高次元の双対弧–過去 15 年間を振り返って

吉荒 聡
東京女子大学現代教養学部数理科学科

2012 年 8 月 20 日 (月) に京都大学数理解析研究所で行われた講演で使用した原稿 (beamer 形式で作成) をほぼそのまま article 形式に圧縮したものがこの記事の本文である. 最後に補足説明と DHO (DA すべてではない) に関連する筆者が知る論文をすべて集めた文献を付けた.

1 高次元の双対弧 (DA) と双対超卵形 (DHO) –定義と動機，実例

1.1 定義

DA, DHO の形式的定義から始める．筆者のサーベイ [36] も参照されたい.

Definition 1 U を $\mathbb{F}_q$ 上のベクトル空間とする. U の n-次元部分空間の集まり $\mathcal{A}$ が n-**DA** *(over* $\mathbb{F}_q$*)* であるとは次が満たされること*:*

1. $\dim(X \cap Y) = 1$ *for all* $X, Y \in \mathcal{A}$ *with* $X \neq Y$*,*
2. $X \cap Y \cap Z = \{0\}$ *for any pairwise distinct* $X, Y, Z \in \mathcal{A}$*.*

$\mathcal{A}$ の**生成空間** $\mathcal{A}(\mathcal{A})$ とは*,* そのメンバー全体が生成する U の部分空間のこと*:* $\mathcal{A}(\mathcal{A}) := \langle X \mid X \in \mathcal{A} \rangle$.

次の事実はすぐに示せる.

Lemma 2 n*-DA* $\mathcal{A}$ *over* $\mathbb{F}_q$ は高々$((q^n-1)/(q-1))+1$ 個の部分空間の集まり.

$((q^n-1)/(q-1))+1$ 個のメンバーから構成される n-DA over $\mathbb{F}_q$ のことを n-**双対超卵形** (**dimensional dual hyperoval**, 略して **DHO**) と呼ぶ.

DA の 被覆, 商; 同型，自己同型群; 部分 DA, 直和といった標準的な概念も定義できる. (後 2 者は [36] では触れられていない.)

Definition 3 $\mathcal{A}$*,* $\mathcal{B}$*:* n*-DAs over* $\mathbb{F}_q$ *with* $|\mathcal{A}| = |\mathcal{B}|$. $\mathbf{A} := \mathbf{A}(\mathcal{A})$*,* $\mathbf{B} := \mathbf{A}(\mathcal{B})$. $\mathbf{A}$ から $\mathbf{B}$ への $\mathbb{F}_q$*-semilinear surjective map* ρ が存在して
$X \in \mathcal{A}$ に対して $\rho(X) \in \mathcal{B}$ で*,* $X \neq Y \in \mathcal{A}$ のとき $\rho(X) \neq \rho(Y)$
のとき*,* $\mathcal{A}$ は $\mathcal{B}$ の**被覆** *(cover),* $\mathcal{B}$ は $\mathcal{A}$ の**商** *(quotient)* という.

$\dim(\mathbf{A}) = \dim(\mathbf{B})$ のとき，上のような写像 ρ が存在すれば $\mathcal{A}$ は $\mathcal{B}$ と**同型**といい*,* ρ を**同型写像**という. $\mathcal{A} = \mathcal{B}$ のとき $\mathcal{A}$ からそれ自身への同型写像の全体は群をなす．これを $\mathrm{Aut}(\mathcal{A})$ と書いて $\mathcal{A}$ の**自己同型群**という.

Definition 4 $\mathcal{B}$ は n'*-DA,* $\mathcal{A}$ は n*-DA over* $\mathbb{F}_q$ とする. ただし $2 \leq n' \leq n$.
このとき $\mathcal{B}$ が $\mathcal{A}$ の**部分 DA** であるとは，$B \in \mathcal{B}$ に対して $B \subset A$ を満たす $A \in \mathcal{A}$ が *(*唯一つ*)* 存在すること.

n*-DA* $\mathcal{A}$ が部分 *DA* $\mathcal{B}_j$ *(*$j = 1, \ldots, m$*)* の**直和**であるとは*,*
$\mathcal{A}(\mathcal{B}_j) := \{A \in \mathcal{A} \mid B \subset A \text{ for some } B \in \mathcal{B}_j\}$ とするとき $\mathcal{A}$ が $\mathcal{A}(\mathcal{B}_j)$ *(*$j = 1, \ldots, m$*)* の直和であること.

1.2 動機

このような概念を立てた動機は, 主に**有限単純群を記述する幾何**に発する．この幾何の**重要な組み立て材料**のひとつとしての **circle 幾何の表現**が DA であり，1-DA は既に古典的な概念である．またアフィン拡大を考えると階数 3 の幾何が作れる．これらについてざっと説明する．

有限単純群を説明する幾何（建物と散在幾何) は

(射影平面を含む) 一般化された多角形,
circle 幾何，Petersen 幾何, tilde 幾何

という限られたクラスの単純な公理系を満たす階数 2 の幾何構造を組み立てて得られる．Lie 型の群に対する幾何「**建物**」(射影空間はその一例) 一般化された多角形を組み立てて得られる．散在型の単純群に対しては，これに更に上の階数 2 の幾何を組み合わせる．

さて散在型単純群をどの様に把握すべきか？と考えたとき, $\rightarrow$ すべてを統一的に考え得るのは，今のところ「幾何」のみである．従って, この幾何の組み立て材料に登場する一般化された多角形以外の幾何，特に **circle 幾何** はどの様な数学に登場するか？を追究することは重要であろう．

Circle 幾何とは単に v 点集合 V とその 2 点部分集合全体 $V^{(2)}$ を，(対称化した) 包含関係 $*$ により結合構造と見なしたもの: $C_v = (V, V^{(2)}; *)$. そのベクトル空間での表現の一つが**高次元の弧** (**dimensional dual arc**) なのである．

ある固定したベクトル空間 U を取り, V の各点 p に U の一定次元 n の部分空間 $X(p)$ を指定し, V^2 の各対 $\{p, q\}$ に一定次元 n' の部分空間 $X(\{p, q\})$ を指定し, $*$ が U における包含関係に対応するようにしたものが circle 幾何 C_v のベクトル表現である．

ここで $X(\{p, q\}) = X(p) \cap X(q)$ 及び $n' = 1$ として「異なる $V^{(2)}$ の対は異なる 1 次元部分空間に対応する」(intersection property を満たす）と要請すると, 自然に，DA の 2 番目の公理: 「任意の互いに相異なる点 p, q, r に対して $X(p) \cap X(q) \cap X(r) = \{0\}$」が得られる．この表現が n-DA に他ならない．

$n = 1$ のとき, 1-DA $\mathcal{A}$ ($|\mathcal{A}| \geq 3$) の生成空間は 3 次元で, 1-DA, 1-DHO の概念は，**射影平面上の弧，超卵形**の双対という古典的対象に他ならない．ここには豊かな成果と応用がある: 例えば,

1. (Segre) 1-DA $\mathcal{A}$, $|\mathcal{A}| = q + 1$ は非退化二次曲線上の射影点に対応.
2. 1-DHO $\mathcal{A}$ ($|\mathcal{A}| = q + 2$) が存在するならば q は 2 のべき.
3. 1-DHO は oval polynomial で記述される.

また n-DA $\mathcal{A}$ over $\mathbb{F}_q$ からその**アフィン拡大** $\mathrm{Af}(\mathcal{A})$ という階数 3 のインシデンス幾何が得られる．$\mathcal{A}$ が DHO で $q = 2$ のときには，これは **semibiplane** (射影平面の類似: 2 点を通る線が 0 or 2 本， 2 線上にある点は 0 or 2 個, etc.) となる．このとき，自己同型群 $\mathrm{Aut}(\mathcal{A})$ が $\mathcal{A}$ のメンバー上に二重可移 $\Leftrightarrow$ $\mathrm{Af}(\mathcal{A})$ が flag-transitive.

基本的な未解決問題

1. n-DHO over $\mathbb{F}_q$ が存在するならば q は 2 のべきか?
   n が偶数または $n = 3$ ならば，これは成立する [4].

2. n-DHO over $\mathbb{F}_q$ の ambient space $\mathcal{A}$ の次元は
   $2n \leq \dim(\mathcal{A}) \leq n(n+1)/2$ を満たすか？ $q \neq 2$ であればこれは正しい [34].
   $q = 2$ のとき $\dim(\mathcal{A}) - 2 \leq n(n+1)/2$ は示せる.

1.3 実例

1.3.1 単連結な DHO の例

n-DA が**単連結**とは，真に大きい生成空間を持つ n-DA で被覆されないこと．

生成空間の次元が最大 $n(n+1)/2$ (従って単連結) であるような n-DHO の無限系列は 4 つ知られている．

> **Huybrecht DHO** $\mathcal{H}(d,\mathbb{F}_2)$ ([11] で登場している) と
> その微少変形である **Buratti-Del Fra DHO** $\mathcal{D}(d,\mathbb{F}_2)$
> ([1] で登場して以来 [5] [29] などで研究されている),
> **Veronesean DHO** $\mathcal{V}(n,\mathbb{F}_{2^e})$
> ([31] [32] で本質的には DHO として記述されている) と
> その微少変形である **Taniguchi DHO** $\mathcal{T}(n,\mathbb{F}_2)$ ([24] で登場).

その他に無限系列に属さない散在的な例として，**Mathieu DHO** ($q=4$, $n=3$) が知られている．この名称は, 自己同型群が $3.M_{22}.2$ であることから来ている．(本質的には [13] で発見され, DHO として [12], [14] で研究されている.)

生成空間の次元が $n(n+1)/2$ より小さい単連結 n-DHO の例も色々知られている．[33],[16],[27].

1.3.2 4 つの無限系列の統一的モデル

V を $\mathbb{F}_2$ 上の n 次元ベクトル空間, $(e_i)_{i=0}^d$ を V の基底 ($d := n-1$) とする．

$x=\sum_{i=0}^d x_ie_i \in V$, $y=\sum_{i=0}^d y_ie_i \in V$ に対して

$$x\cap y := \sum_{i=0}^d x_iy_ie_i,\ \ x\setminus y := x+(x\cap y),\ \overline{x} := x+(x\cap e_0)$$

とおく. 対称テンソル積

$$S^2(V) := (V\otimes V)/A^2(V),\ A^2(V) := \langle x\otimes y+y\otimes x \mid x,y\in V\rangle$$

を考え，その元 $(x\otimes y)+A^2(V)\in S^2(V)$ を簡単のため $x\otimes y$ と記す．また $x\wedge y := (x\otimes y)+(x\cap y)\otimes(x\cap y)$ とおく．

$s,x\in V$ に対して, 次の 4 つの $S^2(V)$ のベクトルを考える．

1. $v(s,x) := s\otimes x$,
2. $h(s,x) := (x\otimes x)+(s\wedge x) = s\otimes x+(x\setminus s)\otimes(x\setminus s)$,
3. $d(s,x) := h(s,x)+(\overline{s}\cap\overline{x})\otimes e_0$,
4. $t(s,x) := h(s,x)+(x\setminus s)\otimes e_0$.

$V(s) := \{v(s,x)\mid x\in V\}$, 同様に $H(s)$, $D(s)$, $T(s)$ を定める．但し $T(e_0) := \{x\otimes e_0\mid x\in V\}$ とする．また $V(\infty)=T(\infty) := \{x\otimes x\mid x\in V\}$ とおく．

Proposition 5 (Taniguchi-Yoshiara 2012 [30]) 以上の記号のもとで, 次の同型が得られる．

1. $\mathcal{V}(n,\mathbb{F}_2)\cong\{V(s)\mid s\in(V\setminus\{0\})\cup\{\infty\}\}$,
2. $\mathcal{H}(n,\mathbb{F}_2)\cong\{H(s)\mid s\in V\}$,
3. $\mathcal{D}(n,\mathbb{F}_2)\cong\{D(s)\mid x\in V\}$,
4. $\mathcal{T}(n,\mathbb{F}_2)\cong\{T(s)\mid s\in(V\setminus\{0\})\cup\{\infty\}\}$.

1.3.3 幾つかの事実 [44]

1. $\mathcal{V}(n, \mathbb{F}_{2^e})$ 中には $\mathcal{V}(n-1, \mathbb{F}_{2^e})$ が部分 DHO として存在するが, $\mathcal{V}(n, \mathbb{F}_{2^e})$ は二つの $\mathcal{V}(n-1, \mathbb{F}_2)$ と同型な部分 DHO の直和には書けない.
2. $\mathcal{H}(n, \mathbb{F}_2)$ は $\mathcal{H}(n-1, \mathbb{F}_2)$ と同型な二つの部分 DHO の直和である.
3. $\mathcal{D}(n, \mathbb{F}_2)$ は $\mathcal{D}(n-1, \mathbb{F}_2)$ と同型な二つの部分 DHO の直和である.
4. $\mathcal{H}(n, \mathbb{F}_2)$ と $\mathcal{D}(n, \mathbb{F}_2)$ のアフィン拡大は同一の semibiplane により被覆される.

2 研究の流れ

2.1 主な動向

1. 1996 頃: Pasini, Huybrechts, Yoshiara が共同研究の一環として興味を持つ. Yoshiara は Mathieu DHO 及び Extended generalized quadrangle として得られる DA への関心から.
2. 1999: Pasini-Huybrechts が二重可移な DHO over $\mathbb{F}_q$ $(q > 2)$ として Mathieu DHO を特徴付け [12].
3. 1999: $2n$ 次元の生成空間を持つ n-DHO over $\mathbb{F}_2$ の無限族 $\mathcal{S}_{h,m}$ の構成. 自己同型群を決定, 同型問題を解決 (Yoshiara) [33].
4. 2000: Del Fra による 2-DHO over $\mathbb{F}_q$, $q = 2, 4$ の分類 [4].
5. 2001: Pasini-Yoshiara による $\mathrm{Af}(\mathcal{S}_{h,m})$ の普遍被覆の研究 [16, 17].
6. 2003: Buratti-Del Fra による DHO $\mathcal{D}(n, \mathbb{F}_2)$ の構成 [1].
7. 2004: Ambient space の次元に関する制限 (Yoshiara) [34].
8. 2006: Yoshiara による survey ('Dimensional dual arcs') の公刊 [36].
9. 2006: Edel-Kyureghyan-Pott による単項式と CCZ-同値でない APN 関数の発見.
10. 2007,2008: Quadratic APN 関数 f に対する DHO $\mathcal{S}[f]$ の構成. (Göloğlu-Pott, Yoshiara) [10, 38]
11. 2008: Yoshiara による二重可移な DHO over $\mathbb{F}_q$ $(q = 2)$ の分類 (translation group の重要性) [39, 40].
12. 2008: Edel による $\mathcal{S}[f]$ の特徴付け [8].
13. 2009: Taniguchi による DHO $\mathcal{T}(n, \mathbb{F}_2)$ の構成 [24].
14. 2010: Taniguchi-Yoshiara による $\mathcal{V}(n, \mathbb{F}_2)$, $\mathcal{H}(n, \mathbb{F}_2)$, $\mathcal{D}(n, \mathbb{F}_2)$ の商 DHO の研究 (addition formula を用いる) 開始 [28, 29].
15. 2011: Edel 予想の解決 (Yoshiara) [43].
16. 2011: Edel-Dempwolff による bilinear DHO の研究 [9].
17. 2012: Dempwolff-Kantor による doubly DHO の研究 [9, 7].

2.2 ここ数年ではっきりしてきたこと

DHO は (Bent, AB, APN 等) 非線形関数に対する “幾何”であり，その良い部分クラスを研究対象として取り出すことで

“代数”,“幾何”,“数論”(有限体上の)

をつなぐ架け橋となる理論体系を作り出すことが期待できる.

3 非線形関数の幾何としての DHO

3.1 非線形関数

APN, AB, Bent 関数など非線形関数に関しては, まず文献 [2] を参照のこと.

Definition 6 (非線形関数) 2^n 元体 $F = \mathbb{F}_{2^n}$ を素体 $\mathbb{F}_2$ 上の n 次元空間とみなす. 関数 $f : F \to F$ が

1. **almost perfect nonlinear***(APN)* とは, すべての $0 \neq a \in F$, $b \in F$ に対して $|\{x \in F \mid f(x+a) - f(x) = b\}| \leq 2$ であること.
2. **quadratic** であるとは, $B_f(x, y) := f(x+y) + f(x) + f(y) + f(0)$ により定義される $B_f : F \times F \to F$ が双線形であること.

APN 関数は平面関数の偶標数版. 暗号における応用上重要とされる. 2006 年の Edel-Kyureghyan-Pott による発見までは, すべて単項式と CCZ-同値になるものしか知られていなかった.

Definition 7 (二つの同値関係) $F \oplus F = \{(x, y) \mid x, y \in F\}$ を $\mathbb{F}_2$ 上の $2n$ 次元空間と見なす.
関数 $f, g : F \to F \cong \mathbb{F}_{2^n}$ に対して

1. f が g に **CCZ-同値** *(Carlet-Chirpin-Zinoviev, $f \sim g$)* とは,
   f の**グラフ** $G(f) := \{(x, f(x)) \mid x \in F\}$ *($\subseteq F \oplus F$)* を g のグラフ $G(g)$ に移すような $F \oplus F$ 上の全単射アフィン写像が存在すること.
2. f が g に **EA-同値** *(Extended affine, $f \sim' g$)* とは,
   $g(x)^\delta = f(x^\alpha + c) + x^\beta + d$ *($\forall x \in F$)* を満たす
   F 上の線形写像 α, β, δ *(α, δ は全単射)* 及び $c, d \in F$ が存在すること.

Proposition 8 (基本的事実)
1. 二つの関数が *EA*-同値ならば *CCZ*-同値.
2. f, g が *CCZ*-同値のとき，f が *APN* ならば g も *APN*.
3. f, g が *CCZ*-同値のとき，f が *quadratic* であっても g は *quadratic* とは限らない.
4. f, g が *EA*-同値のとき，f が *quadratic* ならば g も *quadratic*.
5. *EA*-同値性は群の軌道として記述できる. *(*従って *EA*-同値であるか否かは *CCZ*-同値であるかどうか調べるのに比べて, ずっと調べやすい.)

3.2 非線形関数の幾何

3.2.1 Quadratic APN 関数 f に付随する DHO $\mathcal{S}[f]$

f を $F = \mathbb{F}_{2^n}$ 上の quadratic APN 関数とし, $B_f(x,y) := f(x+y) + f(x) + f(y) + f(0)$ $(x, y \in F)$ とおく.
$t \in F$ に対して $F \oplus F$ の部分空間 $X(t)$ を次により定める.

$$X(t) := \{(x, B_f(x,t)) \mid x \in F\}.$$

Proposition 9 (Y 2008 [38])

1. $\mathcal{S}[f] := \{X(t) \mid t \in F\}$ は *n-DHO over* $\mathbb{F}_2$*, ambient space* は $F \oplus F$*.*
2. $(x \otimes x) + (x \wedge t)$ を $(x, B_f(t))$ に対応させる $F \wedge F$ から $F \oplus F$ への全射線形写像 ρ により, $\mathcal{H}(n, \mathbb{F}_2)$ は $\mathcal{S}[f]$ を *cover* する.

3.2.2 APN 関数 f に付随するグラフ $\Gamma(f)$

$F \cong \mathbb{F}_{2^n}$ 上の関数 f に対して, 頂点集合を $F \oplus F := \{(a,x) \mid a, x \in F\}$,
隣接関係を, (a,x) と (b,y) が結ばれるのは $x + y = f(a+b) + f(0)$ のとき,
と定義して得られるグラフを $\Gamma(f)$ と書く. [17] に原型がある.
f が APN 関数 $\Leftrightarrow$ $\Gamma(f)$ が semibiplane の incidence graph.

3.2.3 同値性の言い換え

Proposition 10 (Y 2010, [42]) *([17] に本質的に示されている. [10]でも DHO という言葉を使ってはいないが, 同じことが述べられている)*
f, g を $F \cong \mathbb{F}_{2^n}$ 上の *APN* 関数とするとき次が成立.

1. $f \sim g$ *(CCZ* 同値*)* $\Leftrightarrow$ $\Gamma(f)$ と $\Gamma(g)$ がグラフとして同型.
2. f, g が *quadratic* のとき,
   $f \sim' g$ *(EA* 同値*)* $\Leftrightarrow$ $\mathcal{S}[f]$ と $\mathcal{S}[g]$ が *DHO* として同型.

3.2.4 Edel 予想の解決とその拡張

Theorem 11 (Y 2012 [43]) f, g を $F \cong \mathbb{F}_{2^n}$ 上の *quadratic APN* 関数とする. このとき $f \sim g$ *(CCZ* 同値*)* $\Leftrightarrow$ $f \sim' g$ *(EA* 同値*).*

この結果は, 発見された quadratic APN 関数の無限族が本当に新しいものかどうか調べる作業を簡易化する. 実際に知られている APN 関数の無限族は, すべて単項式で表せるものに CCZ-同値であるか, または quadratic APN 関数である.

また, 証明は驚くほど初等的であり, 群論に関してはシローの定理と, 非自明な 2-群の中心が非自明であることしか使わない.

この結果は少し拡張された意味での APN 関数（定義域と値域が異なっても良い）に対しても成立することが, Dempwolff-Edel の論文 [9] で示された.

アイデアは, DHO の自己同型群と関数のグラフの自己同型群の関係を精密に記述するというもので, Edel 氏による quadratic APN 関数に付随する DHO の特徴付け [8] を使う. 実は私も初めはこの方向での証明を目指して, 出来たように思ったが, はっきり示していない部分があることに気付いて, 原証明を検討するうちに, 殆どの群論的考察を省いて非常に初等的な証明にたどり着いたという経緯がある. その意味では, Dempwolff-Edel 氏の証明は, 群論的発想による正統的な証明であるといえる.

3.2.5 Quadratic APN 関数の幾何的言い換えと個数に関する予想

$F \cong \mathbb{F}_{2^n}$ 上の quadratic APN 関数 f は線形写像 $\bar{f} : F \wedge F \to F$ で $\bar{f}(x \wedge y) = B_f(x, y)$ を満たすものを引き起こすが，ここで $W := Ker(\bar{f})$ は次を満たす．

$$\dim(W) = \dim(F \wedge F) - n,\ x \wedge y \in W \text{ ならば } x \wedge y = 0.$$

Proposition 12 *([41] の後半に述べられたのが初めて？その他 Edel, Nakagawa もこの事実を認識)*
「$F \cong \mathbb{F}_{2^n}$ 上の *quadratic APN* 関数の *EA*-同値類全体」と
「上の条件を満たす $F \wedge F$ の部分空間 W の集合の $GL(F)$-*(diagonal action)* 共役類」は *bijective* に対応．

すなわち，有限体 $F \cong \mathbb{F}_{2^n}$ 上の quadratic APN 関数は，$F \wedge F$ 中の余次元 n の部分空間 W で $x \wedge y\ (\neq 0)$ の形の元を含まないものに対応しているので，これらの $GL(F)$-共役類を調べることにより，次が示せるのではないかと期待される．

予想 $N(n) := {}^{\#}\{\text{APN-maps on } \mathbb{F}_{2^n}/(\text{CCZ-equiv.})\}$ とするとき，
$N(n)$ は n に関して指数関数的に増大する．

4 代数構造との関連と Doubly DHO

4.1 代数構造

n-DHO $\mathcal{S}$ over $\mathbb{F}_{2^n}$ は，生成空間 $\mathbf{A} = \mathbf{A}(\mathcal{S})$ の次元が $2n$ で，$Y \cap X = \{0\}$ $(\forall X \in \mathcal{S})$ を満す n-次元部分空間 Y が存在するとき，Y 上 **split** するという．

このとき $\mathcal{S}$ のメンバー $X(0)$ を一つ定めれば，$\mathcal{S} \setminus \{X(0)\}$ のメンバー X を $X = X(t) \Leftrightarrow X(0) \cap X = \langle t \rangle$ と定めることにより $X(0)$ の元 t で添数付けることが出来る．更に，$X(t)$ の任意の元 v は次の形に一意的に分解できて，$f_t : X(0) \to Y$ は線形写像となる．

$$v = x + f_t(x), \quad x \in X(0), f_t(x) \in Y.$$

従って $X(0)$ 上の右分配的な “積 $(x, t) \mapsto f_t(x)$” $(Y = X(0)$ とみて$)$ に関する代数構造 $(X(0); +, *)$ が定まる．例えば，quadratic APN 関数 f に対する DHO $\mathcal{S}[f]$ は split して，$x * t = f_t(x) = B_f(x, t)$.

奇標数の有限体上の最も非線形な関数 (平面関数) g に対して同様に定義される積 $*$ に関しては，代数構造 $(X(0); +, *)$ と g から定まる射影平面の性質との関連がよく調べられている．

その類似として，一般に split DHO over $\mathbb{F}_2$ から得られるこの代数構造に関する理論展開が期待される．(基本論は Yoshiara 2009 のノート [41]．すべての DHO は split するか？)

Proposition 13 (Dempwolff-Edel 2012 [9]) $\mathcal{S}$ を $\dim(\mathbf{A}(\mathcal{S})) = 2n$ である n-*DHO over* $\mathbb{F}_2$ とする．

このとき $\mathcal{S}$ が $\mathbf{A}(\mathcal{S})$ の n-次元部分空間 Y に関して *split* しており，かつ先の積 $*$ が双線形となるように添数付けが出来る．*($\mathcal{S}$ が* **bilinear***)* $\Leftrightarrow \mathrm{Aut}(\mathcal{S})$ の部分群 T で $\mathcal{S}$ のメンバー上に正則で，Y 上自明に作用するもの *(***translation group***)* が存在する．

更に，上記論文では，二つの bilinear n-DHO から bilinear $(n+1)$-DHO を構成する方法が記述されている．これは 部分 DHO の直和として得られる DHO に関する一般論に拡張される (Y 2012 [44]).

4.2 Doubly DHO

$\dim(\mathbf{A}(\mathcal{S})) = 2n$ である n-DHO $\mathcal{S}$ over $\mathbb{F}_2$ で，各メンバーが $\mathbf{A}(\mathcal{S})$ 上の非特異双一次ないしは二次形式に関する全等方的部分空間であるもの (DHO of **polar type**) は Yoshiara 2006 [35] により始めて考察され, Taniguchi により拡張された [23], [26], [6]:

Definition 14 $\mathbf{A}$ は $2n$ 次元空間で, 非特異双一次ないしは二次形式 Q を備えたもの. $\dim(\mathbf{A}(\mathcal{S})) = \mathbf{A}$ である *n-DHO $\mathcal{S}$ over $\mathbb{F}_2$* が **doubly DHO** とは, $X \in \mathcal{S}$ の Q に関する直交空間 $X^\perp$ を集めて得られる集合 $\mathcal{S}^\perp := \{X^\perp \mid X \in \mathcal{S}\}$ が *n-DHO over $\mathbb{F}_2$* であること.

Proposition 15 (Dempwolff 2012 [6]) $\mathcal{S}$ を $\mathbf{A}(\mathcal{S}) = \mathbf{A}$ の次元が $2n$ である *n-DHO over $\mathbb{F}_2$* とする.

1. $\mathcal{S}$ が *doubly DHO* $\Leftrightarrow \cup_{X\in\mathcal{S}} X \setminus \{0\}$ の特性関数 $f : \mathbf{A} \to \mathbb{F}_2$ が *bent.*
2. $\mathcal{S}$ が Y に関して *split* する *doubly DHO* $\Leftrightarrow$ $\cup_{X\in\mathcal{S}} X \cup Y$ の特性関数 $g : \mathbf{A} \to \mathbb{F}_2$ が *bent.*

ここで $f : V = (\mathbb{F}_2)^{2m} \to \mathbb{F}_2$ が **bent** とは，任意の $v \in V$ に対し

$$\hat{f}(v) := \sum_{v\in V} (-1)^{f(x)+x\cdot v} = \pm 2^m.$$

Remark 16 $\dim(V) = 2m-1$ のとき $f : V \to V$ が *quadratic APN* $\Leftrightarrow$ 各 $0 \neq a \in V$ に対する $f_a(x) = f(x) \cdot a$ に対して $\hat{f_a}(v) \in \{0, \pm 2^m\}$.

先の命題に基づいて, Dempwolff-Kantor は Kantor の orthogonal spread に対する手法を応用して, 多くの DHO of polar type を構成した [7]. これは APN 関数の個数に関する予想を解決する手がかりになる可能性がある.

5 補足

講演時において説明できなかった点などを思いつくままに補う.

有限単純群を説明する幾何 DA を研究する動機の一つとして，Lie 型の単純群に対する建物などの「有限単純群を説明する幾何」に言及したが，これに関して講演直後に質問があった. そこで回答したように，この幾何は「現象として存在する」のであって，理論的にこのような幾何の存在が保証されるわけではない. この幾何は各有限単純群が旗上可移に作用するような階数 3 以上の結合幾何で, ある素数 p に対する centric radical p-subgroups のなす simplicial complex と homotopy 同値であることが多い（建物はその例). この構造に関しては，過去の代数学シンポジウムで筆者による講演及び千葉大の澤辺氏による講演がなされている. 筆者は散在型単純群に対する radical p-subgroups を分類しているが, そのトポロジーへの応用については
Classifying spaces of sporadic groups, D. J. Benson and Stephen D. Smith, Mathematical Surveys and Monographs, 47, 2008, Amer. Math. Soc. を見られよ.

DHO 以外の DA　講演では DHO に話を限定したが, extended quadrungle を構成する種になる **Y-family** など, DHO でない DA の部分クラスにも非常に面白いものが存在する．しかし，最近は殆ど研究されていないようである．射影平面上の弧との類比でいえば，maximal arc に相当するものの研究などが望まれるが，殆ど手が付けられていない. 筆者のサーベイ [36, Section 6] とそこに挙げられた文献を参照.

DHO の自己同型群　DHO の自己同型群，自己同型群によるの分類などに関して面白い話題があるが，講演では Edel-Dempwolff の結果 [9] 以外には触れなかった. サーベイ [36, Section 3] 及び数年前の筆者の講演録などが参考になるだろう. 手段は比較的基本的な群論によるものが多く, 二重可移群の分類結果以外，有限単純群の分類を使用していない．なお，[9] では Timemsfeld によるある TI-subgroups を持つ有限群の分類 (Groups with weakly closed TI-subgroups, Math. Z. 143 (1975), 243–278) の 3 節前半の議論が頻繁に使われている．Gularnick よる素数べき指数の部分群を持つ単純群の分類（これは有限単純群の分類に依存する）も使われているが，この結果を使わずに個別議論によって処理することが出来る.

非線形関数の幾何としての DHO − 2006 年の衝撃　(標数 2 の有限体上の) 非線形関数の幾何学的研究の手段として, 二元体上の DHO が有効であるという認識がここ数年で確立したと思われる．2006 年のサーベイ [36] には構成のごく一部 (5.5 節の最後) に不十分な記述しか与えられていなかった (APN 関数はすべて単項式に同値と思われていた時代に書いたので, レフェリーがこの記述を丁寧に書くことに批判的であった) ことに比べると, 隔世の感がある．2006 年の APN 関数における革新的な発見 (**Edel-Kyureghyan-Pott** による, 2.1 節の 9) がそのきっかけであったのはいうまでもない．講演の後半は，非線形関数を記述する幾何としての DHO の側面の解説であったが，とにかく非線形関数に関連する進展にはめざましいものがある.

Quadratic APN 関数の EA-同値類の個数に関する予想　講演後の質問に「個数に関する予想は quadratic APN 関数の EA-同値類に限定しても成立すると考えているか」という旨のものがあったが，そのときにも回答したように，現時点では筆者はそのように予想している．現時点では quadratic でない APN 関数の無限系列は単項式に CCZ-同値なものしか知られていないし，十分多くの quadratic APN 関数があると考えるのは無理ではないように思う．ただ，quadratic でない APN 関数は $\mathbb{F}_{2^6}$ 等で知られており, 体が大きくなると quadratic でも単項式にも同値でない奇妙な APN 関数が続々と発見される可能性は残っている.

現時点で知られている有限体 $F \cong \mathbb{F}_{2^n}$ 上の APN 関数 $f(x)$ の無限系列には次の 7 個がある．始めに単項式 $f(x) = x^d$ の形の関数と CCZ-同値なものを挙げる．d のみを挙げる．$w_2(d)$ とは d を $d = \sum_{i=0}^{n-1} a_i 2^i$ $(a_i \in \{0, 1\})$ の形に 2 進展開したとき $a_i \neq 0$ を満たす i の個数 (2-weight) を表す.

名称	指数 d	条件	$w_2(d)$
Gold	$2^s + 1$	$(s, n) = 1$	2
Kasami	$2^{2s} - 2^s + 1$	$(s, n) = 1$	$s + 1$
Welch	$2^t + 3$	$n = 2t + 1$	3
Niho	$2^t + 2^{t/2} - 1$, t 偶数 $2^t + 2^{(3t+1)/2} - 1$, t 奇数	$n = 2t + 1$	$(t + 2)/2$ $t + 1$
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	$t + 3$

この表で, 異なる系列に属する関数は大きな n に対しては CCZ-同値ではない．また，一つの系列でもパラメーターの取り方により，幾つかの CCZ-同値類に分かれ得る．

次に単項式に CCZ-同値でない APN 関数の無限系列として知られているのは，２０１１年現在, 次の 7 系列である．パラメータの取り方によって同値なものがあるが，一般には異なる系列に属する関数どうしは CCZ-同値ではない．

(1) $n = 3m$, $m \in \mathbb{Z}$, $(m, 3) = 1$, $m \geq 3$ のときのみ定義される．

$$f(x) = x^{2^s+1} + \zeta^{2^m-1} x^{2^{mi}+2^{m(3-i)+s}}.$$

この関数は $(s, i; \zeta)$ により定まる． ここで, s, i は $s \in \{1, \ldots, n-1\}$, $(s, n) = 1$; $i \in \{0, 1, 2\}$, $i \equiv sm \pmod 3$ を満たす整数で ζ は F の原始元.

(2) $n = 4m$, $m \in \mathbb{Z}$, $(m, 2) = 1$, $m \geq 3$ のときのみ定義される．

$$f(x) = x^{2^s+1} + \zeta^{2^m-1} x^{2^{mi}+2^{m(4-i)+s}}.$$

この関数は $(s, i; \zeta)$ により定まる．ここで s, i は $s \in \{1, \ldots, n-1\}$, $(s, n) = 1$; $i \in \{0, 1, 2, 3\}$ を満たす整数で ζ は F の原始元.

(3) $n = 2m$, $(2, m) = 1$ を満たす整数 m が存在するときのみ定義される．

$$f(x) = \zeta x^{2^{2^s+1}} + \zeta^{2^m} x^{2^{m+s}+2^m} + \zeta' x^{2^m+1} + \sum_{i=1}^{m-1} \gamma_i x^{2^{m+i}+2^i}.$$

この関数は $(s; \zeta, \zeta'; \gamma_1, \ldots, \gamma_{m-1})$ により定まる．ここで s は $1 \leq s \leq n-1$, $(s, n) = 1$ を満たす整数, ζ と ζ' は F の原始元, γ_i $(i = 1, \ldots, m-1)$ は F の部分体 $\mathbb{F}_{2^m}$ の元.

(4) 任意の自然数 n に対して定義される．$\mathrm{tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$.

$$f(x) = x^3 + \mathrm{tr}(x^9).$$

(5) $n = 3m$ and $(m, 3) = 1$ を満たす整数 m が存在するときのみ定義される．

$$f(x) = \zeta x^{2^{-m}+2^{m+s}} + \zeta^{2^m} x^{2^s+1} + \eta x^{2^{m+s}+2^s}.$$

この関数は $(s; \zeta, \eta)$ により定まる．ここで s は $1 \leq s \leq n-1$, $(s, n) = 1$, $s \equiv -m \pmod 3$ を満たす整数, ζ は F の原始元で η は部分体 $\mathbb{F}_{2^m}$ の元.

(6) $n = 3m$, $(m, 3) = 1$ を満たす整数 m が存在するときのみ定義される．

$$f(x) = \zeta^{2^m} x^{2^{-m}+2^{m+s}} + \zeta x^{2^s+1} + \eta x^{2^{-m}+1}.$$

この関数は $(s; \zeta, \eta)$ により定まる．ここで s は $1 \leq s \leq n-1$, $(s, n) = 1$, $s \equiv -m \pmod 3$ を満たす整数, ζ は F の原始元で η は部分体 $\mathbb{F}_{2^m}$ の元.

(7) $n = 3m$, $(m, 3) = 1$ を満たす整数 m が存在するときのみ定義される．

$$f(x) = \zeta^{2^m} x^{2^{-m}+2^{m+s}} + \zeta x^{2^s+1} + \eta x^{2^{-m}+1} + \eta' \zeta^{2^m+1} x^{2^{m+s}+2^s}.$$

この関数は $(s; \zeta, \eta, \eta')$ により定まる．ここで s は $1 \leq s \leq n-1$, $(s, n) = 1$, $s \equiv -m \pmod 3$ を満たす整数, ζ は F の原始元で η は部分体 $\mathbb{F}_{2^m}$ の元.

更に最近，次の (8) における関数は適当なパラメータを取ると上記の系列以外の $F = \mathbb{F}_{2^{2m}}$ 上の新しい APN 関数を与えることが示されている．また上記の無限系列の幾つかは (9) の形に構成できることも示されている．ここで，ベクトル空間として $\mathbb{F}_{2^{2m}}$ を直和 $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m} = \{(x, y) \mid x, y \in \mathbb{F}_{2^m}\}$ と同一視している．

Proposition 17 *(8)* $n = 2m$, $m \geq 2$, m は偶数とせよ．$(s, n) = 1$ を満たす整数 s, 偶数 i 及び $\alpha \in F \setminus \{x^3 \mid x \in F\}$ に対して，次式で定められる F 上の関数 f は *APN* である．

$$f(x, y) := (x^{2^s+1} + \alpha x^{(2^s+1)2^i}, xy).$$

(9) $n = 2m$ を偶数，i, j は $(m, i - j) = 1$ を満たす整数とする．$\mathbb{F}_{2^m}$ の元 g_i $(i = 1, 2, 3, 4)$, ただし $g_1 \neq 0$, $g_4 \neq 0$, に対して

$$g(x, y) := g_1 x^{2^{i+j}} + g_2 x^{2^i} y^{2^j} + g_3 x^{2^j} y^{2^i} + g_4 y^{2^{i+j}}$$

とおく．このとき F 上の関数 f を $f(x, y) := (g(x, y), xy)$ により定めると，f が *APN* であるための必要十分条件は $g(x, 1) = g_1 x^{2^{i+j}} + g_2 x^{2^i} + g_3 x^{2^j} + g_4$ が $\mathbb{F}_{2^m}$ に解を持たないことである．

小さな n の値であっても，$F \cong \mathbb{F}_{2^n}$ 上の APN 関数の完全な分類は難しく，完成しているのは $n = 6$ までに過ぎない．$n = 5$ の時には x^3 (Gold), x^5 (Gold), x^{-1} (inverse) を代表とする 3 個の CCZ-同値類に分かれる．$n = 6$ の時には 14 個の CCZ-同値類があり，単項式を代表に持つものは 1 個で，13 個は quadratic 関数を代表とするが，注目すべきことに quadratic 関数も単項式も含まない類が一つある．$n = 7$, 8, 9 の時は，それぞれ少なくとも 19, 23, 11 個の同値類が知られている．

Non-linearity と APN 関数　APN 関数の定義を与えたのは K. Nyberg で 1993 年の Eurocrypt '93 においてであるという（講演時には誤って J. Dillon といったような気がするが訂正する）．APN 関数の定義自体は差分に注目した設定である．非線形関数 f には，その成分関数と線形関数（アフィン関数）達との関数空間での距離の最小値 (f の **nonlinearity** $N(f)$) に注目した定義もあり，これを満たす関数を **almost bent**(**AB**) という．実は AB 関数はつねに APN 関数であり，AB 関数が存在するのは n が奇数のときで，n が奇数のときには quadratic APN 関数という概念と quadratic AB 関数という概念は一致する．講演後の質問の一つは，nonlinearity とも関連するように思われたので，以下補足説明する

まず $F \cong \mathbb{F}_{2^n}$ から二元体 $\mathbf{F}_2$ への写像 g (F 上の形式) と x 成分が $g(x)$ で与えられる長さ 2^n の行ベクトル ${}^t(..., g(x), ...)$ とを同一視して，F 上の形式全体を長さ $N = |F| = 2^n$ の数ベクトル空間 $(\mathbb{F}_2)^N$ とみなす．このとき形式 f, g 間の距離 $\delta(f, g)$ をそのハミング距離とする: $\delta(f, g) := {}^{\#}\{x \in F \mid f(x) \neq g(x)\}$. この距離は次のようにも表示できる: $\delta(f, g) = 2^{n-1} - \frac{1}{2}(\sum_{x \in F} (-1)^{f(x)+g(x)})$, ここでここで二元体の元 $c = f(x) + g(x)$ に対する $(-1)^c$ は $c = 0$ か $c = 1$ に応じて 1 か -1 という整数を表すと理解する．g がアフィン形式の場合には適当な $b \in F$ と $\varepsilon \in \mathbb{F}_2$ に対して $g(x) = \mathrm{Tr}(bx) + \varepsilon$ がすべての $x \in F$ に対して成立する (このとき $g = T_b + \varepsilon$ と書く) ので $\delta(f, T_b + \varepsilon) = 2^{n-1} - \frac{(-1)^\varepsilon}{2} \sum_{x \in F} (-1)^{f(x)+\mathrm{Tr}(bx)}$ である．

ここに現れる項 $\sum_{x \in F} (-1)^{f(x)+\mathrm{Tr}(bx)}$ は，可換群 $(F, +)$ から複素数の乗法群 $\mathbb{C}^\times$ への 関数 $\tilde{f}(x) := (-1)^{f(x)}$ と可換群 $(F, +)$ の加法指標 $\tilde{\chi}_b(x) := (-1)^{\mathrm{Tr}(bx)}$ の内積値の $|F| = 2^n$ 倍であり，複素関数 $\tilde{f}$ (実際には整数値を取る) の $\tilde{\chi}_b$ における**離散フーリエ係数** (ないしは Walsh 係数) と呼ばれる．

さて有限体 $F \cong \mathbb{F}_{2^n}$ 上の関数 $f : F \to F$ と $a \in F$, $a \neq 0$, に対して f の a 方向の**成分形式** f_a とは $f_a(x) := \mathrm{Tr}(af(x)) = \sum_{i=0}^{n-1}(ax)^{2^i}$ で与えられる F 上の形式である．(f が quadratic という条件は, その成分関数 f_a がすべて二次形式であることと同値である.) この形式 f_a に対する複素関数 $\tilde{f}_a$ の指標 $\tilde{\chi}_b$ における離散フーリエ係数のことを $f^{\mathcal{W}}(a,b)$ と書く：

$$f^{\mathcal{W}}(a,b) := \sum_{x\in F}(-1)^{\mathrm{Tr}(af(x)+bx)}, \quad a \in F^\times = F \setminus \{0\}, b \in F.$$

元に戻って，成分形式 f_a とアフィン形式の距離とは, $g = T_b + \varepsilon$ がアフィン関数を動くときの距離 $\delta(f_a, T_b + \varepsilon)$ の最小値であり，関数 f とアフィン形式の距離とは様々な成分関数 f_a $(a \in F^\times)$ に対するこの距離の最小値と定義される．この値を f の **nonlinearity** と呼び $NL(f)$ と書く：

$$\begin{aligned} NL(f) &:= 2^{n-1} - \frac{1}{2}\max_{a\in F^\times, b\in F}|\sum_{x\in F}(-1)^{\mathrm{Tr}(af(x)+bx)}| \\ &= 2^{n-1} - \frac{1}{2}\max_{a\in F^\times, b\in F}|f^{\mathcal{W}}(a,b)|. \end{aligned}$$

$NL(f)$ がなるべく大きいような写像 f が最も非線形的とよばれるのにふさわしいことになる．

指標の直交関係を用いて, $NL(f)$ は高々 $2^{n-1} - 2^{(n-1)/2}$ であり，等号が成立する条件は離散フーリエ係数 $f^{\mathcal{W}}(a,b)$ が (a, b の取り方に依存するが) 0 または $\pm 2^{(n+1)/2}$ という 3 種類のどれかの値であることが示せる．

Definition 18 $NL(f) = 2^{n-1} - 2^{(n-1)/2}$ またはこれと同値な条件「$a \in F^\times$, $b \in F$ に対して $f^{\mathcal{W}}(a,b) \in \{0, \pm 2^{(n+1)/2}\}$ 」を満たすような関数 $f : F \cong \mathbb{F}_{2^n} \to F$ を **almost bent**(略して **AB**) という．

定義から $NL(f)$ は整数なので $F \cong \mathbb{F}_{2^n}$ 上の AB 関数 f が存在するとき n は奇数である．(n が偶数の時 $F \cong \mathbb{F}_{2^n}$ から F への関数 f に対して $N(f) \leq 2^n - 2^{n/2}$ と予想されている.) 単項式 APN 関数のうち, Welch と Niho 系列は AB であり, Gold と Kasami 系列は n が奇数の場合は AB である．

Proposition 19 $F \cong \mathbb{F}_{2^n}$ 上の関数 f に対し, 上記の記号のもとで次が成立.
1. f が APN である $\Leftrightarrow \sum_{a\in F^\times, b\in F} f^{\mathcal{W}}(a,b) = 2^{4n+1} - 2^{3n+1}$.
2. f が AB であれば APN である（もちろん逆は成立しない）.
3. n が奇数で f が *quadratic* の時には, f が APN であることと, f が AB であることは同値.

上の命題の 3 が 4 章最後の Remark である．なお，講演時には機器故障のため十分な時間お見せできなかった, スライドの最終ページにおいては，この Remark で quadratic という形容詞を抜かしていた．そこを読み取って混乱してしまった聴衆にはお詫びしたい．

APN 関数と bent 関数　4 章の最後に Dempwolff-Kantor の結果により DHO から様々な bent 関数が見つかるので, APN 関数が見つかる可能性が期待できる旨を述べた．これは，知られている APN 関数の離散フーリエ係数の値に対する観察事実と関係しているので，以下補足説明したい．

$F \cong \mathbb{F}_{2^n}$ から F への関数 f に対して, その $a = 1$ に対する成分形式 f_1 を考えると, 離散フーリエ係数 $f^{\mathcal{W}}(1,b)$ $(b \in F)$ は $\sum_{x\in F}(-1)^{\mathrm{Tr}(f(x)+bx)}$ と書ける．そこで記号を流用して，F_{2^n} 上の形式 f に対して $f^{\mathcal{W}}(1,b) := \sum_{x\in F}(-1)^{\mathrm{Tr}(f(x)+bx)}$ とおく．

Definition 20 $F \cong \mathbb{F}_{2^n}$ から $\mathbb{F}_2$ への関数 (形式) f が **bent** であるとは $f^{\mathcal{W}}(1,b) = \sum_{x\in F}(-1)^{\mathrm{Tr}(f(x)+bx)}$ の値が $\pm 2^{n/2}$ のいずれかであること.

$f^{\mathcal{W}}(1,b)$ は整数であるから, $F \cong \mathbb{F}_{2^n}$ から $\mathbb{F}_2$ への bent 関数が存在すれば n は偶数である. なお, 通常「bent 関数」というが, 二元体上に値を取るので以下では「bent 形式」と呼ぶ. f が bent 形式であることと, f と F 上のアフィン形式との距離が最大であることは同値である (これが名称 bent の由来である).

ここで 偶数 n に対する $F \cong \mathbb{F}_{2^n}$ 上の知られている APN 関数 f の成分形式 f_1 が bent 関数に極めて近いものであるという観察に注意しよう. APN 関数に対する離散フーリエ係数 $f^{\mathcal{W}}(a,b)$ ($a \in F^\times$, $b \in F$) の値はグラフの原点を固定する CCZ-同値により不変である. 離散フーリエ係数の値をまとめたスペクトラム (次の段の記述参照) は, ほぼすべての知られている APN 関数について計算されており, n が奇数の場合は AB 関数と同じで, n が偶数の場合には, $n = 6$ における唯一の例外 (これも quadratic に CCZ-同値) を除いて Gold 関数に同じ (下のスペクトラムの表の (2)) となる. $a = 1$ のときに $f^{\mathcal{W}}(1,b) = \pm 2^{n/2}$ しか出てこない (従って成分関数 f_1 は bent 形式となる) のはどのときか, 筆者はまだ完全に調べてはいないが, 幾つかの無限族ではこれが成立している. 実際にはかなりの例で, 任意の $a \in F^\times$ に対する成分形式 f_a は bent 形式になっていると思われる. 一般には, $F = \mathbb{F}_{2^{2m}}$ 上の関数 f が quadratic であるときには, f が APN であれば, 少なくとも $(2/3)(2^{2m}-1)$ 個の $a \in F^\times$ に対して, 成分関数である二次形式 f_a は bent であること (これは非特異であることに他ならない) が示せる.

ともかく, bent 関数 b が出てくるときに, $f_1 = b$ を満たす APN 関数 f が存在する可能性がある. 4 節で紹介した Dempwolff の結果 [6] は DHO of polar type から bent 形式を生み出すので, 多くの DHO of polar type が構成されるという Dempwolff-Kantor の結果 [7] によると, とにかく DHO に関連した多くの bent 形式が出来る. これらが APN 関数に繋がるものであるのかどうかは, これから緊急に調べねばならない課題である. 講演の最後で述べたかったのは, このようにして $\mathbf{F}_{2^n}$ (n 偶数) 上の APN 関数が多く出てくるのではないかという期待である. (もちろん bent 関数自体はいくらでもといっても良いほど数多く存在するので, それらは一般には APN 関数の成分関数になるとは思えないが, DHO に関連して出てくる点が多少の期待を抱かせる.)

APN 関数 f に対する離散フーリエ係数の値の集合 $\{f^{\mathcal{W}}(a,b) \mid a \in F^\times, b \in F\}$ を (重複度を込めて) f の**フーリエスペクトラム** という. フーリエ係数の絶対値の集合は重複度を込めて定まるが, スペクトラムは $f(0) = 0$ と正規化しないと定まらない. 以下正規化しておく. スペクトラムは, 2 元体上長さ $2^n - 1$, 次元 $2n$ のある符号のウェイト分布として記述できる. APN 関数のスペクトラムとして登場するのは, 次の極めて限られた多重集合 (1)–(5) であることが観察されている (α の重複度を $m(\alpha)$ と記した. (5) では α $[m(\alpha)]$ を与えた.) :

(1) AB 関数 (n が奇数) に対するスペクトラム $\{0, \varepsilon 2^{(n+1)/2} \mid \varepsilon = \pm 1\}$,
$m(0) = (2^{n-1}+1)(2^n-1)$, $m(\varepsilon 2^{(n+1)/2}) = (2^n-1)(2^{n-2} + \varepsilon 2^{(n-3)/2})$.

(2) 偶数 n の Gold 関数のスペクトラム $\{0, \varepsilon 2^{n/2}, \varepsilon 2^{(n/2)+1} \mid \varepsilon = \pm 1\}$,
$m(0) = (2^n-1)(2^{n-2}-1)$, $m(\varepsilon 2^{n/2}) = (2/3)(2^n-1)(2^{n-1} + \varepsilon 2^{(n-2)/2})$,
$m(\varepsilon 2^{(n+2)/2})(1/3)(2^n-1)(2^{n-3} + \varepsilon 2^{(n-4)/2})$.

(3) Inverse 系列のスペクトラム: これは Kloosterman sum の値 $+1$ であり, $-2^{(n+2)/2}+1 \le s \le 2^{(n+2)/2}+1$, $s \equiv 0 \pmod 4$ を満たす整数 s すべてからなる. 重複度は $H((s-1)^2 - 2^n)$ (Hurwitz-Kronecker 類数).

(4) Dobbertine 系列に対するスペクトラム ($2^{n/5}$ の倍数だが $2^{(2n/5)+1}$ では割れない整数幾つかからなる. 詳細は略. 重複度は未定らしい).

(5) $n=6$ の例外関数 $x^3+\zeta^{11}x^5+\zeta^{13}x^9+x^{17}+\zeta^{11}x^{33}+x^{48}$ (ζ は原始元) に対する $\{32[3], 16[160], 8[1656], 0[891], -8[1288], -16[96], -32[1]\}$.

$n=6$ における quadratic 関数にも単項式にも CCZ-同値でない APN 関数の散在例については，そのスペクトラムは (2) である．このような現象の理解のため，APN 関数のフーリエスペクトラムに関する，より理論的な研究も重要であろう．

奇妙な関数　前世紀中頃に定義された奇標数の有限体上の非線形関数（平面関数）の概念は，自己同型群がある程度大きい射影平面の構成を動機としたものであったが，奇標数の presemifield などの代数構造の研究を促した．この偶標数での類似の追究が目下の重要課題の一つであり，具体的な APN 関数の構成にも繋がる可能性がある．偶標数の quasifield との関連は，ambient space の次元が $2n$ の n-DHO over $\mathbb{F}_2$ においては谷口氏の研究 [22] により知られているが，今の場合 ambient space の次元は一つ上がる．Taniguchi-Yoshiara の論文で言及されているように，特に $F\cong\mathbb{F}_{2^n}$ (n odd) 上の bilinear map $B(x,y)=x^4y+xy^4+(xy)+(xy)^2$ から構成される bilinear DHO は Buratti-Del Fra DHO $\mathcal{D}(n,\mathbb{F}_2)$ の quotient であるが，この関数 B の形が Coulter-Matthews semifield の積を与える関数 $C(x,y)=x^9y+xy^9+xy^3+(xy)^3$ ($\mathbb{F}_{3^n}$ (n odd) 上で定義される) と非常に似ている点は示唆的である．

幾つかの重要な未解決問題　基本的に重要な未解決問題として「split しない n-DHO は存在するか」がある．今のところ，知られている DHO の例は Taniguchi DHO $\mathcal{T}(n,\mathbb{F}_2)$ を除いてすべて split しているが，n が大きいとき $\mathcal{T}(n,\mathbb{F}_2)$ が split しているかどうかは, 講演で解説した非常に簡明な記述 (1.3 節 Proposition 5) が得られたにもかかわらず，現時点では未解決である．

また，生成空間の次元が $n(n+1)/2$ (可能な最大値と思われる) であるような n-DHO (ないしはメンバー数が $(q^n-1)/(q-1)$ の n-DA) over $\mathbb{F}_q$ の無限系列は $q>2$ のときに Veronesean DHO に限るのか, $q=2$ のときには Veronesean, Huybrechts, Buratti-Del Fra, Taniguchi DHO に限るのか否かも, 非常に重要な問題であるが，本格的な研究はまだない. DA についての問題は Segre による射影平面上の非退化二次曲線の特徴付けの高次元版であり, van Maldeghem-J.Thas による結果 [31, 32] はあるが，DHO の言葉でのすっきりした特徴付けが欲しい.

対極的に，生成空間の次元が $2n-1$ (可能な最小値) であるような n-DHO over $\mathbb{F}_q$ については [3, 4, 22] 等の研究があり, quasifields からの構成が知られているが, もう少しはっきりとした分類が出来るようにも思われる.

谷口浩朗氏と中川暢夫氏の DHO 研究への貢献　講演では強調できなかったが，DHO 研究に対する香川高専の谷口浩朗氏の一連の重要な貢献について言及したい.

$\mathcal{H}(n,\mathbb{F}_2)$, $\mathcal{D}(n,\mathbb{F}_2)$, $\mathcal{V}(n,\mathbb{F}_2)$, $\mathcal{T}(n,\mathbb{F}_2)$ の統一的記述に関しては，谷口氏による一連の先行研究 [21, 24, 25] がここに至る道を切り開いたといえよう．谷口氏のアイデアは Del Fra の発想 [1, 5] を徹底的に推し進めたもので, n-DHO の二つの異なるメンバーの交叉 (1 次元空間) 中の唯一の非零ベクトルの言葉で DHO を記述する試みである [21]. 上述の先行研究やその後の筆者との共同研究 [28, 29] では，このベクトル達が満たす関係式 (addition formula) に注目することで, これらの DHO を特徴付けないしは定義することに成功し, 与えられた DHO がその商である判定条件も与えた．Coulter-Matthews の関数の偶標数版である，上記の奇妙な関数 B を発見したのも谷口氏である．氏が発見した $\mathcal{T}(n,\mathbb{F}_2)$ におけるこれらの交叉零ベクトルの具体形 (２０１２年５月の香川大学でのセミナー及び弘前大学での 2012 年度代数学シンポジウムで発表) に示唆されて，筆者が最終的にまとめたのが 1.3 節で与えた記述である．

谷口氏の上記の発想は Dempwolff-Kantor の研究にも繋がるものであり，筆者の DHO of polar type の概念 [36, Section 4], [35, 15] を発展させて, DHO の‘双対’をはっきり定義して研究を開始したのも氏である [23, 26]. Doubly DHO には奇標数の semifield 上の Knuth cube symmetry に対応する対称性があるが, これにいち早く着目したのも谷口氏であった.

また DHO そのものの研究には数多い寄与はないが (しかし [14] には Mathieu DHO に関する優れた特徴付けと記述がある), 筆者の目を有限体上の関数とのつながりに向けてくれ，非線形関数などについて様々なことを学び得たのは，近畿大学の中川暢夫氏（本年４月で常勤職からは退職された）による小集会やセミナーでの情熱に満ちた解説と活発な討議によるところが大きい.

中川さんと谷口さんには, DHO, DA への興味を分かち合う日本人研究者として, 今までの筆者の研究を支えてくれ, 大きな刺激と展望を与えて頂いたことに対して感謝したい.

Conclave–DHO の別名　2007 年 6 月に Shaw 氏という数学者から, DHO と同じ概念を 1996 年のイタリア Assisi における集会 (Combinatorics ’96–私や Pasini, Huybrechts も参加) で発表し, 司会者から **conclave** という名称を頂いたという報告を受けた. (私の記憶には無い.) その発表をまとめた論文 [18] では確かに DHO と同じ概念が定義されている. 従って，DHO の概念が初めて発表されたのは，1999 年のほぼ同時期で, 全く独立のようである. なお，論文 [18] 及びその後の論文 [19] は, 3-DHO over $\mathbb{F}_2$ の幾つかの例の記述であり, Del Fra [4] の分類に含まれている部分が多い. 今のところ, 他に conclave の名称が使われている数学論文は無いようである.

References

[1] M. Buratti and A. Del Fra, Semi-Boolean Steiner quadruple systems and dimensional dual hyperovals, Advances in Geometry, 3 (2003), Special Volume, S245–S253.

[2] C. Carlet, Vectorial Boolean functions for cryptography and error correcting codes, in P. Hammer, Y. Camera (Eds.), Boolean methods and Models, Cambridge University Press (2010).

[3] B. Cooperstein and J. Thas, On generalized k-arcs in $PG(2n, q)$, Ann. Combin., 5 (2001), 141–152.

[4] A. Del Fra, On d-Dimensional Dual Hyperovals, Geometriae Dedicata, 79 (2000), 157–178.

[5] A. Del Fra and S. Yoshiara, Dimensional dual hyperovals associated with Steiner systems, European Journal of Combinatorics, 26 (2005), 173–194.

[6] U. Dempwolff, Dimensional doubly dual hyperovals and bent functions, manuscript, 2012.

[7] U. Dempwolff and W. M. Kantor, Dimensional dual hyperovals, symplectic and orthogonal spreads, in preparation.

[8] Y. Edel, On quadratic APN functions and dimensional dual hyperovals, Designs, Codes and Cryptography, 57 (2010), 35-44.

[9] U. Dempwolff and Y. Edel, Dimensional dual hyperovals and APN functions with translation groups, J. Algebraic Combin., to appear.

[10] F. Göloğlu and A. Pott, Almost perfect nonlinear functions: a possible geometric approach, in Coding Theory and Cryptography II, S.Nikova, B.Preneel, L.Strorme and J.Thas eds., Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten, 2007, pp. 75–100.

[11] C. Huybrechts, Dimensional dual hyperovals in projective spaces and $c.AG^*$ geometries, Discrete Math., 255 (2002), 503–532.

[12] C. Huybrechts and A. Pasini, Flag transitive extensions of dual affine spaces, Contributions to Algebra and Geometry, 40 (1999), 503–532.

[13] W. Jónsson and J. McKay, Canadian J. Math., 28 (1976), 929–937.

[14] N. Nakagawa, On 2-dimensional dual hyperovals of polar type, Utilitas Mathematica 76 (2008), 101–114.

[15] N. Nambu and S. Yoshiara, Conditions for a class of dimensional dual hyperovals to be of polar type, Finite Fields Appl., 13 (2007), 1117–1126.

[16] A. Pasini and S. Yoshiara, On a new family of flag-transitive semibiplanes, European Journal of Combinatorics, 22 (2001), 529–545.

[17] A. Pasini and S. Yoshiara, New distance regular graphs arising from dimensional dual hyperovals, *Europ. J. Combinatorics* **22** (2001), 547–560.

[18] R. Shaw, Configurations of planes in PG$(5, 2)$, Discrete Math. 208/209 (1999), 529–546.

[19] R. Shaw and J. G. Maks, Conclaves of planes in PG$(4, 2)$ and certain planes external to the Grassmannian $\mathcal{G}_{1,4,2} \subset$ PG$(9, 2)$, Journal of Geometry, ??.

[20] H. Taniguchi, On a family of dual hyperovals over $GF(q)$ with q even, European Journal of Combinatorics, 26 (2005), 195–199.

[21] H. Taniguchi, On isomorphism problem of some dual hyperovals in PG(2d+1,q) with q even, Graphs and Combinatorics, 23 (2007), 455–465.

[22] H. Taniguchi, On some d-dimensional dual hyperovals in $PG(2d, 2)$, Finite Fields and Their Applications, 14 (2008), 1010–1019.

[23] 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.

[24] H. Taniguchi, A new family of dual hyperovals in $PG(d(d + 3)/2, 2)$ with $d \geq 3$, Descrete Mathematics, 309 (2009), 418–429.

[25] H. Taniguchi, On d-dimensional Buratti-Del Fra type dual hyperovals in $PG(3d, 2)$, Descrete Mathematics, 310 (2010), 3633–3645.

[26] H. Taniguchi, On the duals of the dual hyperoval from APN function $f(x) = x^3 + \mathrm{tr}(\mathrm{x}^9)$, Finite Fields Appl., to appear.

[27] H. Taniguchi and S. Yoshiara, On dimensional dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\tau}$, Innovations in Incidence Geometry, 1 (2005), 197–219.

[28] H. Taniguchi and S. Yoshiara, New quotients of d-dimensional Veronesean dual hyperoval in $PG(2d+1,2)$, Innov. Incidence Geo., 12 (2011), 151–165.

[29] H. Taniguchi and S. Yoshiara, A new construction of the d-dimensional Buratti-Del Fra dual hyperoval, Europ. J. Combin., 33 (2012), 1030–1042.

[30] H. Taniguchi and S. Yoshiara, A unified description of four simply connected dimensional dual hyperovals, preprint, August, 2012.

[31] J. Thas and H. van Maldeghem, Characterizations of quadric and hermitian veroneseans over finite fields, J. Geometry, 76 (2003), 282–293.

[32] J. Thas and H. van Maldeghem, Characterizations of the finite quadric veroneseans $\mathcal{V}_n^{2^n}$, Quarterly J. Math., 55 (2004), 99–113.

[33] S. Yoshiara, A family of d-dimensional dual hyperovals in $PG(2d+1,2)$, European Journal of Combinatorics, 20 (1999), 589–603.

[34] S. Yoshiara, Ambient spaces of dimensional dual arcs, J. Alg. Combin., 10 (2004), 5–23.

[35] S. Yoshiara, Some remarks on dimensional dual hyperovals of polar type, Bull. Belgian Math. Soc. Simon Steven, 12 (2006), 925–936.

[36] S. Yoshiara, Dimensional dual arcs – a survey, pp.247–266, in: Finite Geometires, Groups, and Computation, eds. A. Hulpke, B. Liebler, T. Penttila, and A. Seress, Walter de Gruyter, Berlin-New York, 2006.

[37] S. Yoshiara, Notes on Taniguchi's dimensional dual hyperovals, European Journal of Combinatorics, 28 (2007), 674–684.

[38] S. Yoshiara, Dimensional dual hyperovals associated with quadratic APN functions, Innovations in Incidence Geometry, 8 (2008), 147–169.

[39] S. Yoshiara, A characterization of a class of dimensional dual hyperovals with doubly transitive automorphism groups and its applications, European Journal of Combinatorics, 29 (2008), 1521–1534.

[40] S. Yoshiara, Dimensional dual hyperovals with doubly transitive automorphism groups, European Journal of Combinatorics 30, 747–757 (2009)

[41] S. Yoshiara, Notes on split dimensional dual hyperovals, (Incomplete manuscript) (2009).

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

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

[44] S. Yoshiara, Disjoint unions of dimensional dual hyperovals, manuscript, May 2012.