論 文 内 容 の 要 旨

論文題目　Algebraic Soft-Decision Decoding of a Class of Linear Block Codes
(代数的手法に基づく誤り訂正符号の軟判定復号方式に関する研究)

氏名　神 谷 典 史

近年、各種デジタル通信・記録システムが急速な勢いで普及しており、情報を伝達・蓄積する際に雑音等によって生じるエラーから情報を保護する技術の重要性が増している。誤り訂正符号化技術はこのためのキーテクノロジーの一つとして広く知られている。符号理論は、経済的、かつ信頼性の高いシステムの構築を目的とした誤り訂正符号化、及びその復号方式に関する理論であり、その歴史は 1948 年の Shannon による通信路符号化定理の発見、あるいは 1950 年の Hamming による Hamming 符号の発明にはじまるとされている。以来、理論・実用の両面から多くの研究がなされている。

符号理論では、通常、システムの信頼性を表す指標として受信情報が正しく復号されない確率（復号誤り率）を採用し，経済性を表す指標として通信路コスト（符号化率）、及び符号化・復号のコスト（計算量）を採用する。一般に信頼性(復号誤り率)と経済性（特に復号の計算量）はトレードオフの関係にあり、このトレードオフ関係は符号理論における最重要研究課題の一つである。

誤り訂正符号の復号法は、硬判定復号と軟判定復号に大別される。前者の硬判定復号では、通信路（復調器）の出力系列に対し、各成分毎独立に送信情報を推定して得られた系列（硬判定系列）のみに基づいて送信情報系列を推定する。このように通信路の出力系列を一旦硬判定系列に変換することにより、一般に復号処理は簡易化されるが、この硬判定系列への変換に伴う情報の損失を免れない。これに対し、通信路出力が持つ情報をなるべく損なうこと無く復号過程に利用しようとするのが後者の軟判定復号である。Hamming 符号の発明以来、符号理論において最も研究成果が蓄積されたものの一つに BCH 符号に代表

される代数的（及び代数幾何的）符号構成法とその硬判定復号（限界距離復号）法に関する理論、所謂代数的符号理論があり、符号理論における他の研究領域と比較してその完成度は極めて高い。一方、代数的符号への軟判定復号の適用に関しては前述のトレードオフ関係に直結する重要な研究課題であるにもかかわらず研究が十分に進んでいるとは言い難い。

本研究は、理論・実用の両面において特に重要な代数的符号のクラスについて経済的かつ効率的な軟判定復号アルゴリズムを提供することを目的とし、Berlekamp, Chase, Forney らの先駆的研究に基づいて幾つかの軟判定復号方式とアルゴリズムを提案する。提案する一連の軟判定復号アルゴリズムは、復号器の出力となる候補符号語を逐次生成する繰り返し形軟判定復号であり、いずれも本研究で得られた基本アルゴリズムを繰り返し用いることにより構成されているという点で共通点がある。各軟判定復号アルゴリズムの基本的な構造はほぼ同一であるという特長を有している。本学位論文は以下に示すように全部で七つの章と一つの付録からなる。

第１章では、符号理論における中心的な研究課題の一つである復号問題について触れ、硬判定復号と軟判定復号の違い、最適（最尤）復号、及び準最適復号の基本戦略等について述べる。

第２章では、本論文で扱う軟判定復号器を構成する上で基礎となるアルゴリズムを提案する。まず軟判定復号において核となる処理が四つのタイプに分類できることを示す。次いで、各タイプの処理についてそれを実行する効率的なアルゴリズムを構成する。ここで構成する四つのアルゴリズム（Ⅰ～Ⅳ）の内、アルゴリズムⅠは、本論文の付録で示されるように、ある種の多重系列を生成するシフトレジスタ合成問題を解くためのアルゴリズムに一致し、第３章で扱う一般化最小距離（GMD）復号、及び第５章で提案する復号方式に応用される。アルゴリズムⅡは、アルゴリズムⅠの入出力関係を反転させたものであり、Ⅰと組み合わせて第６章で扱う Chase 復号に応用される。また、アルゴリズムⅢは Berlekamp-Massey アルゴリズムと本質的に同等であり、ⅣはⅢの入出力関係を反転させたものである。さらに本章では、これら四つのアルゴリズムを統一的に記述することが可能であることを示す。

第３章では、代数的符号に関する効率的な GMD 復号アルゴリズム（one-pass GMD decoding algorithm）を提案する。一般に、GMD 復号では限界距離復号アルゴリズムを繰り返し適用することによって復号器出力の候補符号語集合を算出するため、限界距離復号アルゴリズムの計算量の d 倍（d は符号の設計距離）のオーダーの計算量を必要とする。ここで提案する GMD 復号アルゴリズムの計算量のオーダーは、限界距離復号の計算量のオーダーに一致する。即ち、GMD 復号に要する計算量のオーダーを 1/d に減らすことができる。尚、GMD 復号アルゴリズム高速化については、アプローチの仕方は異なるものの、他の研究者によっても類似の結果が報告されている。計算量の削減は次の理由による。従来の GMD 復号アルゴリズムにおいて、第 k 回目の限界距離復号結果と第 k ＋１回目限界

距離復号結果の相関に注目し、それを用いることで、ｋ回目の結果から、（限界距離復号を実行するよりも遥かに少ない手順で）直接ｋ＋１回目の結果を算出することが可能となる。このアイディアは、Chase 復号にも適用することができ、それによって効率的な Chase 復号アルゴリズムを構成できることが第６章で示される。

第４章では、GMD 復号で得られた候補符号語集合の中で最も尤度の高い符号語が、すべての符号語の中で最も尤度の高い最尤の符号語となるための十分条件について検討する。このような十分条件として、Taipale-Pursley（TP）基準が知られている。これに対し、本章では新たな十分条件を導入する。これは一般に TP 基準よりも緩く、より必要十分に近い条件であることが示される。また、その判定が極めて単純な手続きによって簡単に実行できることも特長の一つである。

第５章では、計算量を大幅に増やすことなく、GMD 復号の復号誤り率特性を改善し、より最尤復号の特性に近づける方法について検討する。具体的には、第３章で構成した GMD 復号アルゴリズムに基づいて、より多くの候補符号語を効率的に算出する方法を提案する。さらに本章では、計算機シミュレーションによって誤り率特性を評価することで提案アルゴリズムの効果を示す。

第６章では、効率的な Chase 復号アルゴリズム（one-pass Chase decoding algorithm）、及びそれに基づいた最尤復号アルゴリズムを提案する。GMD 復号の場合と同様、計算量のオーダーは従来比１/ｄとなる。ここで提案するアルゴリズムは第２章のアルゴリズムⅠ，Ⅱを組み合わせて得られる。また最尤復号に関しては、候補符号語が最尤であるための十分条件の導入が最近多くの研究者によって検討されており、これによって最尤復号の平均計算量が低減されることが計算機シミュレーション等によって確認されている。本章では、Kaneko らの結果に基づいてこの最尤性判定条件についても検討する。

第 7 章では、本論文の結果をまとめる。また、付録では第２章のアルゴリズムⅠとある種の多重系列を生成するシフトレジスタ合成問題との関連を明らかにする。