博士論文

符号の距離構造と信号設計への応用

昭和45年12月

指導教官　宮川 洋

東京大学工学系研究科
電気工学専門課程

今井秀樹

まえがき

本論文は筆者が東大工学系研究科博士課程に進学した昭和43年4月から，現在（昭和45年12月）に至るまでに行なった研究をまとめたものである．

本論文の主要な部分は才2～6章の五つの章よりなる．才2～5章では符号理論の問題を扱い，才6章では信号理論の問題が扱われている．

符号理論は工学理論の中では，もっとも美しい理論体系をもつものの一つであろう．この美しさがある程度生かされたのは，才3章の修正 Preparata 符号と才5章の $\gamma\beta$－平面においてである．

しかし，符号理論はそれが美しいだけに，その本来の目的である誤り制御機構をもつ通信系の設計に応用しようという場合，数多の問題が生じる．才2章ではこのような問題を扱っている．符号理論が工学理論である限り，このような通信系の設計問題がもっとも重要な位置を占めるべきであろう．

符号理論が適用できるのは，誤り制御機構をもつ通信系に対してだけではない．オ4章では符号分割多重PCM通信方式と呼ばれるやや特殊な通信方式に符号理論が応用される．

符号理論は信号理論とも密接な関連をもつ．信号理論も，符号理論とはやや異なった立場から，よりよい通信系の構成を目指すものである．オ6章では信号設計の問題が論じられる．

本論文のオ3章およびオ4章は既に信学会論文誌に掲載された（文献(50)，(58)）．また，オ5章も同誌に掲載が予定されている（文献(66)）．オ2章とオ6章はその一部を信学会全国大会および連合大会に発表したのみで，大部分未発表である（文献(40)，(77)）．

なお，本論文における数値計算はすべて，東大大型計算機センターのHITAC 5020を用い，プログラムはFORTRAN Ⅳによった．

謝　辞

本研究を進めるに当り，終始直接御指導頂いた本学宮川洋教授，全般にわたり，種々御検討頂いた本学瀧保夫教授，羽鳥光俊助教授ならびに日電岩垂好裕博士に深謝する。

また，オ5章に関し，貴重な御助言を頂いた本学航研野村民也教授，伊藤紘二講師，生研安田靖彦助教授ならびに同章の問題提起および細部にわたる検討をして頂いた航研福田明君に深甚な謝意を表す。

また，オ3章に対し，貴重な示唆となる卒業研究をして頂いた中島一郎君，および本研究全般にわたり，御討論頂いた瀧，宮川両研究室の方々に深謝する。

目　次

第1章　序　論 ---------- 1

1.1　論文の構成　1
1.2　論文の背景　2
1.3　論文の概要　6
1.4　用語について　15

第2章　誤り訂正符号の多相位相変調通信方式への応用 -- 19

2.1　はじめに　20
2.2　誤り訂正符号における距離と最小距離復号　22
2.3　誤り訂正符号を用いた多相位相変調通信方式　32
2.4　最小距離復号を行う場合の信頼度函数　42
2.5　ハミング距離とリー距離に対する信頼度函数　58
2.6　リー距離誤り訂正符号　69
2.7　二値符号の変換による多相位相変調通信方式の構成　97
2.8　(0, 1, ∞) 距離誤り訂正符号　111
2.9　各種方式の比較　118
2.10　むすび　127

第3章　二値誤り訂正符号の新しい修正法 ---------- 130

3.1　はじめに　130
3.2　Preparata 符号　133
3.3　修正 Preparata 符号　136
3.4　修正 Preparata 符号の復号　153
3.5　二値 BCH 符号の新しい修正法　164
3.6　二重誤り訂正二値準完全符号の新しい構成法　170
3.7　むすび　181

第4章　回線分離符号の構造と構成法 ---------- 182

4.1　はじめに　183

4.2 回線分離符号の定義 186
4.3 σ'-同値類とT-同値類の構造 190
4.4 最小距離が1の最適回線分離符号 199
4.5 回線分離符号の構成法 203
4.6 補題の証明および式の導出 212
4.7 むすび 220

第5章 M系列およびM系列符号の二次元への拡張 221
5.1 はじめに 222
5.2 二次元線形巡回符号および最大面積行列をもつ平面 224
5.3 γβ-平面およびγβ-平面符号の定義 229
5.4 γβ-平面の構造および主定理 232
5.5 γβ-平面を生成する線形再帰関係 243
5.6 γβ-平面符号に関連のある符号 248
5.7 γβ-平面の自己相関函数 254
5.8 γβ-平面の多次元への拡張 262
5.9 むすび 270

第6章 多次元線形通信系の大域的最適化 271
6.1 はじめに 272
6.2 多次元線形通信系 275
6.3 置換多面体の理論 279
6.4 一般逆行列を受信機に用いる多次元線形通信系の最適化 289
6.5 無ひずみ条件のある場合の多次元線形通信系の最適化 306
6.6 むすび 310

第7章 結言 312
7.1 主要な結論 312
7.2 今後の問題 314

付録I 原始多項式表 316

付録Ⅱ　低伝送速度の符号を用いる多相位相変調通信方式 ---------- 322
A2.1　M元ディジタル信号による通信方式　323
A2.2　直交符号族　326
A2.3　メモリー符号　330

付録Ⅲ　置換多面体の理論の応用について ---------- 338
A3.1　直交行列の最適化問題　338
A3.2　閉じた線形制約領域における最適化問題　341

文　献 ---------- 344

第1章

序論

1.1 論文の構成

本論文の主要な部分はつぎの五つの章からなっている。

オ2章　誤り訂正符号の多相位相変調通信方式への応用

オ3章　二値誤り訂正符号の新しい修正法

オ4章　回線分離符号の構造と構成法

オ5章　M系列およびM系列符号の二次元への拡張

オ6章　多次元線形通信系の大域的最適化

これらは独立して研究されたものであるが，その根底となる基本的考え方は軌を一にしている．すなわち，本論文は符号（または信号）の"距離"を中心とした数学的構造を解明し，それにより符号（または信号）の構成法，あるいは諸性質について論じたものである．各章により距離の取り上げ方に多少の差異はあるが，いずれの場合にも距離は，きわめ

て重要な役割を演ずる。また，本論文の目的とするところは，よりよい通信系を実現することであるが，本論文（特に才5章，才6章）に示される理論は通信以外にも応用を分野をもつと考えられる。

各章とも，他の章で得られた結果は用いていない。しかし，才2～5章の距離に対する基本的概念は共通しており，才2章 2.2節で述べる考え方が基礎となっている。また才6章における信号理論的考え方と，才2～5章の符号理論的考え方を結ぶものとして，付録Ⅱが設けられている。

1.2 論文の背景

本論文の基礎となる理論は符号理論と信号理論である。ここで，本論文がこれらの理論において，どのような位置に置かれるものであるかをみてみよう。

符号理論は1948年のShannonの雑音のある通信路における符号化定理[12]に始まる。符号理論の初めの目的は，この定理によって与えられる通信の限界を達成する誤り訂正符号を構成することにあった。しかし，現在に至るまでこの目的は

完全には達成されていない。それ以後，符号理論は，誤り訂正符号の理論的限界を究めること，またより簡単で能率のよい誤り訂正符号を見出すこと，さらに誤り訂正符号の構造を解明することなどを目的とし，いくつかの分野に分れ，発展してきた。

その一つの大きな分野は代数的符号理論と呼ばれるものである。これは代数的に誤り訂正符号を構成し，また符号化復号を行おうというもので，1950年のハミング符号からはじまり，BCH符号，Reed-Muller符号などの多くの符号が見出された[(1)(2)(4)(5)]。また，この分野におけるバースト訂正符号の発展も見逃せない[(3)(13)]。もう一つの大きな分野は確率的符号理論と呼ばれるもので，符号化定理の精密化[(4)(32)]や確率的復号法（逐次復号法）[(14)(3)]の研究において大きな成果を生んでいる。さらに，完全符号などの最適な符号に対する研究も一つの分野をなしている[(15)(23)]。しかし，多くの場合，最適な符号は簡単な組織的方法で構成することができず，また符号化復号が困難であるため，この分野は主として数学的興味によって支えられてきた。

ところで，誤り訂正符号は，冗長度の付加による情報伝送速度の低下，コスト増大等の代償として，受信情報の信頼性を高めることを目的としているのであるから，その取扱いとしては通信系全体のシステム設計の一環として考えるべきであるが，従来の誤り訂正符号は方式設計の一環としてよりもむしろ独立した手法として扱われてきた傾向にある*。特に誤り訂正符号における距離は従来予め与えられたものとして考えられ，方式設計上どのような意味をもつかが明らかとされていなかった。

本論文オ2章は，誤り訂正符号を多相位相変調方式に応用する場合の諸問題点を，距離の問題を中心として論ずる。また，オ3章では比較的簡単に符号化および復号ができ，しかも組織符号として最適な二値二重誤り訂正符号の構成法を示す。

以上述べた誤り訂正符号の研究のほかに，符号を他の目的に利用しようという研究も並行して行われてきた。この中で

---

*最近，岩垂によって符号理論を方式設計の一環としてとらえる試みがなされている[24][25]。（オ2章参照）

代表的なものはコンマフリー符号[16][6]などの同期誤り訂正符号，RADAなどにおいてアドレスとして割り当てられる符号[54][55]の研究などである．本論文第4章では符号分割多重PCM通信方式においてアドレスとして用いられるのに適した符号——回線分離符号の構造と構成法について述べる．

また，M系列によって代表されるような特殊な自己相関函数をもつ系列も，特別な符号の一つの符号語としての立場から符号理論において論じられるとともに，種々の応用分野との関連において，盛んに研究されてきた[6][57][60][61]．本論文第5章ではM系列の二次元への拡張について論ずる．

符号理論において，やや特殊な意味をもつ符号に直交符号，シンプレックス符号，陪直交符号などがある[6]．これはReed-Muller符号として論ずることもできるが，信号理論と密接な関係をもっている（付録II参照）．

信号理論は統計理論における検出推定理論に始まる．その後，単に最適な検出，推定をするばかりではなく，信号を設計してよりよい通信系を構成しようという問題にも興味が向けられた．このような信号設計問題には，いわゆるM元ディジ

タル信号の設計問題[17][18]とアナログ信号の設計問題[19][69]との二つの分野がある。前者の問題において一般的に最適な信号を求めるのは，簡単な場合を除いてきわめて難かしく，信号の構造に一定の制約を設け，その中で最適なものを見出そうという努力が多くなされている[20][21]。付録IIでは，このような問題を論ずる。

アナログ信号の設計問題においては，多くの場合微分的方法を用いるため，大域的に最適化することが難かしい。これに対し，本論文オ6章では多次元線形通信系の大域的最適化問題を扱う。

1.3 論文の概要

ここで，各章の内容のあらましを述べておこう。

オ2章では多相位相変調方式に対し，誤り訂正符号を応用する場合の種々の問題点が論じられる。この章では，通信系の構成を簡単にするために，ディジット毎の検出 —— 最小距離復号を行なう通信系を考える。このような場合，信頼性の高い通信を行うためには，誤り訂正符号における距離が重要な内

題となることを明らかにする。そこで，種々の距離を用いた方式を評価する手段として，信頼度函数を導入し，その上界と下界を導く。これにより，低伝送速度の符号がこの通信系に対し不利であることなどを明らかとし，さらにハミング距離とリー距離を比較して，リー距離が多相位相変調方式に対し，有効であることを示す。つぎに，リー距離に対して能率よく構成される誤り訂正符号について論ずるが，ここではかなり限定された符号しか得られない。このため，より一般的に通信系を構成する方法として，二値符号を多値符号に変換して用いる方式を考え，その信頼度函数を評価し，この方式がハミング距離を用いる場合よりはかなりすぐれたものであることを示す。また，距離をさらに一般化するオー歩として，$(0, 1, \infty)$ 距離を考え，この距離に対し構成される符号の例を示し，これがある場合には非常に有効であることを明らかにする。

オ3章では，二値誤り訂正符号（Preparata符号，BCH符号）の符号長を能率よく伸ばす方法を示す。これは，二値誤り訂正符号を実際の通信に適用する場合必要となる技術であ

る．特に，オ2章の二値符号を多値符号に変換する方式を用いる場合に重要である．この章の前半では Preparata 符号[44]を基礎として，組織符号として最適な二重誤り訂正 二値非線形組織符号が構成できることを示す。この符号を修正 Preparata 符号と呼ぶ．修正 Preparata 符号は Preparata 符号より符号長が長く，検査ビットが1ビット多い符号であり，符号化および復号が比較的簡単に行える．この章の後半では二値BCH符号の符号長を伸ばす方法が論じられている．これは原理的には前半の方法とほとんど同様な方法であり，能率がよいと思われる．また，この方法によって，準完全な二値二重誤り訂正符号が得られることを示す。

オ4章では，符号分割多重ＰＣＭ通信方式において，回線分離のための距離を考え，それにより回線分離符号を定義し，その距離構造と構成法について論ずる．符号分割多重ＰＣＭ通信方式は同一周波数帯域内に多数の回線を非同期多重化し，各回線に割り当てられた符号語（アドレス）によって回線を分離しようというものである．この章では，この通信方式においてアドレスとして用いられる符号に適したものとして回

線分離符号を考え，その基礎的構造を代数的な面から明らかにする。また，その結果を用いて回線分離符号の一例につき，その符号語数の上界と下界を求める。さらに回線分離符号の実用的な三種の構成法を示す。

第5章では，M系列およびM系列符号の二次元への拡張について論じている。M系列およびM系列符号は通信のみならず広い分野に応用されている。ここで得られる結果も，光通信，パターン認識等広い応用分野をもつと考えられる。M系列の性質を二次元に拡張したものとして，最大面積行列をもつという性質が考えられる[62]。この章では，この性質をもつ平面（半無限行列）を構成するかなり一般的と思われる方法が，二次元線形巡回符号の概念を用いて導かれる。このようにして構成された平面を$\gamma\beta$－平面と呼ぶ。さらに$\gamma\beta$－平面が興味深い種々の特徴をもつことを明らかにし，特にその自己相関函数が応用上きわめて重要な特徴をもつことが示される。

第6章は線形通信系の最適化に関するものであり，第2章～第5章が符号理論の問題を扱うのに対し，ここでは信号設

計の問題が扱われる．線形通信系はその構成が簡単である点などから，きわめて興味深い．線形通信系の一つに多次元線形通信系がある．これは有限個のアナログ情報を並列に伝送する通信系で，送信機では情報を送信行列を用いて線形変換することにより送信信号を作り，受信機では受信信号を受信行列を用いて線形変換することにより復調を行う。この章では，このような通信系において，はじめに受信行列として送信行列の一般逆行列を用いるという条件の下に，復調出力の二乗平均誤差を最小とする送信行列を求め，ついで無ひずみ条件の下に二乗平均誤差を最小とする送信行列と受信行列を求める．その結果，このいずれの場合も送，受信行列は情報および雑音の共分散行列の固有値と固有ベクトルによって表わせることが示される．また，最適化に際しては置換多面体の理論を用い，大域的に最適な解を求めている．

付録Ⅰには才2章および才5章で，実際に符号を構成する場合に必要となる GF(p)（p：素数）の上の既約多項式の表が示されている．

付録Ⅱには，才2章の補足として，低伝送速度によって生

相変調された信号を用い，最尤検出を行う通信系について述べてある。

付録Ⅲでは，オ6章で導かれた置換多面体の理論の他の問題への応用について論じる。

以上各章の内容について簡単に述べた。つぎに全体を通してみておこう。

本論文の目的とするところは，よい通信系を構成する方法を見出すことにある。通信系の"よさ"としては種々考えられ，またおのおのの場合によって，その基準も異なるであろう。しかし，かなり一般的に適用できる基準として，つぎのようなものがある。

(a) 所定の情報伝送速度に対し，受信情報の信頼性の高いこと（あるいは所定の受信情報の信頼度に対し，情報伝送速度の高いこと）。

(b) 経済的であること。

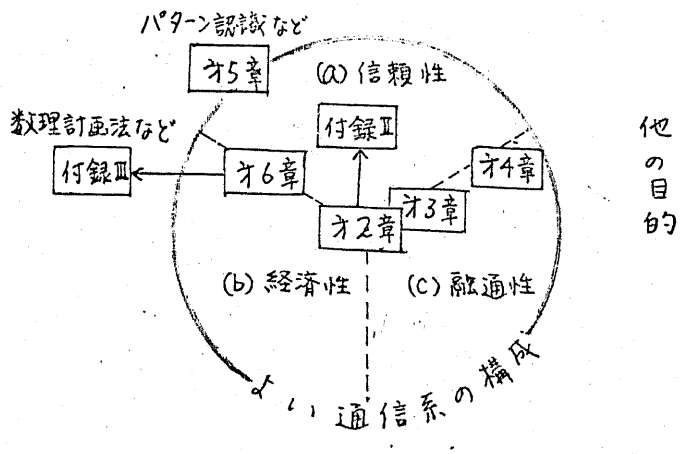
(c) 融通性の高いこと。

(b)には通信系の構成の複雑さが大きな影響を及ぼす。特に符号を用いる場合は，その符号化および復号がもっとも支配

的な要素となる。(C)の融通性には，設計上の融通性，すなわち種々の要求に応じた通信系を構成できること，および通信系を実際に運用する場合の融通性がある。

各章によって，この(a)(b)(C)に対する重みの置き方が異なっている。これを図1.1に示す。

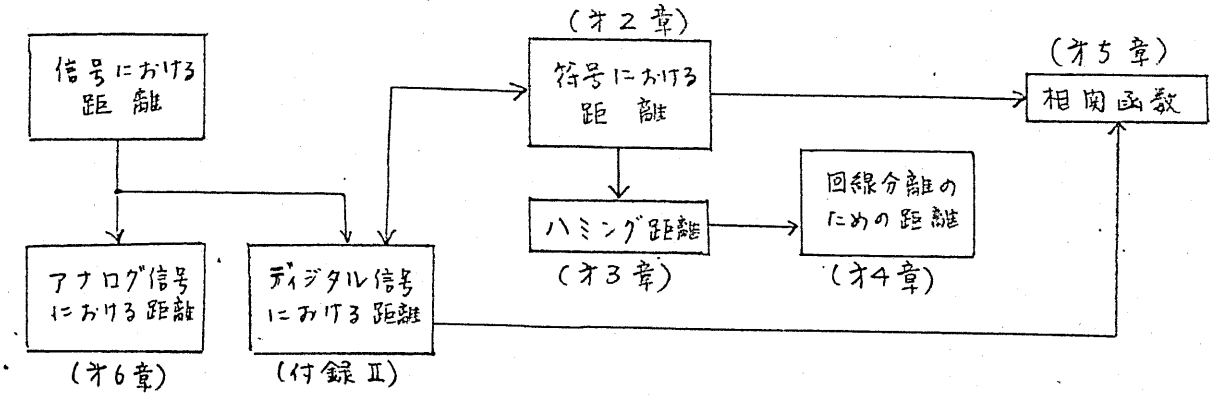
図1.1 各章の目的



各章では，この目的を達成するために，符号（または信号）の構造の解明および構成法の研究がなされている。符号（または信号）の構造の解明に当っては各章とも距離が重要な役割を演ずる。各章で用いられる距離を図1.2に示す。

符号における基本的距離については才2章2.2で詳しく述べる。そのような距離のもっとも代表的なものがハミング距離である。回線分離のための距離はこのハミング距離を基礎

図1.2　各章で用いられる距離



として定義される．符号における距離は特別な符号においては，その符号に対応する系列（または平面）の自己相関函数と対応づけることができる．この関係はオ5章で述べる．また，符号を用いる通信系であっても，符号によって変調された信号に対して距離を定義する方が便利な場合もある．付録IIで述べるM元ディジタル信号を用いる通信系がその例である．

つぎに，図1.3に各章で論じられる符号の間の関連を，従来の符号との関係をも含めて図示する．符号についての説明は各章にゆずる．また，従来の符号については参考文献が示してある．

なお，図1.1～1.3は厳密な意味をもつ訳ではなく，直観的な理解を容易にするために示したものである．

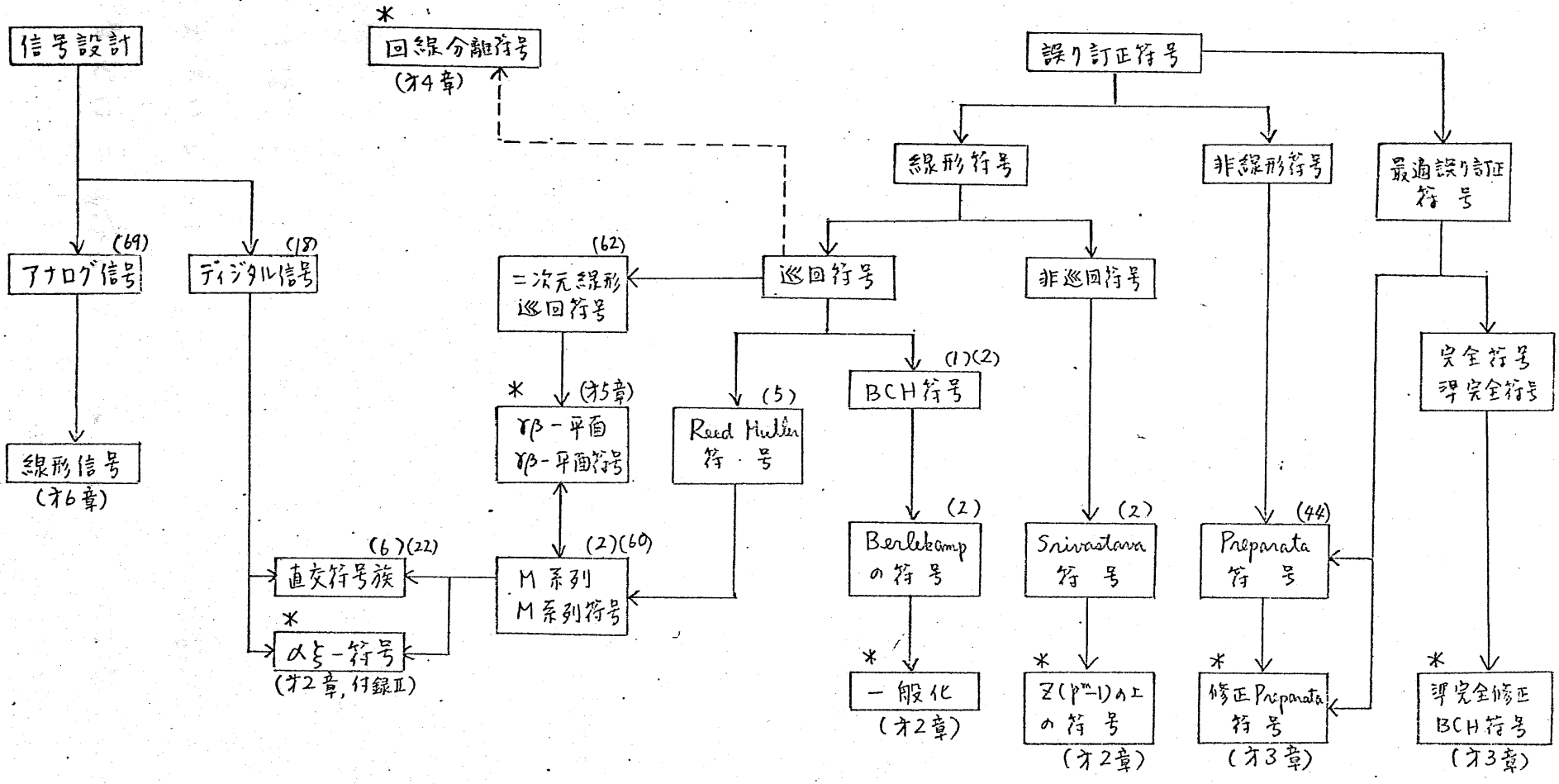


図 1.3　本論文に関連のある符号

＊印は本論文で新しく提案される符号

( ) 内の数字は文献を示す。

1.4 用語について

本論文において，用語は統一されているが，記号は各章において，もっとも自然と思われる用い方をしたため，必しも統一されていない．

本論文における数学的用語は標準的なものを用いているので，たとえば文献(7)(9)(11)を参照されたい．また，本論文独自の用語は本文中，または脚注によって説明されている．

ここでは，符号理論，信号理論の一般的用語で，やや紛らわしいと思われるものを説明する．

誤り訂正符号：誤りを訂正することのみを目的とする符号をいうが，しばしば，誤り検出符号，誤り訂正検出符号などをも含め，誤りを制御できる符号を総称して誤り訂正符号と呼ぶ．

q値符号：q進符号，q元符号などとも呼ばれるが，ここではq値符号をとった．第2章では，一般の加群の上の符号も考えているので，qは一般に2以上の整数を指す．第3章，第4章では二値符号のみが扱われる．第5章では，ガロア体$GF(q)$の上の符号を考えるのでqは素数のべきに限る．

（長さnの）語と（n次元）ベクトル：加群 $S(q)$ の上の n 字組 $(a_0, a_1, \cdots, a_{n-1})$（$a_i \in S(q)$; $i = 0, 1, \cdots, n-1$）を（長さnの）語と呼ぶ。特に，$S(q)$ が環（あるいは体）の構造をもつときは（n次元）ベクトルとも呼ぶ。

シンボルとディジット：$S(q)$ の元がシンボルであり，ディジットは本来，符号語におけるシンボルを数える単位であるが，これらは厳密には区別されない。二値符号の場合には，シンボルおよびディジットの代わりにビットをも用いる。また，ディジットは符号語によって変調された信号波形における，符号語のーシンボルに対応する区間（1タイムスロット）の意味で用いることもある。

伝送速度：本論文では符号の rate の意味で用いる。単位は（ビット／シンボル）である。実際の情報伝送速度（ビット／秒）との対応については才2章 2.3 参照。なお，$S(q)$ の上の符号の伝送速度の高低は，$\log_2 q$ を基準としてする。すなわち，$\log_2 q$ に近い伝送速度をもつ符号を高伝送速度の符号という。

最適符号：本論文では一定の符号長および最小距離に対し

符号語数が最大となる符号をいう。

能率のよい符号：一定の符号長および最小距離に対し，符号語数が比較的多い符号をいう。

組織符号：本論文では，情報シンボルと検査シンボルを区別できる符号をいう。なお，符号長 n，情報シンボル数 k の組織符号を (n, k) 符号と表わす。

修正符号：符号の基本的構造を余り変えることなく，符号長を短縮または伸長するか，あるいは情報シンボル数を増減した符号をいう。拡大符号（符号に全パリティ検査シンボルを一つ付け加えて得られる符号，短縮化符号（第3章3.1参照）などの総称。

M系列：通常M系列というときは二値のものをいうが，本論文では $GF(q)$ の上のものをも含めてM系列と呼ぶ。また，M系列というとき，無限（または半無限）の系列を意味するときと，一周期分を意味するときがある。本論文でも混乱を生じない限り，両者ともM系列と呼ぶ。

Reed-Muller 符号：本論文では拡張された Reed-Muller 符号[5]を単に Reed-Muller 符号と呼ぶ。

信号語：M元ディジタル信号を用いる場合，符号における符号語と同様に，各信号波形を信号語と呼ぶ。

以上のほかの，符号理論，信号理論における一般的用語については，文献(1)(2)(5)を参照されたい。

第2章

誤り訂正符号の多相位相変調通信方式への応用

本章では多相位相変調通信方式に対し，誤り訂正符号を応用する場合の種々の問題点について論ずる．本章の理論は誤り訂正符号を実用化する場合の基礎的概念となるものである．

誤り訂正符号によって多相位相変調された信号をディジット毎に検出し，代数的復号法あるいはその他の比較的簡単な方法で復号しようという場合，符号における"距離"をどのように選ぶかということが非常に重要な問題となる。本章ではこのような符号における距離の問題を様々な角度から検討する。

本章で論ずる距離は符号における距離として，もっとも基本的なものである。ここでは，距離は二つの役割を荷負う．一つは通信路の確率的性質を誤り訂正符号の構造に反映させ

ることであり，他の一つは，誤り訂正符号の構成法および復号における評価量となることである．

2.1 はじめに

通信系に誤り訂正符号を導入する目的は，一定の情報伝送速度に対し，受信情報の信頼性を向上させること（あるいは受信情報の信頼度を許容範囲内に保つとき，情報伝送速度を上げること）にある．しかしその場合，通信系の構成が簡単であることが，きわめて重要な条件として課せられる．したがって，誤り訂正符号の理論におけるもっとも重要な問題は，符号化および復号が簡単で，しかも能率のよい符号を見出すことにある．

さて，実際の通信系に対し，誤り訂正符号を適用しようとする場合，上記の問題は一応つぎの二段階に分けることができるであろう．

(i) 誤り訂正符号における距離として，どのようなものを選ぶべきか．

(ii) その距離に対し，符号化および復号が簡単で，しかも

能率のよい符号を見出す。

ところが，従来の誤り訂正符号の理論においては，(i)はほとんど考慮されることがなく，予め与えられた距離（たとえばハミング距離）に対し，(ii)の問題を解く努力がなされてきた。二値符号のみを考える場合には，確かに(i)は余り問題とはならない。しかし，より自由に，多値符号まで含めて通信系を設計する場合，(i)はきわめて重要な問題となってくる。

本章の目的は，誤り訂正符号によって多相位相変調を行う通信系を考え，(i)をも考慮して符号理論を再検討することにある。

2.2では誤り訂正符号における距離の概念を明らかにし，2.3では対象とする通信方式（誤り訂正符号を用いた多相位相変調通信方式）に対し説明を加える。2.4ではこの通信系において用いられる符号の距離を評価する一つの函数として信頼度函数を考え，その上界と下界を導出する。ついで2.5で，ハミング距離とリー距離に対する信頼度函数の上，下界の計算例を示し，リー距離がこの通信系により適していることを明らかにする。また，2.6ではリー距離に対して能率よ

く構成される新しい誤り訂正符号について述べる。

2.7では，この通信系を構成する一つの簡単な方法として，二値符号を多値符号に変換して用いる方式を考える。はじめに，どのような変換が適当であるかを検討し，ついでこの場合の信頼度函数を評価して，ハミング距離，リー距離を用いた場合と比較する。さらに，2.8では多相位相変調に適した距離として，$(0, 1, \infty)$距離を定義し，この距離に対して構成される符号の例を示す。

最後に，2.9で種々方式に対する復号誤り率等の特性の計算例を示し，比較する。

2.2 誤り訂正符号における距離と最小距離復号

本節では，次節以下の準備として，誤り訂正符号における距離，最小距離復号等について述べる。本節での種々の定義は，従来の符号理論における定義より一般化されている。

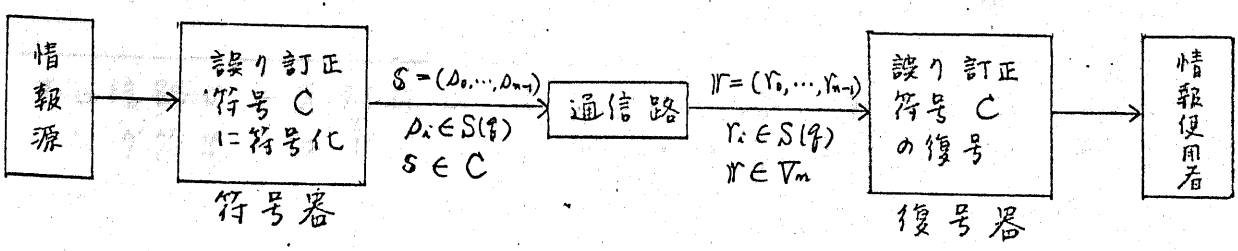
q（正整数）個の元からなる加群を$S(q)$とし，各成分が$S(q)$に属するn字組（n-tuple）$v = (v_0, v_1, \cdots, v_{n-1})$

$(v_i \in S(q)\ ;\ i=0,1,\cdots,n-1)$ のすべての集合を V_n で表わす。V_n の元 v はまた語 (word) ともいう。V_n の部分集合 C が通信等において，誤り訂正（信頼性の向上）を目的として用いられるとき，C を（加群 $S(q)$ の上の）誤り訂正（ブロック）符号と呼ぶ。また，$S(q)$ を符号 C のシンボル集合という。なお，ここでは $S(q)$ を加群としたが，$S(q)$ を単なる集合と考えても，本節の議論の多くは，そのまま成立する。

図2.1に誤り訂正符号 C を用いた，抽象化された通信系のモデルを示す。

符号器における符号化は情報源からの情報に応じて C の元（符号語）$s=(a_0,a_1,\cdots,a_{n-1})$ を選ぶことにより行われる。また，通信路は実際の通信系においては，変復調器なども含めたもので，この意味で超通信路と呼ぶこともある。通

図2.1　誤り訂正符号を用いる通信系



信路の出力（受信語） $\mathbf{r}=(r_0, r_1, \cdots, r_{n-1})$ の各成分は確率変数の標本値となっている。$\mathbf{r}$ の各成分は必しも $S(q)$ に属する必要はなく，erasure などを許す場合もあるが(1)，本論文では，$r_i \in S(q)$ $(i=0,1,\cdots,n-1)$ の場合のみを考える。

復号器では，受信語 $\mathbf{r}$ に基づいて，送信された符号語を推定する。

ここで，このような通信系において，誤り訂正符号 C の各符号語の送出される確率が等しいとしよう。このとき，復号誤り率を最小とするためには，最尤復号法を用いればよい。これは，符号語 $\mathbf{v}$ $(\in C)$ で条件付けられた受信語 $\mathbf{r}$ の確率 $P[\mathbf{r}|\mathbf{v}]$（尤度函数）を最大とする $\mathbf{v}$ を送信されたと判定することにより行われる。しかし，現在のところ，最尤復号法を簡単に行う方法はなく，ごく限られた例を除いて誤り訂正符号 C のすべての符号語と受信語 $\mathbf{r}$ を比較するしかない*。それゆえ，このような復号法は一般に，符号語

---

* 通信路が二元対称通信路である場合，たとえば，二値ハミング符号，および二値二重誤り訂正 BCH 符号に対しては，比較的簡単な最尤復号法が存在する(1)(2)。

数のごく少ない符号にしか適用できない。

より簡単な復号法を得るためには，つぎの二点を考える必要がある。

(i) 復号の基準として，簡単な"距離"を用いる。

(ii) ある種の受信語 y に対しては復号の失敗を許す。

このような考え方に基づく復号法が最小距離復号法と呼ばれるものである。最小距離復号法について述べる前に誤り訂正符号における距離を定義しておこう。

誤り訂正符号における距離としては，ハミング距離とリー距離がよく知られている[2]が，ここでは，より一般的に定義する。誤り訂正符号における距離は $S(q)$ において定義された距離によって定められる。$S(q)$ の任意の二つの元 x, y に一意に対応する非負の実数を $d(x, y)$ とし，これがつぎの距離の三公理を満たすとする。

(1) $d(x, x) = 0$。逆に $d(x, y) = 0$ なら $x = y$。

(2) $d(x, y) = d(y, x)$

(3) 三角不等式を満たす。すなわち，$S(q)$ の任意の三つの元，x, y, z に対し，

$$d(x,y)+d(y,z) \geq d(x,z)$$

が成立する.

このとき, V_n の任意の二つの元 $\mathcal{x}=(x_0, x_1, \cdots, x_{n-1})$ と $\mathcal{y}=(y_0, y_1, \cdots, y_{n-1})$ の間の距離を

$$d[\mathcal{x}, \mathcal{y}] = \sum_{i=0}^{n-1} d(x_i, y_i) \qquad (2.1)$$

によって定める. このように定義された距離 $d[\mathcal{x}, \mathcal{y}]$ が, 距離の三公理を満たすことはいうまでもない. 距離 $d[\mathcal{x}, \mathcal{y}]$ および $d(x,y)$ を誤り訂正符号 C に対する距離と呼ぶ*.

また, 誤り訂正符号 C の任意の異なる二つの符号語間の距離の最小値を C の最小距離と呼び, d_{min} で表わす. すなわち,

$$d_{min} = \min_{\substack{\mathcal{x},\mathcal{y}\in C \\ \mathcal{x}\neq\mathcal{y}}} d[\mathcal{x}, \mathcal{y}] \qquad (2.2)$$

最小距離に関するつぎの定理は符号理論の基本定理を一般化したものである.

---

* $d(x,y)$ を定義しないで, 直接 $d[\mathcal{x}, \mathcal{y}]$ を定義することにより, 誤り訂正符号における距離をさらに一般化できる. たとえば, バースト誤りを考慮する場合には, このような定義が必要となるであろうが, 本章では $d(x,y)$ による定義で十分である.

定理 2.1 ：誤り訂正符号 C の最小距離を d_{min} とする．このとき，受信語 $\mathbf{r}$ ($\in V_n$) に対し，

$$d[\mathbf{v}, \mathbf{r}] < \frac{d_{min}}{2} \qquad (2.3)$$

となる C の符号語 $\mathbf{v}$ が存在するとすれば，それは唯一つである．

証明は距離の定義から明らかである．

式(2.3)を満たす $\mathbf{v}$ ($\in C$) が存在するようなすべての受信語 $\mathbf{r}$ に対して，$d[\mathbf{v}, \mathbf{r}]$ を最小とするような $\mathbf{v}$ ($\in C$) を求め得るが，それ以外の受信語 $\mathbf{r}$ に対しては，$d[\mathbf{v}, \mathbf{r}]$ が最小となるような $\mathbf{v}$ ($\in C$) を求め得るとは限らない（多くの場合，求め得ない）復号法を最小距離復号法（minimum distance decoding ; MD-復号法と略す）* と呼ぶ．

MD-復号を行うとき，復号結果にはつぎのような三種の場合が生じ得る．

(a) 正しく復号される場合，すなわち，復号結果と送信さ

---

* d_{min} を式(2.2)で定義される厳密な最小距離ではなく，名目上の最小距離（BCH bound[2] などで求まる最小距離）として，MD-復号を定義することも少なくない．

れた符号語が一致する場合.

(b) 誤まって復号される場合. すなわち, 復号結果と送信された符号語が異なる場合.

(c) 復号不能の場合. すなわち, 誤りは検出されるが, 送信された符号語を求め得ない場合.

送信された符号語 S と受信語 W との距離 $d[S, W]$ が $d_{min}/2$ より小さい場合, MD-復号による結果は常に (a) となる. また, $d[V, W] < d_{min}/2$ となる V ($\in C$) が存在し, $V \neq S$ であるとすれば, 常に (b) となるが, それ以外の場合には, 一般に (a), (b), (c) のいずれにもなり得る (通常, (a) となる確率は小さい). (b) となる確率が復号誤り率であり, 復号誤り率と (c) となる確率の和が "正しく復号できない確率" である. しかし, 後者もしばしば復号誤り率と呼ばれる.

いうまでもなく, MD-復号においては復号誤り率は最尤復号法に比べ, ある程度増大するが, 復号が著しく簡単化できる場合がある. MD-復号法として重要なものに, 代数的復号法[2]およびしきい値復号法[26]がある。これらの復号法が

適用できる符号にはかなり制限はあるが，しきい値復号法をさらに一般化し，すべての線形符号に対して，ハミング距離を用いたMD－復号法が可能となるような方法も提案されている[27]．

さて，MD－復号法を考える場合，符号における距離の選択がきわめて重要な問題となる．距離$d[x, y]$は復号誤り率および，符号化復号過程の複雑さに直接的影響を与える．それゆえ，距離の選択はつぎのような点を考慮して行わねばならない．

(i) 距離$d[x, y]$は通信路の確率的性質にできるだけ整合したものであること．すなわち，復号誤り率をできるだけ小さくできるものであること．

(ii) その距離を用いた復号法，あるいは符号構成法などが簡単であること．

ところが，現在の符号理論においては，二値符号の場合を除いて，距離は後者の要求から定められることがほとんどである．本章の主要な目的の一つは前者の要求をできるだけ考慮し，しかも後者の要求を満たす距離を考えることにある．

これまで距離をかなり一般的に論じてきた。しかし，多くの興味ある場合は距離 $d(x, y)$ $(x, y \in S(q))$ が $x-y$ $(\in S(q))$ のみの函数となっている場合である。このときには種々の議論が著しく簡単化される。ここで，このような距離に対し

$$W(x) = d(x, 0) \tag{2.4}$$

を定義しておこう。$W(x)$ を x の重みと呼ぶ。また，V_n の元 $\mathcal{X} = (x_0, x_1, \cdots, x_{n-1})$ に対しても，

$$W[\mathcal{X}] = \sum_{i=0}^{n-1} W(x_i) \tag{2.5}$$

によって重みを定義する。

また，このような場合，受信語 $\mathcal{R}$ と送信された符号語 S との差 $\mathcal{R}-S$ を誤り語，または単に誤りと呼び $\mathcal{E}$ で表わす。このとき，MD-復号は，

$$W[\mathcal{E}] < \frac{d_{min}}{2}$$

となる誤り語 $\mathcal{E}$ はすべて正しく訂正するが，それ以外の誤り語は正しく訂正できるとは限らないと言い換えることができる。

ところで，誤り訂正符号における距離を論ずるとき，$d($

x, y) が三角不等式を満たすという条件を除いた方が便利なことがある。2.8で述べる $(0, 1, \infty)$ 距離はそのような例である。このような距離をこれまでに定義したものと区別するために，特に擬距離* と呼ぶこともある。

擬距離に対しても，誤り訂正符号 C の最小 (擬) 距離 d_{min} を

$$d_{min} = \min_{\substack{v \in V_n \\ x, y \in C \\ x \neq y}} \{ d[x, v] + d[v, y] \} \qquad (2.6)$$

によって定義すれば，MD-復号法を考えることができる。この場合のMD-復号法の基礎となるのはつぎの定理である。

定理 2.2 ： 誤り訂正符号 C の最小 (擬) 距離を d_{min} とする。このとき，受信語 r ($\in V_n$) に対し，

$$d(v, r) \leq \frac{d_{min}}{2}$$

となる C の符号語 v が存在すれば，それは唯一つである。

証明はきわめて容易であるので省略する。

---

*数学的用法と異なることに注意。

2.3 誤り訂正符号を用いた多相位相変調通信方式

本節では，本章で論ずる誤り訂正符号を用いた多相位相変調通信方式を説明し，その特性および評価基準について述べる．

2.3.1 通信系のモデル

用いられる誤り訂正符号 C の符号長を n，符号語数を M とし，符号の伝送速度を $R = \log_2 M / n$（ビット／シンボル）によって定義する．また，符号語の各成分は加群 $S(q)$ の元であるとする．

図2.2の通信系において，符号器では情報源からの情報に応じて，C の符号語を選び超通信路に送出する．ここで，C の各符号語が送出される確率は等しいと仮定しておこう．

図2.2の ω は符号器と超通路を結ぶものであり，$S(q)$ から法を q とする整数の剰余環 $Z(q)$（$Z(q)$ の元は $q-1$ 以下の非負の整数で表わす）の上への1対1の写像である。$S(q)$ 自身が法を q とする整数の剰余環であるときは，ω は

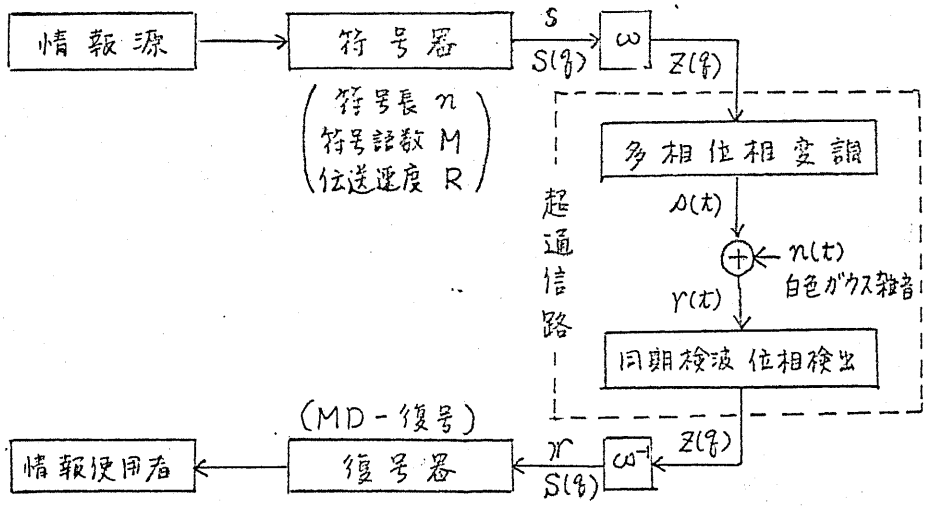


図 2.2 通信系のモデル

恒等写像として無視することにする。なお，ω および ω^{-1} は前節では超通信路に含まれていたが，ここでは説明の便宜上，超通信路は ω および ω^{-1} を含まないとする。

超通信路は位相変調器，（狭義の）通信路，位相検出器からなる。位相変調器では $Z(q)$ の各元に対応して q 相位相変調を行う。通信路には片側電力スペクトル密度が N_0，平均値が 0 の加法的白色ガウス雑音が存在する。位相検出器では，受信信号の各ディジット毎に，位相を復調，判定する。

ω^{-1} は ω の逆写像であり，位相検出器からの出力（$Z(q)$ の元）を $S(q)$ の元に写像する。また，復号器では MD-復号を行う。

超通信路について，もう少し詳しく述べておこう．送信される符号語 $S=(s_0, s_1, \cdots, s_{m-1})$ の各ディジット s_i あるいは $\omega(s_i)$ $(\in Z(q))$ に対応して，変調では，$i\Delta T \leq t \leq (i+1)\Delta T$ の間

$$s(t) = \sqrt{2S}\cos\left(2\pi f_0 t + \omega(s_i)\frac{2\pi}{q}\right) \qquad (2.7)$$

となる信号を送出する．ここで，S の送信は $t=0$ から始まるものとする．また，f_0 は搬送周波数，ΔT は1ディジットを送信するのに要する時間であり，$\Delta T \cdot f_0$ は整数となると仮定しておく．

位相検出器によって受信される信号は

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

である．$n(t)$ は白色ガウス雑音であり，平均値が0，片側電力スペクトル密度が N_0 である．すなわち，

$$\overline{n(t)} = 0 \qquad (2.8)$$

$$\overline{n(t)\,n(u)} = \frac{N_0}{2}\delta(t-u) \qquad (2.9)$$

ここに，$\overline{\cdot}$ は平均を示し，δ はディラックのデルタ函数である．位相検出器では，$i\Delta T \leq t \leq (i+1)\Delta T$ において $r(t)$ の位相を最適検出する．これは原理的には，

$$x = \frac{2}{\sqrt{N_0 \Delta T}} \int_{i\Delta T}^{(i+1)\Delta T} r(t) \cos(2\pi f_0 t)\, dt \qquad (2.10)$$

$$y = \frac{2}{\sqrt{N_0 \Delta T}} \int_{i\Delta T}^{(i+1)\Delta T} r(t) \sin(2\pi f_0 t)\, dt \qquad (2.11)$$

を計算し，

$$\theta = \tan^{-1} \frac{y}{x} \qquad (2.12)$$

が

$$(2r-1)\frac{\pi}{q} \leq \theta < (2r+1)\frac{\pi}{q} \quad (r \in Z(q)) \qquad (2.13)$$

であるとき，オr相が送られてきたと判定すればよい[28][29]．

2.3.2 超通信路の遷移確率

つぎに，超通信路の遷移確率を示しておこう。式(2.10)，(2.11)のx，yはつぎの結合確率密度をもつことが容易に確かめられる．

$$p(x,y) = \frac{1}{2\pi} \exp\left\{ -\frac{(x-\bar{x})^2 + (y-\bar{y})^2}{2} \right\} \qquad (2.14)$$

ここに

$$\bar{x} = \sqrt{\frac{2E_D}{N_0}} \cos\left(\omega(s_i)\frac{2\pi}{q}\right) \qquad (2.15)$$

$$\bar{y} = \sqrt{\frac{2E_D}{N_0}} \sin\left(\omega(s_i)\frac{2\pi}{q}\right) \qquad (2.16)$$

であり，E_D は1ディジット当りの信号エネルギ $S\Delta T$ である．

したがって，Δ_i が送られたときの検出位相 γ の確率，すなわち，式(2.12)の θ が式(2.13)の範囲に入る確率は

$$P[\gamma \mid \omega(\Delta_i)] = \iint_{\mathcal{D}(x,y,\gamma)} p(x,y)\,dx\,dy \qquad (2.17)$$

で与えられる。ここに積分領域 $\mathcal{D}(x,y,\gamma)$ は図2.3に示すように，原点を端点とし，角度 $(2\gamma-1)\pi/q$ と $(2\gamma+1)\pi/q$ の半直線にはさまれる領域である。

明らかに，$P[\gamma \mid \omega(\Delta_i)]$ は $\gamma-\omega(\Delta_i)$ $(\in Z(q))$ にしかよらない。すなわち，

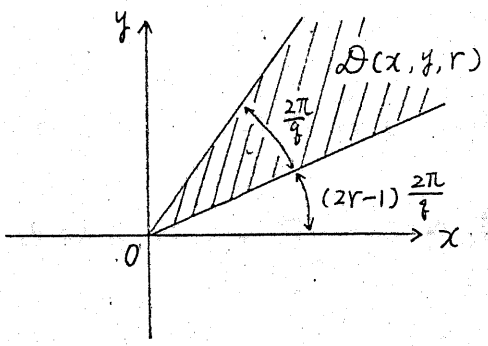
$$P[\gamma \mid \omega(\Delta_i)] = P[\gamma-\omega(\Delta_i) \mid 0]$$

また，用いられる符号の伝送速度を R（ビット/シンボル）とすれば，E_D は

$$E_D = E_B R$$

となる。ここに E_B は1情報ビット当りの信号エネルギーであ

図 2.3　積分領域 $\mathcal{D}(x,y,\gamma)$



る．ゆえに，式(2.16)は

$$P[r \mid \omega(\Delta_i)] = P[j \mid 0] = \iint_{\theta(x,y,r)} \frac{1}{2\pi} \exp\left[-\frac{1}{2}\{(x-\sqrt{2\rho R})^2 + y^2\}\right] dx\,dy \tag{2.18}$$

となる．ただし．$j = r - \omega(\Delta_i)$ $(\in Z(q))$，$\rho = E_B / N_0$ である。

また，明らかに，$P[j \mid 0] = P[-j \mid 0]$ $(-j \in Z(q))$ が成立する．

ここで，

$$P_0(\rho R) = P[0 \mid 0]$$

$$P_j(\rho R) = P[j \mid 0] + P[-j \mid 0] = 2P[j \mid 0] \quad (0 < j < \frac{q}{2}) \tag{2.19}$$

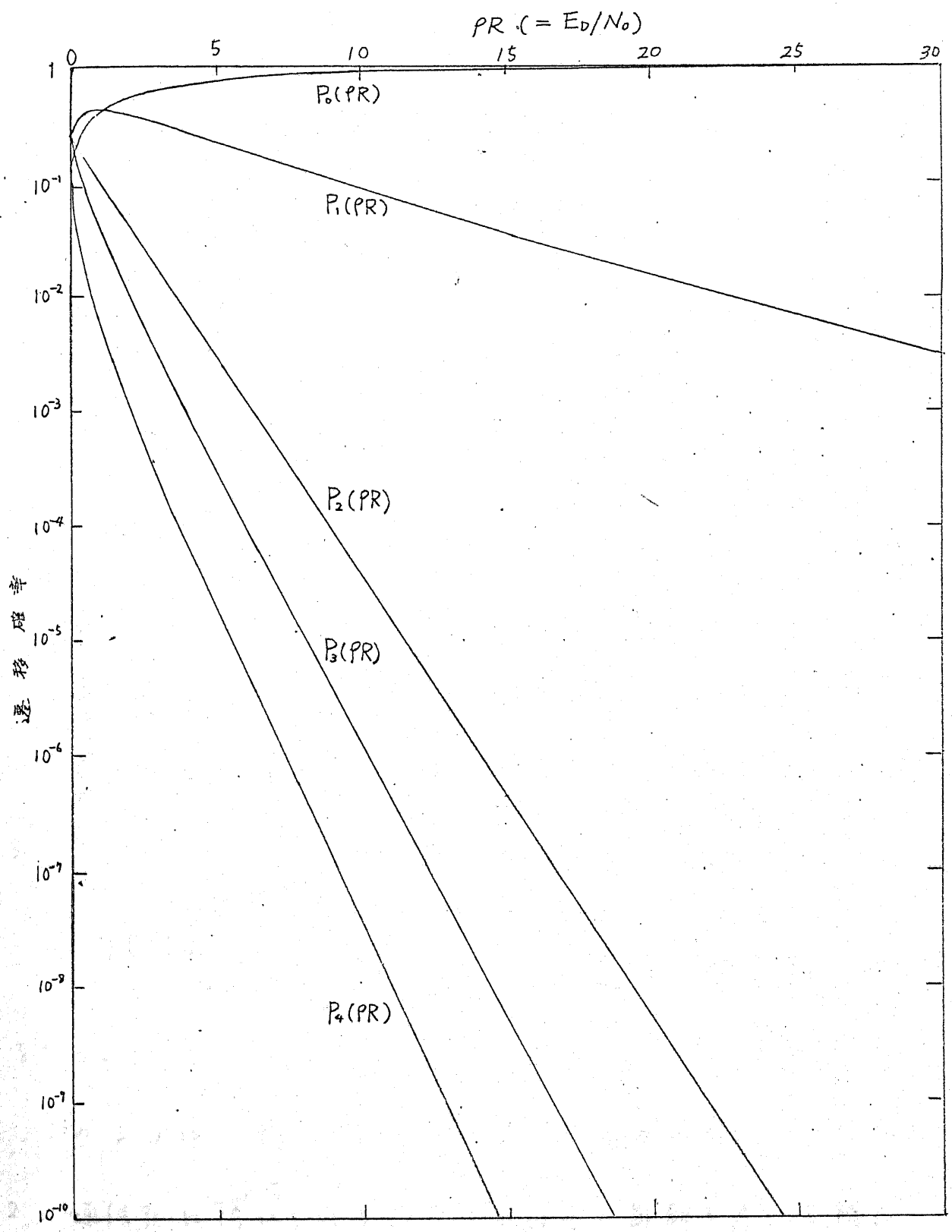
$$P_{\frac{q}{2}}(\rho R) = P[\tfrac{q}{2} \mid 0] \quad (q \text{が偶数であるとき})$$

を定義しておこう．$P_j(\rho R)$ は各ディジットが j 相だけ誤まって検出される確率である．$P_j(\rho R)$ の計算例を $q=8$ の場合について，図2.4に示す。

この図にみるように，$P_j(\rho R)$ の間には大きな差がある．特に，$P_2(\rho R)$ は $P_1(\rho R)$ に比べ著しく小さい．q が十分大きいとし，簡単な近似式によって．この差をみてみよう．

式(2.18)は式(2.12)の θ を用いて，つぎのように書き

図 2.4　超通信路の遷移確率の計算例 ($q = 8$)



直せる[30].

$$P[j|0] = \int_{(2j-1)\pi/q}^{(2j+1)\pi/q} p(\theta)\,d\theta$$

$$p(\theta) = \frac{1}{2\pi} e^{-\rho R} + \frac{\sqrt{2\rho R}\cos\theta}{2\pi} e^{-\rho R\sin^2\theta} \int_{-\infty}^{\sqrt{2\rho R}\cos\theta} e^{-\frac{u^2}{2}}\,du$$

ここで，$\sqrt{2\rho R}\cos\theta \gg 1$ とすれば，正規分布のよく知られた近似式[30]

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{u^2}{2}}\,du \approx 1 - \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}\,x} \qquad (2.20)$$

を用いて，つぎの $p(\theta)$ の近似式を得る。

$$p(\theta) \approx \frac{\sqrt{2\rho R}\cos\theta}{\sqrt{2\pi}} e^{-\rho R\sin^2\theta}$$

θ を十分小さいとし（すなわち q が $2j\pi$ に比べ十分大きいとし），$\sin^2\theta \approx \theta^2$，$\cos\theta \approx 1$ と近似して，再び式(2.20)を用いれば，

$$P_j(\rho R) \approx \frac{q}{(2j-1)\sqrt{\pi^3 \rho R}} e^{-(2j-1)^2 \rho R \frac{\pi^2}{q^2}} \qquad \left(\begin{array}{c} \rho R \gg 1 \\ 0 < j \ll \frac{q}{2} \end{array}\right)$$

を得る。

このように，$P_j(\rho R)$ の間に大きな差のあることが，図2.2の通信系に用いられる誤り訂正符号の距離を考える際に，きわめて重要な点となる。

2.3.3 評価基準

図2.2のような誤り訂正符号を用いた通信方式を評価する場合，その基準として，受信情報の信頼性，情報伝送度，帯域巾，送信エネルギーあるいは送信電力，経済性，装置化の難易などがある．いうまでもなく，これらは相互に関連し合っている．これらの評価基準を表わすパラメータとして種々考えられるが，ある程度規格化して扱うためには，“正しく復号できない確率” P_{NDC}，符号の伝送速度 R（ビット/シンボル），1情報ビット当りの信号エネルギーと雑音の電力スペクトル密度の比 ρ（$= E_B/N_0$），および符号長 n，シンボル数 q を用いると便利である．

経済性や装置化の難易は符号化および復号のアルゴリズムにより大きく支配される．しかし，同一のアルゴリズムを用いる場合には，符号長 n とシンボル数 q が簡単な目安となるであろう．

符号の伝送速度 R（ビット/シンボル）は通信系の情報伝送速度 $\mathcal{R}$（ビット/秒）とつぎのような関係にある．

$$\mathcal{R} = \log_2 M / (n\Delta T) = R/\Delta T \qquad (2.21)$$

ここに，ΔT は1ディジットを送信するのに要する時間である．

$q \geq 3$ の場合は，所要帯域巾 W は $1/\Delta T$ となる*．$q=2$ の場合は，所要帯域巾は実際の通信系をいかに構成するかによるが，$1/2\Delta T$ ととることが可能である．それゆえ，符号の伝送速度 R は

$$R = \begin{cases} \mathcal{R}/W & : \quad q \geq 3 \text{の場合} \\ \mathcal{R}/2W & : \quad q = 2 \text{の場合} \end{cases} \qquad (2.22)$$

となる量を表わすと考えられる．すなわち，符号の伝送速度は帯域巾で規格化した情報伝送速度に対応するものである．

P_{NDC} は復号誤り率と復号不能の確率の和である．復号不能の場合は誤りを検出できるから，復号誤り率と復号不能の確率を区別して扱うことが望ましいが，これらを区別して計算することはきわめて難かしい．また，P_{NDC} を計算する場合にも，次節に述べる（仮定3）のような近似が必要である．このとき P_{NDC} は ρR，n，q および符号の最小距離 d_{min} によって定まる．

---

* この場合の帯域巾は，丁度 W だけ周波数の異なる搬送波を用いるとき，まったく干渉のない通信を行えることを意味する．

2.4 最小距離復号を行う場合の信頼度函数

2.2で述べたように，誤り訂正符号における距離を選択する場合，考慮すべき一つの点は，その距離が超通信路の確率的性質に整合しているかどうかということである．これをみるために，ここでは信頼度函数を用いよう．

2.4.1 信頼度函数

ある距離 $d[x, y]$ が定義された符号長 n，伝送速度 R の誤り訂正符号のうちで，図2.2の通信系に用いたとき"正しく復号できない確率"が最小となる符号に対する"正しく復号できない確率"を $P_{NDC}^{\circ}(n, R; \rho)$ で表わす．ここに $\rho = E_B/N_0$ である．このとき，図2.2の通信系に対する信頼度函数を

$$E(R;\rho) = \lim_{n\to\infty} \frac{1}{n} \ln P_{NDC}^{\circ}(n, R; \rho) \qquad (2.23)$$

で定義する．

信頼度函数 $E(R;\rho)$ は距離が"正しく復号できない確率"に及ぼす影響を符号の個性にはよらず，純粋に比較できると

いう意味で重要であるが，$E(R;P)$ を正確に評価することはきわめて難かしく，式(2.23)の右辺の極限が存在するかどうかも分っていない。しかし，通信系が一定の条件を満たすような場合には，比較的簡単に $E(R;P)$ の下界と上界*を評価することは可能である。

ここでは，図2.2の通信系に対し，つぎのような仮定をおく。

(仮定1) 距離 $d(x,y)$ が $x-y$ のみの函数となる。

(仮定2) 任意の i, j, k ($\in Z(q)$) に対し，距離 $d(x,y)$ および写像 ω がつぎの二つの式のうちいずれかを満たす。

$$d(\omega^{-1}(i), \omega^{-1}(i+k)) = d(\omega^{-1}(j), \omega^{-1}(j+k))$$

または

$$\begin{cases} d(\omega^{-1}(i), \omega^{-1}(i+k)) = d(\omega^{-1}(j), \omega^{-1}(j-k)) \\ d(\omega^{-1}(i), \omega^{-1}(i-k)) = d(\omega^{-1}(j), \omega^{-1}(j+k)) \end{cases}$$

(仮定3) 最小距離を d_{min} とすると，MD-復号によって

---

* 厳密に言えば $\frac{1}{n}\ln P_{Noc}(n,R;P)$ の下極限の下界と上極限の上界。

$W[e] < d_{min}/2$ となる誤り e はすべて正しく訂正できるが，それ以外の誤りは正しく訂正できない。

（仮定2）はたとえば，（仮定1）が満たされ，かつ，シンボル集合 $S(g)$ が $\mathbb{Z}(g)$ となっているような場合には満たされる（このとき ω は恒等写像とすることに注意）。また，実際の MD－復号（特にしきい値復号）においては，$W[e] \geq d_{min}/2$ となる誤りを正しく訂正できることもあるが，通常このような確率は小さく，（仮定3）は実際の MD－復号に対してもよい近似であると思われる。

以下，このような仮定の下に，$E(R;P)$ の下界と上界を求めよう。なお，最尤復号を用いる場合の信頼度函数については多くの研究がなされている[3][31][32][33]が，MD－復号を行う場合については，まだ研究されていないようである。

2.4.2 信頼度函数の下界

信頼度函数 $E(R;P)$ の下界 $E_L(R;P)$ は誤り訂正符号に対する Gilbert の下界[1][2]と，多項分布函数の限界の理論[31]を用いて導くことができる。

ここで，V_n に含まれるすべての語に対する重みの集合を D_n とおこう。すなわち，

$$D_n = \{ W[X] \mid X \in V_n \} \tag{2.24}$$

このとき，やや一般化された Gilbert の下界はつぎの定理で与えられる。

定理2.3 (Gilbert)[2]：成分が加群 $S(q)$ に属し，重みが d 以下の長さ n の語の総数を $V_d^{(n)}$ で表わす。

$$V_d^{(n)} \leq e^{n(\ln q - R\ln 2)} \tag{2.25}$$

を満たす最大の d ($\in D_n$) を d_0 とおけば，符号長 n，伝送速度 R（ビット/シンボル）の符号で，最小距離が少くとも $d_0+\delta$ となるものが存在する。ここに δ は次式で与えられる。

$$\delta = \min_{\substack{x,y \in S(q) \\ W(x) > W(y)}} \{ W(x) - W(y) \} \tag{2.26}$$

つぎに，多項分布に関する Chernov の限界を示しておこう。有限個の点からなる離散的集合（標本空間）を X とし，X の上の確率変数を $\phi(x)$ ($x \in X$)，確率分布を $P(x)$ ($x \in X$) とする。つぎに，$(x_0, x_1, \cdots, x_{n-1})$ ($x_i \in X$) と

なるn字組すべての集合をX^nで表わし，X^nの各点$\mathcal{X}=(\chi_0, \chi_1, \cdots, \chi_{n-1})$には確率分布を

$$P[\mathcal{X}] = \prod_{i} P(\chi_i) \qquad (2.27)$$

によって定義する．ここで

$$\Phi_n[\mathcal{X}] \equiv \sum_{i=1}^{n-1} \phi_i(\chi_i) \leq nr \qquad (2.28)$$

となるすべての$\mathcal{X}$ $(\in X_n)$の集合を$\Lambda(nr)$で表わすとき，

$$F(nr) = \sum_{\mathcal{X}\in\Lambda(nr)} P[\mathcal{X}] \qquad (2.29)$$

が多項分布函数である。すなわち，多項分布函数$F(nr)$は$\Phi_n[\mathcal{X}]$がnr以下となる確率である。

$F(nr)$の上界と下界は確率変数$\phi(\chi)$の半不変数

$$\gamma(s) = \ln \sum_{\chi\in X} e^{s\phi(\chi)} P(\chi) \qquad (2.30)$$

を用いて求められる．

定理2.4*：多項分布函数$F(nr)$はつぎのような不等式を満たす。

---

*ここに示す結果は，はじめChernovらによって導かれ，Shannon，Fano[31]によって使い易い形にまとめられたものである．

$$F(nr) \leq \exp\{-n[\Delta\gamma'(\Delta)-\gamma(\Delta)]\} \quad (\Delta \leq 0) \quad (2.31)$$

$$1-F(nr) \leq \exp\{-n[\Delta\gamma'(\Delta)-\gamma(\Delta)]\} \quad (\Delta \geq 0) \quad (2.32)$$

$$F(nr) \geq \exp\{-n[\Delta\gamma'(\Delta)-\gamma(\Delta)]-C(n,\Delta)\} \quad (\Delta \leq 0) \quad (2.33)$$

$$1-F(nr) \leq \exp\{-n[\Delta\gamma'(\Delta)-\gamma(\Delta)]-C(n,\Delta)\} \quad (\Delta \geq 0) \quad (2.34)$$

ここに，パラメータ Δ は

$$\gamma'(\Delta) \equiv \frac{d\gamma(\Delta)}{d\Delta} = r \quad (2.35)$$

によって定められる．また，$C(n,\Delta)$ は，$\lim_{n\to\infty} C(n,\Delta) = 0$ となる項で，次式で与えられる．

$$C(n,\Delta) = \frac{q-1}{2}\ln(2\pi n) + |\Delta|\Delta + \frac{q}{12} + \frac{1}{n}\sum_{x\in X}\frac{e^{\Delta\phi(x)-\gamma(\Delta)}}{P(x)} \quad (2.36)$$

ここに，q は X に含まれる元の数であり，Δ は

$$\Delta = \max_i [\phi(x_{i+1}) - \phi(x_i)] \quad (2.37)$$

によって定義される。ただし，x ($\in X$) の添字は

$$\phi(x_i) \geq \phi(x_j) \qquad (i > j)$$

となるようにつけるものとする．

以上の準備の下に，信頼度函数の下界を求める．はじめに，定理2.3の $\nabla a^{(n)}$ の上界を導こう．$\nabla a^{(n)}$ は重みが d 以下の長さ n の語の総数，すなわち，

$$W[x] = \sum_{i=0}^{n-1} W(x_i) \leq d$$

となるような語 $x = (x_0, x_1, \cdots, x_{n-1})$ $(x_i \in S(q))$ の総数である．このことから，$X = S(q)$ とおき，$P(x) = \frac{1}{q}$ $(x \in X)$ となる確率分布および $\phi(x) = W(x)$ $(x \in X)$ となる確率変数を考えれば，$V_d^{(n)}$ はこのような X, P, ϕ に関する多項分布函数 $F(nr)$ を用いて，

$$V_d^{(n)} = q^n F(nr) \qquad (2.38)$$

と書けることが分る．それゆえ，式 (2.31) を用いれば，

$$V_d^{(n)} \leq \exp\{n[\ln q - \rho\gamma'(\rho) + \gamma(\rho)]\} \quad (\rho \leq 0) \qquad (2.39)$$

と書けることが分る．ここに，

$$\gamma(\rho) = \ln \sum_{x \in X} \frac{1}{q} e^{\rho\phi(x)} = \ln \sum_{x \in S(q)} e^{\rho W(x)} - \ln q \qquad (2.40)$$

であり，ρ は

$$\gamma'(\rho) = \frac{d}{n} \qquad (2.41)$$

により定められる．

明らかに，定理 2.3 の式 (2.25) の左辺を式 (2.39) の右辺で置き換えても，定理の結論は成立する．したがって，つぎの補題を得る．

補題2.5：加群 $S(\mathfrak{f})$ の上の符号長 n，伝送速度 R の符号で，

$$\gamma'(\Lambda) - \gamma(\Lambda) = R \ln 2 \quad (\Lambda \leq 0) \qquad (2.42)$$

$$\frac{d}{n} = \gamma'(\Lambda)$$

によって定められる d に対し，最小距離 d_{min} が

$$\frac{d_{min}}{n} \geq \frac{d - \Delta + \delta}{n} \qquad (2.43)$$

を満たすものが存在する．ここに，$\gamma(\Lambda)$ は式(2.40)，δ は式(2.26)で与えられ，Δ は

$$\Delta = \max_{i} [W(x_{j+1}) - W(x_j)]$$

によって定義される．ただし x ($\in S(\mathfrak{f})$) の添字は

$$W(x_i) \geq W(x_j) \qquad (i > j)$$

となるようにつけるものとする。

つぎに，最小距離 d_{min} の符号を用い，MD－復号を行なう場合の"正しく復号できない確率" P_{NDC} について考えよう．2.4.1 の（仮定3）から P_{NDC} は

$$W[e] = \sum_{i=0}^{n-1} W(e_i) \geq \frac{d_{min}}{2}$$

となる誤り語 e が生じる確率である．ところが（仮定2）

から，誤り語の成分 $e_i (\in S(g))$ の重み $W(e_i)$ の確率分布は送信語には関係せず，超通信路の遷移確率 $P[\omega(e_i)|0]$ $(= P[-\omega(e_i)|0]\ ;\ \omega(e_i) \in Z(g))$ に等しい．それゆえ，式(2.32)から，P_{NDC} はつぎの不等式を満たすことが分る。

$$P_{NDC} \leq \exp[-n\{\sigma g'(\sigma) - g(\sigma)\}] \quad (\sigma \geq 0) \tag{2.44}$$

ここに，

$$g(\sigma) = \ln \sum_{x \in S(g)} e^{\sigma W(x)} P[\omega(x)|0] \tag{2.45}$$

である．ただし，$P[\omega(x)|0]$ は式(2.18)で与えられている．また，パラメータ．σ は

$$g'(\sigma) \equiv \frac{dg(\sigma)}{d\sigma} = \frac{d_{min} - \delta}{2n} \tag{2.46}$$

で定められる．ただし，δ は式(2.36)で与えられるものである．

補題2.5と式(2.44)を組合せ，$n \to \infty$ とすれば，結局つぎの結果を得る．

定理2.6：加群 $S(g)$ の上の符号を図2.2の通信系に用いた場合，距離 $d(x, y)$ と写像 ω が2.4.1の（仮定1,2）

満たすならば，信頼度函数 $E(R;\rho)$ はつぎのような下界 $E_L(R;\rho)$ をもつ．

$$E_L(R;\rho) = \sigma r - g(\sigma) \tag{2.47}$$

ここに，$\sigma(\geq 0)$ および r は

$$r = g'(\sigma) = \gamma'(\rho)/2 \tag{2.48}$$

で定められ，$\rho(\leq 0)$ は

$$\rho\gamma'(\rho) - \gamma(\rho) = R\ln 2 \tag{2.49}$$

で定められる．ただし，$g(\sigma)$ は式(2.45)，$\gamma(\rho)$ は式(2.40)で与えられている．

$E_L(R;\rho)$ はかなり複雑な形をしており，実際に求めるには数値計算によらねばならない．この場合，つぎのような手順によればよい．

(1) 与えられた ρ，および R から式(2.18)により，各 $x(\in S(\beta))$ について $P[\omega(x)|0]$ を計算する．

(2) R から，Newton-Raphson 法[34]により，式(2.49)を満たす ρ を求め，$r=\gamma'(\rho)/2$ を計算する．

(3) (1)で求めた $P[\omega(x)|0]$ および(2)で求めた r を用い，Newton-Raphson 法により，式(2.48)を満た

すべてを求める。

(4) $g(\sigma)$ を計算する。

(5) (1)～(4) を各 R について繰返し，式 (2.47) の $E_L(R;\rho)$ を各 R について求める。

このような信頼度函数の下界 $E_L(R;\rho)$ のほかに，$E_L(R;\rho)$ が正となるような伝送速度 R の限界 $R_{efL}(\rho)$ も距離を比較する際に有用である*。与えられた ρ ($=E_B/N_0$) において，この限界内の伝送速度に対しては，符号長 n を無限に大きくしたとき，確率1で正しく復号のできる符号の存在することが保証される。

$R_{efL}(\rho)$ を求めるには，式 (2.47)～(2.49) において，$E_L(R;\rho)=0$ とし，それに対応する R を求めればよいが，一般に $R_{efL}(\rho)$ は各 ρ に対して二価函数となるので，実際にはつぎのように図式的に求める方が簡単である。

(1) ρR ($=E_D/N_0$) が与えられたものとし，式 (2.18) により，$P[w(x)|0]$ を計算する。

(2) $\gamma = g'(0) = \sum_{x\in S(\rho)} W(x) P[w(x)|0]$ を計算する (

---

* $R_{efL}(\rho)$ の添字 ef は error free の略。

$\sigma g'(\sigma) - g(\sigma) = 0$ を満たす σ は0であることに注意)

(3) $\gamma'(\Delta) = 2r$ を満たす Δ (≤ 0) を Newton-Raphson 法により計算する。

(4) $\{\Delta\gamma'(\Delta) - \gamma(\Delta)\} / \ln 2$ を計算する。これを $R^*_{efL}(\rho R)$ で表わす。

(5) (1)～(4) を各 ρR について繰返し，横軸を ρR として $R^*_{efL}(\rho R)$ を描く。

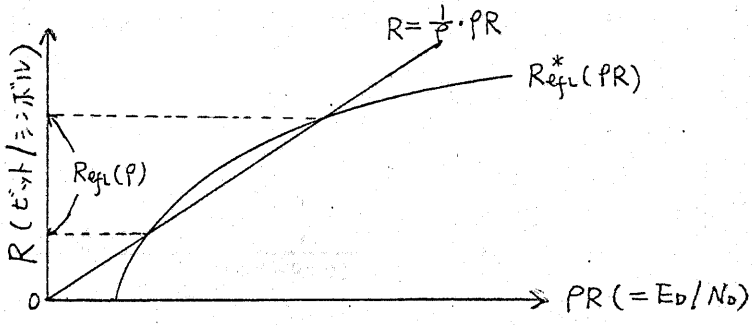
(6) 各 ρ について，原点を通り勾配が $1/\rho$ となる直線と $R^*_{efL}(\rho R)$ の交点を求めると，これが $R_{efL}(\rho R)$ となる（図2.5参照）。

ここで，

$$R^*_{efL}(\rho R) = 0 \qquad (2.50)$$

となる ρR について考えてみよう。このとき，$\Delta = 0$ である

図2.5　$R_{efL}(\rho)$ の図式的計算



から，

$$\gamma'(\rho) = \bar{d} \equiv \sum_{x \in S(\mathcal{G})} \frac{W(x)}{\mathcal{G}}$$

したがって，式(2.50)を満たす ρR は

$$\frac{\bar{d}}{2} = \sum_{x \in S(\mathcal{G})} W(x) P[\omega(x) | 0]$$

を満たさねばならない。ところが $\rho R = 0$ とすると，この式の右辺は $\bar{d}$ となる。ゆえに，式(2.50)を満たす ρR は正でなければならない．したがって，図2.5から明らかなように $R_{opt}(\rho) \longrightarrow 0$ となるとき $\rho \longrightarrow \infty$ となる。

2.4.3 信頼度函数の上界

信頼度函数 $E(R;\rho)$ の上界を求めるには，誤り訂正符号についての Eliasの上界を用いればよい．これはつぎの定理で与えられる。

定理2.7 (Elias)[2]：加群 $S(\mathcal{G})$ の上の符号長 n，伝送速度 R の符号の最小距離 d_{min} は，n 以下の任意の正整数 t に対し，

$$\frac{d_{min}}{n} \leq \frac{\frac{t}{n}\left(2 - \frac{t}{\bar{d}n}\right)}{1 - \frac{e^{n(\ln \mathcal{G} - R\ln 2)}}{V_t^{(n)}}} \qquad (2.51)$$

を満たす。ここに，$V_x^{(n)}$ は重みが t 以下の長さ n の語の総数である。また，$\bar{d}$ は

$$\bar{d} = \sum_{x \in S(g)} \frac{W(x)}{g} \tag{2.52}$$

で与えられる。

ここで，式 (2.33) (2.38) を用いれば，

$$\frac{e^{n(\ln q - R\ln 2)}}{V_x^{(n)}} \leq e^{-n\{\Delta\gamma'(\Delta) - \gamma(\Delta) - R\ln 2\} - C(n,\Delta)} \tag{2.53}$$

を得る。ただし，$\gamma(\Delta)$ は式 (2.40)，$C(n,\Delta)$ は式 (2.36) で与えられている。また，パラメータ Δ (≤ 0) は

$$\gamma'(\Delta) = t/n$$

により定められる。したがって，任意に小さい正数 ε に対し，

$$\Delta\gamma'(\Delta) - \gamma(\Delta) - R\ln 2 = \varepsilon\ (>0) \tag{2.54}$$

となるように $\frac{t}{n}$ を選べば，$n \longrightarrow \infty$ のとき，式 (2.51) の右辺の分母は 1 となる。ゆえに，このとき，式 (2.54) により定められる $\gamma'(\Delta)$ を用いれば，式 (2.51) は

$$\frac{d_{min}}{n} \leq \gamma'(\Delta)\left(2 - \frac{\gamma'(\Delta)}{\bar{d}}\right) \tag{2.55}$$

となる。

一方，式(2.34)から最小距離 d_{min} の符号を用いたときにMD-復号法によって正しく復号できない確率 P_{NDC} の下界

$$P_{NDC} \geq \exp\{-n[\sigma g'(\sigma) - g(\sigma)] - C(n,\sigma)\} \quad (2.56)$$

を得る．ここに，$g(\sigma)$ は式(2.45)に示されるものであり，パラメータ σ は式(2.46)により定められる．

式(2.55)と式(2.56)からただちに，つぎの結果を得る．

定理2.8：加群 $S(q)$ の上の符号を図2.2の通信系に用いた場合，2.4.1の（仮定1，2，3）が満たされるなら，信頼度函数 $E(R;P)$ はつぎのような上界をもつ．

$$E_u(R;P) = \sigma r - g(\sigma) \quad (2.57)$$

ここに，$\sigma(\geq 0)$ および r は

$$r = g'(\sigma) = \gamma'(\rho)\{1 - \gamma'(\rho)/2\bar{\alpha}\} \quad (2.58)$$

により定められ，$\rho(\leq 0)$ は

$$\rho\gamma'(\rho) - \gamma(\rho) - R\ln 2 = \varepsilon(>0) \quad (2.59)$$

により定められる．ただし，$g(\sigma)$，$\gamma(\rho)$，$\bar{\alpha}$ はそれぞれ式(2.45)，(2.40)，(2.52)で与えられるものであり，ε は任意に小さい正数である．

$E_U(R;\rho)$ は $E_L(R;\rho)$ と全く同様にして計算することができる。また，実際の数値計算においては $\varepsilon=0$ とおいて差支えない。

$E_U(R;\rho)$ が正となる伝送速度 R の限界 $R_{efU}(\rho)$ も，$R_{efL}(\rho)$ と同様に計算できる。

ここで，前項の $R^*_{efL}(\rho R)$ に対応して，$R^*_{efU}(\rho R)$ を定義しよう。すなわち，

$$R^*_{efU}(\rho R)=\frac{1}{\ln 2}\{\lambda\gamma'(\lambda)-\gamma(\lambda)\}$$

であり，λ は

$$\gamma'(\lambda)\{1-\gamma'(\lambda)/2\bar{d}\}=\sum_{x\in S(f)}W(x)P[\omega(x)|0]$$

により定められる。$R^*_{efU}(\rho R)=0$ となる ρR は前項と同様にして，

$$\frac{\bar{d}}{2}=\sum_{x\in S(f)}W(x)\,P[\omega(x)|0]$$

を満たすものであることが分る。これは前項の結果と全く同一のものである。すなわち，$\rho R=0$ の付近では $R^*_{efL}(\rho R)$ と $R^*_{efU}(\rho R)$ は等しくなり，したがってまた，$R_{efL}(\rho)$ と $R_{efU}(\rho)$ も $R_{ef}\to 0$ となるときのふるまいは一致する。前項最後に述べたことから明らかなように，このことは P_{NDC}

≈ 0 となる通信を行う場合，伝送速度が0に近いような符号を用いると，非常に大きい（中位の伝送速度の符号を用いる場合よりもはるかに大きい）ρ ($= E_B/N_0$) を要することを意味する．

2.5 ハミング距離とリー距離に対する信頼度函数

本節では，ハミング距離とリー距離に対する信頼度函数の下界 $E_L(R;\rho)$ と上界 $E_U(R;\rho)$ および，これらが正であるような伝送速度の限界 $R_{efL}(\rho)$, $R_{efU}(\rho)$ の計算例を示す。

ハミング距離 $d_H(x,y)$ は任意の加群 $S(q)$ の上で，つぎのように定義される[1]．

$$d_H(x,y)=\begin{cases}0 & ; \ x=y\\ 1 & ; \ x\neq y\end{cases} \qquad (2.60)$$

明らかに，$d_H(x,y)$ は $x-y$ のみの函数であり，重み

$$W_H(x)=d_H(x,0)=\begin{cases}0 & ; \ x=0\\ 1 & ; \ x\neq 0\end{cases} \qquad (2.61)$$

が定義できる．$W_H(x)$ をハミング重みと呼ぼう．ハミング

距離に対しては，写像 ω $(S(q) \to Z(q))$ としてどのようなものを考えても，2.4.1 の（仮定 1，2）が満たされることはただちに確かめられる。

リー距離 $d_L(x, y)$ は q を法とする整数の剰余環 $Z(q)$ の上で定義され，

$$d_L(x, y) = \min\{|x-y|, q-|x-y|\} \qquad (2.62)$$

となるものである[2]。$d_L(x, y)$ も $x-y$ のみにより，リー重み

$$W_L(x) = d_L(x, 0) = \min\{|x|, q-|x|\} \qquad (2.63)$$

が定義できる。明らかに，リー距離も 2.4.1 の（仮定 1，2）を満たす（ω は恒等写像とし，無視する）。

$Z(q)$ の上のハミング距離とリー距離は $q=2, 3$ の場合，一致することはいうまでもない。

ハミング距離，リー距離に対する $E_L(R;\rho)$，$E_U(R;\rho)$，$R_{efL}(\rho)$，$R_{efU}(\rho)$ は 2.4.2，2.4.3 に述べた方法によって求めることができる。特に，$q=2$ の場合は，$E_L(R;\rho)$，$E_U(R;\rho)$ の式からパラメータ ρ，σ を消去することができ，つぎのようなやや簡単な形にすることができる。

$$E_L(R;\rho) = -(1-\gamma)\ln(1-\rho) - \gamma\ln\rho - H(\gamma)$$

ここに，
$$H(x) = -x\ln x - (1-x)\ln(1-x)$$

$$\rho = \int_{-\infty}^{0} \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{1}{2}(x-\sqrt{2\rho R})^2\right\} dx$$

であり，γ は

$$\ln 2 - H(2\gamma) = R\ln 2$$

により定められる。

また，$E_U(R;\rho)$ は $E_L(R;\rho)$ と同じ式で与えられ，γ は次式により定められる．

$$\ln 2 - H\left(\frac{1}{2} - \sqrt{\frac{1}{4}-\gamma}\right) = R\ln 2 + \varepsilon$$

ここに ε は任意に小さい正数である．

$q=2$ の場合について，種々の ρ $(=E_B/N_0)$ における $E_L(R;\rho)$ と $E_U(R;\rho)$ を図2.6に示し，$R_{efL}(\rho)$ と $R_{efU}(\rho)$ を図2.7に示す．図2.6にみるように，$E_L(R;\rho)$ と $E_U(R;\rho)$ にはかなりの開きがある。これは，Gilbert の下界と Elias の上界の差に由来する．しかし，$E_L(R;\rho)$ と $E_U(R;\rho)$ は同様な傾向を示し．また $E_L(R;\rho)$ はこのような信頼度函数をもつ符号を，少くとも原理的には構成できるという，

図 2.6　二値符号に対する $E_L(R;\rho)$ と $E_U(R;\rho)$
($\rho(=E_B/N_0) = 5.0;\ 10.0,\ 20.0$)

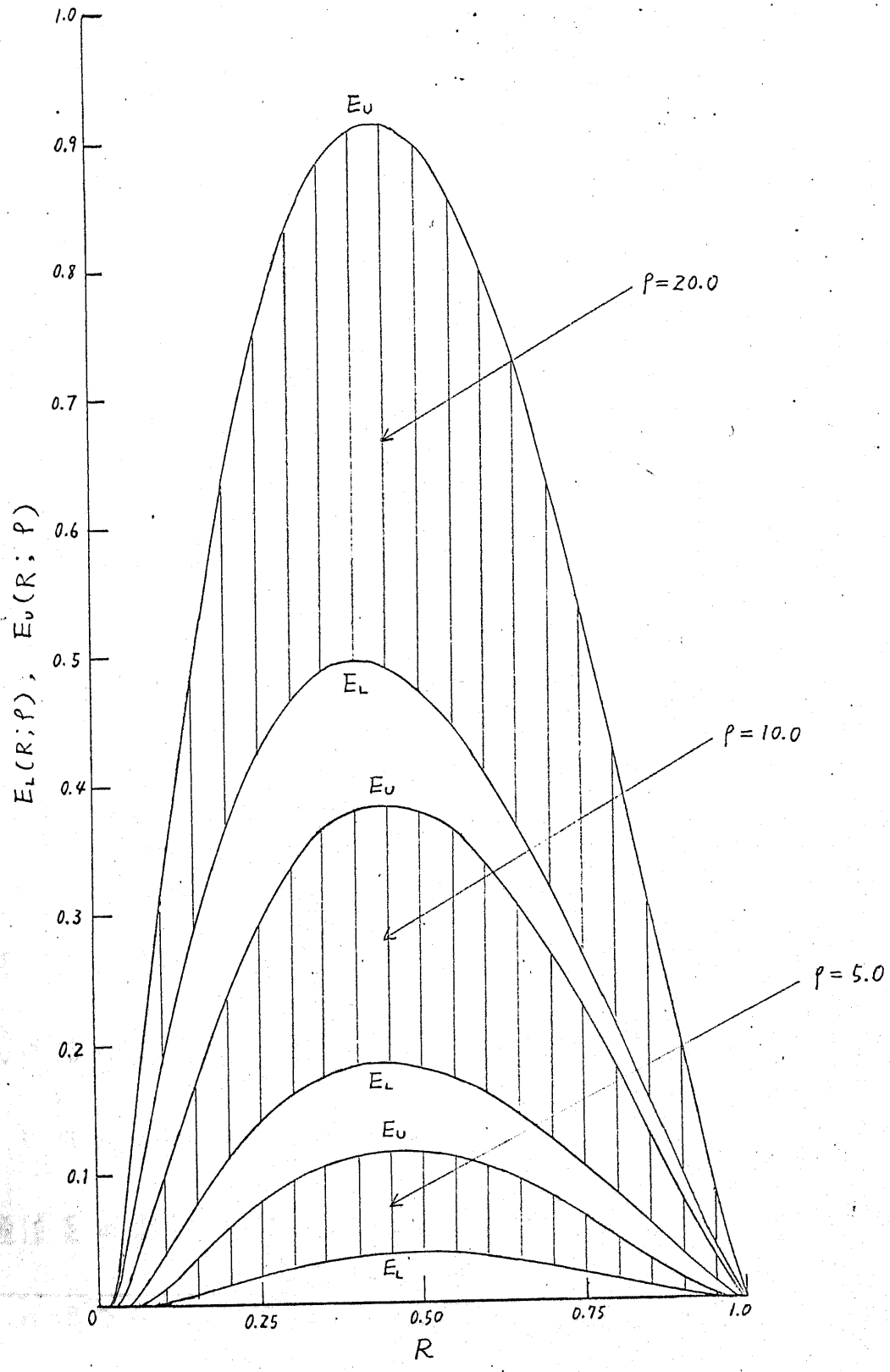
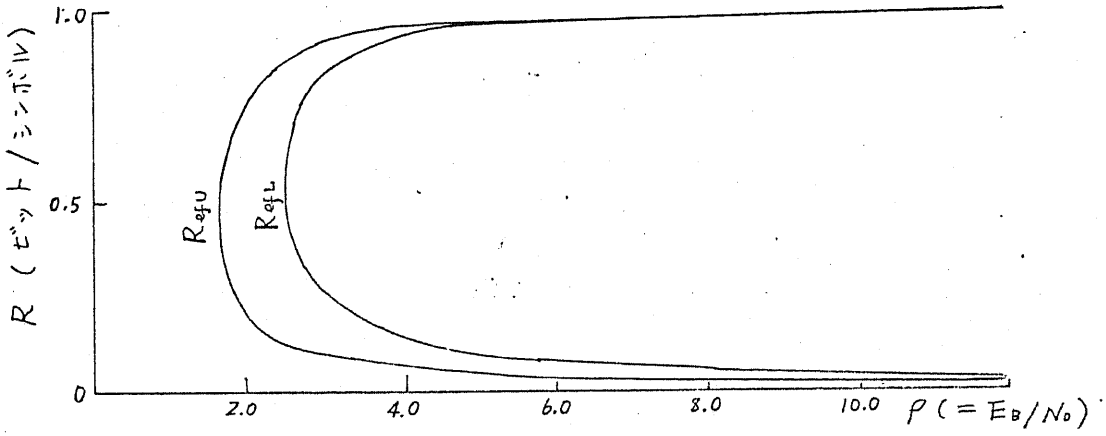


図 2.7　二値符号に対する $R_{ofL}(\rho)$ と $R_{ofU}(\rho)$



$E_U(R;\rho)$ に比べ，やや明確な意味をもつので，以下主として $E_L(R;\rho)$ と $R_{ofL}(\rho)$ によって論ずる．

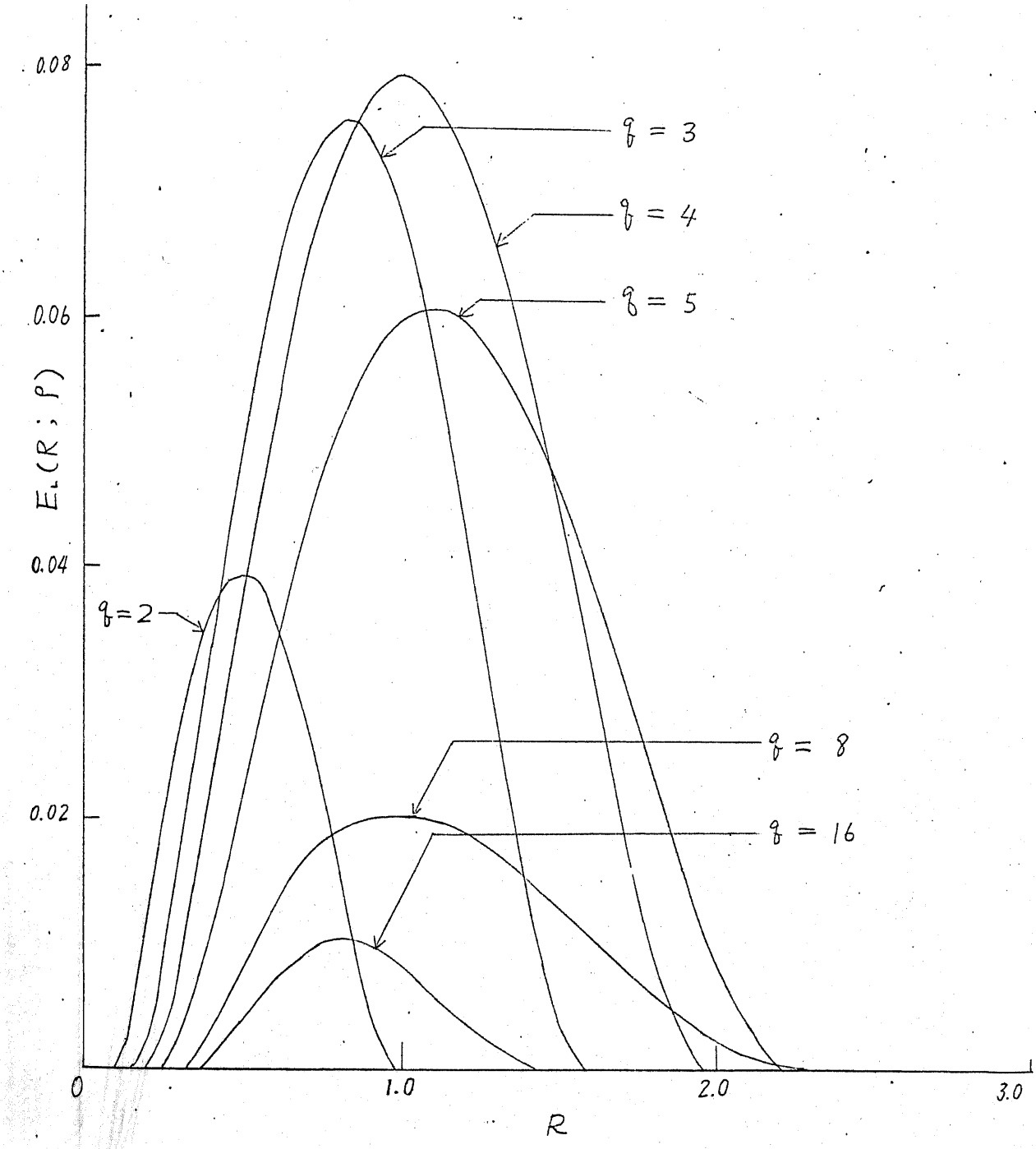
図2.8にリー距離に対する $E_L(R;\rho)$ を $\rho=5.0$, 10.0 の場合について示し，図2.9にはリー距離に対する $R_{ofL}(\rho)$ $R_{ofU}(\rho)$ を示す。図2.9には付録Ⅱで述べるような受信信号に対して最適な処理を行う，符号を用いた多相位相変調通信方式の信頼度函数が正であるような伝送速度 R の限界 $R_{of}^{opt}(\rho)$ も比較のため示してある。* 本章の方式とこの方式との差は通信系の構成を簡単にするために支払うべき代価である。

---

* この場合には $R_{of}^{opt}(\rho)$ は厳密に求まる。文献 (33) 参照．

図 2.8　リー距離に対する $E_L(R;\rho)$

(a)　$\rho\,(=E_b/N_0)=5.0$



(b) $\rho = 10.0$

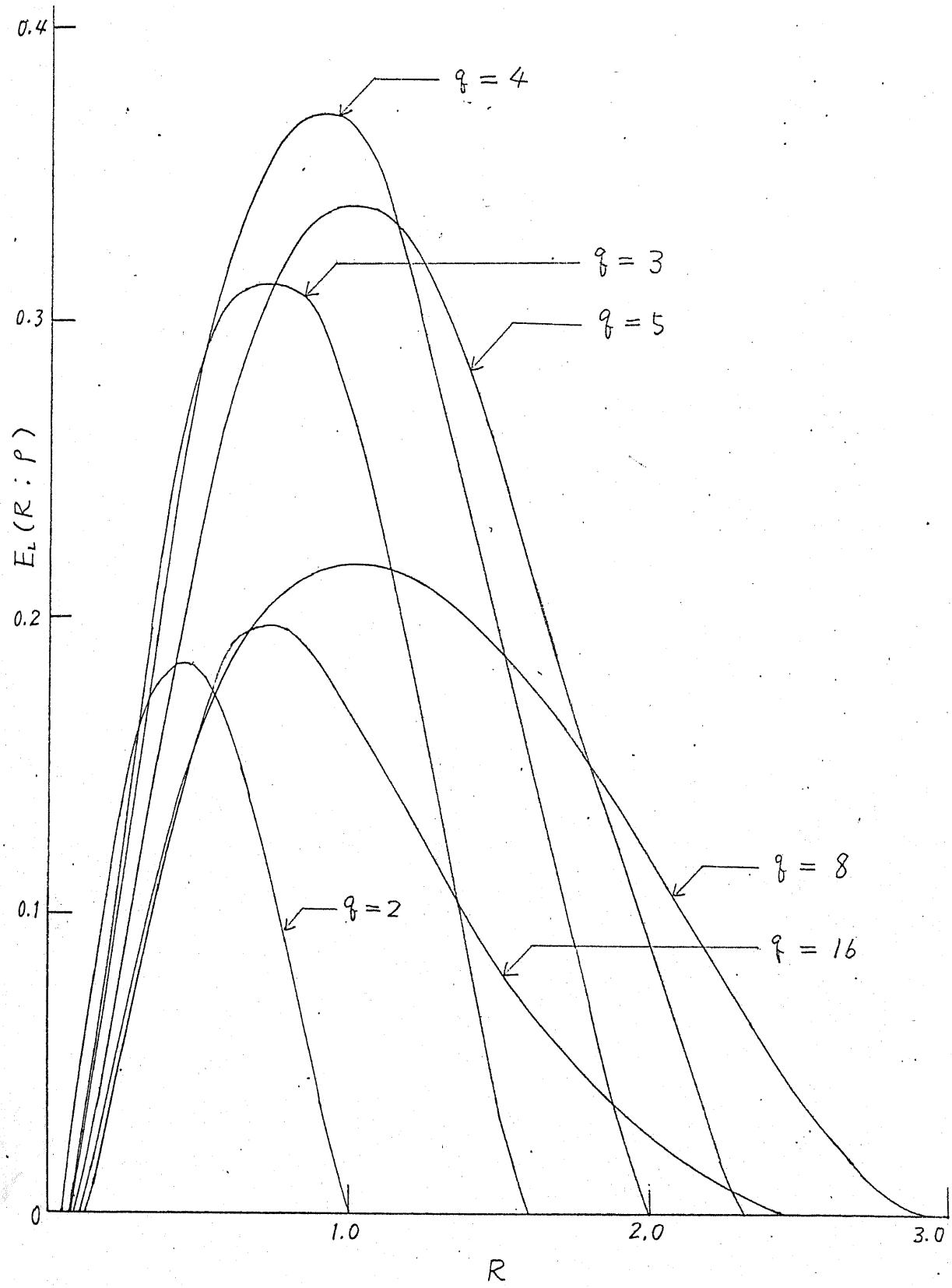
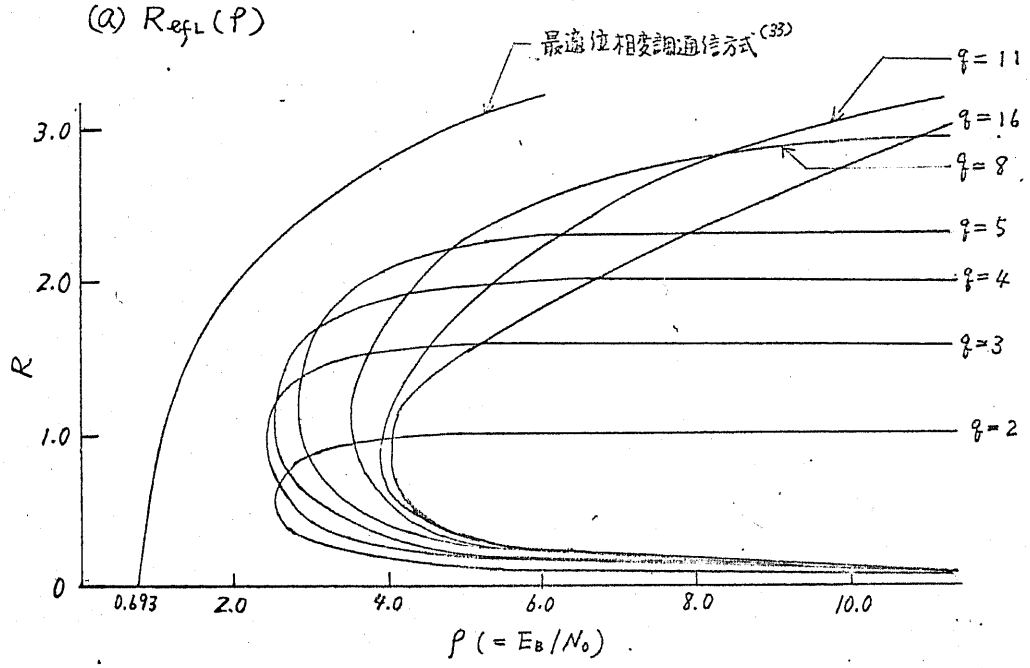


図 2.9　ρ 一 距離 に 対 す る $R_{efL}(\rho)$ と $R_{efU}(\rho)$

(a) $R_{efL}(\rho)$



(b) $R_{efU}(\rho)$

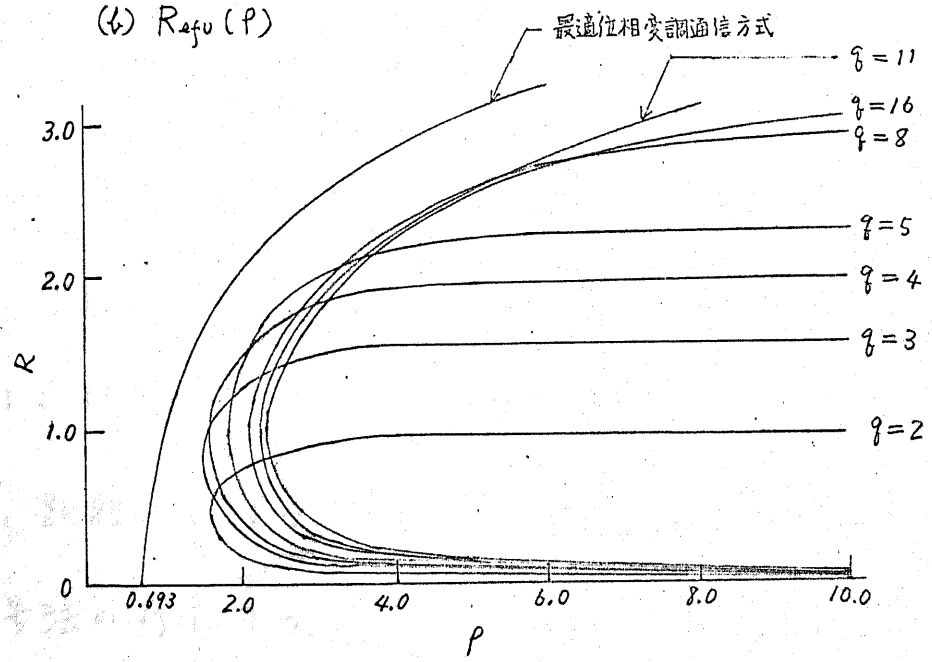


図2.10にはリー距離とハミング距離に対する $E_L(R;\rho)$ を比較して示し，図2.11には $R_{crit}(\rho)$ を比較して示す．なおこれらの図において，Gray距離と示してあるものについては2.7で述べる．

これらの図から，つぎのような結論を得る．

(i) 多相位相変復調を行う超通信路に対しては，リー距離はハミング距離よりも，はるかによく整合している．また，この差は q が大きくなる程大きい．

(ii) 図2.2の通信系に対しては，リー距離を用いても，低伝送速度の符号はきわめて能率が悪い．

(i)は，2.3.2で述べたように超通信路の遷移確率に著しいばらつきがあることから容易に想像できるであろう．それがここではある程度定量的に示された訳である．いうまでもなく，多相位相変復調を行う超通路に対してリー距離がもっともよく整合しているという訳ではない．しかし，2.2で述べた，距離に対するもう一つの要求，簡単な符号構成法および復号法の存在すること，を考慮に入れると，現在のところリー距離以上に超通信路に整合した距離を考えても余り意味

図 2.10　ハミング距離，リー距離，Gray 距離に対する $E_L(R;P)$
；$q = 8$　，　$P\,(= E_B/N_0) = 10.0$

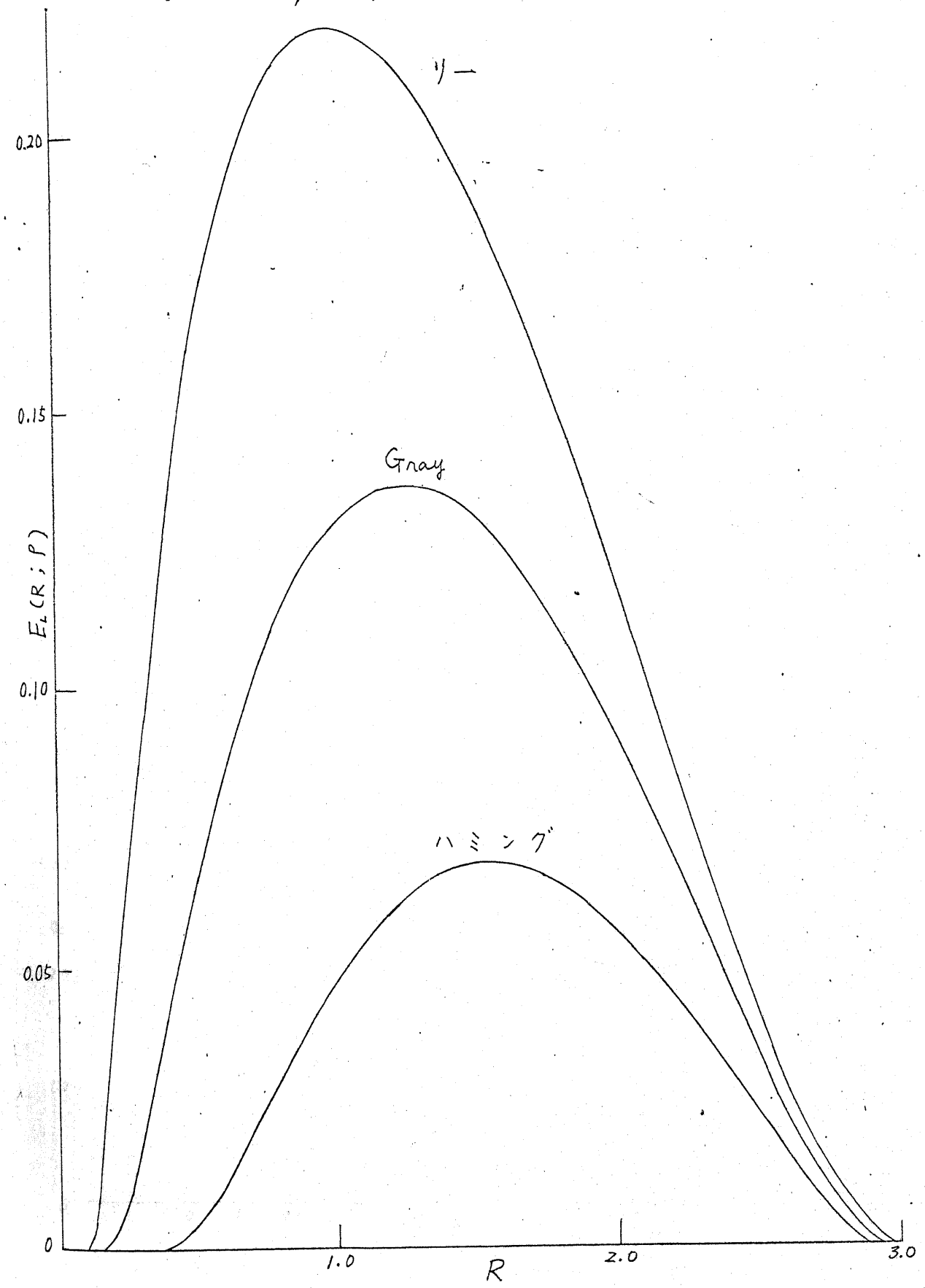
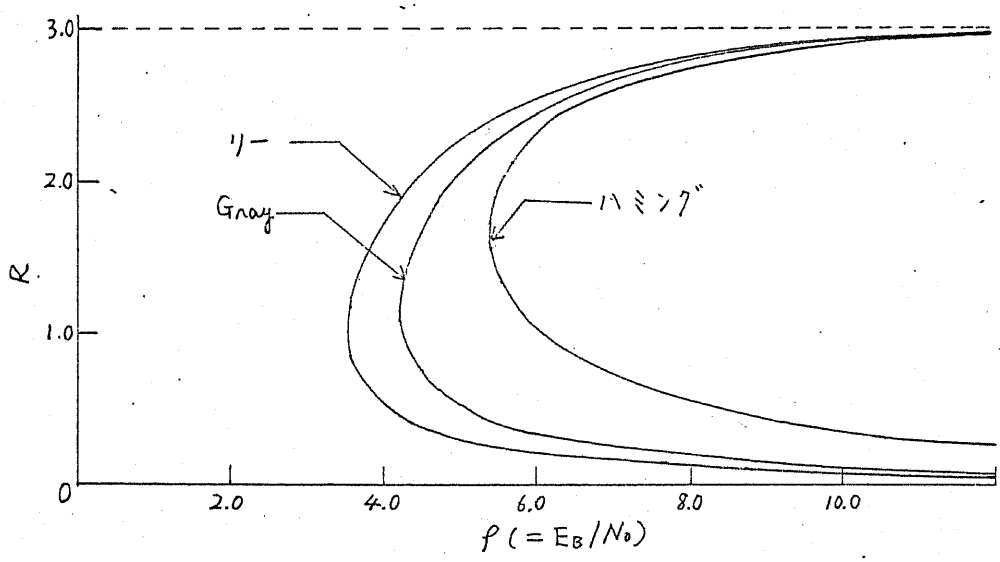
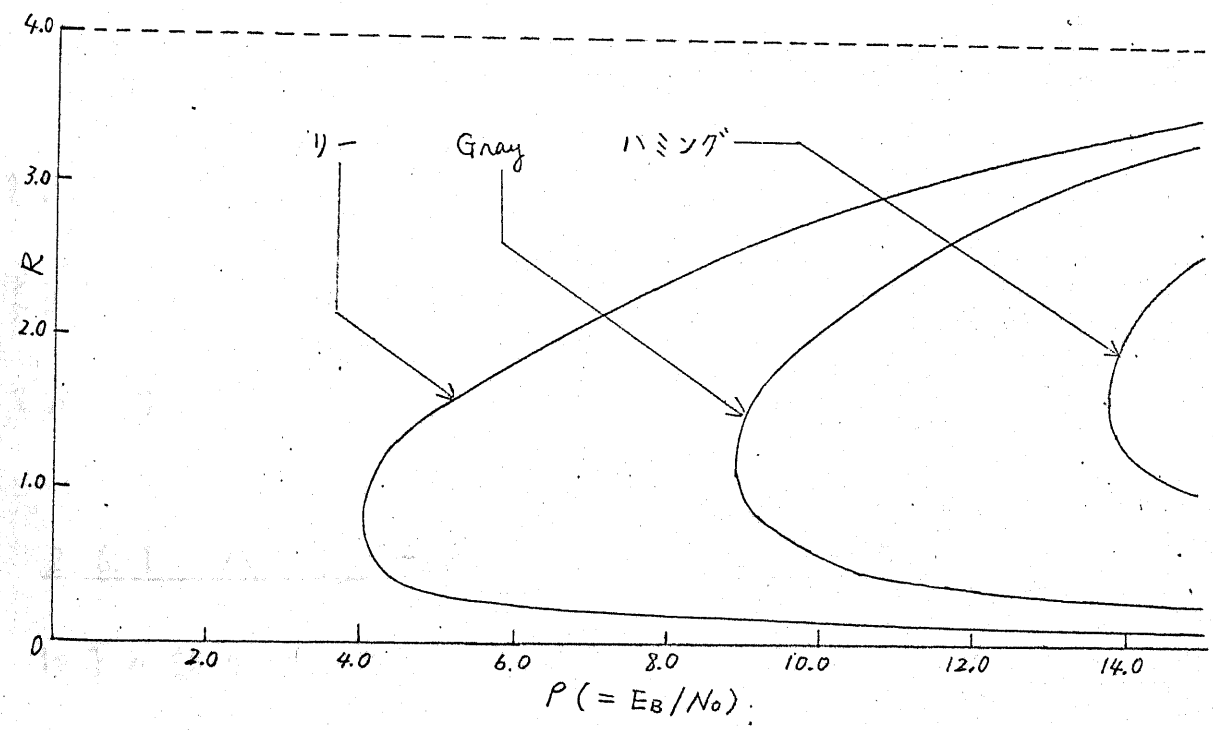


図 2.11 ・ ハミング距離, リー距離, Gray 距離に対する $R_{efl}(\rho)$

(a) $q = 8$



(b) $q = 16$



はないであろう。(ii)は前節最後に述べたことから分るように，一般の距離に対して同様なことが言える。

2.6 リー距離誤り訂正符号

前節でリー距離が多相位相変調通信方式に対し，ハミング距離よりも優れていることを知った。しかし，これまで，リー距離を用いた誤り訂正符号の理論はきわめて少ない。本節では，リー距離を用いて構成される二，三の新しい誤り訂正符号について述べる。

ここで，ある距離Xを用いて構成され，また復号される符号をX距離誤り訂正符号と呼ぶことにしよう。

いうまでもなく，ハミング距離誤り訂正符号はリー距離誤り訂正符号としても用いることができる。そこではじめに，従来知られているハミング距離誤り訂正符号について概説しておこう。

2.6.1 ハミング距離誤り訂正符号 —— 概説

従来の誤り訂正符号の理論は，そのほとんどがハミング距

離を用いたものである。これはハミング距離が種々の数学的に取扱い易い性質をもっているからであろう。たとえば，線形符号の最小ハミング距離は（パリティ検査行列の階数＋1）として与えられ，この性質は符号の構成法あるいは復号法において重要な役割を演ずる．

ハミング距離誤り訂正符号として重要なものにBCH符号[1][2]，Reed-Muller符号[1][5]，幾何学的符号[2][4]*，剰余符号[2]およびSrivastava符号[2]がある．これらは，いずれもがロア体GF(q)（q：素数のべき）の上の線形符号であり，前四者は巡回符号（または，それを修正したもの）として構成できる。復号について言えば，BCH符号，Reed-Muller符号およびSrivastava符号は代数的復号が可能であり，二値Reed-Muller符号および幾何学的符号はしきい値復号法によって簡単な復号ができる[1][2][4][5]．しかし，Reed-Muller符号および幾何学的符号はBCH符号に比べ，一般に能率がよくない。また，剰余符号にはかなり能率のよい符号があるが，

---

* BCH符号，Reed-Muller符号，幾何学的符号はその構成の上からはPolynomial codeとして統一的に論ずることができる[35]．

簡単な復号法は知られていない。さらに、Srivastava 符号は、その能率は BCH 符号と同程度であるが、符号化および復号は BCH 符号に比べ、やや複雑となる。それゆえ現在のところ、ハミング距離誤り訂正符号としては BCH 符号がもっとも重要なものであろう。

BCH 符号はつぎのように定義される。α を $GF(q^m)$ の任意の元とし、$\alpha^l, \alpha^{l+1}, \cdots, \alpha^{l+d-2}$ を根として含む $GF(q)$ の上の最小次数の多項式を $g(x)$ とする。このような $g(x)$ を生成多項式とする $GF(q)$ の上の符号が BCH 符号である。その符号長 n は $\alpha^l, \alpha^{l+1}, \cdots, \alpha^{l+d-2}$ の位数の最小公倍数であるが、$d=2$ の場合を除き n は α の位数と一致する[1]。また、BCH 符号の最小（ハミング）距離 $d_{H\min}$ は少くとも d となることが導ける（BCH bound[1][2]）。ある種の BCH 符号に対しては、さらに詳しく $d_{H\min}$ の値が研究されているが[2][46]、BCH 符号の通常の代数的復号法においては、重みが $(d+1)/2$ 以上の誤りの訂正は保証されない。言い換えれば、BCH 符号の復号においては最小距離 $d_{H\min}$ は d とみなされる。BCH 符号の検査シンボル数、すなわち、

生成多項式 $g(x)$ 次数は簡単な形では表わせない。しかし，その上界として $m(d-1)$ をとり得ることは明らかである．また，$l=1$ となる場合には，$m(d-1)$ を q で割った商を Q とするとき，検査シンボル数の簡単な上界として $m(d-1)-Q$ を得る。特に $q=2$，$d=2t+1$ のときは検査ビット数の上界は mt となる．

符号長が q^m-1 となる BCH 符号を原始 BCH 符号と呼ぶ．原始 BCH 符号で $l=1$ となるものは，もっとも標準的 BCH 符号であり，このような符号の中に優れたものが多い。

$q=2$ の場合には，以上述べた符号の他にも種々の重要な符号がある[36][44]．これらの中で Preparata 符号および修正 Preparata 符号については次章で述べる。

さて，ハミング重みが t 以下の誤りを訂正できる符号によって，リー重みが t 以下のすべての誤りを訂正できることはいうまでもない．しかし，明らかに，このような符号はリー距離誤り訂正符号としては能率の悪いものである．次項以下で，より能率のよいリー距離誤り訂正符号について述べよう．

2.6.2 Berlekamp の符号とその一般化

現在知られているリー距離誤り訂正符号はきわめて限られており，その中である程度一般性をもつのは Berlekamp の見出した符号[2]だけである．ここでは，この Berlekamp の符号とそれをやや一般化した形の符号について述べておく．

α を1の原始 $2n$ 次根[7]，t を $\frac{p-1}{2}$（p：素数）以下の正整数とし，$\alpha, \alpha^3, \alpha^5, \cdots, \alpha^{2t-1}$ を根として含む $GF(p)$ の上の最小次数の多項式を $g(x)$ とする。α の定義から明らかなように，$g(x)$ は $x^{2n}-1$ を割り切り，x^n-1 を割り切らないから，$g(x)$ は x^n+1 を割り切る．それゆえ，$g(x)$ により符号長 n の (-1)-巡回符号* を構成できる．また α を含む $GF(p)$ の最小の拡大体[7]を $GF(p^m)$ とすれば，この符号の検査ディジット数は高々 mt となる**．Berlekamp は，さらに，このような符号のリー最小距離が少なくとも $2t+1$

---

* $x^n-\xi$（$\xi \in GF(q)$）を割り切る多項式によって生成される（$(x^n-\xi)$ を法とする多項式の剰余環の上で定義される）符号長 n の符号をリー巡回符号と呼ぶ．文献(2) p.303 参照．

** α として $GF(p^m)$ の原始元を選ぶときには丁度 mt となることが容易に確かめられる．

となること*，および この符号が BCH 符号の復号に類似した代数的な方法で復号でき，t 重み t 以下の誤りを訂正できることを示した。

Berlekamp の符号は GF(p) の上の符号長 2n の BCH 符号の検査シンボルをおよそ半分除いたものであるということができる**．ただし，符号長は 1/2 に縮められている。

ここで，Berlekamp の符号をやや一般化しておこう。

GF(p^m) の 0 および 1 でない任意の元を c とし，GF(p^m) の元のつぎのような二つの集合 A_1 と A_2 を考える。

$$A_2 = cA_1 \equiv \{cx \mid x \in A_1\}$$

$$A_1 \cap A_2 = \phi$$

ここに ϕ は空集合を示す。いま A_1 に含まれる元の数を n とし，A_1 の元を $a_0, a_1, \cdots, a_{n-1}$ で表わそう。このとき，つぎのようなパリティ検査行列 H をもつ GF(p) の上の符号を考えよう。

$$H = \{ a_{j-1}^{i} (1 - c^i) \} \quad (i = 1, \cdots, 2t,\ j = 1, \cdots, n)$$

---

* $t = \frac{p-1}{2}$ ととるときは，下度 p となることが示されている[2]。

** α として GF(p^m) の原始元を選ぶときは下度半分となる。

$$= \begin{bmatrix} a_0(1-C) & a_1(1-C) & a_2(1-C) & \cdots\cdots & a_{n-1}(1-C) \\ a_0^2(1-C^2) & a_1^2(1-C^2) & & & a_{n-1}^2(1-C^2) \\ a_0^3(1-C^3) & \vdots & & & \vdots \\ \vdots & & & & \\ a_0^{2t}(1-C^{2t}) & a_1^{2t}(1-C^{2t}) & \cdots\cdots & \cdots\cdots & a_{n-1}^{2t}(1-C^{2t}) \end{bmatrix} \cdot \qquad (2.64)$$

ここに H の各成分は $GF(p)$ の上の縦ベクトルとして表わされているものとし，各 i ($1 \leq i \leq 2t$) に対し，$a_0^i(1-C^i)$，…，$a_{n-1}^i(1-C^i)$ は同一次元のベクトルとして表わす。

このような符号に対し，つぎの定理が導ける。

定理 2.9：$t \leq \frac{p-1}{2}$ であるとき，式 (2.64) のパリティ検査行列をもつ $GF(p)$ の上の符号の最小リー距離は少くとも $2t+1$ である。

(証明) $GF(p)$ の上の長さ n の語の各成分の位置を a_i で表わすこととする。すなわち，語の $i+1$ 番目の成分の位置を a_i で表わすこととする。ここで，誤り語 e において 0 でない成分の位置を X_j ($j = 1, \cdots, e$)，またその値を Y_j ($j = 1, \cdots, e$) とする。ただし，e は e に含まれる 0 でない成分の数である。Y_j は $GF(p)$ の元であるが，ここでは，$-\frac{p-1}{2} \leq Y_j \leq \frac{p-1}{2}$ の範囲内の整数で表わすとしよう。このとき e のリー重みは

$$W_L[e] = \sum_{j=1}^{e} |Y_j|$$

となる。さらに，X_j'，X_j'' をつぎのように定める。

$$X_j' = \begin{cases} cX_j & ; Y_j > 0 \\ X_j & ; Y_j < 0 \end{cases} \qquad X_j'' = \begin{cases} X_j & ; Y_j > 0 \\ cX_j & ; Y_j < 0 \end{cases}$$

ここで，つぎの二つの多項式を定義する*。

$$\sigma(z) = \prod_j (1 - X_j' z)^{|Y_j|} \tag{2.65}$$

$$\overline{\sigma}(z) = \prod_j (1 - X_j'' z)^{|Y_j|} \tag{2.66}$$

これらを error locator と呼ぼう。

ある誤り語 e に対し，$\sigma(z)$ または $\overline{\sigma}(z)$ を知ることができれば，その誤り語を完全に定めることができる。これは $\sigma(z)$ の根 $1/X_j'$ とその多重度 $|Y_j|$ を求め，$X_j' \in A_1$ であれば，$X_j = X_j'$，$Y_j = -|Y_j|$，$X_j' \in A_2$ であれば $X_j = c^{-1} X_j'$，$Y_j = |Y_j|$ とすればよい。

以下，誤り語のリー重みが t 以下なら，式(2.64)のパリティ検査多項式によって得られるシンドロームから $\sigma(z)$ および $\overline{\sigma}(z)$ が求まることを示す。このため，つぎのような

---

* $\sigma(z)$ は Berlekamp の符号に対する error locator に対応するものである。文献(2) p.212 参照。

の有理函数 $U(z)$ を用いる。

$$U(z)=\frac{\sigma(z)}{\bar{\sigma}(z)}=\frac{\prod_i (1-X_i z)^{|Y_i|}}{\prod_i (1-X_i z)^{|Y_i|}}=\prod_i \left(\frac{1-cX_i z}{1-X_i z}\right)^{Y_i} \qquad (2.67)$$

$U(z)$ を z で微分して整理すれば、

$$U'(z)=U(z)\left\{\sum_i Y_i\left(\frac{X_i}{1-X_i z}-\frac{cX_i}{1-cX_i z}\right)\right\} \qquad (2.68)$$

を得る。さらに $\frac{X_i}{1-X_i z}$ および $\frac{cX_i}{1-cX_i z}$ を z のべき級数に展開して

$$U'(z)=U(z)\left\{\sum_{\nu=1}^{\infty}\left[\sum_i X_i^{\nu}(1-c^{\nu})Y_i\right]z^{\nu}\right\}z^{-1} \qquad (2.69)$$

が導ける。ここで、

$$\Delta_\nu=\sum_i X_i^{\nu}(1-c^{\nu})Y_i \qquad \nu=1,2,\cdots \qquad (2.70)$$

$$\Delta(z)=\sum_{\nu=1}^{\infty}\Delta_\nu z^{\nu} \qquad (2.71)$$

とおき、式 (2.69) に代入すれば、

$$zU'(z)=U(z)\Delta(z) \qquad (2.72)$$

を得る。

ところで、$\nu=1,\cdots,2t$ に対して式 (2.70) の Δ_ν は式 (2.64) の H に対するシンドロームとして得られる。一方、$U(z)$ をべき級数に展開して、

$$U(z)=\sum_{\nu=0}^{\infty}U_\nu z^{\nu}$$

とおけば，式(2.72)から

$$\begin{aligned} U_1 &= U_0 S_1 \\ 2U_2 &= U_0 S_2 + U_1 S_1 \\ 3U_3 &= U_0 S_3 + U_1 S_2 + U_2 S_1 \\ &\vdots \\ 2tU_{2t} &= U_0 S_{2t} + U_1 S_{2t-1} + \cdots + U_{2t-1} S_1 \end{aligned} \qquad (2.73)$$

を得る．明らかに $U_0 = U(0) = 1$ であるから，$t \leq (p-1)/2$ である限り，$S_1, \cdots, S_{2t}$ から $U_1, \cdots, U_{2t}$ を順次求めていくことができる。言い換えれば，$\sigma(z)/\bar{\sigma}(z)$ のべき級数展開の $2t$ 次以下の項はシンドロームから一意に定まる。それゆえ，このようなべき級数に対し，リー重みが t 以下の誤り語に対する error locator $\sigma(z)$ および $\bar{\sigma}(z)$ が一意に定まることを言えば定理は証明される。

もし，一意でないとすれば，

$$\frac{\rho(z)}{\bar{\rho}(z)} - \frac{\sigma(z)}{\bar{\sigma}(z)} = z^{2t+1} m(z) \qquad (2.74)$$

となる t 次以下の別の error locator $\rho(z)$, $\bar{\rho}(z)$ が存在する．ただし，$m(z)$ は無限次元の多項式である。式(2.74)の両辺に $\bar{\rho}(z)\cdot\bar{\sigma}(z)$ を掛けて，$\rho(z)\bar{\sigma}(z)$ および $\bar{\rho}(z)\sigma(z)$

の次数が $2t$ 次以下であることを考慮すると,

$$P(z)\bar{\sigma}(z) - \bar{P}(z)\sigma(z) = 0$$

を得る. ゆえに, $P(z)/\bar{P}(z) = \sigma(z)/\bar{\sigma}(z)$. すなわち, $\sigma(z)/\bar{\sigma}(z)$ は一意に定まる. $\sigma(z)$ と $\bar{\sigma}(z)$ は共通根をもたないから互いに素であり, $\sigma(0) = \bar{\sigma}(0) = 1$ であるから, $\sigma(z)$ と $\bar{\sigma}(z)$ も一意に定まる. (証明終)

定理2.9の符号の復号は証明から明らかなように, シンドロームから式(2.73)により $U_1, U_2, \cdots, U_{2t}$ を求め, これにより, 式(2.67)の $\sigma(z)$ を求めることにより行える. $\sigma(z)$ を求めるためには,

$$\bar{\sigma}(z)\left(\sum_{i=0}^{2t} U_i z^i\right) = \sigma(z) \bmod z^{2t+1} \qquad (2.75)$$

を t 次以下の多項式 $\bar{\sigma}(z)$, $\sigma(z)$ について解けばよいが, これはBCH符号の復号における Berlekamp のアルゴリズムをそのまま適用できる (文献(2), p. 184 参照).

ここで, $1 - c^i = 0$ となる $2t$ 以下の正整数 i すべての集合を I とすれば, 定理2.9の符号はまた,

$$H' = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_0^2 & a_0^2 & & & \vdots \\ \vdots & \vdots & & & \vdots \\ a_0^{2t} & a_1^{2t} & & & a_{n-1}^{2t} \end{bmatrix} \qquad (2.76)$$

となる行列 H' から，$\{a_j^i \mid j=0,1,\cdots,n-1, i\in I\}$ となる成分を除いた行列をパリティ検査行列とする符号と考えることができる。それゆえ各 i ($1\leq i\leq 2t$) について，$\{a_j^i \mid j=0,1,\cdots,n-1\}$ を含む $GF(p)$ の最小の拡大体を $GF(p^{m_i})$ とすれば，この符号の検査シンボル数は高々 $\sum_{\substack{i\in I\\ 1\leq i\leq 2t}} m_i$ となる。したがって，一般に c として位数の小さいものを選ぶほど，検査シンボル数を減らし得る。

ところで，定理2.9の符号において $c=-1$ とし α を1の原始 $2n$ 次根，$A_1=\{\alpha^i \mid i=0,1,\cdots,n-1\}$ とすれば，Berlekamp の符号となる。-1 は1を除いて位数が最小となるが GF 体の元であるから，定理2.9の符号の中で Berlekamp の符号が通常もっとも優れていると思われる。

2.6.3 $\mathbb{Z}(p^m-1)$ の上のリー距離誤り訂正符号

Berlekamp の符号および定理2.9の符号に課せられるもっとも大きな制約の一つは訂正できるリー重みの最大値が $(p-1)/2$ となることであり，もう一つは $GF(p)$ (p：素数) の上でしか構成できないということである。

本項に述べる符号は p^m-1 を法とする整数の剰余環 $Z(p^m-1)$ の上で構成できるが，訂正できる誤りの一重み対しては同様の制約が課せられる．また，符号長がかなり厳しく制限される．

α を $GF(p^m)$ の原始元とし，$GF(p^m)$ における対数を

$$\log_\alpha \alpha^i = i$$

によって定義する．ここに，i は $Z(p^m-1)$ の元である．

ここで，つぎのようなパリティ検査行列 H をもつ $Z(p^m-1)$ の上の符号を考える．

$$H=\begin{bmatrix} \log_\alpha \frac{b_1-a_0}{a_0b_1-1} & \log_\alpha \frac{b_1-a_1}{a_1b_1-1} & \log_\alpha \frac{b_1-a_2}{a_2b_1-1} & \cdots & \log_\alpha \frac{b_1-a_{m-1}}{a_{m-1}b_1-1} \\ \log_\alpha \frac{b_2-a_0}{a_0b_2-1} & \log_\alpha \frac{b_2-a_1}{a_1b_2-1} & \cdots & & \vdots \\ \vdots & \vdots & & & \vdots \\ \log_\alpha \frac{b_x-a_0}{a_0b_x-1} & \log_\alpha \frac{b_x-a_1}{a_1b_x-1} & \cdots & \cdots & \log_\alpha \frac{b_x-a_{m-1}}{a_{m-1}b_x-1} \end{bmatrix} \tag{2.77}$$

ここに，$\{a_0, a_1, \cdots, a_{m-1}, b_1, \cdots, b_x\}$ は $GF(p^m)$ の異なる元の集合であり，$0, 1, -1$ は含まないとする．また，x $(\in GF(p^m))$ がこの集合に含まれていれば x^{-1} は含まれないとする．したがって，この符号の符号長は，$p=2$ のと

まで，最大限

$$n = \frac{p^m - 2}{2} - t \tag{2.78}$$

となり，$p \geq 3$ のとき，最大限

$$n = \frac{p^m - 3}{2} - t \tag{2.79}$$

となる。また，最小ハミング距離はつぎの定理で与えられる。

定理 2.10 ：式(2.77)をパリティ検査行列とする $\mathbb{Z}(p^m - 1)$ の上の符号の最小ハミング距離は少くとも $2t+1$ となる。

(証明) $\mathbb{Z}(p^m - 1)$ の上の長さ n の語の各成分の位置を，前項と同様 a_i $(i = 0, 1, \cdots, n-1)$ で表わし，誤り語の 0 でない成分の位置と値をそれぞれ，X_j $(\in GF(p^m))$，Y_j $(\in \mathbb{Z}(p^m - 1))$ $(j = 1, \cdots, e)$ で表わす。ただし，Y_j は $-\frac{p^m - 2}{2} \leq Y_j \leq \frac{p^m - 1}{2}$ の範囲内の整数で表わすものとする。

ここで，シンドロームを $s_1, s_2, \cdots, s_t$ としよう。ただし，s_i は式(2.77)のパリティ検査行列の i 行に対応するものとする。したがって，

$$s_i = \sum_j Y_j \log_\alpha \left(\frac{b_i - X_j}{X_j b_i - 1} \right) = \log_\alpha \prod_j \left(\frac{b_i - X_j}{X_j b_i - 1} \right)^{Y_j}$$

ゆえに，

$$\prod_j \left(\frac{b_i - X_j}{X_j b_i - 1}\right)^{Y_j} = \alpha^{p_i} \quad i = 1, \cdots, t \qquad (2.80)$$

を得る．いま

$$U(z) = \prod_j \left(\frac{z - X_j}{X_j z - 1}\right)^{Y_j} \qquad (2.81)$$

となる函数を定義すれば，式(2.80)は t 個の点において $U(z)$ の値を指定する式となっている．

ここで，$U(z)$ をつぎの形で表わそう．

$$U(z) = \frac{\sigma(z)}{\tilde{\sigma}(z)}$$

ここに，$\sigma(z)$ は0次の係数が1となる多項式であり，error locator となる．$\tilde{\sigma}(z)$ は，$\sigma(z)$ の根の逆元を根として含み，おのおのの対応する根について同一の多重度をもつから，$\sigma(z)$ の相反多項式となっている．すなわち，

$$\tilde{\sigma}(z) = \sigma(z^{-1}) z^{\deg \sigma(z)}$$

ただし，$\deg \sigma(z)$ は $\sigma(z)$ の次数を示す．

$\sigma(z)$ が定まれば，その根と多重度を求めることによって，X_j と Y_j を知ることができるから，誤り語のリー重みが t 以下のとき，すなわち，

$$\sum_j |Y_j| \leq t \qquad (2.82)$$

のとき，式 (2.80) から $\sigma(z)$ が一意に定まることを言えば定理は証明されたこととなる．

ここで，式 (2.80) すなわち

$$\sigma(b_i) / \tilde{\sigma}(b_i) = \alpha^{\rho_i} \qquad i = 1, 2, \cdots, t \quad (2.83)$$

が成立すれば，$\tilde{\sigma}(z)$ が $\sigma(z)$ の相反多項式であることから

$$\sigma(b_i^{-1}) / \tilde{\sigma}(b_i^{-1}) = \alpha^{-\rho_i} \qquad i = 1, 2, \cdots, t \quad (2.84)$$

が成立すること，および常に，

$$\sigma(-1) / \tilde{\sigma}(-1) = 1 \quad (2.85)$$

となることに注意しておこう．

いま，式 (2.82) が満たされるとしよう．このとき明らかに

$$\deg \sigma(z) = \deg \tilde{\sigma}(z) \leq t$$

ここで，t 次以下の多項式 $p(z)$ および $\eta(z)$ が存在して，

$$\frac{p(b_i)}{\eta(b_i)} = \alpha^{\rho_i} \qquad \frac{p(b_i^{-1})}{\eta(b_i^{-1})} = \alpha^{-\rho_i} \qquad i = 1, 2, \cdots, t$$

$$\frac{p(-1)}{\eta(-1)} = 1$$

であるとする．このとき $p(z)$ はシンドローム ρ_i $(i = 1, \cdots, t)$ によって定まる error locator となる可能性がある．ところが，

$$r(z) = \sigma(z)\eta(z) - \tilde{\sigma}(z)p(z)$$

とおけば，ただちに，

$$r(b_i) = 0 \qquad r(b_i^{-1}) = 0 \qquad i = 1, \cdots, t$$

$$r(-1) = 0$$

となることが導ける．$\{b_i\}$ に対する仮定により，b_i, b_i^{-1} $(i = 1, \cdots, t)$ および -1 はすべて異なるから，$r(z)$ は $2t+1$ 個の異なる根をもつ．しかも，$r(z)$ の次数は仮定から $2t$ 以下であるから，$r(z) = 0$ でなければならない．ゆえに $\sigma(z)/\delta(z)$ は式 (2.80) から一意に定まる．しかも $\sigma(z)$ と $\delta(z)$ は互いに素であり，$\sigma(0) = 1$ であるから，$\sigma(z)$ は一意に定まる．　(証明終)

なお，この符号のように，いくつかの点における error locator の値をシンドロームから求めるという考え方は，Srivastava によってハミング距離誤り訂正符号に対し用いられたものである（文献 (2)，p. 350 参照）．

この符号の復号はつぎのようにすればよい．

(1) シンドローム A_i $(i = 1, \cdots, t)$ を計算する．

(2) $\dfrac{\sigma(b_i)}{\delta(b_i)} = \alpha^{A_i}$，$\dfrac{\sigma(b_i^{-1})}{\delta(b_i^{-1})} = \alpha^{-A_i}$ $(i = 1, \cdots, t)$，$\dfrac{\sigma(-1)}{\delta(-1)} = 1$

および $\sigma(0)=1$ を満たす互いに素な t 次以下の多項式 $\sigma(z)$, $\zeta(z)$ を求める。

(3) $\sigma(z)$ の根 X_j' およびその多重度 $|Y_j|$ を求め，$X_j'=a_i$ となる位置 a_i が存在すれば，誤りの位置を $X_j=a_i$，その値を $Y_j=|Y_j|$ とする。また $X_j'=a_i^{-1}$ となる a_i が存在すれば $X_j=a_i$，$Y_j=-|Y_j|$ とする。

なお，(2) の $\sigma(z)$ と $\zeta(z)$ $(=\tilde{\sigma}(z))$ を求めるには，Srivastava の符号の復号における Berlekamp のアルゴリズムを用いればよい（文献(2)，P. 351 参照）。

さて，本項に示した符号は環の上の符号であるので，組織符号になるとは限らない。それゆえ，その符号語数を定めるのは一般には難かしく，実際にパリティ検査行列を作って調べてみなければならない。しかし，$a_0, a_1, \cdots, a_{n-1}$ および $b_1, \cdots, b_t$ を適当に選択することによって，多くの場合 $Z(p^m-1)$ の上の組織符号となり，その検査ディジット数が高々 t となることが期待できる。

最後にいくつかの例を示しておこう。

例2.1) $Z(p^m-1)$ の上のリー距離誤り訂正符号

(i) $p=2$, $m=4$, $p^m-1=15$, $n=5$, $t=2$ の場合：α を $\alpha^4+\alpha+1=0$ を満たす $GF(2^4)$ の原始元とし，$\{a_0, a_1, \cdots, a_4\}=\{\alpha, \alpha^2, \cdots, \alpha^5\}$, $\{b_1, b_2\}=\{\alpha^6, \alpha^7\}$ とする。このとき，式(2.77)のパリティ検査行列 H は

$$H=\begin{bmatrix} 2 & 1 & -5 & 7 & -3 \\ -3 & 5 & -1 & 6 & -2 \end{bmatrix}$$

となる。H から，行操作により

$$H'=\begin{bmatrix} 1 & 0 & -3 & -7 & 1 \\ 0 & 1 & 1 & 6 & -5 \end{bmatrix}$$

を得る。ゆえに，この符号の生成行列（の転置行列）は

$$G^t=\begin{bmatrix} -1 & 5 & 1 & 0 & 0 \\ 7 & -6 & 0 & 1 & 0 \\ 3 & -1 & 0 & 0 & 1 \end{bmatrix}$$

となる。したがって，この符号は $Z(15)$ の上の $(5, 3)$ 符号であり，最小リー距離は5である。

(ii) $p=5$, $m=2$, $p^m-1=24$, $n=8$, $t=3$ の場合：α を $\alpha^2+\alpha+2=0$ を満たす $GF(5^2)$ の原始元とし，$\{a_0, a_1, \cdots, a_8\}=\{\alpha, \alpha^2, \cdots, \alpha^8\}$, $\{b_1, b_2, b_3\}=\{\alpha^9, \alpha^{10}, \alpha^{11}\}$ とする。このとき，

$$H=\begin{bmatrix} 5 & -6 & 9 & 1 & -4 & -10 & 11 & -7 \\ 8 & 3 & -6 & 11 & -7 & -9 & 4 & 5 \\ -2 & 8 & 5 & 10 & 6 & 7 & 9 & -3 \end{bmatrix}$$

となる。行操作により，

$$H'=\begin{bmatrix} 1 & -3 & 0 & 0 & 11 & -10 & 12 & -1 \\ 0 & 9 & 0 & 1 & 7 & 7 & -10 & 9 \\ 0 & 0 & 1 & 0 & 6 & -7 & -7 & -3 \end{bmatrix}$$

を得る．ゆえに，この場合も組織符号となる（1，3，4番目のシンボルを検査シンボルとることができる）．したがって，この符号は $\mathbb{Z}(24)$ の上の $(8, 5)$ 符号であり，最小り一距離は 7 である．

(iii) $p=2$，p^m-1 が素数の場合：このときは $\mathbb{Z}(p^m-1)$ は体となるから，常に組織符号となる．この符号の符号長は $n=\frac{p^m-2}{2}-t$ までとることができ，最小り一距離は少くとも $2t+1$，検査シンボル数は高々 t となる．それゆえ GF (p^m-1) $(=\mathbb{Z}(p^m-1))$ の上の符号長 $\frac{p^m-2}{2}$ の Berlekamp の符号に比べ，検査シンボル数は等しいかまたは少ないが，符号長は短かくなる．

2.6.4 低伝送速度のリー距離誤り訂正符号

2.5で述べたように，低伝送速度の符号は図2.2のような通信系に対しては著しく不利である．しかし，低伝送速度の符号は付録IIで述べるような通信系においては有効であり，信号設計問題との関連において興味がもたれる。

2.6.4.1 M系列符号のリー距離の構造

低伝送速度の符号として代表的なものはM系列符号（maximum length FSR code[2]）である．これは，$GF(q^m)$の原始元をαとするとき，αの$GF(q)$の上の最小多項式$h_\alpha(x)$をパリティ検査多項式とする$GF(q)$の上の符号長q^m-1，情報シンボル数mの巡回符号であり，多くの興味深い性質をもっている．ここでは，M系列符号のリー距離の構造についてみておこう．

M系列符号は一般のガロア体$GF(q)$の上で定義できるが，このような場合にも，2.3で述べた写像ωを導入して，リー距離を定義することにしよう。すなわち，$GF(q)$からqを法とする整数の剰余環$Z(q)$の上への1対1の写像をωとし，$Z(q)$の上で定義されたリー距離d_Lにより$GF(q)$に

おけるリー距離を

$$d_{L\omega}(x,y) = d_L(\omega(x), \omega(y)) \quad (x, y \in GF(q))$$

によって定義する。このとき、つぎの定理が導ける。

定理2.11*: $GF(q)$ の上の符号長 q^m-1 のM系列符号において、符号語 0 から他の符号語へのリー距離はすべて等しく $q^m\bar{d}$ で与えられる。また 0 でない符号語 $\mathcal{X}$ から他の符号語 $\mathcal{Y}$ へのリー距離 $d_{L\omega}[\mathcal{X}, \mathcal{Y}]$ はつぎのようになる。

$$d_{L\omega}[\mathcal{X},\mathcal{Y}] = \begin{cases} q^{m-1} \sum_{x \in GF(q)} d_L(\omega(x), \omega(y)) & ; \ \mathcal{X} = a\mathcal{Y} \text{ となる } a(\neq 0) \in GF(q) \text{ が存在する場合} \\ q^m\bar{d} & ; \text{その他の場合} \end{cases}$$

ここに、$\bar{d}$ は次式で定められる。

$$\bar{d} = \begin{cases} \dfrac{q}{4} & ; q \text{ が偶数のとき} \\ \dfrac{q^2-1}{4q} & ; q \text{ が奇数のとき} \end{cases}$$

(証明) $GF(q)$ の上の符号長 q^m-1 のM系列符号に対し、つぎの性質が知られている**.

---

* M系列符号のリー距離の構造については文献(2)の Theorem 13.52 にも述べられているが、この Theorem は不完全であり、$q = p$ (素数) のM系列符号にしか適用できない。

** 文献(61)参照。またM系列符号は第5章の $\gamma\beta$ - 平面符号の特殊な場合となっているので、(a)は系5.7.1、(b)は補題5.6からただちに導ける。

(a) M系列符号の0でない符号語（M至列）には，その成分として，0が$q^{m-1}-1$個，その他の元がおのおのq^{m-1}個含まれる。

(b) M系列符号の0でない任意の二つの符号語を$\mathcal{X}=(x_0, \cdots, x_{q^m-2})$，$\mathcal{Y}=(y_0, \cdots, y_{q^m-2})$とするとき，$\mathcal{Y}=a\mathcal{X}$となる$a$（$\in GF(q)$）が存在しなければ，集合$\{(x_i, y_i) \mid i=0, \cdots, q^m-2\}$には$(0,0)$となる組合せは$q^{m-2}-1$回，それ以外のGF(q)の元のあらゆる組合せは$q^{m-2}$回づつ現れる。

ここで，
$$\sum_{y \in GF(q)} d_L(w(x), w(y)) = q\bar{d} \quad (\forall x \in GF(q))$$
となることに注意すれば，定理の前半は(a)からただちに導ける．また定理の後半は$\mathcal{Y}=a\mathcal{X}$（$a \in GF(q)$）となる場合は(a)から，それ以外の場合は(b)から明らかである。

（証明終）

このようにGF(q)の上のM系列においては，一般にリー距離の構造は対称ではない。しかし，任意のa（$\in GF(q)$）に対し
$$\sum_{x \in GF(q)} d_L(w(x), w(ax)) = q\bar{d} \qquad (2.86)$$

となるような写像 ω が存在するときは，リー距離に関して等距離符号（任意の二つの異なる符号語間の距離がすべて等しい符号）となり，Plotkin の上界* に達するという意味で最適な符号である．特に $q=p$（素数）の場合は ω は恒等写像を考えればよいから，

$$\sum_{x\in GF(q)} d_L(\omega(x),\omega(ax)) = \sum_{x\in GF(q)} d_L(x,ax) = \sum_{x\in GF(q)} W_L((1-a)x)$$
$$= q\bar{a}$$

となり，式(2.86)が成立する．

これ以外の場合にも，たとえば $q=4$ の場合，GF(4) の元 $0, 1, \alpha, \alpha^2$（α：1の3次根）に，それぞれ $Z(4)$ の元 0, 1, 2, −1 を ω により対応させれば，容易に式(2.86)の成立することが確かめられる．しかし，一般に式(2.86)の成立するような ω が存在するかどうかは分っていない．

2.6.4.2 αs−符号

低伝送速度の符号として，M系列符号のほかに一次 Reed-

---

* 加群 $S(q)$ の上の符号長 n，符号語数 M の符号の最小距離 d_{min} は

$$d_{min} \leq \frac{n\bar{a}}{1-M^{-1}}$$

を満たす(2)．ここに $\bar{a}=\sum_{x\in S(q)} a(x,0)/q$ である．

Muller 符号[5]がよく知られている。これはパリティ検査多項式を $(x-1)h_\alpha(x)$ とする符号長 q^m-1，情報シンボル数 $m+1$ の巡回符号.（一次の修正 Reed-Muller 符号*）に全パリティ検査シンボルをつけ加えたものである．しかし，この符号はすべての成分が等しくなるような符号語を含んでいるから，最小リー距離は高々 q^m となり，q が大きい場合，リー距離誤り訂正符号としては能率のよいものではない。そこで，ここでは一次の修正 Reed-Muller 符号を一般化し，つぎのような符号を考えよう。

定義（$\alpha\xi$-符号）：α を $GF(q^m)$ $(m\geq 2)$ の原始元とし，$h_\alpha(x)$ を $GF(q)$ の上の α の最小多項式とする。また ξ $(\neq 0)$ を $GF(q)$ の元とする。このとき，パリティ検査多項式を $(x-\xi)h_\alpha(x)$ とする $GF(q)$ の上の符号長 q^m-1，情報シンボル数 $m+1$ の符号を $\alpha\xi$-符号と呼ぶ．

$\xi=1$ とすれば，$\alpha\xi$-符号は一次の修正 Reed-Muller 符号となる。$\xi\neq 1$ であれば，$\alpha\xi$-符号にはすべての成分が

---

* これに対し，M系列符号は一次の短縮化 Reed-Muller 符号とも呼ばれる．

等しくなるような符号語は含まれないから，その最小り－距離は一次の修正 Reed-Muller 符号より大きくなる可能性がある．しかし，現在のところ，αs－符号の最小り－距離を数式的に求めることはできない．そこで，ここでは GF(p)（p：素数）の上のαs－符号について，種々の p と m に対し，最大の最小り－距離をもつαs－符号を計算機で求めた結果を示すに止める．表2.1にこのようなαs－符号の s と最小り－距離 $d_{L\min \alpha s}$ を示す．表中の $d_{L\min U}$ は Plotkin の上界であり，

$$d_{L\min U} = \frac{(p^2-1)(p^m-1)}{4p(1-p^{-m-1})}$$

で与えられる．

なお付録Ⅱの表 A2.2 に $5 \leq p \leq 19$　$p^m - 1 < 20000$ となるすべてのαs－符号について最小り－距離が示してある．

さて，GF(p) の上のαs－符号の最小り－距離の計算はつぎのように考えれば，ある程度簡単化できる．

明らかに GF(p) の上のαs－符号 $C_{\alpha s}$ の最小り－距離 $d_{L\min \alpha s}$ は $C_{\alpha s}$ の最小り－重みに一致する．ここで，$h_\alpha(x)$

表 2.1　最小リー距離が最大となるαξ-符号

n：符号長 $(=p^m-1)$，M：符号語数 $(=p^{m+1})$，$\beta=\alpha^{\frac{p^m-1}{p-1}}$

$d_{L\min\alpha\xi}$：最小リー距離，$d_{L\min U}$：Plotkin の上界

p	m	2	3	4	5	6
5	n	24	124	624	3124	15624
	M	125	625	3125	15625	78125
	ξ	β, β^3	β	β, β^3	β	β, β^3
	$d_{L\min\alpha\xi}$	26	136	736	3666	18686
	$d_{L\min U}$	29	149	749	3749	18949
7	n	48	342	2400	16806	
	M	343	2401	16807	117649	
	ξ	β, β^4	β^4	β^5	β^4	
	$d_{L\min\alpha\xi}$	75	572	4079	28663	
	$d_{L\min U}$	80	586	4114	28810	
11	n	120	1330	14640		
	M	1331	14641	161051		
	ξ	β^9	$\beta^2, \beta^4, \beta^6, \beta^8$	β, β^6		
	$d_{L\min\alpha\xi}$	306	3539	39696		
	$d_{L\min U}$	327	3627	39927		
13	n	168	2196			
	M	2197	28561			
	ξ	β^5, β^{11}	β^7			
	$d_{L\min\alpha\xi}$	515	6970			
	$d_{L\min U}$	543	7095			
17	n	288	4912			
	M	4913	83521			
	ξ	$\beta^5, \beta^7, \beta^{13}, \beta^{15}$	β^9			
	$d_{L\min\alpha\xi}$	1168	20458			
	$d_{L\min U}$	1220	20804			
19	n	360	6858			
	M	6859	130321			
	ξ	β^{17}	β^{14}			
	$d_{L\min\alpha\xi}$	1641	32219			
	$d_{L\min U}$	1705	32485			

をパリティ検査多項式とするM系列符号を C_α，ゼーをパリティ検査多項式とするGF(P)の上の符号長 $n(=p^m-1)$ の符号を C_ξ で表わそう。C_ξ の生成行列は

$$G_\xi = [\xi^0\ \xi^1 \cdots \xi^{n-1}]$$

である。すなわち，$\xi=(\xi^0, \xi^1, \cdots, \xi^{n-1})$ とおけば，C_ξ は $C_\xi = \{a\xi \mid a \in GF(P)\}$ と表わせる。

$C_{\alpha\xi}$ は C_α と C_ξ の直和（C_α と C_ξ を含む最小の線形部分空間）であるから，$C_{\alpha\xi} = \{a\xi + \chi \mid a \in GF(P),\ \chi \in C_\alpha\}$ と書ける。さらに S を巡回置換を与える作用素，χ_0 を C_α の0でない符号語とすれば，

$$C_{\alpha\xi} = \{S^i(a\xi + \chi_0) \mid i=0,1,\cdots,n-1,\ a=1,2,\cdots,p-1\} \cup C_\xi \cup C_\alpha$$

となることは容易に確かめられる。ここで，C_α が最適な符号であることを考慮すれば，$C_{\alpha\xi}$ の最小リー距離 $d_{L\min\alpha\xi}$ は C_ξ の最小リー距離 $d_{L\min\xi}$ と，集合 $B=\{a\xi+\chi_0 \mid a=1,2,\cdots,p-1\}$ の最小リー重み $W_{L\min B}$ の最小値 $\min[d_{L\min\xi}, W_{L\min B}]$ で与えられることが分る。

なお，ξ を $\beta=\alpha^{\frac{p^m-1}{p-1}}$（GF(P)の原始元）のべきによって

定義しておけば，αをー符号の最小リー距離が GF(p^m) の原始元 α の選び方によらないことはいうまでもない。

表2.1からαをー符号の中にはリー距離誤り訂正符号としてかなり能率のよいものがあることが分る。しかし，本項のはじめにも述べたように，低伝送速度の符号は所詮，本章で論じている通信方式に応用することは不利であり，αをー符号についても，最小リー距離よりも，付録IIで述べる最大の相互相関係数が問題となる。

2.7 二値符号の変換による多相位相変調通信方式の構成

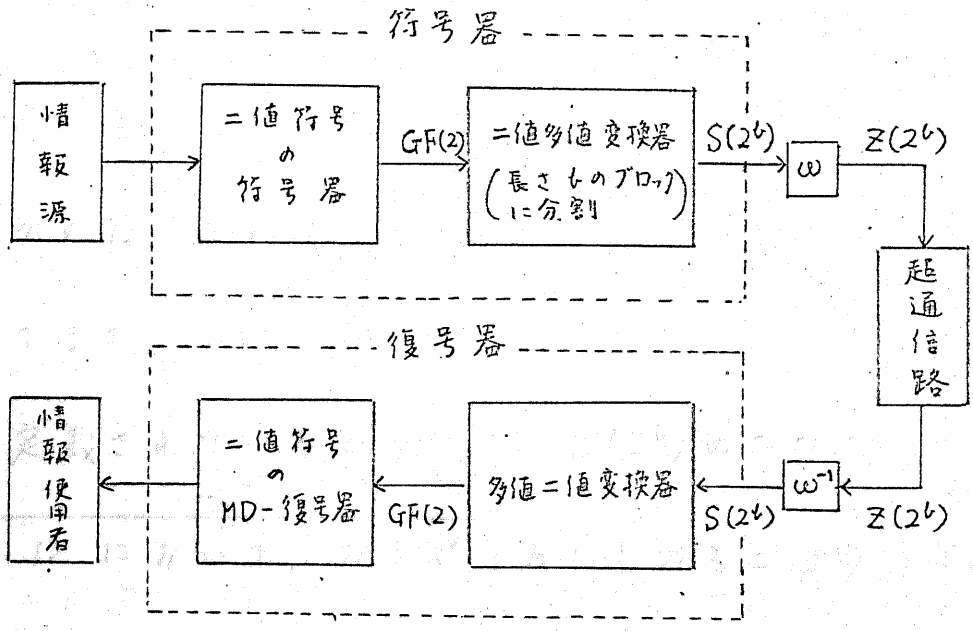
2.5でハミング距離に比べ，リー距離が多相位相変復調を行う超通信路に対し，はるかに適していることを知った。しかし，リー距離に対して能率よく構成できる符号は2.6で述べたように，現在のところごく限られたものしかない。そこで，ここでは二値符号を多値符号に変換することにより，簡単に構成され，しかもハミング距離を用いる場合よりもすぐれた特性を示す通信方式について述べる。

なお，本節で述べる通信方式は，筆者とは独立に岩垂によってほぼ同時に研究され発表された[24][25][40]．しかし，岩垂の研究がより実用的な立場に立っているのに対し，筆者の研究はより理論的な面に重点を置き，一般的に論じている．

2.7.1 通信系の構成

図2.2の通信系において，符号器を二値符号の符号器と二値符号から多値符号への変換器によって構成し，復号器を多値符号から二値符号への変換器および二値符号のMD-復号器によって構成した図2.12の通信系を考える．

図2.12 二値多値変換を用いる通信系



情報源からの情報はまず，二値符号に符号化される．ついで，符号化された系列を長さ ℓ ディジットのブロックに分割する。この各ブロックを $S(2^\ell)$ の元と考えることにする。ここに，$S(2^\ell)$ は長さ ℓ の $GF(2)$ の上のベクトルすべての集合，すなわち $GF(2)$ の直積集合 $GF(2)^n$ である．つぎに，$S(2^\ell)$ から 2^ℓ を法とする整数の剰余環 $Z(2^\ell)$ の上への1対1の写像 ω によって，$S(2^\ell)$ の元を $Z(2^\ell)$ の元へ写像し，超通信路に送出する*．受信側では超通信路の出力を ω^{-1} および多値二値変換器で二値系列に変換し，二値符号の復号器によって MD-復号を行う．

ここで，二値符号の符号長 N は ℓ の倍数であるとし，二値符号の符号語は $n = N/\ell$ のブロックに分割されるとしよう．この場合には図2.12の符号器は，情報を $S(2^\ell)$ の上の長さ n の符号に符号化するものと考えることができる。したがってまた，二値符号に対しハミング距離および重み d_H, W_H が定義されているとすれば，$S(2^\ell)$ の上の符号に対し，

---

* 図2.12 において，ω まで含めたものを二値多値変換器とするのが実際に則しているが，符号の構造から言えば，ω を分けて考える方が自然である。

$S(2^b)$ の任意の二つの元 $x=(x_1, x_2, \cdots, x_b)$, $y=(y_1, y_2, \cdots y_b)$:
$(x_i, y_i \in GF(2) ; i=1, \cdots, b)$ の間の

$$d_T(x, y) = \sum_{i=1}^{b} d_H(x_i, y_i)$$

となる距離および重み

$$W_T(x) = \sum_{i=1}^{b} W_H(x_i)$$

が定義されていて，復号器においては，このような距離によりMD－復号を行うと考えることができる。いうまでもなく，二値符号の最小距離が d_{min} であれば，$S(2^b)$ の上の符号の最小距離も d_{min} である。

このように，$S(2^b)$ の上の符号の距離構造は本質的に二値符号のそれと異ならないが，写像 ω との関連において，一般に 2.4.1 の（仮定2）が満たされず，"正しく復号できない確率" 等の厳密な解析はきわめて難かしい。

2.7.2 準最適な写像

$S(2^b)$ の上の符号および超通信路の遷移確率 $P[j|i]$ が与えられたとき，"正しく復号できない確率" を最小とするような写像 ω を求める問題は興味深いが，厳密に解くことは

きわめて困難であると思われる．そこで，ここでは

$$\bar{D} = \sum_{j=0}^{2^{\nu}-1} P[j|0]\, D_j \qquad (2.87)$$

$$D_j = \frac{1}{2^{\nu}} \sum_{k=0}^{2^{\nu}-1} d_T(\omega^{-1}(k), \omega^{-1}(k+j)) \qquad (2.88)$$

となる $\bar{D}$ を最小とする問題を考えることにする．すなわち，$S(2^{\nu})$ の上の符号において，$S(2^{\nu})$ の各元が等確率で現われるとき，誤り語 $e = (e_0, e_1, \cdots, e_{n-1})$ $(e_i \in S(q))$ の重み $W_T[e] \left(= \sum_{i=0}^{n-1} W_T(e_i)\right)$ の平均値が最小となるような写像 ω を求める。このような ω を準最適な写像（または変換）と呼ぶことにしよう。

ここでは，さらに，超通信路において，$j+1$ 相以上誤る確率が j 相誤る確率よりも十分小さく，

$$P_j(\rho R) > 2^{\nu} \{P_{j+1}(\rho R) + P_{j+2}(\rho R) + \cdots + P_{2^{\nu}-1}(\rho R)\}$$

$$j = 0, 1, \cdots, 2^{\nu-1}-1 \qquad (2.89)$$

が満たされると仮定しておこう．ここに $P_j(\rho R)$ は式 (2.19) で定義されているものである．この仮定は ρR $(= E_b/N_0)$ が十分大きい場合には妥当であろう（図 2.4 参照）．

ここで，$D_0 = 0$，$D_j = D_{-j}$，$P[j|0] = P[-j|0]$ となることに注意すれば，この仮定により，ω の最適化は，は

じめに D_1 を最小とする ω の集合を求め，つぎにその集合において D_2 を最小とする部分集合を求めるという手順で順次行えることが分る．

いま，$\omega^{-1}(i) = \chi_i$ ($i \in Z(2^\nu)$, $\chi_i \in S(2^\nu)$) とおけば，式(2.88) は

$$D_j = \frac{1}{2^\nu} \sum_{k=0}^{2^\nu-1} d_T(\chi_k, \chi_{k+j}) \qquad (j=0,1,\cdots,\nu)$$

となる。ただし，χ の添字は，法を 2^ν として定めるものとする。それゆえ，最適な ω を求める問題は順序づけられた $S(2^\nu)$ の元の集合 $S_{ordn}(2^\nu) = \{\chi_0, \chi_1, \cdots, \chi_{2^\nu-1}\}$ の距離構造に関する問題となる．

明らかに $D_1 \geq 1$ であり，$D_1 = 1$ となるのは $S_{ordn}(2^\nu)$ が単一距離符号 * となる場合に限る。このとき $D_2 = 2$ となることはいうまでもない。D_3 以下を順次最小としていくために，単一距離符号のつぎのような表現法[37]を用いよう．

$\chi_i = (\chi_1^{(i)}, \chi_2^{(i)}, \cdots, \chi_\nu^{(i)})$ と $\chi_{i+1} = (\chi_1^{(i+1)}, \cdots, \chi_\nu^{(i+1)})$ の異なる成分の番号を a_i とする．すなわち，χ_i と χ_{i+1} は $\chi_{a_i}^{(i)}$ と $\chi_{a_i}^{(i+1)}$ のみが異なる．このような a_i を用いれば単一距離符号は

---

* $d_T(\chi_i, \chi_{i+1}) = 1$ $(i=0,1,\cdots,2^\nu-1)$ となる符号[37][39]．

$(a_0 a_1 \cdots a_{2^k-1})$ $(1 \leq a_i \leq k)$ となる系列によって表現できる. 単一距離符号のこのような表現に対し, つぎの補題が導ける.

補題2.12[33]: k 以下の正整数からなる長さ 2^k の系列 $(a_0 a_1 \cdots a_{2^k-1})$ が単一距離符号の表現であるための必要十分条件は, つぎの(1)(2)が成立することである.

(1) この系列に含まれる成分において, $1, 2, \cdots, k$ のおのおのに等しいものの数がすべて正の偶数となる.

(2) この系列に含まれる長さが偶数の任意の真の部分系列(長さが 2^k より短かい部分系列, 巡回的部分系列 $a_j a_{j+1} \cdots a_{2^k-1} a_0 a_1 \cdots a_k$ も含む)に含まれる成分において, $1, 2, \cdots, k$ のおのおのに等しいものの数がすべて偶数(0も含む)となる.

(証明) 部分系列 $a_i \cdots a_{i+j-1}$ に含まれる成分において, $1, 2, \cdots, k$ のおのおのに等しいものの数がすべて偶数であれば, またそのときに限り, $\chi_i = \chi_{i+j}$ となることから明らかである. (証明終)

さて, $(a_0 a_1 \cdots a_{2^k-1})$ で表現された単一距離符号に対し, $W_T(\chi_i + \chi_{i+j})$ は部分系列 $a_i \cdots a_{i+j-1}$ (a の添字は法を 2^k

として定める）に j 数個含まれる元の数であるから，これを $O_i^{(j)}$ とおくと，D_j はつぎのように書ける．

$$D_j = \frac{1}{2^b} \sum_{i=0}^{2^b-1} O_i^{(j)}$$

ここで，D_3 を最小とする単一距離符号について考えよう．このため単一距離符号の表現系列から，$O_0^{(3)}\ O_1^{(3)} \cdots O_{2^b-1}^{(3)}$ となる系列を作る．明らかに，この系列の成分は 1 または 3 である．しかも，$b \geq 2$ であれば，この系列に 11 となる部分系列（巡回的なものも含める）が含まれることはない．実際，もし含まれるとすれば，元の単一距離符号の表現系列 $(a_0 a_1 \cdots a_{2^b-1})$ に $cdcd$ $(1 \leq c, d \leq b)$ となる部分系列が含まれ，補題 2.12 と矛盾する．したがって D_3 を最小とする $O_i^{(3)}$ の系列は 1 3 1 3 1 3 … 1 3 となる系列，またはその巡回置換である．このような $O_i^{(3)}$ の系列を与える単一距離符号の表現系列 $(a_0 a_1 \cdots a_{2^b-1})$ には一つおきに同じ値をとる成分が現われねばならない．すなわち，

$$(a^{(0)} a_0^{(1)} a^{(0)} a_1^{(1)} a^{(0)} a_2^{(1)} \cdots a^{(0)} a_{2^b-1}^{(1)}) \quad a_i^{(1)} \neq a^{(0)}$$

または，この巡回置換でなければならない．ここで，

$$(a_0^{(1)} a_1^{(1)} \cdots a_{2^b-1}^{(1)}) \qquad (2.90)$$

となる系列を考えると，補題2.12から，これは再び符号語数2^{b-1}の単一距離符号の表現系列でなければならないことが分る。このため，$D_4 \sim D_8$は定まってしまう。D_9を最小とするためには，式(2.90)の系列に対し，D_3の場合とほとんど同様に考えて，この系列が

$$(a^{(1)}a_0^{(2)}a^{(1)}a_1^{(2)}\cdots a^{(1)}a_{2^{b-1}}^{(2)}) \qquad a_i^{(2)} \neq a^{(1)}$$

となる形，またはその巡回置換でなければならないことが分る。また，$(a_0^{(2)}\ a_1^{(2)}\cdots a_{2^{b-1}}^{(2)})$は単一距離符号の表現系列となる必要があり，$D_{10} \sim D_{16}$は定まってしまう。以下同様にして$D_8$の最小化を行えることは明らかであろう。

このようにして得られる表現系列は一つおきに同じ値をとる成分が現れ，そのような成分を除いた系列においてもまた同じ構造が現われるような系列となる。すなわち，

$$(a^{(0)}a^{(1)}a^{(0)}a^{(2)}a^{(0)}a^{(1)}a^{(0)}a^{(3)}a^{(0)}a^{(1)}a^{(0)}a^{(2)}a^{(0)}\cdots\cdots) \quad (2.91)$$

となるような系列（あるいはその巡回置換）である。この系列が表現している単一距離符号は通常のGray符号[29][37]にほかならない。したがって，

定理2.13：超通信路の遷移確率が式(2.89)を満たすとき，

準最適な写像 ω は $\{\omega^{-1}(0), \omega^{-1}(1), \cdots, \omega^{-1}(2^b-1)\}$ が Gray 符号となるようなものである。

この定理に示されるような写像 ω を b 次元の Gray 写像または Gray 変換と呼び，ω_G で表わすこととする。また，$Z(2^b)$ の上で，

$$d_G(i, j) = d_T(\omega_G^{-1}(i), \omega_G^{-1}(j)) \quad (i, j \in Z(2^b)) \quad (2.92)$$

により定義される距離を Gray 距離と呼ぶことにする。

ここで，式(2.91)の系列を丁度半分に切った二つの系列において，その右端の成分 $a^{(b-1)}$ を $a^{(b-2)}$ でおきかえるとき，これらの二つの系列がともに $b-1$ 次元の Gray 符号を表現していることに注意すれば，b 次元の Gray 変換に対する Gray 距離は $b-1$ 次元の Gray 変換に対する Gray 距離から容易に求まることが分る。

$b=2 \sim 4$ のときの Gray 距離を表 2.2 に示す。この表にみるように，$b=2$ のときは Gray 距離はリー距離と一致する。

表 2.2　Gray 距離 $d_G(k, k+j)$

$b=2$

j \ k	すべての k
0	0
1	1
2	2
3	1

$b=3$

j \ k	$2i$	$2i+1$
0	0	0
1	1	1
2	2	2
3	1	3
4	2	2
5	3	1
6	2	2
7	1	1

$b=4$

j \ k	$4i$	$4i+1$	$4i+2$	$4i+3$
0	0	0	0	0
1	1	1	1	1
2	2	2	2	2
3	1	3	1	3
4	2	2	2	2
5	3	1	3	3
6	2	2	4	4
7	1	3	3	3
8	2	2	2	2
9	3	3	3	1
10	4	4	2	2
11	3	3	1	3
12	2	2	2	2
13	3	1	3	1
14	2	2	2	2
15	1	1	1	1

2.7.3　Gray 変換を用いる場合の信頼度函数

ここで，図 2.12 の通信系において，写像 ω に Gray 変換 ω_G を用いた場合の信頼度函数について考えてみよう。

$S(2^n)$ の上に対して定義された距離 $d_T(x, y)$ は 2.4.1 の（仮定 1）は満たすが，写像として ω_G を用いた場合（仮定 2）は一般には満たさない．実際，（仮定 2）を式 (2.92) で定義される Gray 距離で書き直せば，任意の i, j, k $(\in$

$Z(2^b)$ に対し，

$$d_G(i, i+k) = d_G(j, j+k)$$

または $\begin{cases} d_G(i, i+k) = d_G(j, j-k) \\ d_G(i, i-k) = d_G(j, j+k) \end{cases}$

が成立するということになり，表2.2から分るように，$b=2, 3$ の場合しか満たされない。すなわち，$b \geq 4$ の場合，誤り語 e の重み $W_T[e]$ の確率分布は送信語によって異なる。それゆえ，$b \geq 4$ のとき，2.4 の方法で信頼度函数の上，下界を求めることはできない。そこで，ここでは $W_T[e]$ の分布を平均的分布で置き換え，送信語にはよらないとして，信頼度函数の近似的下界を求めることとする。

すなわち，Gray 距離 $d_G(k, k+j)$ において，

$$d_G(k, k+j) = l \quad (0 \leq l \leq b)$$

となるすべての (k, j) の集合を $K \times J(l)$ とし，

$$P_l' = \frac{1}{2^b} \sum_{(k,j) \in K \times J(l)} P[k+j \mid k] = \frac{1}{2^b} \sum_{(k,j) \in K \times J(l)} P[j \mid 0] \tag{2.93}$$

を計算する。この P_l' を用い，式(2.45)の $g(\sigma)$ を

$$g(\sigma) = \ln \sum_{l=0}^{b} e^{\sigma l} P_l'$$

とおき，定理2.6により $E_L(R;P)$ を求める．

このような近似は，$S(2^\nu)$ の上の符号の符号語の各成分に $S(2^\nu)$ の元が等確率で現われるとし，式(2.92)のGray距離を，

$$\overline{d_G}(k,k+j)=\left\{\sum_{i=0}^{2^\nu-1} d_G(i,i+j)+d_G(i,i-j)\right\}/2^{\nu+1}$$

となる j $(\in Z(2^\nu))$ のみによる平均的距離で置き換えたことを意味する．ところで，表2.2にみるように，

$$d_G'(k,k+j)=\{d_G(k,k+j)+d_G(k,k-j)\}/2$$

は k について，余り異ならない．したがって $\overline{d_G}(k,k+j)$ は $d_G'(k,k+j)$ の（特に j の小さいところで）かなりよい近似となっている．一方，超通信路の遷移確率は $P[j|0]=P[-j|0]$ を満たすから，$d_G(k,k+j)$ のかわりに $d_G'(k,k+j)$ を用いても，P_{NDC} は正しい値が得られ，したがって信頼度函数も正しく評価できる．それゆえ，上記の近似はかなりよい近似であると思われる．

なお，$\nu=2$ の場合の信頼度函数が $Z(4)$ の上のL一距離誤り訂正符号のそれと一致することはいうまでもない．

図2.10，2.11に上記のようにして計算された信頼度函数の

下界および $E_L(R;P)$ が正となる伝送速度 R の限界 $R_{tL}(P)$ をハミング距離，リー距離を用いた場合と比較して示す。

これらの図にみるように，二値符号に Gray 変換を用いる通信方式はハミング距離を用いる方式と，リー距離を用いる方式の中間に位置するものである。しかし，リー距離誤り訂正符号としては，現在のところ，最小距離等に厳しい制約の課されたものしか知られていないのに対し，二値誤り訂正符号は十分一般的なものが存在するから，本節の方式は現在のところ，実用上もっとも重要なものであろう。

2.7.4 二値誤り訂正符号の符号長の修正

これまで，二値誤り訂正符号の符号長 N はブロックの長さ q で割り切れるとした。図 2.12 の通信系を構成する場合に，この条件は必しも必要ではないが，N が q で割り切れない場合には通信路における一つの誤りが二つの受信語に影響を及ぼす場合があり，"正しく復号できない確率" を増大させることがある。しかも通信系の構成がやや複雑となり，解析も著しく難かしくなるから，N は q で割り切れることが

望ましい。したがって，二値符号の本来の符号長を短縮または伸長することが必要となる場合が生ずる。二値符号が組織符号である場合，符号長を短縮する方法はよく知られている[1]が，符号長を能率よく伸ばす方法はこれまで知られていなかった。このような方法については次章で述べる。

2.8 $(0, 1, \infty)$ 距離誤り訂正符号

2.8.1 $(0, 1, \infty)$ 距離

リー距離は多相位相変調に対し，かなり有効な距離ではあるが，$\rho (= E_B/N_0)$ が十分大きいところでは，なお無駄があると思われる。このような場合には，2.3でみたように，超通路において2相以上誤まって検出される確率は1相だけ誤まって検出される確率に比べ非常に小さい。そこで，$\Sigma(\beta)$ の上の符号長 n の符号を考え，この符号長内で2レベル以上の誤りが生じる確率が，1レベルの誤りが $t+1$ 個以上生じる確率に比べても小さいとすれば，1レベルの誤りだけを t 個まで訂正できる符号で，リー重みあるいはハミング重みが t 以下の誤りを訂正する符号とほとんど同一の復号誤り率を

得ることができる。しかも，この場合には訂正すべき誤りのパターンの数が少ないから，より伝送速度の高い符号を構成できるであろう。

このような符号は $Z(q)$ の上で定義されたつぎのような距離を用いていることとなる。

$$d_\infty(x,y)=\begin{cases}0 & ; x=y\\ 1 & ; x=y+1 \text{ および } x=y-1\\ \infty & ; \text{その他の場合}\end{cases}$$

$$(x, y \in Z(q)) \qquad (2.94)$$

この距離を $(0, 1, \infty)$ 距離と呼ぶことにする。明らかに，$d_\infty(x,y)$ は $x-y$ のみの函数となる。そこで，

$$W_\infty(x) = d_\infty(x,0) \qquad (x \in Z(q))$$

を $(0, 1, \infty)$ 重みと呼ぼう。

$(0, 1, \infty)$ 距離は距離の公理のうち，三角不等式は満たさず，2.4で述べた擬距離であるが，そこに述べたように，最小距離，MD－復号を定義できる。

いうまでもなく，q 値符号における $(0, 1, \infty)$ 重みが有限な誤りは $\left[\frac{q}{3}\right]$ 値符号を用いれば問題とならない。ただし，

[ ] はガウス記号である。したがって，(0, 1, ∞) 距離を用いた符号はその伝送速度が $\log_2\left[\frac{q}{3}\right] \approx \log_2 q - \log_2 3$ (ビット/シンボル) 以上でなければ意味がない。このように (0, 1, ∞) 距離の応用面はかなり限定されているが，高伝送速度が要求され，かつ $\rho\,(=E_b/N_0)$ を十分大きくとれるような場合には有効となる。

2.8.2 (0, 1, ∞) 距離誤り訂正符号の構成法

本項ではパリティ検査行列のテンソル積による (0, 1, ∞) 距離誤り訂正符号の構成法について述べる。

二つの線形符号を合成して作られる符号としてテンソル積符号が知られている[39]。これはつぎのように定義される。

GF(q) の上の (n_1, n_1-r_1) 線形符号を C_1，$GF(q^{r_1})$ の上の (n_2, n_2-r_2) 符号を C_2 とする。C_1 のパリティ検査行列は GF(q) の上の $r_1 \times n_1$ 行列であるが，各列を $GF(q^{r_1})$ の元とみなし，

$$H_1 = [\, h_1^{(1)} \;\; h_2^{(1)} \cdots h_{n_1}^{(1)} \,] \quad (h_i^{(1)} \in GF(q^{r_1}))$$

となる形で表わす。また，C_2 のパリティ検査行列を

$$H_2 = \begin{bmatrix} h_{11}^{(2)} & h_{12}^{(2)} & \cdots & h_{1n_2}^{(2)} \\ h_{21}^{(2)} & \cdots & \cdots & \vdots \\ \vdots & & & \vdots \\ h_{r_21}^{(2)} & \cdots & \cdots & h_{r_2n_2}^{(2)} \end{bmatrix} \quad (h_{ij}^{(2)} \in GF(q^{r_1}))$$

とする。このとき，H_2 と H_1 のテンソル積（クロネッカー積）

$$H = H_2 \otimes H_1 = \begin{bmatrix} h_{11}^{(2)} H_1 & h_{12}^{(2)} H_1 & \cdots & h_{1n_2}^{(2)} H_1 \\ h_{21}^{(2)} H_1 & \cdots & \cdots & \vdots \\ \vdots & & & \vdots \\ h_{r_21} H_1 & \cdots & \cdots & h_{r_2n_2}^{(2)} H_1 \end{bmatrix} \quad (2.95)$$

の各成分を $GF(q)$ の上の r_1 次元（縦）ベクトルとして表わした $GF(q)$ の上の $r_1r_2 \times n_1n_2$ 行列をパリティ検査行列とする $GF(q)$ の上の符号を C_1 と C_2 のテンソル積符号と呼ぶ。明らかに，テンソル積符号の符号長は n_1n_2，検査シンボル数は r_1r_2 である。

ここで，つぎの定理を導いておこう。

定理2.14：$(0, 1, \infty)$ 重みが t_1 以下の誤りを訂正できる $GF(p)$（p：素数）の上の (n_1, n_1-r_1) 符号を C_1，ハミング重みが t_2 以下の誤りを訂正できる $GF(p^{r_1})$ の上の (n_2, n_2-r_2) 符号を C_2 とする。このとき，C_1 と C_2 のテンソル積符号は，$t_1 \neq n_1$ なら $(0, 1, \infty)$ 重みが $\min(t_1, t_2)$ 以下の誤り

を訂正でき，$t_1 = n_1$ なら $(0, 1, \infty)$ 重みが t_2 以下の誤りを訂正できる．

(証明) $t_1 \neq n_1$ のときを考える。誤り語を $e = (e_1, e_2, \cdots, e_{n_2})$ としよう。ただし，$e_i = (e_{i1}, e_{i2}, \cdots, e_{im_1})$ $(e_{ij} \in GF(p))$ であり，$W_\infty[e] \leq \min(t_1, t_2)$ とする．また，テンソル積符号のパリティ検査行列（式（2.95））に対するシンドローム を $(\lambda_1, \lambda_2, \cdots, \lambda_{r_2})$ とする。ただし，λ_i は式 (2.95) の H の第 i 行に対応するもので，$GF(p^{r_1})$ の元とする．明らかに

$$\lambda_i = \sum_{j=1}^{n_2} h_{ij}^{(2)} H_1 e_j^t \quad (i = 1, \cdots, r_2)$$

ただし，e_j^t は e_j の転置ベクトルを示す。仮定から，$H_1 \cdot e_j^t$ $(j = 1, \cdots, n_2)$ のうちで 0 でないものは高々 t_2 個である．ゆえに，λ_i $(i = 1, \cdots, r_2)$ に対し，C_2 の復号法を用いることにより，$H_1 e_j^t$ を定め得る．再び，仮定により，$W_\infty[e_j] \leq t_1$ であるから，$H_1 e_j^t$ から e_j を定め得る．

$t_1 = n_1$ のときも全く同様に証明できる　　(証明終)

ここで，$p \geq 11$ とし，$p > 3^i$ を満たす最大の正整数 i を n_1 とする．このとき，パリティ検査行列

$$H_1 = [1 \ 3 \ 3^2 \cdots 3^{n_1-1}] \qquad (2.96)$$

により定義される GF(P) の上の (n_1, n_1-1) 符号を考えよう。誤り語を $e = (e_0, e_1, \cdots, e_{n_1-1})$ $(e_i \in GF(P))$ とすると、H_1 に対するシンドロームは

$$\rho = \sum_{i=0}^{n_1-1} e_i 3^i$$

となる。$P > 3^{n_1}$ であるから、$-1 \leq e_i \leq 1$ であれば、ρ は e に対して一意に定まる。すなわち、C_1 は $(0, 1, \infty)$ 重みが n_1 以下の誤りをすべて訂正できる。また、実際に ρ から e を求めること（C_1 の復号）もきわめて容易である。

つぎに、ハミング重みが t_2 以下の誤りを訂正できる GF(P) の上の (n_2, n_2-r_2) 符号を C_2 とすれば C_1 と C_2 のテンソル積符号は定理 2.14 により $(0, 1, \infty)$ 重み t_2 以下の誤りを訂正できる。また、この符号の符号長は $n_1 n_2$、検査シンボル数は r_2 であるから、伝送速度 R は

$$R = \left(\frac{n_1 n_2 - r_2}{n_1 n_2}\right) \log_2 P = \log_2 P - \frac{r_2}{n_1 [\log_3 P]} \log_2 P$$

となる。これから；ただちに、$R > \log_2 \left[\frac{P}{3}\right]$ となることが確かめられる。すなわち、この符号は意味をもつ符号である。

この符号の復号は定理2.14の証明中に述べたようにしてはじめに C_2 の復号を行い、ついで C_1 の復号を行えばよい。C_1 の復号は著しく簡単であるから、この場合の復号の複雑さは C_2 の復号法によって決まる。

ここで、このような符号の応用面について、例によって考えてみよう。いま、通信系に要求される伝送速度 $R = \mathcal{R}/W$（2.3.3参照）が3（ビット/シンボル）、"正しく復号できない確率" P_{NDC} が 10^{-6} であるとする。また、符号器および復号器の複雑さに対する制約から符号長 n は250前後、シンボル数 q は10前後におさえられるとしよう。このとき、これまで述べた符号の中で比較的効率よく適用し得るものに対する所要 $\rho(=E_B/N_0)$ を表2.3に示す。

表2.3　テンソル積符号と他の符号の比較
（$R \approx 3.0$, $P_{NDC} \leq 10^{-6}$, $q \leq 11$, $n \leq 250$）

符号	R	q	n	検査シンボル数	訂正できる誤りの重み	$\rho(=E_B/N_0)$
テンソル積符号	2.98	11	240	33	9 (0, 1, ∞)	15.5
(短縮化) BCH符号	2.96	11	250	33	7 ハミング	18.8
(短縮化) BCH符号	3.00	11	250	36	6 ハミング	20.3
BCH符号	3.00	11	120	16	4 ハミング	21.3
符号化しない場合	3.00	8	1	0	0	27.4

表中のテンソル積符号は，[1, 3] となるパリティ検査行列をもつ GF(11) の上の符号長2の符号 C_1 と GF(11) の上の符号長120，検査シンボル数33，最小（ハミング）距離19のBCH符号 C_2 とのテンソル積符号である．また短縮化BCH符号は本来の符号長が1330となるもので，大巾な短縮化が必要となる．なおBerlekampの符号等では上述の要求を満たすものは作れない．

この表にみるように，この場合にはテンソル積符号がもっともすぐれている．このように，高伝送速度が要求され，符号長等に制約のあるときには，本節で述べた符号が有効となる場合もある．

2.9 各種方式の比較

本節では，これまで述べた各種の方式において，現在用い得るもの（適用できる誤り訂正符号の存在するもの）のうち，かなり一般性をもつと思われるつぎの三種の方式を比較する．

(I) 多値BCH符号をハミング距離誤り訂正符号として用いる方式．

(Ⅱ) Berlekamp の符号をリー距離誤り訂正符号として用いる方式.

(Ⅲ) 二値BCH符号に対しGray変換を用いる方式.

2.9.1 評価基準

評価基準としては2.3.3で述べたように,"正しく復号できない確率" P_{NDC}, 符号の伝送速度 R(ビット/シンボル), 1情報ビット当りの信号エネルギーと雑音の電力スペクトル密度の比 ρ($=E_B/N_0$)および符号長 n, シンボル数 q を用いる.

(Ⅰ), (Ⅱ), (Ⅲ) のいずれも符号化はきわめて容易であり, 復号は Berlekamp のアルゴリズム[2]を用いて行える。それゆえ通信系の構成の複雑さの目安としては一応 $n\log_2 q$ をとることができるであろう。なお, Berlekamp のアルゴリズムの複雑さを支配するものとして, 符号の最小距離も大きな要因となるが, これを評価基準に加えると煩雑となるので, ここでは無視する.

2.9.2 "正しく復号できない確率" P_{NDC} の計算

P_{NDC} の計算は 2.4.1 の（仮定3）をおいて行う．すなわち，最小距離を d_{min} とするとき，重みが $W[e] < d_{min}/2$ となる誤り e が生じたときには完全に正しく復号できるが，それ以外の場合には正しく復号できないとする．それゆえ，P_{NDC} は，$W[e] < d_{min}/2$ となる誤り e の発生する確率を P_{DC} とするとき $P_{NDC} = 1 - P_{DC}$ で与えられる．$W[e]$ の確率分布が送信語によって異ならないときには，P_{DC} は多項分布を計算することにより得られる．

符号長 n，伝送速度 R，最小ハミング距離 d_{Hmin} のハミング距離誤り訂正符号の P_{NDC} は，よく知られているように次式で与えられる．

$$P_{NDC} = 1 - \sum_{i=0}^{t} \binom{n}{i} p^i q^{n-i} \qquad t = \left[\frac{d_{Hmin}-1}{2}\right]$$

$$p = 1 - P_0(\rho R) \qquad q = P_0(\rho R)$$

ここに，$[\ ]$ はガウス記号であり，$P_0(\rho R)$ は式 (2.19) に与えられている．

また，符号長 n，伝送速度 R，最小リー距離 d_{Lmin} のリー距離誤り訂正符号の P_{NDC} は

$$P_L(z) = \left\{ \sum_{j=0}^{L} P_j(\rho R) z^j \right\}^n \qquad L = \left[\frac{\ell}{2}\right]$$

となる z に関する多項式の $\left[\frac{d_{L\min} - 1}{2}\right]$ 次以下の係数の和を P_{DC} とし，$P_{NDC} = 1 - P_{DC}$ により計算できる．ただし $P_j(\rho R)$ は式 (2.19) に与えられている．

Gray 変換を用いる場合は，$\ell \geq 4$ のとき P_{NDC} を厳密に計算することは難かしいので，2.7.3 と同様な近似を用いる．ブロックの長さが ℓ，二値符号の符号長が $N = n\ell$，伝送速度が $R' = R/\ell$ であるとすると，Gray 変換を用いる場合の P_{NDC} は式 (2.93) P_l' を用い，

$$P_G(z) = \left(\sum_{l=0}^{\ell} P_l' z^l \right)^n$$

となる多項式の $\left[\frac{d_{\min} - 1}{2}\right]$ 次以下の項の係数の和を P_{DC} とし，$P_{NDC} = 1 - P_{DC}$ により求める．この近似は 2.7.3 で述べたように，かなりよい近似であると思われる．

2.9.3 符号の構成

BCH 符号および Berlekamp の符号を構成するためには，GF(q) の上の原始多項式を知らねばならない．これは GF(p) (p：素数) の上の原始多項式から求められる．GF(2) の原始

多項式は文献(1)に詳しい表がある。また $p=3\sim47$ の場合の原始多項式は付録Ⅰに示してある。

BCH符号およびBerlekampの符号の(名目上の)、最小距離は容易に求まる。また、情報シンボル数は、(符号長)−(生成多項式の次数)として計算できる。生成多項式の次数は符号長の短い場合には、生成多項式の根として指定されているがα 体の元とその共役元*の数を調べることにより、容易に計算できる。符号長が長い場合の計算法については、文献(2) Chap. 12 を参照されたい。

2.9.4 計算例

図2.13に二値BCH符号の P_{NDC} を R の函数として、$\rho(=E_b/N_0)=5.0$ のときに示す。図2.14には(I)と(Ⅲ)との P_{NDC} を R の函数として比較して示す。図2.15には $P_{NDC}=10^{-5}$ としたときの種々の符号の ρ と W/R の関係を示す。この図においては $n\log_2 q\approx120$ となるように符号長

---

* $\xi\in GF(q^m)$ に対し、ξ^{q^i} $(i=1,2,\cdots)$ となる元を ξ の(GF(q)の上の)共役元と呼ぶ。文献(2)(7)参照。

図2.13　二重BCH符号の P_{NDC} − R特性
$\rho\ (= E_B/N_0) = 5.0$

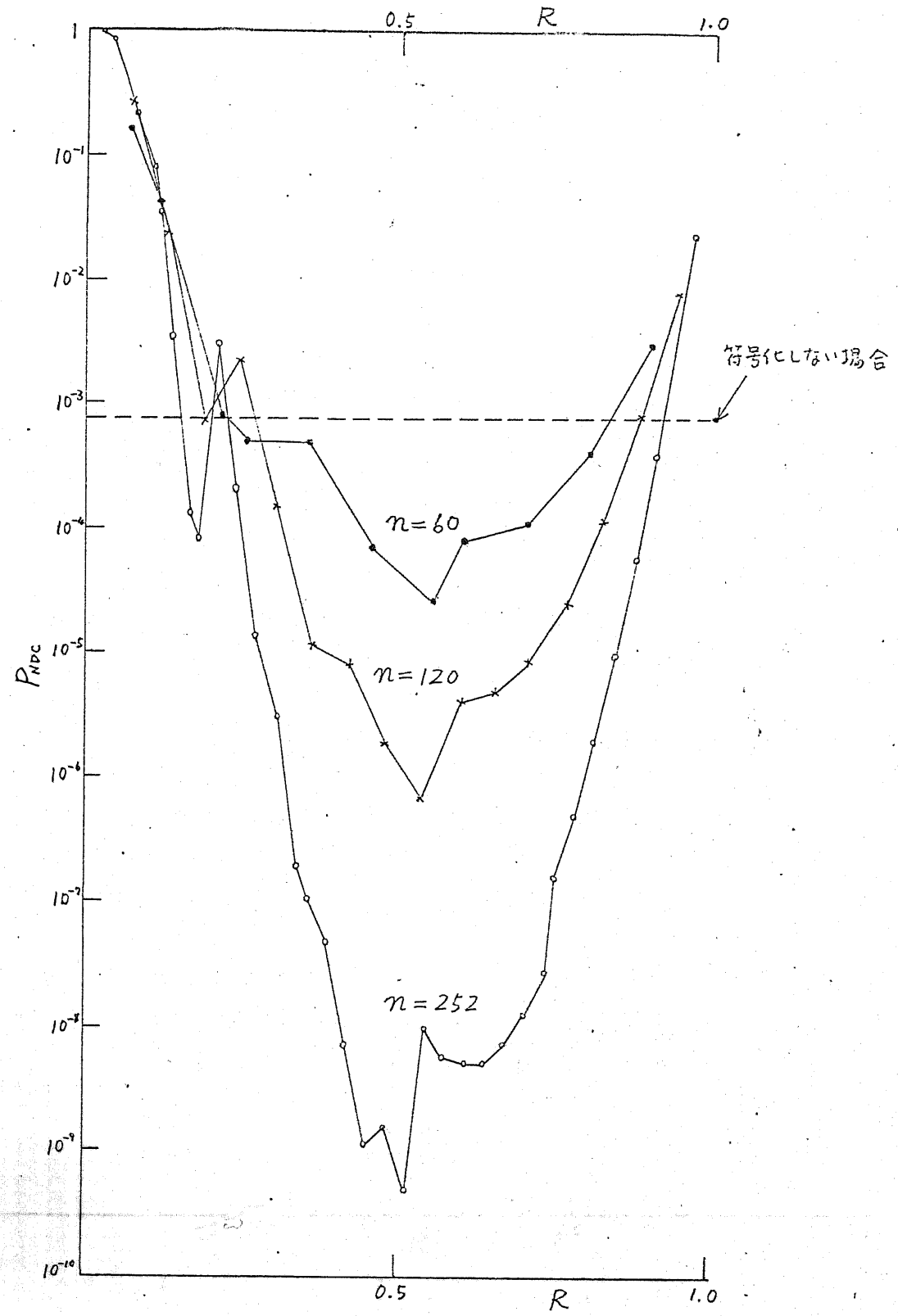


図 2.14　多値 BCH 符号と二値 BCH 符号を Gray 変換した符号の P_{NDC} — R 特性

$q = 8$　　$n = 40$　　$\rho\,(= E_B/N_0) = 10.0$

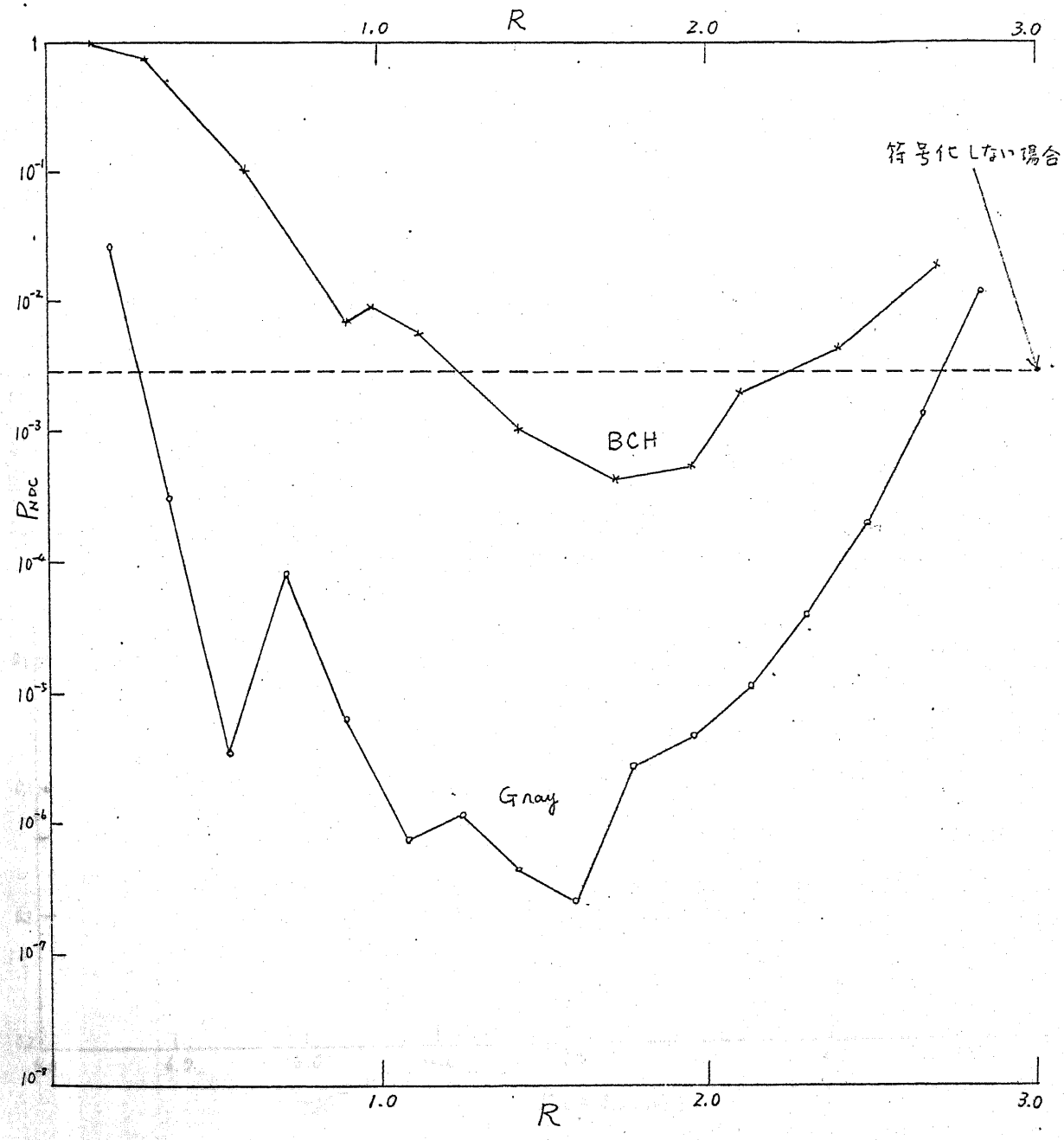
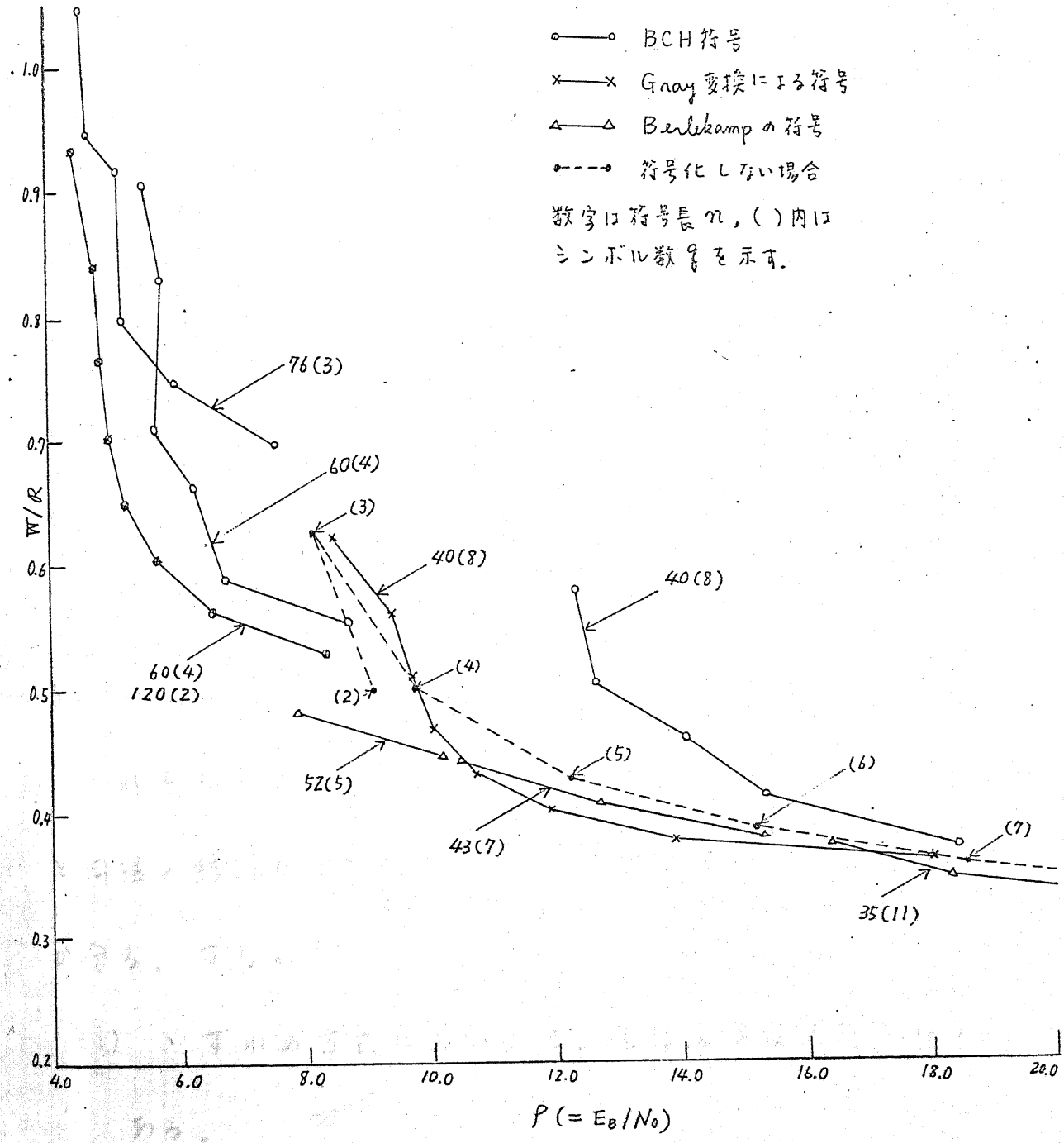


図2.15　各種符号の $\rho - W/R$ 特性
($n \log_2 q \approx 120$)
($P_{NDC} = 10^{-5}$)



を定めてある。このため，多くの符号長を本来のものから短縮して用いる必要がある。この図は P_{NDC} と通信系の複雑さが同一という条件の下で，$P-W/R$ 特性を比較していると考えることができる。W/R は所要帯域巾（Hz）と通信系の情報伝送速度（ビット/秒）との比であり，符号の伝送速度（ビット/シンボル）との関係は式(2.22)に与えられている。この図において，W/R が同程度であれば P の小さいもの，また P が同程度であれば W/R の小さいものがすぐれた符号であるということができる。なお，この図では，同一の符号系において，W/R，P ともにより小さい符号が存在するような符号（特に，低伝送速度の符号）は，大部分除いてある。

これらの図から，信頼度函数の比較によって得られた結論と同様の結論が実際に存在する符号に対しても成立することが分る。すなわち，

(i) いずれの方式においても，低伝送速度の符号は不利である。

(ii) Gray 変換を用いる方式は，ハミング距離誤り訂正符

号を用いる方式よりも，はるかにすぐれた特性を示す。

(iii) Berlekamp の符号（リー距離誤り訂正符号）は，$\log_2 q$ にごく近い伝送速度のものしか存在しないが，その部分ですぐれた特性を示す。

(iv) $W/R > 0.5$ のときには，二値符号を用いれば十分である。

2.10 むすび

本章では，多相位相変調方式に対し，誤り訂正符号を応用する場合の種々の問題点について論じた。

はじめに，誤り訂正符号における距離について，一般的な立場から論じ，最小距離復号を行う場合，距離が非常に重要な問題となることを指摘した。ついで，距離を評価する手段として，信頼度函数を導入し，その上界と下界を導いた。これを用いて，ハミング距離とリー距離を比較し，リー距離が多相位相変調通信方式に対し有効であることを示した。

そこで，リー距離誤り訂正符号の構成法を考えたが，これはかなり限定されたものしか得られなかった。このため，リ

一距離誤り訂正符号に代るものとして，二値符号を Gray 変換して得られる符号を考え，その場合の信頼度函数を評価した。その結果，この符号がハミング距離誤り訂正符号よりはかなりすぐれたものであることを確かめた。

また，多相位相変調通信方式に適したもう一つの距離として，$(0, 1, \infty)$ 距離を考え，この距離に対し構成される符号の例を示し，これがある場合には非常に有効であることを明らかにした。

最後に，現在知られている符号を用いる場合に対し，その特性を計算し比較した。

以上の結果，現在のところ，帯域にある程度余裕のあるような場合，すなわち $W/R > 0.5$ のときには，二値誤り訂正符号がすぐれており，帯域がかなり制限され，$W/R \leq 0.5$ であるような場合には，その構成の簡単さおよび一般性から言っても，また，その特性から言っても二値誤り訂正符号を Gray 変換した符号がすぐれていると考えられる。しかし，$W/R \leq 0.5$ のときには，場合によっては Berlekamp の符号，さらには $(0, 1, \infty)$ 距離によるテンソル積符号が有効なことも

ある．また，いずれの場合にも低伝送速度の符号は著しく不利である．などの結論が得られた。

本章の理論は，誤り訂正符号を実用化する場合の基礎的理論となるものであり，多相位相変調ばかりでなく，他の変調方式に対しても同様な考え方が適用できるであろう。

今後に残された最大の問題はリー距離誤り訂正符号として，より一般的なものを見出すことである。また，最小距離復号を用いる場合の信頼度函数をより正確に評価することも今後の研究に期待される。

第3章

二値誤り訂正符号の新しい修正法

本章では，二値誤り訂正符号（Preparata符号，BCH符号）の符号長を能率よく伸ばす方法について述べる．このような方法は，誤り訂正符号を用いた通信系の，より自由な設計を可能とする．特に，才2章2.7で述べたGray変換を用いる通信方式に対し，有効である．

本章の距離に対する基本的考え方は前章と同様であるが，ここでは，二値符号のみを論ずるため，ハミング距離だけを扱う．

3.1 はじめに

才2章で，二値誤り訂正符号をGray変換する方式が，多相位相変調通信に対し，実用上もっとも重要なものであることを知った．この場合2.7.4で述べたように，二値符号の符

号長を本来の符号長から，短縮または伸長することが必要となる場合が生じる．

また，二値誤り訂正符号をそのまま用いる通信系を考えても，要求される情報伝送速度を達成する符号を構成するために，しばしば，符号長を適当に短縮または伸長することが必要となる．

このように，誤り訂正符号の符号長を本来のものから短縮または伸長する技術は実用上きわめて重要である。組織符号の符号長を短縮するのは，いくつかの情報シンボルを0とおいて，これらのシンボルを除くことにより簡単に行える。ただし，このようにして大巾な短縮を行えば，得られた符号は能率のよくないものになることは言うまでもない。それゆえ，短縮化のみでは符号長の十分自由な設計は行えず，能率よく符号長を伸ばす方法が必要となる。ところが，符号長を伸ばす方法は全パリティ検査ディジットを一つ付け加えることによる拡大（extension）など，ごく簡単な方法以外には知られていなかった。

本章ではPreparata符号および二値BCH符号の符号長を

能率よく伸ばす方法について論ずる。

Preparata 符号（P-符号と略記する）は符号長が $2^{n+1}-1$，情報ビット数が $2^{n+1}-2n-2$（n：3以上の奇数）となる最適な* 二重誤り訂正二値非線形組織符号であり，符号化及び復号が比較的簡単に行える。(44) 3.2でこの符号について，さらに説明を加える。

3.3では，このP-符号の符号長を能率よく伸ばす方法を示す。このようにして得られる符号を修正 Preparata 符号（modified Preparata code，mP-符号と略記する）と呼ぶことにする。mP-符号の符号長は $2^{n+1}-1+|J|$（n：3以上の奇数，$|J|$：ある条件を満たす正整数）であり，同一の n に対し，P-符号より符号長が $|J|$ だけ長い。mP-符号の情報ビット数は $2^{n+1}-2n-3+|J|$，検査ビット数は $2n+2$ であり，P-符号に比べ検査ビットが1ビット多くなっている。mP-符号はP-符号と同様，きわめてすぐれた性質をもっている。mP-符号の特長を次に列挙しよう。

---

* 一定の符号長と最小距離に対し，符号語数が最大となる符号を最適符号と呼ぶ。

(i) 二値組織符号としては最適な二重誤り訂正符号であり，短縮化BCH符号[1]の4倍の符号語数をもつ．

(ii) 組織符号であるため符号化が容易である。

(iii) BCH符号の復号[1][2]に類似した代数的な方法で，比較的簡単に復号できる。

3.3，3.4では，これらの性質を中心として，mp-符号について論ずる．

また，3.5では二値BCH符号の符号長を，mp-符号の場合と類似した方法で，能率よく伸ばせることを示す。この場合にも検査ビットは1ビット増すだけでよい。

ところで二値二重誤り訂正原始BCH符号は準完全符号となることが知られている[2]．3.6では，3.5で述べる方法により，このようなBCH符号の符号長を伸ばしても，再び準完全符号を構成し得ることが示される．

3.2 Preparata符号

修正Preparata符号について述べる前に，ここではその準備としてPreparata符号[44]について簡単に述べておこう．

誤り訂正符号の研究において，古くから，できるだけよい符号を発見しようという試みがなされてきた．このような試みの中から，いくつかの非線形符号が試行錯誤的な方法によって見出された．これらの符号の中で1968年 Nordstrom と Robinson [41] によって発見された二重誤り訂正二値非線形符号は重要である．この符号はNR-符号と呼ばれ，符号長が15，情報ビット数が8の組織符号であり，また，符号語数が Johnson の上界 [42] に達する最適な符号である．ついで，Preparata [43] [44] は，NR-符号の構造を調べ，その一般化に成功した．この符号を Preparata 符号（P-符号）と呼ぶ．P-符号は多項式によって定義するのがもっとも便利である．

n を3以上の奇数とし，$x^{2^n-1}+1$ を法とする GF(2) 上の多項式環を R_n とする（R_n の元は 2^n-2 次以下の多項式で表わす）．以下多項式は原則として R_n の元と考える．また $a(x)=\sum_j a_j x^j$ $(\in R_n)$ によって，多項式 $a(x)$ の係数からなる長さ 2^n-1 の系列 $(a_{2^n-2}, a_{2^n-3}, \cdots, a_1, a_0)$ をも表わす．

ここで，つぎのような記号を定義しておこう．

α : $GF(2^n)$ の原始元

$g_1(x)$ ：α の最小多項式

$\{m(x)\}$ ： $g_1(x)$ によって生成される二値ハミング $(2^n-1, 2^n-n-1)$ 符号

$\{A(x)\}$ ： $1, \alpha, \alpha^3$ を根として含む最小次数の多項式によって生成される二値 BCH $(2^n-1, 2^n-2n-2)$ 符号

$f(x)$ ： $f(x)g_1(x)=0$, $f(\alpha)=1$ となる多項式（このような多項式の存在は文献(44), Lemma 3に証明されている）

$$\{g(x)\} = \{ax^l \mid a \in GF(2),\ 0 \le l < 2^n-1\}$$

$$u(x) = (x^{2^n-1}+1)/(x+1)$$

このとき，Preparata 符号はつぎのように定義される。

定義 3.1 （Preparata 符号）

$$v' = (m(x),\ i,\ (m(1)+i)u(x)+m(x)+A(x))$$

$$u' = (g(x),\ 0,\ g(x)f(x))$$

$(m(x) \in \{m(x)\}$, $i \in GF(2)$, $A(x) \in \{A(x)\}$

$g(x) \in \{g(x)\})$

となる二種の $2^{n+1}-1$ 次元ベクトル v', u' に対し $z = v' + u'$ となる形のベクトルすべての集合を Preparata 符号（P－符号）と呼ぶ。

P－符号は最小（ハミング）距離が5の二値非線形組織（$2^{n+1}-1$, $2^{n+1}-2n-2$）符号である。また，符号語数がJohnsonの上界に達する最適な符号であり，同一の符号長の二重誤り訂正BCH符号の2倍の符号語数をもつ。さらに，符号化および復号が比較的簡単に行える。なお，$n=3$の場合P－符号はNR－符号となる。

3.3 修正Preparata符号

3.3.1 修正Preparata符号の定義

2^n-1を法とする整数の剰余環をZ_nとする（Z_nの元は2^n-2以下の非負の整数で表わす）．また，Jをつぎの条件(†)を満たすZ_nの部分集合としよう。

条件(†)：αのべきの集合$\{\alpha^{3j} \mid j \in J\}$において，任意の四つの異なる元の和$\alpha^{3i}+\alpha^{3j}+\alpha^{3k}+\alpha^{3l}$（$i<j<k<l$, $i,j,k,l \in J$）が0とならない。

また，Jに含まれる元の数を$|J|$で表わす．

つぎに，このようなJに対応して，つぎのようなR_nの部分集合を定義する。

$$\{C(x)\} = \{ C(x) \mid C(x) = \sum_j c_j x^j,\ C(1) = 0,$$

$$j \notin J \text{ のとき } c_j = 0 \}$$

すなわち，$\{C(x)\}$ は係数の和が0となり，$c_j (j \in J)$ 以外の係数がすべて0となる多項式の集合である。また，つぎの多項式を定義しておく。

$g_c(x)$: $g_c(x) = x^s g_1(x) (s \in Z_n)$, $g_c(\alpha^3) = 1$ となる多項式

このような $g_c(x)$ が存在することは容易に確かめられる。実際 $g_1(\alpha^3) = \alpha^t (t \in Z_n)$ であれば，$s = -t \cdot 3^{-1}$ (3^{-1} に Z_n における3の逆元を示す*) とすればよい。

ここで，修正 Preparata 符号を定義しよう。

定義 3.2 (修正 Preparata 符号)：

$$v = (m(x),\ i,\ (m(1)+i)u(x) + m(x) + a(x) + C(x)g_c(x),\ C(x))$$

$$u = (g(x),\ 0,\ g(x)f(x),\ 0)$$

($m(x) \in \{m(x)\}$, $i \in GF(2)$, $a(x) \in \{a(x)\}$, $g(x) \in \{g(x)\}$, $C(x) \in \{C(x)\}$)

---

* n が奇数であるから，3と $2^n - 1$ は互いに素となり，Z_n において，3^{-1} は一意に定まる。

となる2種の $3\cdot 2^n-2$ 次元ベクトル v, w に対し, $z = v + w$ となる形のベクトルすべての集合を修正 Preparata 符号（mP－符号）と呼び, $\mathcal{M}_n$ または $\mathcal{M}_n(J)$ で表わす。

mP－符号の符号長は見掛け上 $3\cdot 2^n-2$ であるが, 実際には $c(x)$ の J に属さない次数の項の係数がすべて0となるから, 符号長は $2^{n+1}-1+|J|$ と考えることができる。$|J|$ の値については次節で論ずる。

mP－符号は 3.3.4 で示すように非線形組織符号となる。その情報ビット数は, $\{m(x)\}$, $\{s(x)\}$, $\{c(x)\}$ の情報ビット数がそれぞれ, 2^n-1-n, 2^n-2-2n, $|J|-1$ であり, さらに, $g(x)$ $(\in\{g(x)\})$ および v $(\in GF(2))$ を自由に選べることから, $2^{n+1}-2n-3+|J|$ となることが分る。すなわち, mP－符号は二値非線形組織 $(2^{n+1}-1+|J|,\ 2^{n+1}-2n-3+|J|)$ 符号である。

ところで, 実際の符号化および復号を考えると, J として $\{0, 1, 2, \cdots, |J|-1\}$ となる集合で条件(†)を満たすものを選ぶことが望ましい。このとき $\{c(x)\}$ は $|J|-1$ 次

以下の多項式となり，符号化および復号が簡単化される。このようにして選ばれた J を特に J^* と書き，J^* を用いて構成された $mP-$ 符号を特に $0mP-$ 符号と呼ぶことにする。

3.3.2 $mP-$ 符号の符号長

$mP-$ 符号の（実際の）符号長は $2^{n+1}-1+|J|$ である。本節では $|J|$ の値について考えよう。

条件（十）を満たす有る集合 J が与えられれば，J から任意に j' 個の元を除いた集合 J' は再び条件（十）を満たすから，J' を用いて符号長 $2^{n-1}-1+|J'|=2^{n+1}-1+|J|-j'$ の $mP-$ 符号を作ることができる。したがって，J としては $|J|$ のできるだけ大きい集合を見出すことが望ましい。そこで，$|J|$ の可能な最大値を $|J|_{max}$ とし，この値の上界と下界について考えよう。

条件（十）は“$\{\alpha^{3j}|j\in J\}$ の任意の異なる二つの元の和がすべて異なる”と言い換えることができるから，$|J|_{max}$ は

$$\binom{|J|_{max}}{2} \leq 2^n-1 \qquad (3.1)$$

を満たさねばならない。この式によって $|J|_{max}$ の上界が与えられる。

一方，$|J| + \binom{|J|}{3} < 2^n - 1$ であれば，$GF(2^n)$ の0でない元で，$\alpha^{3j}\ (j \in J)$ または $\alpha^{3j} + \alpha^{3k} + \alpha^{3l}\ (j < k < l,\ j, k, l \in J)$ という形では表わせないものが存在する。

このような元の一つを α^{3i} とし，J に i を付け加えた集合をあらたに J とおくと，この集合 J は再び条件(†)を満たす。ゆえに $|J|_{max}$ は

$$|J|_{max} + \binom{|J|_{max}}{3} \geq 2^n - 1 \qquad (3.2)$$

を満たす。この式によって $|J|_{max}$ の下界が与えられる。

つぎに，0mP－符号の場合について考えよう。$\{0, 1, \cdots, |J^0| - 1\}$ となる集合 $J = J^0$ で条件(†)を満たすものに含まれる元の数 $|J^0|$ の最大値は $GF(2^n)$ の原始元 α（したがって $g_1(x)$）の選び方によって異なる。そこで，これを，$|J^0(\alpha)|_{max}$ と書こう。$|J^0(\alpha)|_{max}$ の上界としては式(3.1)を用いることができる。また，下界はつぎの補題で与えられる。

補題 3.1 ： 任意の原始元 α に対し $|J^{\circ}(\alpha)|_{max} \geq n+1$ となる。

（証明） $\beta = \alpha^3$ とおく。このとき条件(†)は

$$\left.\begin{array}{l} \beta^i + \beta^j + \beta^k + \beta^l \neq 0 \\ (i<j<k<l,\ i,j,k,l \in J) \end{array}\right\} \qquad (3.3)$$

となる。β は $GF(2^n)$ の原始元となるから，$\beta^0, \beta^1, \cdots \beta^{n-1}$ は $GF(2^n)$ の $GF(2)$ の上の n 次元ベクトル空間の基底となる。ゆえに，$J=\{0,1,\cdots,n-1\}$ に対しては式(3.3)の成立することは明らかである。

つぎに，$\beta^i+\beta^j+\beta^k+\beta^n=0$ $(0 \leq i<j<k<n)$ とすれば，β の最小多項式 $g_3(x)$ は $x^n+x^k+x^j+x^i$ とならねばならない。したがって $g_3(x)$ は $x+1$ で割り切れる。しかるに $g_3(x)$ は既約多項式であるから，これは矛盾である。ゆえに $J=\{0,1,\cdots,n\}$ に対して式(3.3)は成立する。

（証明終）

さらに詳しく $|J^{\circ}(\alpha)|_{max}$ を定めるためには個々の原始元 α について調べる必要がある。つぎの二つの補題は $|J^{\circ}(\alpha)|_{max}$ を実際に求める上で有用である。

補題 3.2 ： 任意の原始元 α に対し，次式が成立する。

$$|J^{\circ}(\alpha)|_{max} = |J^{\circ}(\alpha^{2^i})|_{max} \quad (i：正整数) \qquad (3.4)$$

$$|J^{\circ}(\alpha)|_{max} = |J^{\circ}(\alpha^{-1})|_{max} \qquad (3.5)$$

(証明) 式 (3.4) は明らかである。式 (3.5) を証明する。

$\beta = \alpha^3$, $d_0 = |J^{\circ}(\alpha)|_{max} - 1$ とおく。$0 \leq i < j < k < l \leq d_0$ となるすべての i, j, k, l に対し $\beta^i + \beta^j + \beta^k + \beta^l \neq 0$ であるから，$i' = d_0 - i$, $j' = d_0 - j$, $k' = d_0 - k$, $l' = d_0 - l$ とおけば，$0 \leq l' < k' < j' < i' \leq d_0$ となるすべての i', j', k', l' に対し $\beta^{-i'} + \beta^{-j'} + \beta^{-k'} + \beta^{-l'} = \beta^{-d_0}(\beta^i + \beta^j + \beta^k + \beta^l) \neq 0$ となることが分る。$\beta^{-1} = (\alpha^{-1})^3$ であるから，$|J^{\circ}(\alpha^{-1})|_{max} \geq d_0 + 1 = |J^{\circ}(\alpha^{-1})|_{max}$ が導ける。(証明終)

補題 3.3 ： $\beta = \alpha^3$ の最小多項式 $g_3(x)$ が $g_3(x) = 1 + x^m + x^n$ となる三項式であるときは

$$|J^{\circ}(\alpha)|_{max} = n + \min[m, n-m]$$

(証明) $m \leq (n-1)/2$ と仮定する。β^n, β^{n+1}, $\cdots$, β^{n+m-1} を $\{\beta^0, \beta^1, \cdots \beta^{n-1}\}$ を用いて表わせば，

$$\beta^n = \beta^0 + \beta^m$$

$$\beta^{n+1} = \beta^1 + \beta^{m+1}$$

$$\beta^{n+m-1} = \beta^{m-1} + \beta^{2m-1}$$

となる。これからただちに，$\beta^{i}+\beta^{j}+\beta^{k}+\beta^{l}\neq 0$ $(0\leq i<j<k<l\leq n+m-1)$ となることが導ける。

一方，$1+\beta^{2m}+\beta^{n}+\beta^{n+m}=0$ であるから，$|J^{\circ}(\alpha)|_{max}=n+m$ となる。

また，$m\geq (n+1)/2$ のときは補題 3.2 を用いれば，$|J^{\circ}(\alpha)|_{max}=n+(n-m)$ を得る。 （証明終）

表 3.1 に $n=3, 5, 7$ の場合について，すべての $GF(2^n)$ の原始元 α に対する $|J^{\circ}(\alpha)|_{max}$ とそれに対応する OmP-符号の符号長と情報ビット数を示しておく。ただし，補題 3.2 によって $|J^{\circ}(\alpha)|_{max}$ が等しくなるものは省略してある。また各 n について式 (3.1)，(3.2) による $|J|_{max}$ の上界と下界もあわせ示してある。

3.3.3 mP-符号の最小距離

mP-符号 $\mathcal{M}_n$ は非線形符号であるので，その最小距離 d_{min} は $\mathcal{M}_n$ の任意の二つの異なる符号語 f_1, f_2 の和

表 3.1　$m=3, 5, 7$ の $OmP-$ 符号の符号長と情報ビット数

m	$\|J\|_{max}$ 上界	$\|J\|_{max}$ 下界	α	$\|J^0(\alpha)\|_{max}$	符号長	情報ビット
3	4	4	α_0, α_0^3	4	19	11
5	8	7	α_0, α_0^3	6	69	57
			α_0^5	7	70	58
7	16	10	$\alpha_0, \alpha_0^3, \alpha_0^5, \alpha_0^{19}$	8	263	247
			α_0^{13}	9	264	248
			α_0^9, α_0^{21}	10	265	249
			α_0^7, α_0^{11}	11	266	250

(注) α_0 は $GF(2^m)$ の原始元でつぎのように定めてある。$m=3$ のとき $\alpha_0^3+\alpha_0^2+1=0$ を満たすもの。$m=5$ のとき $\alpha_0^5+\alpha_0^2+1=0$, $m=7$ のとき $\alpha_0^7+\alpha_0^3+1=0$。

J_0+J_1 の重み（成分中の1の数）の最小値として求めなければならない。すなわち，

$$d_{min} = \min_{\substack{J_0, J_1 \in \mathcal{M}_m \\ J_0 \neq J_1}} W[J_0+J_1] \qquad (3.6)$$

ここに，$W[J]$ は J の重みを示す。

ここで，J_0+J_1 に関する Preparata の結果（文献(44), p. 384）をわずかに修正したつぎの補題を示しておこう。

補題 3.4：$\zeta = J_0+J_1$ はつぎのように分解できる。

$$\zeta = (\zeta_0(x),\ \zeta,\ \zeta_1(x),\ \zeta_2(x))$$

$$= (m(x),\ i,\ (m(1)+i)u(x)+m(x),\ c(x)) + s(x)+c(x)g_c(x)$$

$$+(g(x),\quad 0,\quad g(x)f(x),\quad 0)$$

$$+(0,\quad 0,\quad m'(x)+m'(1)u(x),\quad 0)$$

ここに，$m(x)\in\{m(x)\}$，$\iota\in GF(2)$，$s(x)\in\{s(x)\}$，$c(x)\in\{c(x)\}$，$g(x)\in\{g(x)\}$ である。また，$m'(x)$ は $m'(x)=g(x)+g_0(x)+g_1(x)$（$g_0(x)$，$g_1(x)\in\{g(x)\}$），かつ $m'(x)\in\{m(x)\}$ となる多項式である（したがって，$g(x)=0$ のときは $m'(x)=0$，$g(x)\neq 0$ のときは $m'(x)$ は0または三項式となる）。

つぎに，$c(x)$ の重み（係数中の1の数）$W[c(x)]$ に関して，つぎの補題を導いておく。

補題 3.5：$c(\alpha^3)=0$ を満たす0でない $c(x)\in\{c(x)\}$ が存在すれば，$W[c(x)]\geq 6$ となる。

（証明）$c(\alpha^3)=0$ を満たす $c(x)$ は1，$\beta=\alpha^3$ を根として含む最小次数の多項式によって生成されるBCH符号の符号語である。したがって $W[c(x)]\geq 4$ であり，また $W[c(x)]$ は偶数である。ところが，Jの定義から $W[c(x)]=4$ となる $c(x)$ は存在しない。ゆえに $W[c(x)]\geq 6$。

（証明終）

以上の準備の下につぎの定理を導こう。

定理 3.1：$mP-$符号の最小距離は5である。

(証明) 補題 3.4 の ζ において $c(x)=0$ のときは ζ の重みは $P-$符号の二つの異なる符号語の和の重みと等しく，Prie-parata により，その最小値は5となることが導かれている(44)。

$c(x)\neq 0$ の場合を考えよう。ここで

$$\omega_0 = W[\zeta_0(x)] \qquad \omega = \zeta^{*}$$

$$\omega_1 = W[\zeta_1(x)] \qquad \omega_2 = W[\zeta_2(x)]$$

$$\omega_t = W[\zeta] = \omega_0 + \omega + \omega_1 + \omega_2$$

とおき，表 3.2 に $\omega_0, \omega, \omega_1, \omega_2, \omega_t$ のとり得る値を分類して示す。

表中の (a)～(f) を説明しよう。

(a) $\zeta_0(x) = m(x) \neq 0$ であるから $\omega_0 \geq 3$

(b) $c(x)\neq 0$, $c(1)=0$ であるから $\omega_2 \geq 2$

(c) $g(x)=0$ から $\zeta_1(x) \in \{m(x)\}$, しかも $\zeta_1(x)\neq 0$

---

* ζ は $GF(2)$ の元であるが，ω は重みを表わし実数として扱われる。

表 3.2 ζ の重みの最小値 ($c(x) \neq 0$ の場合)

$g(x)$	$m(x)$	i	$\zeta_1(x)$	重み w_0	重み w	重み w_1	重み w_2	重み w_t
$=0$	$\neq 0$	$*$	$*$	≥ 3 (a)			≥ 2 (b)	≥ 5
	$=0$	$=0$	$\neq 0$			≥ 3 (c)	≥ 2 (b)	≥ 5
			$=0$				≥ 6 (d)	≥ 6
		$\neq 0$	$\neq 0$ (g)		1	≥ 3 (c)	≥ 2 (b)	≥ 6
$\neq 0$	$\neq 0$	$*$	$\neq 0$ (h)	≥ 2 (e)		≥ 1	≥ 2 (h)	≥ 5
	$=0$	$=0$	$\neq 0$ (h)	1		≥ 2 (f)	≥ 2 (h)	≥ 5
		$\neq 0$	$\neq 0$ (h)	1		≥ 1	≥ 2 (h)	≥ 5

(注) $*$ は $=0$ でも $\neq 0$ でもよいことを示す。

であるから $w_1 \geq 3$

(d) $g(x) = m'(x) = m(x) = 0$ であるから, $\zeta_1(x) = s(x) + c(x) g_c(x)$ となる。$\zeta_1(x) = 0$ であるから $\zeta_1(\alpha^3) = c(\alpha^3) = 0$。ゆえに補題 3.5 から $w_2 \geq 6$ *

(e) $w_0 \geq W[m(x)] - W[g(x)] \geq 2$

(f) $\zeta_1(x) \neq 0$, $\zeta_1(1) = 0$ であるから $w_1 \geq 2$

(g) $\zeta_1(1) = i \neq 0$ であるから $\zeta_1(x) = 0$ となることはない。

(h) $g(x) \neq 0$ のとき $\zeta_1(\alpha) = g(\alpha) \neq 0$ であるから $\zeta_1(x) = 0$ となることはない。

---

* $|T| < 6$ のときは $c(x) \neq 0$ のとき $\zeta_1(x) = 0$ となることはない。

以上によっていずれの場合も $wt \geq 5$ となることがわかる。

（証明終）

3.3.4 m_l P－符号の組織符号としての形

はじめに，m_l P－符号 $\mathcal{M}_{m_l}$ が非線形符号であることを確かめておこう。もし，$\mathcal{M}_{m_l}$ が線形符号であれば，補題 3.4 から

$$(0, 0, m_l'(x) + m_l'(1)u(x), 0) \in \mathcal{M}_{m_l}$$

でなければならない。ゆえに，$m_l'(x) + m_l'(1)u(x) \in \{S(x)\}$。したがって，$m_l'(\alpha^3) = 0$ となる。一方，$m_l'(x) \in \{m_l(x)\}$ であるから，$m_l'(\alpha) = 0$ である。このことは $m_l'(x)$ が二重誤り訂正 BCH 符号の符号語であることを意味する。しかるに $m_l'(x) \neq 0$ であれば，$m_l'(x)$ は三項式であったから矛盾が生じる。

このように m_l P－符号は非線形符号であるが，情報ビットと検査ビットが分離できるという意味での組織符号でもある。これをつぎに示そう。

文献 (44) に P－符号がつぎの形の組織符号であることが示されている。

$$(i^{(0)}_{2^n-2}, \cdots, i^{(0)}_1, i^{(0)}_0, i, i^{(1)}_{2^n-2}, \cdots,$$

$$i^{(1)}_{2^n+1}, p_{2n}, \cdots, p_1, p_0) \qquad (3.7)$$

ここに"i"は情報ビット，"p"は検査ビットを示す。

p_l $(l=0, 1, \cdots, 2n)$ は $i_0=(i^{(0)}_{2^n-2}, \cdots, i^{(0)}_1, i^{(0)}_0)$，$i$ および $i_1=(i^{(1)}_{2^n-2}, \cdots, i^{(1)}_{2^n+1})$ を変数とする非線形関数 π_l により $p_l=\pi_l(i_0, i, i_1)$ として定められる。π_l は $g_1(x)$ が三項式であるときは $n-1$ 次の多項式となり，それ以外の場合は一般に n 次の多項式となる。π_n の具体的な形については文献(44)，p. 388 を参照されたい。

ところで，n P－符号は $c(x)\,g_c(x) \in \{m(x)\}$ となることに注意するとつぎの形にも書けることがわかる。

$$(m(x)+g(x),\ i,\ (m(1)+i)u(x)+m(x)+S(x)+g(x)f(x),\ 0)$$

$$+(c(x)g_c(x),\ 0,\ 0,\ c(x))$$

$$(m(x) \in \{m(x)\},\ g(x) \in \{g(x)\},\ i \in GF(2),$$

$$S(x) \in \{S(x)\},\ c(x) \in \{c(x)\})$$

この形の n 項のベクトルのはじめから $2^{n+1}-1$ 番目までの成分は，P－符号となっている。また $\{c(x)\}$ は検査ビットが1ビットの線形符号と考えることができる。このことと式

(3.7)からただちにmlP－符号が組織符号となることがわかる。

つぎにmlP－符号の組織符号としての形をmlを用いて表わしておこう。簡単のために0mlP－符号の場合について示す。$j_0=|J^{\perp}|$とおけば，上述の議論から，0mlP－符号はつぎの形の組織符号であることがわかる。ただし，0mlP－符号において常に0となるような位置（2^{n+1}番目から$3\cdot 2^{n}-2-j_0$番目までの位置）は除いてある。

$$(i^{(0)}_{2^n-2},\cdots,i^{(0)},i,i^{(1)}_{2^n-2},\cdots i^{(1)}_{2n+1},$$

$$p^{(1)}_{2n},\cdots,p^{(0)}_{0},i^{(2)}_{j_0-1},\cdots,i^{(2)}_{1},p^{(2)}_{0}) \qquad (3.8)$$

ここに“i”は情報ビット，“p”は検査ビットを示し，検査ビットはつぎのように定められる。

$$p_l^{(1)}=\pi_l(\tilde{i}_0,i\ \ i_1) \qquad l=0,1,\cdots,2n$$

$$p_0^{(2)}=i^{(2)}_{j_0-1}+\cdots+i_2^{(2)}+i_1^{(2)}$$

ただし，$\tilde{i}_0=i_0+\tilde{i}_2$，$i_0=(i^{(0)}_{2^n-2},\cdots,i_0^{(0)})$，$i_1=(i^{(1)}_{2^n-2},\cdots,i^{(1)}_{2^n+1})$であり，$\tilde{i}_2$は$c(x)=i^{(2)}_{j_0-1}x^{j_0-1}+i^{(2)}_{j_0-2}x^{j_0-2}+\cdots+i_1^{(2)}x+(i^{(2)}_{j_0-1}+\cdots+i_2^{(2)}+i_1^{(2)})$と$g_c(x)$の積$c(x)g_c(x)(\in R_{ml})$の係数からなる$2^n-1$次元ベクトルである。

一般のmlP－符号の組織符号としての形も同様にしておの

ることができる。

3.3.5 mP－符号の最適性

符号長Nの二値組織符号がt重誤り訂正符号であれば，その情報ビット数Kは $\sum_{i=0}^{t}\binom{N}{i} \leq 2^{N-K}$ を満たさねばならない(1)。したがって，N，Kおよびtが

$$2^{N-(K+1)} < \sum_{i=0}^{t}\binom{N}{i} \qquad (3.9)$$

を満たすならば，符号長がNで K+1 以上の情報ビット数をもつt重誤り訂正二値組織符号は存在しない。この意味で式(3.9)を満たすような情報ビット数Kをもつ符号長Nのt重誤り訂正二値組織符号は組織符号としては最適な符号ということができる。

mP－符号の符号長は $N=2^{m+1}-1+|J|$，情報ビット数は $K=2^{m+1}-2m-3+|J|$ であるから

$$\sum_{i=0}^{2}\binom{N}{i} - 2^{N-(K+1)} = 2^{m+1}\cdot|J| - 2^{m}+1+\binom{|J|}{2}$$

となる。ゆえに $|J|>0$ であれば $\sum_{i=0}^{2}\binom{N}{i} > 2^{N-(K+1)}$ であ

る。したがって，つぎの定理を得る。

定理 3.2：mP－符号は組織符号としては最適な符号である。

線形符号は組織符号であるから，mP－符号は少なくとも，同一符号長の最適な二値二重誤り訂正線形符号と等しい情報ビット数をもつ。

ところで，符号長 19 の最適な二値二重誤り訂正線形符号の情報ビット数は 10 となることが知られている[45]。これに対し，$n=3$ のとき 0mP(19, 11) 符号を作ることができる（表 3.1 参照）から，この場合，mP－符号は最適な線形符号の2倍の符号語数をもつ。

しかし，一般の場合については現在のところ，最適な線形符号の情報ビット数が明確に定められていないので，mP－符号と最適な線形符号の情報ビット数の間に差があるかどうかはわかっていない。

しかし，最適な線形符号を構成する一般的な方法は見出されていない。従来知られている方法で mP－符号と同一符号長の二値二重誤り訂正符号を構成するには，BCH 符号の短

縮化* によるのが一般的である。この場合，符号長 $2^{m+2}-1+|J|$ の符号を作るには $2^{m+2}-1$ の符号長のBCH符号を短縮化する必要がある**。この符号の検査ビット数は $2(m+2)$ である(1)。これに対し，mP－符号の検査ビット数は $2m+2$ であるから，mP－符号はこのような短縮化BCH符号の4倍の符号語数をもつ。

3.4 修正 Preparata 符号の復号

mP－符号の符号化はmP－符号の組織符号としての形を用いて比較的簡単に行なうことができる。ここではmP－符号の復号について考えよう。

二元通信路を通してmP－符号の符号語を送信する通信系を考える。送信ベクトルを $\mathfrak{z}_t=(\mathfrak{z}_{t_0}(x),\mathfrak{z}_t,\mathfrak{z}_{t_1}(x),\mathfrak{z}_{t_2}(x))$ $(t\in\mathfrak{M}_m(J))$ とし，誤りベクトルを $\mathfrak{e}=(e_0(x),e,e_1(x),$

---

* 情報ビットを除いて符号長を短縮化することを言う。短縮化によって最小距離が増大することもあるが，一般にはそのようなことは保証されない。

** 非原始BCH符号 (nonprimitive BCH code)(1) を用いて構成する方法も考えられるが，この方法では一般に余りよい符号を作ることはできない。

$e_2(x)$)，受信ベクトルを $r = (r_0(x), r_1(x), r_2(x))$ $= g_t + e$ とする．ここに $g_{tl}(x)$, $e_l(x)$, $r_l(x) \in R_n$ $(l = 0, 1, 2)$，また $g_t, e, r \in GF(2)$ であり，g_t, e, r は $GF(2)$ の上の $3 \cdot 2^n - 2$ 次元ベクトルである．また，$g_{t2}(x)$ の J に属さない次数の項の係数はすべて0であるから，$e_2(x)$, $r_2(x)$ の J に属さない次数の項の係数もすべて0であると考えてよい．

ここで，受信ベクトル r に対し，つぎのような線形符号の場合シンドロームに似た量を定義する．

$$\sigma_0 = r_0(\alpha) = g(\alpha) + e_0(\alpha)$$

$$\sigma_1 = r_1(\alpha) = g(\alpha) + e_1(\alpha)$$

$$\sigma = r_0(\alpha^3) + r_1(\alpha^3)$$

$$= g(\alpha^3) + c(\alpha^3) + e_0(\alpha^3) + e_1(\alpha^3)$$

$$\sigma_2 = r_2(\alpha^3) = c(\alpha^3) + e_2(\alpha^3)$$

$$d = r + r_1(1) = e + e_1(1)$$

$$d_2 = r_2(1) = e_2(1)$$

ここに，$g(x) \in \{g(x)\}$, $c(x) \in \{c(x)\}$ である．

これらの量もシンドロームと呼ぶことにしよう．これらの

中 σ_0, σ_1, σ, d は Preparata によって P-符号の復号のために導入されたシンドローム[44]と同じものであり，σ_2, d_2 が mP-符号の復号のためにさらに必要となる量である。また

$$\begin{aligned}\rho &= \sigma + \sigma_2 + (\sigma_0 + \sigma_1)^3 \\ &= g(\alpha^3) + e_0(\alpha^3) + e_1(\alpha^3) \\ &\quad + e_2(\alpha^3) + (e_0(\alpha) + e_1(\alpha))^3\end{aligned}$$

を定義しておく。

ここで，わずかに修正された Preparata の補題（文献[44], Lemma 9）を示しておこう。

補題 3.6：任意の受信ベクトル r に対して

$$r + g = (0, e', e_1'(x), e_2'(x))$$

$$(e' \in GF(2),\ e_1'(x),\ e_2'(x) \in R_n)$$

となり，$d_2 = 0$ であれば $W[e_1'(x)] \leq 3$, $e_2'(x) = 0$, $d_2 = 1$ であれば $W[e_1'(x)] \leq 3$, $W[e_2'(x)] = 1$ を満たす $g \in \mathcal{M}_n$ が存在する。

この補題を用いると mP-符号をシンドロームによって特徴づけることができる。

補題 3.7：$r \in \mathcal{M}_n$ となる必要十分条件は

$$\rho + \sigma_0^3 = 0, \quad \rho + \sigma_1^3 = 0, \quad d = 0, \quad d_2 = 0 \qquad (3.10)$$

となることである。

(証明) $\rho + \sigma_0^3 = 0$, $\rho + \sigma_1^3 = 0$ が $\sigma_0 + \sigma_1 = 0$, $\sigma + \sigma_2 = \sigma_0^3$ と同値であることに注意すると，シンドロームの定義から，$r \in \mathcal{M}_n$ であれば式 (3.10) の成立することは明らかである。逆を示そう。補題 3.6 から，式 (3.10) を満たす r は適当な $f \in \mathcal{M}_n$ を用いて

$$r = f + (0, e', e_1'(x), 0) \quad (W[e_1'(x)] \leq 3)$$

と書ける。しかるに $\sigma_0 + \sigma_1 = 0$ から $e_1'(\alpha) = 0$, $\sigma + \sigma_2 = \sigma_0^3$ から $e_1'(\alpha^3) = 0$ となり，しかも $W[e_1'(x)] \leq 3$ であるから $e_1'(x) = 0$ でなければならない。また $d = 0$ から $e' = 0$ となる。 (証明終)

ここで，受信ベクトル $r = f_t + e$ に最も近い $\mathcal{M}_n$ の符号語を f_r としよう。このとき，$r + f_r$ を誤差ベクトルと呼び，$\varepsilon = (\varepsilon_0(x), \varepsilon, \varepsilon_1(x), \varepsilon_2(x))$, $(\varepsilon_l(x) \in R_n (l = 0, 1, 2), \varepsilon \in GF(2))$ で表わすことにする。ε と実際の誤りベクトル e には $\varepsilon = e + f_t + f_r$ となる関係があり，特に $W[e] \leq 2$ のときは $\varepsilon = e$ である。また，$\varepsilon_2(x)$ も

$e_2(x)$ と同様 $\mathcal{T}$ に属さない次数の項の係数はすべて0である。

ここで，$\varepsilon_0 = W[\varepsilon_0(x)]$, $\varepsilon_1 = W[\varepsilon_1(x)]$, $\varepsilon_2 = W[\varepsilon_2(x)]$ および $\varepsilon_t = W[E]$ を定義しておく。

以下 $\mathcal{V}$ のシンドローム A と E の関係を求めていく。つぎの補題 3.8 ～ 3.10 は文献(44)の Theorem 2.1～2.3 と本質的には同じものである。

補題 3.8：$d_2 = 0$, $\rho + \sigma_0^3 = 0$, $\rho + \sigma_1^3 \neq 0$ となる必要十分条件は $\varepsilon_0(x) = 0$, $\varepsilon_1(x) = x^{k_1}$, $\varepsilon_2(x) = 0$ となることである。また $d_2 = 0$, $\rho + \sigma_0^3 \neq 0$, $\rho + \sigma_1^3 = 0$ となる必要十分条件は $\varepsilon_0(x) = x^{k_0}$, $\varepsilon_1(x) = 0$, $\varepsilon_2(x) = 0$ となることである。ここに k_1 は $\alpha^{k_1} = \sigma_0 + \sigma_1$ によって定められる。また $\varepsilon = d + \varepsilon_1(1)$ である。

補題 3.9：$d_2 = 0$, $\rho + \sigma_0^3 \neq 0$, $\rho + \sigma_1^3 \neq 0$, $d = 1$ となる必要十分条件は $\varepsilon_0(x) = x^{k_0}$, $\varepsilon = 0$, $\varepsilon_1(x) = x^{k_1}$, $\varepsilon_2(x) = 0$ となることである。ここに，k_0 と k_1 は $\alpha^{k_0} = \sigma_1 + \{\sigma + \sigma_2 + \sigma_0\sigma_2(\sigma_0 + \sigma_2)\}^{3^{-1}}$ と $\alpha^{k_1} = \sigma_0 + \{\sigma + \sigma_2 + \sigma_0\sigma_1(\sigma_0 + \sigma_1)\}^{3^{-1}}$ によって定められる。ただし 3^{-1} は $\mathbb{Z}_n$ における3の逆元である。

補題 3.10： $d_2=0$, $\rho+\sigma_0^3\neq 0$, $\rho+\sigma_1^3\neq 0$, $d=0$, $\sigma_0+\sigma_1\neq 0$, $Tr[(\rho+\sigma_0^3)/(\sigma_0+\sigma_1)^3]=0$ となる必要十分条件は $\varepsilon_0(x)=0$, $\varepsilon=0$, $\varepsilon_2(x)=x^{k_1}+x^{k_2}$, $\varepsilon_2(x)=0$ となることである。ここに k_1, k_2 は y に関する二次方程式 $y^2+(\sigma_0+\sigma_1)y+(\rho+\sigma_0^3)/(\sigma_0+\sigma_1)=0$ の二つの解 α^{k_1}, α^{k_2} によって定められる。ただし，

$$Tr(\xi)=\sum_{i=0}^{n-1}\xi^{2^i}\quad(\xi\in GF(2^n))$$

である。

また $d_2=0$, $\rho+\sigma^3\neq 0$, $\rho+\sigma^3\neq 0$, $d=0$, $\sigma_0+\sigma_1\neq 0$, $Tr[(\rho+\sigma_0^3)/(\sigma_0+\sigma_1)^3]=1$ となる必要十分条件は $\varepsilon_0(x)=x^{k_1}+x^{k_2}$, $\varepsilon=0$, $\varepsilon_1(x)=0$, $\varepsilon_2(x)=0$ となることである。ここに k_1, k_2 は $y^2+(\sigma_0+\sigma_1)y+(\rho+\sigma_1^3)/(\sigma_0+\sigma_1)=0$ の解 α^{k_1}, α^{k_2} によって定められる。

mLP—符号の復号のためには，さらにつぎの補題 3.11～3.13 が必要となる。

補題 3.11： $d_2=0$, $\rho+\sigma_0^3\neq 0$, $\rho+\sigma_1^3\neq 0$, $d=0$, $\sigma_0+\sigma_1=0$ かつ $\alpha^{3k_1}+\alpha^{3k_2}=\rho+\sigma_0^3$ となる $k_1, k_2\in J$ が存在する必要十分条件は $\varepsilon_0(x)=0$, $\varepsilon_1(x)=0$, $\varepsilon=0$, $\varepsilon_2(x)=$

$x^{k_1}+x^{k_2}$ となることである。

(証明) はじめに，補題に示されている $\mathcal{E}=(\varepsilon_0(x), \varepsilon, \varepsilon_1(x), \varepsilon_2(x))$ が誤差ベクトルとなるような受信ベクトルに対するシンドロームが補題の条件を満たすことを示す。$\mathcal{E}$ と $\mathcal{M}_n$ の符号語 $\mathcal{F}$ との和 $\mathcal{V}=\mathcal{F}+\mathcal{E}$ に対するシンドロームは $\sigma_0=g(\alpha)$, $\sigma_1=g(\alpha)$, $\rho=g(\alpha^3)+\varepsilon_2(\alpha^3)=\{g(\alpha)\}^3+\varepsilon_2(\alpha^3)$, $d=0$, $d_2=0$ となる。ゆえに，$\rho+\sigma_0^3=\rho+\sigma_1^3=\varepsilon_2(\alpha^3)=\alpha^{3k_1}+\alpha^{3k_2}\neq 0$, $\sigma_0+\sigma_2=0$。また，明らかに $k_1, k_2\in J$ である。

つぎに，補題の条件を満たすシンドロームを与える受信ベクトルに対する誤差ベクトルが補題に与えられている $\mathcal{E}$ となることを示す。このため $\mathcal{E}'=(\varepsilon_0'(x), \varepsilon', \varepsilon_1'(x), \varepsilon_2'(x))=(0, 0, 0, x^{k_1}+x^{k_2})$ $(\varepsilon_2'(\alpha^3)=\rho+\sigma_0^3,\ k_1, k_2\in J)$ とおき，補題の条件を満たすシンドロームを与える受信ベクトル $\mathcal{V}$ と $\mathcal{E}'$ の和を $\mathcal{V}'=\mathcal{V}+\mathcal{E}'$ とする。このとき $\mathcal{V}'$ に対するシンドロームを σ_0', σ_1', ρ', d', d_2' とすると，$\sigma_0'=\sigma_0$, $\sigma_1'=\sigma_2$, $\rho'=\rho+\varepsilon_2'(\alpha^3)$, $d'=0$, $d_2'=0$ となる。ゆえに $\rho'+\sigma_0'^3=\rho'+\sigma_1'^3=\rho+\sigma_0^3+\varepsilon_2'(\alpha^3)=0$。したがって，補題 3.7 から $\mathcal{V}'\in\mathcal{M}_n$ である。しかるに $\mathcal{M}_n$ の最小距離は 5 であり，$W[\mathcal{E}']=2$ で

あるから，ξ'は誤差ベクトルとならねばならない。すなわち

$\xi = \xi'$。　　（証明終）

つぎの二つの補題は補題 3.11 と同様な手法によってきわめて容易に証明できるので，証明は省略する。

補題 3.12：$d_2 = 1$，$d = 0$，$\sigma_0 + \sigma_1 \neq 0$ かつ $\alpha^{3k_1} = \rho + \sigma_1^3$ となる $k_1 \in J$ が存在する必要十分条件は $\varepsilon_0(x) = x^n$，$\varepsilon = 0$，$\varepsilon_1(x) = 0$，$\varepsilon_2(x) = x^{k_1}$ となることである。ここに n は $\alpha^n = \sigma_0 + \sigma_1$ によって定められる。

また，$d_2 = 1$，$d = 1$，$\sigma_0 + \sigma_1 \neq 0$ かつ $\alpha^{3k_0} = \rho + \sigma_0^3$ となる $k_0 \in J$ が存在する必要十分条件は $\varepsilon_0(x) = 0$，$\varepsilon = 0$，$\varepsilon_1(x) = x^n$，$\varepsilon_2(x) = x^{k_0}$ となることである。ここに $\alpha^n = \sigma_0 + \sigma_1$ である。

補題 3.13：$d_2 = 1$，$\sigma_0 + \sigma_1 = 0$ かつ $\alpha^{3k} = \rho + \sigma_0^3$ となる $k \in J$ が存在する必要十分条件は $\varepsilon_0(x) = 0$，$\varepsilon = \alpha$，$\varepsilon_1(x) = 0$，$\varepsilon_2(x) = x^k$ となることである。

補題 3.7 ～ 3.13 から ρ 符号はつぎのようにして復号できることがわかる。

表 3.3　mP－符号の復号法

	$\rho+\sigma_0^3$	$\rho+\sigma_1^3$	σ	σ_2	$\sigma_0+\sigma_1$	訂正法	ε_0	ε	ε_1	ε_2
1	0	0	0	0	*	$\varepsilon=0$	0	0	0	0
2	0	0	1	0	*	$\varepsilon_0(x)=\varepsilon_1(x)=\varepsilon_2(x)=0,\ \varepsilon=1$	0	1	0	0
3	0	≠0	0	0	*	補題 3.8 の ε により訂正	0	0	1	0
4	0	≠0	1	0	*		0	1	1	0
5	≠0	0	0	0	*		1	0	0	0
6	≠0	0	1	0	*		1	1	0	0
7	≠0	≠0	1	0	*	補題 3.9 の ε により訂正	1	0	1	0
8	≠0	≠0	0	0	≠0	補題 3.10 の ε により訂正	2	0	0	0
9	≠0	≠0	0	0	≠0		0	0	2	0
10	≠0	≠0	0	0	=0	補題 3.11 の ε により訂正	0	0	0	2
11	*	*	0	1	≠0	補題 3.12 の ε により訂正	1	0	0	1
12	*	*	1	1	≠0		0	0	1	1
13	*	*	0	1	=0	補題 3.13 の ε により訂正	0	0	0	1
14	*	*	1	1	=0		0	1	0	1

(注)　＊はその項のシンドロームの値が分類に不要であることを示す。また，ε_0, ε, ε_1, ε_2 はおのおのの場合に訂正が可能な誤りのパターンを示す。

mP－符号の復号法

(1)　受信ベクトル $\mathbf{r}$ からシンドローム σ_0, σ_2, σ, σ_2, ρ を計算する。

(2)　シンドロームの値によって表3.3のような14通りの場合に分け，おのおのの場合に対応する補題に示されている ε を求める。

(3) $r+\varepsilon$ として受信ベクトルを訂正する。

(注1) 表3においてδとγは $\mathrm{Tr}[(\rho+\sigma_0^3)/(\sigma_0+\sigma_1)^3]=0,1$ によって区別する。また，この場合には，二次方程式を解く必要があるが，これは比較的簡単である（たとえば文献(2)，p.244参照）。

(注2) 表3.3の10の場合には補題3.11の k_1, k_2 を定める必要がある。これは $\alpha^j=(\rho+\sigma_0^3+\alpha^{3i})^{3^{-1}}$ $(i\in J)$ を計算し，$j\in J$ となるものが見出されたときの i を k_1，j を k_2 とすればよい。

以上の復号法によって誤りが2個以下のときは正しく復号できる。誤りが3個以上あるときは，受信ベクトルと距離が2以下の $\mathfrak{M}_n$ の他の符号語が存在すれば誤って復号されるが，このほかに，つぎのような場合が生じ得る。

10'. 表3.3の10の場合に $\alpha^{3k_1}+\alpha^{3k_2}=\rho+\sigma_0^3$ となる k_1, $k_2\in J$ が存在しない。

11'. 11の場合に $\alpha^{k_1}=(\rho+\sigma_1^3)^{3^{-1}}$ となる $k_1\in J$ が存在しない。

12'. 12の場合に $\alpha^{k_0}=(\rho+\sigma_0^3)^{3^{-1}}$ となる $k_0\in J$ が存在しない。

13'. 13および14の場合に $\alpha^k=(\rho+\sigma_0^3)^{3-1}$ となる $k\in J$ が存在しない。

このような場合には3個以上の誤りが生じたことを検出できる。

以上の復号法において，かなりの計算時間を要すると思われるのは（注2）に示した表3.3の10の場合の $\varepsilon_2(x)$ の計算であろう。しかし，一般にmlP－符号の符号長に比較して $|J|$ はかなり小さいので，実際には余り問題とはならない。

また，0mlP－符号を用いる場合には表3.3の10～14の復号過程における $\varepsilon_2(x)$ の計算がかなり簡単化できる。

本節ではmlP－符号の代数的復号法を示した，mlP－符号の復号においては $GF(2^m)$ の上で演算が行なわれる。これに対し，同一符号長の二値二重誤り訂正短縮化BCH符号（3.3.5参照）の復号においては $GF(2^{m+2})$ の上で演算を行なう必要がある。しかし，mlP－符号の復号法は場合分けが多く，その復号器は短縮化BCH符号の復号器に比べ，なお多少複雑になると思われる。しかし，mlP－符号は組織符号としては最適な符号であるから，復号がやや複雑となっても許容し得

る場合が多いであろう.

3.5 二値BCH符号の新しい修正法

二値BCH符号に対しても, Preparata符号の場合とほとんど同様な手法によって符号長を伸ばすことができる.

修正Preparata符号の場合と同様に, m を3以上の整数とし, $x^{2^{m-1}}+1$ を法とするGF(2)の上の多項式環を R_m とする. また, α をGF(2^m)の原始元とする.

つぎに, t を正整数とし, $\alpha, \alpha^3, \cdots, \alpha^{2t-1}$ を根として含む最小次数の多項式を生成多項式とする符号長 $N_B = 2^m - 1$ の t 重誤り訂正二値BCH符号を $B_{m,t}$ で表わす.

ここで, $B_{m,t-1}$ ($\alpha, \alpha^3, \cdots, \alpha^{2t-3}$ を根として含む最小次数の多項式を生成多項式とする $t-1$ 重誤り訂正二値BCH符号)が α-BCH符号[46]であるとしよう. すなわち, $B_{m,t-1}$ の生成多項式が α^{2t-1} を根として含まないとする. この場合, ここでは $B_{m,t}$ を α^+-BCH符号と呼ぶことにする. 本節の修正法はこのような α^+-BCH符号を対象とするものであり, 以下では $B_{m,t}$ は α^+-BCH符号であると仮定する.

つぎに，$g_{ct}(x)$ を $\alpha, \alpha^3, \cdots, \alpha^{2t-3}$ を根として含み，

$$g_{ct}(\alpha^{2t-1}) \neq 0$$

となる多項式とする。$B_{m,t}$ が α^+-BCH 符号であるから，このような多項式 $g_{ct}(x)$ は存在する。たとえば，α-BCH 符号 $B_{m,t-1}$ の生成多項式を $g_{ct}(x)$ とすればよい。

また，2^m-1 を法とする整数の剰余環を Z_m とし，J_t をつぎの条件 (††) を満たす Z_m の部分集合とする。

条件 (††)：α のべきの集合 $\{\alpha^{(2t-1)j} \mid j \in J_t\}$ において，$2t$ 個以下 4 個以上の任意の偶数個の元の和

$$\alpha^{(2t-1)j_1} + \alpha^{(2t-1)j_2} + \cdots + \alpha^{(2t-1)j_{2l}}$$

$$(j_1 < j_2 < \cdots < j_{2l}, \quad 2 \leq l \leq t)$$

が 0 となることはない。

ここで J_t に含まれる元の数を $|J_t|$ で表わすことにする。

つぎに，このような J_t に対応して，つぎのような R_m の部分集合を定義する。

$$C_{m,t}(J_t) = \{ c(x) \mid c(x) = \sum c_j x^j, \ c(1) = 0, \ j \notin J_t \text{ のとき } c_j = 0 \}$$

このとき，つぎのような符号を定義する。

定義 3.3 （修正 BCH 符号）：

$$v = (b(x) + C(x) g_{Jt}(x),\ C(x))$$

$$(\ b(x) \in B_{m,t}\ ,\ C(x) \in C_{m,t}(J_t)\ )$$

となる形の $2^{m+1}-2$ 次元ベクトルすべての集合を，ここでは修正 BCH 符号と呼び，$\mathcal{M}_{m,t}(J_t)$ で表わすこととする。

mP-符号の場合と同様に修正 BCH 符号の実効符号長 N および情報ビット数 K は

$$N = 2^m - 1 + |J_t| \qquad K = K_B + |J_t| - 1$$

となる。ただし K_B は d^+-BCH 符号 $B_{m,t}$ の情報ビット数である。

$|J_t|$ の可能な最大値を $|J_t|_{max}$ とすると，$|J_t|_{max}$ の上界と下界は mP-符号の場合とほとんど同様に求められ，それぞれ

$$\sum_{i=0}^{[\frac{t}{2}]} \binom{|J_t|_{max}}{2i} \leq 2^m - 1 \qquad (3.11)$$

$$\sum_{i=0}^{t} \binom{|J_t|_{max}}{2i+1} \geq 2^m - 1 \qquad (3.12)$$

から導ける。ここに [ ] はガウス記号である。

つぎに，修正 BCH 符号の誤り訂正能力についてみてみよ

う。

定理3.3：d^+－BCH符号 $B_{m,t}$ から構成される修正BCH符号 $\mathcal{M}_{m,t}(J_t)$ の最小距離は少くとも $2t+1$ である。

（証明） $t_1(X) = b(X) + C(X)\,g_{ct}(X)$，$v = (t_1(X), C(X))$ （$b(X) \in B_{m,t}$，$C(X) \in C_{m,t}(J_t)$）とおく。v が修正BCH符号 $\mathcal{M}_{m,t}(J_t)$ の符号語である。明らかに $\mathcal{M}_{m,t}(J_t)$ は線形符号であるから，その最小距離は $v(\neq 0)$ の最小重みである。

はじめに，$t_1(X) \neq 0$ の場合を考えよう。$C(X) = 0$ とすると $t_1(X) \in B_{m,t}$，ゆえに v の重み $W[v]$ は少くとも，$2t+1$ となる。$C(X) \neq 0$ とすると，$t_1(X) \in B_{m,t-1}$．ゆえに，$W[t_1(X)] \geq 2t-1$ となる。しかも $C(1) = 0$ であるから $W[C(X)] \geq 2$。したがって $W[v] \geq 2t+1$ となる。

つぎに，$t_1(X) = 0$ としよう。このとき $t_1(\alpha^{2t-1}) = 0$．しかるに $b(\alpha^{2t-1}) = 0$，$g_{ct}(\alpha^{2t-1}) \neq 0$ であるから，$C(\alpha^{2t-1}) = 0$ を得る。このとき，$C(X)$ および J_t の定義から，$C(X) \neq 0$ であれば（すなわち $v \neq 0$ であれば）$W[C(X)] \geq 2t+2$ となることが分る。したがって，$v \neq 0$ のとき，$W[v] \geq$

$2t+2$ となる。

ゆえに，いずれの場合にも $v \neq 0$ である限り，$W[v] \geq 2t+1$ である。 (証明終)

つぎに，修正BCH符号 $\mathcal{M}_{m,t}(J_t)$ の復号について考えよう。受信ベクトルを $r=(r_1(x), r_2(x))$，誤りベクトルを $e=(e_1(x), e_2(x))$ とする。ただし，$r_1(x)$, $r_2(x)$, $e_1(x)$ $e_2(x) \in R_n$ であり，m 系列符号の場合と同様に，$r_2(x)$, $e_2(x)$ の J_t に属さない次数の項の係数は0であるとする。

ここで，つぎのシンドロームを定義する。

$$s_{2i-1} = r_1(\alpha^{2i-1}) = e_1(\alpha^{2i-1}) \quad i=1,2,\cdots,t-1 \tag{3.13}$$

$$\begin{aligned} s_{2t-1} &= r_1(\alpha^{2t-1}) + r_2(\alpha^{2t-1}) g_{ct}(\alpha^{2t-1}) \\ &= e_1(\alpha^{2t-1}) + e_2(\alpha^{2t-1}) g_{ct}(\alpha^{2t-1}) \end{aligned} \tag{3.14}$$

$$d = r_2(1) = e_2(1) \tag{3.15}$$

修正BCH符号の復号法はつぎのような手順で行える。

(1) 受信ベクトル r からシンドローム $s_1, s_3, \cdots, s_{2t-1}$ および d を計算する。

(2) $s_1, s_3, \cdots, s_{2t-1}$ に対して，BCH符号の復号法を用い，$e_1(x)$ を求める。

(3) $e_1(\alpha^{2t-1})$ を計算し，式 (3.14) によって $e_2(\alpha^{2t-1})$ を求める。

(4) $e_2(\alpha^{2t-1})$ および $\alpha = e_2(1)$ から $e_2(x)$ を求める。

(注1) 通常の二値BCH符号の復号法（Petersonの方法[1]，あるいはBerlekampの方法[2]）においては，t' ($t' \leq t$) 個の誤りが生じているときには，復号の計算において，実際には $s_1, s_3, \cdots, s_{2t'-1}$ だけしか用いられない。それゆえ，$W[e] \leq t$ であるとすれば，(2) の過程で s_{2t-1} が用いられるのは $e_2(x) = 0$ すなわち，$s_{2t-1} = e_1(\alpha^{2t-1})$ のときに限る。したがって，$W[e] \leq t$ である限り，(2) によって常に正しく $e_1(x)$ を定め得る。

(注2) J_t の定義から，$(e_2(\alpha^{2t-1}), e_2(1))$ は重み t 以下のすべての異なる誤りベクトル $e_2(x)$ に対し異なる（$W[e_2'(x)] \leq t$, $W[e_2''(x)] \leq t$, $e_2'(\alpha^{2t-1}) = e_2''(\alpha^{2t-1})$, $e_2'(1) = e_2''(1)$ とすれば，$e_2'(\alpha^{2t-1}) + e_2''(\alpha^{2t-1})$ は，α のべき $\alpha^{(2t-1)j}$ ($j \in J_t$) の $2t$ 個以下，偶数個の和であり，しかも0となる）。それゆえ，$W[e] \leq$

tであれば，(4)によって一意に$e_2(x)$を定め得る。

ただし，現在のところ，$(e_2(\alpha^{2t-1}), e_2(1))$から$e_2(x)$を簡単に求める方法はなく，すべての可能な組み合せを調べる必要がある。

以上，二値BCH符号の新しい修正法について述べた。この方法は，特にtが小さい場合きわめて有効である。事実，$t=2$の場合は次節で述べるように，この方法によって準完全符号を得ることができる。

3.6 二重誤り訂正二値準完全符号の新しい構成法

二重誤り訂正二値準完全符号は，その符号で，二値ベクトルすべての集合を剰余類展開したとき，各剰余類に含まれる最小重みのベクトルの重みが3以下となる符号であり，二元対称通信路に用いたとき，Peterson[1]の定義する意味で最適な符号となっている。すなわち，最尤復号を行なったとき，同一の符号長と情報ビット数の線形符号のうちで誤り率が最小となる。

二重誤り訂正二値準完全符号としては，二重誤り訂正二値原始BCH符号（3.5で定義した$B_{m,2}$）がよく知られている[2]。また嵩らは，二元対称通信路に対しPetersonの意味での最適な符号を求めるある程度簡単化されたアルゴリズムを提案し，計算機を用いて，いくつかの二重誤り訂正二値準完全符号を求めた[47]。

本節では，3.5で述べたBCH符号の修正法によっても，二重誤り訂正二値準完全符号を構成できることを示す。

ここでは，nは3以上の奇数とするが，他の記号および仮定は3.5と同様とする。なお，二重誤り訂正二値BCH符号$B_{n,2}$はd^+-BCH符号となるから，3.5の修正法が適用できることは，いうまでもない（αの最小多項式にα^3が根として含まれるとすれば，$2^i \equiv 3 \bmod (2^m-1)$となる整数$i$が存在しなければならないが，これは不可能である）。

ここで，J_2^*をつぎの二つの条件を満たすZ_nの部分集合としよう。

条件(T)：αのべきの集合$\{\alpha^{3j} \mid j \in J_2^*\}$において，任意の四つの異なる元の和$\alpha^{3j_1}+\alpha^{3j_2}+\alpha^{3j_3}+\alpha^{3j_4}$（$j_1<j_2$

$< j_3 < j_4$, $j_1, j_2, j_3, j_4 \in J_2^*$) が0とならない。

条件(ttt)：GF(2^m)の任意の元aに対し，J_2^*に，$a = \alpha^{3j_1} + \alpha^{3j_2} + \alpha^{3j_3}$ となる j_1, j_2, j_3 ($j_1 < j_2 < j_3$)，または $a = \alpha^{3j}$ となる j が含まれる。

条件(T)は3.3の条件(T)と同じものであり，また $t=2$ とすれば，3.5の条件(tt)とも同じものである。それゆえ，J_2^* は，3.5の J_2 にさらに条件(ttt)を課したものとなっている。ただし，本節では n は3以上の奇数に限っていることに注意しておこう。

条件(T)(ttt)を満たす J_2^* が存在することは容易に確かめられる。実際，J_2^* はつぎのようにして作ることができる。はじめに，$\alpha^{3i_1} + \alpha^{3i_2} + \alpha^{3i_3} = 0$ となる i_1, i_2, i_3 ($i_1 < i_2 < i_3$) および i_4 ($\neq i_1, i_2, i_3$) の集合を J とし，つぎに $\alpha^{3j_1} + \alpha^{3j_2} + \alpha^{3j_3}$ ($j_1 < j_2 < j_3$, $j_1, j_2, j_3 \in J$) または α^{3j} ($j \in J$) という形で表わせない GF(2^m) の元 α^{3i} があるとき，i を J につけ加えていけば，J が最終的に条件(T)(ttt)を満たす集合 J_2^* となることは明らかである。

明らかに，J_2^* に含まれる元の数 $|J_2^*|$ は

$$|J_2^*| + \binom{|J_2^*|}{3} \geq 2^n$$

を満たす*。

このような J_2^* を用い，3.5の方法で構成される二重誤り訂正二値修正BCH符号が準完全符号となることが，つぎの定理で示される。

定理3.4：符号長 2^n-1（n：3以上の奇数）の二重誤り訂正二値BCH符号 $B_{n,2}$ から J_2^* を用いて構成される修正BCH符号 $\mathcal{M}_{n,2}(J_2^*)$ は準完全符号となる。

(証明) 受信ベクトル $r=(r_1(x), r_2(x))$ にもっとも近い $\mathcal{M}_{n,2}(J_2^*)$ の符号語を $t=(t_1(x), t_2(x))$ とし，

$$\varepsilon = (\varepsilon_1(x), \varepsilon_2(x)) = (r_1(x)+t_1(x), r_2(x)+t_2(x))$$

とおく。r に対する式(3.13)～(3.15)のシンドロームは

$$A_1 = \varepsilon_1(\alpha)$$

$$A_3 = \varepsilon_1(\alpha^3) + \varepsilon_2(\alpha^3)$$

$$d = \varepsilon_2(1)$$

---

* このような考え方により，式(3.2)の $|J|_{max}$ の下界を僅かに改善できるが，ほとんどの場合，この改善は無意味である。

でちえられる。ただし，$g_{c2}(x)$ を $g_{c2}(\alpha^3)=1$ となるように選ぶものとする（このような $g_{c2}(x)$ が存在することについては 3.3.1 参照）。

$\mathcal{M}_{n,2}(J_2^*)$ が準完全符号であることをいうためには，このようなシンドロームの可能な任意の値に対し $W[\mathcal{E}] \leq 3$ となる $\mathcal{E}$ が存在することを証明すればよい。ここで，$\mathcal{E}$ とシンドロームの関係を求めていこう。

(1) $\sigma_1=0$，$\sigma_3=0$，$d=0$ となる必要十分条件は $\mathcal{E}=0$ となることである。

((1) の証明) 十分であることは明らか。必要であることを証明する。$\mathcal{M}_{n,2}(J_2^*)$ の符号語は

$$v = (b(x) + C(x)g_{c2}(x),\ C(x))$$

$$(b(x) \in B_{n,2},\quad C(x) \in C_{n,2}(J_2^*))$$

となる形であるが，$B_{n,2}$ は準完全符号であり[2]，$C_{n,2}(J_2^*)$ には J_2^* に対応する位置に重みが偶数となるあらゆるベクトルが含まれるから，任意の受信ベクトル W に対し

$$W[\mathcal{E}_1(x)] \leq 3,\quad W[\mathcal{E}_2(x)] \leq 1$$

となる $\mathcal{E}$ が存在する。ゆえに $\mathcal{E}$ としては重みが4以下の

ものを考えればよい。 $d=0$ であるから, $W[\varepsilon_2(x)]=0$, 2 または 4 となる。 $W[\varepsilon_2(x)]=0$ すなわち, $\varepsilon_2(x)=0$ のときは, $W[\varepsilon_1(x)] \leq 3$ ($B_{m,\pi}$ が準完全符号であるから). しかるに, $\beta_1=0$, $\beta_3=0$ から $\varepsilon_1(x)=0$ でなければならない。また $W[\varepsilon_2(x)]=2$ のときは $W[\varepsilon_1(x)] \leq 2$ となる $\varepsilon_1(x)$ を考えればよいが, $\beta_1=0$ から, $\varepsilon_1(x)=0$。したがって $\beta_3=0$ から $\varepsilon_2(\alpha^3)=0$ となり矛盾を生じる。同様に $W[\varepsilon_2(x)]=4$ とすると, $\varepsilon_2(\alpha^3)=0$ となり, J_2^* の定義から, これは不可能である。ゆえに, 常に $\varepsilon=0$ となる。

((1) の証明終)

以下の (2) ~ (6) は補題 3.8 ~ 3.13 とほとんど同様な手法によりきわめて容易に証明できる。

(2) $\beta_1 \neq 0$, $\beta_3 \neq 0$, $d=0$, $\beta_1^3+\beta_3=0$ となる必要十分条件は $\varepsilon_1(x)=x^h$, $\varepsilon_2(x)=0$ となることである。ここに h は $\beta_1=\alpha^h$ により定められる。

(3) $\beta_1 \neq 0$, $\beta_3 \neq 0$ $d=0$, $\beta_1^3+\beta_3 \neq 0$, $Tr[1+\beta_3\beta_1^{-3}]=0$ となる必要十分条件は $\varepsilon_1(x)=x^{h_1}+x^{h_2}$, $\varepsilon_2(x)=0$ となることである。ここに h_1, h_2 は $z^2+\beta_1 z+(\beta_1^3+\beta_3)/\beta_1$

$=0$ の解 α^{h_1}, α^{h_2} から定められる.

(4) $\rho_1=0$, $\rho_3\neq 0$, $d=0$ かつ $\rho_3=\alpha^{3h_1}+\alpha^{3h_2}$ となる $h_1, h_2 \in J_2^*$ が存在する必要十分条件は $\varepsilon_1(x)=0$, $\varepsilon_2(x)=x^{h_1}+x^{h_2}$ となることである.

(5) $\rho_1=0$, $\rho_3\neq 0$, $d=0$ かつ $\rho_3=\alpha^{3h}$ となる $h\in J_2^*$ が存在する必要十分条件は $\varepsilon_1(x)=0$, $\varepsilon_2(x)=x^h$ となることである.

(6) $\rho_1\neq 0$, $d=1$, $\rho_1^3+\rho_3=\alpha^{3h_2}$ となる $h_2\in J_2^*$ が存在する必要十分条件は $\varepsilon_1(x)=x^{h_1}$, $\varepsilon_2(x)=x^{h_2}$ となることである.

以上の (1)～(6) の場合は, いずれも ε が一意に定まり, $W[\varepsilon]\leq 2$ となる. このほかにシンドロームの値により, つぎのような場合を生じる可能性がある.

(3′) (3) において $Tr[1+\rho_3\rho_1^{-3}]\neq 0$ となる場合.

(4′) (4) において $h_1, h_2\in J_2^*$ となる h_1, h_2 が存在しない場合.

(5′) (5) において $h\in J_2^*$ となる h が存在しない場合.

(6′) (6) において $h_2 \in J_2^*$ となる h_2 が存在しない場合。

(7) $\alpha_1 = 0$, $\alpha_3 = 0$, $d = 1$ となる場合.

これらのいずれの場合にも, $W[\varepsilon] \leq 3$ となる ε が存在することを示す。

(3′) 任意の α_1, α_3 ($\in GF(2^n)$) に対し, $Tr[1+\alpha_3\alpha_1^{-3}] \neq 0$ のときは.

$$\alpha_1 = X_1 + X_2 + X_3$$

$$\alpha_3 = X_1^3 + X_2^3 + X_3^3$$

を満たす互いに異なり, かつ 0 でない X_1, X_2, X_3 ($\in GF(2^n)$) が存在することが証明されている (文献 (2), P. 425). このことから (3′) の場合, $W[\varepsilon_1(x)] = 3$, $\varepsilon_2(x) = 0$ となる ε の存在することは明らかである。

(4′) (3′) と同様にして, $W[\varepsilon_1(x)] = 3$, $\varepsilon_2(x) = 0$ となる ε の存在することが容易に導ける。

(5′) J_2^* の定義から, ただちに $\varepsilon_1(x) = 0$, $W[\varepsilon_2(x)] = 3$ となる ε の存在することが分る。

(6′) $\alpha_1^3 + \alpha_3 = \alpha^{3h_2}$ となる $h_2 \in J_2^*$ が存在しないような任意の α_1, α_3 ($\in GF(2^n)$) に対して,

$$\rho_1 = X_1 + X_2 \qquad (3.16)$$

$$\rho_3 = X_1^3 + X_2^3 + \alpha^\delta \qquad (3.17)$$

となる X_1, X_2 ($\in GF(2^n)$, $X_1 \neq X_2$, $X_1, X_2 \neq 0$) および, $\delta \in J_2^*$ が存在することを示そう。

$\gamma = \alpha^{3\delta} + \rho_3$ とおけば, 式 (3.16)(3.17) から,

$$X_1 X_2 = \gamma \rho_1^{-3}$$

ゆえに, X_1, X_2 は

$$z^2 + \rho_1 z + (\rho_1^3 + \gamma)\rho_1^{-1} = 0 \qquad (3.18)$$

の解である。この式が解をもつ必要十分条件は

$$Tr[(\rho_1^3 + \gamma)\rho_1^{-3}] = 1 + Tr[(\alpha^{3\delta} + \rho_3)\rho_1^{-3}] = 0 \qquad (3.19)$$

すなわち, $Tr[\alpha^{3\delta}\rho_1^{-3}] = Tr[\rho_3 \rho_1^{-3}]$ となることである。

ところで, J_2^* の定義から, $\{\alpha^{3\delta} \mid \delta \in J_2^*\}$ には $GF(2)$ の上で, 互いに独立な n 個の元が含まれていることが分る。ゆえに $\{\alpha^{3\delta}\rho_1^{-3} \mid \delta \in J_2^*\}$ にも $GF(2)$ の上で互いに独立な n 個の元が含まれ, $GF(2^n)$ の任意の元はそのような元の線形結合で表わせる。しかも, $GF(2^n)$ には Tr を 1 とするものが含まれるから[2], Tr が $GF(2^n)$ から $GF(2)$ の上へ

線形な写像であることに注意すれば，$Tr[\alpha^{3j}\rho_1^{-3}]=1$ となる $j\in J_2^*$ の存在することが分る。

一方，$\alpha^{3j_1}+\alpha^{3j_2}+\alpha^{3j_3}=0$ となる j_1, j_2, j_3 $(\in J_2^*)$ が存在するから，$Tr[\alpha^{3j}\rho_1^{-3}]=0$ となる $j\in J_2^*$ も存在する。

ゆえに，式(3.19)を満たす $j\in J_2^*$ は存在し，したがって式(3.19)には解 X_1, X_2 $(\in GF(2^m))$ が存在する。しかも $\rho_1\neq 0$，$\rho_1^3+\gamma=\rho_1^3+\rho_3+\alpha^{3j}\neq 0$ であるから，$X_1\neq X_2$，$X_1 X_2\neq 0$ である。このことは $W[\varepsilon_1(x)]=2$，$W[\varepsilon_2(x)]=1$ となる ε の存在することを意味する。

(ク) J_2^* の定義から $\varepsilon_1(x)=0$，$W[\varepsilon_2(x)]=3$ となる ε が存在する。

以上によって，あらゆるシンドロームの値に対し $W[\varepsilon]\leq 3$ となる ε の存在することが証明された。　(証明終)

本節で述べた二重誤り訂正三値準完全符号の構成法は，高らの方法[47]に比べると一般性に欠けるが，より簡単に構成できる。

最後に，本節の方法によって得られる準完全符号の簡単な例を示しておこう。

例5.1）二重誤り訂正準完全修正BCH符号の例：$n=5$ とし，$GF(2^5)$ の原始元 α を $1+\alpha+\alpha^3+\alpha^4+\alpha^5=0$ によって定める。このとき，たとえば，

$$J_2^* = \{0, 1, 2, 3, 4, 15, 18\}$$

と選ぶことができる。事実，$\beta=\alpha^3$ とおき，$\{\beta^j \mid j\in J_2^*\}$ を $GF(2)$ の上の5次元ベクトルとして表わせば，

$\beta^0=(1\,0\,0\,0\,0)$　　$\beta^4=(0\,0\,0\,0\,1)$

$\beta^1=(0\,1\,0\,0\,0)$　　$\beta^{15}=(1\,1\,1\,1\,1)$

$\beta^2=(0\,0\,1\,0\,0)$　　$\beta^{18}=(1\,1\,0\,0\,0)$

$\beta^3=(0\,0\,0\,1\,0)$

となり，明らかに，任意の四つの異なる元の和は0とならない。また，任意の $GF(2)$ の上の5次元ベクトルを，β^j（$j\in J_2^*$）または $\beta^{j_1}+\beta^{j_2}+\beta^{j_3}$（$j_1<j_2<j_3$，$j_1, j_2, j_3\in J_2^*$）となる形で表わせることも容易に確かめられる。

ゆえに，このような J_2^* を用いて，符号長38，情報ビット数27の二重誤り訂正準完全符号を作り得る。

3.7 むすび

本章前半では，修正 Preparata 符号（mP－符号）を定義し，その諸性質と復号法について述べた。

はじめに，mP－符号の符号長の上界と下界を求め，つぎに，mP－符号の最小距離が5となること，および mP－符号が非線形組織符号となることを示し，さらに mP－符号が BCH 符号の復号に類似した代数的方法で復号できることを示した。

また，mP－符号の中で符号化および復号がより簡単となる 0mP－符号を定義し，いくつかの例を示した（表 3.1）。

Preparata 符号と mP－符号によって，二重誤り訂正符号としては，かなり広範囲の符号長にわたり，きわめてすぐれた非線形符号が存在することが明らかとなった。今後の多重誤り訂正非線形符号の研究が期待される。

本章後半では，修正 BCH 符号を定義し，その符号長の上界と下界，最小距離，復号法について論じた。また，二重誤り訂正修正 BCH 符号には準完全符号となるものが存在することを明らかにした。

電気 47 II
受理 45.12.24

第4章

回線分離符号の構造と構成法

才2章と才3章では符号は誤り訂正のために用いられた。本章では符号は符号分割多重PCM通信方式において，回線を分離するために用いられる．それゆえ，ここでは距離は回線間の分離のよさを表わす量として定義される．

符号分割多重PCM通信方式は同一周波数帯域内に多数の回線を非同期多重化し，各回線に割り当てられた符号語（アドレス）によって回線を分離しようというものである．本章では，この通信方式において，アドレスとして用いられるのに適したものとして，回線間の相互干渉を一定値以下におさえるような性質をもつ符号 —— 回線分離符号を考え，その基礎的構造を代数的な面から明らかにする．また，回線分離符号の実用的な三種の構成法を示す．

4.1 はじめに

回線の多重化方式としては周波数分割多重化方式と時分割多重化方式がよく知られているが，このほかに符号分割多重化方式（非同期多重化方式）がある。この方式は同一周波数帯域内に多数の回線を非同期多重化し各回線に割り当てられた符号語（アドレス）によって回線を分離しようというものである。この方式の特長として，周波数帯域の利用効率がよいこと，加入者の通信系への接続が容易であること，通信系の構成が簡単であることなどがあげられ，これらの点から移動体間の通信方式としてすぐれていると考えられている。

さらに，この多重化方式をＰＣＭ回線に適用したものとして符号分割多重ＰＣＭ通信方式[51][52][53]がある。これはＰＣＭ系列（ＰＣＭ符号器の出力の二値系列）の各ディジットに各回線に固有な一定長の二値符号語をアドレスとして割り当て，搬送波をこのアドレスによって２相ＰＭすることにより回線を分離する方式で，特に，移動体間の衛星通信方式として提案されたものである。本章はこの符号分割多重ＰＣＭ通信方式に用いられる，回線を分離するための符号への応用を目的

として，特殊な性質をもつブロック符号を数学的に定義し，その構造と構成法について論じたものである。

つぎに，回線分離のための符号に要求される性質について述べる。ある回線に割り当てられた二値符号語を $v=(v_0, v_1, \cdots, v_{n-1})$ としよう。また集合 $\{0, 1\}$ における v_i の補元を $\bar{v}_i$ で表わし，$(\bar{v}_0, \bar{v}_1, \cdots, \bar{v}_{n-1})$ を $\bar{v}$ と書くことにする。このとき符号分割多重ＰＣＭ通信方式はＰＣＭ系列の０に対しては v を，１に対しては $\bar{v}$ を対応させる。たとえば，ＰＣＭ系列が０１１０… であれば $v_0 \cdots v_{n-1}\ \bar{v}_0 \cdots \bar{v}_{n-1}\ \bar{v}_0 \cdots \bar{v}_{n-1}\ v_0 \cdots v_{n-1} \cdots$ となる二値系列を作る。このようにして得られた v と $\bar{v}$ からなる二値系列によって搬送波を２相ＰＭして送出する。受信側では搬送波を v によって２相ＰＭした局部信号を用いて相関受信を行ない，ＰＣＭ系列の各ディジットを復調する。

このような原理により，同一周波数帯域内に多数の回線を非同期多重化した場合の最も大きな問題は回線間の相互干渉である。ここでは議論を簡単にするために各回線の搬送波は同一の周波数をもつとする。このとき，回線間の相互干渉を

小さくするためには各回線にアドレスとして割り当てられる符号が適当な条件を満たす必要がある。要約すれば，すべての回線にアドレスとして割り当てられた二値符号語の集合をCとすると，Cはつぎの二つの性質をもつことが必要である。

(i) Cの任意の符号語 $v=(v_0, v_1, \cdots, v_{n-1})$ の成分を任意に巡回置換して得られる $u=(v_i, \cdots, v_{n-1}, v_0, \cdots, v_{i-1})$ $(i=0, 1, \cdots, n-1)$ および $\bar{u}$ とCのv以外のすべての符号語とのハミング距離が定められた値より小さくならない。

(ii) Cの任意の符号語 v と $\bar{v}$ を連ねてできる長さnの系列 $w=(v_i, \cdots, v_{n-1}, \bar{v}_0, \cdots, \bar{v}_{i-1})$ $(i=0, 1, \cdots, n-1)$ および $\bar{w}$ とCのv以外のすべての符号語とのハミング距離が定められた値より小さくならない。

(i)はある回線においてPCM系列の継続する二のディジットが00または11であるとき，その回線の送信信号と他の回線の受信機における局部信号との相関を一定値以下におさえるために必要な条件であり，(ii)はPCM系列の継続する二つのディジットが，01または10であるときの相関をおさえるための条件である。

本章では，このような二つの性質をもつ二値ブロック符号Cを回線分離符号と呼び，はじめにその構造の基礎となる二値ベクトル空間の代数的構造について論じ，次いでこの符号の3種の構成法を示す。

本章の回線分離符号に類似した符号として，Gilbertの提案した cyclically permutable error-correcting code[54][55]がある。これは(i)の条件は満たすが，(ii)の条件を考慮していないために，符号分割多重PCM通信方式に応用することはできない。

なお，本章においては複雑な補題の証明，式の導出等は一括して4.6節に示す。

4.2 回線分離符号の定義

本節では回線分離符号を数学的に明確に定義する。

各成分がGF(2)(各元を0，1で表わす)に属するn次元ベクトルすべての集合をB_nとする。また$v_i \in GF(2)$の補元を$\bar{v}_i$で表わし，$v=(v_0, v_1, \cdots, v_{n-1}) \in B_n$に対して$\bar{v}=(\bar{v}_0, \bar{v}_1, \cdots, \bar{v}_{n-1})$をvの補符号語と呼ぶことにする。ここで$B_n$の

上のつぎの二つの作用素を定義する。

$$S: v=(v_0, \cdots, v_{n-1}) \to Sv=(v_{n-1}, v_0, \cdots, v_{n-2})$$

$$T: v=(v_0, \cdots, v_{n-2}) \to Tv=(v_{n-1}, v_0, \cdots, v_{n-2})$$

$$(v \in B_n)$$

Sを巡回置換作用素，Tを反転巡回置換作用素と呼ぼう。また，S, Tのべき乗の作用素S^i, T^i（i：正整数）をつぎのように定義する。

$$S^i: v \to S^i v = \overbrace{S(S(\cdots(S}^{i} v))\cdots)$$

$$T^i: v \to T^i v = \overbrace{T(T(\cdots(T}^{i} v))\cdots)$$

$$(v \in B_n)$$

このときT^i（i：正整数）はS^iによって

$$T^i v = S^i v + e_0 + e_1 + \cdots + e_{i-1} \qquad (\forall v \in B_n)$$

と書ける。ここにe_jは$(j \bmod n)+1$番目の成分が1で他が0の単位ベクトルである。さらに$S^0=T^0=I$（恒等作用素）としよう。$S^n=T^{2n}=I$であるから，$S^i(i=0, 1, \cdots)$のうち異なるものはn個，$T^i(i=0, 1, \cdots)$のうち異なるものは$2n$個である。これらの作用素の集合をそれぞれΣ, $\mathbb{T}$とすれば，

$$\Sigma=\{S^i \mid i=0, 1, \cdots, n-1\}, \quad \mathbb{T}=\{T^i \mid i=0, 1, \cdots, 2n-1\}$$

と書ける。ここで，S^i, $S^j \in \Sigma$ の積 $S^i \cdot S^j$ を $(S^i \cdot S^j)v = S^i(S^j v)$ $(^\forall v \in B_n)$ によって定義すれば，明らかに Σ はこの積に関して巡回群となる。また，T において同様に積を定義すれば T も巡回群となる。

二つのベクトル v, $u \in B_n$ に対し，$v = S^i u$ となる $S^i \in \Sigma$ が存在するとき，v と u は Σ－共役であるという。すべての互いに Σ－共役な B_n の元の集合を σ－同値類と呼び，σ_i（i：正整数）または，それに含まれる一つの元（代表元）v を用いて $\sigma(v)$ と表わそう。同様に T によって τ－同値類を定義して τ_i または $\tau(v)$ で表わす。これらは重複を許して

$$\sigma(v) = \{ S^0 v,\ S^1 v,\ \cdots,\ S^{n-1} v \}$$

$$\tau(v) = \{ T^0 v,\ T^1 v,\ \cdots,\ T^{2n-1} v \}$$

と書ける。さらに，$\sigma(v) \cup \sigma(\bar{v})$ を σ'－同値類と呼び σ'_i または $\sigma'(v)$ で表わす。このとき，二つのベクトル v, $u \in B_n$ の間の“距離”をつぎのように2種定義する。

$$d'_\sigma(v, u) = \min_{\substack{x \in \sigma'(v) \\ y \in \sigma'(u)}} W[x + y] \qquad (4.1)$$

$$d_\tau(v, u) = \min_{\substack{x \in \tau(v) \\ y \in \tau(u)}} W[x + y] \qquad (4.2)$$

ここに $W[x]$ は x の重み（成分中の1の数）を示す。$d_\sigma(v,u)$ を σ-距離，$d_\tau(v,u)$ を τ-距離と呼ぼう。また二つの同値類間に次式で距離を定義する。

$$d_\sigma[\sigma(v),\sigma(u)] = d_\sigma(v,u) \qquad (4.3)$$

$$d_\tau[\tau(v),\tau(u)] = d_\tau(v,u) \qquad (4.4)$$

これらの定義が代表元のとり方によらないことは明らかであろう。S, T および距離の定義からただちにつぎの2式が導ける。

$$d_\sigma[v,u] = \min_{x\in\sigma(u)} W[v+x] \qquad (4.5)$$

$$d_\tau[v,u] = \min_{x\in\tau(u)} W[v+x] \qquad (4.6)$$

以上の準備の下に回線分離符号を定義する。二値ベクトルの集合 $C(\subset B_n)$ に属する任意の二つのベクトル v, u が，$d_\sigma(v,u)>0$, $d_\tau(v,u)>0$ を満たすとき C を回線分離符号という。また，

$$d_{\sigma\min} = \min_{\substack{v,u\in C\\ v\neq u}} d_\sigma(v,u) \qquad (4.7)$$

$$d_{\tau\min} = \min_{\substack{v,u\in C\\ v\neq u}} d_\tau(v,u) \qquad (4.8)$$

をそれぞれ δ'－最小距離，τ－最小距離と呼ぼう。このとき，次式の d_{min} をこの符号の最小距離という。

$$d_{min} = \min [d_{\delta' min}, d_{\tau min}] \qquad (4.9)$$

さらに，一定の最小距離に対し，最大の符号語数をもつ回線分離符号を最適回線分離符号と呼ぶ。

4.3 δ'－同値類と τ－同値類の構造

前節の定義から分かるように回線分離符号の構造の基礎となるものは δ'－同値類と τ－同値類である。本節ではこれらの同値類の構造について考察する。

4.3.1 δ'－同値類と τ－同値類の数

本項では B_n における δ'－同値類と τ－同値類の数を求めよう。

はじめに，n が奇数の場合を考える。このとき，異なる $2i$ 個の元をもつ δ'－同値類の数を $n_\delta^\circ(2i)$ とする。i は明らかに n の約数でなければならない。一般に i が n の約数であることを $i|n$ と表わす。n が奇数のときは $\delta(v)$ と $\delta(\bar{v})$ が異な

るから，$n_\sigma^\circ(2i)$ は i 個の異なる元をもつ σ－同値類の数の $1/2$ に等しい。σ－同値類の数は，Möbius の反転公式[2]を用いれば，きわめて容易に計算できて，結局次式を得る。

$$n_\sigma^\circ(2i) = \sum_{j|i} \frac{1}{2i} \mu(j) 2^{i/j} \quad (i|n) \qquad (4.10)$$

ここに $\mu(j)$ は Möbius 関数[2]で，総和は i を割り切るすべての正整数 j についてとることを意味する。これを用いると B_n における σ'－同値類の数 $N_\sigma^\circ(n)$ はつぎのようになる。

$$N_\sigma^\circ(n) = \sum_{i|n} n_\sigma^\circ(2i) \quad (n: odd) \qquad (4.11)$$

n が奇数のときはつぎの補題によって τ－同値類と σ'－同値類を 1 対 1 に対応づけることができる。しかも，互いに対応する同値類に含まれる元の数は等しい。

補題 4.1：n が奇数のとき $T^n x + x = 0 = (0, 0, \cdots, 0)$ を満たす B_n の元の一つを g_0 とすれば任意の $v \in B_n$ に対し，つぎの 2 式が成立する。

$$\sigma'(v) + g_0 = \{x + g_0 / x \in \sigma'(v)\} = \tau(v + g_0) \qquad (4.12)$$

$$\tau(v) + g_0 = \{y + g_0 / y \in \tau(v)\} = \sigma'(v + g_0) \qquad (4.13)$$

証明は 4.6.1 に示す。この補題から，$2i$ 個 $(i|n)$ の異な

る元をもつて一同値類の数 $n_e^{\circ}(2i)$ は $n_o^{\circ}(2i)$ に等しく，またて一同値類の総数 $N_e^{\circ}(n)$ は $N_o^{\circ}(n)$ に等しいことがわかる。

つぎに n が偶数の場合を考えよう。このとき $n = 2^l n_o$ と書ける。ここに l は正整数で，n_o は奇数である。このときも σ-同値類の数から σ'-同値類の数を求めることができるのであるが，n が偶数であるために $\sigma(\nu) = \sigma(\bar{\nu})$ となる σ-同値類が存在し，それゆえ $\sigma'(\nu) = \sigma(\nu)$ となることがある。この点に注意すれば，一つの σ'-同値類に含まれる元の数は i を n_o の約数として $2^{k+1}i$ $(k = 0, 1, \cdots, l)$ となり，$2^{k+1}i$ 個の元をもつ σ'-同値類の数 $n_o^{e}(2^{k+1}i)$ は

$$n_o^{e}(2^{k+1}i) = \begin{cases} \dfrac{1}{i}\sum_{j \mid i} \mu(j) 2^{i/j} & ; k = 0 \\ \dfrac{1}{2^{k+1}i}\left\{ \sum_{j \mid 2^k i} \mu(j) 2^{\frac{2^k i}{j}} + \sum_{j \mid i} \mu(j) 2^{\frac{2^{k-1}i}{j}} \left(2^{\frac{2^{k-1}i}{i}} - 1\right) \right\} & ; 0 < k < l \\ \dfrac{1}{2^{l+1}i}\left\{ \sum_{j \mid 2^l i} \mu(j) 2^{\frac{2^l i}{j}} - \sum_{j \mid i} \mu(j) 2^{\frac{2^{l-1}i}{i}} \right\} & ; k = l \end{cases}$$

$(i \mid n_o)$ (4.14)

となることが容易に導ける（4.6.2参照）。またσ'-同値類の総数$N_\sigma^e(n)$はつぎのようになる。

$$N_\sigma^e(n) = \sum_{k=0}^{l} \sum_{i \mid n_0} n_\sigma^e(2^{k+1} i) \quad (n = 2^l n_0) \qquad (4.15)$$

一方，一つのτ-同値類に含まれる元の数はiをn_0の約数として$2^{l+1} i$となり，$2^{l+1} i$個の元をもつτ-同値類の数$n_\tau^e(2^{l+1} i)$はつぎのようになる（4.6.3参照）。

$$n_\tau^e(2^{l+1} i) = \sum_{j \mid i} \frac{1}{2^{l+1} i} \mu(j) 2^{\frac{2^l i}{j}} \quad (i \mid n_0) \qquad (4.16)$$

τ-同値類の総数$N_\tau^e(n)$はこれを用いて，

$$N_\tau^e(n) = \sum_{i \mid n_0} n_\tau^e(2^{l+1} i) \quad (n = 2^l n_0) \qquad (4.17)$$

と書ける。さらに，式(4.15)，(4.17)から容易に

$$N_\sigma^e(n) - N_\tau^e(n) = \sum_{k=1}^{l} \sum_{i \mid n_0} n_\tau^e(2^k i) > 0$$

となることが導ける。すなわち，nが偶数の場合は，B_nにおいてσ'-同値類がτ-同値類よりも多い。

本項ではB_nにおけるσ'-同値類とτ-同値類の構造をその個数の面から明らかにした。本項の結果は4.4で最小距離が1の最適回線分離符号の符号語数を評価する際に用いられる。

4.3.2 δ'-同値類とτ-同値類の距離構造

本項ではδ'-同値類間の式(4.3)で定義される距離の構造およびτ-同値類間の式(4.4)で定義される距離の構造について調べる。

はじめに，δ'-同値類の距離構造について考えよう。nを法とする既約剰余類[10]の作る乗法群をR_nとし，その元をnより小さい正整数で表わすことにする。R_nの位数(元の数)は$\varphi(n)$である。ただしφは Euler のφ関数[8]である。$r \in R_n$に対応してつぎのようなB_nの上の作用素を定義する。

$$P_r : v = (v_0, \cdots, v_{n-1}) \to P_r v = (v_{\lambda_0}, v_{\lambda_1}, \cdots, v_{\lambda_{n-1}})$$

$$\lambda_i = r^{-1} i \bmod n \quad (r \in R_n,\ v \in B_n)$$

この作用素のつぎの性質は容易に導ける。

(a). P_rはベクトルの成分の置換を与える。

(b). $\{P_r / r \in R_n\}$は積に関して群をなす。これをΠとしよう。ΠとR_nはP_rをrに対応させることによって同形となる(Πにおける"積"は4.2に示したΣにおける積と同様に定義される)。

(c). $S^i P_r v = P_r S^{r^{-1} i} v \quad (\forall v \in B_n)$

任意の σ' 一同値類 $\sigma'(v)$ に対し $\{P_r x \mid x \in \sigma'(v)\}$ を $P_r\sigma'(v)$ と書くと (c) からつぎの性質が導ける。

(d). $P_r\sigma'(v) = \sigma'(P_r v)$ $(^\forall v \in B_n)$

この性質から P_r をすべての σ' 一同値類の集合 Ω'_σ の上の作用素と考えることができる。ここで σ_i', $\sigma_j' \in \Omega'_\sigma$ に対し $P_r\sigma_i' = \sigma_j'$ となる $P_r \in \Pi$ が存在するとき σ_i' と σ_j' は Π 一共役であるといい，互いに Π 一共役な σ' 一同値類すべての集合を Π 一同値類と呼ぶことにする。Π 一同値類はその一つの元 σ_i' を用いて $\{P_r\sigma_i' \mid r \in R_n\}$ と表わせる。ただし，この中には重複するものもある。

(a), (c), (d) を用いれば σ' 一同値類の距離構造に関するつぎの定理が直ちに導ける。

定理 4.2： Ω'_σ におけるすべての Π 一同値類から一つづつ任意に σ' 一同値類を選ぶ。これを σ_1', σ_2', ..., σ_l' としよう。ここに l は Ω'_σ における Π 一同値類の数である。このとき σ_i' $(1 \leq i \leq l)$ を含む Π 一同値類に含まれる任意の σ' 一同値類 $P_r\sigma_i'$ $(r \in R_n)$ と他のすべての σ' 一同値類との σ' 一距離は σ_i' と他のすべての σ' 一同値類との σ' 一距離によってつぎのよう

に定まる。

$$d_{\sigma'}[P_r\sigma_i', P_{r'}\sigma_j'] = d_{\sigma'}[\sigma_i', P_{r'r^{-1}}\sigma_j']$$

$$r, r' \in R_{2l}\ ]\ \leq i, j \leq k \qquad (4.18)$$

つぎにて一同値類の距離構造について考えよう。lが奇数のときはつぎの定理によって，て一同値類とσ'一同値類の距離構造を完全に対応づけることができる。

定理 4.3： lが奇数のとき $T^2\chi + \chi = 0$を満たすB_{2l}の元の一つをg_0とする。このとき任意の二つのて一同値類$\tau(v)$, $\tau(u)$の間のて一距離は$\sigma'(v+g_0)$と$\sigma'(u+g_0)$の間のσ'一距離に等しい。すなわち，

$$d_\tau[\tau(v), \tau(u)] = d_{\sigma'}[\sigma'(v+g_0), \sigma'(u+g_0)] \qquad (4.19)$$

証明は補題 4.1と距離の定義から明らかであろう。

lが偶数のときは，このような簡単なて一同値類とσ'一同値類との対応関係はない。しかし，このときにも，て一同値類の距離構造について定理 4.2に対応する定理を導くことができる。

$2l$を法とする既約剰余類の作る乗法群をR_{2l}とし，その元を$2l$より小さい正整数で表わすことにする。R_{2l}の位数

は $\varphi(2n)$ である。$r \in R_{2n}$ に対応して B_n の上の作用素 Q_r をつぎのように定義する。

$$Q_r : v = (v_0, \cdots, v_{n-1}) \to Q_r v = (v_{\lambda_0}, v_{\lambda_1}, \cdots v_{\lambda_{n-1}})$$

$$\lambda_i = r^{-1} i \bmod n \quad (r \in R_{2n},\ v \in B_n)$$

Q_r が P_r と同様 (a), (b), (c) の性質をもつことはただちに確かめられる。ここで，つぎの2式を満たすベクトルの集合 $\{h_r \mid r \in R_{2n}\}$ $(\subset B_n)$ を導入しよう。

$$(I+S) h_r = Q_r (e_1 + e_2 + \cdots + e_{r-1-1}) \quad (r \in R_{2n}) \quad (4-20)$$

$$Q_r h_{r'} + h_r = h_{rr'} \quad (r, r' \in R_{2n}) \quad (4-21)$$

このような $\{h_r \mid r \in R_{2n}\}$ が存在することは容易に証明できる（4.6.4 参照）。この h_r と Q_r を用いて B_n の上の作用素、F_r をつぎのように定義する。

$$F_r : v \longrightarrow F_r v = Q_r v + h_r \quad (r \in R_{2n},\ v \in B_n)$$

F_r は v 一同値類に対し，v' 一同値類に対する P_r の性質と同じような性質をもつ。事実，P_r の性質 (b), (c), (d) に対応してつぎの性質を証明できる（4.6.5 参照）。

(b'). $\{F_r \mid r \in R_{2n}\}$ は積に関して群をなす。これを $\mathfrak{D}$ とする。$\mathfrak{D}$ と R_{2n} は F_r を r に対応させることによって同形となる。

(c'). $T^i F_r v = F_r T^{r-1} v$ ($\forall v \in B_n$)

(d'). $F_r \tau(v) = \tau(F_r v)$ ($\forall v \in B_n$)

(d')からすべてのτ一同値類の集合Ω_τにおいてΦ一同値類をΠ一同値類と同様に定義できることがわかる。Φ一同値類はその一つの元τ_iを用いて$\{F_r \tau_i / r \in R_{2n}\}$と書ける。

このとき，定理4.2に対応する定理はつぎのようになる。

定理4.4：Ω_τにおけるすべてのΦ一同値類から一つづつ任意にτ一同値類を選ぶ。これを$\tau_1, \tau_2, \cdots, \tau_l$としよう。$l$は$\Omega_\tau$におけるΦ一同値類の総数である。このとき，$\tau_i$ ($1 \leq i \leq l$)を含むΦ一同値類に含まれる任意のτ一同値類$F_r \tau_i$ ($r \in R_{2n}$)と他のすべてのτ一同値類とのτ一距離はτ_iと他のすべてのτ一同値類とのτ一距離によってつぎのように定まる。

$$d_\tau [F_r \tau_i, F_{r'} \tau_j] = d_\tau [\tau_i, F_{r' r^{-1}} \tau_j]$$

$$r, r' \in R_{2n} \quad 1 \leq i, j \leq l \qquad (4.22)$$

(証明) $v \in \tau_i$とする。このとき

$$d_\tau [F_r \tau_i, F_{r'} \tau_j] = \min_{x \in \tau_j} W[Q_r v + h_r + Q_{r'} x + h_{r'}]$$

$$= \min_{x \in \tau_j} W[v + Q_{r^{-1}} h_r + Q_{r' r^{-1}} x + Q_{r^{-1}} h_{r'}]$$

式(4.21)から $Q_{r-1}h_r + Q_{r-1}h_{r'} = P_{r'r-1}$ となるから

$$= \min_{x \in \mathcal{X}} W[v + F_{r'r-1}x]$$

$$= d_\tau[\tau_i, F_{r'r-1}\tau_j] \qquad \text{(証明終)}$$

本項では δ' 一同値類と τ 一同値類の距離構造を調べ，定理4.2，4.3，4.4を得た。これらの定理は回線分離符号を計算機で探索する際に有用となろう。たとえば，最適回線分離符号を探索するためには，δ' 一同値類間の δ' 一距離と τ 一同値類間の τ 一距離を計算する必要があるが，これは定理4.2，4.3，4.4を用いてある程度簡単化できる。しかし，最適回線分離符号の探索にはぼう大な計算量を要し，そのような簡単化を行なってもL=10以上の最適な符号を求めるのは非常にむずかしい。

4.4 最小距離が1の最適回線分離符号

最小距離が1の回線分離符号は実用上の興味には乏しい。しかし，現在のところ，最適回線分離符号について，その符号語数をかなり詳しく知ることのできるのは最小距離が1のものだけである。本節では，この符号の符号語数の上界と下

界を求める。

はじめに符号長 n が奇数の場合を考えよう。最小距離が1の回線分離符号はその任意の二つの符号語が異なる σ-同値類および τ-同値類に属す。したがって最小距離が1の最適回線分離符号の符号語数 M_n は B_n における σ-同値類の数 $N_\sigma^\circ(n)$, τ-同値類の数 $N_\tau^\circ(n)$ のいずれよりも大きくない。すなわち,

$$M_n \leq N_\tau^\circ(n) = N_\sigma^\circ(n)$$

つぎに, M_n の下界を求めるために B_n のつぎのような2種の類別を考える。両方の類別ともに, 一つの類は $2n$ 個以下の元をもち, その他のすべての類は $2n$ 個の元をもつようにする。また, 才1の類別においては $2n$ 個の元をもつすべての σ-同値類を類とし, 才2の類別においては $2n$ 個の元をもつすべての τ-同値類を類とするものとする。明らかに $2^{n-1}/n$ 以下の任意の正整数 i について一方の類別の $i+1$ 個の類が他方の類別の i 個の類の和集合に含まれることはない。したがって, 2種の類別に関する定理(たとえば文献(10) p.55)から両方の類別に共通な完全代表系(すべての類から一つづ

つ代表元を選んで作った集合）が存在することがわかる。この代表系に属する代表元のうち，二つの類別に関して $2n$ 個の元をもつ δ 一同値類および t 一同値類を代表する元だけを選べば，これは明らかに回線分離符号となる。$2n$ 個の元をもつ δ 一同値類と t 一同値類の数は等しく $n_\delta^\circ(2n)$（式(4.10)）となる。このとき，この回線分離符号の符号語数 m' が

$$m' \geq [2n_\delta^\circ(2n) - 2^{n-2}/n]$$

を満たすことは明らかであろう。ここに［ ］はガウス記号である。$m \geq m'$ であるから，結局次式を得る。

$$[2n_\delta^\circ(2n) - 2^{n-2}/n] \leq m \leq N_t^\circ(n) \qquad (4.23)$$

n が具体的に与えられると多くの場合，式（4.23）の導出に用いた2種の類別を $2n$ 個以下の元をもつ δ 一同値類と t 一同値類も考慮に入れてもう少し詳しく定めることにより，式(4.23)の下界を多少改善することができる。特に，n が3以上の素数のときは $m = 1 + (2^{n-2} - 1)/n$ となることが容易に導ける。

n が偶数の場合も奇数の場合もほとんど同様にして最小距離が1の最適回線分離符号の符号語数 m は

$$[n_0^e(2n)+n_2^e(2n)-2^{n-1}/n] \le m \le N_2^e(n) \qquad (4.24)$$

を満たすことが導ける。ここに $n_0^e(2n)$, $n_2^e(2n)$, $N_2^e(n)$ はそれぞれ式 (4.14), (4.16), (4.17) で与えられている。この場合もれが具体的に与えられると m の下界を改善することができる。特に, $n=2^k$ のときには $m=2^{n-1}/n$ となることは容易に確かめられる。

つぎに, n が十分大きいときの m の値について考えよう。このときには, 式 (4.23), (4.24) の上界と下界のすべてについて, その最大の項は $2^{n-1}/n$ となり, それ以外の項の和の絶対値は $2^{[n/2]}$ 以下であることが容易にわかる。したがって, 式 (4.23), (4.24) の上界, 下界は n が十分大きいとき $2^{n-1}/n$ で近似できる。すなわち, このとき $m \approx 2^{n-1}/n$ となる。

表 4.1 に $n=3\sim19$ の範囲の最小距離が 1 となる最適な回線分離符号の符号語数の上界と下界を示す。下界については, 式 (4.23), (4.24) によって計算されたものと, これらの式を導出する際に用いた二種の類別を $2n$ 個以下の元をもつ同値類と一同値類をも考慮に入れて, さらに詳しく定めることにより改善された下界とを示してある。この表から, 分

るように最小距離が1の最適回線分離符号の符号語数は，その上界，下界ともにきわめて $2^{n-1}/n$ に近い値をとる。

表 4.1 最小距離が1の最適な回線分離符号の符号語数

n	d'-同値類の数	符号語数			$2^{n-1}/n$
		上界 (t'-同値類の数)	下界		
			改善された下界	式 (4.23) (4.24)	
* 3	2	2	2	1	1.3
* 4	4	2	2	0	2.0
* 5	4	4	4	3	3.2
* 6	8	6	6	3	5.3
* 7	10	10	10	9	9.2
* 8	19	16	16	12	16.0
* 9	30	30	30	28	28.4
* 10	56	52	52	47	51.2
* 11	94	94	94	92	93.1
12	180	172	171	164	170.7
* 13	316	316	316	312	315.1
* 14	596	586	586	575	585.1
15	1095	1095	1093	1088	1092.3
* 16	2068	2048	2048	2032	2048.0
* 17	3856	3856	3856	3854	3855.1
18	7316	7286	7282	7250	7281.8
* 19	13798	13798	13798	13796	13797.1

* 印は符号語数の上界と下界が一致するものを示す。

4.5 回線分離符号の構成法

本節では回線分離符号の3種の構成法を示す。これらの構

成法によっては必ずしも最適回線分離符号を構成することはできないが，十分実用に供し得る符号を作ることができると思われる。

4.5.1 巡回符号からの構成法

符号長 n が奇数の二値巡回符号を考える。このような符号は生成多項式 $g(x)$ によって特性づけられるが，また 1 の原始 n 乗根[7]の一つ α と l 個の互いに異なる整数の組 $\rho_1, \rho_2, \cdots, \rho_l$ $(0 \leq \rho_i < n)$ を指定することによって特性づけることもできる。それには $\alpha^{\rho_1}, \alpha^{\rho_2}, \cdots, \alpha^{\rho_l}$ を根として含む $GF(2)$ 上の最小次数の多項式を $g(x)$ とすればよい。ただし $\rho_1, \cdots, \rho_l$ は $\alpha^{\rho_1}, \cdots, \alpha^{\rho_l}$ の位数の最小公倍数が n となるように定められているとする。たとえば，BCH符号は $n = 2^t$ (t：正整数)，$\rho_i = i$ $(i = 1, 2, \cdots, 2t)$ となる符号である。

回線分離符号を構成するためには，$\rho_i \neq 0$ $(i = 1, \cdots, l)$ となる二値巡回符号を用いる。このことは $g(x)$ に $1+x$ が因数として含まれないこと，したがって符号語としてすべて

の成分が1のベクトル 1^n が含まれることを意味する(1)。上記の巡回符号は群符号であるから，このとき任意の符号語 b に対し，その補符号語 $b' = b + 1^n$ もまた符号語となる。このことから，任意の符号語 b に対し $\sigma'(b)$ がこの符号に含まれることがわかる。このような符号から回線分離符号をつぎのようにして作ることができる。

構成法 1：符号長が n（奇数），最小距離が d_0（$d_0 \geq 3$）で生成多項式に $1+x$ を因数として含まない二値巡回符号を $C_0(n, d_0)$ とする。$C_0(n, d_0)$ に含まれるすべての σ' 同値類から一つづつ符号語を取り出して作った符号語の集合を C_1 とすると，C_1 は回線分離符号となる。

はじめに，C_1 が回線分離符号となることを示す。C_1 の構成法から，C_1 の σ' 最小距離 d'_{min} が d_0 に等しいことは明らかである。すなわち，

$$d'_{min} = d_0 \qquad (4.25)$$

一方，C_1 の τ 最小距離 $d_{\tau min}$ は 4.6.6 に示すように次式を満たす。

$$d_{\tau min} \geq [(d_0+1)/2] - 1 \qquad (4.26)$$

ここに[ ]はガウス記号である。式(4.25), (4.26) および仮定 $d_0 \geq 3$ から C_2 は回線分離符号となり，その最小距離 d_{min} が次式を満たすことがわかる。

$$d_0 \geq d_{min} \geq [(d_0+1)/2] - 1 \qquad (4.27)$$

つぎに C_2 の符号語数 M を求める。M は $C_0(n, d_0)$ に含まれる σ 一同値類の個数に等しく，これは n が奇数であるから $C_0(n, d_0)$ に含まれる σ 一同値類の数の 1/2 である。巡回符号の σ 一同値類の数はすでに求められているが[56]，ここではよりまとまった形を示しておこう。導出は基本的には文献(56)と同一であり，生成多項式の根の構造を調べることによって，行なえる。1から $n-1$ までの整数の集合を N とする。N の二つの元 i, j に対し $i = 2^p j \bmod n$ となる整数 p が存在するとき $i \sim j$ と書く。$i \sim j$ となる関係は同値関係であるから，N をこれによって類別できる。このときの各類を N_i ($i = 1, 2, \cdots$) とし，またそれぞれの類に含まれる元の数を m_i ($i = 1, 2, \cdots$) とする。ここで，n および l 個の整数 $\rho_1, \rho_2, \cdots, \rho_l$ によって定まるつぎのような整数関数を定義する。

$$\nu(j; n, \rho_1, \cdots, \rho_l) = \sum_{N_i \cap E(j) \neq \phi} m_i$$

ここに $E(j)$ は $n/GCD(\rho_i, n)$ (GCD は最大公約数を示す) が j を割り切るような ρ_i の集合である。

また Φ は空集合を示す。ここで，本項はじめに述べたようにして $C_0(n, d_0)$ が $\rho_1, \cdots, \rho_e$ によって特性づけられているとしよう。このとき $C_0(n, d_0)$ に含まれる σ 一同値類の数，すなわち C_1 の符号語数 m は

$$m = \sum_{\substack{j,i \\ j \mid i \mid n}} \frac{1}{2i} \mu(j) \cdot 2^{i/j - \nu[(i/j)n, \rho_1, \cdots \rho_e]} \qquad (4.28)$$

となる。この式はやや複雑であるが，k_0 を $C_0(n, d_0)$ の情報ビット数とするとき，m が

$$m \geq [(2^{k_0-1})/n] + 1 \qquad (4.29)$$

を満たすことは明らかであろう。

以上で，巡回符号から構成法1によって最小距離 d_{min} が式 (4.27) を満たし，符号語数 m が式 (4.28) で与えられる回線分離符号を構成できることがわかった。表 4.2 に BCH 符号から得られる回線分離符号の符号語数と，最小距離の上界，下界の例を示す。表中“実現できる最小距離”の欄には実際に BCH 符号の σ 一同値類から符号語をランダムに選ん

で作った2〜6種の回線分離符号のd_{min}の最大の値を示してある。

式(4.27), (4.29)から，任意に与えられたd°_{min}, m°に対し，適当な巡回符号を選べば，構成法1によって$d_{min} \geq d^{\circ}_{min}$, $m \geq m^{\circ}$となる回線分離符号を構成できることがわかる。この意味で構成法1はかなり一般的な構成法といえよう。しかし必ずしもよい回線分離符号が得られるとは限らない。たとえば，表4.2で$n=15$, $m=72$, $d_{min}=1$となる符号が実際に得られているが，4.4の結果を用いると$n=15$, $d_{min}=1$の最適回線分離符号の符号語数は10^{93}ないし10^{95}となり，約15倍の符号語数をもつことがわかる。

ところで，構成法1は巡回符号の個々のd'-同値類からの符号語の選び方を指定していない。この選び方によっては，d_{min}式を(4.27)の範囲内で大きくすることも可能である。構成法1を改善するためには，そのような符号語の選び方を見出す必要があり，これは今後に残された問題である。

表4.2 BCH符号から構成した回線分離符号

符号長 (n)	符号語数 (m)	最小距離 (d_{min})		実現できる最小距離
		上界	下界	
15	72	3	1	1
15	6	5	2	3
31	34	11	5	6
63	10	27	13	19
127	130	55	27	40

4.5.2 コンマフリー符号からの構成法

符号長nのブロック符号Cから任意の符号語v, uを取り出したとき, $v=(v_0, v_1, \cdots, v_{n-1})$, $u=(u_0, u_1, \cdots, u_{n-1})$を連ねてできる長さ$n$の系列$(v_i, v_{i+1}, \cdots, v_{n-1}, u_0, \cdots, u_{i-1})$ $(i=1, 2, \cdots, n-1)$とCのすべての符号語とのハミング距離の最小値をd_cとする。$d_c>0$のときCをコンマフリー符号と呼び, d_cをコンマフリー指数という。この定義からコンマフリー符号を用い, つぎのようにして回線分離符号を構成できることがわかる.

コンマフリー指数がd_cで, すべての符号語に対しその補符号語を含む二値コンマフリー符号を二つの互いに共通元をもたない集合に分割し, どちらの集合も他の集合に含まれるす

べての符号語の補符号語を含むようにする。このとき，これらの集合はいずれも回線分離符号となり，その最小距離はd_cより小さくない。

上記の条件を満たしd_cの大きいコンマフリー符号として符号長2^n($n \geq 4$)の階直交符号のすべての符号語に長さ2^n-1のM系列の適当な部分に0または1をそう入した系列を加えて作られる符号が知られている(6)。表4.3にこのようなコンマフリー符号から構成された回線分離符号の例を示す。この表の回線分離符号を作るために用いたコンマフリー符号およびそのコンマフリー指数は文献(6)による。また最小距離は式(4.9)の定義によって直接計算したものである。

この表から，コンマフリー符号から構成された回線分離符号は，BCH符号から構成された，ほぼ等しい符号長と符号語数をもつ回線分離符号と同程度の最小距離をもつことがわかる。また，この構成法による回線分離符号を用いるときは，そのコンマフリーの性質を同期に利用することができる。しかし，上記のようなコンマフリー符号は符号長，符号語数のきわめて限られたものしか知られていないため，この方法で

構成できる回線分離符号の種類もきわめて限られている。

表4.3 コンマフリー符号から構成した回線分離符号

符号長 (n)	符号語数 (m)	コンマフリー指数 (d_c)	最小距離 (d_{min})
16	16	2	2
32	32	6	6
64	64	14	16
128	128	30	41

4.5.3 Kronecker積による構成法

符号長がn', n'', 符号語数がm', m'', 最小距離がd_{min}', d_{min}''の二つの回線分離符号をC', C''としよう。C'とC''は同じものであってもよい。C'の符号語を行ベクトルとして表わし，その成分0, 1をそれぞれ実数-1, 1で表わす。このときC'のすべての符号語を行として並べた$m' \times n'$行列を$A=\{a_{ij}\}$とする。このようなAをC'の行列による表記ということにしよう。同様にC''の行列による表記をBとする。このときAとBのKronecker積

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots\cdots & a_{1n'}B \\ a_{21}B & & & \vdots \\ \vdots & & & \\ a_{m'1}B & \cdots\cdots & & a_{m'n'}B \end{bmatrix}$$

が行列による表記となるような符号 C は回線分離符号となる。明らかに C の符号長は $n'n''$, 符号語数は $m'm''$ となる。また C の最小距離が $\min[n'd_{min}'', n''d_{min}']$ となることも容易に確かめられる。

この方法は符号長の長い回線分離符号を構成する際に有効である。符号長が長い場合巡回符号からの構成法は非常に複雑な計算を要する。またコンマフリー符号から構成できる回線分離符号の種類は限られたものである。これに対し，本項の方法によれば多くの種類の回線分離符号を簡単に作ることができる。

4.6 補題の証明および式の導出

4.6.1. 補題 4.1 の証明

g_0 を含む一同値類は $T(g_0) = \{g_0, Tg_0\}$ と書ける。しか

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots\cdots & a_{1n'}B \\ a_{21}B & & & \vdots \\ \vdots & & & \\ a_{m'1}B & \cdots\cdots & & a_{m'n'}B \end{bmatrix}$$

が行列による表記となるような符号 C は回線分離符号となる。明らかに C の符号長は $n'n''$, 符号語数は $m'm''$ となる。また C の最小距離が $\min[n'd_{min}'', n''d_{min}']$ となることも容易に確かめられる。

この方法は符号長の長い回線分離符号を構成する際に有効である。符号長が長い場合巡回符号からの構成法は非常に複雑な計算を要する。またコンマフリー符号から構成できる回線分離符号の種類は限られたものである。これに対し、本項の方法によれば多くの種類の回線分離符号を簡単に作ることができる。

4.6 補題の証明および式の導出

4.6.1 補題 4.1 の証明

g_0 を含む一同値類は $T(g_0) = \{g_0, Tg_0\}$ と書ける。しか

なに $T^n g_0 = \bar{g}_0 \in \tau(g_0)$ であり，$g_0 \neq \bar{g}_0$ であるから $Tg_0 = \bar{g}_0$。

したがって

$$S^i g_0 + g_0 = \begin{cases} e_0 + e_1 + \cdots + e_{i-1} & ; \ i \text{ even} \\ e_0 + e_1 + \cdots + e_{n+i-1} & ; \ i \text{ odd} \end{cases}$$

ゆえに $S^i v + g_0 = S^i(v + g_0) + S^i g_0 + g_0$

$$= \begin{cases} T^i(v + g_0) & ; \ i \text{ even} \\ T^{n+i}(v + g_0) & ; \ i \text{ odd} \end{cases}$$

したがって $S^i v + g_0 \in \tau(v + g_0)$ (4.30)

同様に $S^i \bar{v} + g_0 \in \tau(v + g_0)$ (4.31)

一方

$$T^i(v + g_0) = \begin{cases} S^i v + g_0 & ; \ i \text{ even} \\ S^i \bar{v} + g_0 & ; \ i \text{ odd} \end{cases}$$

ゆえに

$$T^i(v + g_0) \in \sigma'(v + g_0) \quad (4.32)$$

式 (4.30), (4.31), (4.32) から (4.12) が導ける。また式 (4.13) は式 (4.12) からただちに導ける。

4.6.2 式 (4.14) の導出

σ - 同値類に含まれる元の数は n の約数であり，これは，

$2^k i$ $(k = 0, 1, \cdots, l \ ; \ i \mid n)$ の形で表わせる。$2^k i$ 個の元をもつ σ 一同値類の数を $m_\sigma(2^k i)$ で表わせば，これは Möbius の反転公式[2]を用いて，

$$m_\sigma(2^k i) = \sum_{j \mid 2^k i} \frac{1}{2^k i} \mu(j) 2^{\frac{2^k i}{j}} \tag{4.33}$$

となることが分る．ここで，このような σ 一同値類のうち，$\sigma(v) = \sigma(\bar{v})$ となるものの数を求めよう。

$\sigma(v) = \sigma(\bar{v})$ であれば，$S^p v = \bar{v}$ となる正整数 p が存在する。ところが $S^{2p} v = v$ となるから，$p = 2^{k-1} i$ でなければならない。したがって，$2^k i$ 個の元をもち，$\sigma(v) = \sigma(\bar{v})$ となる σ 一同値類の数 $m'_\sigma(2^k i)$ は

$$S^{2^{k-1} i} v = \bar{v} \tag{4.34}$$

$$S^j v \neq v \qquad j = 1, 2, \cdots, 2^k i - 1 \tag{4.35}$$

を満たす v の数の $1/2^k i$ に等しい。ところで，式(4.34)を満たす v の個数は $k \leq l$，$i \mid n$ となることから，容易に $2^{2^{k-1} i}$ となることが分る。これは i のすべての約数 i_0 に対し，$S^{2^{k-1} i_0} v = \bar{v}$，$S^j v \neq v$ $(j = 1, 2, \cdots, 2^k i_0 - 1)$ となる v の個数の総和に等しい。それゆえ，Möbius の反転

公式を用いれば，

$$m_\sigma'(2^k i) = \sum_{j \mid i} \frac{1}{2^k i} \mu(j) 2^{\frac{2^{k-1} i}{j}} \qquad (4.36)$$

を得る。式(4.33)(4.36)および

$$n_\sigma^e(2^{k+1} i) = \begin{cases} m_\sigma(i)/2 + m_\sigma'(2i) & ; \ k=0 \\ \{m_\sigma(2^k i) - m_\sigma'(2^k i)\}/2 + m_\sigma'(2^{k+1} i) & ; \ 0 < k < l \\ \{m_\sigma(2^l i) - m_\sigma'(2^l i)\}/2 & ; \ k = l \end{cases}$$

となることを用いれば，式(4.14)が導ける。

4.6.3 式(4.16)の導出

一つのT-同値類に属する元の数が t であれば，

$$T^t v = v \qquad (4.37)$$

となる $v \in B_n$ が存在する。いま $v = (v_0, v_1, \cdots, v_{n-1})$ を GF(2) の上の多項式 $v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$ で表わそう。このとき，式(4-37)は

$$(1+x^t) v(x) = 1 + x + \cdots + x^{t-1} \mod (x^n - 1)$$

となる。ゆえに，$f(x)$ を任意の多項式として，

$$\{(1+x) v(x) + 1\}(1 + x + \cdots + x^{t-1})$$

$$= f(x)(1-x^{n_0})^{2^l} \qquad (4.38)$$

を得る。$(1+x)v(x)+1$ が $1+x$ を因数として含まないことから，式(4.38)を満たす $v(x)$ が存在するためには，$2^{l+1} \mid t$ が必要であることが分る。また，明らかに $t \mid 2n$ であるから，$t = 2^{l+1}i$ $(i \mid n_0)$ となる。このとき，式(4.38)を満たす $n-1$ 次以下の多項式 $v(x)$ の数は $2^{2^l i}$ となることが容易に導ける。すなわち，$t = 2^{l+1}i$ に対し，式(4.37)を満たす v は $2^{2^l i}$ 個ある。これは i のすべての約数 j について $n_\tau^e(2^{l+1}j)$ の総和であるから Möbius の反転公式を用いれば，ただちに式(4.16)が導ける。

4.6.4 式(4.20)(4.21)を満たす h_r の存在

任意の $r \in R_{2n}$ について，r，$2n-r$ は奇数であるから，式(4.20)の右辺のベクトルの重みは偶数である。したがって，式(4.20)を満たす h_r はすべての $r \in R_{2n}$ について二つづつ存在し，一方を h_r とすれば，他方は $\overline{h_r}$ である。

ここで，R_{2n} の生成元[10]の集合を $\Lambda = \{\lambda_1, \lambda_2, \cdots, \lambda_g\}$ とし，$\lambda_i (\in \Lambda \subset R_{2n})$ を r とおいたときの式(4.20)を満

たす二つのベクトルのうちの一方を任意に選ぶ。このようにして得られたベクトルの集合 $\{h_{\lambda_i} \mid \lambda_i \in \Lambda\}$ において，"積" をつぎのように定義する

$$h_{\lambda_i} \cdot h_{\lambda_j} = Q_{\lambda_i} h_{\lambda_j} + h_{\lambda_i}$$

また，すべての R_{2n} の元 $r = \prod_i \lambda_i^{e_i}$ に対し，h_r を

$$h_r = \prod_{i=1}^{g} (h_{\lambda_i})^{e_i} \qquad (4.39)$$

によって定める。このとき $\{h_r \mid r \in R_{2n}\}$ は上に定義した積に関して R_{2n} と同型な群となり，したがって，任意の h_r, $h_{r'}$, $h_{rr'}$ $(r, r' \in R_{2n})$ は式 (4.21) を満たす。また，

$$S^i Q_r v = Q_r S^{r-i} v \quad (\forall v \in B_n)$$

となることを用いれば，任意の $r = \prod_i \lambda_i^{e_i} \in R_{2n}$ に対し，式 (4.39) のようにして作られた h_r が式 (4.20) を満たすことは容易に証明できる。

4.6.5 F_r の性質 (b'), (c'), (d') の証明

(b') 任意の $v \in B_n$, $r, r' \in R_{2n}$ に対し，

$$F_r F_{r'} v = F_r (Q_{r'} v + h_{r'}) = Q_{rr'} v + Q_r h_{r'} + h_r$$

$$= Q_{rr'} v + h_{rr'} = F_{rr'} v$$

となることから明らかである。

(c') 式(4.20)から $h_r + T^i h_r = Q_r(e_0 + e_1 + \cdots + e_{i r^{-1}-1})$ が導ける。これを用いると,

$$T^i F_r v = S^i Q_r v + T^i h_r$$

$$= Q_r S^{i r-2} v + Q_r(e_0 + e_1 + \cdots + e_{i r^{-1}-1}) + h_r$$

$$= Q_r T^{i r-1} v + h_r = F_r T^{i r-1} v$$

(d') $F_r \tau(v) = \{F_r T^i v / i = 0, 1, \cdots, 2n-1\}$

$= \{T^{ir} F_r v / i = 0, 1, \cdots, 2n-1\}$

$= \{T^j F_r v / j = 0, 1, \cdots, 2n-1\}$

$= \tau(F_r v)$

4.6.6 式(4.26)の導出

$C_0(n, d_0)$ の符号語において 1 が継続して現われる箇所を run と呼ぶ。1 が孤立して現われるときも一つの run とみなし,また最初と最後のディジットがともに 1 であるときは頭部の run と尾部の run をまとめて一つの run とする。このとき, 0 および $1^n = (1, 1, \cdots, 1)$ でない任意の符号語 v の run の数を r とすると, $W[v + Sv] = 2r$ となる。$v + S$

($\neq 0$) も $C_0(n, d_0)$ の符号語であるから，$2r \geq d_0$，すなわち

$$r \geq [(d_0 + 1)/2] \qquad (4.40)$$

を得る。ここで，C_1 の任意の二つの符号語を v，u ($v \neq u$) とし，$0 \leq i \leq n-1$ となる任意の整数 i について $w = (w_0, w_1, \cdots, w_{n-1}) = v + T^i u$ を定義する。w の w_0 から w_{i-1} までの部分に含まれる 1 の数と w の run の数を d_1，r_1 とし，残りの部分に含まれる 1 の数と w の run の数を d_2，r_2 とすれば，明らかに $d_1 \geq r_1$，$d_2 \geq r_2$ また $v + S^i u$ の run の数を r とすると $r_2 \geq r - r_1 - 1$ となることが容易に示される。さらに $v + S^i u$ ($\neq 0, 1^n$) $\in C_0(n, d_0)$ であるから r は式 (4.40) を満たす。ゆえに

$$W[w] = d_1 + d_2 \geq r_1 + r_2 \geq r - 1$$
$$\geq [(d_0 + 1)/2] - 1 \qquad (4.41)$$

また，$n \leq i \leq 2n-1$ となる i に対しても $v + S^i \bar{u}$ の run の数を r とすれば，まったく同様にして $w = v + T^i u$ の重みが式 (4.41) を満たすことがわかる。ところで $d_{T\min}$ はこのような任意の v，u，i ($0 \leq i \leq 2n-1$) に対する $w = v + T^i u$ の重みの最小値である。このことと式 (4.41)

から式(4.26)が導ける。

4.7 むすび

本章では回線分離符号を定義し，はじめに，その構造の基礎となる二値ベクトルのσ-同値類とτ-同値類の構造を明らかにした。また，その結果を利用して最小距離が1の最適回線分離符号の符号語数の上界と下界を求めた。これらの検討結果が今後の回線分離符号の研究に役立てば幸である。

つぎに，実用的な回線分離符号の3種の構成法を示した。これらの方法のうちで巡回符号から構成する方法が最も一般的であるが，同期が問題となるような場合にはコンマフリー符号から構成するのがよいであろう。また，符号長の長い回線分離符号の構成に際しては Kronecker 積による方法が有効である。

しかし，回線分離符号の研究はまだ端緒についたばかりであり，今後に残された問題が少なくない。特に，最小距離の大きい最適回線分離符号の性質およびその構成法についての今後の研究が期待される。

第5章

M系列およびM系列符号の二次元への拡張

第2章 2.6.4 で述べられているM系列およびM系列符号は，付録Ⅱに示されているM元信号を用いる通信系への応用をはじめ，広い応用分野をもっている．これはM系列の自己相関函数，あるいはM系列符号の距離構造に著しい特徴があるためである。

本章では，このようなM系列およびM系列符号の二次元への拡張について述べる。ここではM系列の性質を二次元に拡張したものとして最大面積行列をもつという性質を考え，この性質をもつ平面（二次元の配列）のかなり一般的と思われる構成法を示す。この構成法によって得られる平面を $\gamma\beta$－平面と呼ぶ。また，自己相関函数をはじめとする $\gamma\beta$－平面の種々の性質が論じられる。ここで得られる結果もM系列

と同様，巾広い応用分野をもつと考えられる。

本章では距離は表面には現れない。しかし，距離に対応するものとして自己相関函数が扱われる。これは，ここでは才2章 2.2の距離の定義と同様，一般的に定義される。

5.1 はじめに

M系列（最大長シフトレジスタ系列）およびM系列符号は才2章 2.6.4でも述べられているが，ここで再び説明を加えておこう。$GF(q^m)$の原始元をαとし，αの$GF(q)$の上の最小多項式を$h_\alpha(x)$とする。このとき，$h_\alpha(x)$をパリティ検査多項式とする$GF(q)$の上の符号長q^m-1，情報シンボル数mの巡回符号をM系列符号と呼び，M系列符号の0でない符号語をM系列という。ただし，M系列というとき，同一のM系列を繰返し並べた無限系列（または半無限系列）を意味することもある。この場合には，M系列符号の符号長q^m-1はM系列の周期となる。

M系列およびM系列符号は応用上重要な数多くの特徴をもち，様々な角度から研究されている[6][50][60][61]。

M系列のもっとも重要な性質の一つは，周期が q^m-1 のM系列において，ある一周期内から始まるすべての相続くmディジットの集合を考えるとき，これが $GF(q)$ のエのすべてのm次元ベクトルから0ベクトルを除いた集合と一致するという性質であり，この性質からM系列の自己相関函数の特徴なども導かれる。この性質を二次元に拡張したものとして福田らは最大面積行列をもつという性質を考え，この性質が応用上きわめて重要であることを示した[47]。しかし，これまで最大面積行列をもつ平面（二次元の配列，半無限行列）の構成法は知られていなかった。

本章では，最大面積行列をもつ平面のがなり一般的と思われる一つの構成法を示す。これは，次節で述べる二次元線形巡回符号の概念を利用した構成法である。ここでは，これによって構成される平面を $\gamma\beta$ 一平面，またそれに対応する二次元巡回符号を $\gamma\beta$ 一平面符号と呼ぶことにする。本章ではこの $\gamma\beta$ 一平面および $\gamma\beta$ 一平面符号の構成法およびその諸性質について論ずる。

はじめに 5.2で準備として，二次元線形巡回符号および

最大面積行列をもつ平面について説明する。5.3ではγβ－平面およびγβ－平面符号を代数的に定義し，5.4でγβ－平面が最大面積行列をもつ平面であることを証明する。さらに，そこでγβ－平面が最大面積行列をもつ平面として十分一般的なものであることを確かめる。また5.5ではγβ－平面を線形再帰関係によって具体的に構成する方法を示す。ついで，5.6ではγβ－平面とM系列の対応およびγβ－平面符号と他の二次元符号との関係を明らかにする。5.7ではγβ－平面の自己相関函数について論じ，これが応用上重要な特徴をもつことを示す。また5.8で，γβ－平面の多次元への拡張について述べる。

5.2 二次元線形巡回符号および最大面積行列をもつ平面

二次元線形巡回符号および最大面積行列をもつ平面の概念は福田らによって定義された[62]。ここではこれらを説明しておく。なお，本節におけるいくつかの定義は福田らの定義より一般化されている。

5.2.1 二次元線形巡回符号

$GF(q)$（q：素数のべき）の上の次のようなN×M行列A（N×M平面とも呼ぶ）を考える。

$$A = \{a_{ij}\} = \begin{bmatrix} a_{00} & a_{01} & a_{02} & \cdots & a_{0M-1} \\ a_{10} & a_{11} & & & \vdots \\ \vdots & & \ddots & & \vdots \\ a_{N-10} & \cdots & & & a_{N-1M-1} \end{bmatrix} \qquad (5.1)$$

$$; a_{ij} \in GF(q)$$

このような行列すべての集合を $V_{N\times M}$ で表そう。明らかに $V_{N\times M}$ は $GF(q)$ の上の NM 次元ベクトル空間をなす。$V_{N\times M}$ の線形部分空間 C を面積 $N\times M$ の二次元線形符号と呼ぶ。C の次元が K であるとき、C の基底をなす $N\times M$ 行列 $G_1, G_2, \cdots, G_K$ を垂直方向に並べた三次元行列を C の生成（三次元）行列と呼ぶ。以下では、生成行列を $GF(q)$ の上の K 次元ベクトル空間 V_K の元を成分とする $N\times M$ 行列 $G=\{g_{ij}\}$（$g_{ij} \in V_K$）で表わす。

$V_{N\times M}$ の元 $A=\{a_{ij}\}$, $B=\{b_{ij}\}$ に内積 $(A, B) = \sum_{i=0}^{N-1}\sum_{j=0}^{M-1} a_{ij} b_{ij}$ を導入し、二次元線形符号 C のこの内積に関する直交補空間を C の双対符号と呼ぶ。また、C の双対符号

の生成行列 $H=\{h_{ij}\}$ を C のパリティ検査行列という。ここに、h_{ij} は $NM-K$ 次元ベクトル空間 V_{NM-K} の元である。$N\times M$ 行列 A が二次元線形符号 C の符号語である必要十分条件は、明らかに

$$\sum_{i=0}^{N-1}\sum_{j=0}^{M-1} a_{ij}h_{ij}=0 \qquad \begin{pmatrix} a_{ij}\in GF(q) \\ h_{ij}\in V_{NM-K}\end{pmatrix} \qquad (5.2)$$

となることである。

二次元線形符号 C の任意の符号語を $A=\{a_{ij}\}$ とするとき、任意の整数 k, l に対し $N\times M$ 行列 $\{a_{i+k,j+l}\}$ (a_{uv} の添字 $u; v$ はおのおの法を N, M として定める) が再び、C に属すとき、C を面積 $N\times M$ の二次元線形巡回符号と呼ぶ。

二次元線形巡回符号を論ずる場合には、イデアル (x^N-1, y^M-1) を法とする $GF(q)$ の上の二変数多項式の剰余環 $\Lambda(x^N-1, y^M-1)$ を用いると便利である。以下では $\Lambda(x^N-1, y^M-1)$ の元は x について $N-1$ 次、y について $M-1$ 次以下の二変数多項式で表わす。また、本章における多項式の演算は特に断わらない限り、$\Lambda(x^N-1, y^M-1)$ において行うものとする。

ここで，$\nabla_{N\times M}$ の元 $A=\{a_{ij}\}$ を $x^i y^j$ の係数が a_{ij} となる多項式 $a(x,y)$ によって表わす。これによって多項式 $a(x,y)$ ($\in \mathcal{A}(x^N-1, y^M-1)$) と平面 A を同一視することにする。このとき，二次元線形符号 C が巡回符号であるための条件は，$a(x,y)\in C$ のとき，任意の整数 k,l に対して $x^k y^l a(x,y)\in C$ となることであるといい換えることができる。

5.2.2 最大面積行列をもつ平面

つぎのような $GF(q)$ の上の半無限行列（平面とも呼ぶ）を考える。

$$A_\infty = \begin{bmatrix} a_{00} & a_{01} & a_{02} & \cdots & \\ a_{10} & a_{11} & & \ddots & \\ a_{20} & & & & \\ \vdots & & & & \end{bmatrix} \qquad (a_{ij}\in GF(q)) \tag{5.3}$$

A_∞ において，

$$a_{ij} = a_{i+p_x,\,j} = a_{i,\,j+p_y} \tag{5.4}$$

が成立するような正整数 p_x，p_y が存在し，かつ p_x，p_y が式(5.4)が成立するような最小の正整数であるとき，A_∞ は

周期 (P_x, P_y) をもつという。

また，ある正整数 N_x，N_y に対し，A_∞ に含まれるすべての $(N_x+n_x-1)\times(N_y+n_y-1)$ 行列において，この行列に含まれるすべての $n_x \times n_y$ 行列が互いに異なり，かつ 0 行列以外の GF(q) の上のすべての $n_x \times n_y$ 行列が現れるような正整数 n_x，n_y が存在するとき，A_∞ は面積 $N_x \times N_y$ の最大面積行列をもつという。$N_x \times N_y$ 行列が最大面積行列であるためには，明らかに

$$N_x \cdot N_y = q^{n_x n_y} - 1 \qquad (5.5)$$

が必要である[62]。

さらに，周期 (P_x, P_y) をもつ平面が面積 $N_x \times N_y$ の最大面積行列をもつとき，$P_x = N_x$，$P_y = N_y$ であるなら，A_∞ を M 平面と呼ぶ。

さて，$N \times M$ 行列 A を繰返し並べることによって，平面 A_∞ を作ることができる。この A_∞ はいうまでもなく周期をもつ。このような平面 A_∞ を以下では単に A あるいは $a(x, y)$ によって表わすことにする。A が二次元線形巡回符号の符号語であるときは，平面 A $(=A_\infty)$ は線形再帰関係[62]に

よって生成できる。たとえば C のパリティ検査方程式（式(5.2)）を用いればよい。

5.3 γβ-平面および γβ-平面符号の定義

q を素数のべき，n，m を正整数とする。また μ，λ をつぎの条件を満たすような正整数とする。

$$\lambda\mu \mid q^n - 1 \tag{5.6}$$

$$\frac{q^n-1}{\mu} \mid q^k - 1 \quad \text{ならば} \quad k \geq n \tag{5.7}$$

$$GCD\left(\lambda, \frac{q^{nm}-1}{q^n-1}\mu\right) = 1 \tag{5.8}$$

ここに $a \mid b$ は b が a で割り切れることを示し，$GCD(a, b)$ は a と b の最大公約数を示す。

つぎに，$GF(q^{nm})$ の原始元を α とし，η を $q^{nm}-1$ と素な正整数として，

$$\gamma = \alpha^{\frac{q^{nm}-1}{q^n-1}\mu} \qquad \beta = \alpha^{\eta\lambda} \tag{5.9}$$

を定義する。ここで，γ が $GF(q^n)$ の元であることに注意しておこう。

γ の位数を e_γ，β の位数を e_β とすると，明らかに

$$e_\gamma = \frac{q^n - 1}{\mu} \qquad e_\beta = \frac{q^{nm} - 1}{\lambda} \tag{5.10}$$

さらに，γ の $GF(q)$ の上の最小多項式を $h_\gamma(x)$，β の $GF(q^n)$ の上の最小多項式を $h_\beta(y)$ とする．$h_\gamma(x)$，$h_\beta(y)$ は定数（おのおの $GF(q)$，$GF(q^n)$ の 0 でない元）倍を除いて一意に定まり[7]，その次数は次の補題によって与えられる。

補題 5.1：$h_\gamma(x)$ は n 次，$h_\beta(y)$ は m 次の既約多項式である。

（証明）$h_\gamma(x)$ の次数は $\mu(q^d - 1) = 0 \mod (q^n - 1)$ を満たす最小の正整数 d である[2]。式 (5.7) からただちに $d = n$ となることが分る。一方 $h_\beta(y)$ の次数は

$$\eta\lambda(q^{nd} - 1) = 0 \mod (q^{nm} - 1) \tag{5.11}$$

を満たす最小の正整数 d である．$\lambda \mid q^n - 1 \mid q^{nm} - 1$ であり，η と $q^{nm} - 1$ は互いに素であるから，これは

$$q^{nd} - 1 = 0 \mod \left(\frac{q^{nm} - 1}{\lambda}\right)$$

を満たす最小の正整数でもある。ここで $q^{nd} - 1 = \frac{q^{nm} - 1}{\lambda} \cdot a$ （a：正整数）とおく。$\lambda \mid q^n - 1$ であるから $\lambda \leq q^n - 1$。それゆえ

$$q^{nd}-1 \geq \frac{q^{nm}-1}{q^n-1}\,a=(q^{n(m-1)}+q^{n(m-2)}+\cdots+q^n+1)a>q^{n(m-1)}-1$$

ゆえに $d>m-1$。しかるに $d=m$ とするとき式(5.11)は成立するから，式(5.11)を満たす最小の正整数，すなわち $h_\beta(y)$ の次数は m となる。 (証明終)

ここで，$GF(q)$ の上の x に関する $n-1$ 次以下のすべての多項式の集合を P_{n-1} とし，$a(x)(\in P_{n-1})$ に $a(\gamma)(\in GF(q^n))$ を対応させる。$h_\gamma(x)$ が n 次の既約多項式であることから，このような対応によって P_{n-1} の元と $GF(q^n)$ の元が1対1に対応することは明らかである。つぎに，$h_\beta(y)=\sum_{i=0}^{m-1} c_i y^i$ の係数 $c_i(\in GF(q^n))$ に，この対応によって，$c_i(x)(\in P_{n-1})$ を対応させ，$\sum_{i=0}^{m-1} c_i(x)y^i$ を $h_{r\beta}(x,y)$ で表わす。

このとき，$\Lambda(x^{e_r}-1,\ y^{e_\beta}-1)$ における連立方程式

$$\begin{cases} h_\gamma(x)f(x,y)=0 & (5.12)\\ h_{r\beta}(x,y)f(x,y)=0 & (5.13)\end{cases}$$

を満たす $GF(q)$ の上の二変数多項式 $f(x,y)(\in\Lambda(x^{e_r}-1,\ y^{e_\beta}-1))$ すべての集合を $r\beta$ - 平面符号と呼び $C_{r\beta}$ で表わ

す。また $C_{\gamma\beta}$ の0でない符号語を $\gamma\beta$ - 平面と呼ぶことにする。

5.4 $\gamma\beta$ - 平面の構造および主定理

5.4.1 $\gamma\beta$ - 平面の基礎構造

定義から、$\gamma\beta$ - 平面符号 $C_{\gamma\beta}$ は明らかに面積 $e_\gamma \times e_\beta$ の二次元線形巡回符号である。以下では、5.2で述べたように、x, y に関する多項式の演算は特に断わらない限り、$\mathcal{A}(x^{e_\gamma}-1, y^{e_\beta}-1)$ 上で行うものとする。

ここで、$f(x,y)=\sum_{i=0}^{e_\beta-1} f_i(x)y^i$ とおけば、式(5.12)から

$$h_\gamma(x) f_i(x) = 0 \quad (0 \le i < e_\beta) \qquad (5.14)$$

を得る。ゆえに、$f_i(x)$ は $h_\gamma(x)$ をパリティ検査多項式とする符号 C_γ の符号語である。C_γ の符号語 $a(x)$ は $GF(q^n)$ の元 $a(\gamma)$ と1対1に対応する（$a(x), b(x) \in C_\gamma$ に対し、$a(x)=b(x)$ なら $a(\gamma)=b(\gamma)$。逆に $a(\gamma)=b(\gamma)$ であれば、$a(x)-b(x)$ は1の e_γ 次根[7]をすべて含む。ゆえに $a(x)=b(x)$）。ゆえに、式(5.12)を満たす $f(x,y)$ は $GF(q^n)$ 上の y に関する多項式 $f(\gamma, y)$ と1対1に対応する。このこ

とから．式(5.12),(5.13)の解$f(x,y)$は$GF(q^n)$の上のyに関する方程式

$$h_\beta(y)\, f(\gamma, y) = 0 \qquad (5.15)$$

の解$f(\gamma,y)$と1対1に対応することが分る。特に$f(x,y)=0$は明らかに$f(\gamma,y)=0$に対応する．

$h_\beta(y)$の次数はmであるから，式(5.15)の解の個数はq^{nm}である。したがって，$\gamma\beta$-平面符号$C_{\alpha\beta}$の符号語数はq^{nm}となる。

つぎの補題は$\gamma\beta$-平面の構造を調べる上できわめて重要である。

補題5.2：$\gamma\beta$-平面$f(x,y)$に対し，$a(x,y)$($\in A(x^{e_\gamma}-1, y^{e_\beta}-1)$)が

$$a(x,y)\, f(x,y) = 0 \qquad (5.16)$$

を満たす必要十分条件は$a(\gamma,\beta)=0$となることである。

(証明) 式(5.15)から$f(\gamma,\beta)\neq 0$がただちに導ける。ゆえに，式(5.16)が成立すれば$a(\gamma,\beta)=0$となる．

逆を証明しよう．$h_{\gamma\beta}(x,y)$をyの多項式とみて，そのy^mの係数を$C(x)$とする．$C(x)$は$n-1$次以下の0でない多

項式であるから，

$$\bar{C}(x)\,C(x) = 1 \mod h_\gamma(x)$$

となる多項式 $\bar{C}(x)$ が存在する。明らかに，$\bar{C}(x)\,h_{\gamma\beta}(x,y)$ の y^m の係数は $1 + C'(x)\,h_\gamma(x)$ の形に表わせる。これを用いると，任意の多項式 $a(x,y)$ は

$$a(x,y) = h_{\gamma\beta}(x,y)\,a_1(x,y) + h_\gamma(x)\,a_2(x,y) + a_3(x,y)$$

の形に分解できることが分る。ただし，$a_3(x,y)$ は y について $m-1$ 次以下の多項式である。$a(\gamma,\beta) = 0$ とすると，$a_3(\gamma,\beta) = 0$．ゆえに $a_3(\gamma,y) = 0$ でなければならない。すなわち，$a_3(x,y) = h_\gamma(x)\,a_4(x,y)$ と書ける。ゆえに，

$$a(x,y) = h_{\gamma\beta}(x,y)\,a_1(x,y) + h_\gamma(x)\,(a_2(x,y) + a_4(x,y))$$

を得る。したがって，式 (5.12), (5.13) から

$$a(x,y)\,f(x,y) = 0$$

となる。 (証明終)

この補題から，$\gamma\beta$ - 平面 $f(x,y)$ に対し，

$$x^\lambda f(x,y) = f(x,y)$$

$$y^\mu f(x,y) = f(x,y)$$

を満たす最小の正整数 λ, μ はそれぞれ e_γ, e_β となること

が分る。ゆえに $\gamma\beta$ - 平面 $f(x, y)$ の周期 (p_x, p_y) は

$$p_x = e_\gamma = \frac{q^n - 1}{\mu} \qquad p_y = e_\beta = \frac{q^{nm} - 1}{\lambda} \tag{5.17}$$

で与えられる。

周期 (p_x, p_y) は $\gamma\beta$ - 平面を x 方向および y 方向へ巡回置換したときの性質を示すものであるが，一般の巡回置換に対しては，つぎの補題が導ける。

補題 5.3： $\gamma\beta$ - 平面 $f(x, y)$ に対し

$$x^i y^j f(x, y) = f(x, y) \quad (0 \le i < p_x,\ 0 \le j < p_y) \tag{5.18}$$

が成立する必要十分条件は

$$\begin{cases} i = -\eta\lambda k \mod p_x \\ j = \dfrac{q^{nm} - 1}{q^n - 1}\mu k \end{cases} \qquad 0 \le k < \frac{q^n - 1}{\mu\lambda} \tag{5.19}$$

となることである。

(証明) 補題 5.2 から，式 (5.18) が成立する必要十分条件は

$$\gamma^i \beta^j = 1 \tag{5.20}$$

すなわち $$\beta^j = \gamma^{-i}$$

となることである。両辺を e_γ 乗して，

$$(\beta^{e_\gamma})^j = 1$$

ゆえに，β^{e_γ} の位数を $e_{\beta\gamma}$ とすると j は $e_{\beta\gamma}$ で割り切れねば

ならない。 $e_{\beta\gamma}$ は

$$e_{\beta\gamma} = \frac{e_\beta}{GCD(e_\gamma, e_\beta)} = \frac{q^{nm}-1}{\lambda GCD\left(\frac{q^n-1}{\mu}, \frac{q^{nm}-1}{\lambda}\right)}$$

で与えられる[2]。式(5.6)および(5.8)を用いれば,

$$GCD\left(\frac{q^n-1}{\mu}, \frac{q^{nm}-1}{\lambda}\right) = \frac{q^n-1}{\mu\lambda}$$

となることがただちに導ける。ゆえに

$$e_{\beta\gamma} = \frac{q^{nm}-1}{q^n-1}\mu \qquad (5.21)$$

いま, $j = k e_{\beta\gamma}$ とおくと,

$$\gamma^i \beta^j = \gamma^i \beta^{k e_{\beta\gamma}} = \gamma^{i+n\lambda k}$$

ゆえに, 式(5.20)の成立する必要十分条件は

$$\begin{cases} i \equiv -n\lambda k & \bmod e_\gamma \\ j \equiv k e_{\beta\gamma} & \bmod e_\beta \end{cases} \qquad k = 0, 1, \cdots$$

となることであり, これからただちに式(5.19)が導ける。

(証明終)

ここで, N_x, N_y をつぎのように定義する。

$$\begin{cases} N_x = e_\gamma = p_x = \dfrac{q^n-1}{\mu} \\ N_y = e_{\gamma\beta} = \dfrac{q^{nm}-1}{q^n-1}\mu = \dfrac{q^{nm}-1}{N_x} \end{cases} \qquad (5.22)$$

このとき, つぎの系は補題から明らかである。

系 5.3.1 : $\gamma\beta$-平面 $f(x,y)$ の y について N_y-1 次以下の部分を $f'(x,y)$ とおく．このとき $f(x,y)$ はつぎのように表せる．

$$f(x,y)=\sum_{k=0}^{K-1} x^{l(k)} y^{N_y k} f'(x,y) \qquad (5.23)$$

ここに，

$$l(k)=-\eta\lambda k \mod P_x$$

$$K=\frac{q^m-1}{\mu\lambda}$$

である．

5.4.2 $\gamma\beta$-平面符号の $\gamma\beta$-平面による表現および生成行列

補題 5.3 から，$0\le i<N_x$，$0\le j<N_y$ となる i; j に対して $x^i y^j f(x,y)=f(x,y)$ となるのは $i=j=0$ のときに限ることが分る。また，$N_x N_y=q^{mm}-1$ となり，$\gamma\beta$-平面符号 $C_{\gamma\beta}$ の符号語数は q^{mm} であったから，$C_{\gamma\beta}$ はつぎの補題のように表現できる。

補題 5.4 : $\gamma\beta$-平面符号 $C_{\gamma\beta}$ はその 0 でない任意の符号語（$\gamma\beta$-平面）$f(x,y)$ を用いて，つぎのように書ける。

$$C_{\gamma\beta}=\{x^i y^j f(x,y) \mid 0\le i<N_x,\ 0\le j<N_y\}\cup\{0\} \qquad (5.24)$$

つぎに，$\gamma\beta$-平面符号 $C_{\gamma\beta}$ の生成行列を求めよう．$\gamma\beta$-平面を $f(x, y)$ とし

$$a(x, y) f(x, y) = 0$$

を満たすすべての $a(x, y)$ に対して

$$\tilde{a}(x, y) = x^{p_x} y^{p_y} a(x^{-1}, y^{-1})$$

となる多項式の集合を $\bar{C}_{\gamma\beta}$ で表わす．$\bar{C}_{\gamma\beta}$ が $C_{\gamma\beta}$ の双対符号となっていることは，$C_{\gamma\beta}$ が二次元線形巡回符号であることから容易に確かめられる．補題 5.2 から，$b(x, y) = \sum_{i=0}^{p_x-1} \sum_{j=0}^{p_y-1} b_{ij} x^i y^j \in \bar{C}_{\gamma\beta}$ となる必要十分条件は $b(\gamma^{-1}, \beta^{-1}) = 0$．すなわち

$$\sum_{i=0}^{p_x-1} \sum_{j=0}^{p_y-1} b_{ij} \gamma^{-i} \beta^{-j} = 0 \qquad (5.25)$$

となることである．したがって，式 (5.2) に注意すれば，$\bar{C}_{\gamma\beta}$ のパリティ検査行列，すなわち $C_{\gamma\beta}$ の生成行列は

$$G = \{g_{ij}\} = \{\gamma^{-i} \beta^{-j}\} = \{\alpha^{-Ny i - \eta\lambda j}\} \qquad (5.26)$$

となる $GF(q^{nm})$ の上の $p_x \times p_y$ 行列であることが分る．

以上に得られた主要な結果をつぎに定理の形でまとめておこう．

定理 5.5 : 式 (5.6) (5.7) (5.8) を満たすような正整数

n, m, μ, λ および $GF(q^{nm})$ の原始元 α と $q^{nm}-1$ と素な正整数 η によって定められる $GF(q)$ の上の $\gamma\beta$ - 平面符号 $C_{\gamma\beta}$ は面積 $p_x \times p_y = \frac{q^n-1}{\mu} \times \frac{q^{nm}-1}{\lambda}$，符号語数 q^{nm} の二次元線形巡回符号であり，その生成行列は式(5.26)で与えられる。また $C_{\gamma\beta}$ はその0でない任意の符号語 $f(x, y)$ を用い式(5.24)のように表わせる。

5.4.3 主定理

ここでは，5.4.2の結果を用い，$\gamma\beta$ - 平面が面積 $N_x \times N_y$ の最大面積行列をもつことを示す。このために，つぎの補題が必要である。

補題 5.6： p_x-1 以下の n 個の非負整数の集合を I，p_y-1 以下の m 個の非負整数の集合を J とし，$\gamma\beta$ - 平面符号 $C_{\gamma\beta}$ の生成行列 G において，nm 個の成分 $\{g_{ij} \mid i \in I, j \in J\}$ が $GF(q)$ の上で互いに独立であるとする。また，$C_{\gamma\beta}$ の任意の0でない符号語 $f(x, y)$ に対し，

$$f^{(k,\ell)}(x, y) = \sum_{i=0}^{p_x-1} \sum_{j=0}^{p_y-1} f_{ij}^{(k,\ell)} x^i y^j = x^k y^\ell f(x, y) \quad (5.27)$$

とおき，$f^{(k,\ell)}(x, y)$ の nm 個の係数の集合

$$\omega_{kl} = \{ f_{ij}^{(k,l)} \mid i \in I,\ j \in J \} \qquad (5.28)$$

を定義する。このとき，k, l が $0 \leq k < N_x$，$0 \leq l < N_y$ のあらゆる値をとるとき，ω_{kl} にはすべては0でない $GF(q)$ の元のあらゆる組合せが一度づつ現れる。

（証明） $C_{\gamma\beta}$ の次元が nm であり，生成行列 G の nm 個の成分 $\{ g_{ij} \mid i \in I,\ j \in J \}$ が互いに独立であることから，$a(x,y)$ $(\in C_{\gamma\beta})$ の係数の集合 $\{ a_{ij} \mid i \in I,\ j \in J \}$ には，$a(x,y)$ が $C_{\gamma\beta}$ のすべての符号語（0も含む）を動くときに，nm 個の $GF(q)$ の元のあらゆる組合せが一度づつ現れることが分る。このことと補題5.4から，ただちにこの補題が結論できる。 （証明終）

ここで，

$$\sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \lambda_{ij} g_{ij} = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \lambda_{ij} \gamma^{-i} \beta^{-j} = 0 \qquad (5.29)$$

$$(\lambda_{ij} \in GF(q))$$

であるとしよう．ところが，β^{-1} の $GF(q^n)$ の上の最小多項式の次数は明らかに m，また γ^{-1} の $GF(q)$ の上の最小多項式の次数は n となるから，式(5.29)が成立するのは，すべての λ_{ij} が0となるときに限る。ゆえに $I = \{0, 1, \cdots, n-1\}$，

$J=\{0,1,\cdots,m-1\}$ とすると $\{g^{i,j}\mid i\in I, j\in J\}$ は互いに，GF(g)の上で互いに独立となる．ゆえに，最大面積行列の定義における n_x，n_y をそれぞれ n，m とすれば，補題5.6からただちに本章のもっとも主要な結果が得られる。

定理5.7：$\gamma\beta$－平面は周期 $(p_x, p_y)=\left(\frac{g^n-1}{\mu}, \frac{g^{nm}-1}{\lambda}\right)$ をもち，面積 $N_x\times N_y=\frac{g^n-1}{\mu}\times\frac{g^{nm}-1}{g^n-1}\mu$ の最大面積行列をもつ。特に $\mu\lambda=g^n-1$ となるときは $\gamma\beta$－平面はM平面となる。これを $\gamma\beta$－M平面と呼ぶ。

なお補題5.6から明らかなように，n_x，n_y としては n，m をとる必要は必しもなく，$n_xn_y=nm$ となる n_x，n_y で，生成行列Gに含まれる任意の $n_x\times n_y$ 行列に属する成分がGF(g)の上で互いに独立であるようなものであればよい．

つぎの系は最大面積行列の定義と系5.3.1から明らかである。

系5.7.1　$\gamma\beta$－平面 $f(x,y)$ に含まれる任意の $N_x\times N_y$ 行列には，その成分として0が $g^{nm-1}-1$ 個，それ以外のすべてのGF(g)の元がおのおの g^{nm-1} 個づつ含まれる。また $f(x,y)$ 全体には0が $(g^{nm-1}-1)(g^n-1)/\mu\lambda$ 個，それ以外のすべ

ての GF(q) の元がおのおの $q^{m-1}(q^n-1)/\mu\lambda$ 個づつ含まれる。

5.4.4 面積 $K\times(q^N-1)/K$ の最大面積行列をもつ $\gamma\beta$-平面

$\gamma\beta$-平面が面積 $N_x\times N_y$ の最大面積行列をもつとすれば、5.2で述べたように、$N_x\cdot N_y=q^N-1$（N：正整数）の形になっていなければならない。また、$\gamma\beta$-M平面が構成できたとすれば、$N_x=\lambda$, $N_y=\frac{q^m-1}{q^n-1}\mu$ であるから、式(5.8)により、N_x と N_y は互いに素でなければならない。それでは、これらの逆は成立するであろうか。この問題に対し、つぎの定理が導ける。

定理5:8： q^N-1 の任意の約数 K および $L=(q^N-1)/K$ に対し、面積 $K\times L$ の最大面積行列をもつ $\gamma\beta$-平面が存在する。また K と L が互いに素であるときは面積 $K\times L$ の最大面積行列をもち周期が (K,L) となる $\gamma\beta$-M平面が存在する。

（証明） n を $K\mid q^n-1$, $n\mid N$ となる最小の正整数とする。このような n が存在することは明らかである。つぎに、$\mu=$

$(q^n-1)/K$ とし，さらに λ を K の約数で λ と $(q^N-1)/K$ が互いに素となるものとする。このような λ は少くとも一つは存在する。たとえば，$\lambda=1$ とすればよい。このようにして選んだ n, m, μ, λ は明らかに式 (5.6) (5.7) (5.8) を満たす。それゆえ α を $GF(q^N)$ の原始元，η を q^N-1 と素な任意の正整数とすれば，$n, m, \mu, \lambda, \alpha, \eta$ によって，面積 $K\times L$ の最大面積行列をもつ $\gamma\beta$－平面が構成できる。

K と L が素であるときは，$\lambda=K$ を選べるから，$\mu\lambda=q^n-1$ となり，$\gamma\beta$－M 平面を作ることができる。(証明終)

この定理から，$\gamma\beta$－平面が最大面積行列をもつ平面としてかなり一般的なものであることが分る。

5.5 $\gamma\beta$－平面を生成する線形再帰関係

$\gamma\beta$－平面を実際に作るには，式 (5.26) の生成行列を用いてもよいが，式 (5.12) (5.13) から，$\gamma\beta$－平面を生成する線形再帰関係を導くこともできる。

いま，最小多項式 $h_\gamma(x)$，$h_\beta(y)$ として 0 次の係数が 1 となるものを選ぶ。このとき，$h_\gamma(0)=1$，$h_{\gamma\beta}(x,0)=1$ とな

る。ここで、$\widehat{h_\gamma}(x)=x^n h_\gamma(x^{-1})$ の x^i の係数を $\widehat{h_i}$，また $\widetilde{h_{\gamma\beta}}(x,y)=x^{n-1}y^m h_{\gamma\beta}(x^{-1},y^{-1})$ の x^iy^j の係数を $\widetilde{h_{ij}}$ とする。このとき，式(5.12)(5.13)は $f(x,y)=\sum_{i=0}^{p_x-1}\sum_{j=0}^{p_y-1} f_{ij}x^iy^j$ の係数を用いて，次のように書き直せる。

$$f_{k+n,l}=-\sum_{i=0}^{n-1}\widehat{h_i}\,f_{k+i,l} \tag{5.30}$$

$$f_{k+n-1,l+m}=-\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\widetilde{h_{ij}}\,f_{k+i,l+j} \tag{5.31}$$

ただし f_{uv} の添字 u，v はそれぞれ p_x，p_y を法として定めるものとする。

式(5.30)(5.31)は $\gamma\beta$ - 平面を生成する線形再帰関係を具体的な形で表わしたもので，$\{f_{ij}\mid i=0,1,\cdots,n-1,\ j=0,1,\cdots,m-1\}$ に対し，初期状態を与えれば，これらの式によって，$\gamma\beta$-平面 $f(x,y)$ の係数 f_{ij} がすべて順次定まる。

また，$h_{\gamma\beta}(x,0)=x^{n-1}$ と選び（$h_\beta(0)=\gamma^{n-1}$ とすればよい）$\widetilde{h'_{\gamma\beta}}(x,y)=x^{n-1}y^m h_{\gamma\beta}(x,y)$ の係数を $\widetilde{h'_{ij}}$ とすれば，式(5.31)のかわりに，

$$f_{k,l+m}=-\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\widetilde{h'_{ij}}\,f_{k+i,l+j} \tag{5.32}$$

を用いることができる。すなわち，式(5.30)(5.32)によっても $\gamma\beta$ - 平面を生成することができる。

例5.1) $q=2$, $n=3$, $m=2$, $\mu=1$, $\lambda=q^n-1=7$, $\eta=1$ とし, $GF(2^6)$ の原始元 α は $\alpha^6+\alpha+1=0$ によって定める (x^6+x+1 が原始多項式であることは文献(1)参照)。この場合は $\mu\lambda=q^n-1$ であるからM平面となり,

$$p_x=N_x=(q^n-1)/\mu=7 \qquad p_y=N_y=(q^{nm}-1)\mu/(q^n-1)=9$$

である。また, $\gamma=\alpha^9$ の $GF(2)$ の上の最小多項式は

$$h_\gamma(x)=x^3+x^2+1$$

であり, 線形再帰関係として式(5.30)(5.32)を用いるとすれば, $\beta=\alpha^7$ の $GF(2^3)$ の上の最小多項式として

$$h_\beta(y)=\gamma^2(y^2+(\gamma+1)y+1)$$

をとればよい。このとき

$$h_{\gamma\beta}(x,y)=x^2y^2+y+x^2$$

となる。したがって

$$\widehat{h}_\gamma(x)=x^3+x+1$$

$$\widehat{h}'_{\alpha\beta}(x,y)=y^2+x^2y+1$$

を得る。ゆえに, 式(5.30)(5.32)は

$$f_{k+3,l}=f_{k,l}+f_{k+1,l}$$

$$f_{k,l+2}=f_{k,l}+f_{k+2,l+1}$$

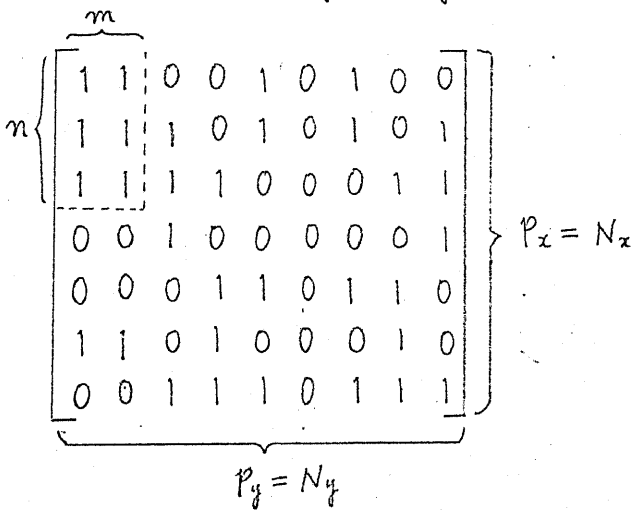
となる．これを用いると図5.1のγβ－M平面が生成できる．

図5.1　γβ－M平面の例

$q=2$，$n=3$，$m=2$，$\mu=1$，$\lambda=7$，$\eta=1$

$\alpha^6+\alpha+1=0$　　$\gamma=\alpha^9$　　$\beta=\alpha^7$

$P_x=N_x=7$　　$P_y=N_y=9$



例5.2）$q, n, m, \mu, \eta, \alpha$は例5.1と同様に定め，$\lambda=1$とする．このとき，$\gamma=\alpha^9$，$\beta=\alpha$であり，

$P_x=(q^n-1)/\mu=7$　　$P_y=(q^{nm}-1)/\lambda=63$

$N_x=P_x=7$　　$N_y=(q^{nm}-1)\mu/(q^n-1)=9$

となる．γのGF(2)上の最小多項式は例5.1と同様，

$$h_\gamma(x)=x^3+x^2+1$$

であり，線形再帰関係として，式(5.30)(5.32)を用いるとすれば，βの最小多項式として，

図 5.2　$\gamma\beta$ − 平面の例

$q=2$, $n=3$, $m=2$, $\mu=1$, $\lambda=1$, $\eta=1$

$\alpha^6+\alpha+1=0$　　$\gamma=\alpha^9$, $\beta=\alpha$

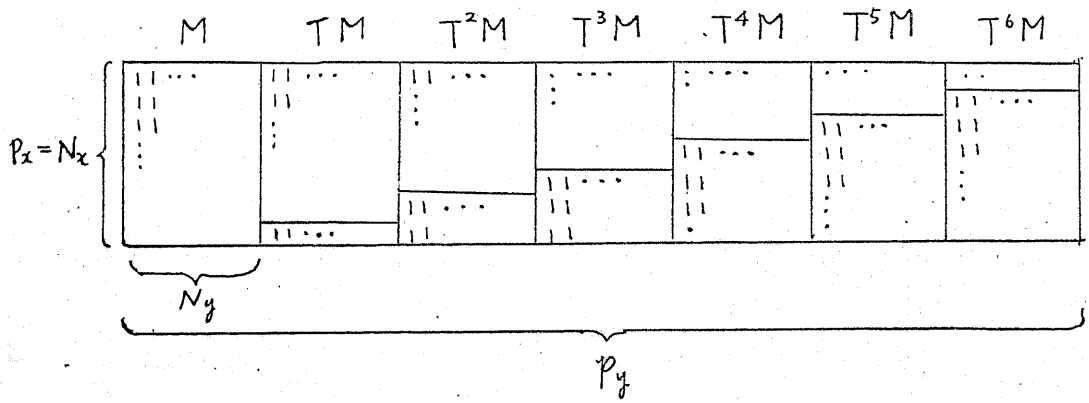
$P_x=7$　　$P_y=63$　　$N_x=7$　　$N_y=9$

(a) 面積 $N_x \times N_y = 7 \times 9$ の最大面積行列

$$M=\begin{bmatrix} \overbrace{1\ 1}^{m} & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\b\\c\end{matrix}}\right\}n \\ \\ \\ \\ \\ \\ \\ \end{matrix} \left.\vphantom{\begin{matrix}a\\b\\c\\d\\e\\f\\g\end{matrix}}\right\} P_x=N_x$$

$\underbrace{\qquad\qquad}_{N_y}$

(b) $\gamma\beta$ − 平面の一周期内における最大面積行列の配置



$$T=\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \vdots \\ 0 & 0 & 0 & 1 & \ddots \\ \vdots & \vdots & & \ddots & 0 \\ 0 & \vdots & & & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix} \left.\vphantom{\begin{matrix}a\\b\\c\\d\\e\\f\\g\end{matrix}}\right\} 7$$

$\underbrace{\qquad\qquad}_{7}$

$$h_\beta(y) = \gamma y^2 + \gamma^4 y + \gamma^2$$

をとればよい。このとき、

$$h_{r\beta}(x, y) = xy^2 + (1 + x + x^2)y + x^2$$

となる。したがって、

$$\widetilde{h_r}(x) = x^3 + x + 1$$

$$\widetilde{h_{r\beta}}'(x, y) = y^2 + (1 + x + x^2)y + x$$

ゆえに、式(5.30)(5.32)は

$$f_{k+3,\ell} = f_{k,\ell} + f_{k+1,\ell}$$

$$f_{k,\ell+2} = f_{k+1,\ell} + f_{k,\ell+1} + f_{k+1,\ell+1} + f_{k+2,\ell+1}$$

となる。これにより、図5.2の $\gamma\beta$ - 平面が生成できる。

5.6 $\gamma\beta$ - 平面符号と他の符号の関連

5.6.1 $\gamma\beta$ - 平面とM系列の対応

$GF(q^{nm})$ の原始元 α の $GF(q)$ の上の最小多項式を $h_\alpha(z)$ とし、$h_\alpha(z)$ をパリティ検査多項式とする符号長 $q^{nm}-1$ の巡回符号を C_α で表わす。C_α はM系列符号あるいは一次の短縮化Reed-Muller符号[5]と呼ばれる符号である(第2章2.6.4参照)。C_α と $\gamma\beta$ - 平面符号との対応がつぎの定理に

に示される。

定理5.9：$e_\alpha = q^{nm}-1$ とおき，z に関する $e_\alpha-1$ 次以下の GF(q) の上のすべての多項式の集合を $P_{e_\alpha-1}$ で表わす。また，x について N_x-1 次，y について N_y-1 次以下の GF(q) の上のすべての多項式の集合を P とする。さらに P の元 $a'(x,y)$ に対し

$$a(x,y)=\sum_{k=0}^{K-1} x^{l(k)} y^{N_y k} a'(x,y)$$

となる $a(x,y)$ すべての集合を Q とおく。ただし

$$l(k)=-\eta\lambda k \bmod P_x \qquad K=(q^n-1)/\mu\lambda$$

である。

ここで，Q から $P_{e_\alpha-1}$ への写像 θ を

$$\theta:\ a(x,y)\rightarrow a(z)=a'(z^{N_y},z^{\lambda}) \bmod (z^{e_\alpha}-1) \quad (5.33)$$

によって定義する。ただし $a'(x,y)$ ($\in P$) は $a(x,y)$ の y について N_y-1 次以下の部分をとり出した多項式である。このとき θ は Q から $P_{e_\alpha-1}$ の上への1対1の写像となる。

また，$\gamma\beta$ - 平面符号 $C_{\alpha\beta}$ は Q に含まれ，その θ による像は M系列符号 C_α となる。また逆に $P_{e_\alpha-1}$ に含まれる長さ e_α の M系列符号の，θ の逆写像 θ^{-1} ($P_{e_\alpha-1}\rightarrow Q$) による像

は $\gamma\beta$ - 平面符号となる。

(証明) θ はつぎの二つの写像 θ_1, θ_2 の合成写像 $\theta_2 \circ \theta_1$ である。

$$\theta_1 : a(x, y) \to a'(x, y)$$

$$\theta_2 : a'(x, y) \to a(z) = a'(z^{N_y}, z^{\eta\lambda}) \mod (z^{e_\alpha} - 1)$$

θ_1 は明らかに Q から P の上への1対1の写像である。また, θ_2 によって $a'(x, y)$ の係数 a_{ij} ($0 \le i < N_x$, $0 \le j < N_y$) は $a(z)$ の z^l ($l = N_y i + \eta\lambda j \mod e_\alpha$) の項の係数 a_l にうつる。ここで,

$$l_1 = N_y i_1 + \eta\lambda j_1 \mod e_\alpha \quad \begin{pmatrix} 0 \le i_1, i_2 < N_x \\ 0 \le j_1, j_2 < N_y \end{pmatrix}$$

$$l_2 = N_y i_2 + \eta\lambda j_2 \mod e_\alpha$$

であるとしよう。$l_1 = l_2$ とすれば $\alpha^{l_1} = \alpha^{l_2}$。ゆえに, $\gamma^{i_1}\beta^{j_1} = \gamma^{i_2}\beta^{j_2}$。すなわち

$$\gamma^{i_1 - i_2}\beta^{j_1 - j_2} = 1 \qquad (5.34)$$

となる。ところが, 補題5.3の証明から明らかなように, $-N_x < i_1 - i_2 < N_x$, $-N_y < j_1 - j_2 < N_y$ において式(5.34)が成立するのは $i_1 = i_2$, $j_1 = j_2$ のときに限る。また, $N_x N_y = q^{nm} - 1 = e_\alpha$ であるから, θ_2 によって (i, j)

$(0 \leq i < N_x,\ 0 \leq j < N_y)$ と l $(0 \leq l < e_\alpha)$ とは1対1に対応する。すなわち，$a(f)$ の係数は $a'(x, y)$ の係数をこの対応によって並べ替えたものである。以上によって $\theta = \theta_2 \cdot \theta_1$ が1対1の全射であることが分った。

系5.3.1から $C_{\alpha\beta}$ の符号語 $f(x, y)$ は Q に属すことが分る。また，$f(x, y)$ の係数 f_{ij} に対応する $C_{\alpha\beta}$ の生成行列 G の成分は $\alpha^{-N_y i - \eta\lambda j} = \alpha^{-l}$ であるから，$C_{\alpha\beta}$ の θ による像 $\theta C_{\alpha\beta}$ は次の生成行列をもつ。

$$\left[\alpha^0\ \alpha^{-1}\ \alpha^{-2}\ \cdots\ \alpha^{-e_\alpha+1}\right] \qquad (5.35)$$

ここに，α^{-l} は $GF(q)$ の上の nm 次元縦ベクトルとして表わすものとする。この行列はM系列符号 C_α の生成行列に他ならない。また，容易に確かめられるように $\gamma\beta$ - 平面符号の像以外に $P_{e_{\alpha-1}}$ に含まれる長さ e_α のM系列符号は存在しない。このことから，逆は明らかである。 (証明終)

この定理から，$\gamma\beta$ - 平面は $GF(q)$ の上の長さ $q^{nm}-1$ のM系列に θ の逆写像を作用させることによっても構成できることが分る。$\gamma\beta$ - 平面を計算機を用いて実際に構成するような場合には，このようにして作るのが，もっとも簡単で

あると思われる。

また，$\gamma\beta$－平面符号 $C_{\gamma\beta}$ のある種の構造は，この定理によって対応するM系列符号 C_α の性質を調べることにより，簡単に知ることのできる場合もある。たとえば，C_α を不変に保つ置換[5]に θ の逆写像によって対応する置換は $C_{\alpha\beta}$ を不変に保つ。

5.6.2 $\gamma\beta$－平面符号と直積符号との関係

符号理論において，二次元に配列した符号としては，巡回積符号（cyclic product code）[3]などの直積符号（direct product code, iterated code）[1][2]がよく知られている。直積符号は本章で述べた $\gamma\beta$－平面符号とは，その目的も構成理論もまったく異なるが，つぎの定理に示すような関係をもつ。

定理5.10： γ, β の $GF(q)$ の上の最小多項式をそれぞれ $h_\gamma(x)$, $h_\beta'(y)$ とおき，$h_\gamma(x)$ をパリティ検査多項式とする $GF(q)$ の上の長さ p_x の巡回符号を C_γ，$h_\beta'(y)$ をパリティ検査多項式とする $GF(q)$ の上の長さ p_y の巡回符号を C_β' とする。このとき，$\gamma\beta$－平面符号 $C_{\gamma\beta}$ は，C_γ と

C_β' の直積符号 $C_\gamma \times C_\beta'$ の部分符号となっている。

特に，$C_{\gamma\beta}$ が $C_\gamma \times C_\beta'$ と一致するのは $p_x\ (= N_x)$ が，$q-1$ の約数となっているときに限る。

(証明) $C_{\gamma\beta}$ の生成行列 $G = \{\gamma^{-i}\beta^{-j}\}$ の形から，$\gamma\beta$ - 平面符号 $f(x,y) = \sum_{i=0}^{p_x-1}\sum_{j=0}^{p_y-1} f_{ij}x^i y^j$ において，$\sum_{i=0}^{p_x-1} f_{ik}x^i$ ($k = 0,1,\cdots,p_y-1$) は C_γ に属し，$\sum_{j=0}^{p_y-1} f_{lj}y^j$ ($l = 0,1,\cdots,p_x-1$) は C_β' に属することが分る。ゆえに $C_{\gamma\beta} \subseteq C_\gamma \times C_\beta'$ である。

また，$C_\gamma \times C_\beta'$ の次元（情報シンボル数）は（C_γ の次元）×（C_β' の次元）であるから，$n \times$（$h_\beta'(y)$ の次数）となる。$h_\beta'(y)$ の次数は

$$\lambda\eta(q^d-1) = 0 \mod (q^{nm}-1)$$

を満たす最小の正整数 d として求められる[2]。$\lambda \mid q^n-1$ および η が $q^{nm}-1$ と素であることから，q^d-1 は

$$q^d-1 = \frac{q^{nm}-1}{q^n-1}\,a = (q^{n(m-1)} + q^{n(m-2)} + \cdots + q^n + 1)a \quad (a: \text{正整数})$$

となる形で書けねばならない。ところが，この式の右辺の形からただちに分るように，右辺が q^d-1 となる形になるためには $a \geq q^n-1$ でなければならない。ゆえに $d \geq nm$。このことからただちに $h_\beta'(y)$ の次数が nm となることが分る。

ゆえに，$C_\gamma \times C_\beta'$ の次元は n^2m である。これに対し $C_{\gamma\beta}$ の次元は nm であるから，$C_{\gamma\beta} = C_\gamma \times C_\beta'$ となるのは $n=1$ のときに限る。$p_x = (q^n-1)/\mu$ であるから，このとき $p_x \mid q-1$ となる。 (証明終)

この定理の証明から明らかなように，$\gamma\beta$ - 平面符号は一般に直積符号のきわめて小さな部分符号となっている。

5.7 $\gamma\beta$ - 平面の自己相関函数

5.7.1 自己相関函数の定義

はじめに，自己相関函数を一般的に定義しておこう。

GF(q) の直積 GF(q) × GF(q) から実数への写像

$$\varphi : (a, b) \longrightarrow \varphi(a, b)$$

を定義する。ただし，φ はつぎの三つの条件を満たすと仮定する。すなわち，任意の GF(q) の二つの元 a, b に対し，

$$\varphi(a, b) = \varphi(b, a) \qquad (5.36)$$

また，任意の GF(q) の元 a に対し，

$$\varphi(a, a) > 0 \qquad (5.37)$$

さらに，

$$\sum_{a\in GF(q)}\sum_{b\in GF(q)}\varphi(a,b)=0 \qquad (5.38)$$

φ は $GF(q)$ の元に実際に何を対応させるかによって定めるべきものであり，この仮定は多くの場合妥当であろう。平面 $a(x,y)$ に対し，この φ によって自己相関函数をつぎのように定義する．

$$\rho_\varphi(\tau_1,\tau_2)=\sum_{i=0}^{p_x-1}\sum_{j=0}^{p_y-1}\varphi(a_{ij},a_{i+\tau_1,j+\tau_2})\Big/\Delta \qquad (5.39)$$

ここに，p_x，p_y は平面 $a(x,y)$ の周期であり，a_{uv} の添字 u, v はそれぞれ法を p_x，p_y として定めるものとする。また，Δ は次式で与えられる．

$$\Delta=\sum_{i=0}^{p_x-1}\sum_{j=0}^{p_y-1}\varphi(a_{ij},a_{ij}) \qquad (5.40)$$

式(5.37)から Δ は正である．

ここで，さらに $GF(q)$ の元 a に対し

$$\chi(a)=\sum_{b\in GF(q)}\varphi(b,ab) \qquad (5.41)$$

を定義しておく．

(注意) ここで定義された自己相関函数は，第2章 2.2 で述べた符号における距離と密接な関連をもつ．

いま，写像 φ が式(5.36)(5.37)(5.38)に加え，さらに異な

る GF(q) の任意の二つの元 a, b に対し.

$$\varphi(a,a)+\varphi(b,b)-2\varphi(a,b)>0$$

を満たすと仮定しよう。このとき

$$d(a,b)=\varphi(a,a)+\varphi(b,b)-2\varphi(a,b)$$

によって GF(q) の上に距離 $d(a,b)$ を定義する. 明らかに $d(a,b)$ は非負の実数であり, 才2章 2.2 に示した距離の三公理のうち, (i)(ii) を満たす。しかし, 三角不等式は満たすとは限らない。したがって $d(a,b)$ は才2章 2.2 で述べた意味で擬距離となっていることもある.

さらに, GF(q) の上の任意の二つの $p_x \times p_y$ 行列 $A=\{a_{ij}\}$, $B=\{b_{ij}\}$ に対しても, 才2章と同様に

$$d[A,B]=\sum_{i=0}^{p_x-1}\sum_{j=0}^{p_y-1} d(a_{ij},b_{ij})$$

によって距離を定義する。ここで B として $B=\{a_{i+\tau_1,j+\tau_2}\}$ となるものをとるとする。ここに τ_1, τ_2 はおのおの p_x, p_y 以下の非負の整数であり, $i+\tau_1$, $j+\tau_2$ はそれぞれ法を p_x, p_y として定めるものとする。このとき, 平面 A (A を線速し並べた半無限行列) の自己相関函数と距離 $d[A,B]$ は明らかに, つぎの関係をもつ.

$$d[A,B] = 2\sum_{i=0}^{p_x-1}\sum_{j=0}^{p_y-1}\{\varphi(a_{ij},a_{ij}) - \varphi(a_{ij},a_{i+\tau_1,j+\tau_2})\}$$

$$= 2\Lambda(1 - \rho_\varphi(\tau_1,\tau_2))$$

ただし，Λは式(5.40)で定義されているものである．

5.7.2 $\gamma\beta$ - 平面の自己相関函数

$\gamma\beta$ - 平面の自己相関函数は 5.5 の結果を用いて導くことができる．

定理 5.11： $\gamma\beta$ - 平面の一周期内における自己相関函数 $\rho_\varphi(\tau_1,\tau_2)$ $(0 \le \tau_1 < p_x,\ 0 \le \tau_2 < p_y)$ はつぎのようになる．

$$\begin{cases} \tau_1 = -\eta\lambda k + K_1 e l \mod p_x \\ \tau_2 = N_y k + K_2 e l \mod p_y \end{cases} \tag{5.42}$$

$$(0 \le k < (q^m-1)/\mu\lambda,\ 0 \le l < q-1)$$

となる τ_1, τ_2 に対しては

$$\rho_\varphi(\tau_1,\tau_2) = \{q^{nm-1}\chi(\delta^l) - \varphi(0,0)\}/\sigma \tag{5.43}$$

ここに，N_y は式(5.22)で与えられ，K_1, K_2 は次式を満たす整数である．

$$N_y K_1 + \eta\lambda K_2 = 1 \mod (q^{nm}-1) \tag{5.44}$$

また，$e = (q^{nm}-1)/(q-1)$ であり，δ は GF(q) の原

始元で　$\delta = \alpha^e$　で定義される。さらに

$$\sigma = q^{nm-1}\chi(1) - \varphi(0,0) \tag{5.45}$$

である。

式(5.42)以外の τ_1, τ_2 に対しては

$$f_\varphi(\tau_1, \tau_2) = -\varphi(0,0)/\sigma \tag{5.46}$$

となる。

(注意) 式(5.8)より $GCD(N_y, \eta\lambda) = 1$ であるから，式(5.44)を満たす K_1, K_2 はユークリッドアルゴリズム[8]を用いれば容易に求められる。

(証明) 系5.7.1から式(5.40)の ρ は

$$\rho = \{q^{nm-1}\chi(1) - \varphi(0,0)\}(q^n-1)/\mu\lambda \tag{5.47}$$

となることがただちに導ける。

つぎに，$\gamma\beta$ - 平面 $f(x,y)$ に対し，式(5.27)によって，$f^{(i,j)}(x,y)$ を定義すれば $f_\varphi(\tau_1, \tau_2)$ はつぎのように書き直せる。

$$f_\varphi(\tau_1, \tau_2) = \sum_{i=0}^{P_x-1}\sum_{j=0}^{P_y-1} \varphi\left(f_{00}^{(i,j)}, f_{\tau_1,\tau_2}^{(i,j)}\right)/\rho$$

さらに，系5.3.1および式(5.45)(5.47)から

$$f_\varphi(\tau_1, \tau_2) = \sum_{i=0}^{N_x-1}\sum_{j=0}^{N_y-1} \varphi\left(f_{00}^{(i,j)}, f_{\tau_1,\tau_2}^{(i,j)}\right)/\sigma \tag{5.48}$$

ここで，$\gamma^{\tau_1}\beta^{\tau_2} \in GF(q)$ であるとしよう。このとき補題5.2から

$$x^{\tau_1} y^{\tau_2} f(x, y) = \gamma^{\tau_1}\beta^{\tau_2} f(x, y)$$

を得る。ゆえに，式(5.48)は

$$\begin{aligned} P_\varphi(\tau_1, \tau_2) &= \sum_{i=0}^{N_x-1} \sum_{j=0}^{N_y-1} \varphi\left(f_{00}^{(i,j)}, \gamma^{\tau_1}\beta^{\tau_2} f_{00}^{(i,j)}\right)/\sigma \\ &= \sum_{i=0}^{N_x-1} \sum_{j=0}^{N_y-1} \varphi\left(f_{ij}^{(0,0)}, \gamma^{\tau_1}\beta^{\tau_2} f_{ij}^{(0,0)}\right)/\sigma \end{aligned} \quad (5.49)$$

となる。系5.7.1および式(5.41)を用いれば，さらに

$$P_\varphi(\tau_1, \tau_2) = \{q^{nm-1}\chi(\gamma^{\tau_1}\beta^{\tau_2}) - \varphi(0,0)\}/\sigma \quad (5.50)$$

となることが容易に確かめられる。

つぎに，$\gamma^{\tau_1}\beta^{\tau_2} \in GF(q)$ となる τ_1, τ_2 を導こう。いま $\gamma^{\tau_1}\beta^{\tau_2} = \delta^l = \alpha^{el}$ $(0 \le l < q-1)$ とすれば

$$N_y \tau_1 + \eta\lambda \tau_2 = el \mod (q^{nm}-1) \quad (5.51)$$

となる。両辺に K_1 を掛け，式(5.44)を用いれば，

$$\tau_1 - \eta\lambda K_2 \tau_1 + K_1 \eta\lambda \tau_2 = K_1 el \mod (q^{nm}-1)$$

を得る。したがって，$\lambda \mid q^{nm}-1$ に注意すれば

$$\tau_1 = K_1 el \mod \lambda$$

でなければならない。全く同様にして

$$\tau_2 = K_2 el \mod N_y$$

を得る。ここで、

$$\tau_1 = K_1 e l + \lambda k_1 \qquad \tau_2 = K_2 e l + \lambda k_2$$

とおき、式(5.51)に代入すれば

$$k_1 = -\eta k_2 \mod (q^n-1)/\mu\lambda$$

となる。これから、$k_2 = k$ とおけば、ただちに、式(5.42)が導ける。また、そのとき式(5.50)は式(5.43)となる。

式(5.42)以外の τ_1, τ_2 では $\gamma^{\tau_1}\beta^{\tau_2} \notin GF(q)$ となるから、明らかに、$C_{\gamma\beta}$ の生成行列 G において、g_{00} ($\in GF(q)$) および $g_{\tau_1\tau_2}$ ($= \gamma^{-\tau_1}\beta^{-\tau_2} \notin GF(q)$) を含む $GF(q)$ の上で互いに独立な nm 個の成分を選び得る。ゆえに補題5.6から、$(f_{00}^{(i,j)}, f_{\tau_1\tau_2}^{(i,j)})$ $(0 \le i < N_x,\ 0 \le j < N_y)$ には $(0,0)$ は $q^{nm-2}-1$ 回、それ以外の $GF(q)$ の二つの元のすべての組合せはおのおの q^{nm-2} 回づつ現れることが分る。このことと、式(5.38)および式(5.48)から、式(5.46)を得る。(証明終)

この定理から、$\gamma\beta$ 一平面の自己相関函数 $\rho_\varphi(\tau_1, \tau_2)$ はつぎのような特徴をもつことが分る。

(i) $\rho_\varphi(\tau_1, \tau_2)$ は高々 q 通りの値しかとらない。

(ii) $0 \le \tau_1 < N_x$, $0 \le \tau_2 < N_y$ の範囲では $-\varphi(0,0)/\sigma$ と

異なる $P_\varphi(\tau_1, \tau_2)$ の値が現れるのは高々 $q-1$ 個の点においてである。

(iii) 式(5.42)で与えられる (τ_1, τ_2) の集合 T^2 において，任意の一つの元を $(\tau_1^\circ, \tau_2^\circ)$ とすると，

$$\{(\tau_1 - \tau_1^\circ, \tau_2 - \tau_2^\circ) \mid (\tau_1, \tau_2) \in T^2\}$$

となる集合は，法を (p_x, p_y) として再び T^2 となる。

この意味で，$-\varphi(0,0)/\sigma$ と異なる $P_\varphi(\tau_1, \tau_2)$ の値が現れる点は $\gamma\beta$-平面において一様に分布している。

このように，$\gamma\beta$-平面の自己相関函数には著しい特徴があり，種々の応用が考えられる。

つぎに，二値 $\gamma\beta$-平面の自己相関函数の例を示しておこう。

例5.3) $q=2$ とし，φ を

$$\varphi(0,0) = \varphi(1,1) = 1$$

$$\varphi(1,0) = \varphi(0,1) = -1$$

によって定める。このとき，$\chi(1)=2$，$e=0 \mod(2^{nm}-1)$，$\delta=1$，$\sigma = 2^{nm}-1$ となる。ゆえに，$\gamma\beta$-平面の自己相関函数は次式で与えられる。

$$\rho_\varphi(\tau_1,\tau_2)=\begin{cases} 1\ ; & \begin{cases}\tau_1=-\lambda k \bmod p_x \\ \tau_2=N_y k\end{cases} \quad \left(0\le k<\dfrac{2^n-1}{\mu\lambda}\right) \\ \dfrac{-1}{2^{nm}-1}\ ; & \text{その他の場合}\end{cases}$$

5.8 γβ-平面の多次元への拡張

γβ-平面はまた容易に多次元に拡張することができる。ここでは三次元への拡張について述べておく。四次元以上への拡張も同様に行える。

議論はほとんど二次元の場合と並行しているので，ここでは概略を述べるに止める。

二次元の場合の最大面積行列をもつという性質に対応して，三次元の場合にも"最大容積（三次元）行列"をもつという性質を定義することが可能である。ここに述べるγβδ-立体はそのような最大容積行列をもつ立体（三次元の配列）となっている。

また，三次元線形巡回符号，あるいは生成四次元行列なども二次元の場合から，簡単な拡張によって定義できる。

5.8.1 γβδ－立体および γβδ－立体符号の定義

q を素数のべき，n_1, n_2, n_3 を正整数とする．また，μ_1, μ_2, λ_1, λ_2 をつぎの条件を満たす正整数とする．

$$\mu_1 \mid q^{n_1}-1 \tag{5.52}$$

$$\mathrm{GCD}\left(\frac{q^{n_1 n_2}-1}{q^{n_1}-1}\mu_1,\ \lambda_1\right)=1 \tag{5.53}$$

$$\mu_1\lambda_1 \mid \mu_2(q^{n_1}-1) \tag{5.54}$$

$$\mathrm{GCD}\left(\frac{q^{n_1 n_2 n_3}-1}{q^{n_1 n_2}-1}\mu_2,\ \lambda_2\right)=1 \tag{5.55}$$

$$\mu_2\lambda_2 \mid q^{n_1 n_2}-1 \tag{5.56}$$

$$\frac{q^{n_1}-1}{\mu_1} \mid q^k-1 \quad \text{であれば} \quad k \geq n_1 \tag{5.57}$$

$$\frac{q^{n_1 n_2}-1}{\lambda_1} \mid q^{n_1 l}-1 \quad \text{であれば} \quad l \geq n_2 \tag{5.58}$$

つぎに，$\mathrm{GF}(q^{n_1 n_2 n_3})$ の原始元を α とし，η_1, η_2 を $q^{n_1 n_2 n_3}-1$ と素な正整数として，

$$\gamma=\alpha^{\frac{q^{n_1 n_2 n_3}-1}{q^{n_1}-1}\mu_1} \qquad \beta=\alpha^{\frac{q^{n_1 n_2 n_3}-1}{q^{n_1 n_2}-1}\lambda_1\eta_1} \qquad \delta=\alpha^{\lambda_2\eta_2}$$

を定義する．これらの位数はそれぞれ

$$e_\gamma=\frac{q^{n_1}-1}{\mu_1} \qquad e_\beta=\frac{q^{n_1 n_2}-1}{\lambda_1} \qquad e_\delta=\frac{q^{n_1 n_2 n_3}-1}{\lambda_2} \tag{5.59}$$

となる．ここで，

$h_r(x)$: γ の $GF(q)$ の上の最小多項式

$h_\beta(y)$: β の $GF(q^{n_1})$ の上の最小多項式

$h_\delta(z)$: δ の $GF(q^{n_1 n_2})$ の上の最小多項式

を定義する。明らかに

$$\deg h_\gamma(x) = n_1$$

$$\deg h_\beta(y) = n_2$$

$$\deg h_\delta(z) = n_3$$

である。ただし，deg は次数を示すものとする。

ここで，二次元の場合と同様にして，$h_\beta(y)$ の係数を $GF(q)$ の上の x の多項式に対応させることにより，$GF(q)$ の上の x, y の多項式 $h_{\gamma\beta}(x, y)$ を作る。すなわち，$h_{\gamma\beta}(\gamma, y) = h_\beta(y)$ となる x について $n_1 - 1$ 次以下，y について $n_2 - 1$ 次以下の多項式を $h_{\gamma\beta}(x, y)$ とするのである。同様に，$h_\delta(z)$ から，$h_{\beta\delta}(\beta, z) = h_\delta(z)$ となる $GF(q^{n_1})$ の上の多項式 $h_{\beta\delta}(y, z)$ を作り，これからさらに $h_{\gamma\beta\delta}(\gamma, y, z) = h_{\beta\delta}(y, z)$ となる $GF(q)$ の上の多項式 $h_{\gamma\beta\delta}(x, y, z)$ を作る。

このとき，法を $(x^{e_r} - 1, y^{e_\beta} - 1, z^{e_r} - 1)$ とする多項式の剰余環 $\Lambda(x^{e_r} - 1, y^{e_\beta} - 1, z^{e_r} - 1)$ の上の連立方程式

$$\begin{cases} h_\gamma(x) f(x,y,z) = 0 & (5.60) \\ h_{\gamma\beta}(x,y) f(x,y,z) = 0 & (5.61) \\ h_{\gamma\beta\delta}(x,y,z) f(x,y,z) = 0 & (5.62) \end{cases}$$

を満たす $GF(q)$ の上の多項式 $f(x,y,z)$ すべての集合が，$\gamma\beta$-平面符号の三次元への拡張となっている。これを $\gamma\beta\delta$-立体と呼び $C_{\gamma\beta\delta}$ で表わす。また $C_{\gamma\beta\delta}$ の0でない符号語を $\gamma\beta\delta$-立体と呼ぶ。

5.8.2 $\gamma\beta\delta$-立体の構造

$\gamma\beta\delta$-立体 $C_{\gamma\beta\delta}$ は明らかに三次元線形巡回符号である。また，二次元の場合と同様な手順を繰返すことによって，式 (5.60) (5.61) (5.62) の解 $f(x,y,z)$ が

$$h_\delta(z) f(\gamma,\beta,z) = 0 \qquad (5.63)$$

の解 $f(\gamma,\beta,z)$ と1対1に対応することが分る。したがって，$C_{\gamma\beta\delta}$ の符号語数は $q^{m_1 m_2 m_3}$ となる。

二次元の場合の補題 5.2 に対応してつぎの補題が導ける。

補題 5.12： $\gamma\beta$-平面 $f(x,y,z)$ に対し，多項式 $a(x,y,z)$ $(\in \Lambda(x^{e_\gamma}-1, y^{e_\beta}-1, z^{e_\delta}-1))$ が，

$$a(x,y,z)\,f(x,y,z)=0$$

を満たす必要十分条件は $a(\gamma,\beta,\delta)=0$ となることである。

証明は二次元の場合とほとんど同様である。

この補題から、$\gamma\beta\delta$ー立体の周期 (p_x, p_y, p_z) は

$$p_x=e_\delta \qquad p_y=e_\beta \qquad p_z=e_\delta \tag{5.64}$$

で与えられることが分る。

また、$\gamma\beta\delta$ー立体符号は、二次元の場合の補題5.4と同様つぎのように表現できる。

補題5.13：$\gamma\beta\delta$ー立体符号 $C_{\gamma\beta\delta}$ はその0でない符号語 $(\gamma\beta\delta$ー立体$)\ f(x,y,z)$ を用いて、つぎのように表せる。

$$C_{\gamma\beta\delta}=\{x^i y^j z^k f(x,y,z) \mid 0\le i<N_x,\ 0\le j<N_y,\ 0\le k<N_z\}\cup\{0\} \tag{5.65}$$

ただし、N_x, N_y, N_z は次式で与えられる。

$$N_x=\frac{q^{n_1}-1}{\mu_1} \qquad N_y=\frac{(q^{n_1n_2}-1)\mu_1}{(q^{n_1}-1)\mu_2} \qquad N_z=\frac{q^{n_1n_2n_3}-1}{q^{n_1n_2}-1}\mu_2 \tag{5.66}$$

(略証) $0\le i<N_x$, $0\le j<N_y$, $0\le k<N_z$ となる i, j, k の範囲で、$i=j=k=0$ の場合を除いては、次式の成立しないことを言えばよい。

$$\frac{q^{n_1n_2n_3}-1}{q^{n_1}-1}\mu_1 i + \frac{q^{n_1n_2n_3}-1}{q^{n_1n_2}-1}\eta_1\lambda_1 j + \eta_2\lambda_2 k = 0 \mod (q^{n_1n_2n_3}-1) \tag{5.67}$$

式(5.66)を用いて書き直せば,

$$N_z\left(N_y i + \frac{\eta_1\lambda_1}{\mu_2} j\right) + \eta_2\lambda_2 k = 0 \mod (q^{n_1n_2n_3}-1)$$

となる. 式(5.56)から $N_z \mid q^{n_1n_2n_3}-1$. ゆえに式(5.55)を用いれば

$$k = 0 \mod N_z$$

を得る。したがって, $0 \le k < N_z$ で式(5.67)が成立するのは $k=0$ のときに限る. このとき

$$N_y i + \frac{\eta_1\lambda_1}{\mu_2} j = 0 \mod \frac{q^{n_1n_2}-1}{\mu_2}$$

となる。式(5.52)から $N_y \mid (q^{n_1n_2}-1)/\mu_2$ であり, 式(5.53)より, N_y と $\eta_1\lambda_1/\mu_2$ は互いに素となるから,

$$j = 0 \mod N_y$$

ゆえに, $0 \le j < N_y$ であれば $j=0$ でなければならない。このとき, 式(5.67)から $i = 0 \mod N_x$ となり, 式(5.67)が成立するのは $i=j=k=0$ のときに限ることが分る.

(略証終)

BCH平面符号の生成(四次元)行列は, 二次元の場合と全く同様に考えて,

$$G=\{g_{ijk}\}=\{\gamma^{-i}\beta^{-j}\delta^{-k}\} \qquad (5.68)$$

となることが分る．すなわち，G の要素 g_{ijk} ($\in GF(q^{n_1n_2n_3})$) を $GF(q)$ の上の $n_1n_2n_3$ 次元ベクトルとして表わし，このようなベクトルの ijk 成分を (i,j,k) 要素とする $GF(q)$ の上の三次元行列 G_l ($l=1,\cdots,n_1n_2n_3$) が $C_{\gamma\beta\delta}$ の基底をなすのである．

明らかに G の要素 $\{g_{ijk}\mid 0\le i<n_1,\ 0\le j<n_2,\ 0\le k<n_3\}$ は $GF(q)$ の上で互いに独立であるから，補題 5.13 を用い，二次元の場合と同様にして，つぎの定理を容易に導くことができる．

定理 5.14：$\gamma\beta\delta$-立体は周期 $(P_x,P_y,P_z)=\left(\frac{q^{n_1}-1}{\mu_1},\ \frac{q^{n_1n_2}-1}{\lambda_1},\ \frac{q^{n_1n_2n_3}-1}{\lambda_2}\right)$ をもち，容積 $N_x\times N_y\times N_z=\frac{q^{n_1}-1}{\mu_1}\times\frac{(q^{n_1n_2}-1)\mu_1}{(q^{n_1}-1)\mu_2}\times\frac{q^{n_1n_2n_3}-1}{q^{n_1n_2}-1}\mu_2$ の最大容積行列をもつ．特に，$\mu_1\lambda_1=\mu_2(q^{n_1}-1)$，$\mu_2\lambda_2=q^{n_1n_2}-1$ となるときには，$P_x=N_x$，$P_y=N_y$，$P_z=N_z$ となる．この場合を $\gamma\beta\delta$-M立体と呼ぶ．

定理 5.8 に対応する定理はつぎのようになる．

定理5.15： $K_1 \cdot K_2 \cdot K_3 = q^N - 1$ とする。このとき，容積 $K_1 \times K_2 \times K_3$ の最大容積行列をもつ $\gamma\beta\delta$-立体が存在する。また，K_1，K_2，K_3 のどの二つも互いに素であれば，容積 $K_1 \times K_2 \times K_3$ の最大容積行列をもつ $\gamma\beta\delta$-M立体が存在する。

（略証） n_1 を $K_1 \mid q^{n_1} - 1$，$n_1 \mid N$ となる最小の正整数とする。つぎに n_2 を $K_1 \cdot K_2 \mid q^{n_1 n_2} - 1$，$n_1 n_2 \mid N$ となる最小の正整数とし，$\mu_2 = (q^{n_1 n_2} - 1) / K_1 \cdot K_2$ とする。さらに，λ_1 を式(5.53)(5.54)(5.58)を満たすように選び，λ_2 を式(5.55)(5.56)を満たすように選ぶ。このような λ_1，λ_2 は少くとも一組は存在する。たとえば，$\lambda_1 = \mu_2$，$\lambda_2 = 1$ とすればよい。これらのパラメータが式(5.52)～(5.58)を満たすことは明らかであり，また $K_1 = N_x$，$K_2 = N_y$，$K_3 = N_z$ となる。

K_1，K_2，K_3 のどの二つも互いに素なら $\lambda_1 = \mu_2 (q^{n_1} - 1) / \mu_1$ $\lambda_2 = (q^{n_1 n_2} - 1) / \mu_2$ と選ぶことができ，$\gamma\beta\delta$-M立体を構成できる。 （略証終）

以上 $\gamma\beta$-平面の三次元への拡張について概略を述べた。ここでは自己相関函数については省略したが，これも二次元の場合と全く同様な手法で求めることができる。三次元の場

合の自己相関函数も，5.7.2の(i)(ii)(iii)に対応する性質をもつことは容易に類推できるであろう．

5.9 むすび

本章では最大面積行列をもつ平面として，$\gamma\beta$-平面を示し，その構成法および自己相関函数などの諸性質を明らかにした．

今後に残された問題は，理論的な面では，最大面積行列をもつ平面で$\gamma\beta$－平面以外のものが存在するか，また存在するとすれば，どのようなものであるかということである．しかし，より重要な問題は$\gamma\beta$－平面および$\gamma\beta$－平面符号の応用面を開発することであろう．

なお，式(5.9)のβの定義におけるηは福田によって見出されたものであり，これにより，$\gamma\beta$－平面の細かな構造はより豊かなものとなった．

また，現在，福田らの努力により，$\gamma\beta$－平面のより詳しい構造が明らかにされつつある[67]．

第6章

多次元線形通信系の大域的最適化

前章までは，符号の構造および構成法について論じてきた．これらは，符号の設計問題とも言えるであろう．これに対し，本章では信号の設計問題を扱う．信号設計問題には大きく，二つの方向がある．一つはいわゆるM元ディジタル信号の設計問題で，符号理論とも密接な関係をもつ．これについては付録IIに解説されている．他の一つはアナログ信号の設計問題であり，本章で論ずるのは，この問題の一つの例である．

アナログ通信系として，線形通信系はその構成が簡単である点などから興味深い．線形通信系の一つに多次元線形通信系がある．これは有限個のアナログ情報を並列に伝送する通信系で，送信機では情報を送信行列を用いて線形変換することにより，送信信号を作り，受信機では受信信号を受信行列を用いて線形変換することにより復調を行う．本章はこのよ

うな通信系の最適化に関するものである。

はじめに、受信行列として送信行列の一般逆行列を用いるという条件の下に復調出力の二乗平均誤差を最小とする送信行列を求め、ついで無ひずみ条件の下に二乗平均誤差を最小とする送信行列と受信行列を求める。このような問題は一応解かれてはいるが、これまで局所的に最適であることしか言えていない。これに対し、本章では置換多面体の理論を用い大域的に最適な解を求めている。

本章では、特に距離を論ずることはしない。しかし、本章における評価量（復調出力の二乗平均誤差）は信号空間における距離（リーマン計量）として扱うこともできる(70)。このような立場から言えば、ここでは、信号空間における信号と雑音のなす距離構造、およびそれによる信号の設計の問題を論じていることとなる。

6.1 はじめに

受信情報の信頼を評価基準として通信系を設計する場合、送、受信機が線形であるという条件を課すことは、一般にか

なり厳しい制約となる。実際，多くの場合，非線形な送，受信機を用いることによって，線形の場合よりも品質の高い通信を行うことができる。しかし，線形通信系は，オーに送，受信機の構成が簡単であること，したがって経済的に有利であり，また取扱いも容易であること，さらに概念的に簡単であり，解析が容易であることなどの点から，きわめて興味深いものと言える。

線形通信系の一つのモデルに，図6.1に示すような多次元線形通信系がある。これは有限個のアナログ情報を並列に伝送する通信系で，送信機では情報を送信行列によって線形変換することにより送信信号を作り，受信機では受信信号を受信行列を用いて線形変換することにより復調を行う方式である。いうまでもなく，この通信系のモデルは有限個のアナログ情報を直列に伝送する通信系のモデルに書きかえることもできる。また，波形を伝送する一般のアナログ通信系は標本値のみを考えれば，このような通信系のモデルによって近似できることも少くない。

多次元線形通信系の受信機の最適化については古くから論

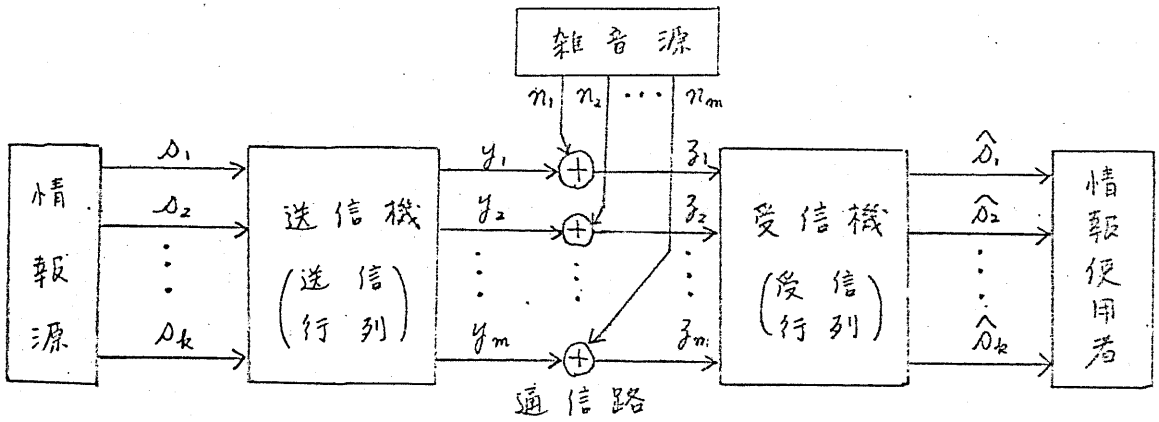


図 6.1　多次元線形通信系の構成

じられている[68]。また，送信機をも含めた通信系の最適化に関する問題も，原理的には甘利[69][70]によって解かれている。また，その後田中ら[71]によって，より分り易い形で解かれた。しかし，これらの最適化は微分的方法を用いているため，得られた結果が大域的に最適（globally optimum）であるかどうか分かっていなかった。

本章では，置換多面体の表現に関する定理を導き，これによって，ある条件の下に多次元線形通信系の最適化を行う。はじめに，受信行列として送信行列の一般逆行列を用いるという条件の下に，多次元線形通信系において，復調出力と情報の間の二乗平均誤差を最小とする送信行列を求める。ついで，無ひずみ条件のある場合について（ただし，受信行列と

して送信行列の一般逆行列を用いるという条件は除いて）二乗平均誤差を最小とする送信行列と受信行列を求めている。後者の場合，結果として，最適な受信行列が送信行列の一般逆行列となることが示される。なお，後者の結果は田中ら[71]の結果と一致している。

一般逆行列による受信方式は，よく用いられる逆行列による受信の一般化として考えられたもので，送信行列や雑音が一定の条件を満たす場合には，最尤推定となる。また，無ひずみ条件は，復調出力中の信号成分が元の情報と一致するという条件で，実際の通信においては望ましい条件である。

6.2 多次元線形通信系

ここで，本章で論ずる多次線形通信系について述べておこう。図6.2に多次元線形通信系をベクトルを用いて表わす。この通信系に対し，つぎのような仮定をする。ただし，$\mathbf{S}$, $\mathbf{y}$などの太字は縦ベクトルを表わすものとする。また，本章では実数のみを扱う。

情報源：情報ベクトル $\mathbf{S}$ を発生する。 $\mathbf{S}$ は n 次元確率

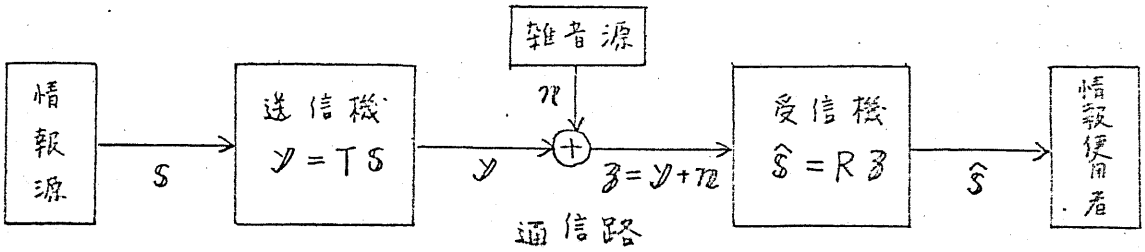


図6.2　多次元線形通信系の構成 —— ベクトル表示

ベクトル s. の標本ベクトルで，k 次元ユークリッド空間に属す。s の平均値は0ベクトル（0 で表わす）とし，共分散行列を Σ_s とする。すなわち，

$$\mathcal{E}_s[s]=0 \qquad \mathcal{E}_s[ss^t]=\Sigma_s \qquad (6.1)$$

ここに $\mathcal{E}_s$ は s に関する平均を示し，s^t は s の転置ベクトルである。

送信機：情報ベクトル s から送信行列 T を用い，

$$y=Ts \qquad (6.2)$$

によって送信ベクトル y を作り，通信路に送出する。y は m 次元ユークリッド空間に属す。また T は $m\times k$ 行列である。

通信路：入力端において，平均送信電力がつぎのように制限されている。

$$\mathcal{E}_S[\|\mathcal{Y}\|^2] \leq mS_0 \qquad (6.3)$$

ここに $\|\ \|$ はユークリッドノルムを示す．すなわち，

$$\|\mathcal{Y}\| = \sqrt{\mathcal{Y}^*\mathcal{Y}}$$

また，通信路には加法的雑音 $\mathcal{N}$ が存在する．$\mathcal{N}$ は $\mathcal{S}$ と独立な m 次元確率ベクトル $\mathcal{N}$ の標本ベクトルで，m 次元ユークリッド空間に属す．$\mathcal{N}$ の平均値は 0，共分散行列は $N_0 \Psi_N$ であるとする．すなわち，

$$\mathcal{E}_N[\mathcal{N}] = 0 \qquad \mathcal{E}_N[\mathcal{N}\mathcal{N}^*] = N_0 \Psi_N \qquad (6.4)$$

ここに，$\mathcal{E}_N$ は $\mathcal{N}$ に関する平均を示す．また N_0 は雑音の一自由度当りの平均電力である．すなわち，

$$N_0 = \mathcal{E}_N[\|\mathcal{N}\|^2]/m \qquad (6.5)$$

受信機：受信ベクトル $\mathcal{Z}$（$=\mathcal{Y}+\mathcal{N}$）から受信行列 R を用い，

$$\hat{\mathcal{S}} = R\mathcal{Z} \qquad (6.6)$$

により，$\mathcal{S}$ の推定量 $\hat{\mathcal{S}}$ を得る．$\hat{\mathcal{S}}$ は k 次元ユークリッド空間に属し，R は $k \times m$ 行列である．また，$\hat{\mathcal{S}}$ を復調ベクトルと呼ぶことにする．

共分散行列はよく知られているように半正値対称であるが

[68]，ここではさらに，つぎのような仮定をおく。すなわち，情報ベクトルおよび雑音の共分散行列 Φ_S，$N_0\Phi_N$ はともに正値とし，Φ_S の固有値を $\mu_1, \mu_2, \cdots, \mu_k$，$\Phi_N$ の固有値を $\lambda_1, \lambda_2, \cdots, \lambda_m$ とする。これらは仮定により，すべて正である。固有値の添字は

$$\begin{aligned} &\mu_1 \geq \mu_2 \geq \cdots \geq \mu_k > 0 \\ &0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_m \end{aligned} \tag{6.7}$$

となるようにつける．また，固有値からなるベクトル

$$\mu = \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_k \end{pmatrix} \qquad \lambda = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{pmatrix} \tag{6.8}$$

を定義しておく．

本章の目的は，このような多次元通信系において，受信行列 R に送信行列 T の一般逆行列を用いる場合，および無ひずみ条件のある場合に，復調ベクトル $\hat{S}$ と情報ベクトル S との二乗平均誤差

$$\sigma^2 = \mathcal{E}_S \mathcal{E}_N [\| \hat{S} - S \|^2] \tag{6.9}$$

を最小とする送信行列および受信行列を求めることである。

このための準備として，次節で置換多面体の理論について述べる。

6.3 置換多面体の理論

n次元ベクトル $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)^t$ の成分のあらゆる置換を行なって得られる $N=n!$ 個のベクトルを $\alpha_1(=\alpha)$, α_2, α_3, $\cdots$, α_N としよう。この中には重複するものもあり得る。$\alpha_1,\alpha_2,\cdots,\alpha_N$ を含む最小の凸集合を $P_n(\alpha)$ とする。すなわち，

$$P_n(\alpha)=\{x \mid x=\sum_{i=1}^{N} c_i\alpha_i,\ \sum_{i=1}^{N} c_i=1,\ c_i\geq 0\} \quad (6.10)$$

このような $P_n(\alpha)$ に関するつぎの Schur の定理は古くから知られている[72]。

定理6.1 (Schur)：各自然数 l ($1\leq l\leq n$) に対して，n以下の正整数の集合 $\{1,2,\cdots,n\}$ の l個の元よりなる部分集合 J 全体の族を $\mathcal{M}_l$ とする。このとき $x=(x_1,x_2,\cdots,x_n)^t\in P_n(\alpha)$ となる必要十分条件は

$$\max_{J\in\mathcal{M}_l}\left(\sum_{j\in J}x_j\right)\leq\max_{J\in\mathcal{M}_l}\left(\sum_{j\in J}\alpha_j\right) \quad l=1,2,\cdots,n-1 \quad (6.11)$$

かつ

$$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} \alpha_i \qquad (6.12)$$

となることである。

ここで，一般性を失うことなく，

$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$$

を仮定しておこう。このとき，n個の文字$\{1, 2, \cdots, n\}$の適当な置換 p を用いて，

$$x_{p(1)} \geq x_{p(2)} \geq \cdots \geq x_{p(n)}$$

となるようにすれば，式(6.11)は

$$x_{p(1)} \leq \alpha_1$$

$$x_{p(1)} + x_{p(2)} \leq \alpha_1 + \alpha_2$$

$$\vdots \qquad\qquad \vdots$$

$$x_{p(1)} + x_{p(2)} + \cdots + x_{p(n-1)} \leq \alpha_1 + \alpha_2 + \cdots + \alpha_{n-1}$$

と書き直すことができる。このことから，$P_n(\alpha)$ は α_1, $\alpha_2, \cdots, \alpha_N$ を端点とする多面体となっていることが分る[73]。そこで，これを α によって生成される置換多面体と呼ぶことにする。明らかに，置換多面体は $n-1$ 次元のベクトル空間に含まれる。図6.3に，$\alpha = (2, 1, 0)$ によって生成され

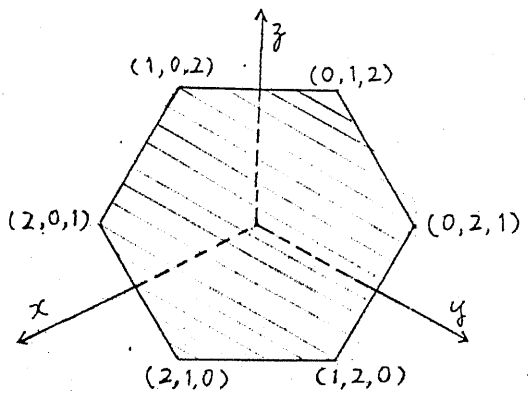


図 6.3　$\alpha=(2,1,0)$ によって生成される置換多面体

る置換多面体の例を示す。

つぎの補題は定理 6.1 からただちに導ける。

補題 6.2：n 次元ベクトル $x=(x_1, x_2, \cdots, x_n)^t$ が置換多面体 $P(\alpha)$ に含まれるとする。このとき

$$x_l = \rho\alpha_l + (1-\rho)\alpha_{l+1} \quad (0 \le \rho \le 1,\ 1 \le l \le n)$$

であるとすれば，$n-1$ 次元ベクトル $(x_2, x_3, \cdots x_n)^t$ は，$n-1$ 次元ベクトル

$$\beta = (\alpha_1, \alpha_2, \cdots, \alpha_{l-1}, (1-\rho)\alpha_l + \rho\alpha_{l+1}, \alpha_{l+2}, \cdots, \alpha_n)^t$$

によって生成される置換多面体 $P_{n-1}(\beta)$ に含まれる。

置換多面体はまた，doubly stochastic 行列（全成分が非負であり，各行，各列の成分の和が 1 となる正方行列）を用いて表わすこともできる。doubly stochastic 行列に関する

Birkoff-von Neumann の定理[72]を用いると，容易につぎの定理が導ける．

定理6.3（Birkoff-von Neumann）：n次元ベクトル x が置換多面体 $P_n(\alpha)$ に含まれる必要十分条件は $x = D\alpha$ となるn次の doubly stochastic 行列 D が存在することである．

証明はたとえば文献(72)を参照されたい．

このように置換多面体は種々の表し方が可能である．ここでさらに，置換多面体の表現に関する新しい定理を導いておこう．その前に，つぎの記号を定義しておこう．

n次正方行列 $M = \{m_{ij}\}$ の対角成分 $m_{11}, m_{22}, \cdots, m_{nn}$ をn次元ベクトルとして表わしたものを $Diag\, M$ とする．すなわち

$$Diag\, M = (m_{11}, m_{22}, \cdots, m_{nn})^t$$

定理6.4：n次元ベクトル x が置換多面体 $P_n(\alpha)$（$\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)^t$）に含まれる必要十分条件は

$$x = Diag(W^t A W) \qquad (6.13)$$

となる直交行列 W が存在することである．ただし，A は

固有値を $\alpha_1, \alpha_2, \cdots, \alpha_m$ とする m 次対称行列とする．

（証明）はじめに，任意の直交行列 W に対し，式(6.13)で与えられる α は $P_m(\alpha)$ に含まれることを示す．A をつぎのように対角化する直交行列を W_A としよう．

$$W_A A W_A^t = \begin{bmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \alpha_m \end{bmatrix} \qquad (6.14)$$

これを用いると式(6.13)は

$$x = \left[(W_A W)^t \right]^{*2} \alpha$$

と書ける．ただし，M^{*2} は行列 M の各成分を二乗して得られる行列を示す．$W_A W$ は直交行列であるから $\left[(W_A W)^t \right]^{*2}$ は明らかに doubly stochastic 行列である．それゆえ，定理6.3により，$x \in P_m(\alpha)$ を得る．

つぎに，任意の x ($\in P_m(\alpha)$) に対して，式(6.13)を満たす直交行列 W が存在することを示そう．一般性を失うことなく，A を式(6.14)の右辺で与えられるような対角行列と仮定しておく．A が対角行列でなければ，予め A を式(6.14)のような直交行列 W_A を用いて対角化しておけば

よい。

以下，帰納法を用い，式(6.13)を満たす少くとも一つの直交行列 W が存在することを示す。

$n=2$ の場合，主張が成立することは，ただちに確かめられる。$n=l-1$ の場合まで主張が成立するものとし，$n=l$ の場合を考える。$X \in P_l(\alpha)$ であるから，定理6.1によって

$$x_1 = p\alpha_k + (1-p)\alpha_{k+1} \qquad (6.15)$$

を満たす k ($1 \leq k \leq l$)，p ($0 \leq p \leq 1$) が存在する。はじめに，W の第1列として

$$w_1 = (w_1^{(1)}, w_2^{(1)}, \cdots, w_l^{(1)})^T \qquad (6.16)$$

$$w_i^{(1)} = \begin{cases} \sqrt{p} & ; \ i=k \\ \sqrt{1-p} & ; \ i=k+1 \\ 0 & ; \text{その他の場合} \end{cases}$$

となる l 次元ベクトルを選ぶ。さらに，W の第2～l 列 $w_2, w_3, \cdots, w_l$ を $l-1$ 次元ベクトル $u_1, u_2, \cdots, u_{l-1}$ を用いて

$$w_{i+1} = Q u_i \quad i=1,2,\cdots,l-1 \qquad (6.17)$$

と表わすことにする。ただし，Q は次式で定義される $l \times (l-1)$ 行列である。

$$Q = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \sqrt{1-p} & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & -\sqrt{p} & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & 0 \; 1 \end{bmatrix} \begin{matrix} 1 \\ 2 \\ \vdots \\ k-1 \\ k \\ k+1 \\ k+2 \\ \vdots \\ \vdots \\ l \end{matrix} \qquad (6.18)$$

明らかに，式(6.17) の $w_2, \cdots, w_l$ は式(6.16) の w_1 と直交する。また，$Q^t Q$ が $l-1$ 次の単位行列となることから，$l-1$ 以下の任意の正整数 i, j に対し，

$$w_{i+1}^t \, w_{j+1} = u_i^t Q^t Q \, u_j = u_i^t u_j$$

となる。ゆえに，u_i を列とする $l-1$ 次正方行列 $U = [u_1 \, u_2 \cdots u_{l-1}]$ が直交行列となれば，$W = [w_1 \, w_2 \cdots w_l]$ も直交行列となる。

ここで

$$\begin{cases} \beta_i = \alpha_i & (i = 1, \cdots, k-1) \\ \beta_k = (1-p)\alpha_k + p\alpha_{k+1} & \\ \beta_j = \alpha_{j+1} & (j = k+1, \cdots, l-1) \end{cases} \qquad (6.19)$$

とおき，これらによって，

$$\beta = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{l-1} \end{pmatrix} \qquad B = \begin{bmatrix} \beta_1 & 0 & \cdots & 0 \\ 0 & \beta_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \beta_{l-1} \end{bmatrix}$$

を定義する．$x \in P_l(\alpha)$，$x_1 = p\alpha_k + (1-p)\alpha_{k+1}$ であるから，補題 6.2 によって，$(x_2, x_3, \cdots, x_l)^t \in P_{l-1}(\beta)$ となる．ゆえに，帰納法の仮定により，

$$(x_2, x_3, \cdots, x_l)^t = Diag[U^t B U] \qquad (6.20)$$

を満たす $l-1$ 次直交行列 U が存在する．しかも，式(6.17)，(6.19)から，

$$[w_2 \cdots w_l]^t A [w_2 \cdots w_l] = U^t B U$$

となる．したがって，w_1 を式(6.16)のように定め，式(6.20)を満たす直交行列 U に対し，式(6.17)で $w_2, \cdots, w_l$ を定めれば，直交行列 $W = [w_1 w_2 \cdots w_l]$ は式(6.13)を満たす．　(証明終)

つぎの系は定理および固有ベクトルの定義から，ただちに導ける．

系 6.4.1：$x = Diag(W^t A W)$ (W：直交行列) で与えられる x のスカラー函数 $f(x)$ が $P_n(\alpha)$ において，上に

凸な函数* であれば，$f(\alpha)$ は少くとも $P_n(\alpha)$ の端点の一つにおいて最小値をとる．また，この端点を $\alpha^0 = (\alpha_1^0, \alpha_2^0, \cdots, \alpha_m^0)^*$ とすれば（α^0 は α の成分の順序を適当に並べかえたベクトル），j 番目列（$j = 1, \cdots, n$）が A の固有値 α_j^0 に対する固有ベクトルとなっているような直交行列 W_A は α に対応する。すなわち $\alpha^0 = Diag(W_A^t A W_A)$ を満たす．

この系を用いることによって，多次元線形通信系の大域的最適化を行うことができる．ここで，もう一つ置換多面体の興味深い表現定理を導いておこう．この定理の応用については付録Ⅲで述べる．

定理 6.5：n 次元ベクトル α が置換多面体 $P_n(\alpha)$ に含まれる必要十分条件は

$$\alpha = [(I-S)^{-1}(I+S)]^{*2}\alpha \qquad (6.21)$$

となる逆対称行列（$S = -S^*$ となる行列）が存在すること

---

* ある凸な領域 Ω に含まれる任意の二つのベクトル α_1, α_2 および任意の p（$0 < p < 1$）に対し，

$$f(p\alpha_1 + (1-p)\alpha_2) \geq p f(\alpha_1) + (1-p) f(\alpha_2)$$

を満たす函数 $f(\alpha)$ を Ω において（広義の）上に凸な函数という．

である。

(証明) n次正格直交行列 W (行列式が1となる直交行列) はn次逆対称行列 S を用いて,

$$W = (I-S)(I+S)^{-1} = (I+S)^{-1}(I-S) \qquad (6.22)$$

と表せる[74]. ここに I は単位行列である。ところで $Diag(W^t A W)$ は W の第1列 w_1 を $-w_1$ で置き換えても, 変らない. それゆえ, 定理6.4の直交行列として, 正格のものだけを考えても定理はそのまま成立する. したがって, 定理6.4, 式(6.13)の A を予め対角化したものとし, W に式(6.22)を代入すれば, ただちに定理が導ける。 (証明終)

この定理は置換多面体 $P_n(\alpha)$ に属するベクトルを, まったく制約条件の付かないパラメータで表わし得ることを示している点で重要である. すなわち, $P_n(\alpha)$ の定義式(6.10), 定理(6.1)(6.3)(6.4)はいずれも $P_n(\alpha)$ を一定の制約条件の付いたパラメータで表わしているのに対し, 定理6.5では, 逆対称行列 S の対角線から上の $n(n-1)/2$ 個の成分をパラメータとして $P_n(\alpha)$ を表わすことができ, しかもこれらのパラメータには何の制約条件もない。

以上，二つの新しい定理を中心に，置換多面体の理論について述べた。次節から再び本論に戻り，多次元線形通信系の最適化について論ずる。なお，本節の理論の応用については付録Ⅲで述べる。

6.4 一般逆行列を受信機に用いる多次元線形通信系の最適化

6.4.1 一般逆行列による受信

送信行列の逆行列を受信機に用いる通信方式は実際にしばしば用いられる。送信行列 T の一般逆行列* (T^+ で表わす) を受信機に用いる通信方式は，このような通信方式の自然な拡張として考えられたものである。送信行列の一般逆行列を用いる受信方式は，復調ベクトルの二乗平均誤差で評価した場合，最適な受信方式ではないが，概念的に簡単であり，

---

* $m \times k$ 行列 A に対し，

$$AXA = A \qquad XAX = X$$
$$(AX)^t = AX \qquad (XA)^t = XA$$

の四式を満たす $k \times m$ 行列 X がただ一つ存在する。これを A の一般逆行列といい，通常 A^+ で表わす。文献 (75)(76) 参照。

解析が容易であることのほかに，特別な場合にはつぎのような性質をもつ。

(i) 送信行列 T の階数が k の場合は無ひずみ条件を満たす。

(ii) 通信路雑音 n が正規分布に従うとする。このとき，TT^+ が Φ_N と可換な場合，たとえば T の階数が m の場合，あるいは通信路雑音が白色である場合，すなわち，$\Phi_N = I_m$（m 次の単位行列）となる場合には最尤推定となる。

(証明) (i) 送信行列 T を，次項で述べるように，式(6.24)のように分解したとき，T の一般逆行列 T^+ が式(6.25)のように書けることから，T の階数が k のときは，$RT = T^+T = I_k$ となることが分る。これは無ひずみ条件にほかならない（6.5 参照）。

(ii) n が正規分布にしたがう確率ベクトルであるから，s の対数尤度は

$$\log P(z|s) = -\{(z-Ts)^* \Phi_N^{-1}(z-Ts)\}/2N_0 + \log\{(2\pi N_0)^{-\frac{m}{2}} |\Phi_N|^{-\frac{1}{2}}\}$$

ここに $|\Psi_N|$ は Ψ_N の行列式を示す。したがって S の最ゆう推定量は上式の右辺オー項を最小とする S として求められる。Ψ_N^{-1} は正値対称行列であるから，

$$(\Psi_N^{-\frac{1}{2}})^t \Psi_N^{-\frac{1}{2}} = \Psi_N^{-\frac{1}{2}} (\Psi_N^{-\frac{1}{2}})^t = \Psi_N^{-1}$$

を満たす $\Psi_N^{-\frac{1}{2}}$ が存在する(74)。これを用いると，

$$(\mathfrak{z} - TS)^t \Psi_N^{-1} (\mathfrak{z} - TS) = \| \Psi_N^{-\frac{1}{2}} \mathfrak{z} - \Psi_N^{-\frac{1}{2}} TS \|^2$$

それゆえ，S の最ゆう推定量 $\hat{S}_{ML}$ は一般逆行列の性質*を用いれば，

$$\hat{S}_{ML} = \{ (\Psi_N^{-\frac{1}{2}} T)^+ \Psi_N^{-\frac{1}{2}} \} \mathfrak{z}$$

を得る。ところで，TT^+ と Ψ_N が可換の場合には

$$(\Psi_N^{-\frac{1}{2}} T)^+ = T^+ \Psi_N^{\frac{1}{2}}$$

となることが容易に導ける。実際，この場合 $A = \Psi_N^{-\frac{1}{2}} T$, $A^+ = T^+ \Psi_N^{\frac{1}{2}}$ とおけば，これらが一般逆行列の定義式 $AA^+A = A$, $A^+AA^+ = A^+$, $(AA^+)^t = AA^+$, $(A^+A)^t = A^+A$ をすべて満たすことはただちに確かめられる。ゆえに，このとき

$$\hat{S}_{ML} = T^+ \mathfrak{z} \qquad (6.23)$$

---

* b を m 次元ベクトル，A を $m \times n$ 行列とし，$x^0 = A^+ b$ とおけば，任意の n 次元ベクトル x に対して $\|Ax - b\| \geq \|Ax^0 - b\|$ となる。文献(76)，P.71参照。

となる。特に，T の階数が m のときは，TT^+ が単位行列となり，雑音が白色の場合には Φ_N が単位行列となるから，TT^+ と Φ_N は可換となり，S の最ゆう推定量は式 (6.23) で与えられる。 (証明終)

(i) の無ひずみ条件は実際の通信において望ましい条件である。また (ii) は情報ベクトルの確率的性質によらない性質であり，最大事後確率推定を用いた受信方式などに比べると，一般逆行列による受信方式は (ii) の条件を満たす場合，情報源の確率的性質の変動に対し，比較的安定であると思われる。

6.4.2 最適化のための準備

はじめに，送信行列 T を扱い易い形に書き直しておこう。T の階数を r ($0 < r \leq \min(m, k)$) とすると，$m \times k$ 行列はつぎのように分解できる[79]。

$$T = UDV \tag{6.24}$$

ここに U は m 次直交行列，V は k 次直交行列であり，D は (i, i) 成分 ($i = 1, 2, \cdots, r$) が $\sqrt{d_i}$ ($d_i > 0$) で他の成分が 0 の $m \times k$ 行列である。すなわち，

$$D = \begin{bmatrix} \sqrt{d_1} & & & 0 \\ & \sqrt{d_2} & & \\ & & \ddots & \\ 0 & & & \sqrt{d_r} \end{bmatrix}_{m} \quad \underbrace{\qquad\qquad}_{k}$$

これに対し，T の一般逆行列 T^+ は

$$T^+ = V^T D_1 U^T \qquad (6.25)$$

となる[75]．ここに V^T，U^T は V，U の転置行列であり，D_1 は (i,i) 成分 $(i=1,2,\cdots,r)$ が $1/\sqrt{d_i}$ で他の成分が 0 の $k \times m$ 行列である．

ここで V の第 i 行列を k 次元ベクトル v_i^T $(i=1,\cdots,k)$，U の第 i 列を m 次元ベクトル u_i $(i=1,\cdots,m)$ で表わしておこう．すなわち，

$$V = [v_1\ v_2 \cdots v_k]^T \qquad U = [u_1\ u_2 \cdots u_m] \qquad (6.26)$$

このとき，平均送信電力の制限（式 (6.3)）は

$$\mathcal{E}_S[\|y\|^2] = \mathcal{E}_S[\|TS\|^2] = \mathcal{E}_S[\|DVS\|^2]$$

$$= \mathrm{Tr}[DV\Phi_S V^T D^t] = \sum_{i=1}^{r} d_i v_i^T \Phi_S v_i \le m S_0 \qquad (6.27)$$

となる．また，二乗平均誤差 σ^2（式 (6.9)）は

$$\sigma^2 = \mathcal{E}_S \mathcal{E}_N [\|(T^T T - I_k)S + T^+ n\|^2]$$

$$= \mathcal{E}_S \mathcal{E}_N [\|(I_{k,r} - I_k)VS + D_1 U^T n\|^2]$$

$$= \sum_{i=r+1}^{k} v_i^T \Phi_S v_i + N_0 \sum_{i=1}^{r} \frac{1}{d_i} u_i^T \Phi_N u_i \qquad (6.28)$$

と書ける．ただし，I_k は k 次の単位行列，$I_{k,r}$ は (i,i) 成分（$i=1,\cdots,r$）が 1 で他の成分が 0 の k 次正方行列である．式（6.28）の第一項は情報の一部を送信しないときに生ずる雑音であり，第二項は通信路雑音による項である．

ここで，

$$\xi_i = v_i^T \Phi_S v_i \qquad i = 1,\cdots,k \qquad (6.29)$$

$$\eta_i = u_i^T \Phi_N u_i \qquad i = 1,\cdots,m \qquad (6.30)$$

とおこう．これによって，式（6.27）および式（6.28）はそれぞれ，

$$\sum_{i=1}^{r} d_i \xi_i \leq m S_0 \qquad (6.31)$$

$$\sigma^2 = \sum_{i=r+1}^{k} \xi_i + N_0 \sum_{i=1}^{r} \frac{\eta_i}{d_i} \qquad (6.32)$$

となる．また，

$$\xi = \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_k \end{pmatrix} \qquad \eta = \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_m \end{pmatrix} \qquad d = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} \qquad (6.33)$$

を定義しておこう．ξ および η は 6.3 で定義した記号 Diag を用いれば，式（6.26），（6.29）（6.30）から，

$$\xi = \mathrm{Diag}\,(V \Phi_S V^*) \tag{6.34}$$

$$\eta = \mathrm{Diag}\,(U^t \Phi_N U) \tag{6.35}$$

と表わせることが分る。このように，ξ，η がそれぞれ，V，U の函数となっていることを強調するため，$\xi(V)$，$\eta(U)$ と書くこともある。

また，式(6.32)の σ^2 を d，ξ，η および γ の函数として，$\sigma^2(d, \xi, \eta, \gamma)$ と表わすこともある。

以上によって，最適な送信行列 T を求める問題は，式(6.31)の条件の下に，$\sigma^2(d, \xi, \eta, \gamma)$ を最小とする d，$\xi(V)$，$\eta(U)$ および γ を求める問題となった。これを次項で行なおう。

6.4.3 最適化

前項までの準備の下に，本項では一般逆行列を受信機に用いる多次元線形通信系において，大域的に最適な送信行列 T を求める。このために，はじめに，$\xi(V)$，$\eta(U)$ および γ が与えられているとして，d を最適化し，つぎに $\xi(V)$ と γ が与えられているとして $\eta(U)$ の最適化を行い，つい

で γ が与えられているとして，$\xi(\nabla)$ の最適化を行う。最後に γ を最適化しなければならないが，これは N_0, S_0. および $\mathbb{E}_S$, $\mathbb{E}_N$ の固有値などが具体的に与えられないと行えない。

6.4.3.1 d の最適化

式(6.31)の条件の下に，式(6.32)の σ^2，したがって，$\sum_{i=1}^{r}(\eta_i/d_i)$ を最小とする d を求めればよい。ξ, η, d の成分はすべて正であるから，Cauchy の不等式* を用いて，

$$\left(\sum_{i=1}^{r} d_i\xi_i\right)\left(\sum_{i=1}^{r}\frac{\eta_i}{d_i}\right) \geq \left(\sum_{i=1}^{r}\sqrt{\xi_i\eta_i}\right)^2 \qquad (6.36)$$

を得る。等号が成立するのは，

$$d_i^2\xi_i / \eta_i = C\ (\text{定数}) \quad i=1,\cdots,r \qquad (6.37)$$

のときに限る。式(6.31)を用いれば

$$\left(\sum_{i=1}^{r}\frac{\eta_i}{d_i}\right) \geq \frac{1}{mS_0}\left(\sum_{i=1}^{r}\sqrt{\xi_i\eta_i}\right)^2 \qquad (6.38)$$

となる。等号が成立するのは，式(6.37)および

---

* $(a_1^2+a_2^2+\cdots+a_m^2)(b_1^2+b_2^2+\cdots b_m^2) \geq (a_1b_1+a_2b_2+\cdots+a_mb_m)^2$
等号は $a_1:a_2:\cdots:a_m = b_1:b_2:\cdots:b_m$ のときに限って成立する。

$$\sum_{i=1}^{r} \alpha_i \xi_i = m S_0 \qquad (6.39)$$

が満たされるときに限る。ゆえに，σ^2 を最小とする α を $\alpha^\circ = (\alpha_1^\circ, \alpha_2^\circ, \cdots, \alpha_r^\circ)^t$ とおけば，

$$\alpha_i^\circ = \frac{m S_0}{\sum_{j=1}^{r} \sqrt{\xi_j \eta_j}} \sqrt{\frac{\eta_i}{\xi_i}} \qquad i = 1, \cdots, r \qquad (6.40)$$

となる。このとき，二乗平均誤差は

$$\sigma^2(\alpha^\circ, \xi, \eta, r) = \sum_{i=r+1}^{k} \xi_i + \frac{N_0}{m S_0} \left(\sum_{i=1}^{r} \sqrt{\xi_i \eta_i} \right)^2 \qquad (6.41)$$

で与えられる。

6.4.3.2 $\eta(U)$ の最適化

r および ξ が与えられているとして，$\sigma^2(\alpha^\circ, \xi, \eta, r)$ を最小とする $\eta(U)$ を求める。これには $\sum_{i=1}^{r} \sqrt{\xi_i \eta_i}$ を最小とする $\eta_1, \eta_2, \cdots, \eta_r$ を求めればよい。$\sum_{i=1}^{r} \sqrt{\xi_i \eta_i}$ は $\eta_1, \eta_2, \cdots, \eta_r$ の函数と考えるとき，よく知られているように $\eta_i \geq 0$ $(i = 1, \cdots, r)$ において上に凸な函数である。したがって，これはまた，η の函数と考えても $\eta_i \geq 0$ $(i = 1, \cdots, m)$ において上に凸な函数である。ここで，

$$f_1(\eta) = \sum_{i=1}^{r} \sqrt{\xi_i \eta_i}$$

を定義しておこう。

$\overline{R}_N$ の固有値 $\lambda_1, \lambda_2, \cdots, \lambda_m$ はすべて正であったから，λ によって生成される置換多面体 $P_m(\lambda)$ に含まれるベクトルの成分はすべて正である．それゆえ，$f_1(\eta)$ は $P_m(\lambda)$ において上に凸な函数である．しかも，η は式 (6.35) で与えられる m 次元ベクトルであるから，系 6.4.1 により，$f_1(\eta)$ は $P_m(\lambda)$ の端点において最小値をとる．

つぎに，$P_m(\lambda)$ の端点のうちで $f_1(\eta)$ を最小とする点 $\eta^0 = (\eta_1^0, \eta_2^0, \cdots, \eta_m^0)$ を求めよう．明らかに，η^0 のはじめの r 個の成分 $\eta_1^0, \eta_2^0, \cdots, \eta_r^0$ は $\lambda_1, \lambda_2, \cdots, \lambda_m$ の中の小さい方から r 個選んだ $\lambda_1, \lambda_2, \cdots, \lambda_r$ を適当な順序に並べかえたものである．ところで，η_j と η_l $(1 \leq j < l \leq r)$ の順序を入れかえることによる $f_1(\eta)$ の変化は

$$\sqrt{\xi_j \eta_l} + \sqrt{\xi_l \eta_j} - \sqrt{\xi_j \eta_j} - \sqrt{\xi_l \eta_l} = (\sqrt{\xi_j} - \sqrt{\xi_l})(\sqrt{\eta_l} - \sqrt{\eta_j})$$

となるから，$\xi_j > \xi_l$，$\eta_j > \eta_l$ のときは η_j と η_l を交換することによって $f_1(\eta)$ を小さくできる．このことから，

$$\xi_1 \geq \xi_2 \geq \cdots \geq \xi_r \qquad (6.42)$$

と仮定すれば，η^0 のはじめの r 個の成分は

$$\eta_i^0 = \lambda_i \qquad i = 1, \cdots, r \qquad (6.43)$$

で与えられることが分る（式(6.7)に注意）．η^0 の後の $m-r$ 個の成分は，たとえば，つぎのようにすればよい。

$$\eta_i^0 = \lambda_i \qquad i = r+1, \cdots, m \tag{6.44}$$

このような η^0 に式(6.35)によって対応する直交行列を U^0 とすれば，U^0 は λ_i（$i=1,\cdots,m$）に対する Σ_N の固有ベクトル $\tilde{u}_i$ を第 i 列とする行列である．すなわち，

$$U^0 = [\tilde{u}_1 \tilde{u}_2 \cdots \tilde{u}_m] \tag{6.45}$$

ただし，$\tilde{u}_i' \tilde{u}_j = \delta_{ij}$（クロネッカーのデルタ）（$i \leq i, j \leq m$）としておく。

また，このとき二乗平均誤差は

$$\sigma^2(\alpha^0, \xi, \eta^0, r) = \sum_{i=r+1}^{k} \xi_i + \frac{N_0}{m S_0} \left(\sum_{i=1}^{r} \sqrt{\xi_i \lambda_i} \right)^2 \tag{6.46}$$

となる．ただし，$\xi_1, \xi_2, \cdots, \xi_r$ の添字は式(6.42)を満たすようにつけてあるものとする．

いうまでもなく，$\eta_{r+1}^0, \cdots, \eta_m^0$ は式(6.44)のように選ぶ必要はなく，$\eta^0 \in P_m(\lambda)$ の範囲で自由に選んでよい．言い換えれば U^0 の第 $r+1$ 列から第 m 列までは，互いに直交し，かつ $\tilde{u}_1, \cdots, \tilde{u}_r$ のすべてと直交するような，ノルムが

1となるベクトルを選びさえすればよい。

6.4.3.3　$\xi(V)$の最適化

rが与えられているとして，$\sigma^2(d^0, \xi, \eta^0, r)$を最小とする$\xi(V)$を求める．ここで，

$$f_2(\xi) = \sigma^2(d^0, \xi, \eta^0, r)$$

とおこう．

はじめに，$f_2(\xi)$がΣ_sの固有値を成分とするベクトルμによって生成される置換多面体$P_k(\mu)$において上に凸な函数であることを示す。$\xi_1 = (\xi_{11}, \xi_{12}, \cdots, \xi_{1k})^t$，$\xi_2 = (\xi_{21}, \xi_{22}, \cdots, \xi_{2k})^t$を$P_k(\mu)$に含まれる任意の二つのベクトルとする。$0 < p < 1$となる任意の$p$に対し，

$$p\xi_{1i}\lambda_i > 0 \quad , \quad (1-p)\xi_{2i}\lambda_i > 0 \quad (i=1, \cdots, r)$$

となることに注意して，Minkowakiの不等式*を用いれば，

$$\left(\sum_{i=1}^{r}\sqrt{p\xi_{1i}\lambda_i + (1-p)\xi_{2i}\lambda_i}\right)^2 \geq p\left(\sum_{i=1}^{r}\sqrt{\xi_{1i}\lambda_i}\right)^2 + (1-p)\left(\sum_{i=1}^{r}\sqrt{\xi_{2i}\lambda_i}\right)^2$$

---

* $a_1, a_2, \cdots, a_n ; b_1, b_2, \cdots, b_n > 0$，$p > 1$ならば，

$$\left[\sum_{i=1}^{n}(a_i + b_i)^p\right]^{\frac{1}{p}} \geq \left[\sum_{i=1}^{n}(a_i)^p\right]^{\frac{1}{p}} + \left[\sum_{i=1}^{n}(b_i)^p\right]^{\frac{1}{p}}$$

等号は$a_1 : a_2 : \cdots : a_n = b_1 : b_2 : \cdots : b_n$のときに限って成立する．

を得る。このことから，ただちに $f_2(\xi)$ が $P_k(\mu)$ において上に凸な函数であることが確かめられる。したがって，系 6.4.1 から，$f_2(\xi)$ は少くとも $P_k(\mu)$ の端点の一つで最小値をとる。$P_k(\mu)$ の端点は μ の成分を並べかえたベクトルで表わせたから，$f_2(\xi)$ を最小とする $\xi=\xi^0$ は，k 個の文字 $\{1,2,\cdots,k\}$ の適当な置換

$$p:(1,2,\cdots,k)\longrightarrow(p(1),p(2),\cdots,p(k))$$

によって

$$\xi^0=(\mu_{p(1)},\mu_{p(2)},\cdots,\mu_{p(k)})^t \qquad (6.47)$$

の形に書ける。ただし，式 (6.42) の仮定から，

$$\mu_{p(1)}\geq\mu_{p(2)}\geq\cdots\geq\mu_{p(r)} \qquad (6.48)$$

でなければならない。また ξ^0 に式 (6.34) によって対応する直交行列 V^0 は，$\mu_{p(i)}$ $(i=1,\cdots,k)$ に対する $\mathfrak{H}_S$ の固有ベクトルを $\tilde{v}_{p(i)}$ とするとき

$$V^0=[\tilde{v}_{p(1)}\ \tilde{v}_{p(2)}\cdots\tilde{v}_{p(k)}]^t \qquad (6.49)$$

と表わせる。ただし，固有ベクトルは $\tilde{v}_{p(i)}^*\tilde{v}_{p(j)}=\delta_{ij}$ $(1\leq i,j\leq k)$ と定めるものとする。

以上によって，つぎの定理が証明できた。

定理 6.6 ： 一般逆行列を受信機に用いる多次元線形通信系において，復調ベクトルと情報ベクトルの間の二乗平均誤差 σ^2 を最小とする送信行列 T^0 はつぎの形に書ける．

$$T^0 = [\tilde{u}_1 \tilde{u}_2 \cdots \tilde{u}_m] \begin{bmatrix} \sqrt{d_1^0} & 0 & \cdots & 0 \\ 0 & \sqrt{d_2^0} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 0 \end{bmatrix} [\tilde{v}_{p(1)} \tilde{v}_{p(2)} \cdots \tilde{v}_{p(k)}] \tag{6.50}$$

ここに，r は $\min(m, k)$ 以下の適当な正整数，$\tilde{u}_i$ $(i = 1, \cdots, m)$ は Φ_N の固有値 λ_i $(\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_m)$ に対する固有ベクトル，$\tilde{v}_{p(i)}$ $(i = 1, \cdots, k)$ は Φ_S の固有値 $\mu_{p(i)}$ $(\mu_1 \geq \mu_2 \geq \cdots \geq \mu_k)$ に対する固有ベクトルである．ただし，固有ベクトルは $\tilde{u}_i^* \tilde{u}_j = \delta_{ij}$ $(1 \leq i, j \leq m)$，$\tilde{v}_{p(i)}^* \tilde{v}_{p(j)} = \delta_{ij}$ $(1 \leq i, j \leq k)$ となるものを選ぶとする．また，p は k 個の文字 $\{1, 2, \cdots, k\}$ の適当な置換であり，$\mu_{p(1)} \geq \mu_{p(2)} \geq \cdots \geq \mu_{p(k)}$ を満たすものとする．さらに，d_i^0 $(i = 1, \cdots, r)$ は次式で与えられる．

$$d_i^0 = \frac{m S_0}{\sum_{j=1}^{r} \sqrt{\mu_{p(j)} \lambda_j}} \sqrt{\frac{\lambda_i}{\mu_{p(i)}}} \quad (i = 1, \cdots, r) \tag{6.51}$$

このような送信行列 T^0 を用いたとき，二乗平均誤差 σ^2

はつぎのようになる．

$$\sigma^2 = \sum_{i=r+1}^{m} \mu_{p(i)} + \frac{N_0}{m S_0} \left(\sum_{i=1}^{r} \sqrt{\mu_{p(i)} \lambda_i} \right)^2 \qquad (6.52)$$

なお，置換 p および正整数 r はこの式の右辺を最小とするように定められているものとする．

定理の導出の過程から明らかなように，一般に最適な送信行列は一意には定まらない．定理に示されている送信行列は最適なものの一つである．

この定理では，置換 p と最適送信行列 T^0 の階数 r は具体的には与えられていない．これを定めるためには Ξ_N，Ξ_S の固有値 λ，μ および mS_0/N_0 の数値を具体的に知る必要がある．しかし，たとえば mS_0/N_0 が十分大きいような場合，すなわち，通信路が十分良いものである場合には p と r が定まることがある．これを つぎの系に示そう．

系 6.6.1 ： $m \geq k$ で．

$$\frac{2k \mu_1 \lambda_k}{\mu_k} \leq \frac{m S_0}{N_0} \qquad (6.53)$$

となるときには，$r = k$，$p(i) = i$ $(i = 1, \cdots, k)$ が最適な送信行列を与える．

(証明) 任意の置換 p，および k より小さい任意の正整数 j に対し，次式の成立することから明らかである．

$$\sum_{i=j+1}^{k} \mu_{p(i)} + \frac{N_0}{mS_0}\left(\sum_{i=1}^{j}\sqrt{\mu_{p(i)}\lambda_i}\right)^2 - \sum_{i=j+2}^{k} \mu_{p(i)} - \frac{N_0}{mS_0}\left(\sum_{i=1}^{j}\sqrt{\mu_{p(i)}\lambda_i}\right)^2$$

$$\geq \mu_k - \frac{N_0}{mS_0}\cdot 2k\mu_1\lambda_k \geq 0$$

(証明終)

本節では受信行列として，送信行列の一般逆行列を用いる多次元線形通信系において，復調ベクトルと情報ベクトルの間の二乗平均誤差を最小とする送信行列の形を求め，定理6.6を得た。定理6.6は直観的に言えば，情報中の平均電力の大きい（固有ベクトル方向の）成分は通信路の雑音の小さい部分を通して伝送し，平均電力の小さい成分は雑音の大きい部分を通して伝送することを意味している．また，情報ベクトルの次元数が通信路の次元数より大きければ，情報中のいくつかの成分を送信できないのはいうまでもないが，たとえ，通信路の次元数に余裕があっても，通信路に雑音の非常に大きな部分があれば，そのような部分を用いない方が結果として，復調ベクトルの二乗平均誤差は小さくなることも，

定理6.6の一つの結論である。これに対し，系2.1は通信路が十分良質の場合には，情報をすべて送るのが最適であることを示している。

ところで，容易に確かめられるように，$T^{\circ}(T^{\circ})^{+}$ と $\overline{\mathrm{o}}_N$ とは可換である。したがって，6.4.1で述べたことから分るように，通信路雑音が正規分布に従うとすれば，定理6.6の通信系においては，受信機で最ゆう推定が行なわれている。定理6.6は受信機において最ゆう推定をするという条件の下に最適化を行なったものではないが，雑音が正規分布に従う場合，このような条件の下で通信系を最適化した結果は定理6.6に一致するのではないかと思われる。しかし，この証明は今後に残された問題である。

また，本節に得られた通信系は，系6.6.1のような特別な場合は無ひずみ条件を満たすが，一般にはこの条件を満たさない。それでは，一般逆行列を受信機に用いるという条件を除き，無ひずみ条件を課した場合，最適な多次元線形通信系はどのようなものであろうか。この点について次節で述べる。

6.5 無ひずみ条件のある場合の多次元線形通信系の最適化

無ひずみ条件とは，すでに述べたように復調出力中の信号成分が希望信号と一致するという条件である。言い換えれば，仮りに通信路の雑音が無いとしたときに，復調出力と希望信号が一致するという条件である。このような条件は通信系の情報や雑音の確率的性質の変動に対する安定性などの点から実際の通信において望ましい条件とされている。

本節では無ひずみ条件のある場合に，多次元線形通信系において，復調ベクトルと情報ベクトルとの間の二乗平均誤差を最小とする送信行列と受信行列を求める。

無ひずみ条件を送信行列 T と受信行列 R で表わせば，

$$RT = I_k \quad (k\text{次の単位行列}) \tag{6.54}$$

となる。この条件を満たすためには，明らかに $m \geq k$ でなければならない。また，T および R の階数はともに k である必要がある。

はじめに R を

$$R = V^* D_1 U^T \tag{6.55}$$

と分解しておこう。ここに V は k 次，U は m 次の直交行列であり，D_1 は (i,i) 成分 $(i=1,\cdots,k)$ が $1/\sqrt{d_i}$ ($d_i>0$) で他の成分が 0 の $k\times m$ 行列である。

一方送信行列 T は式(6.54)と式(6.55)から，

$$T = U D_2 V \quad ; \quad D_2 = D + G \qquad (6.56)$$

と書けることが分る。ここに D は (i,i) 成分 $(i=1,\cdots,k)$ が $\sqrt{d_i}$ で，他の成分が 0 の $m\times k$ 行列であり，G は第 1 行から第 k 行までがすべて 0 となり，他の成分が任意の $m\times k$ 行列である。

このとき，平均送信電力は

$$\begin{aligned} \mathcal{E}_S[\|\mathcal{Y}\|^2] &= \mathcal{E}_S[\|TS\|^2] = \mathrm{Tr}[D_2 V \Phi_S V^* D_2^*] \\ &= \mathrm{Tr}[DV\Phi_S V^* D^*] + \mathrm{Tr}[DV\Phi_S V^* G^*] \\ &\quad + \mathrm{Tr}[GV\Phi_S V^* D^*] + \mathrm{Tr}[GV\Phi_S V^* G^*] \qquad (6.57) \end{aligned}$$

となる。この式の右辺の第 2 項と第 3 項が 0 となることは容易に確かめられる。ここで 6.4.2 と同様に，式(6.34)，(6.35)によって，V，U に対し ξ，q を定義しておこう。このとき，平均送信電力制限の条件は

$$\mathcal{E}_S[\|\mathcal{Y}\|^2] = \sum_{i=1}^{k} d_i \xi_i + q \le mS. \qquad (6.58)$$

$$g = \mathrm{Tr}\left[G V \Phi_S V^t G^T\right]$$

となる。

Φ_S は正値であるから，$g \geq 0$，$g = 0$ となるのは G が 0 行列となるときに限る。

一方，二乗平均誤差（式(6.9)）は

$$\sigma^2 = \varepsilon_N\left[\|R\eta\|^2\right] = \sum_{i=1}^{k} \frac{\eta_i}{d_i} \qquad (6.59)$$

となる。

以下，前節で用いた手法により最適化が行える。ただし，この場合には d，$\xi(V)$，$\eta(U)$ のほかに G についても最適化をしなければならない。σ^2 を d，ξ，η，G の函数として，$\sigma^2(d, \xi, \eta, G)$ と書いておこう。

はじめに，d について最適化を行なう。最適な d を d° とすれば，Cauchy の不等式および式(6.58)から，d° は

$$d_i^* = \frac{mS_0 - g}{\sum_{i=1}^{r} \sqrt{\xi_i \eta_i}} \sqrt{\frac{\eta_i}{\xi_i}} \qquad i = 1, \cdots, k \qquad (6.60)$$

で与えられ，そのとき σ^2 は

$$\sigma^2(d^\circ, \xi, \eta, G) = \frac{N_0}{mS_0 - g}\left(\sum_{i=1}^{k} \sqrt{\xi_i \eta_i}\right)^2 \qquad (6.61)$$

となることが分る。明らかに $\sigma^2(\alpha^0, \xi, \eta, G)$ は G が 0 行列となるとき，最小となる。ゆえに $D_2 = D$，すなわち，

$$T = UD_2V = UDV \tag{6.62}$$

のとき，与えられた ξ，η に対し σ^2 は最小となる。

このとき，式(6.55)，(6.62)から R は T の一般逆行列となることが分る．したがって，以下 $\xi(V)$ と $\eta(U)$ の最適化は，前節の 6.4.3.2，6.4.3.3 とまったく同様に行えることは言うまでもない。

以上の結果をつぎの定理にまとめておこう。

定理 6.7 ：無ひずみ条件があるとき，多次元線形通信系において，復調ベクトルと情報ベクトルの間の二乗平均誤差を最小とする送信行列は定理 6.6，式(6.50) の行列 T^0 において，$r = k$，$p(i) = i$ $(i = 1, \cdots, k)$ としたものであり，受信行列は送信行列の一般逆行列である．

このとき，二乗平均誤差は次式で与えられる．

$$\sigma^2 = \frac{N_0}{mS_0}\left(\sum_{i=1}^{k}\sqrt{\mu_i\lambda_i}\right)^2 \tag{6.63}$$

本節では，無ひずみ条件を制約条件とした場合に，多次元

線形通信系の最適化を行った．定理6.7は定理6.6と全く異なった意味をもっているが，結果的にはきわめて類似しており，定理6.7の場合にも受信行列として一般逆行列を用いる結果となっている．また，この場合も定理6.7で得られた結果が大域的に最適なものであることはいうまでもない．

なお，定理6.7は田中ら[71]によって局所的に最適化されたものと，結果的には一致している．

6.6 むすび

アナログ線形通信系の一つである多次元線形通信系において，はじめに受信行列として送信行列の一般逆行列を用いる場合に，復調ベクトルと情報ベクトルの間の二乗平均誤差を最小とする送信行列を求めた．ついで，無ひずみ条件のある場合に，二乗平均誤差を最小とする送信行列と受信行列を求めた．このいずれの場合も最適な送，受信行列は情報ベクトルおよび雑音の共分散行列の固有値と固有ベクトルで表わせることを示した．

最適化に際しては，絶対不等式と置換多面体の理論を用い，

大域的最適化を行なった。本章で示した置換多面体の理論は他の最適化問題への応用も可能であると思われる。これについては付録Ⅲで述べる。

しかし，本章では多次元線形通信系において送信行列と受信行列の関係に一定の制約条件をつけて行なったものであり，送信行列と受信行列を無条件で同時にしかも大域的に最適化する問題は未解決である（局所的最適化は甘利[69]によって行なわれている）。

また，本章では，復調出力の二乗平均誤差を評価基準としたが，評価基準はこのほかにも種々考えられる。それらの評価基準に対して多次元線形通信系を最適化する問題も今後に残されている。

第7章

結　言

本論文では，符号理論および信号理論における種々の問題を，主として符号の距離構造の面からとり上げ，検討した。ここでは，はじめに各章の主要な結論をまとめ，ついで今後の問題について述べておく．

7.1　主要な結論

第2章では，誤り訂正符号を実際の通信系に適用し，ディジット毎の検出――最小距離復号を行う場合，符号における距離の選択が，通信系の信頼性，その他に非常に大きな影響を及ぼすことをみた（2.2，2.5，2.9節）．また，多相位相変調通信方式に対して，リー距離を用いた符号がすぐれていること（2.5節），一般に低伝送速度の符号はきわめて不利であること（2.3，2.5節）などを知った。さらに，現在のと

ころ，もっとも実用的と思われる方式は，二値符号からGray変換によって得られる符号を用いる方式であることを示した（2.7，2.9節）．

第3章では，Preparata符号と二値BCH符号の符号長を能率よく伸ばす方法を導いた．これにより得られる修正Preparata符号は，組織符号として最適な二重誤り訂正二値非線形符号であり（定理3.1，3.2），符号化および復号も容易であること（3.4節）を示した．また，二重誤り訂正二値BCH符号から，この章の方法によって準完全符号を構成できることを知った（定理3.4）．

第4章では，符号分割多重PCM通信方式のアドレスとして用いられる符号に適したものとして，回線分離符号を考え，その構造の基礎となる二値ベクトルのある種の同値類の構造を明らかにした（4.3節）．また，回線分離符号の実用的な三種の構成法を示した（4.5節）．

第5章では，M系列およびM系列符号を二次元に拡張したものとして，$\gamma\beta$－平面および$\gamma\beta$－平面符号を考え，その代数的構成法を示した（5.3節，定理5.7）．また，その構

造を種々の面から明らかにし，特に，その自己相関函数が応用上著しい特徴をもつことを示した（定理 5.11，5.7 節）．

第6章では，置換多面体の表現に関する定理（定理 6.4，6.5）を導き，その結果を用いて，多次元線形通信系において，受信行列に送信行列の一般逆行列を用いる場合，および無ひずみ条件のある場合に，大域的最適化に成功した（定理 6.6，6.7）．

7.2 今後の問題

第2章で残された問題は，最小距離復号を用いる場合の信頼度函数をより正確に評価すること，リー距離を用いた誤り訂正符号の理論をさらに発展させること，距離をより一般化した場合に構成できる符号を見出すことなどである．

第3章では，非線形符号の理論をより発展させ，多重誤りを訂正できるすぐれた非線形符号について研究する必要がある．

第4章では，最小距離の大きい最適回線分離符号の性質および構成法についての今後の研究が期待される．

第5章においては，基礎理論は一応完成していると思われるので，今後応用面の開発が望まれる。

第6章で示した置換多面体の理論も，今後の応用についての研究が期待される．また，多次元線形通信系については，より一般的な条件の下での大域的最適化の問題が今後に残されている。

付録 I

原始多項式表

表 A1.1 に 3 以上 47 以下のすべての素数 p および $p^m - 1 \leq 10^6$ となるすべての正整数 m について GF(p) の上の m 次の原始多項式を一つづつ示す.

GF(2) の上の原始多項式は Peterson[1] の巻末に, 34 次以下のものが示されている.

$GF(p^n)$ (n: 正整数) の上の m 次のすべての既約多項式は, GF(p) の上の nm 次の原始多項式の根を α とするとき, $i p^{ni} = 1 \mod (p^{nm} - 1)$ を満たす最小の正整数 j が m となるような正整数 i に対し, α のべき α^i とその $GF(p^n)$ の上の共役元 $\alpha^{ip^{nj}}$ ($j = 1, \cdots, m-1$) を根とする $GF(p^n)$ の上の多項式を作ることにより得られる[2].

表 A1.1 において, 一次の原始多項式は文献 (11) の数表 1 により, GF(3) の上の 4 次以下の原始多項式は文献 (59) の p.30 Table I によるが, それ以外の原始多項式は計算機によ

って探索したものである。

原始多項式の探索は，GF(p) の上の m 次の多項式を順次発生させ，その根の位数が p^m-1 になるかどうかを判定することにより行なった。位数の判定はつぎのような直接的方法を用いた。

(1) 発生した多項式を $f(x)$ とし，$f(0)=0$ あるいは $f(1)=0$ であれば棄てる。

(2) $f(x)$ の根を α とし，$\alpha^1, \alpha^2, \cdots, \alpha^i$ $\left(i \leq \frac{p^m-1}{p-1}\right)$ を逐次計算し，$i < \frac{p^m-1}{p-1}$ のとき $\alpha^i \in GF(p)$ となれば，その多項式は棄てる。

(3) $\beta = \alpha^{\frac{p^m-1}{p-1}}$ に対し，$\beta^1, \beta^2, \cdots, \beta^i$ $(i \leq p-2)$ を逐次計算し，$\beta^i = 1$ となれば，その多項式はすてる。

(1)(2)(3) で棄てらなかった多項式は原始多項式であることはいうまでもない。

表A1.1　GF(P)の上のm次の原始多項式
（P:素数，$3 \leq P \leq 47$，$p^m - 1 < 10^6$）

GF(3)

次数 m	位数 p^m-1	原始多項式 $p(x)$
1	2	$-1+x$
2	8	$-1+x+x^2$
3	26	$1-x+x^3$
4	80	$-1+x+x^4$
5	242	$1-x+x^5$
6	728	$-1-x+x^6$
7	2186	$1-x^2+x^7$
8	6560	$-1-x^3+x^8$
9	19682	$1-x-x^2-x^3+x^9$
10	59048	$-1-x-x^3+x^{10}$
11	177146	$1-x^2+x^{11}$
12	531440	$-1+x-x^2-x^3-x^4+x^{12}$

GF(5)

m	p^m-1	$p(x)$
1	4	$-2+x$
2	24	$2-x+x^2$
3	124	$-2-x+x^3$
4	624	$-2-x-x^2+x^4$
5	3124	$-2-x+x^5$
6	15624	$2-x+x^6$
7	78124	$-2-x+x^7$
8	390624	$-2-x-x^2+x^8$

GF(7)

m	p^m-1	$p(x)$
1	6	$-3+x$
2	48	$3-x+x^2$
3	342	$2-x+x^3$
4	2400	$3-x-x^2+x^4$
5	16806	$-3-x+x^5$
6	117648	$3-2x-x^2+x^6$
7	823542	$-3-x+x^7$

GF(11)

m	p^m-1	$p(x)$
1	10	$-2+x$
2	120	$-3-x+x^2$
3	1330	$4-x+x^3$
4	14640	$2-x+x^4$
5	161050	$-2-x^2+x^5$

GF(13)

m	p^m-1	$p(x)$
1	12	$-6+x$
2	168	$2-x+x^2$
3	2196	$-6-2x+x^3$
4	28560	$-6-2x-x^2+x^4$
5	371292	$-6-2x+x^5$

GF(17)

m	p^m-1	$p(x)$
1	16	$7+x$
2	288	$-7-x+x^2$
3	4912	$-3-x+x^3$
4	83520	$-6-x+x^4$

GF(19)

m	p^m-1	$p(x)$
1	18	$9+x$
2	360	$-5-x+x^2$
3	6858	$4-x+x^3$
4	130320	$-4-2x+x^4$

GF(23)

m	p^m-1	$p(x)$
1	22	$-10+x$
2	528	$-4-x+x^2$
3	12166	$-10-x+x^3$
4	279840	$11-x+x^4$

GF(29)

m	p^m-1	$p(x)$
1	28	$-10+x$
2	840	$14-x+x^2$
3	24388	$-3-x+x^3$
4	707280	$-3-x+x^4$

GF(31)

m	p^m-1	$p(x)$
1	30	$14+x$
2	960	$-7-x+x^2$
3	29790	$-3-x+x^3$
4	923520	$-9-2x+x^4$

GF(37)

m	p^m-1	$p(x)$
1	36	$-5+x$
2	1368	$-15-x+x^2$
3	50652	$-2-x+x^3$

GF(41)

m	p^m-1	$p(x)$
1	40	$-6+x$
2	1680	$-7-x+x^2$
3	68920	$-13-x+x^3$

GF(43)

m	p^m-1	$p(x)$
1	42	$15+x$
2	1848	$-9-x+x^2$
3	79506	$-20-x+x^3$

GF(47)

m	p^m-1	$p(x)$
1	46	$-10+x$
2	2208	$-8-x+x^2$
3	103822	$-5-x+x^3$

付録 II

低伝送速度の符号を用いる多相位相変調通信方式

第2章で，ディジット毎の検出 —— 最小距離復号を行う通信系に対しては，低伝送速度の符号は適さないことを明らかにした。この付録は，第2章を補足するために，低伝送速度の符号により多相位相変調された信号を用いる通信方式について述べたものである．ここでは，第2章とは異なり，受信信号に対して最適な処理（最尤検出）が行われるため，低伝送速度の符号が有効となる．

ここに用いられる距離に対する基本的な考え方は第2章のそれと類似している．しかし，第2章の距離が有限集合の上で定義されたのに対し，ここでは距離は実数の上に定義される．

この付録における新しい結果は，第2章で述べた α_0 - 符号が，ここで述べる通信方式に対し有効であることを示した

ことにある。

なお，ここでは第2章で用いた記号をそのまま用いる。

A2.1 M元ディジタル信号による通信方式

深宇宙通信などのように，送信電力は小さいが，帯域は十分取り得るような場合に対しては，いわゆるM元ディジタル信号を用いる通信方式[6][14]が適している。この方式の送信側は第2章の通信方式と同様に構成される。すなわち，情報源からの情報に応じ，qを法とする整数の剰余環$Z(q)$の上の符号長n，符号語数M，伝送速度R（ビット/シンボル）の符号*Cの符号語$S_k = (a_0^{(k)}, a_1^{(k)}, \cdots, a_{n-1}^{(k)})$ $(1 \leq k \leq M)$が選ばれ，これにより位相変調された信号$s_k(t)$が通信路に送出される。$s_k(t)$は第2章の式(2.7)と同様，次式で定義される。

$$s_k(t) = \sqrt{2S}\cos\left(2\pi f_0 t + a_i^{(k)}\frac{2\pi}{q}\right) \qquad i\Delta T \leq t \leq (i+1)\Delta T$$
$$i = 0, 1, \cdots, n-1$$

---

*ここでは$Z(q)$の上の符号のみを考える。これは，後に述べるように，この場合の距離が信号を含む空間上で定義され，符号のシンボル集合の選択は，余り問題とはならないからである。

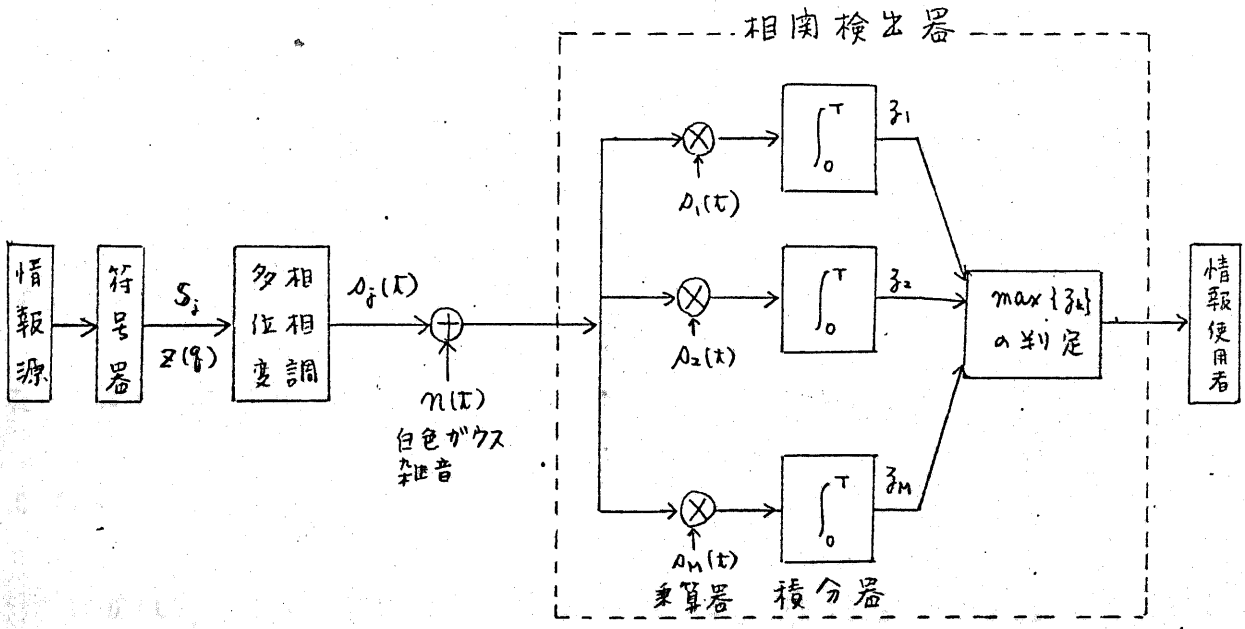
ここに，f_0，ΔT 等は第2章と同様に定義されている*

一方，受信側では，受信信号 $r(t)$ に対し，検出誤り率 P_E が最小となるような信号検出を行う．

ここで，さらに通信路の雑音 $n(t)$ が平均値0，片側電力スペクトル密度 N_0 の加法的白色ガウス雑音であるとし，送信側で各符号語の選ばれる確率が等しいと仮定する．この場合には最適検出は相関検出器で行われ，M元ディジタル信号を用いる通信系は図A2.1のような構成となる[14]．

相関検出器では，$r(t)$ からユークリッド距離 $\int_0^T (r(t)-\rho_i(t))^2 dt$

図A2.1　M元ディジタル信号を用いる通信系



*M元ディジタル信号は等エネルギー信号として，より抽象的に論ずることができる[14]が，ここでは第2章の補足の意味で，符号により位相変調された信号のみを論ずる．

の意味でもっとも近い信号語 $a_j(t)$ を求める操作を行なっていると考えられる．それゆえ，$a_j(t)$ が送られたとき，$r(t)$ にもっとも近い信号語が $a_j(t)$ となる確率を $1-P_{E|j}$ で表わすと，検出誤り率 P_E は次式で与えられる．

$$P_E = \frac{1}{M}\sum_{j=1}^{M} P_{E|j}$$

このことから，図A2.1の通信系では距離は信号を含む空間において定義するのが自然であることが分るであろう。

図A2.1の通信系に対する信頼度函数*の上界と下界は求められており，また，信頼度函数が正である伝送速度 R の限界 $R_{ef}(\rho)$ はこの場合には厳密に求めることができる(33)。$R_{ef}(\rho)$ はリー距離を用いた場合の $R_{ef0}(\rho)$ と比較して図2.8に示してある．この図から分るように，この通信方式は第2章の通信方式より $\rho(=E_b/N_0)$ のより広い範囲で用い得る．また，同一の ρ に対して，誤り率が小さくなることはいうまでもない．

しかし，この通信方式においては，受信器の複雑さは符号

---

*検出誤り率 P_E に対し，第2章の P_{NDC} に対する信頼度函数と同様に定義される．

語数に比例するから，符号語数の少い符号，したがって低伝送速度の符号を用いざるを得ない．第2章の方式においては低伝送速度の符号はきわめて不利であったが，この方式では図2.8から分るように，Pの小さいところで低伝送速度の符号は有効である．

このような通信系に適する符号（または信号）の研究は，M元ディジタル信号の設計問題として種々行われている[18][20][21]が，もっとも重要なものはつぎに述べる直交符号族である．

A2.2 直交符号族

図A2.1の通信系に用いられる符号として，よく知られているものに，直交符号，シンプレックス符号（超直交符号），陪直交符号[6]およびN－直交符号[22]がある．これらを，ここでは直交符号族と呼ぶことにしよう。

直交符号，シンプレックス符号，陪直交符号は通常アダマール行列から構成され二値であるが，符号長が q^m（シンプレックス符号に対しては q^m-1）となる $Z(q)$ の上の符号に拡張することは容易である．この場合"直交"の意味は符号

によって多相位相変調された信号が直交しているということである。

$Z(q)$ の上の直交符号は q^m-1 以下のすべての q 進数を列としてもつ $Z(q)$ の上の $m \times q^m$ 行列を生成行列とすることにより構成できる[22]。また，$Z(q)$ の上のシンプレックス符号は直交符号の生成行列からすべての成分が0の列を除いた行列を生成行列とする符号である。一方，陪直交符号を $Z(q)$ の上に一般化するには，$Z(q)$ の上の直交符号の生成行列にすべての成分が1の行をつけ加えた行列を生成行列とする符号を作ればよい。このような符号が $N-$ 直交符号である。

直交符号族によって変調された信号は種々の特徴をもつ。その一つは対称信号となっていることである。対称信号とは，各信号語から他の信号語への距離分布が同一となる信号である。明らかに，対称信号においては，どの信号語が送られた場合にも検出誤り率は等しい。すなわち，$P_E = P_{Ei}$ $(i=1,\cdots,M)$ となる。P_E は次式で与えられる[6]。

$$P_E = \int_{\chi}^{\infty} d\zeta_1 \int_{-\infty}^{\chi} \cdots \int p(\zeta_1, \zeta_2, \cdots, \zeta_M)\, d\zeta_2 \cdots d\zeta_M$$

ここに，$p(z_1, z_2, \cdots, z_M)$ は図A2.1の積分器の出力 $z_1, z_2, \cdots, z_M$ の結合確率密度で，次式で与えられる．

$$p(z_1, z_2, \cdots, z_M) = \frac{1}{(2\pi)^{\frac{M}{2}} |\Lambda|} \exp\{(z-\bar{z})\Lambda^{-1}(z-\bar{z})^t\} \tag{A2.1}$$

ここに，$z = (z_1, z_2, \cdots, z_M)$，$\bar{z} = (\bar{z}_1, \bar{z}_2, \cdots, \bar{z}_M)$ であり，$(z-\bar{z})^t$ は $z-\bar{z}$ の転置ベクトルを示す．また，Λ は (i, j) 成分が $\frac{N_0}{2ST}\rho_{ij}$ となるM×M行列で，ρ_{ij} は

$$\rho_{ij} = \frac{1}{ST}\int_0^T s_i(t)s_j(t)\,dt$$

で与えられる．さらに，$\bar{z}_i$ は z_i の平均値で $ST\rho_{1i}$ に等しい．

ρ_{ij} は信号語 $s_i(t)$ と $s_j(t)$ の間の相互相関係数であり，$s_i(t)$ と $s_j(t)$ のユークリッド距離の間につぎの対応がある．

$$\int_0^T (s_i(t)-s_j(t))^2\,dt = 2ST(1-\rho_{ij})$$

式(A2.1)の簡単な近次式として

$$P_E \leq \frac{L}{\sqrt{4\pi(ST/N_0)(1-\rho_{max})}} \exp\left\{-\frac{ST}{N_0}(1-\rho_{max})\right\}$$

がよく知られている[14]．ここに ρ_{max} は

$$\rho_{max} = \max_{\substack{i\neq 1 \\ 1\leq i\leq M}} \{\rho_{ij}\}$$

であり，L は $\{\rho_{ij} \mid 1 \le j \le M, j \neq i\}$ のうちで，これに近い値を有するものの数である．

このことは，誤り率 P_E が信号語間の最小（ユークリッド）距離によって大きく支配されることを意味する．それゆえ，信号設計の一つの目安として，信号語間の最小距離，または ρ_{max} をとることができる．直交符号族に対する ρ_{max} は表 A 2.1 のようになる．

直交符号，シンプレックス符号によって変調された信号はまた，等相関信号である．これは各信号語から他の信号語への距離がすべて等しい信号であり，等距離信号とも呼ぶ．等距離信号に対しては，誤り率 P_E は簡単に計算され，相互相関係数を ρ とするとき，次式で与えられる．

$$P_E = 1 - \int_{-\infty}^{\infty} \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}} \left[\Phi\left(x + \sqrt{\frac{2ST}{N_0}(1-\rho)} \right) \right]^{M-1} dx \quad (A2.2)$$

表 A2.1　直交符号族に対する ρ_{max}

符　号	シンボル数	符号長	符号語数	ρ_{max}
直交符号	q	N	N	0
シンプレックス符号	q	$N-1$	N	$-\frac{1}{N-1}$
N－直交符号（陪直交符号を含む）	q	N	qN	$\max\{0, \cos\frac{2\pi}{q}\}$

ここに $\Phi(y) = \int_{-\infty}^{y} \frac{e^{-\frac{u^2}{2}}}{\sqrt{2\pi}} du$ である.

N－直交符号（陪直交符号も含む）は等距離信号ではないが，誤り率 P_E の式は比較的簡単となり，$\mathrm{GF}(q)$ の上の符号長 q^m の符号に対し，

$$P_E = 1 - \iint_B \frac{e^{-\frac{x_1^2+x_2^2}{2}}}{2\pi} \left[\iint_{A(x_1)} \frac{e^{-\frac{y_1^2+y_2^2}{2}}}{2\pi} dy_1 dy_2 \right]^{q^{m-1}-1} dx_1 dx_2$$

で与えられる[22]. ただし，積分領域 $A(x_1)$ は $k = 1, 2, \cdots, q$ に対し，

$$\cos\left(\frac{2k-3}{q}\pi\right) \cdot y_1 + \sin\left(\frac{2k-3}{q}\pi\right) \cdot y_2 < x_1 + \sqrt{\frac{2ST}{N_0}}$$

となる領域であり，B は $k = 2, 3, \cdots, q$ に対し，

$$x_1 - \cot\left(\frac{k-1}{q}\pi\right) \cdot x_2 > -\sqrt{\frac{2ST}{N_0}}$$

となる領域である．なお陪直交符号に対しては，P_E の式はさらに簡単化される[6].

A2.3 αs－符号

第2章 2.6.4.2 で述べたαs－符号も図A2.1のような通信系に適した符号である。この符号は $\mathrm{GF}(p)$ の上で構成され，符号長 p^m-1，符号語数 p^{m+1} となる符号であるから，$\mathrm{GF}(p)$ の上の符号長 p^m のN－直交符号とほぼ等しい伝送速

度をもつ。しかも，N－直交符号の ρ_{max} が p の大きいところでは非常に大きくなるのに対し，α_ζ－符号においては，ρ_{max} をかなり小さくとることができる。しかし，現在のところ，α_ζ－符号の ρ_{max} を数式的に求めることはできず，計算機に頼らざるを得ない。その場合，2.6.4.2で述べたことを用い，計算をかなり簡単化することはできる。

なお，$\zeta=1$ となる α_ζ－符号は，それに全パリティ検査シンボルを付け加えれば，GF(p) の上のN－直交符号＊となり，このようなN－直交符号とほとんど同様なふるまいを示す。

表A2.2，$5\leq p\leq 19$，$p^m-1\leq 20000$ となるすべての素数 p および整数 $m(\geq 2)$ に対し，GF(p) の上の符号長 p^m-1 のすべての α_ζ－符号の ρ_{max} を示す。また，表A2.3には $23\leq p\leq 47$ となるすべての素数 p に対し，符号長 p^2-1 $(m=2)$，$\zeta=1$，β $(\beta=\alpha^{p+1})$ となる α_ζ－符号の ρ_{max} を示す。なお，これらの表には α_ζ－符号の最小ハミング距離も併せ示してある。

＊この場合は一次の Reed-Muller 符号となる。

αξ－符号は GF(p)（＝Z(p)）の上の線形符号であるから，これにより位相変調された信号は明らかに，対称信号となる。しかし，検出誤り率 P_E を厳密に計算することはきわめて難かしい。そこで，ここではαξ－符号の ρ_{max} に等しい相互相関係数をもつ等相関符号の誤り率 P_{EU}（式(A2.2)）により，αξ－符号の誤り率の上界をおめることにする。

図A2.2に，$P_E=10^{-5}$ のとき，GF(p) の上のN－直交符号および陪直交符号と比較して，αξ－符号の P－W/R 特性を示す。ただし，αξ－符号に対しては $P_{EU}=10^{-5}$ の場合であり，また，$5\leq p\leq 19$ となる素数 p に対するαξ－符号については各 m について ρ_{max} が最小となるもののみを示し，$23\leq p\leq 47$，$m=2$ のαξ－符号については $\xi=\beta$ $(=\alpha^{p+1})$ の場合のみを示してある。なお W/R と符号の伝送速度 R との関係は式(2.22)に示されている。

この図から分るように，αξ－符号は図A2.1の通信系に対し，かなりすぐれた特性を示し，図A2.1の通信系を設計する場合の符号の選択の範囲を広げるものである。

表 A2.2　αξ-符号の最小リー距離と ρ_{max} — I

$(5 \leq p \leq 19,\quad p^m - 1 < 20000)$

n：符号長 $(= p^m - 1)$　　R：伝送速度（ビット/シンボル）

$d_{L\min}$：最小リー距離　　$\beta = \alpha^{\frac{p^m-1}{p-1}}$

○：最大の $d_{L\min}$　　＊：最小の ρ_{max}

$p = 5$

m	2		3		4		5	
n	24		124		624		3124	
R	2.90×10^{-1}		7.49×10^{-2}		1.86×10^{-2}		4.46×10^{-3}	
ξ	$d_{L\min}$	ρ_{max}	$d_{L\min}$	ρ_{max}	$d_{L\min}$	ρ_{max}	$d_{L\min}$	ρ_{max}
β^0	24	0.3090	124	0.3090	624	0.3090	3124	0.3090
β	○ 26	＊0.1269	○136	＊0.0975	○736	＊0.0228	○3666	＊0.0220
β^2	24	0.3090	124	0.3090	624	0.3090	3124	0.3090
β^3	○ 26	＊0.1269	132	0.1129	○736	＊0.0228	3656	0.0298

m	6	
n	15624	
R	1.04×10^{-3}	
ξ	$d_{L\min}$	ρ_{max}
β^0	15624	0.3090
β	○18686	＊0.0045
β^2	15624	0.3090
β^3	○18686	＊0.0045

$p = 7$

m	2		3		4		5	
n	48		342		2400		16806	
R	1.75×10^{-1}		3.28×10^{-2}		5.85×10^{-3}		1.00×10^{-3}	
ξ	$d_{L\min}$	ρ_{max}	$d_{L\min}$	ρ_{max}	$d_{L\min}$	ρ_{max}	$d_{L\min}$	ρ_{max}
β^0	48	0.6235	342	0.6235	2400	0.6235	16806	0.6235
β	○ 75	＊0.1106	544	0.0891	4044	0.0171	28628	0.0090
β^2	72	0.1250	565	0.0467	4044	0.0171	28656	＊0.0054
β^3	48	0.6235	342	0.6235	2400	0.6235	16806	0.6235
β^4	○ 75	＊0.1106	○572	＊0.0294	4044	0.0171	○28663	0.0066
β^5	72	0.1250	560	0.0638	○4079	＊0.0121	28512	0.0104

$p = 11$

m	2		3		4	
n	120		1330		14640	
R	8.65×10^{-2}		1.04×10^{-2}		1.18×10^{-3}	
ξ	$d_{L\min}$	$\rho_{\max}$	$d_{L\min}$	$\rho_{\max}$	$d_{L\min}$	$\rho_{\max}$
β^0	120	0.8413	1330	0.8413	14640	0.8413
β^1	305	0.0796	3506	0.0389	○39696	0.0070
β^2	299	0.1116	○3539	0.0319	39608	0.0105
β^3	300	0.0833	3452	0.0556	39674	0.0080
β^4	300	0.0833	○3539	*0.0302	39660	*0.0067
β^5	120	0.8413	1330	0.8413	14640	0.8413
β^6	300	0.0833	○3539	0.0319	○39696	0.0070
β^7	299	0.1116	3450	0.0489	39608	0.0105
β^8	299	0.1116	○3539	*0.0302	39674	0.0080
β^9	○306	*0.0784	3450	0.0580	39660	*0.0067

$p = 13$

m	2		3	
n	168		2196	
R	6.61×10^{-2}		6.74×10^{-3}	
ξ	$d_{L\min}$	$\rho_{\max}$	$d_{L\min}$	$\rho_{\max}$
β^0	168	0.8855	2196	0.8855
β^1	510	0.0692	6906	0.0368
β^2	448	0.2171	5856	0.2171
β^3	420	0.3443	5490	0.3443
β^4	448	0.2171	5856	0.2171
β^5	○515	*0.0542	6938	*0.0259
β^6	168	0.8855	2196	0.8855
β^7	510	0.0692	○6970	0.0260
β^8	448	0.2171	5856	0.2171
β^9	420	0.3443	5490	0.3443
β^{10}	448	0.2171	5856	0.2171
β^{11}	○515	*0.0542	6874	0.0350

$p = 17$

m	2		3	
n	288		4912	
R	4.26×10^{-2}		3.33×10^{-3}	
ξ	$d_{L\min}$	$\rho_{\max}$	$d_{L\min}$	$\rho_{\max}$
β^0	288	0.9325	4912	0.9325
β	1160	*0.0546	20438	0.0225
β^2	1080	0.1952	18420	0.1952
β^3	1150	0.0681	20196	0.0332
β^4	720	0.5124	12280	0.5124
β^5	o1168	0.0574	20420	0.0226
β^6	1080	0.1952	18420	0.1952
β^7	o1168	0.0578	20320	0.0262
β^8	288	0.9325	4912	0.9325
β^9	1160	*0.0546	o20458	*0.0204
β^{10}	1080	0.1952	18420	0.1952
β^{11}	1150	0.0681	20376	0.0206
β^{12}	720	0.5124	12280	0.5124
β^{13}	o1168	0.0574	20374	0.0239
β^{14}	1080	0.1952	18420	0.1952
β^{15}	o1168	0.0578	20340	0.0253

$p = 19$

m	2		3	
n	360		6858	
R	3.54×10^{-2}		2.48×10^{-3}	
ξ	$d_{L\min}$	$\rho_{\max}$	$d_{L\min}$	$\rho_{\max}$
β^0	360	0.9458	6858	0.9458
β	1629	*0.0493	31934	0.0209
β^2	1587	0.0843	32201	0.0117
β^3	1200	0.4178	22860	0.4178
β^4	1629	0.0561	32214	*0.0100
β^5	1620	0.0560	31896	0.0220
β^6	1200	0.4178	22860	0.4178
β^7	1584	0.0871	32014	0.0173
β^8	1584	0.0871	32081	0.0142
β^9	360	0.9458	6858	0.9458
β^{10}	1584	0.0871	32010	0.0180
β^{11}	1587	0.0843	31880	0.0244
β^{12}	1200	0.4178	22860	0.4178
β^{13}	1631	0.0561	31778	0.0265
β^{14}	1620	0.0561	o32219	0.0103
β^{15}	1200	0.4178	22860	0.4178
β^{16}	1584	0.0871	32015	0.0172
β^{17}	o1641	0.0520	31932	0.0223

表 A2.3　$\alpha\xi$ - 符号の最小リー距離と ρ_{max} - II

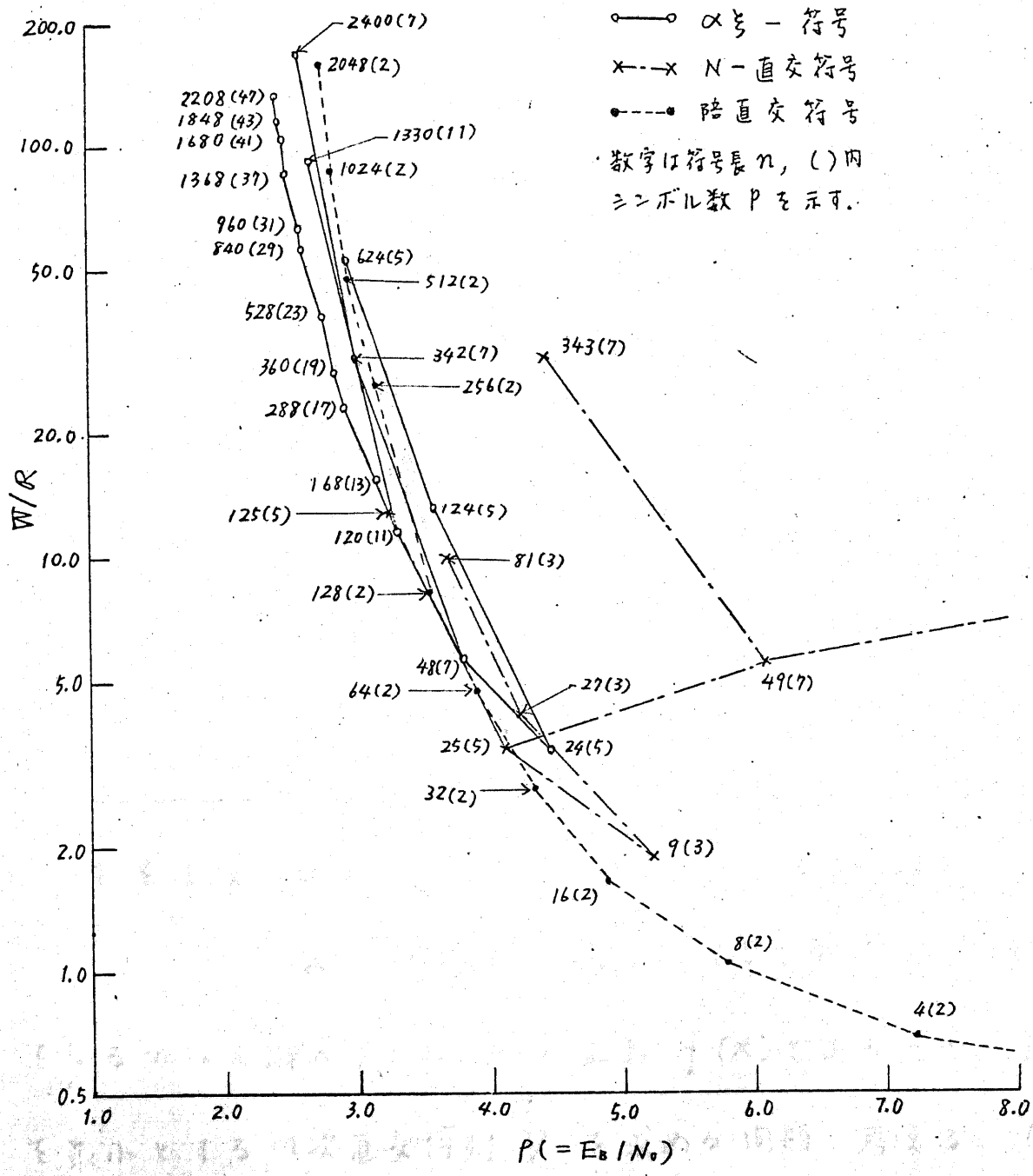
$(23 \leq p \leq 47,\ m=2,\ \xi=1,\ \beta(=\alpha^{p+1}))$

n : 符号長 $(=p^2-1)$　　R : 伝送速度 (ビット/シンボル)

$d_{L\,min}$: 最小リー距離

p	n	R	ξ	$d_{L\,min}$	ρ_{max}
23	528	2.57×10^{-2}	1	528	0.9629
			β	2915	0.0413
29	840	1.74×10^{-2}	1	840	0.9766
			β	5894	0.0331
31	960	1.55×10^{-2}	1	960	0.9794
			β	7215	0.0311
37	1368	1.14×10^{-2}	1	1368	0.9856
			β	12330	0.0262
41	1680	9.57×10^{-3}	1	1680	0.9882
			β	16820	0.0237
43	1848	8.81×10^{-3}	1	1848	0.9894
			β	19125	0.0226
47	2208	7.55×10^{-3}	1	2208	0.9911
			β	26410	0.0208

図 A2.2　αシ－符号，N－直交符号，
陪直交符号の P－W/R 特性
（$P_E = 10^{-5}$）



付録 III

置換多面体の理論の応用について

第6章 6.3 で述べた置換多面体の理論は，それ自体数学の問題として興味深いばかりではなく，ある種の最適化問題への応用が可能であると思われる．事実，第6章における最適化は，この理論を用いることによって簡単に，しかも大域的に行うことができた．ここでは，さらに二通りの最適化問題への適用法について考える．なお，ここでも 6.3 で用いた仮定および記号をそのまま用いる．

A3.1 直交行列の最適化問題

A を与えられた n 次対称行列とし，評価函数が，

$$x = \mathrm{Diag}(V^t A V) \quad (V: n\text{次直交行列})$$

となる n 次元縦ベクトル x の函数 $f(x)$ であるとき，$f(x)$ を最小とする n 次直交行列 V を求める問題を考える．なお Diag は第6章 6.3 で定義されている記号である．

第6章，6.4.3.2，6.4.3.3における $\mathcal{L}(U)$，$\mathcal{F}(V)$ の最適化はこのような問題に帰着した。ここでは，より一般的に考えよう。

この問題を，直交行列 V の成分を変数として直接解くのは通常，かなりむずかしい。これは，変数の数が多く，また，それらにかなり複雑な制約条件（直交という条件）がついているからである。

これに対し，置換多面体の理論を用いるつぎのような解法が考えられる。

(1) A を対角化する直交行列および A の固有値を求める。すなわち，

$$V_A A V_A^t = A_D \equiv \begin{bmatrix} \alpha_1 & & 0 \\ & \alpha_2 & \\ 0 & & \ddots \\ & & & \alpha_n \end{bmatrix}$$

となる n 次直交行列 V_A，および $\alpha_1, \alpha_2, \cdots, \alpha_n$ を求める。

(2) $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)^t$ によって生成される置換多面体 $P_n(\alpha)$ において，$f(x)$ を最小とする点 $x^0 = (x_1^0, x_2^0, \cdots, x_n^0)^t$ を求める。

(3) $\mathcal{X}^0$ に

$$\mathcal{X}^0 = Diag(\mathcal{W} A_D \mathcal{W}^t)$$

によって対応する n 次直交行列 $\mathcal{W} = [w_1 w_2 \cdots w_n]$ を求める。

(4) $\mathcal{V}^0 = \mathcal{W} \mathcal{V}_A$ が求める直交行列である。

(注) (3) において $\mathcal{W}$ を求めるのは定理 6.3 の証明を用いて，逐次行えばよい。すなわち，

(i) 式(6.15)を満たす k および ρ を求め，w_1 を式(6.16)によって定める。（ただし，$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$ を仮定しておく）。

(ii) 式(6.19)により，$\beta_1, \beta_2, \cdots, \beta_{n-1}$ を求める（$\beta_1 \geq \beta_2 \geq \cdots \geq \beta_{n-1}$ となることに注意）。

(iii) $x_2 = \rho' \beta_{k'} + (1-\rho') \beta_{k'+1}$ を満たす k' および ρ' を求め

$$u_i^{(1)} = \begin{cases} \sqrt{\rho'} & ; \ i = k' \\ \sqrt{1-\rho'} & ; \ i = k'+1 \\ 0 & ; \text{その他の場合} \end{cases}$$

によって $u_1 = (u_1^{(1)}, u_2^{(1)}, \cdots, u_{n-1}^{(1)})^t$ を定める。

(iv) 式(6.17)により w_2 を定める.

(v) 以下同様に,次元を逐次下げて $w_3, w_4, \cdots, w_n$ を定めていく.最後に w_{n-1} と w_n は同時に定まる.

ここで述べた解法によれば,元の問題では変数が n^2 個(直交行列 V の成分の数)であるのに対し,変数を n 個に減らして解くことができる.ただし,(2)の過程における最適化は制約条件が非常に多く,$f(\alpha)$ の形によっては α° を求めることはかなり困難となる.しかし,才6章の場合のように $P_n(\alpha)$ において $f(\alpha)$ が上に凸であったり,あるいは,制約条件をつけないときの $f(\alpha)$ の最小値が $P_n(\alpha)$ に含まれるような場合には簡単に行える.

このような形の最適化問題は,多次元線形通信系においても,評価量として二乗平均誤差ではなく,より複雑なものを用いる場合などに現れることがある.

A3.2 閉じた線形制約領域における最適化問題

閉じた線形制約領域 R (線形不等式で与えられる領域[73])において,n 変数函数 $f(\alpha) = f(x_1, x_2, \cdots, x_n)$ を最小とす

る問題を考えよう。

$\mathcal{R}$ の端点を $P_1, P_2, \cdots, P_N$ とする。このとき $\mathcal{R}$ に含まれる任意のベクトル α は

$$\alpha = \sum_{i=1}^{N} \xi_i P_i \quad \left(\sum_{i=1}^{N} \xi_i = 1, \ \xi_i \geq 0 \ (i=1,\cdots,N) \right)$$

と表わせる。そこで，$f(\alpha)$ を $\xi = (\xi_1, \xi_2, \cdots, \xi_N)^t$ の函数として $f_\xi(\xi)$ と表わせば，はじめの問題は $\sum_{i=1}^{N} \xi_i = 1$, $\xi_i \geq 0$ $(i=1,\cdots,N)$ となる ξ の領域 $\mathcal{R}_\xi$ で $f_\xi(\xi)$ を最小にする問題となる。ところで，この様な ξ の領域 $\mathcal{R}_\xi$ は，$\alpha = (1,0,0,\cdots,0)^t$ とすれば，α によって生成される置換多面体 $P_N(\alpha)$ にほかならない。

ゆえに，定理 6.5 により，ξ $(\in \mathcal{R}_\xi = P_N(\alpha))$ は N 次の逆対称行列 S を用い，

$$\xi = [(I-S)^{-1}(I+S)]^{*2}\alpha \qquad (A3.1)$$

と表わせる。ここで，

$$S = \begin{bmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1N} \\ -a_{12} & 0 & a_{23} & & a_{2N} \\ -a_{13} & -a_{23} & 0 & \ddots & \\ \vdots & & \ddots & \ddots & a_{N-1N} \\ -a_{1N} & -a_{2N} & \cdots & -a_{N-1N} & 0 \end{bmatrix}$$

とおき，式 (A3.1) を $f_\xi(\xi)$ に代入すれば，$f(\alpha)$ は結局

α_{ij} ($i=1,\cdots,N-1$; $j=i+1,\cdots,N$) の函数と考えることができる。しかも，このような α_{ij} にはまったく制約条件はつかない。すなわち，閉じた線形制約領域 R における n 変数函数 $f(x)$ の最小化問題は，制約条件のつかない $N(N-1)/2$ 変数函数の最小化問題に帰着する。ここに，N は R の端点の数である。

このように閉じた線形制約領域における非線形計画問題は，常に制約のない問題に変換できる。これは理論的には，きわめて興味深い事実であるが，実際問題としては，この変換のための変数の増加は一般に，非常に厖大なものとなり，制約のない問題とすることによって，必しも計算が簡単となる訳ではない。しかし，特に R がはじめから置換多面体であったり，または置換多面体に簡単に変換し得る形であるときには，このような方法が有効であることもあるであろう。

これらの問題に対しては，なお今後の研究が必要である。

文　献

共通

(1) W. W. Peterson : " Error - correcting codes ", John Wiley (1961).

(2) E. R. Berlekamp : " Algebraic coding theory ", McGraw - Hill (1968).

(3) R. G. Gallager : " Information theory and reliable communication ", John Wiley (1968).

(4) H. B. Mann ed. : " Error - correcting codes ", John Wiley (1968).

(5) 嵩, Lin, Peterson : " Reed - Muller 符号とその拡張について ", 信学論(C), 51-C, P. 98 (昭 43-03).

(6) S. W. Golomb ed. : " Digital communications ", Prentice - Hall (1964).

(7) B. L. van der Waerden : " Algebra I, II ", Springer (1955).

(8) 稲葉 : " 整数論 ", 共立 (昭 31).

(9) 正田, 浅野 : " 代数学 I ", 岩波 (昭 37).

(10) 浅野, 永尾 : " 群論 ", 岩波 (昭 41)

(11) 日本数学会編 : " 数学辞典 才2版 ", 岩波 (昭 43).

第1章

(12) C. E. Shannon : " A mathematical theory of communications ", Bell Syst. tech. J., 27, P.379 (1948).

(13) 岩垂 : " バースト訂正符号の統一的取扱い ", 信学論 (A), 52-A, P.305 (昭44-08).

(14) J. M. Wozencraft and I. M. Jacobs : " Principles of communication engineering ", John Wiley (1965).

(15) M. J. E. Golay : " Notes on digital coding ", Proc. IRE, 37, 6, P.657 (1949)

(16) S. W. Golomb, B. Gordon and L. R. Welch : " Comma-free codes ", Can. J. Math., 10, 2, P.202 (1958).

(17) H. Landau and D. Slepian : " On the optimality of the regular simplex code ", Bell Syst. tech. J., 45, 8, P.1247 (1966).

(18) C. L. Weber : " Elements of detection and signal design ", McGraw-Hill (1968).

(19) 尾佐竹, 田中 : " 最適アナログ変調の一方式 ", 信学論 (B), 51-B, 2, P.49 (昭43-02).

(20) D. Slepian : " Permutation modulation ", Proc. IEEE, 53, 3, P.228 (1955).

(21) 伊藤 : " 巡回変換群を用いた通信方式 ", 信学論 (B), 52-B, 11, P.697 (昭44-11)

(22) I. S. Reed and R. A. Scholtz : " N-orthogonal phase-modulated codes ", IEEE Trans., IT-12, 3, P.388 (1966).

(23) 宮川，今井："非線形誤り訂正符号"，信学誌（治：研究動向），53，5，P.670 （昭45－05）.

才2章

(24) 岩垂："符号理論の実用上の諸問題"，京大数研講究録 95，P.93 （昭45－08）.

(25) 岩垂："誤り制御方式を持つ通信方式設計の基礎概念"，昭45 全大，S.9－3.

(26) J.L. Massey："Threshold decoding"，MIT Press (1963).

(27) W.C. Gore："Generalized threshold decoding of linear codes"，IEEE Trans., IT-15，5，P.590 (1969).

(28) C.W. Helstrom："Statistical theory of signal detection"，Pergamon (1960).

(29) W.R. Bennett and J.R. Davey："Data transmission"，McGraw-Hill (1965).

(30) W.B. Davenport, Jr. and W.L. Root："An introduction to the theory of random signals and noise"，McGraw-Hill (1958).

(31) R.M. Fano："Transmission of information"，MIT Press (1963).

(32) C.E. Shannon, H.G. Gallager and E.R. Berlekamp："Lower bounds to error probability for coding on discrete memoryless channels I, II"，Inform. Control，10，P.65, P.522 (1967).

(33) A. D. Wyner : " Bounds on communication with polyphase coding ", Bell Syst. tech. J., 45, p. 523 (1966).

(34) 森口，高田：" 数値計算法 I "， 岩波 (昭 33)

(35) T. Kasami, S. Lin and W. W. Peterson : " Polynomial codes ", IEEE Trans., IT-14, P.307 (1968).

(36) S. L. Hakimi and J. G. Bredeson : " Graph theoretic error-correcting codes ", IEEE Trans., IT-14, p.584, (1968).

(37) E. N. Gilbert : " Gray codes and paths on the n-cube ", Bell Syst. tech. J., 37, p.815 (1958)

(38) 池田，中道，大沼：" Digit sequence による単位距離 2 進化 10 進符号の分類と総数 "， 昭 45 全大，139.

(39) J. K. Wolf : " On codes derivable from the tensor product of check matrices ", IEEE Trans., IT-11, p.281 (1965).

(40) 宮川，今井：" 誤り訂正符号を用いた多相位相変調通信の限界 "， 昭 45 全大，19.

才 3 章

(41) A. W. Nordstrom and J. P. Robinson : " An optimum nonlinear code ", Inform. Control, 11, P. 613 (1968).

(42) S. M. Johnson : " A new upper-bound for error-correcting codes ", IRE Trans., IT-8, p.203 (1962).

(43) F. P. Preparata : "Weight and distance structure of Nordstrom-Robinson quadratic code", Inform. Control. 12, p. 406 (1968).

(44) F. P. Preparata : "A class of nonlinear double-error correcting codes", Inform. Control, 13, p. 378 (1968).

(45) T. J. Wagner : "A remark concerning the minimum distance of binary group codes", IEEE Trans., IT-11, p. 458 (1965).

(46) 嵩, Lin, Peterson : "アフィン変換に不変に保たれる線形符号の性質および BCH 符号の最短距離について", 信学誌, 50, p. 1617 (昭42-09)

(47) N. Tokura and T. Kasami : "A search procedure for finding optimum group code for binary symetric channel", IEEE Trans., IT-13, 4, p. 587 (1967).

(48) 宮川, 今井, 中島 : "修正 Preparata 符号について", 信学会インホメーション理論研資 (昭45-07)

(49) 宮川, 今井 : "最適な二重誤り訂正非線形組織符号 —— 修正 Preparata 符号について", 京大数研講究録 95, p. 81 (昭45-08)

(50) 宮川, 今井, 中島 : "修正 Preparata 符号 —— 組織符号として最適な非線形二重誤り訂正符号", 信学論(A), 53-A, 10, p. 531 (昭45-10).

才4章

(51) A. B. Glenn : "Code division multiplex system", 1964 IEEE Internat. Conv. Record, 12, Pt 6.

(52) 今井：“符号分割多重通信方式と帰還通信路の基礎的研究”，東大工学部修士論文（昭43）.

(53) 宮川，今井：“非同期CDM通信におけるパルス波形”，昭43 連大 2017.

(54) E.N. Gilbert：“Cyclically permutable error-correcting codes”，IEEE Trans., IT-9, 3, p.175 (1963).

(55) P.G. Neumann：“On a class of cyclically permutable error-correcting codes”，IEEE Trans., IT-10, p.75 (1964).

(56) J. MacWilliams：“The structure and properties of binary cyclic alphabets”，Bell Syst. tech. J., 44, 22, p.303 (1965).

(57) 宮川，今井：“回線分離符号の構造と構成法”，信学会インホメーション理論研資（昭45-01）.

(58) 宮川，今井：“回線分離符号の構造と構成法”，信学論（A），53-A，1，P.51（昭45-01）.

第5章

(59) W.H. Kautz ed.：“Linear sequential switching circuits”，Holden-Day (1965).

(60) S.W. Golomb：“Shift register sequences”，Holden-Day (1967).

(61) 中村，岩垂：“多値スクランブラについて”，信学会通信方式研資（昭45-07）.

(62) 野村，福田："多次元巡回符号と線形再帰空間"，昭45全大 S.9-7.

(63) H.O. Burton and E.J. Weldon："Cyclic product codes"，IEEE Trans., IT-11，p.433 (1965).

(64) 野村，宮川，今井，福田："最大面積行列をもつ平面の構成法"，信学会インホメーション理論研資（昭45-11).

(65) 野村，宮川，今井，福田："最大面積行列をもつ平面の諸性質"，信学会インホメーション理論研資（昭45-11).

(66) 野村，宮川，今井，福田："最大面積行列をもつ平面の構成法と諸性質"，信学論(A) 掲載予定.

(67) 野村，宮川，今井，福田："最大面積行列をもつ線形再帰平面 —— M系列の二次元への拡張"，昭46全大投稿中.

オ6章

(68) A.V. Balakrishnan ed.："Communication theory"，McGraw-Hill (1968).

(69) 甘利："情報空間論 —— 信号空間の量子化と帯域幅圧縮"，信学誌，48，10，p.1709 (昭40-10).

(70) 甘利："情報理論"，ダイヤモンド社（昭45).

(71) 辰佐竹，田中："最適通信方式 —— マトリックス変換による伝送路と情報の整合問題"，信学論(A)，52-A，12，p.513 (昭44-12).

(72) G.C. Rota and L.H. Harper : "Matching theory, an introduction", Waltham (1967).

(73) G. Hadley : "Nonlinear and dynamic programming", Addison-Wesley (1964).

(74) 遠山 : "行列論", 共立 (昭37).

(75) R. Penrose : "A generalized inverse for matrices", Proc. Camb. Phil. Soc. 51, p.406 (1955).

(76) 古屋 : "一般逆行列 I", 数理科学, p.68 (昭42-05).

(77) 宮川, 今井 : "一般逆行列を用いて復調を行う線形多次元通信系の最適化", 昭44全大 133.