数理解析研究所講究録
第 1687 巻 2010 年 110-117

Geometric and algebraic structures related to highly nonlinear functions

S. Yoshiara
Department of Mathematical Sciences
Tokyo Woman's Christian University

This article is obtained by editing the slides of my talk given at the conference.

1 Summary

Throughout this talk,

F is a finite field of p^n elements with p a prime number,
V is the vector space underlying F (so V is of dimension n over $\mathbb{F}_p$).

We consider two classes of functions on V, called **planar**(or **nonlinear** (**NL**)) and **almost pefectly nonlinear** (**APN**), defined only when $p=2$.

With each of these functions, an algebraic structure and some geometric stuctures are associated. For a planar function, the associated geometric structure is an affine plane with some transitivity. The associated algebraic structure is commutative **presemifield** iff the function is **Dembowski-Ostrom**(DO).

For an APN function, the associated geometric structure is a semibiplane. The associative algebraic structure is distributive iff the function is **quadratic**. For a quadratic APN function, we may associate another geometric structure, a certain dimensional dual hyperoval over $\mathbb{F}_2$ with second smallest ambient space.

Algebraic structures associated with planar (resp. APN) functions are realized as the epimorphic images of a vector space $W:=(V\otimes V)/A(V)$ (resp. $(V\otimes V)/S(V)\cong A(V)$). The corresponding kernel K is a subspace of W of codimension n in W and contains no vectors corresponding to lines (1-dimensional subspaces) of V.

Exhausting DO PN (resp. quadratic APN) functions up to EA-equivalence is essentially equivalent to finiding all such subspaces K up to the diagonal action of $GL(V)$.

I discuss explicit descriptions of $(V\otimes V)/S(V)\cong A(V)$ which seems efficient to examine such subspaces. My final aim is to establish the following statement:

Conjecture 1 *The number of such subspaces grows exponentially as n is getting larger.*

2 Highly Nonlinear Functions

2.1 Planar(or PN) and APN functions

For a function f on V and $0\neq a\in V$, consider the map $\delta(f)_a$ on V defined by $\delta(f)_a(x):=f(x+a)-f(x)$.

If f is linear, then $\delta(f)_a$ takes a single value $f(a)$, namely, $|\delta(f)_a(V)|=1$ for every $0\neq a\in V$. So the opposite property to the linearity is that $|\delta(f)_a(V)|$ is large as possible for every $0\neq a\in V$. Observe that $|\delta(f)_a(V)|\leq|V|$ if p is odd, and $|\delta(f)_a(V)|\leq|V|/2$ if $p=2$, because $\delta(f)_a(x+a)=\delta(f)_a(x+a)$ $(x\in V)$ in this case.

Definition 1 *With the previous notation,*

- f *is called* **planar** *(or* **perfect nonlinear** *(***PN***))* *if* $|\delta(f)_a(V)| = |V|$. *Equivalently,* $\delta(f)_a$ *is bijective for every* $0 \neq a \in V$.
- f *is called* **almost perfect nonlinear** *(***APN***)* *if* $|\delta(f)_a(V)| = |V|/2$. *Equivalently,* $\delta(f)_a$ *is a two to one map for every* $0 \neq a \in V$.

It can be shown that if there exits a PN function on V then p is odd.

2.2 Examples of APN functions

The following maps are APN on $F \cong \mathbb{F}_{2^n}$ for every n.

$$\begin{aligned} g(x) &= x^{2^e+1} \text{ with g.c.d.(e, n)} = 1, \\ f(x) &= x^3 + \sum_{i=0}^{n-1} x^{2^i}. \end{aligned}$$

The second one was found around 2007. Including this family, several infinite series of APN functions are constructed recently (see e.g. [1, Table 2]). The following is the first example of a quadratic APN map which is not graph-equivalent to any monomial map.

Example 1 *[4] On* $F \cong \mathbb{F}_{2^{10}}$, $f(x) = x^3 + ux^{36}$ $(u \in F)$ *is APN iff* $u \in \omega K^\times \cup \omega^2 K^\times$, *where* $K = \mathbb{F}_{2^5}$ *and* $\omega^3 = 1 \neq \omega \in K$.

2.3 Graph and Extended affine equivalences

Let f and g be functions on V.

Definition 2 *We say that* f *is* **graph-equivalent** *(or* **CCZ-equivalent***) to* g *if there are* $\mathbb{F}_p$*-linear maps* α, β, γ *and* δ *on* V *and* $c, d \in V$ *s.t.* $(x, y) \mapsto (x^\alpha + y^\gamma, x^\beta + y^\delta) + (c, d)$ *is a bijection on* $V \oplus V$ *sending* $\Gamma_f = \{(x, f(x)) \mid x \in V\}$ *to* Γ_g.

If we may take $\gamma = 0$ *in the above,* f *is called* **extended affine** *(***EA***)***-equivalent** *to* g. *Thus* f *is EA-equivalent to* g *if* $g(x^\alpha + c) = x^\beta + d + f(x)^\delta$ *for every* $x \in V$.

2.4 Some properties on equivalence

Proposition 1 (Some properties on equivalence) *If* f *is PN (resp. APN), then a function* g *graph-equivalent to* f *is PN (resp. APN).*
If p *is odd, then a function graph-equivalent to* f *is also EA-equivalent to* f. *If* f *is DO, then any function EA-equivalent to* f *is DO.*

Thus in odd characteristic case, the concept of graph-equivalence coincides with that of EA-equivalence. If $p = 2$, there are examples of graph-equivalent APN functions which are EA-inequivalent.

2.5 DO functions and quadratic functions

Definition 3 *A function f on a field $F \cong \mathbb{F}_{p^n}$ is called* **Dembowski-Ostorm(DO)***, if f is represented by a polynomial in $F[X]$ of shape*

$$a + \sum_{i=0}^{n-1} a_i X^{p^i} + \sum_{0 \le i < j \le n-1} a_{ij} X^{p^i + p^j}.$$

If $p = 2$, a DO function is referred to as a **quadratic** *function.*

3 Structures associated with planar functions

3.1 A geometric interpretation of a planar function

Let f be a function on V. Define an incidence structure $\mathbb{I}(f)$ as follows: the set of **points** is $V \oplus V$, and the set of **lines** is $\{L(a,b), L(c) \mid a,b,c \in V\}$, where $L(a,b)$ and $L(c)$ are just symbols indexed by $(a,b) \in V^2$ and $c \in V$. Incidence is given by $(x,y) \in L(a,b)$ iff $y - b = f(x-a)$, and $(x,y) \in L(c)$ iff $x = c$.

The following is easy to verify (e.g.[2]).

Proposition 2 (A geometric interpretation of a PN function) *Let f be a function on V. Then f is PN iff $\mathbb{I}(f)$ is an affine plane.*

3.2 Algebraic structure associated with a DO planar function

For a function f on V and $0 \neq a \in V$, we consider the following structure on V.

Definition 4 (Algebraic structure $\mathbb{A}(f)$) *$\mathbb{A}(f) := (V; +, \circ_f)$, where $\circ_f = \circ$ is an operation on V defined by $x \circ y := f(x+y) + f(x) + f(y) + f(0)$ $(x, y \in V)$.*

If f is DO and planar (so p is odd), then the algebraic structure $\mathbb{A}(f)$ is a commutative **presemifield**, whose definition will be given below (notice that this definition involves the even characteristic case).

Definition 5 *A* **presemifield** *V is a set with operations $+$ and $\circ$, satisfying:*

(S1) *$(V, +)$ is a group with identity element 0.*

(S2) *$x \circ (y+z) = x \circ y + x \circ z$ and $(x+y) \circ z = x \circ z + y \circ z$ for all $x, y, z \in V$.*

(S3) *$x \circ y = 0$ implies $x = 0$ or $y = 0$.*

Let f be a DO planar function on V. Then (S2) follows from the assumption that f is DO. (S3) is equivalent to the condition that $\delta_y(f) = f(x+y) + f(y) = f(x) + f(0)$ has a single solution x for each $0 \neq y \in V$, which is the definition of a PN function.

3.3 Coulter-Henderson's result

In fact, Coulter-Henderson showed that the concept of commutative presemifields with p odd is equivalent to the concept of DO planar functions. See [2] for the details.

4 Structures associated with APN functions

4.1 Geometric interpretation of APN functions

Let f be a function on V. Define an incidence structure $\mathbb{I}(f)$ as follows: the set of **points** is $V \oplus V$, and the set of **blocks** is $\{B(a,b) \mid a,b \in V\}$, where $B(a,b)$ is just a symbol indexed by $(a,b) \in V^2$. Incidence is given by $(x,y) \in B(a,b)$ iff $y - b = f(x-a) + f(0)$. (Notice the similarity of the incidence to that of $\mathbb{A}(f)$ for PN functions.)

Proposition 3 *[9] For a function f on V, f is APN iff the incidence structure $\mathbb{I}(f)$ is the incidence graph of a* **semibiplane**. *Two APN functions f and g are graph-equivalent iff $\mathbb{I}(f)$ is isomorphic to $\mathbb{I}(g)$ as graphs.*

The later part of the proposition was observed by several researchers, including Dillon and Pott [6]. Here we recall a formal definition of a semibiplane.

Definition 6 *An incidence structure $(\mathcal{P}, \mathcal{B}; *)$ is called a* **semibiplane** *if for any two distinct elements in $\mathcal{P}$ (resp. $\mathcal{B}$) there are exactly 0 or 2 elements of $\mathcal{B}$ (resp. $\mathcal{P}$) incident with both of them, and its incidence graph is connected, where the incidence graph of $(\mathcal{P}, \mathcal{B}; *)$ is the graph on $\mathcal{P} \cup \mathcal{B}$ in which two vertices are ajacent if the corresponding elements are incident in $(\mathcal{P}, \mathcal{B}; *)$.*

4.2 A geometric interpretation of quadratic APN functions

Theorem 1 *[8] Let f be a function on V with $\dim(V) = n$ over $\mathbb{F}_2$. Then f is quadratic APN iff the associated structure $\mathcal{S}[f]$ is a* **DHO** *over $\mathbb{F}_2$ (with ambient space of dimension $2n$ if $n \geq 3$). Two quadratic APN functions f and g are extended affine equivalent iff $\mathcal{S}[f]$ is isomorphic to $\mathcal{S}[g]$ as dimensional dual hyperovals.*

We recall a formal definition of a DHO (dimensional dual hyperoval).

Definition 7 *A collection $\mathcal{S}$ of $(d+1)$-dimensional subspaces of a vector space W over $\mathbb{F}_q$ is called a d-***dimensional dual hyperoval** *(***DHO***) over $\mathbb{F}_q$, if any two distinct members of $\mathcal{S}$ intersect at a 1-dimensional subspace, any three mutually distinct members of $\mathcal{S}$ intersect at the zero subspace, and $|\mathcal{S}| = ((q^{d+1}-1)/(q-1)) + 1$.*

A subspace of W spanned by all members of $\mathcal{S}$ is called the **ambient space** *of $\mathcal{S}$.*

5 Universal algebraic observations

In the algebraic structure $\mathbb{A}(f)$ defined for a function f on F (or its underlying space V), the multiplication $\circ$ is given by $x \circ y = f(x+y) + f(x) + f(y) + f(0)$. In particular, $\circ$ is commutative: $x \circ y = y \circ x$.

If f is DO, then $\circ$ satisfies the left and the right distributive lows. If f is PN (so that p is odd), then $x \circ y = 0$ iff $x = 0$ or $y = 0$. Remark in this case, $x \circ x \neq 0$ for $x \neq 0$. If f is APN (so that $p = 2$), then $x \circ y = 0$ iff $x = 0$ or $y = 0$ or $x = y$.

Summarizing, we have

Proposition 4 (Algebraic structures for PN and APN functions) *Assume that f is a function defined on a finite vector space V over $\mathbb{F}_p$ with p odd (resp. $p = 2$). Then f is DO and PN (resp. quadratic APN) iff algebraic system $\mathbb{A}(f)$ satisfies the following (A1)-(A4) (resp. (A1),(A2),(A3') and (A4)):*

(A1) $(V; +)$ *is a vector space over* $\mathbb{F}_p$.

(A2) $\circ$ *is left and right distributive.*

(A3) $x \circ y = 0$ *if and only if* $x = 0$ *or* $y = 0$.

(A3') $x \circ y = 0$ *if and only if* $x = 0$ *or* $y = 0$, *or* $x = y$.

(A4) $\circ$ *is symmetric.*

If f is DO PN (so p is odd), the axioms (A1)-(A4) are nothing more than axioms for commutative presemifield.

In the rest of this section, we consider an arbitrary algebraic structure $(V; +, \circ)$ satisfying either axioms (A1)-(A4) (so it is just a commutative semifield) or axioms (A1),(A2),(A3') and (A4). This algebraic consideration allows us to involve commutative presemifields in characteristic $p = 2$. This also makes clear the relation between commutative semifields in characteristic 2 and the algebraic structure corrresponding to quadratic APN functions.

By axiom (A3) (resp. $(A3')$) and (A4), the form $V \times V \ni (x, y) \mapsto x \circ y \in V$ is an **symmetric** (resp. **alternating**) bilinear map on V. From the universality of tensor product, there is an $\mathbb{F}_p$-linear surjection $\tilde{\rho}$ from $V \otimes V$ onto V such that $\tilde{\rho}(x \otimes y) = x \circ y$ for all $x, y \in V$.

As $\circ$ is symmetric, $\tilde{\rho}$ vanishes on the subspace $A(V)$ of $V \otimes V$ consisting of $x \oplus y + y \oplus x$ for **distinct** $x, y \in V$: $A(V) := \langle x \otimes y + y \otimes x \mid x, y \in V \rangle$. (Notice that $x \otimes x + x \otimes x = 0$ for $x = y$, if $p = 2$.) Thus $\tilde{\rho}$ induces a surjective linear map ρ from $V \otimes V/A(V)$ onto V.

If f is quadratic APN, $\circ$ vanishes on the larger subspace $S(V)$ of $V \otimes V$ spanned by $A(V)$ and $V^{(2)} = \{x \otimes x \mid x \in V\}$: namely, $S(V) = \langle x \otimes y + y \otimes x, x \times x \mid x, y \in V \rangle$. Thus $\tilde{\rho}$ induces a surjective linear map ρ from $V \otimes V/S(V)$ onto V.

The kernel $K := \mathrm{Ker}(\rho)$ has codimension n in $(V \otimes V)/A(V)$ or $(V \otimes V)/S(V)$, according as $\circ$ satisfies (A1)-(A4) or (Ai) ($i = 1, 2, 4$) and (A3'). Moreover, K has the following property by axiom (A3), where $x \otimes y$ ($\in V \otimes V$) is identified with its image $(x \otimes y) + A(V)$ in $(V \otimes V)/A(V)$:

$$K \cap \{x \otimes y \mid x, y \in V\} \quad = \quad \{0\}.$$

If f is quadratic APN, then the following property follows from (A3'), where $x \otimes y$ ($\in V \otimes V$) is identified with its image $(x \otimes y) + S(V)$ in $(V \otimes V)/S(V)$: (notice that as $x \otimes x \in V^{(2)}$, we only need $x \otimes y$ for **distinct** $x, y \in V$.)

$$K \cap \{x \otimes y \mid x \neq y \in V\} \quad = \quad \{0\}.$$

Conversely, if a subspace K of $W := (V \otimes V)/A(V)$ satisfies

$$\mathrm{codim}(K) = \dim(W) - \dim(K) = n \text{ and } K \cap \{x \otimes y \mid x, y \in V\} = \{0\}.$$

then the operation $\circ$ on $(V;+)$ defined by $x \circ y := \alpha((x \otimes y) + K)$ for $x, y \in V$ satisfies the axiom of a commutative presemifield, where α is any isomorphism of W/K with V.

Similar conclusion holds for $\bar{W} := (V \otimes V)/S(V)$. Namely, if a subspace K of $\bar{W} := (V \otimes V)/S(V)$ satisfies the following two properties

$$\mathrm{codim}(K) = \dim(\bar{W}) - \dim(K) = n \text{ and } K \cap \{x \otimes y \mid x \neq y \in V\} = \{0\}.$$

then the operation $\circ$ on $(V;+)$ defined by $x \circ y := \alpha((x \otimes y) + K)$ for $x, y \in V$ satisfies the axioms (A1),(A2),(A3') and (A4), where α is any isomorphism of $\bar{W}/K$ with V.

A canonical form of quadratic APN functions

5.1 Canonical form of a quadratic APN function

Now we return to the case when $\circ = \circ_f$ is detemined by a quadratic function f on V: $x \circ_f y = f(x+y) + f(x) + f(y) + f(0)$. Notice that $\circ_f$ coincides with $\circ_g$ iff $f + g$ is an affine function on V. Hence the conclusion of previous section shows the following canonical description of quadratic APN functions, beacuse $A(V)$ can be identified with $(V \otimes V)/S(V)$ via $x \wedge y \mapsto x \otimes y + S(V)$.

This result was first obtained by examining the universal DHO of $\mathcal{S}[f]$.

Let Γ be the set of all $\mathbb{F}_2$-linear surjections γ from $A(V)$ to V with $\mathrm{Ker}(\gamma) \cap \{a \wedge b \mid a, b \in V\} = \{0\}$, and let Af be the set of $\mathbb{F}_2$-affine maps on V. Fix a basis $\{e_i\}_{i=1}^n$ for V over $\mathbb{F}_2$. For every (γ, α) of $\Gamma \times Af$, the following map $f_{\gamma,\alpha}$ is quadratic APN on V:

$$f_{\gamma,\alpha} : a = \textstyle\sum_{i=1}^n a_i e_i \mapsto \sum_{1 \leq i < j \leq n} a_i a_j (e_i \wedge e_j)^\gamma + a^\alpha.$$

Theorem 2 *[10] Every quadratic APN map on L is uniquely written as $f_{\gamma,\alpha}$ for (γ, α). Namely, there is a bijection between the set of quadratic APN maps on L and the set $\Gamma \times Af$.*

5.2 Equivalence

Theorem 3 *[10] For two quadratic APN maps $f_{\gamma,\alpha}$ and $f_{\gamma',\alpha'}$, they are EA-equivalent iff* $\mathrm{Ker}(\gamma)$ *and* $\mathrm{Ker}(\gamma')$ *belong to the same orbit under the diagonal action of $GL(V)$: $g(a \wedge b) = g(a) \wedge g(b)$ $(a, b \in V)$.*

5.3 Core problem

Thus, finiding all the EA-equivalence classes of quadratic APN maps on V is equivalent to finding all $GL(V)$-orbit on the set of subspaces K of $(V \otimes V)/S(V) =: \bar{W}$ such that:

$$\mathrm{codim}(K) = \dim(\overline{W}) - \dim(K) = n \text{ and } K \cap \{a \wedge b \mid a \neq b \in V\} = \{0\}$$

We call a subspace K of $\bar{W}$ with the above property **line-skew**.

When $p = 2$, $\bar{W} = (V \otimes V)/S(V)$ is a quotient of $W = (V \otimes V)/A(V)$.

> **(Question)** Are there some relations between subspaces K of codimension n in W which yield commutative semifields (namely, $K \cap \{x \otimes y \mid x, y \in V\} = \{0\}$) and subspaces $\bar{K}$ of codimension n in $\bar{W}$ which yield quadratic APN functions (namely, $\bar{K} \cap \{x \otimes y \mid x \neq y \in V\} = \{0\}$).

6 Some explicit description of $A(V)$

6.1 Alternating form scheme $Alt(V)$

We assume that $p = 2$. Then $(V \otimes V)/S(V) \cong A(V)$ by identifying $x \otimes y + S(V)$ with $x \wedge y := x \otimes y + y \otimes x$.

$A(V)$ can also be identified with the space $Alt(V)$ of all alternating bilinear forms on V, by identifying $x \wedge y$ with the alternating form of **rank** 1 with $f(x, y) = 1$. Here the rank of an alternating form f is $(\dim(V) - \dim Rad(f))/2$.

Recall that $Alt(V)$ is an association scheme with respect to the distance δ given by $\delta(f, g) =$ the rank of $f - g$. Thus a subspace K of $Alt(V)$ of codimension n is line-skew iff it does not contain form of rank 1 iff any two distinct forms of K are at distance at least 2.

6.2 Line skew subspace as designs in $Alt(V)$

Delsarte and Goethals [3] investigated a subset D of $Alt(V)$ in which two distinct elments are at distance at least d. They obtained the bound $|D| \leq 2^{n(n+1-2d)/2}$ or $|D| \leq 2^{(n-1)(n+2-2d)/2}$ according as n is odd or even. As $\dim(K) = \dim(Alt(V)) - n = n(n-3)/2$, this bound is attained by K if n is odd.

With current terminologies in algebraic combinatorics, we have:

Proposition 5 (Line-skew space as Delsarte design) *Assume that $n = 2m + 1$ is odd. A subspace K of $Alt(V)$ is line-skew iff it is a $(m-1)$-**design** in $Alt(V)$ in the sense of Delsalte.*

The previous theorem gives us several strong information about a line-skew subspace, if $\dim(V) = n$ is odd (e.g. [7]). However, so far I could not obtain explicit informations on the numbers of such spaces.

6.3 Another explicit description of $Alt(V)$

We identify V with the field $F \cong \mathbb{F}_{2^n}$, and denote by $F_0 \cong \mathbb{F}_{2^{n/2}}$ the subfield of F of degree 2 if n is even. We set $l = \lfloor n/2 \rfloor$.

Then $Alt(V)$ is isomorphic to $V^l = V^m = \{(b_k)_{k=1}^l \mid b_k \in V\}$ if $n = 2m + 1$ is odd, and to the subspace of V^l with b_l lies in F_0 if $n = 2m + 2$ is even.

The explicit isomorphism can be described. In particular,

Proposition 6 (Subsets corresponding to rank 1 forms) *the set of rank 1 alternating forms corresponds to $\mathcal{L} := \{(x^{2^k+1}(y + y^{2^k}))_{k=1}^l \mid x, y \in F \setminus \mathbb{F}_2\}$.*

6.4 Some line-skwe subspaces

For every $1 \leq e \leq l$ coprime with n, the e-th entry $x^{2^e+1}(y + y^{2^e})$ is nonzero for any vector $(x^{2^k+1}(y + y^{2^k}))_{k=1}^l$ of $\mathcal{L}$. Thus the subspace K_e of V^l consisting of all vectors (b_k) with $b_k = 0$ does not contain any vector of $\mathcal{L}$. As K_e has codimension n in $Alt(V)$ (identified with the subspace of V^l described above), K_e is a line-skew subspace. The canonical projection map $\rho : Alt(V) \rightarrow Alt(V)/K_e$ composed with an identification $Alt(V)/K_e \ni (b_k)_{k=1}^l + K_e \mapsto b_k \in V$ gives $x \wedge y \mapsto x^{2^e}y + xy^{2^e}$. Hence this corresponds to the Gold function $g(x) = x^{2^e+1}$.

We also have line-skew subspace K consisting of $(b_k)_{k=1}^l$ with $b_1 + \sum_{i=0}^{n-1} b_3^{2^i}$. This gives the APN map $f(x) = x^3 + \sum_{i=0}^{n-1}(x^9)^{2^i}$.

When $n = 10$, $K = \{(b_k)_{k=1}^5 \mid b_1 = ub_3^4\}$ is a line-skew subspace yielding APN function $e(x) = x^3 + ux^{36}$.

6.5 Some comments

The last description of $Alt(V)$ seems explicit enough to find 'easy' examples of skew-free subspaces, and so quadratic APN functions.

Recently, Dillon, Edel and Pott [5] introduce the idea of 'switching' of APN functions, and produces many new examples of APN functions (including non-quadratic examples). In my setting, switching relation may be interpreted as two line-skew subspaces sharing a hyperplane. I am wondering if this suggests some new direction to generalize the idea of switching.

References

[1] L.Budaghyan and C.Carlet, Classes of quadratic APN trinomials and hexanomials and related structures, *IEEE Trans. Inf. Theory*, **54**(5), 2354-2357 (2008):

[2] R.S.Couletr and M.Henderson, Commutative presemifields and semifields, Adv. Math **217** (2008), 282–304.

[3] P.Delsarte and J.M.Goethals, Alternating bilinear forms over $GF(q)$, Journal of Combin. Theory (A) **19**, 26–50 (1975).

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

[5] Y.Edel and A.Pott, A new almost perfect nonlinear function which is not quadratic, *Advances in Mathematics of Communications*, **3**, 59–81 (2009). doi:10.3934/amc.2009.3.59

[6] 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.

[7] A.Munemasa, An analogue of t-designs in the association schemes of alternating forms, Graphs and Combinatorics **2**, 259–267 (1986).

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

[9] S.Yoshiara, Notes on APN functions, semibiplanes and dimensional dual hyperovals, submitted for publication, 2009.

[10] S.Yoshiara, Notes on split dimensional dual hyperovals, preprint, 2009.