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　6　月　7　日現在

機関番号：３２６５２
研究種目：基盤研究（Ｃ）
研究期間：2009～2012
課題番号：２１５４００２５
研究課題名（和文）　高次元双対弧と非線形関数

研究課題名（英文）　Dimensional Dual Arcs and 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

研究成果の概要（和文）：対称暗号理論で著名な APN 関数などの非線形関数を扱う（特に同値性に関する問題）うえで、semibiplane や DHO （高次元超卵形）という幾何学的対象が有用であることが示された. その方向で, quadratic な APN 関数が CCZ-同値であれば EA-同値であること（Edel 予想）が示された. 二重可移な自己同型群を持つDHOの分類が得られた. ４種類の単連結 DHO の統一的記述を得た.

研究成果の概要（英文）：It is shown that the concepts of DHO(dimensional dual hyperovals) and semibiplanes are useful in studying nonlinear functions (specifically, analyzing equivalence problem) such as APN functions, which are remarkable in symmetric cryptography. With this geometric approach, a conjecture by Y. Edel was established, which states that two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent. DHOs with doubly transitive automorphism groups are classified. We obtain a unified description of four classes of simply connected DHOs.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	800,000	240,000	1,040,000
2010 年度	600,000	180,000	780,000
2011 年度	600,000	180,000	780,000
2012 年度	600,000	180,000	780,000
年度			
総　計	2,600,000	780,000	3,380,000

研究分野：数物系科学
科研費の分科・細目：数学・代数学
キーワード：DHO (高次元超卵形), APN 関数, S-box, CCZ-同値, EA-同値, 二重可移群, split DHO, bilinear DHO, semibiplane

１．研究開始当初の背景

平面上の二次曲線の持つ「どの３点も同一直線上にない」という幾何学的性質に注目し、この性質を持つ射影平面上の点集合を弧と呼ぶ。1955 年に Segre は射影平面が奇標数の有限体で係数づけられるとき、最大個数の点からなる弧（卵形）は二次曲線となることを示した。偶標数の場合には最大個数の点からなる弧は超卵形と呼ばれ、o-多項式という種々の条件を満たす多項式によって記述される。この意味で o-多項式は二次式の一般化であり、その構成と分類に対して様々な努力がなされている。特に 1980 年代の Kantor, Payne, J.Thas による、一般四辺形の自己同

型からなる有限群とその部分群族に注目した一連の研究は、o-多項式の幾何学的構成を可能にした。それを受けて Cherowitzo や Penttila を中心に o-多項式=超卵形の無限系列が構成された(1996 及び 2003 年)。

本研究の主題である高次元双対弧は、射影平面中の弧という概念の（双対の）一般化であり、有限群の部分群複体に関する申請者の研究のなかで、1996 年頃 Pasini, Huybrechts 及び申請者により発案・定式化された。

射影平面に限らず、任意次元のベクトル空間を取り、射影平面中の点（の双対である 2-次元部分空間）を、このベクトル空間の一定次元（d+1 次元）の部分空間に置き換え、次の条件を満たす部分空間の集まり S を考える。「S に属するどの２つの部分空間も 1 次元空間で交わるが、どの３つの部分空間も零空間で交わる。」ベクトル空間の係数体が q 元体であるとき、S を q 元体上の d-双対弧と呼び、S の属する部分空間全体が生成する部分空間を生成空間という。q 元体上の d-双対弧は高々 ((q^{d+1}-1)/(q-1))+1 個のメンバーからなることが示されるが、この上限値及び上限値引く 1 を与える双対弧を、古典論にあわせて、双対超卵形(以下 DHO と略記）及び双対卵形と呼ぶ。1-双対弧は、射影平面における双対弧に他ならない。

このように、二次曲線の持つ幾何学的性質を抽象化・高次元化して得られた d-双対弧の概念は、d=1 に対する古典論を包括する、幾何学的・群論的・数論的研究対象である。1996 年から 2008 年までの間に発案者を始め Del Fra, J.Thas, van Maldeghem, Cooperstein, Wild, Ng, Brown, 谷口, 中川らにより、この概念が豊富な例を持ち、予想以上に様々な数学と関連することが認識されている。

特に、単連結な DHO の様々な構成例が得られたこと、二重可移な DHO の分類に進展が見られたこと(Pasini, Huybrechts,申請者)、Veronese DHO の幾何学的特徴付けが得られたこと(J.Thas, van Maldeghem)、生成空間の次元の上限が示されたこと(申請者)、translation planes と生成次元が最小である 2 元体上のＤＨＯの関連が示されたこと(J.Thas-Cooperstein, 谷口)、後述の APN 関数との関連が示されたこと(申請者)が重要な成果であった。

２．研究の目的

科研費基盤研究(c)「群複体の変形理論と特徴付け」(2001--2004),「群復体の表現と高次元双対弧」(2005--2008)において、申請者は、二元体上のある d-双対超卵形のアフィン拡大として対称性の高い semibiplane が無限系列として得られることを示し、対称性の高い d-双対超卵形の構成・分類問題に取り組んだ。

本研究の目的は、その継承・発展に取り組み、2007 年ごろから申請者が観察した有限体上の非線形関数(APN 関数）との関連を追究し、更に双対弧に関する総合的な研究を行うことである。主眼は次の３点である。

(A) 対称性の高い（二重可移な） d-DHO の分類完成
(B) APN 関数の研究への幾何学的アプローチによる貢献
(C) d-双対弧に対する様々な問題の提唱とその解決

３．研究の方法

(1)本研究の諸課題は、申請者が独自に考案したものであり、基本的には申請者が個人でその解決に取り組んだ。一定の成果を上げた後にも、その後の方向性や、論法の改良などが必要であり、そのためには、国内外の各種研究集会で発表し、その成果について討議を重ねることが重要な方法であった。また、数学研究の常として、関連分野の研究者との密接な連絡、時には詳細な点にわたる討議が研究進展の鍵となった。

(2)課題（A）の解決には、有限群論（特に置換群論、線形群論）に対する知識が必要であり、これらに深い理解と識見を有する、千葉大学の北詰正顕氏、筑波大学の宮本雅彦氏、熊本大学の千吉良直紀氏との協議は役立った。また、Huybrechts 氏と共にこの課題に初めて取り組んだ研究者である A. Pasini 氏とは、電子メイルによる連絡を通じて、成果の報告や議論の交換をし、有益であった。

(3) 課題（B）の解決には、APN 関数の研究者との密接な連絡が有益であった。国内では、近畿大学の中川暢夫氏、国外では Carlet 氏、Pott 氏らに申請者の成果を伝え、討議を重ねて方向性を検討した。2009 年度に行われたベルギーでの集会に参加し、Pott 氏並びに若手研究者の Edel 氏と深く討議した。その後 2009, 2010 年に Edel 氏、Pott 氏を日本に招いて更に進展した話題に関し論じた。また、有限体上の関数を組合せ構造の研究に適用する議論に経験を有する研究者である、熊本大学の平峰豊氏、大分大学の末竹千博氏、福岡大学の秋山献之氏等との討議も有益であった。最後に、新しい単連結 d-DHO を発見した、詫間高専（現在高松高専）の谷口浩朗氏との長期にわたる共同研究は多くの成果を生んだ。その中核となったのは小研究集会「有限幾何とその周辺」であった。更に、この課題と符号理論、semibiplane と呼ばれる結合幾何との関連が観察され、これらに造詣の深い山形大学の原田昌晃氏、九州大学（現在上海交通大学）の坂内英一氏、東北大学の宗政昭弘氏との連絡は有効であった。

(4) 課題 (C) の部分課題として幾つか具体的に設定した問題及びその解決に関しては、谷口浩朗氏との共同研究に負うものが多い。

４．研究成果

（１）「研究課題 (A)：二重可移な DHO の分類」に関しては、二元体以外で定義されたものの分類結果に対する新証明及び二元体上で定義された場合の分類も含めた、ほぼ完全な結果を得た。結果は論文⑥及びそれに先行する論文に発表されている。特に、Yoshiara DHO と呼ばれる DHO の特徴付けを得た。これは有限体上の非線形関数に関して、Gold 関数の特徴付けも与える.
二元体上で定義された二重可移な DHO の自己同型群を見ると、translation groups の重要性が認識される。この分類結果は、最近の Dempwolff 氏と Edel 氏による，いわゆる bilinear DHO という概念への道を開いたと思われる。

（２）「研究課題(B)：APN 関数の研究への幾何学的アプローチによる貢献」に関しては大きな成果が得られた。対称暗号理論における S-box 理論の中核をなす APN 関数について Dillon, Dobbertine, Pott, Edel, Carlet , McGuire らにより，一般論が進展すると同時に幾つかの無限族が構成されている。研究代表者は、これら非線形性の高い関数を幾何学的に扱う道具として semibiplane と DHO が有効であることを論文⑤において提唱した。CCZ-同値と EA-同値が，これらの幾何学的対象の同型に言い換えられることがその中核であるが、この幾何学的考察はその後の APN 関数論の進展に大きくつながったと自負している。
例えば、「新」APN 関数が発見されたとき、それが従来知られている関数と CCZ-同値ではないことを示す必要がある。この問題は一般には面倒で、2009 年ごろまでは理論的に手が付けられていない状況にあった。研究代表者の提唱は、この点に大きく寄与した。
2009--2010 年の若手研究者 Edel 氏との研究連絡を通じて，研究代表者は、いわゆる Edel 予想「quadratic APN 関数が CCZ-同値であれば EA-同値である」を知った。代表者は、論文⑤で示したこれらの同値性の幾何学的言いかえを用いて、簡単な有限群論により予想が正しいことを示した。(論文③) この結果、quadratic な新 APN 関数と既知の APN 関数間の CCZ-同値性の検証という面倒な作業が、EA-同値性の検証というより単純な作業に帰着される。知られている APN 関数の無限系列のすべてが、単項式であるか quadratic であるという現状において、Edel 予想の解決は基本的成果である。これに基づき既知の APN 関数の無限族間の同値性問題は、現在も詳しい検討が進行中である。

（３）上記の研究の発展は、新しい DHO の部分族が重要な対象であることを示唆している。研究代表者は、既に 2009 年ごろに、split する DHO という概念の重要性を提唱し，平面関数と semifield 理論との古典的関連がここに成立することを観察した。それを受けて、二元体上の split DHO の良い部分クラスである bilinear DHO という概念が、最近 Dempwolff, Edel により導入され、その特徴付けや拡大理論など、多くの成果が得られているが、代表者の上記の成果は、ここへの大きな動機付けを与えたとみなせる。更に、代表者が古くに提唱していた「極空間に埋め込める DHO」に関しても、ごく最近 Dempwolff と Kantor が大きな貢献をしており、代表者のまいた種が各方面で芽吹いている印象がある。

(4) 研究課題 (C) として幾つか具体的項目を設定したが、そのうち課題(B)に対する研究成果の蓄積に伴って、知られている単連結 DHO の良い記述、その商の具体的構成、部分 DHO の張り合わせ（特に直和）に対する理論の構成、等が喫緊の課題となった。最後の直和理論の構築は、Dempwolff-Edel の bilinear DHO に対する拡大を例に含むものであり、平成２４年度にほぼ完成した（現在論文作成中)。これに関して、現在知られている４つの単連結 DHO の無限系列に対する良い記述が必要となり、それを論文② 及び①として谷口氏との共同研究により得ることが出来た. また Veronese DHO に対する具体的な商の構成問題に対する一つの結果を、谷口氏との共同研究で論文④として得た。

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　6　件）

①H.Taniguchi and S.Yoshiara, A unified description of four simply connected dimensional dual hyperovals、European Journal of Combinatorics, 査読有, (2013), to appear.　DOI: 10.1016/j.ejc.2013.04.007

② H.Taniguchi and S.Yoshiara, A new construction of the d-dimensional Buratti-Del Fra dual hyperoval, European Journal of Combinatorics, 査読有, 33 (2012), 1030--1042.
DOI: 10.1016/j.ejc.2012.01.002

③ S.Yoshiara, Equivalences of quadratic APN functions, Journal of Algebraic

Combinatorics, 査読有, 35 (2012), 461--475.DOI: 10.1007/s10801-011-0309-1

④ H.Taniguchi and S.Yoshiara, New quotients of the d-dimensional Veronesean dual hyperoval in PG(2d+1, 2), Innovations in Incidence Geometry, 査読有, 12 (2011), 15 pp.

⑤S.Yoshiara, Notes on APN functions, semibiplanes and dimensional dual hyperovals, Designs,Codes and Cryptography, 査読有, 56 (2010), 197--218.

⑥S.Yoshiara, Dimensional dual hyperovals with doubly transitive automorphism groups,European Journal of Combinatorics, 査読有, 30 (2009), 747--757.

〔学会発表〕(計 8 件)
①吉荒聡, 非線形関数を巡って, 日本数学会特別企画公演, 2013 年 03 月 23 日, 京都大学吉田南キャンパス

②吉荒聡, 高次元の双対弧−過去１５年間を振り返って, 第５７回代数学シンポジウム, 2012 年 08 月 20 日, 京都大学数理解析研究所

③吉荒 聡, 有限体上の関数への群論的アプローチ, 研究集会「有限体とそれに関する代数的組合せ論」2012 年 3 月 3 日, 神戸学院大学ポートアイランドキャンパス

④吉荒 聡, Around equivalences on APN functions, Vertex Operator Algebras, Finite Groups and Combinatorics, 京都大学数理解析研究所研究集会, 2010 年 12 月 13 日, 京都大学理学部

⑤吉荒 聡, 非線形関数に関連した幾何構造と代数系, 研究集会「代数的組合せ論および関連する群と代数」, 平成 21 年(2009) 11 月 19 日, 信州大学理学部

⑥吉荒 聡, Codes and graphs associated with APN functions, 研究集会「Designs and Codes」, 平成 21 年(2009) 6 月 22--23 日, ヒルズサンピア山形

⑦吉荒 聡, A geometric construction of semifields --Introduction to recent results by Ball-Ebert-Lavrauw, 小研究集会「有限幾何とその周辺」, 平成 21 年(2009) 8 月 7 日, 東京女子大現代教養学部

⑥吉荒 聡, Some geometric approaches to APN functions, Galois Geometries and Applications 2009, 平成 21 年(2009) 5 月 25 日, Ghent University (Belgium)

６．研究組織
(1)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