様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ４ 月 ２３ 日現在

機関番号：３２６６０
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ０４４９０

研究課題名（和文）双対多点代数曲線符号の高速リスト復号に関する研究

研究課題名（英文）Study on an efficient list decoding for dual codes of multipoint codes on algebraic curves

研究代表者

藤沢　匡哉（FUJISAWA, Masaya）

東京理科大学・工学部情報工学科・准教授

研究者番号：１０３４５４３１

交付決定額（研究期間全体）：（直接経費）　　2,000,000円

研究成果の概要（和文）：本研究では、多点代数曲線符号の双対符号に対して、限界距離復号法の効率的手法であるBerlekamp-Massey-Sakata(BMS)アルゴリズムを拡張することによって訂正限界を超えた復号を可能にするリスト復号の効率的な復号法を与え、さらに効率的に復号を行うためにリスト復号の際に発生する無駄な分岐を確率的に削減する方法について検討した。極小多項式の更新に関係する次数、スパン、票数等を利用した確率的選択を検討したが有効な成果は得られなかった。
最終的な成果としては、これらの研究のために作成した代数曲線符号のリスト復号のpython言語によるライブラリが挙げられる。

研究成果の学術的意義や社会的意義
本研究において多点代数曲線符号の双対符号に対するリスト復号法の基本的なアルゴリズムについてpython言語によるライブラリを作成しており、これらは今後のリスト復号の研究に活用できると考えている。例えば、pythonでは深層学習のライブラリが整っており、これらと連携した手法の検討が容易に出来るようになる。また、符号の訂正能力を超えて訂正ができるリスト復号は、記録媒体のような情報の再送が難しい状況においては重要な技術であるといえ、社会的な貢献もあると考えている。

研究成果の概要（英文）：This study gives a decoding method for list decoding that enables decoding beyond the correction capability by extending the Berlekamp-Massey-Sakata (BMS) algorithm, which is known as an efficient method for bounded distance decoding, for the dual codes of multi-point codes on algebraic curves. Furthermore, a efficient method for probabilistically reducing unnecessary branches in list decoding was investigated. Stochastic selection using the degree, span, number of votes, etc. related to the update of minimal polynomials was considered, but no effective results were obtained.
A final result is a library in the python language for list decoding of algebraic curve codes created for this study.

研究分野：符号理論

キーワード：代数曲線符号　多点符号　BMSアルゴリズム　リスト復号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

通信機器・記録装置において発生する誤りの影響を取り除くための技術の 1 つに誤り訂正符号がある．誤り訂正符号は，情報を効率的に伝送するためにある一定の規則に従って情報を付加することによって通信路で発生した誤りをある範囲（これを訂正限界という）までならば訂正可能にする技術である．通常，誤り訂正符号を設計する際には，通信路が悪い状況を想定した時に発生する誤りを訂正できるように訂正限界を決め，その限界以内の誤り訂正を保証する限界距離復号を用いる．これに対して，訂正限界を超えた個数の誤りを訂正するリスト復号法がある．限界距離復号では復号後に得られる符号語は 1 つであるが，リスト復号では正しい符号語を含む設計距離内(訂正限界を超える) にあるすべての符号語が複数列挙される．

高い信頼性を保証する必要がある CD・DVD や HD などの記録系に用いられることが多い代数的符号の中で重要な符号として，リード・ソロモン符号や代数曲線符号が存在する．代数的符号の中でも代数曲線符号は符号長が大きく，優れた性能を持つため次世代符号として期待されている．近年，記録・通信の大容量化が進む中，ノイズの影響はより一層大きくなり，高い誤り訂正能力をもつ符号が必要となっている．このような状況において，多点代数曲線符号は従来研究されてきた 1 点代数曲線符号の一般化であり，符号構成の自由度が増すため，優れた性能をもつことが示されており注目されている．

代数曲線符号に対する復号法は，最初に双対符号に対する限界距離復号が研究され，その拡張として様々な研究が発展してきた．我々は，多点代数曲線符号に対する限界距離復号法の高速復号法を 1 点代数曲線符号の高速復号法である Berlekamp-Massey-Sakata 法(1994) を拡張することにより，主符号(2014) および双対符号(2016) のそれぞれについて提案してきた．一方，リスト復号法については，Sudan によって 1997 年に与えられた Reed-Solomon 符号に対する方法をもとにして発展してきた．Matsumoto，Geil，Ruano(2016) は，代数曲線符号の主符号の限界距離復号法である Lee-Amoros-O'Sullivan 法(2014) を拡張し，限界距離復号を行う際の多数決において算出されるすべての候補シンドロームに対して復号を行うことにより，リスト復号が可能であることを示した．この手法は Sudan により提案されたリスト復号法と異なり，多数決論理を用いながら逐次的に候補符号語を求める方法となっている．

主符号に対する復号法は符号語と受信語に基づいた補間多項式を求める問題，双対符号に対する復号法はシンドローム系列を生成する最簡な多項式を求める問題とみなすことができ，互いに関連している．Reed-Solomon 符号においては，主符号・双対符号それぞれに対して，符号の性質，および，復号法について詳細に検討され，互いの関係についても明らかにされている．これに対して，代数曲線符号の双対符号に対するリスト符号の研究はほとんどなく，この復号法の検討は，研究の網羅性の観点から，および，主符号に対する復号法との互いの手法の関係について統一的に見ることによる新しい知見の獲得の可能性からも重要であると考える．そこで，まず，我々は Matsumoto，Geil，Ruano の手法と同様な考え方で，限界距離復号法の高速復号法である Sakata-Fujisawa 法(2016) を拡張することにより，リスト復号法を与える．さらに，リスト復号は訂正能力を超えたところから探索する分岐が膨大に増えていくため，計算時間も膨大となる点が問題であり，計算時間の削減が期待されている．

２．研究の目的

多点代数曲線符号の双対符号に対して，Berlekamp-Massey-Sakata(BMS)アルゴリズムを拡張することによって，訂正能力を超えた復号を可能にするリスト復号のアルゴリズムを与える．リスト復号は可能性のある符号語を列挙する復号法であり，復号には膨大な時間がかかる．そこで，代数的な計算法として知られているグレブナ基底の計算アルゴリズム(Buchberger's algorithm)に対して確率的な手法を取り入れることにより高速なアルゴリズム(F4)を実現した J.C. Faugere による研究を参考にして，確率的な手法をリスト復号に取り入れて高速なリスト復号を与える．

さらに，Reed-Solomon 符号では主符号と双対符号に対する復号法の関係について明らかになっているが，本研究を通して Reed-Solomon 符号の拡張である代数曲線符号においても主符号と双対符号のリスト復号法の関係を明らかにする．

３．研究の方法

まず，1 点代数曲線符号の双対符号の高速復号法である Berlekamp-Massey-Sakata アルゴリズムを拡張し，リスト復号法を与える．この復号法では，未知シンドロームを求める段階で正しい候補値を与える極小多項式のグループを多数決論理によって定めるが，多数決論理により

与えられる候補値のそれぞれについて分岐して現れるシンドロームのすべてについて復号を行うことになる．このように訂正能力を超えたところから分岐が膨大に広がる．そこで，効率的に計算を行うために，すべての分岐を探索するのではなく確率的に可能性の高い極小多項式を選択して計算を進める方法の可能性について検討する．そのために，多数決における各シンドロームに対する極小多項式（誤り位置多項式の候補となる多項式）の関係を明らかにして，それらを効率的に求める方法を検討する．例えば，極小多項式に付随するの次数・スパン・票数との関係について何らかの知見が得られないか検討する．この検討のためにはリスト復号法の実装が必要であるが，深層学習などのライブラリの充実を考慮して，従来の研究で準備していた C 言語による限界距離復号法のプログラムを Python 言語に変換し，リスト復号法のプログラムを作成する．1 点代数曲線符号に対する効率的なリスト復号法を与えた後は，それらの効率について詳細に検討を行い，主符号と双対符号に対するリスト復号法の関係について明らかにする．最終的には，多点代数曲線符号に対しても同様のリスト復号法が成立することを示す．

４．研究成果

多点代数曲線符号の双対符号に対して、Berlekamp-Massey-Sakata(BMS)アルゴリズムを拡張することによって，訂正能力を超えた復号を可能にするリスト復号のアルゴリズムを与えた．しかし，極小多項式の次数・スパン・票数から得られる知見により確率的に無駄な分岐を減少させる方法については有効な手段は得られていない．

これらの調査に必要な代数曲線符号のリスト復号のプログラムを C 言語から Python 言語に書き直したことは，Python 言語の深層学習ライブラリとの連携についての今後の検討の展開のしやすさを考えると，１つの成果として挙げられる．

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関