様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月２９日現在

研究種目：基盤研究(C)
研究期間：２００７～２００８
課題番号：１９５６０３６９
研究課題名（和文）　多点代数曲線符号の高速復号法について

研究課題名（英文）　On fast decoding of multipoint codes from algebraic curves

研究代表者
阪田　省二郎（Shojiro　Sakata）
電気通信大学・ 名誉教授
研究者番号：２００６４１５７

研究成果の概要：
本研究は、今まで本研究代表者が着々と実施してきた１点代数曲線符号の効率的な復号法の研究をさらに発展させ、より広い符号クラスである多点代数曲線符号に対し、高速な復号法を導入することが目的である。本研究の成果として、代数幾何符号を構成するのに使われる代数曲線の中で最も重要なHermite曲線を考え、その上で定義できる２点代数曲線符号について、その高速な復号法を確立した。特に、１点代数曲線符号の復号法の拡張として、２点Hermite曲線符号の訂正半径までの誤り訂正を可能とする多数決論理を組み込んだ高速復号法を与えた。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	900,000	270,000	1,170,000
２００８年度	800,000	240,000	1,040,000
年度			
年度			
年度			
総　計	1,700,000	510,000	2,210,000

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：(1)情報通信工学 (2)代数学 (3)アルゴリズム (4)代数幾何符号
(5)高速復号法 (6)多点代数曲線符号 (7)１点代数曲線符号 (8)BMSアルゴリズム

１．研究開始当初の背景

「代数曲線符号」は代数幾何符号とも呼ばれる誤り訂正符号の広範なクラスであるが、ロシアの V.D. Goppa によって 1977 年に初めて提唱された。この符号は現在実用化されている RS 符号等の代数的誤り訂正符号の自然な拡張であるとともに、それらに比べてさらに優れた誤り訂正性能をもっていることが証明されてから、その実用化を目指して世界的な規模で盛んに研

究が行われているものである。特に、近年益々その必要性が高まりつつある、より高速、かつ、より正確な情報通信を可能とし、高度情報化社会を支える基盤をより強固なものとするためには、このような高性能な誤り訂正符号の「高速な復号法」の開発が不可欠である。従来主に研究が進められた代数曲線符号は、定義曲線上の特定の 1 点における局所的性質を利用した「 1 点代数曲線符号」と呼ばれるもので、このクラスの符号については、本研究代表者が初めて提唱したアルゴリズム［1］（BMS アルゴリズムと呼ばれる）を適用し、世界的に他の多くの研究者達と競合しつつ拡張、発展させた高速復号法［2］が有効である。しかし、これら 1 点代数曲線符号は、一般の代数曲線符号の部分クラスであり、より広く、定義曲線の複数個の点における性質をも利用した「多点代数曲線符号」のクラスについては、未だそれらの高速復号法の研究は始められたばかりであった。数学者達によってこれら多点代数曲線符号の構造の一部を明らかにする研究成果が得られていた［3］が、復号法についての結果は殆ど与えられていなかった。

代数幾何符号は、その導入直後、ロシアの研究者達を中心に盛んに研究が進められ、最適な符号性能の下界である Varshamov-Gilbert 限界を超えるよい符号の系列が含まれることが明らかにされた。その後、設計距離の半分までの誤り訂正を実現する限界距離復号法の研究が世界的に盛んに行われ、中でも、J. Justesen と T. Hoeholdt の研究グループは、初めて代数幾何符号の有効な復号法を示したばかりでなく、彼等の方法に、BMS アルゴリズムを適用して高速化が可能であることを指摘した。それ以来、本研究代表者は、彼等との研究交流を開始し、密接な研究協力の下、高速な限界距離復号法について著しい成果を挙げ、それを発表してきた([2]等)。これと殆ど同時期に、本研究代表者の成果と同等な研究発表が続出した（[4]等）が、このことは本研究代表者の行ってきた代数曲線符号に対する復号法の研究の先見性と意義を証明するものと考えられる。一方、最近になって、従来の RS 符号、さらには、代数幾何符号に対するリスト復号法が M. Sudan 等により与えられた。これは、通常の誤り訂正限界を超える復号を多項式計算量をもつ代数的なアルゴリズムによって達成し、その結果として軟判定復号を多項式時間で実現可能とするものであり、最尤復号の性能に迫ることを目指している。本研究代表者は、このリスト復号に対しても、それを高速化するための様々な提案を行ってきた([5]等)。以上のように、高速復号法の研究において、本研究代表者は世界的な評価の下で、鋭意その研究成果を着々と挙げて来た。しかし、これらの結果を実用化に導くには、現在までに得られた成果だけでなく、さらなる探求が必要であるが、本研究代表者の今までの研究実績が、そのための強力な手がかりを与えることが期待された。

関連文献:

[1] S. Sakata, Finding a minimal set of linear
recurring relations capable of generating a given
finite two-dimensional array, J. Symbol. Comp.,
Vol.5, pp.321--337, 1988.
[2] S. Sakata, H.E. Jensen, T. Hoeholdt, Generalized Berlekamp-Massey decoding of algebraic geometric codes up to half the Feng-
Rao bound, IEEE Trans. Inform. Theory, Vol. 41,No.6, Part I, pp.1762--1768, 1995.
[3] M. Homma, S.J. Kim, Goppa codes with Weirstrass pairs, J. Pure Appl. Algebra, Vol.162, pp.273--290, 2001.

[4] K. Saints, C. Heegard, Algebraic-geometric
codes and multidimensional cyclic codes: A uni-
fied theory and algorithms for decoding using
Groebner bases, IEEE Trans. Inform. Theory,

Vol.41, No.6, Part I, pp.1752--1761, 1995.
[5] S. Sakata, On fast interpolation
method for Guruswami-Sudan list decoding
of one-point AG codes, in Applied Algebra,
Algebraic Algorithms and Error-Correct-
ing Codes: Proc. AAECC-14 (Eds. S. Boztas,
I.E. Shparlinski), Springer Verlag:
Berlin, pp.172--181, 2001.

２．研究の目的

本研究では、今まで本研究代表者が着々と実施してきた 1 点代数曲線符号の効率的な復号法の研究をさらに発展させ、より広い符号クラスである多点代数曲線符号に対し、高速な復号法の導入を目指す。研究の開始時点では、最近分かってきた２点符号の構造を用いて、その高速復号法をいかに構築するかを探求する。同時に、以上のための理論体系の構築ばかりでなく、具体的な符号に対しこの高速アルゴリズムを適用したときの、実際的な特徴、性能を明らかにするため、種々の条件の下でのシミュレーションを行う準備にかかる。特に、より多くの点数の多点符号の高速復号法を模索する一方で、2点符号についての復号法を実現し、そのシミュレーションを行うことによって、実用化に向けての問題点を整理し、その解決策を練っていく。

３．研究の方法

(1) 新しいアルゴリズムの追求: 現在までの研究結果を整理するとともに、残された問題点を追求し、新しいアルゴリズムを探究する。まず、本研究代表者が今まで 1 点代数曲線符号に対して展開してきた方法を拡張し、当初のアイデアに基づき、2 点代数曲線符号の高速復号アルゴリズムを構築する。その間、既に得られている多点代数曲線符号の構造に関する知見を整理しておく。

(2) シミュレーション: 以上の理論的な研究と併せて、新たに導く２点代数曲線符号、および、３個以上の点により定義される多点代数曲線符号の高速復号アルゴリズムのシミュレーションを行う。まず、理論的な研究が進捗した段階で、構成した２点代数曲線符号の高速復号アルゴリズム、および、できれば３点以上の多点代数曲線符号の高速復号アルゴリズムを計算機上にインプリメントし、これらの方法をシミュレートするプログラムを実現する。そして、計算機実験によりこれらのアルゴリズムの実際的な時間計算量等の性能を調べる。

(3) 研究交流、研究発表: 情報理論とその応用学会、電子情報通信学会等に参加し、国内の関連分野の研究者と研究交流・研究打ち合せを行う。一方、コンピュータネットワークを通じて、以前より研究協力を継続的に行っているデンマーク工科大学のグループと情報交換を行い、研究の進捗を図る。また、関連国際学会、特に、IEEE国際情報理論シンポジウム等に参加し、アイデア段階での予備的成果の発表を行う。

(4) 分担: 以上の研究過程において、研究代表者と研究分担者は協力して理論上の問題解決に当たる一方、代表者がアルゴリズムの提案を行う。その上で、構築するアルゴリズムのインプリメントとシミュレーションを、研究代表者の統括の下で実施する。研究成果を論文としてまとめる仕事は、研究代表者が中心となって行う。

４．研究成果

本研究は、今まで本研究代表者が着々と実施してきた１点代数曲線符号の効率的な復号法の研究をさらに発展させ、より広い符号クラスである多点代数曲線符号に対し、高速な復号法を導入することが目的である。本研究の成果として、代数幾何符号を構成するのに使われる代数曲線の中で最も重要なHermite曲線を考え、その上で定義できる２点代数曲線符号について、その高速な復号法を確立した。特に、１点代数曲線符号の復号法の拡張として、２点Hermite曲線符号の訂正半径までの誤り訂正を可能とする多数決論理を組み込んだ高速復号法を与えた。そして、計算機シミュレーションによりその有効性と高速性を確認した。この成果を、電子情報通信学会等の学会誌に再投稿するべく改訂を行っているが、preprint の形でまとめた論文（電子情報通信学会英文論文誌のフォーマット）を作成した。そこには、本研究成果の主要な内容を盛り込んであるので、以下にその抜粋を掲載する（数式部分は Latex source formで記載; Latex によりコンパイルすれば、通常の数式表示が得られる)。なお、３点以上の多点符号に対する有効な高速復号法は未だ得られなかった。

その他、本研究に関連する成果として、先ず、電子情報通信学会基礎境界ソサイエティ Fundamentals Review の第１巻第３号に「代数的符号理論」一般についての解説記事を出版（電子出版）した。さらに、2009年にSpringer社から出版される論文集 Groebner Bases, Coding and Cryptography 中に、これら高速復号法の基本である BMS（Berlekamp-Massey-Sakata）アルゴリズムと代数曲線符号の復号への応用に関する２編の解説論文を発表する。また、やはり2009年に公開される電子情報通信学会知識データベース「符号理論」篇中に記載した２項目、「代数幾何符号」と「代数幾何符号の復号法」を発表する。2007年末、および、2008年末にそれぞれ開催された 第30回、第31回 情報理論とその応用シンポジウム では、代数幾何符号の新しい復号法であるリスト復号の拡張についての高速化の試みと代数曲線符号の並列的な復号法についての研究発表を行った。

以上の成果は、今後さらにシミュレーション等を重ねて、改良を加えることにより、近い将来、これらの方法が実用化される際、有用な指針となるであろうと考えている。

発表予定論文抜粋（Latex source file）:

Title: Fast decoding of two-point Hermitian codes

Author: S. Sakata, M. Fujisawa

Summary: Two-point AG codes are a natural extension of one-point AG codes which have been investigated by many researchers. Depending on the values of parameters, they have similar or better performances in comparison with one-point codes. We present a fast decoding method of two-point Hermitian codes as a generalization of fast decoding methods of one-point codes. The special structure of 2D syndrome arrays of these codes allows us to apply a modification of the BMS algorithm to decoding them up to the generalized order bound.

1. Introduction

Hermitian codes [Stichtenoth 1988] are a typical class of algebraic geometry (AG) codes which has been not used yet in practice as Reed-Solomon codes, but which seems to have the best chance of being used eventually [Justesen, Hoeholdt 2004]. Although RS codes are optimal linear codes in the sense that they have the largest minimum distance among all the linear codes of the same codelength and dimension (the Singleton bound), they cannot have codelength larger than the size q of the defining finite field ${¥bf F}_q$. It is known that we can have AG codes of larger codelengths which have better performance and that there are a series of AG codes with correction performance approaching the Varshamov-Gilbert bound or more [Tsfasman, Vladut, Zink 1982] [Tsfasman, Vladut 1991]. Furthermore, AG codes are a natural extension

of the conventional practical algebraic codes, and some basic decoding methods [Skorobogatov, Vladut 1990] [Feng, Rao 1993] based on Gaussian elimination and their fast versions based on the BMS algorithm have been proposed for them. But, there still remain many things to be investigated about construction and decoding of AG codes [Sakata 2008]. A codeword of an (N,K) AG code over a finite field ${¥bf F}_q$ is given as a vector $c=(c_j)$ with $c_j=f(P(j))$, $1¥leq j¥leq N$ for a set ${¥cal P}=¥{P(j)¥mid 1¥leq j¥leq N¥}$ of points $P(j)$ on an algebraic curve (or surface) ${¥cal X}$ over ${¥bf F}_q$ and a linear space ${¥cal L}$ (of dimension K) of algebraic functions f on ${¥cal X}$ having values in ${¥bf F}_q$. While a Reed-Solomon code (of codelength $N=q-1$) over ${¥bf F}_q$ is defined by the pair $({¥cal P},{¥cal L})$ for the set ${¥cal P}$ of points on a straight line ${¥cal X}$ over ${¥bf F}_q$ (or rather the set ${¥cal P}$ of all nonzero elements $P(j)=¥theta^{j-1}$ for a primitive element $¥theta$ of ${¥bf F}_q$) and the linear space ${¥cal L}$ of polynomials (rational functions) of degree $K-1$ or less, a one-point Hermitian code over ${¥bf F}_q$ with $q=q_1^2$ is defined by the pair $({¥cal P},{¥cal L})$ for the set ${¥cal P}$ of all the points $P(j)=(p_1(j),p_2(j))$ ($¥in {¥bf F}_q^2$), $1¥leq j¥leq N$ on the Hermitian curve ${¥cal X}$:

¥begin{eqnarray}
x^{q_1+1}=y^{q_1}+y ¥label{eqn:hermitian}
¥end{eqnarray}

and a linear space ${¥cal L}={¥cal L}(m P_{¥infty})$ of algebraic functions (bivariate polynomials) on ${¥cal X}$, where the codelength N is the number q_1^3 of all affine points P_j of the curve ${¥cal X}$ and ${¥cal L}$ is composed of functions having a single pole with pole order less than or equal to a fixed integer m ($<N$) at the unique point $P_{¥infty}$ of infinity on the (projective) Hermitian curve.

One-point AG codes such as one-point Hermitian codes are a class of important AG codes defined by a linear space of algebraic functions having a single pole on their defining curve, which have been treated by many researchers (see [Hoeholdt, Lint, Pellikaan 1998]). Recently, as a natural extension of researches on one-point AG codes, two-point AG codes have been investigated. Two-point AG codes such as two-point Hermitian codes are AG codes defined by a linear space of algebraic functions having only two poles on their defining curve. These two-point codes have similar and sometimes better performances in comparison with one-point codes, depending on the values of parameters [Matthews 2001] [Matthews 2004] [Homma 2004] [Homma, Kim 2005] [Homma, Kim 2006].

For one-point codes it is known that, in case of codes from plane curves such as one-point Hermitian codes, one obtains a syndrome array defined over a subset of the two-dimensional (2D) integral lattice ${¥bf Z}_0^2$ from a received word, where ${¥bf Z}_0^2$ is the set of pairs of nonnegative integers, so that one can have a class of fast decoding methods up to the designed distance called the Feng-Rao bound of those codes [Sakata, Justesen, Madelung, Jensen, Hoeholdt 1995] [Sakata, Jensen, Hoeholdt 1995] by applying the BMS algorithm [Sakata 1988] [Sakata 1990] to such a 2D array.
But, it seems that one does not have such a simple structure over ${¥bf Z}_0^2$ for more general AG codes different from one-point codes so that one cannot have a direct application of the BMS algorithm or similar fast algorithms to decode them.
Recently a class of codes called codes from order domains, which is a generalization of one-point AG codes, and their decoding method up to the order bound, which is a generalization of the Feng-Rao bound, based on the BMS algorithm have been presented [Geil 2002]. Furthermore, for multiple-point codes, the generalized order bound [Beelen 2007] and a basic decoding method up to that bound [Beelen06] have been introduced, whose calculation is based on Gaussian elimination.

In this paper we present an extension of the BMS algorithm to the case of an incomplete array (in the sense of the definition described in the last paragraph of Section 2 and in Section 3). By applying this modified algorithm to syndrome arrays of dual two-point Hermitian codes, which still have some nice structure, we can have an efficient decoding method of these codes up to the generalized order bound. The layout of this paper is as follows: we give a review of one-point codes and their fast decoding methods in Subsection 2.1, and discuss

two-point Hermitian codes and their structure in Subsection 2.2 as preliminaries. Then, we present a generalization of the BMS algorithm called the submodule BMS algorithm in Section 3, and discuss fast decoding of two-point Hermitian codes up to the generalized order bound in Section 4. In Section 5, we give some concluding remarks.

(中略)

5. Concluding Remarks

We have given a nontrivial modification of BMS algorithm for incomplete arrays defined over a subset of a stable set in the whole 2D lattice ${¥bf Z}_0^2$. By applying this submodule BMS algorithm with majority logic to a syndrome array defined over such a subset, we can decode the dual two-point Hermitian code up to the generalized order bound introduced by Beelen [Beelen07]. This decoding algorithm can be applied to codes from norm-trace curves [Geil 2003] which are a generalization of Hermitian curves. The computational complexity of our algorithm is ${¥cal O}(N^{¥frac{7}{3}})$ similar to the BMS algorithm of decoding one-point codes. At present, generalization of our method to either three- or more-point Hermitian codes or two-point codes from other kinds of curves seems to be difficult, which will be our future work.

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 6 件）
(1) 阪田省二郎, 代数幾何符号の復号法, 電子情報通信学会知識ベース, 「符号理論」篇, 電子情報通信学会, 2009 (to be published in the homepage).
(2) 阪田省二郎, 代数幾何符号, 電子情報通信学会知識ベース, 「符号理論」篇, 電子情報通信学会, 2009 (to be published in the homepage).
(3). S. Sakata, The BMS algorithm and decoding of algebraic geometry codes, Groebner Bases, Coding and Cryptography (eds. M. Sala, et.), Springer, 2009 (to be published).
(4) S. Sakata, The BMS algorithm, Groebner Bases, Coding and Cryptography (eds. M. Sala, et.),
Springer, 2009 (to be published).
(5) 阪田省二郎, 代数的符号理論, Fundamentals Review, vol.1, no.3, pp.44--57: http:/www.ieice.org/ess/ESS/Fundam-Review.html, 電子情報通信学会基礎境界ソサイエティ, 2007.
(6) M. Fujisawa, S. Sakata, A construction of high rate quasi-cyclic regular LDPC codes from cyclic-difference families with girth 8, IEICE Transactions: Fundamentals, vol.E90-A, no.5, pp.1055--1061, 2007.

〔学会発表〕（計 2 件）

(1) 藤沢匡哉, 阪田省二郎, 1点代数曲線符号に対する array-vector BMS 復号法に関する一考察, 第 31 回情報理論とその応用シンポジウム予稿集, 日光, 鬼怒川温泉, pp.727--730, 28 Nov. 2008.
(2) 阪田省二郎, 藤沢匡哉, Decoding of AG codes beyond GS list decoding radius, 第30回情報理論とその応用シンポジウム予稿集, pp.27--30, 三重, 賢島, 28 Nov. 2007.

〔図書〕（計 1 件）

(Eds.) M. Sala, T. Mora, L. Perret, S. Sakata, C. Traverso, Groebner Bases, Coding, and Cryptography, Springer Verlag (総ページ数: 390), 2009

６．研究組織

(1)研究代表者

阪田、省二郎 (Shojiro Sakata)
電気通信大学 名誉教授
研究者番号：20064157

(2)研究分担者

栗原、正純 (Masazumi Kurihara)
電気通信大学 電気通信学部 助教
研究者番号：90242346

藤沢、匡哉 (Masaya Fujisawa)
東京理科大学 第二工学部 講師
研究者番号：10345431