様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成　25 年　4　月 20 日現在

機関番号：32660
研究種目：基盤研究（C）
研究期間：2010 年　～　2012 年
課題番号：22560391
研究課題名（和文）
多点代数曲線符号の符号化および復号処理の高速化に関する研究
研究課題名（英文）
Research on fast encoding and decoding of multipoint codes from algebraic curves
研究代表者
藤沢匡哉（Fujisawa Masaya）
東京理科大学・工学部経営工学科・准教授
研究者番号：10345431

研究成果の概要（和文）：
本研究では，これまで研究してきた代数幾何符号の復号法の研究を発展させ，1 点代数曲線符号の拡張である多点代数曲線符号に対して高速な復号法を与えた．多点代数曲線符号が 1 点代数曲線符号の部分符号となることを利用して，1 点代数曲線符号の高速復号法である BMS(Berlekamp-Massey-Sakata)アルゴリズムを拡張して適用することで多点代数曲線符号においても高速復号ができることを示し，主符号（L 符号，関数型符号），および，　双対符号（Ω符号，留数型符号）のぞれぞれに対する高速復号法を提案した．

研究成果の概要（英文）：
In this researches, we presented fast decoding methods for primal and dual multipoint codes from algebraic curves which are a broad class of algebraic geometry codes derived from algebraic functions which have multiple poles on their defining curvs.　Since multipoint codes can be viewed as subcodes of one-point codes, they can be decoded efficiently by using the BMS algorithm.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
22 年度	500,000	150,000	650,000
23 年度	400,000	120,000	520,000
24 年度	500,000	150,000	650,000
年度			
年度			
総　計	1,400,000	420,000	1,820,000

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
キーワード：　符号化、誤り訂正符号

１．研究開始当初の背景

通信中に発生する誤りの影響を取り除くための技術である誤り訂正符号は，通信機器のみならず記録装置においても利用され，さらに暗号や秘密分散といったセキュリティの分野においても利用される重要な技術である．これらの応用を考える上で大きな符号長を持ち，優れたパラメータを持つ誤り訂正符号は極めて有用であると言える．このような性能をもち次世代誤り訂正符号として期待されているものの１つに１点代数曲線符号があるが，この符号に比べさらに優れた符号パラメータを持つ多点代数曲線符号と呼ばれる符号が存在する．しかし，1 点代数曲線符号では多項式により符号化・復号処理が取り扱えたのに対し，多点代数曲線符号では

有理関数を取り扱う必要があり，処理が複雑となる．本研究では，多点代数曲線符号を 1 点代数曲線符号の部分符号とみなすことが出来ることに着目し，多項式処理に基づいた符号化・復号処理アルゴリズムにより高速化を目指す．

２．研究の目的

多点代数曲線符号が 1 点代数曲線符号の部分符号となることを利用して，1 点代数曲線符号の高速復号法である BMS (Berlekamp-Massey-Sakata)アルゴリズムを拡張して適用することで多点代数曲線符号においても高速復号ができることを示し，主符号（L 符号，関数型符号），および，双対符号（Ω符号，留数型符号）のぞれぞれに対する高速復号法を提案し，それらの有効性を示す．

３．研究の方法

復号法に関しては 2 点エルミート符号に対する高速復号法である BMS アルゴリズムを拡張し，多点エルミート符号に適用する．配列の設定や関数の取り扱いなどについて詳細に検討を行い，シミュレーションを行うことにより，復号法の実際的な特徴・性能を明らかにする．代数曲線符号の復号法については過去に研究を行っており，本研究にも役立てることができる．また，このアルゴリズムを実装してシミュレーションを行い，実用化に向けての問題点を整理する．

次に符号化の高速化について検討する．符号化はグレブナ基底の計算が必要となるが一般にこの計算は複雑になる．さらに多点代数曲線符号の場合には有理関数の形で取り扱うことになり，従来の 1 点代数曲線符号における符号化の処理より複雑になる．復号法で得られた知見を利用し，符号の構成をうまく限定することで，特殊な状況において高速にグレブナ基底を計算することが可能な BMS アルゴリズムを適用できる．このように高速符号化アルゴリズムを与え，このアルゴリズムが適用可能な符号のクラスの探索，および，整理を行う．

４．研究成果

多点代数曲線符号が 1 点代数曲線符号の部分符号となることを利用して 1 点代数曲線符号の高速復号法である BMS (Berlekamp-Massey-Sakata)アルゴリズムを修正して適用することで多点代数曲線符号においても高速復号ができることを示し、主符号（L 符号、関数型符号）に対する高速復号法を提案した．本手法では order bound までの復号は保証されないが，訂正限界を超えても order bound までは高い確率で復号が k のウであることをシミュレーションにより示した．

次に，双対符号（Ω符号、留数型符号）に対しても高速復号法を提案した．本手法では，受信語からは直接計算できない未知シンドロームを多数決により決定する方法（多数決法）が多点符号に対しても拡張して適用可能であることを示し，従来の設計距離よりさらに大きな設計距離である order bound まで復号可能となることを示した．

これら成果に基づいて，多数決論理が適用できる場合に利用可能である Feng-Rao の 1 点代数曲線符号に対する改良符号の構成法を様々な代数曲線に対して得られる多点符号に対して適用し，符号の性能の評価を行った．結果として，エルミート符号（エルミート曲線により構成される符号）およびいくつかの Cab 曲線符号（Cab 曲線により構成される符号）に対して、1 点符号の改良符号よりも優れた改良多点符号が存在することを示した．

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 2 件）

① Masaya Fujisawa, Shojiro Sakata, ``Improved multipoint codes from Hermitian curves, '' Proceedings of International Symposium on Information Theory and its Applications, 査読有, pp.431--435, Oct. 2012.

② Masaya Fujisawa, Shojiro Sakata, ``On a fast decoding of multipoint codes from algebraic curves, '' Proceedings of 2011 IEEE International Symposium on Information Theory, 査読有, pp.1022--1026, July 2011.

〔学会発表〕（計 4 件）

① 藤沢 匡哉，阪田 省二郎, ``多点代数曲線符号の高速復号について'', 第 33 回情報理論とその応用シンポジウム予稿集, 松代, 2010 11/30-12/3.

② 藤沢 匡哉，阪田 省二郎, ``改良多点エルミート曲線符号について'', 岩手, 第 34 回情報理論とその応用シンポジウム予稿集, 2011 11/29 - 12/2.

③ Shojiro Sakata, Masaya Fujisawa, ``A fast decoding of multipoint codes from algebraic curves up to the order

bound,'' Proceedings of the 34th Symposium on Information Theory and Its Applications, Iwate, 2011 11/29 - 12/2.

④ 藤沢 匡哉, 阪田 省二郎, ``多点Cab曲線符号の改良符号について'', 第 35 回情報理論とその応用シンポジウム予稿集, 別府, 2012 12/11 - 14.

〔図書〕(計　0 件)

〔産業財産権〕
○出願状況（計 0　件)

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　件)

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
藤沢匡哉 (Fujisawa Masaya)
東京理科大学・工学部経営工学科・准教授
研究者番号：10345431

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：