

修士論文 (1998年度)

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 大学院総合理工学研究科
知能システム科学専攻 樺島研究室

村山 立人

Statistical Mechanics of Low-Density Parity-Check Codes

Department of Computational Intelligence and Systems Science
Interdisciplinary Graduate School of Science and Engineering
Tokyo Institute of Technology

Tatsuto Murayama

Abstract

The performance of low-density parity-check codes is investigated via methods of statistical mechanics. Low-density parity-check codes is first invented by Gallager, which was abandoned shortly after its introduction due to the limited computational abilities and recently rediscovered by MacKay and Neal as MN codes. In these codes, a message is encoded to the codeword which comprises products of the message bits selected by two randomly-constructed sparse matrices. The typical case analysis of statistical mechanics indicates a practical property of the particular family of the codes, which could not be found within the framework of worst case analysis. Further, decoding aspects are considered by investigating solutions obtained by a mean field approach, which is identical to the commonly used belief propagation.

1 序論

情報の本質を定量的に捉え、それを扱うための理論的な枠組を数学的に体系化して、現在進行しているデジタル技術革命の数理的基礎を与えた Shannon の論文「通信の数学的理論」が発表されてから、半世紀が経とうとしている [1].

Shannon の論文以前では、遠隔地の受信者に誤りが発生する確率のある通信路を通してメッセージを確実に伝えようとすると、どうしても長い時間がかかるはずだと考えられていた。メッセージを受信者に正確に伝えるためには、その代償として通信速度を限りなく小さく押えなければならないと思うのが常識だからである。しかし、通信路符号化に関する Shannon の定理は、通信路が持つ固有の通信路容量より少しでも小さい通信速度であれば、その通信速度でほとんど誤りなくメッセージを受信者に伝えることができる」と述べている。この驚愕の事実の発見と共に、情報を定量的に扱える学問として情報理論が誕生したのである。

Shannon によって発見された通信路容量は Shannon 限界と呼ばれ、メッセージを加工して受信者に誤りなく伝えるソフトウェア技術としての誤り訂正符号が達成可能な通信速度の上限を与えている。ところが、Shannon の通信路符号化定理の証明は非構成的で、圧倒的多数の符号が Shannon 限界を達成していることを示唆しているに過ぎない。実際、Shannon 限界を達成することが知られているランダム符号では、メッセージの長さ N に対して符号化と復号化の段階で要求される計算量が $O(e^{aN})$ (a は定数) にもなってしまい、およそ実用的とはいえない。符号理論の究極の目標は、Shannon 限界を達成する実用的な誤り訂正符号を構成することにあるはずだが、多くの試みが失敗したせいで、符号理論の中心的テーマは必ずしも Shannon 限界の達成を目標としない代数符号の研究に移ってしまった。ところが、1962 年に Gallager によって提案され [2], 最近になって MacKay と Neal に再発見された [3] 低密度パリティ検査符号 (LDPC 符号) は Shannon 限界を達成可能で、かつ実用的な計算量で符号化と復号化ができること

が判明した [4]. この符号では非ゼロ要素の合計が各行 K 個, 各列 C 個になるように作成したランダム行列 C_s と, 非ゼロ要素の合計が各行各列共に L 個になるように作成したランダム正方行列 C_n によって選択された 2 値メッセージ ξ のビットで符号語が構成される. 通信路で混入する 2 値ノイズを ζ と書いて, メッセージとノイズを対等に取り入れたパリティ検査方程式

$$C_s \xi + C_n \zeta = C_s S + C_n \tau \quad (1.1)$$

を 2 値ベクトル S, τ について解くことが復号化の操作に対応している.

本論文では, 性能評価に統計力学を用いることで従来の最悪時解析では不可能だった典型時の厳密な解析をした [5]. その結果, ある符号は実用上に有利な性質を持っていることを示すことができた. さらに, 実用的な計算量の復号化技術であるビリーフ・プロパゲーションを統計力学の立場で解析する.

本論文は, 以下のように構成される. まず, 第 1 章で情報理論における本論文の位置付けを確認した. 第 2 章では誤り訂正符号の簡単な解説のあと, 本論文で注目している LDPC 符号について, その構成方法を詳しく説明する. さらに, LDPC 符号の復号化の手続きがパリティ検査方程式 (1.1) を解くのと同値であり, それが統計力学の立場ではスピングラスの基底探索に対応することを指摘する. LDPC 符号が誤り訂正符号として, どのくらい効率的で信頼性のある通信手段を提供できるかは, 結局のところ, この復号化がどれだけうまくいくにかかっている. 続く第 3 章では, 以下の章を理解するために最低限必要な統計力学の知識を Bayes 統計の立場で解説する. その後, 第 4 章ではまずパリティ検査方程式 (1.1) 自体が正確に解けるための条件を与え, 第 5 章で復号化の実用的な手段としてビリーフ・プロパゲーションを用いたときに (1.1) が正確に解けるための条件を導出する. 第 6 章は結語とし, まとめと本論では触れられなかった話題を指摘する.

2 低密度パリティ検査符号

2.1 誤り訂正符号

メッセージを送りたい送信者と, それを受け取りたい受信者がいるものとする. そして, 両者が誤りが発生する確率のある通信路を通してのみメッセージを送受信できる状況を考える. 簡単のため, メッセージは長さ N の 2 値ベクトル $\xi = (\xi_1, \xi_2, \dots, \xi_N)$ で表現されているとする. これを 1 ビット当たり確率 p で値が独立に反転してしまう 2 値対称通信路を通して送信する (図 1.1). そのため, このままでは受信者は 1 ビット当たり確率 $1-p$ でしか正確に情報を得ることができない. このとき, 送信者はメッセージ ξ をより長い符号語 $J^0 = (J_1^0, J_2^0, \dots, J_M^0)$ に変換して

(符号化) から送信し, 受信者は通信路から受け取った符号語からもとのメッセージ ξ を復元する (復号化) ことが行われる. このようなプロトコル (通信規約) でメッセージが誤って伝わるのを減少させることが可能である. いま, 送信者は 2 値対称通信路を通して 1 ビットのメッセージ 0 を送りたいものとしよう. 1 回 0 を送信するだけでは, 受信者に正しく 0 が伝わる確率は 2 値対称通信路の定義から $1-p$ である. そこで, 送信の信頼性を高めるために, 3 回続けて 0 をメッセージとして送ったときに, 受信者が受け取ったメッセージの中に 0 が 2 個以上あれば 0 が送られたと推定するプロトコルを考える. この多数決を模したプロトコルで送信されたメッセージ 0 が遠隔地の受信者に正しく伝わる確率は $1 - (p^3 + 3p^2(1-p))$ である. このとき, 受信者が正しいメッセージを受け取る確率が $1-O(p)$ から $1-O(p^2)$ に上がっていることが分かる. しかし, 全く同じ情報をやりとりしているのに, この場合は 3 倍の時間がかかってしまっている. このように, メッセージに冗長性を持たせて通信コストを上げるかわりに, メッセージが誤って伝わってしまう危険を下げるソフトウェア技術のことを誤り訂正符号化法という (図 1.2). では, どのくらいメッセージに冗長性を持たせて符号化すれば, 誤りなく復号化が可能になるのだろうか? この問題に対して, Shannon は今から半世紀も前に解答を与えた [1].

定理 2.1 (通信路符号化定理) 符号化の冗長度を符号化率 $R = N/M$ で定義する. このとき, 通信路の性質で決まる有限の臨界値 $R_c (> 0)$ が存在し, $R < R_c$ なら 1 ビット当たりの誤り率を 0 にするような符号化法が $N, M \rightarrow \infty$ の極限で存在する. 2 値対称通信路では

$$R_c = 1 - H_2(p) \quad (2.1)$$

である. ただし, 2 値エントロピーを

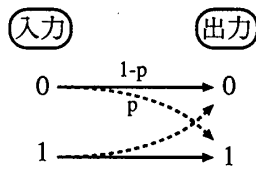
$$H_2(p) = -p \log_2 p - (1-p) \log_2 (1-p) \quad (2.2)$$

で定義する.

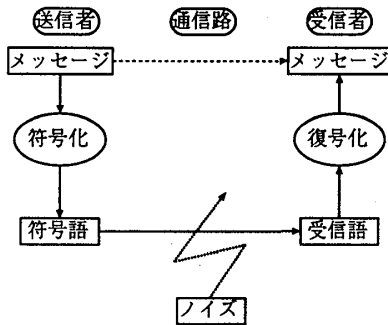
通信路を既与としたとき, 通信路符号化定理 2.1 で登場する冗長度の臨界値 R_c のことを, その通信路の Shannon 限界と呼ぶ. つまり, Shannon 限界を越えないようにうまく符号語を構成しさえすれば, 誤りなくメッセージの送受信を行えることを定理 2.1 は主張しているのである.

2.2 低密度パリティ検査符号

いま, N 次元の 2 値ベクトルとして表現できるメッセージ ξ が M 次元の 2 値ベクトル J^0 に多少長めに符号化されて, 1 ビット当たりの誤り率が p の 2 値対称通信路を用いて送信されるものとする. 受信された符号語 J は誤りを含んでいる可能性があるため, 元のメッセージを復元するように適切に復号化されなければならない.



1.1: 2値対称通信路



1.2: 誤り訂正符号

図 1: 誤り訂正符号

LDPC符号では、ランダムに作成した2つのスパース行列 C_s と C_n に基づいて符号語が構成される。行列 C_s は M 行 N 列の行列で、非ゼロ要素の合計が各行 K 個、各列 C 個になるように作成する。同様にして、行列 C_n は M 行 M 列の正方行列で、非ゼロ要素の合計が各行各列共に L 個になるように作成する。こうして、ランダム行列 C_s 、 C_n を特徴づけるパラメータ K, C, L を指定することで特定の符号を選択したことになる。通信を行う際、メッセージの送信者と受信者には、これらの行列が当然公開されている。さて、符号化では、正方行列 C_n の2を法とする逆行列を求め、行列 $C_n^{-1}C_s\xi$ (modulo 2) を計算する。このとき、ベクトル $J^0 = C_n^{-1}C_s\xi$ (modulo 2) がLDPC符号の符号語を構成することになる。次に、復号化では、まず行列 C_n と受信した2値ノイズ ζ を含んでいる受信語 $J^1 = J^0 + \zeta$ (modulo 2) の積を計算して $J = C_s\xi + C_n\zeta$ を求める(図2)。そうしておいて、パリティ検査方程式

$$C_s\xi + C_n\zeta = C_sS + C_n\tau \quad (2.3)$$

を2値ベクトル S, τ について、何らかの手段で解くことになる。このときに用いられる近似的探索の技術がMacKayによって提案されたビリーフプロパゲーション(BP)であり[4]、後に樺島とSaadによって統計力学的な見地から再発見され物理的な基礎を与えられたTAP復号化法である[6]。

LDPC符号のひとつであるMN符号では、メッセージ ξ に含まれているアルファベット 0, 1 の出現確率を任意

に設定することができて、必ずしも 0, 1 が半々の出現確率を持つとは限らない場合をも想定している[3]。これに対し、低密度パリティ検査符号を初めて提案したGallagerは、そこまで言及してはいなかった[2]。結局、MN符号とはGallager符号の自然な拡張になっているが、本質的な意味においては両者は同一の誤り訂正符号だということができる。以下、本論文では、低密度パリティ検査符号(LDPC符号)に表記を統一する。

2.3 低密度パリティ検査符号と希釈スピングラス模型

LDPC符号の復号化では、パリティ検査方程式(2.3)を解くことになる。LDPC符号が誤り訂正符号として、どのくらい効率的で信頼性のある通信手段を提供できるかは、結局のところ、この復号化がどれだけうまくいくにかかっている。当然のことながら、メッセージの長さ N と符号長 M が有限の値をとる場合に、パリティ検査方程式(2.3)の理論的解析を厳密に行うことは非常に難しい。そこで、本論文では $K, C, L \ll N$ のもとで符号化率 $R = N/M$ を一定に保ちながら $N, M \rightarrow \infty$ とした熱力学的極限に対して解析的に系の性質を調べることにする。さらに、この極限における非線形多体系の巨視的な性質の導出を得意とする統計力学の計算技術を利用するために、パリティ検査方程式(2.3)の求解を、スピングラスと呼ばれるランダム系の代表的な数学的模型における基底状態探索に対応づける。

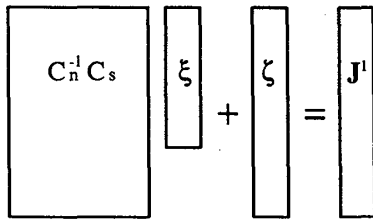
1989年にSourlasは実用的な誤り訂正符号として有名なパリティ検査符号とランダム系の統計力学で研究されていたスピングラス模型の数学的類似性を指摘した[7]。本論文では、Sourlasにならい、メッセージ ξ 、ノイズ ζ 、受信語と C_n の積 J 、スピン変数 S 、 τ を構成している $\{0, 1\}$ 上で表現されたビット系列を $\{1, -1\}$ 上の表現に変換し、さらに $\{0, 1\}$ 上で定義された足し算を $\{1, -1\}$ 上で定義されたかけ算に翻訳する。すると、パリティ検査方程式(2.3)はボンド J^0 に関する M 元連立方程式

$$\prod_{i \in I(\mu)} \xi_i \prod_{j \in J(\mu)} \zeta_j = \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \quad (2.4)$$

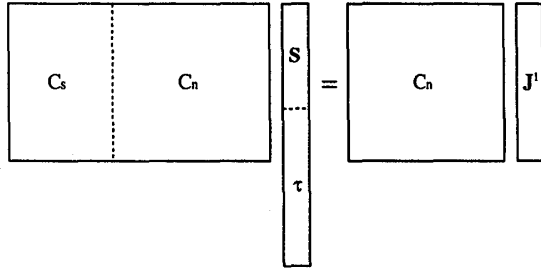
$$\Leftrightarrow \prod_{i \in I(\mu)} (\xi_i S_i) \prod_{j \in J(\mu)} (\zeta_j \tau_j) = 1 \quad (2.5)$$

と同値になる。ここで $I(\mu)$ はボンド J の第 μ 成分 J_μ を構成するメッセージビットの指標の集合、 $J(\mu)$ はノイズビットの指標の集合である。すると方程式(2.5)は、スピン変数 S に関しては K 体の相互作用が M 個だけ存在し、スピン変数 τ に関しては L 体の相互作用が M 個だけ存在する希釈されたスピングラスの基底状態探索を表現しているという物理的解釈が成立する。

スピングラスの理論は、ランダム系の統計力学において近年活発に研究が進められていた分野である。全結合系と



2.1: 符号化, 送信, 受信



2.2: 復号化

図 2: LDPC 符号のプロトコル

呼ばれる各スピン変数がそれ以外の全てのスピン変数と相互作用するモデルでは、系の巨視的な振舞を支配する自由エネルギーと呼ばれる評価関数を平均場理論に基づいては自動的に計算する技術が確立されている。ところが、本論文で扱うことになる希釈スピングラスの理論はまだ未開拓で、技術的にも非常に困難な問題を多く含んでいる興味深い研究対象である。もちろん、パリティ検査方程式(2.3)の振舞を調べるのが最終目的には違いないが、希釈スピングラスモデルの物理的性質を解明することや、そのために必要となる解析的な手続きを与える処方箋を確立することも、非常に興味のある話題である。

3 統計力学

3.1 Bayes 統計

相関を持った事象 x と y が同時に観測される結合確率 $P(x, y)$ は、事象 x が観測された条件で事象 y が観測される条件付き確率 $P(y|x)$ と事象 x が観測される確率 $P(x)$ の積で与えられて

$$P(x, y) = P(x)P(y|x) \quad (3.1)$$

と表せる。この結合確率は x と y に対して対称であるので、Bayes 公式

$$P(x|y) = \frac{P(x)P(y|x)}{\sum_x P(x)P(y|x)} \quad (3.2)$$

を導くことができる。Bayes 公式(3.2)においては $P(x)$ を事前確率、 $P(y|x)$ を事後確率と呼ぶ。Bayes 公式(3.2)の持つ多くの有用な性質を積極的に活用する統計的方法論が Bayes 統計であり、通常の統計学とは違った新しさがある。

3.2 統計力学

一般に、多体系はさまざまな状態を取り得る。その系で実現可能な状態数は、系の要素数、すなわち自由度 N が増加するにつれて指数関数的に爆発してしまうので、いったいそのうちのどの状態が有力で、典型的な系の性質に貢献しているのかが重要な関心事になる。この問題に、自由度 N が極めて大きくなった極限を想定することで厳密な解答を与えるのが統計力学である。

歴史的に、統計力学の方法はほとんど自然界の物質に適用され、統計物理学と呼ばれる物性科学の 1 大分野を形成するに至った。ところが、純粋に数学的な立場で眺めると、統計力学は大自由度極限を扱った Bayes 統計といえる。物質を構成する分子の微視的な状態を事前に知ることは不可能であるため、伝統的な統計力学では系の状態に関する事前知識は存在しないことを前提にした議論が一般的だった。これは Bayes 統計の枠組では、理由不十分の原則が適用されていることになる。ただし、統計力学を人工的な考察対象が多い情報理論の研究に応用しようと試みるときは、事前知識が存在するほうがむしろ自然である。よって、本節では Bayes 統計を意識した統計力学の解説を簡単に行う。

統計力学では、多体系を構成する要素をサイトと呼び、各サイトを区別するため指標 i ($i = 1, \dots, N$) を付ける。そして、サイト i の状態をスピン変数 S_i で表現し、全サイトの動的変数の値を状態ベクトル S で指定することで、系の状態を記述する。また、 p 個のサイト $i_1, \dots, i_p$ の間で存在する p 体相互作用をボンド $J_{(i_1, \dots, i_p)}$ で表現し、全相互作用の形式をベクトル J で指定することで、特定の系を選択したことになる。このとき、エネルギー曲面の構造を反映したハミルトニアンと呼ばれる評価関数 $H(J|S)$ を構成できる¹。ハミルトニアンの値は、系が状態 S にあるときに持つ全エネルギーであると定義されている。

ある特定の系、つまりボンド J を選択したとき、状態 S が実現される確率 $P(S|J)$ の評価の仕方は 2 通り存在する。系の温度 $T = 1/\beta$ が既与のときは、Boltzmann 分布(正準分布)

$$P(S|J) = \frac{1}{Z(J)} P_0(S) \exp(-\beta H(J|S)) \quad (3.3)$$

に従うとした統計に基づく計算が容易である。ここで登場する規格化因子

$$Z(J) = \sum_S P_0(S) \exp(-\beta H(J|S)) \quad (3.4)$$

¹統計力学では $H(S|J)$ という表記が一般的だが、本論文では Bayes 公式(3.2)との対応が明確になる表記を採用した。

は分配関数と呼ぶ。

逆に、温度とは共役な関係にある1自由度当たりのエネルギー e が既与のときは、小正準分布

$$P(S|J) = \frac{1}{V(J)} P_0(S) \delta(H(J|S) - Ne) \quad (3.5)$$

に従う。このとき、規格化因子

$$V(J) = \sum_S P_0(S) \delta(H(J|S) - Ne) \quad (3.6)$$

も(小正準分布の)分配関数と呼ぶことにする。

この2つの方法は、 $N \rightarrow \infty$ の熱力学的極限では Legendre 変換を介した整合性があり、同一の結果を与えることが知られている。ただし、 $P_0(S)$ は状態 S に関する事前知識を表現している事前分布である。結局、統計力学とは、事前分布 $P_0(S)$ で表現された事前知識に、ハミルトニアン $H(J|S)$ で表現した相互作用の影響を加味し、事後分布 $P(S|J)$ がもたらす巨視的な性質を解明する方法論であるといえる。

さて、系の巨視的な性質は秩序変数と呼ばれるいくつかの変数によって完全に記述できる。ここでは、秩序変数 $Q(S)$ が見付けられたとして、その1自由度当たりの値を q と書くことにする。当然、秩序変数 q に対応する系の微視的な状態 S は無数に存在しているかもしれない。統計力学では、これらの状態をすべて同一の巨視的な変数 q でラベル付けし直し、非本質的な差異を取り除くことによって、情報を縮約し見通しのよい議論を行うことができる。

確率分布(3.3)や(3.5)が与えられたときに実現する秩序変数 q^* を求めるには次のようにすればよい。小正準分布(3.5)に従う統計集団を想定したときは、秩序変数 $Q(S)$ が1自由度当たり一定となる分配関数(3.6)の部分

$$V(J, q) = \sum_S P_0(S) \delta(H(J|S) - Ne) \delta(Q(S) - Nq) \quad (3.7)$$

を定義する。分配関数を求めるには、まず部分(3.7)を計算してから、秩序変数 q に関する和

$$V(J) = \int dq V(J, q) \quad (3.8)$$

をとることを考える。ところが、自由度 N が大きいと、分配関数の部分 $V(J, q)$ は秩序変数 q に関して急峻な関数となる。特に、 $N \rightarrow \infty$ の熱力学的極限では、ある確定的な値 q^* 以外では0となる Dirac の δ 関数になる。このとき、分配関数の部分(3.7)は分配関数の全体(3.6)と一致する。よって、この秩序変数の値 q^* を与える状態の集団が、系の典型的な性質を決定していると考えられる。

さらにこのとき、微視的な状態 S に関する事後分布 $P(S|J)$ とハミルトニアン $H(J|S)$ の関係を記述した(3.5)に対応する、秩序変数 q を用いた巨視的な視点からの記述

$$V(J, q) = \exp[Ns(J, q)] \quad (3.9)$$

が成立する。ここで、 $s(J, q)$ は1自由度当たりのエントロピーと呼ばれる評価関数で、 $O(1)$ の値をとる。 q^* を求めるためには、1自由度当たりのエントロピー

$$s(J, q) = \frac{1}{N} \ln V(J, q) \quad (3.10)$$

を秩序変数 q について偏微分して、鞍点方程式を導出すればよい。鞍点解が複数存在する場合には、それぞれについてエントロピーを計算し、その値が最も大きい解を採用する。

これに対し、正準分布を仮定した分配関数の方法による処方箋は1自由度当たりの自由エネルギー $f(J, q)$ を求めることが目標になる。まず、 β は系がハミルトニアン $H(J|S)$ に対してどのくらい敏感かを表現していることに注意する。例えば、 $\beta \rightarrow \infty$ では極めて系は敏感で、ハミルトニアン $H(J|S)$ の値が最も小さい基底状態しか実現していないことを意味する。逆に、 $\beta \rightarrow 0$ では極めて系は鈍感で、ハミルトニアン $H(J|S)$ は状態の実現確率 $P(S|J)$ にはほとんど影響を与えない。このときも、小正準分布のときと同様、秩序変数 q を用いた巨視的な視点からの記述

$$Z(J, q) = \exp[-N\beta f(J, q)] \quad (3.11)$$

が成立する。このときも、分配関数の部分

$$Z(J, q) = \sum_S P_0(S) \exp[-\beta H(J|S)] \delta(Q(S) - Nq) \quad (3.12)$$

を定義して、秩序変数 q の実現に貢献している微視的な状態 S の事後分布を足し合わせている。分配関数(3.4)は、ちょうど分配関数(3.6)と同じ役割を果たしている。結局、系の典型的な性質を議論するためには、1自由度当たりの自由エネルギー

$$f(J, q) = -\frac{1}{\beta N} \ln Z(J, q) \quad (3.13)$$

を最小化するような秩序変数の値 q^* を求めることになる。

3.3 レプリカ法

ランダムな相互作用 J が凍結して存在するクエンチ系では、ハミルトニアン自体にランダム変数 J が含まれることになる。小正準分布では、分配関数 $V(J, q)$ はランダム変数 J の与えられ方に依存するが、熱力学的極限では大数の法則によりエントロピー密度は J に依らず平均値

$$s(q) = \frac{1}{N} \langle \ln V(J, q) \rangle_J \quad (3.14)$$

に等しくなる。この性質は自己平均性と呼ばれ、ボンド J の詳細によらないエントロピー密度(3.14)は、系の典型的な性質を支配している。

エントロピー密度(3.14)の評価はランダム変数 $V(J, q)$ に関する対数の平均評価なので厳密に行うことは難しい。

しかしながら、熱力学極限では任意の正数 a に関する恒等式

$$\ln a = \lim_{n \rightarrow 0} \frac{a^n - 1}{n} \quad (3.15)$$

を用いて式(3.14)の右辺を $V(J, q)$ の n 次のモーメントに帰着させ、それを鞍点評価することでこの困難を回避することができる。 n 次のモーメント $\langle V(J, q)^n \rangle_J$ の評価が、同じランダムさを共有する n 個の同一系全体を1個の系とみなしたときの評価と同じになるので、この計算技術をレプリカ法と呼ぶ。

3.4 平均場近似

系の微視的な情報を秩序変数 q に縮約せずに、事後分布 $P(S|J)$ が各サイトごとと独立に依存していると見なし、この立場で事後分布

$$P(S|J) = \prod_{i=1}^N P(S_i|J) \quad (3.16)$$

を評価するのが平均場近似である。この方法のメリットは、系の典型的な性質を理解するのに重要な状態の事後分布平均の導出が計算量的な意味で容易に行えるという点にある。相互作用が一樣な強磁性体だと、理由不十分の原則と系の対称性により、各サイトにおけるスピン変数 S の事後分布は一樣で

$$P(S|J) = [P(S|J)]^N \quad (3.17)$$

と書ける。このため、強磁性体の事後分布 $P(S|J)$ は、事後分布 $P(S|J)$ の平均場方程式のみで記述できる。ところがランダム系では、相互作用はサイト間によって符号も大きさも違い、それに対応してスピン変数 S_i の事後分布もサイト i に依存する。このため、各サイトごとに異なった方程式を立てなければならず、系の自由度 N と同じだけの連立方程式を扱うことが避けられない。本節では、やはり Bayes 統計の立場から、(特定の)ランダム系において有効な平均場近似の枠組を概観する。

系が Boltzmann 分布に従うのなら、ある特定の状態 S が実現する確率は

$$P(S|J) = \frac{1}{Z(J)} P_0(S) \exp(-\beta H(J|S)) \quad (3.18)$$

と評価できる。このとき、ボンド J の成分ごとにハミルトニアンを分解して

$$H(J|S) = \sum_{j=1}^N g(J_\mu|S) \quad (3.19)$$

と書いておく。ボンド J の成分 J_μ の確率分布を評価するときに、 J_μ 自身の反作用場を排除した補助的な確率分布 $P(S|\{J_{\nu \neq \mu}\})$ を導入して事後分布を評価していくのが特

徴である。これは、純粋に周りからの影響だけを取り入れて事後分布を構成することに相当する。

Boltzmann 因子は式(3.19)を利用して

$$\exp(-\beta H(J|S)) = \prod_{\mu=1}^N \exp(-\beta g(J_\mu|S)) \quad (3.20)$$

と分解できるので、右辺に登場する Boltzmann 重み

$$w_B(J_\mu|S) = \exp(-\beta g(J_\mu|S)) \quad (3.21)$$

には、状態 S が既与のときにボンドの第 μ 成分が J_μ になる確からしさという意味がある。

Boltzmann 重み(3.21)を用いると、確率分布 $P(S|\{J_{\nu \neq \mu}\})$ の中でスピン変数の第 k 成分の値 S_k が既与のとき、ボンドの第 μ 成分の値が J_μ である確からしさを与える有効 Boltzmann 重みが

$$\begin{aligned} W_{\text{eff}}(J_\mu|S_k, \{J_{\nu \neq \mu}\}) \\ = \sum_{\{S_i \neq k\}} \exp(-\beta g(J_\mu|S)) \prod_{i \neq k} P(S_i|\{J_{\nu \neq \mu}\}) \end{aligned} \quad (3.22)$$

と評価できる。ただし、 $P(S_i|\{J_{\nu \neq \mu}\})$ は確率分布 $P(S|\{J_{\nu \neq \mu}\})$ が既与のとき、スピン変数の第 i 成分の値が S_i になる条件付きの確率分布である。

有効 Boltzmann 重み(3.22)が計算できるためには、確率分布 $P(S_i|\{J_{\nu \neq \mu}\})$ が与えられていることが必要である。ところが、事前分布 $P_0(S_k)$ が既知のとき、この確率分布は評価できて、

$$P(S_k|\{J_{\nu \neq \mu}\}) = \alpha_{\mu k} P_0(S_k) \prod_{\nu \neq \mu} W_{\text{eff}}(J_\nu|S_k, \{J_{\sigma \neq \nu}\}) \quad (3.23)$$

と表せる。ただし、 $\alpha_{\mu k}$ は規格化因子で

$$\alpha_{\mu k}^{-1} = \sum_{S_k = \pm 1} P_0(S_k) \prod_{\nu \neq \mu} W_{\text{eff}}(J_\nu|S_k, \{J_{\sigma \neq \nu}\}) \quad (3.24)$$

を満たしている。

式(3.22), (3.23)は自己無撞着なので、これを有効 Boltzmann 重み $W_{\text{eff}}(J_\mu|S_k, \{J_{\nu \neq \mu}\})$ と確率分布 $P(S_k|\{J_{\nu \neq \mu}\})$ について解いた後、現実の物理場を表現している事後分布は近似的に

$$P(S_k|J) = \alpha_k P_0(S_k) \prod_{\mu=1}^N W_{\text{eff}}(J_\mu|S_k, \{J_{\nu \neq \mu}\}) \quad (3.25)$$

と求められる。また系が小正準分布に従うと仮定しても、Boltzmann 重み(3.21)を適当に読み代えることで、同様の議論が成立する。確率分布に関する方程式(3.22)-(3.25)は、ボンド J を与えたときの各サイトにおけるスピン変数の事後分布 $P(S_i|J)$ を与えているが、ボンド分布 $P(J)$ に対して平均を取ると、レプリカ法から導かれる結果を再現することが知られている。

4 低密度パリティ検査符号の統計力学的解析

4.1 低密度パリティ検査符号の統計力学的解析

LDPC 符号の性能を評価するには、ハミルトニアン

$$\begin{aligned} H(\xi, \zeta, D|S, \tau) \\ = \sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \\ \times \delta[-1; J_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \cdot S_{i_1} \cdots S_{i_K} \tau_{j_1} \cdots \tau_{j_L}] \end{aligned} \quad (4.1)$$

を定義すればよい。メッセージ ξ を推定するスピン変数として S を導入し、さらに通信路で混入することが同然見込まれるノイズ ζ の推定にも別のスピン変数 τ を導入してフラストレーションを排除し、系の自明な基底状態がそのままメッセージの完全な復号化に対応しているように定式化した。ここで、テンソル D は、メッセージに関する各指標 i に対して C 成分のみ 1 であとは 0、ノイズに関する各指標 j に対して L 成分のみ 1 であとは 0 となるスパーステンソルである。 δ は Kronecker の δ 関数で、いまの場合は系の状態を表現しているスピン変数の積 $S_{i_1} \cdots S_{i_K} \tau_{j_1} \cdots \tau_{j_L}$ が受信語 J のビット $J_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} = \xi_{i_1} \cdots \xi_{i_K} \zeta_{j_1} \cdots \zeta_{j_L}$ と異なるときハミルトニアン(4.1)の値が増加するように定義されている。要するに、ハミルトニアン(4.1)は、スパーステンソル D で受信した符号語 J のビットを指定し、 δ 関数で系の状態 (S, τ) から拾ってきたスピン変数の積 $S_{i_1} \cdots S_{i_K} \tau_{j_1} \cdots \tau_{j_L}$ が受信したビットを復元し得るかを確認している誤り検出のための相互作用を表現している。

メッセージとノイズをスピン変数 S, τ で推定するとき、メッセージとノイズが本来持つ事前分布 $P_0(\xi), P_0(\zeta)$ にスピン変数の事前分布を一致させたときが Bayes 最適な復号化の戦略を与えることが知られている [9]。Bayes 最適な戦略とは、問題に含まれる確率分布に関する最適化操作を施し、平均的に最適な性能を得るための戦略である。符号の復号化という枠組におけるこの戦略は、スピングラスにおける西森温度の議論 [10] と本質的に等価になることが伊庭によって指摘されているので [11]、以後この事前分布に関する条件を西森条件と呼ぶことにする。このとき、スピン変数 S の事後分布は

$$P_{\text{opt}}(S, \tau | \xi, \zeta, D) = \frac{P_0(S)P_0(\tau)}{V(\xi, \zeta, D)} \delta(H(\xi, \zeta, D|S, \tau)) \quad (4.2)$$

と表せる。この事後分布を利用して Bayes 最適な復号化を実行するには、まずスピン変数の事後分布平均

$$\langle S_i \rangle_{\text{opt}} = \sum_{S_i} S_i P_{\text{opt}}(S, \tau | \xi, \zeta, D) \quad (4.3)$$

を計算し、メッセージを

$$\xi_i^{\text{opt}} = \text{sign}(\langle S_i \rangle_{\text{opt}}) \quad (4.4)$$

と推定すればよい。

Shannon 理論では、確率過程として記述される情報源から発生するメッセージ ξ のバイアス f_s は既知である。もちろん、既与のメッセージがバイアス f_s を持つように加工したと考えてもよい。この事前知識を用いて Bayes 最適な復号化を行うには、意図的に外場

$$F_s = \frac{1}{2} \ln \left(\frac{f_s}{1-f_s} \right) \quad (4.5)$$

をかけて、スピン変数 S のバイアスが f_s になっている状態のみ選択すればよい。このとき、スピン変数 S に関する事前分布は結局

$$P_0(S) = \frac{1}{(2 \cosh F_s)^N} \exp \left(F_s \sum_{i=1}^N S_i \right) \quad (4.6)$$

と書ける。同様に、ノイズ τ を Bayes 最適に推定するための外場 F_n を構成できる。誤り訂正符号の枠組では、通信路の性質に関する知識は既与とするので、メッセージ 1 ビット当たりの誤り率 $p = 1 - f_n$ は事前知識として利用することが可能である。このとき、外場

$$F_n = \frac{1}{2} \ln \left(\frac{f_n}{1-f_n} \right) \quad (4.7)$$

をかけて、スピン変数 τ のバイアスが f_n になっている状態のみ選択すればよい。やはり、スピン変数 τ に関する事前分布は

$$P_0(\tau) = \frac{1}{(2 \cosh F_n)^N} \exp \left(F_n \sum_{j=1}^M \tau_j \right) \quad (4.8)$$

になる。

ハミルトニアンが(4.1)で与えられる希釈スピングラスでは、基底状態のエネルギーは 0 になる。よって、この模型に統計力学の処方箋を適用する場合には、エネルギーが既与であると仮定する小正準集団を想定し、分配関数を計算するのが賢明である。いま、ハミルトニアン(4.1)と事前知識 $P_0(S), P_0(\tau)$ が既与であるので、分配関数は

$$V(D, \xi, \tau) = \sum_{S, \tau} P_0(S) P_0(\tau) \delta(H(\xi, \zeta, D|S, \tau)) \quad (4.9)$$

となる。

さてここで、解析的な議論を進めるために、スピン変数 S, τ と符号語 J のゲージを一齐に取り換える。

$$\begin{aligned} J_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \\ \rightarrow J_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \xi_{i_1} \cdots \xi_{i_K} \zeta_{j_1} \cdots \zeta_{j_L} = 1 \\ S_i \rightarrow S_i \xi_i \\ \tau_j \rightarrow \tau_j \zeta_j \end{aligned} \quad (4.10)$$

ゲージ変換(4.10)を行うと、ハミルトニアン(4.1)はメッセージ ξ とノイズ ζ に依存しなくなっている。ただし、ゲージを意図的に取り換えたので、メッセージとノイズに関する平均は確率分布

$$P(\xi_i) = f_s \delta(\xi_i - 1) + (1 - f_s) \delta(\xi_i + 1) \quad (4.11)$$

$$P(\zeta_j) = f_n \delta(\zeta_j - 1) + (1 - f_n) \delta(\zeta_j + 1) \quad (4.12)$$

を用いることに注意する。

ハミルトニアン(4.1)は、スパーステンソル D 、メッセージ ξ 、ノイズ ζ というランダム変数に依存するので、レプリカ法によるエントロピー密度の評価が必要になる。Wong-Sherringtonにならい、スパーステンソル D に対する拘束条件を

$$\begin{aligned} & \delta \left(\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} - C \right) \\ &= \int_0^{2\pi} \frac{dZ}{2\pi} Z^{-(C+1)} Z^{\sum_{\langle i_2, i_3, \dots, i_K \rangle} D_{\langle i_1, i_2, \dots, i_K; j_1, \dots, j_L \rangle}} \end{aligned} \quad (4.13)$$

$$\begin{aligned} & \delta \left(\sum_{\langle i_1, \dots, i_K; j_1, j_2, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, j_2, \dots, j_L \rangle} - L \right) \\ &= \int_0^{2\pi} \frac{dY}{2\pi} Y^{-(L+1)} Y^{\sum_{\langle j_2, j_3, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, j_2, \dots, j_L \rangle}} \end{aligned} \quad (4.14)$$

のように複素積分表示して和をとると

$$q_{\alpha, \beta, \dots, \gamma} = \frac{1}{N} \sum_{i=1}^N Z_i \langle S_i^\alpha S_i^\beta \dots S_i^\gamma \rangle_{\text{opt}} \quad (4.15)$$

$$r_{\alpha, \beta, \dots, \gamma} = \frac{1}{N} \sum_{j=1}^N Y_j \langle \tau_j^\alpha \tau_j^\beta \dots \tau_j^\gamma \rangle_{\text{opt}} \quad (4.16)$$

が秩序変数となることがわかる [8]。ここで、 $\alpha, \beta, \dots, \gamma$ はレプリカを表す指標、 $\langle \dots \rangle_{\text{opt}}$ は Bayes 最適な戦略である西森条件における事後分布での平均を表す。

希釈スピングラス模型の有効磁場分布は Gauss 分布と仮定することはできない。そのため、平均と分散を指定するだけでは不十分で、ここでは式(4.15)、(4.16)のように多数の秩序変数を導入しなければならない。レプリカ対称性を仮定した場合、秩序変数(4.15)、(4.16)とそれに共役な変数 $\hat{q}_{\alpha, \beta, \dots, \gamma}$ 、 $\hat{r}_{\alpha, \beta, \dots, \gamma}$ を連続的な確率分布 $\pi(x)$ 、 $\hat{\pi}(\hat{x})$ 、 $\rho(y)$ 、 $\hat{\rho}(\hat{y})$ のモーメントとして表現して

$$q_{\alpha, \beta, \dots, \gamma} = a_q \int dx \phi(x) x^l \quad (4.17)$$

$$\hat{q}_{\alpha, \beta, \dots, \gamma} = a_{\hat{q}} \int d\hat{x} \hat{\phi}(\hat{x}) \hat{x}^l \quad (4.18)$$

$$r_{\alpha, \beta, \dots, \gamma} = a_r \int dy \rho(y) y^l \quad (4.19)$$

$$\hat{r}_{\alpha, \beta, \dots, \gamma} = a_{\hat{r}} \int d\hat{y} \hat{\rho}(\hat{y}) \hat{y}^l \quad (4.20)$$

とおくと、確率分布(4.17)-(4.20)自体を秩序関数として取り扱えて計算が容易になる。ただし、 a_q 、 $a_{\hat{q}}$ 、 a_r 、 $a_{\hat{r}}$ は規格化定数、 l は相互作用しているレプリカの個数である。さらに、積分は区間 $[-1, 1]$ で行うものと約束する。

レプリカ法の処方箋にしたがって計算を進めると、エントロピー密度は最終的に

$$\begin{aligned} & s(\pi, \hat{\pi}, \rho, \hat{\rho}) \\ &= \frac{1}{N} \langle \ln V(D, \xi, \tau, \pi, \hat{\pi}, \rho, \hat{\rho}) \rangle_{, D} \\ &= -\frac{C}{K} \ln 2 - C \int dx d\hat{x} \pi(x) \hat{\pi}(\hat{x}) \ln(1 + x\hat{x}) \\ &\quad - \frac{CL}{K} \int dy d\hat{y} \rho(y) \hat{\rho}(\hat{y}) \ln(1 + y\hat{y}) \\ &\quad + \frac{C}{K} \int \left[\prod_{k=1}^K dx_k \pi(x_k) \right] \left[\prod_{l=1}^L dy_l \rho(y_l) \right] \\ &\quad \times \ln \left[1 + \prod_{k=1}^K x_k \prod_{l=1}^L y_l \right] \\ &\quad + \int \left[\prod_{k=1}^C d\hat{x}_k \hat{\pi}(\hat{x}_k) \right] \\ &\quad \times \left\langle \ln \left[e^{F_s \xi} \prod_{k=1}^C (1 + \hat{x}_k) + e^{-F_s \xi} \prod_{k=1}^C (1 - \hat{x}_k) \right] \right\rangle_{\xi} \\ &\quad + \frac{C}{K} \int \left[\prod_{l=1}^C d\hat{y}_l \hat{\rho}(\hat{y}_l) \right] \\ &\quad \times \left\langle \ln \left[e^{F_r \zeta} \prod_{l=1}^C (1 + \hat{y}_l) + e^{-F_r \zeta} \prod_{l=1}^C (1 - \hat{y}_l) \right] \right\rangle_{\zeta} \end{aligned} \quad (4.21)$$

となる(付録 A)。エントロピー密度(4.21)は確率分布(4.17)-(4.20)の汎関数で表現されているので、変分条件から秩序関数 $\pi(x)$ 、 $\hat{\pi}(\hat{x})$ 、 $\rho(y)$ 、 $\hat{\rho}(\hat{y})$ が決定できる。その結果、復号化のパフォーマンスを測るメッセージ ξ とスピン変数 S のオーバーラップは

$$m = \frac{1}{N} \langle \sum_{i=1}^N \xi_i \text{sign}(S_i) \rangle_{\text{opt}} = \int dz \phi(z) \text{sign}(z) \quad (4.22)$$

$$\begin{aligned} & \phi(z) = \int \left[\prod_{l=1}^C dy_l \hat{\pi}(y_l) \right] \\ & \times \left\langle \delta \left(z - \tanh \left(F_s \xi + \sum_{j=1}^C \tanh^{-1} y_j \right) \right) \right\rangle_{\xi} \end{aligned} \quad (4.23)$$

と表現される。エントロピー密度(4.21)の変分を率直に実

行すれば、秩序関数が満足すべき鞍点方程式として結局

$$\pi(x) = \int \prod_{l=1}^{C-1} d\hat{x}_l \hat{\pi}(\hat{x}_l) \times \left\langle \delta \left(x - \tanh \left(\xi F_s + \sum_{l=1}^{C-1} \tanh^{-1} \hat{x}_l \right) \right) \right\rangle_{\xi} \quad (4.24)$$

$$\hat{\pi}(\hat{x}) = \int \prod_{l=1}^{K-1} dx_l \pi(x_l) \int \prod_{l=1}^L dy_l \rho(y_l) \delta \left(\hat{x} - \prod_{l=1}^{K-1} x_l \prod_{l=1}^L y_l \right) \quad (4.25)$$

$$\rho(y) = \int \prod_{l=1}^{L-1} d\hat{y}_l \hat{\rho}(\hat{y}_l) \times \left\langle \delta \left(y - \tanh \left(\zeta F_n + \sum_{l=1}^{L-1} \tanh^{-1} \hat{y}_l \right) \right) \right\rangle_{\zeta} \quad (4.26)$$

$$\hat{\rho}(\hat{y}) = \int \prod_{l=1}^K dx_l \pi(x_l) \int \prod_{l=1}^{L-1} dy_l \rho(y_l) \delta \left(\hat{y} - \prod_{l=1}^K x_l \prod_{l=1}^{L-1} y_l \right) \quad (4.27)$$

を得る。

LDPC 符号の性能を調べるには、まず鞍点方程式(4.24)-(4.27)を解析的あるいは数値的に解いて、鞍点条件を満足する秩序関数 $\pi(x)$, $\hat{\pi}(\hat{x})$, $\rho(y)$, $\hat{\rho}(\hat{y})$ を求める。これらをエントロピー密度(4.21)に代入して極値を評価し、エントロピー密度の最大値を与える秩序関数を用いてオーバーラップ(4.22)を計算することで、Bayes 最適に復号化されたときの典型的な性能を理論的に評価することが可能になる。

4.2 相転移描像

秩序関数は鞍点方程式の解になっているときに物理的な意味を持つ。ところが、鞍点方程式(4.24)-(4.27)には δ 関数と連続分布が混在した解が存在するので、一般的な議論を解析的に行うのは非常に困難である。ただし、メッセージにバイアスがないときは強磁性解

$$\begin{aligned} \pi(x) &= \delta(x-1), & \hat{\pi}(\hat{x}) &= \delta(\hat{x}-1) \\ \rho(y) &= \delta(y-1), & \hat{\rho}(\hat{y}) &= \delta(\hat{y}-1) \end{aligned} \quad (4.28)$$

と常磁性解

$$\begin{aligned} \pi(x) &= \delta(x), & \hat{\pi}(\hat{x}) &= \delta(\hat{x}), & \hat{\rho}(\hat{y}) &= \delta(\hat{y}) \\ \rho(y) &= \langle \delta(y - \tanh \zeta F_n) \rangle_{\zeta} \end{aligned} \quad (4.29)$$

が自明な解として例外的に求まる。これらの解が鞍点方程式を満たしていることは容易に確認できる。しかし、物理的な意味のある解が別の δ 関数や連続分布から構成されていない保証はなく、そもそも解(4.28)と解(4.29)の安定性も不明である。これらの疑問を解決するため、鞍点方程

式(4.24)-(4.27)を数値的に評価してしまう方法がある。本論文では、本来連続である積分区間 $[-1, 1]$ を 10000 個に分割し、Monte-Carlo 法を用いて近似的に積分を実行することで数値的に鞍点方程式の解を調べた。

さて、自明な解である強磁性解(4.28)と常磁性解(4.29)を式(4.21)に代入してエントロピー密度を計算してみる。すると簡単な計算から、強磁性解のエントロピー密度

$$s_{\text{ferro}} = F_s \tanh F_s + \frac{C}{K} F_n \tanh F_n \quad (4.30)$$

と常磁性解のエントロピー密度

$$s_{\text{para}} = -\frac{C}{K} \ln 2 + \ln 2 \cosh F_s + \frac{C}{K} \ln 2 \cosh F_n \quad (4.31)$$

を得ることができる。このとき、解(4.28), (4.29)の安定性が依然として不明であることを忘れてはならない。ところが、この差を計算してみると

$$\begin{aligned} \Delta s &= s_{\text{ferro}} - s_{\text{para}} \\ &= \frac{C}{K} \ln 2 - \ln 2 \left[H_2(f_s) + \frac{1}{R} H_2(f_n) \right] \end{aligned} \quad (4.32)$$

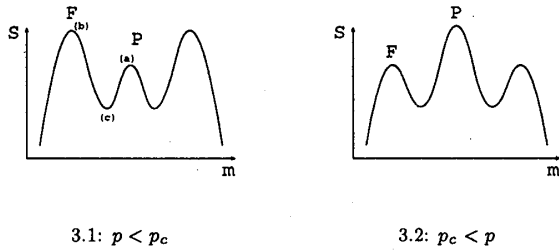
となることから分かるように、常磁性解と強磁性解のエントロピー密度が逆転する条件で通信路容量、すなわち Shannon 限界が決定されている。実際、 $H(f_s) = 1$ ので

$$R = 1 - H_2(f_n) \quad (4.33)$$

となっている。統計力学の処方箋にしたがった計算で、情報理論の基礎ともいえる通信路符号化定理の結果が再現されることは、理論の整合性や信頼性の観点からも望ましく、また極めて興味深い結果だといえる。

メッセージにバイアスがなく、 $K \geq 3$ あるいは $L \geq 3$ が満たされるときには、鞍点方程式(4.24)-(4.27)を数値的に評価すると解(4.28)と解(4.29)が常に共存し、それ以外の解は存在しないことが分かった。もちろん、復号化は Bayes 最適戦略として知られる西森条件のもと行われたと仮定している。このとき、強磁性相(強磁性解のエントロピー密度が最大の相、つまり復号化が成功する相)と常磁性相(常磁性解のエントロピー密度が最大の相、つまり復号化が失敗する相)の 1 次転移が起こる(図 3)。図 5.1 は、常磁性解と強磁性解が起こす 1 次転移の様子を誤り率 p の関数として描いた。太線と細線は安定解に対応し、太線はエントロピー密度最大を与えている。

$K, L \geq 3$ の LDPC 符号では、常磁性解と強磁性解に対応した準安定な 2 状態が共存する混合状態で系が記述されている。この準安定状態のことを純粋状態と呼び、純粋状態間における状態の推移はエントロピー障壁の存在により非常に困難になっている。つまり、図 3.2 において常磁性解 P に対応した純粋状態 a から強磁性解 F に対応した純粋状態 b に系の状態が推移するためには、途中に存在する中間状態 c を経由しなければならない。ところが、中間状

図 3: $K \geq 3$ または $L \geq 3$ のエントロピー曲面

態 c は純粋状態 a, b に比較してずっと小さなエントロピー密度を持っている。すると、中間状態 c は純粋状態 a, b を大きなエントロピー障壁で隔てる役割を果している。障壁の大きさ Δ は熱力学的極限 $N \rightarrow \infty$ で発散するから、純粋状態 a, b は互いに推移することが困難な準安定な状態であることが理解できる。このことは、系の初期状態がどの純粋状態の引き込み領域に存在したかで、実現される状態が決定してしまうことを意味する。つまりメッセージにバイアスがない $K, L \geq 3$ の LDPC 符号では、初期条件を強磁性解の引き込み領域にとることさえ可能なら、この符号は驚くべきことに Shannon 限界を達成してしまうことになる。もちろん、メッセージにバイアスがあるときには、鞍点方程式(4.24)-(4.27)の自明な解が不明なので、解析的な議論はあきらめて Monte-Carlo 法などによる数値解析を実行する。図 6 が LDPC 符号の相図である。常磁性相 (右上) と強磁性相 (左下) の相境界は Shannon 限界を除いてレプリカ法で得られた鞍点方程式(4.24)-(4.27)を Monte-Carlo 法で数値的に評価した。図 6.1 は $K, L \geq 3$ のときに常磁性相と強磁性相の間に 1 次転移が起こる相境界を評価した。バイアスがない場合 $H_2(f_s) = 1$ は符号化率 R を変化させて Shannon 限界を示した。バイアスがある場合 ($\square$) は $K = L = 3, L = 6$ のときにメッセージのバイアス f_s を変化させてレプリカ法による鞍点方程式を評価した。この図から、解析的な計算が困難なメッセージのバイアスがある場合でも、事実上 Shannon 限界に匹敵する情報伝送率で復号化が可能である。 $K \geq 3$ あるいは $L \geq 3$ を満たす LDPC 符号の唯一の弱点は、常磁性解の引き込み領域を避けて復号化を行う必要があるという非現実的な要請である。このことは、 $K, L \geq 3$ の強磁性相が混合状態で記述されていることの直接の帰結であり、復号化を多少工夫したところで解決できる類の性質ではない。

$K, L \geq 3$ の LDPC 符号はバイアスのないとき Shannon 限界を達成し、強磁性相から常磁性相の 1 次転移で特徴づけられた。それとは対照的に、 $K = L = 2$ の LDPC 符号は Shannon 限界の達成は不可能で、異なった物理的な性質があることが判明した。自明な解(4.28), (4.29)はある誤り率で不安定になり物理的な意味を失ってしまうので、

この場合は解析的な議論はあきらめて、Monte-Carlo 積分を用いて鞍点方程式(4.24)-(4.27)を数値的に評価することになる。その結果、次のような複雑な相転移描像が得られた。まず誤り率が大きい領域では常磁性解が唯一安定に存在するが(図 4.1), 誤り率が p_1 に達した段階で、安定だがエントロピー密度の値はまだ小さい強磁性解が現れる(図 4.2)。誤り率が p_2 になると、今度は常磁性解が不安定化し、メッセージの復号化に対応していない準最適な強磁性解が支配的になる(図 4.3)。やがて、誤り率が p_3 に達するとメッセージの復号化に対応した本来の強磁性解と立場が逆転し(図 4.4), さらに誤り率がスピノーダル点 p_s になったときに最適な強磁性解が唯一安定に存在することになる(図 4.5)。このとき、例えば準最適な強磁性解を鞍点方程式を数値的に解いて評価すると、付録 C に示されているように連続分布で構成されている非自明な解になる(図 6)。また $K = L = 2$ の場合も、強磁性解と常磁性解のエントロピー密度の値は Shannon 限界で逆転することに違いはないが、物理的な意味は全くない。 $K = L = 2$ の符号は、 $K, L \geq 3$ の符号に比較して、Shannon 限界の達成という意味では性能が劣る。実際、誤り率を上げていくと最適な強磁性解と常磁性解のエントロピー密度の値が逆転する以前に準最適な強磁性解とのあいだで逆転が起こってしまう。図 5.2 には、最適あるいは準最適な強磁性解と常磁性解を誤り率 p の関数で描いた。太線と細線は安定解で太線がエントロピー密度の最大を与えるのは図 5.1 と同様で、点線は不安定解を与えている。

図 6.2 では、メッセージにバイアスがないとき ($f_s = 0.5$) に、メッセージの復号化に対応した最適な強磁性解に加えて準最適な強磁性解が出現するスピノーダル点 p_s をレプリカ法で得られた鞍点方程式を Monte-Carlo 法で数値積分することで評価した ($\diamond$)。この線(スピノーダル線)を境界にして左下の領域では、最適な強磁性解に対応する純粋状態で系が記述できるので、混合状態の場合に重要だった引き込み領域の大きさなどを一切考慮することなしにメッセージの復号化が実現できる。つまり、スピノーダル線は実用上の最大符号化率を与えている。そして、この図から分かるように、スピノーダル点 p_s は Shannon 限界 p_c に接近していて、実用的な観点からは全く遜色ないといえる。とりわけ、誤り率がスピノーダル点 p_s に達するまでは最適な強磁性解が唯一安定に存在しているので、 $K, L \geq 3$ の符号の場合のように、常磁性解の引き込み領域を避けるといった非現実的な要請がない点は、強調してもし過ぎることはないだろう。LDPC 符号は、むしろ $K = L = 2$ の場合の方が実用上有利な性質を備えているのである。

4.3 平均場近似によるレプリカ解析の評価

前節で示された LDPC 符号の相転移描像の正当性は、ハミルトニアン(4.1) からエントロピー密度(4.21)を評価し

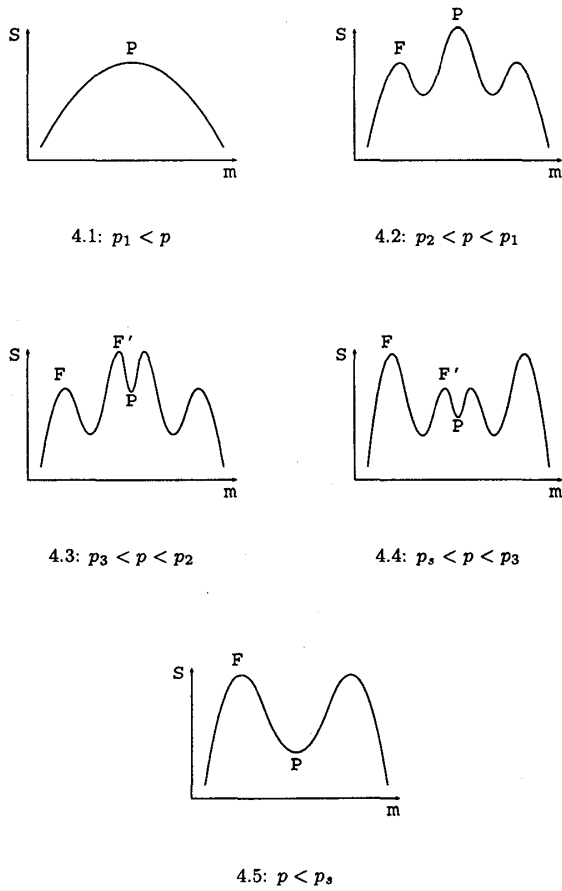


図 4: $K = 2$ かつ $L = 2$ のエントロピー曲面

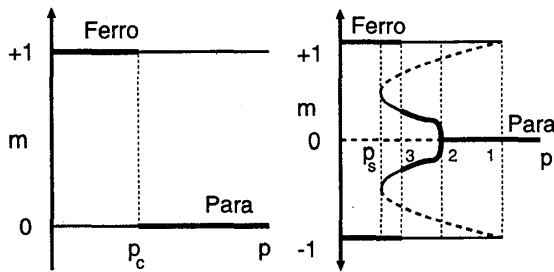


図 5: 鞍点方程式の解

たレプリカ法による解析の信頼性に依存している。本節では、レプリカ法による解析の信頼性そのものを評価するため、エントロピー密度を全く別のアプローチで評価することを考える。このとき、新たに計算したエントロピー密度の変分条件が、スピン変数の事後分布を与える自己無撞着な鞍点方程式を導く。この事実を利用して、レプリカ解析で得られた鞍点方程式に含まれる秩序関数と、スピン変数の事後分布を与えるパラメータの分布を直接比較することで、両者の整合性を示す。

ハミルトニアン(4.1)より、小正準分布の分配関数として

$$V(J) = \sum_{S, \mu=1}^M \Theta \left(J_\mu \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right) \prod_{i=1}^N e^{F_S S_i} \prod_{j=1}^M e^{F_\tau \tau_j} \quad (4.34)$$

を採用してよい。ただし $I(\mu)$ はボンド J の第 μ 成分 J_μ を構成するメッセージビットの指標の集合、 $J(\mu)$ はノイズビットの指標の集合であった。このとき、任意の確率分布 $\hat{P}_\mu(S, \tau)$ について

$$V(J) = \left\langle \prod_{\mu=1}^M \frac{\Theta \left(J_\mu \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}_\mu(S, \tau)} \right\rangle_{\hat{P}} \times \sum_{S, \mu=1}^M \hat{P}_\mu(S, \tau) \prod_{i=1}^N e^{F_S S_i} \prod_{j=1}^M e^{F_\tau \tau_j} \quad (4.35)$$

が厳密に成立する。ただし、平均 $\langle \dots \rangle_{\hat{P}}$ を

$$\langle \dots \rangle_{\hat{P}} = \frac{\sum_{S, \dots} \prod_{\mu=1}^M \hat{P}_\mu(S, \tau)}{\sum_{S, \dots} \prod_{\mu=1}^M \hat{P}_\mu(S, \tau)} \quad (4.36)$$

と定義した。いま $M \rightarrow \infty$ の熱力学的極限で、平均 $\langle \dots \rangle_{\hat{P}}$ と積 $\prod_{\mu=1}^M$ の操作を交換したとき

$$\frac{1}{M} \ln \left\langle \prod_{\mu=1}^M \frac{\Theta \left(J_\mu \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}_\mu(S, \tau)} \right\rangle_{\hat{P}} = \frac{1}{M} \ln \prod_{\mu=1}^M \left\langle \frac{\Theta \left(J_\mu \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}_\mu(S, \tau)} \right\rangle_{\hat{P}} \quad (4.37)$$

が成立すると仮定する。このとき、付録 B にあるように確率分布 $P_\mu(S, \tau)$ を新たに導入し、平均 $\langle \dots \rangle_{P_\mu}$ を

$$\langle \dots \rangle_{P_\mu} = \sum_{S, \dots} \dots P_\mu(S, \tau) \quad (4.38)$$

と定義すれば、(4.37) の右辺の平均 $\langle \dots \rangle_{\hat{P}}$ は平均 $\langle \dots \rangle_{P_\mu}$ を用いて

$$\left\langle \frac{\Theta \left(J_\mu \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}_\mu(S, \tau)} \right\rangle_{\hat{P}} = \frac{\left\langle \Theta \left(J_\mu \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right) \right\rangle_{P_\mu}}{\left\langle \hat{P}_\mu(S, \tau) \right\rangle_{P_\mu}} \quad (4.39)$$

と書き換えられる。ここで、分布 P_μ , $\hat{P}_\mu$ はサイトの指標 i, j について独立な成分の積で近似できて (平均場近似)

$$P_\mu(S, \tau) = \prod_{i \in I(\mu)} \left(\frac{1 + S_i m_{\mu i}^S}{2} \right) \prod_{j \in J(\mu)} \left(\frac{1 + \tau_j m_{\mu j}^\tau}{2} \right) \quad (4.40)$$

$$\hat{P}_\mu(S, \tau) = \prod_{i \in I(\mu)} \left(\frac{1 + S_i \hat{m}_{\mu i}^S}{2} \right) \prod_{j \in J(\mu)} \left(\frac{1 + \tau_j \hat{m}_{\mu j}^\tau}{2} \right) \quad (4.41)$$

と表現できると仮定する。このときに、分配関数からエントロピー密度を計算すると

$$\begin{aligned} & \frac{\ln V(J)}{N} \\ &= \frac{1}{N} \sum_{\mu=1}^M \ln \left(\frac{1 + J_\mu \prod_{i \in I(\mu)} m_{\mu i}^S \prod_{j \in J(\mu)} m_{\mu j}^\tau}{2} \right) \\ & - \frac{1}{N} \sum_{\mu=1}^M \sum_{i \in I(\mu)} \ln \left(\frac{1 + m_{\mu i}^S \hat{m}_{\mu i}^S}{2} \right) \\ & - \frac{1}{N} \sum_{\mu=1}^M \sum_{j \in J(\mu)} \ln \left(\frac{1 + m_{\mu j}^\tau \hat{m}_{\mu j}^\tau}{2} \right) \\ & + \frac{1}{N} \sum_{i=1}^N \ln \left[e^{F_s} \prod_{\mu \in M(i)} \left(\frac{1 + \hat{m}_{\mu i}^S}{2} \right) \right. \\ & \quad \left. + e^{-F_s} \prod_{\mu \in M(i)} \left(\frac{1 - \hat{m}_{\mu i}^S}{2} \right) \right] \\ & + \frac{1}{N} \sum_{j=1}^M \ln \left[e^{F_n} \prod_{\mu \in M(j)} \left(\frac{1 + \hat{m}_{\mu j}^\tau}{2} \right) \right. \\ & \quad \left. + e^{-F_n} \prod_{\mu \in M(j)} \left(\frac{1 - \hat{m}_{\mu j}^\tau}{2} \right) \right] \end{aligned} \quad (4.42)$$

を得る (付録 B)。ただし、 $M(i)$ ($M(j)$) はメッセージビット ξ_i (ノイズビット ζ_j) を含んだメッセージの指標全体の集合を表す記号である。ここで、エントロピー密度 (4.42) のパラメータ $m, \hat{m}$ に対する変分条件より鞍点方程式

$$m_{\mu k}^S = \tanh \left(\sum_{\nu \in M(k)/\mu} \tanh^{-1} \hat{m}_{\nu k}^S + F_s \right) \quad (4.43)$$

$$m_{\mu l}^\tau = \tanh \left(\sum_{\nu \in M(l)/\mu} \tanh^{-1} \hat{m}_{\nu l}^\tau + F_n \right) \quad (4.44)$$

$$\hat{m}_{\mu k}^S = J_\mu \prod_{i \in I(\mu)/k} m_{\mu i} \prod_{j \in J(\mu)} \hat{m}_{\mu j}^\tau \quad (4.45)$$

$$\hat{m}_{\mu l}^\tau = J_\mu \prod_{i \in I(\mu)} m_{\mu i} \prod_{j \in J(\mu)/l} \hat{m}_{\mu j}^\tau \quad (4.46)$$

が導かれる。ただし、 $M(k)/\mu$ は集合 $M(k)$ からその要素 μ を取り除いた集合を意味する。鞍点方程式 (4.43)-(4.46)

が得られたので、これを数値的に評価することでエントロピー (4.42) を最大化させるパラメータ $m_{\mu i}^{S*}, \hat{m}_{\mu i}^{S*}, m_{\mu j}^{\tau*}, \hat{m}_{\mu j}^{\tau*}$ を求めることができる。

このとき、分布 $P_\mu(S, \tau)$, $\hat{P}_\mu(S, \tau)$ のサイトに関する独立性を特徴づけるため補助的に導入されたパラメータ $m_{\mu i}^S, \hat{m}_{\mu i}^S, m_{\mu j}^\tau, \hat{m}_{\mu j}^\tau$ と、レプリカ解析の途中で導入された秩序関数 $\pi(x)$, $\hat{\pi}(\hat{x})$, $\rho(y)$, $\hat{\rho}(\hat{y})$ の間には密接な関係がある。実際、各パラメータの値から

$$m_k^S = \tanh \left(\sum_{\nu \in M(k)} \tanh^{-1} \hat{m}_{\nu k}^S + F_s \right) \quad (4.47)$$

$$m_l^\tau = \tanh \left(\sum_{\nu \in M(l)} \tanh^{-1} \hat{m}_{\nu l}^\tau + F_n \right) \quad (4.48)$$

$$\hat{m}_k^S = J_\mu \prod_{i \in I(\mu)} m_{\mu i} \prod_{j \in J(\mu)} \hat{m}_{\mu j}^\tau \quad (4.49)$$

$$\hat{m}_l^\tau = J_\mu \prod_{i \in I(\mu)} m_{\mu i} \prod_{j \in J(\mu)} \hat{m}_{\mu j}^\tau \quad (4.50)$$

を計算して

$$m_i^S \leftrightarrow x, \quad \hat{m}_i^S \leftrightarrow \hat{x}, \quad \tau_j^\tau \leftrightarrow y, \quad \hat{\tau}_j^\tau \leftrightarrow \hat{y} \quad (4.51)$$

という対応関係を認めれば、パラメータから秩序関数を構成することができる。つまり、秩序関数の定義されている区間 $[-1, 1]$ を有限個の区間 $[x_d, x_{d+1}]$ ($d = 0, \dots, D$) に分割し、各サイト i におけるパラメータ $m_{\mu i}^S$ の値が与えられたら、 $m_{\mu i}^S \in [x_d, x_{d+1}]$ を満足する i の個数を調べ、適当に規格化をして秩序関数の区間 $[x_d, x_{d+1}]$ における代表点の値 $\pi(x_d)$ と同一視すればよい。

実際、レプリカ解析で登場する秩序関数との間にある対応関係 (4.51) を用いて秩序関数に対応するパラメータ分布を構成すると、両者の形状はほぼ一致していることが分かる (付録 C の図 6)。このことから、前節で示した相転移描像の根拠となるレプリカ解析と平均場近似 (4.40), (4.41) に基づくエントロピーの近似的評価の枠組は無矛盾であるといえる。異なったアプローチによる解析が両立可能であることから、レプリカ解析も平均場近似も信頼性の高い解析法であると結論できる。

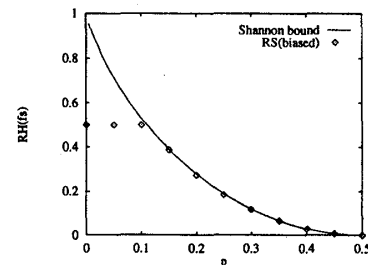


図 6.1 常磁性相と強磁性相の間に 1 次転移が起こる相境界を評価した。バイアスがない場合 $H_2(f_s) = 1$ は符号化率 R を変化させて Shannon 限界を示した。バイアスがある場合 (□) は $K = L = 3$, $L = 6$ のときにメッセージのバイアス f_s を変化させてレプリカ法による鞍点方程式を評価した。

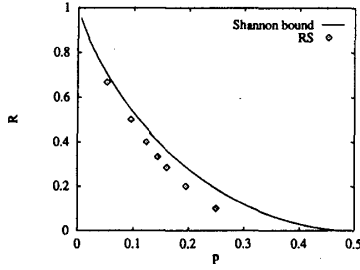


図6.2 メッセージにバイアスがないとき ($f_s = 0.5$) に、メッセージの復号化に対応した最適強磁性解に加えて準最適強磁性解が出現するスピノーダル点 p_s をレプリカ法で得られた鞍点方程式を Monte-Carlo 法で数値積分することで評価した (o)。

図 6 LDPC 符号の相図

5 現実的な復号化技術

5.1 ビリーフ・プロパゲーション

第4章での議論から、LDPC符号が優れた性能を持つ符号であることが分かった。実際、スピン変数 S の事後分布平均

$$\langle S_i \rangle_{\text{opt}} = \sum_{S_i} S_i P_{\text{opt}}(S, \tau | \xi, \zeta, D) \quad (5.1)$$

を計算し、Bayes 最適復号化

$$\xi_i^{\text{opt}} = \text{sign}(\langle S_i \rangle_{\text{opt}}) \quad (5.2)$$

を実行すれば理論上の最高性能を発揮できる。ところが、この Bayes 最適戦略は計算量の観点からは破綻している。事後分布平均(5.1)の評価には $O(e^{\alpha N})$ (α は定数)の計算量が必要になっているのである。これは、実用的には適用できない復号化法であるといえる。そのため、現実的な計算量でメッセージを推定する復号化法が提案されている。本節では、MacKayにより Bayes 統計的アプローチで見出され、後に樺島と Saad によって平均場近似の枠組において理解されるに至ったビリーフ・プロパゲーション (BP) について、その構成法を [6] に基づいて議論する。

本節では、正準分布に基づく定式化を行う。このとき、ハミルトニアンにはレプリカ解析で出発点にした(4.1)を少し修正して

$$\begin{aligned} H(D, J | S, \tau) \\ = - \sum_{\langle i_1, \dots, i_k; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_k; j_1, \dots, j_L \rangle} J_{\langle i_1, \dots, i_k; j_1, \dots, j_L \rangle} \\ \times S_{i_1} \dots S_{i_k} \tau_{j_1} \dots \tau_{j_L} \end{aligned} \quad (5.3)$$

を採用するものとする。今回は、ボンド J に関するランダム平均を実行しないので、ハミルトニアン(5.3)を存在

するボンドに対しての指標 $\mu = 1, \dots, M$ について書き直して

$$\begin{aligned} H(J | S, \tau) &= \sum_{\mu=1}^M g(J_\mu | S, \tau) \\ &= \sum_{\mu=1}^M J_\mu \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \end{aligned} \quad (5.4)$$

とする。ボンド J_μ はもちろん

$$J_\mu = \prod_{i \in I(\mu)} \xi_i \prod_{j \in J(\mu)} \zeta_j \quad (5.5)$$

のことである。こうしておけば、Boltzmann 重みが簡単に表現できて

$$w_B(J_\mu | S, \tau) = \exp(-\beta g(J_\mu | S, \tau)) \quad (5.6)$$

となる。この系では、2種類のスピン変数 S_i, τ_j が状態を記述しているので、 J_μ の確率分布を評価するときにも2種類の補助的な確率分布

$$P(S | \{J_{\nu \neq \mu}\}) = \prod_{i=1}^N P(S_i | \{J_{\nu \neq \mu}\}) \quad (5.7)$$

$$P(\tau | \{J_{\nu \neq \mu}\}) = \prod_{j=1}^M P(\tau_j | \{J_{\nu \neq \mu}\}) \quad (5.8)$$

を導入する必要がある。重み(5.6)を用いると、確率分布(5.7), (5.8)の中でスピン変数 S の第 k 成分の値 S_k が既与のとき、ボンドの第 μ 成分の値が J_μ である確からしさを与える重みが

$$\begin{aligned} W_{\text{eff}}(J_\mu | S_k, \{J_{\nu \neq \mu}\}) \\ = \sum_{\{S_i \neq k\}} w_B(J_\mu | S, \tau) \prod_{i \neq k} P(S_i | \{J_{\nu \neq \mu}\}) \prod_{j=1}^M P(\tau_j | \{J_{\nu \neq \mu}\}) \end{aligned} \quad (5.9)$$

と評価できる。復号化の枠組では、事前分布(メッセージのバイアス)

$$P_0(S_k) = \frac{1}{2}(1 + \tanh F_s S_k) \quad (5.10)$$

が既知であるので、スピン変数 S に関する確率分布は評価できて

$$P(S_k | \{J_{\nu \neq \mu}\}) = \alpha_{\mu k} P_0(S_k) \prod_{\nu \neq \mu} W_{\text{eff}}(J_\nu | S_k, \{J_{\sigma \neq \nu}\}) \quad (5.11)$$

と表せる。またここで、補助的に導入した確率分布に関する局所磁場を導入して

$$\frac{1 + S_k m_{\mu k}^S}{2} = P(S_k | \{J_{\nu \neq \mu}\}) \quad (5.12)$$

$$\frac{1 + S_k \hat{m}_{\mu k}^S}{2} = \hat{\alpha}_{\mu k} W_{\text{eff}}(J_\mu | S_k, \{J_{\nu \neq \mu}\}) \quad (5.13)$$

などと定義する。ただし、 $\alpha_{\mu k}$, $\hat{\alpha}_{\mu k}$ は規格化因子で

$$\alpha_{\mu k}^{-1} = \sum_{S_k = \pm 1} P_0(S_k) \prod_{\nu \neq \mu} W_{\text{eff}}(J_\nu | S_k, \{J_{\sigma \neq \nu}\}) \quad (5.14)$$

$$\hat{\alpha}_{\mu k}^{-1} = \sum_{S, \tau} w_B(J_\mu | S, \tau) \prod_{i \neq k}^N P(S_i | \{J_{\nu \neq \mu}\}) \prod_{j=1}^M P(\tau_j | \{J_{\nu \neq \mu}\}) \quad (5.15)$$

を満たしている。スピン変数 τ についても同様に議論して、 $m_{\mu l}^\tau$ と $\hat{m}_{\mu l}^\tau$ を定義することができる。結局、平均場方程式として

$$m_{\mu k}^S = \tanh \left(\sum_{\nu \in M(k)/\mu} \tanh^{-1} \hat{m}_{\nu k}^S + F_s \right) \quad (5.16)$$

$$m_{\mu l}^\tau = \tanh \left(\sum_{\nu \in M(l)/\mu} \tanh^{-1} \hat{m}_{\nu l}^\tau + F_n \right) \quad (5.17)$$

$$\hat{m}_{\mu k}^S = J_\mu \prod_{i \in I(\mu)/k} m_{\mu i} \prod_{j \in J(\mu)} \hat{m}_{\mu j}^\tau \quad (5.18)$$

$$\hat{m}_{\mu l}^\tau = J_\mu \prod_{i \in I(\mu)} m_{\mu i} \prod_{j \in J(\mu)/l} \hat{m}_{\mu j}^\tau \quad (5.19)$$

を得る ($\beta \rightarrow \infty$)。いままでの議論のように、補助的な確率分布を用いた平均場方程式の構成は Thouless, Anderson, Palmer という 3 人の物理学者によって初めてなされたと考えられる。そのため、この種の平均場方程式は TAP 方程式と呼ばれている [12]。

BP では TAP 方程式(5.16)-(5.19) が復号化のアルゴリズムを記述している。つまり、パラメータ $m_{\mu k}^S, m_{\mu l}^\tau, \hat{m}_{\mu k}^S, \hat{m}_{\mu l}^\tau$ をメッセージとノイズのバイアスに関する事前知識を反映させた適当な初期値、例えば

$$m_{\mu k}^S = \tanh(F_s), m_{\mu l}^\tau = \tanh(F_n), \hat{m}_{\mu k}^S = 0, \hat{m}_{\mu l}^\tau = 0 \quad (5.20)$$

に設定し、TAP 方程式を同期的に繰り返し適用していくことによって収束させる。そして、メッセージの事後分布平均を近似的に

$$m_\mu^S = \tanh \left(\sum_{\mu \in M(i)} \tanh^{-1} \hat{m}_{\mu i}^S + F_s \right) \quad (5.21)$$

と計算し、最終的なメッセージの推定値として

$$\xi_i^{\text{opt}} = \text{sign}(m_i^S) \quad (5.22)$$

を得る。このとき、スピン変数 S の事後分布平均の近似値(5.21) が厳密な事後分布平均の値(5.1) に一致していれば、BP は Bayes 最適な復号化法を与えている。

図 7 に、第 4 章ですでに示したレプリカ法による鞍点方程式の評価と本節で構成した BP による復号化による最大情報伝達率の比較を行った。このとき、メッセージは $N = 10000$ の大きさで、TAP 方程式による復号化は 10

試行の平均で評価した。また、誤差は極めて小さいので誤差棒は省略した。図 7.1 ではメッセージのバイアス f_s を変化させたときに、強磁性相 (復号化が成功する状態) と常磁性相 (復号化が失敗する状態) の 1 次転移が起こる相境界を評価した。バイアスがない場合 (+) とある場合 (○) の TAP 方程式による評価に加えて、バイアスがある場合の鞍点方程式の評価 (□) が描かれている。ただし、強磁性相の引き込み領域は非常に小さく、事前知識なしにこの相を探索することは実質的に不可能になっている。図 7.2 ではメッセージのバイアスがないとき ($f_s = 0.5$)、復号化に対応した安定な強磁性解に加えて準安定な強磁性解が出現する線 (スピノーダル線) を鞍点方程式 (○) と TAP 方程式 (+) によって評価した。スピノーダル線 (○) より左下では、強磁性解が唯一安定であるので初期条件に関わらず、TAP 方程式によってこの相を探索することができる。つまり、これが実用上の復号化の限界を与える。

BP が収束するまでにかかる計算量は経験的に $O(N)$ で、十分実用に耐える復号化法であるといえる。この計算コストの劇的な削減は、スピン変数 S の事後分布平均を近似的に評価した結果である。

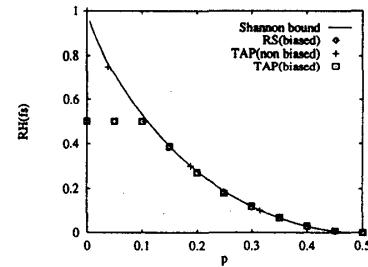


図 7.1 メッセージのバイアス f_s を変化させたときに、強磁性相 (復号化が成功する状態) と常磁性相 (復号化が失敗する状態) の 1 次転移が起こる相境界を評価した。バイアスがない場合 (+) とある場合 (○) の TAP 方程式による評価に加えて、バイアスがある場合の鞍点方程式の評価 (□) が描かれている。

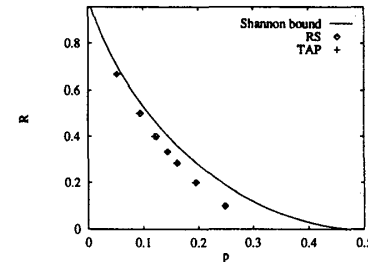


図 7.2 メッセージのバイアスがないとき ($f_s = 0.5$)、復号化に対応した安定な強磁性解に加えて準安定な強磁性解が出現する線 (スピノーダル線) を鞍点方程式 (○) と TAP 方程式 (+) によって評価した。

図 7 BP

5.2 ビリーフ・プロパゲーションと平均場近似

前節の結果から、BPはTAP方程式(5.16)-(5.19)を(事前知識を反映させた)パラメータの適当な初期値から同期的に更新していくアルゴリズムであることが理解できる。このとき、TAP方程式(5.16)-(5.19)が近似的に構成したエントロピー密度(4.42)の鞍点方程式(4.43)-(4.46)と一致している事実は注目に値する。4.3節の議論を参考にすれば、LDPC符号のレプリカ解析(平均場理論)とTAP方程式の方法(平均場近似)の与える結果は同一であると強く予想できる。レプリカ解析がBayes最適な復号化法に基づいていることを思い出せば、TAP方程式によって情報を縮約して計算量的な節約を行ったBPは、熱力学的極限でBayes最適戦略に一致することになる。実際、図7はBPの極めて高い性能を示している。つまり、BPは理論的な保証が存在する有用な復号化技術なのである。

6 結語

本論文では、低密度パリティ検査符号(LDPC符号)のBayes最適な復号化の過程が多体相互作用を持つ希釈スピングラスの基底状態探索に帰着することに注目し、レプリカ法と共に平均場理論を適用することで、あらゆるLDPC符号の性能をその典型的な場合に評価することに成功した。その結果、従来の最悪時解析では不可能だった $K=2$ かつ $L=2$ における符号の典型的な挙動が解明され、その他の場合と比較して実用的上有利な性質があることが判明した。この符号を用いた場合、最適に復号化を行えば、メッセージの復号化が失敗する確率がほとんどないことが統計的に示されたのである。さらに詳しく調べると、この符号の最大符号化率はほぼ通信路容量に達し、何の最適化も施されていない現時点でも極めて高性能な符号であることが分かった。さらに、現実的な復号化の技術としてBayes統計の立場から考案されたビリーフ・プロパゲーション(BP)が、統計力学の立場ではランダム系の平均場近似として導入されるTAP方程式によって基礎付けられることに注目した。このとき、レプリカ解析とTAP方程式を導出した平均場近似の議論における理論的整合性から、BPがBayes最適な復号化法にせまる高性能な実用的復号化技術であることを確認した。また、本論では触れなかったが、LDPC符号の符号化/復号化の過程には計算量的な一方向性が存在する。このため、LDPC符号を利用した公開鍵暗号方式が可能である。興味深い話題であるが、本論文の主題から逸脱してしまう感が否めないため、最後に軽く指摘しておくに止める。

謝辞

指導教官の樺島祥介先生には、レプリカ法やTAP方程式などランダム系の物理学の基礎的な技術を粘り強く指導していただき、研究全般の方向づけをして頂きました。物理学科の西森秀稔先生には、学部時代からセミナーに参加させていただくなど大変お世話になりました。また、樺島研究室の嶋崎政一君をはじめ、中村一尊君、佐塚直也君には、いろいろな議論を通して貴重なアドバイスを頂きました。その他、ここには紹介しきれなかったけれどもお世話になった方々に心からお礼申し上げます。

参考文献

- [1] C.E. Shannon, *Bell Sys. Tech. J.*, **27**, 379 (1948); **27**, 623 (1948).
- [2] R.G. Gallager, *IRE Trans. Info. Theory*, **IT-8**, 21 (1962).
- [3] D.J.C. MacKay and R.M. Neal, *Elect. Lett.*, **33**, 457 (1997).
- [4] D.J.C. MacKay, *IEEE Trans. IT*, in press (1998).
- [5] Y. Kabashima T. Murayama and D. Saad, submitted to *Phys. Rev. Lett.* (1998)
- [6] Y. Kabashima and D. Saad, *Euro. Phys. Lett.*, **44** 668 (1998).
- [7] N. Sourlas, *Nature*, **339**, 693 (1989).
- [8] K.Y.M. Wong and D. Sherrington, *J. Phys. A*, **20**, L793 (1987).
- [9] H. Nishimori, *J. Phys. Soc. Jpn*, **62**, 2973 (1993).
- [10] H. Nishimori, *J. Phys. C*, **13**, 4071 (1980).
- [11] Y. Iba, to appear in *J. Phys. A* (1998).
- [12] D. Thouless, P.W. Anderson and R.G. Palmer, *Phil. Mag.*, **35**, 593 (1977).

付録

A レプリカ法によるエントロピー密度の評価

ハミルトニアン(4.1) より, 分配関数は Θ 関数を用いて

$$V(J) = \sum_{S_i} \exp \left(F_s \sum_{i=1}^N S_i + F_n \sum_{j=1}^M \tau_j \right) \prod_{\mu=1}^M \Theta \left(J_\mu \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right) \quad (\text{A.1})$$

と表現できる. 本文中にあるように, ここでゲージ変換(4.10)を行うと

$$V(\xi, \zeta, J) = \sum_{S_i} \exp \left(F_s \sum_{i=1}^N \xi_i S_i + F_n \sum_{j=1}^M \zeta_j \tau_j \right) \prod_{\mu=1}^M \Theta \left(\prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right) \quad (\text{A.2})$$

となり, 交換相互作用の形式が簡単になる. もちろん, その代償としてメッセージとノイズの事前分布にランダム変数 ξ, ζ が含まれるようになる. さらに, スパーステンソル D を導入して, サイトの指標に注目した表現をとることにすれば

$$\begin{aligned} V(\xi, \zeta, D) &= \sum_{S_i} \exp \left(F_s \sum_{i=1}^N \xi_i S_i + F_n \sum_{j=1}^M \zeta_j \tau_j \right) \\ &\times \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} [1 - D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} + D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \Theta(S_{i_1} \cdots S_{i_K} \cdot \tau_{j_1} \cdots \tau_{j_L})] \end{aligned} \quad (\text{A.3})$$

と変形することは容易である. ここで, 通常のレプリカ法の処方箋に従って

$$\begin{aligned} \langle V(\xi, \zeta, D)^n \rangle_{, D} &= \sum_{S^1, \dots, S^n} \sum_{\tau^1, \dots, \tau^n} \left\langle \exp \left(F_s \sum_{i=1}^N \xi_i \sum_{\alpha=1}^n S_i^\alpha \right) \right\rangle \left\langle \exp \left(F_n \sum_{j=1}^M \zeta_j \sum_{\alpha=1}^n \tau_j^\alpha \right) \right\rangle \\ &\times \left\langle \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \prod_{\alpha=1}^n \left\{ 1 + \frac{1}{2} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha - 1) \right\} \right\rangle_D \end{aligned} \quad (\text{A.4})$$

を計算するのが当面の目標になるが, 事前分布に関する項はすぐに求まって

$$\left\langle \exp \left(F_s \sum_{i=1}^N \xi_i \sum_{\alpha=1}^n S_i^\alpha \right) \right\rangle = \prod_{i=1}^N \left\{ f_s \exp \left(F_s \sum_{\alpha=1}^n S_i^\alpha \right) + (1 - f_s) \exp \left(-F_s \sum_{\alpha=1}^n S_i^\alpha \right) \right\} \quad (\text{A.5})$$

などを得る. 問題なのはスパーステンソル D の処理であるが, Wong-Sherrington の方法に従えば

$$\begin{aligned} &\left\langle \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \prod_{\alpha=1}^n \left\{ 1 + \frac{1}{2} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha - 1) \right\} \right\rangle_D \\ &= N^{-1} \sum_D \prod_{i=1}^N \delta \left(\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} - C \right) \prod_{j=1}^M \delta \left(\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} - L \right) \\ &\times \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \prod_{\alpha=1}^n \left\{ 1 + \frac{1}{2} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha - 1) \right\} \end{aligned} \quad (\text{A.6})$$

を評価することができる. ただし

$$N = \sum_D \prod_{i=1}^N \delta \left(\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} - C \right) \prod_{j=1}^M \delta \left(\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} - L \right) \quad (\text{A.7})$$

は規格化定数である。規格化定数 N を評価するには、まず Kronecker の δ 関数が

$$\delta(x) = \int_0^{2\pi} \frac{d\lambda}{2\pi} e^{i\lambda x} \quad (\text{A.8})$$

と積分表示できることを利用する。すると (A.7) は

$$\begin{aligned} N &= \sum_D \prod_{i=1}^N \delta \left(\sum_{\langle i_2, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_2, \dots, i_K; j_1, \dots, j_L \rangle} - C \right) \prod_{j=1}^M \delta \left(\sum_{\langle i_1, \dots, i_K; j_2, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_2, \dots, j_L \rangle} - L \right) \\ &= \sum_D \prod_{i=1}^N \left\{ \int_0^{2\pi} \frac{d\lambda_i}{2\pi} \exp \left[i\lambda_i \left(\sum_{\langle i_2, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_2, \dots, i_K; j_1, \dots, j_L \rangle} - C \right) \right] \right\} \\ &\quad \times \prod_{j=1}^M \left\{ \int_0^{2\pi} \frac{d\lambda_j}{2\pi} \exp \left[i\lambda_j \left(\sum_{\langle i_1, \dots, i_K; j_2, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_2, \dots, j_L \rangle} - L \right) \right] \right\} \\ &= \prod_{i=1}^N \left\{ \int_0^{2\pi} \frac{d\lambda_i}{2\pi} e^{-iC\lambda_i} \right\} \prod_{j=1}^M \left\{ \int_0^{2\pi} \frac{d\lambda_j}{2\pi} e^{-iL\lambda_j} \right\} \\ &\quad \times \sum_D \prod_{i=1}^N \left\{ \prod_{\langle i_2, \dots, i_K; j_1, \dots, j_L \rangle} e^{i\lambda_i D_{\langle i_2, \dots, i_K; j_1, \dots, j_L \rangle}} \right\} \prod_{j=1}^M \left\{ \prod_{\langle i_1, \dots, i_K; j_2, \dots, j_L \rangle} e^{i\lambda_j D_{\langle i_1, \dots, i_K; j_2, \dots, j_L \rangle}} \right\} \\ &= \prod_{i=1}^N \left\{ \int_0^{2\pi} \frac{d\lambda_i}{2\pi} e^{-iC\lambda_i} \right\} \prod_{j=1}^M \left\{ \int_0^{2\pi} \frac{d\lambda_j}{2\pi} e^{-iL\lambda_j} \right\} \\ &\quad \times \sum_D \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \left\{ (e^{i\lambda_{i_1}} \dots e^{i\lambda_{i_K}} e^{i\lambda_{j_1}} \dots e^{i\lambda_{j_L}})^{D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle}} \right\} \end{aligned} \quad (\text{A.9})$$

と表現できる。さらに $Z_i = e^{i\lambda_i}$, $Y_j = e^{i\lambda_j}$ などと置いて置換積分を実行すれば

$$\begin{aligned} N &= \prod_{i=1}^N \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \prod_{j=1}^M \left\{ \oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \right\} \sum_D \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \left\{ (Z_{i_1} \dots Z_{i_K} Y_{j_1} \dots Y_{j_L})^{D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle}} \right\} \\ &= \prod_{i=1}^N \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \prod_{j=1}^M \left\{ \oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \right\} \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (1 + Z_{i_1} \dots Z_{i_K} Y_{j_1} \dots Y_{j_L}) \end{aligned} \quad (\text{A.10})$$

を得る。このとき、熱力学的極限では

$$\begin{aligned} &\prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} [1 + (Z_{i_1} \dots Z_{i_K} \cdot Y_{j_1} \dots Y_{j_L})] \\ &= \exp \left[\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \ln \{1 + (Z_{i_1} \dots Z_{i_K} \cdot Y_{j_1} \dots Y_{j_L})\} \right] \\ &= \exp \left[\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (Z_{i_1} \dots Z_{i_K} \cdot Y_{j_1} \dots Y_{j_L}) + (\text{高次項}) \right] \end{aligned} \quad (\text{A.11})$$

と展開して高次項が無視できる。すると

$$N = \prod_{i=1}^N \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \prod_{j=1}^M \left\{ \oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \right\} \exp \left(\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} Z_{i_1} \dots Z_{i_K} Y_{j_1} \dots Y_{j_L} \right) \quad (\text{A.12})$$

となる。さらに

$$\frac{1}{K!} \left(\sum_{i=1}^N Z_i \right)^K = \sum_{\langle i_1, \dots, i_K \rangle} Z_{i_1} \dots Z_{i_K} + (\text{低次項}) \quad (\text{A.13})$$

$$\frac{1}{L!} \left(\sum_{j=1}^M Y_j \right)^L = \sum_{\langle j_1, \dots, j_L \rangle} Y_{j_1} \dots Y_{j_L} + (\text{低次項}) \quad (\text{A.14})$$

と展開したとき、熱力学的極限では低次項の貢献が無視できる。よって

$$N = \prod_{i=1}^N \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \prod_{j=1}^M \left\{ \oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \right\} \exp \left[\frac{1}{K!} \left(\sum_{i=1}^N Z_i \right)^K \frac{1}{L!} \left(\sum_{j=1}^M Y_j \right)^L \right] \quad (\text{A.15})$$

となる。ここで、恒等式

$$1 = \int dq \delta \left(\sum_{i=1}^N Z_i - q \right) \quad (\text{A.16})$$

$$1 = \int dr \delta \left(\sum_{j=1}^M Y_j - r \right) \quad (\text{A.17})$$

を利用して、 δ 関数を積分表示すれば

$$\begin{aligned} N &= \int dq \delta \left(\sum_{i=1}^N Z_i - q \right) \int dr \delta \left(\sum_{j=1}^M Y_j - r \right) \prod_{i=1}^N \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \prod_{j=1}^M \left\{ \oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \right\} \exp \left(\frac{q^K}{K!} \frac{r^L}{L!} \right) \\ &= \int dq \int \frac{d\hat{q}}{2\pi i} \exp \left[\hat{q} \left(\sum_{i=1}^N Z_i - q \right) \right] \int dr \int \frac{d\hat{r}}{2\pi i} \exp \left[\hat{r} \left(\sum_{j=1}^M Y_j - r \right) \right] \\ &\quad \times \prod_{i=1}^N \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \prod_{j=1}^M \left\{ \oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \right\} \exp \left(\frac{q^K}{K!} \frac{r^L}{L!} \right) \\ &= \int dq \int \frac{d\hat{q}}{2\pi i} \int dr \int \frac{d\hat{r}}{2\pi i} \exp \left(\frac{q^K}{K!} \frac{r^L}{L!} - q\hat{q} - r\hat{r} \right) \prod_{i=1}^N \left[\oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \exp(\hat{q}Z_i) \right] \prod_{j=1}^M \left[\oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \exp(\hat{r}Y_j) \right] \end{aligned} \quad (\text{A.18})$$

となる。複素積分を実行すると

$$\prod_{i=1}^N \left[\oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \exp(\hat{q}Z_i) \right] = \left(\frac{\hat{q}^C}{C!} \right)^N \quad (\text{A.19})$$

$$\prod_{j=1}^M \left[\oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \exp(\hat{r}Y_j) \right] = \left(\frac{\hat{r}^L}{L!} \right)^M \quad (\text{A.20})$$

となるので

$$N = \text{extr}_{\{q, \hat{q}, r, \hat{r}\}} \left\{ \exp \left[\frac{q^K}{K!} \frac{r^L}{L!} - q\hat{q} - r\hat{r} + NC \ln \hat{q} - N \ln(C!) + ML \ln \hat{r} - M \ln(L!) \right] \right\} \quad (\text{A.21})$$

を得る。このとき、鞍点条件より

$$q = \frac{NC}{\hat{q}} \quad (\text{A.22})$$

$$\hat{q} = \frac{q^{K-1}}{(K-1)!} \frac{r^L}{L!} \quad (\text{A.23})$$

$$r = \frac{ML}{\hat{r}} \quad (\text{A.24})$$

$$\hat{r} = \frac{r^{L-1}}{(L-1)!} \frac{q^K}{K!} \quad (\text{A.25})$$

が成立しているので、規格化定数は結局

$$N = \left(\frac{\hat{q}^C}{C!} \right)^N \left(\frac{\hat{r}^L}{L!} \right)^M \exp \left(\frac{q^K}{K!} \frac{r^L}{L!} - q\hat{q} - r\hat{r} \right) \quad (\text{A.26})$$

となる。

規格化定数 N の計算と同じ方針で, (A.6) を評価できる. 実際

$$\begin{aligned}
 & \left\langle \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \prod_{\alpha=1}^n \left\{ 1 + \frac{1}{2} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha - 1) \right\} \right\rangle_D \\
 &= N^{-1} \sum_D \prod_{i=1}^N \delta \left(\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} - C \right) \prod_{j=1}^M \delta \left(\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} - L \right) \\
 & \quad \times \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \prod_{\alpha=1}^n \left\{ 1 + \frac{1}{2} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha - 1) \right\} \\
 &= N^{-1} \sum_D \prod_{i=1}^N \int \frac{d\lambda_i}{2\pi} \exp \left[i\lambda_i \left(\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} - C \right) \right] \\
 & \quad \times \prod_{j=1}^M \int \frac{d\lambda_j}{2\pi} \exp \left[i\lambda_j \left(\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} - L \right) \right] \\
 & \quad \times \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \prod_{\alpha=1}^n \left\{ 1 + \frac{1}{2} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha - 1) \right\} \\
 &= N^{-1} \sum_D \prod_{i=1}^N \left\{ \int \frac{d\lambda_i}{2\pi} e^{-iC\lambda_i} \right\} \prod_{j=1}^M \left\{ \int \frac{d\lambda_j}{2\pi} e^{-iL\lambda_j} \right\} \\
 & \quad \times \prod_{i=1}^N \left\{ \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} e^{-i\lambda_i D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle}} \right\} \prod_{j=1}^M \left\{ \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} e^{-i\lambda_j D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle}} \right\} \\
 & \quad \times \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \prod_{\alpha=1}^n \left\{ 1 + \frac{1}{2} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha - 1) \right\} \\
 &= N^{-1} \sum_D \prod_{i=1}^N \left\{ \int \frac{d\lambda_i}{2\pi} e^{-iC\lambda_i} \right\} \prod_{j=1}^M \left\{ \int \frac{d\lambda_j}{2\pi} e^{-iL\lambda_j} \right\} \\
 & \quad \times \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (e^{-i\lambda_{i_1}} \cdots e^{-i\lambda_{i_K}} e^{-i\lambda_{j_1}} \cdots e^{-i\lambda_{j_L}})^{D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle}} \\
 & \quad \times \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \prod_{\alpha=1}^n \left\{ 1 + \frac{1}{2} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha - 1) \right\} \tag{A.27}
 \end{aligned}$$

となるので, $Z_i = e^{i\lambda_i}$, $Y_j = e^{i\lambda_j}$ などと置いて積分変数を変換すれば

$$\begin{aligned}
 & \left\langle \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \prod_{\alpha=1}^n \left\{ 1 + \frac{1}{2} D_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha - 1) \right\} \right\rangle_D \\
 &= N^{-1} \prod_{i=1}^N \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \prod_{j=1}^M \left\{ \oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \right\} \\
 & \quad \times \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \left[1 + (Z_{i_1} \cdots Z_{i_K} \cdot Y_{j_1} \cdots Y_{j_L}) \prod_{\alpha=1}^n \frac{1}{2} (1 + S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha) \right] \tag{A.28}
 \end{aligned}$$

を得るのはそんなに難しいことではない. 規格化定数のときと同様に, 熱力学的極限では

$$\begin{aligned}
 & \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \left[1 + (Z_{i_1} \cdots Z_{i_K} \cdot Y_{j_1} \cdots Y_{j_L}) \prod_{\alpha=1}^n \frac{1}{2} (1 + S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha) \right] \\
 &= \exp \left[\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \ln \left\{ 1 + (Z_{i_1} \cdots Z_{i_K} \cdot Y_{j_1} \cdots Y_{j_L}) \prod_{\alpha=1}^n \frac{1}{2} (1 + S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha) \right\} \right] \\
 &= \exp \left[\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} (Z_{i_1} \cdots Z_{i_K} \cdot Y_{j_1} \cdots Y_{j_L}) \prod_{\alpha=1}^n \frac{1}{2} (1 + S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha) + (\text{高次項}) \right] \tag{A.29}
 \end{aligned}$$

と展開したとき、高次項の貢献は無視できる。すると

$$\begin{aligned}
& \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \left[1 + (Z_{i_1} \cdots Z_{i_K} \cdot Y_{j_1} \cdots Y_{j_L}) \prod_{\alpha=1}^n \frac{1}{2} (1 + S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha) \right] \\
& \simeq \exp \left[\sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} Z_{i_1} \cdots Z_{i_K} \cdot Y_{j_1} \cdots Y_{j_L} \prod_{\alpha=1}^n \frac{1}{2} (1 + S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha) \right] \\
& = \exp \left[\frac{1}{2^n} \sum_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} Z_{i_1} \cdots Z_{i_K} \cdot Y_{j_1} \cdots Y_{j_L} \right. \\
& \quad \times \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} (S_{i_1}^{\alpha_1} \cdots S_{i_1}^{\alpha_m}) \cdots (S_{i_K}^{\alpha_1} \cdots S_{i_K}^{\alpha_m}) (\tau_{j_1}^{\alpha_1} \cdots \tau_{j_1}^{\alpha_m}) \cdots (\tau_{j_L}^{\alpha_1} \cdots \tau_{j_L}^{\alpha_m}) \left. \right] \\
& = \exp \left[\frac{1}{2^n} \left\{ \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} \sum_{\langle i_1, \dots, i_K \rangle} (S_{i_1}^{\alpha_1} \cdots S_{i_1}^{\alpha_m} Z_{i_1}) \cdots (S_{i_K}^{\alpha_1} \cdots S_{i_K}^{\alpha_m} Z_{i_K}) \right. \right. \\
& \quad \times \sum_{\langle j_1, \dots, j_L \rangle} (\tau_{j_1}^{\alpha_1} \cdots \tau_{j_1}^{\alpha_m} Y_{j_1}) \cdots (\tau_{j_L}^{\alpha_1} \cdots \tau_{j_L}^{\alpha_m} Y_{j_L}) \left. \left. \right\} \right] \tag{A.30}
\end{aligned}$$

となる。ただし

$$\begin{aligned}
& \prod_{\alpha=1}^n (1 + S_{i_1}^\alpha \cdots S_{i_K}^\alpha \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha) \\
& = 1 + \sum_{\alpha=1}^n S_{i_1}^\alpha \cdots S_{i_K}^\alpha \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha + \sum_{\langle \alpha_1, \alpha_2 \rangle} (S_{i_1}^{\alpha_1} S_{i_1}^{\alpha_2}) \cdots (S_{i_K}^{\alpha_1} S_{i_K}^{\alpha_2}) (\tau_{j_1}^{\alpha_1} \tau_{j_1}^{\alpha_2}) \cdots (\tau_{j_L}^{\alpha_1} \tau_{j_L}^{\alpha_2}) \\
& \quad + \cdots + \sum_{\langle \alpha_1, \dots, \alpha_n \rangle} (S_{i_1}^{\alpha_1} \cdots S_{i_1}^{\alpha_n}) \cdots (S_{i_K}^{\alpha_1} \cdots S_{i_K}^{\alpha_n}) (\tau_{j_1}^{\alpha_1} \cdots \tau_{j_1}^{\alpha_n}) \cdots (\tau_{j_L}^{\alpha_1} \cdots \tau_{j_L}^{\alpha_n}) \\
& = \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} (S_{i_1}^{\alpha_1} \cdots S_{i_1}^{\alpha_m}) \cdots (S_{i_K}^{\alpha_1} \cdots S_{i_K}^{\alpha_m}) (\tau_{j_1}^{\alpha_1} \cdots \tau_{j_1}^{\alpha_m}) \cdots (\tau_{j_L}^{\alpha_1} \cdots \tau_{j_L}^{\alpha_m}) \tag{A.31}
\end{aligned}$$

と展開したことに注意する。さらに

$$\frac{1}{K!} \left(\sum_{i=1}^N S_i^{\alpha_1} \cdots S_i^{\alpha_m} Z_i \right)^K = \sum_{\langle i_1, \dots, i_K \rangle} (S_{i_1}^{\alpha_1} \cdots S_{i_1}^{\alpha_m} Z_{i_1}) \cdots (S_{i_K}^{\alpha_1} \cdots S_{i_K}^{\alpha_m} Z_{i_K}) + (\text{低次項}) \tag{A.32}$$

と展開したとき、やはり熱力学的極限では低次項の貢献は無視できることに注目する。

$$\begin{aligned}
& \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \left[1 + (Z_{i_1} \cdots Z_{i_K} \cdot Y_{j_1} \cdots Y_{j_L}) \prod_{\alpha=1}^n \frac{1}{2} (1 + S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha) \right] \\
& = \exp \left[\frac{1}{2^n} \left\{ \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} \sum_{\langle i_1, \dots, i_K \rangle} (S_{i_1}^{\alpha_1} \cdots S_{i_1}^{\alpha_m} Z_{i_1}) \cdots (S_{i_K}^{\alpha_1} \cdots S_{i_K}^{\alpha_m} Z_{i_K}) \right. \right. \\
& \quad \times \sum_{\langle j_1, \dots, j_L \rangle} (\tau_{j_1}^{\alpha_1} \cdots \tau_{j_1}^{\alpha_m} Y_{j_1}) \cdots (\tau_{j_L}^{\alpha_1} \cdots \tau_{j_L}^{\alpha_m} Y_{j_L}) \left. \left. \right\} \right] \\
& \simeq \exp \left[\frac{1}{2^n} \left\{ \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} \sum_{\langle i_1, \dots, i_K \rangle} \frac{1}{K!} \left(\sum_{i=1}^N S_i^{\alpha_1} \cdots S_i^{\alpha_m} Z_i \right)^K \sum_{\langle j_1, \dots, j_L \rangle} \frac{1}{L!} (\tau_{j_1}^{\alpha_1} \cdots \tau_{j_L}^{\alpha_m} Y_{j_1} \cdots Y_{j_L})^L \right\} \right] \tag{A.33}
\end{aligned}$$

そして、恒等式

$$1 = \int dq_{\alpha_1, \dots, \alpha_m} \delta \left(\sum_{i=1}^N S_i^{\alpha_1} \cdots S_i^{\alpha_m} Z_i - q_{\alpha_1, \dots, \alpha_m} \right) \tag{A.34}$$

$$1 = \int dr_{\alpha_1, \dots, \alpha_m} \delta \left(\sum_{j=1}^M \tau_j^{\alpha_1} \cdots \tau_j^{\alpha_m} Y_j - r_{\alpha_1, \dots, \alpha_m} \right) \tag{A.35}$$

を利用して、鞍点法を適用すれば

$$\begin{aligned}
 & \prod_{\langle i_1, \dots, i_K; j_1, \dots, j_L \rangle} \left[1 + (Z_{i_1} \cdots Z_{i_K} \cdot Y_{j_1} \cdots Y_{j_L}) \prod_{\alpha=1}^n \frac{1}{2} (1 + S_{i_1}^\alpha \cdots S_{i_K}^\alpha \cdot \tau_{j_1}^\alpha \cdots \tau_{j_L}^\alpha) \right] \\
 &= \prod_{m=0}^n \prod_{\langle \alpha_1, \dots, \alpha_m \rangle} \int dq_{\alpha_1, \dots, \alpha_m} \delta \left(\sum_{i=1}^N S_i^{\alpha_1} \cdots S_i^{\alpha_m} Z_i - q_{\alpha_1, \dots, \alpha_m} \right) \int dr_{\alpha_1, \dots, \alpha_m} \delta \left(\sum_{j=1}^M \tau_j^{\alpha_1} \cdots \tau_j^{\alpha_m} Y_j - r_{\alpha_1, \dots, \alpha_m} \right) \\
 &\quad \times \exp \left[\frac{1}{2^n} \left\{ \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} \frac{q_{\alpha_1, \dots, \alpha_m}^K}{K!} \frac{r_{\alpha_1, \dots, \alpha_m}^L}{L!} \right\} \right] \\
 &\simeq \text{extr}_{\{q, \hat{q}, r, \hat{r}\}} \left\{ \exp \left[\frac{1}{2^n} \left\{ \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} \frac{q_{\alpha_1, \dots, \alpha_m}^K}{K!} \frac{r_{\alpha_1, \dots, \alpha_m}^L}{L!} \right\} \right. \right. \\
 &\quad - \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} q_{\alpha_1, \dots, \alpha_m} \hat{q}_{\alpha_1, \dots, \alpha_m} - \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} r_{\alpha_1, \dots, \alpha_m} \hat{r}_{\alpha_1, \dots, \alpha_m} \\
 &\quad \left. \left. + \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} \hat{q}_{\alpha_1, \dots, \alpha_m} \sum_{i=1}^N S_i^{\alpha_1} \cdots S_i^{\alpha_m} Z_i + \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} \hat{r}_{\alpha_1, \dots, \alpha_m} \sum_{j=1}^M \tau_j^{\alpha_1} \cdots \tau_j^{\alpha_m} Y_j \right\} \right] \quad (\text{A.36})
 \end{aligned}$$

となっている。ここで、さらなる工夫が必要になる。秩序変数が多数出現したので、それらを無限自由度を持つ関数で表現する。このとき、レプリカ対称性を仮定して秩序関数 $\pi(x), \hat{\pi}(\hat{x}), \rho(x), \hat{\rho}(\hat{x})$ を

$$q_{\alpha_1, \dots, \alpha_m} = q \int dx \pi(x) x^l \quad (\text{A.37})$$

$$\hat{q}_{\alpha_1, \dots, \alpha_m} = \hat{q} \int d\hat{x} \hat{\pi}(\hat{x}) \hat{x}^l \quad (\text{A.38})$$

$$r_{\alpha_1, \dots, \alpha_m} = r \int dy \rho(y) y^l \quad (\text{A.39})$$

$$\hat{r}_{\alpha_1, \dots, \alpha_m} = \hat{r} \int d\hat{y} \hat{\rho}(\hat{y}) \hat{y}^l \quad (\text{A.40})$$

が満たされる $[-1, 1]$ 上の分布関数として導入する。このとき

$$\begin{aligned}
 \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} \frac{q_{\alpha_1, \dots, \alpha_m}^K}{K!} \frac{r_{\alpha_1, \dots, \alpha_m}^L}{L!} &= \frac{q^K}{K!} \frac{r^L}{L!} \sum_{m=0}^n \binom{n}{m} \int \prod_{k=1}^K dx_k \pi(x_k) x_k^m \int \prod_{l=1}^L dy_l \rho(y_l) y_l^m \\
 &= \frac{q^K}{K!} \frac{r^L}{L!} \prod_{k=1}^K \int dx_k \pi(x_k) \prod_{l=1}^L \int dy_l \rho(y_l) \left(1 + \prod_{k=1}^K x_k \prod_{l=1}^L y_l \right)^n \quad (\text{A.41})
 \end{aligned}$$

$$\begin{aligned}
 \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} q_{\alpha_1, \dots, \alpha_m} \hat{q}_{\alpha_1, \dots, \alpha_m} &= q \hat{q} \sum_{m=0}^n \binom{n}{m} \int dx d\hat{x} \pi(x) \hat{\pi}(\hat{x}) x^m \hat{x}^m \\
 &= q \hat{q} \int dx d\hat{x} \pi(x) \hat{\pi}(\hat{x}) (1 + x \hat{x})^n \quad (\text{A.42})
 \end{aligned}$$

$$\begin{aligned}
 \sum_{m=0}^n \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} \hat{q}_{\alpha_1, \dots, \alpha_m} \sum_{i=1}^N S_i^{\alpha_1} \cdots S_i^{\alpha_m} Z_i &= \hat{q} \sum_{i=1}^N Z_i \int d\hat{x} \hat{\pi}(\hat{x}) \sum_{m=0}^n \hat{x}^m \sum_{\langle \alpha_1, \dots, \alpha_m \rangle} S_i^{\alpha_1} \cdots S_i^{\alpha_m} \\
 &= \hat{q} \sum_{i=1}^N Z_i \int d\hat{x} \hat{\pi}(\hat{x}) \prod_{\alpha=1}^n (1 + S_i^\alpha \hat{x}) \quad (\text{A.43})
 \end{aligned}$$

などが成立する。すると、式(A.4)は結局

$$\begin{aligned}
& \langle V(\xi, \zeta, D)^n \rangle_{\xi, \zeta, D} \\
&= \sum_{s^1 \dots s^n} \sum_{1 \dots n} \prod_{i=1}^N \left\{ f_s \exp \left(F_s \sum_{\alpha=1}^n S_i^\alpha \right) + (1 - f_s) \exp \left(-F_s \sum_{\alpha=1}^n S_i^\alpha \right) \right\} \\
&\quad \times \prod_{j=1}^M \left\{ f_n \exp \left(F_n \sum_{\alpha=1}^n \tau_j^\alpha \right) + (1 - f_n) \exp \left(-F_n \sum_{\alpha=1}^n \tau_j^\alpha \right) \right\} \\
&\quad \times N^{-1} \prod_{i=1}^N \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \prod_{j=1}^M \left\{ \oint \frac{dY_j}{2\pi i} Y_j^{-(L+1)} \right\} \\
&\quad \times \text{extr}_{\{\pi, \hat{\pi}, \rho, \hat{\rho}\}} \left\{ \exp \left[\frac{1}{2^n} \left\{ \frac{q^K}{K!} \frac{r^L}{L!} \int \prod_{l=1}^K dx_l \pi(x_l) \int \prod_{l=1}^L dy_l \rho(y_l) \left(1 + \prod_{l=1}^K x_l \prod_{l=1}^L y_l \right)^n \right. \right. \right. \\
&\quad \left. \left. - q\hat{q} \int dx d\hat{x} \pi(x) \hat{\pi}(\hat{x}) (1 + x\hat{x})^n - r\hat{r} \int dy d\hat{y} \rho(y) \hat{\rho}(\hat{y}) (1 + y\hat{y})^n \right. \right. \\
&\quad \left. \left. + \hat{q} \sum_{i=1}^N Z_i \int d\hat{x} \hat{\pi}(\hat{x}) \prod_{\alpha=1}^n (1 + S_i^\alpha \hat{x}) + \hat{r} \sum_{j=1}^M Y_j \int d\hat{y} \hat{\rho}(\hat{y}) \prod_{\alpha=1}^n (1 + \tau_j^\alpha \hat{y}) \right] \right\} \quad (\text{A.44})
\end{aligned}$$

と書ける。ここまで整理できたら、状態和をとって

$$\begin{aligned}
& \sum_{s^1 \dots s^n} \prod_{i=1}^N \left\{ f_s \exp \left(F_s \sum_{\alpha=1}^n S_i^\alpha \right) + (1 - f_s) \exp \left(-F_s \sum_{\alpha=1}^n S_i^\alpha \right) \right\} \prod_{i=1}^N \left\{ \oint \frac{dZ_i}{2\pi i} Z_i^{-(C+1)} \right\} \\
&\quad \times \exp \left[\hat{q} \sum_{i=1}^N Z_i \int d\hat{x} \hat{\pi}(\hat{x}) \prod_{\alpha=1}^n (1 + S_i^\alpha \hat{x}) \right] \\
&= \left(\frac{\hat{q}^C}{C!} \int \prod_{l=1}^C d\hat{x}_l \hat{\pi}(\hat{x}_l) \left\langle \prod_{\alpha=1}^n \left\{ e^{\xi F_s} \prod_{l=1}^C (1 + \hat{x}_l) + e^{-\xi F_s} \prod_{l=1}^C (1 - \hat{x}_l) \right\} \right\rangle_{\xi} \right)^N \quad (\text{A.45})
\end{aligned}$$

などどすることができる。レプリカトリックを認めると、簡単に分配関数の対数のランダム平均

$$\begin{aligned}
& \frac{1}{N} \langle \ln V(\xi, \tau, D\pi, \hat{\pi}, \rho, \hat{\rho}) \rangle_{\xi, \zeta, D} \\
&= \text{extr}_{\{\pi, \hat{\pi}, \rho, \hat{\rho}\}} \left\{ \frac{1}{N} \exp \left[-NC \left\{ \int dx d\hat{x} \pi(x) \hat{\pi}(\hat{x}) \ln(1 + x\hat{x})^n - 1 \right\} - ML \left\{ \int dy d\hat{y} \rho(y) \hat{\rho}(\hat{y}) \ln(1 + y\hat{y})^n - 1 \right\} \right. \right. \\
&\quad \left. \left. + \frac{1}{2^n} \left\{ \frac{NC}{K} \int \left[\prod_{k=1}^K dx_k \pi(x_k) \right] \left[\prod_{l=1}^L dy_l \rho(y_l) \right] \ln \left[1 + \prod_{k=1}^K x_k \prod_{l=1}^L y_l \right]^n - 1 \right\} \right] \right. \\
&\quad \times \left(\int \left[\prod_{k=1}^C d\hat{x}_k \hat{\pi}(\hat{x}_k) \right] \left\langle \left(\left[e^{F_s \xi} \prod_{k=1}^C (1 + \hat{x}_k) + e^{-F_s \xi} \prod_{k=1}^C (1 - \hat{x}_k) \right] \right)^n \right\rangle_{\xi} \right)^N \\
&\quad \times \left(\int \left[\prod_{l=1}^C d\hat{y}_l \hat{\rho}(\hat{y}_l) \right] \left\langle \left(\left[e^{F_r \zeta} \prod_{l=1}^C (1 + \hat{y}_l) + e^{-F_r \zeta} \prod_{l=1}^C (1 - \hat{y}_l) \right] \right)^n \right\rangle_{\zeta} \right)^N \quad (\text{A.46})
\end{aligned}$$

が求まるので、エントロピー密度は

$$\begin{aligned}
 & \frac{1}{N} \langle \ln V(D, \xi, \tau, \pi, \hat{\pi}, \rho, \hat{\rho}) \rangle_{\xi, \zeta, D} \\
 &= -\frac{C}{K} \ln 2 - C \int dx d\hat{x} \pi(x) \hat{\pi}(\hat{x}) \ln(1 + x\hat{x}) - \frac{CL}{K} \int dy d\hat{y} \rho(y) \hat{\rho}(\hat{y}) \ln(1 + y\hat{y}) \\
 &+ \frac{C}{K} \int \left[\prod_{k=1}^K dx_k \pi(x_k) \right] \left[\prod_{l=1}^L dy_l \rho(y_l) \right] \ln \left[1 + \prod_{k=1}^K x_k \prod_{l=1}^L y_l \right] \\
 &+ \int \left[\prod_{k=1}^C d\hat{x}_k \hat{\pi}(\hat{x}_k) \right] \left\langle \ln \left[e^{Fs\xi} \prod_{k=1}^C (1 + \hat{x}_k) + e^{-Fs\xi} \prod_{k=1}^C (1 - \hat{x}_k) \right] \right\rangle_{\xi} \\
 &+ \frac{C}{K} \int \left[\prod_{l=1}^C d\hat{y}_l \hat{\rho}(\hat{y}_l) \right] \left\langle \ln \left[e^{F\tau\zeta} \prod_{l=1}^C (1 + \hat{y}_l) + e^{-F\tau\zeta} \prod_{l=1}^C (1 - \hat{y}_l) \right] \right\rangle_{\zeta}
 \end{aligned} \tag{A.47}$$

となる。

B 平均場近似によるエントロピーの評価

ハミルトニアン(4.1)より、小正準分布の分配関数として

$$V(J) = \sum_{S,} \prod_{\mu=1}^M \Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right) \prod_{i=1}^N e^{F_S S_i} \prod_{j=1}^M e^{F_{\tau} \tau_j} \tag{B.1}$$

を採用してよい。ただし $I(\mu)$ はボンド J の第 μ 成分 J_{μ} を構成するメッセージビットの指標の集合、 $J(\mu)$ はノイズビットの指標の集合であった。このとき、任意の確率分布 $\hat{P}_{\mu}(S, \tau)$ について

$$\begin{aligned}
 V(J) &= \sum_{S,} \prod_{\mu=1}^M \Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right) \prod_{i=1}^N e^{F_S S_i} \prod_{j=1}^M e^{F_{\tau} \tau_j} \\
 &= \sum_{S,} \frac{\prod_{\mu=1}^M \Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\prod_{\mu=1}^M \hat{P}_{\mu}(S, \tau)} \frac{\prod_{\mu=1}^M \hat{P}_{\mu}(S, \tau)}{\sum_{\{S, \tau\}} \prod_{\mu=1}^M \hat{P}_{\mu}(S, \tau)} \sum_{S,} \prod_{\mu=1}^M \hat{P}_{\mu}(S, \tau) \prod_{i=1}^N e^{F_S \xi_i S_i} \prod_{j=1}^M e^{F_{\tau} \zeta_j \tau_j} \\
 &= \left\langle \prod_{\mu=1}^M \frac{\Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}_{\mu}(S, \tau)} \right\rangle_{\hat{P}} \sum_{S,} \prod_{\mu=1}^M \hat{P}_{\mu}(S, \tau) \prod_{i=1}^N e^{F_S S_i} \prod_{j=1}^M e^{F_{\tau} \tau_j}
 \end{aligned} \tag{B.2}$$

が厳密に成立する。ただし、平均 $\langle \dots \rangle_{\hat{P}}$ を

$$\langle \dots \rangle_{\hat{P}} = \frac{\sum_{S,} \dots \prod_{\mu=1}^M \hat{P}_{\mu}(S, \tau)}{\sum_{S,} \prod_{\mu=1}^M \hat{P}_{\mu}(S, \tau)} \tag{B.3}$$

と定義した。このとき

$$\begin{aligned}
& \left\langle \prod_{\mu=1}^M \frac{\Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}_{\mu}(S, \tau)} \right\rangle_{\hat{P}} \\
&= \left\langle \prod_{\mu=1}^M \left(\left\langle \frac{\Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}(S, \tau)} \right\rangle_{\hat{P}} \right. \right. \\
&\quad \left. \left. + \left(\frac{\Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}(S, \tau)} - \left\langle \frac{\Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}(S, \tau)} \right\rangle_{\hat{P}} \right) \right) \right\rangle_{\hat{P}} \\
&= \left\langle \prod_{\mu=1}^M \left(\left\langle \frac{\Theta_{\mu}}{\hat{P}_{\mu}} \right\rangle_{\hat{P}} + \Delta_{\mu} \right) \right\rangle_{\hat{P}} \\
&= \prod_{\mu=1}^M \left\langle \frac{\Theta_{\mu}}{\hat{P}_{\mu}} \right\rangle_{\hat{P}} \times \left\langle \prod_{\mu=1}^M \left(1 + \frac{\Delta_{\mu}}{\left\langle \frac{\Theta_{\mu}}{\hat{P}_{\mu}} \right\rangle_{\hat{P}}} \right) \right\rangle_{\hat{P}} \\
&= \prod_{\mu=1}^M \left\langle \frac{\Theta_{\mu}}{\hat{P}_{\mu}} \right\rangle_{\hat{P}} \times \sum_{m=0}^M \sum_{\langle \mu_1, \dots, \mu_m \rangle} \frac{\langle \Delta_{\mu_1} \dots \Delta_{\mu_m} \rangle_{\hat{P}}}{\left\langle \frac{\Theta_{\mu_1}}{\hat{P}_{\mu_1}} \right\rangle_{\hat{P}} \dots \left\langle \frac{\Theta_{\mu_m}}{\hat{P}_{\mu_m}} \right\rangle_{\hat{P}}} \tag{B.4}
\end{aligned}$$

となるが、すべての次数 m に対して熱力学的極限で

$$\frac{\sum_{\langle \mu_1, \dots, \mu_m \rangle} \langle \Delta_{\mu_1} \dots \Delta_{\mu_m} \rangle_{\hat{P}}}{\binom{M}{m}} \xrightarrow{M \rightarrow \infty} 0 \tag{B.5}$$

が成立することを仮定すれば

$$\frac{1}{M} \ln \left\langle \prod_{\mu=1}^M \frac{\Theta_{\mu}}{\hat{P}_{\mu}} \right\rangle_{\hat{P}} = \frac{1}{M} \ln \prod_{\mu=1}^M \left\langle \frac{\Theta_{\mu}}{\hat{P}_{\mu}} \right\rangle_{\hat{P}} \tag{B.6}$$

が導かれる。ただし

$$\Theta_{\mu} = \Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right) \tag{B.7}$$

$$\hat{P}_{\mu} = \hat{P}_{\mu}(S, \tau) \tag{B.8}$$

$$\begin{aligned}
\Delta_{\mu} &= \frac{\Theta_{\mu}}{\hat{P}_{\mu}} - \left\langle \frac{\Theta_{\mu}}{\hat{P}_{\mu}} \right\rangle_{\hat{P}} \\
&= \frac{\Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}(S, \tau)} - \left\langle \frac{\Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right)}{\hat{P}(S, \tau)} \right\rangle_{\hat{P}} \tag{B.9}
\end{aligned}$$

と略記した。さらに

$$P_{\mu}(S, \tau) = \frac{\prod_{\nu \neq \mu} \hat{P}_{\nu}(S, \tau)}{\sum_{S, \tau} \prod_{\nu \neq \mu} \hat{P}_{\nu}(S, \tau)} \tag{B.10}$$

を定義して、 $P_{\mu} = P_{\mu}(S, \tau)$ と略記すると

$$\left\langle \frac{\Theta_{\mu}}{\hat{P}_{\mu}} \right\rangle_{\hat{P}} = \sum_{S, \tau} \frac{\Theta_{\mu}}{\hat{P}_{\mu}} \frac{\hat{P}_{\mu} \prod_{\nu \neq \mu} \hat{P}_{\nu}}{\sum_{S, \tau} \prod_{\nu=1}^M \hat{P}_{\nu}} = \frac{\sum_{S, \tau} \Theta_{\mu} \prod_{\nu \neq \mu} \hat{P}_{\nu}}{\sum_{S, \tau} \prod_{\nu=1}^M \hat{P}_{\nu}} = \frac{\sum_{S, \tau} \Theta_{\mu} P_{\mu}}{\sum_{S, \tau} P_{\mu}} \tag{B.11}$$

が成立する。このとき、(B.2) は

$$V(J) = \prod_{\mu=1}^M \frac{\left\langle \Theta \left(J_{\mu} \prod_{i \in I(\mu)} S_i \prod_{j \in J(\mu)} \tau_j \right) \right\rangle_{P_{\mu}}}{\left\langle \hat{P}_{\mu}(S, \tau) \right\rangle_{P_{\mu}}} \sum_{S, \tau} \prod_{\mu=1}^M \hat{P}_{\mu}(S, \tau) \prod_{i=1}^N e^{F_S S_i} \prod_{j=1}^M e^{F_{\tau} \tau_j} \tag{B.12}$$

となる。ただし、平均 $\langle \dots \rangle_{P_\mu}$ を

$$\langle \dots \rangle_{P_\mu} = \sum_{S_i} \dots P_\mu(S, \tau) \quad (\text{B.13})$$

と定義した。そして分布 P_μ , $\hat{P}_\mu$ がサイトの指標 i, j について独立な成分の積で近似できて (平均場近似)

$$P_\mu(S, \tau) = \prod_{i \in I(\mu)} \left(\frac{1 + S_i m_{\mu i}^S}{2} \right) \prod_{j \in J(\mu)} \left(\frac{1 + \tau_j m_{\mu j}^\tau}{2} \right) \quad (\text{B.14})$$

$$\hat{P}_\mu(S, \tau) = \prod_{i \in I(\mu)} \left(\frac{1 + S_i \hat{m}_{\mu i}^S}{2} \right) \prod_{j \in J(\mu)} \left(\frac{1 + \tau_j \hat{m}_{\mu j}^\tau}{2} \right) \quad (\text{B.15})$$

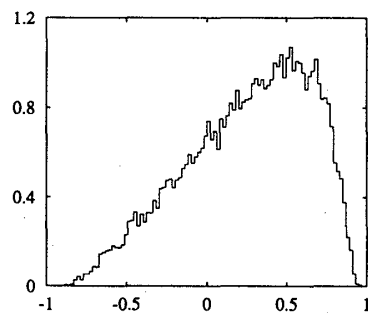
と表現できると仮定する。このとき、(B.14), (B.15) を (B.12) に代入し、エントロピー密度を計算すると

$$\begin{aligned} & \frac{\ln V(J)}{N} \\ &= \frac{1}{N} \sum_{\mu=1}^M \ln \left(\frac{1 + J_\mu \prod_{i \in I(\mu)} m_{\mu i}^S \prod_{j \in J(\mu)} m_{\mu j}^\tau}{2} \right) \\ & - \frac{1}{N} \sum_{\mu=1}^M \sum_{i \in I(\mu)} \ln \left(\frac{1 + m_{\mu i}^S \hat{m}_{\mu i}^S}{2} \right) \\ & - \frac{1}{N} \sum_{\mu=1}^M \sum_{j \in J(\mu)} \ln \left(\frac{1 + m_{\mu j}^\tau \hat{m}_{\mu j}^\tau}{2} \right) \\ & + \frac{1}{N} \sum_{i=1}^N \ln \left[e^{F_s} \prod_{\mu \in M(i)} \left(\frac{1 + \hat{m}_{\mu i}^S}{2} \right) + e^{-F_s} \prod_{\mu \in M(i)} \left(\frac{1 - \hat{m}_{\mu i}^S}{2} \right) \right] \\ & + \frac{1}{N} \sum_{j=1}^M \ln \left[e^{F_n} \prod_{\mu \in M(j)} \left(\frac{1 + \hat{m}_{\mu j}^\tau}{2} \right) + e^{-F_n} \prod_{\mu \in M(j)} \left(\frac{1 - \hat{m}_{\mu j}^\tau}{2} \right) \right] \end{aligned} \quad (\text{B.16})$$

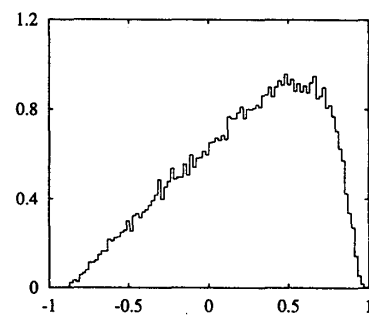
を得る。

C 秩序関数とパラメータ分布

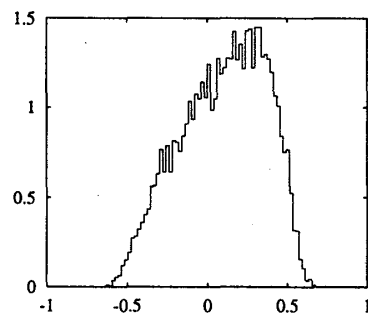
$K = L = 2, C = 4$ の場合に臨界点 (スピノーダル点 p_s) 近傍で求まる秩序関数をレプリカ法 (左) と TAP 方程式 (右) で数値的に評価した。レプリカ法による評価では、各々の秩序関数を区間 $[-1, 1]$ を 1001 個の短冊に分割したヒストグラムで表現し、1 ステップ 1000000 回の Monte-Carlo 法で鞍点方程式 (4.24)-(4.27) を 100000 回繰り返し評価して収束させた。TAP 方程式による評価では、 $N = 10000 (M = 20000)$ の系に対して西森条件を考慮した初期条件から 10000 回 TAP 方程式 (5.17)-(5.20) を繰り返し、収束解を求めた。



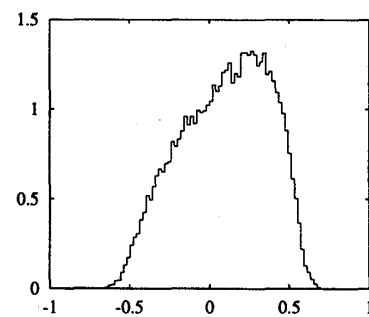
6.1: 秩序関数 $\pi(x)$



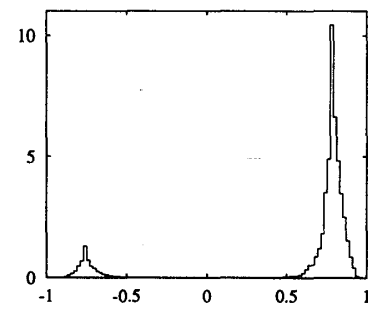
6.2: パラメータ分布 $P(m^S)$



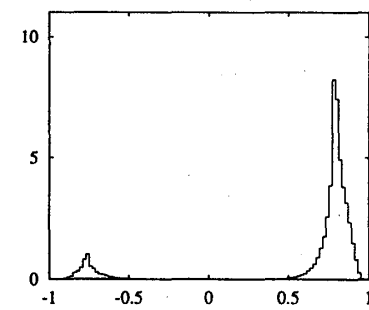
6.3: 秩序関数 $\pi(\hat{x})$



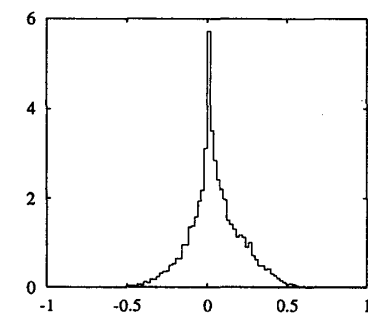
6.4: パラメータ分布 $P(\hat{m}^S)$



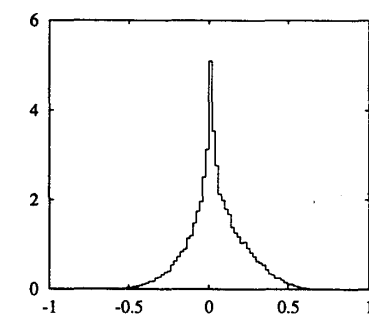
6.5: 秩序関数 $\rho(x)$



6.6: パラメータ分布 $P(m^T)$



6.7: 秩序関数 $\rho(\hat{x})$



6.8: パラメータ分布 $P(\hat{m}^T)$

図 6: 秩序関数とパラメータ分布