科学研究費助成事業　　研究成果報告書

平成　２６　年　　４　月　　５　日現在

機関番号：５６２０３
研究種目：基盤研究(C)
研究期間：2011～2013
課題番号：２３５４００３７

研究課題名（和文）有限体上の関数と有限幾何学

研究課題名（英文）Study on functions on finite fields and finite geometry

研究代表者
谷口　浩朗（TANIGUCHI, Hiroaki）

香川高等専門学校・一般教育科・教授

研究者番号：６０３７００３７

交付決定額（研究期間全体）：（直接経費）　　1,700,000円、（間接経費）　　510,000円

研究成果の概要（和文）：暗号分野で研究されているAPN関数から構成される高次元双対超卵形(DHO)（これをAPNDHOという）の研究，それを拡張した双線形DHOについての研究を行った。
双線形DHOがAPNDHOであるための必要十分条件を与えAPNDHOの双対やTransposeを定義しそれらが新しいDHOになる例を構成した。次にBuratti-Del Fra型のDHOの全く新しい構成方法を発見しそれが双線形DHOであることを確認し普遍被覆(Universal cover)がAPNDHOと全く同じであることも発見し低い次元への具体的な埋め込みも構成した。また古典的な４つのDHOに対して共通の表示があることを発見した。

研究成果の概要（英文）：We mainly study on APN DHO(constructed from APN functions) and bilinear DHO. We give a necessary and sufficient condition for a bilinear DHO to be an APN DHO. Using this result, we show that the dual and the transpose of the dual of the DHOs from some APN function are not known (by that time). We also give a new construction of the Buratti-Del Fra DHO. Using this construction, we show that the Buratti-Del Fra DHO is a bilinear DHO, and that the universal cover of the Buratti-Del Fra DHO is same as that of the Huybrechts DHO (APN DHO). We also give an example of a quotient of the Buratti-Del Fra DHO in PG(2d+1,2). Next, we give an uniform description for four known (all known) d-dimensional DHOs in PG(d(d+3)/2,2)(classical DHOs). We give some examples of simply connected d-dimensional DHOs in PG(n,2) with n>2d+1. Moreover, we construct many new symmetric bilinear DHOs in PG(n,2) for 2d+1<n<d(d+3)/2.

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：代数的組合せ論　双対超卵形　有限幾何学　APN関数

１．研究開始当初の背景

高次元双対超卵形(DHO と省略する)の定義は Huybrechts と Pasini によって 1999 年に与えられた。当初は有限群と関連する幾何に関連して研究されていたが，2005 年に単項式でない APN (Almost Perfect Non-linear Function) 関数が発見され，有限幾何学的対象と暗号の設計に関わる APN 関数を関係づけて研究しようとする動きが始まった。(A.Pott など。) その中で Quadratic な APN 関数から構成される高次元双対超卵形(DHO)の同型問題が APN 関数の CCZ 同値と同じであるという Edel 予想が 2012 年に吉荒聡氏によって解決された(アナウンスは 2011 年ごろ。）その中で APN 関数からできる DHO についての研究，また関連する Huybrecht DHO や Buratti-Del Fra DHO およびそれらの Quotient についての研究の機運が高まってきた状況があった。たとえば Huybrects DHO の Quotient が APN DHO である，などということもはっきりと理解されてきていた。また Edel 氏や筆者により APN 関数から構成される DHO に対して Semifield における Knuth の cube に相当するものを考えると 6 個の関連する DHO ができることもわかってきていた。本研究を開始した当初は，DHO の研究に APN 関数の研究者が参入し，上記の結果を踏まえながら，DHO 研究は次のステップにさしかかろうとしていたときであった。

２．研究の目的

高次元双対超卵形(DHO)や関連する Semi-biplane の方面から有限体上の関数を追求することにより， APN 関数や関連する領域の研究をリードすること試みを行おうとしていた。具体的には以下の項目について，DHO をはじめとする有限幾何的対象との関係を深く追求し，また新しい DHO を発見していくのが本研究の目的であった。

(1) DHO と APN 関数や拡張された APN 関数(APN 関数が定義されているベクトル空間と値をとるベクトル空間が異なってもよいとする)との関係を探る。
(2) DHO とベクトル空間上定義された双線形写像との関係を探っていく。
(3) 関連する新しい DHO の発見を試みる。

DHO 研究の（この報告書を書いているときの）現状では多くの研究者が(2)の双線形写像と関係する DHO の一種として APN 関数から定義される DHO を研究する方向に向かっている。双線形写像と関連する DHO の研究が一つの大きな流れになっており，また研究も深化している

３．研究の方法

以下のような方法で研究を行うことを考えていた。

(1) 様々な例が存在する APN 関数から構成される DHO の「双対」や「双対の Transpose」の構造を調べ，新しい DHO であるかどうか判定する。

(2) また，双線形写像から構成される DHO の構造を解明する。

(3) 同型写像があればそれは(APN 関数から構成される DHO のように)簡明な形をしていると予想されるが，それを Semi-biplane を用いることにより解明する。

(4) また新しい双線形 DHO を構成する。

研究を開始した当初は以上のように考えていたわけだが、結果としては，1 番については特定の APN 関数について結果を得たにとどまった。2 番については，非常に奥の深い（研究に意味のある）問題であることが判明してきている。 現在も継続してこの問題に取り組んでいる。3 番については，私自身は双線形 DHO が APN 関数から構成される DHO であるための必要十分条件を与えた。完全な回答は Y.Edel と U.Dempwolff によって，私のその結果の別証明を考える中で，先に与えられてしまった（此の結果の出版は 2014 年)。 残念なことであった。4 番についてはいくつかの新しい構成を得ることができた。これらの構成の原理を探ることにより，この方面の研究がさらに深化しつつあるのが現在の状況である。

このように当初予定した研究方法通りには行かない部分もあった。しかし筆者の研究は（予定した方向以外の）別の方向にも発展し，結果として多方面の成果を得ることができたと考えている。

４．研究成果

以下のように多方面の成果を得ることができた。

(1) 双線形 DHO が APN 関数から来る DHO であるための必要十分条件を与えた。此の結果は Dempwolff と Edel たちによって拡張され，大きな理論となって発展している。また APN 関数 $f(x)=x^3+Tr(x^9)$から構成される DHO の双対の DHO および双対の Transpose をとった DHO は双線形な DHO となるがそれまで知られていなかったものであることを示した。

(2) Buratti-Del Fra 型の DHO は表示の複雑さから存在すらも疑われていたが，全く新しい構成方法を発見した。その構成により初めて Buratti-Del Fra 型の DHO は双線形 DHO の一種であることが確定した。また Buratti-Del Fra 型の DHO の普遍被覆(Universal cover)が Huybrechts 型の

DHO(APN DHO)と全く同じであることを発見した。これらの間にはまだ未発見の深い関係があることが推測される。非常に低い次元(2d+1次元)の射影空間への具体的な埋め込み（Quotient）も発見することができた。(d 次元の Buratti-Del Fra DHO 自体は d(d+3)/2 次元の射影空間で定義されていることを思い起こしてほしい。)

(3) Buratti-Del Fra 型および Veronesean の変形型の DHO はその表示の複雑さ故取り扱いが非常に難しかったが，それらに簡明な表示式が存在することを発見した。（２.と全く別方向の取り組み。）その後，最高次元(d(d+3)/2次元)の射影空間を生成する d 次元 DHO すべてに対し「uniform description」があることを発見した。

(4) Simply connected で生成(射影)空間の次元が高い(2d+1 次元より大きい) d-次元 DHO は全く知られていなかったが，そのような例が存在することを初めて示した。これには Dempwolff と Edel による Extension の方法を拡張し，それを用いてそのような DHO をいくつも構成することにより存在を示した。

(5) 生成空間の次元が比較的高い(2d+1<n<d(d+3)/2 次元射影空間を生成する，という意味)d-次元 DHO の研究はほとんどなされていなかったが，そのような双線形 DHO で非同型なものを多数構成することができた。それらの同型問題を研究する中で Quotient と自己同型群の関係など色々な性質を証明することができた。これに関しては現在研究が大きく進展しているところである。

(6) d-次元の Deformation of Veronesean DHO の 3d 次元射影空間への（多くの非同型な）埋め込みを構成した。また d-次元の Veronesean DHO の今まで知られていなかった 2d+1 次元射影空間への（多くの非同型な）埋め込みを構成した。

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 10 件）

① Hiroaki Taniguchi and Satoshi Yoshiara, A unified description of four simply connected dimensional dual hyperovals, European Journal of Combinatorics (査読有), 36, 143--150, (2014)

② Hiroaki Taniguchi, Simple expressions of the Buratti-Del Fra dual hyperoval and the deformation of the Veronesean dual hyperoval, Electronic Notes in Discrete Mathematics (査読有), 40, 359--364, (2013)

③ Hiroaki Taniguchi, Some examples of simply connected dual hyperovals, Finite Fields and their Applications (査読有), 22, 45--50, (2013).

④ 谷口浩朗, d-dimensional symmetric bilinear dual hyperovals, 第 30 回代数的組合せ論シンポジウム報告集(査読無), pp69–74, (2013)

⑤ Hiroaki Taniguchi, On the dual of the dual hyperoval from APN function $f(x)=x^3+Tr(x^9)$, Finite Fields and Their Applications (査読有), 18, 210--221, (2012)

⑥ Hiroaki Taniguchi, Quotients of the deformation of Veronesean dual hyperoval in $PG(3d,2)$, Discrete Mathematics (査読有), 312, 498--508, (2012)

⑦ Hiroaki Taniguchi and Satoshi Yoshiara, A new construction of the d-dimensional Buratti-Del Fra dual hyperoval, European Journal of Combinatorics (査読有), 33, 1030--1042, (2012)

⑧ Hiroaki Taniguchi and Satoshi Yoshiara, New quotients of the d-dimensional Veronesean dual hyperoval in $PG(2d+1,2)$, Innovations in Incidence Geometry (査読有), 12, 151--165, (2012)

⑨ 谷口浩朗, Simple expressions of Buratti-Del Fradual hyperovals, 第 29 回代数的組合せ論シンポジウム報告集(査読無), pp106–112, (2012)

⑩ 谷口浩朗, On a description of the Buratti-Del Fra dual hyperoval and its quotient, 谷口浩朗, 第 28 回代数的組合せ論シンポジウム報告集(査読無), pp128--134, (2011).

〔学会発表〕（計 12 件）

① 谷口浩朗, On a description of the Buratti-Del Fra dual hyperoval and its quotient 2011.6.22, 第28回代数的組合せ論シンポジウム, 大分大学

② Hiroaki Taniguchi, A quotient of the d-dimensional Buratti-Del Fra dual hyperovals in $PG(2d+1,2)$ with

d even, 2011.7.11-15, The 10th International Conference on Finite Fields and their Applications, Ghent University, Belgium

③ 谷口浩朗, Veronesean DHO とその周辺, 2011.12.10, 「有限幾何とその周辺」小研究集会, 大分大学

④ 谷口浩朗, Translation dual hyperoval について, 2012.3.3, 研究集会「有限体とそれに関連する代数的組合せ論」, 神戸学院大学

⑤ 谷口浩朗, 高次元dual hyperovalのいろいろな構成, 2012.5.26, 「香川セミナー」, 香川大学

⑥ 谷口浩朗, Simple expressions of the Buratti-Del Fra dual hyperoval and the deformation of Veronesean dual hyperoval, 2012.6.19, 第29回代数的組合せ論シンポジウム, 弘前大学

⑦ Hiroaki Taniguchi, On expressions of the Buratti-Del Fra dual hyperoval and the deformation of Veronesean dual hyperoval, Combinatorics, 2012. 9. 10-14, Perugia, Italy

⑧ 谷口浩朗, ある対称・双線形高次元双対超卵形の性質, 2013.5.10, 小研究集会「有限幾何とその周辺」, 大分大学

⑨ 谷口浩朗, d-dimensional symmetric bilinear dual hyperovals, 2013.6.18, 第30回代数的組合せ論シンポジウム, 静岡大学

⑩ Hiroaki Taniguchi, d-dimensional symmetric bilinear dual hyperovals in V(((1/r)d^2+3d+2)/2,2) with r>1, The 11th International Conference on Finite Fields and their Applications, 2013.7.21-26, Magdeburg University, Germany

⑪ 谷口浩朗, Buratti-Del Fra型のDHOについて, 2013.11.30, 小研究集会「有限幾何とその周辺」, 大分大学

⑫ 谷口浩朗, Bilinear dual hyperovalについて, 2014.3.7, 代数的組合せ論ミニ集会, 神戸学院大学

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕
ホームページ等　なし

６．研究組織
(1)研究代表者
谷口浩朗（Hiroaki Taniguchi）
香川高等専門学校・一般教育科・教授
研究者番号：60370037

(2)研究分担者：該当無し

(3)連携研究者：該当無し