様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　５　月　２６　日現在

機関番号：　３４４１９
研究種目：　基盤研究(C)
研究期間：　2011～2014
課題番号：　２３５４００３５

研究課題名（和文）正則アフィン平面から派生する有限体上の関数の研究

研究課題名（英文）Researches of functions on finite fields coming regular affine planes

研究代表者
中川　暢夫（NAKAGAWA, Nobuo）

近畿大学・理工学部・研究員

研究者番号：１００８８４０３

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：暗号理論では有限体上の関数で非線形度が高いものが重要である。そのような関数の一つにAPN関数がある。これらをEA同値類にわけて考える。当研究では2元体のn次線形群が作用するある置換群の可遷域の個数は非同値なquadratic APN関数の異なる同値類の総数に等しいことを示した。また、有限体上のある線形方程式の解が丁度2個である時の必要十分条件をその係数の関係式で求め,その応用として３つのAPN関数を構成し、これらを置換群の視点から特徴付けた。更にAPN関数の中で最重要なGold関数にEA同値な関数の表示を明確にした。

研究成果の概要（英文）：In the cryptography theory,it is important to construct functions over finite fields which have hight non-linearities. Almost perfect nonlinear(APN) functions are one of them. APN functions are classified in EA-equivalent classes. In the study,I consider some permutation group (G,S) where G is the linear group of degree n over GF(2) and S is a set of subspaces of the alternative product of a finite field F with some properties. I proved the number of G-orbits on S equals to the namber of EA equivalent classes of quadratic APN functions on F.I obtained some conditions that a special linear equation over a finite field has exactly two solutions and as a application of the results, I constructed three APN functions and decided subspaces corresponding to these functions up to EA-equivalence. Moreover I obtained an effective expression of APN functions which are equivalent to Gold functions which are most interesting ones among APN functions.

研究分野：　代数学

キーワード：　APN functions　finite fields　permutation group　EA-equivalence　plnar functions　alternative product　cryptography　linear equations

１．研究開始当初の背景

有限射影平面の位数は素数冪であろうという予想は Prime Power Conjecture としてよく知られているが条件なしで解決するには難問である。そこで、比較的大きな自己同型群をもつ有限射影平面や有限アフィン平面の研究が 50 年程前から多くの数学者によりなされてきた。射影平面についていうと、
点の集合の上に 2 重可遷群をもつ場合はデザルグ平面であることが Ostrom と Wagner により示された。
その後、Flags 上可遷に作用する自己同型
を有する場合は例外を除いてデザルグ平面になることが Kantor により示された。
点の集合上に可遷に作用する自己同型群を有する射影平面がどのようなものであるかは未解決である。
アフィン平面の場合は点の集合の上に可遷でさらに primitive に作用する自己同型を有する場合は translation plane になることが平峰豊により示された。点の集合に可遷でかつ正則に作用する自己同型をもつ場合は難問として未解決で残されてきたが、
二つの同じ位数の群 G と H の直積が点の集合に正則に作用して、H に入る各自己同型がこのアフィン平面に背景写像として作用するときは、G から H への planar 関数なるものが定義されて、この関数を決める問題となる。G と H が可換群のときはある奇素数 p に対し G と H は p-群になることが Blokhuis,Jungnickel 及び Schmidt により示された。更にこのとき G と H は基本可換 p-群に比較的近い構造を持つことを、以前当研究代表者が示した。
planar 関数で既知のものは両方の群が基本可換 p-群のものばかりであるが、この場合は有限体上の関数とみることができる。
有限体上の planar 関数は暗号理論に深く係わることが 20 年程前 Nyberg により指摘された。以来 planar 関数の研究は有限幾何ばかりでなく暗号理論の視点からも注目されてきた。標数 2 の有限体上の関数で planar 関数に相当するのが APN 関数である。ある尺度で測ると両方とも非線形度が最も高いものであるという共通点をもつ。
S-box を介して暗号を実用的に構成する際に標数 2 の有限体上の APN 関数や bent 関数が使用される。そのため、このような関数をできるだけ多く構成し、これらがどれぐらい多くありうるかを評価し、できれば非同値な APN 関数や bent 関数を分類することが求められてきた。
また標数が奇素数 p の有限体 F 上の quadratic planar 関数から GF(p)を部分構造にもつ可換 Semifield が構成され、逆に可換 Semifield から quadratic planar 関数が構成されることは当研究代表者等により調べられていたが、両者の関係をもっと精密に調べることが求められていた。

２．研究の目的

有限体の関数間に EA 同値であるかないかが定義され、EA 同値なものは本質的に同じものと考えてよい。
非同値な quadratic APN 関数の個数を評価し、分類すること、標数 p(奇素数)で同じバージョンの問題である非同値な quadratic planar 関数の個数を評価し分類することが当研究の目的であった。
また、quadratic planar functions に有限 Commutative semifields が対応することを明確にし、quadratic planar functions の EA-同値類と有限 Commutative semifields の同型類が 1 対 1 に対応するのかしないのかを見極めることも研究の目的であった。
可能なら、APN 関数や planar 関数と有限幾何やグラフとの係りを調べることも目的としていた。

３．研究の方法

標数 2 の有限体 F 上の quadratic APN 関数を F の交代積のある条件を満たす部分空間達の集合に作用する線形群 GL(F)での置換群の可遷域の個数を評価することにより、APN 関数の非同値な個数を評価し、できれば分類することが当研究の方法である。
奇標数の有限体 F 上の quadratic planar 関数についても上記の方法で F 上非同値な quadratic planar 関数の個数を評価して、分類をするのが当研究の方法である。
もう一つは有限体上の線形方程式の解の個数がこの体の中で惟一つまたは丁度二つである必要十分条件を求め、その応用として APN 関数もしくは planar 関数を構成することである。この研究を進めるにあたり、パリ大学で有限体上の関数で優れた研究を行っている C.Carlet 氏及び有限体と有限幾何の分野で先見性と独創力をもつ東京女子大の吉

荒聡氏と当研究の協力関係を保ち、折にふれ集中セミナーを行って研究の方向を見定めた。

４．研究成果

有限体 F 上の非同値な quadratic APN 関数の個数が F の交代積のある条件を満たす部分空間の集合に作用する線形群の置換群の可遷域の個数と等しいことを示した。(APN 関数の一つの EA 同値類が置換群の一つの可遷域に対応することを示し、この対応が 1:1 であることを示したのである。)
また、この個数があるパラメーターの交代和で表されることを示した。そして、それぞれのパラメーターの上限と下限を求めた。
標数 2 の体で濃度 2 冪の冪が偶数である場合で、F 上のある線形方程式の、F での解の個数が丁度 2 個である必要十分条件を係数の間の関係式で表すことにより求めた。
この応用として３つの APN 関数を構成し、これらの関数に対応する部分空間の形を決めた。
また APN 関数の中で最も重要な関数である Gold functions と同値になる関数がどのような形の関数であるかを明確にした。
奇素数 p に対し、濃度 p の n 乗の体 F で F 上非同値な quadratic planar 関数の個数が F の対称積のある条件を満たす部分空間の集合に作用する線形群 GL(F)の置換群の可遷域の個数に等しいことを示した。
F 上の quadratic planar 関数に F の対称積のある部分空間が 1:1 に対応することを利用して２種類の planar 関数の特徴付を行った。
更に、GF(p^n)上の quadratic planar Function を与えれば、GF(p)上 n 次元の有限可換 semifield が構成でき、逆に GF(p)上 n 次元の可換 semifield から GF(p^n)上の quadratic planar が構成できることをもう少し精密化した。
濃度が 2 の n 乗の体 F 上の 4 次の線形方程式の解の個数が i(i=1,2,4)であるような方程式の個数 N(i)を決めた。F 上 8 次の線形方程式の解の個数 i(i=1,2,4,8)であるような方程式の個数 N(i)のうち、N(1)と N(2)を決めた。
奇素数 p に対し、濃度 p の 2k 冪の有限体から GF(p)へのある条件を満たす bent 関数から強正則グラフが構成される。この条件を満たす bent 関数は二つ知られている。
P が 19 以下のとき、これらの二つの bent 関数から得られる強正則グラフが同型でないことを示した。
自然数 n について、$GL(n,2)$の主な部分群を決めた。

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　　1 件）

(1) On equations of Finite Fields of characteristic 2 and APN functions, Nobuo Nakagawa, to appear in AKCE International Journal of Graphs and Combinatorics （査読有）,2015(印刷中)

〔学会発表〕（計　　9 件）

(1) 有限体上の線形方程式の解の個数について、熊本組み合せ論研究集会-代数的デザイン論とその周辺,熊本県、熊本大学くすのき会館,2015/1/11

(2) On equations of Finite Fields of characteristic 2 and APN functions, Eighth Shanghai Conference on Combinatorics, Shanghai Jiao Tong Univ.,China(中国)2014/5/25

(3)On flag-transitive translation planes, 代数組み合せ論ミニ集会、兵庫県、神戸学院大学ポートアイランドキャンパス B 号館、2014/3/7

(4)有限射影平面及び有限アフィン平面の分類問題、田澤新成先生退職記念集会、大阪府、近畿大学東大阪キャンパス G 館,2014/2/20

(5)On differential spectrums of power functions over GF(2^m), 有限幾何とその周辺研究集会、大分県、大分大学工学部、2013/11/30

(6) On quadratic planar functions from the viewpoints of permutation groups, 11-th International Conference on Finite Fields and Their Applications, Ott-van-Guericke Univ. Magdeburg, Germany(ドイツ), 2013/7/26

(7)「有限幾何とその周辺」の研究集会の 35 年の軌跡、兵庫県、神戸学院大学、ポートアイランドキャンパス B 号館、2012/3/3

(8)On non-isomorphic problems of strongly regular graphs constructed by p-ary bent functions, Workshop on Algebraic Combinatorics, Shanghai Jiao Tong Univ. China(中国), 2011/9/15

(9) On non-isomorphic problems of strongly regular graphs constructed by p-ary bent functions, The 10th International Conference on Finite Fields and Their Applications, Ghent Univ. Belgium, 2011/7/11

〔図書〕（計　0 件）

ホームページ等
なし

６．研究組織
(1)研究代表者
中川 暢夫（ NAKAGAWA Nobuo ）
近畿大学・理工学部・研究員
研究者番号：10088403

(2)研究分担者
（なし ）

研究者番号：

(3)連携研究者
（なし ）

研究者番号：