早稲田大学審査学位論文(博士)の要旨
2912

早稲田大学大学院理工学研究科

博 士 論 文 概 要

論 文 題 目

BCH 符号の BCH 限界を超える復号法と
その軟判定復号法への応用に関する研究

A Study on Decoding Methods beyond the BCH Bound for BCH Codes
and its Application to Soft-Decision Decoding

申 請 者
小林 学
Manabu Kobayashi

機械工学専攻・情報数理応用研究

1999 年 10 月

今日の高度な情報化社会は，情報・通信システムに深く依存しており，近年のハードウエアの進歩，インターネットや携帯電話などの爆発的普及に伴い，情報・通信システムはますます巨大で複雑なものとなっている．このように様々な情報・通信システムに深く依存している現代社会では，情報の伝達や記憶に対する信頼性の確保は情報化社会の存立基盤にかかわる重要な課題である．情報・通信システムにおける通信媒体や記録媒体はあわせて通信路と呼ばれ，この通信路を介して伝達・記憶される情報は，電波障害や媒体の傷などの確率的に発生する雑音の影響を受ける．このような雑音の影響を取り除くために用いられる誤り訂正符号は，情報・通信システムの重要な基盤技術の一つとなっている．

誤り訂正符号では誤りの訂正・検出が可能な符号の構成方法すなわち符号化法と，その誤り訂正方法すなわち復号法の二者に関する議論が中心となり，符号理論として体系化されている．誤り訂正符号を用いた情報・通信システムは，符号化と呼ばれる操作を行うことにより伝達すべき情報を符号語へ写像し，この符号語を通信路へ入力する．通信路を経て受信側では雑音の影響を受けた受信系列を受け取り，この系列に対し復号化の操作を行うことにより送信された符号語を推定し，最終的にこの符号語に対応する情報を受信者へ出力する．

誤り訂正符号の中でも理論上優れた性能をもち，かつ実用上も極めて重要なクラスの符号にBose-Chaudhuri-Hoquenghem(BCH)符号がある．このBCH符号の一つであるReed-Solomon(RS)符号は，CD(compact disk)，DVD(digital versatile disk)，衛星通信など，広く実用に供されている．本研究では，特に2元BCH符号に対する復号化の問題を対象としている．

復号法は大きく分けて硬判定復号法と軟判定復号法の2種類に大別される．BCH符号に対する硬判定復号法は，受信側で得られる受信信号を最も粗く量子化した系列に対し，BCH符号の代数的構造を用いて送られた符号語を推定する復号法であり，代数的復号法とも呼ばれる．このときBCH符号では，一意に訂正可能な誤りの個数を定めるBCH限界と呼ばれる重要なパラメータが知られている．その結果，BCH限界をdと表したとき，その誤り訂正が可能な個数は$t = \lfloor \frac{d-1}{2} \rfloor$個以下の誤りを一意に訂正可能である．ここで，$\lfloor x \rfloor$は$x$を越えない最大の整数である．広くCDやDVDなどに用いられている復号法は，このt個以下の誤りのみを訂正する復号法であり限界距離復号法と呼ばれる．限界距離復号法は，BCH符号に対する代数的構造から基本方程式と呼ばれるガロア体上の連立一次方程式を高速に解くことにより行われるため，その計算量は非常に少なく符号長の多項式オーダで済む．これに対し，通常の限界距離復号法では求めることのできないt個以上の誤りを訂正することのできる復号法としてBCH限界を超える復号法が提案されている．しかしこの復号法は連立方程式の係数に未知変数が存在してしまうため，この未知変数を求めつつ連立方程式の解を求めなければならないため，通常その計算量が限界距離復号法より大幅に大きくなってしまう問題点がある．

一方，軟判定復号法は受信信号から得られる受信シンボル毎の信頼度情報を有

効に利用する復号法である．したがって硬判定復号法に比べ復号誤り確率を小さくすることができる．中でも最尤復号法は復号誤り確率を最小とするが，基本的にはすべての符号語の尤度を比較しなければならないため，計算量が符号長の指数オーダとなり実現性が問題となる．最尤復号法の計算量を低減する手法として，線形符号の構造を用いたトレリスダイアグラム(グラフ構造)を効率的に用いる復号法や，信頼度の順序に応じて生成行列を置換し，これに基づき候補となる符号語を多数生成する復号法など，様々な研究がなされている．近年ハードウェアの進歩により，実際これらの手法を用いて衛星通信に最尤復号法が用いられることが決定している．また最尤復号法と比べ，復号誤り確率の多少の劣化はあるが，その計算量を大幅に低減する研究も盛んである．中でも代数的復号を複数回繰り返し，候補となる符号語を複数生成する軟判定復号法としてGeneralized Minimum Distance (GMD)復号法，Chase復号法などは著名である．Chase復号法は，受信系列の中で誤っている確率の高いシンボルに重点的にテスト的な誤りを加え，その系列に対し限界距離復号を繰り返し，なるべく尤度の高い符号語を生成する軟判定復号法である．このテスト的な誤りはテスト誤り系列と呼ばれ，どのようなテスト誤り系列を用いるかにより復号法の性能が大きく左右される．Chase復号法以降，このテスト誤り系列の選び方によりさらに復号誤り確率や計算量を低減する研究も数多く研究されている．これらの復号法はそれぞれ長所，短所をあわせ持つが，主たる評価基準である復号誤り確率とその復号法に必要な計算量は通常トレードオフの関係にある．したがってなるべく両者をともに小さくする復号法が好ましいが，いまだ十分とは言えず改善の余地が大きい．

本研究はこの代数的復号を複数回繰り返す従来の軟判定復号法に対し，復号誤り確率及び計算量を低減することを目的とする．本研究の主な着眼点は，複数回繰り返す代数的復号として従来は限界距離復号を用いていたのに対し，BCH限界を超える復号を用いることにある．そのために，本研究は主に次の3つの提案を行っている．

(1) 従来のBCH限界を超える復号に対し，不必要な計算量を削減し，かつ効率良く計算する手法の開発．

(2) (1)を効率良く複数回用い，復号誤り確率を劣化させることなく軟判定復号法の計算量を低減させる手法の提案．

(3) 従来の軟判定復号法において，おのおの独立に複数回行われていた限界距離復号法に対し，前回の限界距離復号の結果から次の限界距離復号の結果を直接導くアルゴリズムの導出．

(3)のアルゴリズムは，従来のBCH限界を超える復号アルゴリズムを修正することにより導いている．さらに，(3)のアルゴリズムを(2)の復号法へ応用することもできる．このように，本研究ではBCH限界を超える復号を詳しく解析し，これを

応用した軟判定復号法が従来の軟判定復号法の復号誤り確率を劣化させることなく，その計算量を大幅に低減させることができることを示す．

本論文ではまず第2章において情報・通信システムのモデルや誤り訂正符号の原理，従来の代数的復号とこれを複数回用いる軟判定復号法などについて述べる．特に以下の各章に共通となる定義や従来法について詳細に記す．

第3章ではBCH限界を超える復号法の計算量を削減する手法について述べる．この節では限界距離復号法を行うアルゴリズムの性質を検討することにより，従来のBCH限界を超える復号法における未知変数の数を減らす．また残った未知変数の間にある関係を方程式として表し，この方程式をあらかじめ部分的に解いておき，この関係を満たす解のみを探索することにより，復号にかかるガロア体上の演算回数を大幅に低減する手法を提案する．

第4章では，まず第3章で述べたBCH限界を超える復号法を効率良く従来のChase復号法など代数的復号を複数回用いる軟判定復号法へ用いることによる効果を詳細に解析する．さらにテスト誤り系列に誤り訂正符号の符号語を用いる新しい軟判定復号法を提案する．この手法の着眼点は，互いにある程度距離を持った系列をテスト誤り系列とし，探索する符号語の範囲をなるべく広く，かつ隙間なくうめることにある．結果的にこの復号法は従来の軟判定復号法の復号誤り確率を劣化させることなくその代数的復号回数を大幅に低減させることができることを示す．したがってその主要な計算量であるガロア体の演算回数も低減される．

第5章は，従来の軟判定復号法において複数回おのおの独立に行われる限界距離復号に対し，前回の結果を用いて次回の限界距離復号法の結果を直接導くアルゴリズムを提案する．限界距離復号法は2元の通信路情報を用いて基本方程式と呼ばれる連立方程式を高速に解くことにより行われる．従来の軟判定復号法は，この限界距離復号法をおのおの独立に複数回用いるため，復号にかかる計算量は限界距離復号回数に比例する．これに対し第5章では，おのおのの限界距離復号法において得られる基本方程式間の関係を導出し，以前行った限界距離復号法の結果（基本方程式の解）から次に行う限界距離復号法の結果を直接求めるアルゴリズムを導出する．さらにこのアルゴリズムを用いた効果的な軟判定復号法を提案し，復号に要するガロア体の演算回数を解析する．その結果，主要な計算量が従来手法より大幅に改善されることを示す．さらに，本章で提案するアルゴリズムを第4章で述べた軟判定復号法へ適用すると，第4章の復号で必要であった計算の一部がこのアルゴリズムを利用することにより不要となる．また，第4章の復号法において計算された結果をこのアルゴリズムにおいて利用することもできる．したがって両者を組み合わせることにより，相乗効果による更なる計算量削減が可能となる．

最後に，第6章において得られた成果を要約し，残された今後の課題と展望について述べる．