高次元の dual hyperoval に関連する距離正則グラフ
Distance regular graphs arising from dimensional dual hyperovals

谷口浩朗 *
Hiroaki Taniguchi
香川高等専門学校
National Institute of Technology, Kagawa College

1 はじめに

以下は 2018 年 12 月 12 日に RIMS 研究集会で発表させていただいた内容をまとめたものである。前半の 30 分は「高次元の dual hyperoval に関連する距離正則グラフ」という題で話をさせていただき，後半の 20 分は別の話「ある 2 次的な APN 関数の構成について」話をさせていただいた。前半の話は現在まだ進展中で preprint の状態であるが，後半の話の方は雑誌 Designs, Codes and Cryptography に掲載予定 [13] ですので後半に関して本稿で証明が省略されている箇所についてはそちらをご覧下さい。

2 高次元の dual hyperoval に関連する距離正則グラフ

2.1 Introduction

第 2 節の目的は，Pasini 氏と吉荒氏の 2001 年の次の結果を拡張することである。

定理 1 (Pasini-Yoshiara[14])
$Af(\mathcal{S}_{B_{\sigma\tau}})$ のインシデンスグラフが距離正則である必要十分条件は $\sigma\tau$ がガロア群 $Gal(K/GF(2))$ の生成元であることである。

ここで，$\mathcal{S}_{B_{\sigma\tau}}$ は吉荒氏の (Yoshiara's) dual hyperoval (以降，高次元の dual hyperoval を DHO と表す) といわれる DHO であり，$Af(\mathcal{S}_{B_{\sigma\tau}})$ はそのアファイン拡大といわれるものである。以降 $K = GF(2^n)$ を $n \geq 4$ である有限体とし，$K^* = K\backslash\{0\}$ と表す。一般に，ある性質を満たす $GF(2)$-bilinear mapping $B : K \times K \to K$ から $t \in K$ によってパラメトライズされた n 次元のベクトル空間を $X(t) := \{(x, B(x,t)) \mid x \in K\}$ で定めるとき，$\mathcal{S}_B := \{X(t) \mid t \in K\}$ は $GF(2)$ 上の $2n$ 次元ベクトル空間 $K \times K$ 内における n 次元の DHO となっている。Yosiara's DHO も $GF(2)$-bilinear mapping $B_{\sigma\tau}(x,t) = x^\sigma t + xt^\tau$ で定義された DHO である。(σ, τ は $Gal(K/GF(2))$ の生成元とする。)

さて，$GF(2)$ 上の $2n$ 次元ベクトル空間 $K \times K$ 内における適当な内積に関し，n 次元のベクトル空間 $X(t)$ の直交補空間を $X(t)^\perp$ で表し，$\mathcal{S}_B^\perp := \{X(t)^\perp \mid t \in K\}$ と定めると，これは一般には DHO になって

*taniguchi@t.kagawa-nct.ac.jp

いない。$\mathcal{S}_B$ と $\mathcal{S}_B^{\perp}$ が共に DHO になるとき，もとの DHO $\mathcal{S}_B$ は DDHO(Doubly dual hyperoval) とよばれている [8]。Bilinear mapping $B^o : K \times K \to K$ をもとの B から $B^o(x,y) := B(y,x)$ で定め，$\mathcal{S}_B^o := \mathcal{S}_{B^o}$ と定義する。このとき，もし $\mathcal{S}_B$ が DDHO であれば，$\mathcal{S}_B^{\perp}$, $\mathcal{S}_B^o$, $\mathcal{S}_B^{\perp o}$, $\mathcal{S}_B^{o\perp}$, $\mathcal{S}_B^{o\perp o}$ もそれぞれ DDHO であることがわかっている。非常に多くの興味深い性質を持つ DDHO が Dempwolff によって構成されている [8]。また APN 関数から構成される DHO が DDHO である必要十分条件について，および Yoshiara's DHO が DDHO である必要十分条件は $\sigma\tau$ がガロア群 $Gal(K/GF(2))$ の生成元であること，については谷口 [12] をご覧下さい。数理研における講演では定理 1 の拡張である以下の定理を証明することが目的であった。

定理 2
$\mathcal{S}_B$ が DDHO であれば，$Af(\mathcal{S}_B)$ のインシデンスグラフは距離正則である。

DDHO でない例においては，調べている限りインシデンスグラフは距離正則になっていない。それで「距離正則である必要十分条件が DDHO であること」と予想しているが，残念ながらまだ定理 2 の逆の証明は出来ていない。ここでアフィン拡大 $Af(\mathcal{S}_B)$ の定義を（遅ればせながら）述べておく。DHO $\mathcal{S}_B$ のアフィン拡大 $Af(\mathcal{S}_B) := \{\mathcal{P}, \mathcal{B}, *\}$ とは，点の集合 $\mathcal{P} = \{(1,x,y) \mid x,y \in K\}$ とブロックの集合 $\mathcal{B} = \{(0,t,z) \mid t,z \in K\}$ にインシデンス関係 $(1,x,y) * (0,t,z)$ を $y + z = B(x,t)$ が成り立つこと，として定義したものである。DHO との関係がわかりやすい別の幾何学的な定義も存在するが，インシデンス関係が調べやすいこともあり本稿ではこの定義を採用する。

2.2 A condition for DDHO

$\mathcal{S}_B$ を DHO とし，その $GF(2)$-bilinear mapping B を用いて，$x \in K^*$ に対して H_x を $H_x := \{B(x,t) \mid t \in K\} \subset K$ として定めると，B が DHO を定義するという性質から H_x は 2 元体上の n 次元ベクトル空間 $K = GF(2^n)$ における $n-1$ 次元部分空間 (hyperplane) になっていることがわかる。このとき，次のことが証明できる。

命題 3
以下が同値である。*(1) $\mathcal{S}_B$ が DDHO。*
(2) $\psi : K^* \ni x \mapsto H_x$ が 1 対 1 写像。
(3) $\{H_x \mid x \in K^*\}$ が $K = GF(2^n)$ 内の $(n-1)$ 次元部分空間全体の集合と一致する。

数理研での講演ではこの証明に十分時間が割けなかったこともあり，以下にもう少し正確な証明を述べることにする。上記 H_x と同様に，$H'_t := \{B(x,t) \mid x \in K\} \subset K$ と定義する。また $t \in K^*$ に対し $\beta_t \in K^*$ を $H'_t := \{t \in K \mid Tr(\beta_t t) = 0\}$ として定める。これは β_t を「すべての $x \in K$ に対し $Tr(\beta_t B(x,t)) = 0$ が成り立つただ一つの K^* の元」として定めるのと同じことである。次に写像 ϕ を $\phi : K^* \ni t \mapsto \beta_t \in K^*$ として定める。このとき以下が成り立つ。なお内積は $(x,t) \cdot (x',t') = Tr(xx' + tt')$ を使用している。

命題 4
$\mathcal{S}_B^{\perp}$ が DHO であることと ϕ が 1 対 1 であることは同値である。.

証明　$X(0)^{\perp} = \{(0,\beta) \mid \beta \in K\}$ であるので，$X(0)^{\perp} \cap X(t)^{\perp} = \{(0,\beta) \mid Tr(\beta B(x,t)) = 0 \ \forall x \in K\} = \langle (0,\beta_t) \rangle$ となる。よってもし ϕ が 1 対 1 でないなら，$\mathcal{S}_B^{\perp}$ は intersection に関する DHO の定義を満たさない。(2 つの異なる n 次元部分空間 $X(t_1)^{\perp}, X(t_2)^{\perp}$(ただし $t_1, t_2 \in K^*, t_1 \neq t_2$) が $X(0)^{\perp}$ と同一の 1 次元部分空間で交わってしまう。) 次に ϕ が 1 対 1 と仮定する。$s \neq t$ とすると，$X(s)^{\perp} \cap X(t)^{\perp} = \{(\alpha,\beta) \mid Tr(\alpha x + \beta B(x,t)) = 0, Tr(\alpha x + \beta B(x,s)) = 0 \ \forall x \in K\}$ であるので，2 つの式を加えると $Tr(\beta B(x, s+t)) = 0 \ \forall x \in K$ となり，$\beta = \beta_{s+t}$ がわかる。$s \neq 0, t \neq 0$ のときは $K \ni x \mapsto Tr(\beta_{s+t} B(x,t))$

は non trivial な線形写像で kernel は K の $(n-1)$ 次元部分空間 (hyperplane) であるので，$\alpha \in K^*$ で $Tr(\alpha x) = Tr(\beta_{s+t}B(x,t))(\forall x \in K)$ を満たすものがただ一つ定まる。このとき $X(s)^\perp \cap X(t)^\perp = \langle(\alpha, \beta_{s+t})\rangle$ となっている。s,t のどちらかが 0 のときは先に見たとおりである。(2 つの n 次元空間は 1 次元部分空間で交わる。) 次に s, t_1, t_2 を互いに異なる K の元とする。このとき，ϕ は 1 対 1 という仮定により，$X(s)^\perp \cap X(t_1)^\perp = \langle(*, \beta_{s+t_1})\rangle \neq \langle(*, \beta_{s+t_2})\rangle = X(s)^\perp \cap X(t_2)^\perp$ となる。(3 つの異なる n 次元部分空間の交わりは 0 ベクトル空間となる。) $|\mathcal{S}_B^\perp| = |\mathcal{S}_B| = 2^n$ は定義から明らかなので，$\mathcal{S}_B^\perp$ が DHO であるための条件を満たしていることがわかる。 ∎

系 5
以下が同値である。*(1)* $\mathcal{S}_B$ が *DDHO*。
(2) $\psi' : K^* \ni t \mapsto H'_t$ が *1* 対 *1* 写像。
(3) $\{H'_t \mid t \in K^*\}$ が $K = GF(2^n)$ 内の $(n-1)$ 次元部分空間全体の集合と一致する。

証明 $t \in K^*$ に対し $\beta_t \in K^*$ を $H'_t := \{t \in K \mid Tr(\beta_t t) = 0\}$ として定めたことより，$\phi : K^* \ni t \mapsto \beta_t \in K^*$ が 1 対 1 であることと，$\psi' : K^* \ni t \mapsto H'_t$ が 1 対 1 であることは同値である。また $|K^*|$ は K の $(n-1)$ 次元部分空間 (hyperplane) 全体の個数と同じなので，「ψ' が 1 対 1 である」ことと「$\{H'_t \mid t \in k^*\}$ が K の $(n-1)$ 次元部分空間 (hyperplane) 全体である」ことは同値である。 ∎

さて 2.1 節の $\mathcal{S}_B^o$ (これは $\mathcal{S}_B$ が DHO ならば常に DHO である) は，$\mathcal{S}_B^o = \{X(x) \mid x \in K\}$ ここに $X(x) := \{(t, B^o(t,x)) \mid t \in K\} = \{(t, B(x,t)) \mid t \in K\}$ と定義されているので，上と同様にして以下のことがわかる。

系 6
以下が同値である。*(1)* $\mathcal{S}_B^o$ が *DDHO*。
(2) $\psi : K^* \ni x \mapsto H_x$ が *1* 対 *1* 写像。
(3) $\{H_x \mid x \in K^*\}$ が $K = GF(2^n)$ 内の $(n-1)$ 次元部分空間全体の集合と一致する。

ところで Y. Edel [9] Section 5 により，「$\mathcal{S}_B$ が DDHO である」ことと「$\mathcal{S}_B^o$ が DDHO である」ことは同値であることがわかっている。このことにより命題 3 が成立することがわかる。

2.3 Automorphisms of $Af(\mathcal{S}_B)$

$Af(\mathcal{S}_B) = \{\mathcal{P}, \mathcal{B}, *\}$ は以下の同型写像を持つことが $(1,x,y) * (0,t,z) \Longleftrightarrow y + z = B(x,t)$ よりすぐに確かめられます。$a, b, c \in K$ とします。

1. $\tau_a : \begin{cases} (1,x,y) \mapsto (1,x,y+B(x,a)) \in \mathcal{P} \\ (0,t,z) \mapsto (0,t+a,z) \in \mathcal{B} \end{cases}$.

2. $\tau'_b : \begin{cases} (1,x,y) \mapsto (1,x+b,y) \in \mathcal{P} \\ (0,t,z) \mapsto (0,t,z+B(b,t)) \in \mathcal{B} \end{cases}$.

3. $t_c : \begin{cases} (1,x,y) \mapsto (1,x,y+c) \in \mathcal{P} \\ (0,t,z) \mapsto (0,t,z+c) \in \mathcal{B} \end{cases}$.

2.4 On incidence graph of $Af(\mathcal{S}_B)$

前節によって $(1,x,y) \in \mathcal{P}$ は適当な自己同形写像により $(1,0,0)$ に移されることがわかる。$Af(\mathcal{S}_B) = \{\mathcal{P}, \mathcal{B}, *\}$ において，点 $(1,0,0)$ から距離 i の元全体の集合を Γ_i と表すことにする。 また $x \in K^*$ に対し $\kappa(x) \in K^*$ を $B(x,\kappa(x)) = 0$ を満たす元として定める。（DHO の性質よりただ一つ定まる。）集合 Γ_i および Γ_i のサイズ $|\Gamma_i|$ について以下のことがわかる。

- $|\Gamma_1| = q$。 $\Gamma_1 = \{(0,t,0) \mid t \in K\}$。
- $|\Gamma_2| = q(q-1)/2$。$\Gamma_2 = \{(1,x,B(x,t)) \mid x \in K^*, t \in K\}$。
- $|\Gamma_3| = q(q-1)$。$\Gamma_3 = \{(0,s,B(x,s+t)) \mid B(x,s+t) \neq 0\} = \{(0,s,p) \mid s,p \in K, p \neq 0\}$。
- $|\Gamma_4| = (q+2)(q-1)/2$。$\Gamma_4 = \{(1,y,B(y,s)+B(x,s+t)) \mid B(x,s+t) \neq 0\} = \{(1,y,A) \mid y,A \in K, B(y,t) \neq A\ \forall t \in K\}$。

ここで $|\Gamma_1| + |\Gamma_3| = q + q(q-1) = q^2 = |K \times K|$ および $|\{(1,0,0)\}| + |\Gamma_2| + |\Gamma_4| = 1 + q(q-1)/2 + (q+2)(q-1)/2 = q^2 = |K \times K|$ ということから $\{(1,0,0)\} \cup \Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \cup \Gamma_4 = \mathcal{P} \cup \mathcal{B}$ であり，インシデンスグラフの直径は 4 であることがわかる。

$j = 1,2,3,4$ とし $\Gamma_0 = \{(1,0,0)\}$, $\Gamma_5 = \emptyset$ と見なす。$b_j \in \Gamma_j$ に対して $\Gamma_{j-1}(b_j)$ を b_j とインシデントな Γ_{j-1} の元全体のなす集合，$\Gamma_{j+1}(b_j)$ を b_j とインシデントな Γ_{j+1} の元全体のなすの集合，と定める。$b_j \in \Gamma_j$ に対して常に $|\Gamma_{j-1}(b_j) \cup \Gamma_{j+1}(b_j)| = q$ であることに注意する。以下のことがわかる。

- $|\Gamma_2(b_1)| = q-1$。ここに $b_1 = (0,t,0) \in \Gamma_1$。$\Gamma_2((0,t,0)) = \{(1,x,B(x,t)) \mid x \in K^*\}$。
- $|\Gamma_1(b_2)| = 2$。ここに $b_2 = (1,x,B(x,t)) \in \Gamma_2$。$\Gamma_1((1,x,B(x,t)) = \{(0,t',0) \mid B(x,t) = B(x,t')\} = \{(0,t,0),(0,t+\kappa(x),0)\}$。
- $|\Gamma_3(b_2)| = q-2$。ここに $b_2 = (1,x,B(x,t)) \in \Gamma_2$。$\Gamma_3((1,x,B(x,t))) = \{(0,s,B(x,s+t)) \mid s \in K, B(x,s+t) \neq 0\}$。
- $|\Gamma_3(b_4)| = q$。ここに $b_4 = (1,y,A) \in \Gamma_4$。$\Gamma_3((1,y,A)) = \{(0,s,A+B(y,s)) \mid s \in K\}$。

以上は $b_1 \in \Gamma_1, b_2 \in \Gamma_2, b_4 \in \Gamma_4$ の取り方によらず，常に一定値であることがわかる。したがって $b_3 \in \Gamma_3$ に対して $\Gamma_2(b_3)$, および $\Gamma_4(b_3)$ を調べることが問題になるわけであるが，一般にこれらのサイズは b_3 の取り方によって変動することが知られている。そのため $\Gamma_2(b_3)$, および $\Gamma_4(b_3)$ のサイズが b_3 の選び方によらず一定になる条件を調べたい訳である。なお，$|\Gamma_2(b_3)| + |\Gamma_4(b_3)| = q$ であるので，$\Gamma_2(b_3)$ のサイズが一定ならば $\Gamma_4(b_3)$ のサイズも一定になることがわかる。

命題 7
$\mathcal{S}_B$ が *DDHO* であるならば，すべての $b_3 \in \Gamma_3$ に対して常に $|\Gamma_2(b_3)| = q/2 - 1$ である。

この命題の逆も成り立つと考えている。

系 8
$\mathcal{S}_B$ が *DDHO* であるならば，すべての $b_3 \in \Gamma_3$ に対して常に $|\Gamma_4(b_3)| = q/2 + 1$ である。

以下の補題 9, 補題 10，補題 11 を用いて命題 7 の証明を行う。$b_3 \in \Gamma_3$ は適当な $s,p \in K, p \neq 0$ を用いて，常に $b_3 = (0,s,p)$ と表せることに注意する。

補題 9
$b_3 = (0, s, p)$ に対して，$|\Gamma_2(b_3)| = |\{x \in K^* \mid H_x \ni p\}|$ が成り立つ。

証明 2.2 節において $x \in K^*$ に対して hyperplane H_x を $H_x = \{B(x,t) \mid t \in K\}$ と定義した。任意の固定された $s \in K$ に対して $H_x = \{B(x, s+t) \mid t \in K\}$ としてもよいことに注意する。さて $b_3 = (0, s, p) \in \Gamma_3$ を任意に選び一つ固定しておく。このとき $(1, x, B(x,t)) \in \Gamma_2$ がこの b_3 とインシデントである条件を調べる。$(1, x, B(x,t))$ が b_3 とインシデントであると仮定すると，$B(x,t) + p = B(x,s)$ であるので $B(x, s+t) = p$ となるから $H_x \ni p$ でなければならない。逆に $H_x \ni p$ となる任意の $x \in K^*$ に対して，($H_x \ni p$ より適当な t が存在して $p = B(x, s+t)$ と表されているので) $A = p + B(x,s) (= B(x,t))$ と定めることにより固定された $b_3 = (0, s, p)$ とインシデントな元 $(1, x, A) \in \Gamma_2$ がただ一つ定まる。 ∎

補題 10
$|\Gamma_2(b_3)|$ が任意の $b_3 = (0, s, p)$ に対して一定である必要十分条件は，$|\{x \in K^* \mid H_x \ni p\}| = q/2 - 1$ がすべての $p \in K^*$ に対して成り立つことである。

証明 補題 9 により，$|\Gamma_2(b_3)|$ が任意の $b_3 \in \Gamma_3$ に対して一定であるならば $|\Gamma_2(b_3)| = q/2 - 1$ であることを示せば十分である。Γ_2 と Γ_3 を各点を結んだ辺の数を 2 重に数えると $|\Gamma_2| \cdot |\Gamma_3(b_2)| = |\Gamma_2(b_3)| \cdot |\Gamma_3|$ が成り立つので，$q(q-1)/2 \times (q-2) = |\Gamma_2(b_3)| \times q(q-1)$ ということから，$|\Gamma_2(b_3)|$ が一定値であるならば $|\Gamma_2(b_3)| = q/2 - 1$ であることがわかる。 ∎

補題 11
K を 2 元体上の n 次元ベクトル空間とみなす。K のすべての *hyperplane*($n-1$ 次元ベクトル空間) のうち，$p \in K^*$ をふくむ *hyperplane* の数は ($p \neq 0$ によらず) $q/2 - 1$ である。

証明 双対性により，hyperplane 上の 0 以外の点の個数 $2^{n-1} - 1 = q/2 - 1$ と同一である。 ∎

証明 [命題 7 の証明] $\mathcal{S}_B$ が DDHO であるならば，命題 3 より $\{H_x \mid x \in K^*\}$ は K のすべての hyperplane の集合と一致する。(さらに $\psi : x \mapsto H_x$ は 1 対 1 写像である。) 補題 11 より，このとき $|\{x \in K^* \mid H_x \ni p\}| = q/2 - 1$ が すべての $p \in K^*$ に対して成り立つ。補題 9 より，このときすべての $b_3 \in \Gamma_3$ に対して常に $|\Gamma_2(b_3)| = q/2 - 1$ である。 ∎

命題 7 と系 8 およびそれまでの結果により，$\mathcal{S}_B$ が DDHO のとき $Af(\mathcal{S}_B)$ のインシデンスグラフの直径は 4 であり intersection array は $\begin{Bmatrix} q & q-1 & q-2 & q/2+1 & * \\ * & 1 & 2 & q/2-1 & q \end{Bmatrix}$ となることがわかった。このようにして定理 2 が証明できることがわかった。

3 ある 2 次的な APN 関数の構成

2 元体 $\mathbb{F}_2$ 上のベクトル空間 $\mathbb{F}_2^n$ 上の関数 F が APN 関数であるとは, F がすべての $a \in \mathbb{F}_2^n \backslash \{0\}$ と $b \in \mathbb{F}_2^n$ に対して，解の個数 $|\{x \in \mathbb{F}_2^n \mid F(x+a) + F(x) = b\}| \leq 2$ を満たすことである。APN 関数は 1993 年に Nyberg によって差分攻撃に強い耐性をもつ暗号の設計のため導入された。F が 2 次的であるとは $F(x+y) + F(x) + F(y) + F(0)$ が $x, y \in \mathbb{F}_2^n$ について $\mathbb{F}_2$-bilinear であることである。$\mathbb{F}_2^n$ 上の 2 個の関数 F_1, F_2 について，直積 $\mathbb{F}_2^n \times \mathbb{F}_2^n$ の適当な $\mathbb{F}_2$-アフィン同型写像によってグラフ $\{(x, F_1(x)) \mid x \in \mathbb{F}_2^n\}$ がグラフ $\{(x, F_2(x)) \mid x \in \mathbb{F}_2^n\}$ に移されるとき，関数 F_1 と F_2 は CCZ 同値であるという。$\mathbb{F}_2^n$ 上の関数 F の Γ-rank とは，点 $(a,b) \in \mathcal{P} = \mathbb{F}_2^n \times \mathbb{F}_2^n$ とブロック $(u,v) \in \mathcal{B} = \mathbb{F}_2^n \times \mathbb{F}_2^n$ に隣接関係 $(a,b) \sim (u,v)$ を $F(a+u) = b + v$ と定義した 2 部グラフにおいて，そのインシデンス行列の $\mathbb{F}_2$ 上の階数である。

命題 12 (Edel-Pott[10])
F_1 と F_2 が CCZ 同値ならば Γ-$rank$ は等しい。

有限体 $\mathbb{F}_{2^n}$ の直積 $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ 上の以下の形の APN 関数について考える。

$$F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ni (x, y) \mapsto (xy, G(x, y)) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$$

の場合について考えたい。F が APN 関数になる条件は Carlet [7] の 4.2.1 の最初で与えられており, たとえば F が 2 次的な関数の場合，APN である条件は

1. $G(x, y)$ が x の関数として APN
2. $G(x, y)$ が y の関数として APN
3. $G(x, \alpha x)$ がすべての $\alpha \in \mathbb{F}_{2^n}^{\times}$ に対して APN

である。(Carlet 氏のこれらの条件については吉荒先生にお教えいただいた。)

3.1 Known Examples and their Γ-ranks on $\mathbb{F}_{2^8}$

現在までの所知られているこのような APN 関数の例は以下の 2 種類である。

定理 13 (Carlet[7])
$GCD(n, i-j) = 1$ で $s, t, u, v \in \mathbb{F}_{2^n}$, $s \neq 0, t \neq 0$ とし，$G(x, y) = sx^{2^i+2^j} + ux^{2^i}y^{2^j} + vx^{2^j}y^{2^i} + ty^{2^i+2^j}$ とする。このとき $F(x, y) := (xy, G(x, y))$ が APN 関数である必要十分要件は $G(x, 1) = sx^{2^i+2^j} + ux^{2^i} + vx^{2^j} + t = 0$ が $\mathbb{F}_{2^n}$ に解を持たないことである。

$G'(x, y) = x^{2^m+1} + ax^{2^m}y + bxy^{2^m} + cy^{2^m+1}$ で $G'(x, 1) = x^{2^m+1} + ax^{2^m} + bx + c = 0$ が $\mathbb{F}_{2^n}$ に解を持たないもの（ただし $GCD(n, m) = 1$ で $a, b, c \in \mathbb{F}_{2^n}$）としたとき，定理 1 の $F(x, y)$ は $F'(x, y) := (xy, G'(x, y))$ のどれかに線形同値であるのでこのような形の G' についてだけ調べればよい。$\mathbb{F}_{2^8}$ においては $m = 1$ および $m = 3$ それぞれの場合に $(a, b, c \neq 0$ とすると)1200 個ずつこのような $G'(x, y)$ が存在する。

定理 14 (Zhou-Pott[15])
$n \geq 2$, $GCD(n, m) = 1$ で $\alpha \in \mathbb{F}_{2^n}^{\times}$, $\sigma \in Aut(\mathbb{F}_{2^n})$，$G(x, y) = x^{2^m+1} + \alpha y^{(2^m+1)\sigma}$ とする。このとき $F(x, y) := (xy, G(x, y))$ が APN 関数である必要十分要件は $\alpha \notin \{a^{2^m+1}(t^{2^m} + t)^{1-\sigma} \mid a, t \in \mathbb{F}_{2^n}\}$ である。

系 15 (Zhou-pott[15])
$n \geq 2$ 偶数, $GCD(n, m) = 1$ で $\alpha \in \mathbb{F}_{2^n}^{\times}$ とし，$G(x, y) = x^{2^m+1} + \alpha y^{(2^m+1)2^i}$ とする。このとき α が $non-cubic$ で i が偶数ならば $F(x, y) := (xy, G(x, y))$ は APN 関数である。

定理 14 および系 15 の関数 $F(x, y)$ は $i = 0$ の場合（つまり $\sigma = id$ の場合）は, Calret 氏の定理 13 の中の関数に含まれる。

以下の補題は $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ において行列 $\begin{pmatrix} 1 & L \\ 0 & 1 \end{pmatrix}$ の作用を考えれば自明。

補題 16
$\mathbb{F}_{2^n}$ 上の関数 F と $\mathbb{F}_2$-線形写像 L に対し F, $F + L$ は CCZ 同値。

適当な $\lambda, \beta, \gamma \in \mathbb{F}_{2^n}$ に対し，y を $y + \lambda x$ と置き換え線形変換 $(x, y) \mapsto (x, \beta y^{2^{-j}})$ を作用させると，定理 13 の F は以下の系 17 の $F^{'}$ と線形写像 $L(x, y) = (\gamma x^2, 0)$ との和 $F^{'} + L$ に移されるので，次の系が成り立つことがわかる。

系 17
Carlet 氏の定理 *13* の関数 $F(x, y)$ は，$F^{'}(x, y) = (xy, G^{'}(x, y))$ の形の関数と *CCZ* 同値。ここに $G^{'}(x, y) = x^{2^m+1} + axy^{2^m} + by^{2^m+1}$, ただし $m = i - j$ で $G(x, 1) = x^{2^m+1} + ax + b$ は $\mathbb{F}_{2^n}$ に解を持たない，としている。

Carlet 氏の定理 13 の関数 $F(x, y)$ は系 17 の $F^{'}(x, y)$ と CCZ 同値なので，Γ-rank は G ではなく $G^{'}(x, y) = x^{2^m+1} + axy^{2^m} + by^{2^m+1}$ の形の関数の場合について計算すれば十分である。$\mathbb{F}_{2^8}$ 上で, Carlet 氏の関数 $F^{'}(x, y)$ の Γ-rank を Magma で計算するとすべて 13200 であり，Edel-Pott の論文 [10] の table 10 にある 2.1 の関数 $x^3 + x^{17} + u^{16}(x^{18} + x^{33}) + u^{15}x^{48}$ の Γ-rank と一致する。

Zhu-Pott 氏の系 15 の関数 $F(x, y)$ は $\mathbb{F}_{2^8}$ 上では $m = 1$ または $m = 3$, および $i = 0$ または $i = 2$，の可能性しかないが，Zhu-Pott[15] によると，$\mathbb{F}_{2^8}$ 上で $i = 0$ の場合（Carlet 氏の族に属する場合）は Γ-rank は 13200 であり，$i = 2$ の場合は 13642 になる。これらは私のコンピュータでも確認済みである。つまり $\mathbb{F}_{2^8}$ 上では，Carlet 氏の定理 13 の関数と，$m = 1$ または $m = 3$ で $i = 2$ の場合の Zhu-Pott 氏の系 15 の関数は CCZ 非同値である。

3.2 ほんの少しの変形

今回，以下の例を発見したので報告したい。

定理 18
$GCD(n, m) = 1$ で $a, b \in \mathbb{F}_{2^n}$, $b \neq 0$ とし，

$$G(x, y) = x^{2^{2m}+2^{3m}} + ax^{2^{2m}}y^{2^m} + by^{2^m+1}$$

とする。このとき $F(x, y) := (xy, G(x, y))$ が *APN* 関数である必要十分要件は $P(x) := x^{2^m+1} + ax + b = 0$ が $\mathbb{F}_{2^n}$ に解を持たないことである。

上記 $P(x)$ は Projective polynomial と呼ばれ詳しく研究されている。この定理 18 は以下のようにも言い換えられる。（吉荒先生による。）

定理 19 (定理 18 の言い換え)
$GCD(n, m) = 1$ で $a, b \in \mathbb{F}_{2^n}^{\times}$ とし，$G(x, y) = x^{2^m+1} + axy^{2^m} + by^{2^m+1}$*(Carlet* 氏の定理 *1* の形の関数*)* とする。このとき

$$F(x, y) := (x^{2^{-2m}}y, G(x, y)), \text{ または } F(x, y) := (xy^{2^{2m}}, G(x, y))$$

が *APN* 関数である必要十分要件は $G(x, 1) = x^{2^m+1} + ax + b = 0$ が $\mathbb{F}_{2^n}$ に解を持たないことである。

つまり，定理 19 は Carlet 氏の定理 13 において bent 関数を $B(x, y) = xy$ の代わりに $B(x, y) = x^{\tau}y$ と置き換えた形をしている。($x^{\tau} := x^{2^{-2m}}$ とする.)

証明 [定理 18 の証明.] Carlet 氏の条件 1,2,3 を確かめればよい。条件 1,2 は自明である。条件 3 については $G(x, \alpha x) = x^{2^{2m}+2^{3m}} + a\alpha^{2^m}x^{2^{2m}+2^m} + b\alpha^{2^m+1}x^{2^m+1}$ であるので $z := g(x) = x^{2^m+1}$(Gold 関数) とおくと，$G(x, \alpha x)$ は Gold 関数 g と線形関数 $L_\alpha(z) = z^{2^{2m}} + a\alpha^{2^m}z^{2^m} + b\alpha^{2^m+1}z$ の合成になっている。そこで $G(x, \alpha x)$ が APN である必要十分要件は線形写像 L_α が全単射，つまり $L_\alpha(z) = 0$ が $z = 0$ 以外の解を持たないことで

ある。ここで条件 $b \neq 0$ を使うと，このことは $L_\alpha(z)/z = z^{2^{2m}-1} + a\alpha^{2^m} z^{2^m-1} + b\alpha^{2^m+1} = 0$ が $\mathbb{F}_{2^n}$ に解を持たないことと同値。$z^{2^m-1} = s$ と置き換えると，このことは $L_\alpha(z)/(\alpha^{2^m+1}z) = (s/\alpha)^{2^m+1} + a(s/\alpha) + b = 0$ が $\mathbb{F}_{2^n}$ に解を持たないことと同値である。さらに $t := s/\alpha$ とおき変えると，APN 関数である必要十分条件は $P(t) := L_\alpha(z)/(\alpha^{2^m+1}z) = t^{2^m+1} + at + b = 0$ が $\mathbb{F}_{2^n}$ に解を持たないことであることがわかる。 ∎

定理 3 の APN 関数の $\mathbb{F}_{2^s}$ 上の Γ-rank は $GCM(n,m) = 1$ で $P(x) := x^{2^m+1} + ax + b = 0$ (ただし $a, b \neq 0$) が $\mathbb{F}_{2^n}$ に解を持たない条件の下で計算を終了した。その結果は $m = 1$ および $m = 3$ どちらにもかかわらず, また $a \neq 0$ の値にかかわらず，$b^5 = 1$ のとき Γ-rank は 13700 であり，$b^5 \neq 1$ のとき Γ-rank は 13798 であった。（なお $a = 0$ のときは Zhu-Pott の結果に含まれる。）$\mathbb{F}_{2^s}$ においては 3 個（以上）の CCZ 同値類を持っている。なお Γ-rank の値 (13700, 13798) を持った APN 関数は Edel-Pott[10] の $\mathbb{F}_{2^s}$ 上の APN 関数表 (Table 9, 10) に掲載されておらず Budaghyan 等 [6] の $\mathbb{F}_{2^s}$ 上の APN 関数表 (Table 3) にも掲載されていない。

Examples	Γ-rank in $\mathbb{F}_{2^s}$
定理 1 (Carlet), 系 1 (Zhou-Pott, $i = 0$)	13200
系 1 (Zhou-Pott, $i = 2$)	13642
定理 3 ($a = 0$)	13642
定理 3 ($a \neq 0$ and $b^5 = 1$)	13700
定理 3 ($a \neq 0$ and $b^5 \neq 1$)	13798

3.3 関連する $\mathbb{F}_{p^n}$ 上の（非可換な）presemifields

以下 p を素数 (2 でもよい) とし $F := \mathbb{F}_{p^n}$ とする。K を F の部分体で $\sharp K \geq 3$ とし $\langle\sigma\rangle = Gal(F/K)$ とする。また $\alpha \in F\backslash\{0\}$ をノルムが $N_K^F(-\alpha) \neq 1$ を満たすとする。さらに $x \circ_\alpha y := x^\sigma y + \alpha x y^\sigma$ と定める (Albert's twisted field)。

定理 20
$P(x) := x^{\sigma+1} + ax + b = 0$ は F に解を持たないとする。$(x,s),(y,t) \in F \times F$ に積 $*$ を以下の様に定義すると，$(F \times F, +, *)$ に *Presemifiled* の構造を入れることが出来る。

$$(x,s) * (y,t) := ((x \circ_\alpha y)^{\sigma^2} - a(x^\sigma t - \alpha y^\sigma s)^\sigma - b(s \circ_\alpha t),\ xt + ys).$$

注意 : $a = 0$ で $\alpha = 1$ のときは Zhou-Pott による可換な半体の構成に含まれる [15]。このとき $N_K^F(-1) \neq 1$ より p と拡大次数 $[F : K]$ は奇数である。

証明 $(x,s)*(y,t)$ は (x,s) または (y,t) に関して加法的 (additive) である。$(x,s) \neq (0,0)$ かつ $(x,s)*(y,t) = (0,0)$ と仮定して $(y,t) = (0,0)$ を証明する。まず $x = 0$ または $s = 0$ の場合は自明。$x \neq 0$ かつ $s \neq 0$ と仮定して $(y,t) = (0,0)$ を証明する。$(y,t) \neq (0,0)$ と仮定して矛盾を導く。第 2 式から $y \neq 0$ かつ $t \neq 0$ でなければならない。すると第 2 式より $s/x = -t/y = \beta \in F^\times$ となる $\beta \neq 0$ が存在する。$s = \beta x$, $t = -\beta y$ を第 1 式に代入すると，$(x \circ_\alpha y)^{\sigma^2} + a\beta^\sigma (x \circ_\alpha y)^\sigma + b\beta^{\sigma+1}(x \circ_\alpha y) = 0$ となる。$x \circ_\alpha y = z$ とおくと，$z^{\sigma^2} + a\beta^\sigma z^\sigma + b\beta^{\sigma+1} z = 0$ となる。ここで仮定より $z \neq 0$ なので $z^{\sigma^2-1} + a\beta^\sigma z^{\sigma-1} + b\beta^{\sigma-1} = 0$ となる。次に $z^{\sigma-1} = X$ とおくと $X^{\sigma+1} + a\beta^\sigma X + b\beta^{\sigma+1} = 0$ となる。$z \neq 0$ ならば $X = z^\sigma/z$ より $X \neq 0$ となることに注意する。この両辺を $\beta^{\sigma+1}$ で割って，さらに $Y := X/\beta$ とおくことにより，$Y^{\sigma+1} + aY + b = 0$ となる。ところがこれは $P(x) := x^\sigma + ax + b$ とおくとき $P(x) = 0$ が F に解を持たない, という仮定に ($Y \neq 0$ という解があるので) 矛盾する。よって最初から $z := s \circ_\alpha t = 0$ でなければならなかった。$x \neq 0$ かつ $s \neq 0$ と仮定したので，$(y,t) = (0,0)$ でなければならない。 ∎

さて，半体 (semifield)S の不変量として「Right Nucleus」「Middle Nucleus」「Left Nucleus」が以下の表のように定義される。例えば $N_r = \{r \in S \mid (x \star y) \star r = x \star (y \star r) \forall x, y \in S\}$ と見てほしい。

Right Nucleus $r \in N_r$	Middle Nucleus $m \in N_m$	Left Nucleus $l \in N_l$
$(x \star y) \star r = x \star (y \star r)$	$(x \star m) \star y = x \star (m \star y)$	$(l \star x) \star y = l \star (x \star y)$

定理 20 の Presemifield から半体を構成できるが，その Nuclei が以下の様になることがわかった。

定理 21

定理 *20* の *Presemifield*$(F \times F, +, *)$ から，改めて積を $((x,s) * (1,0)) \star ((1,0) * (y,t)) := (x,s) * (y,t)$ と定義し直すことにより，半体 $(F \times F, +, \star)$ で $(1,0) * (1,0)$ を単位元とするものが定まる。体の拡大次数が $[F : K] \geq 3$ と仮定する。このとき半体 $(F \times F, +, *)$ の *Nuclei* は以下の様になる。

Right Nucleus N_r	*Middle Nucleus* N_m	*Left Nucleus* N_l
K	K *(if* $a \neq 0$*)*	K

さて，定理 20 から構成される半体は，Bierbrauer 達の Projection Construction による半体の構成にそっくりである，との指摘が複数のレフェリー達からあった。しかし，次の命題からわかるように，定理 20 から構成される半体とは Middle Nucleus が異なるので isotopic ではあり得ないことがわかる。

命題 22 (Presemifield $B(p, m, a, \alpha, b)$ [2][3][4])

Let $p = 2$ または p 奇素数とする。$F = \mathbb{F}_{p^n}$ を有限体, K を F の部分体，$\langle \sigma \rangle = Gal(F/K)$ $\sigma \neq id$ とする。さらに $\alpha \in F$ を $N_K^F(-\alpha) \neq 0, 1$ を満たすとする。また $P(x) := p_1 x^{\sigma+1} + p_2 x + p_3 x^{\sigma} + p_4$ $(p_1 \neq 0)$ が F に解を持たないとする。*Presemifield* の積を以下の様に定める。

$$(x,t) * (y,s) = (p_1(x \circ_\alpha y) - p_2(x^\sigma t - \alpha s y^\sigma) + p_3(s^\sigma y - \alpha x t^\sigma) - p_4(s \circ_\alpha t), \quad xt + ys).$$

このとき以下が成り立つ。

Right Nucleus N_r	*Middle Nucleus* N_m	*Left Nucleus* N_l
K	*Quadratic extension of* K	K

参　考　文　献

[1] A. A. Albert, On non associative division algebras, Trans. Amer. Math. Soc. 72 (1952) 292–309. Generalized twisted fields, Pacific Journal of Mathematics, 8 (1961) 1–8.

[2] D. Bartoli, J. Bierbrauer, G. Kyureghyan, M. Giulietti, S. Marcugini, F. Pambianco, A family of semifields in characteristic 2, Journal of Algabraic Combinatorics 45 (2017) 455–473.

[3] J. Bierbrauer, Projective polynomials, a projection construction and a family of semifields, Des. Codes Cryptogr. 79 (2016) 183–200.

[4] J. Bierbrauer, D. Bartoli, G. Faina, S. Marcugini, F. Pambianco, A family of semifields in odd characteristic, Des. Codes Cryptogr. 86 (2018) 611–621.

[5] A. Bluher, On $x^{q+1} + ax + b$, Finite Fields and their Applications, 10 (2004), 285–305.

[6] L. Budaghyan, T. Helleseth, et.al, Some Results on the Known Classes of Quadratic APN Functions, Lecture Notes on Computer Science, 10194 (2017), 3–16.

[7] C. Carlet, Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions Des.Codes Cryptogr. 59 (2011), 89–109.

[8] U. Dempwolff, Dimensional doubly dual hyperovals and bent functions, Innovations in Incidence Geometry, 13(2013), 149–178.

[9] Y. Edel, On some representations of quadratic APN functions and dimensional dual hyperovals, RIMS Kokyuroku, 1687(2010), 118–130.

[10] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, Adv. Math. Commun. 3 (2009) 59–81.

[11] T. Helleseth and A. Kholosha, On the equation $x^{2^l+1} + x + a = 0$ over $GF(2^k)$, Finite Fields and their Applications, 14 (2008), 159–176.

[12] H. Taniguchi, On the duals of certain d-dimensional dual hyperovals in $PG(2d + 1, 2)$. Finite Fields and Their Applications. 15 (2009), 673–681.

[13] H. Taniguchi, On some quadratic APN functions, to appear in Des. Codes Cryptogr.

[14] A. Pasini and S. Yohsiara, New Distance Regular Graphs Arising from Dimensional Dual Hyperovals, Europ. J. Combinatorics. 22 (2001), 547–560.

[15] Y. Zhou and A. Pott, A new family of semifields with 2 parameters, Advances in Mathematics. 234 (2013), 43–60.