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

平成　３０　年　　４　月　１２　日現在

機関番号：　５６２０３
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2017
課題番号：　２６４０００２９

研究課題名（和文）高次元のdual hyperovalと関連する有限体上の関数

研究課題名（英文）Study on higher dimensional dual hyperovals and related functions on finite fields

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）　　2,200,000円

研究成果の概要（和文）：新たに発見した高次元双対超卵形S_c(l,GF(2r))を用いて単連結な高次元双対超卵形（DHOと略記）で同型でない例を大量に構成することが出来た。それらのDHOの間に成り立つ被覆する/される関係を数c,l,rを用いて記述することに成功し，それらのDHOの自己同形群も決定することが出来た。また（１個の）可換な半体を用いてDHOを構成することに成功しそれらの間の同型問題を決定した。この構成方法を有限個の必ずしも可換でない半体にまで拡張し，さらにある条件のもとでそれらの同型問題を決定した。最後に，あるBent関数を用いた（それまで知られていなかった）２次的なAPN関数の構成にも成功した。

研究成果の概要（英文）：We discovered a family of dual hyperovals S_c(l,GF(2r)), where l, r integers and c an element of the field GF(2r). Using these dual hyperovals S_c(l,GF(2r)), we construct many simply connected examples which are not known before. We describe the cover and quotient relations among them using elements c and the integers l and r, and determined the automorphism groups of them. Next we construct dual hyperovals using a commutative presemified and determined the isomorphism problems among them. By extending this idea, we also construct dual hyperovals using many presemifields which may not be commutative. We determined the isomorphism problems among them under the specific conditions, such as the presemifields are not isotopic to commutative presemifields. Lastly, we construct a quadratic APN function using a bent function of special type. Only two examples of such constructions were known before. It is proved that our construction are not equivalent to the former two examples.

研究分野：　代数的組合せ論

キーワード：　代数学　代数的組合せ論　有限幾何学　高次元双対超卵形　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，当初の線形群の幾何との関連だけでなく有限体上の(秘密鍵暗号の設計に関わる)APN 関数，bent 関数や o-多項式と関係すること・有限射影平面に関係する Spread や符号と関係することが次々とわかってきていた。さて d-次元 DHO の生成する空間の次元 n は 2d+1 と(d+1)(d+2)/2 の間であると考えられているが n=(d+1)(d+2)/2（生成空間の最大次元）の場合 4 個の DHO (Huybrechts DHO, Buratti-Del Fra DHO, Veronesean DHO, Taniguchi DHO(筆者の構成したもの))の存在が知られている。n=2d+1 および 2d+2 の場合の DHO については多くの研究があり熱気を持って調べられて来ていた。例えば Kantor と Dempwolff が Symplectic spread や Orthogonal spread との関係を活用して，2d+2 次元の生成空間をもつ非同型な DHO を大量に構成していた。しかるに，2d+2<n<(d+1)(d+2)/2 の場合については（n=(d+1)(d+2)/2 の DHO の射影による像になっている場合を除き）当時 DHO の存在自体すら全くわかっていなかった状況であった。このような DHO の存在を確かめるために（n=(d+1)(d+2)/2 の DHO の射影による像にはなっていない）多くの DHO の例を構成しそれらの性質を調べることが必要とされていた。

２．研究の目的

研究を開始した当時，筆者はそれまで知られていなかった生成空間の次元 n が 2d+2<n<(d+1)(d+2)/2 をみたすような一連の DHO (以降「S_c(l,GF(2 r)」と表します。ここに c は有限体 GF(2 r)の元，l は自然数。) をちょうど発見し，その具体例を手がかりとすることによって (当時は全くわかっていなかった) 生成空間の次元の高い DHO の研究を進めていく方針であった。またこの DHO は有限体上の(一般化された)APN 関数から構成された DHO に近い性質を持っていたため，APN 関数に似た有限体上の関数を発見できるのではないかという期待もあった。

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）当時新たに発見したばかりの生成空間の次元の高い DHO 達の性質を十分調べていく。また自己同型群を計算することにより生成空間の次元の高い DHO 達の性質を調べる。
（２）新たに発見した生成空間の次元の高い DHO 達と同様の構成の可能性を探究する。
（３）構成された DHO から有限体上の関数を構成する。
（４）有限体上の関数と生成空間の高い DHO との関係を追求する。

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番については研究が進み期待もしていなかった成果を得ることが出来た。２番については１番の構成と標数 2 の半体を結びつけることにより半体の性質を利用した多くの DHO の構成を発見することが出来た。しかし１番と２番の研究（特に２番の研究）が思いがけずに進展したため多くの時間をそちらに振り向けたこともあり，３番と４番については研究期間の最後の方まで思うように時間をかけることが出来ず，研究期間が終わりに近づいた頃ようやく今まで知られていなかった APN 関数の属を発見することが出来た次第であった。（なおこの発見に続き現在研究は次の段階に進んでいる。）
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出来た。

（１）単連結な DHO に関しては当時「限られたタイプの数種類のもの」かつ「生成空間の次元が非常に低いもの」しか存在がわかっていなかった。筆者の構成した族に属する DHO である 「S_c(l,GF(2 r)」 がある簡単な条件を満たせば単連結という性質を満たすことを見いだし，その結果非常に多くの非同型な，しかも生成空間の次元が高い，単連結な DHO を見いだすことが出来た。さらにこの単連結な DHO に対して Dempwolff-Edel による DHO の Extension という方法を用いると，さらに次元の高い生成空間をもつ，非同型な単連結 DHO の例が非常に多く構成できることがわかった。(対称で双線形な DHO に対しては 2 段階まで Extension という方法が適用できる。)

（２）筆者の構成した DHO の族である「S_c(l,GF(2 r)」の自己同型群を決定することが出来た。この証明は細かい点で非常に微妙な議論を必要とし証明は長い。また c=1 の場合と c が 1 でない場合では，性質に大きな違いがあるがあることがわかった。

（３）筆者の構成した DHO の族である「S_c(l,GF(2 r))」に属する２つの DHO 達「S_c1(l1,GF(2 r1)」と「S_c2(l2,GF(2 r2)」が，(c1 と c2 がガロア群の作用により互いに移り合いさらに) 整数「l1,l2」と「r1,r2」に関するある簡単な条件を満たせば、互いに

被覆する（被覆される）という関係があることを発見した（必要十分条件）。また被覆する（される）という関係にある場合の自己同形群の関係も決定した。

（４）標数 2 の可換な半体(SemiField)から，S_c(GF(2^r),1)の構成と似たような方法を用いて新しい高次元双対超卵形が構成できることを発見し，それらの性質を調べた。特に構成に使用する可換な半体達が Kantor の構成した半体達である場合には，それから高次元双対超卵形が構成される条件，およびそれら高次元双対超卵形達が同型であるための簡明な必要十分条件を見いだした。

（５）（４）の可換な半体から DHO を構成する方法を拡張し，３個の半体（そのうち２個は可換な半体，もう一つの半体は可換で有る必要がない）から新たな高次元双対超卵形が構成できることを見いだした。さらにある仮定の下に３個ずつの半体（全部で６個）から構成された２個の高次元双対超卵形が同型で有るための必要十分条件を見出した。さらに特に Kantor の可換な半体および Albert の半体を利用して構成した上記の高次元双対超卵形について，非常に具体的な同型判定条件を与えた。これは Jha, Jhonson, Biliotti による Albert の半体に関する詳しい研究（1999 年）を利用している。

（６）Taniguchi の高次元双対超卵形といわれている，筆者が 2009 年に発見した高次元双対超卵形について，その構成を一般化することによって今まで知られていなかった高次元双対弧（族のメンバーの個数が DHO より少ない）が構成できた。この双対弧は今まで知られていない興味深い加法公式を持っていることを示した。

（７）（５）の構成方法をさらに拡張し，任意有限個の半体（その一部は可換な半体である必要が有る）から DHO を構成する方法を発見した。この構成方法は「可換な半体を用いるパート」と「可換で有る必要がない半体を用いるパート」の両方が必要で，また「可換な半体のパートの番号付に対応した可換で有る必要がないパートの半体の番号付」が自然に定まっている。この構成により得られた DHO の同型問題を以下の特別な場合に解決した。①（DHO を構成する半体の内「可換な半体のパート」が互いにイソトピックでない場合）2 つの DHO が同型となる必要十分条件は「可換な半体のパート」の半体達の間にうまく対応をつけると対応する可換な半体達がイソトピックでありかつ「可換で有る必要のない半体のパート」についても（その対応により）イソトピックまたは反イソトピック（積の順を逆にするとイソトピック）になっていることである。②（DHO を構成する半体の内「可換で有る必要がない半体のパート」の半体達がすべて非可換である場合）2 つの DHO が同型となる必要十分条件は対応する非可換な半体達が互いにイソトピックまたは反イソトピックであることである。

（８）特別な bent 関数 B(x,y)=xy を用いた２次的な APN 関数を構成した。特別な bent 関数 B(x,y)を用いた構成は以前に２例(Carlet 氏による例および Zhu-Pott 氏達による例)が知られていたが、特別な有限体上においては今回発見した APN 関数の構成は以前知られていた２例と本質的に異なるということをコンピュータを用いて示した。また同様の構成方法で（非可換な）半体が構成できることも示した。

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 6 件）

① Hiroaki Taniguchi, New dimensional dual hyperovals, which are not quotients of the classical dual hyperovals, Discrete Mathematics, Vol. 337 (2014), pp65–75（査読有）

② Hiroaki Taniguchi, Some examples of simply connected dual hyperovals II, Finite Fields and Their Applications, Vol.36 (2015), pp1–13（査読有）

③ Hiroaki Taniguchi, Bilinear dual hyperovals from binary commutative presemifields, Finite Fields and Their Applications Vol.42 (2016) 93–101（査読有）

④ Hiroaki Taniguchi, On some bilinear dual hyperovals, Discrete Mathematics Vol.340 (2017) 3154–3166（査読有）

⑤ Hiroaki Taniguchi, Bilinear dual hyperovals from binary commutative presemifields II, Finite Fields and their Applications Vol. 49, (2018), 62–79（査読有）

⑥ 谷口浩朗, On higher dimensional dual hyperovals, 第 32 回代数的組合せ論シンポジウム報告集, pp94--99 (2016)（査読無）

〔学会発表〕（計 17 件）

① Hiroaki Taniguchi, On Covering maps of Bilinear Dual Hyperovals, Combinatorics 2014, Gaeta, Italy, 1 July

② 谷口浩朗, 高次元の dual hyperoval について, Workshop on Galois point and related topics, 2014 年 9 月 14 日, 滋賀大学

③ 谷口浩朗, Some examples of simply connected dual hyperovals 本組合せ論研究集会「代数的デザイン論とその周辺」, 2015 年 1 月 10 日, 熊本大学

④ 谷口浩朗, 単連結な高次元 dual hyperoval の例, 平成 26 年度 日本数学会 中国・四国支部例会 1 月 25 日, 徳島大学

⑤ Hiroaki Taniguchi, On some dual hyperovals, Fq12, 15 July 2015, Saratoga Springs (USA)

⑥ Hiroaki Taniguchi, On some bilinear dual hyperovals, Giornate di Geometria, 17 September 2015, Caserta (Italy)

⑦谷口浩朗, 高次元双対超卵形について, 第 32 回代数的組合せ論シンポジウム, 2015 年 6 月 23 日, 金沢大学（金沢）

⑧ 谷口浩朗, On some bilinear dual hyperovals, 「有限幾何とその周辺」研究集会, 2015 年 9 月 27 日, 東京女子大学

⑨ 谷口浩朗, 半体と高次元双対超卵形, 「有限幾何とその周辺-平峰先生を偲んで」研究集会, 2016 年 3 月 6 日, 熊本大学

⑩ Hiroaki Taniguchi, Bilinear dual hyperovals from binary commutative presemifields, Combinatorics 2016, 28 May 2016, Maratea, Italy

⑪谷口浩朗, 3 つの半体から構成される dual hyperoval について, 研究集会「有限幾何とその周辺」２０１６年9月４日, 東京女子大学

⑫ Hiroaki Taniguchi, Dual Hyperovals from Commutative Presemifields, 48th Southeastern International Conference on Combinatorics, Graph Theory & Computing, 9 March 2017, Florida Atlantic University, Boca Raton, USA

⑬谷口浩朗, Bilinear でない高次元双対超卵形の例, 研究集会「有限幾何とその周辺」２０１７年3月２４日, 東京女子大学

⑭Hiroaki Taniguchi, Bilinear DHO from three or more presemifields, The 13th International Conference on Finite Fields and their Applications, 8 June 2017, Gaeta, Italy

⑮Hiroaki Taniguchi, A variation of the dual hyperoval S_c using presemifields, The fifth Irsee Finite Geometry Conference, 15 September 2017, Kloster Irsee, Germany

⑯谷口浩朗, 非可換な半体から構成される DHO, 研究集会「有限幾何とその周辺」２０１７年9月3日, 熊本大学

⑰谷口浩朗, ある２次的な APN 関数について, 研究集会「有限幾何とその周辺」, ２０１８年3月２５日, 東京女子大学

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

(4)研究協力者：該当無し