高次元の双対弧–平面中の二次曲線から出発して

吉荒 聡 (Satoshi Yoshiara)
東京女子大学・数理学科
Department of Mathematics, Tokyo Woman's Christian University
167-8585 東京都杉並区善福寺 2-6-1
yoshiara@lab.twcu.ac.jp

1 はじめに

この概説では、高次元の双対超卵形 (dimensional dual hyperoval) という新しい研究対象に対して、そのモデルとなった射影平面上の超卵形に関する古典的な研究成果を簡単にふり返った後、古典論と同様に、この概念が「組合せ幾何学」・「群論」・「数論」という 3 つの観点を結びつける機能を持った、研究価値のある対象であることを主張したい。2005 年以前の成果に対する概説は 2004 年の Pingree Park Conference で行われた講演を集めた論文集中に存在する [27] ので、本稿では、上記 3 つの観点に関連する部分について最近の成果に重点を置いて説明する。また、双対超卵形に限定し、具体例の詳細や極空間中への埋め込み問題については省略した。国内研究集会における講演記録 (日本語） [21], [23], [25], [26], [28] を見ると、高次元の双対超卵形に関する筆者の研究の道筋がたどれる。

2 古典論

2.1 射影空間と極空間、その組み立て材料としての射影平面と GQ

有限体 $GF(q)$ (q は素数のべき）上の $n+1$ 次元ベクトル空間 V の i 次元部分空間からなる集合 V_i $(i = 1, \ldots, n)$ に、それらの包含関係により定められる結合関係 $*$ (incidence) を考え合わせたもの $\mathbf{PG}(V) = (V_1, \ldots, V_n; *)$ が、$GF(q)$ 上の（デザルグ的）**射影空間** (projective space) であった。特に $n = 2$ のとき、この構造は $GF(q)$ 上の**射影平面**と呼ばれ、V_1, V_2 に属する元をそれぞれ射影点、（射影）直線という。$U_{i-1} \subset U_{i+2}$ を満たす V の $i-1$ 及び $i+2$ 次元部分空間 U_{i-1}, U_{i+2} を固定すると、これらと結合関係にある（つまり U_{i-1} を含み U_{i+1} に含まれるような）i 次元と $i+1$ 次元部分空間の全体は $GF(q)$ 上の射影平面の構造を持っている。この意味で、射影空間は射影平面から組み立てられている。

V 上の非退化な双一次ないしは二次形式 f が与えられたとき V_i の元 W で W 上への f の制限が 0 写像になるものを f に関する全等方的 i 次元部分空間と呼ぶ。その全体のなす集合を $V_i[f]$ とすれば、i が $(n+1)/2$ を超えるときには $V_i[f]$ は空集合である。空集合でない $V_i[f]$ の集まりに射影空間 $\mathbf{PG}(V)$ を制限して得られる構造 $\mathbf{P}[f](V) := (V_1[f], \ldots, V_w[f]; *)$ $(w = (n+\varepsilon)/2,\ -1 \le \varepsilon \le 1)$ が、f に関する**極空間** (polar space) である。極空間も、上と同様な意味で、射影平面と 2 種類の対象から成る極空間（階数 2 の極空間という）か

ら組み立てられている。ここで、射影平面と階数 2 の極空間は、それぞれ、三角形と四角形の一般化といえる次のような幾何学的特性を持っていることに注意する。

射影点と射影直線を頂点とし、それらが結合関係にあるとき結ぶことにより得られるグラフを考えると、このグラフの直径（二頂点間の距離の最大値）d は、射影平面または階数 2 の極空間に応じて 3 または 4 であり、グラフの内径（自明でないサイクルの長さの最小値）は直径の 2 倍である。このような性質を持つ階数 2 の結合構造は**一般化された d-辺形** (**generalized d-gon**) と呼ばれ、射影空間（A 型の Chevalley 群が作用する）や極空間（$B, C, D, {}^2A, {}^2D$ 型の Chevalley 群が作用する）を始めとするいわゆる**建物** (**building**–Chevalley 群の放物型部分群によるコセットからなる単体複体, Tits による球面型の建物理論から始まる）は、generalized d-gon により組み立てられている。（建物が、十分多くの対象を持って有限な場合には d は $2, 3, 4, 6$ ないし 8 のどれかの値となる。）
このように射影平面と階数 2 の極空間（または一般化された 4 辺形、以下 **GQ** と略す）は、（有限無限の別なく）幾何学において基本的に重要な研究対象である。

一般化された三辺形や四辺形の定義は、点と線と呼ばれる対象からなる階数 2 の結合構造とみたとき、次のように幾何学的に表現できる。ここで、点が線と結合関係にあるときに、点は線の上にある、線は点を通る、等と言うことにし、2 点が**共線** (collinear) であるとは、これらの点を含む線が存在することを言う。

定義 1 一般化された三辺形（**射影平面**）を定義する性質：
相異なる二つの点を通るような線が唯一つ存在し、相異なる線は丁度一点で交わる。

定義 2 一般化された四辺形 *(GQ)* を定義する性質：
相異なる二つの点を通る高々一本存在する。また、線 l とその上にない点 P を指定したとき、l 上の点 Q で、P と共線なものが唯一つ存在する。

一般化された d-辺形において、一つの線上にある点の個数が一定数 $s+1$ で、一つの点を通る線の個数が一定数 $t+1$ であるとき、**位数** (**oreder**) が (s, t) であるという。$s, t \geq 2$ で d が奇数のときは常に $s = t$ であるので、この場合には位数は s と表現する。$GF(q)$ を係数とする 3 次元ベクトル空間の 1, 2 次元部分空間のなす射影平面の位数は q である。$GF(q)$ を係数とする 4 次元ベクトル空間上に定められた非退化交代形式 f に関する全等方な 1 次元と 2 次元部分空間のなす GQ は $W(q)$ と書かれるが、その位数は (q, q) である。また、$GF(q^2)$ を係数とする 4 次元ベクトル空間上に定められた非退化ユニタリ形式 f に関する全等方な 1 次元と 2 次元部分空間のなす GQ は $H(3, q^2)$ と書かれ、その位数は (q^2, q) である。

2.2 射影平面上の弧と超卵形

有限体 $GF(q)$ 上の $n+1$ 次元ベクトル空間 $V = GF(q)^{n+1}$ 上に定義された非退化な二次形式 f に関する極空間 $\mathbf{PG}(V)[f]$ を考える。この極空間が 2 種類以上の対象からなるためには、全等方的な 2 次元部分空間が必要であるから、$n \geq 3$ でなければならない。しかし、n が最も小さい値 2 のときでも、射影平面 $\mathbf{PG}(V) = \mathbf{PG}(2, q)$ において f の零点のなす集合 $V(f)$ のみを考える事も出来る。$V(f)$ の点は二次式を満たすから、どの射影

直線 l を取っても l と $V(f)$ の交点は高々 2 個の射影点からなる。$V(f)$ の持つこの幾何学的性質を取り上げて名前を付ける。

定義 3 $GF(q)$ 上の射影平面 $\mathbf{PG}(2,q)$ の点からなる集合 $\mathcal{A}$ は、次の性質を満たすとき、**弧** *(***arc***)* と呼ばれる：$\mathbf{PG}(2,q)$ の全ての射影直線 l に対して $|l \cap \mathcal{A}| \leq 2$ である。

$\mathbf{PG}(2,q)$ 中の弧は、高々 $q+2$ 個の射影点からなり、$|\mathcal{A}| = q+2$ となるのは q が偶数のときに限ることが示せる。

定義 4 $GF(q)$ 上の射影平面 $\mathbf{PG}(2,q)$ の $q+1$ 点からなる弧を**卵形** *(***oval***)*, $q+2$ 点からなる弧を**超卵形** *(***hyperoval***)* という。

q が奇数のときには、最大の点からなる弧は卵形であるが、この幾何学的性質のみから二次曲線であるという代数的性質が復元される。つまり、次の事実が言える。以下、記号 $[x,y,z]$ は非零ベクトル (x,y,z) を含む射影点 $GF(q)(x,y,z)$ を表す。

定理 5 *(Segre* の定理*)* q を奇数の素数べきとする。このとき $\mathbf{PG}(2,q)$ 中の任意の卵形 $\mathcal{O}$ に対して、適当な座標の射影変換を行えば $\mathcal{O}$ は、次の形に書ける。

$$\mathcal{O} = \{[1,t,t^2] \mid t \in GF(q)\} \cup \{[0,0,1]\}.$$

q が偶数、すなわち 2 のべきであるときには、似たような結果は出せるが、二次式とは限らない。

命題 6 $q = 2^e$ とする。このとき $\mathbf{PG}(2,q)$ 中の任意の超卵形 $\mathcal{H}$ に対して、適当な座標の射影変換を行えば $\mathcal{H}$ は、次の形に書ける。

$$\mathcal{H} = \{[1,t,f(t)] \mid t \in GF(q)\} \cup \{[0,0,1],[0,1,0]\}.$$

ここで $f(X)$ は次の性質を満たす $GF(q)$ 係数の次数 $q-2$ 以下の多項式である。

(0) $f(0) = 0$, $f(1) = 1$.

(1) $f(X)$ が誘導する写像 $GF(q) \ni x \mapsto f(x) \in GF(q)$ は全単射である。

(2) 任意の $t \in GF(q)$ に対して、$f_t(X) := (f(X+t) + f(t))/X$ により多項式 $f_t(X)$ $(\in GF(q)[X])$ が定められるが、$f_t(X)$ もまた $GF(q)$ 上の全単射を引き起こす。*(*$f_t(0) = 0$ とする。*)*

上の命題の性質 (0),(1),(2) を満たす多項式 $f(X) \in GF(q)[X]$ を、**o-polynomial** と呼ぶ。(o は oval の意であろう。) 二次式 $f(X) = X^2$ は、確かに o-多項式であるが、o-多項式はこれに限らない。例えば、$q = 2^e$, e が奇数のとき、$f(X) = X^6$ は o-多項式である。

そこで、o-多項式とはどの様なものか、果たして分類できるものなのかということが問題になる。一見、この問題は、単なる有限体上の数論の問題であり、偶標数の有限体に関する病的現象の些末な追究のようにも見えるのだが、案外奥が深くて、幾何学的対象、特に GQ との興味深い関連が見えてきている。以下、これについて概観する。

o-多項式は分類できるほど少数でないのは確かであろう。o-多項式の直接の性質については [8, Section 8] を参照されたい。ここには紹介されていないが、Glynn 氏の有用な結果 [7] もある。

2.3 Elation GQ と Kantor 族

偶標数の有限体 $GF(q)$ に対して、$GF(q)$ 上の射影平面中の超卵形という有限幾何学的な概念と $GF(q)$ 係数の o-多項式という代数的概念とは同じであった。超卵形はまた、一般四辺形という（有限）幾何での概念とも深く関連する。例えば、射影平面 $\mathbf{PG}(2,q)$, $q=2^e$, 中の超卵形 $\mathcal{H}=\{P_1,\ldots,P_{q+2}\}$ の各点 P_i $(i=1,\ldots,q+2)$ を $V=GF(q)^3$ 中の 1 次元部分空間と見て P_i によるコセット $x+P_i$ $(x\in V)$ のことを線と呼び、V のベクトルのことを点と呼び、結合関係 $*$ は包含関係により定める。 すると、点の全体 $\mathbf{P}=V$、線の全体 $\mathbf{L}=\cup_{i=1}^{q+2}(V/P_i)$ 及び $*$ からなる階数 2 の結合構造 $(\mathbf{P},\mathbf{L};*)$ は、位数 $(q-1,q+1)$ の GQ をなす事がわかる。これを Tits の GQ と呼んで $T_2^*(\mathcal{H})$ と書く。

先に GQ の例として、交代形式から得られる $W(q)$ とユニタリ形式から得られる $H(3,q^2)$ について紹介した。これら、極大全等方部分空間が 2 次元であるような交代、ユニタリ、直交形式から生じる GQ を古典的な GQ と呼ぶが、これらは十分多くの自己同型を持っている。特に、一点 P とそれを通る線のそれぞれを（全体として）動かさないような自己同型は P に関する elation と呼ばれ、重要である。

定義 7 位数 (s,t) の *GQ* $\Gamma=(\mathbf{P},\mathbf{L};*)$ とその点 P に対して、次が満たされるとき、Γ は *elation point* P に関する **elation GQ** であるという：P とそれを通る線すべてを固定するような自己同型全体のなす群 G が P と共線でない点 *(*全部で s^2t 個ある）の全体に正則（可移であり、どの自明でない自己同型も固定点を持たない）に作用する。
*(*位数 s^2t の*)*群 G のことを、点 P における **elation group** という。

古典的な GQ はすべて、任意の点に関する elation GQ である。上の定義を一見すると、elation GQ とは、ある種の代数的（群論的）条件を満たす有限幾何上の概念であるが、実は、次の結果が示すように、これは純群論的な対象である。

定理 8 *(Kantor 1980)*

(1) Γ は点 P に関する *elation GQ* で、有限位数 (s,t) を持つものとする。P での *elation group* を G とする。P と共線ではない点 Q を固定し、Q を通る Γ の線を l_i *(*$i=1,\ldots,t+1$*)* と書く。l_i 上の点で P と共線なもの（唯一つ存在する）を X_i と書く。このとき、G における点 X_i の *stabilizer* を H_i, G における線 l_i の *stabilizer* を H_i^* とすれば *(*$i=1,\ldots,t+1$*)*、$\{1,\ldots,t+1\}$ 中の任意の相異なる i,j,k に対して次が成立する。

$$|G|=s^2t,|H_i|=s,|H_i^*|=st,H_i\le H_i^*,H_i\cap H_j^*=1,H_iH_j\cap H_k=1.$$

上の条件を満たす有限群 G の部分群の族 $\{H_i,H_i^*\mid i=1,\ldots,t+1\}$ を **Kantor 族** *(***Kantor family***)*という。

(2) 逆に、*Kantor family* $\{H_i,H_i^*\mid i=1,\ldots,t+1\}$ を持つ位数 s^2t の有限群 G があれば、それから適当な点 P に対する *elation GQ* で、P における *elation group* が G であり、位数が (s,t) であるものが構成できる。

このように、「ある幾何構造をその (局所的な) 自己同型群から復元する」というアイデアに基づく研究は、射影平面に対しては、古くに Andre が行っている。射影平面において elation GQ に対応する概念は　translation plane である。7.2 章参照。

例えば、q を任意の素数のべきとし、射影平面 $PG(2,q)$ 中の卵形 $\mathcal{O}=\{H_1,\ldots,H_q\}$ をとり、それぞれの H_i を加法群 $G=GF(q)^3$ の部分群と見る。$\mathcal{O}$ は卵形 ($q+1$ 点からなる。超卵形ではない！) なので、各点 H_i における $\mathcal{O}$ の接線 H_i^* が存在する。これも G の位数 q^2 の部分群と見るとき、$\{H_i, H_i^* \mid i=1,\ldots,t+1\}$ は G における Kantor family をなし、従って位数 (q,q) の elation GQ を定める。この GQ を $T_2(\mathcal{O})$ と書く。

2.4　q-clan から出来る GQ 中に潜む卵形

上記の例では、Kantor 族を持つ有限群は可換群（ベクトル空間）であったが、一般には可換とは限らない。(しかし、ある素数 p に対する p-群であろうと予想される。) 例えば、ユニタリ形式が定める GQ $H(3,q^2)$ (位数は (q^2,q)) は任意の点に関して elation GQ であるが、その elation group は次の群 G と同型な位数 $q^5=(q^2)^2q$ の非可換群である。

$G=\{(\alpha,c,\beta) \mid \alpha,\beta\in GF(q)^2, c\in GF(q)\}$,
ここで演算は次で定める。${\alpha'}^T$ は α' の転置を表す。
$(\alpha,c,\beta)(\alpha',c',\beta')=(\alpha+\alpha', c+c'+\beta(\alpha')^T, \beta+\beta')$.

この非可換群 G の中で Kantor family を探そうという試みが Payne 及び Kantor によりなされた。彼らの結果を合わせた形で表現すると次のようになる。 そのため記号を設定しよう。$GF(q)$ の元を成分とする 2 次正方行列 A に対して、群 G の部分群 $H(A)$, $H^*(A)$ 等を次のように定める。

$H(A)=\{(\alpha,\alpha A\alpha^T,\alpha(A+A^T)) \mid \alpha\in GF(q)^2\}$,
$H(\infty)=\{(0,0,\alpha) \mid \alpha\in GF(q)^2\}$,
$H^*(A)=\{(\alpha,c,\alpha(A+A^T)) \mid \alpha\in GF(q)^2, c\in GF(q)\}$,
$H^*(\infty)=\{(0,c,\alpha) \mid \alpha\in GF(q)^2, c\in GF(q)\}$.

定理 9 *(Payne 1985+Kantor 1986)*　$\mathbf{C}$ を q 個の $GF(q)$ 成分 2 次正方行列からなる集合とする。このとき、$\{H(A),H^*(A) \mid A\in\mathbf{C}\cup\{\infty\}\}$ が、上で定義した非可換群 G の *Kantor family* をなすための必要十分条件は、どの相異なる $A,B\in\mathbf{C}$ についても次が満たされることである*:* 任意の $(0,0)\neq x\in GF(q)^2$ に対して $x(A-B)x^T\neq 0$.
この条件が満たされるとき $\mathbf{C}$ のことを **q-clan**　という。

定義 10 上の定理から、任意の *q-clan* $\mathbf{C}$ に対して、上記の非可換群 G を *elation group* とする位数 (q^2,q) の *elation GQ* が構成される。この *GQ* のことを $GQ(\mathbf{C})$ と書く。

さて、射影平面中の卵形の観点から重要なのは、q が偶数ならば、q-clan から構成できる elation GQ の中には卵形が潜んでいる、という事実である。

命題 11 *(Payne 1985)* $\mathbf{C}$ を $q=2^e$ に対する q-*clan* とする。P を GQ $GQ(\mathbf{C})$ の *elation point* とし Q を P と共線でないような $GQ(\mathbf{C})$ の点とする。このとき P と Q を含むような位数 (q,q) の部分 GQ Γ_i *(*$i=1,\ldots,q+1$*)* が $q+1$ 個存在し、Γ_i は適当な $\mathbf{PG}(2,q)$ 中の卵形 O_i に対する $T_2(O_i)$ の形をしている。

$\mathbf{PG}(2,2^e)$ 中の卵形 $\mathcal{O}$ の全ての点における接線は共通点を通り、その共通点を付け加えて $\mathcal{O}$ は一意的に超卵形 $\tilde{\mathcal{O}}$ に拡張できる。そこで、上の定理から、2^e-clan $\mathbf{C}$ が発見できれば elation GQ $GQ(\mathbf{C})$ 及びその部分 GQ $T_2(\mathcal{O}_i)$ という幾何学的構成を経て、超卵形 $\tilde{\mathcal{O}}_i$、従って $GF(2^e)$ 係数の o-多項式という数論的対象が得られる。

$$2^e\text{-clan } \mathbf{C} \to GQ(\mathbf{C}) \to T_2(O_i) \to \tilde{O}_i.$$

Example (Payne 1985) 奇数 e に対する $q=2^e$ を取り、

$$\mathbf{C}=\{\begin{pmatrix} t & t^3 \\ 0 & t^5 \end{pmatrix} \mid t\in GF(q)\}$$

とすれば、これは q-clan である。このとき、上の注意から次の o-多項式が得られる。

$$f(X)=X^{1/6}+X^{1/2}+X^{5/6}$$

ここで $1/m$ は m 乗写像 $(m=2,6)$ の逆写像に対応する整数 ($q-1$ を法とする) を表す。

上の考えを更に推し進めて、幾つかの o-多項式の無限列が得られた。実際には、小さい 2^e に対する計算機を用いた発見と推測を理論的に確かめていくという形で行われ、その一般形が発表されたのは 1996 年と 2003 年である。その具体形は上の例のように簡単に記述できないので、Penttila 氏の優れた概説 [10] を参照していただくこととし、その原理となった優れた判定条件のみを挙げる。ここに現れる超卵形のかたまり $\mathcal{H}_s$ $(s\in GF(q)\cup\{\infty\})$ を **herd** と呼ぶ。

定理 12 *(Cherowitzo-Penttila-Pinneri-Royle 1996)* $q=2^e$ とし、$GF(q)$ 上の関数 f, g で $f(0)=0=g(0)$ を満たすものに対して

$$\mathbf{C}(f,g):=\{\begin{pmatrix} f(t) & t^{1/2} \\ 0 & g(t) \end{pmatrix} \mid t\in GF(q)\}$$

とおく。また $s\in GF(q)$ に対して $f_s(t):=f(t)+(st)^{1/2}+sg(t)$,

$$\mathcal{H}_s:=\{[1,t,f_s(t)] \mid t\in GF(q)\}\cup\{[0,0,1],[0,1,0]\},$$
$$\mathcal{H}_\infty:=\{[1,t,g(t)] \mid t\in GF(q)\}\cup\{[0,0,1],[0,1,0]\}.$$

とすれば、次の条件は互いに同値である。

(i) $\mathbf{C}(f,g)$ が q-*clan.*

(ii) 全ての相異なる $s,t\in GF(q)$ に対して、$GF(q)$ の元 $(f(s)+f(t))(g(s)+g(t))/(s+t)$ の絶対トレース *(*拡大 $GF(q)/GF(2)$ に対するトレース*)* の値は 1.

(iii) すべての $s\in GF(q)\cup\{\infty\}$ に対して $\mathcal{H}_s$ は $\mathbf{PG}(2,q)$ 中の超卵形である。

2.5 古典論のまとめ

上に述べたように q-clan という概念は、重要な役割を果たしているが、やや技巧的に設定されたものという印象を与える。しかし、この概念は、射影空間 $PG(3,q)$ 中の円錐面 C を固定したとき（頂点以外の）C 上の点を分割するような q 個の平面の族という有限幾何学的概念 (**flock** という）と同値である事が知られている。また、先に触れた translation plane (elation GQ に対応する射影平面) とも深い関連がある。詳細は、論説 [10] 及び著書 [2] を参考にして欲しい。

このようにして、ある種の有限幾何学的及び群論的考察を通じて、有限体上の数論的対象である o-多項式（二次式の拡張と考えられる）がまとまって発見されたのである。平面上の二次曲線の持つ自明な幾何学的性質を抽象化しただけに見える弧、卵形、超卵形といった対象は、実は多くの概念を結びつける興味深い存在である。

そこで、射影平面中の弧（ないしは最大弧としての超卵形）という概念の高次元化を考え、この対象と、様々な有限幾何学的、群論的、数論的対象との関連を追究しようと言うのは極めて自然な成り行きである。高次元化により、代数位相幾何学的（組合せ幾何学的）論法が適用できる余地が開けることも期待された。その試みは、1996 年頃に Pasini, Huybrechts 及び筆者により開始され、「高次元の超卵形論」が進展している。これらについて語るのが次章以下の本論である。

3 高次元への一般化

3.1 基本的な定義

射影平面 $PG(2,q)$ 上の弧 $\mathcal{A}$ の双対（点と線を入れ替えたもの）$\overline{\mathcal{A}}$ を**双対弧** (dual arc) と呼ぶが、これは次の性質を満たす線の集合である。

> $\mathcal{A}$ の、どの相異なる 3 つのメンバーを取っても、それらの交わりは空集合（ベクトル空間としては零空間）である。

更に、$\mathcal{A}$ は射影平面 $PG(2,q)$ の線からなる集合であるから、

> $\mathcal{A}$ の相異なる 2 つのメンバーに対して、その交わりは射影点（ 1 次元部分空間）である。

射影平面中の射影直線に限定せずに、これらの性質だけを持つような、一定次元の部分空間の族を考えようというのが、高次元の双対弧という概念のアイデアである。

定義 13 q を素数のべき、d を 1 以上の整数とする。q 元体上の有限次元ベクトル空間 V の幾つかの $d+1$ 次元部分空間からなる族 $\mathcal{A}$ が次の 2 つの性質を満たすとき、$\mathcal{A}$ を $GF(q)$ 上の d **次元双対弧** *(d-**dimensional dual hyperoval**,* 略して *d-**dual hyperoval**)* と呼ぶ。

(DA1) $\mathcal{A}$ の、どの相異なる 2 つのメンバー X, Y を取っても、それらの交わり $X \cap Y$ は 1 次元部分空間である。

(DA2) $\mathcal{A}$ の、どの相異なる3つのメンバー X, Y, Z を取っても、それらの交わり $X \cap Y \cap Z$ は零部分空間 $\{0\}$ である。

$\mathcal{A}$ に属する部分空間全てが生成する V の部分空間 $\langle X \mid X \in \mathcal{A} \rangle$ のことを、双対弧 $\mathcal{A}$ の **ambient space** *(***生成空間***)* という。生成空間の $GF(q)$ 上のベクトル次元が $n+1$ であるとき、$\mathcal{A}$ のことを 「$PG(n,q)$ 中の d-双対弧」と表現することもある。

このとき、次の事実が確かめられる。

補題 14 $GF(q)$ 上の d-双対弧 $\mathcal{A}$ に属するメンバーの総数 $|\mathcal{A}|$ は、高々 $(q^{d+1}-1)/(q-1)$ である。

実際に、$\mathcal{A}$ から一つのメンバー X を取って固定するとき、$\mathcal{A} - \{X\}$ から X の 1 次元部分空間全体のなす集合 $PG(X)^{(0)}$ への写像 ρ を、$\rho(Y) := X \cap Y$ として定めれば、性質 (DA1) により、ρ は $PG(X)^{(0)}$ への写像であり、性質 (DA2) により、ρ は単射である。そこで、$|\mathcal{A}| - 1 \leq |PG(X)^{(0)}| = (q^{d+1}-1)/(q-1)$ を得る。

最大個数のメンバーからなる双対弧に名を与えよう。

定義 15 $GF(q)$ 上の d-双対弧 $\mathcal{A}$ は、$|\mathcal{A}| = (q^{d+1}-1)/(q-1)$ を満たすとき、d-**双対超卵形** *(*d-**dual hyperoval***)* と呼ばれる。

この概念は、射影平面上の双対弧という古典的な概念を包括する。

補題 16 $GF(q)$ 上の 1-双対超卵形 $\mathcal{H}$ の生成空間 U は 3 次元であり、$\mathcal{H}$ は、射影平面 $PG(U)$ における古典的な意味での双対超卵形である。逆に、射影平面中の古典的な意味での双対超卵形は、1-双対超卵形である。

古典論で展開されたのと同様に、この対象「高次元の双対超卵形、ないしは双対弧」が、様々な対象を結びつける中心的な役割を果たすことが期待される。実際、そのような様相が見えるというのが、本稿において筆者が主張したいことである。その定義をみれば、有限幾何学的対象であることは言うまでもないが、のみならず、組合せ幾何学的（トポロジー的）観点、群論的観点、数論的観点のそれぞれが、この対象を有効に研究する手段を与え、逆に、この対象が、それぞれの観点での問題を提供する。

多少唐突だが、まず用語を定義してしまおう。次の概念が定式化できるのは、高次元に拡張したときの最大のメリットであり、次章で見るように、これは組合せ幾何学の観点に直結する。

定義 17 $\mathcal{A}$ および $\overline{\mathcal{A}}$ を $GF(q)$ 上の d-双対弧とする。$\mathcal{A}$ の生成空間を U とし、$\overline{\mathcal{A}}$ の生成空間を $\overline{U}$ とする。U から $\overline{U}$ への $GF(q)$-半線形写像 ρ で、次の性質を持つものが存在するとき、$\mathcal{A}$ は $\overline{\mathcal{A}}$ の**被覆** *(cover)*である、$\overline{\mathcal{A}}$ は $\mathcal{A}$ の**商** *(quotient)*であるという。

(1) $\mathcal{A}$ のそれぞれのメンバー X に対して $\rho(X)$ は $\overline{A}$ に属する $\overline{U}$ の $d+1$ 次元部分空間である。

(2) $\mathcal{A} \ni X \mapsto \rho(X) \in \overline{A}$ は、（部分空間の集合としての）$\mathcal{A}$ から $\overline{\mathcal{A}}$ への全単射である。

特に、$\dim_{GF(q)}(U) = \dim_{GF(q)}(\overline{U})$ であるとき、上の条件を満たす写像 ρ が存在すれば、ρ は全単射であり、$\mathcal{A}$ と $\overline{\mathcal{A}}$ は互いの被覆となる。このとき $\mathcal{A}$ と $\overline{\mathcal{A}}$ は**同型** *(isomorphic* ないしは *equivalent)* と呼ばれる。また、d-双対弧 $\mathcal{A}$ を被覆する双対弧が $\mathcal{A}$ と同型なものに限るとき、$\mathcal{A}$ を**単連結**という。

与えられた双対弧が自分自身以外の商を持つかどうかは、次のように判定できる。

補題 18 *[24, Proposition 3.8]* $GF(q)$ 上 $n+1$ 次元のベクトル空間 U を生成空間とする $GF(q)$ 上の d-双対弧 $\mathcal{A}$ に対して、次は同値である。

(1) $2d \leq m \leq n-1$ を満たす m に対して、 $PG(m,q)$ 中の双対弧 $\overline{\mathcal{A}}$ で $\mathcal{A}$ の商となるものが存在する。

(2) U の非零部分空間 K で、全ての $\mathcal{A}$ の相異なるメンバー X, Y に対して $(X+Y)\cap K = \{0\}$ を満たすものが存在する。

定義 17 において、$\mathcal{A}$ と $\overline{\mathcal{A}}$ の生成空間 U と $\overline{U}$ が一致するとき、写像 ρ の全体を考えることにより、自然に群論的観点が提供される。

定義 19 $\mathcal{A}$ を $GF(q)$ 上の d-双対弧で生成空間が U であるものとする。U からそれ自身への全単射な半線形写像 σ *(*つまり U に付随する射影空間 $PG(U)$ の自己同型）であって、$\mathcal{A}^\sigma = \mathcal{A}$ をみたすもののことを、$\mathcal{A}$ の自己同型写像という。$\mathcal{A}$ の自己同型写像の全体が、写像の合成に関してなす群を $\mathrm{Aut}(\mathcal{A})$ と書いて、$\mathcal{A}$ の**自己同型群** *(automorphism group)* と呼ぶ。

U 上のスカラー変換全体のなす群 $Z \cong GF(q)^\times$ は、常に $\mathrm{Aut}(\mathcal{A})$ に含まれているので、文献などでは、$\mathrm{Aut}(\mathcal{A})/Z$ のことを、$\mathcal{A}$ の自己同型群と定義するものが多い。

3.2 実例

さて、高次元の双対超卵形として、どのような例があるのであろうか？ある意味ではたくさん存在する。しかし、単連結（被覆が自分自身に限る）な例として知られているものは、次のものしかない。これらについて、ここでは詳しい描写は省略する。[27, Section 5] 及びそこに与えられた文献を参照されたい。以下、自然数 d に対して $D := d(d+3)/2$ とおく。

(v) (Veronese 双対超卵形) $q = 2^e$ を任意の 2 べき、d は任意の自然数とする。このとき、Veronese 構成により $GF(q)$ 上の d-双対超卵形 $\mathcal{V}_d(q)$ で生成空間の次元が $D+1$ であるものが得られる [27, 5.2]。自己同型群は特別なメンバーを固定してしまい、$\mathcal{V}_d(q)$ 上可移ではない。

(ta) (Taniguchi 双対超卵形 [15], [16], [17]）$q = 2^e$ を任意の 2 べき、d, n は $d \geq n$ を満たす任意の自然数、σ は体の拡大 $GF(q^n)/GF(q)$ のガロア群の生成元とする。このとき、Buratti-Del Fra の変形法を修正して、Veronese 双対超卵形の変形として、$GF(q)$ 上の d-双対超卵形 $\mathcal{T}_d(q)$ で生成空間の次元が $D+1$ であるものが得られる。自己同型群は $\mathcal{T}_d(q)$ 上可移ではない。

(h) (Huybrechts 双対超卵形) d は任意の自然数とする。このとき、cap 構成を $GF(2)^{d+2}$ 中の超平面の補集合に適用して、$GF(2)$ 上の d-双対超卵形 $\mathcal{H}_d$ で生成空間の次元が $D+1$ であるものが得られる [27, 5.3]。自己同型群は、$\mathcal{H}_d$ 上に三重可移に作用する群 $2^{d+1} : SL_{d+1}(2)$ である。

(bd) (Buratti-Del Fra 双対超卵形) d は任意の自然数とする。このとき、Huybrechts 双対超卵形の変形 (deformation) として、$GF(2)$ 上の d-双対超卵形 $\mathcal{D}_d$ で生成空間の次元が $D+1$ であるものが得られる [27, 5.4]。自己同型群は、$\mathcal{D}_d$ 上に可移であるが、二重可移ではなく作用する。

(m) (Mathieu 双対超卵形) $GF(4)$ 上の 2-双対超卵形 $\mathcal{M}$ で、生成空間の次元が 6 であるものが存在する。自己同型群 $\mathrm{Aut}(\mathcal{M})$ は $\mathcal{M}$ 上に 22 次のマシュー群 (の自己同型群) を引き起こし、三重可移である [27, 5.1]。

(y) (Yoshiara 双対超卵形) d は任意の自然数とする。σ は拡大 $GF(2^{d+1})/GF(2)$ のガロア群 $\mathrm{Gal}(d+1)$ の生成元、ϕ は $GF(2^{d+1})$ 上の全単射で o-多項式で与えられるものとする。このとき、σ, ϕ の取り方に従って、$GF(2)$ 上の d-双対超卵形 $\mathcal{S}^{d+1}_{\sigma,\phi}$ で生成空間の次元が $2d+2$ ($\sigma\phi = id_{GF(2^{d+1})}$ の場合には $2d+1$) であるものが得られる [27, 5.5]。ϕ がガロア群 $\mathrm{Gal}(d+1)$ に入らないとき自己同型群は $\mathcal{S}^{d+1}_{\sigma,\phi}$ 上可移ではない。一方、ϕ がガロア群 $\mathrm{Gal}(d+1)$ に入るとき自己同型群は $\mathcal{S}^{d+1}_{\sigma,\phi}$ 上二重可移に作用する。

これらの他に、谷口氏による構成 [14],[27, 5.6] があるが、これは Veronese 双対超卵形により被覆される [29]。また、最近の筆者による構成 [32] は、Huybrechts 超卵形により被覆される (6 章を参照)。$GF(2)$ 上の双対超卵形で生成空間の次元が $2d+1$ であるものは、非常にたくさんある (7.3 章参照)。

3.3 基本的な未解決問題

射影平面 $PG(2,q)$ において、双対超卵形が存在するのは q が 2 のべきであるときに限られた。高次元の双対超卵形についても、同じ事が成立すると予想される。つまり、「$GF(q)$ 上の d-双対超卵形が存在するならば、q は 2 のべきである」と予想されているが、完全な解決を見ていない [27, 2.3]。d が偶数の時が未解決であり、従来の簡単な組合せ的論法のみでは、多分うまくいかない。

更に、$GF(q)$ 上の d-双対超卵形 $\mathcal{S}$ の生成空間の次元 (以下 $n+1$ とする) はどの範囲にあるか？という問題を考えよう [27, 2.4]。明らかに $2d \le n$ である。[24] において、「$q > 2$ ならば $n \le d(d+3)/2$」および「$q = 2$ ならば $n \le (d(d+3)/2)+2$」という成果が得られており、(q が 2 のべきで) $q > 2$ の場合には、Veronese 双対超卵形 $\mathcal{V}_d(q)$ の存在から、この上限は best bound になっている。 $q = 2$ のときにも、$n \le d(d+3)/2$ ではないかと予想されているが、示されていない。

4 組合せ幾何とのつながり

4.1 双対超卵形に付随する単体複体

定義 17 において、双対弧（超卵形）の被覆という概念を導入したが、この用語は位相幾何学における被覆の概念に由来する。

一般に高次元の双対弧 $\mathcal{S}$ から、次のようにして階数 2 の結合構造 (incidence geometry) が構成できる。$d = 1$ の場合、この構成（の双対）は Tits の GQ $T_2^*(\mathcal{H})$ に相当する（2.3 章参照)。

定義 20 $\mathcal{S}$ を $GF(q)$ 上の d-双対弧とし、その生成空間を U と書く。$\dim_{GF(q)}(U) = n$ とする。U を含む $GF(q)$ 上 $n+1$ 次元のベクトル空間 W を取り、固定する。このとき $\mathcal{S}$ の**アフィン拡大** $Af(\mathcal{S})$ とは、次のように定義される $\mathbf{P}$ *(***点**の集合と呼ぶ*)* と $\mathbf{B}$ *(***ブロック**の集合と呼ぶ*)* という 2 つの集合と、それらの間の対称的関係 $*$ から構成される構造 $(\mathbf{P}, \mathbf{B}; *)$ のことである。

> $\mathbf{P}$ は、$W \setminus U$ の 1 次元部分空間の全体からなる集合である。
> $\mathbf{B}$ は、W の $d+2$ 次元部分空間 Y で $Y \cap U$ が $\mathcal{S}$ のメンバーになるようなものの全体のなす集合である。
> $p \in \mathbf{P}$ と $B \in \mathbf{B}$ に対して $p * B$ であるのは、包含関係 $p \subset B$ があるとき、かつそのときに限るとする。

$\mathcal{S}$ が 二元体上の超卵形である場合には、そのアフィン拡大 $Af(\mathcal{S})$ は **semibiplane** となる。すなわち、次の性質を持つ。

(1) 任意の相異なる点 $p, q \in \mathbf{P}$ に対して、p と q の両方に関係するブロックが丁度 2 個存在する。

(2) 任意の相異なるブロック $B, C \in \mathbf{B}$ に対して、B と C の両方に関係する点が丁度 2 個存在する。

このとき $(\{p, q\}, \{B, C\})$ ($p, q \in \mathbf{P}$, $B, C \in \mathbf{B}$, p, q は共に B, C の双方と incident) という形の対を**線**と呼び、線の全体のなす集合を $\mathbf{L}$ と書く。

線と点及びブロックとの関係 $*$ を包含関係により定めて $Af(\mathcal{S})$ を拡張して得られる階数 3 の結合構造 $(\mathbf{P}, \mathbf{L}, \mathbf{B}; *)$ を二元体上の双対超卵形 $\mathcal{S}$ から得られる $c.c^*$-**geometry** というが、この結合構造の旗 ($\mathbf{P} \cup \mathbf{L} \cup \mathbf{B}$ の部分集合で、互いに関係する対象からなるもの) を単体複体として (次元 2 の）抽象単体複体が得られる。これを $\Delta(\mathcal{S})$ と書くことにする。次の事実が、双対超卵型に対する被覆という用語の由来である。

補題 21 $\rho : U \to \overline{U}$ が、$GF(2)$ 上の d-双対超卵形 $\mathcal{S}$ *(*生成空間は U*)*から $GF(2)$ 上の d-双対超卵形 $\overline{\mathcal{S}}$ *(*生成空間は $\overline{U}$*)*への被覆写像であれば、ρ は単体複体 $\Delta(\mathcal{S})$ から単体複体 $\Delta(\overline{\mathcal{S}})$ への被覆写像を引き起こす。

従って、二元体上の双対超卵形 $\mathcal{S}$ の被覆を調べる際には、抽象単体複体 $\Delta(\mathcal{S})$ の被覆空間を調べる事が役に立つ。このように、$\mathcal{S}$ の性質の解析に位相幾何学的な手段・観点が有効になる。これは、生成空間を射影平面に限定した古典論には見られなかった方法論である。

例えば、例 3.2 (y) における二元体上の双対超卵形 $\mathcal{S}^{d+1}_{\sigma,\sigma^{-1}}$ は、d-双対超卵形が取りうる最小の生成空間 ($2d+1$ 次元) を実現しているが、そのアフィン拡大 $Af(\mathcal{S}^{d+1}_{\sigma,\sigma^{-1}})$ は elation semibiplane とよばれる semibiplane のクラスに属することが確かめられる。このクラスに対応する抽象単体複体が単連結であることが示されているので、補題 21 から $\mathcal{S}^{d+1}_{\sigma,\sigma^{-1}}$ 自身が単連結であることがわかる [12, Theorem 1.9]。

σ,τ が共にガロア群 $\mathrm{Gal}(d+1)$ にはいる場合の Yoshiara 双対超卵形 $\mathcal{S}^{d+1}_{\sigma,\tau}$ に対する単体複体 $\Delta(\mathcal{S}^{d+1}_{\sigma,\tau})$ の普遍被覆は [13] で研究されており、d が小さいときには、多くの場合 $\Delta(\mathcal{S}^{d+1}_{\sigma,\tau})$ の普遍被覆は自分自身に一致する事が観察される。一般に d が偶数で $\sigma,\tau,\sigma\tau$ のすべてが $\mathrm{Gal}(d+1)$ の生成元であれば $\Delta(\mathcal{S}^{d+1}_{\sigma,\tau})$ は単連結であろうと予想されている。補題 21 から、予想が正しければ、これらの場合には $\mathcal{S}^{d+1}_{\sigma,\tau}$ は単連結である。

しかし、$\Delta(\mathcal{S})$ の普遍被覆空間は、ある双対超卵形 $\mathcal{T}$ に対する $\Delta(\mathcal{T})$ の形とは限らない。例えば、Huybrechts 双対超卵形 $\mathcal{H}_d$ の生成空間の次元は $d(d+3)/2$ であり、$\mathcal{H}_d$ は双対超卵形としては単連結であるが、対応する単体複体 $\Delta(\mathcal{H}_d)$ の普遍被覆は、遙かに大きな単体複体 (2^{d+1} 次元の超立方体を半分とした複体) である。そこで、双対超卵形の範疇を離れて、ベクトル空間ではなくファイバーが非可換群となる場合も許容した枠組みを定義し、そこでの普遍被覆的な対象について論じるという研究方向もある。これは、インシデンス幾何の非可換表現論と呼ばれる分野に属する。例えば Huybrechts 双対超卵形とその変形である Buratti-Del Fra 双対超卵形に関するこのような研究としては [5] を参照されたい。

4.2 Wrapping number

一般に、単体複体の被覆空間を調べるにはその基本群の計算が鍵である。2 元体上の双対超卵形 $\mathcal{S}$ に付随する単体複体 $\Delta(\mathcal{S})$ を含む、色々な結合幾何の旗のなす単体複体の基本群を計算するための様々な手段は Pasini 等により開発されている。そのうち、$\Delta(\mathcal{S})$ の基本群に直結するものではないが、有効なのが **wrapping number** と呼ばれる数を計算する方法である [11]。この数は、$Af(\mathcal{S})$ が付随する $c.c^*$-geometry のみならず、任意の $c.c^*$-geometry 及び $C_2.c$-geometry に対して定義できるが、特に二元体上の双対超卵形 $\mathcal{S}$ の同型類に対して定まる自然数 $w(\mathcal{S})$ である。その形式的な定義はやや面倒なので、ここでは述べないが、二元体上の双対超卵形 $\mathcal{S}$ の生成空間が小さい次元を持ち、メンバーの具体的な表示が扱いやすい場合には、定義に則して計算できる。$\Delta(\mathcal{S})$ に特定した場合の定義は、[12, p.531] を参照。wrapping number は次の性質を持つので、非常に便利である。

補題 22 *$GF(2)$ 上の d-双対超卵形 $\overline{\mathcal{S}}$ の wrapping number $w(\overline{\mathcal{S}})$ と、その被覆 $\mathcal{S}$ の wrapping number $w(\mathcal{S})$ は等しい。*

Yoshiara 双対超卵形 $\mathcal{S}^{d+1}_{\sigma,\tau}$ (σ,τ は拡大 $GF(2^{d+1})/GF(2)$ のガロア群 $\mathrm{Gal}(d+1)$ の生成元）に対する wrapping number は σ, τ が定める $GF(2^{d+1})$ 上の全単射関数 f_ε

$f_\varepsilon(x) := 1 + (1 + x^\varepsilon)^{\varepsilon^{-1}}$ $(x \in GF(2^{d+1}))$,
ここで $\varepsilon := (\sigma - 1)/(\tau - 1)$

に対して、f_ε^2 の位数と一致する。特に $w(\mathcal{S}^{d+1}_{\sigma,\tau}) = 1$ であるのは $\sigma = \tau$ であるとき、かつそのときに限ることが知られている [12, Proposition 3.6]。

Huybrechts 双対超卵形 $\mathcal{H}(d)$ が $\mathcal{S}^{d+1}_{\sigma,\sigma}$ を被覆することが示せるので、$w(\mathcal{H}(d)) = 1$ である。また、Veronese 写像を使って定義される Veronese 双対超卵形で二元体上で定義されるもの $\mathcal{V}_d(2)$ に対しては、この双対超卵形で被覆されるような Yoshiara 双対超卵形を選んで、その wrapping number を計算して $w(\mathcal{V}_d(2)) = 2$ を得る ([29])。

wrapping number の計算は重要であるが、次のクラス‘小さな’ d-双対超卵形に対しては、まだ行われていないと思われる。一つは $\mathcal{S}^{d+1}_{\sigma,\phi}$ で、ϕ がガロア群 $\mathrm{Gal}(d+1)$ に入らない場合である (特殊な場合には計算例あり [29])。もう一つは、次章で触れる位数 2 べきの有限 translation plane (ないしは標数 2 の有限 quasi field Q) から構成されるような $PG(2d, 2)$ 中の双対超卵形である。Yoshiara のクラスに入る場合には $\mathcal{S}^{d+1}_{\sigma,\sigma^{-1}}$ となるので、wrapping number は 3 となることが知られている。どちらの計算も、単連結性を調べる際においても何らかの情報を提供するであろう。

5 群論とのつながり–線形群と置換群

5.1 二重可移な双対超卵形の分類

生成空間 U が $n+1$ 次元の $GF(q)$ 上の d-双対超卵形 $\mathcal{S}$ の自己同型群 $\mathrm{Aut}(\mathcal{S})$ は、U 上の $GF(q)$-半線形全単射変換のなす群 $GL_{n+1}(q) : Z_e$ (ここで $q = p^e$, p 素数とする）の部分群として線形群であると同時に、$\mathcal{S}$ の $((q^{d+1} - 1)/(q - 1)$ 個の）メンバー上の置換群としての性格も持つ。$\mathrm{Aut}(\mathcal{S})$ が、$\mathcal{S}$ のメンバー上に二重可移な置換群を引き起こすことと、そのアフィン拡大 $Af(\mathcal{S})$ に付随する階数 3 の結合構造が、その極大旗の全体に可移な作用を持つことは同値である。

例えば、σ,τ がガロア群 $\mathrm{Gal}(d+1)$ の生成元であるとき、二元体上の双対超卵形 $\mathcal{S}^{d+1}_{\sigma,\tau}$ (例 3.2(y)) はメンバー上二重可移な自己同型を持つので、付随する semibiplane $Af(\mathcal{S}^{d+1}_{\sigma,\tau})$ は極大旗上可移な自己同型群を持つ。極大旗上可移な自己同型群を持つ semibiplane は、以前はごく僅かしか知られていなかったが、この構成により、非常に多くの例が知られるに至った [12]。一般に、極大旗全体の上に可移な自己同型群を持つ結合構造は、群論的にも扱いやすく、対称性の高さから来る有用性もあり、様々な研究がなされている。

この観点から、特に $\mathrm{Aut}(\mathcal{S})$ が ($\mathcal{S}$ のメンバー上に) 二重可移であるような $GF(q)$ 上の d-双対超卵形 $\mathcal{S}$ の分類が初めに試みられた [9]。結果として、$q = 2$ であるか、$(q, d) = (4, 2)$ で $\mathcal{S}$ は Mathieu 双対超卵形 (例 3.2(m)) に同型となるか、またはありそうもない場合 (q は奇数で、幾つかの条件が付く）のどれかとなることが示された。この結果は Mathieu 双対超卵形の特徴付けの一つとも見なせるが、$q = 2$ の時には自己同型群の構造その他について一切の情報を与えていない、ありそうもない場合が完全に消えていない、と言う不

満点もあった。それは、双対超卵形の自己同型群という、線形群でもあり置換群でもある群の利点を生かさずに、付随する結合構造の自己同型群のみを考えたことに由来すると考えられる。

最近、筆者は [9] の結果を更に進めて、上の「ありそうもない場合」が実際起こらないことを示し、$q = 2$ の場合の自己同型群の構造も大きく制限できることを示した [31]。特に、自己同型群 $\mathrm{Aut}(\mathcal{S})$ は「アフィン形」の二重可移群であり、$\mathcal{S}$ の 2^{d+1} 個のメンバー上に正則に作用する（基本可換 2-群である）正規部分群 N を持ち、$\mathrm{Aut}(\mathcal{S})$ は N と、一つのメンバーを固定する部分群 A の半直積 $N : A$ である。更に、有限体上の関数を用いた方法により、Yoshiara 双対超卵形の一つの特徴付けも得られ、それに従って $PG(2d+1, 2)$ 中の d-双対超卵形で、二重可移な自己同型群を持つものの分類も得られた [32]。例えば、次が示されている。

命題 23 *[32, Corollary 4]* d が偶数で $d + 1$ と $2^{d+1} - 1$ は互いに素とする。このとき、$PG(2d + 1, 2)$ 中の d-双対超卵形 $\mathcal{S}$ に対して、$\mathcal{S}$ が二重可移な自己同型群を持つことと、$\mathcal{S}$ が $\mathrm{Gal}(d + 1)$ の生成元 σ, τ に対する $\mathcal{S}^{d+1}_{\sigma,\tau}$ と同型となること、は同値である。

[32, Theorem 3] において、$PG(2d + 1, 2)$ 中の二重可移な d-双対超卵形の例外的な可能性として残されているものがある。これらの可能性における生成空間の次元は高々 6 であり、非常に制限されている。自己同型群は $\mathrm{Aut}(\mathcal{S}) = N : A$, ここで N は位数 2^{d+1} の基本可換 2-群という形であったので、A として可能な群の同型類を示す。

(1) $d = 2$ で $A \cong SL_3(2)$.

(2) $d = 3$ で $A \cong SL_2(4)$, S_5, A_6 または S_6.

(3) $d = 5$ で $A \cong SL_2(8)$, $SL_2(8).3$, $Sp_6(2)$, $G_2(2)'$ または $G_2(2)$.

これらの例のうち、(1) は実際に起こる。$\mathcal{S} = \mathcal{S}^3_{\sigma,\sigma}$ とすると $\mathrm{Aut}(\mathcal{S}^3_{\sigma,\sigma}) \cong 2^3 : SL_3(2)$ である。その他の例が本当に起こるのかどうか、検討する必要がある。本当に存在するならば、新しくしかも誠に興味深い、二重可移な双対超卵形の例が発見されたことになる。

5.2 自己同型の固定点が誘導する双対卵形

d-双対超卵形の非自明な自己同型の持つ著しい特色は、「この自己同型により固定される部分構造に、d より小さい自然数 e に対する e-次元超卵形の構造が入る」という点にある。この点もまた、射影平面中の超卵形から脱却して、高次元版を考えたことの効果である。少し制限した形でこの特色を述べよう。

定理 24 $q = 2^f$ を 2 のべきとする。$GF(q)$ 上の d-双対弧 $\mathcal{S}$ の自己同型 σ で、位数が 2 であり、$\mathcal{S}$ の生成空間 U 上に $GF(q)$-線形写像を引き起こすものを取る。もし、σ が $\mathcal{S}$ の 3 個以上のメンバーを固定するならば、$1 \le e \le d - 1$ を満たすある自然数 e に対して $GF(q)$ 上の e-双対弧 $\mathcal{S}[\sigma]$ が次のようにして構成され、$\mathrm{Aut}(\mathcal{S})$ における σ の *centralizer* は $\mathcal{S}[\sigma]$ の上の自己同型群を引き起こす。

σ が固定する $\mathcal{S}$ のメンバーのなす集合を $\mathcal{S}(\sigma)$ とし、それぞれの $X \in \mathcal{S}(\sigma)$ に対して、$C_X(\sigma) := \{x \in X \mid x^\sigma = x\}$ とする。これらを集めた集合を $\mathcal{S}[\sigma] := \{C_X(\sigma) \mid X \in \mathcal{S}(\sigma)\}$ とする。

$\mathcal{S}$ が双対超卵形であることから、involution σ が $\mathcal{S}(\sigma)$ に属するメンバー X の上に忠実に作用することが示せる。また、X は $GF(2)$ 上のベクトル空間であるから $C_X(\sigma)$ の $GF(2)$ 上の次元は少なくとも $(d+1)f/2$ 以上であることがわかる。つまり $e+1 \geq (d+1)f/2$ であるから、e が与えられれば、d の可能性は $d \leq (2(e+1)/f) - 1$ と限定される。そこで、上の結果から、あるクラスの双対超卵形の分類を行うとき、次元の小さいものから帰納的に定めていくという方法が原理的に適用できることになる。これは、有限単純群の分類が、「involution (位数 2 の元) と可換な部分群の構造を決めると、全体の単純群の構造を限定することが出来る」という原理 (Brauer-Fowler の principle) に支えられていたことと対比出来る現象である。

例えば、前章末にあげた問題の一つ、$GF(2)$ 上の 5-双対超卵形 $\mathcal{S}$ で、その自己同型群が $N : G_2(2)$ $(N \cong 2^6)$ という形のものがあるか？という問いを考察するとき、$G_2(2)$ の中の involution σ を取り ($G_2(2)$ における σ の centralizer C の可能な形は決まる)、σ が固定するメンバー（それは $C_N(\sigma)$ に対応する）から上の定理から構成される e-双対超卵形 $\mathcal{S}(\sigma)$ ($e = 1$ または 2 である）で C が作用する可能性のあるものを考察していくのである。

上の定理 24 は [22, Lemma 4] として現れ、[32, Lemma 15] ではアフィン型二重可移群に対して特定された形で有効に用いられている。上の観察の一般化や、それに伴う問題提起についての詳細は、論説 [25], [28] を参照されたい。

6 数論とのつながり–ＡＰＮ関数

6.1 APN-関数

暗号論では、平文を幾つかのブロックに分けて標数 2 の有限体上の元と見て、それらを転換するするときに、種々の攻撃に際してなるべく安全な転換法を工夫する必要がある。この転換は **S-box** (substitution box) と呼ばれているようだが、数学的には、有限体 $GF(q)$ $(q = 2^{d+1})$ からそれ自身への写像（関数）に過ぎないと考えられる。この関数が線形関数に近いとそれを破る攻撃法が存在するという理由で、暗号論では、有限体からそれ自身の写像で、なるべく線形関数から離れたものを具体的に作ることが重要である。線形関数から離れているか、どの様に測るかについては様々な考え方があるが、一つの考えとして差分関数に注目するというものがある。

つまり、有限体 $GF(q)$ 上の関数 f に対して、$t \in GF(q)^\times$ によるその差分 $f(x+t) - f(x)$ を考える。f が線形関数の場合には、これは一定値 $f(t)$ を取ってしまうので、逆に $\{f(x+t) - f(x) \mid x \in GF(q)\}$ がなるべく大きくなるものを考える。最も極端な例はすべての $t \in GF(q)^\times$ に対して $GF(q) \ni x \mapsto f(x+t) - f(x) \in GF(q)$ が全単射となるような関数 f であるが、このような関数が存在すれば、q は奇数であることが示せる。この

ような関数は、**平面関数** (planar function) と呼ばれ、この関数の存在と $GF(q) \times GF(q)$ を点集合とする、ある種のアフィン平面の存在が同値であることが知られている。

q が偶数の時には $f((x+t)+t) - f(x+t) = f(x+t) - f(x)$ であるから、$\{f(x+t) - f(x) \mid x \in GF(q)\}$ が取りうる最大値は $q/2$ である。このような場合に関数 f に名前を付ける。

定義 25 偶標数の有限体 $GF(q)$, $q = 2^{d+1}$, からそれ自身への関数 f は、任意の $t \in GF(q)^\times$ に対して $\#\{f(x+t) - f(x) \mid x \in GF(q)\} = q/2$ であるとき、**ほぼ非線形** *(***almost perfect nonlinear** 略して *APN)* であると呼ばれる。

$g(x) = x^{2^m+1}$ ($x \in GF(q)$, $q = 2^{d+1}$, m は $d+1$ と互いに素) という関数は APN 関数であり、**Gold 関数**と呼ばれている。

$GF(q)$, $q = 2^{d+1}$, の上の関数 f, g が**アフィン** (resp. **拡大アフィン**) **同値**であるとは、適当な全単射 $GF(2)$-線形写像 σ, τ と適当な $a, b \in GF(q)$（resp. 及び適当な $GF(2)$-線形写像 μ）が存在して、全ての $x \in GF(q)$ に対して

$$g(x) = f(x^\sigma + a)^\tau + x^\mu + b$$

が成立することをいう。f が APN であれば、f と拡大アフィン同値な関数も APN である。(最近、これをもっと拡張した CCZ-同値という概念があり、こちらはより自然なようだが扱いが難しいので、ここでは触れない。)

さて、ごく最近まで、APN 関数は単項式で与えられる関数に拡大アフィン同値ではないかと予想されていた。しかし、その予想を破る例が２００５年頃から発見され、APN 関数に関する関心が急速に高まっている [6],[1]。筆者は２００２年頃に $GF(2^{d+1})$ 上のある種の APN 関数が二元体上の d-双対超卵型を与えることに気付いていた (Gold 関数 x^{2^m+1} が与える双対超卵形は Yoshiara 双対超卵形の一つ $\mathcal{S}^{d+1}_{\sigma,\sigma}$, $x^\sigma = x^{2^m}$ になる) が、上の予想に災いされて、特に面白い双対超卵形につながらないと思い、それ以上の追究をすることはなかった。ところが、Carlet 氏を初めとする最近の単項式関数と非同値な APN 関数の発見により、もう一度この構成を見直すことになった。

定義 26 $GF(q)$, $q = 2^{d+1}$, 上の関数 f は、任意の $x, y, z \in GF(q)$ に対して次を満たすとき**代数的に二次** *(***quadratic***)* と呼ばれる。

$$f(x+y+z) + f(x+y) + f(y+z) + f(z+x) + f(x) + f(y) + f(z) + f(0) = 0.$$

この条件は、有限体上の関数 f が $x^{2^i+2^j}$ の形の単項式の $GF(q)$-係数の和で書けることと同値である。

最近発見された、単項式関数と非同値な APN 関数の例はみな quadratic であり、定数をシフトして $f(0) = 0$ とできる。例えば、$GF(2^{10})$ 上の関数 $f(x) = x^3 + ux^{36}$ (u は $GF(2^{10}) \setminus GF(2^5)$ の固定した元）は、単項式関数と拡大アフィン同値ではないような quadratic な APN 関数である事が知られている [6]。

6.2 Quadratic APN 関数から出来る双対超卵形

$q = 2^{d+1}$, f を $GF(q)$ 上 quadratic な APN 関数で $f(0) = 0$ を満たすものとする。このとき、$GF(2)$ 上の d-双対弧 $\mathcal{S}^{d+1}[f]$ で、生成空間の次元が $2d+2$（一応 $2d+1$ となる可能性もある）であるものが、次のように構成できる [32]。

$V = GF(q) \oplus GF(q) = \{(x, y)\ x, y \in GF(q)\}$ とおき、$GF(2)$ 上の $2d+2$ 次元ベクトル空間と見る。$x, y \in GF(q)$ に対して $b(x, y) := f(x+y) + f(x) + f(y)$ とおくと、f が quadratic で $f(0) = 0$ であることから b は V から $GF(q)$ への $GF(2)$-bilinear form であり、f が APN 関数であることから、$b(x, y) = 0$ となるのは $x = 0$ または $y = 0$ または $x = y$ であるとき、かつそのときに限る。

それぞれの $t \in GF(q)$ に対して V の $d+1$ 次元部分空間 $X(t)$ を

$$X(t) := \{(x, b(t, x)) \mid x \in GF(q)\}$$

とおき、これらを集めた集合を $\mathcal{S}^{d+1}[f] := \{X(t) \mid t \in GF(q)\}$ とする。このとき、$\mathcal{S}^{d+1}[f]$ は $GF(2)$ 上の d-双対超卵形で、その生成空間は V またはその超平面 $GF(q) \oplus H_1$ に一致することがわかる。ここで、一般に $s \in GF(q)^\times$ に対して $H_s := \{b(s, x) \mid x \in GF(q)\}$ であり、$\mathcal{S}^{d+1}[f]$ の生成空間が V と一致しないのは、全ての $s \in GF(q)^\times$ に対して $H_s = H_1$ のとき、かつそのときに限る。（このような場合は起こらないように思われるが、今のところ、一般論として排除できない。）

このようにして、任意の $GF(q)$ 上の quadratic APN 関数 f から $GF(2)$ 上の d-双対超卵形 $\mathcal{S}^{d+1}[f]$ が作れるが、その著しい特徴は、任意の $t \in GF(q)$ に対して ‘平行移動’ $\tau_t : (x, y) \mapsto (x, y + b(t, x))$ が自己同型となることである。これらの平行移動を集めた群 $T := \{\tau_t \mid t \in GF(q)\}$ は位数 2^{d+1} の基本可換 2-群で、$\mathcal{S}^{d+1}[f]$ のメンバー上に正則に作用する。実は一般に、$\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ は T を正規部分群に持ち、T とメンバー $X(0)$ の固定部分群 A の半直積であることがわかる。しかしながら、一般には A は $\mathcal{S}^{d+1}[f] \setminus \{X(0)\}$ の上には可移に作用しない。例えば [6] に現れた $GF(2^{10})$ 上の APN 関数 $f(x) = x^3 + \omega x^{36}$ (ω^3 は $GF(2^{10})$ の位数 3 の元）に対しては、$\mathrm{Aut}(\mathcal{S}^{10}[f]) \cong 2^{10} : (Z_{33}.Z_5)$ という形である [32]。

上の例は、厳密には新しい双対超卵形ではない。というのは、$\mathcal{S}^{d+1}[f]$ は Huybrechts 双対超卵形 $\mathcal{H}_d$ により被覆されることが示せるからである。しかしながら、これは、$GF(2)$ 上の生成空間の次元が $2d+2$ であるような d-双対超卵形の新しい例を多く与える。例えば、例 3.2 のうち、生成空間の次元が $2d+2$ であるような $GF(2)$ 上の d-双対超卵形は Yoshiara 双対超卵形 $\mathcal{S}^{d+1}_{\sigma,\phi}$ であるが、ϕ がガロア群 $\mathrm{Gal}(d+1)$ に入らなければ、$\mathrm{Aut}(\mathcal{S}^{d+1}_{\sigma,\phi})$ は $\mathcal{S}^{d+1}_{\sigma,\phi}$ のメンバーの上に可移に作用しないので、特に $\mathcal{S}^{d+1}[f]$ とは同型ではない。そこで、$\mathcal{S}^{d+1}[f]$ が $\mathcal{S}^{d+1}_{\sigma,\phi}$ と同型であるならば、$\phi = \tau$ は $\mathrm{Gal}(d+1)$ に入る。$\mathcal{S}^{d+1}_{\sigma,\tau}$ の中で、Huybrechts 双対超卵形で被覆されるものは $\sigma = \tau$ に限ることが、wrapping number を計算して示されているので、$\mathcal{S}^{d+1}_{\sigma,\tau}$ が APN 関数 f に付随する超卵形 $\mathcal{S}^{d+1}[f]$ と同型になるのは、$\sigma = \tau$ のときに限るのである。

ともかく、上の構成は、APN 関数とあるクラスの二元体上の双対超卵形のつながりを示している。アフィン同値な APN 関数からは同値な超卵形が構成されることも示せる。今の段階では、APN 関数の構成について、超卵形の理論から貢献できることはないが、

Huybrechts 双対超卵形の商は多数存在するので、（将来的には）単項式関数と同値でない quadratic APN 関数の存在を示すのに、超卵形の同型類を用いたアプローチが考えられるように思われる。

7 有限幾何学的対象との関連–translation plane, GQ

7.1 Generalized quadrangle

$d = 1$ に対する古典的な 1-双対超卵形は、generalized quadrangle という（有限）幾何学的な対象と密接な関係にあった。4.1 章で定義した、二元体上の d-双対超卵形 $\mathcal{S}$ のアフィン拡大 $Af(\mathcal{S})$ から定義される階数 3 の (3 種類の対象からなる）結合構造は $c.c^*$-geometry と名付けられていたが、これは、$C^2.c$-geometry と呼ばれる generalized quadrangle の拡張になっている階数 3 の構造と関連する [11]。$C_2.c$-geometry においては、一つの'ブロック' を固定したとき、それと incident な点及び線が generalized quadrangle の構造を持っている。 実は、あるクラスの高次元の双対弧（双対超卵形ではない）のアフィン拡大として、$C_2.c$-geometry を作り出すことが出来る。このような双対弧は **Y-族**と呼ばれており、興味深い研究対象であるが、ここでは詳細は省く。[27, Section 6] とそこに引用された文献等を参照されたい。

7.2 Translation plane

アフィン平面 A から出発して、直線の平行類を無限遠点、その全体を無限遠線 l_∞ として、A を射影平面 $\mathbf{P}(A)$ に埋め込むことが出来る。この射影平面の自己同型ですべての無限遠点を固定するが A の点を固定しないものを **translation** という。Translation の全体と恒等写像のなす群 T が、A の点上に可移に作用するとき、A を **translation plane**, T をその **translation group** と呼ぶ。

Translation plane A があると、A の点集合はある集合 Q の直積 $Q \times Q$ の形に表現でき、しかも、アフィン平面としての構造から集合 Q の上に二種類の演算 $+$ と $*$ が定義できて、この演算に関して Q は **quasi field** の構造を持つ。すなわち、$(Q; +)$ は可換群で、$*$ と $+$ は右側分配律を満たし、零元は $*$ に関して零として働き、$*$ に関する単位元が存在し、任意の $a, b, c \in Q$, $a \neq 0$, $a \neq b$ に対して $a * x = b$ を満たす $x \in Q$ ならびに $x * a - x * b = c$ を満たす $x \in Q$ が、それぞれ一意的に存在する。

逆に、quasi field Q から出発して translation plane $A(Q)$ を次のように構成できる。点集合を $Q \times Q$, それぞれの $m, b, c \in Q$ に対して $l(m, b) := \{(x, x * m + b) \mid x \in Q\}$, $l(c) := \{(c, x) \mid x \in Q\}$ とおいて、線の集合を $\{l(m, b), l(c) \mid m, b, c \in Q\}$ とし、結合関係は包含関係で定める。

そこで、quasi field という代数的な概念と translation plane という（群作用付きの）組合せ論的概念は同じものであるが、更に、この概念は可換群 G の（２個以上の）部分群からなる族 $\{H\}$ で、$\{H \setminus \{1\}\}$ が $G \setminus \{1\}$ の分割を与えるもの（G の **spread** という）という概念と同じものであることも知られている。Translation plane A の translations の

なす群 T は可換群であり、無限遠点 p の固定部分群 T_p からなる部分群の族 $\{T_p\}$ は T の spread である。逆に、この spread から translation plane A が復元できる。

Quasi field $(Q;+,*)$ に対して、Q の部分集合 K で $(K;+,*)$ が可換体の構造を持つもののうち、最大のものが定義できる。これを Q の **kernel** といい、$K(Q)$ と書く。Q は $K(Q)$ 上のベクトル空間の構造を持つので、Q が有限であれば、translation plane $A(Q)$ の点集合 $Q\times Q$ は、$K(Q)$ 上 $2\dim_{K(Q)}(Q)$ 次元のベクトル空間になり、原点 $(0,0)$ を含む線 $l(m,0)$ $(m\in Q)$ および $l(0)$ は $\dim_{K(Q)}(Q)$ 次元の部分空間である。

7.3 ある translation plane のクラスを用いた $PG(2d,2)$ 中の d-双対超卵形の構成

Q を有限な quasi field とし、その kernel $K(Q)$ が二元体 $GF(2)$ を含むとする。このとき、$K(Q)$ 上のベクトル空間 Q は二元体上のベクトル空間と見なせるが、その次元 $dim_{GF(2)}(Q)$ を $d+1$ とする。このとき、Q の非零元 v の取り方に応じて、二元体 $GF(2)$ 上の d-双対超卵形で、生成空間の次元が $2d+1$ であるものが、次のように構成できる。この観察は、谷口氏 [18], [19] による。

Translation plane $A(Q)$ の原点を通る直線の族 $\{l(m,0),l(0)\mid m\in Q\}$ は、$|Q|+1=2^{d+1}+1$ 本の直線からなり、ベクトル空間 $A(Q)$ の ($GF(2)$ 上の $d+1$ 次元) 部分空間による分割を与える、この直線のうち v を含むものを l_∞, 残りを l_i $(i=1,\dots,2^{d+1})$ と書くことにする。剰余ベクトル空間 $U:=(Q\times Q)/\{0,v\}$ を考え、標準的な準同型を $\rho:(x,y)\mapsto(x,y)+\{0,v\}$ とする。このとき、ρ による l_i の像のなす族 $\mathcal{S}(Q,v):=\{\rho(l_i)\mid i=1,\dots,2^{d+1}\}$ は、$GF(2)$ 上の d-双対超卵形をなすことが確かめられる。その生成空間は U, $\dim_{GF(2)}(U)=2d+1$ である。

この構成は、生成空間の次元が最小値 $2d+1$ であるような $GF(2)$ 上の d-双対超卵形という概念が、位数が 2 べきの有限 translation plane、同じ事だが標数 2 の quasi field という概念を包括している事を示す。上の具体的な構成を利用した谷口氏の計算例を見ると、非同型な quasi field から、非同型な $PG(2d,2)$ 中の d-双対超卵形が構成されると期待される。一方、quasi field は非常に多くの同型類を持つ（その部分類をなす semifield に限定しても、大きさが 2^{d+1} の semifield の同型類の個数 $f(d+1)$ は $d+1$ の多項式では書けない程多くあると予想されている）ので、上の構成は、$PG(2d,2)$ 中の双対超卵形は「非常に多く」存在する事を示す。

更に、注意することは、d-双対超卵形 $\{\rho(l_i)\}$ のメンバー全体の合併 $\cup_{i=1}^{2^{d+1}}\rho(l_i)$ の U における補集合に $\{0\}$ を付け加えれば、U の d 次元部分空間 $\rho(l_\infty)=l_\infty/\langle v\rangle$ が得られる点である。一般に、生成空間の次元が $2d+1$ であるような $GF(2)$ 上の d-双対超卵形に関して、そのメンバーの合併の補集合に $\{0\}$ を付け加えれば、生成空間の d 次元部分空間が得られる [3], [4]. 生成空間の次元が $2d+1$ であるような $GF(2)$ 上の d-双対超卵形のうち、上のように構成されるものがどの程度あるのかは調べるべきであろう。

一方、$q>2$ の場合、$PG(2d,q)$ 中の d-双対超卵形については、殆ど研究がされていない。$PG(4,4)$ 中の 2-双対超卵形の分類すらも、知られていないようである。

References

[1] L. Budaghyan, C. Carlet, P. Felke and G. Leander, An infinite class of quadratic APN functions which are not equivalent to power mappings, Proceedings of the IEEE International Symposium on Information Theory 2006, Seattle, USA, Jul. 2006.

[2] I. Cardinali and S. E. Payne, q-Clan Geometries in Characteristic 2, Frontiers in Math., Birkhäuser, 2007.

[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, Geom. Dedicata, 79 (2000), 157–178.

[5] A. Del Fra and A. Pasini, The universal representation group of Huybrechts's dimensional dual hyperoval, Innov. Incidence Geom. 3 (2006), 121–148.

[6] Y. Edel, G. Kyureghyan and A. Pott, A new APN function which is not equivalent to a power mapping, IEEE Trans. Inform. Theory, 52 (2006), 744–747.

[7] D. G. Glynn, Two new sequences of ovals in finite Desarguesian planes of even order, Combinatorial Math. X, Springer Lecture Notes in Math. 1063 (1983), 217–229.

[8] J. W. P. Hirschfeld, Projective Geometries over Finite Fields, 2nd edn, Oxford Mathematical Monographs, Clarendon Press, Oxford, 1998.

[9] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, Contrib. Algebra Geom. 40 (1999), 503–532.

[10] T. Penttila, Applications of computer algebra to finite geometry, pp.203–221, in: Finite Geometires, Groups, and Computation, eds. A. Hulpke, B. Liebler, T. Penttila, and A. Seress, Walder de Gruyter, Berlin-New York, 2006.

[11] A. Pasini and G. Pica, Wrapping polygons in polygons, Ann. Comb. 2(1998), 325–349.

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

[13] A. Pasini and S. Yoshiara, New distance regular graphs arising from dimensional dual hyperovals, European J. Combin. 22 (2001), 547–560.

[14] H. Taniguchi, A family of dual hyperovals over $GF(q)$ with q even, Europ. J. Combin. 26 (2005), 195–199.

[15] H. Taniguchi, On d-dual hyperovals in $PG(d(d+3)/2, 2)$, Electronic Notes in Discrete Math. 26 (2006), 131–138.

[16] H. Taniguchi, A new family of dual hyperovals in $PG(d(d+3)/2, 2)$ with $d \geq 3$, to appear in Disctere Math., special issue devoted to the conference "Combinatorics 2006".

[17] H. Taniguchi, On automorphism of some d-dimensional dual hyperovals in $PG(d(d+3)/2, 2)$, submitted for publication.

[18] H. Taniguchi, On d-dimensional dual hyperovals in $PG(2d, 2)$ coming from finite translation affine planes, 第 24 回代数的組合せ論シンポジウム報告集 (June 28–30, 2007, Kinki Univ., Osaka), to appear.

[19] H. Taniguchi, On d-dimensional dual hyperovals in $PG(2d, 2)$ coming from finite translation affine planes, submitted for publication.

[20] H. Taniguchi and S. Yoshiara, On the dimensional dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\phi}$, Innov. Incidence Geom. 1 (2005), 197–219.

[21] S. Yoshiara, Higher dimensional dual hyperovals, 第 15 回代数的組合せ論シンポジウム報告集 (June 22–25, 1998, Kanazawa Univ., Kanazawa), p.115–127, December, 1998.

[22] S. Yoshiara, A family of d-dimensional dual hyperovals in $PG(2d+1, 2)$, Europ. J. Combin. 20 (1999), 589–603.

[23] S. Yoshiara, 高次元の双対弧の構成とその埋め込み次元, 第 19 回代数的組合せ論シンポジウム報告集 (July 1–3, 2002, Kumamoto Univ., Kumamoto), p.77–86, December, 2002.

[24] S. Yoshiara, Ambient spaces of dimensional dual arcs, J. Alg. Combin. 19 (2004), 5–23.

[25] S. Yoshiara, 極空間中の双対弧, 第 21 回代数的組合せ論シンポジウム報告集 (June 28–30, 2004, Shinshu Univ., Matsumoto), p.57–68, October, 2004.

[26] S. Yoshiara, 高次元の双対弧 — 平面上の二次曲線の高次元化, 第 22 回代数的組合せ論シンポジウム報告集 (June 29–31, 2005, Ehime Univ., Matsuyama), to appear.

[27] 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.

[28] S. Yoshiara, Dimensional dual hyperovals admitting large automorphism groups, 数理研研究集会「群論とその周辺」報告集 (December 18–21, 2006, Kyoto Univ.), to appear.

[29] S. Yoshiara, Note on Taniguchi's dimensional dual hyperovals, Eur. J. Combin. 28 (2007), 674–684.

[30] S. Yoshiara, Dimensional dual hyperovals with doubly transitive automorphism groups, to appear in Eur. J. Combin.

[31] S. Yoshiara, A characterization of a class of dimensional dual hyperovals with doubly transitive automorphism groups and its applications, submited for publication.

[32] S. Yoshiara, Dimensional dual hyperovals associated with quadratic APN functions, submited for publication.

2007 年 10 月 10 日提出