様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月　 ６ 日現在

機関番号：３２６７０
研究種目：基盤研究(C)（一般）
研究期間：2012～2015
課題番号：２４５４００５２

研究課題名（和文）代数幾何符号の一般理論の研究

研究課題名（英文）Research on the general theory of algebraic-geometric codes

研究代表者
中島　徹（Nakashima, Toru）

日本女子大学・理学部・教授

研究者番号：２０２４４４１０

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：誤り訂正符号の技術は現代の情報通信に於いては不可欠である。その中でも有限体上の代数多様体の幾何学を用いて構成される代数幾何符号は優れた漸近的性質を備えている。当課題ではこれまで知られている全ての代数幾何符号を統一する一般理論を確立することを提唱し、その基本的性質に関して研究を行った。その結果、関数体上の代数多様体や算術的多様体上のベクトル束を用いて新しいタイプの代数幾何符号を構成し、それらのパラメーターを決定することに成功した。

研究成果の概要（英文）：The technique of error-correcting codes is an indispensable tool in the modern data transmission. Among them, the algebraic-geometric codes constructed from the geometry of algebraic varieties defined over finite fields are equipped with excellent asymptotic properties. In the present research, we proposed to establish the general theory which unifies the known algebraic-geometric codes and investigated its fundamental properties. As a result of the research, we constructed some algebraic-geometric codes of novel type from vector bundles on algebraic varieties defined over function fields or arithmetic varieties and determined their parameters.

研究分野：代数幾何学

キーワード：代数幾何符号　ベクトル束

１．研究開始当初の背景

（１）ブロック符号と畳み込み符号

デジタルデータを送信する際には通常誤りが発生する。生じた誤りを訂正するためには誤り訂正符号と呼ばれる数学的手法が用いられる。送信の効率性や訂正可能な誤りの個数などの符号の性能は、長さ、次元、最小距離などパラメーターと呼ばれる量によって測ることができる。誤り訂正符号は大きくブロック符号と畳み込み符号に分けられる。ブロック符号とは有限体上のベクトル空間の部分空間であり、CD や DVD の再生、QR コードなど我々の身近なところでも用いられている。一方、畳み込み符号とは有限体上の 1 変数有理関数体上のベクトル空間の部分空間である。畳み込み符号は変数 t を時間と見做して過去のデータにも依存した符号化を行うため、ブロック符号よりも高い誤り訂正能力を持ち、宇宙空間での通信や携帯電話に用いられる。

（２）Goppa 符号と Savin 符号

ブロック符号の中でも代数曲線上の直線束を用いて構成される Goppa 符号は代数幾何の方法を用いて次元や最小距離の評価が可能であり、高い性能を備えていることが知られている。近年 Savin によって代数曲線上の高階のベクトル束を用いて Goppa 符号の一般化が定義された(Savin 符号)。彼の研究では、ベクトル束に対して弱安定性と呼ばれる条件を仮定すると符号のパラメーターの評価が出来ることが示された。符号理論ではバースト誤りに対応するためにデータの送信順序を変更するインターリーブと呼ばれる操作が用いられるが、Savin 符号は Goppa 符号のインターリーブ化を代数幾何的観点から一般化した符号と見做すことが可能である。

（３）中島による Savin 符号の研究

一般のベクトル束は直線束と比較して階数という自由度をもつため、Savin 符号は Goppa 符号より高い性能をもつ可能性があると期待された。当研究の代表者である中島は、平成２１年度から平成２３年度にかけて科学研究費補助金基盤研究(C)（「ベクトル束の評価写像を用いた誤り訂正符号の研究」）の補助を受けて、Savin 符号の性質に関して研究を行った。その結果、弱安定性条件を一般化したα-安定性概念を導入して Savin 符号のパラメーターの評価式を改良することに成功した。また、フロベニウス写像による安定束の順像を用いてα-安定なベクトル束を曲線上に構成する方法を開発し、Savin 符号の多くの具体例を与えた。

（４）畳み込み符号の代数幾何的研究

ブロック符号と比較すると畳み込み符号の代数幾何的研究はこれまで殆ど行われてこなかったが、最近 Perez-Porras-Sotelo は 1 変数有理関数体上定義された曲線上の直線束の大域切断を有限個の有理点で評価することにより、代数幾何の手法を用いて畳み込み符号を構成できることを示した(畳み込み Goppa 符号)。一方、彼らの研究では Savin 符号と畳み込み符号を統一的に扱うための代数幾何符号の理論はまだ確立されていなかった。

２．研究の目的

１．で述べたように代数幾何学の手法は近年ブロック符号から畳み込み符号にわたる広い範囲の誤り訂正符号に用いられるようになって来た。そこで当課題では以下に述べる具体的目標を設定した。

（１）　一般代数幾何符号のパラメーター

Savin の研究と Perez-Porras-Sotelo の研究に触発され、当課題ではブロック符号と畳み込み符号およびそれらのインターリーブ化を代数幾何学の手法により統一する理論を確立することを目的とした。そのために有限体上有限生成の体(以下関数体と呼ぶ)の上で定義された射影多様体とその上のベクトル束を用いて、Goppa 符号、Savin 符号および畳み込み Goppa 符号の概念を同時に一般化した符号（一般代数幾何符号）を定義し、そのパラメーターを決定することを課題とした。

（２）一般代数幾何符号の漸近的性質

符号の無限列のパラメーターが無限大の近傍でどのように振る舞うかという漸近的性質を明らかにすることは符号理論の重要な問題である。当課題では、関数体上の射影多様体とその上のベクトル列の族を上手く選ぶことによって良い漸近的性質をもつ一般代数幾何符号の列を構成することを目的とした。

（３）一般代数幾何符号の復号法

畳み込み符号の復号法としては Viterbi 復号法が良く知られているが、代数幾何的復号法は未だ見つかっていない。当課題では、Goppa 符号の代数幾何的復号法である Johnson の方法を関数体の場合にまで拡張することによって一般代数幾何符号の効率的復号法を開発することを目的とした。

（４）Arakelov 幾何との関係

符号の無限列の自然な例として固定した直線束の n 回テンソル積から定まる符号列がある。このような符号列の次元の漸近的振る舞いは Arakelov 幾何の最近の研究に於いて現れて来たエルミート直線束の体積と密接に関係しているため、算術的多様体の交点理論と符号理論との間に未知の関係があることが予想された。そこで、当課題では一般代数

幾何符号と Arakelov 幾何の関係を解明することを目的とした。

３．研究の方法

当課題では、２．で述べた目的を達成するために以下のような研究方法を取った。

（１）関数体上の代数多様体のモデル
関数体上定義された射影多様体 X とその上のベクトル束 E の組(X,E)が与えられたとき、X を生成ファイバーとする有限体上のファイブレーション Y→B 及び Y 上のベクトル F で X 上 E に一致する F の組(Y,F)を(X,E)のモデルと呼ぶ。X の K-有理点はモデル Y の B 上での切断 B→Y と対応するため、(X,E)から定義される一般代数幾何符号のパラメーターの性質を調べるためにモデル(Y,F)を用いることが有効であると期待された。当課題では F が安定束の場合には高次のコホモロジー群が消えて符号のパラメーターの評価が可能になると予想した。そこで与えられた(X,E)から安定なモデル(Y,F)を構成し、一般代数幾何符号のパラメーターを決定することを計画した。

（２）安定ベクトル束の制限定理
一般代数幾何符号の漸近的性能の研究に於いては、関数体上の射影多様体 X 上に弱安定ベクトル束の十分多くの族を構成する必要がある。そのためには X のモデル上の安定ベクトル束 F を X 上へ制限することによって X 上の弱安定束を構成することが重要である。このような安定束の制限定理は曲面の場合には既に中島が以前の研究で証明していたが、より一般に、与えられた非特異射影多様体上の安定束を因子へ制限したときに弱安定となることを適当な仮定の下で成り立つことが予想された。そこで当課題では高次元の場合にも制限定理を証明することによって漸近的に良い一般代数幾何符号の列を構成することを計画した。

（３）Arakelov 幾何学
整数論と代数幾何の双方の分野では代数体と関数体で類似の結果が平行して成立することが良く知られている。この哲学に基づくと、一般代数幾何符号の「算術的類似」が存在する可能性が期待される。体上の代数幾何学の算術的類似は Arakelov 幾何学と呼ばれる。有限体上の代数曲線とその上のベクトル束の算術的類似は算術的曲線(即ち代数体の整数環の素イデアルの集合)X とその上のエルミートベクトル束(E,h) (即ちベクトル束 E と無限遠点上でのエルミート計量 h の対)である。当課題では、エルミートベクトル束を有限個の点で評価することによって Savin 符号の算術的類似を構成し、(E,h)に Arakelov 幾何を用いて適当な安定性条件の下で符号のパラメーターを評価することを計画した。

４．研究成果

当課題では、３．で述べた方法を用いて研究を行い、以下の様な成果を得た。

（１）一般代数幾何符号のパラメーター
関数体 K の上で定義された非特異射影多様体 X とその上のベクトル束 E の大域切断を X の有限個の K-有理点で評価することにより、一般代数幾何符号 C(X,E)を定義した。K の超越次数が１で E が直線束の場合には C(X,E)は Perez-Porras-Sotelo の定義した畳み込み Goppa 符号に一致し、E が高階のベクトル束の場合にはそのインターリーブ化を与えていると見做せる。当課題では K の基礎体上の超越次数が1の場合に C(X,E)の考察を行った。その結果、X が代数曲線の場合には、適当な安定モデルの存在を仮定すると C(X,E)の次元を計算出来ることが証明出来た。特に X が楕円曲線の場合には n 個の X の有理点があれば 0<d<rn を満たす整数 r と d に対しては階数 r と次数 d をもつ半安定束が存在することが Pumplun の定理から導かれる。この事実から、Mordell-Weil 群(即ち X のが正の階数をもつ楕円曲線上では、幾らでも大きな次元をもつ一般代数幾何符号の無限列が存在することが導かれる。
より一般に K の超越次数が 2 以上の場合には符号 C(X,E)は「高次元畳み込み符号」と呼ばれる符号を代数幾何的に構成したものになっているが、この方面では残念ながら成果が挙げられなかったため今後の課題としたい。

（２） 算術的 Savin 符号の構成
当課題の当初の予定では一般代数幾何符号の研究が主な目的であったが、研究の過程で Arakelov 幾何を用いて新しいタイプの代数幾何符号を構成することに成功した。より具体的には、算術的曲線 X とその上のエルミートベクトル束(E,h)の算術的切断(即ち E の大域切断で h に関するノルムが１以下のもの)を X の各点で評価することにより Savin 符号の算術的類似(算術的 Savin 符号)を構成した(論文①)。この符号は E が自明な直線束の場合には、Grusuwami-Lenstra によって導入された代数体符号に一致することが分かる。ここで代数体符号とは代数体 K の整数環の有限個の素イデアルでの剰余体達の直和を用いて定義される非線形符号である。このような符号は素イデアル毎に異なる有限体が現れるため、固定した有限体上のベクトル空間を用いるブロック符号の範疇から外れる符号であり、K の整数論的性質によってパラメーターの評価ができる。当課題ではエルミートベクトル束(E,h)に対してα安定性の概念を定義し、更に Bost による slope 不等式を用いてα安定なエルミートベクトル束の算術的切断に関する消滅定理を証明できた。その結果、(E,h)がα安定性条件を満たすときに最小距離の下からの評価を与えることに

成功した。また、算術的曲線上の半安定エルミート束を用いて算術的 Savin 符号の具体例を構成した。

（3）α安定束の制限定理の一般化
有限体上定義された非特異代数曲面とその上の安定ベクトル束 E が与えられたとき、十分大きい次数の超曲面切断への E の制限がα-安定になることを Langer の定理を用いて証明した(論文④)。この結果により、代数曲線上に多くのα-安定束を構成することが可能になるため符号の具体例を与えることが出来た。更に Langer の定理の代わりに Hein の定理を用いることにより、曲面の場合に従来のものより評価の良い制限定理を証明することにも成功した(論文②)。これによって符号のパラメーターの評価式を改良することが出来た。なお、最近の研究では上に述べた結果は任意次元の非特異射影多様体の場合にまで一般化することに成功している。また、高次元射影多様体で接束が p-半安定(即ち任意回数のフロベニウス写像による引き戻しが半安定)という仮定の下では、フロベニウス写像による安定束の順像がα-安定になることを Sun の定理を用いて証明した。これにより、射影空間や大きい次数の一般型超曲面上の安定束からα-安定束を構成することが可能になった。

（4）安定束の存在定理
高次元代数多様体上でどの様な階数とチャーン類をもつ安定ベクトル束が存在するかを決定することは性能の良い代数幾何符号を構成するために重要である。しかしながら安定束の存在問題は代数曲面や射影空間などの場合を除いて一般には解決されていない。当課題では、安定束の「漸近的存在問題」の概念を定式化して弱い形での存在を考察することにした。これは安定束の無限列(安定束の large family)で階数と判別式が与えられた増大度をもつものが存在するか、という問題である。特にアーベル多様体の場合を考察し、漸近的存在問題に対する一定の解答を与えた(論文③)。具体的には、テータ因子の完全交差として得られる余次元 2 の部分多様体から Serre 対応を用いて階数 2 の安定束を作り、逐次拡大によって高階の安定束を構成した。

（5）安定束のモジュライ空間の幾何学
非特異射影多様体上で固定した階数とチャーン類をもつ安定束の同型類全体はモジュライ空間と呼ばれる代数多様体を成す。2 つの層の拡大として表せる安定束全体は special component と呼ばれるモジュライ空間の特別な既約成分を定める。当課題では special component の幾何学に関して幾つかの結果を得た(論文⑤)。まず、コホモロジーの消滅によって special component が非特異になるための十分条件を与え、次元の計算を行った。また、以前中島が証明した Brill-Noether 双対性を用いて special component 達の間に双有理写像を構成した。

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 5 件）

① T.Nakashima,
Construction of codes from Arakelov geometry, Des. Codes and Crypt. 73(2014), 47-54　査読有
② T.Nakashima
AG codes and vector bundles on rational surfaces, Int. J. Pure and Appl. Math. 96(2014), 329-342　査読有
③ T.Nakashima
Large families of stable bundles on abelian varieties, Proc. Amer. Math. Soc. 141(2013), 2225-2231　査読有
④ T.Nakashima
Parameters of AG codes from vector bundles, Finite Fields and Their Appl. 18(2012), 746-759　査読有
⑤ T.Nakashima
Special components of the moduli of stable sheaves, Communications in Algebra 10(2012), 3759-3770　査読有

〔学会発表〕（計 3 件）

① 中島　徹
ベクトル束と代数幾何符号, 代数曲線シンポジウム、神奈川工科大学アクティブラーニング横浜(神奈川県横浜市西区)、2015 年 12 月 19 日
② T.Nakashima
AG codes from restriction of vector bundles to divisors、Arithmetic, Geometry and Coding Theory、国際数学研究センター(Luminy、フランス)、2015 年 5 月 19 日
③ 中島　徹
Arakelov geometry and coding theory,
京都大学代数幾何セミナー、京都大学理学部数学科(京都府京都市左京区)、2012 年 12 月 21 日

６．研究組織

(1)研究代表者

中島　徹（NAKASHIMA TORU）
日本女子大学・理学部・教授
研究者番号：20244410

(2)研究分担者
なし