様式 C-19

科学研究費補助金研究成果報告書

平成２３年　５月２３日現在

研究種目：若手研究（スタートアップ）
研究期間：２００８～２００９
課題番号：２０８６００７９
研究課題名（和文）擬似ランダム性にもとづく性能のよい誤り訂正符号の構成に関する研究

研究課題名（英文）Constructions of Error-Correcting Codes Based on Pseudorandomness

研究代表者
安永　憲司（ヤスナガ　ケンジ）
東京工業大学・大学院情報理工学研究科・特任助教
研究者番号：５０５１０００４

研究成果の概要（和文）：
ランダムに構成したように見える「擬似ランダム」なオブジェクトのいくつかは，共通の構造をもつことが明らかになった．そのオブジェクトとは，リスト復号可能符号，擬似乱数生成器，エクスパンダグラフなどである．多項式に対する擬似乱数生成器と性能のよい誤り訂正符号は，ある条件下では等価であることがわかった．多項式をもとにした誤り訂正符号に対する復号法を，より一般的な符号に対して適用できるように拡張した．

研究成果の概要（英文）：
It was realized that many pseudorandom objects, such as list-decodable code, pseudorandom generator, and expander graph, have a common structure. Also it was realized that pseudorandom generators for polynomials are equivalent to good error-correcting codes under a certain condition. We generalized a decoding algorithm for codes based on polynomials to be applicable to more general class of codes.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,330,000	399,000	1,729,000
2009 年度	1,200,000	360,000	1,560,000
年度			
年度			
年度			
総　計	2,530,000	759,000	3,289,000

研究分野：符号理論
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：誤り訂正符号，擬似ランダム性

１．研究開始当初の背景

誤り訂正符号とは，送信メッセージに冗長性を付加することで通信路中に発生した誤りを受信者側で訂正する技術のことである．性能のよい誤り訂正符号とは，符号化レート（通信路に送信する系列の長さに対する元のメッセージの長さ）が与えられたとき，できるだけ多くの誤りを訂正できる符号のことである．符号の最小距離がｄであるときｄ/2個未満の誤りは必ず誤り訂正ができるため，性能のよい符号とは最小距離の大きい符号

のことを指す.

符号をランダムに構成するランダム符号について以下のことが知られている.

(1) ２元符号ではランダム符号以上の性能をもつ符号は知られていない
(2) 明確な形で定義可能な符号でランダム符号と同性能のものは知られていない

つまり，ランダム符号は非常に性能のよい符号ではあるが，実際には利用できない符号である．また，非２元の符号ではReed-Solomon符号をはじめ性能のよい符号が知られているが，結局応用する際には２元符号として利用しており，２元符号としての性能はランダム符号に及ばない．ランダム符号と同等または非常に近い性能をもつ２元符号の構成は符号理論に残された大きな課題の一つである．

ランダムに構成したものと同等もしくは非常に近い性能をもつ擬似ランダムオブジェクトを構成する研究が近年盛んである．その中でもエクスパンダグラフと呼ばれるグラフは，理論計算機科学やグラフ理論の研究者によって最近目覚ましい成果を上げている．エクスパンダグラフは様々な分野で応用されており，通信ネットワークの構成法，データ格納法，確率的アルゴリズムで必要な乱数のサイズを削減する方法，NP問題の近似困難性の証明など多岐にわたっている．

２．研究の目的

ランダムに構成した符号はよい性能をもつことが知られているが，実際に利用するには明確な形で符号を定義する必要があり，ランダムに構成するという方法は現実的な方法ではない．そこで本研究では，明確な形で定義可能である擬似ランダム性をもつオブジェクト（エクスパンダグラフ等）を利用して性能のよい誤り訂正符号を構成することを目的とする．

誤り訂正符号としては，効率的な復号アルゴリズムが存在することが重要である．そこで，擬似ランダムなオブジェクトから構成された誤り訂正符号に対して，性能のよい復号アルゴリズムを開発することも目的とする．

３．研究の方法

本研究では，擬似ランダムオブジェクトを用いて性能のよい符号を構成することを考える．例えば，擬似ランダムオブジェクトとして，エクスパンダグラフが考えられる．符号を定義するための生成行列やパリティ検査行列は，自然な形でグラフとして表現することができる．そのグラフにエクスパンダグラフを利用することで，最小距離の大きな符号を構成することを目指す.

また，その他の擬似ランダムオブジェクトと誤り訂正符号の関連性についても調査を行う.

申請者はこれまでに符号の誤り訂正能力について研究を行ってきており，最近は１次リード・マラー符号の訂正能力の理論的分析を行っている．この１次リード・マラー符号は非常に興味深い性質をもつことがわかってきた．１次リード・マラー符号の生成行列からオール１の行を取り除いた行列Ｇを考える．すると，任意の２元符号の生成行列は，この行列Ｇから列をいくつか削除することで得られる．そして，削除する列をランダムに選択すれば，それはランダム符号となるのである．この削除する列の選択をランダムでなく（決定的に）擬似ランダムに選択すれば，最小距離の大きな符号の構成が期待できる（図２参照）.

４．研究成果

擬似ランダムオブジェクトについて調査を行った．エクスパンダグラフを用いた符号の構成に関する研究はいくつか存在しているため，それを手がかりとして擬似ランダムオブジェクトについて調査した．その結果，誤り訂正符号のリスト復号可能符号とエクスパンダグラフ，擬似乱数生成器，乱数抽出器，困難性増幅器，標本抽出器は，非常に密接な関係があることがわかった．より具体的には，これらの擬似ランダムオブジェクトは，共通の構造をもっており，すべてのオブジェクトは統一的な枠組みで特徴づけ可能である．もちろん個々のオブジェクトにおいて特徴づけの細かい差は存在するが，いずれもほぼ同じ特徴づけが可能であることがわかった.

統一的な特徴づけが可能であるが，それぞれのオブジェクトには違いも存在する．興味のあるパラメータが異なっていることが多い．また，この統一的な枠組みでは，アルゴリズムの効率という観点は考慮していない．例えば，リスト復号可能符号では，符号が効率的に構成できなければならないし，リスト復号アルゴリズムも効率的に実行できることが望まれる．しかし，そのようなアルゴリ

ズムの効率に関しては統一的枠組みでは明示的に現れない.

また，多項式に対する擬似乱数生成器は性能のよい誤り訂正符号とある条件下では等価であることがわかった．誤り付き補間集合というものを考えると，次数が 1 の多項式を考えた場合，誤り付き補間集合と，多項式に対する擬似乱数生成器の写像は等価である．次数が 2 以上の場合，多項式に対する擬似乱数生成器の写像は，誤り付き補間集合であることがわかる．しかし，誤り付き補間集合が擬似乱数生成器であるかどうかは明らかになっていない．誤り付き補間集合とは，Reed-Muller 符号と呼ばれる誤り訂正符号の符号語の座標の部分集合のうち，一定割合の誤りを含んだとしてもその部分集合の座標から符号語（多項式）を補間できるような集合のことである.

次に，Reed-Muller 符号のリスト復号アルゴリズムについて研究を行った．リスト復号とは，受信語から符号語をひとつ出力するのではなく，符号語の候補をリストとして出力することを許す復号法である．符号語としてひとつしか出力を許さない場合は，最小距離の半分までしか確実に復号をすることはできなかったが，複数のリストを出力してもよいことにすると，この限界を超えることができる.

Reed-Muller 符号のリスト復号としては，Goldreich-Levin によるハードコアビットの存在性証明が 1 次 Reed-Muller 符号の復号法に対応するという結果が知られている．その後，Gopalan, Klivans, Zuckerman によって，Goldreich-Levin アルゴリズムを自然に 2 次以上に拡張した復号アルゴリズムが提案された．このアルゴリズムはリスト復号として非常にすぐれた性能をもつ．さらに，Dumer,Kabatiansky,Tavernier は，アルファベットサイズが 2 の場合について，Gopalan らのアルゴリズムの改良を行った．その改良においては，Reed-Muller 符号が Plotkin 構成と呼ばれる一般的な構成法をもとに作られていることを利用している.

そこで本研究では，Dumer らの拡張を，アルファベットサイズが 2 よりも大きい場合にさらに拡張することを考えた．Plotkin 構成は，アルファベットが 2 の場合に定義される概念である．そのため，Plotkin 構成をアルファベットが 3 以上の場合に拡張する必要がある．そこで，自然な形で，一般のアルファベットに対して拡張した Plotkin 構成の概念を定義した．そして，一般化した Plotkin 構成をもとにして，Dumer らのアルゴリズムを一般のアルファベットサイズ q に一般化することに成功した．ただし，r 次 Reed-Muller 符号を考える場合，q < r を満たす必要がある．提案復号法のリスト復号半径は，Gopalan らの提案した復号法と一致している．一方で，復号のための時間計算量の評価が異なる．時間計算量に関しては，それを評価するためには Reed-Muller 符号の構造に関するさらなる研究が必要なため，単純には比較できない．ただ，アルファベットサイズがある程度大きい場合は，提案復号法は Gopalan らの復号法よりも時間がかかってしまうため，アルファベットサイズがある程度小さい場合に効果的なアルゴリズムであることが期待できる.

提案した復号法は，Plotkin 構成と呼ばれる構造を再帰的にもつような符号ならば適用可能なことがわかった．つまり，Reed-Muller 符号だけでなく，他の符号に対しても適用可能なのである．そこで，その他の符号として提案復号法が適用可能な符号について調査した．その結果，最近 Arikan によって提案された分極符号と呼ばれる符号に適用できる可能性があることがわかった．分極符号は，定義を広い意味で捉えると，Reed-Muller 符号の一般化として定義される．つまり，分極符号の特殊な場合が Reed-Muller 符号である．このように分極符号を定義したとき，分極符号が提案復号法を適用可能なための十分条件を導出した.

分極符号は，効率的な復号によって通信路容量を達成する符号として注目が集まっている．提案した復号法は，その分極符号に対するリスト復号アルゴリズムになっている．しかし，アルゴリズムが適用できるための十分条件を示すことにとどまっているため，今後は，具体的な分極符号の構成に対して適用可能なであることを示すことが必要になると考えられる．Gopalan らによって提案されたリスト復号アルゴリズムは，リスト復号として非常に性能が優れていた．また，分極符号は通信路容量を達成する符号として知られている．これらの組合せである分極符号に対するリスト復号は，高い性能を示すことが期待される.

５．主な発表論文等
（研究代表者，研究分担者及び連携研究者には下線）

〔学会発表〕（計 1 件）
① 安永憲司、List decoding for Reed-Muller codes and its application to polar codes、第 32 回情報理論とその応用シンポジウム、2009 年 12 月 2 日、山口県山口市

６．研究組織

(1)研究代表者

安永　憲司（YASUNAGA KENJI）

東京工業大学・大学院情報理工学研究科・

特任助教

研究者番号：５０５１０００４