数理解析研究所講究録
第2053巻 2017年 98-110

標準的な有限群論に基づく単項 APN 関数の同値関係判定

吉荒 聡
Satoshi Yoshiara
東京女子大学 現代教養学部 数理学科
yoshiara@lab.twcu.ac.jp

1 序

この原稿は 2016 年 12 月 7 日 (水) 午前 10 時から 10 時 50 分に京都大学数理解析研究所 4 階大教室で行われた筆者の講演「標準的な有限群論に基づく単項 APN 関数の同値関係判定」の一部を再現したものである. 紹介した主定理は既に論文 [4] 中の Theorem 1 として公刊されているので, 詳細に興味を持たれた方はこの論文をご参照ください.

この定理 (Theorem 1) は APN 関数と呼ばれている, 標数 2 の有限体上の関数の同値性に関する結果である. APN 関数は情報科学において有用で, 構成問題を柱として盛んに研究されている. 幾つかの無限系列が構成されており, 固定した大きさの体にも幾つかの異なる APN 関数が定義される. しかし, これらが本質的に異なるものであるのかどうかは, 従来真剣に検討されてこなかった問題である. Theorem 1 を用いて, 筆者は知られている無限系列が単項関数である場合に, この問題に完全な解答を与えることが出来た.

Theorem 1 の証明は線形代数と標準的な有限群論を用いるだけの初等的なものである. その粗筋を紹介するのが講演の主目的であったが, それに先立って APN 関数を含む非線形関数論の研究に関する概観を与えたので, この原稿でもその一部を再記する.

以下, F は p^n 元体 $\mathbb{F}_{p^n}$ (p は素数) を表し, F と F の直積 $F\times F=\{(x,y)\mid x,y\in F\}$ を $F\oplus F$ とも書く. F を p 元体上の n 次元ベクトル空間, $F\oplus F$ を p 元体上の $2n$ 次元ベクトル空間とみなす.

$F\oplus F$ 上の線形写像 λ は, F 上の線形写像 $\alpha,\beta,\gamma,\delta$ により $(x,y)^\lambda=((x)\alpha+(y)\gamma,(x)\beta+(y)\delta)$, $(x,y\in F)$ と書ける. この状況を, より印象的に

$$\lambda=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$$

と書くことにする. ここで, 例えば $(x)\alpha$ はベクトル $x\in F$ の線形写像 α による像を示す. この原稿では, 線形及びアフィン写像はベクトルに右から作用する形に書くことにする. 一方, 非線形な写像 f による $x\in F$ の像は $f(x)$ と書く.

2 非線形関数

有限体 F から F への関数で, 知られている暗号破り法 (差分法と線形法) に強い耐性を持つものは, 線形関数からなるべく遠い関数であることが知られている. これらの非線形関数は, 1960 年代後半から情報科学において注目を集める対象となり, 多くの研究が積み重ねられている. 実は, ある種の非線形関数は 1950 年代以来, 有限幾何の研究において, 平面関数として知られていた. 平面関数が存在するのは, 有限体 F の標数 p が奇素数である時に限

るが, 情報科学の立場からは標数 $p=2$ の有限体上の関数が重要である. 偶標数の有限体上で, 最も非線形度の高い関数が準完全非線形関数 (almost perfect nonlinear function–略してAPN 関数) である.

2.1 d-一様関数–非線形関数の形式的定義

関数 $f:F\to F$ が ($F=\mathbb{F}_{p^n}$ を素体 $\mathbb{F}_p$ 上のベクトル空間と見て) 線形であるとは, 任意の元 $x,y\in F$ について $f(x+y)=f(x)+f(y)$ が成立することである. この定義を差分関数の観点から述べれば, 任意の固定した元 $a\in F$ における差分関数 $f_a:F\ni x\mapsto f(x+a)-f(x)\in F$ が $f(a)$ という一定値を取る関数ということである. そこで, 感覚的には, 非線形度が高い関数とは, それぞれの元 $a\in F$ における差分関数 f_a が多くの値を取る関数であると考えられる. これを言い換えれば, それぞれの元 $a\in F$ における差分関数 f_a に対して, どの元 $b\in F$ の逆像 $\{x\in F\mid f_a(x)=b\}$ も大きな値を取らない, ということになる. ただし, $a=0$ のときには f_0 は零関数という定数関数になってしまうから, a は $F^\times:=F\setminus\{0\}$ を動くとする.

そこで, 差分関数の逆像の大きさに注目して, 関数 $f:F\to F$ の非線形度を次のように定義する.

定義 1 d を非負整数とする. 有限体 $F=\mathbb{F}_{p^n}$ 上の関数 $f:F\to F$ が **d-一様** *(d-uniform)* であるとは, すべての $a\in F^\times$ とすべての $b\in F$ に対して, 方程式 $f(x+a)-f(x)=b$ の F における解 x の個数が d 個以下であることとする:

$$\#\{x\in F\mid f(x+a)-f(x)=b\}\le d\quad\forall a\in F^\times, b\in F.$$

特に, 1-一様な関数および 2-一様な関数を, それぞれ**完全非線形関数** *(perfect nonlinear function)* および**準完全非線形関数** *(almost perfct nonlinear function)* と呼ぶ. これらを略記して, 完全非線形関数を **PN 関数**, 準完全非線形関数を **APN 関数**と呼ぶのが通例である.

f が有限体 F 上の PN 関数であることは, 各元 $a\in F^\times$ における差分関数 $f_a(x)=f(x+a)-f(x)$ が F 上の全単射であることとは同値である. f が単項関数 $f(x)=x^d$ の場合には, f が F 上の PN 関数であるための必要かつ十分な条件は, 区間 $[1,|F|-2]$ の属するすべての整数 t に対して, $A(t):=\lfloor dt/(|F|-1)\rfloor$ とおくとき,

$$\sum_{r=0}^{t}(-1)^r\binom{t}{r}\sum_{j=1}^{A(t)}\binom{dt-dr}{(|F|-1)j-dr}\equiv 0\pmod p$$

が成立することである.

2.2 PN 関数と幾何学の関連

PN 関数は**平面関数** (planar function) とも呼ばれる. その理由は, F 上の完全非線形関数 f が存在することと, $F\times F$ を点集合とする (ある対称性を持つ) 射影平面が存在することが同値であるという事実による. より一般に, Dembowski と Ostrom は平面関数を, 群の間の関数として, 次のように定義した.

二つの有限群 G と H に対して, G から H への写像 $f: G \to H$ が**平面関数**であるとは, 単位元と異なる任意の $a \in G^\times := G \setminus \{1_G\}$ に対して, $f_a(x) := f(xa)f(x)^{-1}$ $(x \in G)$ により定義される写像 f_a が群 G から群 H への全単射であること.

Dembowski と Ostrom は, 1960 年代初めに, 有限群 G から H への平面関数 f が存在するならば, $|G| = |H|$ であり, $G \times H$ を点集合とするある種の対称性を持つ射影平面が構成できること、しかもその逆も成立することに気づいた. 平面関数を構成することにより, 当時としては新しい射影平面が幾つか構成されたのである. 実は, 現在に至るまで, 知られた平面関数 $f: G \to H$ の例においてはすべて, $G \cong H \cong$ ある有限体の加法群 $(F; +)$ となっている. これは, 有名な未解決問題である.

未解決問題 1 有限群 G から H への平面関数が存在すれば, ある有限体 F に対し $G \cong H \cong (F; +)$ か?

PN 関数に限らず, 有限体上の関数に関する定義を, 同じ位数の有限群の間の関数に関する定義に拡張する試みは重要であろう. 例えば, 有限体上の関数が quadratic であるという定義は, 次のように拡張するのが自然であろう. 有限群 G, H に対して, 関数 $f: G \to H$ が **qudariatic** とは, $x, y \in G$ に対して $b_f(x, y) := f(xy)f(x)^{-1}f(y)^{-1}f(1_G)$ として定義される関数 b_f が, 第一変数 x 及び第二変数 y に関して準同型写像であること. 2015 年 10 月に, 当時日本大学理工学部 D1 の中村周平氏は, 有限群 G から H の間に quadratic な平面関数 f が存在すれば, 上の未解決問題は正しいことをエレガントな方法で示した.

平面関数 (PN 関数) はまた, 非結合代数と深い関連がある. 積に関する結合法則以外のすべての非可換体の公理を満たす代数構造を, **semifield** という. 次の事実が知られている.

- $(F; +, \circ)$ (p 奇素数) が有限な semifield であれば, $f(x) = (1/2)(x \circ x)$ は F 上の PN 関数.
- F (p 奇素数) 上の PN 関数 f が $f(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i+p^j}$ という形 (**Dembowski-Ostorm 多項式**という) ならば, $x \circ y := f(x + y) - f(x) - f(y)$ により定義される積を考えると $(F; +, \circ)$ は有限可換 semifield.

完全非線形関数 (PN 関数) は, Dembowski と Ostrom が定義した平面関数を有限体上に限った概念であるが, 非線形関数という全く別の観点から情報科学において導入されたわけである. 次に述べるように, 情報科学で主体である偶標数の有限体上では完全非線形関数は存在しない. このため, 情報科学においては準完全非線形関数 (APN 関数) に興味が集中したが, Zhou は 2012 年に偶標数の体上にも完全非線形関数の概念を拡張した. この関数から射影平面が構成できるが, 残念ながら今のところ新しいものは出て来ていないようである.

2.3 APN 関数は偶標数の体上における最も非線形な関数

次の観察が示すように, APN 関数は偶標数の体上における最も非線形な関数である.

観察 有限体 F 上の完全非線形関数が存在するならば, F の標数 p は奇数.

Proof. なぜならば, F の標数が 2 のときには

$$f(x+a)-f(x)=f((x+a)+a)-f(x+a)$$

であるから, $f(x+a)-f(x)=b$ の解 x に対して $x+a$ $(\neq x)$ もまたその解. □

そこで, 計算機の世界での運用上は, 標数 2 の有限体上の最も非線形な関数である APN 関数がより有用と考えられ, 情報科学の研究者は関数の構成に精力を注いできた. 主な成果を挙げると,

- 1993 年に情報科学の研究者 Nyberg らが命名.
- Dobbertin は単項 APN 関数の系列を構成 1993〜2008.
- Edel-Kureghyan-Pott による単項でない APN 関数の発見 2006.
- Carlet, Pott, McGuire らを中心に, 単項でない APN 関数の無限系列の熾烈な構成競争が繰り広げられる 2006〜2010.

となるが, 現在のところ, 発見された単項 APN 関数 f は, 2^6 元体上の一つの例外を除いて, すべて単項であるかまたは二次的 (quadratic), すなわち

$$f(x)=f(0)+\sum_{i,j=0}^{n-1}a_{ij}x^{2^i+2^j}$$

$(a_{ij}\in F)$ という形である. quadratic 関数と DO-多項式との類似に注意.

2.4 CCZ-同値–非線形関数から新しい非線形関数を構成する

天下りであるが, 二つの関数の間のある同値関係を次のように定義する. F 上の関数 f に対して, そのグラフ $G(f)$ とは, $G(f):=\{(x,f(x))\mid x\in F\}$ として定義される $F\oplus F$ の部分集合のこととする.

定義 2 F 上の関数 f が関数 g に **CCZ-同値**とは, $F\oplus F$ 上のアフィン全単射 μ であって f のグラフを g のグラフに移す $(G(f)^\mu=G(g))$ ものが存在すること.

CCZ という名称は, この概念が初めて現れた論文 1998 の著者 Carlet, Charpin and Zinoviev の頭文字を集めたものである.

関数のグラフの全単射アフィン写像による像は, 一般にはある関数のグラフの形にはならないことに注意せよ. 実際に, $\lambda+(c,d)$ を $F\oplus F$ 上の全単射アフィン写像 (λ が線形写像で, $(c,d)\in F\oplus F$ は定数和の部分) とすると, $\lambda=\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}$, すなわち $(x,y)\lambda=((x)\alpha+(y)\gamma,(x)\beta+(y)\delta)$ $(\forall x,y\in F)$ を満たす F 上の線形写像 $\alpha,\beta,\gamma,\delta$ が存在するので, 関数 f のグラフ $G(f)=\{(x,f(x))\mid x\in F\}$ のベクトル $(x,f(x))$ の $\lambda+(c,d)$ による像は

$$(x,f(x))\lambda+(c,d)=((x)\alpha+(f(x))\gamma+c,x\beta+(f(x))\delta+d)$$

であり, x が F の元を動くとき, $(x,f(x))$ が関数 g のグラフ $G(g)$ を作るための必要かつ十分な条件は,

(g1) 写像 $F \ni x \mapsto (x)\alpha + (f(x))\gamma \in F$ が全単射であり, かつ

(g2) $g((x)\alpha + (f(x))\gamma + c) = (x)\beta + (f(x))\delta + d$ がすべての $x \in F$ について成立する,

と述べることが出来る. 上の条件のうち, どちらも無条件には成立しえない.

CCZ-同値という概念の非線形関数論における重要性は, 「CCZ-同値は d-一様性を保つ」という事実による. すなわち, 次が示せる.

命題 3 有限体 F 上の関数 f が d-一様関数であるならば, f と *CCZ*-同値な任意の関数 g も d-一様である. 特に, *PN* 関数と *CCZ*-同値な関数は *PN* であり, *APN* 関数と *CCZ*-同値な関数は *APN* である.

1998 の CCZ による論文では, APN 関数のみについてこの性質が検証された. この論文では, CCZ 同値の定義がかなり異なる形で与えられている. 後でみるように, PN 関数については, CCZ-同値という概念は EA-同値という概念と同等であり, その定義から, 上の事実が PN 関数について成立していることはすぐわかる. 従って PN 関数に関する上の命題は改めて言うまでもない事実として認識されていた. また, 一般に d-一様関数に対して上の命題が成立することも, 群環の形で書いてみるとすぐわかるので, この事実を認識していた研究者は筆者や多分 Pott 氏や Carlet 氏を含めて多数いると推測する. しかし, 筆者の知る限り, 上の命題が証明も含めて明記されたのは Dempwolff による 2016 年の preprint が初めてである.

2.5 拡大アフィン同値–より精密な同値

f が PN 関数である場合, f と g が CCZ-同値であれば, それを与える $F \oplus F$ 上のアフィン全単射 $\lambda + (c, d)$ は部分空間 $\{(0, y) \mid y \in F\}$ を不変にすることが示される. すなわち λ を F 上の線形写像 $\alpha, \beta, \gamma, \delta$ により $\lambda = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ と書くならば, $\gamma = 0$ である.

この事実を確認しよう. まず, α は単射である. 実際, α の核が $a \neq 0$ を含むならば, f が PN 関数なので, 差分関数 f_a が全単射であるから, $f(x+a) - f(x)$ が γ の核に入るような元 $x \in F$ が存在する. このとき $(x+a)\alpha + (f(x+a))\gamma = (x)\alpha + (f(x))\gamma$ となり, これは条件 (g1) (写像 $x \mapsto (x)\alpha + (f(x))\gamma$ の単射性) に反する. すると $\gamma = 0$ である. 実際, γ の像が $(b)\gamma \neq 0$ を含むならば, α が単射従って全単射であるから, $(a)\alpha = (b)\gamma$ を満たす $a \in F$ が存在する. $a \neq 0$ であり, 差分関数 f_a は全単射であるから, $f(x+a) - f(x) = -b$ を満たす $x \in F$ が存在する. すると $(x+a)\alpha + (f(x+a))\gamma = (x)\alpha + (f(x))\gamma + (a)\alpha + (-f(x) + f(x+a))\gamma = (x)\alpha + (f(x))\gamma + (a)\alpha - (b)\gamma = (x)\alpha + (f(x))\gamma$ であり, これは条件 (g1) に反する.

この性質 $\gamma = 0$ が満たされるとき, 条件 (g1) は写像 α が全単射であることと同値で, これは $\lambda = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$ の全単射性から保証される. また条件 (g2) は次の形となる.

すべての $x \in F$ について $g((x)\alpha + c) = (f(x))\delta + d + (x)\beta$.

これは関数 $g(x)$ が関数 $f(x)$ から変数変換を施して得られることを示す. この事実を踏まえて, 次のように定義する.

定義 4 F 上の関数 f が g に**拡大アフィン同値** *(extended affine*-略して **EA 同値***)* とは, F 上の全単射線形写像 α, δ 及び F 上の線形写像 β 及び $c, d \in F$ が存在して次の等式が成立すること.

$$g((x)\alpha + c) = (f(x))\delta + d + (x)\beta, \quad \forall x \in F.$$

この関係は単純な変数変換による関係なので, 検証することが容易である. また, ある群の作用による軌道と見なせることが知られている. 更に, EA-同値は CCZ-同値で保存されない幾つかの性質を保つ. 主要な性質を挙げると,

- PN 関数については, CCZ-同値と EA-同値は同じ概念.
- PN, APN (より一般に d-一様) 関数に EA-同値な関数は PN, APN (d-一様).
- Quadratic 関数に EA-同値な関数は quadratic. (Quadratic 関数に CCZ-同値でも, quadratic でない関数の例は存在する.)

2.6 同値性の幾何学的言いかえ (吉荒 2010)

詳しくは触れないが, d-一様性を保つ CCZ-同値ならびに EA-同値という性質を幾何学的に言い換えることが出来る. 特に, quadratic APN 関数から DHO という組合せ構造 (私が研究対象としてきた構造–射影平面中の超卵型という概念の高次元化) が定義され, その DHO としての同値性が APN 関数としての EA-同値性に翻訳できる, という事実が, 私を APN 関数の同値性の検証に引き込んだ動機であった.

F 上の APN 関数 f に対して, semibiplane と呼ばれる性質を持つあるグラフ Γ_f が定義され, また quadratic APN 関数 f に対し DHO という組合せ構造 $\mathcal{S}[f]$ が定義されて, 次を満たす.

- f と g が CCZ-同値 $\Leftrightarrow$ Γ_f と Γ_g がグラフとして同型.
- f と g が EA-同値 $\Leftrightarrow$ $\mathcal{S}[f]$ と $\mathcal{S}[g]$ が DHO として同型.

従って, APN 関数 f に対する $\mathrm{Aut}(\Gamma_f)$ は CCZ-同値性の判定に, quadratic APN 関数 f に対する $\mathrm{Aut}(\mathcal{S}[f])$ は EA-同値性の判定に, それぞれ使える.

3 既知の APN 関数

知られている APN 関数の無限系列はすべて, 単項式 x^d または quadratic 関数 $\sum_{i,j} a_{ij} x^{2^i+2^j}$ に CCZ-同値である.

- Gold 関数は, 単項 かつ quadratic APN 関数として知られている唯一の例.
- 単項式にも quadratic 関数にも CCZ-同値でない, 唯一知られている APN 関数の例は $\mathbb{F}_{2^6}$ 上のもの.

この章では, 現時点で知られている APN 関数を簡潔に紹介する.

3.1 単項式で表示できる APN 関数の6つの無限系列

単項式で表される APN 関数の無限系列として, 現時点では次の 6 系列が知られている. 故 Dobbertin 氏は, 単項 APN 関数のすべての無限系列はこれで尽くされていると予想していたようである.

表 1: $\mathbb{F}_{2^n}$ 上の知られている単項 APN 関数 x^d

名称	べき指数 d	条件	代数的次数
Gold	2^s+1	$(s,n)=1$, $1\le s<n/2$	2
Kasami	$2^{2s}-2^s+1$	$(s,n)=1$, $2\le s<n/2$	$s+1$
Welch	2^t+3	$n=2t+1, n\ge 9$	3
Niho	$2^t+2^{t/2}-1$, t even $2^t+2^{(3t+1)/2}-1$, t odd	$n=2t+1\ge 13$ $n=2t+1\ge 11$	$(t/2)+1$ $t+1$
Inverse	2^n-2	$n=2t+1$	$n-1$
Dobbertin	$2^{4t}+2^{3t}+2^{2t}+2^t-1$	$n=5t$	$t+3$

未解決問題 2 単項 APN 関数を分類せよ.

3.2 知られている qudaratic APN 関数の無限系列

以下に, 現時点で知られている quadratic APN 関数の無限系列を重なりがないようにまとめた. 筆者の知る限りでは, これが現時点での最新の情報である.

表 2: $F\cong\mathbb{F}_{2^n}$. s は整数で $1\le s\le n-1$, $(n,s)=1$.
i は整数; ζ,ζ':F の原始元; η,η':部分体 $\mathbb{F}_{2^m}$ の元.

(1) $n=3m$, $(m,3)=1$, $m\ge 3$: $i\in\{1,2\}$, $i\equiv sm \pmod 3$.
$f(x)=x^{2^s+1}+\zeta^{2^m-1}x^{2^{mi}+2^{m(3-i)+s}}$.

(2) $n=4m$, $(m,2)=1$, $m\ge 3$: $i\in\{1,3\}$.
$f(x)=x^{2^s+1}+\zeta^{2^m-1}x^{2^{mi}+2^{m(4-i)+s}}$.

(3) $n\ge 7$: $f(x)=x^3+\mathrm{tr}(x^9)$. (tr は F 上の絶対トレース.)

(4) $n=3m$, $(m,3)=1$; $s\equiv -m \pmod 3$, $\eta\eta'\ne 1$.
$f(x)=\zeta^{2^m}x^{2^{-m}+2^{m+s}}+\zeta x^{2^s+1}+\eta x^{2^{-m}+1}+\eta'\zeta^{2^m+1}x^{2^{m+s}+2^s}$.

3.3 二つの一般的構成法–quadratic APN 関数を構成

更に, 筆者の知る限り, 次の二つの一般的な APN 関数の構成法が知られているが, どちらも quadartic なものを与える.

表 3: $n=2m$, $F=\mathbb{F}_{2^n}$, $K=\mathbb{F}_{2^m}$. $\beta\in F\setminus K$.
F と $K\times K$ を $F\ni x+y\beta\leftrightarrow(x,y)\in K\times K$ により同一視.

(a) 整数 s: $(s,m)=1$, 偶数 i 及び $\alpha \in K \setminus \{x^3 \mid x \in K\}$ に対し,
$f(x,y) := (x^{2^s+1} + \alpha y^{(2^s+1)2^i}, xy)$ は F 上の APN 関数.

(b) 整数 i,j, $(i-j,m)=1$; $g_l \in K$ $(l=1,\ldots,4)$, $g_1 \neq 0$, $g_4 \neq 0$;
$G(x,y) := g_1 x^{2^i+2^j} + g_2 x^{2^i} y^{2^j} + g_3 x^{2^j} y^{2^i} + g_4 y^{2^i+2^j}$ とおく.
F 上の写像 $f(x,y) := (G(x,y), xy)$ が APN $\Leftrightarrow$
多項式 $G(X,1)$ が K 中に解を持たない.

4 APN 関数の同値性に関する筆者の結果

筆者は, APN 関数が互いに同値であるか否かの検証を気にかけてきた. その動機は, 一つは筆者の DHO 研究との関連によるものであり, またこの種の問題に群論的思考が有効であるとの見通しによるものである. 現時点で知られている APN 関数が, 一つの例外を除いて, 単項なものと quadratic なものであり, 後者には DHO という幾何学的構造との関連があるので, 筆者の研究は次のような流れで行われた.

Quadratic APN 関数間の同値性

定理 5 *[3]* $F=\mathbb{F}_{2^n}$ 上の *quadratic APN* 関数 f, g に対し, f と g が *CCZ*-同値 $\Leftrightarrow$ f と g は *EA*-同値.

証明は初等的で, DHO への帰着と簡単な群論に基づく. この結果は, 将来発見されるものも含む quadratic APN 関数の間の CCZ-及び EA-同値性問題を原理的に解決している. しかし, 例えば上記に紹介した既知の quadratic APN 関数間に EA-同値が存在しないことを点検するのは, 一方が Gold 関数 (これは単項かつ quadratic) ないしは Carlet 関数 (表 2 の (3)) でない限り面倒であり, まとまった結果は公刊されていない.

単項 APN 関数と quadratic APN 関数の同値性

定理 6 *[4, Theorem 2] (2013年に得られた成果)*
f を有限体 $F \cong \mathbb{F}_{2^n}$ 上の *quadratic APN* 関数, g を F 上の単項 *APN* 関数とする. f と g が *CCZ*-同値である $\Leftrightarrow$ f が *Gold* 関数に *EA*-同値かつ $g(x)=x^d$ のべき指数 d は $2^a(2^s+1)$, $(s,n)=1$, の形.

この結果により, EA-同値を除き, Gold 関数は単項かつ quadratic な唯一の APN 関数である. この結果はまた, 将来発見されるものも含む単項 APN 関数と quadratic APN 関数の間の CCZ-同値性問題を原理的に解決している.

単項 APN 関数間の同値性

定理 7 *[4, Theorem 1] (2015年に得られた成果)*
f および g を有限体 $F=\mathbb{F}_{2^n}$ 上の単項 *APN* 関数とし, そのべき指数を d, e とする. $f(x)=x^d$, $g(x)=x^e$: このとき, f と g が *CCZ*-同値 $\Leftrightarrow$ ある整数 $a \in [0, n-1]$ が存在して, 次のいずれかが成立.

(A) $e \equiv 2^a d \ (mod\ 2^n - 1)$.

(B) $de \equiv 2^a \ (mod\ 2^n - 1)$.

この結果は, 将来発見されるものも含む単項 APN 関数の間の CCZ-同値性問題を, べき指数間の単純な合同式の検証に帰着するものであり, 原理的には同値性問題を解決している. 次の章で紹介するのは, この定理の証明の概要である.

既知の単項 APN 関数間の同値性 上述の定理の応用として, 既知の単項 APN 関数間の同値性問題が完全に解決された. 詳細は [4, Proposition 2] を参照されたい. 概要を述べれば, 次のようになる.

> Gold 関数と Kasami 関数が CCZ-同値である場合が, $n = 5$ の場合に起こる: $x^{1+2} \sim x^{1-2^2+2^4}$ on $\mathbb{F}_{2^5}$. しかし, それ以外は, 表 1 に記した (Gold, Kasami, などの) 族名称の異なる二つの単項 APN 関数は CCZ-非同値である. また, 同じ属の単項 APN 関数の場合も, (表の範囲の) パラメーターが異なれば CCZ-非同値である.

Plataeued APN 関数間の同値性 この結果には, 講演では全く触れる時間がなかったが, 簡略に報告する.

Quadratic 関数の概念を拡張して, **plateaued 関数**という概念が定義される. 詳細は [5] を参照されたい. 例えば, Kasami 関数は plateaued 関数であることが示される [6].

定理 8 *[5, Theorem 3]* $F = \mathbb{F}_{2^n}$ 上の *APN* 関数 f, g が共に *plateaued* であり, 更に f が単項であるとする. このとき, f と g が *CCZ*-同値であれば *EA*-同値.

これを使って, Kasami 関数とその他の単項関数の同値性問題を解決することも出来る.

未解決問題 3 Plateaued という性質は EA-同値により不変だが, CCZ-同値により不変であるか?

未解決問題 4 上述の諸定理の結果は, d-一様な関数に対して一般化できるか?

単項 APN 関数に対する結果は, 最後に報告するように, 既に Dempwolff が究極的な形に一般化した.

5 群論をどう用いるのか? Thm.1 の証明の概略

本章では, 本稿の主目的である [4, Theorem 1] の証明の概略を述べる.

5.1 関数の自己同型群

$AGL(F\oplus F)$ は $F\oplus F$ 上の全単射アフィン変換全体のなす群を表す:

$$AGL(F\oplus F)=\{\lambda+(c,d)\mid c,d\in F,\lambda=\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}\in GL(F\oplus F)\}.$$

$AGL(F\oplus F)\cong 2^{2n}:GL(2n,\mathbb{F}_2)$ である.

関数 $f:F\to F$ のグラフ $G_f:=\{(x,f(x))\mid x\in F\}$ の**自己同型群** $\mathrm{Aut}(f)$ とは, 次に定義される $AGL(F\oplus F)$ の部分群のこととする.

$$\mathrm{Aut}(f):=\{\lambda+(c,d)\in AGL(F\oplus F)\mid (G_f)(\lambda+(c,d))=G_f\}.$$

5.2 単項 APN 関数の自己同型群

$f_d(x)=x^d$ を単項 APN 関数とする. $\mathrm{Aut}(f_d)$ の重要な部分群を紹介する.

そのため $b\in F^\times$ による積を m_b と書く: $m_b:F\ni x\mapsto xb\in F$. m_b はベクトル空間 F の全単射線形変換, すなわち $m_b\in GL(F)\cong GL(n,\mathbb{F}_2)$ である. このとき, 任意の $b\in F^\times$ に対して, $F\oplus F$ 上の写像

$$(x,y)\mapsto(xb,xb^d)=(x,y)\begin{pmatrix}m_b&0\\ 0&m_{b^d}\end{pmatrix}$$

は $\mathrm{Aut}(f_d)$ の元であり, b が $F^\times$ を動くとき, それらの全体は, $\mathrm{Aut}(f)$ 中の位数 2^n-1 の巡回部分群をなす. この $\mathrm{Aut}(f_d)$ の部分群を $Z^{(d)}$ と記す:

$$Z^{(d)}:=\{\begin{pmatrix}m_b&0\\ 0&m_{b^d}\end{pmatrix}\mid b\in F^\times\}.$$

巡回群 $Z^{(d)}$ は $F\oplus F$ の次の部分空間 X,Y を不変にしている.

$$X:=\{(x,0)\mid x\in F\},\quad Y:=\{(0,y)\mid y\in F\}.$$

5.3 基本的なアイデア

根幹はある部分群の共役性を示すことである. つまり, 証明は以下の (1), (2) の二つに分かれる. $F\cong\mathbb{F}_{2^n}$ とする.

(1) 主張「$\mathrm{Aut}(f_d)$ の任意の位数 2^n-1 の巡回群は $Z^{(d)}$ に共役」を示す.
(2) 共役性の主張 (1) から Theorem 1 が示される.

まず, (1) の概略を述べる. $n=6$ の場合は, 個別に処理する. $n\neq 6$ とすると, Zsigmondy の定理により, 2^n-1 には, いわゆる **2-primitive prime divisor** が存在する. これは, 2^n-1 を割り切るが, n より小さい自然数 i に対する 2^i-1 は割り切らないような素数 p のことである.

共役性の主張 (1) を示すための基本方針 p を 2^n-1 の 2-primitive prime divisor とする. 巡回群 $F^\times$ の (唯一の) シロー p-部分群 P に対し,

$$Z_P^{(d)} := \{\begin{pmatrix} m_b & 0 \\ 0 & m_{b^d} \end{pmatrix} \mid b \in P\}$$

とおく. このとき, 次の結果が示せる [4, Prop.1, Cor.2].

(1-1) $n \neq 6$ のとき, $Z_P^{(d)}$ は $\mathrm{Aut}(f_d)$ の Sylow p-部分群.

(1-2) $Z_P^{(d)}$ の $\mathrm{Aut}(f_d)$ における中心化群 C に対し, $[C : Z^{(d)}] \leq 2$.

上の (1-1), (1-2) から, (1) における共役性の主張が導かれることを示そう.

$\mathrm{Aut}(f_d)$ の任意の位数 2^n-1 の巡回部分群 Z を取る. $|Z| = |Z^{(d)}| = 2^n-1$ だから, Z のシロー p-部分群 Z_p と $Z^{(d)}$ のシロー p 部分群 $Z_P^{(d)}$ の位数は等しい. 主張 (1-1) から, Z_p と $Z_P^{(d)}$ は共に, 群 $\mathrm{Aut}(f)$ のシロー p-部分群である. 従って, シローの定理により, Z_p と $Z_P^{(d)}$ は群 $\mathrm{Aut}(f)$ において共役であり, $g^{-1}Z_pg = Z_P^{(d)}$ を満たす $g \in \mathrm{Aut}(f_d)$ が存在する. よって, これらの部分群の中心化群 $C_{\mathrm{Aut}(f)}(Z_p)$ と $C_{\mathrm{Aut}(f)}(Z_P^{(d)})$ も共役である: $g^{-1}C_{\mathrm{Aut}(f)}(Z_p)g = C_{\mathrm{Aut}(f)}(Z_P^{(d)})$.

Z は可換だから, $C_{\mathrm{Aut}(f)}(Z_p)$ の位数 2^n-1 の部分群で, $g^{-1}Zg$ は $g^{-1}C_{\mathrm{Aut}(f)}(Z_p)g = C_{\mathrm{Aut}(f)}(Z_P^{(d)})$ の位数 2^n-1 の部分群である. 一方, $Z^{(d)}$ は可換だから, $Z^{(d)}$ も $C_{\mathrm{Aut}(f)}(Z_P^{(d)})$ の位数 2^n-1 の部分群である. 主張 (1-2) から, $Z^{(d)}$ は $C_{\mathrm{Aut}(f)}(Z_P^{(d)})$ の位数 2^n-1 の唯一の部分群である. 従って, $g^{-1}Zg = Z^{(d)}$ であり, (1) の共役性が示された.

(1-1),(1-2) の証明 主張 (1-1) に関しては, $|GL(F\oplus F)| = |GL_{2n}(2)| = 2^{n(2n-1)}\prod_{i=1}^{2n}(2^i-1)$, $2^{n+i}-1 \equiv 2^i-1 \pmod{2^n-1}$ から容易に確かめられる.

主張 (1-2) の証明の粗筋を述べる. ここで基本的な役割を果たすのは, 線形代数である. W を先の $F\oplus F$ の部分空間 X, Y のいずれかとする. $Z_P^{(d)}$ の生成元 λ が W 上に引き起こす線形変換の最小多項式を m_{λ_W} とする. このとき, 次が成立する.

- m_{λ_W} は既約多項式.
- $F_W = \{f(\lambda_W) \mid f(t) \in \mathbb{F}_2[t]\}$ は F と同型な有限体.
- $m_{\lambda_X} = m_{\lambda_Y} \Leftrightarrow$ ある $a \in \mathbb{Z}$ が存在して $d \equiv 2^a \pmod{|P|}$.

これらの事実に基づき, λ 従って $Z^{(d)}$ の群 $GL(F\oplus F)$ における中心化群 $C_0 := C_{GL(F\oplus F)}(\lambda)$ を計算することが出来る [4, Lemma 5].

- $m_{\lambda_X} \neq m_{\lambda_Y}$ のとき, $C_0 = \{(\alpha, \delta) \mid \alpha \in F_X^\times, \delta \in F_Y^\times\}$.
- $m_{\lambda_X} = m_{\lambda_Y}$ のとき, $F = F_X = F_Y$ と見て, $C_0 = \{\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \mid \alpha_{ij} \in F\} \cong GL_2(F)$.

$C = C_0 \cap \mathrm{Aut}(f_d)$ から C を計算する. 前者の場合, $C = Z^{(d)}$ であることが示され, 後者の場合, $GL_2(F)$ の部分群の分類を用いて (1-2) が結論出来る.

共役性の主張 (1) から Theorem 1 を示す. 最後に, 共役性の主張から定理が導かれることのスケッチを与える. $n=6$ のときには直接示す. そこで $n \neq 6$ としてよい.

$f_d(x)=x^d$ と $f_e(x)=x^e$ は APN 関数で, CCZ-同値であるとし, 同値を与える $AGL(F\oplus F)$ の元 α' を取る. $(G_{f_d})\alpha' = G_{f_e}$ だから, $\alpha' Z^{(e)} \alpha'^{-1}$ と $Z^{(d)}$ は共に $\mathrm{Aut}(f_d)$ の位数 2^n-1 の巡回部分群である. 従って, 共役性の主張 (1) より, $g^{-1}\alpha' Z^{(e)} \alpha'^{-1} g = Z^{(d)}$ を満たす $\mathrm{Aut}(f_d)$ の元 g が存在する. $\lambda := g^{-1}\alpha'$ とおくと, $\lambda \in AGL(F\oplus F)$ で $Z^{(e)} = \lambda^{-1} Z^{(d)} \lambda$ である. $(0,0)\lambda = (0,0)$ はすぐ確かめられるので $\lambda \in GL(F\oplus F)$ である.

ここで, 次の事実に注意する [4, Cor.1]. 論文 [4] では, この命題を補題 5 の応用として示したが, より単純に計算で示すことも可能である.

> $F\oplus F$ の自明でない $Z^{(d)}$-不変部分空間は
> $X=\{(x,0) \mid x\in F\}$ と $Y=\{(0,y) \mid y\in F\}$ のみ.

もちろん, 同じことが $Z^{(e)}$ についても成立する.

ここで, $(X)\lambda$ と $(Y)\lambda$ は $F\oplus F$ の自明でない $Z^{(e)}(=\lambda^{-1}Z^{(d)}\lambda)$-不変部分空間であることに注意する. すると $Z^{(e)}$ についての上の事実から, $\{(X)\lambda, (Y)\lambda\} = \{X, Y\}$ である. 従って, 次のいずれかが成立する.
(A) $(X)\lambda = X$ かつ $(Y)\lambda = Y$, または (B) $(X)\lambda = Y$ かつ $(Y)\lambda = X$.

(A) のときには $\lambda = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$ の形で, $\alpha\delta^{-1}$ は Singer 群 $\{m_b \mid b\in F^\times\}$ の部分群で, F 上既約に作用するものを正規化する. そのような部分群の正規化群は Singer 群の正規化群に一致する (例えば Huppert, Endlich Gruppen の Satz II.7.3) から, その形を見ると定理 1 の場合 (A) を得る. (B) のときには $\lambda = \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}$ の形で, $\beta\gamma^{-1}$ は Singer 群 $\{m_b \mid b\in F^\times\}$ の F 上既約な部分群を正規化する. その群の正規化群の形から, 定理 1 の場合 (B) を得る.

以上概観したように, 共役性の主張 (1) が示されれば, 定理 Theorem 1 が得られるのである.

5.4 Dempwolff による Theorem 1 の究極的一般化

いささか驚くべきことに, Thm 1 における仮定「f, g は APN 関数である」も「F の標数が 2 である」ことも, 不要であることが, ごく最近 Dempwolff により示された.

定理 9 (Dempwolff, preprint, 2016) *f, g は $F=\mathbb{F}_{p^n}$ (p は奇素数でもよい) 上の単項関数とし, $f(x)=x^d$, $g(x)=x^e$ とおく.*

このとき, f と g が CCZ-同値 $\Leftrightarrow$ ある整数 $a\in[0, n-1]$ が存在して, 次のいずれかが $mod\ p^n-1$ で成立.

$$(A)\ \ e \equiv p^a d, \quad (B)\ \ de \equiv p^a.$$

論文 [4] においては, 2-primitive divisor の存在と共に, APN 関数という性質から, 幾つかの巡回群の作用の既約性が簡単に導かれ, それが議論の流れを非常にすっきりとさせている.

他方, Dempwolff の証明では, primitive divisor が存在する場合は私の論法をそのまま踏襲し, 既約な場合に帰着する議論を行う. この部分でも有限群の詳細な表現論を用いるが, 流

れとしてはすっきりとしている. しかし, primitive divisor が存在しない場合, $n=2$ で p がフェルマー素数の場合, を扱うにはかなり大変な議論を要するようである. 例えば, 4 次の線形群 $GL_4(q)$ のある種の部分群の分類を行う必要がある.

有限体上の関数の立場に立てば, $n=2$ という場合はほぼ無視できると思われる. 比較してみると, 私の扱った偶標数の有限体上の APN 関数の場合は, 議論の本質が明快に現れており, なおかつ, 線形代数と標準的な有限群論の結果のみで議論が完結するという, 非常に幸運な場合であったという印象を持つ.

References

[1] K. U. Schmidt and Y. Zhou, Planar functions over fields of characteristic two, Journal of Algebraic Combinatorics **40**(2), 503–526 (2014).

[2] S. Yoshiara, Notes on APN functions, semibiplanes and dimensional dual hyperovals, Designs, Codes and Cryptography **56**, 197–218 (2010).

[3] S. Yoshiara, Equivalences of quadratic APN functions, Journal of Algebraic Combinatorics **35**, 461–475 (2012).

[4] S. Yoshiara, Equivalences of power APN functions with power or quadratic APN functions, Journal of Algebraic Combinatorics **44**(3), 561–585 (2016).

[5] S. Yoshiara, Equivalences among plateaued APN functions, to appear in Designs, Codes and Cryptography. DOI:10.1007/s 10623-016-1298-0.

[6] S. Yoshiara, Plateauedness of Kasami APN functions, submitted for publication.