数理解析研究所講究録
第 1756 巻 2011 年 13-21

Around equivalences on APN functions

東京女子大学 現代教養学部 数理科学科 吉荒 聡 (Satoshi Yoshiara)
Department of Mathematics, Tokyo Woman's Christian University,
Suginami-ku, Tokyo 167-8585, Japan *yoshiara@lab.twcu.ac.jp*

1 Introduction

The aim of this article is to announce that a conjecture made by Y. Edel is affirmatively solved. In this section, let me roughly describe what is this conjecture and discuss some effects of the affirmative solution to this conjecture. The precise definitions of the undefined or roughly defined terminologies below (indicated by the bold face letters) except semibiplanes and dimensional dual hyperovals will be given in the subsequent sections. For semibiplanes and dimensional dual hyperovals, see e.g. [8] or [10].

Edel's conjecture is concerning a class of functions on a finite field of even characteristic with extremely high nonlinearity. It is called an **APN function**(almost perfect nonlinear) and defined as a function whose differential at every nonzero element induces a two to one map. APN functions are known to have strong resistance against standard attacks to the cryptosystem, so that the main interest of researchers in cryptography is to construct explicit APN functions. This tendency is accelerated since the discovery of two APN functions which are not CCZ-equivalent to any power mappings by Y. Edel, G. Kyureghyan and A. Pott in 2006.

There are two kinds of equivalence classes on functions on a finite field, one is called the **extended affine equivalence** and the other the **CCZ equivalence**. If a function is APN, then any functions CCZ or extended affine equivalent to it are APN as well. Thus these equivalences automatically provide many APN functions from one. For two functions, it is usually easier to examine whether they are extended affine equvalent than to examine whether they are CCZ-equivalent, because the extended affine equivalence is attained by just linear changes of variables but the CCZ-equivalence requires more transformations. It turns out that if two APN functions are CCZ-equivalent then they are extended affine equivalent, but the converse is not true in general. However, through his investigations on explicit examples with some help of computers, Y. Edel conjectured that the converse is also true, if we restrict the class of APN functions to that of **quadratic** APN functions. Here a function on a finite field is called quadratic if the differential at any element is linear. Notice that the known infinite families of APN functions which are CCZ-inequivalent to any power mappings consist of quadratic maps.

I have been investigating combinatorial structures associated with APN functions. In fact, we can associate a graph with each APN function, which is the incidence graph of a **semibiplane**. For a quadratic APN function, we can also associated the second combinatorial structure, known as **dimensional dual hyperoval** (over the two element field). It can be shown that two APN (resp. quadratic APN) functions are CCZ-equivalent (resp. extended affine equivalent) if and only if the incidence graphs of semibiplanes (resp. dimensional dual hyperovals) associated with them are isomorphic as graphs (resp. as dimensional dual hyperovals). Based on these geometric interpretations of equivalences, the last summer I succeeded in showing that Edel's conjecture is true, by applying some basic techniques in group theory to the actions of groups of **translations** on the incidence graphs of semibiplanes.

This may provide some contributions to the recent activities in constructing new APN functions. Suppose one found a class of APN functions and would like to show that they are new, in the sense that they are not CCZ-equivalent to the previously known APN functions. If these functions are quadratic, the affirmative solution of Edel's conjecture reduces this task much. Let me explain this point. Notice that the known list of APN functions consists of those CCZ-equivalent to power mappings, five infinite families of quadratic functions (which are inequivalent to any power mappings), and some sporadic examples (defined on small finite fields). Based on an observation that the automorphism group of the associated graph of a power mapping has the multiplicative group of the field, it is not extremely difficult to see that a given function is not CCZ-equivalent to a power mapping, if it is in the case. Thus the main task is to show that a given quadratic function is not CCZ-equivalent to any member of the known five infinite families of quadratic APN functions. The afiirmative solution to Edel'd conjecture makes this task easier: it is now enough to establish the extended affine inequivalence, which is in general much easier to establish the CCZ-inequivalence.

2 APN functions and quadratic functions

Some researchers are interesting in functions on a finite filed which are as nonlinear as possible, because such functions are useful in cryptograph. It is known that they have strong resistance to known methods of attacks, such as the linear and differential cryptanalysis. Recall that a function f on a finite field $F \cong \mathbb{F}_{p^n}$ is called **linear** (over the prime field $\mathbb{F}_p$) if and only if $f(x+y) = f(x) + f(y)$ for all $x, y \in F$. In terms of differentials, this amounts to the following condition: for each $a \in F^\times := F \setminus \{0\}$, the map sending each $x \in F$ to $f(x+a) - f(x)$ (the **differential** at a) takes just a single value $f(a)$. Thus one possible formulation of "nonlinear" functions is to define them as functions f for which the differential $f(x+a) - f(x)$ takes as many values as possible, when a ranges over $F^\times$. Equivalently, a function f on F is regarded "as nonlinear as possible" if the differential map $F \ni x \mapsto f(x+a) - f(x) \in F$ is "as injective as possible" for every $a \in F^\times$. The extremal case is formulated as follows:

Definition 1 *A map f on $F \cong \mathbb{F}_{p^n}$ is called* **perfect nonlinear** *(abbreviated to* **PN***) if the equation $f(x+a) - f(x) = b$ (for variable x) has at most one solution x in F for every $a \in F^\times$ and every $b \in F$.*

If f is PN, then the differential map at a is a bijection for all $a \in F^\times$. The terminology "perfect nonlinear" is commonly used by researchers working in cryptography, but for the geometer, this function is known as a **planar** function. It was introduced first by Dembowski and Ostrom, in order to construct projective planes with some symmetries.

However, a perfect nonlinear function on $F \cong \mathbb{F}_{p^n}$ exists only when p is an odd prime, because x and $x + a$ are sent to the same element $f(x+a) + f(x)$ by the differential map at a, if F has characteristic 2. In this case, the most extremal case is formulated as follows:

Definition 2 *A map f on $F \cong \mathbb{F}_{2^n}$ is called* **almost perfect nonlinear** *(abbreviated to* **APN***) if the equation $f(x+a) - f(x) = b$ (for variable x) has at most two solutions x in F for every $a \in F^\times$ and every $b \in F$.*

Table 1: Known APN power functions x^d on $F \cong \mathbb{F}_{2^n}$

Name	d	Conditions	$w_2(d)$
Gold	$2^i + 1$	$(i, n) = 1$	2
Kasami	$2^{2i} - 2^i + 1$	$(i, n) = 1$	$i + 1$
Welch	$2^t + 3$	$n = 2t + 1$	3
Niho	$2^t + 2^{t/2} - 1$, t even $2^t + 2^{(3t+1)/2} - 1$, t odd	$n = 2t + 1$	$(t+2)/2$ $t + 1$
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	$t + 3$

Table 2: Known infinite families of APN maps CCZ-inequivalent to any power maps

Function on $\mathbb{F}_{2^n}$	Conditions
$x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$	$n = 3k$, $(k, 3) = (s, 3k) = 1$ $k \geq 4$, $i = sk \bmod 3$, $m = 3 - i$, $w \in \mathbb{F}_{2^n}^\times$ has order $2^{2k} + 2^k + 1$
$x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$	$n = 4k$, $(k, 2) = (s, 2k) = 1$, $k \geq 3$, $i = sk \bmod 4$, $m = 4 - i$, $w \in \mathbb{F}_{2^n}^\times$ has order $2^{3k} + 2^{2k} + 2^k + 1$
$x^3 + \mathrm{tr}(x^9)$	$n \geq 7$ $n > 2p$ for smallest $p > 1$ with $p \neq 3$, $(p, n) = 1$.
$x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$	$n = 2m$, $m \geq 3$, $q = 2^m$ $c^{q+1} = 1$, $c \notin \{\lambda^{(2^i+1)(q-1)} \mid \lambda \in L\}$ $(i, m) = 1$, $cb^q + b \neq 0$
$x(x^{2^i} + x^q + cx^{2^i q})$ $+x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$	$n = 2m$, $m \geq 3$, $q = 2^m$ $(i, m) = 1$, $s \notin \mathbb{F}_q$ $X^{2^i+1} + cX^{2^i} + c^q X + 1$ is irreducible over $\mathbb{F}_{2^n}$

Let me briefly introduce the known classes of APN functions. The first one is CCZ-equivalent (for the precise definition, see Definition 5) to one of the power mappings indicated in Table 1. As far as I know, at the present time there are five infinite classes which are not CCZ-equivalent to any power mappings. They are indicated in Table 2. There are several sporadic examples, in the sense that they are only defined on a specific field (of size at most 2^{10}) and not contained in one of the five known infinite families.

Amongst them, the most remarkable one is the function $e(x) = x^3 + ux^{36}$ on $F \cong \mathbb{F}_{2^{10}}$ found by Edel, Kyureghyan and Pott in 2006 [5], where $u$ is any element lying in the cosets $\omega K^\times$ and $\omega^2 K^\times$ for an element $\omega$ of $F$ of order 3 and a subfield $K \cong \mathbb{F}_{2^5}$ of $F$.

Now I shall discuss another class of functions with a motivation from geometry. A perfect nonlinear function $f$ on $F \cong \mathbb{F}_{p^n}$ ($p$ an odd prime) is called **Dembowski-Ostrom** if it is represented by a polynomial over $F$ of the following shape:

$$a + \sum_{i=0}^{n-1} a_i X^{2p^i} + \sum_{0 \le i < j \le n-1} a_{ij} X^{p^i + p^j}.$$

This class of perfect nonlinear function is very much important, as it corresponds to the commutative semifields structure on $F$ [4]. The corresponding notion on $F$ with even characteristic is defined as follows:

Definition 3 *A function $f$ on $F \cong \mathbb{F}_{2^n}$ is called* **quadratic**, *if it is represented by a polynomial over $F$ of the following shape:*

$$a + \sum_{i=0}^{n-1} a_i X^{2^i} + \sum_{0 \le i < j \le n-1} a_{ij} X^{2^i + 2^j}.$$

This notion can be interpreted in the following way:

Proposition 1 *A function $f$ on $F \cong \mathbb{F}_{2^n}$ is quadratric if and only if the map B_f from $F \times F$ to $F$ defined by $B_f(x,y) := f(x+y) + f(x) + f(y) + f(0)$ $(x, y \in F)$ is bilinear.*

In the above example, in Table 1 the Gold function $g(x) = x^{2^e+1}$ with $e$ coprime to $n$ on $F \cong \mathbb{F}_{2^n}$ is quadratic, but none of the rest of power mappings x^d in this table. In view of the exponent $d$, this is immediate from the definition. The five infinite families in Table 2 are all quadratic. Among sporadic examples, except two on $\mathbb{F}_{2^n}$ with $n \le 7$, all others are quadratic [6].

3 Equivalences and Edel's conjecture

Starting from a PN or APN function, how one can construct new PN or APN functions? The standard way is to apply suitable transformations of variables. For example, if $f$ is PN (resp. APN) on $F \cong \mathbb{F}_{p^n}$ with $p$ an odd prime (resp. $p = 2$), then $g = f + (\rho + c)$ for an affine map $\rho + c$ (in which $\rho$ denotes the linear part and $c \in F$ denotes the constant part) is also PN (resp. APN) as well, because the equation $b = g(x+a) - g(x) = f(x+a) - f(x) + \rho(a)$ has exactly one (resp. zero or two) solution(s) $x$ in $F$ for every $a \in F^\times$ and every $b \in F$. We can also consider the composition of a PN or APN function with a bijective affine map: if $f$ is PN (resp. APN) on $F \cong \mathbb{F}_{p^n}$ with $p$ an odd prime (resp. $p = 2$), then $g = f \circ (\rho + c)$ for any bijective affine map $\rho + c$ is again PN (resp. APN), because there are exactly one (resp. zero or two) solution(s) $x \in F$ for the equation $b = g(x+a) - g(x) = f(\rho(x) + \rho(a) + c) - f(\rho(x) + c)$ for every $a \in F^\times$ and every $b \in F$. These observations lead us to the following notion of equivalence.

Definition 4 *Let f and g be functions on $F \cong \mathbb{F}_{p^n}$. We say that f is extended affine equivalent (abbreviated to* **EA***-equivalent) to g, if there are bijective affine maps $\alpha+c$ and $\delta+d$ on F (α, δ are bijective linear maps on F and $c, d \in F$) such that $g\circ(\alpha+c)-(\delta+d)\circ f$ is a linear map.*

It can be verified that the EA-equivalence is an equivalence relation on a set of functions on F. We can easily verify the following facts:

Proposition 2 *Assume that f and g are functions on $F \cong \mathbb{F}_{p^n}$ which are EA-equivalent.*

(1) Assume that p is an odd prime. If f is PN, then g is PN as well. If f is Dembowski-Ostrom, then g is Dembowski-Ostrom as well.

(2) Assume that $p = 2$. If f is APN, then g is APN as well. If f is quadratic, then g is quadratic as well.

The transformations used to define EA-equivalence are just affine transformations on F. Carlet, Charpin and Zinoviev found more transformations on $F \oplus F := \{(x, y) \mid x, y \in F\}$ which yield new PN or APN functions [3].

Definition 5 *Let f and g be functions on $F \cong \mathbb{F}_{p^n}$. We say that f is* **CCZ***-equivalent to g, if there exists a bijective affine map $\rho + (c, d)$ on $F \oplus F$ which sends the* **graph** *$\Gamma(f) := \{(x, f(x)) \mid x \in F\}$ of f to the graph $\Gamma(g) := \{(x, g(x)) \mid x \in F\}$ of g.*

Instead of "CCZ"-equivalence (after Carlet, Charpin and Zinoviev), sometimes the terminology "graph"-equivalence is used. It is straightforward to see that this relation is in fact an equivalence relation on the set of functions on a finite field F. The fundamental fact is the following:

Proposition 3 *Assume that f and g are functions on F which are CCZ-equivalent. If f is PN (resp. APN), then g is PN (resp. APN).*

Notice that there are many linear bijective maps on $F \oplus F$, regarded as a $2n$-dimensional vector space over $\mathbb{F}_p$. In general, any linear map ρ on $F \oplus F$ are determined by a quadruple $(\alpha, \beta, \gamma, \delta)$ consisting of linear maps $\alpha, \beta, \gamma, \delta$ on F such that

$$\rho((x, y)) = (x, y)\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (x^\alpha + y^\gamma, x^\beta + y^\delta)$$

for $x, y \in F$. In this case, we will denote $\rho = \rho(\alpha, \beta, \gamma, \delta)$. Thus at the first sight CCZ-equivalence seems to yield many more PN or APN functions than EA-equivalence. In fact, as the following claim shows, EA-equivalence is a special case of CCZ-equivalence.

Proposition 4 *For functions f and g on $F \cong \mathbb{F}_{p^n}$, f is EA-equivalent to g if and only if there is a bijective affine map $\rho + (c, d)$ on $F \oplus F$ with $\rho = \rho(\alpha, \beta, 0, \delta)$ which maps $\Gamma(f)$ to $\Gamma(g)$.*

Observe that the above condition on ρ (with $\gamma = 0$) is equivalent to say that ρ leaves the subspace $Y := \{(0, y) \mid y \in F\}$ of $F \oplus F$ invariant.

However, in the case of odd characteristic, it turns out that the notion of CCZ-equivalence is identical to that of EA-equivalence.

Proposition 5 *For functions f and g on $F \cong \mathbb{F}_{p^n}$ with p an odd prime, f is CCZ-equivalent to g if and only if f is EA-equivalent to g.*

On the other hand, for functions on $F \cong \mathbb{F}_{2^n}$ the notion of CCZ-equivalence is properly wider than that of EA-equivalence. For example, consider the cubic function $g(x) = x^3$ on $F \cong \mathbb{F}_{2^n}$. It is easy to see that g is quadratic and APN. Assume that $n = 2m+1 > 3$ is odd. In this case, g is bijective. The inverse function g^{-1} is given by the power mapping $g^{-1}(x) = x^{1+2^2+\cdots+2^{2m}}$. As $m > 1$, in view of the exponent, we conlude that g^{-1} is not quadratic. From the latter claim of Proposition 2(2), this implies that a quadratic function g is not EA-equivalent to a non-quadratic function g^{-1}. However, g is CCZ-equivalent to g^{-1}, because the linear map $(x, y) \mapsto (y, x)$ on $F \oplus F$ sends $\Gamma(g) = \{(x, g(x)) \mid x \in F\}$ to $\{(g(x), x) \mid x \in F\} = \{(y, g^{-1}(y)) \mid y \in F\} = \Gamma(g^{-1})$. Thus g^{-1} is a non-quadratic APN function which is CCZ-equivalent but EA-inequivalent to a quadratic APN function g. As this example shows, CCZ-equivalence does not preserve the class of quadratic functions.

Thus CCZ-equivalence in general provides much more APN functions from an APN function than EA-equivalence. However, through his attempt to classify all (quadratic) APN functions on $F \cong \mathbb{F}_{2^n}$ with $n \leq 6$, Y. Edel observed that any CCZ-equivalence class of a quadratic APN function on $F \cong \mathbb{F}_{2^n}$ $(n \leq 6)$ contains just one EA-equivalence class. Namely, he observed the following: if two quadratic APN functions on $F \cong \mathbb{F}_{2^n}$ $(n \leq 6)$ are CCZ-equivalent, then they are in fact EA-equivalent. He conjectured that this holds for any $F \cong \mathbb{F}_{2^n}$.

Notice that this conjecture is equivalent to the following claim.

> For two quadratic APN functions f and g on $F \cong \mathbb{F}_{2^n}$, if there is a bijective affine map $\rho + (c, d)$ on $F \oplus F$ which sends $\Gamma(f)$ to $\Gamma(g)$, then we may arrange ρ to preserve $Y = \{(0, y) \mid y \in F\}$.

I have been interesting in combinatorial objects related to APN functions, because I found my favorite structure "dimensional dual hyperovals" (but just a small part of them) are such objects for quadratic APN functions [10], [11]. I established categorical correspondence between quadratic APN functions up to EA-equivalence and some class of dimensional dual hyperovals (dimensional dual hyperovals over $\mathbb{F}_2$ covered by the Huybrechts dual hyperoval in some specific way) up to isomorphisms. This provides useful automorphisms, called translations, to investigate a quadratic APN function. Furthermore, my earlier investigation joint with A. Pasini of the affine expansions (which are semibiplanes) of wider class of dimensional dual hyperovals [8],[9] alraedy suggested the categorical correspondence between APN functions up to CCZ-equivalence and the incidence graphs of semibiplanes with certain parameters up to graph isomorphism [12]. (Corresponding results in slightly weaker forms are also obtained in [7].) Based on these preparations, I succeeded in showing the above conjecture of Edel by exploiting some standard techniques in group theory and incidence geometry.

Theorem 1 *Let f and g be two quadratic APN functions on $\mathbb{F}_{2^n}$ with $n \geq 2$. Then f is CCZ-equivalent to g if and only if f is EA-equivalent to g.*

I am preparing a paper which includes the whole proof of this theorem [13]. The first draft was carefully studied by Professor Nakagawa and his students, and they report me that they did not find any serious errors in the arguments. I heartly thank Professor Nakagawa and his students for their efforts. I also thank Yve Edel for providing me many useful informations on APN functions including his conjecture, especially when he visited Japan in 2009.

4 Outline of the proof of the main theorem

4.1 Ingredients

We first define a graph associated with any function on $F \cong \mathbb{F}_{2^n}$ [12, Definition 4].

Definition 6 *For a function $f$ on $F \cong \mathbb{F}_{2^n}$, define a graph Γ_f as follows: the set of vertices is $\mathbb{F}_2 \oplus F \oplus F = \{(\varepsilon; x, y) \mid \varepsilon \in \mathbb{F}_2, x, y \in F\}$, where $(0; x, y)$ and $(1; x, y)$ are called* **points** *and* **blocks***; two vertices $(\varepsilon_1; x_1, y_1)$ and $(\varepsilon_2; x_2, y_2)$ are adjacent whenever $\varepsilon_1 + \varepsilon_2 = 1$ and $y_1 + y_2 = f(x_1 + x_2) + f(0)$.*

We denote by $\mathcal{P} := \{(0; x, y) \mid x, y \in F\}$ the set of points and by $\mathcal{B} := \{(1; x, y) \mid x, y \in F\}$ the set of blocks.

This graph has a geometric interpretation for a function to be APN, and also gives a geometric interpretation of CCZ-equivalence [12, Proposition 1,2].

Proposition 6 *Let $f$ and $g$ be functions on $F \cong \mathbb{F}_{2^n}$.*

(1) $f$ is APN iff the graph Γ_f is a connected graph, in which two points (resp. blocks) has exactly 0 or 2 blocks (resp. points) adjacent to both of them.

(2) Assume that $f$ and $g$ are APN functions. Then $f$ is CCZ-equivalent to $g$ if and only if Γ_f and Γ_g are isomorphic as graphs.

The next claim is very much important [12, Lemma 3]. Its proof implicitly uses a standard semibiplane which covers Γ_f for an APN function $f$, appeared already in [8]. Here we denote a vertex $(\varepsilon; x, y)$ of Γ_h ($h = f$ or $g$) by $(\varepsilon; x, y)_h$ in order to distinguish to which graph it belongs.

Proposition 7 *Assume that $\lambda$ is a graph isomorpshism from Γ_f to Γ_g sending $(0; 0, 0)_f$ to $(0; 0, 0)_g$. Then $\lambda$ is linear on $\mathbb{F}_2 \oplus F \oplus F$.*

Now we describe some automorphisms of the graph Γ_f for a (quadratic) APN function $f$. The following maps for any $a, b \in F$ are apparently automorphisms of Γ_f:

$$\iota : (\varepsilon; x, y) \mapsto (\varepsilon + 1; x, y),\ \tau(a, b) : (\varepsilon; x, y) \mapsto (\varepsilon; x + a, y + b).$$

If $f$ is a quadratic APN function, then the following map t_a is an automorphism of Γ_f, which we shall refer to as the **translation** along $a \in F$:

$$(\varepsilon; x, y) \mapsto \varepsilon(1; a, f(a) + f(0)) + (0; x, y + B_f(a, x)),$$
where $B_f(a, y) := f(x + a) + f(x) + f(a) + f(0)$.

Here are informations about the action of a translation on the set of vertices.

Lemma 1 *If f is a quadratic APN function on $F \cong \mathbb{F}_{2^n}$, the following hold for every nonidentical translation t_a $(a \in F^\times)$:*

(1) The group $T = \{t_a \mid a \in F\}$ of translations acts regularly on the set of 2^n blocks adjacent to $(0;0,0)$.

(2) The commutator space $[\mathcal{P}, t_a] := \{\mathbf{x} + \mathbf{x}^{t_a} \mid \mathbf{x} \in \mathcal{P}\}$ of t_a on $\mathcal{P}$ is a subspace of $Y := \{(0;0,y) \mid y \in F\}$ of dimension $n-1$.

(3) The centralizer $C_{\mathcal{P}}(t_a) := \{\mathbf{x} \in \mathcal{P} \mid \mathbf{x}^{t_a} = \mathbf{x}\}$ of t_a on $\mathcal{P}$ is a subspace of dimension $n+1$ containing Y.

Using the above informations, the next key lemma is obtained with notation in Lemma 1. Notice that Y is one of the two subspaces in Lemma 2.

Lemma 2 *For a nonidentity translation t_a $(a \in F^\times)$, there are exactly two subspaces X of $\mathcal{P}$ of dimension n with the following two properties: $[\mathcal{P}, t_a] \subset X \subset C_{\mathcal{P}}(t_a)$, and X does not conatin any point at distance 2 from $(0;0,0)$.*

4.2 Outline

In this last part of the article, I provide an outline of the proof. The notation introduced in the previous subsection will be freely used.

We will first make some reduction. Assume that f and g are quadratic APN functions on $F \cong \mathbb{F}_{2^n}$, which are CCZ-equivalent. By Proposition 6(2), this assumption is equivalent to the existence of a graph isomorphism between the graphs Γ_f and Γ_g defined on $\mathbb{F}_2 \oplus F \oplus F$. The existence of translations allows us to assume that such an isomorphism, say ρ, fixes a point $(0;0,0)$ and a block $(1;0,0)$.

Applying Sylow's theorem and Proposition 7, we may assume that ρ is a linear map on $\mathbb{F}_2 \oplus F \oplus F$ such that a Sylow 2-subgroup S_f of the stabilizer of $(0;0,0)_f$ in $\mathrm{Aut}(\Gamma_f)$ containing the group T_f of translations for Γ_f is sent to a Sylow 2-subgroup S_g of the stabilizer of $(0;0,0)_g$ in $\mathrm{Aut}(\Gamma_g)$ containing the group T_g of translations for Γ_g.

Next we shall investigate the centers of Sylow 2-groups. Based on an observation that the center $Z(S_h)$ of such a Sylow subgroup S_h lies in T_h for both $h = f$ and g, we can calculate the centralizer of $Z(S_h)$ on the set of points of Γ_h. If $|Z(S_f)| \geq 4$, they are equal to the subspace $Y = \{(0;0,y) \mid y \in F\}$ of $\mathbb{F}_2 \oplus F \oplus F$, whence Y is stabilized by ρ. This implies that ρ gives an EA-equivalence of f with g.

Hence we may assume that $|Z(S_h)| = 2$ $(h = f, g)$. In this case, from Lemma 2, the image of Y under ρ is one of the two possible subspaces containing the subspace consisting of $(0;0,y')$ where y' ranges over a hyperplane of F. As we may assume that ρ does not preserve Y, the image of Y under ρ is uniquely determined.

In particular, the values $(x+y)^\pi + x^\pi + y^\pi$ for $x, y \in F$ lies in a 1-dimensional subspace spanned by a specific nonzero element a' of F, where π is a permutation on F such that the image of a block $(1;x,\overline{f}(x))$ is mapped by ρ to $(1;x^\pi,\overline{g}(x^\pi))$ for every $x \in F$.

Then we may introduce a form κ on F, which vanishes at (x,y) exactly when $B_f(x,y) = f(x+y) + f(x) + f(y) + f(0)$ lies in a certain hyperplane H_a of F. We investigate this form to conclude that it is almost the zero form. This gives a final contradiction.

References

[1] C. Bracken, E. Byrne, G. McGuire and G. Nebe, On equivalence of quadratic APN-functions, submitted for publications, 12 May 2009.

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

[3] C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Designs, Codes and Cryptography*, **15**, 125–156 (1998). doi:10.1023/A:1008344232130

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

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

[6] 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

[7] 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.

[8] A. Pasini and S. Yoshiara, On a new family of flag-transitive semibiplanes, *Europ. J. Combinatorics* **22** (2001), 529–545.

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

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

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

[12] S. Yoshiara, Notes on APN functions, semibiplanes and dimensional dual hyperovals, Designs, Codes and Cryptography, 56 (2010), 197–218. DOI: 10.1007/s10623-010-9402-z

[13] S. Yoshiara, Equivalences of quadratic APN functions, in preparation (first draft, July 18, 2010).