様式 C-19

科学研究費補助金研究成果報告書

平成　22　年　6　月　11　日現在

研究種目：若手研究（B）
研究期間：2007～2009
課題番号：19760269
研究課題名（和文）　代数幾何符号および高次元巡回符号のグレブナ基底を用いた符号化・復号化モデル
研究課題名（英文）　Models of encoding and decoding via Grobner basis for algebraic geometry codes and multidimensional cyclic codes

研究代表者
松井　一　（MATSUI HAJIME）
豊田工業大学・大学院工学研究科・准教授
研究者番号：80329854

研究成果の概要（和文）：研究成果は以下の 3 項目に分けることができる。1. 有理点を多数持つ代数曲線および高性能な代数曲線符号・高次元巡回符号の探索。一般化準巡回符号のグレブナ基底を計算するアルゴリズムを導き、探索手法を確立した。2. 代数曲線符号に対する符号化・復号化統合モデルの作成。3. 符号化・復号化統合システムのリード・ソロモン符号への応用。近い将来必要になると考えられる RS 符号システムの回路規模を従来のものと比べ 40%削減できるという見積もりが得られた。

研究成果の概要（英文）：Research results are classified into three subjects as follows. 1. Searching algebraic curves that have many rational points and searching efficient codes on algebraic curves and multidimensional cyclic codes. A method to compute Grobner basis for generalized quasi-cyclic codes has been established, and thereby, a searching method for them has been established. 2. Constructing unified models of encoding and decoding system for codes on algebraic curves. 3. Application of unified system of encoding and decoding for Reed-Solomon codes. The circuit scale of the unified system for the next-generation error-correcting codes has been estimated as 40% reduction of that of the conventional system.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	800,000	0	800,000
2008 年度	400,000	120,000	520,000
2009 年度	400,000	120,000	520,000
年度			
年度			
総　計	1,600,000	240,000	1,840,000

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、エルミート曲線符号、代数幾何符号、代数曲線符号、グレブナー基底、有限体

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ることができ、誤りが起こってもある程度は訂正できるようにするものである。これが現在のデジタル機器の安定性・信頼性を支えている。表１に代表的な誤り訂正符号の大まかな性能比較を示す。現在最も広く用いられている RS 符号は符号長が通常は一定までしか取れず、これを超えようとすると符号化率が下がるという欠点がある。次世代誤り訂正符号の候補はその復号化法により分類するとき、確率的符号と代数的符号に大きく分けることができる。確率的符号には Turbo 符号や Low density parity check（LDPC）符号があり、また代数的符号には RS 符号やその一般化である代数幾何符号がある。確率的符号は符号長を長くするとき Shannon 限界に迫るほどの高い訂正能力を示すが、一般には符号化率が低く、また「エラーフロア」と呼ばれる誤り率の低いところで急激に性能が悪くなる欠点がある。一方、代数幾何符号においてはこういった欠点はなく優れた特性を示す。しかしながら他と比較して計算量が多いという未解決の問題が残されている。

表1：代表的な誤り訂正符号の性能比較

	RS	LDPC Turbo	代数幾何
符号長	△	◎	○
符号化率	○	△	◎
エラーフロア	なし	あり	なし

近年、研究代表者はグレブナー基底と離散 Fourier 変換（DFT）を組み合わせた新しい符号化手法を開発し、2006 年情報理論とその応用シンポジウムにおいて発表した。これによって行列の乗算を使わない符号化が完成し、また組織的符号化法、すなわちデータと冗長を分離して符号化する実用的方式も可能になった。さらに研究代表者は新しい視点から符号化法を提案するだけではなく、それぞれの符号化法に最適な復号化法も明らかにした。しかも、復号化法については通常はシンドロームや誤り値算出と別に論じられることが多かったが、再び DFT を利用することにより符号化法と結びつけることができ、よってデータの符号化から誤りの訂正実行まで完全に効率化することができた。こうして、より実際的な符号化・復号化を統合した性能評価ができる段階に来ている。

２．研究の目的

本研究の目的は、密接な関係を持つ代数幾何符号と高次元巡回符号に対し、グレブナー基底を応用した符号化・復号化アルゴリズムを確立し、シミュレーションモデルを構築し従来の手法との性能比較を行うことにある。これは以下の 3 つに分けることができる

(1). 新しい符号化法、特にグレブナー基底と DFT との融合の理論的完成。また従来の符号化法との性能比較。

(2). 様々な代数幾何符号の符号化・復号化シミュレーションの構築、およびそれらの演算規模の評価。

(3). 符号に適した代数曲線、特にこれまであまり研究されていなかった空間曲線の探索。

またもう一つの研究対象である高次元巡回符号については、代数幾何符号の登場により関心を奪われた形となり研究が不十分のまま残されている。もしも符号としての性能が代数

幾何符号に迫るものであれば、代数曲線の有理点を用いていない分、高次元巡回符号のほうが実現しやすくなる。よってこの方向性についても検討を行う。

今までに代数幾何符号および高次元巡回符号に対し、符号化と復号化の両方を統一的に扱った研究はないと思われる。現在、すでに研究代表者は平面曲線符号の理論的基礎付けを完了しており、さらにこれらに対する符号化・復号化モデルを完成することによりこの分野が大きく前進する。これにより有効性が明らかになり、回路規模および処理速度が求まり、誤り訂正を必要とするデバイスのうちどれで最も効力を発揮するかがわかる。また本研究の影響は工学の範囲だけではなく、現代数学の工学への応用という面で数学界に与える影響も大きく、様々な分野から注目される研究であると考えられる。

３．研究の方法

(1) 有理点を多数持つ代数曲線および高性能な代数曲線符号の探索：高性能な符号を構成する基礎となる有理点を多数持つ代数曲線の探索を行う。次世代DVD用の64キロバイト情報を許容する符号、および次世代HDD用の4キロバイト情報に適する代数曲線を求め、それらの符号を構成し、従来のRS符号やHermite曲線符号と性能比較を行う。探索の指針としては、telescopic生成系および三浦によるC_a^b曲線の高次元への拡張理論を基礎とする。

(2) 代数曲線符号に対する符号化・復号化統合モデルの作成：代数曲線符号に対し、符号化と復号化において共通のグレブナー基底やDFTエンジンを用いることにより、符号化・復号化回路全体としての回路規模を削減する。なお以前の Berlekamp-Massey-阪田アルゴリズム演算器では二次元配列をシリアル化したものをレジスタにフィードバックさせていたが、空間曲線符号に対しては三次元配列に対し極位数順序にしたがって同様にしたものを構成する。

(3) 高性能な高次元巡回符号の探索：提案符号化・復号化法はそのまま高次元巡回符号に対しても適用可能であり、この符号を再評価する。また従来のこの種の符号だけではなく、位置がランダムなものや群となっているもの等々、様々な位置集合に対し符号の最小距離を計算する。高次元巡回符号の最小距離の理論限界についてもグレブナー基底を用いて改善できないか検討する。

(4) 符号化・復号化統合システムのリード・ソロモン符号への応用：現在最も広く用いられているリード・ソロモン符号は有限体GF(256) やGF(1024)上のものであるが、将来的にはGF(4096)上のリード・ソロモン符号を用いることが予定されており、符・復号化器の回路規模増大が問題となる。よって新しい符・復号化統合システムを応用し、回路規模を削減する。離散フーリエ変換の長さが4095のため計算には通常のFFTを用いることはできず、fast prime factor DFT を用いる必要がある。これは4095=63×65と分解し、長さ4095の配列をChinese Remainder Theoremを用いて 63×65 の二次元配列に配置した後、長さ63と65の離散フーリエ変換をそれぞれ計算する必要がある。このように離散フーリエ変換を二度計算することによる遅延をどう解消するかを検討する。

４．研究成果

(1) 有理点を多数持つ代数曲線および高性能な代数曲線符号・高次元巡回符号の探索：これまであまり現実的な符号の観点からは調べられていなかった空間曲線符号、および高次元巡回符号について高能率符号を探索した。その結果、一般化準巡回符号と呼ばれ

る符号のクラスにおいて、高性能な符号が多数含まれることがわかった。また一般化準巡回符号のグレブナー基底を計算するアルゴリズムを導き、探索手法を確立した。さらにその応用として高速かつ回路規模の小さい符号化システムを構成した。

（2）代数曲線符号に対する符号化・復号化統合モデルの作成：グレブナー基底での除法による従来の符号化法とは異なる、離散フーリエ変換を用いた新しい符号化法を確立した。これは本質的に符号語の冗長位置を消失訂正することに相当し、冗長位置が generic と呼ばれる大多数の場合について組織的符号化が可能である。これによって、空間曲線符号に対しても、やはり符号化と復号化において共通のグレブナー基底・DFT エンジンを用いて回路規模を削減できるようになった。

（3）符号化・復号化統合システムのリード・ソロモン符号への応用：現在主流になりつつある GF(4096)上のリード・ソロモン（RS）符号に対し、提案の符号化・復号化統合システムを応用し、回路規模を削減した。その際、離散フーリエ変換の長さが 4095 となり、計算には通常の FFT を用いることはできないため、fast prime factor DFT（Good-Thomas FFT）を用いた。またこのとき離散フーリエ変換を分割し二度計算しなければならないために遅延が生ずるが、この遅延を解消する目的で離散フーリエ変換計算器を二つ持つシステムを評価した。その結果、図 1 に示すとおり、近い将来必要になると考えられる 60 シンボル訂正可能な RS 符号システムの回路規模を従来のものと比べ 40%削減できるという見積もりが得られた。

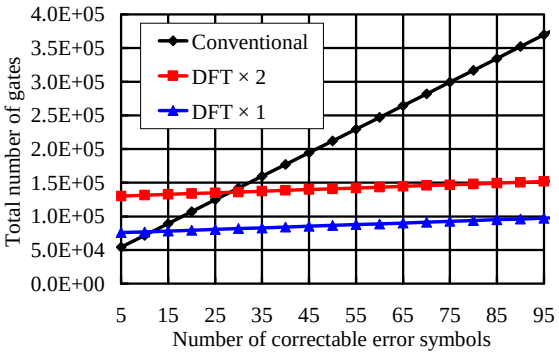

図 1：RS 符号の符・復号化回路規模の比較

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, S. Mita: “A new encoding and decoding system of Reed-Solomon codes for HDD,” IEEE Transactions on Magnetics, Vol. 45, No. 10, pp. 3757-3760, October 2009, 査読有.
2. V. T. Van, H. Matsui, S. Mita: “Computation of Gröbner basis for systematic encoding of generalized quasi-cyclic codes,” IEICE Transactions on Fundamentals, Vol. E92-A, No. 9, pp. 2345-2359, September 2009, 査読有.
3. H. Matsui: “A simple proof of Horiguchi’s error-value formula in decoding of alternant codes and its applications,” IEICE Transactions on Fundamentals, Vol. E92-A, No. 8, pp. 2146-2150, August 2009, 査読有.
4. H. Matsui：“Complexity reduction of encoding and decoding for algebraic-geometric codes by discrete Fourier transforms,” 豊田研究報告, No. 61, pp. 113 - 118, 2008 年 5 月, 査読無し.

〔学会発表〕(計 10 件)

1. H. Matsui, K. Suzuki: “Frame error rate of m-spotty byte error correcting codes,” 第 32 回情報理論とその応用シンポジウム予稿集, pp.351 - 354, December 3 (1-4), 2009.
2. V. T. Van, H. Matsui, S. Mita: “Generalized quasi-cyclic low-density parity-check codes based on finite geometries,” IEEE Information Theory Workshop, pp.158-162, Taormina, Italy, October 13 (11-16), 2009.
3. V. T. Van, H. Matsui, S. Mita: “Low complexity encoder for generalized quasi-cyclic codes coming from finite geometries,” IEEE International Conference on Communications, Dresden, Germany, June 16 (14-18), 2009.
4. V. T. Van, H. Matsui, S. Mita: “An effective systematic encoder implementation for generalized quasi-cyclic codes based on Gröbner bases,” The Second International Conference on Theories and Applications of Computer Science (ICTACS’09), Nha Trang University, Vietnam, February 6-8, 2009.
5. H. Matsui: “Two types of systematic encoding for generalized quasi-cyclic codes,” 第 31 回情報理論とその応用シンポジウム予稿集, pp.731 - 736, October 9 (7-10), 2008.
6. 松井一, Vo Tam Van, 三田誠一:“On a class of generalized quasi-cyclic codes coming from finite geometries -Their systematic encoding and Gröbner basis-,” 電子情報通信学会情報理論研究会, IT2008 - 30, pp.61 - 66, 2008 年 9 月 12 日.
7. H. Matsui: “Unified systems of encoding and decoding for a class of algebraic-geometric codes,” International Symposium on Information Theory and its Applications, pp.400-405, Auckland, New Zealand, December 8 (7-10), 2008.
8. 三田誠一, 松井一:“磁気記録チャネル用信号処理方式の研究経過と今後の展望,” 電子情報通信学会磁気記録・情報ストレージ研究会, MR2007 - 39, pp.53 - 62, 2007 年 12 月 13 日.
9. V. T. Van, H. Matsui, S. Mita: “Systematic encoding for finite geometry LDPC codes based on Gröbner bases,” 第 30 回情報理論とその応用シンポジウム予稿集, pp.424 - 429, November 29 (27-30), 2007.
10. H. Matsui, S. Mita: “Encoding via Gröbner bases and discrete Fourier transforms for several types of algebraic codes,’’ IEEE International Symposium on Information Theory, pp. 2656-2660, Nice, France, June 29 (24-29), 2007.

〔その他〕

ホームページ等

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 (MATSUI HAJIME)

豊田工業大学・大学院工学研究科・准教授

研究者番号：80329854