整数剰余環上の誤り訂正符号と
そのデジタル通信系への応用に関する研究

2000年　3月

中　村　勝　洋

内容梗概

本論文は、筆者が1970年代後半から80年代後半にかけて研究開発した整数剰余環上の誤り訂正符号に関する理論とその応用に関する技術について、これを再度全体的に見直し、若干の修正と説明の追加および今後の展望を加えてまとめ直したものである。

情報を符号化して通信する際に、通信路（記録媒体も含む）で生じた符号誤りを受信側で訂正できるように、もしくは検出できるように、通常、冗長性を付加した符号化が行なわれる。誤り訂正符号技術は、そのための符号化法や復号法に関する技術である。また、そのような符号化法や復号法あるいは符号の性能評価に関する理論を単に符号理論と呼ぶことも多い。誤り訂正符号技術は、大量のマルチメディア情報を高速に通信し、蓄積し、処理するこれからの高度情報化社会において、信頼性の高い情報通信を行うために必要かつ不可欠な技術である。

さて、従来よく研究されてきた誤り訂正符号の大部分は、理論的にみると一般には有限体$GF(q)$の上の符号であり、符号語間の距離はHamming距離に基づくものが殆どである。そしてその理論的体系もある程度確立されてきている。しかしながら、符号の構成法としては必ずしも有限体上に限る必要はなく、通信路における符号誤りの発生の仕方にマッチした距離構造を持つ符号が、有限環など他の集合の上に構成できるのであれば、従来とは異なる新たな性能のよい符号の構成法を確立できる可能性がある。

一方、現実の基幹通信システムは近年益々大容量化を迫られ、高密度のデジタル通信技術を色々と駆使して大容量化を達成する必要性があった。80年代初頭、周波数有効利用の観点から高密度化の進むデジタルマイクロ波無線(DMR)通信システムにおいても、その特性改善のために、変復調技術を含め何がしかの抜本的対策が望まれていた。そこでは必然的に多値信号が採用されており、信号点間の距離に配慮した信号設計が課題となりつつあった。

本論文ではこれらの状況を踏まえて、新たな符号として整数剰余環$Z_q = Z/(qZ)$（integer residue ring modulo q）上の符号を提案し、まずその符号の構成法に関する手法・理論を導いている。その際、整数剰余環Z_q上の線形フィードバックシフトレジスタの性質に関する解析結果をベースとしている。符号語間の距離としては、Lee距離を採用している。これは、符号の適用対象として高密度の信号空間を考慮してのことである。ついで、この符号を現実の回路としてインプリメントするための手法を述べ、符号器・復号器の構成法を導いている。更に、この符号を大容量の通信基幹回線に適用する際の手法について述べており、高密度の信号点間の距離に配慮した効率的な符号系の構成法を提示している。具体的には差動符号化多値QAM(Quadrature Amplitude Modulation ; 直交振幅変調)方式を採用している大容量のデジタルマイクロ波無線通信システムへの適用である。そして、その符号系の良好な特性評価結果も示している。

以上の結果、本論文で導かれた整数剰余環上のLee距離に基づく符号は、DMR通信分野の製品に世界で最初に採用された誤り訂正符号となった。更に言えば、有限体に限らず、有限環の上でも実用的でかつメリットのある符号系を構成できることが理論的にも実用的にも提示

されたことになり、今後の現実のシステムに導入する符号系の選択肢が更に広がったともいえる。

本論文の第１章では、まず符号理論研究の歴史的流れや実用化の状況に簡単に触れた後、本研究が生まれる背景と動機並びに研究の目的について上で述べた事柄を更に詳しく述べている。

第２章では、上記整数剰余環 Z_q 上の Lee 距離に基づく誤り訂正符号の具体的な構成法を導いている。まず符号構成上の観点から、整数剰余環 Z_q 上の線形フィードバックシフトレジスタの性質について考察し、これを拡大環の表現法につなげて、符号構成上の有用な結果をいくつか導いている。つまり拡大環における剰余類に関するいくつかの性質を導いている。ついで、これらの有用な結果をもとに巡回符号の概念を拡張した形で環 Z_q 上の Lee 距離に基づく誤り訂正符号を導き、１重 Lee 誤り訂正符号、２重 Lee 誤りの殆どを訂正する準２重 Lee 誤り訂正符号、および２重 Lee 誤り訂正符号について、それぞれの構成法並びに復号法を与えている。更にはその一般化への試みとその展望についても記している。

第３章ではこれらの符号をインプリメントするための手法を導き、符号器・復号器の構成法について、例題を用いながら述べている。そこでの構成法は、第２章で述べた環 Z_q 上の線形フィードバックシフトレジスタの性質と符号の構成法に基づいており、符号器・復号器が線形フィードバックシフトレジスタを用いた自然な形の手法に従って構成できることを示している。そして BCH 符号など有限体上の符号をインプリメントする場合との違いに重点を置いて述べている。また高速化の観点からその並列処理法についても論じている。更に、実際に開発し実用に供した２重 Lee 誤り訂正符号の LSI についても紹介している。

第４章では、得られた環 Z_q 上の誤り訂正符号を現実の高密度デジタル通信システムに導入する際の技術について述べている。具体的には大容量のデジタルマイクロ波無線 (DMR) 通信システムへの応用について述べている。DMR 通信の世界へ誤り訂正符号を導入するにあたっては、変調系との親和性を保つことによって、符号の持つ能力を最大限発揮させる必要がある。高密度 DMR 通信での信号の変調方式としては、高密度の点から通常、差動符号化多値 QAM 方式が用いられるが、この方式に誤り訂正符号を導入するには、差動符号化と誤り訂正の位置づけ、符号ビットの割り当て、システム構成、更には、電力有効利用の観点から、信号点配置を原点の周りに円形上に取ったときの誤り訂正符号の巧妙な構成法といった様々な手法を導く必要があった。本論文では、これらについて明らかにすると共に、この符号系によって改善された通信システムの特性評価についても解析し、良好な結果を得ていることを示している。そして、本論文で導かれた整数剰余環上の Lee 距離に基づく符号が、DMR 通信分野の製品に世界で最初に採用された誤り訂正符号となったことを述べている。

最後に第５章では、まとめとして、本研究により、整数剰余環 Z_q 上の Lee 距離に基づく誤り訂正符号の構成法が導かれたこと、その符号を用いて高密度の信号空間における効率的な符号系の構成法が提示されたこと、およびそのことが有限体に限らず、有限環の上でも実用的でかつメリットのある符号系を構成できることを意味していること、などを結論づけている。そして今後の現実のシステムに導入する符号系の選択肢が本論文によって更に広がったとしている。また、最近の動向を踏まえた今後の展望についても考察している。

謝辞

本研究を進めるにあたり、終始御理解ある御指導と御助言をいただきました東京大学伏見正則教授に心より感謝致します。また本研究に関し懇切丁寧な御指導と御助言をいただきました東京大学山本博資教授に深く感謝致します。山本研究室の方々にも何かとお世話になりました。併せて感謝致します。また、本研究をまとめるにあたって、東京大学杉原厚吉教授、武市正人教授、速水謙助教授、松井知己助教授には適切な御助言と御指導をいただきました。深く感謝致します。

本研究を学位論文にまとめあげるよう励ましていただいた立命館大学（元東京大学）有本卓教授に心より感謝致します。更に、本研究の学位論文へのまとめあげを再三にわたり促し励まし続けていただいた、大学時代の同窓／先輩でもある専修大学佐藤創教授、電気通信大学小林欣吾教授、星守教授、韓太舜教授および神奈川大学紀一誠教授に心より感謝致します。特に佐藤創教授には本研究をまとめるに際し、多くの御助言をいただき何かとお世話になりました。また電気通信大学のグループには、情報理論研究の立場からの符号研究に関し、その心を学ぶ機会や世界の動向を知る機会を長年にわたる同大学でのIT研究会で与えていただきました。

筆者がNECに入社したときの上司で、その頃から信号設計理論と符号理論との融合、理論と設計の技術者魂を説かれ、感化を受けました現在創価大学の渡部 和教授に心より感謝致します。また、符号理論関連の研究を進めるにあたり、入社の頃以来上司としてまた先達として長きにわたって御指導いただいた、現在多摩大学の岩垂好裕教授に深く感謝致します。そして同じ通信研究部の先輩と後輩でもあった、現在東邦大学の佐藤洋一教授と岡本栄司教授(兼 Wisconsin 大学）に心より感謝致します。当時からQAM通信方式や各種の符号化に関して色々御討論、御教示いただきました。

また本研究を具体化し製品化していく上で、NEC の野口俊武氏、龍敏彦氏、野田誠一氏、そのほか多くの方々にお世話になりました。心より感謝致します。野口氏らが中心になって開発したデジタルマイクロ波無線(DMR)通信装置に本研究成果が取り入れられたことによって、本論文で述べるLee距離に基づく符号が、DMR通信分野の製品に採用された誤り訂正符号として、世界最初のものになりました。特に野田誠一氏とは、最初に採用した1重Lee誤り訂正符号を2重Lee誤り訂正符号へVersion Upするに際し、符号パラメータの選定や符号評価など夜を徹して討論したこともあり、色々な面で最もお世話になりました。氏との出会いという偶然にも感謝したいと思います。

更に、ここに全ての名前をあげることは出来ませんが、NECに入社以来お世話になった、上司の方々、諸先輩方、同僚諸氏にこの場を借りて感謝の意を表します。特に、本研究を推進していく上で、上司として暖かく見守り励まし続けていただいたNECの(故)加藤康雄氏、杉山峰夫氏、石黒辰雄氏、松尾良雄氏、後藤裕一氏、飯沼一元氏、後藤　敏氏に深く感謝致します。また本研究を始めた当初には、NECの渡辺孝次郎氏、明石文雄氏、並木淳治氏、広崎膨太郎氏にも有益な御討論をいただきました。心より感謝致します。更に、日頃符号理論の研究全般にわたって、有益な御討論をいただいているNECの岡村利彦氏、神谷典史氏、有田正剛氏、山西健司氏、竹内純一氏を始めとする多くの若い研究者の方々に心より感謝します。そして、本研究をまとめる上で図表の作成等でお世話になった福島芳美さんに感謝します。

最後になりましたが、筆者の研究生活を終始支え励まし続けてくれた、妻 博子と子供たち寛史、文香に心より感謝します。

2000年3月　　中　村　勝　洋

目 次

第1章　序　論

1.1　本研究の背景と目的

高度情報化社会への急速な進展に伴い、大量のマルチメディア情報を高速に通信し、蓄積し、処理する技術／システムが開発されて来ている。誤り訂正符号技術は、これらの技術を支える一つの重要な技術であり、各種の通信システムや記録システムの信頼性向上を主たる目的とした、情報の符号化法に関する技術である。単に符号理論と言ったときには、この誤り訂正符号の符号化法やその性能限界に関する理論を指すことが多い。符号理論に関する研究は、1948年に発表されたC.E.Shannon[1]の有名な論文、"A Mathematical Theory of Communication"に始まる。そこに記された通信路符号化定理においては、通信路(記憶媒体も広い意味で含む)での符号誤りを限りなく零にできる符号が、一定の条件を満たす符号の中に存在するという事が示されている。その条件とは、符号の中に占める情報部分の割合（ビット／記号）が、各通信路固有に定まる通信路容量（ビット／記号）より小さいという条件である。以来、このような理論的限界を満たす符号を求めて、通信路上で生じた誤りを訂正もしくは検出する符号を構成する試みが数多くなされ、その過程で多くの優れた効率的な符号が構成されてきた。1950年のHamming符号を始めとして、巡回符号、中でもBCH符号、Reed Solomon符号、更には代数曲線符号、畳み込み符号／Viterbi復号法、トレリス符号化変調方式等々の理論的・方式的研究成果は符号理論の中でも代表的なものである[2]-[4]。

これらの成果は、先ずは宇宙通信や衛星通信への応用を皮切りにして、その後の情報のデジ

タル化の波に乗って、あるいはまた、複雑な処理をワンチップ化するLSI技術の発展を背景に、データモデム、移動体通信、半導体メモリ、更には、マルチメディア情報を高速に通信する大容量の基幹通信回線、磁気ディスクあるいはCD(Compact Disc)やDVD(Digital Versatile(／Video) Disc)を含む光ディスクなどの記録媒体、等々の様々な分野で実用的な研究開発を促し、信頼性の高い情報通信を行うのに必要不可欠な技術として応用されてきた。そして、今なお、マルチメディア情報通信システムの高度化・高信頼化に向けて、更に性能の良い符号化方式を求めた理論的・実用的研究開発が進行中である[5]。

ところで、これら従来よく研究されてきた誤り訂正符号の大部分は，理論的にみると、一般には有限体 $GF(q)$ （$q = p^m$ ：素数 p のべき乗）の上の符号であり、その理論的体系も確立されてきている。しかしながら、q を法とする整数剰余環 $Z_q = Z/(qZ)$（integer residue ring modulo q）の上の符号については、$m \neq 1$ のときには、環 Z_qが一般に零因子をもつことによる数学的な取扱いの困難さや、メリットのある適当な応用の場を見出すことの困難さと言ったことから、これまで符号理論の主流的な研究の流れからは遠ざかっていたように思われる。しかしながら、そのような流れの中にあっても既に70年代の頃から、環 Z_q 上の符号の検討結果が細々ながらも少しずつ現われ始めていたと考えられる[7]-[12]。

1938年には、M.Hall[6]による、Z_q の上の線形再帰系列に関する幾分調査的ではあるが先駆的な研究が見られるものの、環 Z_q の上の符号の研究が現れるのは60年代後半からである。環 Z_q の上の符号としては、Z_q の性質からいって、符号語間の距離が、Hamming距離に基づくものと、Lee距離に基づくものとの2通りを考えることができる。前者については70年代にBlake [7][8], ついで，Spiegel[9][10]，そして、Shankar[11]らがその構成法を示している。そこでは、従来のBCH符号やRS符号に似せて、Hamming距離に基づいた Z_q の上の符号を構成することが試みられている。しかしながら、巡回符号を構成することに限定しているた

めに、有限体上の符号と比較したとき、符号の効率性などの面から、有限環の上で符号を構成することのメリットがあまり明らかになっていないように思われる。一方，後者の符号は，前者に類似した性質をいくつか持つものの，前者から直接的に導くことができないので，独自の検討を必要とする．後者の例として 60 年代に Berlekamp[3] の導いた負巡回符号（negacyclic code）がよく知られているが，これは q を素数の場合（m=1 の場合）に限っており、従って結局は環というより有限体の上の符号となっている。一方、宮川等 [12] は 70 年代の中頃、最小 Lee 距離が 3 あるいは 4 の符号を計算機で探索して構成する手法を与えていた。

これらの研究を背景に，もしくは，それらに前後して，70 年代の後半頃から中村 [15]-[23] も、整数剰余環 Z_q の上の符号、中でも特に Z_{2^m} 上 の 2 重 Lee 誤り以下の誤りを訂正する符号について検討し、その一般的な構成法をこれまで提示してきた。そして、その応用の場として、大容量の基幹通信回線としてよく利用されてきた地上のディジタルマイクロ波無線 (Digital Microwave Radio(DMR) 通信システムへの効率的な適用を提示し、現実の符号系として開発してきた [30]-[36]。また他機関での DMR の研究開発にも利用されてきた [37]。その後、これらの研究に触発されて、金子ら [27][28] も、Lee 距離符号の一般化への検討を進めている。また、理論研究としては、環 Z_q上の Hamming 距離に基づく巡回符号の構成法と復号法という Shankar[11] の流れを汲む研究も依然として理論的整備の観点から続いている [14]。更に、A.R.Hammons ら [13] によって環 Z_4の上の線形符号と有限体上の従来の非線形符号との関係が明らかにされている。一方、大容量の基幹通信回線に応用する符号として、その後従来の BCH 符号、畳み込み自己直交符号あるいは Reed Solomon 符号などを一定の条件下に利用した研究開発も報告されている [41]-[45]。

本研究の第 1 の目的は、上記整数剰余環 Z_q上の符号について、筆者がこれまで検討して得られた理論的成果に関し、整理し纏めて提示することにある。つまり、有限体に限らず、有限

環の上でも実用的でかつメリットのある符号を構成できることを示すことにある。本論文では、まず符号構成上の観点から、整数剰余環 Z_q 上の線形フィードバックシフトレジスタの性質について考察する。これは、有限体上の巡回符号が有限体上の線形フィードバックシフトレジスタと密接に関連して構成されていることに着目し、その類似的な構成法がどこまで通じるかを確かめるためである。ついで、そこで導かれた有用な結果をもとに巡回符号の概念を拡張した形で環 Z_q 上の Lee 距離に基づく誤り訂正符号を導く。すなわち、1 重 Lee 誤り訂正符号、準 2 重 Lee 誤り訂正符号[1]、および 2 重 Lee 誤り訂正符号をそれぞれ導き、各々について、その構成法並びに復号法を与える。更にはその一般化への試みと展望について記す。

本研究の第 2 の目的は、得られた環 Z_q 上の符号を具体的にインプリメントするための手法について明らかにすることである。環 Z_q 上の線形フィードバックシフトレジスタの性質についての考察と符号の構成法から、符号のインプリメンテーションについては、環 Z_q 上の線形フィードバックシフトレジスタを用いた手法が自然な形で導ける。その実現法を明らかにするために、BCH 符号等の有限体上の符号のインプリメンテーションとの違いに重点を置いて説明する。また高速化の観点からその並列処理法についても論ずる。更に、実用に供した符号器・復号器の LSI 開発例 [35] を紹介する。

本研究の第 3 の目的は、得られた環 Z_q 上の符号を現実の通信システム、具体的には大容量のデジタルマイクロ波無線（DMR) 通信基幹回線へ応用する技術を明らかにすることである。80 年代初頭、周波数有効利用の観点から高密度化の進む DMR 通信の世界では、その特性改善のために、変復調技術を含め何がしかの抜本的対策が望まれていた。このような中で、本論文で導かれた Lee 距離に基づく誤り訂正符号が、DMR 通信の世界に始めて導入され、高密度 DMR 通信の信頼性の向上に寄与した [31][33][36]。特に 80 年代初めの DMR 通信において、

[1] 1 重 Lee 誤りのすべてと 2 重 Lee 誤りの殆どすべてを訂正する符号

多値化が16値QAM（Quadrature Amplitude Modulation）から64値QAMとなる段階では、所要C/Nの改善と変復調回路（主にアナログ回路）の不完全性を補償する目的で、これらの研究成果としての誤り訂正符号技術は、スペースダイバーシティ技術と並んでDMR通信にとって極めて重要な不可欠の技術となった[33]。DMR通信の世界へ誤り訂正符号を導入するにあたっては、変調系との親和性を保って、符号の持つ能力を最大限発揮させる必要から、従来符号をそのまま直接的に用いることには問題があった。高密度DMRでの信号の変調方式としては、高密度の点から通常、多値QAM方式が用いられるが、この方式に誤り訂正符号を導入するには、差動符号化と誤り訂正との位置づけ、符号ビットの割り当て、システム構成、更には、電力有効利用の観点から、信号点配置を原点の周りに円形上に取ったときの誤り訂正符号の巧妙な構成法といった様々な手法を導く必要があった。本論文では、これらの課題についての解決策を明らかにすると共に、符号によって改善された通信系の良好な特性についての評価も記す。

本論文では更に、本研究で得られた符号とその応用に関連した結論と、最近の動向を踏まえた今後の展望についての考察を述べる。

1.2 本論文の構成

第2章では、整数剰余環Z_q上のLee距離に基づく誤り訂正符号 について、符号の定義、環Z_q上のフィードバックシフトレジスタの性質、整数剰余環の拡大とその表現法、1重Lee誤り訂正符号、準2重Lee誤り訂正符号、2重Lee誤り訂正符号の各構成法と復号法、符号構成の一般化への試みと展望等について述べる。

第3章では、整数剰余環Z_q上の誤り訂正符号をインプリメントするための手法について述べる。すなわち、1重Lee誤り訂正符号、準2重Lee誤り訂正符号、2重Lee誤り訂正符号

の各符号器・復号器の構成、符号化／復号処理の並列化、開発した２重 Lee 誤り訂正符号の LSI 等について述べる。

第４章では、整数剰余環 Z_q上の誤り訂正符号のデジタル通信系への応用について、高密度デジタル通信系への誤り訂正符号の導入と課題について述べたあと、差動符号化多値直交振幅変調系に Lee 距離に基づく誤り訂正符号を導入することを提案し解析する。

最後に第５章で、結論と今後の展望について述べる。

第2章　整数剰余環Z_q上のLee距離に基づく誤り訂正符号

2.1　整数剰余環 Z_q上のLee距離に基づく線形符号　－定義－

本節では、整数剰余環 $Z_q = Z/(qZ)$ の上のLee距離に基づく線形符号 [3] を定義する。整数剰余環 Z_qは、簡単に言えば、整数間に自然数 $q(\geq 2)$ を法とした演算 $(\mathrm{mod}\ q)$ が定義された集合である。

定義 2.1 整数剰余環 Z_q の任意の2元 c, c'に対して、距離 $d_L(c, c')$ を次式で定義する。

$$d_L(c, c') = \min\{ c - c', c' - c \pmod q \} \tag{2.1}$$

ここに，右辺のminは，Z_q上の減算 $c - c'$ および $c' - c \pmod q$ のそれぞれの結果 r を Z_qの元として、$0 \leq r \leq q-1$ の値で表現したとき、小さい方の値を選ぶ操作を意味する。

ここで定義した距離を、整数剰余環 Z_q におけるLee距離とよぶ。 □

例 2.1 環 Z_8の2元2,7に関し、$d_L(2,7) = \min\{2-7, 7-2\} = \min\{3,5\} = 3$ □

このLee距離に基づいて，整数剰余環 Z_q 上の n 次元ベクトル[2]間のLee距離並びに線形符号を以下のように定義する。

[2]一般に環 R の要素の n 字組 $x = (x_1, x_2, \cdots, x_n) \in R^n$に関して、それらの和やスカラー倍が自然に定義されるが、R が体でなければ集合 R^n はベクトル空間をなさない。しかし、それはベクトル空間と類似の性質をもつので、本論文では R^nの要素を“R 上の n 次元ベクトル”とよび，R の要素からなる行列との積によって“線形写像”を表現することにする。

定義 2.2 整数剰余環 Z_q 上の n 次元ベクトル$\boldsymbol{c} = (c_1, c_2, \cdots, c_n)$ と $\boldsymbol{c}' = (c_1', c_2', \cdots, c_n')$ の間のLee距離 $d_L(\boldsymbol{c}, \boldsymbol{c}')$ を各要素間のLee距離の和として、

$$d_L(\boldsymbol{c}, \boldsymbol{c}') = \sum_{i=1}^{n} d_L(c_i, c_i') \tag{2.2}$$

によって定義する。 □

例 2.2 環 Z_8上の3次元ベクトル$\boldsymbol{c} = (1,2,7)$, $\boldsymbol{c}' = (7,5,6)$ に関し、

$$d_L(\boldsymbol{c}, \boldsymbol{c}') = d_L(1,7) + d_L(2,5) + d_L(7,6) = 2+3+1 = 6$$ □

定義 2.3 送信符号語$\boldsymbol{c}$と受信符号語$\boldsymbol{c}^*$との間のLee距離 $d_L(\boldsymbol{c}, \boldsymbol{c}^*)$ が t であるとき，$\boldsymbol{c}^*$には“t重Lee誤りが生じている”という。有限体上の線形符号と同様に，有限環 Z_q 上の線形符号$\boldsymbol{C}$を、次式によって定義する。

$$\boldsymbol{C} = \{\boldsymbol{c}\,;\quad \boldsymbol{c}H = 0 \pmod q\} \tag{2.3}$$

符号語長 N，情報ディジット数 K の符号を (N,K) 符号とよぶ。(N,K) 符号$\boldsymbol{C}$を定義するためのチェック行列 H は N 行 $N-K$ 列の行列である。符号 $\boldsymbol{C}$ の任意の符号語 $\boldsymbol{c} \in \boldsymbol{C}$ に関し、任意の t 重 以下のLee誤りが訂正可能なとき，符号 $\boldsymbol{C}$ は t 重Lee誤り訂正符号であるという。 □

2.2 整数剰余環 Z_q上の線形フィードバックシフトレジスタの性質

本節では、2.1 節で定義された有限環 Z_q上の誤り訂正符号を構成する準備として有限環 Z_q 上の線形フィードバックシフトレジスタ（Linear Feedback Shift Register ; 以後 LFSR と略す）の性質を明らかにする。LFSR の出力系列とも見なせる線形再帰系列に関しては、その極めて一般的な周期性などの性質を調べる理論研究 [6] が古くから行われてはいたが、符号構成論的な工学的観点からの LFSR についての研究は 50 年代にはいってからであると考えられる [24][2]。その後 LFSR は誤り訂正符号その他に種々の工学的応用を持つことになるが、その際考察の対象とされてきたものは、一般には有限体 $GF(q)$ の上の LFSR であり、整数剰余環 Z_qの上の LFSR に関する研究は、q が素数 p の場合（即ち、Z_qが有限体となる場合）を除き、70 年代にはいるまではあまり見当たらなかったように思われる。本節で紹介する筆者の研究 [17]-[20] が始まったのも 70 年代であるが、そこでは符号の構成・解析という観点から Z_q 上の LFSR のフィードバック結線を基本的なものに限り、その上で LFSR の性質をより具体的な形で明らかにし提示している。なお、Z_qの上の LFSR について論じることは、結局のところ、次節で示す有限環 Z_q の拡大環（Extension Ring）の具体的な構造あるいは性質を論じることにつながり、更には、その構造から誤り訂正符号の構成を考察することに、そして第 3 章で見るように、より直接的に具体的な符号器、復号器を構成する際の手段を考察することにつながる。

図 2.1 に Z_q（$q = p^m$; pは素数）の上の LFSR（以後 LFSR(Z_q) と略す）を示す。LFSR(Z_q) としては、他のタイプも考えられるが、結局の所図 2.1 のタイプを基本とする話に還元できるので、ここでは図 2.1 のタイプに限って話を進める。図 2.1 において、LFSR のフィードバック結線を決める特性多項式が次のように定義される。

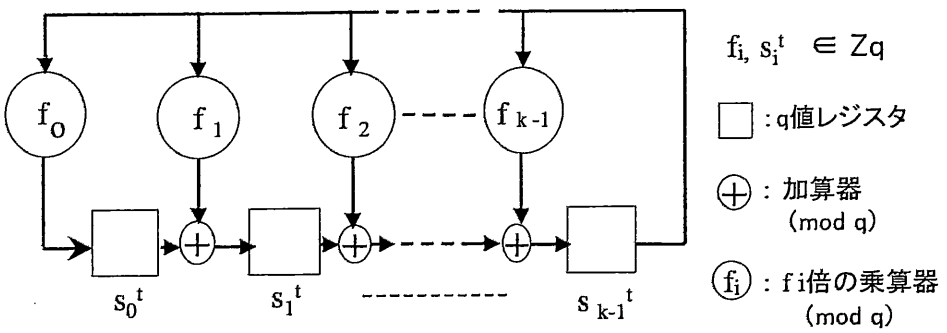

図 2.1: 環 Z_qの上の線形フィードバックシフトレジスタ（LFSR)

定義 2.4 図2.1において, 特性多項式 $f(x)$ 並びに縮約特性多項式 ${}_rf(x)$ を次のように定義する。

$$f(x) = x^k - f_{k-1}x^{k-1} - \cdots - f_1 x - f_0 \tag{2.4}$$

$${}_rf(x) = x^k - {}_rf_{k-1}x^{k-1} - \cdots - {}_rf_1 x - {}_rf_0 \tag{2.5}$$

但し、

$${}_rf_i = f_i \pmod{r;\ r = p^l \quad (1 \le l \le m)} \tag{2.6}$$

$$0 \le {}_rf_i < r \quad (i = 0, 1, \cdots, k-1) \tag{2.7}$$

□

2.2.1 状態ベクトル（列）の分類

まず、図 2.1 で示した時刻 t での状態ベクトル S^tを、レベルという概念で分類する。

定義 2.5 LFSR (Z_q) の状態ベクトル $S^t = (s_0^t, s_1^t, \cdots, s_{k-1}^t)$ がレベル $j(0 \le j \le m-1)$ にあるとは、次のことを言う。即ち、任意の $i(0 \le i \le k-1)$ に対し s_i^tが p^jで割り切れ、かつ少なくとも一つの i に対し s_i^tが p^{j+1}で割り切れないことである。また便宜上、零ベクトルはレベル m にあると定義する。 □

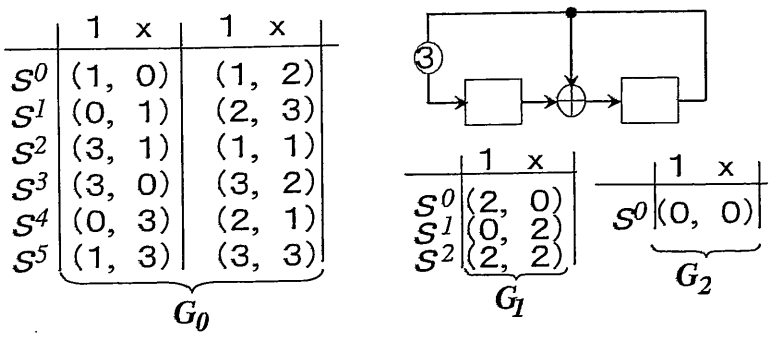

図 2.2: Z_4上の LFSR の一例とその状態ベクトル列

例 2.3 図2.2に Z_4上の LFSR の一例とその状態ベクトル列を示す。図の LFSR の特性多項式は $f(x) = x^2 - x - 3$ で、また $q = 4 = 2^2$より $m = 2$ である。図から分かるように、集合 G_jに属する状態ベクトルはすべてレベル j にあることに注意。 □

次に、状態ベクトル列 $\{S^t\}$ もレベルという概念で分類する。そのために、まず次の性質 2.1 および性質 2.2 を導いておこう。

性質 2.1 LFSR (Z_q) の任意の状態ベクトル列 $\{S^t\}$ が周期系列となるための必要十分条件は、${}_pf_0 \neq 0$が成立することである。 □

(証明) LFSR の状態ベクトル列が周期系列になるということは、その系列の任意の状態ベクトルから出発して有限クロックの間に最初の状態ベクトルに必ず戻る系列になっているということである。これは、状態ベクトルの数が有限である事、任意の状態ベクトル S^tから S^{t+1}は一意に決まる事、逆に任意の状態ベクトル S^{t+1} から S^tが一意に決まるためには${}_pf_0 \neq 0$ となることが条件になる事から成立する。 □

性質 2.2 LFSR (Z_q) において、${}_pf_0 \neq \bar{0}$が成立するならば、各状態ベクトル列 $\{S^t\}$ は、それぞれ、すべて同一のレベルにある状態ベクトルから成る。 □

（証明）S^tがレベル j にあるとし、その要素 s_{k-1}^tが p^{j+1}で割り切れる場合と、そうでない場合に分けて考える。s_{k-1}^tが p^{j+1}で割り切れる場合、次のクロックで状態ベクトルのレベルが変わらないことは明らかである。s_{k-1}^tが p^{j+1}で割り切れない場合、${}_pf_0 \neq 0$ の条件を用いれば、s_0^{t+1}も p^{j+1}で割り切れない。そのため、この場合も次のクロックで状態ベクトルのレベルが変わらないことが分かる。つまり S^tと S^{t+1}とは同一のレベルにある。よって状態ベクトル列 $\{S^t\}$ は、すべて同一のレベルにある状態ベクトルから成る。 □

以後特に断らない限り ${}_pf_0 \neq 0$ とする。

定義 2.6 状態ベクトル列 $\{S^t\}$ がレベル j にあるとは、$\{S^t\}$ に属する任意の状態ベクトルがレベル j にあることをいう。 □

次に、LFSR(Z_q) と LFSR(Z_r) (但し、$q = p^m$, $r = p^{m-i}$) との関係について述べる。これは、mod p^m の演算と mod p^{m-i} の演算の関係に留意すれば容易に導ける。

性質 2.3 LFSR (Z_q) ($q = p^m$) の状態ベクトル列 $\{S^t\}$ がレベル j ($i \leq j \leq m$) にあるならば、系列 $\{p^{-i}S^t\}$ は${}_rf(x)$ (但し、$r = p^{m-i}$) を特性多項式とする LFSR(Z_r) のレベル $(j-i)$ にある系列である。また、その逆も成り立つ。 □

2.2.2 状態ベクトル列（または特性多項式）の周期

本節以降では話を簡明にするため、またあとの基本的な符号構成の話につなげる観点から、LFSR(Z_q) の縮約特性多項式 ${}_pf(x)$ (p は素数) は、環 Z_p上の、従って有限体 $GF(p)$ 上の既約多項式であるものとして話しを進める。このとき、${}_pf(x)$ の（最小）周期を $M({}_pf)$ とすれば、$M({}_pf)$ の値は $p^k - 1$ またはその約数に等しいことはよく知られている [2]。

まず、状態ベクトル列の周期に関しそのレベルとの関係について見ていこう。

性質 2.4 LFSR (Z_q) において、2つの相異なる状態ベクトル列が同一のレベルにあるな

らば、両系列は同一の周期を持つ。但し、逆は一般に成立しない。 □

（証明）２つの相異なる状態ベクトル列を U^t、S^tとする。このとき、$U^0 = (1,0,\cdots,0)$, $S^0 = (s_0^0, s_1^0, \cdots, s_{k-1}^0)$ とし、S^0はレベル０にある任意の状態ベクトルとしても一般性は失われない（性質 2.3 参照）。次に式 (2.6)、(2.7) の場合と同様の意味で、記号${}_rU^t$, ${}_rS^t$, ${}_rs_i^t$ を定義し、証明は帰納法を用いて行う。まず系列 $\{{}_pU^t\}$, $\{{}_pS^t\}$ の周期が共に $\mathrm{M}({}_pf)$ に等しいことは明らか。次に、$1 \le l \le m-1$ として、系列 $\{{}_{p^l}U^t\}$, $\{{}_{p^l}S^t\}$ の周期が相等しいものとする。その周期を N_lとしたとき、系列 $\{{}_{p^{l+1}}U^{N_l}\}$ と $\{{}_{p^{l+1}}S^{N_l}\}$ は次のように表すことができる。

$$ {}_{p^{l+1}}U^{N_l} = (1,0,\cdots,0) + (\eta_0^0, \eta_1^0, \cdots, \eta_{k-1}^0) \tag{2.8} $$

$$ {}_{p^{l+1}}S^{N_l} = ({}_{p^{l+1}}s_0^0, {}_{p^{l+1}}s_1^0, \cdots, {}_{p^{l+1}}s_{k-1}^0) + \sum_{i=0}^{k-1} s_i^0 \eta^i \tag{2.9} $$

但し、η_i^0 は０または p^l の倍数 ($< p^{l+1}$) となるある整数であって、系列 $\{\ \eta^i\ \}$ は $\eta^0 = (\eta_0^0, \eta_1^0, \cdots, \eta_{k-1}^0)$ を初期状態とする系列である。

式 (2.8), (2.9) より、$\eta^0 = \mathbf{0}$ならば、系列 $\{{}_{p^{l+1}}U^t\}$ と $\{{}_{p^{l+1}}S^t\}$ の周期は共に N_lに等しい。また$\eta^0 \neq \mathbf{0}$ならば、系列 $\{{}_{p^{l+1}}U^t\}$ の周期が pN_lとなることは明らかである。また、${}_pf(x)$ が Z_p上の既約多項式であることから、$\eta^i\ (i = 0,1,\cdots,(k-1))$ の各要素をすべて p^lで割った要素からなる k 個のベクトルは、Z_p上で、従って $GF(p)$ 上で互いに線形独立であること、および $s_i^0\ (i = 0,1,\cdots,(k-1))$ の中の少なくとも一つが p で割り切れないことから$\sum_{i=0}^{k-1} s_i^0 \eta^i$が零ベクトル (レベル p^{l+1}以上のベクトル) になり得ないことも導ける。これより、系列 $\{{}_{p^{l+1}}S^t\}$ の周期は、系列 $\{{}_{p^{l+1}}U^t\}$ と同じく pN_lに等しいことが導ける。よって帰納法により、同一レベルにある２つの系列の周期は等しいことが分かる。なお、逆が成立しないことは、例えば図 2.2 の LFSR を Z_8上の LFSR とみなし、その状態ベクトル列の周期を調べると、０レベルの系列も１レベルの系列もその周期が $2N_0 (= 2 * (2^2 - 1) = 6)$ となることから分かる。 □

次に、状態ベクトル列の各レベルに応じた周期を定義する。

定義 2.7 Z_q ($q = p^m$; p は素数) の上の多項式 $f(x)$ を特性多項式とする LFSR (Z_q) において、レベル j にある状態ベクトル列 $\{S^t\}$ の（最小）周期を、LFSR (Z_q) の j レベル（最小）周期あるいは p^{m-j}-ary 周期と定義し、$N(j;{}_qf)$ あるいは略して単に $N(j)$ で表す。 □

なお、$N(j)$ と性質 2.4 の証明中に現われた N_l との関係および 2.2.2 節の冒頭に現れた $M({}_2f)$ との関係は、次式で与えられることに注意。

$$N(j) = N_{m-j} \tag{2.10}$$

$$N(m-1) = M({}_pf) \tag{2.11}$$

性質 2.5 $N(j;{}_qf)$ は、Z_q上の多項式 $f(x)$ で割り切れる多項式 $p^j(x^i-1)$ の次数 i (≥ 1) の中で最小のものに等しい。 □

（証明）$x^i \pmod{f(x)}$ と状態ベクトル S^iとを対応させれば明らか。 □

定義 2.8 $N(j;{}_qf)$ を Z_q 上の多項式 $f(x)$ の j レベル周期あるいは p^{m-j}-*ary* 周期とも呼ぶ。 □

定義 2.9 0 レベル周期（q-ary 周期）$N(0;{}_qf)$ を、単に LFSR(Z_q) の周期、あるいは Z_q上の多項式 $f(x)$ の周期と呼ぶ。 □

j レベル周期 $N(j;{}_qf)$ は更に次のようにも表せる。表現法は異なるが、M.Hall の文献 [6] でも提示されている。

性質 2.6 j レベル周期 $N(j;{}_qf)$ に対して次式が成立する。

$$N(j;{}_qf) = p^{C(j;{}_qf)}M({}_pf) \qquad (0 \leq j \leq m-1) \tag{2.12}$$

$$N(j;{}_qf) = 1 \qquad (j = m) \tag{2.13}$$

但し、$C(j;{}_qf)$ は、$j, q(=p^m)$ 及び $f(x)$ に依存して定まるある整定数で、かつ

$$0 \leq C(j;{}_qf) \leq m-j-1 \tag{2.14}$$

□

（証明）式 (2.8) より、系列 $\{{}_{p^l}U^t\}$ の周期を N_l としたとき、系列 $\{{}_{p^{l+1}}U^t\}$ の周期が N_l 又は pN_l となることが導けるので性質 2.6 は明らか。 □

例 2.4 Z_8 の上の多項式 $f(x)=x^2-x-3$ に対しては、$M({}_2f)=3$, $N(0)=6$, $N(1)=6$, $N(2)=3$, $N(3)=1$ である。 □

特に LFSR(Z_q) あるいは Z_q 上の多項式 $f(x)$ の周期 $N(0)$ に関して言えば、性質 2.6 より、次式が成立する。

$$N(m-1) \leq N(0) \leq p^{m-1}N(m-1) \tag{2.15}$$

$N(m-1)$、つまり p-ary 周期 $M({}_pf)$ は、$f(x)$ が Z_p 上で既約であることから、前述したように、p^k-1 またはその約数に等しい [2]。

また、性質 2.6 より次の定義が可能となる。

定義 2.10 j レベル周期が、任意の $j\,(0 \leq j \leq m-1)$ の値に対し次式で与えられる時、$Z_q\,(q=p^m\,;p$ は素数) の上の多項式 $f(x)$ は、最大周期をもつと定義する。

$$N(j;{}_qf) = p^{m-j-1}M({}_pf) \tag{2.16}$$

また、このとき $f(x)$ は Z_q 上の最大周期多項式であると定義する。 □

容易に分かることであるが、この最大周期多項式はつぎのようにも定義を言いかえることができる。

定義 2.11 Z_q ($q = p^m$; p は素数) 上の多項式 $f(x)$ の周期 $N(0)$ が次式で与えられるとき、$f(x)$ を Z_q 上の最大周期多項式とよぶ。

$$N(0) = p^{m-1}M({}_pf) \tag{2.17}$$

さて、例 2.4 で示した様に、$f(x) = x^2 - x - 3$ は、Z_4 上の最大周期多項式であるが、Z_8 上の最大周期多項式ではない。このことを更に一般的な形でまとめたのが次の性質 2.7 である。

性質 2.7 (A) p を奇素数とした時、Z_{p^2} 上の多項式 $f(x)$ が最大周期多項式ならば、任意の自然数 i に対し、Z_{p^i} の上の多項式とみなした $f(x)$ もまた最大周期多項式である。

(B) Z_{2^3} の上の多項式 $f(x)$ が最大周期多項式ならば、任意の自然数 i に対し、Z_{2^i} の上の多項式とみなした $f(x)$ もまた最大周期多項式である。

(C) Z_{2^3} の上の多項式 $f(x)$ が最大周期多項式となるための必要十分条件は、

$$x^{M({}_2f)} \neq \pm 1 \pmod{{}_4f(x)} \tag{2.18}$$

が成立することである。 □

(証明) (A) 性質 2.4 の証明で用いた記号を使う。条件より、$N_2 = pN_1$ であるから、性質 2.3 および 性質 2.4 より、$N_{l+1} \neq N_l$ (つまり、$N_{l+1} = pN_l$) と仮定した時、$N_{l+2} \neq N_{l+1}$ (つまり、$N_{l+2} = pN_{l+1}$) となる事を、系列 $\{ U^t \}$ についてのみ示せば十分である。

まず、$N_{l+1} = pN_l$ と仮定する。このとき、${}_{p^{l+2}}U^{N_l}$ は、次式のように表せる。

$${}_{p^{l+2}}U^{N_l} = (1, 0, \cdots, 0) + p^l\xi_l \tag{2.19}$$

但し、ξ_l はあるレベル 0 の状態ベクトルである。

また、${\xi_l}^{N_l}$ は、次のように表せる。

$${\xi_l}^{N_l} = \xi_l + p^l\delta_l \tag{2.20}$$

但し、δ_l もあるレベル 0 の状態ベクトルである。

更に、$N_{l+1} = pN_l$ に留意すれば、式 (2.19) と式 (2.20) から、${}_{p^{l+2}}U^{N_{l+1}}$ が次式のように表せることも導ける。

$$ {}_{p^{l+2}}U^{N_{l+1}} = (1,0,\cdots,0) + p(p^l\xi_l) + \frac{p(p-1)}{2}(p^{2l}\delta_l) \tag{2.21} $$

ここで p が奇素数であることから、$\frac{p(p-1)}{2}$ が p の倍数であることに留意すれば、式 (2.21) において $\frac{p(p-1)}{2}(p^{2l}\delta_l)$ はレベル $2l+1$ の状態ベクトルとなる。$l \geq 1$ のとき、$2l+1 \geq l+2$ となるので、$Z_{p^{l+2}}$ においてはこれは 0 ベクトルとなる。一方、$p(p^l\xi_l)$ はレベル $(l+1)$ にあるため、$Z_{p^{l+2}}$ においては 0 ベクトルではない。従って、$Z_{p^{l+2}}$ 上の式 (2.21) において次式が成り立つ。

$$ p(p^l\xi_l) + \frac{p(p-1)}{2}(p^{2l}\delta_l) \neq 0 \tag{2.22} $$

よって、$N_{l+2} \neq N_{l+1}$ となるため、題意が成立する。

(B)　条件より、$p=2$ で、$N_3 = 2N_2 = 4N_1$ である。従って、$p=2\,;\, l \geq 2$ として考えたとき、式 (2.22) が成立すれば、題意が成立することになる。しかるに、$\frac{p(p-1)}{2} = 1$ であり、また $l \geq 2$ のとき $2l \geq l+2$ となるので、式 (2.22) の第 2 項は $Z_{p^{l+2}}$ において 0 ベクトルとなる。第 1 項はレベル $(l+1)$ にあるので 0 ベクトルにはなり得ない。よって式 (2.22) が成立し、題意が成立する。

(C)　Z_{2^3} の上の多項式 $f(x)$ が最大周期多項式であるための条件は、$N_1 \neq N_2$ で、かつ $N_2 \neq N_3$ が成立することである。最初の条件 $N_1 \neq N_2$ は式 (2.18) において $\neq \pm 1$ の個所を $\neq 1$ にした式と等価であるので、第 2 の条件 $N_2 \neq N_3$ について以下に考察する。第 2 の条件は、式 (2.22) において、$p=2\,;\, l=1$ としたときの Z_8 上の次の式と等価である。

$$ 2(2\xi_1) + 2^2\delta_1 \neq 0 \tag{2.23} $$

この式 (2.23) は、Z_2即ち $GF(2)$ 上の次の式と等価である。

$$\xi_1 + \delta_1 \neq 0 \tag{2.24}$$

一方、式 (2.19) と式 (2.20) より、ξ_1 および δ_1 を $GF(2^k)$ の元とみなせば、

$$\xi_1^{N_1} = \xi_1(1 + 2\xi_1) \tag{2.25}$$

$$= \xi_1 + 2\delta_1 \tag{2.26}$$

が成立する。よって、上式より、次式が成立する。

$$\delta_1 = \xi_1 * \xi_1 \ (\text{in GF}(2^k)) \tag{2.27}$$

よって、式 (2.24) より、第 2 の条件 $N_2 \neq N_3$が成立するための条件は、バイナリの状態ベクトルξ_1に対し次式が成立することである。

$$\xi_1 \neq \mathbf{0} \text{ or } \mathbf{1} \ (\text{in GF}(2^k)) \tag{2.28}$$

式 (2.28) を式 (2.19) (但し、$p = 2$; $l = 1$) にあてはめ、$N_1 = M(_2f)$ に留意して考えれば、式 (2.28) が式 (2.18) と等価であることは容易に分かる。以上により、題意が成立する。 □

さて、次に問題となるのは、最大のレベル周期をもつ多項式を直接得るにはどうしたらいいかという問題である。この問に対しては、次の仮説 2.1 が役立つ。

仮説 2.1 Z_pの上で既約な Z_q ($q = p^m$; p は素数) の上の 2 次以上の多項式 $f(x) = x^k - f_{k-1}x^{k-1} - \cdots - f_1x - f_0$ に対し、各係数 f_iが、$0 \leq f_i < p$ を満たすならば、$f(x)$ は Z_q上の最大周期多項式である。 □

例えば，多項式 $x^2 - x - 1$, $x^3 - x - 1$, $x^4 - x - 1$, $x^5 - x^2 - 1$, $x^4 - x^3 - x^2 - x - 1$ などは，任意の m に対して Z_{2^m} 上の最大周期多項式であることが容易に検証できる.

仮説 2.1 は、$GF(p)$ 上のつまり Z_p上の既約多項式表がいくつかの文献 [2],[26] で知られていることから重要な仮説ではあるが、証明は極めて困難で、筆者は未解決問題としても公表 [18][21] している。しかし、未だ解決に至っていない。ただ筆者は、$p=2$ の場合につき、16 次までのすべての既約多項式 $f(x)$ に対し、仮説 2.1 が成立することを、性質 2.7 の (C) を用いて検証済である。また、17 次以上の既約多項式についても未だ反例となるものには出会っていない。この Z_q上の最大周期多項式は、あとで述べる誤り訂正符号を構成する上で重要となる。なお、万一、仮説 2.1 が成立しなくても、次の性質 2.8 を用いれば、Z_q上の最大周期多項式を簡単に求めることができる。

性質 2.8 Z_p上で既約な $Z_q\,(q=p^m)$ 上の多項式 $f(x)=x^k-f_{k-1}x^{k-1}-\cdots-f_1x-f_0$ が最大周期多項式ではないものとする。このとき、ある適当な係数 $f_i\ (0\le i\le(k-1))$ を $f_i+p \pmod q$ に変更することによって、新しい Z_q上の多項式 $f(x)$ が最大周期多項式となるようにすることができる。但し、$k\ge 2$ とする。 □

(証明) 状態ベクトル $U^0=(1,0,\cdots,0)$ として、次式を考える。

$$ {}_{p^2}U^{N_1}=(1,0,\cdots,0)+p\boldsymbol{\xi}_1 \tag{2.29}$$

性質 2.7 より、$f(x)$ が最大周期多項式であるための条件は、p が奇素数のときには、$\boldsymbol{\xi}_1$が $\mathbf{0}=(0,0,\cdots,0)$ に等しくないこと、$p=2$ のときには$\boldsymbol{\xi}_1$ が $\mathbf{0}$ または $\mathbf{1}=(1,0,\cdots,0)$ に等しくないことである。そこで、$f(x)=x^k-f_{k-1}x^{k-1}-\cdots-f_1x-f_0$ の適当な係数 $-f_i$ を $-(f_i+p)$ に変更したとき、上記$\boldsymbol{\xi}_1$にどのような変化が生じるかをみて、$\boldsymbol{\xi}_1$の値を$\mathbf{0}$でも$\mathbf{1}$でもないように制御できるかどうかを調べる。まず係数$-f_0$を$-(f_0+p) \pmod q$ に変更した場合を考える。ここで、

$$U^t=(u_0^t,u_1^t,\cdots,u_{k-1}^t) \tag{2.30}$$

としたとき、係数$-f_0$の変更によってξ_1に付加されるベクトル値は、Z_qの上の多項式 $Q(x) = \sum_{t=0}^{N_1-1} u_{k-1}^t x^{N_1-t-1}$を変更前の特性多項式 $f(x)$ で割ったときの剰余多項式 $R^0(x) = r_0^t + r_1^t x + \cdots + r_{k-1}^t x^{k-1}$について、その係数列からなる剰余ベクトル$\boldsymbol{R}^0 = (r_0^t, r_1^t, \cdots, r_{k-1}^t)$ を p 倍したものであることが導ける。これは図 2.1 が多項式 $f(x)$ による割算回路 [2] であること、$(1, 0, \cdots, 0)$ を初期状態として N_1 クロック回路を動かすことは、x^{N_1} を $f(x)$ で割ることに相当し、その商 $Q(x)$ が右端のレジスタに高次の係数順にでてくること、右端のレジスタに非零の値 u_{k-1}^t が現れたとき、次のクロックで、左端のレジスタに pu_{k-1}^t の値が付加され、最終的に u_{k-1}^t に関し、$pu_{k-1}^t x^{N_1-t-1} \pmod{f(x)}$ の値となって付加されることに留意すれば理解できる。しかも Z_p つまり $GF(p)$ の上で、

$$x^{N_1} - 1 = {}_p f(x) Q(x) \tag{2.31}$$

となり、左辺が $GF(p^k)$ において重根を持たないことに留意すれば、Z_pの上で $Q(x)$ は $f(x)$ で割りきれない。従って、上記剰余ベクトル$\boldsymbol{R}$は Z_pの上で 0 にならない。つまり、式 (2.29) において、ξ_1に非零のベクトルが付加されることになる。

また、一般に係数$-f_i$を$-(f_i + p)$ に変更した場合には、$\boldsymbol{R}^0$を Z_q上の初期状態ベクトルとしてさらに i クロック動かして得られる状態ベクトル$\boldsymbol{R}^i$を p 倍したものが付加される。k 個の状態ベクトル$\boldsymbol{R}^i$ $(0 \leq i \leq k-1)$ は $f(x)$ が Z_p上で既約であることから、Z_p上で考えれば互いに独立なベクトルであり相異なる。よって、ある適当な係数 f_i $(0 \leq i \leq (k-1))$ を $f_i + p \pmod{q}$ に変更することによって、式 (2.29) におけるξ_1の値を**0**でも**1**でもないように制御できることから、新しい Z_q上の多項式 $f(x)$ が最大周期多項式となるようにすることができる。 □

2.2.3 状態ベクトル列の総数

状態ベクトルの総数を各レベルについて求め、それを各レベル周期で割り、更にその総和を求めれば、次の性質 2.9 が導ける。

性質 2.9 Z_q $(q = p^m)$ の上の k 次の多項式 $f(x)$ が、最大周期多項式であるとき、各レベル j の状態ベクトル列の総数$\omega(j)$ および、すべての相異なる状態ベクトル列の総数 W は、次式で与えられる。

$$\omega(j) = p^{(m-j-1)(k-1)}(p^k - 1)/M(_pf) \tag{2.32}$$

$$W = \{(p^{m(k-1)} - 1)/(p^{k-1} - 1)\}\{(p^k - 1)/M(_pf)\} + 1 \tag{2.33}$$

但し、

$$0 \leq j \leq m-1 \quad ; \qquad k \geq 2 \tag{2.34}$$

なお、ここでは、互いにシフトした関係にある状態ベクトル列は、皆同一の系列とみなして数え上げてある。 □

2.2.4 状態ベクトル (列) 間の関係、構造

あとの節で述べる符号の構成に有用な、いくつかの状態ベクトル列間の関係を、次の性質 2.10 にまとめる。

性質 2.10 (A) LFSR (Z_{2^m}) の上の特性多項式 $f(x)$ が最大周期多項式ならば、$m \geq 3$ のとき、レベルが $(m-2)$ 以下にある状態ベクトル列 $\{S^t\}$ と $\{-S^t\}$ は相異なる系列であり、単にシフトした関係にはない。また、$m = 2$ のときには、次式が成り立てば、レベル 0 の系列 $\{S^t\}$ と $\{-S^t\}$ は相異なる系列であり、単にシフトした関係にはない。

$$x^{N(1)} \neq -1 \pmod{f(x)} \tag{2.35}$$

(B) LFSR (Z_{p^m}) (p は奇素数) の縮約特性多項式${}_pf(x)$ が、Z_pつまり $GF(p)$ 上の既約多項式であるならば、状態ベクトル列 $\{S^t\}$ と $\{-S^t\}$ は単にシフトした関係にある同一の系列である。

(C) LFSR (Z_{p^m}) の特性多項式 $f(x)$ は最大周期多項式であるとする。このとき $m \geq 2$ として、レベル j が $(m-2)$ 以下の状態ベクトル列 $\{S^t\} = \{(s_0^t, s_1^t, \cdots, s_{k-1}^t)\}$ に対し、間隔 u でサンプリングして得られる系列 $\{S^{ut}\}$ は、間隔 u をどのように選んでも、系列 $\{ S^t \}$ とは相異なる系列で、単にシフトしたり、あるいは、定数 $(\in Z_{p^m})$ 倍した関係にある系列ではない。但し、$1 < u < N(j)$ □

(証明) (A) 系列 $\{S^t\}$ と $\{-S^t\}$ とが単にシフトした関係にある同じ系列であるとすると矛盾することを導く。$S^0 = (1, 0, \cdots, 0)$ と仮定して証明すれば十分である。S^0から出発して $(-1, 0, \cdots, 0)$ が現れるまでのクロック数の 2 倍のクロック数で S^0に戻ることに留意すれば、まず Z_{2^m}の上で次式が成立する。

$$S^{N(1)} = (-1, 0, \cdots, 0) \tag{2.36}$$

但し、

$$N(1) = 2^{m-2} M({}_2f) \tag{2.37}$$

ここで、$M({}_2f)$ は${}_2f(x)$ の周期を表す。

更に Z_2^mの上の多項式 $f(x)$ が最大周期多項式であることより、$Z_{2^{m-1}}$の上で次式が成立する。

$$S^{N(1)} = (1, 0, \cdots, 0) \tag{2.38}$$

式 (2.36) と式 (2.38) とは、$m \geq 3$ のとき明らかに両立しない。また、$m = 2$ のとき、式 (2.35) が成りたてば、これは、式 (2.36) に矛盾する。よって題意のとおりである。

(B) まず Z_pつまり $GF(p)$ 上での${}_pf(x)$ の周期 $M({}_pf) = N(m-1)$ に対し、Z_p上で次式が成り立つことは明らかである。但し、(A) での証明と同様、$S^0 = (1,0,\cdots,0)$ と仮定する。

$$S^{N(m-1)/2} = (-1,0,\cdots,0) + pV_1(x) \tag{2.39}$$

但し、$V_1(x)$ はある高々$k-1$ 次の多項式である。

次に、帰納的に次式を導く。但し、$V_j(x)$ もある高々$k-1$ 次の多項式である。

$$S^{N(m-j)/2} = (-1,0,\cdots,0) + p^jV_j(x) \tag{2.40}$$

式 (2.40) は、次式 (2.41) が成立することを念頭に置き、そのためには式 (2.40) において、$p > 2$ より、$V_j(x)$ に p^{j-1}でなく p^jがかかる必要があることを認識すれば容易に導ける。

$$S^{N(m-j)} = (1,0,\cdots,0) + p^jV_j(x) \tag{2.41}$$

よって、式 (2.40) において、$j = m$ と置けば、Z_{p^m}において、

$$S^{N(0)/2} = (-1,0,\cdots,0) \tag{2.42}$$

と表せる。このことから題意が成立する。 □

(C) $f(x)$ が Z_q上の最大周期多項式であることから、その j レベル周期 $N(j)$ は、式 (2.16) より $p^{m-j-1}M({}_pf)$ で与えられる。$j \leq m-2$ ならば $m-j-1 \geq 1$ である。一方、系列 $\{S^{ut}\}$ と $\{S^t\}$ とを Z_pにおいて考えたとき、両系列が単にシフトした関係あるいは定数 $(\in Z_p)$ 倍にある同じ系列であるための条件は、u が p を含め p のべき乗倍であることである [24]。従って、Z_{p^m}の上で考えた場合でも、同じ条件は必要である。しかるに $N(j)$ は p の倍数であるから、u が p を含め p のべき乗倍であれば、Z_{p^m}の上の系列 $\{S^{ut}\}$ の周期は $\{S^t\}$ の周期より短くなり、両者は同じ系列とはなりえない。よって題意のとおりである。 □

次に、状態ベクトルに対応する状態多項式を定義した後、状態多項式間に演算を導入し、状態ベクトルの集合がもつ構造について記す。

定義 2.12 LFSR (Z_q) において j レベルにある状態ベクトル $S = (s_0, s_1, \cdots, s_{k-1})$ に対し、多項式 $S(x) = \sum_{i=0}^{k-1} s_i x^i$ を対応づけ、$S(x)$ をその LFSR (Z_q) の j レベルにある状態多項式と呼ぶ。 □

性質 2.11 (A) $f(x)$ を特性多項式とする LFSR (Z_q) において、$S_i(x)$ $(i = 1, 2, \cdots, u)$ をレベル j_iにある Z_q $(q = p^m)$ の上の状態多項式とする。このとき$\Pi_{i=1}^{u} S_i(x) \equiv 0 \pmod{f(x)}$ が成立するのは、$\sum_{i=1}^{u} j_i \geq m$ のとき、その時に限る。また$\sum_{i=1}^{u} j_i < m$ ならば、$\sum_{i=1}^{u} j_i$ は状態多項式$\Pi_{i=1}^{u} S_i(x) \pmod{f(x)}$ のレベルに等しい。

(B) LFSR (Z_q) において、G_jをレベル j にある状態多項式 $S_i(x)$（これを、$p^j \tilde{S}_i(x)$ と表す。）の全集合とする。このとき、$\tilde{G}_j = \{\tilde{S}_i(x)\}$ は$_{p^{m-j}} f(x)$ を特性多項式とする LFSR$(Z_{p^{m-j}})$ のレベル 0 の状態多項式の全集合に等しい。また$\tilde{G}_j$は mod $_{p^{m-j}} f(x)$ の演算のもとに可換な乗法群を構成する。

(C) 状態ベクトル列 $\{S^t\}$ はレベル j にあるとする。このとき、次式が成立する。

$$\sum_{t=0}^{N(j)-1} S^t(x) \equiv 0 \pmod{f(x)} \tag{2.43}$$

□

（証明）(A) はほぼ自明なので、以下 (B)、(C) について証明する。

(B) $\tilde{G}_j$に定義された演算mod $_{p^{m-j}} f(x)$ のもとに、$\tilde{G}_j$の任意の状態多項式 $A(x)$ の逆元が確かに一意に求められることを言えば十分である (単位元はもちろん 1 である)。そのためにまず、$A(x)$ を次のように表す。

$$A(x) = A_0(x) + pA_1(x) + p^2 A_2(x) + \cdots p^{m-j-1} A_{m-j-1}(x) \tag{2.44}$$

$A(x)$ に対する逆元を $B(x)$ とし、$A(x)$ と同様、次のように表す。

$$B(x) = B_0(x) + pB_1(x) + p^2 B_2(x) + \cdots p^{m-j-1} B_{m-j-1}(x) \tag{2.45}$$

まず Z_p上の $k-1$ 次以下の多項式 $B_0(x)$ であるが、これは、$GF(p^k)$ の元とみなした $A_0(x)$ の逆元として一意に求まる。ついで、$B_1(x)$ は、$A(x) * B(x) \pmod{p^{m-j} f(x)}$ において、p の係数多項式が 0 となるように定めればよい。即ち、$A_0(x), A_1(x), B_0(x)$ が与えられたとして、$GF(p^k)$ における式 $A_0(x) * B_1(x) + A_1(x) * B_0(x) = 0$ より一意に求まる。同様にして、$p^2, p^3, \cdots, p^{m-j-1}$のそれぞれの係数多項式が $GF(p^k)$ において 0 となるように、$B_2(x), B_3(x), \cdots B_{m-j-1}(x)$ を順に定めていけばよい。よって、任意の状態多項式 $A(x)$ の逆元が確かに一意に求められる。従って、$\tilde{G}_j$ は $\bmod p^{m-j} f(x)$ の演算のもとに可換な乗法群を構成することが分かる。

(C) まず、$S^t(x) = p^j \tilde{S}^t(x)$ とする。$\tilde{S}^0(x) = 1$ として考えて題意が成立すれば、任意の $S^0(x)$ に対しても成立することは明らかなので、以下$\tilde{S}^0(x) = 1$ に限って考える。このとき、次式が成り立つ。

$$S^{N(j)}(x) - 1 = p^j (\tilde{S}^1(x) - 1)\left(\sum_{t=0}^{N(j)-1} \tilde{S}^t(x)\right) \pmod{f(x)} \tag{2.46}$$

式 (2.46) において、左辺は周期 $N(j)$ の定義よりレベル m 以上にある。また $(\tilde{S}^1(x) - 1) = (x-1)$ はレベル 0 にある。従って、$\sum_{t=0}^{N(j)-1} \tilde{S}^t(x) \pmod{f(x)}$ のレベルは $m-j$ 以上となる。しかるに、

$$\sum_{t=0}^{N(j)-1} S^t(x) = p^j \sum_{t=0}^{N(j)-1} \tilde{S}^t(x) \pmod{f(x)} \tag{2.47}$$

であるから、左辺はレベル m 以上となり、題意が成立する。 □

2.3 整数剰余環の拡大とその表現および性質

本節では Z_q の拡大環 $GR(q,k)$ に関するいくつかの性質について考察し整理する。これらの性質は、2.2 節で述べた Z_q の上の Feedback Shift Register の性質 [17]-[20] ないしは、線形再帰系列の性質 [6] と相対応する関係にあるが、Z_q上の符号を構成する観点からはキーとなる概念となる。本節では、符号構成の観点から本質的な事柄を整理し、より具体的に考察して次節につなげる。

定義 2.13 $q = p^m$ (p は素数、m は正の整数) とし、Z_q の上の k 次多項式 $g(x)$ は Z_p の上で既約であるとする。このとき，$g(x)$ を法とする多項式環 $R_q[x]/(g(x))$ を $R_q[g(x)]$ で表わす。また、$R_q[g(x)]$ を Z_q のガロア拡大環 $GR(q,k)$ と同一視して扱う [20][11]。 □

多項式環 $R_q[g(x)]$、あるいは、拡大環 $GR(q,k)$ の各元は，$k-1$ 次以下の多項式で表現することができる。一例として、$g(x) = x^2 - x - 1$ としたときの多項式環 $R_8[g(x)]$（あるいは拡大環 $GR(8,2)$）の元を表 2.1 に示す。

表 2.1: 多項式環 $R_8[x^2 - x - 1]$（拡大環 $GR(8,2)$）の元

i	x^{i-1}	H_u^J / $L_u^J(x)$	H_1^0	H_2^0	H_3^0	H_4^0	H_1^1	H_2^1	H_1^2	H_1^3
			1	1+4x	7	7+4x	2	6	4	0
1	1		1	1+4x	7	7+4x	2	6	4	0
2	x		x	4+5x	7x	4+3x	2x	6x	4x	(G_3)
3	x^2		1+x	5+x	7+7x	3+7x	2+2x	6+6x	4+4x	
4	x^3		1+2x	1+6x	7+6x	7+2x	2+4x	6+4x	(G_2)	
5	x^4		2+3x	6+7x	6+5x	2+x	4+6x	4+2x		
6	x^5		3+5x	7+5x	5+3x	1+3x	6+2x	2+6x		
7	x^6		5	5+4x	3	3+4x	(G_1)			
8	x^7		5x	4+x	3x	4+7x				
9	x^8		5+5x	1+5x	3+3x	7+3x				
10	x^9		5+2x	5+6x	3+6x	3+2x				
11	x^{10}		2+7x	6+3x	6+x	2+5x				
12	x^{11}		7+x	3+x	1+7x	5+7x				
			(G_0)							

表 2.1 において各元は 1 次式、もしくは定数で表わされている。さらに、各元、例えば多項式 $5+x$ は、

$$5+x \;=\; (1+4x)x^2 \pmod{x^2-x-1}$$

という形に表わされる。つまり，表 2.1 において各元は、一般に

$$L_u^j(x)\, x^{i-1} \qquad (\bmod\ x^2-x-1) \tag{2.48}$$

の形に表わすことができる。このことについて次に一般的に説明する。

まず、拡大環 $GR(q,k)$ は明らかに単位元 1 を有する可換環である。そこで、0 を除く $GR(q,k)$ の元の中で、p^j で割り切れかつ p^{j+1} で割り切れない元 $p^j r_i(x)$ の集合を、

$$G_j \;=\; \{\, p^j r_i(x) \,\} \quad (0 \le j \le m-1) \tag{2.49}$$

で表わし、$\tilde{G}_j = \{\, r_i(x) \,\}$ とすると、$\tilde{G}_j$ は $\bmod p^{m-j}$ の演算のもとに可換な乗法群をなすことがいえる。

更に、$\tilde{G}_j$ は $Z_{2^{m-j}}$ の上で、次に示す巡回部分群 $\tilde{H}_1^j$ を有する。

$$\tilde{H}_1^j \;=\; \{\, 1,\, x,\, x^2,\, \cdots,\, x^{N(j)-1} \pmod{g(x)} \,\} \tag{2.50}$$

但し、$N(j)$ は、定義 2.7 で与えた p^{m-j}-ary 周期（j レベル周期）である。

そこで $\tilde{G}_j$ をこの部分群 $\tilde{H}_1^j$ によって剰余類分解してできる各剰余類を $\tilde{H}_u^j$ $(u = 1, 2, \cdots, \omega(j))$ とし、さらに、その剰余類首を $\tilde{L}_u^j(x)$ とすれば，$\tilde{G}_j$ の任意の元は、$Z_{2^{m-j}}$ の上で、

$$\tilde{L}_u^j(x)\, x^{i-1} \quad (\bmod\ g(x)) \quad (1 \le i \le N(j),\ 1 \le u \le \omega(j)) \tag{2.51}$$

の形に表現できるわけである。ここに、$\omega(j)$ は、式 (2.32) で与えられる$\omega(j)$ に等しい。また G_j の元の個数は $w(j)N(j)$ であることにも注意。

なお、H_u^j ; $L_u^j(x)$ を以下のように定め、それぞれを、$GR(q,k)$ の H_1^j による剰余類、および、その剰余類首とよぶことにする。

$$H_u^j = p^j \tilde{H}_u^j \tag{2.52}$$

$$L_u^j(x) = p^j \tilde{L}_u^j(x) \tag{2.53}$$

(但し、$1 \leq u \leq w(j)$)

さて、$j = m$ の場合に関しても、便宜上次の式を定義しておく。

$$G_m = H_u^m = \{0\} \ ; \ N(m) = 1 \ ; \ L_u^m(x) = 0 \ ; \ \omega(m) = 1 \tag{2.54}$$

以上のように定義すれば、$GR(q,k)$ の任意の元は剰余類首 $L_u^j(x)$ を用いて、

$$L_u^j(x)x^{i-1} \pmod{g(x)} \quad (1 \leq i \leq N(j),\ 1 \leq u \leq \omega(j),\ 1 \leq j \leq m) \tag{2.55}$$

の形で表現される。

表 2.1 においては、各列が剰余類 H_u^j を表わしており、2 行目の各多項式がそれぞれの剰余類に対応する剰余類首 $L_u^j(x)$ を示している。従って、$GR(q,k)$ の各元が式 (2.55) の形に表わされることがいえる。

次に、Lee 誤り訂正符号を構成する上で重要となる剰余類 H_u^j の基本的な性質について述べる。ここで述べる性質は、2.2 節の性質 2.10(A),(B) に対応したものであり、剰余類の単なる順序づけ以外は、同じ事を別の形で表現したものであるため証明は不要と考える。

まず，剰余類 H_u^j の各要素を Z_q の上で -1 倍してできる集合を $-H_u^j$ で表わすものとする。

性質 2.12 多項式 $g(x)$ を Z_q ($q = p^m$: p は素数) の上の最大周期多項式とする。

(A) $p = 2$, $m \geq 3$ のとき，H_u^j と $-H_u^j$ $(0 \leq j \leq m-2)$ は相異なる剰余類である。従って、

$$H_{u+\omega(j)/2}^j = -H_u^j \quad (1 \leq u \leq \omega(j)/2) \tag{2.56}$$

となるように，各剰余類 H_u^j を順序づけることができる.

また、$p=2$, $m=2$ のときは、次の式が成立するならば H_u^0 と $-H_u^0$ は相異なる剰余類である。

$$x^{N(1)} \neq -1 \pmod{g(x)} \tag{2.57}$$

従って、このとき、式 (2.56) が成り立つように、各剰余類 H_u^0 を順序づけることができる。

(B) $p \neq 2$ のとき，H_u^j と $-H_u^j$ は同一の剰余類を形成し、次の式が成立する。

$$L_u^j(x)\, x^i = -L_u^j(x) x^{i+N(m-j)/2} \pmod{g(x)} \quad (0 \leq i < N(m-j)/2) \tag{2.58}$$

□

表 2.1 において、各剰余類首は、$L_1^0(x) = 1 = -7 = -L_3^0(x)$; $L_2^0(x) = 1+4x = -(7+4x) = -L_4^0(x)$; $L_1^1(x) = 2 = -6 = L_2^1(x) \pmod 8$ であり、従ってまた、式 (2.56) が成立している。

次の節以降において、Lee 誤り訂正符号のチェック行列 H が剰余類 H_u^j（あるいはその一部分）の組み合わせとして構成されることをみる.

2.4 1重Lee誤りを訂正する符号 C_Iの構成法と復号法

本節では $Z_q(q=p^m;p$ は素数$)$ 上の1重 Lee 誤り訂正符号 C_Iについて、その一般的な構成法と復号法を与える [17][19][20][47]。

なお、$p=2$ の場合と $p\neq 2$ の場合とではその構成法に若干の違いがあるので、それらの構成法は別々に提示する。また、Z_q の上の高々 $k-1$ 次の多項式 $V(x)=v_1+v_2x+\cdots+v_kx^{k-1}$ と k 次元ベクトル $\boldsymbol{v}=(v_1,v_2,\cdots,v_k)$ との間には1対1対応の関係があるので、両者を同一視して話を進める。

2.4.1 符号 C_Iの構成法を導くための準備

本節では簡単な一構成例を示し、次節での一般的な構成手順につなげる。

例 2.5 Z_8 上の符号として、符号語長 $N=30$、情報ディジット数 $K=28$ の1重Lee誤り訂正 (30,28) 符号の構成例を示す。この符号を規定するチェック行列 H は、図 2.3 に示す 30 行 2 列の行列として構成することができる。以下にその理由を示す。

実際、図 2.3 において、行列 H の第 i 行を $H_i=(h_{i_1},h_{i_2})$ とすれば、任意の相異なる i,j に対して、

$$\begin{cases} H_i \neq -H_i \\ H_i \neq \pm H_j \end{cases} \pmod 8 \tag{2.59}$$

が成立している。従って、送信符号語 $\boldsymbol{c}$ の例えば k 番目の位置に、$\pm 1 \pmod 8$ の誤りが生じた符号語 $\boldsymbol{c}^*$ を受信したとすれば ($d_L(\boldsymbol{c},\boldsymbol{c}^*)=1$ であることに注意)、受信側で計算して得られるシンドローム $\boldsymbol{c}^*H$ が $\pm H_k$ であることから直ちに、誤り位置 k, および、誤り値 $+1$ または -1 を知ることができる。つまり、図 2.3 の H は Z_8 上の 1 重 Lee 誤り訂正符号のチェック行列である。 □

$$
H = \left[\begin{array}{cc|l}
1 & 0 & 1 = 1 \\
0 & 1 & x = x \\
1 & 1 & 1 + x = x^2 \\
1 & 2 & 1 + 2x = x^3 \\
2 & 3 & 2 + 3x = x^4 \\
3 & 5 & 3 + 5x = x^5 \\
5 & 0 & 5 = x^6 \\
0 & 5 & 5x = x^7 \\
5 & 5 & 5 + 5x = x^8 \\
5 & 2 & 5 + 2x = x^9 \\
2 & 7 & 2 + 7x = x^{10} \\
7 & 1 & 7 + x = x^{11} \\
\hline
1 & 4 & 1 + 4x = 1 + 4x \\
4 & 5 & 4 + 5x = (1 + 4x)x \\
5 & 1 & 5 + x = (1 + 4x)x^2 \\
1 & 6 & 1 + 6x = (1 + 4x)x^3 \\
6 & 7 & 6 + 7x = (1 + 4x)x^4 \\
7 & 5 & 7 + 5x = (1 + 4x)x^5 \\
5 & 4 & 5 + 4x = (1 + 4x)x^6 \\
4 & 1 & 4 + x = (1 + 4x)x^7 \\
1 & 5 & 1 + 5x = (1 + 4x)x^8 \\
5 & 6 & 5 + 6x = (1 + 4x)x^9 \\
6 & 3 & 6 + 3x = (1 + 4x)x^{10} \\
3 & 1 & 3 + x = (1 + 4x)x^{11} \\
\hline
2 & 0 & 2 = 2 \\
0 & 2 & 2x = 2x \\
2 & 2 & 2 + 2x = 2x^2 \\
2 & 4 & 2 + 4x = 2x^3 \\
4 & 6 & 4 + 6x = 2x^4 \\
6 & 2 & 6 + 2x = 2x^5
\end{array}\right]
\qquad (\mathrm{mod}\ x^2 - x - 1\ \text{over}\ Z_8)
$$

図 2.3: Z_8上の1重Lee誤り訂正 (30,28) 符号のチェック行列 H

図2.3のチェック行列 H の構造について更に述べる。図2.3に示されたように、H は3つのブロックに分けられ、その第 j 行は次のように、Z_2 の上で既約な (Z_8上の) 多項式 $g(x) = x^2 - x - 1$ を法とする Z_8の上の多項式 $J(x)$ (mod $g(x)$) と1対1に対応させることができる。

$$J(x) = \begin{cases} x^{j-1} & (1 \le j \le 12) \\ (1+4x)x^{j-13} & (13 \le j \le 24) \quad (\text{mod } 8) \\ 2x^{j-25} & (25 \le j \le 30) \end{cases} \tag{2.60}$$

そこで、符号語 $\boldsymbol{c}$ を

$$\boldsymbol{c} = (\, c^0_{1\cdot 1},\, c^0_{1\cdot 2},\, \cdots,\, c^0_{1\cdot 12},\, c^0_{2\cdot 1},\, c^0_{2\cdot 2},\, \cdots,\, c^0_{2\cdot 12},\, c^1_{1\cdot 1},\, c^1_{1\cdot 2},\, \cdots,\, c^1_{1\cdot 6}\,) \tag{2.61}$$

とすれば、式 (2.3) の条件は、次に示す多項式 $C(x)$ が $g(x) = x^2 - x - 1$ で割り切れるとき、そのときに限り$\boldsymbol{c}$ は符号語である、と言い換えることもできる。これは符号器ならびに復号器を設計する際に重要な性質となる。

$$C(x) = \sum_{j=0}^{1} \sum_{u=1}^{s(j)} \sum_{i=1}^{N(3-j)} c^j_{u\cdot i}\, L^j_u(x)\, x^{i-1} \tag{2.62}$$

(但し、 $s(0) = 2,\ s(1) = 1,\ N(3) = 12,\ N(2) = 6,\ L^0_1(x) = 1,\ L^0_2(x) = 1 + 4x,\ L^1_1(x) = 2$)

なお、図2.3 のチェック行列 H の構成の仕方から、式 (2.61) において、$c^0_{1\cdot 1}$ および $c^0_{1\cdot 2}$ は冗長ディジットで、他は情報ディジットである。

ここで例示した (30,28) 符号のチェック行列 H は3つのブロックからなり、各ブロックはそれぞれ表2.1における剰余類 H^0_1, H^0_2 および H^1_1 に対応している。表2.1の各類は式 (2.56) が成立するように順序づけられているから、H^0_1, H^0_2 および H^1_1 からなるチェック行列 H に対して式 (2.59) が成り立つことは当然である。従って、H は1重Lee誤り訂正符号のチェック行列であることが確かめられる。

2.4.2 Z_{2^m}上の1重Lee誤り訂正符号 C_Iの構成手順

前節で例示した構成法は直ちに次のように一般化できる。

Step(1) Z_{2^m} の上の k 次の最大周期多項式 $g(x)$ を選ぶ。但し、$m=2$ のときは 式 (2.57) を満たすものとする。

Step(2) 多項式環 $R_{2^m}[g(x)]$、すなわち拡大環 $GR(2^m,k)$ を前節の手法に従って剰余類分解し，各剰余類 H_u^j を 式 (2.56) が成り立つように順序づける。

Step(3) $j=0,1,2,\cdots,m-2$ の各値に対して、剰余類 H_u^j をそれぞれ $s(j)$ 個ずつ選択し、選ばれた剰余類から構成されるチェック行列 H_I を得る。但し、

$$0 \le s(j) \le w(j)/2 \tag{2.63}$$

とし、$L_1^0(x)=1$ を剰余類首とする剰余類 H_1^0 は必ず選ぶものとする。

チェック行列 H_I は（例えば）次のように表現される。式中、T は転置を意味する。

$$H_I = [H_1^0,\ H_2^0,\ \cdots, H_{s(0)}^0,\ H_1^1,\ H_2^1,\ \cdots, H_{s(1)}^1,\ \cdots,\ H_1^{m-2},\ H_2^{m-2},\ \cdots, H_{s(m-2)}^{m-2}\ ]^{\mathrm{T}} \tag{2.64}$$

Step(4) 1重Lee誤り訂正符号 C_I を、式 (2.64) で与えたチェック行列 H_Iに対し、次式を満たす符号語 $\boldsymbol{c}$ の集合 $\{\ \boldsymbol{c}\ \}$ とする。

$$\boldsymbol{c}\,H_I\ =\ 0 \qquad (\mathrm{mod}\ 2^m) \tag{2.65}$$

ここで、符号語 $\boldsymbol{c}$ の冗長ディジット数は 多項式 $g(x)$ の次数 k であり、符号語 $\boldsymbol{c}$ の先頭 の k ディジットを冗長ディジット、他を情報ディジットとみなせば、符号 C_I は組織符号である点に注意。また、符号長 N，および，情報ディジット数 K は次式で与えられることも記しておこう。

$$N=\sum_{j=0}^{m-2} s(j)N(j), \qquad K=N-k \tag{2.66}$$

□

なお、式 (2.64) のチェック行列 H_I が1重Lee誤り訂正符号のチェック行列となることは，性質2.12(A) より明らかであろう。

さてここで、符号語 $\boldsymbol{c}$ をチェック行列 H_Iの表現に合わせて、以下のように表現することにする。

$$\boldsymbol{c} = (c_1^0, c_2^0, \cdots, c_{s(0)}^0, c_1^1, c_2^1, \cdots, c_{s(1)}^1, \cdots, c_1^{m-2}, c_2^{m-2}, \cdots, c_{s(m-2)}^{m-2}) \tag{2.67}$$

但し、$c_u^j = (c_{u\cdot 1}^j, c_{u\cdot 2}^j, \cdots, c_{u\cdot N(j)}^j)$

2.3 節でも例示したように、式 (2.65) が成立することと、符号語 $\boldsymbol{c}$ に対応する次の多項式 $C(x)$ が $g(x)$ で割り切れることとが等価であることは容易に理解できる。

$$C(x) = \sum_{j=0}^{m-2} \sum_{u=1}^{s(j)} \sum_{i=1}^{N(j)} c_{u\cdot i}^j L_u^j(x)\, x^{i-1} \tag{2.68}$$

なお，剰余類首 $L_u^j(x)$、および，$g(x)$ を、それぞれ、符号 C_I の変換多項式，および，生成多項式とよぶことにする。式 (2.68) が生成多項式 $g(x)$ で割り切れるということは、符号多項式 $C(x)$ の集合が $x^{N(m)} - 1$ を法とする多項式環においてイデアルを構成するということである。但し、通常の巡回符号の場合と異なり、イデアルの1つの元 $C(x)$ と、式 (2.65) を満たす符号語 $\boldsymbol{c}$ との対応関係は、一般には1対多対応の関係にあり、符号 C_I は巡回符号ではなく、その変形として理解できる。

ところで、上記の手法において、すべての j の値 $(0 \le j \le m-2)$ に対して、$s(j) = \omega(j)/2$ とすれば、理論的に符号化率 K/N の最も高い1重Lee誤り訂正符号を得ることができる。その際の符号長 N は，$N = 2^{mk-1} - 2^{k-1}$ であり、符号化率 K/N は $K/N = 1 - \dfrac{k}{2^{mk-1} - 2^{k-1}}$ である。

表 2.2 に、$p = 2$ のときの1重Lee誤り訂正符号 C_I のパラメータ例を示す。

表 2.2: Z_4および Z_8 上の1重Lee誤り訂正符号 C_I のパラメータ例

4-ary codes					8-ary codes				
N	K	K/N	g(x)	$L_u^j(x)$	N	K	K/N	g(x)	$L_u^j(x)$
6	4	.667	x^2-x-1	1	12	10	.833	x^2-x-1	1
14	11	.786	x^3-x-1	1	18	16	.889		1,2
28	25	.893		1,1+2x	24	22	.917		1,1+4x
30	26	.867	x^4-x-1	1	30	28	.933		1,1+4x,2
60	56	.933		1,1+2x	28	25	.893	x^3-x-1	1
90	86	.956		$1,1+2x,1+2x^2$	42	39	.929		1,2
120	116	.967		$1,1+2x,1+2x^2,1+2x+2x^2$	56	53	.946		1,3
62	57	.919	x^5-x^2-1	1	70	67	.957		1,3,2
124	119	.960		1,1+2x	84	81	.964		1,3,1+2x
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

2.4.3 $Z_{p^m}(p \neq 2)$ 上の1重Lee誤り訂正符号 C_I の構成手順

前節で導いた性質2.12Bに留意すれば，$p \neq 2$ のときの1重Lee誤り訂正符号は次のようにして構成される。

Step(1) Z_{p^m} の上の k 次の最大周期多項式 $g(x)$ を選ぶ。

Step(2) 多項式環 $R_{p^m}[g(x)]$（拡大環 $GR(p^m,k)$）を前節の手法に従って剰余類分解し，剰余類 H_u^j を得て，さらに各剰余類 H_u^j を次のように2分する．

$$\begin{cases} H_u^j(1) = \{\, L_u^j(x)\, x^i \,;\, 0 \le i \le N(m-j)/2-1\} \\ H_u^j(2) = \{\, L_u^j(x)\, x^i \,;\, N(m-j)/2 \le i \le N(m-j)\} \end{cases} \tag{2.69}$$

Step(3) $j = 0,1,2,\cdots,m-1$ の各値に対して，2分された剰余類 $H_u^j(1)$ をそれぞれ $s(j)$ 個ずつ選択し，選ばれた剰余類 $H_u^j(1)$ から構成されるチェック行列 H を得る。

$$\text{但し、} \qquad 0 \le s(j) \le \omega(j) \tag{2.70}$$

とし、$L_1^0(x) = 1$ を剰余類首とする剰余類 $H_1^0(1)$ は必ず選ばれるものとする。チェック行列 H_I は（例えば）次のように表現される。これは、式(2.64)において、$m-2$ を $m-1$ に変え

た式になっている。

$$H_I = [H_1^0,\ H_2^0,\ \cdots, H_{s(0)}^0,\ H_1^1,\ H_2^1,\ \cdots, H_{s(1)}^1,\ \cdots,\ H_1^{m-1},\ H_2^{m-1},\ \cdots, H_{s(m-1)}^{m-1}\ ]^{\mathrm{T}} \quad (2.71)$$

Step(4) 1重Lee誤り訂正符号 C_I を、式 (2.71) のチェック行列 H_I に対し、次式を満たす符号語 $\boldsymbol{c}$ の集合 $\{\ \boldsymbol{c}\ \}$ とする。

$$\boldsymbol{c}\, H_I\ =\ 0 \qquad (\mathrm{mod}\ p^m) \quad (2.72)$$

ここで、符号語 $\boldsymbol{c}$ の冗長ディジット数は 多項式 $g(x)$ の次数 k であり，符号語 $\boldsymbol{c}$ の先頭 の k ディジットを冗長ディジット、他を情報ディジットとみなせば、符号 C_I は組織符号である。また、符号長 N，および，情報ディジット数 K は次式で与えられる。

$$N = \sum_{j=0}^{m-1} s(j)N(j)/2, \qquad K = N - k \quad (2.73)$$

□

さて、符号語 $\boldsymbol{c}$ および符号多項式 $C(x)$ は、それぞれ式 (2.67) および式 (2.68) において $m-2$ を $m-1$ に，かつ $N(j)$ を $N(j)/2$ に置き換えて得られる次の式で表現される。

$$\boldsymbol{c}\ =\ (c_1^0,\ c_2^0,\ \cdots, c_{s(0)}^0,\ c_1^1,\ c_2^1,\ \cdots, c_{s(1)}^1,\ \cdots,\ c_1^{m-1},\ c_2^{m-1},\ \cdots, c_{s(m-1)}^{m-1}\ ) \quad (2.74)$$

但し、$c_u^j = (\ c_{u\cdot 1}^j,\ c_{u\cdot 2}^j,\ \cdots\ , c_{u\cdot N(j)/2}^j\ )$

$$C(x)\ =\ \sum_{j=0}^{m-1} \sum_{u=1}^{s(j)} \sum_{i=1}^{N(j)/2} c_{u\cdot i}^j\, L_u^j(x)\, x^{i-1} \quad (2.75)$$

$\boldsymbol{c}$ が H_I をチェック行列とする符号 C_I の符号語であるための条件は“式 (2.72) が成立すること”、もしくは、“$C(x)$ が生成多項式 $g(x)$ で割り切れること”である点は $p=2$ の場合と同じである。また、すべての j の値 $(0 \le j \le m-1)$ に対して、$s(j) = \omega(j)$ とすれば、理

論的に符号化率 K/N の最も高い1重Lee誤り訂正符号が得られる。その際の符号長 N は $N=(p^{mk}-1)/2$ で，符号化率 K/N は、$K/N=1-(2k/(p^{mk}-1))$ で与えられる。

表2.3に $p=3$ のときの1重Lee誤り訂正符号 C_I のパラメータ例を示す。

表 2.3: Z_9上の1重Lee誤り訂正符号 C_I のパラメータ例

N	K	K／N	g(x)	$L_u^j(x)$
12	10	0.833	X^2-2X-1	1
24	22	0.917		1,2
36	34	0.944		1,2,4
40	38	0.950		1,2,4,3
78	75	0.962	X^3-X-2	1
156	153	0.981		1,2
⋮	⋮	⋮		⋮
364	361	0.992		---- 略---
⋮	⋮	⋮	⋮	⋮

2.4.4 1重Lee誤りを訂正する符号 C_Iの復号手順

例2.5の説明からも分かるように、1重Lee誤り訂正符号 C_Iの復号の手順は、有限体上のハミング符号の手順[2]に似せて以下のように整理することができる。

Step(1) 受信した符号語$\boldsymbol{c}^*$に対するシンドローム S を次式で求める。

$$S = \boldsymbol{c}^* H_I \qquad (\mathrm{mod}\ q) \tag{2.76}$$

行列 H は、式(2.64)あるいは式(2.71)で与えたチェック行列 H である。

Step(2) シンドローム S が、$\mathbf{0}\,(\mathrm{mod}\ q)$ ならば誤りなしとする。

Step(3) シンドローム S が、

$$S = \pm H_m^n \tag{2.77}$$

を満たすならば、誤り位置は受信符号語 $\boldsymbol{c}^*$ の先頭から $l = \sum_{i=0}^{n-1} s(i)N(i) + m$ デジット目の位置で、誤り値は± 1（複号同順）である。そこで、受信符号語の l デジット目に∓ 1 (複号同順）を、q を法として (mod q で) 加算することにより1重誤りを訂正する。

Step(4)　シンドローム S が、$\mathbf{0}\,(\mathrm{mod}\ q)$ でなく、式 (2.77) の形にも表現できないときは、訂正不能の誤りが起こったとみなす。

2.5 準2重Lee誤りを訂正する符号 C_{II}^{Q}の構成法

$Z_q(q=p^m;p$は素数$)$上の1重Lee誤り訂正符号から2重Lee誤り訂正符号へと符号を拡張するときに、有限体上での符号構成手法が有限環上でどこまで通じるかを確かめる必要がある。本節では 有限体上での手法を直接的に適用して得られる準2重Lee誤り訂正符号 C_{II}^{Q}について、その一般的な構成法と訂正能力を明らかにする [17][19][20]。符号 C_{II}^{Q}は、Z_q上の1重Lee誤りのすべてと2重Lee誤りのほとんどすべてをそれぞれ訂正できる。この符号を導く手法は、有限体上のBCH 符号 [3][2] を導く手法を適用しているものの、得られる符号はすべての2重Lee誤りを訂正する能力はもたない。しかし、使い方によっては十分に実用的な符号であると考えられる。また、本節の内容は次の2.6節（2重Lee誤りを訂正する符号の構成法）への準備ともなる。

2.5.1 準2重Lee誤り訂正符号 C_{II}^{Q}の構成手順

本節では、Z_q上の準2重Lee誤り訂正符号 C_{II}^{Q} を得るための一般的な手順を記す。

Step(1)　2.4節で述べた Z_q $(q=p^m)$ 上の1重Lee誤り訂正符号 C_{I} を構成する。但し、その変換多項式 $L_u^j(x)$ としては、$j=0$ のものだけが[3]、$s(0)$ 個選ばれているものとする。また、構成した符号 C_{I} の生成多項式を $g_1(x)$、チェック行列を H_1 とする。$g_1(x)$ の次数は k_1 とする。

Step(2)　Z_p上で既約で、Z_q $(q=p^m)$ 上で次式を満たす k_3 $(\leq k_1)$ 次の多項式 $g_3(x)$ を求める。これは、有限体 $GF(q)$ 上で2重誤り訂正BCH 符号 [2] を求めるテクニックを有限環 Z_qにも適用したものである。なおこの場合、3が零因子となるため、以降では、$p\neq 3$ とし

[3]一般には、$j\geq 0$ の多項式を種々選んで構成することも考えられるが、$j=0$ のものをベースにした構成が基本となるので、ここでは不必要な煩雑さを避けるために、$j=0$ のものだけを選んでいる。

て論を進める[4]。

$$g_3(x^3) = 0 \pmod{g_1(x)} \tag{2.78}$$

Step(3) Z_q ($q = p^m$) 上で、次式を満たす高々 $k_3 - 1$ 次の多項式 $R_u(x)$ $(u = 1, 2, \cdots, s(0))$ を求める。

$$R_u(x^3) = (L_u^0(x))^3 \pmod{g_1(x)} \tag{2.79}$$

Step(4) H_1 を構成する各剰余類の長さ、つまり、元（ゲン）の数を N^* とする。

$g_1(x)$ の周期 (p^m-ary 周期) を $N(0)$ とすれば、$p = 2$ のとき $N^* = N(0)$、$p \neq 2$ のとき $N^* = N(0)/2$ である。あるいは、$\tilde{N}$を $p = 2$ のとき、p-ary 周期、$p \neq 2$ のとき、p-ary 周期の 1/2 として、$N^* = p^{m-1}\tilde{N}$とも表現できる。このとき，行列 H_3 を次のように定める。

$$\begin{aligned} H_3 = [&h_{11}(x),\ h_{12}(x),\ \cdots, h_{1N^*}(x),\ h_{21}(x),\ h_{22}(x),\ \cdots, h_{2N^*}(x), \\ &\cdots,\ h_{s(0)1}(x),\ h_{s(0)2}(x),\ \cdots, h_{s(0)N^*}(x)\ ]^{\mathrm{T}} \end{aligned} \tag{2.80}$$

但し、

$$h_{ui}(x) = R_u(x)\, x^{i-1} \pmod{g_3(x)} \qquad (1 \leq i \leq N^*,\ 1 \leq u \leq s(0)) \tag{2.81}$$

なお、式 (2.80) では高々 $k_3 - 1$ 次の多項式 $h_{ui}(x)$ と、その係数を要素とする k_3 次元の縦ベクトルとを同一視して考えている。

Step(5) 求める符号 C_{II}^{Q} のチェック行列 H_{II}^{Q} を次式で定義する。

$$H_{\mathrm{II}}^{Q} = [\ H_1,\ H_3\ ] \tag{2.82}$$

[4]他の符号化法（代数曲線符号など）のテクニックを適用し、この条件をはずすことも考えられるが、本論文では煩雑さを避け、最もポピュラーな BCH 符号のテクニックに沿った論を進める。

Step(6) 準2重Lee誤り訂正符号 C_{II}^{Q} を、式(2.82)で与えたチェック行列 H_{II}^{Q}に対し、次式を満たす符号語 $\boldsymbol{c}$ の集合 $\{\ \boldsymbol{c}\ \}$ とする。

$$\boldsymbol{c}\, H_{\mathrm{II}}^{Q} \ = \ 0 \qquad (\mathrm{mod}\ p^m) \tag{2.83}$$

ここで、符号語 $\boldsymbol{c}$ の冗長ディジット数は 多項式 $g(x)$ の次数 k であり、符号語 $\boldsymbol{c}$ の先頭 の k ディジットを冗長ディジット、他を情報ディジットとみなせば、符号 C_{II}^{Q} は組織符号である。また、符号長 N、および、情報ディジット数 K は次式で与えられる。

$$N = s(0)N^* \quad (N^* \text{については 上記構成手順 (4) を参照}) \tag{2.84}$$

$$k = k_1 + k_3, \qquad K = N - k \tag{2.85}$$

□

上記構成手順で得られた符号 C_{II}^{Q}が、次のようにも表現できることは、2.4節での議論から明らかであろう。

性質 2.13 準2重 *Lee* 誤り訂正符号 C_{II}^{Q} に対する生成多項式 $g(x)$、変換多項式 $B_u(x)$、および式(2.87)で示した符号語に対する符号多項式 $C(x)$ を次のように定義する。

(1) 生成多項式 $g(x)$: $g(x) \triangleq g_1(x)g_3(x)$ (k 次多項式)

(2) 変換多項式 $B_u(x)$: 高々 $k-1$ 次の次の式を満たす多項式

$$B_u(x) \triangleq \begin{cases} L_u^0(x) & (\mathrm{mod}\ g_1(x)) \\ \\ R_u(x) & (\mathrm{mod}\ g_3(x)) \end{cases} \tag{2.86}$$
$$(u = 1,\ 2,\ \cdots,\ s(0))$$

(3) 符号多項式 $C(x)$: 符号語 $\boldsymbol{c}$ に対応する高々 N^*-1 次の多項式

$$\boldsymbol{c} = (\ c_{1\cdot 1},\ c_{1\cdot 2},\ \cdots,\ c_{1\cdot N^*},\ c_{2\cdot 1},\ c_{2\cdot 2},\ \cdots,\ c_{2\cdot N^*},\ \cdots, c_{s(0)\cdot 1},\ c_{s(0)\cdot 2},\ \cdots,\ c_{s(0)\cdot N^*}\ ) \tag{2.87}$$

$$C(x) \triangleq \sum_{u=1}^{s(0)} \sum_{i=1}^{N^*} c_{ui} B_u(x) x^{i-1} \tag{2.88}$$

（但し，$p=2$ のとき $N^*=N(0)$，$p\neq 2$ のとき $N^*=N(0)/2$ とする。）

このとき、符号多項式 $C(x)$ が生成多項式 $g(x)$ で割り切れることと、式 (2.82) のチェック行列 H_{II}^{Q} に対して、

$$\boldsymbol{c} H_{\mathrm{II}}^{Q} = 0 \qquad (mod\ p^m) \tag{2.89}$$

が成立することとは等価である。すなわち、準2重Lee誤り訂正符号 C_{II}^{Q}は、生成多項式 $g(x)$ で割り切れる符号多項式 $C(x)$ に対応する符号語 $\boldsymbol{c}$ の集合 $\{\boldsymbol{c}\}$ として定義することができる。

□

2.5.2 符号 C_{II}^{Q}の2重Lee誤り訂正能力

本節では、2.5.1節で構成された符号 が、1重Lee誤りのすべてと2重Lee誤りのほとんどすべてをそれぞれ確かに訂正できることを示す。

性質 2.14 準2重Lee誤り訂正符号 C_{II}^{Q}は、1重Lee誤りのすべてと2重Lee誤りのほとんどすべてをそれぞれ訂正できる。そのとき、訂正できる2重Lee誤りパターン数の全2重Lee誤りパターン数に対する割合 R_cは以下の式を満たす。

$$\text{(a)} \quad R_C = (2N-4s(0))/(2N-1) \qquad (p=m=2) \tag{2.90}$$

$$\text{(b)} \quad R_C \geq (N-p^{m-1}s(0))/N \qquad (\text{その他}) \tag{2.91}$$

□

（証明）まず誤り位置変数 z^i を次式で定める。

$$z^i = L_u^0(x)\, x^{i-1-(u-1)N^*} \pmod{g_1(x)} \tag{2.92}$$

$$(\ (u-1)N^* + 1 \leq i \leq uN^* \quad (u = 1, 2, \cdots, s(0)) \ )$$

$(L_u^0(x),\ s(0),\ N^*$ については上記構成手順 (1) と (4) を参照)

また、送信符号語 $\boldsymbol{c}$ が、式 (2.87) で表されるとして、$\boldsymbol{c}$ の第 i 番目と第 j 番目 $(i \neq j)$ にそれぞれ E_i および E_j (±1 または 0) の誤りがあったとすれば、受信符号語 $\boldsymbol{c}^*$ に対するシンドローム $S_1(x)$, $S_3(x)$ に関し、まず次式が成り立つ。

$$S_1(x) \triangleq \boldsymbol{c}^* H_1 \ = \ E_i z^i + E_j z^j \pmod{g_1(x)} \tag{2.93}$$

更に、式 (2.78) ～式 (2.81)、および、

$$E_i^3 \ = \ E_i, \quad E_j^3 = E_j \tag{2.94}$$

に留意すれば、

$$S_3(x) \triangleq \boldsymbol{c}^* H_3 \tag{2.95}$$

としたとき、次式が成立することが分かる。

$$S_3(x^3) \ = \ {E_i}^3 z^{3i} + {E_j}^3 z^{3j} \pmod{g_1(x)} \tag{2.96}$$

ここで、$S_1(x)$ が p で割り切れない場合について考える。このとき、式 (2.93)、(2.95) より、次式が導ける (冒頭で述べたように、$p \neq 3$ に注意。)

$$E_i z^i \cdot E_j z^j \ = \ (S_1(x)^3 - S_3(x^3))/(3S_1(x)) \pmod{g_1(x)} \tag{2.97}$$

従って、式 (2.92)、(2.93)、(2.97) より $E_i z^i$ と $E_j z^j$ は一意に定まる[5]。一方、H_1 は1重 Lee 誤り訂正符号のチェック行列をなすから、$E_i z^i$, $E_j z^j$ より、誤り位置 i, j、および誤り値 E_i, E_j が一意に定められ、訂正できることが分かる。

[5]式 (2.93) および式 (2.97) をまず、Z_p で解き、次いで Z_{p^2} で、そのあと Z_{p^3} でという風に順に解いて行けば解が得られる。その際、桁上がりに注意が必要である。$Z_p (p \neq 2)$ での解法は、いわゆる負巡回符号 [3] での解法となる。

なお、E_i、E_j の一方のみが 0 のとき、すなわち1重Lee誤りが生じたとき、$S_1(x)$ は前記変換多項式の選び方から p の倍数とはなり得ない。よって、1重Lee誤りのすべても訂正できる。(1重Lee誤りが生じているか否かは、$S_1(x)^3 = S_3(x^3) \pmod{g_1(x)}$ が成立するか否か、あるいは、式 (2.97) が 0 か否かで区別できる。)

さて、問題は $S_1(x)$ が p の倍数となる場合である。これを考察するためにまず、前記変換多項式 $L_u^0(x)$ としては、一般性を失うことなく、$1+pA_u(x)$ の形に書き表わされるものだけが選ばれているものとする (但し、$A_u(x)$ はある適当な高々 k_1-1 次の $Z_{p^{m-1}}$ の上の多項式)。

このとき、2重Lee誤り以下の誤りが生じたとして、$S_1(x)$ が p の倍数となり得るのは次の場合である。但し、$N(m-1)$ は前記 $g_1(x)$ の p-ary 周期である。

(1) $p=2$ のとき

(a) 誤り位置 i, j の差が $N(m-1)$ の倍数の場合

(b) 1つのディジットに ± 2 の誤りが生じた場合 ($E_i = E_j = \pm 1$, $i=j$)

(2) $p \neq 2$ のとき

誤り位置 i, j の差 $i-j$ が $N(m-1)/2$ の倍数である場合

(2) の場合、E_i, E_j の値によっては $S_1(x)$ が p の倍数とならないときもある点に注意。また、$q=4$ の場合を除き、$S_1(x)$ が p の倍数となっても訂正できる場合があり得る。それは、そのような誤りに対するシンドローム $S_1(x)$、および、$S_3(x)$ と同一のシンドロームをもつ他の相異なる2重Lee誤り以下の誤りパターンが存在しない場合である。

以上の点を考慮すれば、準2重Lee誤り訂正符号 C_{II}^{Q} が訂正できる2重Lee誤りパターン数の全2重Lee誤りパターン数に対する割合 $\bar{R}_C$ は、次のようにして求められる。

符号長 N に対し、2重Lee誤りパターンの総数は、$p=m=2$ のとき、$\binom{2N}{2}=2N^2-N$ で、それ以外のとき、$\binom{2N}{2}+N=2N^2$ である。また，訂正不能な2重Lee誤りパターンの総数は，$p=m=2$ のとき、$\binom{2\cdot 2s(0)}{2}N(1)=(4s(0)-1)N$ であって、それ以外のとき、高々

$$\left(\binom{2p^{m-1}s(0)}{2}+p^{m-1}s(0)\right)N(1)=2p^{m-1}s(0)N$$

である。以上より、式 (2.90) および式 (2.91) は容易に導ける。 □

表 2.4 に準2重 Lee 誤り訂正符号 C_{II}^{Q} のパラメータ例を示す。

表 2.4: 準2重 Lee 誤り訂正符号 C_{II}^{Q} のパラメータ例

N	K	K/N	R_C	g(x)	$B_u(x)$
(a) 4-ary QDLEC codes					
14	8	0.571	0.889	$(x^3-x-1)\cdot(x^3+X^2+2x-1)$	1
28	22	0.786	0.873		$1,1+2x^2+2x^4$
30	22	0.733	0.949	$(x^4-x-1)\cdot(x^4+X^3+x^2-x-1)$	B1(x)=1
60	52	0.867	0.941		$B1(x),B2(x)=3+2x+2x^2+2x^3+2x^5+2x^7$
90	82	0.911	0.939		$B1(x),B2(x),B3(x)=3+2x+2x^3+2x^4+2x^6$
120	112	0.933	0.937		$B1(x),B2(x),B3(x),B4(x)=1+2x^2+2x^4+2x^{5+}2x^{6+}2x^7$
⋮	⋮	⋮	⋮	⋮	⋮ ⋮
(b) 8-ary QDLEC codes					
28	22	0.786	≧0.857	$(x^3-x-1)\cdot(x^3+3X^{2-}6x-1)$	B1(x)=1
56	50	0.893	≧0.857		$B1(x),B2(x)=1+6x^2+2x^4$
⋮	⋮	⋮	⋮	⋮	⋮
224	218	0.973	≧0.857		B1(x),B2(x), ―――――
60	52	0.867	≧0.933	$(x^4-x-1)\cdot$	B1(x)=1
120	112	0.933	≧0..933	$(x^4-3X^3-5x^2-x-1)$	$B1(x),B2(x)=7+6x+2x^2+2x^3+2x^5+4x^6+2x^7$
⋮	⋮	⋮	⋮	⋮	⋮ ⋮
(c) 25-ary QDLEC codes					
310	304	0.981	≧0.984	$(x^3-4x^2-3)\cdot$	B1(x)=1
620	614	0.99	≧0.984	(X^3+2x^2+2x-2)	$B1(x),\ B2(X)=4-12x-12x^2-10x^4-9x^5$
⋮	⋮	⋮	⋮	⋮	⋮ ⋮

2.6 2重Lee誤りを訂正する符号C_{II}の構成法

本節では$Z_q(q=p^m;p$は素数$)$上の2重Lee誤りあるいは1重Lee誤りのすべてをそれぞれ訂正できる2重Lee誤り訂正符号C_{II}について，その一般的な構成法を与える[17][19][20]。構成法としては、前節で得られた準2重Lee誤り訂正符号C_{II}^{Q}の構成法がベースになっており、それにいくらかの変更を加えた形になっている。その際、構成法の一部に探索的部分を残すものの、実際の符号構成においては、例えば、冗長ディジット数10以下程度なら容易に前もって構成しておくことが可能であり、かつ十分実用的で多様な符号を構成できるため、応用上特に問題はない。

2.6.1 符号C_{II}の構成法を導くための準備

本節では、2重Lee誤り訂正符号C_{II}の構成法を示す。この構成法は、符号C_{II}^{Q}を符号C_{II}へ変更するために、式(2.86)で定義した変換多項式$B_u(x)$に対して、すなわち、

$$B_u(x) \triangleq \begin{cases} L_u^0(x) & (\mathrm{mod}\ g_1(x)) \\ R_u(x) & (\mathrm{mod}\ g_3(x)) \end{cases} \qquad (2.98)$$

$$(u=1,\ 2,\ \cdots,\ s(0))$$

に対して、新たな条件を付加するという形で提示される。そこでまず、若干の準備を行なう。

Z_q上の準2重Lee誤り訂正符号C_{II}^{Q}のチェック行列H_{II}^{Q}の各行ベクトルは、2.5節での説明から、次に示す多項式と1対1に対応する。

$$B_u(x)\cdot x^{i\tilde{N}+j}\ \ (\mathrm{mod}\ \ g(x)) \qquad (2.99)$$

$$1\le u\le s(0)\le \tilde{\omega},\quad 0\le i\le p^*-1,\quad 0\le j\le \tilde{N}-1 \qquad (2.100)$$

但し、$\tilde{\omega}$は、$p=2$のとき$\omega(0)/2$、$p\neq 2$のとき$\omega(0)$である（ωについては、2.2.3節参照)。また、$p^*=p^{m-1}$である。更に、$\tilde{N}$は、$p=2$のときはp-ary周期で、$p\neq 2$のときはp-ary

周期の1/2である。

ここで、

$$l = (u-1)p^*\tilde{N} + (i\tilde{N} + j) + 1 \tag{2.101}$$

としたとき、式(2.99)はチェック行列H_{II}^{Q}の第l行を表す多項式である。

さて、そこで、符号C_{II}^{Q}を符号C_{II}へ変更するために、式(2.99)をどのように変更させる必要があるかを考える。

まず、2重Lee誤り訂正符号となるための条件として、符号語の1つのディジットに生じた± 2の誤りを訂正できることが必要である。このことから、直ちに次のことが言える。

$p = 2$のとき、チェック行列H_{II}^{Q}を構成するH_1およびH_3に含まれる0レベルの各剰余類は、前半分のみとする必要がある。従ってその長さN^*は、0レベルでなく1レベルの剰余類の長さとなり、$N^* = N(0)/2 = N(1) = 2^{m-2}N(m-1)$となる。また、選べる剰余類の個数$\tilde{\omega}$も、$\omega(0)/2$から$\omega(1)/2$に減少する（個数が実に$1/2^{k-1}$に減少する。）。このことは、式(2.99)、(2.100)における但し書きを次のように変更する必要があることを意味する。

- 但し、$\tilde{\omega}$は、$p = 2$のときは$\omega(1)/2$で、$p \neq 2$のときは$\omega(0)$である。

  また、$p = 2$のときは$p^* = p^{m-2}$で、$p \neq 2$のときは$p^* = p^{m-1}$である。

  $\tilde{N}$は、$p = 2$のときはp-ary周期で、$p \neq 2$のときはp-ary周期の1/2である。

式(2.99)、(2.100)に対する但し書きをこのように変更することにより、次式が成立する。

$$2B_{u_1}(x) \cdot x^{i_1\tilde{N}+j_1} \neq 2B_{u_2}(x) \cdot x^{i_2\tilde{N}+j_2} \pmod{g(x)} \tag{2.102}$$

但し、$(u_1,i_1,j_1) \neq (u_2,i_2,j_2)$

$$2B_{u1}(x)\cdot x^{i_1\tilde{N}+j_1} \quad \neq -2B_{u2}(x)\cdot x^{i_2\tilde{N}+j_2} \quad (\mathrm{mod}\ g(x)) \tag{2.103}$$

但し、$q=4$のときの$(u_1,i_1,j_1)=(u_2,i_2,j_2)$を除く。

なお、式(2.102)および(2.103)は、符号語の各ディジットに生じた±2の各誤りに対するシンドロームがすべて相異なることを意味する。

さて、以上の準備のもとに、次の性質が成立することを導く。

性質 2.15 チェック行列の第l行、但し、

$$l=(u-1)p^*\tilde{N}+(i\tilde{N}+j)+1,$$

が、以下の多項式の係数列として表現される、$Z_q\,(q=p^m)$上の誤り訂正符号C_*を考える。

$$B_u(x)\cdot x^{i\tilde{N}+j} \quad (\mathrm{mod}\ g(x)) \tag{2.104}$$

$$1\leq u\leq s(0)\leq \tilde{\omega}, \quad 0\leq i\leq p^*-1, \quad 0\leq j\leq \tilde{N}-1 \tag{2.105}$$

但し、$\tilde{\omega}$は、$p=2$のときは$\omega(1)/2$で、$p\neq 2$のときは$\omega(0)$である（ωについては、2.2.3節参照）。また、$p=2$のときは$p^*=p^{m-2}$で、$p\neq 2$のときは$p^*=p^{m-1}$である。$\tilde{N}$は、$p=2$のときはp-ary周期で、$p\neq 2$のときはp-ary周期の1/2である。ここで、上記パラメータのもとに、次の集合B_jを定義する。

$$B_j \triangleq \{\pm B_u(x)\cdot x^{i\tilde{N}+j} \quad (\mathrm{mod}\ g(x))\} \tag{2.106}$$

このとき、符号C_*が2重Lee誤り訂正符号C_{II}となるための条件は、式(2.106)で定義した集合B_0に属する任意の4つの多項式$\beta_1^0(x)$〜$\beta_4^0(x)$に対し、次の式が成立することである。

$$\sum_{l=1}^{4}\beta_l^0(x)\neq 0 \quad (\mathrm{mod}\ q) \tag{2.107}$$

但し、$\beta_1^0(x) \sim \beta_4^0(x)$ のうち、同じ多項式の重複は2個までとする。しかし、$q = 4$ の場合に限り、同じ u, i に対し、$+B_u(x) \cdot x^{i\tilde{N}}$, $-B_u(x) \cdot x^{i\tilde{N}}$ をそれぞれ2個ずつ重複してとることは禁止する。 □

(証明) チェック行列 H を構成する部分行列 H_1 の構成において、変換多項式 $L_1^0(x) = 1$ としていることから、$B_1(x) = 1$ となる。これに合わせて、Z_{p^m} 上の多項式 $B_u(x)$ は、一般性を失うことなく、$Z_{p^{m-1}}$ 上の高々 $k-1$ 次の適当な多項式 $A_u(x)$ を用いて、次の形に書き表せるように選択することができる。

$$B_u(x) = 1 + pA_u(x) \qquad (1 \leq u \leq s(0)) \tag{2.108}$$

このとき、符号 C_* が2重Lee誤り訂正符号 C_{II} になるための条件は、2.5節の性質2.14の証明においても述べたように、シンドローム $S_1(x)$ が p の倍数となる場合にも、2重Lee誤りを訂正できることである。性質2.14の証明で述べたことの繰り返しになるが、$S_1(x)$ が p の倍数となり得るのは次の場合である。但し、$N(m-1)$ は前記 $g_1(x)$ の p-ary 周期である。

＜$S_1(x)$ が p の倍数となる場合＞

(1) $p = 2$ のとき

(a) 誤り位置 i, j の差が $N(m-1)$ の倍数の場合

(b) 1つのディジットに ± 2 の誤りが生じた場合 ($E_i = E_j = \pm 1$, $i = j$)

(2) $p \neq 2$ のとき

誤り位置 i, j の差 $i - j$ が $N(m-1)/2$ の倍数である場合

従って、証明すべき点は、次のようにまとめられる。

(1) 符号語の $(j+1)$ $(0 \leq j \leq \tilde{N} - 1)$ ディジット目から始めて$\tilde{N}$ディジットごとに選んでいったディジット全体のみに着目したとき、そこに生ずる2重以下のLee誤りに対する

シンドローム（$S_1(x)$, $S_3(x)$）がすべて相異なること、つまり2重以下のLee誤りがすべて訂正できること。

(2) 項目 (1) において、$j = j_1$の場合と$j = j_2 (\neq j_1)$の場合の2重Lee誤りを区別できること。

さて、ここで式 (2.106) および (2.107) をよく見ると、式 (2.107) は、上記項目 (1) において、$j = 0$の場合を記述しているに過ぎないことが容易に分かる。項目 (1) が$j = 0$のときに成立すれば、他の$j (\neq 0)$の場合にも成立することは、Z_p上で既約な、Z_{p^m}上の多項式$g_1(x)$, $g_3(x)$を法としたx^j倍の演算（LFSR(Z_{p^m})でjクロック進めることに相当）の性質から明らかである。

問題は、項目 (2) である。ここで、$j = j_1$のときの2重Lee誤りと、$j = j_2$のときの2重Lee誤りとが一致したとすれば矛盾することを導く。例えば、

$$\beta_1^{j_1}(x) + \beta_2^{j_1}(x) = \beta_3^{j_2}(x) + \beta_4^{j_2}(x) \tag{2.109}$$

とすると、

$$\beta_1^{j_1}(x) - \beta_3^{j_2}(x) = -\beta_2^{j_1}(x) + \beta_4^{j_2}(x) \tag{2.110}$$

が成り立つ。両辺とも、jがj_1のときの1重誤りと、j_2のときの1重誤りとによる2重Lee誤りに対するシンドロームを表わす式と見なせる。ところが、$0 \leq j_1, j_2 \leq \tilde{N} - 1$であるので、両辺とも$p$の倍数になることはない。従って、2.5節での説明からこの2重Lee誤りは訂正できるので、式 (2.110) が成立することはない。これは矛盾である。よって上記項目 (2) は成立する。以上により、性質2.15は成立する。- □

性質2.15で示した条件式 (2.107) を満たす符号C_*を、改めて符号C_{II}と名付け、そのチェック行列をH_{II}とすることにする。

2.6.2 Z_q上の2重Lee誤り訂正符号 C_{II} の構成手順

本小節では、2.6.1節で述べた説明を、Z_q上の2重Lee誤り訂正符号 C_{II} の構成手順としてまとめる。

Step(1) 2.4節で述べた Z_q $(q=p^m)$ 上の1重Lee誤り訂正符号 C_{I} を構成する。但し、その変換多項式 $L_u^j(x)$ としては、$j=0$ のものだけを $s(0)$ 個選ぶが、$p\neq 2$ のときは、$s(0)$ は $\omega(0)$ 以下である。$p=2$ のときは、まずその手順として $j=1$ の変換多項式 $L_u^1(x)$ を選び、その後で、$L_u^0(x)=L_u^1(x)/2$ とする。従って±の分を考えると、$s(0)\leq\omega(1)/2$ となる。以後特に断らない限り、$L_u(x)$ は、$L_u^0(x)$ を意味するものとする。更に、各変換多項式を剰余類首とする各剰余類の前半分のみをチェック行列の構成に利用する。構成した符号 C_{I} の生成多項式を $g_1(x)$、チェック行列を H_1 とする。$g_1(x)$ の次数は k_1 とする。

Step(2) Z_p上で既約で、Z_q $(q=p^m)$ 上で次式を満たす k_3 $(\leq k_1)$ 次の多項式 $g_3(x)$ を求める。なお、以降、$p\neq 3$ とする。

$$g_3(x^3)=0 \pmod{g_1(x)} \tag{2.111}$$

Step(3) H_1 を構成する各剰余類の長さ、つまり、元（ゲン）の数を N^* とする。$g_1(x)$ の周期（p^m-ary 周期）を $N(0)$ とすれば、$N^*=N(0)/2$ である。（あるいは、$\tilde{N}$を、$p=2$ のとき p-ary 周期、$p\neq 2$ のとき p-ary 周期の1/2とし、p^*を、$p=2$ のとき p^{m-2}、$p\neq 2$ のとき p^{m-1}とすれば、$N^*=p^*\tilde{N}$とも表現できる。）

Step(4) Z_q $(q=p^m)$ 上で、次式を満たす高々 k_3-1 次の多項式 $R_u(x)$ $(u=1,2,\cdots,s(0))$ を求める。

$$R_u(x^3)=(L_u(x))^3 \pmod{g_1(x)} \tag{2.112}$$

Step(5) 符号C_{II}の生成多項式を$g(x) \triangleq g_1(x)g_3(x)$ (k次多項式) とし、変換多項式$B_u(x)$を高々$k-1$次の次の式を満たす多項式 とする。

$$B_u(x) \triangleq \begin{cases} L_u(x) & (\mathrm{mod}\ g_1(x)) \\ \\ R_u(x) & (\mathrm{mod}\ g_3(x)) \end{cases} \qquad (2.113)$$
$$(u = 1,\ 2,\ \cdots,\ s(0))$$

ここで、多項式の集合Bを、次のように定義する。

$$B \triangleq \{\pm B_u(x) \cdot x^{i\tilde{N}} \pmod{g(x)}\} \qquad (2.114)$$

$$(u = 1,\ 2,\ \cdots,\ s(0)\ ;\ i = 0,\ 1,\ \cdots,\ (p^* - 1))$$

このとき、集合Bに属する任意の4つの多項式$\beta_1(x)$～$\beta_4(x)$に対し、次の式が成立するように、$B_u(x)$の選択を絞る。従ってこのことから、上記手順(1)と(3)での$L_u(x)$, $R_u(x)$の選択にフィードバックがかかる。

$$\sum_{l=1}^{4} \beta_l(x) \neq 0 \pmod{q} \qquad (2.115)$$

但し、$\beta_1(x) \sim \beta_4(x)$のうち、同じ多項式の重複は2個までとする。しかし、$q = 4$の場合に限り、同じu, iに対し、$+B_u(x) \cdot x^{i\tilde{N}}$, $-B_u(x) \cdot x^{i\tilde{N}}$をそれぞれ2個ずつ重複してとることは禁止する。

Step(6) 行列H_3を次のように定める。

$$H_3 = [h_{11}(x),\ h_{12}(x),\ \cdots, h_{1N^*}(x),\ h_{21}(x),\ h_{22}(x),\ \cdots, h_{2N^*}(x),$$
$$\cdots,\ h_{s(0)1}(x),\ h_{s(0)2}(x),\ \cdots, h_{s(0)N^*}(x)\ ]^{\mathrm{T}} \qquad (2.116)$$

但し、

$$h_{ui}(x) = R_u(x)\, x^{i-1} \pmod{g_3(x)} \qquad (1 \leq i \leq N^*,\ 1 \leq u \leq s(0)) \qquad (2.117)$$

なお、式(2.116)では高々 k_3-1 次の多項式 $h_{ui}(x)$ と、その係数を要素とする k_3 次元の縦ベクトルとを同一視して考えている。

Step(7) 求める符号 C_{II} のチェック行列 H_{II} を次式で定義する。

$$H_{\mathrm{II}} = [\, H_1,\, H_3 \,] \tag{2.118}$$

Step(8) 2重Lee誤り訂正符号 C_{II} を、式(2.118)で与えたチェック行列 H_{II} に対し、次式を満たす符号語 $\boldsymbol{c}$ の集合 $\{\ \boldsymbol{c}\ \}$ とする。

$$\boldsymbol{c}\, H_{\mathrm{II}} = 0 \qquad (\mathrm{mod}\ p^m) \tag{2.119}$$

ここで、符号語 $\boldsymbol{c}$ の冗長ディジット数は 多項式 $g(x)$ の次数 k であり、符号語 $\boldsymbol{c}$ の先頭 の k ディジットを冗長ディジット、他を情報ディジットとみなせば、符号 C_{II} は組織符号である。また、符号長 N、および、情報ディジット数 K は次式で与えられる。

$$N = s(0)N^* = s(0)N(0)/2 \tag{2.120}$$

(N^* については 上記 Step(3) を参照)

$$k = k_1 + k_3\,, \qquad K = N - k \tag{2.121}$$

□

＜符号 C_{II} の構成手順 Step(5) に関する補足＞

ここで、上記構成手順 Step(5) に関して補足する。Step(5) に関しては、その一般的な手順を任意の p, k, m について求めることは難しく、大きなパラメータによっては存在しないことも有り得る。しかし、実用的なパラメータとしては小さな値の方が十分利用価値があり、小さ

な値の場合には最後は試行錯誤ででも求めることができる。その際に有用な性質を、特に実用上重要な$p = 2$の場合について若干述べておこう。

(補足1)$p = m = 2$の場合：

集合Bに属するのは、$\pm B_1(x) = \pm 1$のみである。また、符号長Nは$\tilde{N}$に、つまりbinary周期の長さに等しい。このとき、2重Lee誤りでシンドローム$S_1(x)$が$p = 2$の倍数になるのは、各シンボルに$+2(= -2)$の誤りが生じた場合のみである。従って、式(2.115)(その但し書きに注意)を持ち出すまでもなく、この場合の符号は、2重Lee誤り訂正符号であって、$B_1(x) = 1$のみを用いる符号である。

(補足2)$p \neq 2; m = 2$の場合：

チェック行列を構成してみるとすぐ分かることであるが、選択する剰余類の個数は、必ずしも最大数$\omega(0)/2$は選べないことに注意。

(補足3)$p = 2; m = 3$の場合：

集合Bに属するのは、$\{\pm B_u(x), \pm B_u(x) \cdot x^{\tilde{N}} \pmod{g(x)}\}$ $(u = 1, 2, \cdots, s(0)(\leq \omega(1)/2))$である。ここで、$g(x) = g_1(x)g_3(x)$で、$g_1(x)$を$Z_2$で見たとき、$k_1$次の原始多項式であるとする。更に、剰余類の個数$s(0)$を最大の値$\omega(1)/2$に選択できたとすると、その値は式(2.32)より$2^{k_1-1}/2$となるので、集合$B$に属する多項式の個数は、$\pm$の分と$x^{\tilde{N}}$倍の場合も考慮して、その4倍の$2^{k_1}$である。なお、集合$B$に属する多項式を$Z_4$の多項式とみた場合でも、式(2.102)と式(2.103)を考慮すれば、相異なる多項式の個数は2^{k_1}であることに注意。ここで、式(2.113)および式(2.108)に留意して次式を定義する。

$$L_u(x) = 1 + 2A_u^{L1}(x) + 4A_u^{L2}(x) \tag{2.122}$$

$$R_u(x) = 1 + 2A_u^{R1}(x) + 4A_u^{R2}(x) \tag{2.123}$$

$$B_u(x) = 1 + 2A_u^{B1}(x) + 4A_u^{B2}(x) \tag{2.124}$$

上の式において、$L_u(x)$ を決めれば $R_u(x)$ が決まり、$L_u(x)$ と $R_u(x)$ から $B_u(x)$ が決まる。上の議論から、集合 $\{L_u(x)\}$ は、Z_4の多項式と見た場合に 2^{k_1}個の相異なる多項式の集合となることから、$A_u^{L1}(x)$ としては選択し得るすべての多項式が選ばれることになる（ここでは、上記±と $x^{\tilde{N}}$倍もすべて含めて数えている)。そして、各 $A_u^{L1}(x)$ に対し、ひとつの $A_u^{L2}(x)$ が、最終的に式 (2.115) を満たすように対応づけられねばならない。その対応づけは、もちろん1対1である必要はない。この対応づけは、k_1が 3,4,5 程度ならば、試行錯誤的にも決められる。その例は後で掲げる表 2.5 に示す。なお、井上・金子 [28] も上記中村による符号 C_{II} の構成法において、$L_u(x)$ の選び方として、集合 $\{1+2x^i\}\,(i=1,2,\cdots,(k_1-1))$ に含まれる多項式（重複は除く）の積 $\pmod{g_1(x)}$ として 2^{k_1-1}個選ぶことを提案しており、その選び方は k_1 が 3,4,5 のとき有効、6以上のとき無効としている。

(補足 4) $m=m_1\,(\geq 3)$ の2重 *Lee* 誤り訂正符号を、$m=m_2\,(<m_1)$ の2重Lee誤り訂正符号を使って構成する方法：

簡便な方法として図 2.4 に示す方法[6]が考えられる。

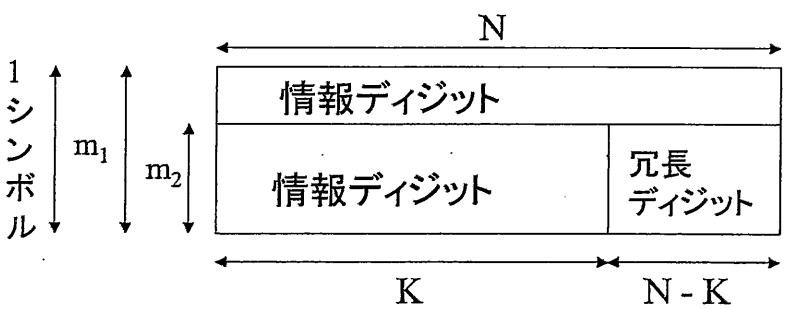

図 2.4: $Z_{p^{m_2}}$ 上の符号をベースに $Z_{p^{m_1}}$ 上の符号を作る方法 $(m_1>m_2)$

図 2.4 において、まず m_1ディジットからなる各シンボルの m_2ディジット分を使って $Z_{p^{m_2}}$ 上の2重Lee誤り訂正符号を作り、残りの (m_1-m_2) ディジット分は符号化しないでそのま

[6]本論文ではこれまで説明の都合上、チェック行列の構成の仕方から冗長シンボルが情報シンボルより先に来る形になっていたが、図では通常の例にならい、その順番を逆順にしてある。

まで符号を構成する。但し、復号の際は、まず $Z_{p^{m_2}}$ 上の符号として復号し、誤り位置と誤り値を得た後、シンボルの修正は m_1 ディジットからなる各シンボル単位の演算で行なう。このとき、構成された符号が2重Lee誤り訂正符号となることは特に説明を要しないであろう。なお、$Z_{p^{m_2}}$ 上の2重Lee誤り訂正符号の符号化率を K/N とすると、新しく構成された $Z_{p^{m_1}}$ 上の符号の符号化率Rは $((m_1 - m_2)N + m_2K)/m_1N$ となる。 □

本節では、Z_{p^m} の上の2重Lee誤り以下を訂正する効率的な符号が新しく導かれた．表2.5に Z_{2^3} 上の2重Lee誤り訂正符号 C_{II} のパラメータ例を示す．

表 2.5: Z_{2^3} 上の2重Lee誤り訂正符号 C_{II} のパラメータ例

N	K	K/N	g(x)	Bu(x)
28	22	0.786	$(x^3-x-1)\cdot(x^3-3x^2-6x-1)$	B1(x)=1, B2(x)=1+6x^2+2x^4
60	52	0.867	$(x^4-x-1)\cdot(x^4-3x^3-5x^2-x-1)$	B1(x)=1, B2(x)=7+6x+2x^2+2x^3+2x^5+4x^6+2x^7
120	112	0.933		B1(x)=1,B2(x)=5+6x^2+4x^4+2x^7+2x^8+6x^9, B3(x)=7+2x+6x^3+6x^4+4x^5+6x^6+4x^7, B4(x)=5+4x+2x^2+4x^3+2x^4+2x^5+6x^6+2x^7
124	114	0.919	$(x^5-x^2-1)\cdot(x^5-3x^4-5x^3-x^2-1)$	B1(x)=1, B2(x)=5+6x^2+4x^4+2x^7+2x^8+6x^9
248	238	0.96		B1(x), B2(x), B3(x)=7+6x+2x^2+2x^4+4x^5+6x^6+4x^7+6x^8+4x^9, B4(x)=3+6x+6x^4+2x^6+6x^7+4x^8+2x^9
372	362	0.973		B1(x), B2(x), B3(x), B4(x), B5(x)=7+2x^2+2x^3+2x^4+6x^5+2x^6+4x^7+4x^8+2x^9, B6(x)=7+6x^3+2x^4+2x^5+6x^6+2x^7+2x^8
496	486	0.98		B1(x), B2(x), B3(x), B4(x), B5(x), B6(x), B7(x)=1+6x+2x^3+4x^4+2x^5+4x^7+6x^8+2x^9, B8(x)=1+6x+6x^2+6x^3+4x^4+2x^5+2x^7

2.7 2重(/準2重)Lee誤りを訂正する符号 $C_{\mathrm{II}}(/C_{\mathrm{II}}^{Q})$ の復号法

本節では $Z_q(q=p^m;p$ は素数$)$ 上の2重あるいは準2重Lee誤りを訂正する符号の復号法についてのべる [22][23][20][48]。前節まで両符号の構成法について述べてきたが、2重Lee誤り訂正符号は、準2重Lee誤り訂正符号に制限を加える形で構成されているため、復号手順の大枠は共通している。そこで以下ではまず2重Lee誤りを訂正する符号 C_{II} の復号手順について述べ、準2重Lee誤りを訂正する符号 C_{II}^{Q} に関しては、符号 C_{II} の復号手順との違いをコメントするにとどめる。

2.7.1 符号 $C_{\mathrm{II}}(/C_{\mathrm{II}}^{Q})$ の復号法を導くための準備

符号 $C_{\mathrm{II}}(/C_{\mathrm{II}}^{Q})$ の復号法としては、いわゆる Syndrome Trapping 法 [50][51] を拡張して適用する手法 [22][23][48] を用いる。すなわち、数式からの直接的な計算結果として、誤り位置および誤り値を算出するのではなく、シンドロームと誤り位置および誤り値との間の関係を示す小さな対応表をいくつか前もって作成しておき、その対応表をうまく用いて誤り位置および誤り値を導き出す手法である。この手法はシンドロームと誤り位置および誤り値との間の対応そのものを直接示す大きな表を用いるのではなく、別のより小さな表を利用して中間解を求め、そのあと中間解とシンドロームとの間にごく簡単な演算を施して、最終の誤り位置および誤り値を算出するところに特徴がある。まず、復号の手順を述べる前にいくつかの準備を行なう。

(準備1) 受信符号語のシンドロームについて整理する。2.5節で述べたように誤り位置変数 z^i を式(2.92)で定義し($(u-1)N^*+1 \le i \le uN^*$ に注意)、誤り値変数を E_i, E_j (± 1 または0)で表す。送信符号語 $\boldsymbol{c}$ が、式(2.87)で表されるとして、$\boldsymbol{c}$ の第 i 番目と第 j 番目にそれぞれ E_i および E_jの誤りがあったとすれば、受信符号語 $\boldsymbol{c}^*$ に対するシンドローム

て以下に示す。

$$S_1(x) = E_i z^i + E_j z^j \pmod{g_1(x)} \tag{2.125}$$

$$= F_l(x)x^{i-1} + F_m(x)x^{j-1} = p^a F_n(x)x^{e-1} \pmod{g_1(x)} \tag{2.126}$$

$$S_3(x^3) = {E_i}^3 z^{3i} + {E_j}^3 z^{3j} \pmod{g_1(x)} \tag{2.127}$$

$$= \left(F_l(x)x^{i-1}\right)^3 + \left(F_m(x)\right)x^{j-1})^3 = p^{a+b}F_w(x)x^{v-1} \pmod{g_1(x)} \tag{2.128}$$

但し、a と b は共に 0 以上の整数で、

$$F_u(x) = +L_u^0(x) \text{ または } -L_u^0(x) \text{ または } 0 \qquad (u = l, m) \tag{2.129}$$

$$F_n(x) = +L_n^a(x)/p^a \text{ または } -L_n^a(x)/p^a \text{ または } 0 \tag{2.130}$$

$$F_w(x) = +L_w^{a+b}(x)/p^{(a+b)} \text{ または } -L_w^{a+b}(x)/p^{(a+b)} \text{ または } 0 \tag{2.131}$$

$$1 \le l, m \le s(0) \tag{2.132}$$

$$1 \le n \le \begin{cases} \omega(a+1) & (p = 2 \text{のとき}) \\ \omega(a) & (p \neq 2 \text{のとき}) \end{cases} \tag{2.133}$$

$$1 \le w \le \begin{cases} \omega(a+b+1) & (p = 2 \text{のとき}) \\ \omega(a+b) & (p \neq 2 \text{のとき}) \end{cases} \tag{2.134}$$

ここで、$L_u^d(x)$ は、$L_u^d(x) = p^d(1 + pA_u^L(x))$ と表される多項式で、2.3 節で述べた拡大環 $GR(q,k)$ の d レベルの剰余類の剰余類首である。従って、$F_u(x)$ $(u = l, m, n, w)$ は p で割りきれない多項式となる。また、$\omega(j)$ は、j レベルの剰余類の総数を示す。2.2.3 節参照。

(準備 2) 特に、$a = 0$ のとき、つまり、$S_1(x)$ が p の倍数でないとき、式 (2.126) および (2.128) より次式が成立する。$F_n(x)$ は、p で割り切れない多項式であることから、逆元が存在することに注意。

$$(F_n(x))^{-1}F_l(x)x^{(i-e)} + (F_n(x))^{-1}F_m(x)x^{(j-e)} = 1 \pmod{g_1(x)} \tag{2.135}$$

$$((F_n(x))^{-1}F_l(x)x^{(i-e)})^3+((F_n(x))^{-1}F_m(x)x^{(j-e)})^3 = p^b(F_n(x))^{-3}F_w(x)x^{v-3e} \pmod{g_1(x)} \tag{2.136}$$

ここで、$p^b(F_n(x))^{-3}F_w(x)x^{v-3e} \pmod{g_1(x)}$ を変形シンドロームと呼び、$(F_n(x))^{-1}F_l(x)x^{i-e}$ と $(F_n(x))^{-1}F_m(x)x^{j-e} \pmod{g_1(x)}$ を中間解と呼ぶことにする。上式より、前もって変形シンドロームと中間解との対応関係を与える対応表Ⅲ-0($a=0$ の場合の対応表Ⅲ) を用意しておけば、変形シンドローム (および $a=0$) より、中間解が対応表Ⅲ-0 を用いて得られることが分かる。

なお、前もって用意する対応表Ⅲ-0 を作るには、次のようにする。まず、すべての2重 Lee 誤り以下の誤りに対するシンドロームをそれぞれ前もって計算し、求めた各シンドロームに対応する変形シンドロームおよび中間解をそれぞれ式 (2.136) の右辺および式 (2.135) の左辺の各項に従って算出する。そして算出された変形シンドロームを入力とし、対応する中間解を出力とする対応表Ⅲ-0 をつくる。変形シンドロームとして値が存在しないところに対応する出力欄には、誤り訂正不能の誤り検出の印をつけておく。また、1重 Lee 誤りに対応する表の出力欄には、便宜上同じ中間解を2つ並べておく。1重 Lee 誤りが生じているか否かをシンドロームから判断するには、次式が成立しているか否かを調べればよい。

$$(F_n(x)x^{e-1})^3 = p^bF_w(x)x^{v-1} \pmod{g_1(x)} \tag{2.137}$$

(準備3) ところで、$F_u(x)\,(u=1,2,\cdots,s(0))$ が、$Z_{p^{m_1}}$ $(m_1<m)$ の上で特定できる (他と区別できる) ときは、上式は $Z_{p^{m_1}}$ の上で解を求めればよい。例えば、$p=2$, $m=3$ のときには、2.6.2 節で述べた構成手順の (補足3) の所で述べたことからも分かるように、$S_1(x)$ が p の倍数でないときには、$F_u(x)$ を Z_4 の上で特定できる (他と区別できる)。そのため、以下

の関係式を利用すれば上の式はより簡単な式になる。

$$(F_u(x))^{-1} = (F_u(x))^{-3} = F_u(x) \quad (\mathrm{mod}\ 4\ ;\ \mathrm{mod}\ g_1(x)) \tag{2.138}$$

更に、$F_u(x)$ を $1+2A_u^F(x)$ で表すことにより、次式が成立する。

$$F_{u_1}(x)\cdot F_{u_2}(x) = (1+2A_{u_1}^F(x))(1+2A_{u_2}^F(x)) = 1+2(A_{u_1}^F(x)+A_{u_2}^F(x)) \quad (\mathrm{mod}\ 4\ ;\ \mathrm{mod}\ g_1(x)) \tag{2.139}$$

従って、積 $F_{u_1}(x)\cdot F_{u_2}(x)$ の計算は、加算 $A_{u_1}^F(x)+A_{u_2}^F(x)\,(\mathrm{mod}\ 2)$ だけの計算で済む。そのためこれらの事実を使えば、インプリメントする上では非常に簡単になる。

（準備4） $S_1(x)$ が p^a の倍数であって、かつ p^{a+1} の倍数でないとき。（但し、a は1以上の整数。）このとき、$S_3(x^3)$ も、p^a で割り切れる。ここで、式 (2.135)、(2.136) を導いたのと同様の手順で次の方程式を導くことができる。$F_n(x)$ は、p で割り切れない多項式であることに注意。

$$(F_n(x))^{-1}F_l(x)x^{(i-e)} + (F_n(x))^{-1}F_m(x)x^{(j-e)} = p^a \quad (\mathrm{mod}\ g_1(x)) \tag{2.140}$$

$$((F_n(x))^{-1}F_l(x)x^{i-e})^3 + ((F_n(x))^{-1}F_m(x)x^{j-e})^3 = p^{a+b}(F_n(x))^{-3}F_w(x)x^{v-3e} \quad (\mathrm{mod}\ g_1(x)) \tag{2.141}$$

従って、2重 Lee 誤り訂正符号である限り、この場合も中間解 $(F_n(x))^{-1}F_l(x)x^{i-e}$ と $(F_n(x))^{-1}F_m(x)x^{j-e}$ は、変形シンドローム $p^b(F_n(x))^{-3}F_w(x)x^{v-3e}$ および a の値を与えれば、前もって用意した対応表Ⅲ-a を用いて特定できる。この場合、中間解同士の積と変形シンドロームとの間に、次式が成立することに注意しておこう。

$$((F_n(x))^{-1}F_l(x)x^{i-e})\cdot((F_n(x))^{-1}F_m(x)x^{j-e}) = (p^{2a} - p^b(F_n(x))^{-3}F_w(x)x^{v-3e}) \,/\, 3 \quad (\mathrm{mod}\ p^{m-a}\ ;\ \mathrm{mod}\ g_1(x)) \tag{2.142}$$

なお、(準備2) と (準備4) をわざわざ区別して書いたのは、用意する対応表を a の値ごとに揃えて、全体として表の大きさを小さくするという狙いを示したかったためである。その際、(準備3) で述べたように、表は $Z_{p^{m_1}}$ の上で作るようにしておくとよい。通常実用的な大きさの符号では、$a = 0, 1$ の場合の対応表を用意すれば十分なことが多いが、一般論としてはそうはいかず、$a = 0\,1, \cdots, \log_p p^*(= *)$ の場合の対応表を前もって準備しておく必要がある。p^*については、2.6.2 節符号 C_{II} の構成手順 Step(3) を参照。

(準備5) なお、上式 (2.126)、(2.128)、(2.135) および (2.136) において、1重 Lee 誤りのときは、$F_m(x) = 0$ 、誤りなし のときには、$F_l(x) = F_m(x) = 0$ となる式が得られる。また±2の誤りの場合には、$i = j$, $E_i = E_j$; $l = m$, $F_l(x) = F_m(x)$ となることにも注意しておこう。

2.7.2 2重 (/準2重)Lee 誤りを訂正する符号 $C_{\mathrm{II}}(/C_{\mathrm{II}}^{Q})$ の復号手順

前節までの準備のもとに、以下2重 Lee 誤りを訂正する $Z_q\,(q = p^m)$ 上の符号 C_{II} の復号手順について述べる。準2重 Lee 誤りを訂正する符号 C_{II}^{Q}に関しては、本節の冒頭で述べたように、符号 C_{II} の復号手順との違いをコメントするにとどめる。

Step(1) 受信符号語 $\boldsymbol{c}^*$ に対するシンドローム $S_1(x)$, $S_3(x)$ を定義式 (2.93) および (2.95) に従って求める。

Step(2) $S_1(x) = 0$ かつ $S_3(x) = 0$ のときは、誤りなしとして Step(12) へ。それ以外のときは、Step(3) へ。

Step(3) シンドローム $S_1(x)$ および $S_3(x)$ を次式のように表現し、それぞれ $(a, F_n(x), e)$ および $(a, F_w(x), v)$ に変換する。ここで、$F_n(x)$ は、p で割り切れない多項式である。また、

a は0以上の整数とする。

$$S_1(x) = p^a F_n(x) x^{e-1} \pmod{p^r\,(r \leq m)\ ;\ \mathrm{mod}\ g_1(x)} \tag{2.143}$$

$$S_3(x^3) = p^{a+b} F_w(x) x^{v-1} \pmod{p^r\,(r \leq m)\ ;\ \mathrm{mod}\ g_1(x)} \tag{2.144}$$

なお、$S_1(x)$ から $(a, F_n(x), e)$ への変換、および $S_3(x)$ から $(a, p^b F_w(x), v)$ への変換は、前もって、すべての2重 Lee 誤り以下の誤りに対するシンドロームに関し計算しておいて、それぞれを対応表Ⅰ、対応表Ⅱとして作っておくとよい。

Step(4) $a = 0$ のとき、つまり $S_1(x)$ が p の倍数でないとき、Step(5) へ。それ以外のときは Step(9) へ。

Step(5) 変形シンドローム $p^b(F_n(x))^{-3} F_w(x) x^{(v-3e)}$ を算出し、前もって用意した変形シンドロームと中間解との対応表Ⅲ-0より、中間解 $F_n(x)^{-1} F_l(x) x^{(i-e)}$ と $F_n(x)^{-1} F_m(x) x^{(j-e)}$ $(\mathrm{mod}\ p^r\,(r \leq m)\ ;\ \mathrm{mod}\ g_1(x))$ を得る。中間解を得たら Step(6) へ。中間解が得られず、訂正不能の出力を対応表Ⅲ-0から得たら、Step(12) へ。

Step(6) Step(5) で得た中間解と Step(3) で得たシンドローム $S_1(x)$ の表現から、解 $F_l(x)x^{i-1}$ と $F_m(x)x^{j-1} \pmod{p^r\,(r \leq m)\ ;\ \mathrm{mod}\ g_1(x)}$ を得る。(±1 の1重 Lee 誤り、あるいは±2の2重 Lee 誤り $(p \neq 2)$ が単独で起こっている場合は、上記対応表Ⅲ-0の作り方から、両者同一となることに注意。) この結果、誤り位置と誤り値を得たことになる。Step(7) へ。

Step(7) 得られた解が1重 Lee 誤りか否かを、式 (2.145) が成立するか否かで判定する。1重 Lee 誤りと判定したら、Step(8) へ。そうでなかったら、Step(11) へ。

Step(8) 得られた解 $F_l(x)x^{i-1}$ に対し、以下の式で与えられる t と E の値を用いて、誤り位置が先頭から t ディジット目、誤り値が E $(= +1$ または $-1)$ であるとして、受信符号語に生じた誤りを訂正する。その際の±1 の演算は、Z_{p^m} の上で m ディジットのシンボル単位に行な

う。まず、

$$F_l(x) = E^* L_l^0(x)\ ;\ (1 \leq l \leq s(0))\ ;\ E^* = +1 \text{または} -1) \tag{2.145}$$

であるとする。そして、

$$t = (l-1)N^* + i \quad ;\ E = E^* \tag{2.146}$$

とする。なお、N^*は2.6.2節のStep(3)を参照のこと。lの値で順序づけられた$L_l^0(x)$の表記法については、2.3節と2.4節再参照のこと。Step(12)へ。

Step(9)　$a \geq 1$のとき、つまり$S_1(x)$がpの倍数であるとき。

変形シンドローム$p^b(F_n(x))^{-3}F_w(x)x^{(v-3e)}$を算出し、前もって式(2.140)と(2.141)に基づいて用意した、変形シンドロームと中間解との対応表Ⅲ-aを用いて、中間解$F_n(x)^{-1}F_l(x)x^{(i-e)}$と$F_n(x)^{-1}F_m(x)x^{(j-e)}$ $(\mathrm{mod}\ p^r\,(r \leq m-a)$;mod $g_1(x))$を得る。中間解を得たらStep(10)へ。中間解が得られず、訂正不能の出力を対応表Ⅲ-aから得たら、Step(12)へ。

Step(10)　Step(9)で得た中間解とStep(3)で得たシンドローム$S_1(x)$の表現から、解$F_l(x)x^{i-1}$と$F_m(x)x^{j-1}$ $(\mathrm{mod}\ p^r\,(r \leq m-a)$; mod $g_1(x))$を得る。($p=2, a=1$のとき、$+2$または-2の2重Lee誤りが1箇所で生じたときは、上記対応表Ⅲ-aは、対応表Ⅲ-0における1重Lee誤りの場合と同様、得られる解が両者同一となるように作成してある。)この結果、誤り位置と誤り値を得たことになる。Step(11)へ。

Step(11)　得られた解$F_l(x)x^{i-1}$と$F_m(x)x^{j-1}$ $(\mathrm{mod}\ p^r(r \leq m-a$; mod $g_1(x))$ に従って、Step(8)で述べたように受信符号語に生じた誤りを訂正処理する。このとき、± 1あるいは± 2の訂正処理の演算は、Z_{p^m}の上でmディジットのシンボル単位に行なう。なお、$+2$または-2の2重Lee誤りが1箇所で生じているときは、同じ誤り位置に同じ1重Lee誤りが2回起こっていると解釈するとよい。Step(12)へ。

Step(12)　復号処理を終了する。

さてここで、「準2重 Lee 誤りを訂正する符号 C_{II}^{Q} の復号手順」についてコメントしておこう。

符号 C_{II}^{Q} の復号手順は符号 C_{II} の復号手順と基本的に同じであるが、上記符号 C_{II} の復号手順 Step(7) において、複数の解が存在して中間解が得られない場合が大部分である。そのため大部分の場合、Step(9) においては訂正不能の出力を対応表Ⅲ-a から得て、Step(12) へ進む点が異なる。なお他の情報をもとに、Step(9) における複数解を特定の一つに決めて出力してしまう復号も勿論考えられる。

2.8 一般化への試みと展望

前節までに、1重Lee誤り訂正符号から2重Lee誤り訂正符号までの符号の構成法および復号法について述べてきた。1重Lee誤り訂正符号については理論的に最適の線形符号が得られ、2重Lee誤り訂正符号についても、限定した範囲ではあるが非常に効率的な符号が得られた。これらを更に一般化し、Lee距離のもとで最適ないしは準最適な符号を完全に構成的な手順として求めることが一つの課題であるが、これはなかなかに大変な課題である。符号のパラメータとして、整数剰余環を規定する p と m、冗長シンボル数に関わる生成多項式の次数 k、訂正能力 t を任意に与えたときに、符号長 N が最大の、従って符号化率最大の最適な線形符号を如何にして求めるかという課題になる。

金子ら [27][28] は、符号長をbinary周期の2倍に限定したとき、筆者の構成法の自然な拡張として Z_{2^m} 上の t 重Lee誤り訂正符号が構成できることや、2重Lee誤り訂正符号として、符号長がbinary周期の $(2^{k_1-1}-1)$ 倍の符号の構成法を与え、更にその拡張の指針も与えている。しかし、最適符号には至っていない。

一般には、m や k の値を大きくとると、チェック行列に取り込める剰余類として、0レベル以上の色々なレベルの剰余類を選択できるようになり、符号長が長く取れるものの最適符号を得るための一般論が困難になる。

恐らく当面は上記パラメータのいくつかを固定して一般解を求める戦略が順当と思われる。例えば、単純な例として、特定の（小さな）値 m での最適符号を一例見出し、そのときの符号長 N および訂正能力 t を固定した上で、この m の値を大きくしたときの符号化率最大の最適符号を得る方法は、明らかに、2.6節の図2.4で示した方法を使えばよい。

一方、例えば、$p=2, m=3$ に固定した上で k や t の値を任意としたとき、最適符号は

どうなるのか、この場合ですら答えはまだ明確に示されていないように思われる[7]。逆にいうと、Z_qの上で符号を考えることの困難さを物語っているようにも見える。いずれにせよ、小さなパラメ-タでの最適符号の例を数多く貯えることが先決と思われる。その上で、例えば一つの方向として今井ら [25] による多段符号化の概念を援用する方法もあるように思われる。また、最近研究が進んでいる、A.R.Hammons ら [13] による環 Z_4の上の線形符号と有限体上の従来の非線形符号との関係も切り込み口の一つの方向として見逃せないように思われる。

[7]ちなみに、2.6 節で得られた符号の中で各 k_1に対し、符号化率最大 (但し、$k_1 \leq 5$) のものは、BCH 符号-like の構成法で得られる符号の中では最適符号である。

第3章　整数剰余環Z_q上の誤り訂正符号のインプリメンテーション

3.1　符号器・復号器の構成

3.1.1　1重Lee誤り訂正符号の符号器・復号器の構成

本節では、1重Lee誤りを訂正する符号の符号器と復号器の構成法 [47] について簡単に述べる。2章で述べた符号は、その構成の仕方から有限体上の 巡回符号の一種である Hamming 符号や BCH 符号と類似している．ただ基本的に異なる点として、有限環 Z_q 上の符号であること、変換多項式を有すること、そのため巡回符号ではないこと、しかし、符号語をいくつかの部分に分け、各部分をそれぞれ対応する変換多項式で変換しつつ重畳してできる符号は巡回符号であること、などがある。特に最後の性質を用いれば、巡回符号と同様、符号多項式割り算回路を利用した符号器・復号器を構成することができる。符号多項式割り算回路としてはフィードバックシフトレジスタ [2]（但し有限環 Z_q 上）を利用することにすれば、問題は変換多項式を如何に回路の中に組み込んでインプリメントするかということになる。これは、入力ディジット列に対し前処理（premultiply）操作を実施することにより解決できる。そのイメージ図を図 3.1 に示す。

図 3.1 は、2.4 節で例示した Z_8 上の 1 重 Lee 誤り訂正 (30, 28) 符号の符号器と復号器を示す大まかなブロック図である。まず符号器においては，多項式の係数列とみなした入力情報ディジット列の最初の 6 ディジットには $2x^2$ を、次の 12 ディジットには $(1+4x)x^2$ を，さらに次の 10 ディジットには x^2 を premultiply しながら，冗長ディジット生成器である Z_8 上

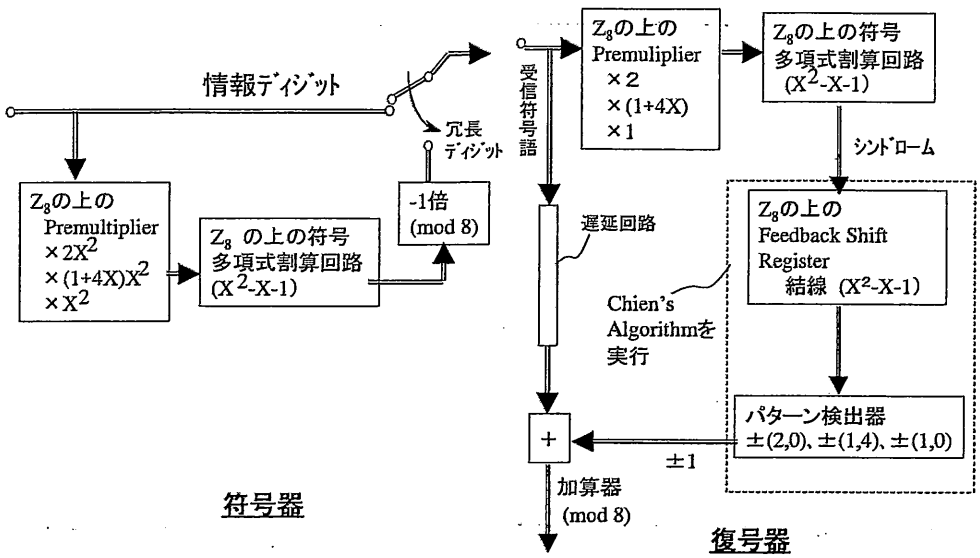

図 3.1: 1 重 Lee 誤り訂正 (30, 28) 符号の符号器・復号器の構成

の符号多項式割り算回路（結線多項式は $x^2 - x - 1$）へ送り込む．各変換多項式を x^2倍しているのは、冗長ディジットを 2 シンボル分最後に付加するためである[8]。情報ディジットが入力され終わった時点でレジスタ内にあるディジット列を -1 倍 (mod 8) したものが冗長ディジット列となる。

復号器の構成も Hamming 符号の復号器に似せて若干拡張した形で構成できる。まず、符号器と似たような操作でフィードバックシフトレジスタを利用してシンドロームを算出する。そのあと，いわゆる Chien's Algorithm[2] を Z_8 上のアルゴリズムとして解釈し直し、6 つのパターン $\pm(2,0)$、$\pm(1,4)$、および$\pm(1,0)$ を検出する。どのパターンをどの時点で検出したかによって，$+1$ または-1 の訂正パルスを出力し、遅延回路から出てくる受信ディジットを訂正する。

[8]前章までは説明の都合上、符号語内では冗長ディジット、情報ディジットの順に並んでいたが、本章以降ではその順番を前章までの符号語の最後からの順にした通常の表記法に従う。従って、情報ディジット、冗長ディジットの順に並ぶものとする。

3.1.2 2重(／準2重)Lee誤り訂正符号の符号器・復号器の構成

2重(／準2重)Lee誤り訂正符号の場合も、符号器は、生成多項式 $g(x)$ で結線が定まるフィードバックシフトレジスタと、変換多項式および冗長シンボル数によって規定される前処理回路(premultiplier)とから構成することによって図3.1とほぼ同様の形で実現できる。一方，復号器の方は有限体上のBCH符号の場合もそうであるように、シンドローム生成回路を $g_1(x)$ 用と $g_3(x)$ 用の2つに分け、そのためのpremultiplierも，$L_u^0(x)$ 倍と $R_u^0(x)$ 倍の2つのグループに分けて実行した方が回路規模の点から望ましい。全体として有限体上のBCH符号と類似した形の回路を構成できるが、2.7節で述べたように Z_q 上の符号特有の処理が必要となるので、以下では、2重Lee誤り訂正符号の復号器について更に詳しく説明する。

なお、上で述べた符号器および復号器の構成の仕方は、式(2.68)や式(2.88)に示した符号多項式 $C(x)$ が、生成多項式 $g(x)$ で割り切れるということに一つの根拠を置いている。

図3.2は Z_q 上の2重Lee誤り訂正符号の復号器の概略を示すブロック図である。処理の流れは、2.7.2節で示した「2重Lee誤りを訂正する符号 C_{II} の復号手順」に沿っている。

(1) 受信した符号語は、復号処理の間、バッファに退避させられるとともに、フィードバックシフトレジスタを利用した符号多項式割算回路に送られる。ここで、シンドローム $S_1(x)$, $S_3(x)$ が生成される。

(2) シンドローム $S_1(x)$ および $S_3(x)$ を、対応表Ⅰ、対応表Ⅱに従って、式(2.143)と(2.144)で示した $(a, F_n(x), e)$ および $(b, F_w(x), v)$ にそれぞれ変換する。このとき、a と b の値の組み合わせ（例えば、$b < 0$ など）によっては、訂正不能の誤りが生じていることが検出できるため、これを検出信号として利用し、Mod加算器M4による訂正動作をすべて禁止する。また、$a = b = m$（但し、$q = p^m$）のときにも、誤りなしとして、訂正動作制御回路を制御して訂正動作を禁止する。なお、対応表は通常ROM(Read Only Memory)を用いて作られる。

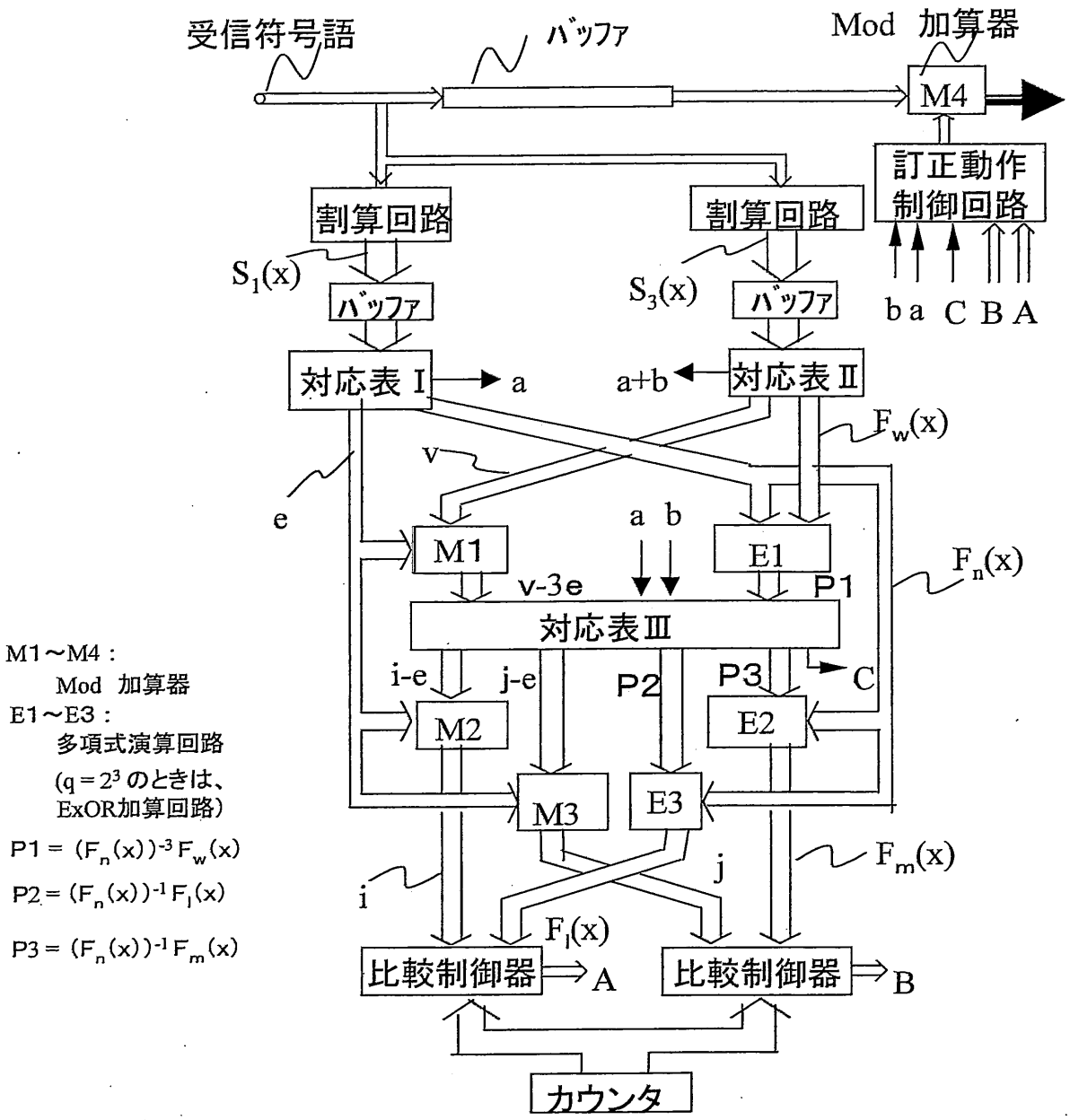

図 3.2: 2重 Lee 誤り訂正符号の復号器の構成

(3) シンドロームを変換して得た多項式をもとに、回路M1とE1を使って、変形シンドローム $p^b(F_n(x))^{-3}F_w(x)x^{v-3e} \pmod{g_1(x)}$ の構成部分を求める。それらをROMで作られた対応表IIIへ入力する。あわせて a と b の情報も入力する。回路M1は、$v-3e$ の値を mod p^r で演算するMod加算器である（$r \leq m$, 2.7.2節の復号手順参照)。回路E1は多項式演算回路であるが、2.7.1節の(準備3)で述べたように、$q = 2^3$のときは、回路E1は単にExOR回路を並べたものになる。

(4) 対応表IIIの出力として、中間解 $(F_n(x))^{-1}F_l(x)x^{i-e}$ と $(F_n(x))^{-1}F_m(x)x^{j-e} \pmod{g_1(x)}$ の構成部分を得る。解がなく、訂正不能のときには、検出情報 C を得る。検出情報 C は、訂正動作制御回路を制御して、Mod加算器M4による訂正動作をすべて禁止する。

(5) 得られた中間解の構成部分 $(F_n(x))^{-1}F_l(x)$ と $(i-e)$、および $(F_n(x))^{-1}F_m(x)$ と $(j-e)$ に、対応表Iの出力として得られた $F_n(x)$ と e をそれぞれ作用させて、i と $F_l(x)$ および j と $F_m(x)$ を得る。i と j は、Mod加算器M2、M3をそれぞれ用いて、$F_l(x)$ と $F_m(x)$ は、多項式演算回路E3、E2をそれぞれ用いて得る。

(6) 先頭から n 番目の受信ディジットが受信バッファから出力されるとき、カウンタの値も n になるものとする。解 $F_l(x)x^{i-1}$ と解 $F_m(x)x^{j-1}$ によってそれぞれ指定される誤り位置の値とカウンタの値とが一致したとき、バッファに格納されていた受信誤りディジットを訂正するべく、比較制御器から検出信号AあるいはBを得る。そのとき、検出信号AあるいはBは、$F_l(x)$ あるいは $F_m(x)$ からそれぞれ指定される誤り値+1または-1の情報を含んでいる、つまり検出している信号とする。これらの検出信号は、Mod加算器M4を用いて受信誤りディジットからその誤り値を減算するべく、訂正動作制御回路を制御する。

(7) なお、検出信号AとBが同一の受信シンボルに対し、同じ誤り値 E ($= \pm 1$) を検出しているときには、2^aE の値をそのシンボルから減ずるべく訂正動作制御回路を制御する。

3.2 符号化／復号処理の並列化

前節で述べた符号器／復号器の構成と2.2節で述べたフィードバックシフトレジスタの周期を念頭に置けば、図3.1、図3.2の符号多項式割り算回路において、冗長デジットないしシンドロームの算出に要するクロック数を減らせることができる。即ち、複数個の前処理（premultiply）をシークエンシャルでなく並列的に同時に実行し各演算結果を合算して多項式割算回路であるシフトレジスタに供給することによって、通常シークエンシャルに処理を行う場合にはN（＝符号長）クロック分要する処理をN_*(＝採用した各剰余類の長さ）クロック分で済ませることが出きる。一種の並列化処理であり、(超) 高速回線等への応用を考える場合には有用である。

この考え方はさらに拡張することができ、有限環上の符号に限らず、有限体上の符号に対しても応用することができる [52][53]。それは、上記各剰余類の長さN^*を更にu等分し[9]、チェック行列の先頭から$i = (l-1)N^*/u + 1$番目$(l = 1, 2, \cdots, u)$の各行に対応する$B_i(x)$を変換多項式として、上で述べた並列化の方法を適用することである。この場合N^*(＝採用した各剰余類の長さ）クロック分のさらに$1/u$クロック分で符号多項式割算回路の処理を済ませることができる。

なお、筆者の文献 [52][53] でも詳しく述べているが、情報ディジット部分と冗長ディジット部分を別々にu等分して処理した方が、回路構成上適している場合もある。符号化での冗長シンボル算出のための処理は、この場合に相当する。

以上、述べたように変換多項式の考え方と並列処理の考え方をうまく結び付けることにより、色々なヴァリエーションを構成することができる。

[9]有限体上の符号では、通常このN^*が符号長Nとなる。uで割り切れないときには、ダミーのシンボルを付加する。

3.3 Lee 距離に基づく 2 重誤り訂正符号 LSI

本節では、大容量デジタルマイクロ波無線通信向けに開発した 2 重誤り訂正符号 LSI について述べる [35]。図 3.3 に示す図が、開発した 2 重 Lee 誤り訂正符号 LSI の外観図である。符号は Z_{2^3} 上の符号であるが、これを効果的に利用して、$2^3 \times 2^3 = 64$ 値あるいは $2^4 \times 2^4 = 256$ 値の Square 多値 QAM 伝送系あるいは Stepped 多値 QAM 伝送系に適用している（4.3 節参照）。送信側 2.5K ゲート、受信側 4.3K ゲートおよび誤り位置演算用 ROM として 64K ビットを要する。符号の性能評価については、4.2 節を参照されたい。ほぼ理論値に一致した訂正能力が確認されている。表 3.1 は、本 LSI の諸パラメータについて記したものである。本 LSI は 10 年前当時の技術 (1.5 μ m) を用いて作ったものであるが、現状の技術（0.35 μ m）を用いれば、更に面積約 1/20、消費電力 1/30 程度になると予想される。2 重誤り訂正符号 LSI としては非常にコンパクトな回路規模で構成されている。

図 3.3: Z_{2^3} 上の 2 重 Lee 誤り訂正符号 LSI

表 3.1: Z_{2^3} 上の 2 重 Lee 誤り訂正符号 LSI 諸元

符号	符号長	496	372	248	124
	情報ディジット数	486	362	238	114
符号化利得		3.2dB	3.4dB	3.6dB	4.0dB
回路規模	符号器	2.5 kGate			
	復号器	4.3 kGate(+ROM:64kb)			
動作速度		50 MHz Typical			
消費電力	符号器	100mW (10MHz)			
	復号器	200mW (10MHz)			

第4章　整数剰余環Z_qの上の誤り訂正符号のデジタル通信系への応用

4.1　高密度デジタル通信系への誤り訂正符号の導入と課題

4.1.1　差動符号化多値直交振幅変調系への誤り訂正符号の導入

ディジタルマイクロ波無線 (Digital Microwave Radio ; DMR) 通信系、あるいは、電話回線を用いたデータ通信系などの分野において、情報伝送の高密度化をはかり、帯域あたりの情報伝送速度を大きくするための努力がこれまで続けられてきた。高密度化の進展にともない、従来単なるオプションとしてしか考えられていなかった誤り訂正符号を、最初からシステム設計の一環として取り入れていく必要性が認識されてきた。その際，効率的な誤り訂正符号を採用するためには、システムの特殊性を十分考慮に入れて、符号の選択・設計を行う必要があった。

高密度デジタル通信系の実現に向けては、まず波形伝送技術、変復調技術等において様々な技術の進展が見られた。その中で、高密度化に伴って増大した伝送路上での雑音の影響を軽減して所要C／N (Carrier to Noise Ratio: 搬送波平均電力対平均雑音電力比) の改善を図るために、あるいは増幅器の非線形領域での利用に伴う信号歪等による残留誤りの低減を図るために、その抜本的な対策として、誤り訂正符号を利用することがDMR通信系において80年代初頭あたりから検討され始めた。高密度デジタル通信系における変復調技術としては、周波数利用効率の高い多値直交振幅変調（Quadrature Amplitude Modulation ; QAM) 方式の利用が主流であったため、誤り訂正符号を導入する上では多値 QAM 方式に親和性のある符号の導入が求められた [33]。

高密度の DMR 通信系は、当初既存の非同期デジタルハイアラキー（PDH : Plesiochronous Digital Hierachy）に沿った形で開発されてきた。そこでの誤り訂正符号としては、米国系の 6GHz 帯 135Mbps(帯域幅 30MHz) の DMR 通信系で、64 値 QAM 方式のもと、まず Z_8 上の 1 重 Lee 誤り訂正 (84,81) 符号が世界に先駆けて適用され開発された [33]。またヨーロッパ系の Lower-6GHz 帯 140Mbps(帯域幅 30MHz) の DMR 通信系で、256 値 QAM 方式のもと、Z_{16} 上の 1 重 Lee 誤り訂正 (72,70) 符号が適用され開発された [34]。これらの符号は第 2 章 2.4 節で述べた符号である。

更に、1988 年、当時の CCITT（Consulting Committee of International Telegraph and Telephone ; 現在、ITU-T に引き継がれている) が、将来の高速広帯域サービスの提供や運用性の充実を考慮して、世界的標準として同期デジタルハイアラキー (SDH : Synchronous Digital Hierachy) を勧告した（CCITT 勧告 G.707,708,709)[39][40]。SDH では、155.52MBPS が情報伝送速度の基本となっており、上記 140Mbps に比べ情報伝送速度が 10%強アップしたため、更に高度の変復調技術やフェーディング等化技術、スペースダイバーシティ技術、誤り訂正符号技術等々が求められた。誤り訂正符号技術としては、冗長度が少なくしかも訂正能力が更に高いものが求められた。そこで、それまでの 1 重誤り訂正符号から 2 重誤り訂正符号で符号化効率の良いものへの Version Up という流れができた。3.3 節の 2 重 Lee 誤り訂正符号 LSI はこの流れに乗って開発されたものであり、符号自体は 2.6 節、2.7 節で述べた符号である。

DMR 通信系用に開発 (もしくは推薦) された誤り訂正符号としては、その後 BCH 符号、畳み込み自己直交符号、RS 符号などが発表されている [41]-[44][38]。ただ符号化率、装置規模、訂正能力（符号化利得 (Coding Gain)）等々全体のバランスから考えて完全な決め手になっているものはない。その点本論文での Lee 距離に基づく符号はバランス的に優れているという特徴はある (3.3 節参照)。

さて、多値 QAM 方式においては色々なデジタル信号処理が施される。そこで、多値 QAM 信号 $S(t)$ は次式のように表されることをまず確認しておこう。

$$S(t) = p(t)\cos\omega_c(t) + q(t)\sin\omega_c(t) \tag{4.1}$$

式 4.1 において、同相成分の信号 $p(t)$ と直交成分の信号 $q(t)$ は、時間軸上で離散的に与えられる多値パルス信号の列として表現される。これが情報を担う多値データの列である。$\omega_c(t)$ はこれら同相・直交成分の信号を運ぶ搬送波である。

ところで、多値 QAM 方式による高密度の DMR 通信系に誤り訂正符号を導入するとき、考慮すべき特殊性あるいは課題として次の点が考えられる。

(1) 多値信号 ··· 従来の 2 値符号では非効率的である。送信シンボル（ディジット）が他シンボルに誤る場合、距離的に近いシンボルには誤りやすいが遠いシンボルには誤りにくい。このことを多値信号ないし多値符号の効率的な符号構成にどのように反映させたらよいのか？高密度化の上で、符号化効率改善への鍵となる。

(2) 直交性 ··· QAM 信号が対象であるので、同相側、直交側で独立に誤り訂正符号化が可能である。このことを通信系での雑音を考慮しながら符号の構成に如何に反映させるか？

(3) 再生搬送波の位相の不確定性、位相スリップの存在 ··· 再生搬送波の位相には、0°, 90°, 180°, 270° の 4 種類の不確定性が存在する。正しい受信信号を得るには、再生搬送波の引き込み位相を検出するか、何らかの手段で不確定性を除去する必要がある。通常使われる解決策として、差動符号化による方法がある。これは、情報を絶対位相に対応させるのではなく、位相差に対応させるものである。しかし、この場合差動復号後に伝送誤りが倍になるという欠点がある。これから逃れる方法はないか？

(4) 高密度の帯域制限系 ··· 帯域制限通信路に対して多値化で高能率伝送を行う事から、符

号化率の非常に高い符号が求められる（冗長度は数％以内）

(5) 多中継システム … DMR 通信系は、基本的に多中継システムであることを考えれば、一ホップに許される絶対遅延時間も制限される。従って、絶対遅延時間に直接関係する符号長も短い事が望まれる（高々500 シンボル程度以内：ここでは、DMR でのホップ数を最大 50、変調速度 25MH z 、DMR に許される絶対遅延時間 1 msec として、(1msec ／ 50) ／ 40nsec ＝ 500 として算出)。

4.2 節において、これらの課題に答える方式として、２章で述べた Lee 距離に基づく誤り訂正符号を利用する方式を提案し解析する。ただその前に、上記 (3) の課題に関し、Lee 距離に基づく誤り訂正符号が差動多相位相変調系にまず適していることを以下に詳しく述べ、4.2 節の提案につなげることにする。

4.1.2 差動符号化多相位相変調系への誤り訂正符号の導入

本節では、特に Z_q の上の Lee 距離に基づく誤り訂正符号が、まず q 相の差動位相変調による通信系に適していることを述べ、次節へつなげる。そして、位相の不確定性に対し、いわゆるトランスペアレント (transparent) な多値符号（後述）を、ここでは Z_q の上の Lee 誤り訂正符号として与えたということを述べる。

まず、差動位相変調系においては、各位相 $2\pi i/q$ は，整数 $i \pmod q$ に１対１に対応させて考えることができる。つまり、各データは Z_q の元として表現できる。そこで、差動位相変調系は、図 4.1 に示す形にモデル化できる。また、データ列 $\theta_{i0}, \theta_{i1}, \theta_{i,2} \cdots$ は、$\theta_i(x) = \theta_{i0} + \theta_{i1}x + \theta_{i2}x^2 + \cdots$ と表現できる。図 4.1 より、q 相の位相変調系、および、差動位相変調系の入出力関係は次のように表わされる。

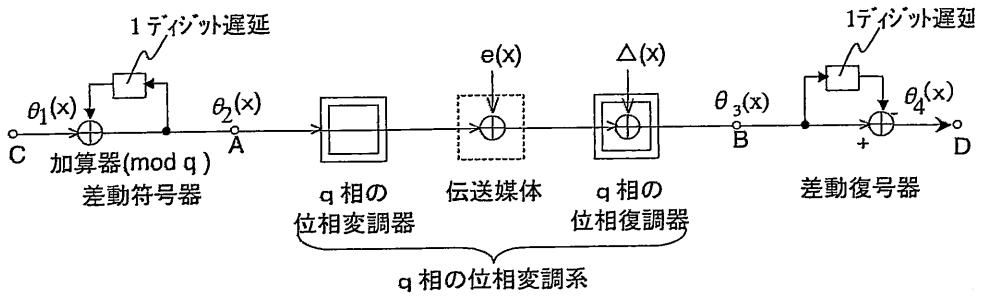

図 4.1: q 相の差動位相変調系のモデル

(1) q 相位相変調系：

$$\theta_3(x) = \theta_2(x) + e(x) + \triangle(x) \pmod{2^m} \tag{4.2}$$

ただし、$e(x)$ は伝送媒体における誤りディジット列 $e(x) = e_0 + e_1 x + e_2 x^2 + \cdots$ で、$\triangle(x)$ は復調器における位相の不確定分 δ を表わす系列 $\triangle(x) = \delta + \delta x + \delta x^2 + \cdots$ である。

(2) q 相差動位相変調系：

$$\theta_4(x) = \theta_1(x) + e(x)(1-x) + (\delta + \alpha - \beta) \tag{4.3}$$

但し、α と β はそれぞれ差動符号器、および、差動復号器の初期値である。

式 (4.3) あるいは図 4.1 から明らかなように、伝送媒体上の誤りは差動復号器を通過することにより約 2 倍に拡大される。そのため、倍化される以前、つまり、図 4.1 の B 点に誤り訂正復号器を置く方式が考えられる。この場合、符号器は当然 A 点に置かれている。しかしながら、その際の問題点として、式 (4.2) からもわかるように、位相復調器による位相の不確定分が残っている状態で誤り訂正を実行しなければならない。逆にいえば，位相の不確定分が誤り訂正の操作に何ら影響を及ぼすことなく誤り訂正復号器を通過するように、そしてその不

確定分は、そのあとの差動復号器で取り除くようにしなければならない。そのための１つの方法として、使用される誤り訂正符号が、２つの条件

(1) 線形である。

(2) 位相の不確定分に対応する語 $(\delta, \delta, \cdots, \delta)$ が１つの正しい符号語である。

を満たすように構成されるならば、式 (4.2) より $\triangle(x)$ は何ら誤り訂正に影響を及ぼさず、そのまま誤り訂正復号器の外に出る。このような符号は位相の不確定に対し、transparent な符号とよばれる [29]。なお、条件 (2) は符号の線形性より、$(1, 1, \cdots, 1)$ を正しい符号語としてもつという表現に置き換えられる点に注意。

さて、この transparent な符号としては、２相データの場合は、例えば BCH 符号などを用いて容易に構成し得ることはよく知られているが、多相データに対して、直接的にどのように構成したらよいか、それまで知られていなかった [19]。

ここで、2.4 節、2.5 節で導いた Z_{p^m} の上の１重 Lee 誤り訂正符号 C_{I}、および準２重 Lee 誤り訂正符号 C_{II}^{Q} についてみると、両符号とも明らかに Z_{p^m} の上で線形である。さらに、式 (2.43) を考慮すれば、任意の j の値（$0 \leq j \leq m-2$）に対し、Z_{p^m} の上で次式が成立することも明らかである。

$$p^j(1 + x + x^2 + \cdots + x^{N(m-j)-1}) = 0 \pmod{g(x)} \tag{4.4}$$

このことから、両符号とも $(1, 1, \cdots, 1)$ を正しい符号語としてもつことがわかる。

したがって、本章で導いた符号 C_{I} および C_{II}^{Q} ともに位相の不確定に対しては transparent な符号である。

また、2.6 節で述べた Z_{p^m} の上の２重 Lee 誤り訂正符号 C_{II} についてみると，もちろん，Z_{p^m} の上で線形であり、また、その構成の仕方から，C_{II} が偶数個の変換多項式を有すると

き、そのときに限って、$(1,1,\cdots,1)$ を正しい符号語としてもつことがわかる。従って、そのとき符号 C_{II} も位相の不確定に対し transparent な符号となる。

以上により，２章で導かれた符号 C_{I}, C_{II}^{Q}, C_{II} は，差動位相変調による通信系に適した符号となっていることがわかる。

4.2 Lee 距離に基づく符号系を導入した差動符号化多値直交振幅変調系の提案・解析

本節では、4.1.1 節で述べた特殊性を持つ差動符号化多値直交振幅変調（QAM）系に対し、Lee 距離に基づく多値 transparent 誤り訂正符号を用いることを提案し解析する。次いで特に 64 値 QAM を例にとりあげ、この多値 transparent 符号が上記特殊性のもとで如何にシステムの一部として取り入れられるかについて詳しく述べるとともに、符号の性能について評価を行う。

まず、差動符号化を併用した多値 QAM 用誤り訂正符号化システムとして図 4.2 に示すシステムを提案する [46]。図に示すように、誤り訂正符号化・復号は差動符号化・復号の内側で行うのが一つの特徴となっている。更に、同一の transparent 誤り訂正符号を同相側、直交側に独立に置いている点が二つ目の特徴である。後で見るように、これらの特徴から、図 4.2 のシステムにおいては、差動復号の前で位相の不確定性があっても伝送誤りの訂正を支障なく行える。そのため、差動復号による誤りの倍化が例えあったとしても、誤り訂正処理後の残留誤りの倍化であるため影響は少なく、誤り訂正回路の訂正能力を損なうことなく動作するシステムとなっている。以下、各ブロックについて、64 値＝ (8×8) 値 QAM の場合を例にとって説

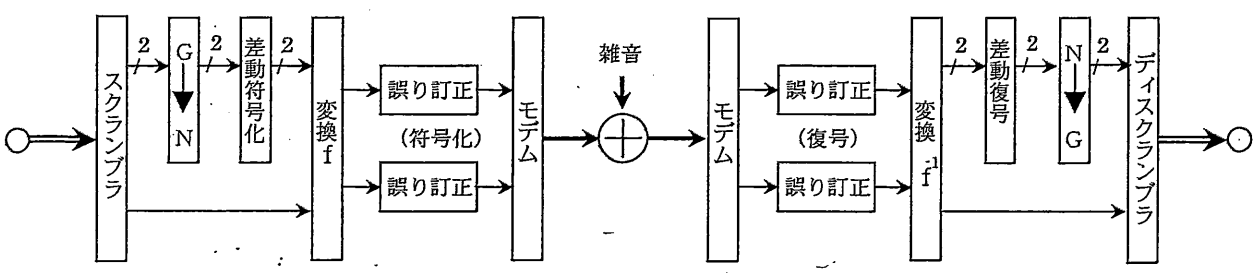

図 4.2: 差動符号化多値 QAM 用誤り訂正符号化システム

明していく。

4.2.1 信号点配置

64 値 QAM の各信号点は、通常 8×8 の各格子点に位置する。4.1.1 節でも述べたように、各信号点は距離的に近い信号点に誤り易い。誤り訂正符号を使うと否とにかかわらず、各信号点のビット表現を定める際には、このことを念頭に置き次の諸点に留意する必要がある。これは，訂正能力以上の誤りが生じた場合のことを考慮しての話である。

(1) 相隣る信号点間のハミング距離（相異なるビット数）をなるべく小さくする。これは、隣接点への誤り確率が大きいことによる。

(2) 原点より遠い相隣る信号点間のハミング距離は，なるべく最小距離 1 とすること。これは，増幅器による非線形歪の影響を少なくするためである。

(3) 差動符号化／復号化に関与するビット数は 2 とする。従って、残りのビット（64 値の場合 $6-2=4$ ビット）は受信時の位相回転に対して不変とすること。これは象限数が $4=2^2$ であり、差動復号によるビット誤りの拡大を最小にするためである。

(4) 差動復号により差動符号化部分の誤りの拡大を防ぐため、象限を越える相隣る信号点間のハミング距離は、なるべく小さくすること。

(5) 平均のビット誤り率が小さくなるようなビット表現にすること。

(6) 信号点のビット表現の定め方は規則的な方が望ましい。解析もし易い。

これらすべての項目を同時に満たすことは難しいが、以上の点を念頭に置いて求めた信号点配置の例を図 4.3 と図 4.4 に示す。なお、図 4.4 の方は 、従来の QAM 方式での信号点配置図としてよく知られている。図 4.3、図 4.4 において、下位 4 ビットは再生搬送波の位相の回

信号点（X，Y）
X：0～3
0＝0 0
1＝0 1
2＝1 1
3＝1 0

Y：0～15
0＝0 0 0 0　8＝1 1 0 0
1＝0 0 0 1　9＝1 1 0 1
2＝0 0 1 1　10＝1 1 1 1
3＝0 0 1 0　11＝1 1 1 0
4＝0 1 1 0　12＝1 0 1 0
5＝0 1 1 1　13＝1 0 1 1
6＝0 1 0 1　14＝1 0 0 1
7＝0 1 0 0　15＝1 0 0 0

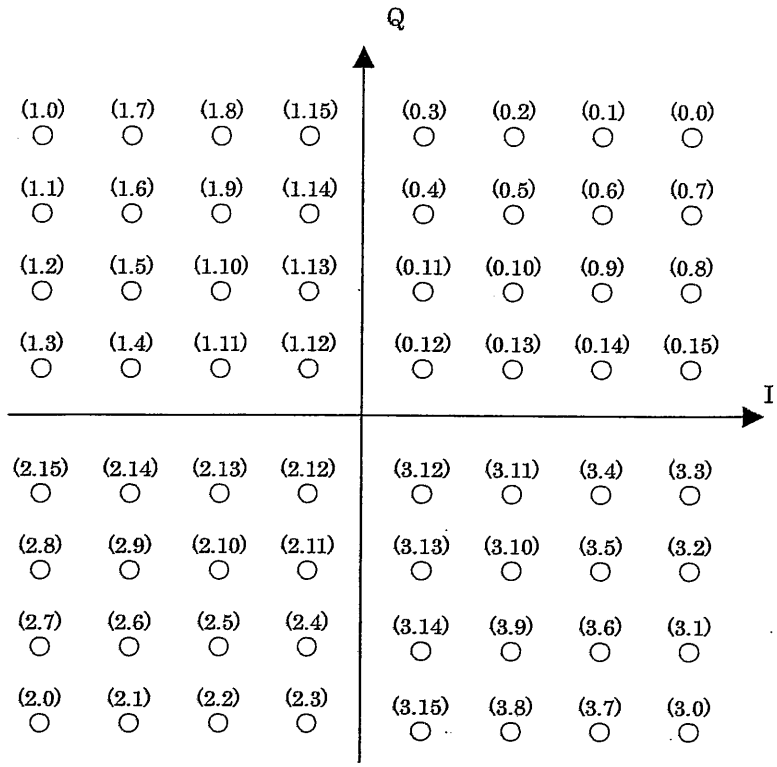

図 4.3: 64 値 QAM 用信号点配置-1

信号点（A.B.C）
A,B,C：0～3
0＝0 0
1＝0 1
2＝1 1
3＝1 0

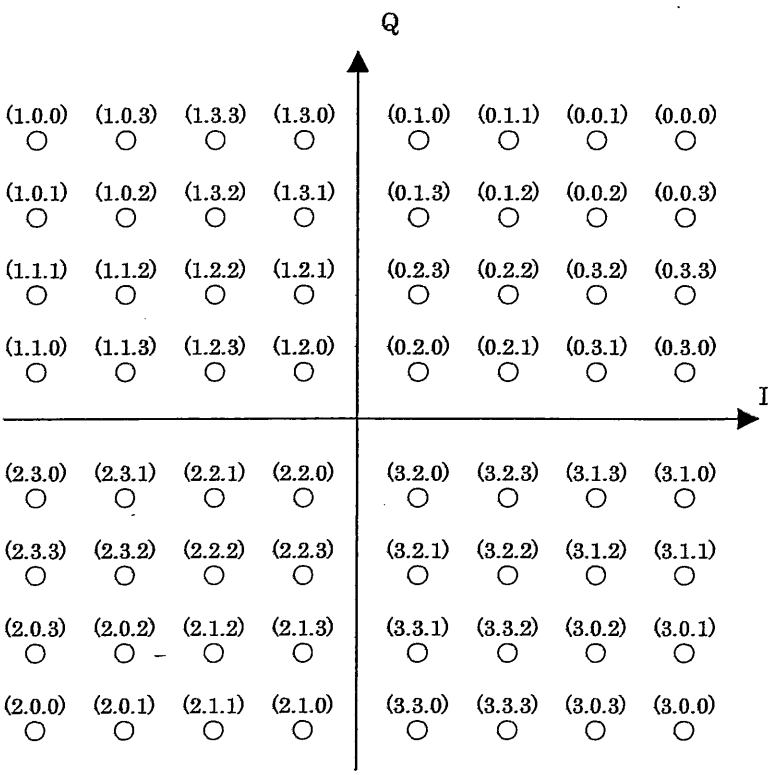

図 4.4: 64 値 QAM 用信号点配置-2

転に対し不変であり、回転対称の構成になっている。また、各信号点を表現する数値は、いわゆるグレイ表現されており、隣接信号点への誤りを極力1ビットに押さえるよう工夫されているが、象限を超える隣接点への誤りがあったとき、下位4ビットに起こる誤りビット数が4となる個所もある。一方、象限内での隣接信号点への誤りは1ビットになるよう押さえられている。どちらの信号点配置を用いても基本的に差はないと考えられる。

4.2.2 スクランブラ，ディスクランブラ

各信号点を表わす 6 ビットの各ラインのビット誤り率を均等化するために、いわゆる PN 系列発生器などを用いてラインの入れ替えを行なうスクランブラ、ディスクランブラを利用する。なお、送信データを擬似的にランダム化することによって、復調を容易にするためにも、スクランブラ、ディスクランブラは用いられる [54]。そのため、もともとモデム内に内蔵してあれば、それを利用することもできる。

4.2.3 差動符号化、復号

4.1.2 節で、多相位相変調方式の場合に即して述べたように、差動符号化・復号により、再生搬送波の位相データの不確定分を取り除くことができる。QAM 方式の場合には、伝送データの各ビットのうち、象限を表わす 2 ビット列を、0〜3 の数値列として、$\{s_i\}$ で表わし、差動符号化された 2 ビット列を $\{d_i\}$ で表わせば、差動符号化は、

$$d_i = d_{i-1} + s_i \pmod 4 \tag{4.5}$$

に従って行われ、復号は、

$$s_i = d_i - d_{i-1} \pmod 4 \tag{4.6}$$

に従って行われる。

図 4.2 における G → N 変換は, 式 (4.5) を通常のナチュラル 4 値表現で計算するための, グレイ・ナチュラル変換を表わす。すなわち、00 → 00, 01 → 01, 11 → 10, 10 → 11 という変換である。N → G 変換はその逆である。

4.2.4 信号点の変換 f とその逆変換 f^{-1}

64 値 QAM の場合、図 4.2 における誤り訂正符号としては、8 値の Lee 距離に基づいた符号を同相側、直交側で用いることになる。この符号の各シンボルは 0 ～ 7 の整数値で表わされ、符号化、復号の演算は 8 を法とした整数演算となる。従って、各信号点は、例えば図 4.5 のように表現されていることが望ましい。図 4.5 において、各信号点の表現を (x, y) とし、x, y のビット表現をナチュラル表現とすれば、この表現は、$-4 \leq x, y \leq 3$ の表現で負の数を 2 の補数で表現しているとみなせる。従ってこれはモデムへの入力信号としても適している。

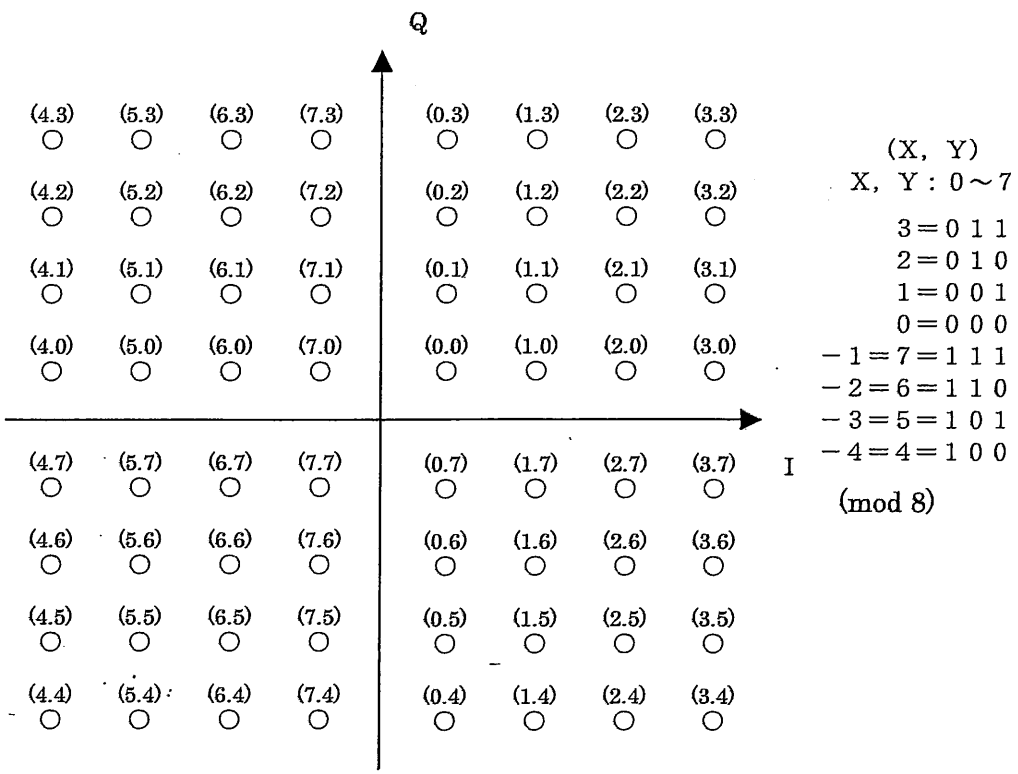

図 4.5: 64 値 QAM 用信号点配置-3

さて、図 4.2 の変換 f、および、その逆変換 f^{-1} は、図 4.3(または図 4.4) の信号点配置の上位 2 ビットをナチュラル表現したものと、図 4.5 の信号点配置-3 の間の変換として定義される。例えば、図 4.6 のような変換となる。

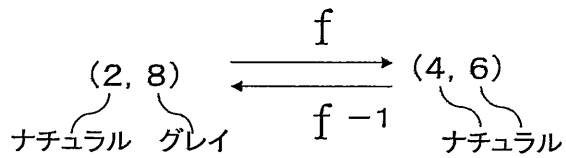

図 4.6: 信号点の変換 f とその逆変換 f^{-1}の一例

4.2.5 多値 transparent 誤り訂正符号

図 4.2 において、誤り訂正符号化および復号は、それぞれ、差動符号化のあとおよび差動復号のまえで行われる。これは、差動復号による誤りの倍化を避けたためである。従って、誤り訂正の復号の段階では、再生搬送波の位相データの不確定分は除去されないままになっている。このような状態でも位相データの不確定分に影響されることなく誤り訂正を正しく実行できる符号が transparent 符号であり、位相の不確定分は誤り訂正復号器をそのまますり抜けて、差動復号器において除去される。

前節において，PSK、あるいは，DPSK 変調方式に対する transparent 符号を定義したが、そのための条件は整数剰余環 Z_q（今の場合，$q = 8$）の上の線形符号で (1, 1, $\cdots$, 1) を正しい符号語としてもつ符号であった。

ここでは前節で示した同一の transparent 符号を同相側、直交側に独立に置くことを提案している。このようにすれば、QAM 方式においても transparent な符号構成となっている。その理由を以下簡単に記しておこう。

図 4.5 において、一つの信号点を (x, y) とし、この信号点がそれぞれ 90°, 180°, 270° 回転したときの信号点を求めると、それぞれ $(7-y, x)$, $(7-x, 7-y)$, $(y, 7-x)$ (mod 8) となる。

ここで、使用する符号が mod 8 の演算に基づいた線形符号であって、かつ、$(1, 1, \cdots, 1)$ を正しい符号語としてもつこと、従って、$(7, 7, \cdots, 7)$ も正しい符号語としてもつこと、および、同相側、直交側で同一の誤り訂正符号を用いていることから、上記 x, y に加えられた誤りは、訂正能力以内の誤りである限り、すべて訂正されることがわかる。ついで、誤りを除去された信号点 (x, y), $(7-y, x)$, $(7-x, 7-y)$ または $(y, 7-x)$ は変換 f^{-1} により、それぞれ、(u, v), $(u+1, v)$, $(u+2, v)$, $(u+3, v)$ （ただし，u に関する加算は mod 4 で考える）で表現される信号点に変化する。u に加算された不確定分 +1, +2, +3 (mod 4) は、差動復号器によって除去される。

なお、このような誤り訂正符号の配置は、バイナリの誤り訂正符号を QPSK 変調方式において transparent な符号として用いる方法 [29] の素直な拡張となっている。

4.2.6 Lee 距離に基づいた符号

図 4.2 における誤り訂正符号としては Lee 距離に基づく q（今の場合，$q = 8$）を法とした、つまり、整数剰余環 Z_q の上の多値誤り訂正符号を使用することを提案した。これは図 4.5 からも分かるように，例えば，最も確率の高い隣接点への誤りは、同相軸あるいは直交軸上における ± 1 (mod 8) の誤りとして、つまり 1 重 Lee 誤りとして表現でき、信号点間の距離と Lee 距離とがうまく整合しているためである。従って、極めて効率的な符号を用いることができると考えられる。

簡単のため、1 重 あるいは 2 重 Lee 誤りを訂正する 8 値の transparent 符号について、そ

表 4.1: Z_8上の transparent Lee 距離符号のパラメータ例

	N	K	K／N
Ⅰ	30	28	0．933
	84	81	0．964
	90	86	0．956
	120	116	0．967
	252	249	0．988
Ⅱ	28	22	0．786
	60	52	0．867
	120	112	0．933
	124	114	0．919
	248	238	0．960
	372	362	0．973
	496	486	0．980

N：符号長　K：情報ディジット数
K/N：符号化率
Ⅰ：1重Lee誤り訂正符号
Ⅱ：2重Lee誤り訂正符号

のパラメータ例を2章の結果より表 4.1 に示す。なお、2章では Z_{2^m} 上の2重 Lee 誤り訂正符号の構成において、符号のチェック行列を構成する剰余類の長さを本来の長さの半分とした。従って、(1, 1, ⋯, 1) を正しい符号語としてもつようにするためには、チェック行列の部分行列 H_{I} に含まれる剰余類の個数 $s(0)$ が偶数となるようなパラメータを持つ符号を選ぶ必要がある。表 4.1 の2重 Lee 誤り訂正符号はこの条件を満たしていることに注意。また表 4.1 には、冗長度がそれほど許されない高密度ディジタルマイクロ波通信や音声回線での高密度データ伝送を念頭において、符号化率 K/N が 0.933 以上となる符号を掲げてある。

4.2.7 符号誤り率特性

本小節では、*Lee* 距離に基づく誤り訂正符号を組み込んだ差動符号化多値 QAM 伝送系に対し、符号誤り率 (Bit Error Rate：BER) 改善特性を算出する式を導く [36][55][56]。符号誤り率は、誤り訂正符号に限らず、一般のデジタル信号の伝送系において、最も重視される評価基準となっている。導く式は伝送系に熱雑音 (加法的白色雑音) が生じたとき符号誤り率はどうなるかという式であり、いくつかの仮定を置いて導いている。実際の BER 改善特性は、変復調系、誤り訂正符号系などを含む全体の伝送系自体の理想的な特性と様々の劣化要因（信号の線形非線形歪み、変復調回路の不完全性）によって決まるが、劣化要因を熱雑音として求めた式は主要な評価尺度である。

以下いくつかのステップを経て符号誤り率に関する式を導くが、容易に導ける式や良く知られている式については説明を略し単に式を掲げるだけにしてある。

（1）2 シンボル間の符号誤り率：

2 つの信号点 A,B 間の距離が $2d$(振幅が$\pm d$) の 2 値信号のガウス雑音による符号誤り率は、つまり A 点から B 点へ（あるいは B 点から A 点へ）誤る確率 P_dは、次式で与えられる。

$$P_d = \int_0^\infty \frac{1}{\sqrt{2\pi}} e^{-(x+d)^2/2\sigma^2} \tag{4.7}$$

$$= \frac{1}{2}\,\mathrm{erfc}(\sqrt{\mathrm{d}^2/2\sigma^2}) \tag{4.8}$$

$$\text{但し、} \quad \mathrm{erfc(x)} = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2}\,dt \tag{4.9}$$

（2）多値 QAM 伝送系でのシンボル誤り率：

$M\,(=(2n)^2)$ 値 QAM 伝送系におけるシンボル誤り率 P_Sは次式で近似できる。

$$P_S = \frac{2(2n-1)}{n} P_d \tag{4.10}$$

式 (4.10) は、以下のようにして導ける。まず、シンボル誤りとしては、支配的な隣の信号点

への誤りのみを仮定する。更に多値 QAM の信号点配置図において、4 隅の信号点は 2 方向にしか誤らないこと、辺上の 4 隅以外の信号点は 3 方向にしか誤らないこと、残りの内部の信号点は 4 方向へ誤る可能性があることを考慮に入れると次式が成立する。次式より、式 (4.10) は容易に導ける。

$$P_S = \frac{1}{(2n)^2}(4 \times 2P_d + 4(2n-2) \times 3P_d + (2n-2)^2 \times 4P_d) \tag{4.11}$$

（3）多値 QAM 伝送系での平均信号電力と搬送波の平均電力：

$M\,(=(2n)^2)$ 値 QAM 伝送系における信号ベクトル長の 2 乗平均値 S は次式で与えられる。これは直接計算すれば容易に得られる。

$$S = \frac{2}{3}(M-1)d^2 \tag{4.12}$$

また搬送波の平均電力を C とすれば、次式が成り立つ（簡単のため、無変調波で考える）。

$$C = \frac{1}{2}S \tag{4.13}$$

（4）多値 QAM 伝送系でのシンボル誤り率と C/N との関係：

$M\,(=(2n)^2)$ 値 QAM 伝送系におけるシンボル誤り率 P_Sは、式 (4.8)、式 (4.10)、式 (4.12) および式 (4.13) より、次式で近似できる。(C/N：Carrier to Noise Ratio)

$$P_S = \frac{2n-1}{n}\mathrm{erfc}\,(\sqrt{\mathrm{d}^2/2\sigma^2}) = \frac{2(\mathrm{2n}-1)}{\mathrm{n}} \cdot \frac{1}{2}\mathrm{erfc}\,(\sqrt{\frac{3}{2(\mathrm{M}-1)}\mathrm{C/N}}) \tag{4.14}$$

以下説明の都合上、$M = 64$ (従って $n = 4$) として、64 値 QAM 伝送系において考える。

（5）シンボル誤り率とビット誤り率との関係：

シンボル誤り率 P_Sとビット誤り率 P_bとの間に次式が成り立つ。但し信号点配置図は、図 4.4

で示した回転対称の信号点配置図を用いるものとする。

$$P_b = \frac{5}{21}P_S \tag{4.15}$$

式 (4.15) を導くためには若干の説明を要する。まず、図 4.4 の信号点配置図において、信号点 (A,B,C) を $((A_1,A_2),(B_1,B_2),(C_1,C_2))$ として表す。同相軸に写像したシンボルのビット表現を (A_1,B_1,C_1)、直交軸に写像したシンボルのビット表現を (A_2,B_2,C_2) とし、それぞれのビット誤り率を p_1、p_2、p_3；q_1、q_2、q_3とする。図 4.4 の信号点配置図に注意して、各シンボル誤りをビット単位に見て、どんなビット誤り率に影響を与えるかに着目すれば、次式が導ける。

$$p_1 = q_1 = \frac{4\times 4}{64}P_d = \frac{1}{4}P_d \quad (\text{差動変換後は}\frac{2}{4}P_d) \tag{4.16}$$

$$p_2 = q_2 = \frac{8\times 4+2\times 2\times 4}{64}P_d = \frac{3}{4}P_d \tag{4.17}$$

$$p_3 = q_3 = \frac{16\times 4+2\times 2\times 4}{64}P_d = \frac{5}{4}P_d \tag{4.18}$$

従って、これらの式と $n = 4$ と置いた式 (4.10) から、次式が成立する。

$$p_1 = q_1 = \frac{1}{14}P_S \quad (\text{差動変換後は} \quad \frac{2}{14}P_S) \tag{4.19}$$

$$p_2 = q_2 = \frac{3}{14}P_S \tag{4.20}$$

$$p_3 = q_3 = \frac{5}{14}P_S \tag{4.21}$$

式 (4.15) は、これらの式 (4.19)〜式 (4.21) の平均をとれば求められる。

（6）誤り訂正符号による BER 改善効果：

受信シンボルの同相成分、直交成分の誤り率をそれぞれ P_I、P_Qとすれば、次式が成り立つ。

$$P_I = P_Q = P_S/2 \tag{4.22}$$

同相軸、直交軸で、それぞれ独立に誤り訂正を施していることから、誤り訂正処理後の受信シンボルの同相成分、直交成分の誤り率をそれぞれ P_I'、P_Q'とすれば、次の近似式が成り立つ。

1 重誤り訂正符号の場合と 2 重誤り訂正符号の場合を分けて記す。

(6-1) 1 重 Lee 誤り訂正符号の場合：

$$P_I' = A_1 \cdot P_I^2 (1-P_I)^{N-2} \approx A_1 \cdot P_I^2 \tag{4.23}$$

$$P_Q' = A_1 \cdot P_Q^2 (1-P_Q)^{N-2} \approx A_1 \cdot P_Q^2 \tag{4.24}$$

但し、

$$A_1 = \frac{3}{N} {}_N C_2 \qquad (N \text{ は符号長}) \tag{4.25}$$

上の式 (4.25) では、訂正能力以上の誤りが生じた場合には、誤った訂正により誤りが 1 つ付加されると仮定している。

ここで、誤り訂正処理後のシンボル誤り率を P_S' とすれば、式 (4.22)〜式 (4.25) より次式が成立する。

$$P_S' \approx \frac{1}{2} A_1 P_S^2 \tag{4.26}$$

また、誤り訂正処理後の受信シンボルの同相成分および直交成分に関し、各構成ビットの誤り率をそれぞれ p_1', p_2', p_3' ; q_1', q_2', q_3' とする。このとき、式 (4.19)〜式 (4.21) および上の式 (4.26) より、以下の式が導ける。

$$p_1' = q_1' \approx \frac{1}{14} \cdot \frac{1}{2} A_1 P_S^2 = \frac{1}{28} A_1 P_S^2 \qquad (\text{差動変換後は} \frac{2}{28} A_1 P_S^2) \tag{4.27}$$

$$p_2' = q_2' \approx \frac{3}{14} \cdot \frac{1}{2} A_1 P_S^2 = \frac{3}{28} A_1 P_S^2 \tag{4.28}$$

$$p_3' = q_3' \approx \frac{5}{14} \cdot \frac{1}{2} A_1 P_S^2 = \frac{5}{28} A_1 P_S^2 \tag{4.29}$$

従って、誤り訂正処理後のビット誤り率を P_b' とすれば、P_b' は上の 3 式を平均することによって、次式で与えられる。

$$P_b' \approx \frac{5}{42} A_1 P_S^2 \tag{4.30}$$

また、訂正前後の BER の関係としてみるときには、上式に式 (4.15) を代入して、次式を得る。

$$P_b' \approx 2.1 A_1 P_b^2 \tag{4.31}$$

例えば、$N = 84$ のとき、

$$P_b' = 2.61 * 10^2 \cdot P_b^2 \tag{4.32}$$

(6-2) 2 重 Lee 誤り訂正符号の場合：

$$P_I' = A_2 \cdot P_I^3 (1 - P_I)^{N-3} \approx A_2 \cdot P_I^3 \tag{4.33}$$

$$P_Q' = A_2 \cdot P_Q^3 (1 - P_Q)^{N-3} \approx A_2 \cdot P_Q^3 \tag{4.34}$$

但し、

$$A_2 = \frac{5}{N} {}_N C_3 \quad (N \text{ は符号長}) \tag{4.35}$$

上の式では、訂正能力以上の誤りが生じた場合には、誤った訂正により、誤りが 2 つ付加されると仮定している。

ここで、誤り訂正処理後のシンボル誤り率を P_S' とすれば、式 (4.22) および式 (4.33)～式 (4.35) より次式が成立する。

$$P_S' \approx \frac{1}{4} A_2 P_S^3 \tag{4.36}$$

また、誤り訂正処理後の受信シンボルの同相成分および直交成分に関し、各構成ビットの誤り率をそれぞれ p_1', p_2', p_3' ; q_1', q_2', q_3' とする。このとき、式 (4.19)～式 (4.21) および上の式 (4.36) より、以下の式が導ける。

$$p_1' = q_1' \approx \frac{1}{14} \cdot \frac{1}{4} A_2 P_S^3 = \frac{1}{56} A_1 P_S^3 \qquad (\text{差動変換後は} \frac{2}{56} A_1 P_S^3) \tag{4.37}$$

$$p_2' = q_2' \approx \frac{3}{14} \cdot \frac{1}{4} A_2 P_S^3 = \frac{3}{56} A_1 P_S^3 \tag{4.38}$$

$$p_3' = q_3' \approx \frac{5}{14} \cdot \frac{1}{4} A_2 P_S^3 = \frac{5}{56} A_2 P_S^3 \tag{4.39}$$

従って、誤り訂正処理後のビット誤り率を P_b' とすれば、P_b' は上の 3 式を平均することによって、次式で与えられる。

$$P_b' \approx \frac{5}{84} A_2 P_S^3 \tag{4.40}$$

また、訂正前後の BER の関係としてみるときには、上式に式 (4.15) を代入して、次式を得る。

$$P_b' \approx 4.41 A_2 P_b^3 \tag{4.41}$$

例えば、$N = 372$ のとき、

$$P_b' = 5.04 * 10^5 \cdot P_b^3 \tag{4.42}$$

式（4.32）および式（4.42）に基づいて、差動符号化 64 値 QAM 伝送系に 1 重 Lee 誤り訂正 (84,81) 符号および 2 重 Lee 誤り訂正 (372,362) 符号をそれぞれ適用したときの、各 BER 改善特性を図 4.7 に示す。また、図 4.8 に、この両符号それぞれを現実の差動符号化 64 値 QAM 伝送系に適用したときの BER 改善特性 (対C／N特性) を示す。図 4.8 では、実測値と計算値の両方で示す。ここで、実測値とは、C／N値を定めて誤り訂正符号装置系を ON にしたときの BER の実測値である。また計算値とは、C／N値を定めて誤り訂正符号装置系（差動符号装置系を含む）を OFF にした時の BER の実測値を式（4.32）および式（4.42）での訂正前ビット誤り率 P_b として、訂正後のビット誤り率 P_b' を計算した値である。図より、訂正後のビット誤り率 P_b' の実測値と計算値は殆ど一致しており、本節での評価手法が有効であることが分かる。また、BER 値 10^{-6} での符号化利得 (Coding Gain) は、1 重 Lee 誤り訂正 (84,81) 符号で約 3dB、2 重 Lee 誤り訂正 (372,362) 符号で約 3.4dB あり、良好な特性を持つ符号であることも分かる。

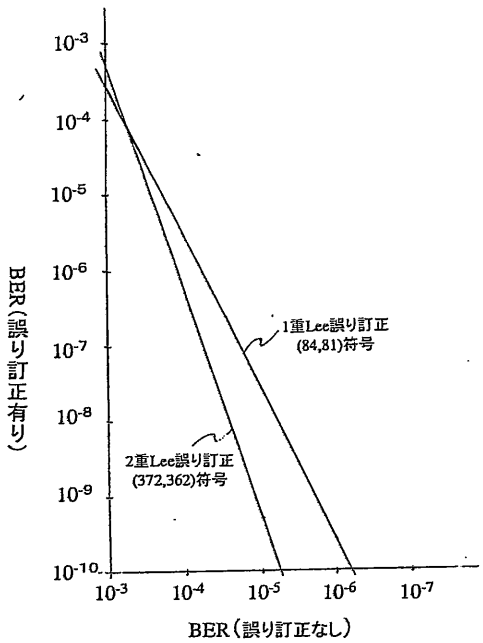

図 4.7: 1 重 Lee 誤り訂正符号／2 重 Lee 誤り訂正符号の BER 改善特性例

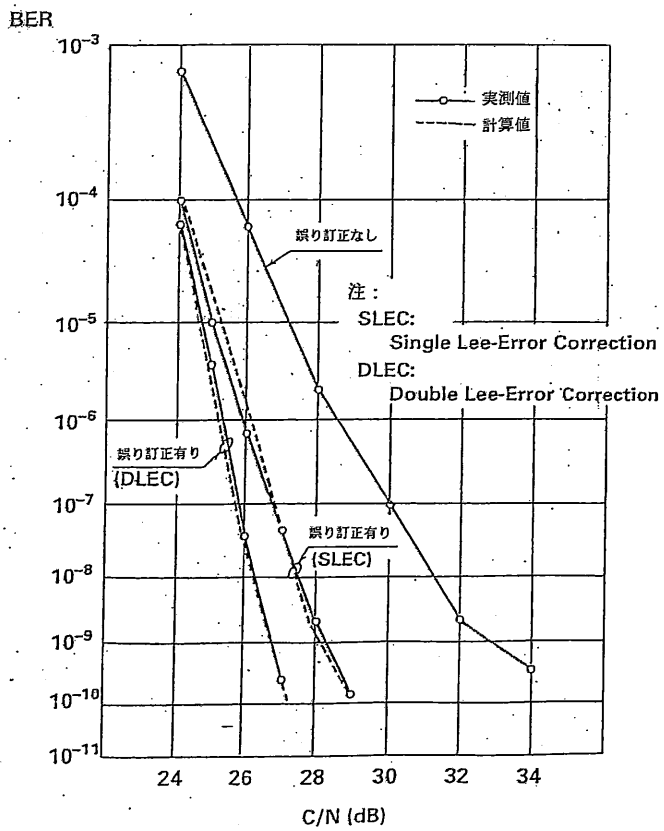

図 4.8: 1 重 Lee 誤り訂正符号／2 重 Lee 誤り訂正符号の BER 改善特性例
—対 C／N 特性—

4.3 電力有効利用の Stepped 多値 QAM 方式に適した符号系の構成

本節では、Square 多値 QAM 方式の信号点の位置を一部変更し、波形歪みを軽減する Stepped 多値 QAM 方式に適した誤り訂正方式について述べる [49]Square 多値 QAM 方式は、信号点を正方格子状に配置した通常の多値 QAM 方式である。変調信号の振幅は位相平面上の原点から信号点までの距離に比例するので、Square 多値 QAM 方式では正方格子の 4 隅の信号点で振幅が最大になる。そこで、4 隅の近傍のいくつかの信号点の位置を変更して信号点群の最外側の点を円形に近くなるように配置した Stepped 多値 QAM 方式を採用することも多い。Stepped 多値 QAM 方式では、変調信号の最大振幅が Square 多値 QAM 方式におけるよりも小さくなるので、伝送路で受ける振幅に依存する歪みが小さいという利点がある。さらに平均信号電力も小さくなる。

図 4.9 に、一例として $2^4 \times 2^4$ の Square 多値 QAM 方式の信号点配置図を示す。また、それを Stepped 多値 QAM 方式に変換した時の信号点配置図を図 4.10 に示す。図 4.9 における 4 隅近傍の黒丸の点が、図 4.10 に示すように近くの辺沿いの黒丸の点に移動し、信号点全体が円に近く、平均信号電力も小さい形になっている。

図 4.9 において、各信号点の座標は同相軸上の座標 I および直交軸上の座標 Q ともに 0〜15 の数字で表してある。また図 4.10 においては、同相軸上の座標 I および直交軸上の座標 Q をともに、(A,b) の形で表し、A は 0〜15 の数字で、図 4.9 に比べ 4 だけ巡回シフトした形で表し、b は黒丸の点のとき 1、白丸の点のとき 0 として表している。

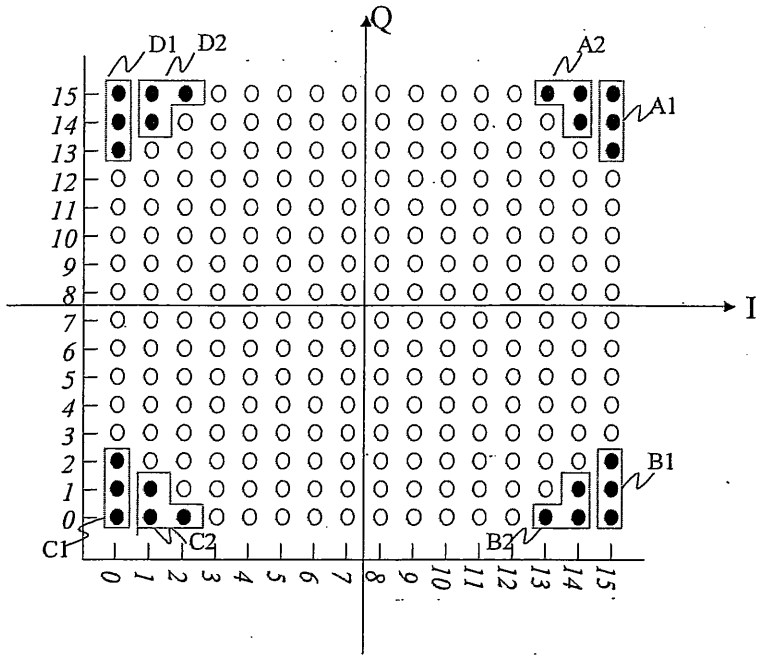

図 4.9: $2^4 \times 2^4$Square 多値 QAM 信号点配置図

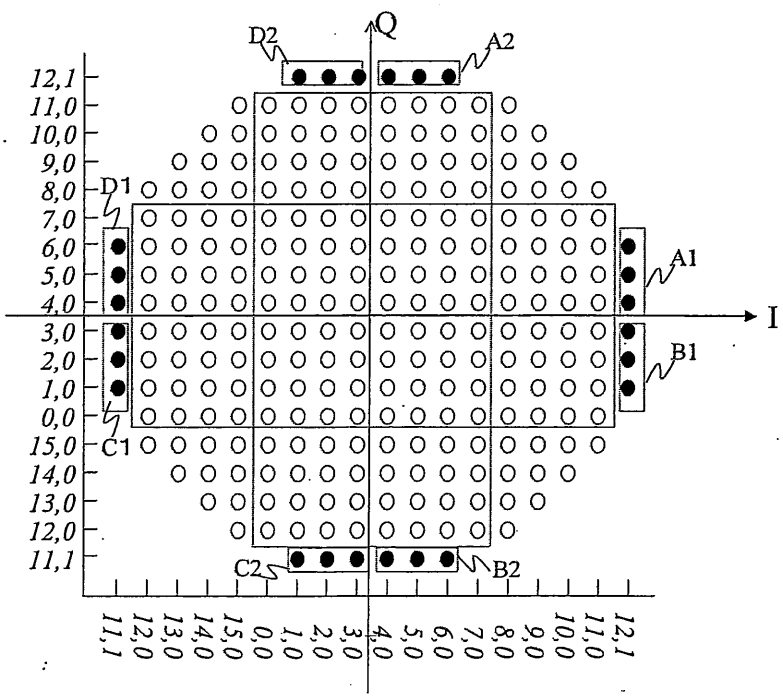

図 4.10: 256 Stepped 多値 QAM 信号点配置図

さて、図 4.10 の信号点配置図が用いられるとして、同相軸、直交軸それぞれに Z_{24} 上の Lee 距離に基づく誤り訂正符号を採用するとした場合、次のような問題点が発生する。

● 誤り訂正符号としては、あくまでも Square 多値 QAM での信号点配置として、情報シンボルと冗長シンボルの間は関係づけられる。従って、情報シンボルだけは、図 4.10 の信号点配置図の上で表現したとしても、冗長シンボルは、図 4.9 の Square 多値 QAM での信号点として計算されてくる。従って図 4.10 の信号点配置図にない、図 4.9 の黒丸の点として計算されてくる場合も起こりうる。その場合、その黒丸の点の座標を無理に図 4.10 の黒丸の点の座標に写像した状態で誤り訂正符号として処理すると、誤り訂正符号の距離構造が変わっているため、写像したシンボルに誤りが生じた場合には、誤り訂正処理に支障をきたす。誤った訂正処理を起こしかねない。そのため、符号化によって生成される冗長シンボルも、図 4.10 の Stepped 多値 QAM での信号点として表現できるようにしたい。

本節では、この問題を解決するための方式について述べる。そのために用いたアイデアのポイントは、2.6 節の図 2.4 で示した手法の利用である。すなわち、同相軸、直交軸それぞれに Z_{2^3} 上の *Lee* 距離に基づく誤り訂正符号を採用し、誤り訂正符号化の処理は、同相軸、直交軸それぞれ 4 本のラインのうちの各 3 本のラインに対してそれぞれ施す。復号においては、Z_{2^3} 上での復号処理の結果得られた±1 あるいは±2 の訂正信号を、各 4 本のライン全体に対してそれぞれ作用させる。その際の∓1 あるいは∓2 の演算は、Z_{24} 上でおこなう。

さて、このような方式を取った場合に、(誤り訂正符号化に使わなかった残りのラインのビットも含めて) 4 ビットとしてみた冗長シンボルが図 4.10 の Stepped 多値 QAM での信号点として表現できるか否かは、各残りの 1 本のラインの利用の仕方に依存する。例えば、表現

できるための十分条件として、各残りの1本のラインを高位の MSD ビットのラインと考えたとき、同相軸の残りの1本も、直交軸の残りの1本も、両方とも同時に値1をとらないこととという条件が考えられる。言い換えれば、どちらか一方の残りのラインを0にすることである。このとき、4ビットとしてみた冗長シンボルは、図 4.10 の縦長または横長の長方形のどちらかの中に含まれる信号点として計算されてくる。この条件を裏返して言えば、冗長シンボルの残りの1ビットを載せたラインは、同相軸、直交軸の各残りの1本のラインを例えば時間的に交互に使用することによって、制御信号など付加情報ビットを載せたラインとして利用できることを意味する。このとき、交互に使用する際の他方の軸のラインのビットは0にしておく。なお、交互に利用するのは、ビットバランスを考えてのことでそれ以上の意味はない。

以上の考え方に従って構成した、送信側、受信側の符号処理系のブロック図をそれぞれ図 4.11 および図 4.12 に示す。説明の都合上、以下の説明は図 4.10 での信号点を想定して行うが、信号点数の異なる場合にも一般化できる。まず送信側の符号処理系の図 4.11 において、Square 多値 QAM における同相軸、直交軸の各 (4 ビットの) シンボル列とみなされた情報シンボル列が信号線 1 と 2 から入力され、符号変換器で図 4.10 における信号点の列にそれぞれマップされる。マップ後の各値 (A,b) は、それぞれ信号線 11 と 21、および信号線 12 と 22 に得られる。値 b が黒丸の信号点か否かを示す。信号線 11 と 12 を流れる各情報シンボル (4 ビット) 列の一部 (3 ビット) がそれぞれ誤り訂正演算回路に送られ、冗長シンボル (3 ビット) の列が信号線 31 および 32 に得られる。冗長シンボルに与える付加ビット (4 ビット目) の値はそれぞれ信号線 41 と 42 から与える。上で述べたように、同時に値1を取らないように制御しさえすれば、この信号線 41、42 を用いて付加情報を送ることができる。情報シンボル列と冗長シンボル列が多重化回路で時間的に多重化され、送るシンボル列 (A,b) が信号線 51 と 61 および信号線 52 と 62 に得られ、変調器で送信信号に変換されて伝送路へ送り出される。

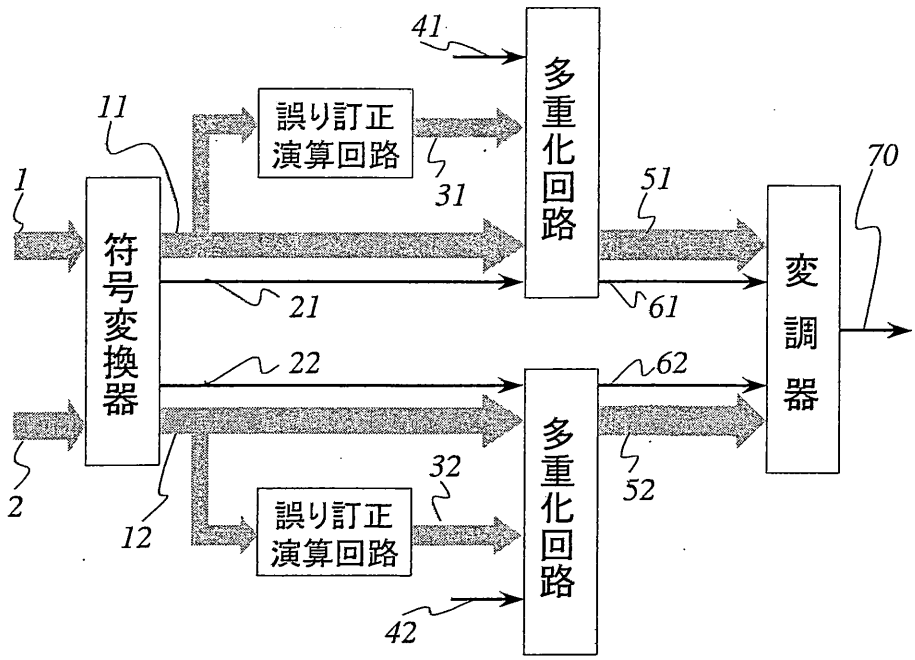

図 4.10: 256 Stepped 多値 QAM 送信側符号処理系

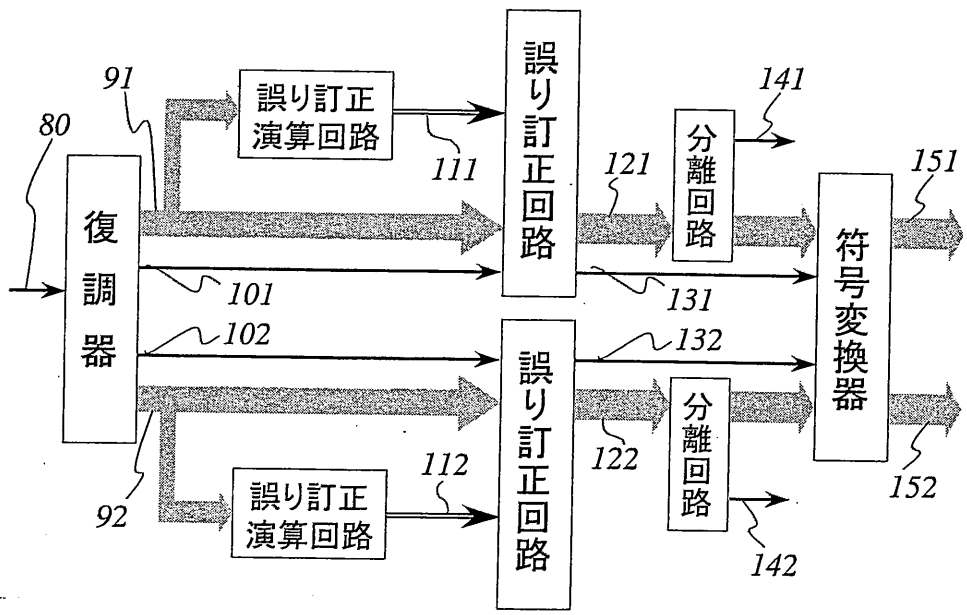

図 4.11: 256 Stepped 多値 QAM 受信側符号処理系

一方、受信側の符号処理系の図 4.11 では、信号線 80 において受信した信号が復調器で、図 4.9 における信号点を示すシンボル列に変換される。シンボル列はそれぞれ信号線 91 と 101 および信号線 92 と 102 に得られる。信号線 91 と 92 の各情報シンボル (4 ビット) 列の一部 (3 ビット) がそれぞれ誤り訂正演算回路に送られ、誤り訂正信号（誤り位置と誤り値 (± 1 または ± 2) の情報を含む）が信号線 111 と 112 に得られる。誤り訂正信号をもとに誤り訂正回路で、各シンボル全体 (4 ビット) に含まれる誤りとして、誤りが訂正 (∓ 1 または ∓ 2 加算 (mod 2^4)) される。訂正後のシンボル列が、信号線 121 と 131 および信号線 122 と 132 に得られる。冗長シンボルに含まれる付加情報は分離回路で取り出され、信号線 141 あるいは 142 に得られる。情報シンボル列は符号変換器で変換され、送られた情報シンボル列として信号線 151、152 に得られる。

第5章　結　論

本論文では、整数剰余環 Z_q 上のLee距離に基づく誤り訂正符号を導き、特に1重Lee誤り訂正符号、準2重Lee誤り訂正符号、および2重Lee誤り訂正符号について、それぞれの具体的な構成法並びに復号法を明らかにした。その際、整数剰余環 Z_q 上の線形フィードバックシフトレジスタの性質について解析し、その結果を拡大環での剰余類を用いた表現法につなげ、それをベースに環 Z_q 上のLee距離に基づく誤り訂正符号を導いた。得られた符号は巡回符号ではないが、巡回符号の概念を拡張した形の符号となっている。符号語間の距離としてLee距離を採用したのは、高密度の信号空間への適用を考慮してのことである。　次に、この符号を現実の回路としてインプリメントするための手法を与え、符号器・復号器の構成法を導いた。そこでは、上で述べた環 Z_q 上の線形フィードバックシフトレジスタの性質と具体的な符号の構成法に従って、符号器・復号器が線形フィードバックシフトレジスタを用いた自然な形の手法に基づいて構成できることを示した。またBCH符号など有限体上の符号をインプリメントする場合との違いに重点を置いて述べた。また高速化の観点からその並列処理法についても論じた。更に、実際に開発し実用に供した2重Lee誤り訂正符号のLSIについても紹介した。

更に、得られた符号を用いて高密度の信号空間における効率的な符号系の構成法を提示した。具体的には差動符号化多値QAM(Quadrature Amplitude Modulation ; 直交振幅変調)方式を採用している大容量のデジタルマイクロ波無線通信システムへの適用を示した。そこでは、差動符号化と誤り訂正の位置づけ、符号ビットの割り当て、システム構成、更には、電

力有効利用の観点から、信号点配置を原点の周りに円形上に取ったときの誤り訂正符号の巧妙な構成法といった様々な手法を導いた。そして符号化率、符号化利得 (Coding Gain) および装置規模などの観点から、その符号系の良好な特性も提示した。そのことによって、有限体に限らず、有限環の上でも実用的でかつメリットのある符号系を構成できることを示した。このことは現実のシステムに導入する符号系の選択肢が本論文によって更に広がったことを示している。

次に今後の展望として、以下２つの側面から述べる。

まず、整数剰余環上の Lee 距離に基づく誤り訂正符号そのものに関して述べる。本論文で導いた整数剰余環上の Lee 距離に基づく誤り訂正符号には、まだまだ未知な面が多い。有限体上の符号と異なり、割り算が一般にはできないことや、加算演算における桁上がりという非線形の現象が、符号構成上のいろいろな見通しをさまたげている。2.8 節でも述べたように、一般の t 重 Lee 誤り訂正符号としての最適符号を如何に構成するかは、これからの研究に委ねられている。それは恐らく、符号パラメータを限定した中での一般化がしばらく続いて、そのデータの蓄積を経たのちに、何がしかのアイデアによって更なる前進があるものと思われる。例えば多段符号化の概念の援用や最近研究が進んでいる環 Z_4 の上の線形符号と有限体上の従来の非線形符号との関係からの切り込みといった方向も考えられる。

次に、高密度の信号空間における符号という観点から述べる。本論文では、得られた整数剰余環上の符号を用いて高密度の信号空間における効率的な符号系の構成法を提示した。差動符号化多値 QAM 方式を採用している大容量のデジタルマイクロ波無線通信システムへの適用である。このシステムへ適用する符号としてはその後、冗長な信号点を時間軸上ではなく、信号空間の中で増やすことによって（信号点間の距離は小さくなるが）帯域拡大を伴わずに信号点の誤りを訂正するトレリス符号化変調、あるいはその変形として帯域拡大を許し、信

号点間の距離を変えないトレリス符号化変調の適用といった方法も有力な方法として採用されている [57]。またブロック符号として Reed Solomon 符号も有力な符号として報告されている [44]。Lee 距離符号の変形ないし拡張もまだまだこれから有り得ると考えられ、DMR 用の符号の選択肢は大きな広がりをみせている。その選択には、対象とするシステムが、符号化率、符号長、符号化利得、装置規模等々で何に重きを置くかに大きく依存する。同一種類の符号でも、重きを置く評価項目で選択する符号のパラメータは変わる。そのため、すべての評価項目において決定的な差がでない限り、これからも選択肢を多く残したまま、現実に適用される符号の開発競争は進むと考えられる。それがまた新たな適用対象を生み新たな地平を開くことにもつながる。

参考文献

[1] C.E.Shannon, " A Mathematical Theory of Communication ", B.S.T.J., Vol.27, pp.379-423, pp.623-656, 1948

[2] W.W. Peterson and E.J.Weldon, 「Error Correcting Codes」, Second Edition, Chapter7, pp.170-205, The MIT Press, Cambridge, Mass., 1972

[3] E. R. Berlekamp, 「Algebraic Coding Theory」, McGraw–Hill Book Co., New York, pp.207-217,1968

[4] 今井, 「符号理論」, 電子情報通信学会, 1990

[5] 今井, "符号理論の応用", 電子情報通信学会誌, Vol.81, No.10, pp.1015-1017, 1998

[6] M. Hall, " An isomorphism between linear recurring sequences and algebraic rings ", Trans. AMS, Vol.40, pp.196-218, 1938

[7] I. F. Blake, " Codes Over Certain Rings ", Information and Control 20, pp.396-404, 1972

[8] I. F. Blake, " Codes Over Integer Residue Rings ", Information and Control 29, pp.295-300, 1975

[9] E. Spiegel, " Codes over Z_m ", Information and Control 35, pp.48-51, 1977

[10] E. Spiegel, " Codes over Z_m, Revisited ", Information and Control 37, pp.100-104, 1978

[11] P. Shankar, " On BCH Codes over Arbitrary Integer Rings ", IEEE Trans. IT., Vol. IT- 25, No.4, pp.480-483, 1979

[12] 宮川, 原島, 金子, "リー誤り訂正符号の一構成法", 電子通信学会全国大会, No.1111, 1975

[13] A. R. Hammons, Jr., P. V. Kumar, A. R Calderbank et al., "The Z_4-Linearity of Kerdock, Preparata, Goethals, and Related Codes ", IEEE Trans. Information Theory, Vol.40, No.2, pp.301-319, 1994

[14] J.C.Interlando et al., " On the decoding of Reed-Solomon and BCH Codes over Integer Residue Rings ", IEEE Trans., IT., Vol.43, No.3, pp.1013-1021, 1997

[15] 中村, " 差動符号化を併用する誤り訂正符号の一構成法 ", 電子通信学会部門別全国大会予稿集, No.13, 1976

[16] 中村, " 差動符号化に適した誤り訂正符号の一理論 ", 電子通信学会総合全国大会予稿集, No.S9–5, 1977

[17] 中村,“Z_{2^m}の上のリー誤り訂正符号の一クラスについて”, 電子通信学会オートマトンと言語研究会, AL.77-51, pp.27-36, 1977

[18] 中村,“Z_qの上の線形フィードバックシフトレジスタについて”, 京都大学数理解析研究所講究録, 組合せ構造とグラフ理論 II, pp.221-235, 1978

[19] K. Nakamura,“A class of error correcting codes for DPSK channels”, Proc. of Int. Conference on Communications (ICC'79), pp.45.4.1-45.4.5, 1979

[20] 中村,“整数剰余環 Z_q の上の線形 Lee 誤り訂正符号とその応用”, 第 2 回情報理論とその応用シンポジウム (SITA'79) 予稿集, pp.59–68, 1979

[21] 中村,“整数剰余環 Z_{2^m}の上の最大周期多項式について”, 第 6 回情報理論とその応用シンポジウム (SITA'83) 予稿集, pp.194-197, 1983

[22] K. Nakamura,“On double Lee-error correction scheme for codes over integer residue ring Z_{2^m}”, Proc. of 1988 Int. Symposium on Information Theory (ISIT'88), p.79, 1988

[23] 中村, 野田,“整数剰余環 Z_{2^m}の上のリー距離に基づく 2 重誤り訂正符号とその応用”, 第 11 回情報理論とその応用シンポジウム (SITA'88) 予稿集, pp.129-130, 1988

[24] S. W. Golomb,「Shift Register Sequences」,Part I, II, pp.1-108, Holden Day Inc., San Francisco, 1967

[25] 今井, 片岡, 宮川,“多段符号化の理論と多相位相変調通信方式への応用”, 電子通信学会論文誌 A, 54-A, No.11, pp.597-604, 1971

[26] 宮川, 岩垂, 今井,「符号理論」, pp.112-137, pp.527-567, 昭晃堂, 1973

[27] 吉井, 金子,“Z_{2^m} 上の t 重リー誤り訂正符号”, 第 9 回情報理論とその応用シンポジウム (SITA'86) 予稿集, pp.99-104, 1986

[28] 井上, 金子,“整数環 Z_{2^m} 上のリー誤り訂正符号について”, 第 11 回情報理論とその応用シンポジウム (SITA'88) 予稿集, pp.131-136, 1988

[29] G. D. Forney and E. D. Bower,“A High-Speed Sequential Decoder: Prototype Design and Test”, IEEE Trans. COM, Vol.COM-19, No.5, pp.821–835, Oct., 1971

[30] 中村,“64 値 QAM 用誤り訂正符号化方式”, 社内技術レポート, TR-KN-47, 1982

[31] 中村,“差動多値 QAM 用誤り訂正符号化システム”, 第 5 回情報理論とその応用シンポジウム (SITA'82) 予稿集, pp.49-52, 1982

[32] K. Nakamura, "Error correction coding to multi-level QAM signal based on the Lee metric", Proc. of 1983 Int. Symposium on Information Theory (ISIT'83), p.79, 1983

[33] T. Noguchi et al. and K. Nakamura, "6GHz 135Mbps Digital Radio System With 64 QAM Modulation", Proc. of Int. Conference on Communications (ICC'83), pp.F2.4.1-F2.4.6, 1983

[34] Y. Yoshida, M. Tahara, T. Ryu, "6GHz 140Mbps Digital Radio Repeater with 256QAM Modulation", Proc. of Int. Conference on Communications (ICC'86), pp.46.7.1-46.7.5, 1986.

[35] 野田, 中村, 他, "デジタル無線通信用2重誤り訂正リー距離符号LSIの開発", 電子情報通信学会春季全国大会, B-924, 1989

[36] K. Nakamura, S. Noda, "Forward Error Correction Scheme with Lee-Metric Codes for Multi-Level QAM Systems", Proc. of Int. Microwave Symposium at Brazil, 1989

[37] Y.Nakamura, Y. Saito and S. Aikawa, "256 QAM Modem for Multicarrier 400 Mbit/s Digital Radio", IEEE J. of Selected Areas in Communications, Vol. SAC-5, No.3, pp.329-335, 1987

[38] H.Ichikawa et al., "Digital Radio System Design with the Network Node Interface", Proc. of International Conference on Communication(ICC'89), 42.4.1-42.4.6, pp.1297-1302, 1989

[39] S.Noda, "Digital Microwave Radio Systems in SDH Network", Proc. of Forum'91(in Telecom'91), pp.159-163, 1991

[40] NEC技報「新同期端局システム特集」, vol.44, No.1, 1991

[41] E.Fukuda et al., "A 256 QAM Digital Radio System with a low rolloff factor of 20% for attaining 6.75 bps/Hz", Proc. of International Conference on Communication(ICC'87), 52.2.1-52.2.5, pp.1798-1802, 1987

[42] Bates,et.al., "Digital Radio Technology in the AT& T Network", Proc. of International Conference on Communication(ICC'87), 19B.6.2-6.7, 1987

[43] S.Bellini et al., "Coding for Error Correction in High Capacity Digital Radio", ECRR, pp.166-172, 1986

[44] 児玉、中村 (誠), "差動符号化多値QAM通信における誤り訂正方式の構成法", 電子情報通信学会論文誌A, Vol.J73-A, No.2, pp.322-330, 1990

[45] 児玉,“誤り訂正・検出回路の並列化技術とその応用に関する研究”, 学位論文 (早稲田大学), 1999

[46] 中村,“誤り訂正多値符号化復号化装置”, 特許公報 (B2), 特公平 6-42682, 1994.6.1 公告

[47] 中村,“誤り訂正符号化および復号化システム”, 特許公報 (B2), 昭 58-50463, 1983.11.10 公告

[48] 中村,“２重誤り訂正装置”, 特許公報 (B2), 昭 62-43371, 1987.9.14 公告

[49] 中村, 野田,“符号誤り訂正装置”, 特許公報 (B2), 特公平 7-71117, 1995.7.31 公告

[50] A. M. Patel et al.,“Syndrome trapping technique for fast double error correction”, Proc. of 1972 Int. Symposium on Information Theory(ISIT'72), p.102, 1972

[51] A. M. Patel,“Double error correcting method and system”, US Patent 3714629, Jan.30, 1973

[52] 中村,“誤り訂正符号の並列処理法について”, 電子通信学会通信方式専門委員会資料, CS78-116, pp.55-62, 1978 年 11 月

[53] 中村,“巡回符号の並列処理について”, 第 7 回情報理論とその応用シンポジウム (SITA84) 予稿集, pp.116-119, 1984

[54] 中村, 岩垂,“多値パルス系列に用いるデータスクランブラについて”, 電子通信学会論文誌, Vol.55-A, No.6, pp.266-273, 1972

[55] 野田,「デジタルマイクロ波通信方式」社内技術研修資料, 1989

[56] E.A.Lee, D.G.Messerschmitt,「Digital Communication」, Second Edition, Kluwer Academic Publishers, Boston, 1994

[57] 中村, 相河, 高梨,“ディジタルマイクロ波方式高信頼変復調技術”, NTT R& D, Vol.39, No.11, pp.1489-1498, 1990