On projective planes of order less than 32

G. Eric Moorhouse

Abstract. By our count, 245 projective planes of order less than 32 are currently known. This list is dominated by the 193 known planes of order 25. Most of these are either translation planes or Hughes planes, or planes obtained from these by the well-known process of repeatedly dualizing and deriving. We describe two new planes obtainable by the quite different method of 'lifting quotients'.

2000 Mathematics Subject Classification: 51E15

1. Quick Survey

We assume the reader is familiar with the notion of a finite projective plane (which in this paper we call simply a *plane*) and related definitions; see e.g. [1, 5, 12] for the relevant background. The two biggest open problems in this research area are

(Q1) Must every plane have prime power order?

(Q2) Must every plane of prime order be Desarguesian?

To date, the best answer to (Q1) is given by the Bruck-Ryser Theorem [2], excluding as possible plane orders all values of $n \equiv 1, 2 \mod 4$ which are not expressible in the form $a^2 + b^2$ for two integers a, b; and the nonexistence of planes of order 10 [14]. The best progress towards (Q2) is the result that a transitive *affine* plane of prime order is Desarguesian; see [9, 11, 28].

In Table 1 we list the number of planes (or a lower bound indicating the number of known planes) of each order $n < 32$ for which at least one plane of order n is known. More complete information, including explicit line sets and generators of the full collineation groups, can be found at [24]. This list of known planes consists of

(i) All translation planes [16, 3, 5, 6] of order less than 32.

(ii) The ordinary Hughes planes of order 9 and 25, and the exceptional Hughes plane of order 25; see [15].

(iii) The Figueroa plane [7, 10] of order 27.

Table 1: Number of Planes of Order $n < 32$

n	no. of planes of order n up to isomorphism	no. of planes of order n up to iso./duality	Remarks
2	1	1	Desarguesian
3	1	1	Desarguesian
4	1	1	Desarguesian
5	1	1	Desarguesian
7	1	1	Desarguesian
8	1	1	Desarguesian
9	4	3	Lam, Kolesova, Thiel [13]
11	≥ 1	≥ 1	Desarguesian
13	≥ 1	≥ 1	Desarguesian
16	≥ 22	≥ 13	Royle [29]
17	≥ 1	≥ 1	Desarguesian
19	≥ 1	≥ 1	Desarguesian
23	≥ 1	≥ 1	Desarguesian
25	≥ 193	≥ 99	[3, 24]
27	≥ 13	≥ 8	[5, 24]
29	≥ 1	≥ 1	Desarguesian
31	≥ 1	≥ 1	Desarguesian

(iv) The Mathon plane of order 16.

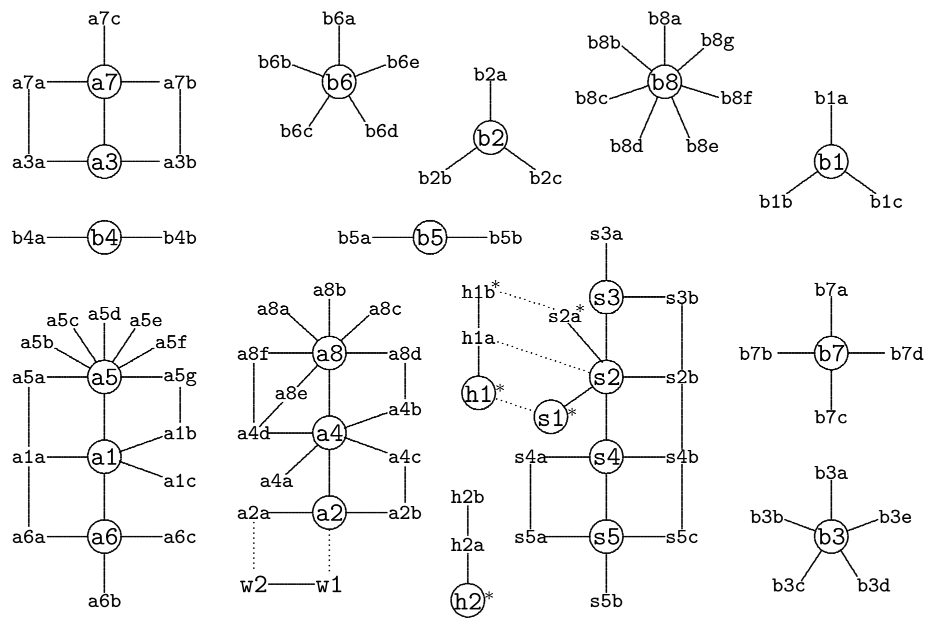
(v) All planes constructible from those of type (i), (ii) and (iv) by dualizing and/or deriving [12], perhaps repeatedly.

(vi) The Wyoming planes `w1` and `w2` of order 25 and their duals, described in Section 2.

The Mathon plane of order 16 (see [29]) was constructed by R. Mathon using net replacement. The Wyoming planes were constructed by the process of lifting quotients, described in Section 3. Our list is closed under the process described in (v); also under the process of lifting quotients by involutions. The known planes of order 25 predominate in Table 1, and we would not be surprised if many more planes of order 25 are yet to be found, possibly by net replacement. More interesting still, however, would be the discovery of any new planes of order 32, or a classification of the translation planes of order 32; but we expect such a list would be quite small.

Figure 1 lists the known planes of order 25 up to duality. The translation planes are indicated `a1`, ... , `a8`; `b1`, ... , `b8`; `s1`, ... , `s5` following the notation of [3]; here `s1` denotes the Desarguesian plane, and `a2` the Dickson nearfield plane. The ordinary and exceptional Hughes planes of order 25 are denoted `h1` and `h2` respectively. The five self-dual planes are indicated by asterisks. Solid edges indicate those pairs of planes in which one plane (or its dual) may be obtained from the other by derivation. Dotted edges indicate those pairs of planes in which one plane (or its dual) may be obtained from the other by the process of lifting quotients.

Figure 1: Known Planes of Order 25



We gratefully acknowledge discussions with W.M. Kantor regarding the structure of the planes `w1` and `w2`.

2. The Wyoming Planes

Here we define the Wyoming Planes `w1` and `w2` of order 25, of Lenz-Barlotti types II.1 and I.1 respectively. Explicit lists of point-line incidences for these planes appear at [24]. The following description, however, is obtained with the aid of `nauty` (for determination of the full automorphism group) and `GAP` (for identifying the structure of this group). Alternative descriptions may be possible by modifying the standard description of the Dickson nearfield plane, in hopes of generalizing this construction; but this we have not done.

The plane `w1` has full collineation group G of order 19200 given by

$$G = \langle g_1, g_2, \ldots, g_8 \rangle \cong (5^2 \times Q_8){:}SL_2(3){:}4 \; < GL_5(5)$$

where Q_8 is quaternion of order 8; here the generators are given by

$$g_1 = \begin{bmatrix} 1&0&0&1&0\\ &1&0&&\\ &0&1&&\\ &&&1&0\\ &&&0&1 \end{bmatrix}, \quad g_2 = \begin{bmatrix} 1&0&0&0&1\\ &1&0&&\\ &0&1&&\\ &&&1&0\\ &&&0&1 \end{bmatrix}, \quad g_3 = \begin{bmatrix} 1&0&0&0&0\\ &2&0&&\\ &0&3&&\\ &&&1&0\\ &&&0&1 \end{bmatrix}, \quad g_4 = \begin{bmatrix} 1&0&0&0&0\\ &0&1&&\\ &4&0&&\\ &&&1&0\\ &&&0&1 \end{bmatrix},$$

$$g_5 = \begin{bmatrix} 1&0&0&0&0\\ &2&0&&\\ &0&3&&\\ &&&2&0\\ &&&0&3 \end{bmatrix}, \quad g_6 = \begin{bmatrix} 1&0&0&0&0\\ &0&1&&\\ &4&0&&\\ &&&0&1\\ &&&4&0 \end{bmatrix}, g_7 = \begin{bmatrix} 1&0&0&0&0\\ &1&1&&\\ &2&3&&\\ &&&1&1\\ &&&2&3 \end{bmatrix}, \quad g_8 = \begin{bmatrix} 1&0&0&0&0\\ &1&0&&\\ &0&2&&\\ &&&1&0\\ &&&0&2 \end{bmatrix}.$$

The plane has five point orbits and five line orbits, and representatives $P_1, \ldots, P_5$; $L_1, \ldots, L_5$ may be chosen having stabilizers

$$G_{P_1} = G_{P_2} = G_{L_1} = G_{L_2} = G; \qquad G_{P_4} = G_{L_4} = \langle g_3, g_4, \ldots, g_8 \rangle,$$

$$G_{P_5} = \left\langle \begin{bmatrix} 1&0&0&0&0\\ &1&0&&\\ &0&2&&\\ &&&3&0\\ &&&0&4 \end{bmatrix}, \begin{bmatrix} 1&0&0&0&0\\ &0&1&&\\ &4&0&&\\ &&&0&2\\ &&&2&0 \end{bmatrix} \right\rangle, \quad G_{L_5} = \left\langle \begin{bmatrix} 1&0&0&0&0\\ &4&0&&\\ &0&4&&\\ &&&0&3\\ &&&3&0 \end{bmatrix}, \begin{bmatrix} 1&0&0&0&0\\ &2&0&&\\ &0&4&&\\ &&&1&0\\ &&&0&3 \end{bmatrix} \right\rangle,$$

$$G_{P_3} = \langle G_{L_5},\, g_1,\, g_2 \rangle, \quad G_{L_3} = \langle G_{P_5},\, g_1,\, g_2 \rangle.$$

The stabilizers have order $|G_{P_i}| = |G_{L_i}| =$ 19200, 19200, 800, 768, 32 for $i = 1, 2, \ldots, 5$. The corresponding point and line orbit sizes are 1, 1, 24, 25, 600. The structure of the plane `w1` is fully determined by specifying, for all $i, j \in \{1, 2, \ldots, 5\}$, the subset $A_{ij} \subseteq G$ such that $P_i^g \in L_j^h$ iff $gh^{-1} \in A_{ij}$. These subsets, and their corresponding sizes, are displayed in matrix form as

$$\begin{bmatrix} G & G & G & \varnothing & \varnothing \\ G & \varnothing & \varnothing & G & \varnothing \\ G & \varnothing & \varnothing & \varnothing & P_3 \\ \varnothing & G & \varnothing & P_4 & P_4 \\ \varnothing & \varnothing & L_3 & L_4 & P_5\{g_1, g_9\}L_5 \end{bmatrix}$$

and

$$\begin{bmatrix} 19200 & 19200 & 19200 & 0 & 0 \\ 19200 & 0 & 0 & 19200 & 0 \\ 19200 & 0 & 0 & 0 & 800 \\ 0 & 19200 & 0 & 768 & 768 \\ 0 & 0 & 800 & 768 & 768 \end{bmatrix}$$

respectively, where

$$g_9 = \begin{bmatrix} 1&0&0&4&4\\ &1&2&&\\ &2&1&&\\ &&&1&2\\ &&&2&1 \end{bmatrix}$$

and we abbreviate the stabilizers G_{P_i}, G_{L_i} by P_i, L_i respectively. The Sylow 5-subgroup $\langle g_1,\, g_2 \rangle$ consists of elations with common centre P_1 and axis L_1; thus the plane is (P_1, L_1)-transitive. The subgroup $Q_8 = \langle g_3,\, g_4\rangle$ consists of homologies with common centre P_2 and axis L_2.

The second Wyoming plane `w2` has full collineation group of order 3200 given by

$$G = \langle g_1, g_2, \dots, g_5\rangle \cong\ 4\times((5{:}4)\wr 2)\ < GL_4(5)$$

where

$$g_1 = \begin{bmatrix}1&0&1&0\\ &1&&\\ &&1&0\\ &&0&1\end{bmatrix},\quad g_2 = \begin{bmatrix}1&0&0&1\\ &1&&\\ &&1&0\\ &&0&1\end{bmatrix},\quad g_3 = \begin{bmatrix}1&0&0&0\\ &2&&\\ &&1&0\\ &&0&1\end{bmatrix},$$

$$g_4 = \begin{bmatrix}1&0&0&0\\ &1&&\\ &&2&0\\ &&0&1\end{bmatrix},\quad g_5 = \begin{bmatrix}1&0&0&0\\ &1&&\\ &&0&1\\ &&1&0\end{bmatrix},\quad g_6 = g_5g_4g_5 = \begin{bmatrix}1&0&0&0\\ &1&&\\ &&1&0\\ &&0&2\end{bmatrix}.$$

Representatives $P_1, \dots, P_7$ of the seven point orbits may be chosen having stabilizers

$$G_{P_1}=\langle g_1,\, g_2,\, g_3,\, g_4,\, g_6\rangle,\quad G_{P_2}=\langle g_1,\, g_2,\, g_3,\, g_4g_6,\, g_5g_4^2\rangle,$$

$$G_{P_3}=\langle g_1,\, g_2,\, g_5,\, g_3g_4,\, g_3g_6\rangle,\quad G_{P_4}=\langle g_1,\, g_2,\, g_3^2g_4g_6^3,\, g_5g_4^2\rangle,$$

$$G_{P_5}=\langle g_3,\, g_4,\, g_5\rangle,\quad G_{P_6}=\langle g_3g_6,\, g_4g_6^3\rangle,\quad G_{P_7}=\langle g_3^3g_4g_6,\, g_4^3g_5g_4\rangle$$

of order 1600, 800, 800, 200, 128, 16, 8; the corresponding point orbits have size 2, 4, 4, 16, 25, 200, 400. Representatives $L_1, \dots, L_7$ of the seven line orbits may be chosen having stabilizers

$$G_{L_1}=G,\quad G_{L_2}=\langle g_2,\, g_3,\, g_4,\, g_6\rangle,\quad G_{L_3}=\langle g_1^2g_2,\, g_3,\, g_5g_4^2,\, g_4g_6\rangle,$$

$$G_{L_4}=\langle g_2,\, g_3g_4g_1,\, g_3^2g_6\rangle,\quad G_{L_5}=\langle g_1^2g_2,\, g_4^3g_5g_4,\, g_3^3g_4g_6\rangle,$$

$$G_{L_6}=\langle g_5,\, g_3g_4,\, g_3g_6\rangle,\quad G_{L_7}=\langle g_5g_4^2,\, g_3^2g_4g_6^3\rangle$$

of order 3200, 320, 160, 80, 40, 32, 8; the corresponding line orbits have size 1, 10, 20, 40, 80, 100, 400. For all $i, j \in \{1, 2, \dots, 7\}$, the subset $A_{ij} \subseteq G$ satisfies $P_i^g \in L_j^h$ iff $gh^{-1} \in A_{ij}$. These subsets, and their corresponding sizes, are displayed in matrix form as

$$\begin{bmatrix}
G & P_1 & \varnothing & P_1 & \varnothing & \varnothing & \varnothing\\
G & \varnothing & P_2 & \varnothing & P_2 & \varnothing & \varnothing\\
G & \varnothing & \varnothing & \varnothing & \varnothing & P_3 & \varnothing\\
G & \varnothing & \varnothing & \varnothing & \varnothing & \varnothing & P_4\\
\varnothing & P_5L_2 & P_5L_3 & \varnothing & \varnothing & P_5 & P_5\\
\varnothing & L_2 & \varnothing & P_6g_3g_5g_1^4L_4 & P_6g_3L_4 & P_6g_1^2L_6 & P_6g_1^2g_2^2L_7\\
\varnothing & \varnothing & P_7g_5L_3 & P_7g_1^4L_4 & P_7\{e, g_4\}L_5 & P_7g_1^4g_2^2L_6 & P_7\{g_1^3, g_1g_2^4g_6\}L_7
\end{bmatrix}$$

and

$$\begin{bmatrix} 3200 & 1600 & 0 & 1600 & 0 & 0 & 0 \\ 3200 & 0 & 800 & 0 & 800 & 0 & 0 \\ 3200 & 0 & 0 & 0 & 0 & 800 & 0 \\ 3200 & 0 & 0 & 0 & 0 & 0 & 200 \\ 0 & 640 & 640 & 0 & 0 & 128 & 128 \\ 0 & 320 & 0 & 80 & 160 & 128 & 128 \\ 0 & 0 & 160 & 160 & 120 & 128 & 128 \end{bmatrix}$$

respectively, where e denotes the identity of G, and we abbreviate the stabilizers G_{P_i}, G_{L_i} by P_i, L_i respectively. The subgroup $Z(G) = \langle g_3 \rangle$ fixes a Baer subplane B. The Sylow 5-subgroup $\langle g_1, g_2 \rangle$ consists of elations of `w2` with common axis L_1 and whose centres are the six points of L_1 in B; thus `w2` is a semi-translation plane [4].

3. Method of 'Lifting Quotients'

The key notion in this method is topological: given a double cover $X \to Y$ of topological spaces, one asks for other spaces in place of X which may form double covers of Y. The appropriate tools for studying this question are found in any discussion of the cohomology of cell complexes; see e.g. [17]. Further details on this method are found in [21, 22, 23].

Let (Π, τ) be a pair consisting of a projective plane Π of order n, and a collineation $\tau \in \mathrm{Aut}(\Pi)$ of order two. From such a pair we construct an incidence structure $\Sigma = \Pi/\tau$ whose points (respectively, blocks) are given by the τ-orbits of length two on the points (resp., lines) of Π. We may safely disregard fixed points and lines of τ, because of the following.

Proposition 3.1. *The plane Π is uniquely reconstructible from the incidences between those of its points and lines not fixed by τ.*

Incidence in Σ is naturally induced by that in Π: a point $P = \{P_0, P_0^\tau\}$ lies on a block $L = \{L_0, L_0^\tau\}$ in Σ, iff P_0 lies in either L_0 or L_0^τ. Here P_0 and L_0 represent a point and line of Π, neither of which is fixed by τ. A *flag* in Σ is an incident point-block pair (P, L). A *digon* in Σ is a substructure $(\{P, Q\}, \{L, M\})$ in which P, Q are distinct points of Σ; and L, M are distinct blocks of Σ, both of which contain P and Q. We may distinguish three possibilities for the structure of Σ:

(i) n is even and τ is an elation of Π. In this case Σ has $\frac{1}{2}n^2$ points, $\frac{1}{2}n^2$ blocks, $\frac{1}{2}n^3$ flags and $\frac{1}{8}n^3(n-1)$ digons. We call Σ an *elation semibiplane.*

(ii) n is odd and τ is a homology of Π. In this case Σ has $\frac{1}{2}(n^2-1)$ points, $\frac{1}{2}(n^2-1)$ blocks, $\frac{1}{2}(n^2-1)(n-1)$ flags and $\frac{1}{8}n(n^2-1)(n-1)$ digons. We call Σ a *homology semibiplane.*

(iii) n is a perfect square and τ is a Baer involution of Π. In this case Σ has $\frac{1}{2}(n^2-\sqrt{n})$ points, $\frac{1}{2}(n^2-\sqrt{n})$ blocks, $\frac{1}{2}n(n^2-\sqrt{n})$ flags and $\frac{1}{8}n(n^2-\sqrt{n})(n-1)$ digons. We call Σ a *Baer semibiplane.*

Fortunately we are able to treat all three of these cases uniformly. It is a straightforward process to write down the most obvious properties such a quotient structure Σ must satisfy by virtue of Π being a projective plane with involutory collineation τ, and to adopt these as axioms for a *semibiplane;* see [30, 31, 32, 21, 22, 23].

Given another pair (Π', τ') consisting of a projective plane of order n with collineation of order two, we say the two pairs are *equivalent* if there is an isomorphism (i.e. collineation) $\theta\colon \Pi \to \Pi'$ such that $\theta \circ \tau = \tau' \circ \theta$. In this case it is clear that the quotient structures $\Sigma = \Pi/\tau$ and $\Sigma' = \Pi'/\tau'$ are isomorphic.

We may reverse the above quotient construction by asking: given Σ as above (obtained either from a known projective plane, or by some other construction known to satisfy the axioms for a semibiplane), we ask for all possible equivalence classes of pairs (Π, τ) such that $\Pi/\tau \cong \Sigma$. This lifting process may have no solution (if Σ was not constructed as the quotient of a known plane) or may have several inequivalent solutions. This suggests the following process for attempting to produce new planes from a known plane Π_0:

Algorithm LIFT-SEMIBIPLANE: Given a plane Π_0,

1. Compute $G = \mathrm{Aut}(\Pi_0)$ using `nauty`.
2. Using `GAP`, list representatives $\tau_1, \dots, \tau_k$ for the conjugacy classes of involutions in G.
3. For each $i = 1, 2, \dots, k$,
   - 3a. Produce the quotient structure $\Sigma_i = \Pi_0/\tau_i$.
   - 3b. Determine representatives (Π, τ) for all equivalence classes of pairs such that $\Pi/\tau \cong \Sigma_i$. In each case test Π to see if it is a previously known plane; if not, store it.

In order to accomplish Step 3b, we first construct from $\Sigma = \Sigma_i$ a cell complex $X = X_\Sigma$ of rank 2, all of whose 2-cells are squares, as follows. The vertices (0-cells) of X are the points and blocks of Σ. The edges (1-cells) of X are the flags of Σ. The faces (2-cells) of X are the digons of Σ. Incidence in X is naturally induced from that in Σ. Note that X is nothing more than the incidence graph of Σ, with the digons 'shaded in', i.e. the incidence graph of Σ is the 1-skeleton of X. For example if Σ is the quotient of a projective plane of order 4 by an elation, one checks [23] that X is the 2-skeleton of a tesseract (4-cube). Let $F = \{0, 1\}$, the field of order two, and let $C^i = C^i(X, F)$ be the F-space of all functions $\{i\text{-cells}\} \to F$ (i.e. the space of *i-cochains*). Let $\delta\colon C^i \to C^{i+1}$ be the usual coboundary operator.

Consider a possible 'lifting' of Σ to a plane Π, in which a typical point P and block L of Σ correspond to pairs of points $\{P_0, P_1\}$ and lines $\{L_0, L_1\}$ in Π. For every such flag (P, L) in Σ, we have either

(0) $P_0 \in L_0$ and $P_1 \in L_1$ in Π; or

(1) $P_0 \in L_1$ and $P_1 \in L_0$ in Π.

Define $\alpha \in C^1$ by $\alpha(P, L) = 0$ or 1 according as case (0) or (1) holds, and denote by Σ^α the resulting 'lifting' of Σ. The condition that Σ^α is a partial linear space, is that $\delta(\alpha) = \sigma$, where $\sigma \in C^2$ is defined by $\sigma(D) = 1$ for every face D of X. Accordingly, we say that $\alpha \in C^1$ is *admissible* if $\delta(\alpha) = \sigma$. Using Proposition 3.1, it is not hard to see that

Proposition 3.2. *'Liftings' from Σ to planes, correspond bijectively to admissible elements of C^1.*

Next observe that if $\alpha, \beta \in C^1$ are admissible, then $\delta(\alpha + \beta) = \sigma + \sigma = 0$. Thus

Proposition 3.3. *The set of admissible elements of C^1 is either empty, or a coset of $Z^1 = \ker \delta\big|_{C^1} : C^1 \to C^2$.*

If $\alpha \in C^1$ is admissible, then every element $\beta \in \alpha + B^1$ is admissible, where $B^1 = \delta C^0 \le C^1$; but for every such β, the lifting Σ^β differs from Σ^α only by certain interchanges (such as $P_0 \leftrightarrow P_1$ or $L_0 \leftrightarrow L_1$) of the names for points and lines. Thus

Proposition 3.4. *Let $\alpha, \beta \in C^1$ be admissible. If $\alpha \equiv \beta \mod B^1$, where $B^1 = \delta C^0 \le C^1$, then $\Sigma^\alpha \cong \Sigma^\beta$.*

We easily obtain

Proposition 3.5. *Given Σ, the equivalence classes of pairs (Π, τ) such that $\Pi/\tau \cong \Sigma$ are in bijective correspondence with the orbits of $Aut(\Sigma)$ on $\{\alpha \in C^1 : \alpha$ admissible$\}/B^1$.*

Note regarding this notation: In view of Proposition 3.3, $\{\alpha \in C^1 : \alpha$ admissible$\}/B^1$ is either empty, or a coset of $H^1 = Z^1/B^1$ in C^1/B^1. In the latter case, the set $\{\alpha \in C^1 : \alpha$ admissible$\}/B^1$ and the space H^1 have the same cardinality, and both are invariant under $\mathrm{Aut}(\Sigma)$; yet the action of $\mathrm{Aut}(\Sigma)$ on these two sets need not be permutation-equivalent.

Corollary 3.6. *If $H^1(X, F) = 0$ then there is at most one equivalence class of pairs (Π, τ) such that $\Pi/\tau \cong \Sigma$.*

The main result of [22] is that if Σ is a homology semibiplane obtained from a Desarguesian plane of odd prime order, then $H^1(X_\Sigma, F) = 0$, and so Σ lifts uniquely to the Desarguesian plane. It should be possible to generalize this result to include arbitrary semibiplanes obtained from Desarguesian planes.

We may now clarify Step 3b of Algorithm LIFT-SEMIBIPLANE given above:

3b.i Solve the linear system $\delta(\alpha) = \sigma$ for $\alpha \in C^1$. List distinct cosets $\alpha_1 + B^1, \ldots, \alpha_s + B^1$ of solutions.

3b.ii Enumerate orbits of $\mathrm{Aut}(\Sigma)$ on $\{\alpha_1+B^1, \ldots, \alpha_s+B^1\}$.

3b.iii For one representative α_i+B^1 of each such orbit, produce the lifted plane Σ^{α_i} and check (see Section 4) to see whether this plane is known.

Step 3b.i requires solving a linear system of $O(n^4)$ linear equations in $O(n^3)$ unknowns, using Gaussian elimination since the system is not at all sparse. Using bitwise operations in C or C++ in order to economize on computer memory, we found this step to be quite feasible for all values of n we have considered. Step 3b.ii is also quite manageable since $\dim H^1(X,F) \le 4$ in every case considered, and so the admissible 1-cochains lie in at most 2^4 cosets of B^1.

Some instances of pairs of planes in which one plane is obtainable by lifting a quotient of the other, are as follows:

(i) For any odd prime power q, the Desarguesian and ordinary Hughes planes of order q^2.

(ii) The Johnson-Walker and Lorimer-Rahilly planes of order 16.

(iii) The Lorimer-Rahilly and derived semifield planes of order 16.

(iv) The two semifield planes of order 16 (having kernels of order 2 and 4).

(v) The Mathon plane of order 16 and its dual.

(vi) The five pairs of planes of order 25 indicated by the dotted edges in Figure 1.

The Wyoming planes represent the first true success of this method of constructing new planes, simply because the other planes listed in (i)–(vi) above were previously constructed by other means.

It is natural to ask for semibiplanes constructed by means other than as quotients of known planes, in the hopes that these may be lifted to give new planes. Many such constructions of semibiplanes are found in the literature, but none (except for those obtained as quotients of known planes) has been found to be liftable to planes. The advantage of starting with known planes and forming quotients, is that this yields such an abundant and ready supply of semibiplanes, with correspondingly higher odds of success.

One may also try to replace the collineation τ of order two by a larger collineation group $G \le \mathrm{Aut}(\Pi)$, hoping to find liftings of Π/G to planes other than the original Π. Unfortunately in the case $|G| > 2$, no efficient algorithm for determining such liftings is known, in contrast with the situation for $|G| = 2$ where the problem reduces to linear algebra.

After implementing Algorithm LIFT-SEMIBIPLANE for all known planes of order less than 32, we implemented a very similar Algorithm LIFT-QUOTIENT for the smallest known generalized n-gons for $n{=}4,6,8$. Here we construct the quotient of a generalized polygon by any collineation of order two, and look for alternative liftings of these quotient structures, thereby conceivably producing new generalized polygons [26]. Unfortunately no new generalized polygons were found, after applying the approach to the 32 smallest generalized quadrangles

(18 up to isomorphism/duality), the 9 smallest generalized hexagons (5 up to isomorphism/duality) and the 2 smallest generalized octagons (1 up to isomorphism/duality). However, it is worth noting that for the generalized quadrangle [27] with parameters $(s,t)=(3,5)$, the quotient structure Σ for an appropriate choice of involutory collineation has $\dim H^1(X_\Sigma, F)=1$. In this case however, the group $\mathrm{Aut}(\Sigma)$ has only one orbit on $\{$admissible 1-cochains$\}/B^1$ so there is only one equivalence class of pairs (Q,τ) consisting of a generalized quadrangle Q and involutory collineation τ such that $Q/\tau\cong\Sigma$. This is not too surprising since the generalized quadrangle with parameters $(s,t)=(3,5)$ is known to be unique up to isomorphism.

4. Isomorphism Testing

The unrivaled tool for computing automorphism groups of graphs and designs, and for testing for isomorphisms between such objects, is B. McKay's software package `nauty` [18, 19]. Given a graph Γ, `nauty` will determine the automorphism group of Γ, and provide a 'canonical' representative of the isomorphism class of Γ. (Thus $\Gamma\cong\Gamma'$ iff the graphs Γ and Γ' have the same canonical representative. This canonical representative is rather subtle to define and may depend somewhat on the choice of computer hardware used in computation.) This can be applied to the bipartite *incidence graph* A_Π of a projective plane Π of order n. If $\mathfrak{P}$ and $\mathfrak{L}$ are the point and line sets of Π, then the graph A_Π has $2(n^2+n+1)$ vertices given by the set $\mathfrak{P}\cup\mathfrak{L}$, and edges corresponding to incident point-line pairs. Note that $\mathrm{Aut}(A_\Pi)$ is isomorphic to the group consisting of all *collineations* and *correlations* of Π, which we denote here by $\mathrm{AUT}(\Pi)$. If desired, we may ask `nauty` to preserve the two parts of the vertex partition, thereby obtaining just the collineation group of Π, which we denote by $\mathrm{Aut}(\Pi)$; thus $[\mathrm{AUT}(\Pi):\mathrm{Aut}(\Pi)]\le 2$.

For reasons that will soon appear, we consider also the *non*-incidence graph Γ_Π, having $2(n^2+n+1)$ vertices given by $\mathfrak{P}\cup\mathfrak{L}$, and edges corresponding to the *non*-incident point-line pairs of Π. This graph is regular of degree n^2, which greatly exceeds the degree $n+1$ of A_Π, and so it would seem to be less desirable for computational purposes.

Projective planes are time-consuming cases for `nauty`. Using a typical desktop personal computer, I found that `nauty` was able to compute $\mathrm{Aut}(A_\Pi)$ for planes of order 16 in a matter of minutes (using Gordon Royle's invariant `cellfano2`, an option in the `nauty` package); planes of order 25 or 27 required hours or days; and planes of order 32 were infeasible. To overcome this computational hurdle, I use the following device which I refer to as 'Conway Doubling', after an idea of J.H. Conway; see [20].

As before, $\Pi=(\mathfrak{P},\mathfrak{L})$ denotes a projective plane of order n. We proceed to define a graph Δ_Π with $4(n^2+n+1)$ vertices (*roughly* a double cover of the *non*-incidence graph Γ_Π) as follows. Let $F=\{0,1\}$ be the field of order two. Vertices of Δ_Π are of the form (P,i) or (L,j) where $P\in\mathfrak{P}$, $L\in\mathfrak{L}$, and $i,j\in F$. To define adjacency in Δ_Π, first index the points on each line using labels $0, 1, 2, \dots, n$ via a fixed (but arbitrary) ordering. Similarly, index the lines through each point using labels $0, 1, 2, \dots, n$. For each *non*-incident point-line pair (P, L) in Π, the incidences between points of L and lines through P naturally yield a permutation $\sigma_{P,L} \in Sym\{0, 1, 2, \dots, n\}$. There are two types of edges in Δ_Π:

(I) $(P, i) \sim (L, j)$ iff $P \notin L$ and $\mathrm{sgn}(\sigma_{P,L}) = (-1)^{i+j}$;

(II) $(P, 0) \sim (P, 1)$, $\quad (L, 0) \sim (L, 1)$.

Type I edges form a double cover of Γ_Π. Type II edges ensure that Δ_Π is connected. Using `nauty`, we compute the group G consisting of all automorphisms of Δ_Π preserving the vertex partition $\{\mathfrak{P} \times F, \mathfrak{L} \times F\}$; also the group G_0 of all automorphisms of Δ_Π preserving both $\mathfrak{P} \times F$ and $\mathfrak{L} \times F$. Let $Z \leq \mathrm{Aut}(\Delta_\Pi)$ be the subgroup of order two generated by

$$(P, 0) \leftrightarrow (P, 1), \quad (L, 0) \leftrightarrow (L, 1).$$

Clearly we have $Z \leq G_0 \leq G \leq \mathrm{Aut}(\Delta_\Pi)$ and $Z \leq Z(\mathrm{Aut}(\Delta_\Pi))$. It is not hard to see that $\mathrm{AUT}(\Pi) \cong G/Z$ and $\mathrm{Aut}(\Pi) \cong G_0/Z$. Moreover, two planes Π, Π' of order n are isomorphic, if and only if the graphs Δ_Π (with distinguished vertex subset $\mathfrak{P} \times F$) and $\Delta_{\Pi'}$ (with distinguished vertex subset $\mathfrak{P}' \times F$, where $\mathfrak{P}'$ is the point set of Π') yield the same canonical representative as computed using `nauty`. Although the graph Δ_Π is somewhat larger than A_Π or Γ_Π , experience shows that the determination of $\mathrm{Aut}(\Pi)$ is *much* faster by this method.

We note that without the type II edges, Δ_Π could be disconnected, in fact a disjoint union of two copies of Γ_Π, with rather large automorphism group $\mathrm{Aut}(\Pi) \wr 2$. In particular, this happens [20] whenever Π is a Desarguesian plane of even order.

Our program for generating planes of small order using the known constructions, typically produced each plane many times. Using `nauty` we were able to store just one canonical representative of each isomorphism class. Evidence that the planes in the resulting list are nonisomorphic, is provided by `nauty` itself. However, an independent certificate of non-isomorphism is desirable so that one need not rely on the correctness of the `nauty` code. For this purpose we have listed fingerprints [25] of all planes in our list. The *fingerprint* of a finite projective plane is an isomorphism invariant, consisting of the multiset of absolute values of the entries of AA^T, where A is the $(n^2{+}n{+}1) \times (n^2{+}n{+}1)$ matrix with (P, L)-entry equal to $\mathrm{sgn}(\sigma_{P,L})$; see [20]. Computing the fingerprint of a plane Π typically requires more execution time than using nauty to compute the canonical representative of A_Π or of Δ_Π; however, once nauty has determined $\mathrm{Aut}(\Pi)$ as outlined above, this information greatly facilitates the computation of the fingerprint of Π. Even here we have not required the assumption that `nauty` is correct, since we verify directly that the generators for $\mathrm{Aut}(\Pi)$ supplied by `nauty` are indeed automorphisms of Π, and we do not need to know that they generate the full automorphism group of Π in order to quickly compute the fingerprint of Π.

References

[1] A. Beutelspacher, 'Projective planes', pp.107–136 in *Handbook of Incidence Geometry,* ed. F. Buekenhout, North-Holland, 1995.

[2] R.H. Bruck and H.J. Ryser, 'The nonexistence of certain finite projective planes', *Canad. J. Math.* **1** (1949), 88–93.

[3] T. Czerwinski and D. Oakden, 'The translation planes of order twenty-five', *J. Combin. Theory Ser. A* **59** (1992), 193–217.

[4] P. Dembowski, *Finite Geometries,* Springer-Verlag, Berlin, 1968.

[5] U. Dempwolff, 'Translation planes of order 27', *Des. Codes and Crypt.* **27** (1994), 105–121.

[6] U. Dempwolff and R. Reifart, 'The classification of translation planes of order 16, I', *Geom. Ded.* **15** no.2 (1983), 137–153.

[7] R. Figueroa, 'A family of not (V, ℓ)-transitive projective planes of order q^3, $q \not\equiv 1$ mod 3, and $q > 2$', *Math. Z.* **181** (1982) no.4, 471–479.

[8] The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.3; 2002. (http://www.gap-system.org/)

[9] D. Gluck, 'A note on permutation polynomials and finite geometries', *Discrete Math.* **80** (1990) no.1, 97–100.

[10] C. Hering and H.-J. Schaeffer, 'On the new projective planes of R. Figueroa', *Combinatorial Theory (Schloss Rauischholzhausen, 1982),* pp.187–190, *Lecture Notes in Math. 969,* Springer-Verlag, Berlin, 1982.

[11] Y. Hiramine, 'A conjecture on affine planes of prime order', *J. Combin. Theory Ser. A* **52** (1989) no.1, 44–50.

[12] D.R. Hughes and F.C. Piper, *Projective Planes,* Springer-Verlag, New York, 1973.

[13] C.W.H. Lam, G. Kolesova and L. Thiel, 'A computer search for finite projective planes of order 9', *Discrete Math.* **92** (1991) no.1–3, 187–195.

[14] C.W.H. Lam, L.H. Thiel and S. Swiercz, 'The nonexistence of finite projective planes of order 10', *Canad. J. Math.* **41** (1989) no.6, 1117–1123.

[15] H. Lüneburg, 'Characterizations of the generalized Hughes planes', *Canad. J. Math.* **28** (1976), 376–402.

[16] H. Lüneburg, *Translation Planes,* Springer-Verlag, Berlin, 1980.

[17] W.S. Massey, *A Basic Course in Algebraic Topology,* Springer-Verlag, New York, 1991.

[18] B.D. McKay, Practical Graph Isomorphism, *Congressus Numerantium* **30** (1981), 45–87. Available at http://cs.anu.edu.au/~bdm/nauty/PGI/

[19] B.D. McKay, `nauty` software. http://cs.anu.edu.au/~bdm/nauty/

[20] G.E. Moorhouse, 'Two-graphs and skew two-graphs in finite geometries', *Linear Algebra and its Applications* **226–228** (1995), 529–551.

[21] G.E. Moorhouse, 'Reconstructing projective planes from semibiplanes', in *Coding Theory and Design Theory, Part II: Design Theory,* ed. D. Ray-Chaudhuri, Springer-Verlag, 1990, pp.280–285.

[22] G.E. Moorhouse, 'On the construction of finite projective planes from homology semibiplanes', *Europ. J. Combinatorics* **11** (1990), 589–600.

[23] G.E. Moorhouse, 'Planes, semibiplanes and related complexes', preprint. http://math.uwyo.edu/~moorhous/pub/planes.pdf

[24] G.E. Moorhouse, 'Projective planes of small order'. http://math.uwyo.edu/~moorhous/pub/planes/

[25] G.E. Moorhouse, 'Fingerprints of projective planes of order 25'. http://math.uwyo.edu/~moorhous/pub/planes25/fing25.html

[26] G.E. Moorhouse, 'Generalised polygons of small order'. http://math.uwyo.edu/~moorhous/pub/genpoly/

[27] S.E. Payne, 'The generalized quadrangle with $(s,t) = (3,5)$, *Congressus Numerantium* **77** (1990), 5–29.

[28] L. Rónyai and T. Szőnyi, 'Planar functions over finite fields', *Combinatorica* **9** (1989) no.3, 315–320.

[29] G. Royle, 'Projective planes of order 16'. http://www.csse.uwa.edu.au/~gordon/remote/planes16/

[30] P. Wild, 'Generalized Hussain graphs and semibiplanes with $k \leq 6$', *Ars Combin.* **14** (1982), 147–167.

[31] P. Wild, 'Incidence graphs and subdesigns of semisymmetric designs', *Discrete Math.* **44** (1983), 201–216.

[32] P. Wild, 'Divisible semibiplanes and conics of Desarguesian biaffine planes', *Simon Stevin* **58** no.1–2 (1984), 153–166.

G. Eric Moorhouse, Department of Mathematics, 1000 E. University Ave., Dept. 3036, University of Wyoming, Laramie, WY 82071, U.S.A.

Email: moorhous@uwyo.edu