様式 C-19

科学研究費補助金研究成果報告書

平成 23 年 6 月 15 日現在

機関番号：５６２０３
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号：２０５４００３４
研究課題名（和文）　様々な有限幾何学的対象と高次元双対超卵形の関係の研究

研究課題名（英文）　The study on higher dimensional dual hyperovals in 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

研究成果の概要（和文）：暗号の分野で活発に研究されている APN 関数との関係を探求し、その関係を利用して新しい高次元双対超卵形を構成した。また半体を用いることによって低い次元に於ける今までに知られていない高次元双対超卵形の構成をおこなった。さらに知られている高い次元における高次元双対超卵形（Veronese 型および Buratti-Del Fra 型の高次元双対超卵形）に対して、それらをより小さい空間において（非常に多く、しかも同型でないような形で）再構成した。

研究成果の概要（英文）：We study on the relation between APN (Almost Perfect Non-linear) functions, which are investigated in the field of cryptography, and dual hyperovals. Using this relation, we construct new dual hyperovals. Next, using semifields, we construct many new dual hyperovals. Moreover, we also construct many new non isomorphic quotients of the Veronesean dual hyperoval, and the Buratti Del Fra dual hyperoval in small dimensional projective spaces.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	500,000	150,000	650,000
２００９年度	500,000	150,000	650,000
２０１０年度	500,000	150,000	650,000
年度			
年度			
総　計	1,500,000	450,000	1,950,000

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：代数的組合せ論

１．研究開始当初の背景

有限体上の射影平面に於ける超卵形は 1950 年代から研究されてきたが、高次元の超卵形は 1990 年代になって模索されはじめ、ようやく 1999 年に Huybrechts と Pasini によって定義が確定した。それで、高次元双対超卵形についての本格的な研究が始まって 10 年しか立っておらず、他の（古くから活発に研究されている数学的な)対象との関係がようやくおぼろげに見えてきた状況であった。

２．研究の目的

本研究の目的は、さまざまな先行研究によって明らかになってきた、射影空間内の高次元双対超卵形(Dimensional Dual HyperOval)と「種々の幾何学的な対象」との関係について調べることである。

以下の項目について、 高次元双対超卵形との関係を追求し、相互の関係を発見し、新しい高次元双対超卵形を発見していくのが本研究の目的であった。

(1)「古典的な Hyper Oval との関係」

我々のそれまでの研究により、古典的な Hyperoval が存在すれば、それから高次元双対超卵形が構成出来ることが分かっていた。ただし具体的な構造まで分かっているのは、古典的な Hyperoval が単項式による o-多項式 (oval polynomial) によって定義される場合だけであった。

(2)「移行平面や半体、概体との関係」

概体や半体があれば、それから高次元双対超卵形が構成出来ることが我々の研究で見当がついていた。それらが本当に新しい構成であるか、またその自己同型群の計算、もとの半体や概体との関係、半体や概体から構成される射影平面との関係などを追求していく。

(3)「暗号理論における S-Box の仕様に関係する APN 関数など、有限体上の関数との関係」

APN 関数と関係する高次元双対超卵形の研究が、暗号理論との関係と相まって非常に重要になることが予想できた。その方向の研究が非常に重要であることが分かっていた。現在､APN 関数は世界中で熱気を持って研究されている。

３．研究の方法

(1)豊富な例が存在する古典的な移行平面や半体・概体について、それぞれから構成される高次元双対超卵形の構造を調べる。とくにそれらの自己同型群や、同型問題を中心に考察していく。(これらはもともと我々の研究で明らかになってきたことであった。)

(2) 暗号理論における S-Box の仕様に関係する APN 関数など、有限体上の関数と高次元双対超卵形の関係について探求する。具体的な APN 関数から構成される高次元双対超卵形やその双対、Transpose などが新しい高次元双対超卵形になっているかどうかを調べていく。また、ごく最近、Quadratic な APN 関数に限れば、APN 関数から構成される双対超卵形が新しいものであれば、APN 関数自身も新しいものであることが証明された。これにより、双対超卵形の研究が APN 関数の研究と密接につながっていることが再確認できた。

(3) Buratti-Del Fra 型の高次元双対超卵形について、様々な埋め込みが（少し APN 関数と異なった関数で）構成できるのではないかと見込まれる。それについて考察する。
Hyubrechts 型の高次元双対超卵形の 2d+1 次元射影空間への埋め込みは APN 関数と深く関係している。Buratti-Del Fra 型の高次元双対超卵形は､Huybrechts 型を変形したものであるから、その低次元への埋め込みは、APN 関数（を変形したもの）と何らかの関係があるのではないかという問題意識がある。

４．研究成果

上記(1)(2)(3)について、多方面の成果を得ることが出来た。それに伴い、高次元双対超卵形の研究は予想以上に進展した。主な具体的な成果は以下の通りである。

(1) 2 元体上の 2d-次元射影空間を生成空間とする高次元双対超卵形の今まで知られていない族を概体を用いて構成した。また、半体を用いた構成についても考察し、多くの非同型な高次元双対超卵形が存在することを示唆した。この内容は Finite Fields and their Applications に掲載されている。また 2 元体上の 2d-次元射影空間を生成空間とする高次元双対超卵形から 1 つの要素（d 次元部分空間）を除いた集合に群が正則に作用しているならば、その高次元双対超卵形は概体(Near Field)を用いて構成されることを証明した。現在この結果を継続して追求し発展させているところである。

(2)吉荒氏によって構成された「Quadratic な APN関数による高次元双対超卵形」の双対がまた高次元双対超卵形になるための必要十分条件を見いだした。これは、Y.Edel氏（ベルギーGhent大学）の提出した問題を解決したものである。このことで、いろいろなAPN関数から全く新しい高次元双対超卵形が「吉荒氏による標準的な構成」以外方法で、つまり双対をとる、またそのTransposeをとる、という方法で構成出来ることが分かった。この内容は Finite Field and their Applicationsに掲載されている。

(3)APN 関数から構成される高次元双対超卵形の双対について研究し、C.Carlet 氏達の構成したAPN関数から構成される高次元双対超卵形については、その双対は本質的に新しい高次元双対超卵形であることを証明した。また、交代的とは限らない双線形型の高次元双対超卵形について研究を行い、その基本的な性質を証明することが出来た。とくにAPN関数から構成される高次元双対超卵形と同型になるための条件を見いだすことが出来た。現在投稿中ではあるが Referee から何度かの手直しを要求されている途中である。なお、この論文中の命題の一つを最近 Y.Edel 氏（Ghent 大学）が追求し、大きく発展させた。(現在 Preprint として何人かの研究者に送付されている。)

(4)Buratti-Del Fra型のd次元双対超卵形のQuotientについて研究し、APN関数を用いた様々な非同型なQuotientsを3d次元射影空間内に構成することに成功した。これにより低次元には非同型なQuotients(埋め込み)が非常に多く存在することが分かった。Buratti-Del Fra型の高次元双対超卵形も何らかの関数（APN関数と関係するかもしれない）と関係するという可能性について確信を持つことが出来た。この内容はDiscrete Mathematics に掲載されている。

(5)（筆者による）Veronesean構成をひねったd(d+3)/2次元内のd-次元双対超卵形（Discrete Mathematics, Vol.309, に掲載されている）のquotientsで、同型でないもの多数を（体のガロア群の生成元を用いて）3d-次元射影空間内に構成した。この場合も低次元に埋め込めば非同型なものが多く存在することを確かめることが出来た。この内容はDiscrete Mathematicsに掲載予定である。

(6)Veronesean双対超卵形の新しいタイプのquotientsで、同型でないもの多数を、体のガロア群の生成元および超平面を用いて、2d+1-次元射影空間内に構成した。Veronesean双対超卵形は、実に様々な低次元射影空間の中への埋め込みがあることが確かめられた。Veronese構成の場合も、何らかの有限体上の関数との関わりがあるのではないかという感覚が強くおこってくる。この内容はInnovations in Incidence Geometryに掲載予定である。

(7)Buratti-Del Fra双対超卵形のquotientを初めて2d+1-次元射影空間内に構成した。これは Coulter-Mathews による Commutative Semifields によるspreadの構成(3元体GF(3)の偶数次の拡大体) 上の結果を、2元体GF(2)の偶数次の拡大体上の結果におき換えたものである、と見なすことが出来る。このことは、半体 (Semifield) とBilinearな高次元双対超卵形との強いつながりを表しているように思われる。また、このことにより、(Semibiplaneの一種、高次元双対超卵形のAffine拡大を経由して)APN関数の変形であるような関数が見つかる可能性が出てきた。さらにBuratti-Del Fra双対超卵形の全く新しい表示方法の提示、Buratti-Del fra型の双対超卵形のアファイン拡大Halved Hypercubeといわれるものでカバーされている、など様々な結果を示すことが出来た。これらの内容については現在投稿中である。

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 谷口浩朗、On d-dimensional Buratti-Del Fra type dual hyperovals in $PG(3d,2)$、Discrete Mathematics、査読有、**Vol.310**、pp3633～3645,2010

②谷口浩朗、On some d-dimensional dual hyperovals in PG(d(d+1)/2,2)、European Journal of Combinatorics、査読有、**Vol.31**、pp401～410、2009

③ 谷口浩朗、On d-dimensional dual hyperovals in PG(2d,2)、Innovations in Incidence Geometry、**Vol.8**、査読有、pp137～145、2009

④谷口浩朗、On the duals of certain dual hyperovals in PG(2d+1、2)、Finite Fields and Their Applications、査読有 **Vol.15**、pp673～681、2009

⑤谷口浩朗、On some d-dimensional dual hyperovals in PG(2d、2)、Finite Fields

and Their Applications、査読有 Vol.14、pp1010～1019、2008

〔学会発表〕(計 9 件)

①谷口浩朗 On dimensional dual hyperovals 研究集会「有限幾何とその周辺」2010 年 11 月 13 日 熊本大学

②谷口浩朗 On the quotients of dual hyperovals Combinatorics2010 2010 年 7 月 1 日 ヴェルバニア、イタリア

③谷口浩朗 On some quotients of dual hyperovals in PG(d(d+3)/2、2) 第 27 回代数的組合せ論シンポジウム 2010年6月22日 高知大学

④谷口浩朗 d-dimensional dual hyperovals in $PG(d(d+3)/2、2)$ and their quotients ミニ集会「代数的組合せ論」2010 年 3 月 18 日 神戸学院大学

⑤谷口浩朗 Buratti-Del Fra 型の高次元双対超卵形について数理解析研究所 共同研究事業　代数的組合せ論および群と代数研究集会 2009 年 11 月 16 日 信州大学

⑥谷口浩朗 Dual of some dual hyperovals 研究集会「有限幾何とその周辺」2009 年 10 月 17 日 近畿大学

⑦谷口浩朗 ある APN 関数から構成される DHO の dual について　研究集会「有限幾何とその周辺」2009 年 8 月 7 日 東京女子大学

⑧谷口浩朗 3D-Cube と高次元双対超卵形 研究集会「有限幾何とその周辺」2009 年 5 月 16 日 東海大学阿蘇キャンパス

⑨谷口浩朗 概体と双対超卵形 研究集会「有限幾何とその周辺」 2009 年 1 月 24 日 福岡大学

６．研究組織

(1)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

(2)研究分担者:該当なし

(3)連携研究者：該当なし