ORTHOMORPHISMS AND THE CONSTRUCTION OF PROJECTIVE PLANES

FELIX LAZEBNIK AND ANDREW THOMASON

Abstract. We discuss a simple computational method for the construction of finite projective planes. The planes so constructed all possess a special group of automorphisms which we call the group of translations, but they are not always translation planes. Of the four planes of order 9, three admit the additive group of the field $GF(9)$ as a group of translations, and the present construction yields all three. The known planes of order 16 comprise four self-dual planes and eighteen other planes (nine dual pairs); of these, the method gives three of the four self-dual planes and six of the nine dual pairs, including the "sporadic" (not translation) plane of Mathon.

2000 Mathematics Subject Classification: 05B15, 05C50, 05C62, 51E15, 68R10.

1. Introduction

We discuss a simple computational method for the construction of finite projective planes. The planes so constructed all possess a special group of automorphisms which we later will define as *translations*, but they are not all what finite geometers call translation planes(e.g., see [3] or [10] or [12]).

Of the four planes of order 9, three admit the additive group of the field $GF(9)$ as a group of translations, and the present construction yields all three. The known planes of order 16 (see [20]) comprise four self-dual planes and eighteen other planes (nine dual pairs); of these, the method gives three of the four self-dual planes and six of the nine dual pairs, including the "sporadic" (not translation) plane of Mathon [5], [14].

2. Graphs without 4-cycles, Planes and Orthomorphisms

We examine here a simple construction for graphs that are the point-line incidence graphs of projective planes. Let G be a finite abelian group, whose order is denoted q. The construction associates with each function $f : G \times G \to G$ a graph which, under certain circumstances, gives rise to a plane. It is convenient to think of f as a $q \times q$ square array or matrix, so that we can speak of the *rows* and *columns* of f (meaning the restrictions of f to $\{a\} \times G$ or $G \times \{a\}$ for some $a \in G$).

2.1. Graph and plane constructions.

2.1. Graph and plane constructions. Let P and L be two copies of $G \times G$. The elements of P are labelled $p = (p_1, p_2)$ and are called *points*, while those of L are labelled $l = [l_1, l_2]$ and are called *lines*.

Date: August 13, 2003.

Key words and phrases. Orthomorphisms, projective planes, translation.

This research was supported partially by a grant from the London Mathematical Society.

Given $f : G \times G \to G$, we define the bipartite graph Γ_f in the following way. The vertex set of Γ_f is $P \cup L$, P and L are color classes, and for $p = (p_1, p_2) \in P$, $l = [l_1, l_2] \in L$,

$$pl \in E(\Gamma_f) \;\text{ iff }\; p_2 + l_2 = f(p_1, l_1)\,. \qquad (\dagger)$$

Clearly the graphs Γ_f having order $2q^2$ are q-regular; indeed, each point $p \in P$ has, for each $l_1 \in G$, exactly one neighbour $[l_1, l_2]$, and likewise each line $l \in L$ has exactly one neighbour (p_1, p_2) for each $p_1 \in G$. Hence the size (number of edges) of Γ_f is q^3.

Next we define a bipartite graph Π_f which contains Γ_f as an induced subgraph. Let P^* be the set formed from P by adding the $q+1$ elements (p), where $p \in G$, and (∞). Likewise let L^* be formed by adding to L the $q+1$ elements $[l]$, $l \in G$, and $[\infty]$. The bipartite graph Π_f has vertex set $P^* \cup L^*$; it contains the graph Γ_f as an induced subgraph, together with additional edges

$$\{(p)[p, l_2] \;:\; p, l_2 \in G\}\;,$$
$$\{[l](l, p_2) \;:\; l, p_2 \in G\}\;,$$
$$\{(\infty)[l] \;:\; l \in G\}\;,$$
$$\{(p)[\infty] \;:\; p \in G\}\;,$$

and $(\infty)[\infty]$. Therefore graph Π_f has both color classes of cardinality q^2+q+1 and is regular of degree $q+1$. It also follows from the definition of Π_f that it contains no 4-cycle if and only if graph Γ_f contains no 4-cycles. The following statement is an immediate corollary of Bollobás [1, Lemma 2.1, pages 309-310] and can be easily checked.

Proposition. *Graph Π_f is isomorphic to the point-line incidence graph of a projective plane of order q if and only if Γ_f contains no 4-cycles.*

(The above method of extending a graph Γ_g to the point-line incidence graph was shown to one of the authors by Ustimenko [21].) Now two distinct vertices (p_1, p_2) and (p_1', p_2') of the graph Γ_f have a common neighbour $[l_1, l_2]$ if and only if $p_2 - p_2' = f(p_1, l_1) - f(p_1', l_1)$ (and so necessarily $p_1 \neq p_1'$). Hence these vertices lie in a 4-cycle if and only if there is some $l_1' \neq l_1$ such that $f(p_1, l_1) - f(p_1', l_1) = f(p_1, l_1') - f(p_1', l_1')$. So the condition that Γ_f have no 4-cycles is equivalent to the following simple condition on the function f:

$$f(a,b) - f(a',b) \;\neq\; f(a,b') - f(a',b') \qquad \text{for all } a \neq a', b \neq b' \in G$$

or, equivalently,

$$f(a,b) - f(a,b') \;\neq\; f(a',b) - f(a',b') \qquad \text{for all } a \neq a', b \neq b' \in G\,.$$

We call the function $d : G \to G$ given by $d(b) = f(a,b) - f(a',b)$ the *difference* of the two rows of f indexed by a and a'. Thus, Γ_f has no 4-cycles if and only if every two rows of f differ by a permutation of G, or, equivalently, every two columns differ by a permutation of G. We call a function f satisfying this condition a *plane* function, since Π_f is a projective plane if and only if f is a plane function.

Remark. Our motivation for these definitions was to study the most general functions f that would produce graphs of girth 4 subject to the condition ($\dagger$). The condition ($\dagger$) itself is a special case of a general construction discussed by Lazebnik and Woldar [13], which was in turn motivated by the construction of graphs of large girth. The number of all functions $f : G \times G \to G$ is very large when $|G| = 16$

but, using the observations developed below, it is possible to make an exhaustive analysis of the case when G is the additive group of the field $\mathbb{F}_{16} = GF(16)$.

Remark. Our notion of a plane function should not be confused with the notion of a planar function introduced by Dembowski and Ostrom in [4] and later used extensively in the contexts of both projective planes and permutation polynomials (see, e.g., Rónyai and Szőnyi [18], Hiramine [11], Gluck [9], Coulter and Matthews [2]). Given two finite groups G and H of the same order, both written additively, but not necessarily commutative, a function $g : G \to H$ is called *planar* if for every $a \in G \setminus \{0\}$ the functions defined by $x \to g(a+x) - g(x)$ and $x \to -g(x) + g(x+a)$ are both bijections from G to H. In the case when both G and H are additive groups of the field $\mathbb{F}_q$, planar functions are often referred to as *difference* permutation polynomials. In this case, following [4], given a planar function g, an incident structure leading to a part of an affine plane is defined as follows: “Points” are the elements of $\mathbb{F}_q \times \mathbb{F}_q$. “Lines” are the symbols $L(a, b)$, with $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$, and the “incidence” I is defined by

$$(x, y)\,\mathrm{I}\,L(a, b) \quad \text{if and only if} \quad y = g(x - a) + b.$$

So a planar function g is equivalent (subject to the unimportant replacement of (a, b) by $(-a, -b)$) to a plane function of the special form $f(x, y) = g(x + y)$. However, in the case when G is the additive group of a field of characteristic 2, no functions f of this kind can satisfy the criterion to be a plane, since if $a = b' \neq a' = b$, then $f(a, b) - f(a', b) = g(a + b) + g(0) = f(a, b') - f(a', b')$. The main results of this paper correspond to the characteristic 2 case, so unfortunately the theory of planar functions cannot help.

2.2. **Isomorphisms.** Let $f, g : G \times G \to G$ and suppose that $\phi : \Gamma_f \to \Gamma_g$ is a graph isomorphism. If ϕ has the property that $\phi : P \to P$, $\phi : L \to L$, and the first coordinates of $\phi(p)$ and $\phi(l)$ depend only on the first coordinates of p and l, respectively, then ϕ extends naturally to an isomorphism $\phi^* : \Pi_f \to \Pi_g$. In this case, we call ϕ a *plane* isomorphism, since if Γ_f contains no 4-cycles, then ϕ^* is an isomorphism of projective planes.

Here are a few straightforward such isomorphisms.

(1) *Translate.* Given $a \in G$, let $\phi : \Gamma_f \to \Gamma_f$ be given by

$$(p_1, p_2) \mapsto (p_1, p_2 + a) \qquad \text{and} \qquad [l_1, l_2] \mapsto [l_1, l_2 - a]\,.$$

For every function f, this gives a plane automorphism of Γ_f to itself. We call the corresponding automorphism of the projective plane a *translation.* Thus, all the planes we construct admit a group of translation which is isomorphic to G, though they are *not* all translation planes in the sense of [10] or [3], or [12], whose definition we decide to omit.

(2) *Zeroize.* Let $c, d : G \to G$ and let $f, g : G \times G \to G$ be given by

$$g(x, y) \;=\; f(x, y) \;+\; c(x) \;+\; d(y)\,.$$

Then there is a plane isomorphism $\phi : \Gamma_f \to \Gamma_g$ given by

$$(p_1, p_2) \mapsto (p_1, p_2 + c(p_1)) \qquad \text{and} \qquad [l_1, l_2] \mapsto [l_1, l_2 + d(l_1)]\,.$$

In particular, by choosing suitable c and d, we see that every Γ_f is plane isomorphic to a Γ_g where the first row and column of g are zero; that is, $g(0, a) = g(a, 0) = 0$ for all $a \in G$.

(3) *Permute.* Let σ and τ be permutations of G, and let $f, g : G \times G \to G$ be given by

$$g(x, y) = f(\sigma x, \tau y).$$

Then there is a plane isomorphism $\phi : \Gamma_f \to \Gamma_g$ given by

$$(p_1, p_2) \mapsto (\sigma^{-1} p_1, p_2) \qquad \text{and} \qquad [l_1, l_2] \mapsto [\tau^{-1} l_1, l_2].$$

In particular, by choosing suitable σ and τ, we see that every Γ_f for which f is a plane function is plane isomorphic to a Γ_g where the second row and column of g are the identity map; that is, $g(1, a) = g(a, 1) = a$ for all $a \in G$, where 1 denotes the second element in some ordering of G (the first element being 0).

Note that this operation applied to a zeroized map (as just previously described) produces another zeroized map. That is, every such Γ_f is plane isomorphic to a Γ_g where the first row and column of g are zero and the second row and column are the identity. We call such a g *normalized.*

(4) *Transpose.* Let $f, g : G \times G \to G$ be given by

$$g(x, y) = f(y, x).$$

Then there is an isomorphism $\phi : \Gamma_f \to \Gamma_g$ given by

$$(p_1, p_2) \mapsto [p_1, p_2] \qquad \text{and} \qquad [l_1, l_2] \mapsto (l_1, l_2).$$

This isomorphism is *not* a plane isomorphism, but there is a natural isomorphism between the plane Π_f and the *dual* of the plane Π_g. Note that, if f is normalized (in the sense just previously described), then so is g.

(5) *Additive transform.* Let $A : G \to G$ be an isomorphism of group G: that is, A is a bijection and $A(a + b) = A(a) + A(b)$ for all $a, b \in G$. Let $f, g : G \times G \to G$ be given by

$$g(x, y) = Af(x, y).$$

Then there is a plane isomorphism $\phi : \Gamma_f \to \Gamma_g$ given by

$$(p_1, p_2) \mapsto (p_1, Ap_2) \qquad \text{and} \qquad [l_1, l_2] \mapsto [l_1, Al_2].$$

The use of the isomorphisms (1) – (5) reduces the number of functions f that need to be examined in any exhaustive computational search.

2.3. **Orthomorphisms.** As shown above, we may restrict our attention to normalized functions. A normalized plane function has its first row and column zero, its second row and column are the identity, and each row differs from any other by a permutation.

An *orthomorphism* of G is a permutation σ of G, such that σ differs from the identity by a permutation; that is, the map $a \mapsto \sigma a - a$ is a permutation of G.

Therefore f is a normalized plane function if and only if its first row and column are zero, its second row and column are the identity, and all other rows are orthomorphisms which fix zero and which pairwise differ by a permutation (or, equivalently, all other columns are orthomorphisms which pairwise differ by a permutation).

For example, if G is the field of order 5 and $f : G \times G$ is the function described by the array

$$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 0 & 3 & 1 & 4 & 2 \\ 0 & 4 & 3 & 2 & 1 \end{array}$$

then f is normalized; moreover, each row is an orthomorphism (for instance, the fourth row differs from the identity by the permutation 02413), and the rows differ pairwise by permutations. Thus f is a normalized plane function and so Π_f is a projective plane — namely, of course, the Desarguesian plane of order 5.

The existence of orthomorphisms for a finite abelian group is given by a theorem of Paige [16, 17]: a finite abelian group admits an orthomorphism if and only if its Sylow 2-subgroup is trivial or non-cyclic. A proof can also be found in Evans [7, page 19]. The necessity of the conditions is also proved in Van Lint and Wilson [22, page 264]. It is easy to see that if a group G has an odd order, then the map $g \to g^2$ is an orthomorphism of G. Paige's theorem implies that $\mathbb{Z}_n$ admits orthomorphisms only if n is odd. For much more on orthomorphisms, on their relation to other notions of combinatorics and geometry, and on orthomorphism graphs (next section) one can consult an excellent monograph by Evans [7].

3. The orthomorphism graph

We consider only orthomorphisms that fix zero; note that, if π is any orthomorphism, then so is the map $x \mapsto \pi(x + a) + b$ for any two elements $a, b \in G$, and it is easy to choose a and b so that the resulting orthomorphism fixes zero.

The orthomorphism graph $\mathrm{Orth}(G)$ has, as vertices, all orthomorphisms of G that fix zero, and $\pi\sigma$ is an edge of $\mathrm{Orth}(G)$ if $\pi - \sigma$ is an orthomorphism of G (necessarily fixing zero).

Let a be any non-zero element of G and let π be a vertex of $\mathrm{Orth}(G)$. Then $\pi(a) \neq 0$ since π fixes zero, and $\pi(a) \neq a$ since π minus the identity is a permutation that fixes zero. Thus $\pi(a) \in G - \{0, a\}$. Moreover, if σ is another vertex of G and $\pi(a) = \sigma(a)$, then $(\pi - \sigma)(a) = 0 = (\pi - \sigma)(0)$ so $\pi\sigma$ is not an edge of G. Therefore $\mathrm{Orth}(G)$ is a $(|G| - 2)$-partite graph.

It follows from the definition of $\mathrm{Orth}(G)$ and from the description of a normalized plane function given in the previous section that normalized plane functions correspond exactly to complete subgraphs, or cliques, of order $|G| - 2$ in $\mathrm{Orth}(G)$. Together with a zero row and the identity row, the orthomorphisms forming the vertices of a clique of order $|G| - 2$ furnish the rows of a normalized plane function.

In the case that $G = \mathbb{F}_q$, the finite field of order q, there is always at least one clique, namely the "trivial" or "linear" clique, whose vertices are the orthomorphisms $x \mapsto ax$, for each $a \in \mathbb{F}_q - \{0, 1\}$. The normalized plane functions corresponding to these linear cliques produce the Desarguesian planes of order q.

More generally, if $q = p^k$ where p is prime, and if $A : \mathbb{F}_q \to \mathbb{F}_q$ is an $\mathbb{F}_p$-linear map, then the map $x \mapsto Ax$ is an orthomorphism provided that both A and $A - I$ are non-singular. If the eigenvalues of A are all primitive roots of $\mathbb{F}_q$, then A^d is an orthomorphism for every $d \leq q - 2$. In this case, the maps $x \mapsto A^d x$, $1 \leq d \leq q - 2$, form a $(q - 2)$-clique in $\mathrm{Orth}(\mathbb{F}_q)$. The plane resulting from the corresponding normalized plane function is Desarguesian. Examples of other cliques in $\mathrm{Orth}(\mathbb{F}_q)$

can be found in Evans [7] or in Wan, Mullen and Shiue [24]. It is a long-standing conjecture that non-Desarguesian planes of prime order do not exist. A weaker long standing conjecture is that non-Desarguesian planes of prime order which admit translations do not exist. In this context the use of the term "translation" is distinct from its regular use in finite geometries. Let p be a point of a projective plane π and let l be a line through p. A (p, l)–*elation* of π is a collineation of π which fixes (as a set) every line through p and every point on l. If $l = l_\infty$, the elation induces a collineation of the corresponding affine plane which is called a *translation* of the affine plane. When we say that π admits a translation, we really mean that π admits a (p, l)–elation. This is consistent with the definition of translation given in subsection 2.2. The relation between the second conjecture and maximum cliques in $\mathrm{Orth}(\mathbb{F}_p)$ is given by a theorem by Evans and McFarland [8], which states that a non-Desarguesian plane of prime order, admitting translations, exists if and only if $\mathrm{Orth}(\mathbb{F}_p)$ contains more than one $(p-2)$-clique.

Much more on this relation, including proofs, can be found in Evans [7].

4. Computational results

The orthomorphism graphs $\mathrm{Orth}(\mathbb{F}_q)$, where $q \leq 16$ is a prime power, were constructed by computer, and the $(q-2)$-cliques in the graph were found. The results are summarized in Table 1. In this table, the column headed n shows the

q	n	e	core	max2	K_{q-2}'s
3	1	0	1	0	1
4	2	1	2	0	1
5	3	3	3	0	1
7	19	10	5	1	1
8	48	288	48	2	8
9	249	1248	249	4	21
11	3441	2016	141	3	1
13	79259	395242	271	5	1
16	15296512	2199658496	–	–	2439392

Table 1. Properties of the orthomorphism graphs $\mathrm{Orth}(\mathbb{F}_q)$.

number of vertices in $\mathrm{Orth}(\mathbb{F}_q)$ and the column headed e shows the number of edges. The column headed "core" shows the number of vertices in the $(q-3)$-core of $\mathrm{Orth}(\mathbb{F}_q)$, the $(q-3)$-core being the subgraph of minimum degree $q-3$ formed by repeatedly removing vertices of degree less than $q-3$ until none remain (of course, all $(q-2)$-cliques lie within the $(q-3)$-core). The column headed "max2" shows the number of vertices in a second-largest maximal complete subgraph, that is, a largest maximal complete subgraph with fewer than $q-2$ vertices. The final column shows the number of $(q-2)$-cliques in $\mathrm{Orth}(\mathbb{F}_q)$.

4.1. The graphs $\mathrm{Orth}(\mathbb{F}_p)$ for prime $p \leq 13$. For $q \leq 7$ the graph $\mathrm{Orth}(\mathbb{F}_q)$ has a very simple structure; in fact $\mathrm{Orth}(\mathbb{F}_q) = K_{q-2}$ for $q \leq 5$, and $\mathrm{Orth}(\mathbb{F}_7)$ consists of K_5 together with 14 isolated vertices. The graph $\mathrm{Orth}(\mathbb{F}_{11})$ has 2640 isolated vertices, and all other vertices have degree at most 8 except for six vertices of degree 162; these vertices correspond to the orthomorphisms $x \mapsto ax$ for $a \in$

$\{3, 4, 5, 7, 8, 9\}$. The graph Orth($\mathbb{F}_{13}$) is relatively more dense; it has only 260 isolated vertices, and 69639 of the 79259 vertices are in the 6-core. But the 7-core has only 973 vertices.

The graphs Orth($\mathbb{F}_p$) for p an odd prime appear to have the property that the second largest clique has $(p-5)/2$ vertices for $p \equiv 3 \pmod 4$ and $(p-3)/2$ vertices for $p \equiv 1 \pmod 4$, $p > 5$. Evans [6] constructed maximal cliques of these sizes in Orth($\mathbb{F}_p$).

4.2. **The graphs Orth($\mathbb{F}_q$) for $q = 8, 9$.** The graph Orth($\mathbb{F}_8$) is 12-regular. The normalized plane functions corresponding to the eight 6-cliques are isomorphic to each other under the isomorphisms described in section 2.2, each therefore giving rise to the Desarguesian plane.

The graph Orth($\mathbb{F}_9$) has minimum degree 6. It has 21 K_7's, falling into three orbits under the isomorphisms of subsection 2.2; these orbits correspond to the Desarguesian plane (3 K_7's), another plane and its dual plane (9 K_7's each). These three planes are all the three planes of order 9 that admit a translation. The last two non-Desarguesian planes are members of an infinite class of so-called Hall planes; see [12]. It is well known that there are exactly four projective planes of order 9, e.g., see [19]. The one that our method does not find is a member of an infinite class of so-called Hughes planes. Hughes planes are self-dual of order q^2 and their collineation groups have no subgroup isomorphic to the additive group of $GF(q^2)$ (follows from [12, Corollary 2, page 201] or from [3, page 247]. All planes of order 9 were discovered by Veblen and Wedderburn [23].

4.3. **The graphs Orth($\mathbb{F}_{16}$).** The graph Orth($\mathbb{F}_{16}$) has minimum degree 109; it has 112 vertices of degree 60160 but the next largest degree is 9984, and the average degree is only 143.8.

There are 2439392 K_{14}'s falling into 33 orbits under the isomorphisms of subsection 2.2. Unlike the case for $q < 16$, it happens here that $(q-2)$-cliques which are not isomorphic under the isomorphisms of section 2.2 sometimes give rise to isomorphic projective planes. In fact, exactly 15 planes appear, three being self-dual and the remainder forming six dual pairs. The planes that appear are all known. Table 2 lists each plane found, together with the number of K_{14}'s giving rise to it, and the number of the 33 orbits that these K_{14}'s make up. The first three planes

Plane	K_{14}'s	Orbits
PG(2,16)	336	1
SEMI2	554400	3
SEMI4	92400	3
HALL	22848	2
LMRH	81600	2
JOWK	81600	2
DSFP	380800	3
DEMP	228480	3
MATH	100800	1

TABLE 2. Planes arising from 14-cliques in Orth($\mathbb{F}_{16}$).

are self-dual — of the remaining 12 planes, only one is listed for each dual pair, the numbers for a plane and its dual being the same.

The names of the planes and their descriptions are taken from Royle [20]. The three self-dual planes are the Desarguesian plane PG(2,16) together with SEMI2 and SEMI4, the semifield planes with kernels $\mathbb{F}_2$ and $\mathbb{F}_4$. The other planes are HALL – the Hall plane, LMRH – the Lorimer-Rahilly plane, JOWK – the Johnson-Walker plane, DSFP – the derived semifield plane, DEMP – the Dempwolff plane, and MATH – the Mathon plane (together with their duals).

It might be noted that one of the planes produced is *not* a translation plane, namely MATH. Representative normalized plane functions are given for the three self-dual planes in Table 3 and for the six non-self-dual planes in Table 4. Since only the additive structure of $\mathbb{F}_{16}$ is involved, the field can be regarded as $\mathbb{F}_2^4$ under addition, and its elements thus correspond in a natural way to the numbers $0, \ldots, 15$. These numbers are written in hexadecimal in Tables 3 and 4.

PG(2,16)	SEMI2	SEMI4
0000000000000000	0000000000000000	0000000000000000
0123456789abcdef	0123456789abcdef	0123456789abcdef
02318ab9cefd4675	02318ab9cefd4675	02318ab9cefd4675
0312cfde47568b9a	0312cfde47568b9a	0312cfde47568b9a
048c62eabf37d951	04c8519dfb37ae62	049d51c8ea73bf26
05af278d369c14be	05eb14fa729c638d	05be14af63d872c9
06bde85371ca9f24	06f9db2435cae817	06acdb71248ef953
079ead34f86152cb	07da9e43bc6125f8	078f9e16ad2534bc
08c4b37fd5196ea2	084ce6a291d57f3b	08e6a24c7f91d53b
09e7f6185cb2a34d	096fa3c5187eb2d4	09c5e72bf63a18d4
0af539c61be428d7	0a7d6c1b5f28394e	0ad728f5b16c934e
0bd67ca1924fe538	0b5e297cd683f4a1	0bf46d9238c75ea1
0c48d1956a2eb7f3	0c84b73f6ae2d159	0c7bf38495e26a1d
0d6b94f2e3857a1c	0da7f258e3491cb6	0d58b6e31c49a7f2
0e795b2ca4d3f186	0eb53d86a41f972c	0e4a793d5b1f2c68
0f5a1e4b2d783c69	0f9678e12db45ac3	0f693c5ad2b4e187

TABLE 3. Normalized plane functions for some self-dual planes of order 16

4.4. **Computational method.** Programs were written in the C language and were run on 800MHz Pentium machines operating Red Hat Linux version 7.2, at the Department of Pure Mathematics in Cambridge.

All the data for $q \leq 11$ can be computed in less than a couple of seconds. For $q = 13$ the orthomorphisms were found in about three seconds but the construction and analysis of the graph $\mathrm{Orth}(\mathbb{F}_{13})$ took a further 25 minutes.

For $q = 16$, the list of 15296512 orthomorphisms was found in just under a day by sixty machines working in parallel. The analysis of the graph and the enumeration of the K_{14}'s, along with their orbits, was performed by thirteen machines acting in parallel over a period of about four days (these machines being the available ones with the required 380Mb of memory).

HALL	LMRH	JOWK
0000000000000000	0000000000000000	0000000000000000
0123456789abcdef	0123456789abcdef	0123456789abcdef
02318ab9cefd4675	02318ab9cefd4756	02318ab9dfec5764
0312cfde47568b9a	0312cfde47568ab9	0312cfde56479a8b
048c62eb5f3a79d1	048d2e5a916c3f7b	049d51c8ea73bf26
05af278cd691b43e	05ae6b3d18c7f294	05be14af63d872c9
06bde85291c73fa4	06bca4e35f91782d	06acdb71359fe842
079ead35186cf24b	079fe184d63ab5c2	078f9e16bc3425ad
08c4b37da51f9e62	08c637afe2b419d5	08c4e63ba25d19f7
09e7f61a2cb4538d	09e572c86b1fd43a	09e7a35c2bf6d418
0af539c46be2d817	0af7bd162c495e83	0af56c827db14e93
0bd67ca3e24915f8	0bd4f871a5e2936c	0bd629e5f41a837c
0c48d196fa25e7b3	0c4b19f573d826ae	0c59b7f3482ea6d1
0d6b94f1738e2a5c	0d685c92fa73eb41	0d7af294c1856b3e
0e795b2f34d8a1c6	0e7a934cbd2561f8	0e683d4a97c2f1b5
0f5a1e48bd736c29	0f59d62b348eac17	0f4b782d1e693c5a

DSFP	DEMP	MATH
0000000000000000	0000000000000000	0000000000000000
0123456789abcdef	0123456789abcdef	0123456789abcdef
02318ab9cefd4756	02318ab9cfde5764	02318ab9cefd6457
0312cfde47568ab9	0312cfde46759a8b	0312cfde4756a9b8
04c96e1ab53fd287	04e96bf3581ca2d7	049d51c8eb72fa63
05ea2b7d3c941f68	05ca2e94d1b76f38	05be14af62d9378c
06f8e4a37bc295d1	06d8e14a97c2f5b3	06acdb71349e8f25
07dba1c4f269583e	07fba42d1e69385c	078f9e16bd3542ca
084eb72fda156c93	087e36cba25d49f1	08e6b35da14f7c92
096df24853bea17c	095d73ac2bf6841e	09c5f63a28e4b17d
0a7f3d9614e82bc5	0a4fbc726d831e95	0ad739e45c812bf6
0b5c78f19d43e62a	0b6cf915e428d37a	0bf47c83d52ae619
0c87d9356f2abe14	0c975d38fa41eb26	0c7be2951f68d3a4
0da49c52e68173fb	0db4185f73ea26c9	0d58a7f296c31e4b
0eb6538ca1d7f942	0ea6d781359fbc42	0e4a682cf3b795d1
0f9516eb287c34ad	0f8592e6bc3471ad	0f692d4b7a1c583e

Table 4. Normalized plane functions for some non-self-dual planes

In order to find isomorphisms between the 33 orbits and to find isomorphisms between the planes produced by the above method and the known planes listed on [20], the excellent `nauty` program of Brendan McKay [15] was used, via the `dreadnaut` utility. This program allows the user to compute certain invariants of a graph which assist in establishing isomorphisms (or the absence of them) between graphs. Two invariants that are thought to work well with the graphs of projective planes, called `cellfano` and `cellfano2`, have been added to the library of invariants in version 2.0 of `nauty`; the second of these new invariants was used in the detection of isomorphisms between the planes in this study, and only about 4 minutes were needed on average to determine whether two planes were isomorphic (the time required being very much larger without the use of the invariant).

4.5. **Other abelian groups.** We have concentrated so far on the case when $G = \mathbb{F}_q$ but in fact it is only the additive group of the field that we have made use of, and we might just as well have used any abelian group for G. As mentioned in subsection 2.3, it is necessary for G to have trivial or non-cyclic Sylow 2-subgroup in order for it to have any orthomorphisms at all. Writing $\mathbb{Z}_n$ for the cyclic group of order n, the groups we have discussed are $\mathbb{Z}_p$ for p prime, together with $\mathbb{Z}_2^2$, $\mathbb{Z}_2^3$, $\mathbb{Z}_3^2$ and $\mathbb{Z}_2^4$, the additive groups of $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_9$ and $\mathbb{F}_{16}$. Of the remaining groups of order at most 16, $\mathbb{Z}_9$ has 225 orthomorphisms and $\mathbb{Z}_{15}$ has 2424195. $\mathbb{Z}_2 \times \mathbb{Z}_4$ has 48 orthomorphisms, and $\mathbb{Z}_2^2 \times \mathbb{Z}_3$ has 16512. These data confirm the results obtained by many authors and are surveyed in Chapter 6 of [7]. The following results are new: $\mathbb{Z}_2 \times \mathbb{Z}_8$ has 14735360 orthomorphisms, $\mathbb{Z}_2^2 \times \mathbb{Z}_4$ has 14886912 and $\mathbb{Z}_4^2$ has 14813184. The maximum size of a complete subgraph in the orthomorphism graph of $\mathbb{Z}_2 \times \mathbb{Z}_8$ is 3, and the graph contains 256000 K_3's. The corresponding data for $\mathbb{Z}_2^2 \times \mathbb{Z}_4$ and $\mathbb{Z}_4^2$ are 1062656 K_6's and 21504 K_6's. It would be interesting to know whether the orthomorphism graph of an abelian group of order n can ever contain an $(n-2)$-clique if the group is not a power of some prime order group.

5. Concluding remarks

As we stated in subsection 2.2 (1), all projective planes produced by our approach will admit a group of automorphisms formed by translations and isomorphic to G. Therefore, in order to find new projective planes, one may try to get rid of this property by changing p_2+l_2 in the definition of Γ_f to $g(p_2, l_2)$, where $g : G\times G \to G$ is an arbitrary function and G is an abelian group of order q. Given $f, g : G \times G \to G$, we define the bipartite graph $\Gamma_{f,g}$ in the following way. The vertex set of $\Gamma_{f,g}$ is $P \cup L$, $P = L = G \times G$ are color classes, and for $p = (p_1, p_2) \in P$, $l = [l_1, l_2] \in L$,

$$pl \in E(\Gamma_{f,g}) \text{ iff } g(p_2, l_2) = f(p_1, l_1)\,.$$

The following property on f, g makes $\Gamma_{f,g}$ q-regular: for given $p1, p2$ and $l1$, the equation $g(p2, l2) = f(p1, l1)$ has a unique solution for $l2$, and symmetrically, for given $l1, l2$ and $p1$, the equation $g(p2, l2) = f(p1, l1)$ has a unique solution for $p2$.

Let $A = A(f)$ and $B = B(g)$ be the matrices (tables) of the functions f and g, respectively, where rows correspond to points (or p's) and columns to lines (or l's). Proofs of the following observations are straightforward:

- $\Gamma_{f,g}$ is q-regular if every row and every column of B contains every entry of A (i.e., every element of the range of f) exactly once. In particular, if B is a Latin square, $\Gamma_{f,g}$ is q-regular.
- If $\Gamma_{f,g}$ is q-regular and A is a Latin square, then so is B.
- If B is a Latin square and no 2×2 submatrix of A is equal to a 2×2 submatrix of B, then $\Gamma_{f,g}$ is both q-regular and contains no 4-cycles.

These observations may provide a basis for a search of new projective planes without translations.

Acknowledgment. The authors are very thankful to Gary Ebert for helpful discussions on the subject of finite projective planes, to Gordon Royle for suggesting reference [19], to Rudi Mathon for suggesting references [5], [14], and to an anonymous referee who brought to our attention references [4] and [2].

References

[1] B. Bollobás, Extremal Graph Theory, Academic Press, London, 1978.
[2] R. Coulter, R.W. Matthews, Planar Functions and Planes of Lenz-Barlotti Class II, *Designs, Codes and Cryptography* **10** (1997), 167–184.
[3] P. Dembowski, Finite Geometries, Springer-Verlag, Berlin, 1968.
[4] P. Dembowski and T.G. Ostrom, Planes of Order n with Collineation Groups of Order n^2, *Math. Zeitschr.* **103** (1968), 239–258.
[5] M.J. de Resmini, On the Mathon plane, *J. Geometry* **60** (1997) 47–64.
[6] A.B. Evans, Maximal sets of mutually orthogonal Latin squares, II, *Europ. J. Combinatorics* **13** (1992), 345–350.
[7] Anthony B. Evans, Orthomorphism graphs of groups. *Lecture Notes in Mathematics* **1535**, Springer-Verlag, Berlin (1992), viii+114 pp.
[8] Anthony B. Evans and Robert L. McFarland, Planes of prime order with translations, in Proceedings of the Fifteenth Southeastern Conference on Combinatorics, Graph Theory and Computing, *Congr. Numer.* **44** (1984) 41–46.
[9] David Gluck, A Note on Permutation Polynomials and Finite Geometries, *Discrete Mathematics* **80** (1990), 97–100.
[10] Handbook on Incidence Geometry: buildings and foundations, Edited by F. Buekenhout, Elsevier, North-Holland, 1995.
[11] Yutaka Hiramine, A Conjecture on Affine Planes of Prime Order, *J. Comb. Theory*, Series A **52** (1989), 44–50.
[12] D.R. Hughes and F.C. Piper, Projective Planes, Springer-Verlag, New York, 1973.
[13] F. Lazebnik and A.J. Woldar, General Properties of Some Families of Graphs Defined by Systems of Equations, *J. Graph Theory* **38** 2001, 65–86.
[14] R. Mathon, On a new projective plane of order 16, Second International Conference in Deinze, 1992. Unpublished talk.
[15] B. McKay, The *nauty* page, `http://cs.anu.edu.au/people/bdm/nauty`
[16] L.J. Paige, Ph.D. Dissertation, University of Wisconsin, 1947.
[17] L.J. Paige, A note on finite abelian groups, *Bull. Amer. Math. Soc.* **53** (1947), 590–593.
[18] L. Rónyai and T. Szőnyi, Planar Functions Over Finite Fields, *Combinatorica* **9** (3) (1989), 315–320.
[19] T.G. Room and P.B. Kirkpatrick, Miniquaternion Geometry. Cambridge University Press, Cambridge, 1971.
[20] G. Royle, Projective Planes of Order 16, informal information web-page available at `http://www.cs.uwa.edu.au/~gordon/remote/planes16`.
[21] V.A. Ustimenko, personal communication, 1992.
[22] J.H. van Lint and R.M. Wilson, A course in combinatorics, Cambridge University Press, Cambridge (1992), xii+530 pp.
[23] O. Veblen and J.H.M. Wedderburn, Non-Desarguesian and non-Pascalian geometries, *Trans. Amer. Math. Soc.* **8** (1907), 379–388.
[24] Daqing Wan, Gary L. Mullen and Peter Jau-Shyong Shiue, The number of permutation polynomials of the form $f(x) + cx$ over a finite field, *Proc. Edinburgh Math. Soc.* (2) **38** (1995), 133–149.

Department of Mathematical Sciences, Ewing Building, University of Delaware, Newark, DE 19716, USA
E-mail address: `lazebnik@math.udel.edu`

Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, United Kingdom
E-mail address: `A.G.Thomason@dpmms.cam.ac.uk`