HOKKAIDO UNIVERSITY

Title	2005年度　混沌系工学特論講義ノート
Author(s)	井上, 純一
Issue Date	2005-11-30T05:17:27Z
Doc URL	http://hdl.handle.net/2115/828
Rights(URL)	http://creativecommons.org/licenses/by-nc-sa/2.1/jp/
Type	learningobject
Note	とりあげた各トピックスに関する最新情報は著者のホームページを参照ください。
Note(URL)	http://www005.upp.so-net.ne.jp/j_inoue/index.html; http://chaosweb.complex.eng.hokudai.ac.jp/~j_inoue/
Additional Information	There are other files related to this item in HUSCAP. Check the above URL.
File Information	konton2005_4.pdf (第4回講義ノート)

Instructions for use

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

混沌系工学特論 配布資料 #4

担当：井上 純一 (情報科学研究科棟 8-13)

URL：http://chaosweb.complex.eng.hokudai.ac.jp/~j_inoue/

Mirror：http://www005.upp.so-net.ne.jp/j_inoue/

平成 17 年 11 月 14 日

目 次

3 スピンモデルと誤り訂正符号 **38**

3.1 情報理論の復習：通信路符号化 39

3.2 雑音がある場合にデータ送信時の誤りを減らす方法 39

3.3 通信路容量 41

3.4 伝送速度と通信路容量 44

3.5 通信路符号化定理とその証明 44

3.5.1 ランダム符号 44

3.5.2 2 元対称通信路に対する通信路符号化定理の証明 45

3.6 スピングラスと誤り訂正符号 47

3.6.1 画像とパリティの同時送信による画像復元 47

3.6.2 パリティの転送とフラストレーション 49

3.6.3 Sourlas 符号 50

3.6.4 平均的性能評価 50

3.6.5 Sourlas 符号の状態方程式とその解析 51

3 スピンモデルと誤り訂正符号

ここまでで, 画像の復元問題を確率論に基づいて行う方法を説明してきた. ベイズ推定の立場からは, 欠落している原画像に関する情報を, 我々の持つ事前知識を事前分布に反映させることで補った. 特に, 2 値画像の場合には局所的には「黒」あるいは「白」のかたまりが現れやすく, このようなクラスタのつなぎ合わせで画像が構成されているという特徴をうまく使うことができた.

しかし, 我々が扱うデータの種類は何も画像だけではない. 画像のような 2 次元の幾何学的な構造を持たない単なるビット列をデータとして扱い, これを復元する場合もありうるであろう. この場合でも事前分布の選択は恣意的ではあるが, 「N ビットの組み合わせの総数 2^N のうちのどの配列 $\{\sigma\}$ 1 つをとっても, それは等確率で現れるはずである」言い方を換えれば「どの配列 $\{\sigma\}$ も, それが出現しやすいとみなせる積極的な理由を持たない」とするのが自然であろうから, $P(\{\sigma\}) = 2^{-N}$ と置くことになる. しかし, これをベイズの公式に代入してみるとわかるように, この事前分布は事後分布に何の影響も与えない. 従って, 我々は原データの欠落を何ら埋めることはできないということになる.

こうした場合, 情報理論では送信すべきデータを加工し, 余分な情報を付加させることにより, 受信者が誤りを検出し, それを訂正できるようなカラクリをシステムに導入する. こうしたデータの加工を**符号化 (encode)** と呼んでいる. 一方, 受信者が元のデータを復元することは**復号 (decode)** である. 先に学んだ画像復元の場合には符号化を特に行わなかった.[1] この部分がここから学ぶ「誤り訂正符号」と前節で学んだ「画像復元」の問題が大きくことなる点の一つである.

ここではまず, 学部で学んだ情報理論の簡単な復習から始める. 復習を必要としない者はすぐに **3.6 スピングラスと誤り訂正符号**に飛んでもよい.

3.1 情報理論の復習：通信路符号化

学部のときに学んだ情報理論における通信路符号化と誤り訂正符号の部分を簡単に復習しておくことにしょう.

3.2 雑音がある場合にデータ送信時の誤りを減らす方法

通信路が誤り確率 p の 2 元対称通信路であり, 送信する記号は $0, 1$ であるとする. 符号器はデータの 1 記号を n 回 (n は奇数) 繰り返して通信路に入力する. 復号器は通信路からの出力を受け取り, n 個の記号の中にある $0, 1$ のうち, 多い方の記号を出力する (つまり, 多数決をとる). このとき, 復号器の出力が符号器の入力と異なる確率は, 例えば $n = 5$ のとき

$$f_{\mathrm{e}}^{(5)}(p) \quad = \quad {}_5C_3 p^3(1-p)^2 + {}_5C_4 p^4(1-p) + p^5 \tag{117}$$

となり, この確率は $n = 7, 9, 11, \cdots$ と繰り返し送信数 n を増やすにつれ

$$f_{\mathrm{e}}^{(5)}(p) > f_{\mathrm{e}}^{(7)}(p) > f_{\mathrm{e}}^{(9)}(p) > f_{\mathrm{e}}^{(11)} > \cdots \tag{118}$$

のように減少していくことが予想される.

実際に $f_{\mathrm{e}}^{(n)}$ をいくつかの n の値に対して, p の関数として計算機でプロットしてみることにしょう. そこで, 具体的に $f_{\mathrm{e}}^{(n)}$ を p の関数として書き出してみると

$$\begin{aligned}
f_{\mathrm{e}}^{(3)}(p) &= 3p^2(1-p) + p^3 \\
f_{\mathrm{e}}^{(5)}(p) &= 10p^3(1-p)^2 + 5p^4(1-p) + p^5 \\
f_{\mathrm{e}}^{(7)}(p) &= 35p^4(1-p)^3 + 21p^5(1-p)^2 + 7p^6(1-p) + p^7 \\
f_{\mathrm{e}}^{(9)}(p) &= 126p^5(1-p)^4 + 84p^6(1-p)^3 + 36p^7(1-p)^2 + 9p^8(1-p) + p^9 \\
f_{\mathrm{e}}^{(11)}(p) &= 469p^6(1-p)^5 + 330p^7(1-p)^4 + 165p^8(1-p)^3 + 55p^9(1-p)^2 + 11p^{10}(1-p) + p^{11}
\end{aligned}$$

等となるので, これらをプロットする. 結果を図 22 に載せる.

(参考)：
ここで,　参考までに, $n \to \infty$ の極限では誤り率 $f_{\mathrm{e}}^{(n)}(p)$ が p の関数としてどのように振舞うのか, を見ておこう. $f_{\mathrm{e}}^{(n)}(p)$ は $n = 2m-1, m = 1, 2, \cdots$ と置き直すことにより

$$f_{\mathrm{e}}^{(m)}(p) \quad = \quad \sum_{l=m}^{2m-1} {}_{2m-1}C_l \; p^l (1-p)^{(2m-1)-l}$$

[1] 復元すべき画像の中には何千年も前の古代の文章もありうるわけで, こうした文献を復元する際に, 「実は古代人が余分な情報を加えておいてくれたはずだ」と考えるのはあまりにも不自然である.

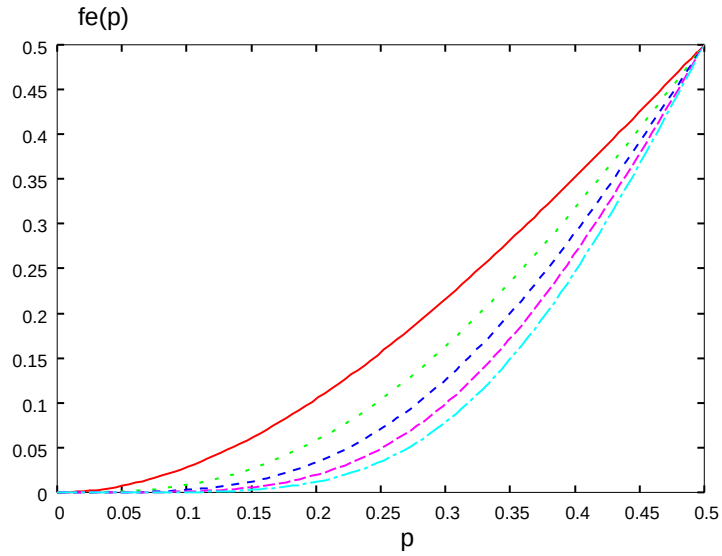

図 22: 誤り確率 $f_{\mathrm{e}}^{(n)}(p)$. 上から $n = 3, 5, 7, 9$, 及び, $n = 11$.

$$
\begin{aligned}
&= \sum_{l=0}^{2m-1} {}_{2m-1}C_l \; p^l (1-p)^{(2m-1)-l} - \sum_{l=0}^{m-1} {}_{2m-1}C_l \; p^l (1-p)^{(2m-1)-l} \\
&= (p+1-p)^{2m-1} - \sum_{l=0}^{m-1} {}_{2m-1}C_l \; p^l (1-p)^{(2m-1)-l} \\
&= 1 - \sum_{l=0}^{m-1} {}_{2m-1}C_l \; p^l (1-p)^{(2m-1)-l} \qquad (119)
\end{aligned}
$$

と書ける.

そこで, まずは $p = 1/2$ を (119) 式に代入してみると

$$
f_{\mathrm{e}}^{(n)}(1/2) = 1 - \left(\frac{1}{2}\right)^{2m-1} \sum_{l=0}^{m-1} {}_{2m-1}C_l \qquad (120)
$$

となるが, 2 項係数に対して ${}_{2m-1}C_l = {}_{2m-1}C_{2m-1-l}$ が成り立つので, 例えば, $m = 3$ のときには

$$
\sum_{l=0}^{5} {}_5C_l = {}_5C_0 + {}_5C_1 + {}_5C_2 + {}_5C_3 + {}_5C_4 + {}_5C_5 = 2({}_5C_0 + {}_5C_1 + {}_5C_2)
$$

となるので, これを参考にすれば一般的に

$$
\sum_{l=0}^{m-1} {}_{2m-1}C_l = \frac{1}{2} \sum_{l=0}^{2m-1} {}_{2m-1}C_l = \frac{1}{2}(1+1)^{2m-1} = 2^{2m-2} \qquad (121)
$$

が成り立つことがわかる. よって, この結果を (120) 式に代入すれば, $p = 1/2$ のとき

$$
f_{\mathrm{e}}^{(n)}(1/2) = 1 - \left(\frac{1}{2}\right)^{2m-1} \sum_{l=0}^{m-1} {}_{2m-1}C_l = 1 - \left(\frac{1}{2}\right)^{2m-1} \times 2^{2m-2} = 1 - \frac{1}{2} = \frac{1}{2}
$$

が得られる.

では, $p \neq 1/2$ の場合はどうなるかであるが, 上記の結果が得られるためには, 関係式：(121) の成立が必要であった. しかし, (119) 式で同種の関係を使いたい場合, p は次の条件を満たさなければならない.

$$p^l(1-p)^{2m-1-l} \quad = \quad (1-p)^l p^{2m-1-l}$$

つまり, $p = 1-p$ を満たすべきなので, $p = 1/2$ のときのみ

$$\sum_{l=0}^{m-1} {}_{2m-1}C_l \; p^l(1-p)^{2m-1-l} \quad = \quad \frac{1}{2}\sum_{l=0}^{2m-1} {}_{2m-1}C_l \; p^l(1-p)^{2m-1-l}$$

が成り立つ[2]. 従って, $p \neq 1/2$ のときには上記の関係式は使えないことになる.

では, この場合に $f_{\mathrm{e}}^{(n)}(p)$ をどのように評価するかというと, 我々が興味を持っている $m \to \infty$ の極限を考えた場合, $2m-1 = M, m-1 = M$ として $M \to \infty$ の極限を考えれば十分である, ということに注目する. すると (119) 式からは

$$\begin{aligned}
\lim_{m\to\infty} f_{\mathrm{e}}^{(n)}(p \neq 1/2) \quad &= \quad 1 - \lim_{m\to\infty} \sum_{l=0}^{m-1} {}_{2m-1}C_l \; p^l(1-p)^{2m-1-l} \\
&= \quad 1 - \lim_{M\to\infty} \sum_{l=0}^{M} {}_{M}C_l \; p^l(1-p)^{M-l} = 1 - \lim_{M\to\infty}(p+1-p)^M = 1-1 = 0
\end{aligned}$$

が得られる. 従って, 結局

$$f_{\mathrm{e}}^{(\infty)} \quad = \quad \begin{cases} 0 & (0 \leq p < 1/2) \\ \frac{1}{2} & (p = 1/2) \end{cases}$$

が求める $n \to \infty$ での誤り確率の振る舞いということになる.

以上の考察から, 反転率 p が $0 \leq p < 1/2$ であるのであれば, 無限回同じ記号を繰り返し送信することにより, 誤り率はゼロとなることがわかる.

3.3 通信路容量

ここでは, ある通信路を介して情報を伝送するとき, 伝送しうる最大情報量である通信路容量について見ていく. この通信路容量は次回学ぶ**通信路符号化定理**で重要な役割を持つことになるが, ここでの目標はまずその定義と意味を確認し, いくつかの簡単な場合について具体的に容量を計算することができるようになることである.

通信路容量：C を次で定義することにしょう.

$$C \quad = \quad \max_{P_X} I(X;Y) \tag{122}$$

上式に出てくる $I(X;Y) = H(Y) - H(Y|X)$ は既に学んだ相互情報量であり, ここでは「入力 X を知ったとき, 出力 Y に関して得られる知識の量」という意味を持つことを思い出そう. また, この式の $\max_{P_X}(\cdots)$ は, 入力 X の全ての可能な確率分布 (入力 X の生成分布) に関して相互情報量を最大化したものを意味する. 従って, この通信路容量は通信路が実質的に伝送できる情報量の最大値を意味する.

この通信路容量の算出法に慣れるために次の例を見ておく.

[2] 式の上からは, この条件：$p^l(1-p)^{2m-1-l} = (1-p)^l p^{2m-1-l}$ を満たす p の値が $p = 1/2$ だけであることが, 誤り確率 f_{e} のデータ数無限大での振る舞いが $p = 1/2$, $p \neq 1/2$ とで異なる原因となっています.

例 1：誤りの無い 2 元対称通信路の通信路容量を求めよ.

(解答)
この場合の入力確率分布を $P_X(0) = p, P_X(1) = 1 - P_X(0) = 1 - p$ であると仮定する. このとき, 誤りの無い通信路の特性が次の条件付き確率：

$$P_{Y|X}(0|0) = P_{Y|X}(1|1) = 1 \tag{123}$$

$$P_{Y|X}(0|1) = P_{Y|X}(1|0) = 0 \tag{124}$$

で特徴付けられることに注意すれば, 出力の確率分布が

$$P_Y(0) = \sum_{x=0,1} P_{Y|X}(0|x)P_X(x) = P_{Y|X}(0|0)P_X(0) + P_{Y|X}(0|1)P_X(1) = p \tag{125}$$

$$P_Y(1) = \sum_{x=0,1} P_{Y|X}(1|x)P_X(x) = P_{Y|X}(1|0)P_X(0) + P_{Y|X}(1|1)P_X(1) = 1 - p \tag{126}$$

で与えられることになる. 従って, この場合の相互情報量 $I(X;Y)$ は

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= -p\log p - (1-p)\log(1-p) \\ &+ P_{Y|X}(0|0)P_X(0)\log P_{Y|X}(0|0) + P_{Y|X}(1|1)P_X(1)\log P_{Y|X}(1|1) = h(p) \end{aligned} \tag{127}$$

となる. ここで, $h(p)$ は既に学んだ **2 値エントロピー関数**であり,

$$h(p) = -p\log p - (1-p)\log(1-p) \tag{128}$$

で与えられる. 従って, ここでの相互情報量 $I(X;Y)$ を p に関して最大化することは, 上の 2 値エントロピー関数を最大化することに等しい. 既に学んだように $h(p)$ は $p = 1/2$ で最大値 1 をとるので, 求める通信路容量 C は

$$C = \max_p I(X;Y) = h(1/2) = 1 \tag{129}$$

である.

例 2：
2 元対称通信路において, 入力を記号 $X \in \{0,1\}$, 出力を記号 $Y \in \{0,1\}$ で表すものとする. このとき次の問いに答えよ.

(1) 入力 X の値を 0, あるいは 1 に固定したときの条件付きエントロピー $H(Y|X=1), H(Y|X=0)$ を求め, それらの結果から条件付きエントロピー $H(Y|X)$ は入力 X の分布 $P(X)$ には依らないことを示せ.
(2) (1) の結果を用いて 2 元対称通信路の通信路容量を求めよ.

(解答)

(1) 入力 X の値がある特定値 $X = x$ をとる条件の下での Y に関する条件付きエントロピーは

$$H(Y|X=x) = -\sum_y P_{Y|X}(y|x)\log P_{Y|X}(y|x) \tag{130}$$

で与えられる．既に学んだ, 条件付きエントロピー $H(Y|X)$ は上記を入力分布で平均したもの

$$H(Y|X) = -\sum_x \sum_y P_{Y|X}(y|x)P_x \log P_{Y|X}(y|x) = -\sum_x \sum_y P_{XY}(x,y) \log P_{Y|X}(y|x) \quad (131)$$

で与えられることに注意しよう．そこで, (130) に具体的に $x = 0, 1$ を入れたものを求めてみると $H(Y|0)$ は

$$\begin{aligned} H(Y|0) &= -\sum_y P_{Y|X}(y|0) \log P_{Y|X}(y|0) \\ &= 1 \quad -P_{Y|X}(0|0) \log P_{Y|X}(0|0) - P_{Y|X}(1|0) \log P_{Y|X}(1|0) \\ &= -(1-p)\log(1-p) - p \log p = h(p) \end{aligned} \quad (132)$$

であり, $H(Y|1)$ もやはり

$$\begin{aligned} H(Y|1) &= -\sum_y P_{Y|X}(y|1) \log P_{Y|X}(y|1) \\ &= -P_{Y|X}(0|1) \log P_{Y|X}(0|1) - P_{Y|X}(1|1) \log P_{Y|X}(1|1) \\ &= -(1-p)\log(1-p) - p \log p = h(p) \end{aligned} \quad (133)$$

となる．ここで $h(p) = -p \log p - (1-p)\log(1-p)$ は既に学んだ 2 値エントロピー関数である．従って, $H(Y|X = x)$ は x の値に依らずに 2 値エントロピー関数で与えられえることがわかった．このことから, 条件付きエントロピー $H(Y|X)$, すなわち, (131) 式は

$$H(Y|X) = -\sum_x H(Y|X = x)P_X(x) = h(p) \sum_x P_X(x) = h(p) \quad (134)$$

となり, 入力分布 $P_X(x)$ には依らなくなる．

(2) (1) の結果から相互情報量は

$$I(X;Y) = H(Y) - h(p) \quad (135)$$

となるので, この 2 元対称通信路の通信路容量 C は

$$C = \max_{P_X} H(Y) - h(p) \quad (136)$$

で与えられる．あとは出力のエントロピー $H(Y)$ を入力分布 $P_X(x)$ に関して最大化すればよい．今考えている入力は 0 と 1 しかとらないものなので, $P_X(0) = q, P_X(1) = 1 - q$ と置いてみると直ちに

$$P_Y(0) = (1-2p)q + p \quad (137)$$

$$P_Y(1) = 1 - p + (2p-1)q \quad (138)$$

が得られる．従って, 出力のエントロピーは q の関数として

$$\begin{aligned} H(Y) &= -[(1-2p)q + p] \log[(1-2p)q + p] \\ &- [1 - p + (2p-1)q] \log[1 - p + (2p-1)q] \end{aligned} \quad (139)$$

で与えられることがわかる．そこで, これを最大化する条件を求めてみると $q = 1/2$ のとき, 最大値 $H(Y) = 1$ をとることになるので, 結局, 求める通信路容量は

$$C = 1 - h(p) \quad (140)$$

となる.

また, 詳しい導出は省略するが, 後に用いる平均が a_0, 分散が a^2 のガウス通信路の通信路容量は

$$C = \frac{1}{2}\log_2\left(1+\frac{a_0^2}{a^2}\right) \tag{141}$$

で与えられる.

3.4 伝送速度と通信路容量

前に見た, $\{0,1\}$ の記号を複数回送信し, 受信側は多数決に従って復号を行う場合, 繰り返し送信回数 n を十分に大きくとれば誤り確率がゼロへと近づくことを見た. しかし, 通信路の**伝送速度** (あるいは**レート**) R を

$$R = \frac{1}{n} \tag{142}$$

で定義すれば (単位は [ビット/繰り返し回数]. n を「時間」であると考えればよい), この伝送速度も n を大きくとるにつれて限りなくゼロになってしまう. これでは誤り確率も伝送速度も同時にゼロになってしまうわけであるから, あまりうれしくはない. しかし, 誤り確率ゼロを実現するためには, 必ずしも R がゼロでなくとも, 伝送速度 R が今回学んだ通信路容量 C よりも小さければ, つまり, $R < C$ であれば, それが可能であることがシャノンによって示されている.

3.5 通信路符号化定理とその証明

$\{0,1\}$ の記号を複数回送信し, 受信側は多数決に従って復号を行う場合, 繰り返し送信回数 n を十分に大きくとれば誤り確率はゼロへと近づくが, しかし, 次に定義される通信路の**伝送速度** (あるいは**レート**) R :

$$R = \frac{1}{n} \tag{143}$$

も同時に n を大きくとるにつれて限りなくゼロになってしまうことを学んだ. しかし, 誤り確率ゼロを実現するためには, 必ずしも R がゼロでなくとも, 伝送速度 R が通信路容量 C よりも小さければ, つまり, $R < C$ であれば, それが可能であることがシャノンによって示されており, **通信路符号化定理**として知られている.

通信路符号化定理

(i) $R < C$ なる任意の伝送速度 R に対し, 任意に小さい復号誤り率 p_E の符号が存在する.
(ii) $R > C$ となる R に対し, 任意に小さな復号誤り率 p_E を持つ符号が存在しない.

今回はこの定理とその証明について詳しく見ていくことにする.

3.5.1 ランダム符号

この定理を証明する際には, **ランダム符号**と呼ばれる一般的ば符号化規則を導入する. この符号の作り方は至って簡単であり, 情報源の記号 $S_1, S_2, \cdots, S_M$ の一つ一つに n 個の $0,1$ の「ランダムな並び」を一つ一つ対応させていくことによって得られる. 具体的には例えば

情報源の記号	ランダム符号
S_1	$100\cdots000$
S_2	$101\cdots010$
S_3	$010\cdots110$
S_4	$011\cdots010$
$\cdots$	$\cdots$
S_M	$111\cdots010$

のように符号化される[3]．ここで, 2^n 個の可能な系列の中の一つが選ばれる確率は 2^{-n} であるから, このようなランダムな符号化によって, 異なる 2 つの情報源の記号 S_i, S_j に同一の符号があてられる確率は 2^{-2n} 程度であり, このような状況は事実的に無視できることになる.

また, $S_1, S_2, \cdots, S_M$ は全て等確率で生成されるものとする．ここで, n 個の並びによって作ることのできる符号の最大値は 2^n 個であるから, 伝送速度を

$$R = \frac{\log M}{n} \tag{144}$$

で定義すれば, 情報源の記号数 M は $M = 2^{nR}$ であり, 符号間の重複がないように, ここでは

$$M = 2^{nR} \leq 2^n \tag{145}$$

つまり, $R \leq 1$ であるとして議論を進めることにする.

3.5.2　2 元対称通信路に対する通信路符号化定理の証明

ここから通信路符号化定理の証明を行っていく.

まず, 定理の (i) を証明しょう．2 元対称通信路のビット誤り率を p とするのであれば, 情報源の記号 $S_1, S_2, \cdots, S_M$ のそれぞれを符号化して得られる $0, 1$ からなる n ビットの中に 2 元対称通信路で転送する際に誤りが生じるビット数はおおよそ np であると見積もることができる[4]．すると, 例えば, S_1 を伝送した際には, 受信者は正しい S_1 の符号から np ビットだけ異なる符号を受取るわけであるが, この n ビット中, np ビットだけ食い違った符号として取りうる個数 w はどれほどであろうか, ということを問題にしたい．つまり, 図 23 の斜線部に存在する系列の個数を調べたい．そのとき, 真の S_1 の符号から np ビットの食い違いを持つ $0, 1$ の系列の中の 1 つが現れる確率 $\hat{p}$ はおおよそ

$$\hat{p} = p^{np}(1-p)^{n(1-p)} = 2^{np\log p + n(1-p)\log(1-p)} = 2^{-nh(p)} \tag{146}$$

であることに着目しょう．ここで, $h(p)$ はこれまでに度々出てきた 2 値エントロピー関数である．従って, 我々が求めたい個数 w はこの逆数で与えられ

$$w = \hat{p}^{-1} = 2^{nh(p)} \tag{147}$$

となる.

[3] ある記号 $0, 1$ を n 回送信し, 多数決復号する例では $M = 2$ ではあるが $000\cdots000$, あるいは $111\cdots111$ を送信するわけであるから, この場合のランダム符号とは異なるものであることに注意されたい.

[4] もちろん, ある記号を伝送した際には np から外れているかもしれないので, 正確には $np \pm \epsilon$ であり, この ϵ が n の増加とともにどのように振舞うのか, を評価しなければならない．しかし, ここでは厳密な議論は避け, 「大数の法則が成り立つ範囲内では np でよい」ということを認めて先に進むことにする．このように 2^n 個の全ての系列の中でその誤りの個数が np であるような系列を (通信路出力の) **典型的な系列**と呼ぶ．ここで見るように 2 元対称通信路の場合には典型的な系列の個数はおおよそ $2^{nh(p)}$ 個と見積もられるが, この個数は全体 2^n のごく小さな部分しか占めない.

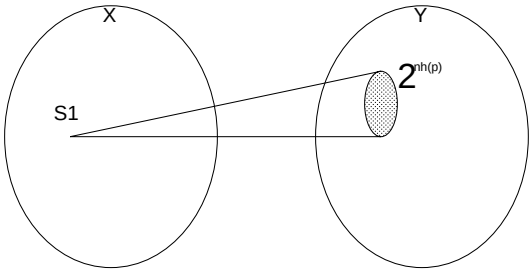

図 23: 入力記号 $S_1, \cdots S_N$ の中の一つ S_1 を 2 元対称通信路を介して伝送すると, 雑音により, 受信系列は $w = 2^{nh(p)}$ 個に広がる.

さて, 受信者が受取った符号からの復号に失敗するのは S_1 以外の $S_2, \cdots, S_M$ までの $M-1$ 個の記号が復号結果として選ばれる場合, つまり, 図 23 の $w = 2^{nh(p)}$ 個の一つ一つが $M-1$ 個の記号のどれかに復号されてしまう場合であるから, 復号誤り率 p_E は M が十分に大きなときに

$$p_E = \frac{M-1}{2^n} \times 2^{nh(p)} \simeq \left(\frac{M}{2^n}\right) \cdot 2^{nh(p)} = 2^{n(R-1+h(p))} \tag{148}$$

と評価できることになる.

ここで, $M = 2^{nR}$ であったことを思い出そう. また, 2 元対称通信路の通信路容量は先に見たように, $C = 1 - h(p)$ であったから, 上の復号誤り率 p_E は

$$p_E = 2^{n(R-C)} \tag{149}$$

と書き直すことができる. ここで n が十分に大きなとき

$$R < C \tag{150}$$

であれば $p_E \to 0$ となることは明らかである. よって (i) が証明された.

次に定理の (ii) を証明する. 符号の伝送により, M 個の情報源記号 $S_1, \cdots, S_M$ の各々はおおよそ $w = 2^{nh(p)}$ 個の系列に広がって受信されるが, n ビットの記号列の並べ方の最大値は 2^n 個であるから, M 個の情報源の記号一つひとつが送信によって収まることのできる箱のサイズは, 「全ての箱のサイズが等しい」とするならば $z = 2^n/M$ であり, この箱のなかに通信路を介した伝送による広がりによって実際に得られる $w = 2^{nh(p)}$ 個の系列が収まらなければならないので (図 24 参) $z > w$, すなわち

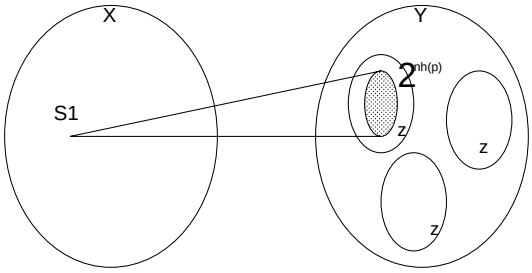

図 24: 通信による広がり w の一つひとつがサイズ $z = 2^n/M$ の「箱」に収まらなければならない.

$$z = \frac{2^n}{M} > 2^{nh(p)} = w \tag{151}$$

つまり

$$2^{n(C-R)} \quad > \quad 1 \tag{152}$$

でなければならないが, これは $R > C$ の場合には不可能. 従って, $R > C$ のとき, $p_E \to 0$ を実現するような符号は存在しない. 従って, 定理の (ii) が証明された.

3.6 スピングラスと誤り訂正符号

通信路符号化定理では, $n \to \infty$ では R がゼロとならなくても, 不等式：$R < C$ が満たされる限り, 復号誤り確率 $p_E \to 0$ となるような符号が存在することを教えているが, では具体的にはそのような符号をいかに構成すればよいのか, に関しては何も教えてくれない. そこで, ここからはスピンモデルを用いた具体的な符号/復号化法を見ていくことにする.

3.6.1 画像とパリティの同時送信による画像復元

先にみた復習の節で, 同じ記号を複数回転送することにより誤り確率を減少させることのできることを学んだ. 例えば, 画像の場合にも, 画像を複数回転送し, 各ビット毎にその多数決をとることで誤り率を低減することができるであろう. しかし, 冗長性を付加したいのであれば, このような方法でなくとも, 例えば画像の生データ $\{\xi\} = (\xi_1, \xi_2, \cdots, \xi_N)$ の他に隣接する画素対：

$$J_{ij} \quad = \quad \xi_i \xi_j \tag{153}$$

を送るのも一つの手であろう. ξ_i, $(i = 1, \cdots, N)$ は ± 1 であるから, この積 (153) は格子上の隣接画素間の**パリティ**に相当する. 正方格子上のこのようなペアはおおよそ $4N/2 = 2N$ 個あるので, これは元々の情報ビット数 N に比べて多くなっている. ここではまず始めにパリティと画像データを同時に送信する場合の画像修復のパフォーマンスについて調べてみたい.

パリティ (153) をやはり 2 元対称通信路を通して転送したとすると, 転送路の確率モデルである尤度は

$$P(\{J\}|\{\sigma\}) \quad = \quad \frac{\mathrm{e}^{\beta_J \sum_{ij} J_{ij}\sigma_i\sigma_j}}{[2\cosh(\beta_J)]^{N_B}} \tag{154}$$

と書ける. ここに, N_B は送信する J_{ij} の個数であり, β_J は J_{ij} の送信をマクロに特徴つけるハイパーパラメータである. ここでは, 画素自体も送るので, $P(\{\tau\}|\{\sigma\})$ と掛け合わせたものがこの通信系の確率モデルであり,

$$P(\{J\}, \{\tau\}|\{\sigma\}) \quad = \quad \frac{\mathrm{e}^{\beta_J \sum_{ij} \sigma_i\sigma_j + h\sum_i \tau_i\sigma_i}}{[2\cosh(\beta_J)]^{N_B}[2\cosh(h)]^N} \tag{155}$$

として与えられる. すると, 直ちにベイズの公式より事後確率が

$$P(\{\sigma\}|\{\tau\}, \{J\}) \quad = \quad \frac{\mathrm{e}^{-\mathcal{H}_{\mathrm{eff}}}}{\sum_{\{\sigma\}} \mathrm{e}^{-\mathcal{H}_{\mathrm{eff}}}} \tag{156}$$

$$\mathcal{H}_{\mathrm{eff}} \quad \equiv \quad -\beta_J \sum_{ij} J_{ij}\sigma_i\sigma_j - J\sum_{ij}\sigma_i\sigma_j - h\sum_i \tau_i\sigma_i \tag{157}$$

で与えられる. 従って, エネルギー関数 (157) に対してシミュレーテッド・アニーリングなどにより, 最小エネルギー状態を見つければ, それが MAP 解となるし, 各画素ごとにアンサンブルを用意し, その多数決をとれば MPM 推定値が得られる. 図 25 に 100×100 の画像サイズのイジングモデルのスナップショット

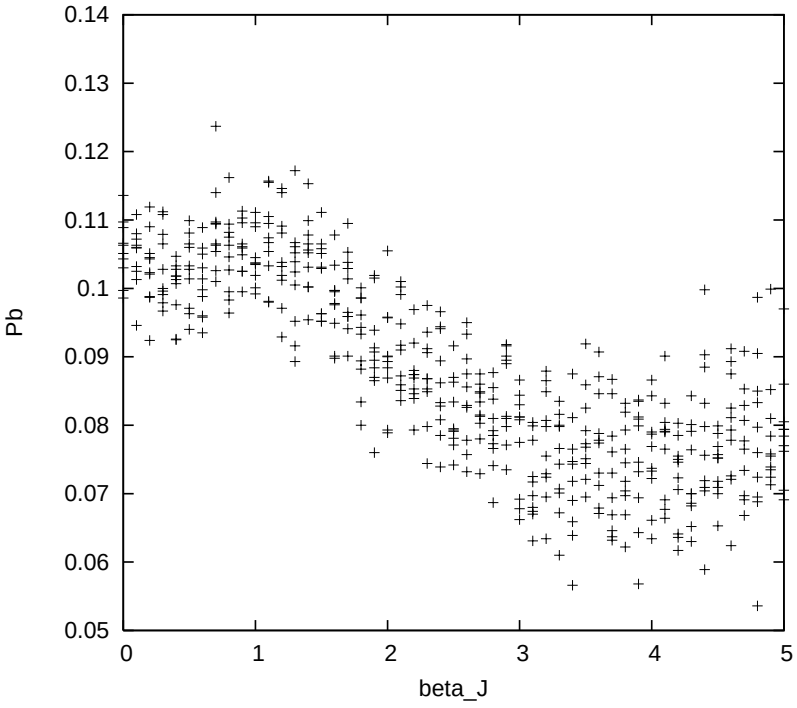

図 25: パリティも送信した場合の画像復元に関するビット誤り率 (MCMC 法による MPM 推定) の β_J 依存性. $\beta_J = 0$ が「従来の」画像復元のパフォーマンス (最適解：$T_m = J^{-1} = T_s = 2.15, h = (1/2)\log[(1-p)/p]$). 100×100 の画像に対して 10 回の独立試行を重ね打ちして描いている.

を原画像に選び, パリティ及び画素を共に誤り率 $p = 0.2$ の転送路で送信した場合の事後確率 (156) に関するマルコフ連鎖モンテカルロ法を用いた MPM 復元の結果をビット誤り率を β_J の関数としてプロットした. この図から明らかに, パリティを同時に送信した場合 ($\beta_J \neq 0$) の方がより小さなビット誤り率が得られることがわかる. 図 26 に図 25 のビット誤り特性を持つ画像復元の典型例を載せた. この図から明らか

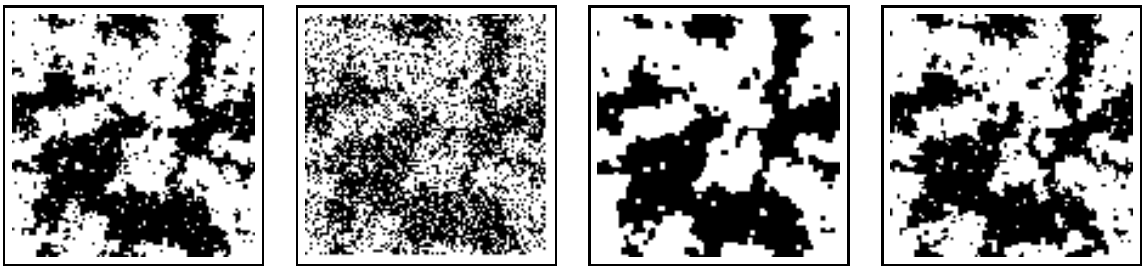

図 26: 右から原画像, 20% の劣化画像, $\beta_J = 0$ での MPM 修復画像, $\beta_J = 4.0$ での MPM 修復画像. パリティも同時送信した場合の方が原画像の局所的な構造までもがうまく復元されている.

に, 画素自体を送った場合 ($\beta_J = 0$) と比べて, パリティも同時に送信する ($\beta_J = 4.0$) 方が画像の持つ細かな構造までもうまく復元できていることがわかる.

3.6.2　パリティの転送とフラストレーション

さて, 我々は画像ではなく特に 2 次元的な幾何構造を持たないビット列を転送することを考えたい. 従って, 先に見たエネルギー関数 (157)1 の $-J\sum_{ij}\sigma_i\sigma_j$ の部分は無視することにする. また, 簡単のため, ここでは, パリティのみを転送する. つまり, エネルギー関数としては, $\beta_J = 1$ として

$$\mathcal{H}_{\rm eff} \quad = \quad -\sum_{ij} J_{ij}\sigma_i\sigma_j \tag{158}$$

を考えることにする. ここで, J_{ij} の転送に際してノイズが無いならば, 受信者側は $J_{ij} = \xi_i\xi_j$ をそのまま受け取るので, エネルギー関数は

$$\mathcal{H}_{\rm eff} \quad = \quad -\sum_{ij} \xi_i\xi_j\sigma_i\sigma_j \tag{159}$$

となる. ここで, 全てのサイト i で同時に $\sigma_i \to \xi_i\sigma_i$ と変換を施すと, このエネルギー関数は $\mathcal{H}_{\rm eff} = -\sum_{ij}\sigma_i\sigma_j$ となり, 強磁性イジングモデルのエネルギー関数と等価になる. こうした確率モデルを**マチス (Mattis) モデル**と呼ぶ. これは**各画素 σ_i が各々自分自身にとっての「上向き」を受け取ったデータ ξ_i の方向に取り直すと, そうして新たに定義し直された「上向き方向」に全ての画素が揃った場合にエネルギーが最小となる**ことを意味している. 従って, 転送路にノイズが無い場合には, エネルギー関数 (158) の最小を与える状態は自明である.

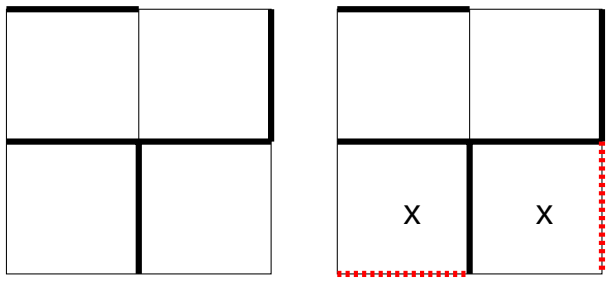

図 27: フラストレーションが無い場合 (左) とフラストレーションがある場合 (右). ×印の部分がフラストレーションの生じている部分.

一方, 転送路にはノイズがあり, J_{ij} がところどころ, その符号を変えていくと, 事情は複雑になる. 図 27 はそうした状況を表している. この左側の図では $J_{ij} = +1$ の結合を太線で描いているが, この図のどの閉路をとって, そのループに存在する J_{ij} の積：$\prod_{ループ} J_{ij}$ を計算してみても, 必ず, $\xi_i\xi_j$ が偶数回ずつ現れるので, この値は正であることがわかる. 一方, 右の図ではノイズにより, 破線の部分が反転してしまうことにより, ×印のついたループに対しては積：$\prod_{ループ} J_{ij}$ は負となる. この量：$\prod_{ループ} J_{ij}$ が負となるループを**フラストレーション**と呼び, フラストレーションがある場合にはエネルギーを最小化する最適なスピン配置 (画素の白黒) を決めることが難しくなる. このように, 結合がその符号も含めてランダムでフラストレーションを有する場合のスピンモデルを**スピングラス**と呼ぶ.

以降で説明する誤り訂正符号 — Sourlas 符号 — はこのスピングラスと密接に関連している.

3.6.3 Sourlas 符号

冗長性の加え方として, 正方格子上の隣接する画素 (ビット) 対 $J_{ij} = \xi_i \xi_j$ ではなく, N 個のビット列のうちの任意の p 対：$J_{i_1 \cdots i_p} = \xi_{i_1} \cdots \xi_{i_p}$ を通信路を介して送ることを考えよう[5]．従って, この場合の通信速度 R は

$$R = \frac{N}{{}_N C_p} \simeq \frac{p!}{N^{p-1}} \tag{160}$$

となる ($N \to \infty, p = \mathcal{O}(1)$). このとき, 通信路は各 $J_{i_1 \cdots i_p}$ ごとに独立なガウス通信路として

$$P(\{J\}|\{\xi\}) = \left(\frac{N^{p-1}}{J^2 \pi p!}\right)^{1/2} \exp\left[-\frac{N^{p-1}}{J^2 p!} \sum_{i_1 < \cdots < i_p} \left(J_{i_1 \cdots j_p} - \frac{J_0 p!}{N^{p-1}} \xi_{i_1} \cdots \xi_{i_p}\right)^2\right] \tag{161}$$

を考える. 従って, このガウス分布の平均 a_0 と分散 a^2 は

$$a_0 = \frac{J_0 p!}{N^{p-1}}, \quad a^2 = \frac{J^2 p!}{2N^{p-1}} \tag{162}$$

であるから, このガウス通信路の通信路容量は

$$C = \frac{1}{2} \log_2 \left(1 + \frac{a_0^2}{a^2}\right) \simeq \frac{J_0^2 p!}{J^2 N^{p-1} \log 2} \tag{163}$$

となるので, R と C の比をとると

$$\frac{R}{C} = \left(\frac{J_0}{J}\right)^2 \frac{1}{\log 2} \tag{164}$$

となる. ここで, (J_0/J) はシグナルノイズ比であることに注意しよう. この関係式 (164) は後に Sourlas 符号とシャノン限界の関係を議論する際に用いるので覚えておくことにしょう.

ところで前に述べたように, 今のビット列送信の場合には事前確率としては $P(\{\sigma\}) = 2^{-N}$ と選ぶのが自然なので, 事後確率は

$$P(\{\sigma\}|\{J\}) = \frac{\exp(\beta_J \sum_{i_1 < \cdots < i_p} J_{i_1 \cdots i_p} \sigma_{i_1} \cdots \sigma_{i_p})}{\sum_{\{\sigma\}} \exp(\beta_J \sum_{i_1 < \cdots < i_p} J_{i_1 \cdots i_p} \sigma_{i_1} \cdots \sigma_{i_p})} \tag{165}$$

として与えられる ($\{\sigma\}$ 等に依らない定数を無視した).

よって, 受信者側はエネルギー関数：

$$\mathcal{H}_{\text{eff}} = -\beta_J \sum_{i_1 < \cdots < i_p} J_{i_1 \cdots i_p} \sigma_{i_1} \cdots \sigma_{i_p} \tag{166}$$

に対し, MAP 法あるいは MPM 法等でオリジナルビットを推定すればよい. このような符号の構成法を **Sourlas 符号**と呼ぶ.

3.6.4 平均的性能評価

画像の場合には平均場モデルを用いることにより, 平均的性能を評価することができた. この Sourlas 符号の場合にもそれが可能である. しかし, 技術的にはやや難しい. その困難はどこから来るのかを以下で説明しよう.

[5] ここまでは特定の格子を想定して議論を進めてきたが, ここからの話は N 個のビット列のうちの任意の組をピックアップするだけであり, 何ら特定の格子には束縛されるものでないことに注意しておこう.

例えば, 簡単のため $p=2$ の場合を考えると, エネルギー関数は

$$H_{\rm eff} = -\beta_J \sum_{ij} J_{ij}\sigma_i\sigma_j \tag{167}$$

である. ここで, 解析が簡単にできるためには, このエネルギー関数がシングル・サイト i のみで書けることが重要であった. 今の場合, 例えば

$$h_i = \sum_j J_{ij}\sigma_j \tag{168}$$

として, 局所場 h_i を導入し, 磁化 $m=(1/N)\sum_i \sigma_i$ を

$$m = \frac{\sum_{\{\sigma\}}\{(1/N)\sum_i \sigma_i\}{\rm e}^{\sum_i h_i\sigma_i}}{\sum_{\{\sigma\}}{\rm e}^{\sum_i h_i\sigma_i}} \tag{169}$$

のようにシングル・サイトの問題として計算し, この外側から $P(\{J\}|\{\xi\})P(\{\xi\})$ に関してデータ平均をとればよいように思える. しかし, $\{\sigma\}$ に関する和は条件 (168) の下で取られなければならない. 従って, 正しくはこの条件をデルタ関数で取り込んで

$$m = \frac{\int_{-\infty}^{\infty}\prod_i dh_i \sum_{\{\sigma\}}\{(1/N)\sum_i \sigma_i\}{\rm e}^{\sum_i h_i\sigma_i}\prod_i \delta(h_i-\sum_j J_{ij}\sigma_j)}{\int_{-\infty}^{\infty}\prod_i dh_i \sum_{\{\sigma\}}{\rm e}^{\sum_i h_i\sigma_i}\prod_i \delta(h_i-\sum_j J_{ij}\sigma_j)} \tag{170}$$

としなければならない. このデルタ関数の部分をフーリエ変換表示：

$$\delta(h_i-\sum_j J_{ij}\sigma_j) = \frac{1}{2\pi}\int_{-\infty}^{\infty} d\hat{h}_i\, {\rm e}^{i\hat{h}_i(h_i-\sum_j J_{ij}\sigma_j)} \tag{171}$$

を用いて書き直すと, 残念ながら指数部分に J_{ij} が再度復活してしまい, 決してシングル・サイトの問題にはならない. こうした場合のデータ平均には**レプリカ法**と呼ばれる方法を用いるのが常套手段となっているが, とても込み入った計算になるので, ここでは結果の状態方程式とその解を示すにとどめる.

3.6.5 Sourlas 符号の状態方程式とその解析

Sourlas 符号に対してレプリカ法による解析を行うと次の状態方程式が得られる.

$$m = [\langle\sigma_i\rangle] = \int_{-\infty}^{\infty} Dx \tanh(G) \tag{172}$$

$$q = [\langle\sigma_i\rangle^2] = \int_{-\infty}^{\infty} Dx \tanh(G) \tag{173}$$

ここで, $Dx = dx{\rm e}^{-x^2/2}/\sqrt{2\pi}$ であり 2, G は

$$G = x\sqrt{\frac{p\beta_J^2 J^2 q^{p-1}}{2}} + \beta_J J_0 p m^{p-1} \tag{174}$$

で定義されている.

この変数 q は**スピングラス秩序変数**と呼ばれるものである. これは低温での「スピンのランダムな凍結」を特徴付ける変数である.

この変数を理解するために, まずは磁化 m の振る舞いについてみて行く. 熱平均 (時間平均) $\langle\sigma_i\rangle$ は高温の常磁性相では各スピンが熱揺らぎのために頻繁に変動し, その長時間平均はゼロ, つまり, $\langle\sigma_i\rangle=0$ で

ある. 従って, ゼロのランダムな配位平均 $[\cdots]$ をとったものも当然ゼロである. 一方, 低温でスピンの凍結が起こるならば, $\langle\sigma_i\rangle$ の値自体は各サイトで有限値にとどまるはずであるが ($\langle\sigma_i\rangle \neq 0$), この値は正負両方の符号を持つため, これを空間にわたってランダムな配位平均を施したもの $[\langle\sigma_i\rangle]$ はゼロになってしまう. 従って, 磁化 m 自体は常磁性相でもスピングラス相でも共にゼロである.

一方, $\langle\sigma_i\rangle^2$ の値は高温の常磁性相ではもちろんゼロ. 従って, スピングラス秩序変数 q はゼロである. 一方の低温でスピンのランダムな凍結が起こっているのであれば, 「凍結」しているわけだから, $\langle\sigma_i\rangle^2$ はもちろん有限値で, かつ, その**符号がサイトに依らずに常に正である**. 従って, これを空間に渡って平均したもの $[\langle\sigma_i\rangle^2]$ も有限値にとどまる. 従って, 常磁性相では $q=0$ であるが, スピングラス相では $q \neq 0$ となるのである.

ことから, この変数 q がゼロか否かでシステムが時間的には揃っている (つまり, 「凍結」している) が空間的にはランダムである相にあるか否かを判断することができる (強磁性相では当然 m, q ともに有限値).

また, この解に対して MPM 推定のビット誤り率は

$$P_b = \frac{1}{2}\left(1 - [\xi_i \mathrm{sgn}(\langle\sigma_i\rangle)]\right) = \frac{1}{2}\left(1 - \int_{-\infty}^{\infty} Dx\, \mathrm{sgn}(G)\right) \tag{175}$$

で与えられる. 図 28 に $p=2$ の場合を載せる. この図より, $T=\beta_J^{-1}$ を増加させるとシステムは 2 次の相

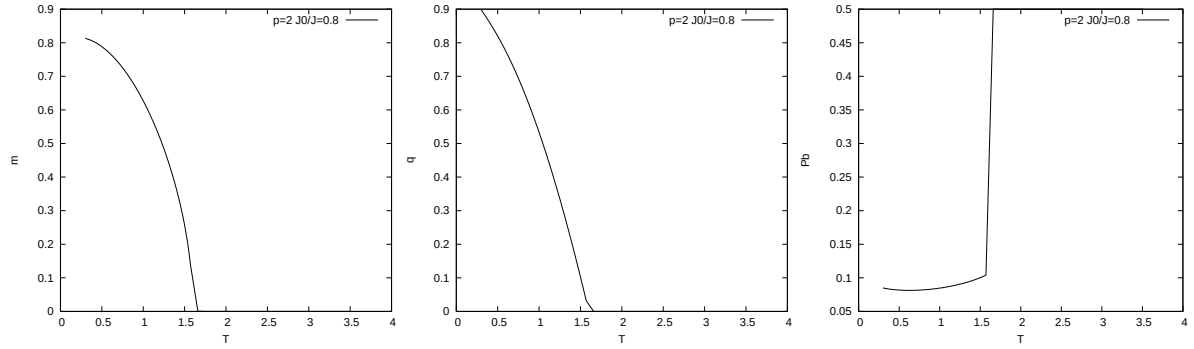

図 28: $p=2$ の場合の結果. シグナルノイズ比は $J_0/J=0.8$ に選んである.

転移を起こし, $P_b=0.5$ の状態へと遷移することがわかる. 同じシグナルノイズ比であっても, $p=3$ にす

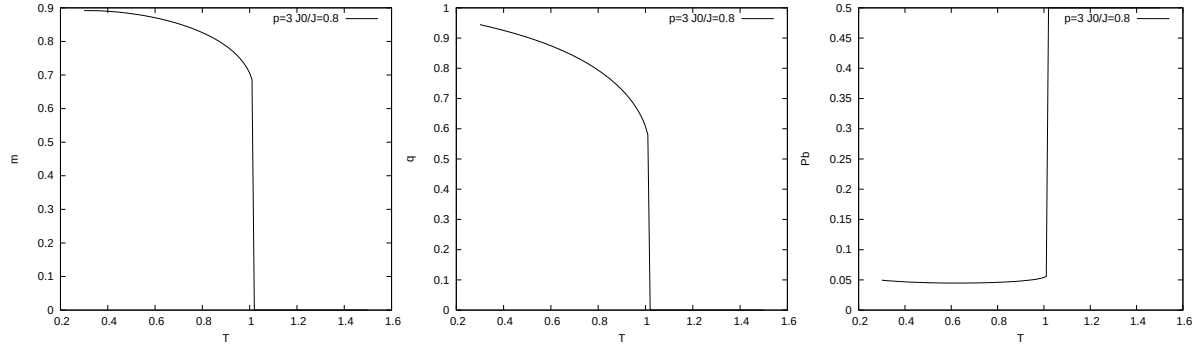

図 29: $p=3$ の場合の結果. シグナルノイズ比は $J_0/J=0.8$ に選んである.

ると, $P_b = 0.5$ の状態への遷移は 1 次の相転移となる (図 29 参照). 一方, 同じ p であっても, シグナルノ

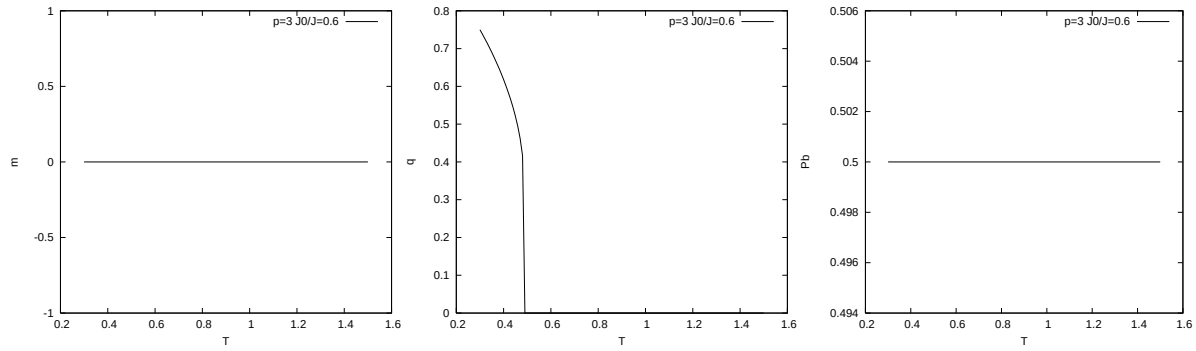

図 30: $p = 3$ の場合の結果. シグナルノイズ比は $J_0/J = 0.6$ に選んである.

イズ比が小さければ, P_b は T の値に依らずに常に 0.5 である (図 30 参照). ここで, 図 30 の中央の図より, $m = 0$ で復号に失敗する相は $q \neq 0$ のスピングラス相であることがわかる. 従って, この結果より, T を低温に固定し, シグナルノイズ比を低下させていくと, システムの状態は [強磁性相]$(m \neq 0, q \neq 0)$ から [スピングラス相] $(m = 0, q \neq 0)$ へと変化し, 復号に失敗することになる. また, MPM 推定の最良性条件は p

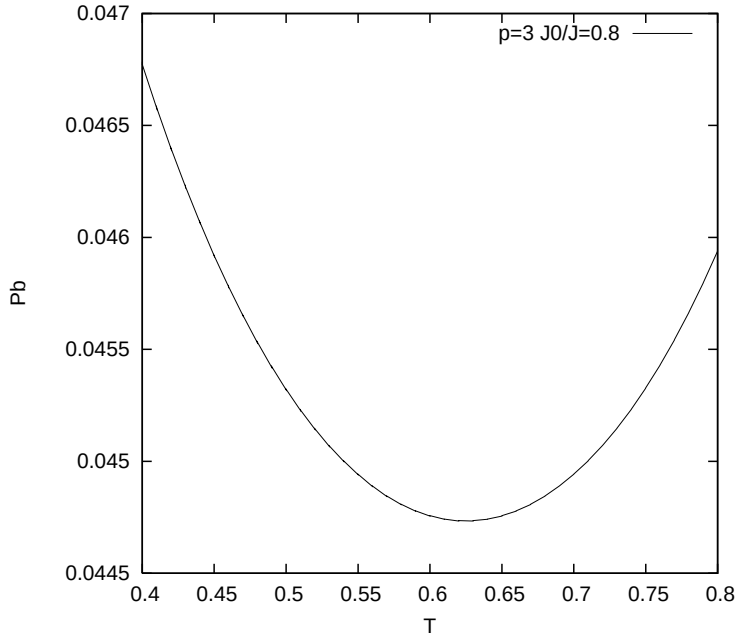

図 31: $p = 3$ の場合の T の最良性. $J_0/J = 0.8$. $T = J^2/2J_0$ でビット誤り率は最小となる.

に依らずに $T = J^2/2J_0$ である (図 31) 参照). このことは (161) 式の指数部分を展開し

$$P(\{J\}|\{\xi\}) \quad = \quad \left(\frac{N^{p-1}}{J^2 \pi p!}\right)^{1/2} P(\{J\})\, \mathrm{e}^{(2J_0/J^2)\sum_{i_1<\cdots<i_p} J_{i_1\cdots i_p}\xi_{i_1}\cdots\xi_{i_p}} \tag{176}$$

$$P(\{J\}) \quad = \quad \exp\left[-\frac{N^{p-1}}{J^2 p!}\sum_{i_1<\cdots<i_p}\left\{(J_{i_1\cdots i_p})^2+\frac{J_0^4 p!^2}{N^{2(p-1)}}\right\}\right] \tag{177}$$

と書き直すことにより, これと事後分布を比較して, 両者が等しくなるためには

$$T^{-1}=\beta_J \quad = \quad \frac{2J_0}{J^2} \tag{178}$$

すなわち

$$T \quad = \quad \frac{J^2}{2J_0} \tag{179}$$

が最適温度として求まることになる. この温度をスピングラスでは**西森温度**と呼ぶ.

最後に, p を大きくしていった場合の振る舞いを調べよう. 図に $p=2,3$, 及び, $p=10$ の場合の結果を載せる. 図 32 にその結果を示す. この図より, p を増加させることによりビット誤り率が減少していく様子が

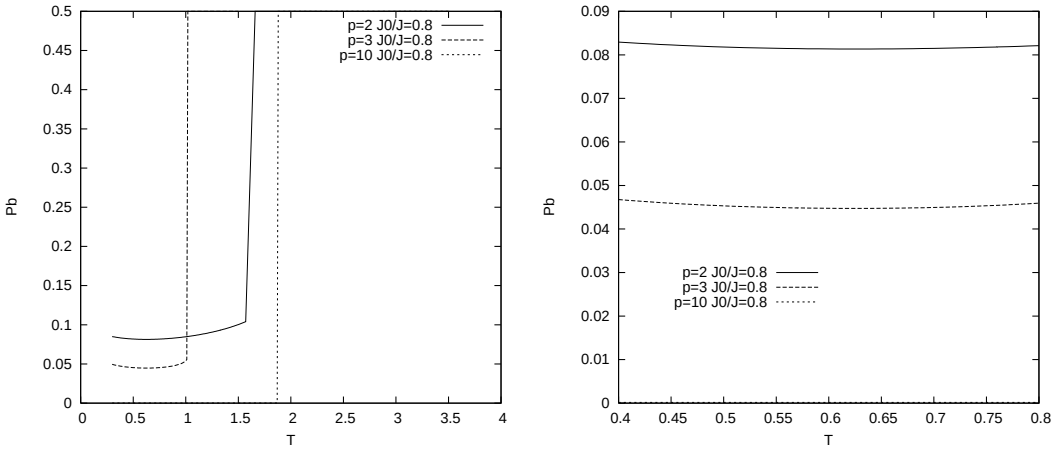

図 32: $p=2,3,10$ の場合のビット誤り率の振る舞い. 右は左図の極小値の周りを拡大したもの.

見て取れる. 実際, この Sourlas 符号では $p\to\infty$ の極限で $P_b=0$ となる領域が存在し, その領域の存在することのできるシグナルノイズ比の下限が $(J_0/J)_c=\sqrt{\log 2}$ であることを詳細な解析 (レプリカ非対称な解析) により示すことができる. つまり, $(J_0/J)\geq(J_0/J)_c=\sqrt{2\pi}$ で $P_b\neq 0$ の相が存在することになるのだが, この臨界点 $(J_0/J)_c$ を先に述べた関係式 (164)：

$$\frac{R}{C} \quad = \quad \left(\frac{J_0}{J}\right)_c^2\frac{1}{\log 2} \tag{180}$$

に代入すると

$$R=C \tag{181}$$

となり, シャノンの関係式を等式で満たすことがわかる. 従って, Sourlas 符号は $p\to\infty$ の極限で漸近的にシャノン限界を満たす符号なのである.