InfoCom Be-TEXT　「情報・符号理論」

演習問題解答例

平成 24 年 4 月 1 日

第 1 章

問 1.1

データのディジタル化は、通信技術に限らず、あらゆる分野で進んでいる。たとえば写真を例にとると、ディジタルカメラの画像データはディジタルデータである。一方、フィルムを使う従来のカメラは、光をフィルム上に塗られた薬品の化学的な変化として記録しており、データが離散化されていないので、アナログデータととらえることができる。この例におけるディジタルデータの得失は、次のように考えられる。まず、“得”、すなわち良いところは、画像をディジタルデータとして１と０だけで表現することにより、写真の完璧な複製が可能となることである。つまり、１と０の系列を保存しておけば、まったく同一の写真を再現できるのである。しかし、“失”、すなわちアナログデータに劣る点として、量子化誤差による画質の劣化が挙げられる。光の色は本来、連続的に変化している。白から黒への変化も、そこには無限の数の「灰色」の階調がある。しかしディジタル化することで、それらの色を、有限の数の符号語で表現しなくてはならないため、階調の数が有限となってしまう。このことは、ディジタルデータによる写真の色は、本来の色から変化してしまっていることを意味する。

問 1.2

音楽や音声は、物理的には空気の振動であるが、マイクロフォンにより電圧の振動に変換される。レコードは、プラスチックの板の上に、電圧の波形をそのまま記録したものである。一方、コンパクトディスク（CD）に記録されているのは、符号である。つまり、マイクロフォンから出力された電圧の波形を標本化し、量子化を経て、符号化する。この符号とは、１と０からなる系列であり、これが CD に記録されている。

問 1.3

CD プレーヤーは、CD 上に記録された符号を読み取っている。しかし、そこに記録されているのは１か０のいずれかしかない。このため、図 1.6 に示すように、読み取った値をある基準値に照らして、それより大きければ１、そうでなければ０であると判定することで、符号の読み取り時に発生する誤りをある程度、避けることができる。また、符号で音楽を

記録している CD では、誤り訂正符号を用いることができるため、さらに誤りを少なくすることができる。

問 1.4

量子化の影響を軽減するためには、符号語の数を増やせばよい。そうすれば、それぞれの符号語に割り当てられた電圧の値の間隔が小さくなるので、量子化誤差も小さくなるからである。符号語の数を増やすためには、符号語の長さ、つまりビット数を大きくする。

第 2 章

問 2.1

無記憶情報源の例として、宝くじの当り・はずれが考えられる。宝くじを複数枚買って、ある 1 枚の宝くじが当たってもはずれても、次の 1 枚の当たり外れに関係ないから、宝くじを情報源、当り、またははずれを情報源シンボルと考えると、これは無記憶情報源としてモデル化できる。一方、記憶のある情報源として、食事のメニューが考えられる。多くの人は、昼食に食べたものと同じものを夕食で再び食べることを避ける。人を情報源、食事のメニューを情報源シンボルと考えると、ある食事は次の食事に影響を与えるので、記憶のある情報源としてモデル化を考えることができる。

問 2.2

問 2.1 で記憶のある情報源として考えた、食事の例を検討してみる。ある時の食事のメニュー選択が、過去の何回分の食事の選択の影響を受けるのかは、人によると言える。ここでは、過去 2 回分の影響を受けるものと仮定する。つまり、夕食は、その日の朝食と昼食の影響を受けて選択されると仮定するのである。すると、それは 2 重マルコフ情報源としてモデル化することができる。

問 2.3

状態遷移図は、図 2.3 のように描くことができる。

問 2.4

状態遷移確率行列は図 2.5 のように書ける。

問 2.5

ある状態から出ている矢印は、次の状態へ移る可能性があることを示しており、その確率が矢印に付して示されている。もし、ある状態から出る矢印に付された確率の合計が 1 となっていない、ということは、その状態から次への遷移のうち、記述されていないものがある、ということになる。すべての遷移が記述されていれば、必ず、確率の合計は 1 となるはずである。

問 2.6

状態遷移確率行列の各要素が示す確率の意味を考えると、この行列の各行の和は 1 になる、と言うことができる。

第 3 章

問 3.1

宝くじにはエルゴード性があるのが理想である。つまり、一人の人が同じ販売所で 1 枚ずつ 1000 枚の宝くじを買ったのと、1000 人の人が 1 枚ずつ、1000 箇所の販売所でそれぞれ宝くじを買ったとき、1000 枚当りの当選確率が同じであれば、宝くじにエルゴード性があると言える。

問 3.2

エルゴードマルコフ情報源は、過渡状態がなく、本質的な状態集合が 1 つしかない、という特徴がある。その結果、状態の遷移を長時間にわたって観察すると、次のような特徴がある。第 1 に、どの状態から出発しても、すべての状態が現れる。第 2 に、どの状態から出発しても、すべての状態が現れる確率が同一である。したがって、ひとつの初期状態から遷移を延々と重ねた結果、他の状態が現れる確率と、たくさんの異なる初期状態から 1 回の遷移を経て現れる状態の確率が一致する。この点に、エルゴード性があると解釈できる。

問 3.3

状態遷移確率行列のそれぞれの要素の確率の意味を考えると、$\mathbf{P}^{\infty}$ の各行が一致するということは、どの状態から出発しても、無限回の遷移の後、それぞれの状態にたどり着く確率は同じになる、ということを意味していると解釈できる。

問 3.4

省略

問 3.5

まず、$\mathbf{P}^{\infty}$ の要素は確率であるから、負の値にはなり得ない。次に、0 にならない理由は、次のように考えられる。ある要素が 0 になったとすれば、その要素に対応する状態は、無限回の遷移にもかかわらず、一度も現れることがない、ということを意味する。このことは、エルゴードマルコフ情報源の定義に反する。エルゴードマルコフ情報源の定義によれば、どの状態から遷移を開始しても、必ず、すべての状態が現れるはずだからである。したがって、$\mathbf{P}^{\infty}$ の各要素はかならず、0 より大きい値となるのである。

第 4 章

問 4.1

日本語の 1 文字あたりの情報量は、英語のそれよりも大きい。これは、日本語の文字が英語よりも多いことに由来する。たとえば、数値例として次のように考えられる。日本語の文字の数を、常用漢字 1945 文字に、ひらがなとカタカナをあわせて、2041 文字と仮定する。新聞を、無記憶情報源と仮定し、それぞれの文字の出現確率が同じであると考えると、1 文字あたりのシャノンの情報量は$\log_2 2041 \approx 11.0$ [bit]と計算できる。一方、英語の文字数を、アルファベットの大文字と小文字の合計 52 文字と仮定すると、1 文字あたりのシャノンの情報量は、$\log_2 52 \approx 5.7$ [bit]となって、日本語 1 文字の情報量より小さな値となることがわかる。

問 4.2

平均情報量は、情報源から出力されるすべての情報源シンボルの情報量の平均（期待値）であるが、その性質は、情報量の定義から、次のような一面を持つ。ある情報源が、どの情報源シンボルを出すのか、すでにわかっているときは、情報源が出力した情報源シンボルに情報はまったく無い。それは、感覚的には理解できることである。身近な例に照らせば、それは、いつも同じことを言う人の話が興味深くないことと同じである。何が出てくるか、完全にわかってしまっているものを出力として見ても、得られる情報はないのである。感覚的に理解できることのことを、シャノンの情報量の計算では、次のように示すことができる。つまり、出力される情報源シンボルがすでにわかっているとき、出現確率は 1 であると考えられるから、シャノンの情報量の定義から、$\log_2 1 = 0$ [bit]となって、情報が無い、ということと矛盾しない。では、逆に、情報量が大きい情報源とはどのような情報

源だと言えるだろうか。それは、今までの考察から考えれば、出力が予測できない情報源であると考えられる。出力が予測できる情報源は平均情報量が小さくなり、予測できない情報源の平均情報量は大きい、と言えるわけである。ここで、「予測できる」ということは、言い換えれば不確定性がない、ということであり、「予測できない」ということは、不確定性が高い、ということである。このため、平均情報量は、情報源の不確定性を現している、とも解釈することが可能である。

第 5 章

問 5.1

平均符号長が短いということは、端的に言えば、符号語の長さが短い、ということである。短い符号語は、伝送にかかる時間も当然ながら短い。このため、高速通信が実現できることから、符号語の長さは短ければ短いほどよい。

問 5.2

結果を下表に示す。

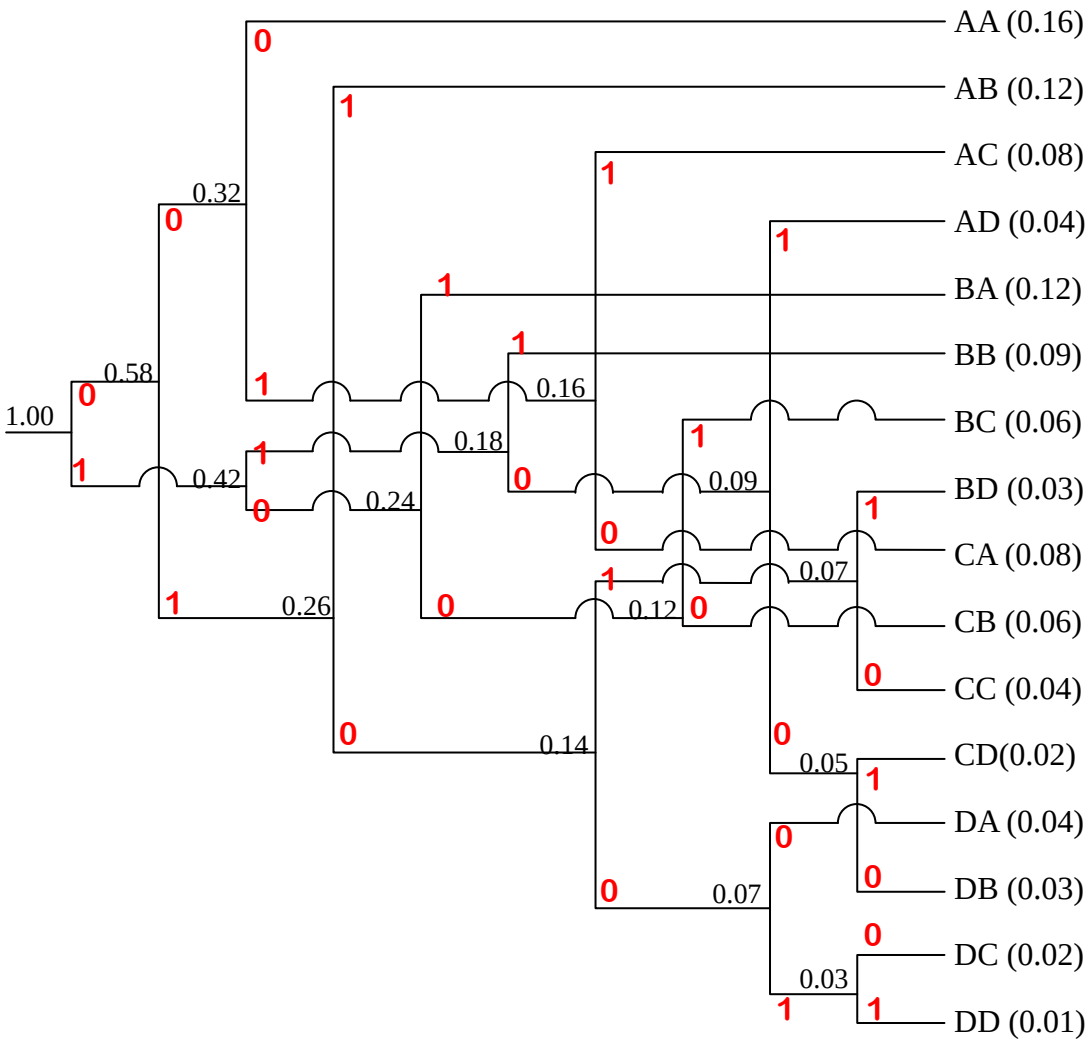
拡大情報源シンボル	出現確率
AA	0.16
AB	0.12
AC	0.08
AD	0.04
BA	0.12
BB	0.09
BC	0.06
BD	0.03
CA	0.08
CB	0.06
CC	0.04
CD	0.02
DA	0.04
DB	0.03
DC	0.02
DD	0.01

この表で、出現確率は次のように計算している。例えば、拡大情報源シンボル A と B が同

時に出現する確率であるから、表 5.3 より A の出現確率 0.4 と B の出現確率 0.3 の積として計算できる。

問 5.3

図 5.6 にならい、次のようにハフマン符号化を行う。



この結果、次のような符号が拡大情報源シンボルに対して割り当てられる。ただし、1 と 0 の割り当て方などにより他の符号も可能であり、下の表はその一例である。

拡大情報源シンボル	出現確率	ハフマン符号
AA	0.16	000
AB	0.12	011
AC	0.08	0011
AD	0.04	1101
BA	0.12	101
BB	0.09	111
BC	0.06	1001
BD	0.03	01011
CA	0.08	0010
CB	0.06	1000
CC	0.04	01010
CD	0.02	11001
DA	0.04	01000
DB	0.03	11000
DC	0.02	010010
DD	0.01	010011

問 5.4

平均符号語長は、それぞれの拡大情報源シンボルの長さと出現確率との積をすべて足せば良い。これを計算すると、3.37[bit]となる。これは、2 次の拡大の結果であるから、式(5.19)にならい、これを 2 で割ると、1.865[bit]となって、式(5.23)で得られた拡大前の情報源シンボルの平均符号語長より短くなっていることが確認できる。

第 6 章

問 6.1

$P(a_1 \mid b_1)$を事後確率と呼び、$P(b_1 \mid a_1)$を事前確率と呼ぶ。事後確率は、シンボルb_1を受信したとき、送信されていたのがシンボルa_1であった確率を意味している。反対に事後確率は、シンボルa_1を送信したとき、受信機がシンボルb_1を受信する確率を表している。

問 6.2

ベイズの定理により、式(6.1)のように関係付けられる。

問 6.3

事後情報量は、数式的には式(6.3)に定義されたように、事後確率によって求めた情報量である。しかし、それが意味するのは、雑音による通信路の不確定性を定量化しているものと解釈できる。

問 6.4

あいまい度は、受信シンボルから見た送信シンボルの不確定性を、すべての送信シンボルと受信シンボルの組み合わせにわたって平均したものである。

問 6.5

散布度は、送信シンボルから見た受信シンボルの不確定性を、すべての送信シンボルと受信シンボルの組み合わせにわたって平均したものである。

第 7 章

問 7.1

ARQ (automatic repeat request)は、受信機に送られたデータに誤りが生じていたとき、その部分を再送するよう、受信機が送信機に要求する仕組みである。再送されたデータが正しく受信されれば、誤りをなくすことができる。したがって ARQ を実現するには、データが誤っていることを受信機が知ることができなくてはならない。ここに用いられるのが、誤り検出符号である。一方、FEC は、forward error correction の頭文字をとったものであり、ここで forward は、送信機から受信機への方向を意味している。つまり、ARQ のように受信機から送信機へのフィードバックなしに、常に送信機から受信機への通信を行うだけで、誤り訂正を行う仕組みを指す。これを実現するのは、誤り訂正符号である。

問 7.2

誤り検出符号と誤り訂正符号の機能を実現する本質的なメカニズムは、これらの符号語間のハミング距離が大きいということである。これは、平たく言えば、符号語同士がよりたくさんのビットで異なっていることを指す。これにより、誤りを含んだ受信符号語が、も

ともと符号表に存在している符号語と重なることをなくすることができ、誤りの検出が可能となる。また、符号語間のハミング距離がさらに大きければ、誤りを含んだ受信符号語が最も近い符号語が正しい符号語であると判定することによって、誤り訂正が可能となる。

問 7.3

N ビットの 2 値系列の組み合わせは、2^N 種類ある。もし n ビットが区別できなくなれば、系列の種類は $2^{(N-n)}$種類に減る。つまり、$2^N/2^{(N-n)}=2^n$ 個の系列が識別できなくなる。

問 7.4

不確定集合とは、受信機から見て識別できない送信符号語のグループであった。上の問 7.3 における 2^n 個の識別できない系列の集合がまさにそれである。式(7.9)は、その不確定グループの数を求めているのであり、それには全体の符号語の数を、不確定集合に属する符号語の数で割ってやればよい。これが、式(7.9)の計算が行っていることである。

問 7.5

それは、無限に長い符号語長をもつ符号語である。符号語の長さが無限に長いと、符号語の種類が無限にできる。つまり、符号空間が無限に大きくなる。そこに属する符号語に、有限の数の情報源シンボルを割り当てれば、符号間距離が無限に大きくなる。このため、どれだけ誤りがたくさん生じても誤り検出・訂正が可能な符号語ができる。

問 7.6

しかし、問 7.5 で述べたような符号語は、長さが無限であるから、有限の時間で送信を完了することができない。つまり、送信できないということになる。また、無限に長くなくとも、非常に長い符号語を用いた場合、伝送に時間がかかる。このため、データ伝送速度が低下するという問題がある。

第 8 章

問 8.1

図 8.1 に示したような畳み込み符号器は、構造的にはトランスバーサルフィルタに等しい。トランスバーサルフィルタの出力は畳み込みという計算によって算出できる。このため、畳み込み符号をトランスバーサルフィルタの出力と見て、畳み込みによって符号化されるとの意味で、畳み込み符号と呼ばれる。

問 8.2

ビタビ復号器がなければ、受信機は復号の際、畳み込み符号と情報源符号との対応を示した符号表を持たなければならない。もし、情報源符号の長さが 100 ビットであった場合、その組み合わせは 2^{100} 個となるため、符号表は巨大なものとなってしまう。受信した符号語を、このような符号表に掲載されたすべての符号語と比較するためには長い時間がかかってしまう。ビタビ復号器は、このような方法を避け、符号表なし復号を可能とするアイデアである。

問 8.3

符号化率は、符号器の入力ビット数を分子に、出力ビット数を分母として計算し、符号化方式の効率を示す。これが低いと、短い入力に対して出力が長くなる符号器を意味し、一般に誤り訂正能力は高くなる。これは、入力された情報源符号の符号語を、より大きな符号空間に写像することを意味するからである。しかし一方で、符号語の長さが長くなると伝送に時間がかかるため、データ伝送速度は低下する。反対に、符号化率が高いと、一般に誤り訂正能力は低くなるが、データ伝送速度の低下は抑えられる。したがって、符号化率の大小は一長一短であって、誤り訂正能力に注目するか、伝送速度の注目するかによってその得失は異なる。

問 8.4

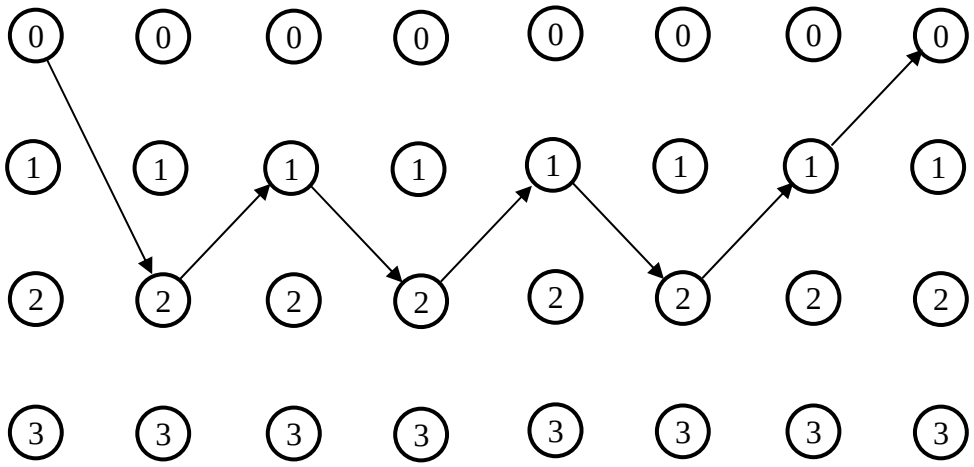
符号器として、図 8.1 に示す構成を想定する。データ系列を 10101 とし、符号器が最後に状態 0 で終わるよう、データ系列の末尾に 00 を付加する。ここではデータ系列 10101 の左が先頭であると考え、右端に 00 を付加することにして、符号器に入力するデータ系列は 1010100 とする。この系列を先頭から符号器に入力すると、符号器は下表のように動作する。

時刻	符号器入力（データ系列）	メモリの値		状態	符号器出力（符号語）	
		θ_1	θ_2		c_1	c_2
0	1	0	0	0	1	1
1	0	1	0	2	0	1
2	1	0	1	1	0	0
3	0	1	0	2	0	1
4	1	0	1	1	0	0
5	0	1	0	2	0	1
6	0	0	1	1	1	1
7	-	0	0	0	-	-

結局、得られた符号語は 11010001000111 となる。（※この符号語系列は、上の表で時刻 0 から 7 の順番に、$c_1, c_2, c_1, c_2,\ldots$の順番で符号器出力を並べたものである。）

問 8.5

図 8.1 の符号器のトレリス線図による表現は、図 8.3 のようであった。このトレリス線図に基づいて、ビタビ復号器により発見される生き残りパスは、下図のようになる。



第 9 章

問 9.1

数学の世界は、無限の数の数字とその演算によって構成されている。それに対して、ガロア体は、有限の数の数字とその演算によって数学世界を定義する。

問 9.2

$1x^4 + 0x^3 + 1x^2 + 0x^1 + 0x^0 = x^4 + x^2$

問 9.3

5 ビットの符号語 10110 で、右から 2 ビット目に誤りが生じたということは、元の符号語 10110 に、00010 が足された結果であると見ることができる。この 00010 を符号多項式で表せば x となり、これが、誤り多項式である。つまり、$E(x) = x$ である。

問 9.4

m 次の原始多項式の根αは、2^m-1 の周期を持つ。したがって、根の周期を調べることによって原始多項式かどうかを判定できる。$x^4 + x^3 + x^2 + 1$の根をα とすると、

$$\alpha^4+\alpha^3+\alpha^2+1=0$$

となるから、

$$\alpha^4=\alpha^3+\alpha^2+1$$

の関係があることがわかる。これを用いてαの周期を次のように求める。

$$\alpha^0=1$$
$$\alpha^1=\alpha$$
$$\alpha^2$$
$$\alpha^3$$
$$\alpha^4=\alpha^3+\alpha^2+1$$
$$\alpha^5=\alpha\alpha^4=\alpha^4+\alpha^3+\alpha=\left(\alpha^3+\alpha^2+1\right)+\alpha^3+\alpha=\alpha^2+\alpha+1$$
$$\alpha^6=\alpha\alpha^5=\alpha^3+\alpha^2+\alpha$$
$$\alpha^7=\alpha\alpha^6=\alpha^4+\alpha^3+\alpha^2=\left(\alpha^3+\alpha^2+1\right)+\alpha^3+\alpha^2=1$$

つまり、$\alpha^7=\alpha^0$となってしまい、周期は 7 であり、2^4-1=15 より短い。よって、$x^4+x^3+x^2+1$は原始多項式ではない。

問 9.5

上の問 9.4 と同様の方法で調べる。x^4+x+1の根をαとすると、

$$\alpha^4+\alpha+1=0$$

となるから、

$$\alpha^4=\alpha+1$$

の関係があることがわかる。これを用いてαの周期を次のように求める。

$$\alpha^0=1$$
$$\alpha^1=\alpha$$
$$\alpha^2$$
$$\alpha^3$$
$$\alpha^4=\alpha+1$$
$$\alpha^5=\alpha\alpha^4=\alpha(\alpha+1)=\alpha^2+\alpha$$
$$\alpha^6=\alpha\alpha^5=\alpha\left(\alpha^2+\alpha\right)=\alpha^3+\alpha^2$$
$$\alpha^7=\alpha\alpha^6=\alpha\left(\alpha^3+\alpha^2\right)=\alpha^4+\alpha^3=(\alpha+1)+\alpha^3=\alpha^3+\alpha+1$$
$$\alpha^8=\alpha\alpha^7=\alpha\left(\alpha^3+\alpha+1\right)=\alpha^4+\alpha^2+\alpha=(\alpha+1)+\alpha^2+\alpha=\alpha^2+1$$
$$\alpha^9=\alpha\alpha^8=\alpha\left(\alpha^2+1\right)=\alpha^3+\alpha$$
$$\alpha^{10}=\alpha\alpha^9=\alpha\left(\alpha^3+\alpha\right)=\alpha^4+\alpha^2=(\alpha+1)+\alpha^2=\alpha^2+\alpha+1$$

$$\alpha^{11} = \alpha\alpha^{10} = \alpha\left(\alpha^2 + \alpha + 1\right) = \alpha^3 + \alpha^2 + \alpha$$
$$\alpha^{12} = \alpha\alpha^{11} = \alpha\left(\alpha^3 + \alpha^2 + \alpha\right) = \alpha^4 + \alpha^3 + \alpha^2 = \left(\alpha + 1\right) + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1$$
$$\alpha^{13} = \alpha\alpha^{12} = \alpha\left(\alpha^3 + \alpha^2 + \alpha + 1\right) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \left(\alpha + 1\right) + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1$$
$$\alpha^{14} = \alpha\alpha^{13} = \alpha\left(\alpha^3 + \alpha^2 + 1\right) = \alpha^4 + \alpha^3 + \alpha = \left(\alpha + 1\right) + \alpha^3 + \alpha = \alpha^3 + 1$$
$$\alpha^{15} = \alpha\alpha^{14} = \alpha\left(\alpha^3 + 1\right) = \alpha^4 + \alpha = \left(\alpha + 1\right) + \alpha = 1$$

結果として$\alpha^{15} = \alpha^0$となり、周期は2^4-1=15 に等しい。よって、$x^4 + x + 1$は原始多項式である。

第 10 章

問 10.1

ポイント 10.2 から、次のように求められる。
$n = 2^4-1 = 15, \quad m = 4, \quad k = n-m = 11$

問 10.2

生成多項式が原始多項式であるとき、検査ビットの数 m は生成多項式の次数に等しく、符号語長 n は 2^m-1 となり、情報ビット数 k は n と m の差となる。この関係から計算すると、(n, k) = (3,1), (7,4), (15,11), (31,26),…などが可能であることがわかる。

問 10.3

10.2.2 項参照。

問 10.4

生成多項式が原始多項式でないとき、符号語の中で検査ビットの数が大きくなる。このため、同じ長さの符号語を使っても、生成多項式が原始多項式でないと、送ることができる情報のビット数が少なくなり、伝送効率が下がるのが問題である。

第 11 章

問 11.1

巡回符号も 1 ビットの誤りに対しては誤り訂正が可能であるが、2 ビット以上の誤りは訂正できない。理由は、あり得るすべての 2 ビット誤りの数に対して、シンドロームの数が

足りないからである。BCH 符号は、多項式の根の数を増やすことによってシンドロームの数を増やし、複数ビットの誤りを訂正できるようにしている。

問 11.2

例えば生成多項式を$G(x)=x^4+x+1$として、誤り多項式を$E_1(x)=x+1$とする。$G(x)$の根αには$\alpha^4=\alpha+1$の関係がある。このため巡回符号は、$E_1(x)=x+1$と$E_2(x)=x^4$を区別することができない。

問 11.3

BCH 符号で 2 ビット誤りに対処するためには、$G(x)$の根αに加え、α^3も根となる多項式を用いる。ここで$E_1(\alpha^3)$と$E_2(\alpha^3)$を計算すると、$E_1(\alpha^3)=\alpha^3+1$と$E_2(\alpha^3)=\alpha^3+\alpha^2+\alpha+1$が得られ、シンドロームは重ならない。このため、$E_1(x)$と$E_2(x)$を区別することができる。

問 11.4

$f(x)=x^4+x+1$を用いて情報系列「1111000」を 2 ビット誤り訂正可能な BCH 符号に符号化する。例 11.1 にならい、式(11.19)の$G(x)=M_1(x)M_3(x)=x^8+x^7+x^6+x^4+1$を用いる。すると、符号語長 n は$f(x)=x^4+x+1$より 2^4-1 = 15、検査ビット数 m は$G(x)$の次数 8、情報ビット数 k は $k = n$-$m = 7$ となって、(15,7)符号を構成できる。情報系列「1111000」を符号多項式で表現すると、$x^6+x^5+x^4+x^3$となり、この右側に検査ビット 8 ビットをつけるから、情報系列を左側に 8 ビットシフトすると、符号多項式は次のように計算できる。

$$W(x)=x^8\left(x^6+x^5+x^4+x^3\right)=x^{14}+x^{13}+x^{12}+x^{11}$$

次に、検査ビットの符号多項式$R(x)$を決定する。それは、$W(x)$を$G(x)$で割ったあまりとなり、これを計算すると次の結果が得られる。

$$R(x)=x^7+x^5+x^4+x^3+x+1$$

結局、符号語の符号多項式は次のように得られる。

$$F(x)=W(x)+R(x)=x^{14}+x^{13}+x^{12}+x^{11}+x^7+x^5+x^4+x^3+x+1$$

つまり、符号語は「111100010111011」となる。

問 11.5

はじめに、$f(x)=x^4+x+1$の根α及びα^3を用いてすべての 2 ビット誤りの誤り多項式に対応するシンドロームを調べ、その対応を表にしておく。ここでは簡単のため、「右から 5 ビット目と 8 ビット目に誤りが生じた時」のシンドロームだけを調べておく。このとき、誤り多項式は$E(x)=x^7+x^4$である。対応するシンドロームはそれぞれ$E(\alpha)=\alpha^3$及び$E(\alpha^3)=\alpha+1$と計算できる。次に、問 11.4 で求めた符号語に、「右から 5 ビット目と 8 ビット目に誤り」が生じた時の符号語は、次のように計算できる。

$$\tilde{F}(x)=F(x)+E(x)=x^{14}+x^{13}+x^{12}+x^{11}+x^5+x^3+x+1$$

αとα^3に対応するシンドロームは、次のように計算できる。

$$\begin{aligned}\tilde{F}(\alpha)&=\alpha^{14}+\alpha^{13}+\alpha^{12}+\alpha^{11}+\alpha^5+\alpha^3+\alpha+1\\&=(\alpha^3+1)+(\alpha^3+\alpha^2+1)+(\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha^2+\alpha)+(\alpha^2+\alpha)+\alpha^3+\alpha+1\\&=\alpha^3=E(\alpha)\end{aligned}$$

$$\begin{aligned}\tilde{F}(\alpha^3)&=\alpha^{42}+\alpha^{39}+\alpha^{36}+\alpha^{33}+\alpha^{15}+\alpha^9+\alpha^3+1\\&=\alpha^{12}+\alpha^9+\alpha^6+\alpha^3+1+\alpha^9+\alpha^3+1\\&=\alpha^{12}+\alpha^6=(\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha^2)=\alpha+1=E(\alpha^3)\end{aligned}$$

したがってシンドロームと一致することから、誤り多項式$E(x)$が特定され、誤りを訂正できる。

第 12 章

問 12.1

理想 LPF にインパルスを入力すると、Sinc 関数が出力される。Sinc 関数は正と負の時間に無限に広がるため、LPF にインパルスが入力される以前からすでに Sinc 関数が出力されていたことになる。つまり、インパルスという原因が発生する前に、Sinc 関数という結果が得られていたということになる。原因があって結果がある、という原則を因果律と呼ぶ。理想 LPF は、この意味で、因果律を満たしていない。

問 12.2

第 4 章で平均情報量について考えた時、それは情報源の予測不可能性、つまり、無秩序さと関係があることを理解した。出力されるシンボルについての予測が最も困難なとき、出力シンボルの情報量は最大となるのであった。つまり、ポイント 4.2 が示すように、情報源のすべての情報源シンボルが等確率で出現するとき、平均情報量は最大となるのである。連続的な確率分布でそれを実現するのは、一様分布である。このため、定理 12.3 が成立する。

問 12.3

ブロードバンド通信とは、直訳すれば、“広帯域通信”である。広帯域とは、帯域幅が広いことを意味する。図 12.19 で、帯域幅とは、周波数軸上の幅を意味する。この幅が広いということは、同図から、矩形パルスの幅が狭いことを意味する。したがって、単位時間内にたくさんのパルスを入れることができるので、高速通信となる。つまり、ブロードバンド通信とは、高速通信を周波数領域から述べた用語であると言える。

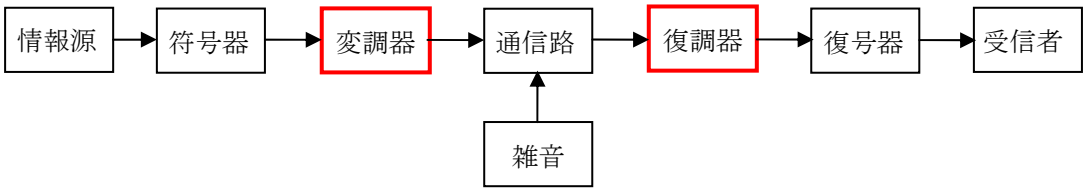
問 12.4

シャノン限界は、式(12.21)で示したように、通信路符号化定理に基づいて伝送速度の上限となる連続的通信路での通信路容量の式で、帯域幅を無限にとった結果として得られる。このことは、第 12 章 4 節で説明したように、無限に長い符号語を伝送することに等しく、そのような符号語は無限に長い符号間距離を持っている。そのような仮想的な特性をもつ符号を対象に考えられたのが、シャノン限界である。一方で、現実に使用される誤り訂正符号は、今後いかなる方式が出てこようとも、符号語長は有限であるから、符号間距離も有限である。このため、絶対にシャノン限界を超えることはできない。

第 13 章

問 13.1

符号語は 1 と 0 という数字である。数字とは概念であって、実体がないので、そのままでは通信路を通すことができない。変調とは、符号語を、通信路を通ることができる信号に変換することである。したがって変調器は、下図のように、変調器は通信路の直前に置かれる。一方、復調器は変調器の逆を実現する。すなわち、通信路を通って来た信号から、符号語を読み取るのである。このため、同図に示すように、復調器は通信路の直後に置かれる。



問 13.2

図 13.2-(1)に QPSK 変調器の構成を示す。データはまず、シリアル・パラレル変換器に入力され、1 列で入力されたデータが 2 ビットずつ出力される。その 2 ビットを(c_1,c_2)と表すと、その組み合わせには(0,0) (0,1) (1,0) (1,1)の 4 種類が現れる。これを、次に位相に写像する。そのやり方は、同図中に示すように、(0,0) (0,1) (1,0) (1,1)をそれぞれ $e^{j\pi/4}$, $e^{-j\pi/4}$, $e^{j3\pi/4}$, $e^{-j3\pi/4}$ に対応付ける。これが、QPSK シンボルとなる。

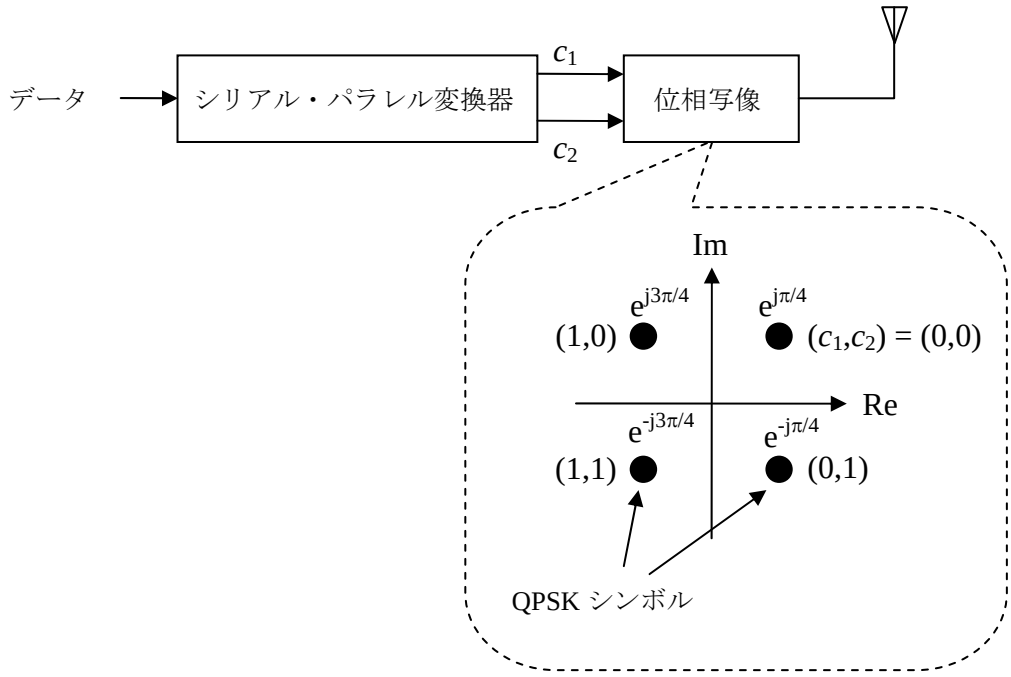


図 13.2-(1) QPSK 変調器の構成

一方、受信機では、雑音によって乱された QPSK シンボルを受信して、対応する 2 ビットのデータを読み取らなくてはならない。そのために、図 13.2-(2)に示すような判定領域を設ける。つまり、受信シンボルが第 1 象限に入ればデータは(0,0)、第 2 象限に入ればデータは(1,0)であったと判定する。

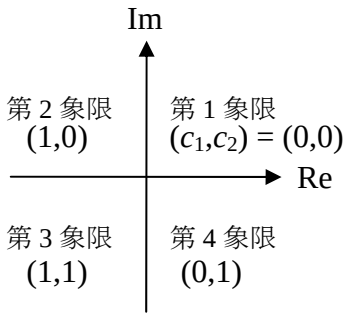


図 13.2-(2) QPSK 復調器における判定領域

詳細は、例えば神谷幸宏著“MATLAB によるディジタル無線通信技術”，コロナ社，2008 年などを参照されたい。

問 13.3

BPSK に比較して QPSK が優れている点は、QPSK は BPSK のデータ伝送速度を 2 倍にしていることである。BPSK では 1 シンボルが 1 ビットを運ぶのに対し、QPSK では 1 シンボルが 2 ビットを運ぶことができる。その反面、複素平面上でシンボル間距離が短くなり、BPSK と同じビット誤り率を達成するのに、BPSK の 2 倍の電力を必要とする。

問 13.4

BPSK 受信機は、雑音が加わって乱された BPSK シンボルの実部を見て、それが 0 以上ならばデータは‘1’、そうでなければ‘0’と判定するのであった（13.2.3 項）。しかし、雑音が非常に大きいと、BPSK シンボルが 1 であったにもかかわらず、受信シンボルは 0 より小さくなっていたということが起こり得る。この時、受信機はデータが‘0’であったと判定するので、誤りが起こる。これが、ビット誤り発生の原理である。

問 13.5

BPSK シンボルには+1 と-1 の 2 つがある。畳み込み符号を軟判定ビタビ復号器で復号するとき、メトリックとして用いるのは、受信シンボルと、これら 2 つの BPSK シンボルへの複素平面上での距離である。つまり、複素平面上で受信シンボルがより近い BPSK シンボルが、より確からしいとの考えを数値的に表現するのが、このメトリックである。