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　５ 年　 ６ 月 １０ 日現在

機関番号：３２６５２
研究種目：基盤研究(C)（一般）
研究期間：2018～2022
課題番号：１８Ｋ０３２５４

研究課題名（和文）非線形関数論への幾何学的アプローチ

研究課題名（英文）Geometric approach to the theory of nonlinear functions

研究代表者
吉荒　聡（Yoshiara, Satoshi）

東京女子大学・現代教養学部・教授

研究者番号：１０２３０６７４

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：本研究の主眼は「一般の非線形関数に対する差分複体論の構築」であったが，差分複体という概念の有効性を示す結果は得られておらず，単にこの概念抜きでも証明できる既知の結果の形式的拡張に留まっている．有限体上の関数に対する代数的次数の概念を導来関数の観点から見直し，成分関数を定める基底の取り方に依存しない性質を定式化するという当初の目論見は，簡単に出来る部分のみしか成功していない．具体的成果は，出発点となったモデル「関数が定めるCayleyグラフ」に関するものに限る．Cayley グラフが距離正則である場合には，その直径やパラメーターなどが極めて制限される．

研究成果の学術的意義や社会的意義
有限体上の非線形関数は情報の暗号化に有効であり1990年代から世界的に多くの研究が蓄積されている．本研究はこのような関数がどの程度存在するのかをその関数の導来関数から構成される差分複体の概念（実関数の微分関数とそのグラフの列の類似と見なせる）により分析しようという試みであったが、今のところ差分複体という概念の有効性を示す結果も、この方向からのアプローチをその証明に必要とする結果も得られていない。既知の結果の形式的拡張が得られるというレベルにとどまっている。新しい成果として挙げられるのは、１次元の複体であるケーレーグラフが強い正則性を持つような非線形関数は極めて限られるという事実である。

研究成果の概要（英文）：The main purpose of the research is to construct a general theory of non-linear functions over a finite field, in terms of ``differential complexes". However, I have not yet obtained any results showing the effectivity of this concept, but just a formal generalization of the known results, which can be proved without using differential complexes. The original aim to describe the concept of the algebraic degree of a non-linear function over a finite field using its derived functions is achieved only at an elementary level.

The only explicit new result is that if the Cayley graph associated with a non-linear function is distance-regular then we have strong restrictions on the algebraic structure of the function and the parameters of the graph.

研究分野：代数学

キーワード：差分複体　非線形関数　導来関数　代数的次数　ケーレーグラフ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

1990 年代に至って, 暗号破りに対する耐性が高い関数として, 線形写像から最も遠い有限体上の関数が情報科学で重要視されるようになり, APN 関数の概念が情報科学の研究者により定義された. 当初は単項式で表せる APN 関数の構成が主であったが, 2006 年の Edel-Kyureghyan-Pott による非単項 APN 関数の構成を機に, 非単項 APN 関数の構成が競って行われた. この趨勢は, 新しい動向を数学に引き起こした.

(A) 偶標数の semifield の構成の活性化,

(B) 偶標数と奇標数を統一した PN 関数の定義とその構成,

および代表者が主導した

(C) 二つの APN 関数の同値性判定に関する理論的研究,

がその主なものである.

APN 性を保つような関数間の同値関係として, CCZ 同値(関数のグラフを他の関数のグラフに移すアフィン全単射が存在する)と EA 同値(変数のアフィン変換で関数が他の関数に移る)という二種類が知られている（二つの関数は EA 同値であれば CCZ 同値である). 発見された APN 関数が新しいものといえるためには, その関数が既知の APN 関数と CCZ 同値でないことを示す必要がある. 判定が難しい CCZ 同値性の代わりに EA 同値性を確かめるだけで済むならば, それが望ましい.

代表者は 2006 年当時, 研究の中心としていた(高次元)双対超卵形のあるクラスとその同型類が, quadratic APN 関数とその EA 同値類に対応するという事実を発見したことをきっかけに APN 関数間の同値性に関する問題に取り組み, 付随する幾何構造への群の作用に注目して, 決定的な結果を幾つか得た.

(1) 二つの quadratic APN 関数が CCZ 同値であれば EA 同値である,

(2) qudratic APN 関数と単項 APN 関数が CCZ 同値ならば,

前者は Gold 関数に EA 同値. 単項 APN 関数たちが CCZ 同値ならばそれらの指数の間に簡単な合同式が成立.

3) Plateaud 関数と plateaued 単項 APN 関数が CCZ 同値ならば EA 同値.

成功のカギは, 非線形関数から良い(不変被覆や商について閉じたクラスの)インシデンス幾何である双対超卵形ないしは semibiplane を構成し, そこへの群の作用を解析した点にある.

２．研究の目的

本研究は, この思想の延長上にある.すなわち, 本研究課題の核心にあるのは次の問いであった: APN 関数の同値性問題の解決において有効であった幾何学的対象--双対超卵形と semibiplane--を, 有限体上の一般の関数に対してどのように一般化するか？

そして, その一般化された対象は関数をどのように規制するのか？

代表者が双対超卵形と semibiplane の一般化の候補と考えたのは, 標数 2 の有限体 F 上の関数 f に対するケーレーグラフ C(f) および F の部分空間 A における f の差分関数 f_A のグラフ全体のなす差分族 D(f) から作られるインシデンス幾何 I(f) で次の性質を持つもの, である:

(i) I(f) の被覆や商も適当な関数 g に対する I(g) の形である,

(ii) f と g が CCZ または EA 同値であれば I(f) と I(g) は同型になる.

そこで次の２点を研究目的として設定した

(1) 上の性質を持つインシデンス幾何 I(f) を構成する,

(2) ケーレーグラフ C(f) またはインシデンス幾何 I(f) に幾何学的な条件を与えたとき, それを満たす関数 f の同値類を分類する.

３．研究の方法

初年度は研究集会における有限体上の関数論および有限幾何に関心を持つ研究者との対面議論により, 代表者が得た成果に対する細かい質疑を通じて進むべき方向を検討した. 次年度以降はコロナ禍により直接参加型の集会が開催出来なかったため, 主にプレプリントの検討と電子メイルによる質疑応答により研究を進めた.

特に大和大学の谷口浩明氏および元近畿大学の中川暢夫氏との研究連絡は, 代表者が次の点に気付く動機づけを与えた点において有用であった. 代数的次数の概念を言い換えることにより, 超卵型の構成に類似した構造（研究当初に構想したインシデンス幾何の一つのモデル）が定められること.

４．研究成果

Cayley グラフは零部分空間が与える差分複体と見なせる. 初年度はこのグラフの持つ意味と

それが距離正則である場合の関数 f の分類を考えた．強い制限が得られ，その成果は京都大学数理解析研究所における集会で口頭発表され，講演録にまとめられた．しかし関数族および生じうる距離正則グラフの同型類の完全決定には至っていない．
具体的には，次の既知の事実の Cayey グラフを通じた初等的な証明を与えた
(1) CCZ-同値が Cayley グラフの同型を引き起こす，
(2) Cayley グラフの隣接行列の固有値が関数 f の Walsh 係数である，
(3) Cayley グラフの連結成分の個数は 1-次元部分空間 A に対応する f_A の値が生成する部分空間の指数である．
これらから関数 f が APN 関数であればその Cayley グラフが連結であることが得られる．この結果の一般化も得られる．また Dillon の観察の別証明を得る．これから APN 関数に対する Cayley グラフの直径が 6 以下であることが示せる．
また AB 関数という APN 関数の重要なクラスについてその Cayley グラフが距離正則であることが代表者により示されていたが，この逆も成立することが言えた．すなわち
APN 関数 f に対し，その Cayley グラフが距離正則であることと f が AB 関数であることは同値である．これは研究目的 (2) として提起した形の問題が Cayley グラフに関して解決した例である．

二元体に値を取る関数について代表者の構想の実効性を確かめるため、これらの関数のなす Reed-Muller 符号について代表者なりの解釈を付した講義録をまとめた．

本研究を通じて，意義のある研究対象になる可能性を感じつつ理論構成を果たせなかった概念は研究計画策定時に考えていた「差分複体」である．標数 2 のベクトル空間 V から W への関数 f を固定するとき，この複体の単体に相当するのは，各部分空間 A に対して 定義される関数 f_A (V のベクトル x を x と A の生成する部分空間の元に対する f の値の和に対応させる) のグラフであった．f の代数的次数を m とするときに m-1 次元の部分空間に対する f_A は線形写像であり，そのグラフの族は二次 APN 関数 f に付随する高次元双対超卵型(このときは m=2)に類似した性質--f にある性質を付与すると共通部分の大きさが一定になる--を持つ．今後，この族（複体ではないがその一部）を幾何学的対象として研究する方向を模索したい．

5．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

1．著者名 Satoshi Yoshiara	4．巻 2148
2．論文標題 有限体上の関数が定める Cayley graph	5．発行年 2020年
3．雑誌名 RIMSKokyuroku（京都大学数理解析研究所講究録）	6．最初と最後の頁 番号 19 (1-9)
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Satoshi Yoshiara	4．巻 342
2．論文標題 Splitness of the Veronesean and the Taniguchi dual hyperovals	5．発行年 2019年
3．雑誌名 Discrete Mathematics	6．最初と最後の頁 844-854
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.disc.2018.11.019	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 吉荒　聡
2．発表標題 有限体上の関数が定める Cayley graph
3．学会等名 「代数的組合せ論と関連する群と代数の研究」(京都大学数理解析研究所研究集会)
4．発表年 2018年

〔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