に用いられる．ただし，ギャラガー符号はアンサンブルとして定義されるので，それらの符号に関する平均$\overline{p_{\mathrm{B}}}$，および$\overline{p_{\mathrm{b}}}$を評価することが自然であろう．

そのうち統計力学の定式化で比較的容易に評価できるのは$\overline{p_b}$の方である．具体的には復号結果の中で推定値$\hat{S}_l$と真値S_l^0とが異なるビットの割合，

$$\mathcal{A}_b(\hat{S}, S^0) \equiv \frac{1}{N}\sum_{l=1}^{N}(1-\delta_{\hat{S}_l, S_l^0}) \tag{11}$$

を真のノイズS^0および行列Aに関し平均化すればよい．ただし，$\delta_{x,y}$は$x=y$のとき1，そうでなければ0となるクロネッカーのデルタである．一方，前節で述べたようにビット誤り率を最小にする復号では，推定値は（クェンチされたランダム変数S^0および行列Aに依存する）事後分布(10)に関するスピンSの平均値で定まる．つまり，$\overline{p_b}$の評価は“熱平均”に対応するSでの平均を“外から”S^0およびAについて“配位平均”する問題となっており，スピングラス理論の標準的解析法であるレプリカ法を応用することで，その実行が可能となる．その際，事後分布(10)は西森温度に対応するため，真の解はレプリカ対称解で記述されることが強く示唆される．そのお陰で評価に必要な計算はそれほど煩雑にはならずに済むのである．

樺島，村山，中村らはギャラガー符号や類似の符号であるマッカイ-ニール符号に関し，以上の接近法によりビット長無限大の極限でのビット誤り率についての詳細な性能評価が可能となることを示している．[2,12] より具体的に言うと，通信路符号化定理が示すような任意に小さな誤り確率を達成できる限界は，熱力学極限において$\overline{p_b}=0$となる復号成功相（強磁性相）と$\overline{p_b}>0$である復号失敗相（スピングラス相，あるいは常磁性相）との間の相転移として理解できること，ならびに自由エネルギーの評価により従来理論では難しかった相境界の具体的決定が可能になることを，彼らは示したのである（図3(a)）．その結果，特に行列Aにおける1の密度が有限になる極限において，ギャラガー符号は通信路符号化定理が示す最良符号の性能限界(1)を達成することが明らかになった．

4.3 ギャラガー形式と垂直相境界

それに比べると，ブロック誤り確率の平均値$\overline{p_B}$の評価は難しい．形式的にはベクトルとしての推定値$\hat{S}$と真値S^0の間でどこかのビットが食い違うことを検出するインジケータ関数，

$$\mathcal{A}_B(\hat{S}, S^0) \equiv 1-\prod_{l=1}^{N}\delta_{\hat{S}_l, S_l^0} \tag{12}$$

を真のノイズS^0および行列Aに関し平均化したものが$\overline{p_B}$である．熱平均と配位平均の構造はビット誤り率の場合と同じであり，原理的にはレプリカ法により評価できるはずである．しかしながら，前節で述べたように，ブロック誤り率を最小にする推定値はハミルトニアンの基底状態に対応するため，ゼロ温度での評価を行わなければならない．これにはレプリカ非対称解の導入が必要となるが，その妥当性の検証が未だ不十分なのである．

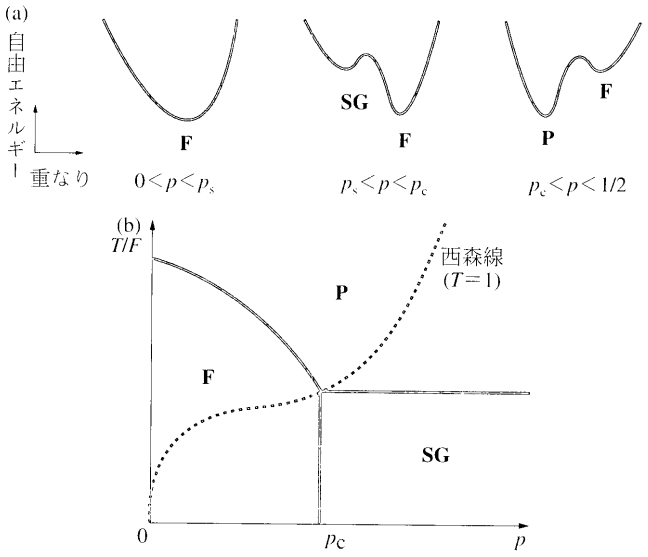

図3 (a) 西森線上でのギャラガー符号($k\geq 3$)の相転移描像．縦軸は自由エネルギー，横軸は真のノイズ(S_l^0)とその推定値($\hat{S}_l$)との重なり$M=(1/N)\sum_{l=1}^{N}S_l^0\hat{S}_l$を表す．臨界値$p_s$以下のノイズでは$M=1$で特徴付けられる復号成功相（強磁性相：**F**）が唯一の熱力学的安定状態となるが，$p=p_s$で$M<1$およびゼロエントロピーで特徴付けられる復号失敗相（スピングラス相：**SG**）が準安定状態として出現する．$p=p_c$($>p_s$)で**SG**は正のエントロピーを持つようになり，常磁性相(**P**)に転移すると同時に自由エネルギーを最小化する熱力学的に優勢な解となる．なお，$k=2$の場合の描像は若干異なる．(b) ギャラガー符号($k\geq 3$)の相図．$F=(1/2)\ln[(1-p)/p]$である．ギャラガー形式により**F**と**SG**との間の相境界p_cは温度に依存しないことが示される．また，$k\to\infty$の極限でp_cはシャノン限界$R=1-p_c\log_2 p_c-(1-p_c)\log_2(1-p_c)$を達成する．

ところが面白いことに，従来の情報理論ではむしろ$\overline{p_B}$の評価の方が進んでおり，この上界を厳密に評価する枠組みが知られている．ギャラガー形式と呼ばれるこの枠組みでは任意の正数$\rho>0$に対して厳密に成り立つ不等式，

$$\overline{p_B}\leq \mathop{\mathrm{Tr}}_{J,S^0}P^{1/(1+\rho)}(J,S^0)\left(\mathop{\mathrm{Tr}}_{S\neq S^0}P^{1/(1+\rho)}(J,S)\right)^{\rho} \tag{13}$$

に基づき上界評価を行う．[13] スピングラス理論に詳しい読者は右辺の形式がレプリカ法と類似していることにお気づきであろう．しかもこの枠組みが発表されたのはスピングラス研究より随分以前の1965年なのである！

ただし，やはり任意の$\rho>0$で右辺を厳密に評価することは困難なため，ギャラガー形式では非負の数$X\geq 0$，および$0<\rho<1$に対するイェンセンの不等式$\overline{X^\rho}\leq\overline{X}^\rho$を用いて一体問題の平均に帰着させる．これは物理における一種の徐冷近似に対応する．また，通常のレプリカ法とは異なり$\rho\to 0$とするのではなく，上界を最小化するようにρを定める．

式(13)に現れる指数$1/(1+\rho)$はボルツマン分布における逆温度に対応するパラメータである．徐冷近似の一種とはいえ，ゼロ温度での解析を最適な有限温度のそれに置き換える発想は物理ではあまり見られないものである．筆者

の知る限りこの指摘はソウラスの論文[1]とほぼ同時期に伊庭が未発表稿の中に記している.*1 ただし，残念ながら当時はスピングラスと符号の関係に現在ほど関心が向けられていなかったため，レプリカ法とギャラガー形式との対応は最近になるまで本格的に検討されることはなかった.

そのような状況の中で，樺島らは式(13)にレプリカ法を適用することでギャラガー符号に関する$\overline{p_B}$の上界評価が一般に改善されることを示した.[14] また，彼らは同じ符号に対してギャラガー形式を利用することにより，復号成功相と（レプリカ対称性が破れたスピングラス相である）失敗相との相境界が温度に依存せず，相図上で西森線から垂直に下りることの証明に成功している（図3(b)).

レプリカ法には分配関数の自然数冪に関する配位平均を実数冪へと解析接続する方法についての未解決問題が存在する.[15] この解析接続の不定性は復号誤り確率の符号長依存性を評価する際に露になることが最近指摘された.[16] ギャラガー形式は適当な状況下でこの問題に対する厳密な解答を与えることが知られており，その解答との比較が今後レプリカ法の基礎付けに有益な示唆を与えることが期待される.

5. 微視的な解析と復号アルゴリズム：TAPの接近法と信念伝搬法

5.1 求解アルゴリズムとしての微視的解析

さて，レプリカ法やギャラガー形式で可能となるのは，事後分布(10)に基づく復号が“行われた”という仮定の下での性能評価である．実験室に放置しておけば自然がボルツマン分布による平均を実行してくれる物理系とは異なり，情報科学の問題では現実的な時間で終了する計算手続きなしに具体的な解を求めることはできない．残念ながら，厳密計算を行う限り事後分布(10)に基づく誤り訂正符号の復号は一般に計算論的に難しい問題であり，長い符号長Nに対して事実上不可能となる．それゆえ，従来の符号研究は主に復号が容易な規則的パリティ検査行列に基づく短い符号の設計に向かっていたのであった.

それでは，これをスピングラスの問題として捉えると，どのような接近法が自然であろうか．具体的に必要なのは，真のノイズ毎に異なる結合J_μによって定まる事後（ボルツマン）分布(10)に対して，スピンS_l毎に微視的な平均値を求めることである．もちろん，見方を変えても“厳密に”平均値を求めるのが難しいことには変わりない．けれども，そういった場合にはとりあえず“近似的”に求めるということが物理では自然な処方箋であろう．更に，この目的に適う計算手法として物理では種々の平均場近似が知られている.

5.2 TAPの接近法と信念伝搬法

ここまで来ればあと一息である．ギャラガー符号はスピングラスの平均場モデルである．強磁性体の平均場モデルである伏見-テンパリーモデルでは，熱力学極限においてナイーブな平均場近似が厳密解を導く．ただし，残念ながらスピングラス系においてはナイーブ平均場近似は必ずしも良い近似ではない．なぜなら，スピングラス系では結合のランダム性に起因して，強磁性体では無視できる自己相互作用の影響（オンサーガー反跳項）が他スピンからの影響と同程度となり，平均場方程式に過剰に寄与してしまうからである.

それに対し，サウレスらはスピングラス研究における有名な平均場モデルであるシェリントン-カークパトリック(SK)モデルに対して，このオンサーガー反跳項の影響はベーテ近似によって除去可能であり，その結果得られる巨視的性質はレプリカ法による予言と高い精度で一致することを発見した.[17] 一般にサウレス-アンダーソン-パルマー(TAP)の方法と称されるこの接近法は，その後SKモデルの疎結合版である王-シェリントンモデルに対しても有効であることが示されている.[18,19] つまり，これまでのスピングラス研究で得られている成果からギャラガー符号ではベーテ近似が有効な近似アルゴリズムの役割を果たすことが予想される.

（再び）驚くべきことに（というより当然とも言えるが），このベーテ近似による復号と非常に近いアルゴリズムが，ギャラガー自身によりギャラガー符号の誕生時点で既に提案されていたのであった.[10] ただし，発見法的に与えられたギャラガーの復号アルゴリズムは，調整すべきパラメータ設定が必ずしも真の事後分布(10)に対する近似計算に対応しておらず，そのため得られる性能はそれほど高くはなかった．また，近似解を求めるために必要な非線形方程式の反復が当時の技術的制約から好まれなかったため，最近までほとんど忘れられた存在となっていたのである.

5.3 様々な分野とのつながり

ところが，意外なところから転機が訪れる．1980年代後半から人工知能の研究においてグラフ状に表現された確率モデルに基づく統計的推論の研究が盛んになり，信念伝播(belief propagation)法というアルゴリズムが“発明された”.[20] 実はこの信念伝播法とは一般のグラフに対するベーテ近似（グラフにループがない場合には転送行列法）に他ならないことが後に示されている.[21] そして，マッカイ(D. J. C. MacKay)らがこのアルゴリズムを真の事後分布(10)に対する近似計算に適用したことで，ギャラガー符号の驚異的な性能の高さが実験的に発見されたのであった.[11]

*1 伊庭幸人：「情報理論における Gallager 形式とレプリカ法」(1989).

以上の経緯からすると，復号アルゴリズムに関するスピングラス理論の役割は，既に存在する技術の統計力学的“後講釈”に過ぎないような印象を与えるかもしれない．ただし，要素間の局所的な関係に基づいて導出されるギャラガーの復号法および信念伝播法とは異なり，ベーテ近似はその背後に自由エネルギーという大域的に定まる変分関数を伴っている．アルゴリズムの収束点を多変数関数の極値条件に対応させるという発想は，従来の情報科学，計算機科学ではあまり考えられてこなかったものであり，スピングラス理論による自由エネルギーという概念の導入は，信念伝播法の動作を解明する上で重要な手がかりを与えたのであった．[22] また，最近ではクラスター変分法など自由エネルギーに基づいた近似法の拡張を信念伝播法に適用し，より実際的な誤り訂正符号の復号や確率推論に応用しようとする研究が活発化しており，[23] それに触発されて，各種平均場近似の数理的構造を計算機科学の視点から解明しようとする研究も始まりつつある．[24]

6. おわりに

線形符号，特にその“平均場モデル”にあたるギャラガー符号を具体例に，誤り訂正符号とスピングラスとの類似性について述べた．情報と物理という異なる背景から誕生した二つの話題が類似した数理モデルで定式化され，またこれまでほとんど本格的な研究交流がなかったにもかかわらず，情報理論・計算機科学と統計力学で類似した解析手法が独立に開発されていたことは興味深い．

いや，むしろ類似した問題でありながら，情報科学と自然科学では現在なぜこれほど研究の進め方や発展の方向性が異なっているのか，という“相違”の方に目を向けるべきかもしれない．ゲノムに代表される大量のデータ，インフラの整備に伴う通信量の飛躍的増大など，情報科学・工学で扱うべき問題は確実に大規模化しており，少なくとも大自由度性という観点において，統計力学の研究対象に近づきつつある．このような状況を反映して，科研費特定領域研究「確率的情報処理への統計力学的アプローチ」（領域代表：東北大学田中和之氏）が平成14年度より発足した．[*2] ここで紹介した誤り訂正符号以外の話題に関しても，類似した（あるいは同一の）問題を介した情報科学と統計力学の本格的交流がまさに始まろうとしている．[25–27] 情報と物理という異文化交流から何が生まれるのか，今後の展開に注目していただけると幸いである．

物理と情報の交流と言えば量子情報を連想する読者も多いのではないであろうか．かなり広い研究領域を指す用語なので一括りにすることははばかれるが，筆者なりの印象では，従来の量子情報に関する理論研究は観測問題の影響を受けて，一体問題で記述される状況（あるいは一体問題に還元できる状況）からの情報抽出に関する効率限界を精密に論じたものが多いように思う．ただし，例えば量子メモリの実現に必要な量子誤り訂正符号を物理的な実現可能性を考慮して構成しようとすると，どうしても多体問題としての視点が重要になってくる．[28] そのため今後は統計力学的な方法の重要性が増し，ひょっとすると，本稿で示した符号とスピングラスモデルとの関係のような類似性が量子系でも活かされてくるのではないかと期待している．

最後に，本稿の内容は村山立人氏（理研），中村一尊，佐塚直也両氏（ともに東工大），ディビッド・サード，レナート・ヴィセンテ，ヨフト・ファン・ムーリックの三氏（ともにアストン大）との共同研究，ならびに伊庭幸人（統数研），西森秀稔（東工大），田中和之（東北大），田中利幸（都立大）の各氏との議論に負うところが大きい．この場を借りて各氏に感謝の意を表したい．

参考文献

1) N. Sourlas: Nature **339** (1989) 693.
2) Y. Kabashima, T. Murayama and D. Saad: Phys. Rev. Lett. **84** (2000) 1355.
3) A. Montanari and N. Sourlas: Eur. Phys. J. B **16** (2000) 107.
4) C. E. Shannon: Bell Syst. Tech. J. **27** (1948) 379 and 623.
5) P. Rújan: Phys. Rev. Lett. **70** (1993) 2968.
6) H. Nishimori: J. Phys. Soc. Jpn. **62** (1993) 2973.
7) N. Sourlas: Europhys. Lett. **25** (1994) 159.
8) Y. Iba: J. Phys. A **32** (1999) 3875.
9) H. Nishimori: Prog. Theor. Phys. **66** (1981) 1169.
10) R. G. Gallager: IRE Trans. Inf. Theory **IT-8** (1962) 21.
11) D. J. C. MacKay: IEEE Trans. Inf. Theory **45** (1999) 399.
12) K. Nakamura, Y. Kabashima and D. Saad: Europhys. Lett. **56** (2001) 610.
13) R. G. Gallager: IEEE Trans. Inf. Theory **IT-16** (1965) 720.
14) Y. Kabashima, N. Sazuka, K. Nakamura and D. Saad: Phys. Rev. E **64** (2001) 046113.
15) J. L. van Hemmen and R. G. Palmer: J. Phys. A **12** (1979) 563.
16) Y. Kabashima, K. Nakamura and J. van Mourik: Phys. Rev. E **66** (2002) 036125.
17) D. J. Thouless, P. W. Anderson and R. G. Palmer: Phil. Mag. **35** (1977) 593.
18) S. Inawashiro and S. Katsura: Physica **100A** (1980) 24.
19) K. Y. M. Wong and D. Sherrington: J. Phys. A **20** (1987) L793.
20) J. Pearl: *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference* (Morgan Kaufmann, 1988).
21) Y. Kabashima and D. Saad: Europhys. Lett. **44** (1998) 668.
22) R. Vicente, D. Saad and Y. Kabashima: J. Phys. A **33** (2000) 6527.
23) J. S. Yedidia, W. T. Freeman and Y. Weiss: *Advances in Neural Information Processing Systems, Vol. 13* (MIT Press, 2001) p. 689.
24) A. L. Yuille: Neural. Compt. **14** (2002) 1691.
25) 樺島祥介：「学習と情報の平均場理論，物理の世界」（岩波書店，2002）．
26) 西森秀稔：「スピングラス理論と情報統計力学，新物理学選書」（岩波書店，1999）［英訳，H. Nishimori: *Statistical Mechanics of Spin Glasses and Information Processing* (Oxford Univ. Press, 2001)］．
27) 堀口　剛，佐野雅己：「情報数理物理，大学院情報理工学2」（講談社サイエンティフィク，2001）．
28) E. Dennis, A. Kitaev, A. Landahl and J. Preskill: quant-ph/0110143 (2001).

[*2] 領域ホームページのURLは http://www.smapip.eei.metro-u.ac.jp

著者紹介

樺島祥介氏：　専門は統計力学，情報理論，学習理論など．モノ（自然現象），コト（情報）を問わず多数の要素が関連して自明でない振舞を示すことに興味がある．

（2002年10月3日原稿受付）

Statistical Mechanics of Information Processing

—An application to error-correcting codes—

Yoshiyuki Kabashima

abstract: Statistical mechanics for equilibrium systems which are described by the Boltzmann distribution can be regarded as a tool box for calculating various averages from large scale probabilistic models. This implies that there is no reason for restricting its employment to natural phenomenon. In this article, we explore a possible extension of statistical mechanics to topics in information sciences illustrating a recent application of spin glass theory to error-correcting codes.

解説

蛋白質機能発現のダイナミクス的側面

木寺詔紀　〈横浜市立大学大学院総合理学研究科　230-0045 横浜市鶴見区末広町 1-7-29　e-mail: kidera@tsurumi.yokohama-cu.ac.jp〉

池口満徳　〈横浜市立大学大学院総合理学研究科　230-0045 横浜市鶴見区末広町 1-7-29　e-mail: ike@tsurumi.yokohama-cu.ac.jp〉

蛋白質は，生物の物質/情報の輸送/変換を行うネットワーク上にある素子である．その素子は，外部からの刺激に応答して引き起こされる立体構造変化によって，on/offのスイッチの切り替えを行うことで動作する．そのような生物機能を実現するメカニズムが，分子としての蛋白質という巨大分子の上に実現されている．それは，物理の言葉でどのように記述され得るのだろうか．ここでは，そのような問題意識に基づいて，蛋白質分子のダイナミクスの描像について，理論的研究の流れに沿って解説しよう．

1. はじめに

蛋白質の機能を形式的に書き下してみると，

外界からの刺激に対する応答として始まる

一連の立体構造の変化とそれに伴う化学反応

ということになるだろう．ここで言う「刺激」とは，多くの場合，ある特定の分子との分子間相互作用-複合体形成であり，その刺激によって蛋白質がその特異的立体構造を変化させ，次の段階の分子間相互作用を引き起こす．このような相互作用の連鎖が生体内の情報のネットワークを形成している．さらに，蛋白質が酵素活性を持てば，基質分子に対して，構造変化に伴った化学反応を起こすこととなる．Emil Fischerが100年余り前に提唱した「鍵と鍵穴†(lock and key)」に始まる剛体的な蛋白質のイメージは，その後多くの実験データの蓄積によって修正され，上に述べたように本質的にダイナミックなものとして認識されるようになってきた．しかし，このダイナミクスは，反応中間体†の結晶構造や分光学的実験によれば，フレキシブルという言葉から想像されるような単純なものとはかなり異なり，相当な存在時間にわたって明確な原子配置を持つ，いくつかの中間体の間を離散的に変化するものと考えられている．[1] これが上に書いた「一連の」という言葉の意味である．実体はともあれ，百聞は一見に如かずといった意味で，このような異なった複数の結晶構造の間をなめらかにつないで作ったムービーを，“Database of Macromolecular Movements” (http://molmovdb.mbb.yale.edu/molmovdb/)[2] に見ることができる．

このように生物機能として実現される蛋白質のダイナミクスは，どのようにして，物質としての蛋白質の上に生まれるのだろうか．この問いに答えるための理論的研究は，その研究の歴史に沿って，孤立した蛋白質の平衡状態における構造ゆらぎの議論から，分子間相互作用への応答として起こる構造変化を扱う非平衡論への移行として括ることができるだろう．平衡論では，主として自然界にある蛋白質の形の多様性が，どのようにダイナミクスの多様性を規定しているかを明らかにする研究であったと言えるだろう．その後，分子間相互作用に伴う構造変化の例が多く結晶構造解析によって明らかにされるに及んで，ダイナミクス研究は生物機能を直接的に問う非平衡論への展開を始めた．

† 印のある言葉は末尾に用語解説あり．