科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　２４　日現在

機関番号：　３３９２４
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５６０４７８

研究課題名（和文）誤り訂正符号の新たな代数的復号法

研究課題名（英文）Modern algebraic decoding of error-correcting codes

研究代表者
松井　一（Matsui, Hajime）

豊田工業大学・工学（系）研究科（研究院）・准教授

研究者番号：８０３２９８５４

交付決定額（研究期間全体）：（直接経費）　　4,200,000円、（間接経費）　　1,260,000円

研究成果の概要（和文）：１．アフィン多様体符号の復号化法における誤り値評価法を高速化した．この部分の高速化のために，シンドロームの拡張と離散フーリエ変換についてのMain Lemmaを用いることにより，符号長の3乗のオーダーであった従来の計算量を，ほぼ2乗のオーダーに改良することができた．
２．高性能な一般化準巡回符号の探索法として，全探索法と素因子分解法を提案した．またこの結果に対する整数環上の符号への類似として，一般化整数符号を新たに定義し，双対符号や探索法，またHecke環を用いた数え上げについての結果を得た．

研究成果の概要（英文）：1. The computational complexity of the error-value estimation in the decoding of affine variety codes has been reduced. The conventional method of the error-value estimation in the decoding of affine variety codes by Berlekamp-Massey-Sakata algorithm employs solving systems of linear equations by Gaussian elimination. In order to reduce its computational complexity, a lemma for the extension of syndrome values and discrete Fourier transforms, called Main Lemma, is established and applied to the error-value estimation. Thereby, the computational complexity third power of the code length has been reduced to the nearly second power of the code length.
2. Efficient search algorithms of high-performance generalized quasi-cyclic codes are proposed. Moreover, as an analogy of these results to the codes over rational integer rings, generalized integer codes have been newly defined, and their dual codes, search algorithms, and an enumeration method via Hecke rings have been investigated.

研究分野：　工学

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　離散フーリエ変換　リード・ソロモン符号　代数幾何符号　アフィン多様体符号　p進数体　グレブナー基底　BCH符号

１．研究開始当初の背景

誤り訂正符号とは，デジタル・データを送信する際これによって冗長と呼ばれるデータを付け加え，一定個数以下の誤りは訂正できるようにしたものである．将来的には現在最も広く使われている Reed-Solomon（RS）符号とその硬判定復号法では性能が不十分になることが示されており，理論的な性能の限界式である Shannon 限界に漸近する符号を見つけ出す問題はこの分野の最重要課題である．2001 年，Low density parity check（LDPC）符号と呼ばれる符号が，sum-product 法と呼ばれる復号法によって Shannon 限界まで 0.0045dB にまで迫ることが Chung らによって示された．しかしながら，LDPC 符号はいくつかの通信規格には採用されたものの，以下に述べるような課題がまだ残されている：１．エラーフロアの存在，２．バースト誤りや強い信頼度を持つ誤りに対する耐性，３．LDPC 符号と RS 符号を組み合わせる際の回路規模の増大．１については，実用的には誤り訂正符号はビット誤り率 10^{-20} 以下としなければならないこともあり，エラーフロアの存在は大きな障害となっている．２については，現実の通信路で起こる誤りは必ずしもガウス分布に従っているとは限らず，信頼度を元に復号を行う sum-product 法のような軟判定復号法では訂正できないことがある．研究代表者が企業の研究者から話を伺ったところによると，現実の応用上はこのような強い信頼度を持った誤りが多く，LDPC 符号のみでは対応しきれない．このため，現行の RS 符号を用いて硬判定および軟判定の両方の復号を行う手法は依然として有力候補のひとつである．これら１・２の弱点を克服するためには，３のような異なるタイプの符号を合わせて使うことが考えられるが，全く構造が異なるため復号化器が複雑化するという新たな問題が生じる．一方，RS 符号に対する Koetter らの代数的軟判定復号法はエラーフロアを持たないものの，次元を上げて復号するためやはり復号化器が複雑化する．こうして Chung らの 2001 年の論文や Koetter らの 2003 年の論文から年月が経過し，新しい代数的復号法が求められている．

２．研究の目的

2001 年，低密度パリティ検査符号が Shannon 限界にほぼ到達することが示された．しかし現実の応用では，加法的でない強い信頼度を持つ誤りを訂正する必要がある．本研究では，このような誤りに対しても耐性のある，代数的軟判定復号法を確立することが目的である．このために主に二つの視点から代数的復号法を取り上げる．一つは代数幾何符号を含むより包括的な誤り訂正符号であるアフィン多様体符号であり，研究代表者がリード・ソロモン符号についてすでに実現している符号化・消失誤り訂正復号化統合システムをアフィン多様体符号に対し一般化する．もう一つは局所体上の符号に対してであり，有限体を含む局所体を用いることにより，新たな代数的軟判定復号法を見出す．

３．研究の方法

（1）　局所体の BCH 符号への応用：

局所体である 2 進数体や 3 進数体を用いた Golay 符号の復号法が示されており，この結果を他の BCH 符号等に拡張し，また他の局所体についても一般化する．例えば 2 進数体上の (7,4) ハミング符号の生成多項式は $G(X)=X^3+\lambda X^2+(\lambda-1)X-1$ である．ただし λ は $\lambda^2-\lambda+2=0$ の根の一方であり $2+2^2+2^5+2^7+2^8+\ldots$ と 2 進展開される．また 2 進数体の拡大体における 1 の原始 7 乗根の一つを ζ とすると，$G(X)$ は ζ,ζ^2,ζ^4 を根に持つ．こうして局所体上の符号に対しても，組織的符号化やシンドローム復号法といった代数的理論を構築する．これらを単なる形式的な一般化とするのではなく，代数的

軟判定復号法の理論的基礎とする.

(2) 局所体の Hensel lifting の符号理論への応用：
Hensel lifting を Koetter らの代数的軟判定復号法に応用するという先行研究があり，この手法を局所体上の符号に応用する．また RS 符号の復号法の一つである Berlekamp-Massey（BM）法は，形式的べき級数体を用いて定式化され示される．この方法を用いて，BM 法と Hensel lifting との関係を明らかにする.

(3) 局所体上の符号に対する離散 Fourier 変換の応用：
誤り訂正符号の符号化と復号化は離散 Fourier 変換(DFT)とその逆変換に対応する．研究代表者は数々の符号に対し DFT を用いた組織的符号化法を示し，また DFT 演算器を共有した符号化・復号化統合システムを構成した．この手法を局所体上の符号に対し一般化する．2 進数体の拡大体における 1 の原始 7 乗根を ζ とすると，例えば 7 点 DFT は $\sum_{i=0}^{6} c_i \zeta^{ij} \quad (j = 0,1,...,6)$ と表される. こうして局所体上の符号に対するコンパクトな符・復号化器を構成する.

４．研究成果

（１）2 進数体上の BCH 符号に対する拡張ユークリッド法による高速な代数的復号法を提案した．既に知られていた 2 進数体および 3 進数体上の Golay 符号に対する連立方程式による復号法の一般化および高速化となっている．数値例として，符号長 15，次元 7 の BCH 符号に対する 2 重誤り訂正を取り上げ，数式処理システム magma を用いて解説した.

（２）一般化準巡回符号を用いた低密度パリティ検査符号（LDPC 符号）の構成について検討した．一般化準巡回符号について成り立つある種の等式および最小ハミング距離の上限下限式を応用して，全探索アルゴリズムの効率化と最適化を行った．構成された LDPC 符号は最小ハミング距離が比較的大きいという特長を持ち，ビット誤り率のグラフにおけるエラーフロア領域の特性改善に効果があった.

（３）リード・ソロモン符号や代数幾何符号などの符号化や復号化にしばしば現れる演算を理論化し，代数的符号理論における一つの補題を確立した．この補題は，二つのベクトル空間，一方は情報シンボルのなすベクトル空間，もう一方は多項式環のある種の商環の元によって添え字づけられたベクトル空間について，これらのベクトル空間の間の標準的同型写像を与える．またこの写像は，グレブナー基底から得られる線形漸化式による拡張写像と離散フーリエ変換の合成写像からなる．次に，この補題をある種のアフィン多様体符号に応用し，符号化・消失誤り訂正復号化統合システムを構築した.

（４）一般化準巡回符号の新しい探索法の提案：一般化準巡回（GQC）符号は，準巡回（QC）符号の符号語における各巡回長が一定でないものとして定義される．GQC 符号には定義より膨大な種類が存在し，ランダムな構成法では効率的な探索を行うことができない．そのため，規則性に則った探索アルゴリズムの考案が必要となる．また，GQC 符号の探索は多元低密度パリティ検査（LDPC）符号の探索にも応用できる. LDPC 符号は高性能な誤り訂正符号として注目されており，GQC 符号の探索アルゴリズムの改良は LDPC 符号の探索の高速化に繋がる．本研究では，GQC 符号を探索するアルゴリズムとして，全探索法と素因子分解法を提案した．全探索法は，GQC 符号の生成多項式行列の満たす等式を Bezout の等式の集まりと見て解いていく方法である.

素因子分解法は，GQC 符号の生成多項式行列の満たす等式を素因子分解することにより全探索法の高速化を行うものである．またこれらのアルゴリズムを用いた探索結果の一例も詳細に解説した．

（５）局所体の整数環上の誤り訂正符号：ここで局所体とは，数論においてよく用いられる数体系であり，本研究で用いたものは，2 進数体と呼ばれるものである．本研究の新しい内容は，2 進整数環という体ではない環上のリード・ソロモン符号を扱ったことである．現在広く用いられているリード・ソロモン符号は有限体の演算を基礎としているが，本研究では，すべての演算を 2 進整数環の中で処理することができることを示した．また 2 を法としてみる操作により，標数 2 の有限体上の符号とリンクするという注目すべき構造を持っていることがわかった．

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）

〔雑誌論文〕（計 4 件）

1. H. Matsui, “On generator matrices and parity check matrices of generalized integer codes,” to appear in Designs, Codes and Cryptography. DOI 10.1007/s10623-013-9883-7. 査読有.
2. H. Matsui, “Lemma for linear feedback shift registers and DFTs applied to affine variety codes,” IEEE Transactions on Information Theory, vol.60, no.5, pp.2751-2769, May 2014. 査読有.
3. 松井一,“線形帰還シフトレジスタ理論とその発展,”電子情報通信学会 技術報告, vol.113, no.319, IT2013-41, pp.1-9, 11 月 19 日, 2013. 査読無.
4. H. Matsui, “Decoding a class of affine variety codes with fast DFT,” International Symposium on Information Theory and its Applications (ISITA2012), Hawaii Convention Center, Honolulu, Hawaii, USA, pp.436-440, October 28-31, 2012. 査読有.

〔学会発表〕（計 11 件）

1. 中島規博, 松井一,“2 次伸長 RS 符号の離散フーリエ変換を用いた復号化法,”電子情報通信学会 総合大会, 基礎・境界講演論文集 A-6-7, p.115, 3 月 18 日－21 日, 2014.
2. 谷川祐介, 松井一, 陳勁嘉,“一般化準巡回符号における自己直交性の効率的な検証,”第 36 回情報理論とその応用シンポジウム予稿集, pp.81-86, 11 月 26 日－29 日, 2013.
3. 高松直斗, 松井一,“アフィン多様体符号における消失誤り訂正の可換図式を用いた定式化,”第 36 回情報理論とその応用シンポジウム予稿集, pp.7-12, 11 月 26 日－29 日, 2013.
4. 松井一, “2 進整数環上のリード・ソロモン符号,” 研究集会「モダン符号理論からポストモダン符号理論への展望」, 九州大学マス・フォア・インダストリ研究所, pp.95-107, 3 月 4－7 日, 2013.
5. H. Matsui, K. Suzuki, “Decoding of Reed-Solomon codes over 2-adic number field with discrete Fourier transforms,”第 35 回情報理論とその応用シンポジウム予稿集, pp.496-501, 12 月 11 日－14 日, 2012.
6. 丹山翔太, 松井一, 王志緯,“一般化準巡回符号の探索における素因子分解法,”第 35 回情報理論とその応用シンポジウム予稿集, pp.419-424, 12 月 11 日－14 日, 2012.
7. 丹山翔太, 松井一, 加藤弘明,“一般化準巡回符号の探索とその計算量評価,” 電

子情報通信学会 情報理論研究会, IT2012-17, pp.51-56, 7月20日, 2012.
8. 熊谷雄一, 松井一, “LDPC符号の一般化準巡回符号を用いた構成と重み分布による評価,” 信号処理ワークショップ2012, 4月10日, 2012.
9. H. Matsui, “Fast erasure-and-error decoding and systematic encoding of a class of affine variety codes,” 第34回情報理論とその応用シンポジウム予稿集, pp.405-410, 11月29日－12月2日, 2011.
10. K. Suzuki, H. Matsui, “Algebraic decoding of 2-adic BCH codes with extended Euclidean algorithm,” 第34回情報理論とその応用シンポジウム予稿集, pp.346-351, 11月29日－12月2日, 2011.
11. 熊谷雄一, 松井一: “一般化準巡回符号による低密度パリティ検査符号の構成,” 第34回情報理論とその応用シンポジウム予稿集, pp.64-68, 11月29日－12月2日, 2011.

〔その他〕

ホームページ等

http://www.toyota-ti.ac.jp/Lab/Denshi/InfoComm/index_ja.html

http://ttiweb.toyota-ti.ac.jp/1432/pub_teacher_show.php?t=154

６．研究組織

(1)研究代表者

松井　一（Hajime MATSUI）

豊田工業大学・大学院工学研究科・准教授

研究者番号：80329854