環境数理モデル特論A（情報理論）

2016年８月８－９日　於岡山大学環境理工学部

渡辺宏太郎　防衛大学校情報工学科教授

参考書

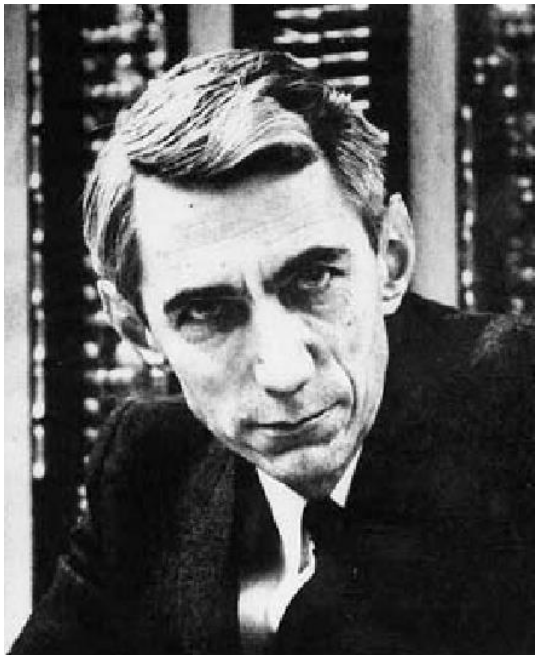
（1）「情報理論と符号理論」 J.A.ジョーンズ，J.M.ジョーンズ著
（2）「情報理論」 今井秀樹著
（3）「例題で学ぶ符号理論入門」 先名健一著
（4）「誤り訂正技術の基礎」 和田山正著
（5）「Error Correction Coding」 Todd K. Moon著

情報理論については（2）を読むとおおよその感じをつかめると思います．
（3）は例題が豊富で大変わかりやすい．
（5）は変調方式を含めてさらに理解を深めるにはよい一冊のように思います．
値段が高いのがネックでしょうか．
（4）は日本語でLDPC符号の解説がされているのがありがたい．

情報理論，符号理論とは

情報の伝達を如何に効率よく，信頼性高く行うかに関する理論．20世紀の半ばにシャノン(C.E. Shannon)により構築された．符号理論はその具体的アルゴリズムにあたるものである

Claude E Shannon's father was also named Claude Elwood Shannon and his mother was Mabel Catherine Wolf. Shannon was a graduate of the University of Michigan, being awarded a degree in mathematics and electrical engineering in 1936. Although he had not been outstanding in mathematics, he then went to the Massachusetts Institute of Technology where he obtained a Master's Degree in electrical engineering and his Ph.D. in mathematics in 1940.



Shannon wrote a Master's thesis *A Symbolic Analysis of Relay and Switching Circuits* . His doctoral thesis was on population genetics.

Shannon joined AT&T Bell Telephones in New Jersey in 1941 as a research mathematician and remained at the Bell Laboratories until 1972.

D Slepian, a colleague at the Bell Laboratories wrote:-

Many of us brought our lunches to work and played mathematical blackboard games but Claude rarely came. He worked with his door closed, mostly. But if you went in, he would be very patient and help you along. He could grasp a problem in zero time. He really was quite a genius. He's the only person I know whom I'd apply that word to.

Shannon published *A Mathematical Theory of Communication* in the *Bell System Technical Journal* (1948). This paper founded the subject of information theory and he proposed a linear schematic model of a communications system. This was a new idea. Communication was then thought of as requiring electromagnetic waves to be sent down a wire. The idea that one could transmit pictures, words, sounds etc. by sending a stream of 1s and 0s down a wire, something which today seems so obvious as we take this information from a server in St Andrews, Scotland, and view it anywhere in the world, was fundamentally new.（ウィキペディアより）

情報伝達のモデル

情報が伝えられてゆく過程は大まかに次の3つから構成される.

（1）伝送される情報

（2）情報を送る人（送信者）と受け取る人（受信者）

（3）情報が伝送される通り道（伝送媒体・手段）

例えばAさんがBさんに携帯電話で電話をかけるときは,

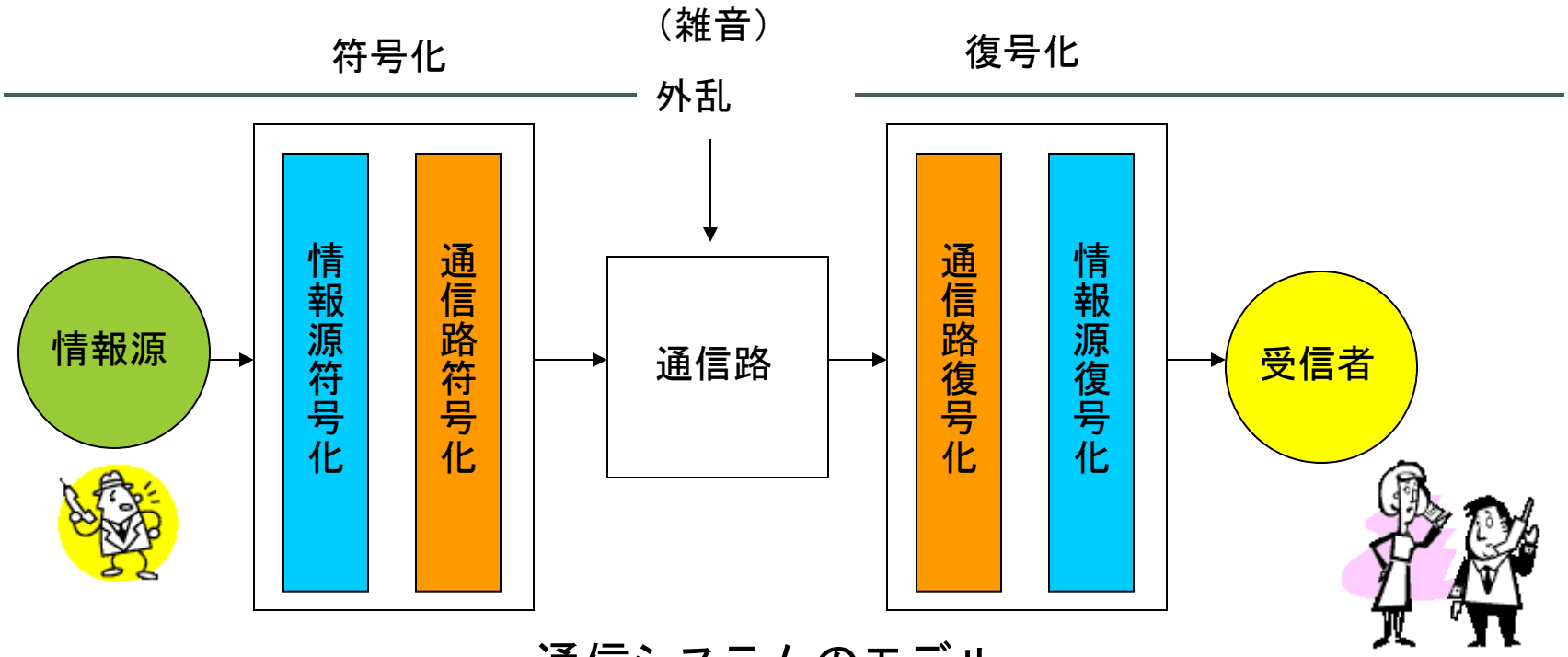
（1）の情報は，Aさんの発する言葉

（2）の送信者はAさんであり，受信者はBさん

（3）の伝送媒体・手段は電波や光ケーブル

である.

前のページの情報伝達のモデルを少し詳しく見ると･･･以下のようなシステムになっていることがわかる.



通信システムのモデル

情報源･･･送信者の発する情報

符号化･･･英文の通信を考える. 英文のまま通信することはできないから英文を符号化する必要がある.

A ⟶ 0x41　　0100 0001

B ⟶ 0x42　　0100 0010

情報源符号化　情報源の統計的性質を利用して効率の向上を図る符号化

例えば各英文字を頻度の高い文字には短い系列を割り当て，頻度の低い文字には長い系列を割り当てる．

具体的方法　ハフマン符号化，ランレングス符号化，シャノン・ファノ符号

情報源復号化　0,1系列から受信者が利用できる元の情報，例えばアルファベット記号に変換する作業

通信路符号化　現実の通信路においては種々の原因に起因して雑音による誤りが生じる．これをできるだけ排除して誤りの無い情報の伝達を実現するためには，これに対する対策を講じる必要がある．この誤り対策のための符号化を通信路符号化という．

例1

0 1 0 ⟶ 0 0 0　1 1 1　0 0 0（各記号を繰り返し3回送る）

（3回中1回誤っても正しく復号できる）

詳しくは符号理論（後半7回）で論じられる．

具体的方法として　ハミング符号，巡回符号，BCH符号等がある．

情報源通信路符号化の比較

符号化	最終目標	実現状況	符号の長さ	定理
情報源符号化	効率化	エネルギー・時間の節約	最短符号の実現	情報源符号化定理（シャノンの第１基本定理）
通信路符号化	信頼性の向上	誤りの検出・訂正	冗長性の付加	通信路符号化定理（シャノンの第２基本定理）

情報源の種類

- 離散情報源 （ディジタル情報源）・・・・だいたいはこちらを仮定する.
- 連続的情報源 （アナログ情報源）

記号の定義

情報源アルファベット(”晴れ”, ”雨”, ”曇り”)といった情報を記号的に $S=\{s_1, s_2, \cdots, s_M\}$ と表したもの. 時刻iでの情報源の出力を X_i で表す.

$X_0, X_1, \cdots, X_{n-1}$ の確率分布を

$$P_{X_0 X_1 \cdots X_{n-1}}(x_0, x_1, \cdots, x_{n-1}) = [X_0 = x_0, X_1 = x_1, \cdots X_{n-1} = x_{n-1} \text{となる確率}]$$

とする. $x_0, x_1, \cdots, x_{n-1}$ は S の任意の元.

何故確率を導入するのか？

頻度の大きい情報源には短い符号化を与え, 頻度の小さい情報源には長い符号化を与えれば直感的に効率的となることから確率導入の意義がわかるだろう.

符号のクラス

符号の分類とその特徴づけを勉強しよう．
情報源アルファベットを実際に伝達する場合，情報源記号を符号に変換することが必要なる．
これを符号化とよぶ．具体的には情報源アルファベット

$$S=\begin{Bmatrix} s_1, & s_2, & \cdots & s_n \\ P(s_1), & P(s_2), & \cdots & P(s_n) \end{Bmatrix}$$

に対する符号を構成することが符号化である．

例

$S=\begin{Bmatrix} a, & b, & c, & d \\ 0.4, & 0.3, & 0.2, & 0.1 \end{Bmatrix}$ としよう．例えばa→0, b→10, c→110, d→1110とすることが符号化である．

平均符号長

符号語 c_k を構成する記号の個数 l_k を**符号語長**とよぶ．**平均符号長** L は

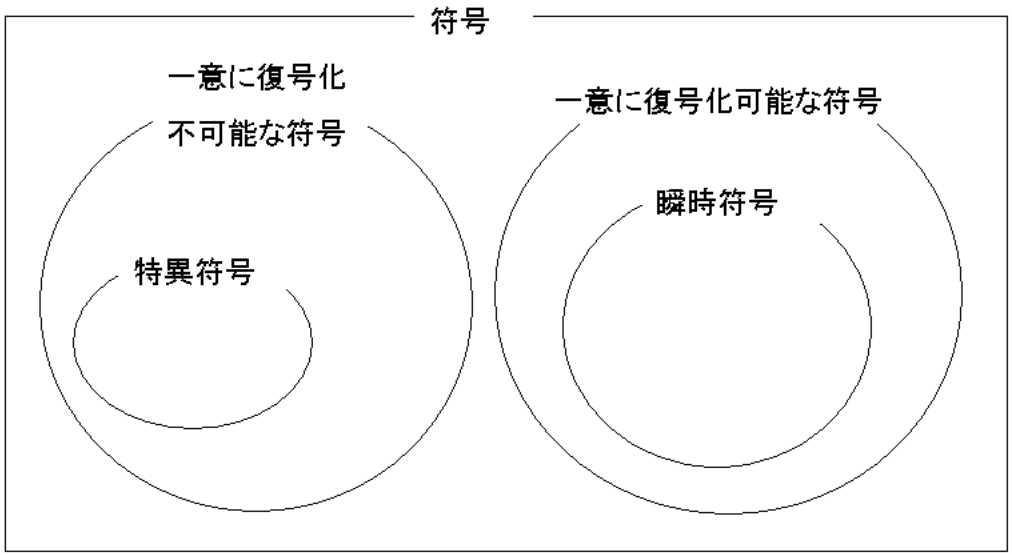
$L=\sum_{k=1}^{n} l_k P(s_k)$ で表される．

例えば例１の平均符号語長は $l_a=1, l_b=2, l_c=3, l_d=4$ だからL=１×0.4+2×0.3+3×0.2+4×0.1=2である．

平均符号長を小さくするには大きい出現確率をもつアルファベットに短い符号，小さい出現確率をもつアルファベットに長い符号を割り当てればよい．

問１　例1でa→1110，b→110，c→10，d→0とすると平均符号長はどうなるか？

符号のクラス



特異符号とは１つの符号語を異なる記号に割り当てた符号である．
瞬時符号とはその符号が送られた瞬間に復号できる符号のことである．

問2　次の符号は上の図のどこにあてはまるか？
(1) a→0, b→10, c→10, d→11
(2) a→0, b→01, c→10, d→11
(3) a→0, b→10, c→110, d→1110
(4) a→0, b→01, c→011, d→0111

（答）
(1) bとcに同じ符号を割り当てているから特異符号である．
(2) 特異符号ではないが，0110がbcなのかadaなのか区別がつかないから一意に復号化不可能な符号である．
(3) ある符号を得たときその符号に続きがあって他の符号になるということはないから瞬時符号である．
(4) 例えばaを得ているとしよう．このとき後に1が来ればc,dの可能性がある．運良く0が来ればaと判断できる．直後に0を得た時点でどの符号を得ているかわかるということは全ての場合にあてはまる．このことからこの符号は一意に復号可能だが瞬時符号でないことがわかる．

問３　（３）と（４）の違いは符号木を描いてみるとよくわかる．符号木を描いてみよ．

問3の答

図から次のことがわかる．

定理　次の（１），（２）は同値である．
（１）瞬時符号である．
（２）全ての符号語が符号木の枝の末端(葉)に割り振られている．

定理　**等長符号**(符号の長さが全て等しい符号)は特異符号でなければ，瞬時符号である．

(証明)　等長符号は符号木の枝の末端(葉)に割り振られている．

問4　情報源S={a, b, c, d, e}を次の表のように符号化した．符号C_1～C_6について以下の問に答えよ．

	C_1	C_2	C_3	C_4	C_5	C_6
a	0	1	0	0	100	1
b	10	110	10	01	101	01
c	110	001	110	011	110	000
d	1110	011	1110	0111	111	0010
e	1011	101	11110	01111	000	0011

（1）C_1，C_2 は一意に復号化不可能な符号らしい．理由を述べよ．

（2）瞬時符号を列挙せよ

（3）情報源Sの発生確率を$S=\left\{\begin{matrix} a, b, c, d, e \\ \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{16} \end{matrix}\right\}$とする．

瞬時符号でこの情報源に最も適した符号はどれか?（ヒント　平均符号長を計算せよ）

問4の答

クラフトの不等式

定理　符号語長 $\{l_1, l_2, \cdots, l_n\}$ をもつr元瞬時符号が存在するための必要十分条件は次の不等式をみたすことである．

$$\sum_{k=1}^{n} r^{-l_k} \leq 1 \qquad \text{(クラフトの不等式)}$$

注意　クラフトの不等式は瞬時符号であるための必要十分条件ではなく瞬時符号が存在するための必要十分条件である．つまり符号語長 がクラフトの不等式をみたしていれば，うまくを構成すれば瞬時符号にできるということである．

注意の例

問2の

（３）a→0，b→10，c→110，d→1110

（４）a→0，b→01，c→011，d→0111

で（３）は瞬時符号で（４）はそうではなかった．しかし，共に　$\sum_{k=1}^{4} 2^{-l_i} = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} = \frac{15}{16} < 1$

となりクラフトの不等式をみたす．よって

「瞬時符号である」　　「クラフトの不等式をみたす」

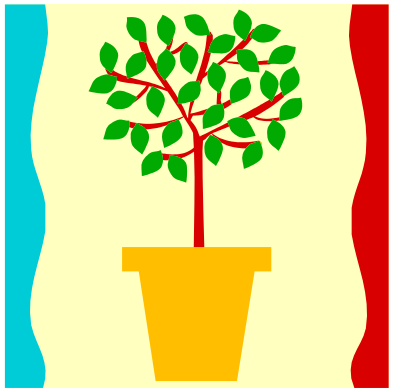
という関係式が成り立つことがわかる．

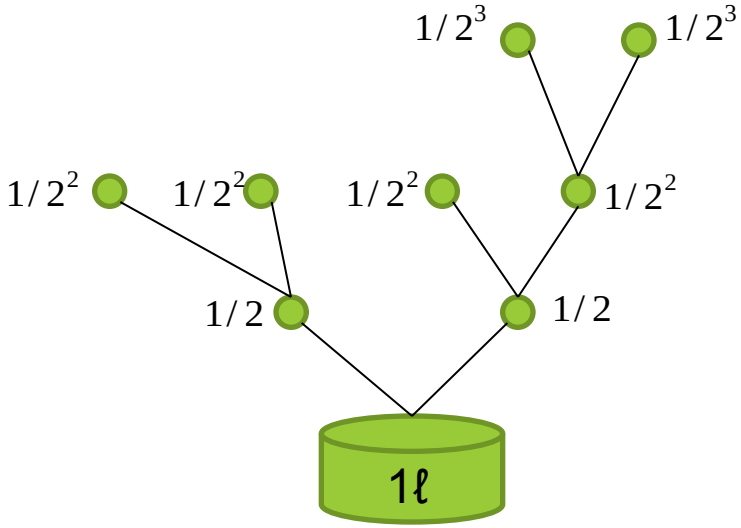
定理の証明

２元符号の場合を考えよう．木の根に量１の水をあたえることにしよう．この水は最初の枝で1/2と1/2に分流し，次の分岐でもまた２分され$1/2^2$と$1/2^2$に分流される．同様にしてm次の分岐では$1/2^m$と$1/2^m$に分流されることがわかる．符号語に対応するノード(葉)の下にバケツをおき，バケツに流れてくる水量をすべてのバケツについて足し合わせたものがクラフトの不等式の左辺となる．

明らかに瞬時符号ではバケツの水の総和は１以下となることがわかる．

逆にクラフトの不等式がみたされるならば，l_k に対して $l_k - 1$ 次の葉を選んでやれば瞬時符号が構成できることがわかる．





問5

情報源S={a, b, c, d}に対する次の符号長を持つ瞬時符号が構成できるかどうか判定せよ．
構成できるものについてはその例を挙げよ．

（1）（1，2，2，2）の２元符号
（2）（1，2，2，2）の３元符号

問5の答

情報源符号化定理

さてシャノンの情報源符号化定理（シャノンの第１定理）について述べる．シャノンの第１定理を述べるためには，N次拡大情報源とエントロピーの概念が必要である．

定義　（N 次拡大情報源）N 次拡大情報源 S^N とは情報源 S の情報源アルファベットから重複を許して N 個とりだしてできるアルファベットを新たな情報源記号とする情報源である．したがって情報源 S のアルファベット数が k ならば N 次拡大情報源 S^N のアルファベット数は k^N である．

例　無記憶情報源

$S=\begin{Bmatrix} a, & b \\ \frac{1}{3}, & \frac{2}{3} \end{Bmatrix}$ に対する２次拡大情報源は $S^2=\{aa,ab,ba,bb\}$ となりその発生確率を求めると $S^2=\begin{Bmatrix} aa, & ab, & ba, & bb \\ \frac{1}{9}, & \frac{2}{9}, & \frac{2}{9}, & \frac{4}{9} \end{Bmatrix}$ である．

問６　次の無記憶情報源Ｓの３次拡大情報源S^3を構成せよ．

$$S=\left\{\begin{matrix} a, & b \\ \frac{1}{4}, & \frac{3}{4} \end{matrix}\right\}$$

問６の答

エントロピー

定義　P(s)を情報源 S のアルファベット s の生起する確率とする.

$H_1(S) = -\sum_{s \in S} P(s) \log_2 P(s)$ を情報源 S の 1 次エントロピーという. 拡大情報源 S^N の 1 次エントロピー $H_1(S^N)$ を N で割った量 $H_1(S^N)/N$ を N 次エントロピーという.

問 7　例の無記憶情報源 S の 2 次エントロピーを計算してみよ. $\log_2()$ の数値化はしなくてよい.

問 7 の答

定義（エントロピー）

N次エントロピーを用いてエントロピーは定義される

$$H(S) = \lim_{N \to \infty} \frac{H_1(S^N)}{N}$$

補題　情報源 S が無記憶情報源ならば N 次エントロピーは 1 次エントロピーに等しい.

（これは，問 7 でやったことだが N=2 について証明してみよう.）

(証明)　情報源 S が無記憶情報源という仮定より 2 次拡大情報源 S^2 の結合確率分布は $P(x_1,x_2)=P(x_1)\times P(x_2)$ である．S^2 の 1 次エントロピーを計算すると

$$
\begin{aligned}
H_1(S^2) &= -\sum_{x_1}\sum_{x_2} P(x_1)P(x_2)\log_2 P(x_1)P(x_2) \\
&= -\sum_{x_1}\sum_{x_2} P(x_1)P(x_2)\log_2 P(x_1) - \sum_{x_1}\sum_{x_2} P(x_1)P(x_2)\log_2 P(x_2) \\
&= -\sum_{x_1} P(x_1)\log_2 P(x_1) - \sum_{x_2} P(x_2)\log_2 P(x_2) \\
&= -2\sum_{x_1} P(x_1)\log_2 P(x_1)
\end{aligned}
$$

よって

$$
\frac{H_1(S^2)}{2} = -\sum_{x_1} P(x_1)\log_2 P(x_1) = H_1(S)
$$

が成り立つ．(証明終わり)

シャノン—ファノ符号

補題　情報源 S に対して次の条件をみたす平均符号長 L をもつ r 元瞬時符号が構成できる．この符号は r 元シャノンーファノ符号とよばれる．

$$H_1(S) \le L < H_1(S)+1 \qquad (1)$$

L は $H_1(S)$ を下回ることはできない．

$H_1(S) = \sum_{s \in S} -P(s)\log_r P(s)$ で定義する

（証明）

$$-\log_r P(s_k) \le l_k < -\log_r P(s_k)+1 \qquad (2)$$

をみたす整数 l_k を決める（一意的に決まる）．もっと言えば,

$$l_k = \left\lceil \log_r \frac{1}{P(s_k)} \right\rceil \qquad (3)$$

である．

ここで（2）の１番目の不等式より

$$-\log_r P(s_k) \le l_k \Leftrightarrow -l_k \le \log_r P(s_k) \Leftrightarrow \log_r r^{-l_k} \le \log_r P(s_k)$$
$$\Leftrightarrow r^{-l_k} \le P(s_k)$$

最後の式を k=1 から n までたすと $\sum_{k=1}^{n} r^{-l_k} \le \sum_{k=1}^{n} P(s_k) = 1$ となりクラフトの不等式をみたす．

よって符号語長 $l_1, l_2, \cdots, l_k$ をもつ r 元瞬時符号が構成可能である．

補題の証明（続き）

次にこうしてつくった r 元瞬時符号が式（１）右辺をみたすことを確かめよう．

（２）の各項に $P(s_k)$ をかけて $k=1,\cdots,n$ の和をとる．

$$-P(s_k)\log_r P(s_k) \le l_k P(s_k) < -P(s_k)\log_r P(s_k) + P(s_k)$$

よって

$$-\sum_{k=1}^{n} P(s_k)\log_r P(s_k) \le \sum_{k=1}^{n} l_k P(s_k) < -\sum_{k=1}^{n} P(s_k)\log_r P(s_k) + \sum_{k=1}^{n} P(s_k)$$

上式は（１）式とまったく同じ式である（確認せよ）．

LがH₁(S)を下回らないことについて

補題

$q_1+\cdots+q_M \le 1,\ q_i \ge 0$とする．ただし$p_i \ne 0$のときは$q_i \ne 0$とする．

このとき

$$-\sum_{i=1}^{M} p_i \log_2 q_i \ge -\sum_{i=1}^{M} p_i \log_2 p_i = H_1(S)$$

が成り立つ．等号は$p_i = q_i\ (i=1,\ldots,M)$のとき，またその時に限って成り立つ．

（証明）$r=2$とする．

$$D = -\sum_{i=1}^{M} p_i \log_2 q_i + \sum_{i=1}^{M} p_i \log_2 p_i = -\sum_{i=1}^{M} p_i \log_2 \frac{q_i}{p_i} = -\sum_{i=1}^{M} \frac{p_i}{\log 2} \log \frac{q_i}{p_i}$$

ここで$\log x \le x-1$だから

$$D \ge \sum_{i=1}^{M} \frac{p_i}{\log 2}\left(1-\frac{q_i}{p_i}\right) = \frac{1}{\log 2}\sum_{i=1}^{M}(p_i-q_i) \ge \frac{1}{\log 2}\left(1-\sum_{i=1}^{M} q_i\right) \ge 0$$

等号成立は$p_i = q_i$のとき，またその時に限る．

$(l_1,\ldots,l_M)$を符号長とする．$q_i = 2^{-l_i} \quad (i=1,\ldots,M)$とおく．$(l_1,\ldots,l_M)$は瞬時符号の符号長なので

$$q_1+\cdots+q_M \le 1$$

が成り立つ．$l_i = -\log_2 q_i \quad (i=1,\ldots,M)$だから平均符号長は

$$L=\sum_{i=1}^{M} -p_i \log_2 q_i$$

だから補題より

$$L \ge H_1(S)$$

が成り立つ．

（証明終）

問８

$S = \begin{Bmatrix} a, & b, & c, & d, & e \\ 0.3 & 0.2 & 0.2 & 0.2 & 0.1 \end{Bmatrix}$ の 2 元シャノンーファノ符号の符号長，平均符号長を求めよ．

問８の答

情報源符号化定理

定理１（情報源符号化定理，シャノンの第１定理）

r 元情報源 S は任意の正数 ε に対して， 1 情報源あたりの平均符号長 L が

$$H(S) \le L < H(S) + \varepsilon \qquad (1)$$

となるような r 元瞬時符号に符号化できる．しかし，どのような一意復号可能な符号をもってしてもこの式の左辺を下回るような符号化はできない．ここで

$H(S) := \lim_{N\to\infty} H_r(S^N)/N$ であり**エントロピー**とよぶ．

（証明）１情報源あたりの平均符号長 L が（1）式をみたすような r 元瞬時符号の存在を情報源 **S が無記憶情報源の場合**に証明しよう．補題を N 次拡大情報源 S^N に対して適用すると平均符号長 L_N が

$$H_1(S^N) \le L_N < H_1(S^N) + 1 \qquad (2)$$

をみたす瞬時符号（シャノン－ファノ符号）が存在する．

情報源符号化定理証明の続き

補題より $H_1(S^N) = NH_1(S)$ だから $H(S) = \lim_{N\to\infty} \frac{H_1(S^N)}{N} = \frac{NH_1(S)}{N} = H_1(S)$．また $L_N = NL$ である．式（2）の両辺を N で割ると

$$H(S) \le L < H(S) + \frac{1}{N}$$

が成り立つことがわかる．**S が無記憶情報源の場合** $H_r(S) = H(S)$ だから 1/N= ε とおくことにより

$$H(S) \le L < H(S) + \varepsilon$$

をみたす r 元瞬時符号が存在することがわかる．（証明終わり）

問 9　無記憶情報源　$S=\begin{Bmatrix} a, & b \\ \frac{1}{6}, & \frac{5}{6} \end{Bmatrix}$ を考える．この情報源に対する 2 次拡大情報源 S^2 を求めシャノンーファノ符号化し，1 情報源記号あたりの平均符号長を求めよ．同様に 3 次拡大情報源 S^3 を求めシャノンーファノ符号化し，1 情報源記号あたりの平均符号長を求めよ．

さらにエントロピーH(S)を求め，1 次，2 次，3 次の順に 1 情報源記号あたりの平均符号長がエントロピーH(S)に近づくことを確かめよ．$\log_2 3=1.584, \log_2 5=2.322$ とする．

ハフマン符号化

定義　（コンパクト符号）ある与えられた情報源 S に対して（N 次拡大情報源でない）に対し一意復号可能な符号に符号化するとき平均符号長を最小にする符号を**コンパクト符号**という．
このコンパクト符号の構成法がハフマン(Huffman)によって与えられている．

2 元ハフマン符号の構成法

（1） 各情報源記号に対する対応する葉を作る．おのおのの葉には，情報源記号の発生確率を記しておく．

（2） 確率の最も小さい 2 枚の葉に対して，1 つの節点を作りその節点と 2 枚の葉を枝で結ぶ．この 2 本の枝の一方には 0，他方には 1 を割り当てる．さらにこの節点に 2 枚の葉の確率の和を記し，この節点を新たな葉と考える．

（3） 葉が 1 枚しか残っていなければ，符号の構成が完了している．そうでなければ，（2）へ戻る．

問 10　情報源 S を $S = \begin{Bmatrix} a, & b, & c, & d \\ 0.6, & 0.25, & 0.1, & 0.05 \end{Bmatrix}$ とする．a,b,c,d のハフマン符号を求めよ．

問 11　情報源 S を $S = \begin{Bmatrix} a, & b, & c, & d \\ 0.35, & 0.3, & 0.2, & 0.15 \end{Bmatrix}$ とする．a,b,c,d のハフマン符号を求めよ．

答えは 2 通りに分かれただろう．
しかし，どちらの符号化も共に平均符号長は２である．このようにハフマン符号は与えられた情報源に対して一意的には決まらない．
しかし，そのような場合でも平均符号長は一致する（そうでないとコンパクト符号にならないから）．
さて次に N 次拡大情報源をハフマン符号化することを考えてみよう．

問 12　無記憶情報源　$S=\begin{Bmatrix} a, & b \\ \frac{1}{6}, & \frac{5}{6} \end{Bmatrix}$ を考える．この情報源に対する 2 次拡大情報源 S^2 を求めハフマン符号化し，1 情報源記号あたりの平均符号長を求めよ．同様に 3 次拡大情報源 S^3 を求めハフマン符号化し，1 情報源記号あたりの平均符号長を求めよ．さらにエントロピーH(S)を求め，1 次，2 次，3 次の順に 1 情報源記号あたりの平均符号長がエントロピーH(S)に近づくことを確かめよ．$\log_2 3=1.584, \log_2 5=2.322$ とする．

一定個数の情報源記号ごとにまとめて符号化する方法を**ブロック符号化**といい，それによって構成される符号を**ブロック符号**という．N 次拡大情報源に対する符号化は N 個の符号をまとめて行うブロック符号化である．特に N 次拡大情報源に対するハフマン符号化は**ハフマンブロック符号化**という．

ところで，ハフマン符号はコンパクト符号でかつ瞬時符号であるから当然平均符号長は前回の 1 次エントロピーに対する不等式

$$H_r(S) \leq L < H_r(S)+1$$

をみたしている．

N 次拡大情報源に対するハフマン符号化（ハフマンブロック符号化）を行えば

$$\frac{H_r(S^N)}{N} \leq L < \frac{H_r(S^N)}{N} + \frac{1}{N}$$

をみたしていることになる．よって次が成り立つ．

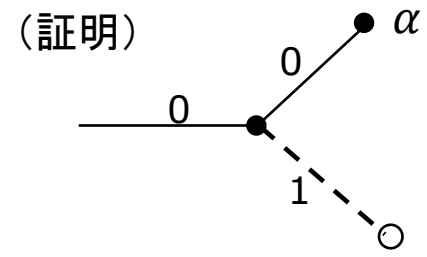
<u>重要</u>

ハフマンブロック符号化を行うと 1 情報源記号あたりの平均符号長は約 1/N の誤差でエントロピーH(S)に近づいて行く．これは，シャノンーファノ符号化によるエントロピーへの近づき方よりも速い．

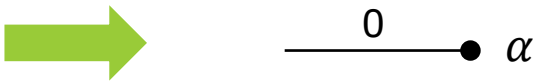
ハフマン符号はコンパクト符号（1）

補題　コンパクト瞬時符号の最も長い符号語に対応する葉は２枚ある．
２枚の葉は確率の最も小さい２つの情報記号に対応する．

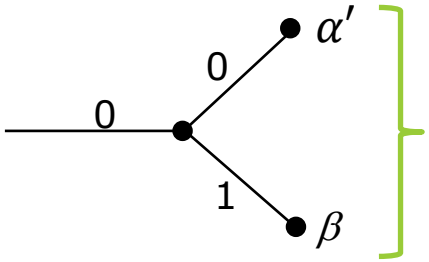
（証明）



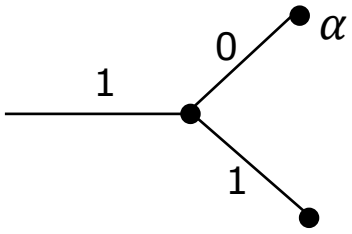
符号が割り当てられていない



平均符号長が短くなる．
コンパクト符号
であることに矛盾



最も長い
符号語

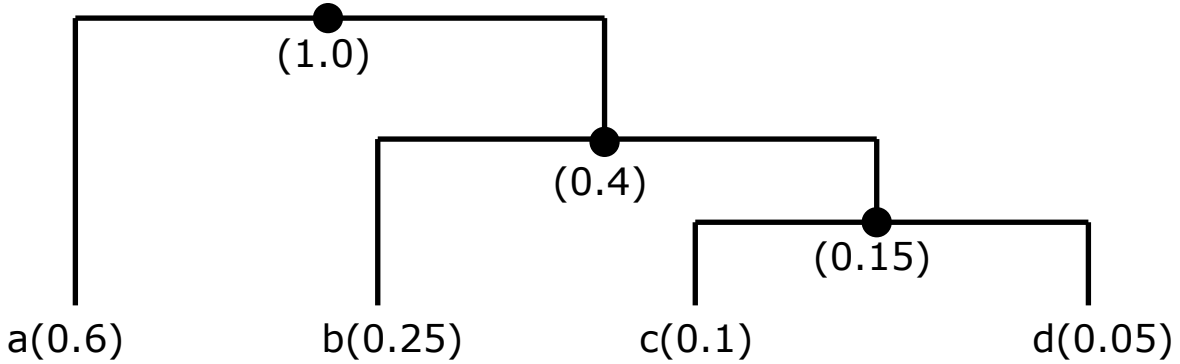


コンパクト符号

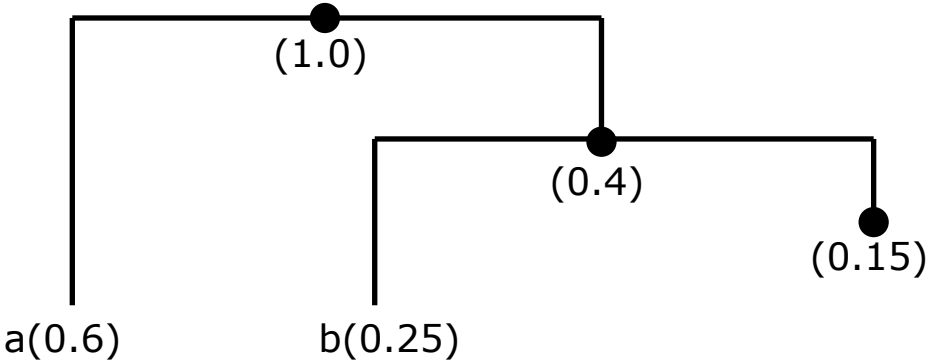
αとα'を交換することで
平均符号長を短くできる

矛盾

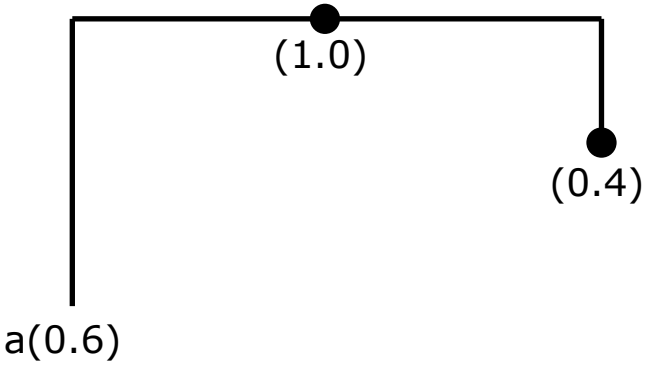
ハフマン符号はコンパクト符号（2）



T_0：ハフマン符号化完成形



T_1：最も確率の小さい２つをまとめた



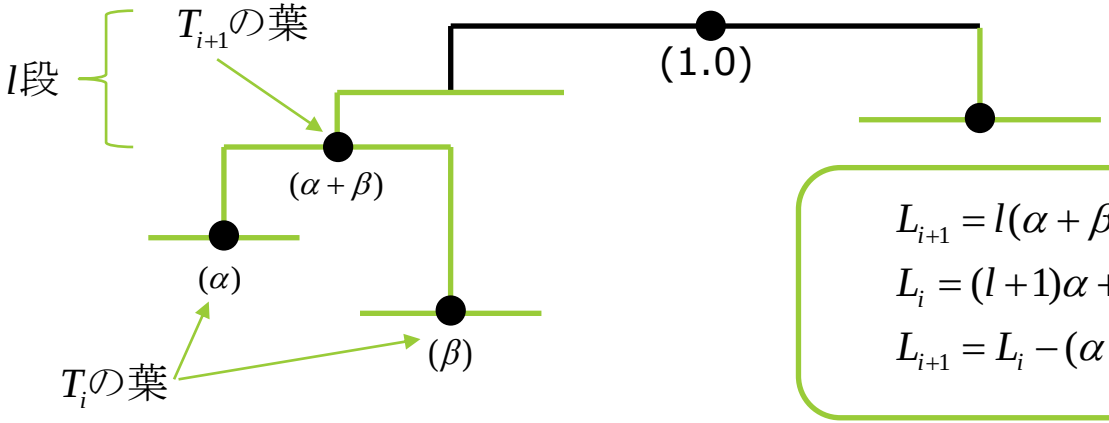
$T_2 = T_{end}$：さらにまとめた

T_{end}は明らかにコンパクト符号化されている．
（情報が２つなので0と1に符号化するしかない）

ハフマン符号はコンパクト符号（3）

T_{i+1}がコンパクト符号化されていると仮定する．T_iもコンパクト符号であることを示す．

L_{i+1}：T_{i+1}の平均符号長，L_i：T_iの平均符号長とする．



$$L_{i+1} = l(\alpha+\beta) + \text{Remainder}$$
$$L_i = (l+1)\alpha + (l+1)\beta + \text{Remainder}$$
$$L_{i+1} = L_i - (\alpha-\beta) \qquad (1)$$

T_iがコンパクト符号化されていないと仮定する．$T_i = \begin{Bmatrix} x_1, & x_2, & \cdots & x_k, & x_{k+1}, & \cdots & x_M \\ p(x_1), & p(x_2), & & \alpha, & \beta, & \cdots & p(x_M) \end{Bmatrix}$

仮定よりT_iと同じ葉と確率を持ちT_iと異なるコンパクト符号化された木T_i'が存在．

よって $L_i' < L_i$　　…(2)　T'_iはコンパクト符号化されているから補題より最長の符号語に対応する

2枚の葉は確率α，βを持つ．α，βをまとめてT'_{i+1}をつくると$L_{i+1}' = L_i' - (\alpha-\beta)$　　…(3)

$$L_{i+1}' = L_i' - (\alpha-\beta) < L_i - (\alpha-\beta) = L_{i+1}$$

となりT_{i+1}がコンパクト符号であることに矛盾する．

平均情報量（エントロピー）

X：実際の天気の（結合）確率分布，　Y：天気予報の（結合）確率分布

$P_{XY}(x,y)$		Y		$P_X(y)$
		晴	雨	
X	晴	0.45	0.12	0.57
	雨	0.15	0.28	0.43
$P_Y(y)$		0.60	0.40	

（１）平均情報量（エントロピー）Xについてのあいまいさ

$$H(X)=\sum_{i=1}^{n}-P_X(x_i)\log_2 P_X(x_i)$$

上の例だと

$$H(X)=-0.57\times\log_2 0.57-0.43\times\log_2 0.43 \quad =0.986\text{（ビット）}$$

条件付きエントロピー

（２）条件付エントロピー　Ｙを知ったとき，Ｘについて残っているあいまいさ

$P_{X\|Y}(x\|y)$		Y	
		晴	雨
X	晴		
	雨		

Ｙ＝晴だったとき，Ｘについての残っているあいまいさは

$$H_{X|晴} = -0.75 \times \log_2 0.75 - 0.25 \times \log_2 0.25$$

$$H_{X|雨} = -0.3 \times \log_2 0.3 - 0.7 \times \log_2 0.7$$

これらを平均すると$0.6 \times 0.811 + 0.4 \times 0.881 = 0.839$（ビット）
式で書くと

$$H(X|Y) = \sum_{j=1}^{m} P_Y(y_j) \sum_{i=1}^{n} -P_{X|Y}(x_i|y_j) \log_2 P_{X|Y}(x_i|y_j)$$

条件付きエントロピー（2）

$$H(X \mid Y) = \sum_{j=1}^{m} P_Y(y_j) \sum_{i=1}^{n} -P_{X|Y}(x_i \mid y_j) \log_2 P_{X|Y}(x_i \mid y_j)$$

上式に

$$P_{X|Y}(x_i \mid y_j) = \frac{P_{XY}(x_i, y_j)}{P_Y(y_j)}$$

を代入してみると

$$H(X \mid Y) = -\sum_{j=1}^{m} \sum_{i=1}^{n} P_Y(y_j) \frac{P_{XY}(x_i, y_j)}{P_Y(y_j)} \log_2 \frac{P_{XY}(x_i, y_j)}{P_Y(y_j)}$$

$$= -\sum_{j=1}^{m} \sum_{i=1}^{n} P_{XY}(x_i, y_j) \log_2 \frac{P_{XY}(x_i, y_j)}{P_Y(y_j)}$$

相互情報量I(X;Y)

（３）相互情報量　I(X;Y)　Ｙを知って得たＸについての情報量

Ｙを知って得たＸについての情報量＝
（Ｘについてのあいまいさ）－（Ｙを知ったとき，Ｘについて残っているあいまいさ）
これを式にすると

$$I(X;Y)=H(X)-H(X\mid Y)$$

$$I(X;Y)=\sum_{i=1}^{n}-P_X(x_i)\log_2 P_X(x_i)+\sum_{j=1}^{m}\sum_{i=1}^{n}P_{XY}(x_i,y_j)\log_2\frac{P_{XY}(x_i,y_j)}{P_Y(y_j)}$$

$$=\sum_{j=1}^{m}\sum_{i=1}^{n}-P_{XY}(x_i,y_j)\log_2 P_X(x_i)+\sum_{j=1}^{m}\sum_{i=1}^{n}P_{XY}(x_i,y_j)\log_2\frac{P_{XY}(x_i,y_j)}{P_Y(y_j)}$$

$$=\sum_{j=1}^{m}\sum_{i=1}^{n}P_{XY}(x_i,y_j)\log_2\frac{P_{XY}(x_i,y_j)}{P_X(x_i)P_Y(y_j)}$$

となる．ＸとＹを入れ替えて考えると　$I(Y;X)=\sum_{i=1}^{n}\sum_{j=1}^{m}P_{YX}(y_j,x_i)\log_2\frac{P_{YX}(y_j,x_i)}{P_Y(y_j)P_X(x_i)}$

$P_{XY}(x_i,y_j)=P_{YX}(y_j,x_i)$　であるからI(X;Y)=I(Y;X)がなりたつ．

$$I(X;Y)=I(Y;X)$$

問13

X：実際の天気の（結合）確率分布，　Y：天気予報の（結合）確率分布が次のように与えられている．このとき，

$P_{XY}(x,y)$		Y		$P_X(x)$
		晴	雨	
X	晴	4/9	2/9	2/3
	雨	1/9	2/9	1/3
$P_Y(y)$		5/9	4/9	

（１）平均情報量H(X)を求めよ

（２）条件付エントロピーH(X|Y)を求めよ

（３）相互情報量I(X;Y)を求めよ

全て $\log_2 3, \log_2 5$を用いて表せ．

通信路の符号化

シャノンの第１定理（情報源符号化定理）では平均符号長をできるだけ短くするように，情報源系列を符号語系列に変換する情報源符号化について勉強した．しかし，情報源符号器の出力をそのまま通信路に入力すると，雑音などの通信路における誤りのため，通信路の出力が入力とは異なる符号語系列になる可能性がある．001101を送信符号とする．このとき通信路内で雑音が入り４ビット目が反転し，001001になってしまったとしよう．このとき，もし同じ符号を3回続けて送信するということにしておけば送信符号は000/000/111/111/000/111となる．ここで４ブロック目が雑音により011となったとしても0と１の多いほうに符号を決定するというルールにしておけば，011を111に訂正することができる．このように符号を冗長化することにより誤り訂正ができるようになる．

上記の符号化は繰り返し符号化とよばれる単純な符号化で送りたい情報ビット数に対して3倍，5倍，７倍のビット数を用いなければならない．

シャノンの第２定理（通信路符号化定理）は冗長度を無限大に漸近させなくとも（繰り返し符号化では明らかにそうなってしまう）任意の $\varepsilon > 0$ 対して十分長い符号長 n_0 が存在して $n > n_0$ ならば復号誤り率が ε 以下とできるような符号が存在することを主張する．

符号長の長さが必要となるものの繰り返し符号化と較べれば，魅力的な結果を述べていることがわかる．

通信路行列

通信路を送信記号$\{x_1, x_2, \cdots, x_s\}$を入力すると受信記号$\{y_1, y_2, \cdots, y_r\}$が出力されるというモデルで表そう．

送信記号x_iに対して受信記号がy_jとなる確率をp_{ij}とする．このp_{ij}の組を行列表現すると

$$T=\begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1r} \\ p_{21} & p_{22} & \cdots & p_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ p_{s1} & p_{s2} & \cdots & p_{sr} \end{pmatrix}$$

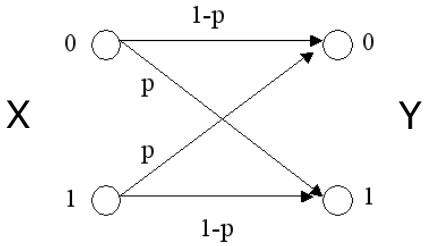
となるが，これを**通信路行列**という．

通信路のモデル

例　2元対称通信路(Binary Symmetric Channel)

送信記号及び受信記号が共に{0, 1}で0->1となる確率p_{01}と1->0となる確率p_{10}がともに等しくなる(=p)となる通信路である.

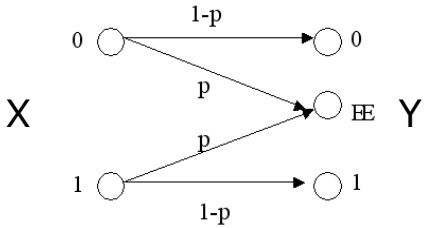
$$T = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$$



例　2元消失通信路(Binary Erasure Channel)

２元消失通信路とは 0 と 1 の中間に消失を表す記号を加えた通信路である．このモデルでは 1->0, 0->1 となる場合を考えない.

$$T = \begin{pmatrix} 1-p\,p & 0 \\ 0 & p1-p \end{pmatrix}$$



問14　次のような送信記号集合 A と通信路行列 T で表される通信路について以下の問いに答えよ．
（A の第２行はアルファベット a_i の発生確率を表し，また $B=\{b_1,b_2\}$ とする）．

$$A=\begin{Bmatrix} a_1, & a_2 \\ \frac{3}{4}, & \frac{1}{4} \end{Bmatrix}, T=\begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{10} & \frac{9}{10} \end{pmatrix}$$

（１）　受信記号の生起確率 $\mathrm{P}(b_1),\mathrm{P}(b_2)$ を求めよ．

（２）　$P(a_i \mid b_j)$，（i, j=1, 2）を求めよ．

問15　次のような送信記号集合 A, 受信記号 B と通信路行列 T で表される通信路について以下の問いに答えよ．　$B=\{b_1,b_2,b_3,b_4\}$ とする．

$$A=\begin{Bmatrix} a_1, & a_2 \\ \frac{3}{4}, & \frac{1}{4} \end{Bmatrix}, T=\begin{pmatrix} \frac{9}{10} & \frac{1}{10} & 0 & 0 \\ 0 & 0 & \frac{1}{5} & \frac{4}{5} \end{pmatrix}$$

（１）　通信路線図を描け

（２）　相互情報量 I(A;B)を求めよ．ヒント（１）から H(A|B)=0 がわかる．

問16　次のような送信記号集合 A, 受信記号 B と通信路行列 T で表される通信路について以下の問いに答えよ．　$B=\{b_1,b_2\}$ とする．

$$A=\begin{Bmatrix} a_1, & a_2, & a_3, & a_4 \\ \frac{1}{2}, & \frac{1}{4}, & \frac{1}{8}, & \frac{1}{8} \end{Bmatrix}, T=\begin{pmatrix} 10 \\ 10 \\ 01 \\ 01 \end{pmatrix}$$

（１）　通信路線図を描け

（２）　相互情報量 I(A;B)を求めよ．ヒント（１）から H(B|A)=0 がわかる．

通信路容量

定義　（通信路容量）送信記号$\{x_1,\cdots,x_s\}$の生起確率を$a=\{\alpha_1,\cdots\alpha_s\}$とする．
$a=\{\alpha_1,\cdots,\alpha_s\}$を変化させて得られる相互情報量I(X;Y)の最大値を通信路容量という．

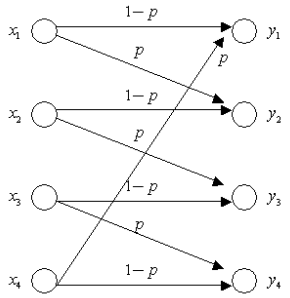
これは，通信路に情報源アルファベットが$\{x_1,\cdots,x_s\}$であるようなあらゆる情報源を接続してみたとき，受信Yから得られるXについての１記号あたりの情報量(相互情報量I(X;Y))の最大値を意味する．１記号あたりの情報量ということを明示するために単位は
ビット/記号を用いる．

問17　２元対称通信路の通信路容量はC=1−H(p)=

$$1+p\log_2 p+(1-p)\log_2(1-p)$$

であることを示せ.

問18　４つの送信記号 x_1, x_2, x_3, x_4 を図の誤りのある通信路を通して伝送する場合を考える．この通信路の通信路容量を計算せよ．（答）　$C=2+p\log_2 p+(1-p)\log_2(1-p)$



復号誤り率

通信路符号の性能を評価するためには，その符号を用いることで受信側において復号結果を誤る確率がどれだけ小さくできるかを調べる必要がある．$x_1, x_2, \cdots, x_s$:送信する符号語．

$g(x_i)$ ：受信側で x_i を送ったと判定する符号(符号語とは限らない)のグループとする．

$x \in g(x_i) \Rightarrow d_H(x, x_i) < d_H(x, x_j)$ $i \neq j$ とする（$d_H(u,v)$ はｕとｖの異なるビット数を表し，

ハミング距離という）．またこのような復号方法を最尤復号という．最尤復号については後で詳しく述べる．

最尤復号では送信記号は等確率で発生することを仮定する

このとき x_i を送信したとき受信側で正しく復号される確率は

$$\Pr(y_i \in g(x_i) | x_i)$$

であり， x_i を送信したとき受信側で誤る確率は

$$\Pr(y_i \notin g(x_i) | x_i) = 1 - \Pr(y_i \in g(x_i) | x_i)$$

である．全ての x_i について受信側で誤る確率を平均した確率を復号誤り率という．

定義（復号誤り率）

$$\Pr_E = \sum_{i=1}^{s} \Pr(x_i) \Pr(y_i \notin g(x_i) | x_i) = 1 - \sum_{i=1}^{s} \Pr(x_i) \Pr(y_i \in g(x_i) | x_i)$$

繰り返し符号の復号誤り率

問19　送信記号及び受信記号が共に{0, 1}で0->1となる確率 p_{01} と1->0となる確率 p_{10} がpである２元対称通信路を考える．0と１の２つの送信記号を同じ記号を３回繰り返して送るという符号化をして送信するとき，復号誤り率を計算せよ．復号は001ならば0, 101ならば1に復号といったように数の多い記号に復号するものとする（これは**最近傍復号**，送信記号の発生確率が等確率ならば**最尤復号**とよばれる）．

符号化率

送信したい情報の個数を M とする．この中から任意に 1 つの情報を選んで通信路に送り出すことにする．このとき 0, 1 で符号化すると最低 $k = \log_2 M \quad (= -\log_2 \frac{1}{M})$ 桁が必要になる. 今, 符号の長さを n(>k)とする. 符号化の冗長度を測る尺度として符号化率を導入する.

定義　（符号化率，伝送レート）

$$R = \frac{\log_2 M}{n}$$

もちろん，n=k とすれば最も効率が良いわけだが，これでは通信路で誤りが発生した場合，全く訂正できない．次の定理は，エラー無しの通信を行うためにはどの程度まで符号化率を高めることができるかということを示す大変重要な定理である.

通信路符号化定理

定理（通信路符号化定理）　通信路容量 C(ビット/記号)である通信路に符号化率 R(ビット/記号)で符号語を送信するものとする．このとき R<C ならば，$n \to \infty$ のとき，復号誤り率 Pr_E をいくらでも 0 に近づける符号が存在する．しかし，R>C ならば，そのような符号は存在しない．

これが，**シャノンの第２定理**である．

一般に通信路符号化定理が示すところは，R<C ならば，復号誤り率が無限に小さくなる符号化の存在を示しているだけであり，具体的符号化の方法を与えているわけではないことに注意しよう．また，通信路符号化定理は決められた符号長，符号語数で復号誤り率が無限に小さくできることをいっているわけではないことにも注意しよう．符号長 n を大きくしていったとき，符号語 M の数も増えるが，このような状況で復号誤り率をゼロにいくらでも近づけることができると言っているのである．具体的符号化の方法を与えているわけではないということが**符号理論**という分野を生み出したとも言える．

通信路符号化定理の証明(1)

通信路は2元対称通信路で送信誤り確率をpとする.

$R < C$とする．$\mathcal{C} = 2^{nR}$=2^k個の符号語からなる集合とする．よって符号化率=$\log_2 2^{nR} / n = k / n = R$.

$\mathbf{u}_i$: 送信語，$\mathbf{v}_i = \mathbf{u}_i + \mathbf{e}$：受信語，$d(\mathbf{u},\mathbf{v})$: $\mathbf{u}$と$\mathbf{v}$のハミング距離

およそnpビットが$\mathbf{u}_i$と$\mathbf{v}_i$は異なっている(nが大きいとき）ので

$$d(\mathbf{u}_i, \mathbf{v}_i) \approx np \qquad (1)$$

最尤復号では$\mathbf{v}_i$は$\mathbf{v}_i$に最も近い符号語$\Delta(\mathbf{v}_i)$に復号されるから復号が誤るときは$d(\mathbf{u}_j, \mathbf{v}_i) \le d(\mathbf{u}_i, \mathbf{v}_i)$をみたす$\mathbf{u}_j \in \mathcal{C}, (i \ne j)$が存在する．よって

$$\Pr_E \le \frac{1}{|\mathcal{C}|} \sum_{\mathbf{u}_j \ne \mathbf{u}_i} \sum_{\mathbf{u}_i \in \mathcal{C}} \Pr\left(d(\mathbf{u}_j, \mathbf{v}_i) \le d(\mathbf{u}_i, \mathbf{v}_i) = np\right) = \frac{1}{|\mathcal{C}|} \sum_{\mathbf{u}_j \ne \mathbf{u}_i} \sum_{\mathbf{u}_i \in \mathcal{C}} \Pr\left(d(\mathbf{u}_j, \mathbf{v}_i) \le np\right) \qquad (2)$$

ここで$\mathcal{C}$は2^nから2^k個の符号語を無作為に選んだ符号（ランダム符号）としてこれに関する両辺の平均をとると(2)の右辺は

$$\frac{1}{|\mathcal{C}|}(|\mathcal{C}|-1)|\mathcal{C}|\Pr(d(\mathbf{u},\mathbf{v}) \le np) = (|\mathcal{C}|-1)\Pr(d(\mathbf{u},\mathbf{v}) \le np)$$

とできる(ジョーンズ-ジョーンズのp. 161-162に詳しく書いてある）.

ここで$\mathbf{u}, \mathbf{v}$は上式をみたす$\{0,1\}^n$の任意の元.

通信路符号化定理の証明(2)

ランダム符号の平均をとっているので$\Pr_E$ではないことに注意.

よって

$$\overline{\Pr_E} \le |\mathcal{C}| \Pr(d(\mathbf{u},\mathbf{v}) \le np) \qquad (3)$$

CはBSCの通信路容量

$$\Pr(d(\mathbf{u},\mathbf{v}) \le np) = \frac{1}{2^n}\sum_{i \le np}\binom{n}{i} \le \frac{1}{2^n} 2^{nH(p)} = 2^{-n(1-H(p)} = 2^{-nC}$$

(3)式へ代入すると

$$\overline{\Pr_E} \le 2^{nR-nC} = 2^{n(R-C)} \to 0 \quad (as\ n \to \infty)$$

平均として復号誤り率が0に収束するわけだから少なくとも1つは復号誤り率$\Pr_E \to 0 \quad (as\ n \to \infty)$が存在しなければならない.

どのような符号であるかは不明

途中の不等式の証明

$p+q=1\ (0 \le p \le 1/2)$ とする.

$$1=(p+q)^n \ge \sum_{i \le pn}\binom{n}{i} p^i q^{n-i} = \sum_{i \le pn}\binom{n}{i}\left(\frac{p}{q}\right)^i q^n \ge \sum_{i \le pn}\binom{n}{i}\left(\frac{p}{q}\right)^{pn} q^n = \sum_{i \le pn}\binom{n}{i} p^{pn} q^{(1-p)n} = \sum_{i \le pn}\binom{n}{i} p^{pn} q^{qn}$$

よって $$\sum_{i \le pn}\binom{n}{i} \le p^{-pn} q^{-qn} = 2^{n(-p\log_2 p - q\log_2 q)} = 2^{nH(p)}$$

ディジタル変調の観点から

さらに進んで情報理論や符号理論の論文を読んで行く場合，最尤復号を行った際のビットエラー率が情報ビット当たりの搬送波のエネルギーとノイズのエネルギーの比で詳しい説明なしに表されることに戸惑ってしまう場合が多いように思います．おそらく，この辺が敷居の高さを高めていて，面白そうに思っても数学分野の人がこの分野に入って行きにくい原因の１つになっているような気がします．この講義では，その敷居の高さを低くすることを目指してみます．

$\varphi:[0,T]$ にサポートをもち（$[0,T]$以外では$\varphi\equiv 0$ということ）

$$\int_0^T \varphi(t)^2\,dt = 1$$

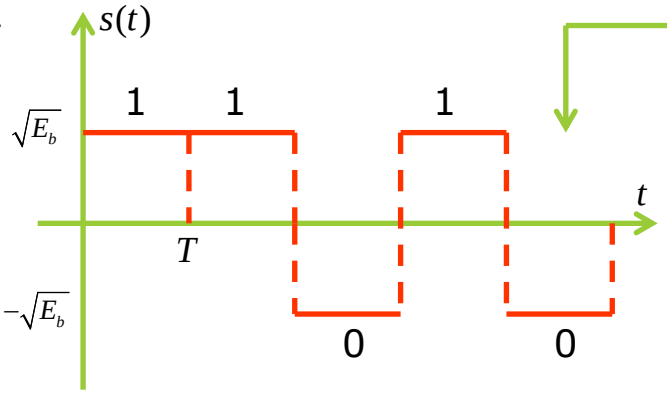
を満たすものとする．このとき搬送波を

$$s(t)=\sum_i a_i\varphi(t-iT),\quad (a_i=\sqrt{E_b}\text{または}-\sqrt{E_b})$$

で表す．このとき

$$\int_{iT}^{(i+1)T} s(t)^2\,dt=\int_{iT}^{(i+1)T} E_b\varphi(t-iT)^2\,dt=E_b\int_0^T \varphi(t)^2\,dt=E_b$$

である．



$\varphi(t)=\sqrt{\frac{1}{2}}\sin(\frac{2\pi nt}{T})$　でもよい．

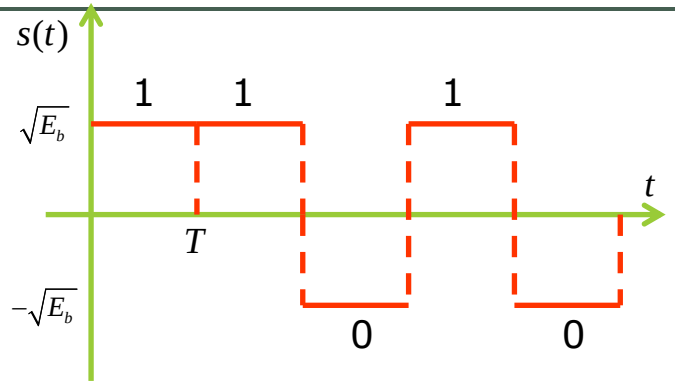
（いや，その方が良いかも）

$$\begin{cases} a_i=\sqrt{E_b} \Rightarrow \text{送信データ}=1 \\ a_i=-\sqrt{E_b} \Rightarrow \text{送信データ}=0 \end{cases}$$

を表すこととする．この送信方法を

Binary Phase Shift Keying(BPSK)変調という．

BPSK変調信号の復号



$$\begin{cases} a_i = \sqrt{E_b} \Rightarrow \text{送信データ} = 1 \\ a_i = -\sqrt{E_b} \Rightarrow \text{送信データ} = 0 \end{cases}$$

従ってE_bの意味は1情報ビットの送信に要する電力である.

受信信号$r(t)$は送信$s(t)$にノイズ$n(t)$が加わったものになる.

$$r(t) = s(t) + n(t)$$

格好つけた言い方をすると
マッチドフィルタリングという

復号は

$$R_i = \int_{iT}^{(i+1)T} r(t)\varphi(t-iT)dt = \int_{iT}^{(i+1)T} (s(t)+n(t))\varphi(t-iT)dt = \sum_j \int_{iT}^{(i+1)T} a_j\varphi(t-jT)\varphi(t-iT)dt + \int_{iT}^{(i+1)T} n(t)\varphi(t-iT)dt$$

$$= \delta_{ij}\int_{iT}^{(i+1)T} a_j\varphi(t-jT)\varphi(t-iT)dt + \int_{iT}^{(i+1)T} n(t)\varphi(t-iT)dt = a_i + \int_{iT}^{(i+1)T} n(t)\varphi(t-iT)dt$$

$$\begin{cases} R_i > 0 \Rightarrow 1\text{に復号} \\ R_i \le 0 \Rightarrow 0\text{に復号} \end{cases}$$

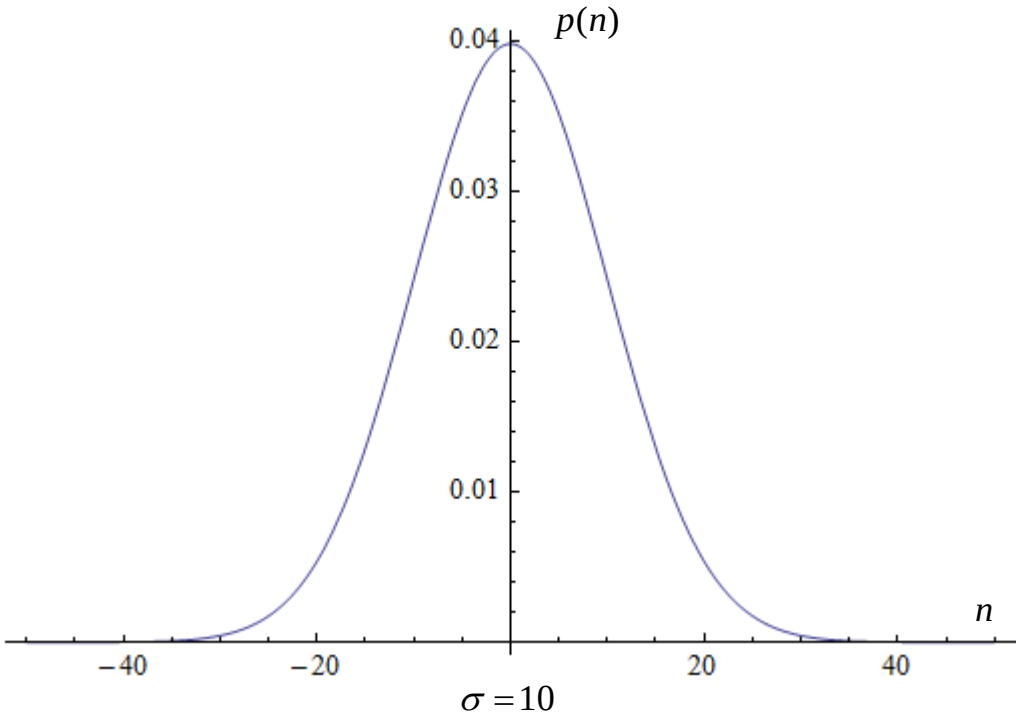
とする. よって$a_i = \sqrt{E}$のときでも $\int_{iT}^{(i+1)T} n(t)\varphi(t-iT)dt \le -\sqrt{E}$ ならば, i番目のデータは0に復号してしまう.

ノイズについて

ノイズは平均0，分散をσとして$\sigma^2 = N_0 / 2$の正規分布に従うとする．すなわち確率密度関数が

$$p(n) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{n^2}{2\sigma^2}}$$

とする．



最尤推定(1)

定理

$R=\mathbf{r}$を受信したとき，

$$\hat{s}=\arg\max_{\mathbf{s}\in\mathcal{S}} p(\mathbf{S}=\mathbf{s}\,|\,R=\mathbf{r})$$

達成する$\mathbf{s}$を復号とすれば，復号誤り率を最小とできる．

（証明）なんだか自明なような気がしますが，では証明してみなさいと言われると以下のようになるのではないでしょうか．

$\Omega_i=\{\mathbf{r}\,|\,\text{decide }\hat{s}=\mathbf{s}_i\}$，$\Omega=\bigcup_{i=1}^{M}\Omega_i$　とすると　$\mathbf{s}_i$を送信したとき，正しく復号する確率は

$$p(\hat{s}=\mathbf{s}_i\,|\,\mathbf{S}=\mathbf{s}_i)=\int_{\Omega_i} p(\mathbf{r}\,|\,\mathbf{s}_i)d\mathbf{r}$$

よって正しく復号する確率は　$\{\mathbf{s}_i\}$に関する平均をとって

$\mathbf{r}$はこの量が最大となるΩ_iに割り当てる

$$P(\mathcal{C})=\sum_{i=1}^{M}\int_{\Omega_i} p(\mathbf{r}\,|\,\mathbf{s}_i)\,p(\mathbf{S}=\mathbf{s}_i)d\mathbf{r}=\sum_{i=1}^{M}\int_{\Omega_i} p(\mathbf{S}=\mathbf{s}_i\,|\,\mathbf{R}=\mathbf{r})\,p(\mathbf{R}=\mathbf{r})d\mathbf{r}$$

$P(\mathcal{C})$を最大とするためには　$\Omega_i=\{\mathbf{r}\,|\,p(\mathbf{S}=\mathbf{s}_i\,|\,\mathbf{R}=\mathbf{r})>p(\mathbf{S}=\mathbf{s}_j\,|\,\mathbf{R}=\mathbf{r}),\ i\neq j\}$　とすればよい．

固定した$\mathbf{r}$に対して$\mathbf{S}$はこの量が最大となる$\mathbf{S}=\mathbf{s}_i$に割り当てられている

最尤推定(2)

ベイズの法則より

$$\hat{s} = \arg\max_{\mathbf{s}\in\mathcal{S}} p(\mathbf{S}=\mathbf{s}\,|\,R=\mathbf{r}) = \arg\max_{\mathbf{s}\in\mathcal{S}} \frac{p(\mathbf{R}=\mathbf{r}\,|\,\mathbf{S}=\mathbf{s})\,p(\mathbf{S}=\mathbf{s})}{p(R=\mathbf{r})} = \arg\max_{\mathbf{s}\in\mathcal{S}} p(\mathbf{R}=\mathbf{r}\,|\,\mathbf{S}=\mathbf{s})\,p(\mathbf{S}=\mathbf{s})$$

最尤推定では$p(\mathbf{S}=\mathbf{s}_i)=1/M\ \ (i=1,\ldots M)$を仮定するから

$$\hat{s} = \arg\max_{\mathbf{s}\in\mathcal{S}} p(\mathbf{R}=\mathbf{r}\,|\,\mathbf{S}=\mathbf{s})$$

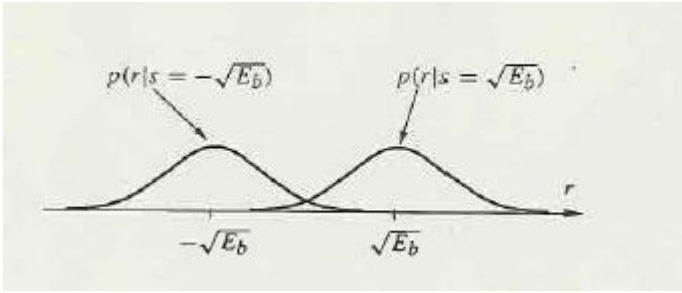
となる.

この量を最大にする $\hat{s}$ を選ぶ推定を最尤推定とよぶ.

$p(R=\mathbf{r}\,|\,\mathbf{S}=\mathbf{s})$は通信路行列から直接わかる量なので計算可能である.

2元対称通信路を考える. $d_H(\mathbf{r},\mathbf{s})=m$とする（受信$\mathbf{r}$と送信$\mathbf{s}$は$m$ビット異なる）.
このとき$p(R=\mathbf{r}\,|\,\mathbf{S}=\mathbf{s})=p^m(1-p)^{n-m}$だから$m$が最小となるような$\mathbf{s}$を復号とすれば最尤復号となる.
すなわち最尤復号は$\mathbf{r}$からのハミング距離が最小となるような符号である.

BPSK変調の場合



$$\mathcal{S}=\{-\sqrt{E_b},\sqrt{E_b}\}$$

$$p(r\mid s=\sqrt{E_b})=\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{1}{2\sigma^2}\left(r-\sqrt{E_b}\right)^2\right),\quad p(r\mid s=-\sqrt{E_b})=\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{1}{2\sigma^2}\left(r+\sqrt{E_b}\right)^2\right)$$

だから $\hat{s}=\begin{cases}\sqrt{E_b} & \text{if } r>0\\ -\sqrt{E_b} & \text{if } r\le 0\end{cases}$

$Q(x):=\frac{1}{\sqrt{2\pi}}\int_x^\infty \exp(-t^2/2)dt$ とおくと $s=-\sqrt{E_b}$のときの復号誤り率$P(\mathcal{E}|\, s=-\sqrt{E_b})$は

$$P(\mathcal{E}\mid s=-\sqrt{E_b})=\int_0^\infty p(r\mid s=-\sqrt{E_b})dr=\frac{1}{\sqrt{2\pi}\sigma}\int_0^\infty \exp\left(-\frac{1}{2\sigma^2}\left(r+\sqrt{E_b}\right)^2\right)dr$$

$$=\frac{1}{\sqrt{2\pi}}\int_{\frac{\sqrt{E_b}}{\sigma}}^\infty \exp\left(-\frac{t^2}{2}\right)dt=Q\left(\frac{\sqrt{E_b}}{\sigma}\right)=Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$$

同様に

$$P(\mathcal{E}\mid s=\sqrt{E_b})=Q\left(\frac{\sqrt{E_b}}{\sigma}\right)=Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$$

BPSK変調におけるビットエラー率

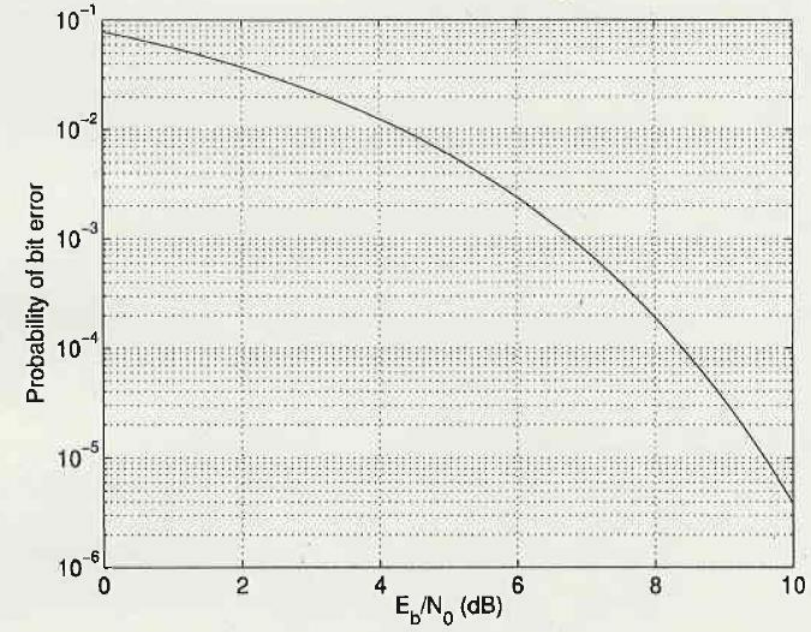


Figure 1.10: Probability of error for BPSK signaling.

$$P(\mathcal{E} \mid s = \pm\sqrt{E_b}) = Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$$

$$\frac{E_b}{N_0}\ (\text{dB}) = 10\log_{10}\left(\frac{E_b}{N_0}\right)$$

符号化率R＝k/nの符号の BPSK変調におけるビットエラー率

総エネルギー=$E_b \times k$

総エネルギー=$E_b \times k$ をn ビットに配分しなければならないから符号１ビット当たりの送信に要する電力（エネルギー）は$\frac{E_b k}{n} = E_b R$となる．$R<1$だからBPSKのE_bから減少することがわかる．

すなわち

$$P(\mathcal{E} \mid s = \pm\sqrt{E_b}) = Q\left(\sqrt{\frac{2RE_b}{N_0}}\right)$$

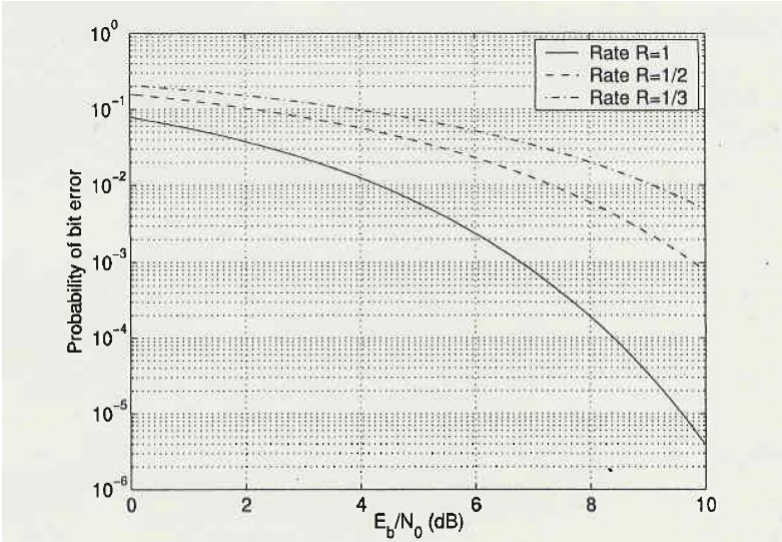


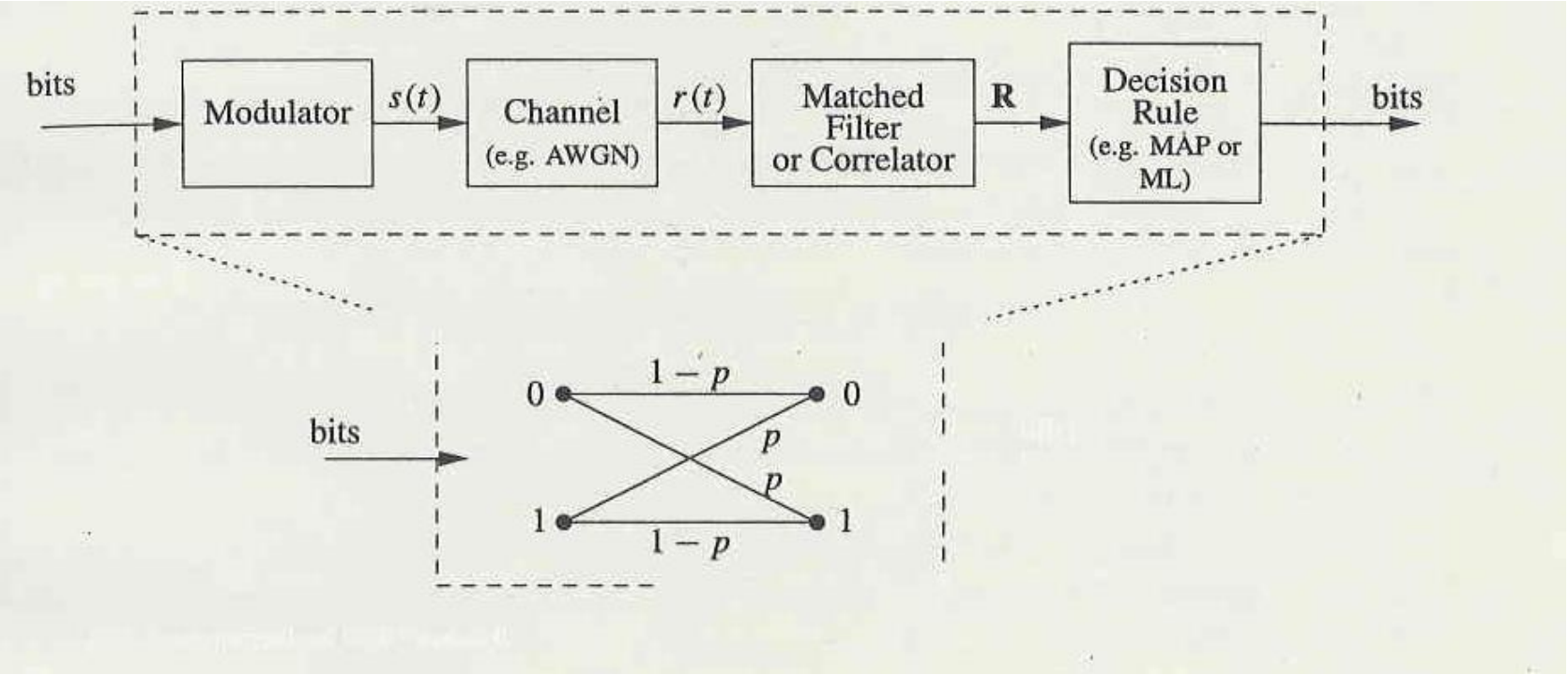
Figure 1.15: Probability of error for coded bits, before correction.

2元対称通信路のビットエラー率とBPSK変調におけるビットエラー率

2元対称通信路のビットエラー率pは

$$p = P(\mathcal{E} \mid s = \pm\sqrt{E_b}) = Q\left(\sqrt{\frac{2RE_b}{N_0}}\right)$$

と考えることができる.



BPSK変調通信路における シャノン限界(1)

2元対称通信路のビットエラー率pはE_b / N_0の関数として

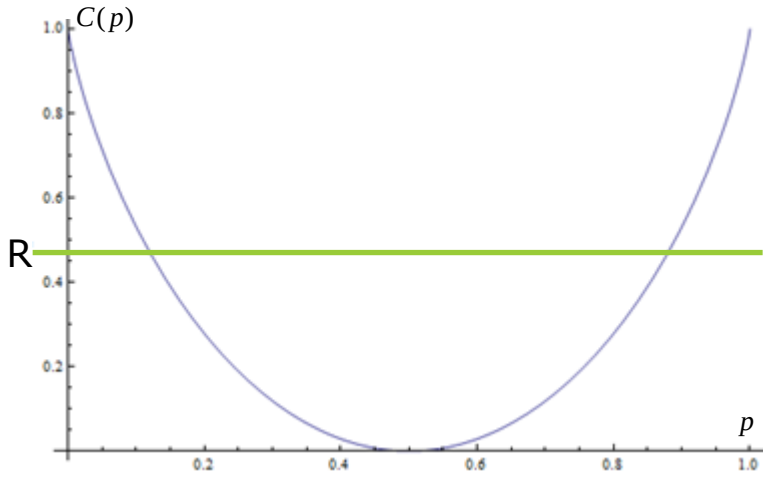
$$p\left(\frac{E_b}{N_0}\right) == Q\left(\sqrt{\frac{2RE_b}{N_0}}\right)$$

と考えることができ,

$\lim_{E_b/N_0 \to \infty} p\left(\frac{E_b}{N_0}\right) = 0$でありかつ, $p\left(\frac{E_b}{N_0}\right)$は$E_b / N_0$に関して単調減少. また通信路容量

$C(p) = 1 + p\log_2 p + (1-p)\log_2(1-p)$

は$0 \le p \le 1/2$で単調減少.



よってある定数$c_{Shannon-H}$が存在して$E_b / N_0 > c_0$ならは

$$C\left(\frac{E_b}{N_0}\right) > R$$

となる.

この定数$c_{Shannon-H}$のことをBPSK変調通信路における

シャノン限界という.

すなわち$E_b / N_0 > c_{Shannon-H}$ならば$C > R$となるわけ

だから通信路符号化定理よりnを大きくとれば

復号誤り率を任意に小さくできる.

BPSK変調通信路における シャノン限界（2）

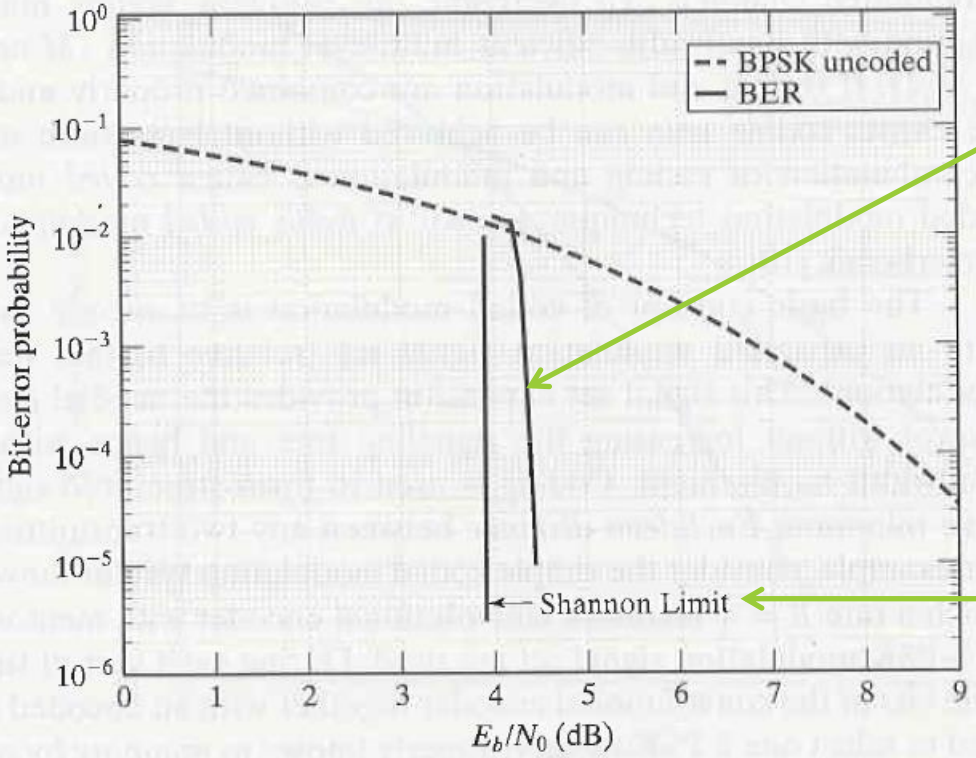


FIGURE 1.12: Bit-error performance of a (65520,61425) low-density parity check code decoded with a soft-decision near-MLD algorithm.

LDPC符号がシャノン限界付近で良い復号性能をもっていることがわかる

このシャノン限界は Binary Additive White Gaussian Noise Channel (BAWGNC通信路の通信路容量に基づいて計算した値である）

間違えやすいところのように思いますが，2元対称通信路の通信路容量に基づく計算ではないことに注意！

BPSK変調通信路における シャノン限界(3)

BAWGNC

BSC

Table 1.1. E_b/N_0 limits for various rates and channels

Rate R	$(E_b/N_0)_{\text{Shannon}}$ (dB)	$(E_b/N_0)_{\text{soft}}$ (dB)	$(E_b/N_0)_{\text{hard}}$ (dB)
0.05	−1.440	−1.440	0.480
0.10	−1.284	−1.285	0.596
0.15	−1.133	−1.126	0.713
0.20	−0.976	−0.963	0.839
1/4	−0.817	−0.793	0.972
0.30	−0.657	−0.616	1.112
1/3	−0.550	−0.497	1.211
0.35	−0.495	−0.432	1.261
0.40	−0.333	−0.236	1.420
0.45	−0.166	−0.030	1.590
1/2	0	0.187	1.772
0.55	0.169	0.423	1.971
0.60	0.339	0.682	2.188
0.65	0.511	0.960	2.428
2/3	0.569	1.059	2.514
0.70	0.686	1.275	2.698
3/4	0.860	1.626	3.007
4/5	1.037	2.039	3.370
0.85	1.215	2.545	3.815
9/10	1.396	3.199	4.399
0.95	1.577	4.190	5.295

*n*回繰り返し符号で出力値の合計に基づいて0, 1を判定する場合など

BAWGNC通信路では，入力Xはバイナリ(0または1) だが，出力Yは連続値(−∞， ∞)を許す．
従って通信路容量：Yを知ったときXについて得る情報量は増大する．

よってBSCの場合より小さいE_b / N_0の値で同じ通信路容量を達成する．
つまりシャノン限界は小さくなる．

BAWGNCの通信路容量

$$I(X;Y)=\sum_{j=1}^{m}\sum_{i=1}^{n}P_{XY}(x_i,y_j)\log_2\frac{P_{XY}(x_i,y_j)}{P_X(x_i)P_Y(y_j)}$$

問20

$$H(Y)=\frac{1}{2}\log_2 2\pi e\sigma^2$$

であることを示せ.

Yが実数全体をとるときは

$$I(X;Y)=\int_{-\infty}^{\infty}\sum_{i=1}^{n}P_{XY}(x_i,y)\log_2\frac{P_{XY}(x_i,y)}{P_X(x_i)P_Y(y)}dy=\int_{-\infty}^{\infty}\sum_{i=1}^{n}P_{Y|X}(y\mid x_i)P_X(x_i)\log_2\frac{P_{Y|X}(y\mid x_i)}{P_Y(y)}dy$$

$$=\int_{-\infty}^{\infty}\sum_{i=1}^{n}P_{Y|X}(y\mid x_i)P_X(x_i)\log_2\frac{P_{Y|X}(y\mid x_i)}{\sum_{j=1}^{n}P_{Y|X}(y\mid x_j)P_X(x_j)}dy$$

$X=\{-\sqrt{E_b},\sqrt{E_b}\},\ p(X=-\sqrt{E_b})=p(X=\sqrt{E_b})=1/2,\ N\sim\mathcal{N}(0,\sigma^2)$とする.　BAWGNC通信路の通信路容量は

$$C=I(X;Y)=\frac{1}{2}\left[\int_{-\infty}^{\infty}p(y\mid\sqrt{E_b})\log_2\frac{p(y\mid\sqrt{E_b})}{\frac{1}{2}\left(p(y\mid\sqrt{E_b})+p(y\mid-\sqrt{E_b})\right)}+p(y\mid-\sqrt{E_b})\log_2\frac{p(y\mid-\sqrt{E_b})}{\frac{1}{2}\left(p(y\mid\sqrt{E_b})+p(y\mid-\sqrt{E_b})\right)}dy\right]$$

$$=\frac{1}{2}\Big[\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(y-\sqrt{E_b})^2}{2\sigma^2}\right)\log_2\left(\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(y-\sqrt{E_b})^2}{2\sigma^2}\right)\right)+\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(y+\sqrt{E_b})^2}{2\sigma^2}\right)\log_2\left(\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(y+\sqrt{E_b})^2}{2\sigma^2}\right)\right)$$

$$-\left(p(y\mid\sqrt{E_b})+p(y\mid-\sqrt{E_b})\right)\log_2\left(\frac{1}{2}\left(p(y\mid\sqrt{E_b})+p(y\mid-\sqrt{E_b})\right)\right)dy\Big]$$

$$=\frac{1}{2}\left[-H(Y)-H(Y)-\int_{-\infty}^{\infty}\left(p(y\mid\sqrt{E_b})+p(y\mid-\sqrt{E_b})\right)\log_2\left(\frac{1}{2}\left(p(y\mid\sqrt{E_b})+p(y\mid-\sqrt{E_b})\right)\right)dy\right]$$

$$=-\int_{-\infty}^{\infty}\phi(y,E_b,\sigma^2)\log_2\phi(y,E_b,\sigma^2)dy-\frac{1}{2}\log_2 2\pi e\sigma^2$$

ここで$\phi(y,E_b,\sigma^2)=\frac{1}{\sqrt{8\pi\sigma^2}}\left[\exp\left(-\frac{(y-\sqrt{E_b})^2}{2\sigma^2}\right)+\exp\left(-\frac{(y+\sqrt{E_b})^2}{2\sigma^2}\right)\right]$

BPSK変調で$R=1/2$のとき，$(E_b/N_0)_{hard}$と$(E_b/N_0)_{soft}$の計算をmathematicaで行ってみる．

$(E_b/N_0)_{hard}$の計算

$\sqrt{\frac{2RE_b}{N_0}}=1.2264$である．

Shannon.nb *

```
E_b / N_ 0 (Soft) E_b is average energy per information bit

Hard

FindRoot[-p * Log[2, p] - (1 - p) * Log[2, (1 - p)] - 0.5 == 0, {p, 0.1}]

{p → 0.110028}

(-p * Log[2, p] - (1 - p) * Log[2, (1 - p)]) /. {p → 0.11002786443835955`}

0.5

NIntegrate[1/Sqrt[2 * Pi] * Exp[-(t^2) / 2], {t, 1.2264, Infinity}]

0.110024

10 * Log[10, (1.2264)^2]

1.77264
```

$(E_b/N_0)_{soft}$の計算

問21（レ）
例にならってBPSK変調で$R=2/3$のとき，
$(E_b/N_0)_{hard}$を求めよ．また
$(E_b/N_0)_{soft}=1.059$(dB)であることを確かめよ．

```
Soft

R = 1 / 2;
x = 10^(0.187 / 10);
sig = Sqrt[2 * R * x]^(-1);
p[y_] :=
 0.5 * (1/Sqrt[2 * Pi] * sig * Exp[-((y - 1)^2) / (2 * sig^2)] +
    1/Sqrt[2 * Pi] * sig * Exp[-((y + 1)^2) / (2 * sig^2)])
-NIntegrate[p[y] * Log[2, p[y]], {y, -Infinity, Infinity}] - 0.5 * Log[2, 2 * Pi * E * sig^2]

0.499995
```

R=C=1/2であることを確かめた．

X, Yが共に実数全体のとき

$X \sim \mathcal{N}\left(0, {\sigma_x}^2\right), N \sim \mathcal{N}\left(0, {\sigma_n}^2\right)$, $Y = X + N$とする.　よって$Y \sim \mathcal{N}\left(0, {\sigma_x}^2 + {\sigma_n}^2\right)$.

この通信路はAWGNC(Additive White Gaussian Noise Channel)とよばれ, その通信路容量は

$$C = I(X;Y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} P_{XY}(x,y)\log_2 \frac{P_{XY}(x,y)}{P_X(x)P_Y(y)}\,dxdy = I(Y;X) = H(Y) - H(Y \mid X) =$$

$$H(Y) - H(X+N \mid X) = H(Y) - H(N \mid X) = H(Y) - H(N)$$

$$= \frac{1}{2}\log_2 2\pi e{\sigma_y}^2 - \frac{1}{2}\log_2 2\pi e{\sigma_n}^2 = \frac{1}{2}\log_2 \frac{{\sigma_y}^2}{{\sigma_n}^2} = \frac{1}{2}\log_2\left(1 + \frac{{\sigma_x}^2}{{\sigma_n}^2}\right)$$

$$\therefore C = \frac{1}{2}\log_2\left(1 + \frac{{\sigma_x}^2}{{\sigma_n}^2}\right)$$ ← シャノンーハートレ

問22(レ)

$Y \sim \mathcal{N}(0, {\sigma_x}^2 + {\sigma_n}^2)$

であることを示せ.

問23

$R = 1/2$のとき, この通信路のシャノン限界

$E_b / N_0 = 0$ (dB)であることを示せ.

この値を$c_{Shannon}$で表すことがある.