Proceedings of the Fifteenth Australasian Workshop on Combinatorial Algorithms, AWOCA 2004 (S-H. Hong, ed.), 2004, pp. 192-198

On the splitting case of a semi-biplane construction

Robert S. Coulter * Marie Henderson *

Dedicated to Jennifer Seberry on the occasion of her 60^{th} birthday.

Abstract

We consider the case where a particular incidence structure splits into two substructures. The incidence structure in question was used previously by the authors to construct semi-biplanes $sbp(k^2, k)$ or $sbp(k^2/2, k)$. A complete description of the two substructures is obtained. We also show that none of the three semi-biplanes, $sbp(18, 6)$, can be described using this construction.

1 Introduction.

Let G and H be finite abelian groups written additively and of the same even order k. We call a function $f : G \to H$ a *semi-planar* function if for every non-identity $a \in G$ the equation

$$\Delta_{f,a}(x) = f(x + a) - f(x) = y,$$

with $y \in H$, has either 0 or 2 solutions $x \in G$. Semi-planar functions are better known in communication security as almost perfect non-linear functions, see [3], or differentially 2-uniform functions, see [2].

A *semi-biplane*, or $sbp(v, k)$, is a connected incidence structure which satisfies the following.

(i) Any two points are incident with 0 or 2 common lines.

(ii) Any two lines are incident with 0 or 2 common points.

Such a design contains v points, and v lines with every point occurring on k lines, and every line containing k points. In [1] the authors developed the following method for constructing semi-biplanes using semi-planar functions.

Let G and H be as above and let $f : G \to H$. Define the incidence structure $S(G, H; f)$ by:

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

When the context is clear, we shall denote the incidence structure simply by $S(f)$. The following is Proposition 9 of [1].

*Department of Mathematical Sciences, Ewing Hall, University of Delaware, Newark, DE, 19716, U.S.A. E-mail:{coulter,marie}@math.udel.edu

Lemma 1 *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$(k^2/2, k)$.*

So the designs of [1] are either connected or consist of two separate substructures of equal size. Also from [1] is the following.

Lemma 2 *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 $k = 2$.*

As there are bijective semi-planar functions known over the additive group of any finite field $\mathbb{F}_q$, with $q = 2^e$ and $e \geq 3$, it follows that there exist *sbp*$(2^{2e}, 2^e)$ for all integers $e \geq 3$. There is only one known class of non-bijective semi-planar functions: the monomials $f(X) = X^{2^\alpha+1}$ over $\mathbb{F}_{2^e}$ are semi-planar if and only if $(\alpha, e) = 1$. Here, too, it can be shown that $S(f)$ is connected provided $e \geq 3$, see Lemma 11 of [1]. When $e = 2$, then we must have $f(X) = X^3$ and $S(f)$ splits into two identical copies of the hypercube $H(4)$ ($H(k)$ is the semi-biplane whose incidence graph is the graph of the k-dimensional hypercube). As $H(k)$ is a *sbp*$(2^{k-1}, k)$, it is easily seen that $S(G, H; f)$ can only describe a hypercube in this case.

In this paper we are interested in the case where $S(f)$ splits into two substructures, as at this point the only known examples which do this are the degenerate case where $k = 2$ or the case $k = 4$ with $G = H = \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$, the hypercube case. We look at the general theory for the case where $S(f)$ splits in Section 2. Our main result gives a complete description of the two substructures in this case, see Theorem 4. Proposition 16 of [4] shows that there are exactly three non-isomorphic *sbp*$(18, 6)$, while there are no *sbp*$(36, 6)$. So if a semi-planar function f over $\mathbb{Z}_6^+$ exists, then $S(\mathbb{Z}_6^+, \mathbb{Z}_6^+; f)$ must split into two substructures. In Section 3, we show that no semi-planar function exists over $\mathbb{Z}_6^+$ and hence none of the three *sbp*$(18, 6)$ can be described by the construction of [1].

2 General Theory

For each pair $a \in G$, $b \in H$ define

$$S(a, b) = \{t \in G : f(t - a) = f(t) + b\}.$$

Note that if f is semi-planar, then for each pair $(a, b) \in G \times H$ with $a \neq 0$, either $|S(a, b)| = 2$ or $|S(a, b)| = 0$.

Lemma 3 *Let G and H be two finite abelian groups (written additively) of even order k and $f : G \to H$ be semi-planar. For each pair $a \in G$, $b \in H$, with $a \neq 0$, $|S(a, b)| = 2$ if and only if*

$$\mathcal{L}(\alpha a, d + b) \cap \mathcal{L}((\alpha + 1)a, d) \neq \varnothing$$

for all $d \in H$ and $\alpha \in \mathbb{Z}$.

Proof: Let $a \in G$, $b \in H$ and $a \neq 0$. For all $d \in H$ and $\alpha \in \mathbb{Z}$, the lines $\mathcal{L}(\alpha a, d + b)$ and $\mathcal{L}((\alpha + 1)a, d)$ intersect (twice) if and only if $y = f(x - \alpha a) + d + b = f(x - (\alpha + 1)a) + d$. Equivalently,

$$f(x - (\alpha + 1)a) - f(x - \alpha a) = b$$

has two solutions. Substituting for $z = x - \alpha a$, we have $f(z-a) - f(z) = b$ has two solutions, or in other words, the lines intersect if and only if $|S(a,b)| = 2$. $\square$

A semi-biplane is called *divisible* if the points can be partitioned into classes so that the following property holds: two points from a class lie on no common line and two points from different classes lie on exactly two lines.

Theorem 1 *Suppose G and H are two finite abelian groups (written additively) of even order k and $f : G \to H$ is semi-planar. If $S(G,H;f)$ splits into two substructures, then the resulting sbp$(k^2/2, k)$ are both divisible.*

Proof: A useful property of $S(f)$ is that it is self-dual, see Theorem 7 of [1]. Hence we need only show the equivalent statement holds for lines. Let S_1 and S_2 be the two substructures of $S(G,H;f)$. Let

$$P_a = \{b \in H \,:\, \mathcal{L}(a,b) \in S_1\}$$

for each $a \in G$. We will show that the set $\{P_a \,:\, a \in G\}$ gives the required classes. From the proof of Proposition 9 of [1] there are exactly $k/2$ elements in each set P_a. Also, every point of S_1 is in $\bigcup_{b \in P_a} \mathcal{L}(a,b)$ as $\mathcal{L}(a,b_1) \cap \mathcal{L}(a,b_2) = \varnothing$ for all distinct $b_1, b_2 \in P_a$ and S_1 contains exactly $k^2/2$ points.

Now choose distinct $a, c \in G$. We claim that $\mathcal{L}(a,b) \cap \mathcal{L}(c,d) \neq \varnothing$ for each $b \in P_a$ and $d \in P_c$. If this was not the case, then there is a non-empty list of lines from P_a which have a common point with $\mathcal{L}(c,d)$, say $\mathcal{L}(a,b_1), \mathcal{L}(a,b_2), \ldots, \mathcal{L}(a,b_t)$, where $t < k/2$. From the definition of incidence, and as f is a semi-planar function, we have a pair of solutions (x,y) for each member of the above list, given by

$$y = f(x-a) + b_i = f(x-c) + d.$$

By substituting $z = x - a$ we obtain

$$\Delta_{f,c-a}(z) = f(z-(c-a)) - f(z) = b_i - d.$$

In other words, $\Delta_{f,c-a}(z) = b_i - d$ has 2 solutions $z \in G$ for each $1 \leq i \leq t$. Overall, this accounts for $2t < k$ of the k values of $\Delta_{f,c-a}(z)$. The remaining values of $\Delta_{f,c-a}(z)$ must therefore correspond to elements $b \in H$ for which $\mathcal{L}(a,b)$ and $\mathcal{L}(c,d)$ intersect and $\mathcal{L}(a,b) \in S_2$. However this contradicts the assumption that $S(G,H;f)$ splits into two substructures. It follows that $|\mathcal{L}(a,b) \cap \mathcal{L}(c,d)| = 2$ for any $b \in P_a$ and $d \in P_c$ where $a, c \in G$ are distinct while $\mathcal{L}(a,b_1) \cap \mathcal{L}(a,b_2) = \varnothing$ where $b_1, b_2 \in H$ are distinct. Hence S_1 is divisible. A similar argument shows S_2 is also divisible. $\square$

Note that from the above proof we know that if $S(f)$ splits, then the lines $\mathcal{L}(a,b)$ and $\mathcal{L}(c,d)$ from the same substructure must intersect when $a \neq c$. This will be used extensively in what follows.

For the remainder of this section we suppose $f : G \to H$ is semi-planar, $|G| = |H| = k > 2$, and $S(f)$ splits into two substructures S_1 and S_2 with $\mathcal{L}(0,0) \in S_1$. Note that, by Lemma 2, f is not a bijection. For $i = 1, 2$, define

$$P_a^i = \{b \in H \,:\, \mathcal{L}(a,b) \in S_i\}.$$

For each $a \in G$, $P_a^1 \cap P_a^2 = \varnothing$ while $P_a^1 \cup P_a^2 = H$, so the subsets P_a^1 and P_a^2 of H, partition H.

Lemma 4 *For non-zero $a \in G$,*

$$P_a^1 = \{b \in H \,:\, |S(a,b)| = 2\},$$
$$P_a^2 = \{b \in H \,:\, |S(a,b)| = 0\}.$$

Proof: As P_a^1 and P_a^2 partition H then we need only consider one of the subsets, say P_a^1. By Lemma 3, $\mathcal{L}(0,0) \cap \mathcal{L}(a,b) \neq \varnothing$ if $|S(a,b)| = 2$. But Theorem 1 shows, by duality, that for $a \neq 0$, $\mathcal{L}(a,b) \in S_1$ if and only if $\mathcal{L}(a,b)$ and $\mathcal{L}(0,0)$ intersect. □

Theorem 2 *The set P_0^1 is the subgroup of H of index 2 and P_0^2 is its coset.*

Proof: If $0 \in P_a^1$, then $\mathcal{L}(0,d) \cap \mathcal{L}(a,d) \neq \varnothing$ for all $d \in H$, by Lemma 3. Thus $P_a^i = P_0^i$ in this case. Let

$$T = \{a \in G \,:\, a \neq 0 \wedge |S(a,0)| = 2\}.$$

As f is not a bijection, there exists a non-zero $a \in G$ for which $f(t-a) = f(t)$ has a solution, which implies T is non-empty. Let $a \in T$. For $b_1 \in P_a^1$, $|S(a,b_1)| = 2$ and $f(x-a) = f(x)+b_1$ has two solutions. Hence for any $b_2 \in P_a^1$, we must have $f(x-a)+b_2 = f(x)+b_1+b_2$ has two solutions, or equivalently, $\mathcal{L}(a,b_2) \cap \mathcal{L}(0,b_1+b_2) \neq \varnothing$. As $b_2 \in P_a^1 = P_0^1$ and $\mathcal{L}(a,b_2)$ intersects $\mathcal{L}(0,b_1+b_2)$, it follows that $b_1+b_2 \in P_a^1 = P_0^1$. To summarise, $b_1, b_2 \in P_0^1$ implies that $b_1+b_2 \in P_0^1$, that is P_0^1 is closed under addition. It follows that P_0^1 is a subgroup of H of index two. As $P_0^1 \cap P_0^2 = \varnothing$ while $P_0^1 \cup P_0^2 = H$, P_0^2 is the coset of P_0^1 in H. □

Lemma 5 *If $P_a^i \cap P_c^i \neq \varnothing$, for $i = 1$ or $i = 2$, then $P_{a-c}^1 = P_{c-a}^1 = P_0^1$.*

Proof: Suppose $P_a^i \cap P_c^i \neq \varnothing$ where $i = 1$ or $i = 2$. Then there exists a $b \in H$ such that $\mathcal{L}(a,b) \cap \mathcal{L}(c,b) \neq \varnothing$. This, in turn, implies that there is a $t \in G$ for which we have $f(t-a) - f(t-c) = 0$. By substituting for $z = t-c$ we obtain $f(z-(a-c)) - f(z) = 0$. So $f(z) = f(z-(a-c))$ which implies $\mathcal{L}(0,0) \cap \mathcal{L}(a-c,0) \neq \varnothing$. As shown in the proof of Theorem 2, since $0 \in P_{a-c}^1$, it follows that $P_{a-c}^1 = P_0^1$ as required. A similar argument shows $P_{c-a}^1 = P_0^1$. □

Consider the set $A = \{a \in G \,:\, P_0^1 = P_a^1\}$. By Lemma 5, whenever $P_a^i \cap P_c^i \neq \varnothing$ for $i = 1$ or $i = 2$, then $a - c \in A$ and $c - a \in A$. Clearly $0 \in A$ and $|A| > 1$. For any $a, c \in A$, successive applications of Lemma 5 show $-c \in A$ and $a - (-c) = a + c \in A$. Hence A is closed and since G is finite, A is a subgroup of G. If $|A| < k/2$, then $|G \setminus A| > k/2$. Now for some fixed $a \in G \setminus A$ we have

$$|\{a - c \,:\, c \in G \setminus A\}| > k/2.$$

But $\{a-c \,:\, c \in G \setminus A\} \subset A$, contradicting $|A| < k/2$. So we must have $|A| \geq k/2$ and since A is a subgroup of G, $|A| = k/2$ or $A = G$. This proves the following statement, common in theme with Theorem 2.

Theorem 3 *The set $A = \{a \in G \,:\, P_0^1 = P_a^1\}$ is either the subgroup of G of index 2 or $A = G$.*

A combination of Theorems 2 and 3 proves our main theorem (which shows that if the structure splits, there are only two possibilities).

Theorem 4 *Let $f : G \to H$ be a semi-planar function where G and H are abelian groups of even order k and A and B the index two subgroups of G and H, respectively. Let $g \in G \setminus A$ and $h \in H \setminus B$. If $S(f)$ splits into two substructures S_1 and S_2, with $\mathcal{L}(0,0) \in S_1$, then either*

(i) $\mathcal{L}(a,b) \in S_1$ if and only if $(a \in G \wedge b \in B)$, or

(ii) $\mathcal{L}(a,b) \in S_1$ if and only if $(a \in A \wedge b \in B) \vee (a \in A + g \wedge b \in B + h)$.

We note that the theorem also holds for the case $k = 2$. In this case, $f(x) = x$ or $f(x) = x + 1$. In either case, f is a bijection and the splitting structures correspond to case (ii). The theorem allows us to show that the two substructures obtained are isomorphic.

Corollary 1 *For any $h \in H \setminus B$, the mapping $\phi_h : G \times H \to G \times H$ defined by*

$$\phi_h(x, y) = (x, y + h)$$

acts as an isomorphism between the two substructures of $S(f)$.

Our final general result, which is a simple extension of [3], Proposition 1, will be needed in the next section.

Lemma 6 *If $f : G \to H$ is a semi-planar function, then*

$$\psi(f(\phi(x) + c)) + d$$

is a semi-planar function from G to H where $\phi \in Aut(G)$, $\psi \in Aut(H)$, $c \in G$, and $d \in H$.

3 The Case $G = H = \mathbb{Z}_6^+$

In this section we consider the case where $G = H = \mathbb{Z}_k^+$ with k even. In this case, we represent the mapping $f : \mathbb{Z}_k^+ \to \mathbb{Z}_k^+$ by $f = \langle b_0, b_1, \ldots, b_{k-1} \rangle$ where $f(i) = b_i$ for $0 \leq i \leq k - 1$.

Lemma 7 *Let $f : \mathbb{Z}_k^+ \to \mathbb{Z}_k^+$ with $k > 4$. If $f(x) = y$ has more than $k/2$ solutions $x \in \mathbb{Z}_k^+$ for any given $y \in \mathbb{Z}_k^+$, then f is not semi-planar.*

Proof: Suppose that the claim does not hold. Then f is semi-planar and there exists $y \in \mathbb{Z}_k^+$ such that $|S| > k/2$ where $S = \{x \in \mathbb{Z}_k^+ : f(x) = y\}$. We wish to show that there exists an $a \in \mathbb{Z}_k^+$ such that $f(x + a) - f(x) = 0$ has more than two solutions. Consider $f = \langle b_0, b_1, \ldots, b_{k-1} \rangle$. As $|S| > k/2$ there must be two consecutive elements of this list which are equal. Using Lemma 6, we may assume $b_0 = b_1 = y$.

If f is semi-planar, then $\Delta_{f,1}(x) = 0$ must have two solutions. There are 2 cases. If $b_2 = y$, then we have three consecutive values of f equal to y and there can be no other consecutive values of f equal. Thus $b_3 \neq y$, and the remaining $k/2 - 2$ values of y must be placed in $k - 4$ places with no consecutive places equal. It can be seen that the only way to assign the remaining y values is $b_j = y$ when j is even. Thus, if $k > 4$, $\Delta_{f,2}(x) = 0$ has more than two solutions, a contradiction. If $b_2 \neq y$, then there are $k - 3$ remaining assignments of which $k/2 - 1$ must be y and where $b_{k-1} \neq y$ as this is equivalent to the previous case by Lemma 1. Provided $k > 4$, it follows that $\Delta_{f,2}(x) = 0$ has at least three solutions, contradicting that f is semi-planar. □

It was shown in [4] that no $sbp(36,6)$ exists while there are three non-isomorphic $sbp(18,6)$. It follows that if a semi-planar function exists over $\mathbb{Z}_6^+$, then the corresponding structure necessarily splits. We now show that this case is not possible. Although this might be tested for computationally, a mathematical proof is preferable.

Theorem 5 *There is no semi-planar function over* $\mathbb{Z}_6^+$.

Proof: Suppose f is a semi-planar function over $\mathbb{Z}_6^+$. By Lemma 6 we may assume that $f(0)=0$ and that no image of f occurs more often than $0 \in \mathbb{Z}_6^+$. Further, by Lemma 7, $f(x)=0$ has at most three solutions. Let

$$f = \langle 0, b_1, b_2, b_3, b_4, b_5 \rangle.$$

As noted, $S(f)$ must split. As before we denote the two substructures by S_1 and S_2 where $\mathcal{L}(0,0) \in S_1$. It follows from Theorem 4 that there are two cases.

First assume $\mathcal{L}(a,b) \in S_1$ if and only if $b \in \{0,2,4\}$. It follows that $b_i \in \{0,2,4\}$ and that $|S(a,0)| = 2$ for all $a \in \mathbb{Z}_6^+$. In particular, from $a=1$ there exists two distinct integers $r, s \in \mathbb{Z}_6^+$ such that $b_{r-1} = b_r$ and $b_{s-1} = b_s$. Appealing to Lemma 6 we may assume, without loss of generality, that $b_{r-1} = b_r = 0$ and $r = 1$. Either $b_s = 0$ or $b_s \in \{2,4\}$. If $b_s = 0$, then since $f(x) = 0$ can have at most three solutions, we must have $s = 2$ and hence $f = \langle 0,0,0,b_3,b_4,b_5 \rangle$ with $b_3, b_4, b_5 \in \{2,4\}$. Now $\Delta_{f,3}(\mathbb{Z}_6^+) = \{2,4\}$. However, as f is semi-planar, the value set of $\Delta_{f,3}$ must have size three. So $b_s \neq 0$ and $s > 2$. As $\phi(x) = -x$ is an automorphism of $\mathbb{Z}_6^+$, we may assume $b_s = 2$ by Lemma 6. There are three possibilities:

$$f = \langle 0,0,2,2,b_4,b_5 \rangle,$$
$$f = \langle 0,0,b_2,2,2,b_5 \rangle,$$
$$f = \langle 0,0,b_2,b_3,2,2 \rangle.$$

In the first case, $b_5 \neq 0$, $b_4 \neq 2$ and $b_4 \neq b_5$. Hence $b_4 = 0$. But then $b_5 \in \{2,4\}$ and either leads to $\Delta_{f,2}(x) = 2$ having three solutions. Similar arguments remove the other two possibilities. It follows that no semi-planar function exists in this case.

Now assume that $\mathcal{L}(a,b) \in S_1$ if and only if $a, b \in \{0,2,4\}$ or $a, b \in \{1,3,5\}$. This time we have $b_i \equiv i \bmod 2$. By considering $\Delta_{f,2}(x)$, an application of Lemma 6 shows we may assume that $b_0 = b_2 = 0$ and $b_4 = 2$. Likewise, we must have $b_i = b_j$ for a pair $i, j \in \{1,3,5\}$. We first consider the situation $f = \langle 0,t,0,t,2,v \rangle$ with $t \neq v$. It is immediate that $t = 5$ as otherwise $\Delta_{f,1}(x) = t$ has at least three solutions. But if $t = 5$ then obviously $v \neq 5$, and also, by considering $\Delta_{f,1}(x)$, $v \neq 1$. So now $t = 5$ and $v = 3$. But then $\Delta_{f,3}(x) = 3$ has four solutions. It remains to deal with the case $f = \langle 0,t,0,v,2,v \rangle$. By considering $\Delta_{f,3}$, it follows that $t = 5$ and $v = 1$. But then $\Delta_{f,1}(x) = 1$ has three solutions. Hence no semi-planar function exists in this case either. All possibilities have been exhausted and the result follows. □

Our last result shows that the splitting case cannot occur when $k = 6$. It is an open problem to determine a semi-planar function over any abelian group of order $k > 4$ where the splitting case occurs. We conjecture that no such function exists.

Acknowledgement

This work is based on results published in [1]. During the development of that article, we sought advice from various people about the type of objects we were constructing. It is a pleasure to acknowledge here that it was Jennifer Seberry who noted our structures were semi-biplanes and suggested several references.

References

[1] R.S. Coulter and M. Henderson, *A class of functions and their application in constructing semi-biplanes and association schemes*, Discrete Math. **202** (1999), 21–31.

[2] 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.

[3] 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.

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