A class of functions and their application in constructing semi-biplanes and association schemes

Robert S. Coulter and Marie Henderson

Centre for Discrete Mathematics and Computing
Department of Computer Science and Electrical Engineering
The University of Queensland
St. Lucia, Queensland 4072
Australia.

Abstract

We give an alternative proof of the fact that a planar function cannot exist on groups of even order. The argument involved leads us to define a class of functions which we call semi-planar. Through the introduction of an incidence structure we construct semi-biplanes using semi-planar functions. The method involved represents a new approach to constructing semi-biplanes and provides infinite classes of semi-biplanes unlike any known to the authors. For a particular class of semi-planar functions, we provide a method to construct association schemes with two associate classes. Such an association scheme is equivalent to a strongly regular graph.

Key words: semi-biplane, association scheme, incidence geometry

1 Planar functions revisited

Let G and H be finite groups written additively but not necessarily abelian. A function $f : G \to H$ is called a *planar function* if for every non-identity $a \in G$ the functions $\Delta_{f,a} : x \mapsto f(a+x) - f(x)$ and $\nabla_{f,a} : x \mapsto -f(x) + f(x+a)$ are bijections. Due to a result of Dembowski and Ostrom [5, Lemma 12], $\nabla_{f,a}$ will be a bijection if and only if $\Delta_{f,a}$ is a bijection. Therefore we only need look at one of these two functions.

⋆ This work was partially supported by an Australian Research Council grant.

Planar functions were introduced by Dembowski and Ostrom [5] to describe affine planes with certain properties. Using a geometric argument Dembowski and Ostrom showed that planar functions could not exist over any finite group of even order. Here we prove the same result using only standard group theory, without any reliance on the assumed structure of the associated plane.

Theorem 1 (Dembowski and Ostrom, 1968) *Let G and H be finite groups of even order written additively but not necessarily abelian. Then there exist no planar functions mapping G to H.*

PROOF. Suppose the mapping $f : G \to H$ is a planar function. Then $\Delta_{f,a}(x) = f(x+a) - f(x)$ is a bijection for each non-identity $a \in G$. For any finite group G of even order there exists a non-zero $g \in G$ satisfying $g + g = 0$ so that g is its own inverse. Consider $\Delta_{f,g}$. As f is planar there exists a unique element $x_0 \in G$ satisfying $\Delta_{f,g}(x_0) = f(g + x_0) - f(x_0) = 0$. From this we also have $f(x_0) - f(g + x_0) = 0$. However

$$\begin{aligned} \Delta_{f,g}(g + x_0) &= f(g + g + x_0) - f(g + x_0) \\ &= f(x_0) - f(g + x_0) \\ &= 0 \end{aligned}$$

contradicting the uniqueness of x_0. □

Effectively, this proof can be viewed as a generalisation of the simple argument used to show there are no planar functions over any finite field of even characteristic, see [14, Proposition 1].

2 Semi-planar functions

An interesting property revealed in the proof just given is this: when dealing with groups of even order, if we have a solution to the equation $f(x+a) - f(x) = y$ then we can always obtain a second. This suggests the following definition.

Definition 2 *Let G and H be finite groups of the same even order written additively but not necessarily abelian. We call a function $f : G \to H$ a* semi-planar function *if for every non-identity $a \in G$ the equation*

$$f(x + a) - f(x) = y,$$

with $y \in H$, has either 0 or 2 solutions $x \in G$.

These functions have also been called almost perfect non-linear functions, see [13], and differentially 2-uniform functions, see [12]. In both cases, the motivation for studying these functions lies with their interesting cross-correlation and non-linear properties. Such properties are of interest in cryptography. Here our motivation stems from combinatorial aspects. As a result of the earlier definitions there are several classes of semi-planar functions already known.

Theorem 3 *Let $f(X) = X^n$, $q = 2^e$ and denote by $\mathbb{F}_q$ the finite field containing q elements. Let us denote by $\mathbb{F}_q$ the additive group of $\mathbb{F}_q$ too.*

(i) If $n = 1$ then f is semi-planar on $\mathbb{F}_q$ if and only if $e = 1$.
(ii) If $n = 2^\alpha + 1$ then f is semi-planar on $\mathbb{F}_q$ if and only if $(\alpha, e) = 1$.
(iii) If $n = 2^{e-1} - 1$ then f is semi-planar on $\mathbb{F}_q$ if and only if e is odd.
(iv) If $n = (2^{3\alpha} + 1)/(2^\alpha + 1)$ then f is semi-planar on $\mathbb{F}_q$ if $(\alpha, e) = 1$.
(v) If $n = 2^{(e+1)/2} - 1$ then f is semi-planar on $\mathbb{F}_q$ if and only if e is odd.
(vi) If $n = 2^{(e-1)/2} + 3$ then f is semi-planar on $\mathbb{F}_q$ if and only if e is odd.

Remarks on proof. The case (i) is trivial. For (ii) see [12, Proposition 3]. Case (iii) follows from [1, Theorem 13]. When e is odd, (iv) is effectively due to the combined results of Kasami [10] and Cusick [4]. For e even, the case (iv) was established recently by Dobbertin in [6]. For a direct proof of (v) see [8, Theorem 1] (an indirect proof is described below). Finally, (vi) is shown in [6].

The monomials described in class (ii) are members of a larger class of polynomials known as Dembowski-Ostrom (DO) polynomials. DO polynomials were introduced in [5] in connection with planar polynomials. They can be described as being any polynomial $f \in \mathbb{F}_q[X]$ (with $q = p^e$) of the shape

$$f(X) = \sum_{i,j=0}^{e-1} a_{ij} X^{p^i + p^j}.$$

It was shown in [3, Theorem 3.2] that the DO polynomials are precisely those polynomials whose difference polynomials $\Delta_{f,a}(X) = f(X + a) - f(X)$ are affine polynomials for all non-zero $a \in \mathbb{F}_q$. Further semi-planar polynomials can be generated using either of the following results.

Proposition 4 ([12, Proposition 1]) *Let G and H be finite abelian groups. Let $A : G \to G$ and $B : H \to H$ be group isomorphisms and let $f : G \to H$ be a semi-planar function. Then $B \circ f \circ A$ is semi-planar.*

Proposition 5 ([12, Proposition 2]) *Let G and H be finite abelian groups and let $f : G \to H$ be a semi-planar bijection. Then the inverse of f is semi-planar.*

In the finite field case, Proposition 4 equates to composing with linearised permutation polynomials, see [11, Section 3.4]. It can be seen from Proposition

5 that Theorem 3(v) is a consequence of Theorem 3(ii) since, for e odd and $n = 2^{(e+1)/2} + 1$, we have $((e+1)/2, e) = 1$, $f(X) = X^n$ is bijective and its inverse is $f^{-1}(X) = X^m$, $m = 2^{(e+1)/2} - 1$.

3 An incidence structure

In [5] Dembowski and Ostrom introduced a functionally dependent incidence structure. They showed that the existence of a planar function was equivalent to the corresponding incidence structure representing an affine plane with particular properties. Motivated by their results we now introduce an incidence structure which we will use to construct combinatorial structures using semi-planar functions.

Definition 6 *Let G and H be finite abelian groups of the same even order written additively and let $f : G \to H$. We define the incidence structure $S(G, H; f)$ by:*

$$\begin{aligned} \textit{Points: } & (x, y) \textit{ with } x \in G \textit{ and } y \in H \\ \textit{Lines: } & \mathcal{L}(a, b) \textit{ with } a \in G \textit{ and } b \in H \\ \textit{Incidence: } & (x, y) \text{ I } \mathcal{L}(a, b) \Leftrightarrow y = f(x - a) + b. \end{aligned}$$

When G and H are the additive group of $\mathbb{F}_q$ for some $q = 2^e$ we will denote the incidence structure simply by $S(f)$.

This incidence structure is modelled on the one used by Dembowski and Ostrom in [5]. If we consider this structure in the case where f is a semi-planar function we have the following theorem.

Theorem 7 *Let G and H be finite abelian groups written additively and of the same even order k. Let $f : G \to H$ be a semi-planar function. Then $S(G, H; f)$ has the following properties.*

(i) It has k^2 points and k^2 lines.
(ii) Each line contains k points and each point is on k lines.
(iii) It is self-dual.
(iv) Every pair of points occur on 0 or 2 lines and every pair of lines intersect in 0 or 2 points.
(v) For every point there are exactly $k(k-1)/2$ other points defined by the lines through it.

PROOF. (i) Trivial as $|G \times H| = k^2$.

(ii) Let $\mathcal{L}(a,b)$ be some line of the incidence structure. Then

$$\mathcal{L}(a,b) = \Big\{\Big(x, f(x-a)+b\Big) \mid x \in G\Big\}$$

and so $|\mathcal{L}(a,b)| = k$. Now choose some point (x,y). Then for each $a \in G$ we can solve for $b \in H$ in the equation

$$y = f(x-a)+b$$

and so the point (x,y) must lie on k lines.

(iii) To see that $S(G,H;f)$ is self-dual simply observe that if $y = f(x-a)+b$ then $-b = f(-a+x)-y$. Thus $(x,y) \in \mathcal{L}(a,b)$ if and only if $(-a,-b) \in \mathcal{L}(-x,-y)$. So we can always interchange lines and points. In other words, $S(G,H;f)$ is self-dual.

(iv) Consider the distinct lines $\mathcal{L}(a,b)$ and $\mathcal{L}(c,d)$ for $a,c \in G$ and $b,d \in H$. If $a = c$ then $b \neq d$ and it can be seen that the two lines do not intersect. So there exist lines which do not have common points. Now suppose that the two lines do have a common point (x,y). Then $a \neq c$ and $f(x-a)+b = f(x-c)+d$ or, equivalently, $f(x-a)-f(x-c) = d-b$. By assumption f is semi-planar and so this equation will have either two solutions or none at all. Since we already have a single solution there must be a second solution. Thus the lines $\mathcal{L}(a,b)$ and $\mathcal{L}(c,d)$ intersect in exactly two points. Note that $a \neq c$ does not imply $\mathcal{L}(a,b)$ and $\mathcal{L}(c,d)$ intersect. It is clear that some lines must intersect. That every pair of points occur on 0 or 2 lines follows from duality.

(v) Let $\mathcal{P}$ be a point of our incident structure. We wish to show that the number of points defined by lines through $\mathcal{P}$ is a constant independent of the point $\mathcal{P}$ chosen. By part (ii) there are k lines through $\mathcal{P}$ and each of these lines contains $k-1$ points other than $\mathcal{P}$. This gives an overall total of $k(k-1)$ points. However, every pair of lines through $\mathcal{P}$ intersect at $\mathcal{P}$ and so must have a second point of intersection which is uniquely defined by the pair of lines chosen. So every point has been counted twice. Thus there are $k(k-1)/2$ points overall. □

In light of the above result the following definition is clearly relevant.

Definition 8 *A connected incidence structure is called a* semi-biplane *if*

(i) any two points are incident with 0 or 2 common blocks;
(ii) any two blocks are incident with 0 or 2 common points.

A semi-biplane has v points, v blocks, each block contains k points and each point is on k blocks. We denote this structure $sbp(v,k)$.

Proposition 9 *Let G and H be finite abelian groups written additively and of the same even order k. Let $f : G \to H$ be a semi-planar function. If $S(G, H; f)$ is connected then it is a $sbp(k^2, k)$. If $S(G, H; f)$ is not connected then $S(G, H; f)$ splits into two sub-structures; both are $sbp(k^2/2, k)$.*

PROOF. By the previous theorem the only requirement to consider is whether the incidence structure is connected or not. From Theorem 7(v) every point is connected to at least $k(k-1)/2$ other points and so there can be at most 2 connected sub-structures contained in $S(G, H; f)$. Clearly, if it is connected then we have an $sbp(k^2, k)$. Suppose $S(G, H; f)$ is not connected. Then we have two sub-structures. By Theorem 7(v) the minimum number of points a sub-structure can contain is $1 + k(k-1)/2$. Define a parallel class to be any set $\{\mathcal{L}(a, b) \mid b \in H\}$ where $a \in G$. (Note that this is not necessarily a description of the full parallel classes.) It is clear that all lines in a parallel class are parallel. Let t be the number of lines from a parallel class in one of the sub-structures. Each of these t lines contains k points. Hence

$$\frac{k(k-1)}{2} + 1 \leq tk \leq k^2 - \frac{k(k-1)}{2} - 1$$

and dividing through by k we have

$$\frac{k-1}{2} + \frac{1}{k} \leq t \leq \frac{k+1}{2} - \frac{1}{k}.$$

Thus

$$\frac{k-1}{2} < t < \frac{k+1}{2}$$

and since t is an integer we must have $t = k/2$. Thus each sub-structure contains exactly one half of the lines from every parallel class and must be a $sbp(k^2/2, k)$. □

By [15, Proposition 14], in the case where $f(X) = X^3$ and G and H are the additive group of $\mathbb{F}_4$, $S(f)$ must split into two sub-structures of 8 points each. Further these sub-structures are identical copies of the same semi-biplane, the hypercube $H(4)$ as described in [15]. We note that this is the only case this construction method will produce the hypercube structure. If there exists a semi-planar function over an abelian group of order 6 then, by [15, Proposition 16], the incidence structure must again split into two sub-structures as there does not exist a $sbp(36, 6)$. The two sub-structures will again be copies of the same semi-biplane, denoted $S_a(18)$ in [15]. The argument involving parallel classes from the proof of the corollary excludes the other two possible $sbp(18, 6)$ structures listed in [15, Proposition 16]. We now consider, in more detail, the problem of whether $S(G, H; f)$ is or is not connected.

Theorem 10 *Let G and H be finite abelian groups written additively and of the same even order k. Let $f : G \to H$ be a semi-planar function. If f is a bijection then $S(G, H; f)$ is connected unless $k = 2$.*

PROOF. Suppose $S(G, H; f)$ splits and f is a bijection. In such cases, for distinct $a, c \in G$ the lines $\mathcal{L}(a, b)$ and $\mathcal{L}(c, b)$ cannot intersect. Consider one of the sub-structures. In our sub-structure the sets $P_a = \{\mathcal{L}(a, b) \mid \text{some } b \in H\}$ form the parallel line-classes. Any line in P_a intersects every line not in P_a (this follows from Theorem 7(v)) and never intersects any line in the class. By our earlier arguments, $|P_a| = k/2$. Let $H_a = \{b \in H \mid \mathcal{L}(a, b) \in P_a\}$. Obviously, $|H_a| = k/2$. For distinct $a, c \in G$, every line in P_a intersects every line in P_c. Since f is bijective then $H_a \cap H_c = \emptyset$ and $H_a \cup H_c = H$. If there exists a third parallel line-class, i.e. $k > 2$, we have a contradiction since $|\cup_{a \in G} H_a| > k$. □

In the trivial case, where $k = 2$, the identity function is the only semi-planar function and the incidence structure does indeed split into two sub-structures.

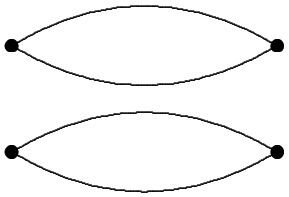

Diagram 1: *The trivial structure generated by the identity when $k = 2$*

In regards to the known semi-planar functions listed in Theorem 3, all are bijections apart from case (ii) when e is even. All of the other semi-planar functions listed in Theorem 3 will therefore generate connected incidence structures. As already noted, the DO monomial X^3 defines, over $\mathbb{F}_4$, an incidence structure which is not connected. In fact, this is the only case where this occurs.

Lemma 11 *Let e be even, α be some natural number satisfying $(\alpha, e) = 1$, and set $q = 2^e$ and $n = 2^\alpha + 1$. Let $f(X) = X^n$. Then the incidence structure $S(f)$ is connected unless $q = 4$.*

PROOF. Fix $b \in \mathbb{F}_q$. Consider a line $\mathcal{L}(a, b)$. Every point $(x, y) \in \mathcal{L}(a, b)$ is contained in a line $\mathcal{L}(c, b)$ with $c \neq a$, if and only if $f(x - a) = f(x - c)$. For fixed $x \in \mathbb{F}_q$, $x \neq a$, there will be $(n, q-1) = 3$ choices of $c \in \mathbb{F}_q$ for which this equation holds (one of which will be $c = a$). So for each point $(x, y) \in \mathcal{L}(a, b)$,

$x \neq a$, there are two distinct lines of the form $\mathcal{L}(c,b)$ with $c \neq a$ containing it. Each of the lines $\mathcal{L}(c,b)$, $c \neq a$, intersecting $\mathcal{L}(a,b)$ do so twice. A simple counting argument now shows that all $q-1$ lines $\mathcal{L}(c,b)$ with $c \neq a$ intersect $\mathcal{L}(a,b)$. An equivalent statement is that the equation $f(x-z)-f(x)=0$ is solvable for all non-zero $z \in \mathbb{F}_q$. By dividing by $f(z)$ this is equivalent to showing the equation $x^{2^\alpha}+x=1$ is solvable. The polynomial $X^{2^\alpha}+X$ has 2^{e-1} distinct images and there are 2^{e-1} elements $x \in \mathbb{F}_q$ which satisfy $Tr(x)=0$. Since $Tr(x^{2^\alpha}+x)=0$ for all $x \in \mathbb{F}_q$ it is clear that $x^{2^\alpha}+x=1$ is solvable if and only if $Tr(1)=0$. This holds as e is even.

Suppose the structure $S(f)$ splits into two semi-biplanes. We use the notation from the previous proof. Consider any $b \in H_a$. From the argument above, all q lines $\mathcal{L}(c,b)$ must be in this sub-structure. By considering all $b \in H_a$, we can account for $q^2/2$ lines in this way. As this is all of the possible lines in the sub-structure, we have $H_a = H_c$ for all $a, c \in \mathbb{F}_q$. Therefore, for every point (x,y) in our sub-structure and every $b \in H_a$, $b \neq y$, there are 3 lines of the form $\mathcal{L}(c,b)$ which contain (x,y). There is a further one line through (x,y) which is $\mathcal{L}(x,y)$. As there are q lines through any point, we have

$$q = 3\Big(\frac{q}{2}-1\Big)+1$$

whereby $q=4$. $\square$

Theorem 10 and Lemma 11 show that all of the known semi-planar monomials listed in Theorem 3 describe $sbp(q^2,q)$ unless $q=2$ or $q=4$ (high school algebra triumphs once again!). All methods of constructing infinite classes of semi-biplanes listed in [9,16,7] generate semi-biplanes whose parameters are never $sbp(k^2,k)$ (there are constructions which yield $sbp(k^2/2,k)$ but the methods are not the same). We note that, by generalising the definition of semi-planar function, the construction method can be generalised to construct semi-symmetric designs. This generalisation will be dealt with in a separate paper. In the current article, we can achieve tighter results by restricting ourselves to the present definition of semi-planar.

4 An association scheme with two associate classes

Definition 12 *An* association scheme with m associate classes *on a v-set X is a family of m symmetric anti-reflexive binary relations on X such that:*

(i) any two distinct elements of X are ith associates for exactly one value of i, where $1 \leq i \leq m$.
(ii) each element of X has n_i ith associates, $1 \leq i \leq m$.

(iii) for each i, $1 \leq i \leq m$, if x and y are ith associates, then there are p^i_{jl} elements of X which are both jth associates of x and lth associates of y.

The numbers v, n_i $(1 \leq i \leq m)$, and p^i_{jl} $(1 \leq i, j, l \leq m)$ are called the parameters of the association scheme. We see that $p^i_{jl} = p^i_{lj}$ and often write $P_i = (p^i_{jl})$.

We now define two binary relations on the points of $S(f)$ which we label R_1 and R_2. For points $\mathcal{P}, \mathcal{Q} \in \mathbb{F}_q \times \mathbb{F}_q$ we have

$$\mathcal{P}R_1\mathcal{Q} \Leftrightarrow \mathcal{P} \text{ and } \mathcal{Q} \text{ are co-incident on exactly 2 lines}$$
$$\mathcal{P}R_2\mathcal{Q} \Leftrightarrow \mathcal{P} \text{ and } \mathcal{Q} \text{ are never co-incident.}$$

We now prove that $S(f)$ and the relations R_1 and R_2 define an association scheme provided the polynomial f is a semi-planar Dembowski-Ostrom monomial which permutes $\mathbb{F}_q$.

Theorem 13 *Let $f(X) = X^{2^\alpha+1}$ be a semi-planar function over $\mathbb{F}_q$ where $q = 2^e$ with e odd. Then the relations R_1 and R_2 define an association scheme on the points of $S(f)$. The parameters of the association scheme are:*

$$n_1 = q(q-1)/2$$
$$n_2 = (q+2)(q-1)/2$$
$$P_1 = \frac{1}{4}\begin{pmatrix} q(q-2) & q^2-4 \\ q^2-4 & q(q+2) \end{pmatrix}$$
$$P_2 = \frac{1}{4}\begin{pmatrix} q(q-2) & q^2 \\ q^2 & (q+4)(q-2) \end{pmatrix}.$$

PROOF. We prove the result by following the definition of an association scheme as given above. Firstly, it is clear that R_1 and R_2 are symmetric and anti-reflexive. As e is odd we have $(2^\alpha+1, q-1) = 1$ and so f is a permutation polynomial over $\mathbb{F}_q$.

(i) It is obvious that for any two distinct points $\mathcal{P}$ and $\mathcal{Q}$ of $S(f)$ we will have either $\mathcal{P}R_1\mathcal{Q}$ or $\mathcal{P}R_2\mathcal{Q}$ but never both.

(ii) See Theorem 7(v) for a proof of n_1 and hence n_2.

(iii) For given points $\mathcal{P}$ and $\mathcal{Q}$, we wish to determine the number of points that are first associates of both of them and to show that it is independent of the points chosen. We do this by first determining the number of intersection points any line through $\mathcal{P}$ has with lines through $\mathcal{Q}$. To simplify the proof, we let $\mathcal{P} = (0,0)$ and the line through $\mathcal{P}$ be $\mathcal{L}(0,0)$. To see that we can do this

without loss of generality observe that, throughout the following argument, we could choose any point and line through that point by making a change of variable.

Let $\mathcal{Q} = (x_0, y_0)$ be the arbitrary second point. The lines through $\mathcal{Q}$ are $\{\mathcal{L}\Big(a, f(x_0+a)+y_0\Big) \mid a \in \mathbb{F}_q\}$. The line in this set with $a = 0$ is parallel with $\mathcal{L}(0,0)$ and so we assume $a \in \mathbb{F}_q^*$. Any intersection point (x, y) of $\mathcal{L}(0,0)$ and $\mathcal{L}\Big(a, f(x_0+a)+y_0\Big)$ must satisfy

$$\begin{aligned} y &= x^{2^\alpha+1} = f(x) \\ y &= f(x+a) + f(x_0+a) + y_0. \end{aligned}$$

So we have

$$\begin{aligned} 0 &= f(x+a) - f(x) + f(x_0+a) + y_0 \\ &= ax^{2^\alpha} + a^{2^\alpha}x + f(a) + f(x_0+a) + y_0 \\ &= ax^{2^\alpha} + a^{2^\alpha}x + ax_0^{2^\alpha} + a^{2^\alpha}x_0 + f(x_0) + y_0 \\ &= a^{2^\alpha}(x+x_0) + a(x+x_0)^{2^\alpha} + c \end{aligned}$$

where $c = f(x_0) + y_0$ is a constant (as x_0 and y_0 are fixed). Letting $z = x + x_0$ we have

$$a^{2^\alpha}z + az^{2^\alpha} = c.$$

Note for the rest of the proof we require $z \neq 0$ and $z \neq x_0$ as we only wish to count those intersection points distinct from $\mathcal{P}$ and $\mathcal{Q}$. If $c = 0$ then $y_0 = f(x_0)$ and so $\mathcal{Q}$ is on the line $\mathcal{L}(0,0)$. Thus the line $\mathcal{L}(0,0)$ will intersect every line through $\mathcal{Q}$ and will define $q-2$ points of intersection other than $\mathcal{P}$ and $\mathcal{Q}$.

Now suppose $c \neq 0$. We wish to determine for how many a is $f(z+a)-f(z) = c+f(a)$ solvable in z. Dividing by $f(a)$ we obtain $\Delta_{f,1}(z/a) = 1 + c/f(a)$. As f is a permutation polynomial and $f(0) = 0$ we have $c/f(a)$ is a permutation function on $\mathbb{F}_q^*$. So our problem reduces to determining for how many $\beta \neq 1$ is the equation $\Delta_{f,1}(z/a) = \beta$ solvable in z and how many distinct solutions are there in such cases. For $\beta \in \mathbb{F}_q$ there are $q/2$ choices of β for which $\Delta_{f,1}(z/a) = \beta$ has 2 solutions and $q/2$ for which it has none. Now the case $\beta = 1$ has the solutions $z/a = 0, 1$. So for $\beta \in \mathbb{F}_q \setminus \{1\}$ there are $(q-2)/2$ choices for which the equation will have a solution. When $\mathcal{P}$ and $\mathcal{Q}$ are 1st associates $z = x_0$ will be a solution. In this case we must remove that β for which $z = x_0$ is a solution (this will not be $\beta = 1$). This leaves $(q-4)/2$ possible choices of β in this case. For each of the possible choices of β there will be two solutions (i.e., two lines with which $\mathcal{L}(0,0)$ intersects) and so this gives a total of $q-4$ intersection points if $\mathcal{P}$ and $\mathcal{Q}$ are 1st associates and $q-2$ if they are not. If they are first associates then there will be two lines through $\mathcal{Q}$ intersecting $\mathcal{L}(0,0)$ at $\mathcal{P}$. Each will intersect $\mathcal{L}(0,0)$ at a second distinct point. These two points have been removed in the previous argument

and so we must now add these two points back in. So overall any line through $\mathcal{P}$ defines $q-2$ intersection points with lines through $\mathcal{Q}$, whether $\mathcal{P}$ and $\mathcal{Q}$ are 1st associates or not.

It remains to determine the number of times we count each intersection point. For chosen arbitrary points $\mathcal{P}$ and $\mathcal{Q}$ we count from the perspective of $\mathcal{P}$. Each of the q lines through $\mathcal{P}$ defines $q-2$ intersection points with lines through $\mathcal{Q}$ giving a count of $q(q-2)$ points. However, each of these points will have been counted 4 times giving an overall count of $q(q-2)/4$ first associates of $\mathcal{P}$ and $\mathcal{Q}$ regardless of whether $\mathcal{P}$ and $\mathcal{Q}$ are first associates or not.

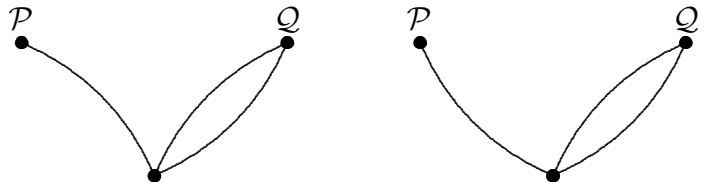

Diagram 2: *Showing how any point that is a first associate of $\mathcal{P}$ and $\mathcal{Q}$ is counted four times in our counting argument.*

Diagram 2 shows how any point of intersection between a line of $\mathcal{P}$ and a line of $\mathcal{Q}$ is counted 4 times. Any point that is a first associate of a point $\mathcal{T}$ is uniquely defined as the intersection point of a pair of lines passing through $\mathcal{T}$. Hence we have, for a chosen line through $\mathcal{P}$ and a chosen point which is a first associate of $\mathcal{P}$ and $\mathcal{Q}$, two lines through $\mathcal{Q}$ which uniquely define it. The chosen line through $\mathcal{P}$ must intersect both of these lines at the same point so counting the point twice. Further, as this point is also a first associate of $\mathcal{P}$ there is a second line through $\mathcal{P}$ which will also count this intersection point twice. We give a second diagram depicting what happens in the case when $\mathcal{P}$ and $\mathcal{Q}$ are on the line chosen although we note it is essentially the same. The key to seeing this is to remember that, in this case, the line chosen going through $\mathcal{P}$ is also a line through $\mathcal{Q}$ and intersects itself. With this in mind it is easy to construct the same argument as for the case shown in Diagram 2.

Diagram 3: *Depicting the special case where $\mathcal{Q}$ is on the line chosen passing through $\mathcal{P}$.*

Finally, having determined p_{11}^1, p_{11}^2 and n_1 it is a simple matter to determine the remaining parameters of the scheme. □

By letting $q = 2k$ in the description of the association scheme given in the above theorem one arrives at the parameters $(4k^2, 2k^2 - k, k^2 - k, k^2 - k)$ corresponding to a class of designs which, under the classification of [2], are known as Menon Designs.

References

[1] T. Beth and C. Ding, *On almost perfect nonlinear permutations*, Advances in Cryptology – Eurocrypt '93 (T. Helleseth, ed.), Lecture Notes in Computer Science, vol. 765, 1993, pp. 65–76.

[2] C.J. Colbourn and J.H. Dinitz (eds.), *CRC Handbook of Combinatorial Designs*, CRC Publishing Co., Florida, 1996.

[3] R.S. Coulter and R.W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. **10** (1997), 167–184.

[4] T.W. Cusick, *Highly nonlinear power functions on finite fields*, unpublished manuscript.

[5] P. Dembowski and T.G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258.

[6] H. Dobbertin, *Construction of bent functions and balanced boolean functions with high nonlinearity*, preprint.

[7] A. Del Fra, *On two new classes of semibiplanes*, Discrete Math. **174** (1997), 107–116.

[8] T. Helleseth and D. Sandberg, *Some power mappings with low differential uniformity*, Appl. Algebra Engrg. Comm. Comput. **8** (1997), 363–370.

[9] D. Hughes, *Biplanes and semi-biplanes*, Combinatorial Mathematics (D.A. Holton and J. Seberry, eds.), Lecture Notes in Mathematics, vol. 686, Springer-Verlag, 1978, pp. 55–58.

[10] T. Kasami, *The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes*, Information and Control **18** (1971), 369–394.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).

[12] K. Nyberg, *Differentially uniform mappings in cryptography*, Advances in Cryptology – Eurocrypt '93 (T. Helleseth, ed.), Lecture Notes in Computer Science, vol. 765, 1993, pp. 55–64.

[13] K. Nyberg and L.R. Knudsen, *Provable security against differential cryptanalysis*, Advances in Cryptology – Crypto '92 (E.F. Brickell, ed.), Lecture Notes in Computer Science, vol. 740, 1992, pp. 566–574.

[14] L. Rónyai and T. Szőnyi, *Planar functions over finite fields*, Combinatorica **9** (1989), 315–320.

[15] P. Wild, *Generalized Hussain graphs and semibiplanes*, Ars Combinatoria **14** (1982), 147–167.

[16] ———, *Some families of semibiplanes*, Discrete Math. **138** (1995), 397–403.