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　元 年　 ６ 月　 ９ 日現在

機関番号：３２６５２
研究種目：基盤研究(C)（一般）
研究期間：2014～2018
課題番号：２６４０００２５

研究課題名（和文）高次元双対超卵形研究の新展開

研究課題名（英文）New trends in the research of dimensional dual hyperovals

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）　　2,300,000円

研究成果の概要（和文）：高次元双対超卵形(DHO)と呼ばれる射影平面上の二次曲線を一般化した自然な対象について，(a) 生成空間の次元の最も精密な上限を示す(c)分裂性を示す(b)応用として既知の APN 関数の同値性問題を解く，を目標とする研究を行い次の成果を得た．
(a) bilinear DHO に対し精密な上限を示し，上限を与える bilinear DHO を分類した．(b) 既知の単項 APN 関数の無限系列に対し，同値性問題を解決した．(c) DHO の具体的なモデルから計算できる関数を用いて分裂性を示す方法を与え，その応用として既知の DHO がすべて分裂していることを確かめた．

研究成果の学術的意義や社会的意義
本研究では，高次元双対超卵型と呼ばれる平面上の二次曲線の一般化である幾何学的な対象を扱う．生成空間の次元問題は，この対象がどの程度大きくなりうるかを追究し，また分裂性の問題は，この対象がどの程度非線形な関数と関連するかを調べている．本研究の成果を通じて，高次元双対超卵型という概念が数学的に自然なものであるのみならず，深く追及すべき数理科学的具体例があることが示された．後者は非線形関数と深く関連しており，それは対称暗号を実装する際に役立つことが知られている．本研究は暗号理論において知られている具体的な非線形関数を統合する数学的理論が高次元超卵型論に内在することを示唆する．

研究成果の概要（英文）：This research has the following three objects: (a) to establish the sharpest upper bound for the dimension of the ambient space, (c) to show the splitness, of a dimensional dual hyperoval (DHO), which is a natural geometric object generalizing conics in a projective plane, and, as an application, (b) to solve the equivalence problem among known APN functions.
I obtained the following results. As for (a), I showed the exact bound for bilinear dual hyperovals and classified those attaining the upper bound. As for (b), I solved the problem with known monomial APN functions. As for (c), I developed several methods to show the splitness of a DHO with a concrete model, based on a certain function which can be calculated from the model. As an application, all known DHO are verified to split.

研究分野：代数学

キーワード：高次元超卵型　生成空間　分裂性　APN関数

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

DHO とは，有限体上のベクトル空間中のある固定した次元の部分空間の束で，ある交差条件を満たすものであり，Pasini, Huybrechts と研究代表者が発案して以来１５年ほどが経過していた．部分空間の次元が２の場合の DHO は，射影平面における古典的な超卵形という概念に一致する．有限体が２元体の場合，DHO は semibiplane という射影平面の拡張に相当する幾何構造を与える．DHO という定式化は，代数的位相幾何学の手法が適用できるという利点を生む．この方向での研究，特に DHO の普遍被覆やその商空間の決定，それらを通じた自己同型群の構造決定は，DHO の概念が得られて以来一貫して重要な DHO 研究の観点である．

申請時の数年前から，射影平面が座標づけを通じて semifield など体を拡張した代数構造や平面関数といった非線形性の高い関数と関連するように，DHO と代数構造や非線形関数と強くかかわることが認識されるにいたった．DHO が対称暗号理論で著名な APN 関数という非線形関数の同値性を説明することが，代表者や著名な差集合の研究者である Pott，その門下から出た Edel により見いだされ，代表者は quadratic APN 関数間の CCZ-同値性がより強い同値性である EA-同値性に帰着出来ることを DHO を通じた群論的手法で示した．これは Dempwolff と Edel により，bilinear DHO という概念の定式化へと発展した．Bilinear DHO は代表者が提唱した分裂性を満たす DHO の典型例であり，DHO を部分 DHO から構成する代表者の幾何学的方法(雑誌論文②)がうまく適用できる．

一方，著名な群論研究者である Kantor は直交幾何の非特異点における射影により斜交幾何と直交幾何における spread という対象間に対応がつくことの類似として，特異点における射影により斜交幾何における spread と直交 DHO (のある類)が対応することを見抜いた．Kantor が構成した非常に多くの spread (これは semifield に対応する)からこの対応を通じて多くの直交 DHO が得られる．代表者には，このような代数構造と分裂 DHO の関連も気になっていた．

２．研究の目的

高次元超卵形(以下 DHO と略記)に対する申請者による過去の研究成果と 1 に記述した研究動向を踏まえて、DHO に関連した幾何構造、算術構造、代数構造に関する以下の諸問題の DHO の視点による解決を試みることを目的とした。取り上げたのは、幾何構造として普遍被覆空間、算術構造として非線形関数、代数構造としては体の公理から結合法則などを除いた semifield などである。具体的には次の課題を解決することを目標とした。

(a) Ambient space の次元に関する予想の証明 (部分 DHO の張り合わせ理論の応用として)
(b) 既知のＡＰＮ関数間の同値性の完全決定
(c) 積構造の構成による DHO の分裂性証明

３．研究の方法

純粋数学の研究なので，個人による試行錯誤が中核となる方法である．数学研究における常套手段である「研究の進展に応じて，集会などにおいて部分的成果を関心の近い研究者仲間に報告し，それに対する種々の質問や批判的意見を受けることにより，次の展望を開く」という方法を援用した．この種の集会のうち最も役立ったのが，研究協力者を中心とした小研究集会「有限幾何とその周辺」であり，そこにおける忌憚のないやり取りと精気に満ちた議論は多くのインスピレーションにつながった．今回の論文成果 8 件のうち，共著論文は 1 件(雑誌論文①)のみであったが，この成果を生んだ共同研究においては，細かい議論に関して，電子メイルによるやり取りや，口頭による議論を行った．単独の思考が研究方法の中核であるため，高い集中度が保てるように，散歩や気分転換なども適宜取り入れた．

４．研究成果

研究目標 (a) については，一般の DHO に対する ambient space の次元に対する予想の完全解決には至らなかった．しかし，bilinear DHO という重要な DHO のクラスについて，予想を証明したばかりではなく，次元の上限を与える bilinear DHO をすべて分類する(Huybrechts DHO と Buratti-Del Fra DHO に限る)という，研究開始以前には予想だにしなかった結果が得られた(雑誌論文⑥)．

研究目標 (b) については，無限族については完全に解決した．現時点で知られている APN 関数の無限族は二次的か単項的であるが，二次的な関数の同値性については研究代表者による結果があった．これに加えて本研究では，二次的 APN 関数と単項的 APN 関数の同値性および単項的 APN 関数間の同値性が決定された(雑誌論文④)．その他 plateaued APN 関数(二次的 APN 関数の拡張)などについても同値性に関する結果を得た(雑誌論文⑤)．また plateaued APN 関数の例も追加した(雑誌論文⑦)．

研究目標 (c) については，DHO の具体的なモデルが得られているとき，そこから計算できる関数(積構造)を用いて分裂性を示す方法を得た．この方法の一部は雑誌論文⑧に記述され，そこでは雑誌論文①で得られた Taniguchi DHO の具体的モデルを用いて Taniguchi DHO の分裂性が示された．この事実と雑誌論文③で示された Mathieu DHO の分裂性から，既知の DHO がすべて分裂していることが確認された．論文⑧では，Veronesean DHO の具体的なモデル(雑誌論文①)から得られる積構造は，可換 semifield と対応することも示された．

５．主な発表論文等

〔雑誌論文〕（計　8　件）

① Satoshi Yoshiara, Splitness of the Veronesean and the Taniguchi dual hyperovals, Discrete Mathematics, **査読あり**, vol.342, 2019, 844-854. DOI: 10.1016/j.disc.2018.11.019

② Satoshi Yoshiara, Plateaudness of Kasami APN functions, Finite Fields and Their Applications, **査読あり**, vol.47 , 2017, 11-32. DOI: 10.1016/j.ffa.2017.05.004

③ Satoshi Yoshiara, Bilinear dual hyperovals in the largest ambient spaces, Journal of Algebraic Combinatorics, **査読あり**, vol. 46, 2017, 533-548. DOI: 10.1007/s10801-017-0763-5

④ Satoshi Yoshiara, Equivalences among plateaued APN functions, Designs, Codes and Cryptography, **査読あり**, vol. 85, 2017, 205-217. DOI: 10.1007/s10623-016-0298-0

⑤ Satoshi Yoshiara, Equivalence of power APN functions with power or quadratic APN functions, Journal of Algebraic Combinatorics, **査読あり**, vol. 44, 2016, 561-585. DOI: 10.1007/s10801-016-1680-z

⑥ Satoshi Yoshiara, An elementary description of the Mathieu dual hyperoval and its splitness, Innovations in Incidence Geometry, **査読あり**, vol. 14, 2015, 81-110.

⑦ Satoshi Yoshiara, Disjoint union of dimensional dual hyperovals, Innovations in Incidence Geometry, **査読あり**, vol. 14, 2015, 43-76.

⑧ Hiroaki Taniguchi and Satoshi Yoshiara, A unified description of four simply connected dimensional dual hyperovals, European Journal of Combinatorics, **査読あり**, vol.36, 2014, 143-150. DOI: 10.1016/j/ejc.2013.04.007

〔学会発表〕（計　8　件）

① **吉荒聡**, **有限体上の関数が定める** Cayley graph, **研究集会「代数的組合せ論と関連する群と代数の研究」**, 2018 **年** 12 **月** 13 **日**, **京都大学数理解析研究所**.

② **吉荒聡**, Ambient space **が最大となる** bilinear DHO, **第** 34 **回代数的組合せ論シンポジウム**, 2017 **年** 6 **月** 17 **日**, **小山工業高等専門学校（図書情報センター棟** 1 **階視聴覚室）**

③ **吉荒聡**, **最大の** ambient space **を持つ** bilinear DHO **の特徴づけ**, **小研究集会「有限幾何とその周辺」**, 2017 **年** 3 **月** 25 **日**, **東京女子大学** 4 **号館**

④ **吉荒聡**, **標準的な有限群論に基づく単項** APN **関数の同値関係判定**, **研究集会「有限群・代数的組合せ論・頂点作用素代数の研究」**, 2016 **年** 12 **月** 7 **日**, **京都大学数理解析研究所**

⑤ **吉荒聡**, **既知の** APN **関数の同値性問題**, **研究集会「代数的組合せ論とその周辺」**,2016 **年** 3 **月** 8 **日**, **東北大学情報科学研究科**

⑥ **吉荒聡**, **群環の部分集合としての** DHO **とその拡張(平峰豊氏に尋ねたかったこと)**, **小研究集会「有限幾何とその周辺–平峰豊先生を偲んで」**, 2016 **年** 3 **月** 5 **日**, **熊本大学理学部**

⑦ **吉荒聡**, Power APN **関数間の** CCZ-**同値性の判定**, **小研究集会「有限幾何とその周辺」**,2015 **年** 9 **月** 27 **日**, **東京女子大学** 4 **号館**

⑧ **吉荒聡**, APN **関数の同値性について**, **「熊本組合せ論研究集会—代数的デザインとその周辺」**, 2015 **年** 1 **月** 10 **日**, **熊本大学くすの木会館**

〔図書〕（計　0　件）

〔産業財産権〕
○出願状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：

出願年：
国内外の別：

○取得状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
取得年：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者
研究分担者氏名：

ローマ字氏名：

所属研究機関名：

部局名：

職名：
研究者番号（8 桁）：

(2)研究協力者
研究協力者氏名：秋山 献之，末竹 千博，谷口 浩朗，中川 暢夫
ローマ字氏名： Kenji Akiyama, Chihiro Suetake, Hiroaki Taniguchi, Nobuo Nakagawa