Projective Geometry and Related Matrices

by

Michelle Davidson

A Thesis submitted to
the Faculty of Graduate Studies
In Partial Fulfillment of the Requirements for the Degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics
University of Manitoba
Winnipeg, Manitoba

0-494-08777-3

Your file Votre référence
ISBN:
Our file Notre référence
ISBN:

THE UNIVERSITY OF MANITOBA

FACULTY OF GRADUATE STUDIES

*****

COPYRIGHT PERMISSION PAGE

Projective Geometry and Related Matrices

BY

Michelle Davidson

A Thesis/Practicum submitted to the Faculty of Graduate Studies of The University of Manitoba in partial fulfillment of the requirements of the degree

of

DOCTOR OF PHILOSOPHY

Contents

Abstract

In 1953, Paige and Wexler introduced a form of the incidence matrix of a finite projective plane organized about a point line incident pair. We introduce generalised permutation Hadamard matrices, which are related to this form. We give another form of the incidence matrix, organized about a point line non-incident pair. We introduce generalised permutation weighing matrices, which are related to this new form. We draw a connection between these two forms, which extends to a connection between the existence of a finite projective plane of Lenz-Barlotti class II.2 and a $GH(n, G)$ whose core is group developed. In the case where a finite projective plane has a Baer subplane, we also present a third form of the incidence matrix. We give a non-existence result for a particular class of generalised Hadamard matrices over a cyclic group.

Using a known construction for orthogonal matrices, we obtain a set of MOLS. Constructions of sets of MOLS of these sizes are known; however this construction gives Latin squares whose rows are all shifts of the first row. Adapting a technique of Hughes, we use collineations of projective planes to construct a Hadamard matrix of order $\frac{q^2-1}{2}$ for certain prime powers q.

We introduce skew arcs, which are sets of points in a projective space, related to parity check matrices of linear error correcting codes. We give some constructions of skew arcs and take an in-depth look at Wagner's [23,14,5] code.

Chapter 1

Background

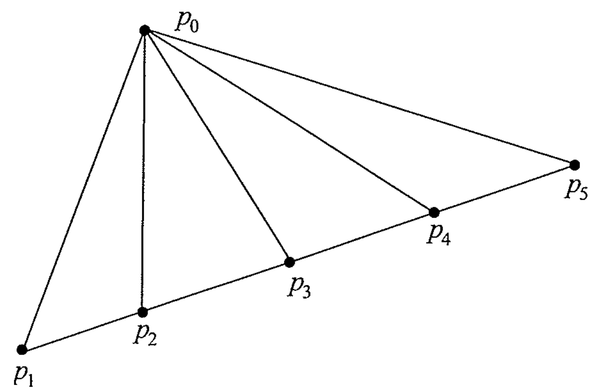
In projective geometry, there are two types of questions asked. One is about configurations, the other is about existence. We touch upon both of these questions, giving some theorems about the existence of projective planes with certain types of automorphism groups, and give a characterization of a particular configuration in projective spaces related to codes.

1.1 Designs

An *incidence structure* is a triple $\mathbf{D} = \{\mathcal{V}, \mathcal{B}, \mathbf{I}\}$ where $\mathcal{V}$ and $\mathcal{B}$ are disjoint sets and $\mathbf{I}$ is a binary relation, called *incidence*, between $\mathcal{V}$ and $\mathcal{B}$, i.e. $\mathbf{I} \subseteq \mathcal{V} \times \mathcal{B}$. If $(p, \ell) \in \mathbf{I}$, we say p is *incident* with ℓ, or that ℓ is *incident* with p. The elements of $\mathcal{V}$ are called *points*, those of $\mathcal{B}$ are called *blocks* or *lines*, those of $\mathbf{I}$ are called *flags*. We will at times refer to an incidence structure as a *design*.

Example 1. A *near pencil* on n points is an incidence structure which has one line

Figure 1.1:



ℓ incident with $n-1$ points and $n-1$ lines, each incident with the point not on ℓ and a distinct point on ℓ.

The following is a near pencil on 6 points:

$$\mathcal{V} = \{p_0, p_1, p_2, p_3, p_4, p_5\}$$

$$\mathcal{B} = \{b_0, b_1, b_2, b_3, b_4, b_5\}$$

$$\mathbf{I} = \{(p_i, b_0) | i \in \{1,2,3,4,5\}\} \cup \{(p_0, b_i) | i \in \{1,2,3,4,5\}\}$$
$$\cup \{(p_i, b_i) | i \in \{1,2,3,4,5\}\}$$

We often represent an incidence structure with a diagram in which lines are represented by curves, and points as distinguished intersections of curves. The above near pencil on 6 points is shown in Figure 1.1.

If $(p, \ell) \in \mathbf{I}$, the notation $p\mathbf{I}\ell$ is commonly used. We also say ℓ *passes through* p, or p *is on* ℓ. If $(p, \ell) \notin \mathbf{I}$ then the pair (p, ℓ) is referred to as an *antiflag*. If $p\mathbf{I}\ell_1$ and $p\mathbf{I}\ell_2$ then the lines ℓ_1 and ℓ_2 *meet* or *coincide* at the point p. If $p_1\mathbf{I}\ell$ and $p_2\mathbf{I}\ell$ then the points p_1 and p_2 *meet* on the line ℓ. If $p\mathbf{I}\ell_i$ for $i = 1, 2, \ldots n$ then the ℓ_i's are *concurrent* or *copointal* at p. Lines that are concurrent at a point are said to *intersect*. If $p_i\mathbf{I}\ell$ for $i = 1, 2, \ldots n$ then the p_i's are *collinear* on ℓ.

We can associate with each element b of $\mathcal{B}$ the set of points that are incident with it. Thus, the elements of $\mathcal{B}$ are treated as subsets of $\mathcal{V}$, and $\mathbf{I}$ will be given by inclusion. Hence we can also write $\mathbf{D} = \{\mathcal{V}, \mathcal{B}\}$ where $\mathcal{B} \subseteq \mathcal{P}(\mathcal{V})$.

Example 2. Thus the design given in Example 1 can be expressed as follows:

$\mathcal{V} = \{p_0, p_1, p_2, p_3, p_4, p_5\}$ as before, and now the 6 lines of $\mathcal{B}$ are given by $\{p_0, p_1\}$, $\{p_0, p_2\}$, $\{p_0, p_3\}$, $\{p_0, p_4\}$, $\{p_0, p_5\}$, $\{p_1, p_2, p_3, p_4, p_5\}$.

Example 3. A *balanced incomplete block design* (BIBD) with parameters (v, b, r, k, λ) is a design with v points and b blocks each of which contain k points, such that every point is in exactly r blocks and every pair of points is together in λ blocks. Since $b = \frac{vr}{k}$ and $r = \frac{\lambda(v-1)}{k-1}$, we can refer to a *BIBD* with parameters (v, b, r, k, λ) as (v, k, λ)-BIBD's. In the case that a *BIBD* has parameters $v = b$, (and hence $k = r$), it is a *symmetric BIBD*. The following is a symmetric BIBD.

The following are the blocks of a BIBD$(11, 5, 2)$: $\{p_1, p_2, p_3, p_4, p_8\}$ $\{p_1, p_2, p_5, p_6, p_7\}$ $\{p_1, p_3, p_6, p_9, p_{10}\}$ $\{p_1, p_4, p_7, p_9, p_{11}\}$ $\{p_1, p_5, p_8, p_{10}, p_{11}\}$

$\{p_2, p_3, p_5, p_9, p_{11}\}$ $\{p_2, p_4, p_6, p_{10}, p_{11}\}$ $\{p_2, p_7, p_8, p_9, p_{10}\}$ $\{p_3, p_4, p_5, p_7, p_{10}\}$ $\{p_3, p_6, p_7, p_8, p_{11}\}$ $\{p_4, p_5, p_6, p_8, p_9\}$.

Example 4. A *parallel class* or *resolution* class in a design (or incidence structure) is a set of blocks that partition the point set. Lines are considered *parallel* if they belong to the same parallel class. A *resolvable* BIBD is a (v, k, λ)-BIBD whose blocks can be partitioned into parallel classes. The following are the blocks of a resolvable (15,3,1) design, arranged into parallel classes. Blocks are the horizontal triples, and the parallel classes are the seven columns of blocks.

A, B, C	A, H, I	A, J, K	A, D, E	A, F, G	A, L, M	A, N, O
D, J, N	B, E, G	B, M, O	B, L, N	B, H, J	B, I, K	B, D, F
E, H, M	C, M, N	C, E, F	C, I, J	C, L, O	C, D, G	C, H, K
F, I, O	D, K, O	D, H, L	F, K, M	D, I, M	E, J, O	E, I, L
G, K, L	F, J, L	G, I, N	G, H, O	E, K, N	F, H, N	G, J, M

Although parallel lines do not meet, in the case of designs, not all lines that do not meet are parallel. From the above example, lines A, B, C and D, K, O are disjoint but not parallel.

We call a point *isolated* if it is on 0 or 1 lines; similarly a line is *isolated* if contains 0 or 1 points. A point *full* if it is on all the lines, and a line is *full* if it contains all the points. Generally, to avoid certain degenerate cases, we assume a design contains no isolated points or lines, no full points or lines, and no repeated lines. A design is *finite* if $\mathcal{V}$ is a finite set (and hence $\mathcal{B}$ and $\mathbf{I}$ are as well). In this case we write $|\mathcal{V}| = v$ and $|\mathcal{B}| = b$.

Definition 1. With every finite design $\mathbf{D}$, we associate a $v \times b$ matrix of 0's and 1's, called its *incidence matrix* A, as follows. Enumerate the sets $\mathcal{V} = \{p_1, p_2, \cdots, p_v\}$ (or, in some cases $\{p_0, p_1, \cdots, p_{v-1}\}$) and $\mathcal{B} = \{\ell_1, \ell_2, \cdots, \ell_b\}$ (or $\{\ell_0, \ell_1, \cdots, \ell_{b-1}\}$). A is defined as $A = [a_{ij}]$ where a_{ij} is 1 if p_i (resp. p_{i-1}) is on ℓ_j (resp. ℓ_{j-1}) and 0 otherwise.

Example 5. The incidence matrix for the near pencil given in Example 1 is:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

For more on designs see [60].

1.2 Projective geometries

1.2.1 Definitions of spaces

There are various definitions of projective space. We shall use the definition in [12], which is equivalent to that in [75]. A similar one is given in [19], except that an extra condition ensures a space of finite dimension. Alternate developments may be found in [10], [27].

Definition 2. A *projective space* is a design that satisfies the following axioms:

P1: For any two distinct points p and q there is exactly one line that is incident with p and with q. This line as is referred to as pq.

P2: Let a, b, c, and d be four distinct points such that the line ab intersects the line cd. Then the line ac intersects the line bd.

P3: Any line is incident with at least three points.

P4: There are at least two lines.

Example 6. The following $(15, 3, 1) - BIBD$ is an example of a projective space (see Example 7). Let the point set be

$\{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \mathfrak{e}, \mathfrak{f}, \mathfrak{g}, \mathfrak{h}, \mathfrak{i}, \mathfrak{j}, \mathfrak{k}, \mathfrak{l}, \mathfrak{m}, \mathfrak{n}, \mathfrak{o}\}$.

The line set is $\{\{\mathfrak{a}, \mathfrak{b}, \mathfrak{e}\}$, $\{\mathfrak{a}, \mathfrak{c}, \mathfrak{f}\}$, $\{\mathfrak{a}, \mathfrak{d}, \mathfrak{g}\}$, $\{\mathfrak{a}, \mathfrak{h}, \mathfrak{k}\}$, $\{\mathfrak{a}, \mathfrak{i}, \mathfrak{l}\}$, $\{\mathfrak{a}, \mathfrak{j}, \mathfrak{m}\}$, $\{\mathfrak{a}, \mathfrak{n}, \mathfrak{o}\}$, $\{\mathfrak{b}, \mathfrak{c}, \mathfrak{h}\}$, $\{\mathfrak{b}, \mathfrak{d}, \mathfrak{i}\}$, $\{\mathfrak{b}, \mathfrak{f}, \mathfrak{k}\}$, $\{\mathfrak{b}, \mathfrak{g}, \mathfrak{l}\}$, $\{\mathfrak{b}, \mathfrak{j}, \mathfrak{n}\}$, $\{\mathfrak{b}, \mathfrak{m}, \mathfrak{o}\}$, $\{\mathfrak{c}, \mathfrak{d}, \mathfrak{j}\}$, $\{\mathfrak{c}, \mathfrak{e}, \mathfrak{k}\}$, $\{\mathfrak{c}, \mathfrak{g}, \mathfrak{m}\}$, $\{\mathfrak{c}, \mathfrak{i}, \mathfrak{n}\}$, $\{\mathfrak{c}, \mathfrak{l}, \mathfrak{o}\}$, $\{\mathfrak{d}, \mathfrak{e}, \mathfrak{l}\}$, $\{\mathfrak{d}, \mathfrak{f}, \mathfrak{m}\}$, $\{\mathfrak{d}, \mathfrak{h}, \mathfrak{n}\}$, $\{\mathfrak{d}, \mathfrak{k}, \mathfrak{o}\}$, $\{\mathfrak{e}, \mathfrak{j}, \mathfrak{o}\}$, $\{\mathfrak{e}, \mathfrak{m}, \mathfrak{n}\}$, $\{\mathfrak{e}, \mathfrak{g}, \mathfrak{i}\}$, $\{\mathfrak{e}, \mathfrak{f}, \mathfrak{h}\}$, $\{\mathfrak{f}, \mathfrak{g}, \mathfrak{j}\}$, $\{\mathfrak{f}, \mathfrak{i}, \mathfrak{o}\}$, $\{\mathfrak{f}, \mathfrak{l}, \mathfrak{n}\}$, $\{\mathfrak{g}, \mathfrak{h}, \mathfrak{o}\}$, $\{\mathfrak{g}, \mathfrak{k}, \mathfrak{n}\}$, $\{\mathfrak{h}, \mathfrak{i}, \mathfrak{j}\}$, $\{\mathfrak{h}, \mathfrak{l}, \mathfrak{m}\}$, $\{\mathfrak{i}, \mathfrak{k}, \mathfrak{m}\}$, $\{\mathfrak{j}, \mathfrak{k}, \mathfrak{l}\}\}$.

Subspaces of projective spaces

We define a collection, U of points of a projective space to be *linear* if, given points p and q in U, then all the points on the line pq are also in U. Then the points of U, together with the lines determined by pairs of those points, will satisfy the first three axioms of a projective space, and form a *subspace* (possibly a degenerate one, as in the case of a single point, or all the points of a single line).

For a set of points X, define the *span* of X, $\langle X\rangle$ to be $\cap\{U|X \subset U, U \text{is a linear set}\}$.

A set of points B is called *independent* if for any subset $B' \subset B$ and point $p \in B\backslash B'$ then $p \notin \langle B'\rangle$.

An independent set of points of a projective space Π which span Π is called a *basis* for Π. Any two bases of a given projective space will have the same number of elements[12]. A finitely generated space has *dimension* d if any basis has $d+1$ points in it.

Dimension formula[12]: Let U and W be subspaces of Π. Then $\dim(\langle U,W\rangle) = \dim(U) + \dim(W) - \dim(U \cap W)$.

For use in the dimension formula, the dimension of a single point p is 0, while $dim(\varnothing) = -1$. A *hyperplane* is a subspace of dimension $d-1$ in a space of dimension d. Using the dimension formula it can be noted that a hyperplane and a line must meet in at least one point.

1.2.2 Constructions

Let V be a vector space of dimension $d+1$, where $d \geq 2$, over a division ring F. Define the geometry $\mathbf{P}(V)$ as follows: the points of $\mathbf{P}(V)$ are the 1-dimensional subspaces of V, the lines of $\mathbf{P}(V)$ are the 2-dimensional subspaces of V, and the incidence of $\mathbf{P}(V)$ is set-theoretical containment.

Theorem 1. *[12]*

$\mathbf{P}(V)$ is a projective space of dimension d.

Proof. (P1) Let p and q be distinct points of $\mathbf{P}(V)$. Let $\langle v_1\rangle$ and $\langle v_2\rangle$ be the corresponding one-dimensional subspaces of V, that is $p = \langle v_1\rangle$ and $q = \langle v_2\rangle$. Since $\langle v_1\rangle \neq \langle v_2\rangle$, v_1 and v_2 are linearly independent; hence $\langle v_1, v_2\rangle$ is a two-dimensional subspace. So $\ell = \langle v_1, v_2\rangle$ is the unique line containing p and q.

(P2) Suppose there are distinct points p, q, r, s in $\mathbf{P}(V)$, with corresponding one dimensional subspaces in V, respectively $\langle v_1\rangle$, $\langle v_2\rangle$, $\langle v_3\rangle$, $\langle v_4\rangle$, where v_i's are pairwise linearly independent. If pq meets rs then there is some v_5 in V contained in $\langle v_1, v_2\rangle \cap \langle v_3, v_4\rangle$. Take $v_5 = a_1 \cdot v_1 + a_2 \cdot v_2 = a_3 \cdot v_3 + a_4 \cdot v_4$; then take $a_1 \cdot v_1 - a_3 \cdot v_3 = a_4 \cdot v_4 - a_2 \cdot v_2 = v_6$. So $\langle v_6\rangle$ is contained in $\langle v_1, v_3\rangle \cap \langle v_2, v_4\rangle$. Hence the lines pr and qs meet at the point $\langle v_6\rangle$.

(P3) The line $\langle v_1, v_2\rangle$ contains the distinct points $\langle v_1\rangle$, $\langle v_2\rangle$, and $\langle v_1 + v_2\rangle$, because v_1 and v_2 are independent.

(P4) Since V has dimension at least 3, then there are three linearly independent vectors v_0, v_1, v_2 and so the lines $\langle v_0, v_1\rangle$ and $\langle v_0, v_2\rangle$ of $P(V)$ are distinct. □

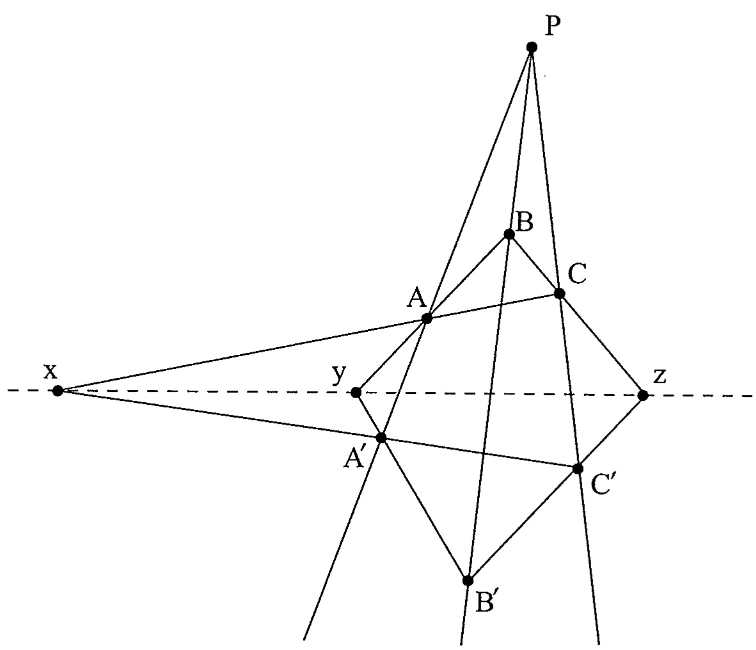
Example 7. The space given in Example 6 is constructed from a 4-dimensional vector space over $GF(2)$. Each point of the space corresponds to the nonzero point point of a line in the vector space as follows: $\mathfrak{a} = (1, 0, 0, 0)$, $\mathfrak{b} = (0, 1, 0, 0)$, $\mathfrak{c} =$

$(0,0,1,0), \mathfrak{d} = (1,1,1,1), \mathfrak{e} = (1,0,1,0), \mathfrak{f} = (1,1,0,0), \mathfrak{g} = (0,1,1,1), \mathfrak{h} = (0,1,1,0), \mathfrak{i} = (1,1,0,1), \mathfrak{j} = (1,0,1,1), \mathfrak{k} = (1,1,1,0), \mathfrak{l} = (0,1,0,1), \mathfrak{m} = (0,0,1,1), \mathfrak{n} = (1,0,0,1), \mathfrak{o} = (0,0,0,1)$.

1.2.3 Desargues' Theorem

Property [Desargues' Theorem]. *Given two triples of points, say A, B, C and A', B', C' such that the lines AA', BB' and CC' all meet at a point P, then points $x = AC \cap A'C'$, $y = AB \cap A'B'$ and $z = BC \cap B'C'$ are collinear.*

Figure 1.2: The Desargues' Configuration



We say that a space is *Desarguesian* if Desargues' Theorem holds for that space.

Theorem 2. *[12] A projective space is Desarguesian only when it is constructed over a skew field.*

Theorem 3. *[12] All projective spaces of dimension 3 or higher are Desarguesian.*

Hence all finite projective spaces of dimension 3 or higher arise from the field by the construction of Section 1.2.2.

1.3 Projective planes

According to Theorem 3, projective spaces of dimension 3 or higher are all Desarguesian, so we now take a closer look at the specific case of two dimensions. We start with a related structure, called an affine plane.

Definition 3. An *affine plane* $\mathcal{A} = \{P, L\}$ *or* $\Pi = \{P, L, \mathbf{I}\}$ *is a incidence structure that has the following properties:*

AP1: Every pair of points meet on a unique line.

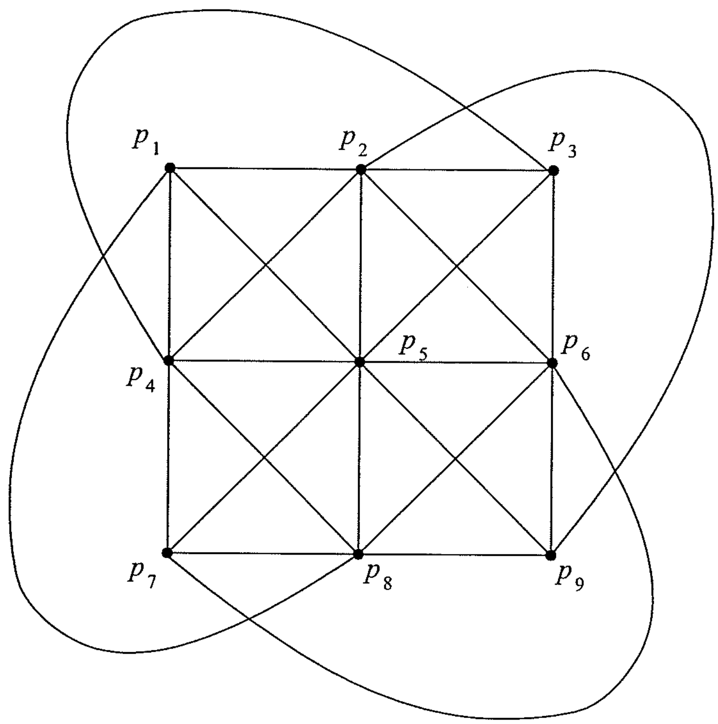
AP2: Given a point p *and a line* ℓ *where* $p \notin \ell$*, there is a unique line* m *such that* $p \in m$ *and* m *and* ℓ *have no points in common.*

AP3: There exist 3 noncollinear points.

Example 8. The following design is an affine plane (see Figure 1.3):

$\mathcal{V} = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9\}$ and $\mathcal{B} = \{\{p_1, p_2, p_3\}, \{p_4, p_5, p_6\}, \{p_7, p_8, p_9\}, \{p_1, p_5, p_9\}, \{p_2, p_6, p_7, \}, \{p_3, p_4, p_8\}, \{p_1, p_4, p_7\}, \{p_2, p_5, p_8\}, \{p_3, p_6, p_9\},$

Figure 1.3: An affine plane



$\{p_3, p_5, p_7\}$, $\{p_2, p_4, p_9\}$, $\{p_1, p_6, p_8\}\}$. **I** is given by set inclusion.

Definition 4. A *projective plane* $\Pi = \{P, L\}$ *or* $\Pi = \{P, L, \mathbf{I}\}$ *is a incidence structure that has the following properties:*

PP1: every pair of points meet on a unique line;

PP2: every pair of lines meet at a unique point;

PP3: there exist 4 points, no three of which are collinear.

Any projective plane is a projective space. Obviously, $PP1 \Rightarrow P1$. Since any pair of lines meet ($PP2$), $P2$ will hold. In this case, let $p = \ell_1 \cap \ell_2$ be the point where lines ℓ_1 and ℓ_2 meet. Let p_1, p_2, p_3, p_4 be the four points, no three of which are collinear (from $PP3$). There are at least two lines, say p_1p_2 and p_1p_3, so $P4$ holds. Also, each line has at least three points as follows: Any line of type p_ip_j will have the point $p_ip_j \cap p_kp_l$, (where $\{i, j, k, l\}$ is a permutation of $\{1, 2, 3, 4\}$). Any other line must meet both p_1p_2 and p_3p_4, both p_1p_3 and p_2p_4, and both p_1p_4 and p_2p_3. At the very least, it is on the point joining each pair, and hence is on at least 3 points. Since a projective space can be generated by 3 noncollinear points, it is a two dimensional projective space.

There is a connection between affine and projective planes: If a line and all the points on it is deleted from a projective plane an affine plane will result. Conversely given an affine plane, a projective plane can be obtained by adding a line in a particular way.

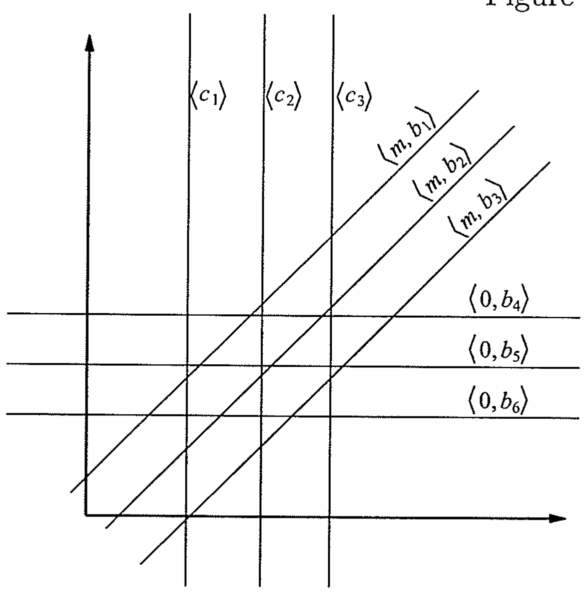
In an affine plane, maximal sets of lines which do not meet form parallel classes, as we will show. Let R be the relation on the lines of an affine plane $\mathcal{A}$ given by $\ell R m$ if $\ell = m$ or ℓ and m have no points in common. The relation R is obviously symmetric and reflexive. Let $hR\ell$ and $\ell R m$ for disjoint lines h, ℓ and m. If h and m had a point in common, say p, then there would be two lines on p which were disjoint from ℓ, which contradicts AP2. Hence R is transitive, and it is an equivalence relation on the lines of $\mathcal{A}$. From AP2, every point is on some line of an equivalence class, hence the lines of $\mathcal{A}$ are partitioned into parallel classes. To get a projective plane, a point is added for each parallel class, incident with each line in that class, and a new line is introduced which is incident to all these new points.

Example 9. One of the best known examples of an affine plane is the familiar real plane $\mathbb{R}^2$. See Figure 1.4

$P = \{(x, y)|x, y \in \mathbb{R}\}$. Lines play their usual role of solutions to equations of the type $y = mx + b$ or $x = c$. These can be represented by

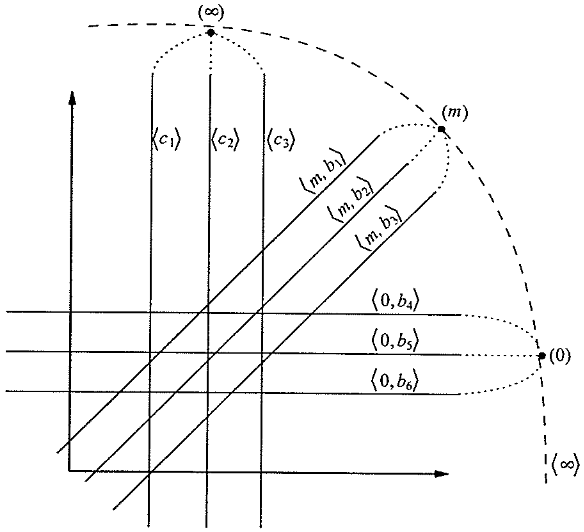
$L = \{\langle m, b\rangle|m, b \in \mathbb{R}\} \cup \{\langle c\rangle|c \in \mathbb{R}\}$

Figure 1.4: $\mathbb{R}^2$



Example 10. Let us build a projective plane by adding a line to the affine plane mentioned in Example 9. Compare Figure 1.4 to Figure 1.5

Figure 1.5: An infinite projective plane



We let $P = \{(x,y)|x,y \in \mathbb{R}\} \cup \{(t)|t \in \mathbb{R}\} \cup \{(\infty)\}$ and

$L = \{\langle x,y\rangle|x,y \in \mathbb{R}\} \cup \{\langle t\rangle|t \in \mathbb{R}\} \cup \{\langle\infty\rangle\}$.

The incidence is as follows:

$(x,y)\mathbf{I}\langle m,b\rangle$ iff $y = mx + b$

$(x,y)\mathbf{I}\langle c\rangle$ iff $x = c$

$(t)\mathbf{I}\langle m,b\rangle$ iff $t = m$

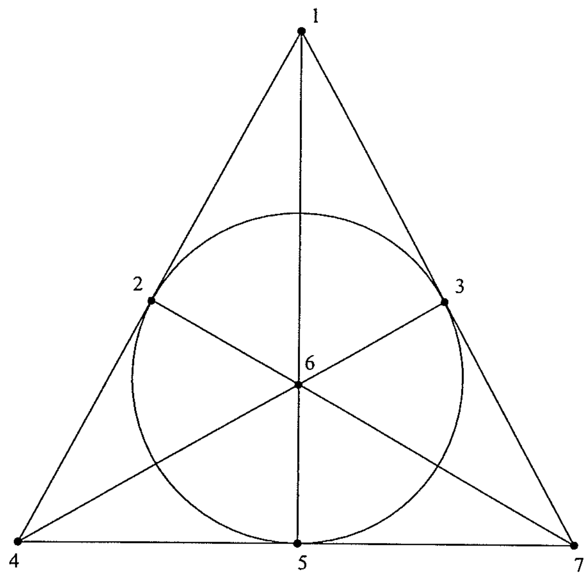
$(t)\mathbf{I}\langle\infty\rangle$ $\forall t \in \mathbb{R}$

$(\infty)\mathbf{I}\langle c\rangle$ $\forall c \in \mathbb{R}$

$(\infty)\mathbf{I}\langle\infty\rangle$

Example 11. The smallest finite projective plane, also known as the Fano plane

Figure 1.6: The Fano plane



(see Figure 1.6), has point set $P = \{1, 2, 3, 4, 5, 6, 7\}$, and lines

$L = \{\langle 1, 2, 4\rangle; \langle 2, 3, 5\rangle; \langle 3, 4, 6\rangle; \langle 4, 5, 7\rangle; \langle 5, 6, 1\rangle; \langle 6, 7, 2\rangle; \langle 7, 1, 3\rangle\}$.

1.3.1 Some elementary properties of projective planes

For a finite projective plane Π, we now consider the number of points on any line, and the number of lines through any point. We start by showing that any two lines of Π have the same number of points. Let ℓ_1 and ℓ_2 be any two lines of Π, and let the point at which they meet be p_0. Let the points of ℓ_1 be $p_0, p_1, \ldots, p_{k_1}$ and let the points of ℓ_2 be $p_0, q_1, \ldots, q_{k_2}$. By $PP3$, there is a point q not on ℓ_1 or ℓ_2.

Let the number of lines through q be $n + 1$. Since q must meet every point of ℓ_1, and it meets distinct points of ℓ_1 on distinct lines, since $q \notin \ell_1$, there are at least

k_1+1 lines through q. Also, since every line through q must meet ℓ_1 in some point, distinct for each line through q, there are exactly k_1+1 lines through q. Similarly with ℓ_2. Hence $k_1 = k_2 = n$. Similarly, any point not on ℓ_1 will have $n+1$ lines on it, and any line not on q will have $n+1$ points on it. Further, for any point on ℓ_2 or ℓ_2 there will be some line not on it containing $n+1$ points, hence it will also be on $n+1$ lines, for any line through q there will be a point not on it which is on $n+1$ lines, hence it will contain $n+1$ points.

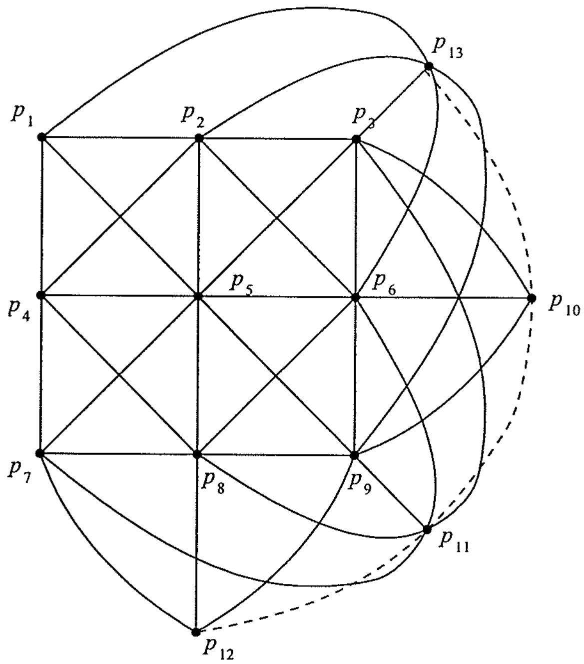
Since every line contains $n+1$ points, and every point is on $n+1$ lines, n the *order* of the projective plane.

To get the total number of points, fix a point Q. Each point of Π meets Q on a unique line, and there are $n+1$ lines through Q, each containing n points other than Q. So in total there are $n(n+1)+1 = n^2+n+1$ points. Similarly, there are n^2+n+1 lines.

We use the notation $PP(n)$ to denote a projective plane of order n. The plane in Example 11 is a $PP(2)$.

Example 12. A PP(3), whose diagram can be seen in Figure 1.7, is given by the point set $P = \{p_1, p_2, \ldots, p_{13}\}$ and the line set $L = \{\ \{p_1, p_2, p_3, p_{10}\}$, $\{p_4, p_5, p_6, p_{10}\}$, $\{p_7, p_8, p_9, p_{10}\}$, $\{p_1, p_5, p_9, p_{11}\}$, $\{p_2, p_6, p_7, p_{11}\}$, $\{p_3, p_4, p_8, p_{11}\}$, $\{p_1, p_4, p_7, p_{12}\}$, $\{p_2, p_5, p_8, p_{12}\}$, $\{p_3, p_6, p_9, p_{12}\}$, $\{p_3, p_5, p_7, p_{13}\}$, $\{p_2, p_4, p_9, p_{13}\}$,

Figure 1.7: A projective plane of order 3



$\{p_1, p_6, p_8, p_{13}\}$, $\{p_{10}, p_{11}, p_{12}, p_{13}\}$ }. This can also be formed by adding a line to the affine plane given in Example 8. Compare Figure 1.3 with Figure 1.7.

Now consider the incidence matrix of a projective plane. By the foregoing discussion, the incidence matrix of $PP(n)$ is an $(n^2+n+1) \times (n^2+n+1)$ matrix of 0's and 1's.

Example 13. The incidence matrix of the plane given in Example 12 is

$$\begin{pmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}.$$

The (i, j)-entry of AA^T will be the number of lines in which p_i meets p_j. This is $n + 1$ if $i = j$ (the number of lines through a point), and 1 otherwise (by $PP1$). Hence $AA^T = nI + J$ (J is defined as the matrix of all 1's of the appropriate size).

1.3.2 Subplanes

A *subplane* Π' of a projective plane Π is a projective plane whose points are a subset of the points of Π and each of whose lines is a subset of a line of Π. Note that a subplane is a not a subspace of a projective plane.

Theorem 4. *[10] If Π' is a subplane of order m of a plane Π of order n where $\Pi' \neq \Pi$ then either $m^2 = n$ or $m^2 + m \leq n$.*

Subplanes of order $\sqrt{n}$ are called *Baer* subplanes.

Theorem 5. *[10] If Π' is a subplane of order m of a projective plane Π of order $n = m^2$ then every line of Π meets Π' in at least one point.*

1.3.3 Coordinatization

The following can be found in [59]. Let Π be a projective plane of order n and let R be a set of n symbols containing the symbols 0 and 1 but not the symbol ∞. We pick 3 non-concurrent lines $\ell_1, \ell_2, \ell_\infty$, let p_X be $\ell_2\ell_\infty$; let p_Y be $\ell_1\ell_\infty$ and let p_O be $\ell_1\ell_2$. Let p_I be a point not on ℓ_1, ℓ_2 or ℓ_∞.

Let p_A be $p_X p_I \cap \ell_1$, let p_B be $p_Y p_I \cap \ell_2$ and let p_J be $p_A p_B \cap \ell_\infty$.

We now set up a correspondence between the symbols of R and the points of $\ell_1 \backslash p_Y$, arbitrarily except that the symbol 1 is assigned to the point p_A and the symbol 0 is assigned to the point p_O.

Now if p_C on $\ell_1 \backslash p_Y$, corresponding to $c \in R$, this point is assigned the coordinates of $(0, c)$. (So p_A is $(0, 1)$ and p_O is $(0, 0)$.)

To get coordinates of a point p_D on $\ell_2 \backslash p_X$, if $p_D p_J \cap \ell_1$ is $(0, d)$ then p_D is $(d, 0)$.

Now if p_E is a point outside of ℓ_1, ℓ_2 and ℓ_∞, $p_E p_X \cap \ell_1$ is $(0, f)$ and $p_E p_Y \cap \ell_2$ is $(g, 0)$ then p_E is (g, f).

If p_Z is a point of $\ell_\infty \backslash p_Y$, and $p_Z p_B \cap \ell_1$ is $(0, m)$ then p_Z is (m). Lastly, the point p_Y is (∞).

We now can assign coordinates to the lines according to the coordinates of the points. If a line ℓ is not on $p_Y = (\infty)$, and $\ell \cap \ell_\infty = (m)$ and $\ell \cap \ell_1 = (0, k)$ then $\ell = \langle m, k \rangle$. If ℓ is on p_Y and $\ell \neq \ell_\infty$, $\ell \cap \ell_2 = (b, 0)$, then $\ell = \langle b \rangle$. $\ell_\infty = \langle \infty \rangle$.

1.3.4 Latin squares

Definition 5. A *Latin square of order n* is an $n \times n$ array whose elements are n distinct symbols (commonly the numerals $1, \ldots, n$) such that each element appears once in every row and once in every column.

Example 14. A Latin square of order 3 :

$$\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{vmatrix}$$

Definition 6. Two Latin squares $A = [a_{ij}]$ and $B = [b_{ij}]$ are called *orthogonal* if the ordered pairs (a_{ij}, b_{ij}), $1 \leq i, j \leq n$, are all possible n^2 ordered pairs.

Example 15. The following Latin squares of order 3 are orthogonal.

$$\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{vmatrix}, \qquad \begin{vmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{vmatrix}$$

Lemma 6. *[47] There are at most $n-1$ mutually orthogonal Latin squares (commonly known as MOLS) of order n.*

If a set of $n-1$ mutually orthogonal Latin squares of order n exists, it is referred to as a *complete set of MOLS.*

Lemma 7. *[47] Every complete set of MOLS corresponds to projective plane of the same order. Every projective plane corresponds to one (or more) complete set of mutually orthogonal Latin squares.*

One way to view this correspondence is through the coordinatization of the plane. As seen in [59], from the coordinatization we can define a planar ternary ring, and from this we can define a complete set of MOLS.

1.3.5 The Lenz - Barlotti classification

Definition 7. A *collineation* of a projective plane is a surjection $\alpha : P \to P$ that preserves lines (hence induces a map $\alpha : L \to L$ such that $p^\alpha \in \ell^\alpha$ iff $p \in \ell$).

Example 16. Define a map α on the points of the Fano plane, seen in Example 11, as follows:

$\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 4$, $\alpha(4) = 5$, $\alpha(5) = 6$, $\alpha(6) = 7$, $\alpha(7) = 1$.

Under α lines map to lines as follows:

$\alpha[1,2,4] = [\alpha(1), \alpha(2), \alpha(4)] = [2,3,5]$, $\alpha[1,5,6] = [\alpha(1), \alpha(5), \alpha(6)] = [2,6,7]$,

$\alpha[1,3,7] = [\alpha(1), \alpha(3), \alpha(7)] = [2,4,1]$, $\alpha[2,3,5] = [\alpha(2), \alpha(3), \alpha(5)] = [3,4,6]$,

$\alpha[2,6,7] = [\alpha(2), \alpha(6), \alpha(7)] = [3,7,1]$, $\alpha[3,4,6] = [\alpha(3), \alpha(4), \alpha(6)] = [3,5,7]$,

$\alpha[4,5,7] = [\alpha(4), \alpha(5), \alpha(7)] = [5,6,1]$.

Observe that this collineation has no fixed points or fixed lines.

Example 17. Define another map β on the points of the Fano plane as follows

$$\beta(1) = 1,\ \beta(2) = 2,\ \beta(3) = 7,\ \beta(4) = 4,\ \beta(5) = 6,\ \beta(6) = 5,\ \beta(7) = 3.$$

Under β lines will map to lines as follows:

$$\beta[1,2,4] = [\beta(1),\beta(2),\beta(4)] = [1,2,4],\ \beta[1,5,6] = [\beta(1),\beta(5),\beta(6)] = [1,6,5],$$

$$\beta[1,3,7] = [\beta(1),\beta(3),\beta(7)] = [1,7,3],\ \beta[2,3,5] = [\beta(2),\beta(3),\beta(5)] = [2,7,6],$$

$$\beta[2,6,7] = [\beta(2),\beta(6),\beta(7)] = [2,5,3],\ \beta[3,4,6] = [\beta(3),\beta(4),\beta(6)] = [7,4,5],$$

$$\beta[4,5,7] = [\beta(4),\beta(5),\beta(7)] = [4,6,3].$$

This collineation fixes the points 1, 2 and 4, and it fixes the lines $[1,2,4]$, $[1,6,5]$ and $[1,7,3]$.

Example 18. Define yet another map γ on the points of the Fano plane as follows:

$$\gamma(1) = 2,\ \gamma(2) = 3,\ \gamma(3) = 1,\ \gamma(4) = 5,\ \gamma(5) = 7,\ \gamma(6) = 6,\ \gamma(7) = 4.$$

Under γ lines map to lines as follows:

$$\gamma[1,2,4] = [\gamma(1),\gamma(2),\gamma(4)] = [2,3,5],\ \gamma[1,5,6] = [\gamma(1),\gamma(5),\gamma(6)] = [2,7,6],$$

$$\gamma[1,3,7] = [\gamma(1),\gamma(3),\gamma(7)] = [2,1,4],\ \gamma[2,3,5] = [\gamma(2),\gamma(3),\gamma(5)] = [3,1,7],$$

$$\gamma[2,6,7] = [\gamma(2),\gamma(6),\gamma(7)] = [3,6,4],\ \gamma[3,4,6] = [\gamma(3),\gamma(4),\gamma(6)] = [1,5,6],$$

$$\gamma[4,5,7] = [\gamma(4),\gamma(5),\gamma(7)] = [5,7,4].$$

This collineation fixes the point 6 and the line $[4,5,7]$.

Definition 8. A *center* of a collineation α is a point p that is fixed linewise by α. Ie.

all lines through p are fixed by α. If a collineation α has a center, then it is referred to as a *central collineation.*

The collineation in Example 17 has the point 1 as its center. Notice that in Example 18, that even though 6 is a fixed point, it is not a center.

Definition 9. An *axis* of a collineation α is a line ℓ that is fixed pointwise by α. I.e. all points on ℓ are fixed by α.

The collineation in Example 17 has line $[1, 2, 4]$ as axis. Note that the fixed line in Example 18 is not an axis.

Lemma 8. *[46] A collineation α has a center iff it has an axis.*

We will refer to a central collineation with center p and axis ℓ as a (p, ℓ)*-collineation.* If $p \in \ell$ then a (p, ℓ)-collineation is called an *elation*, if $p \neq \ell$ then a (p, ℓ)-collineation is called a *homology.*

Lemma 9. *[46] A central collineation is completely determined by its center p, its axis ℓ and its action on one point x ($x \neq p$ $x \notin \ell$).*

Given a point p and a line ℓ in a projective plane Π, Π is called (p, ℓ)*-transitive* if for every pair of points x, x' ($x, x' \neq p$; $x, x' \notin \ell$) where x, x', p are collinear, there exists a (p, ℓ)-collineation α such that $\alpha(x) = x'$.

Lenz

Lenz developed a classification of projective planes based on what configuration of (p, ℓ)-transitivities can exist in the plane for flags (p, ℓ) [71]. There were originally seven different classes, but we will exclude those for which it is known that no planes of that type can exist (see [46]).

Let $\mathfrak{L}$ be $\{(p, \ell) \in P \times L | p \in \ell$ and Π is (p, ℓ)-transitive $\}$. Then Π is said to be:

Class I : $\mathfrak{L} = \varnothing$;

Class II: There exist $p \in P$ and $\ell \in L$, $p \in \ell$ such that $\mathfrak{L} = \{(p, \ell)\}$;

Class III: There exist $q \in P$ and $\ell \in L$, $q \notin \ell$ such that $\mathfrak{L} = \{(p, pq) | p \in \ell\}$;

Class IVa: There exists $\ell \in L$ such that $\mathfrak{L} = \{(p, \ell) | p \in \ell\}$;

Class IVb: There exists $p \in P$ such that $\mathfrak{L} = \{(p, \ell) | \ell \ni p\}$;

Class V: There exist $p \in P$ and $\ell \in L$ such that $\mathfrak{L} = \{(p, h) | h \ni p\} \cup \{(q, \ell) | q \in \ell\}$;

Class VII: $\mathfrak{L} = \{(p, \ell) | p \in \ell\}$.

Barlotti

Barlotti extended the classification set forth by Lenz to include transitivities for antiflags [6].

Let $\mathfrak{B}$ be $\{(p, \ell) \in P \times L | \Pi$ is (p, ℓ)-transitive$\}$

Class I.1: $\mathfrak{B} = \varnothing$;

Class I.2: There exist $p \in P$ and $\ell \in L$, $p \notin \ell$ such that $\mathfrak{B} = \{(p, \ell)\}$;

Class I.3: There exist $p, q \in P$ and $h, \ell \in L$, $p \notin \ell, p \in h, q \notin h, q \in \ell$ such that $\mathfrak{B} = \{(p, \ell), (q, h)\}$;

Class I.4: There exist non-collinear points p, q, r such that $\mathfrak{B} = \{(p, qr), (q, pr), (r, pq)\}$;

Class I.6: There exist $\ell \in L$ and $q \in P$ where $q \in \ell$, and a bijection $\phi : \ell\backslash\{q\} \rightarrow \{h | q \in h \neq \ell\}$ such that $\mathfrak{B} = \{(p, p^{\phi} | p \in \ell\backslash\{q\}\}$;

Class II.1: There exist $p \in P$ and $\ell \in L$, $p \in \ell$ such that $\mathfrak{B} = \{(p, \ell)\}$;

Class II.2: There exist $p, q \in P$ and $h, \ell \in L$, $p, q \in \ell, p \in h, q \notin h$ such that $\mathfrak{B} = \{(p, \ell), (q, h)\}$;

Class III.1: There exist $q \in P$ and $\ell \in L$, $q \notin \ell$ such that $\mathfrak{B} = \{(p, pq) | p \in \ell\}$;

Class III.2: There exist $q \in P$ and $\ell \in L$, $q \notin \ell$ such that $\mathfrak{B} = \{(q, \ell)\} \cup \{(p, pq) | p \in \ell\}$;

Class IVa.1: There exists $\ell \in L$ such that $\mathfrak{B} = \{(p, \ell) | p \in \ell\}$;

Class IVa.2: There exist $\ell \in L$ and $p, q \in P$, $p, q \in \ell$ such that $\mathfrak{B} = \{(r, \ell) | r \in \ell\} \cup \{(q, h) | h \ni p\} \cup \{(p, k) | k \ni q\}$;

Class IVa.3: There exist $\ell \in L$ and an involutory fixed point free permutation t of the points of ℓ such that $\mathfrak{B} = \{(p, \ell) | lp \in \ell\} \bigcup_{p \in \ell} \{(p^t, h) | h \ni p\}$;

Class IVb.1: There exists $p \in P$ such that $\mathfrak{B} = \{(p, \ell) | \ell \ni p\}$;

Class IVb.2: There exists $p \in P$ and lines $h, k \ni p$ such that

$\mathfrak{B} = \{(p,\ell)|\ell \ni p\} \cup \{(q,h)|q \in k\} \cup \{(r,k)|r \in h\}$;

Class IVb.3: There exists $p \in P$ and an involutory fixed point free permutation t of the lines of p such that $\mathfrak{B} = \{(p,\ell)|p \in \ell\} \bigcup_{h \ni p}\{(q,h^t)|q \in h\}$;

Class V: There exist $p \in P$ and $\ell \in L$ such that $\mathfrak{B} = \{(p,h)|h \ni p\} \cup \{(q,\ell)|q \in \ell\}$;

Class VII.1: $\mathfrak{B} = \{(p,\ell)|p \in \ell\}$;

Class VII.2: $\mathfrak{B} = \{(p,\ell)\}$.

Chapter 2

Orthogonal matrices

2.1 Hadamard matrices

Hadamard matrices were first introduced by Hadamard in 1893 [52], and have been the inspiration for much study.

Definition 10. A *Hadamard matrix* H is an $n \times n$ $(-1, 1)$-matrix such that

$$HH^T = nI.$$

We use the notation $H(n)$ to denote a Hadamard matrix of order n.

Example 19. The following is an H(4):

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

A Hadamard matrix has the property that its rows are pairwise orthogonal. It is known that Hadamard matrices of order n can only exist for $n = 1, 2$ or $n = 4a$,

$a \in \mathbb{Z}^+$ and it is conjectured that they exist for all of these values [52]. For more on Hadamard matrices and associated structures see [50].

Two Hadamard matrices are considered *equivalent* if one can be obtained from the other by a series of row switches, column switches, multiplication of a row by -1, or multiplication of a column by -1.

Example 20. The H(4) found in Example 19 is equivalent to

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

which was obtained by switching the second and third rows.

2.2 Weighing matrices

Definition 11. A *weighing matrix* $W = W(n, w)$ is an $n \times n$ $\{-1, 0, 1\}$-matrix which has the property that

$$WW^T = wI.$$

We call w the *weight* of the matrix.

Example 21. The following is a $W(4, 3)$:

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 0 \end{pmatrix}.$$

Two weighing matrices are considered *equivalent* if one can be obtained from the other by a series of row switches, column switches, multiplication of a row by -1, or multiplication of a column by -1.

2.3 Group ring basics

To introduce generalizations of Hadamard and weighing matrices whose elements are from a group, matrix multiplication will be defined over a group ring.

Let $G = \{g_i | i \in \mathsf{N}\}$ be a finite group, where N is some index set, and let R be a commutative ring with unity. Let $R[G]$ be the set of all formal sums

$$\sum_{i \in \mathsf{N}} a_i g_i$$

where $a_i \in R$ and $g_i \in G$. $R[G]$ is the *group ring*, with the following operations: The sum of two elements in $R[G]$ is defined by

$$\sum_{i \in \mathsf{N}} a_i g_i + \sum_{i \in \mathsf{N}} b_i g_i = \sum_{i \in \mathsf{N}} (a_i + b_i) g_i$$

and multiplication is defined by

$$\left(\sum_{i \in \mathsf{N}} a_i g_i \right) \left(\sum_{i \in \mathsf{N}} b_i g_i \right) = \sum_{i \in \mathsf{N}} \left(\sum_{g_j g_k = g_i} a_j b_k \right) g_i.$$

We use the following shorthand notation for the sum of the group elements (times the ring unit)

$$G_{\sum} := \sum_{g \in G} g.$$

The *conjugate* of an element $\alpha = \sum_{i \in \mathsf{N}} a_i g_i$ in the group ring is $\alpha^* := \sum_{i \in \mathsf{N}} a_i(g_i^{-1})$.

We are interested in two specific quotient rings. One is $\mathbb{Z}[G]/G_{\sum}$ for a group G. The other is based on sharply transitive subsets of the symmetric group S_n. A *sharply transitive subset* of S_n is a set A of permutations such that for any pair of positions, a and b, there is exactly one $p \in A$ where $p(a) = b$, and the quotient ring we are interested in is $\mathbb{Z}[S_n]/\mathcal{J}$ where $\mathcal{J}$ is the ideal generated by the sum of the elements of a sharply transitive subset of S_n.

2.4 Generalised Hadamard matrices

Definition 12. A *generalised Hadamard matrix* $GH(n, G)$ is an $n \times n$ matrix $H = [h_{ij}]$, whose entries are elements of a group G, such that, for all $i \neq j$,

$$\sum_{k=1}^{n} h_{ik} h_{jk}^{-1} = \lambda G_{\sum}, \tag{2.1}$$

where λ is an integer, called the *index* of H. Note that if $i = j$, $\sum_{k=1}^{n} h_{ik} h_{jk}^{-1} = n1$, where 1 is the group identity. Write $H^* = [h_{ji}^{-1}]$, transpose followed by entry-wise conjugation in the group ring. In this notation (2.1) becomes $HH^* = nI \bmod G_{\sum}$, with matrix multiplication carried out over the group ring $\mathbb{Z}[G]$.

We note that λ must be the same for all i, j when $i \neq j$. In particular, $\lambda = \frac{n}{|G|}$. We will be most interested in the case where $\lambda = 1$.

Example 22. We let $G = \{1, \gamma, \gamma^2\}$, the cyclic group of three elements. Then

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \gamma & \gamma^2 \\ 1 & \gamma^2 & \gamma \end{pmatrix}$$

is a $GH(3, C_3)$, for

$$HH^* = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \gamma & \gamma^2 \\ 1 & \gamma^2 & \gamma \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \gamma^2 & \gamma \\ 1 & \gamma & \gamma^2 \end{pmatrix} \equiv 3I_3 \bmod (1 + \gamma + \gamma^2).$$

Observe that $\lambda = 1$ for this GH.

Two generalised Hadamard matrices are considered *equivalent* if one can be obtained from the other by a series of row switches, column switches, multiplication of a row (on the left) by an element $g \in G$, or multiplication of a column (on the right) by an element $g \in G$.

2.5 Division tables

To give some motivation for this next definition, we introduce the use of a group's division tables as a method of representing its elements as permutation matrices.

Let G be a group of order n and let C_G be an $n \times n$ array of elements of G in the following way: Let $g_1 = 1, g_2, \ldots, g_n$ be an ordering of the elements of G and take the (i, j)-entry of C_G to be $g_i g_j^{-1}$. We now have a matrix representation of each group element g namely $\mathfrak{P}(g) = [a_{ij}]$ where

$$a_{ij} = \begin{cases} 1 & \text{if } C_G(i,j) = g \\ 0 & \text{otherwise.} \end{cases}$$

We denote the permutation representation of g by $[a_{ij}]$ as $\mathfrak{P}(g)$, and the group of all such permutations as $\mathfrak{P}(G)$. $\mathfrak{P}(G)$ is a subgroup of S_n isomorphic to G.

Example 23. The division table for the group C_3 is:

$\div$	1	γ	γ^2
1	1	γ	γ^2
γ	γ^2	1	γ
γ^2	γ	γ^2	1

So the permutation representation is as follows:

$$\mathfrak{P}(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \mathfrak{P}(\gamma) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \text{ and } \mathfrak{P}(\gamma^2) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

We can introduce a second set of permutation matrices from this table. Let s_i be the permutation that permutes the first row of C_G into the ith row. I.e. $s_i = [b_{jk}]$ where

$$b_{jk} = \begin{cases} 1 & \text{if } C_G(1,j) = C_G(i,k) \\ 0 & \text{otherwise.} \end{cases}$$

We denote the set of all such permutations as S_G.

Lemma 10. *S_G is a group isomorphic to G, and the elements of S commute with the elements of $\mathfrak{P}(G)$. I.e. if $s_i \in S$ and $g \in G$ then $\mathfrak{P}(g)s_i = s_i\mathfrak{P}(g)$.*

Proof. To get from row 1 to row i of C_G, we are simply multiplying (on the right) by the element g_i, so it is obvious that $S \simeq G$.

Suppose $\mathfrak{P}(g)s_i$ has a 1 in the (j,k)th position. Then, for some m_1, the (j,m_1)-entry of $\mathfrak{P}(g)$ is 1 and the (m_1,k)-entry of s_i is 1. Hence, the (j,m_1)-entry of C_G is g and the $C_G(1,m_1) = C_G(i,k)$. Let m_2 be the column of C_G such that $C_G(1,j) = C_G(i,m_2)$.

Now since

$$\begin{aligned} g_{m_2}g_k^{-1} &= g_{m_2}g_i^{-1}g_ig_k^{-1} \\ &= (g_ig_{m_2}^{-1})^{-1}(g_1g_{m_1}^{-1}) \\ &= (g_1g_j^{-1})^{-1}(g_1g_{m_1}^{-1}) \\ &= g_jg_1^{-1}g_1g_{m_1}^{-1} \\ &= g_jg_{m_1}^{-1} \\ &= g \end{aligned}$$

the (j,k)-entry of $s_i\mathfrak{P}(g)$ is also 1. Hence $\mathfrak{P}(g)s_i = s_i\mathfrak{P}(g)$.

□

Example 24. Let G be the dihedral group $D_3 = \{x, y | x^3 = 1, y^2 = 1, yx = x^2y\}$.

Its division table is

$\div$	1	x	x^2	y	xy	x^2y
1	1	x^2	x	y	xy	x^2y
x	x	1	x^2	xy	x^2y	y
x^2	x^2	x	1	x^2y	y	xy
y	y	xy	x^2y	1	x^2	x
xy	xy	x^2y	y	x	1	x^2
x^2y	x^2y	y	xy	x^2	x	1

In this case, the permutation representation of the group G is generated by the matrices $\mathfrak{P}(x) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$, and $\mathfrak{P}(y) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$.
The group S, as described above, is generated by the matrices

$$s_x = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } s_y = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

.

It can be easily checked that $\mathfrak{P}(x)s_x = s_x\mathfrak{P}(x)$, $\mathfrak{P}(y)s_x = s_x\mathfrak{P}(y)$, $\mathfrak{P}(x)s_y = s_y\mathfrak{P}(x)$, and $\mathfrak{P}(y)s_y = s_y\mathfrak{P}(y)$, as expected.

The *centralizer* of a set A in S_n is the set of all elements in S_n which commute with every element of A.

Lemma 11. *The group S is the centralizer of $\mathcal{P}(G)$ in S_n.*

Proof. Suppose s is a permutation in S_n such that $s\mathfrak{P}(g) = \mathfrak{P}(g)s$ for $g \in G$. The

(i,j)-entry of $s\mathfrak{P}(g)s$ is a 1 if, for some m_1, the (i,m_1)-entry of s is 1 and the (m_1,j)-entry of $\mathfrak{P}(g)$ is also 1.

The (i,j)-entry of $\mathfrak{P}(g)s$ is 1 if for some m_2 the (i,m_2)-entry of $\mathfrak{P}(g)$ is 1 and the (m_2,j)-entry of s is 1.

Suppose $C_G(m_1,j) = C_G(i,m_2) = g$, and let z be the row such that $C_G(z,m_1) = C_G(1,i)$. Then

$$\begin{aligned} g_z g_j^{-1} &= g_z g_{m_1}^{-1} g_{m_1} g_j^{-1} \\ &= g_1 g_i^{-1} g_i g_{m_2}^{-1} \\ &= g_1 g_{m_2}^{-1}. \end{aligned}$$

So the z'th row also contains the m_2'th entry of the first row in the j'th column. Hence s is the element of S which permutes the first row of C_G into the z'th row.

□

Let G be a group of order n. We say that an $n \times n$ matrix A is *group developed* over the group G if $A(i,j) = A(s,t)$ whenever $C_G(i,j) = C_G(s,t)$. I.e. a matrix is group developed if the matrix has the same element in each entry that there is a g in C_G.

Example 25. The matrix $\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$ is group developed, matching in this way the pattern of entries in the division table in Example 23.

Example 26. The matrix

$$\begin{pmatrix} a & b & c & d & e & f \\ c & a & b & e & f & d \\ b & c & a & f & d & e \\ d & e & f & a & b & c \\ e & f & d & c & a & b \\ f & d & e & b & c & a \end{pmatrix}$$

is also group developed, matching the division table of the dihedral group given in Example 24.

2.6 Generalised permutation Hadamard matrices

Here is the first of two new generalisations of Hadamard matrices that we introduce for studying projective planes.

Definition 13. A *generalised permutation Hadamard matrix* $GPH(n, m)$ is an $n \times n$ array $H = [P_{ij}]$ whose entries are elements of S_m ($m \times m$ permutations, generally considered to be permutation matrices) such that

$$\sum_{k=1}^{n} P_{ik} P_{jk}^{-1} = sJ$$

for some integer s when $i \neq j$. Note that if $i = j$ then $\sum_{k=1}^{n} P_{ik} P_{jk}^{-1} = nI$. Hence $HH^* = nI \mod J$.

Example 27. The following matrix is a generalised permutation Hadamard matrix.

$$\begin{pmatrix} 0&0&1&0&0&1&0&0&1\\ 0&1&0&0&1&0&0&1&0\\ 1&0&0&1&0&0&1&0&0\\ \\ 0&0&1&0&1&0&1&0&0\\ 0&1&0&1&0&0&0&0&1\\ 1&0&0&0&0&1&0&1&0\\ \\ 0&0&1&1&0&0&0&1&0\\ 0&1&0&0&0&1&1&0&0\\ 1&0&0&0&1&0&0&0&1 \end{pmatrix}$$

Two generalised permutation Hadamard matrices are considered *equivalent* if one can be obtained from the other by a series of row switches, column switches, multiplication of a row (on the left) by an element $p \in S_n$, or multiplication of a column (on the right) by an element $p \in S_n$.

We say that a Hadamard matrix (generalised Hadamard matrix, generalised permutation Hadamard matrix) is in *normalised* form if all the elements in the first row and first column are 1 (group identity, identity matrix). Every Hadamard (generalised Hadamard, generalised permutation Hadamard) matrix is equivalent to a normalised matrix. The submatrix of all the elements except the first row and first column of a normalised matrix will be referred to as its *core*.

2.7 Generalised weighing matrices

Definition 14. A *generalised weighing matrix* $GW(n, w; G)$ is an $n \times n$ matrix $W = [w_{ij}]$ whose entries are either 0 or elements of the group G (note that 0 is the additive identity in the group ring) such that for all $i \neq j$, there is some integer m_{ij} where

$$\sum_{k=1}^{n} w_{ik} w_{jk}^{*} = m_{ij} G_{\Sigma}$$

and for $i = j$, $\sum_{k=1}^{n} w_{ik} w_{jk}^{-1} = w1$ where 1 is the group identity of G. Note that these operations are taken over the group ring, so if $w_{jk} = 0$ then $w_{jk}^{*} = 0$, otherwise $w_{ij}^{*} = w_{ij}^{-1}$. We call w the *weight* of the matrix.

Matrix multiplication is defined over the group ring $\mathbb{Z}[G]$. Then W is a generalised weighing matrix if $WW^{*} = wI \bmod G_{\Sigma}$.

Note that generalised Hadamard matrices are a special case of generalised weighing matrices where the weight is the order of the matrix.

Example 28. Taking $G = \{1, \gamma, \gamma^2\}$ as in Example 22, then the following is a $GW(5, 4; G)$

$$W = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \gamma & \gamma^2 \\ 1 & 1 & 0 & \gamma^2 & \gamma \\ 1 & \gamma & \gamma^2 & 0 & 1 \\ 1 & \gamma^2 & \gamma & 1 & 0 \end{pmatrix}$$

since

$$WW^{*} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \gamma & \gamma^2 \\ 1 & 1 & 0 & \gamma^2 & \gamma \\ 1 & \gamma & \gamma^2 & 0 & 1 \\ 1 & \gamma^2 & \gamma & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \gamma^2 & \gamma \\ 1 & 1 & 0 & \gamma & \gamma^2 \\ 1 & \gamma^2 & \gamma & 0 & 1 \\ 1 & \gamma & \gamma^2 & 1 & 0 \end{pmatrix}$$

$$= 4I_5 \bmod (1 + \gamma + \gamma^2).$$

Two generalised weighing matrices are considered *equivalent* if one can be obtained from the other by a series of row switches, column switches, multiplication of a row (on the left) by an element $g \in G$, or multiplication of a column (on the right) by an element $g \in G$.

2.8 Generalised permutation weighing matrices

This is the second generalization introduced specifically for the study of projective planes.

Definition 15. A *generalised permutation weighing matrix* $GPW(n, w; m)$ is an $n \times n$ matrix $P = [P_{ij}]$ whose entries are elements of S_m ($m \times m$ permutation matrices) or an $m \times m$ matrix of all 0's such that

$$\sum_{k=1}^{n} P_{ik} P_{jk}^* = sJ$$

for some integer $s = s_{ij}$ for all $i \neq j$ and for $i = j$, $\sum_{k=1}^{n} P_{ik} P_{jk}^* = wI_m$. We say that w is the *weight* of the matrix. Hence $PP^* = wI \bmod J$.

Example 29. We let S_3 be generated by $x = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ then the following is a $GPW(5, 4, 3)$:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & x^2y & xy & y \\ 1 & x^2y & 0 & y & xy \\ 1 & xy & y & 0 & x^2y \\ 1 & y & xy & x^2y & 0 \end{pmatrix}$$

Two generalised permutation weighing matrices are considered *equivalent* if one can be obtained from the other by a series of row switches, column switches, multiplication of a row (on the left) by an element $p \in S_n$, or multiplication of a column (on the right) by an element $p \in S_n$.

We will mostly consider GW's and GPW's where the weight is $n-1$ (one less than the size of the array), hence each row (permutation row) will have only one zero (matrix of zero's).

We say that a weighing (generalised weighing, generalised permutation weighing) matrix of weight $n-1$ is in *normalised* form if the elements on the diagonal are 0 and all the other elements in the first row and first column are 1 (group identity, identity matrix). Every weighing (generalised weighing, generalised permutation weighing) matrix of weight $n-1$ is equivalent to a normalised one. The submatrix of all the elements except the first row and first column of a normalised matrix will be referred to as its *core*.

2.9 Power Hadamard matrices

Definition 16. A *Butson Hadamard* matrix $B = B(n, m)$ is an $n \times n$ matrix whose elements are m^{th} roots of unity such that $BB^* = nI$.

Power Hadamard matrices are yet another type of orthogonal matrix and can be seen as a generalization of Butson Hadamard matrices [34]. The entries of a power Hadamard matrix are powers of a variable (usually x), and the conjugate is taken in terms of the ring $\mathbb{Z}[x, x^{-1}]$, hence $(x^a)^* = x^{-a}$.

Definition 17. Let $H = [h_{ij}]$ be a matrix whose entries are powers of an indeterminate x, and let $H^* = [h^*_{ji}]$. If there exists a polynomial $f(x) \in \mathbb{Z}[x]$ such that $HH^* = hI$ where the algebra is in the ring $\mathbb{Z}[x, \frac{1}{x}]/\langle f(x)\rangle$, then H is said to be a *power Hadamard matrix* with respect to $f(x)$, and we write $H = PH(h, f(x))$.

Example 30. The following is a power Hadamard matrix $PH(3, 1 + x + x^2)$:

$$H = \begin{pmatrix} 1 & x & x \\ x & 1 & x \\ x & x & 1 \end{pmatrix}.$$

Since $$HH^* = \begin{pmatrix} 1 & x & x \\ x & 1 & x \\ x & x & 1 \end{pmatrix} \begin{pmatrix} 1 & x^{-1} & x^{-1} \\ x^{-1} & 1 & x^{-1} \\ x^{-1} & x^{-1} & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 3 & x^{-1} + x + 1 & x^{-1} + 1 + x \\ x + x^{-1} + 1 & 3 & 1 + x^{-1} + x \\ x + 1 + x^{-1} & 1 + x + x^{-1} & 3 \end{pmatrix}$$

And now since $x + 1 + x^{-1} = (x^{-1})(x^2 + x + 1)$, the above matrix is

$3I \mod 1 + x + x^2$.

We define $\Phi_k(x)$, the *cyclotomic polynomial of order* k as

$$\Phi_k(x) = \prod_{\substack{\gamma \text{ is a primitive} \\ k^{th} \text{ root of unity}}} (x - \gamma).$$

If r an n length row vector, we use the notation $circ(r)$ for to be an $n \times n$ matrix whose first row is r and each subsequent row is a right shift of the row above it.

Example 31. $circ(1\ x\ y\ z) = \begin{pmatrix} 1 & x & y & z \\ z & 1 & x & y \\ y & z & 1 & x \\ x & y & z & 1 \end{pmatrix}$

Chapter 3

Matrix Forms of the Plane

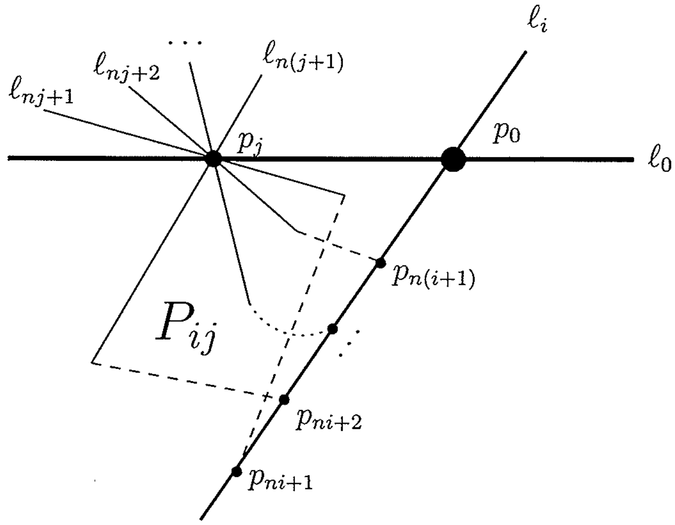
3.1 The flag form of the incidence matrix

The incidence matrix of a finite projective plane has a well known normalised form, developed in 1953 by L.J. Paige and C. Wexler [78]. This form is directly related to complete sets of orthogonal Latin squares [14], [47], [51].

Observe that the incidence matrix of a projective plane was built with an arbitrary ordering of the points and lines of the plane. Picking a particular ordering, we can get a nice structure.

Suppose Π is a projective plane of order n. Select a flag, (p_0, ℓ_0). Let $\ell_1, \cdots, \ell_n$ be the n lines through p_0 other than ℓ_0, and also let $p_1, \cdots, p_n$ be the n points on ℓ_0 other than p_0. Now for $i = 1, \ldots, n$ each ℓ_i has n more points on it, other than p_0. And, since all the lines $\ell_1, \ldots, \ell_n$ already meet (at point p_0), this accounts for all $n(n+1)$ remaining points. Hence label the remaining n points of ℓ_i: $p_{ni+1}, \ldots, p_{n(i+1)}$. Similarly, label the n lines through p_i: $\ell_{ni+1}, \ldots, \ell_{n(i+1)}$. Now consider the incidence

Figure 3.1: Permutations in flag form



matrix of Π with respect to this particular ordering.

We consider the submatrix P_{ij} consisting of the rows $ni+1, \ldots, n(i+1)$ and columns $nj+1, \ldots, n(j+1)$. Since each point $p_{ni+1}, \ldots, p_{n(i+1)}$ must be on exactly one line with point p_j, there must be exactly one 1 in each row of this submatrix. Similarly, each line of $\ell_{nj+1}, \ldots, \ell_{n(j+1)}$ must meet line ℓ_i in some point, so there must be exactly one 1 in each column of this submatrix. Hence this submatrix is an $n \times n$ permutation matrix. See Figure 3.1.

We will refer to the flag (p_0, ℓ_0) as the *anchor* of this form. The submatrix consisting of the rows $n+1, \ldots, n^2+n$ and columns $n+1, \ldots, n^2+n$ is the *kernel*. See matrix in Figure 3.2, showing the kernel as a matrix of permutations.

The kernel of this incidence matrix can be viewed in two ways; (i) as an $n^2 \times n^2$

Figure 3.2: Incidence matrix in flag form

$$
\left(\begin{array}{c|c}
\begin{array}{ccccc}
1 & 1 & 1 & \cdots & 1 \\
1 & 0 & 0 & \cdots & 0 \\
1 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 0 & 0 & \cdots & 0
\end{array}
&
\begin{array}{ccccccccccccccccc}
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & & 0 & 0 & 0 & \cdots & 0 \\
1 & 1 & 1 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 & & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 & 1 & 1 & \cdots & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & & 1 & 1 & 1 & \cdots & 1
\end{array}
\\ \hline
\begin{array}{ccccc}
0 & 1 & 0 & \cdots & 0 \\
0 & 1 & 0 & \cdots & 0 \\
0 & 1 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 1 & 0 & \cdots & 0 \\
\\
0 & 0 & 1 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 1 & \cdots & 0 \\
 & & \vdots & & \\
0 & 0 & 0 & \cdots & 1 \\
0 & 0 & 0 & \cdots & 1 \\
0 & 0 & 0 & \cdots & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 1
\end{array}
&
\begin{array}{cccc}
P_{11} & P_{12} & \cdots & P_{1n} \\
P_{21} & P_{22} & \cdots & P_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
P_{n1} & P_{n2} & \cdots & P_{nn}
\end{array}
\end{array}\right)
$$

matrix of 0's and 1's, and (ii) as an $n \times n$ matrix of permutations, elements of the symmetric group S_n. Considered in this second way, this matrix is a generalised permutation Hadamard matrix; i.e., it is a $GPH(n, n)$.

To see this, view the above matrix in block form.

$$A = \begin{pmatrix} M & B \\ B^T & C \end{pmatrix}$$

where

$$M = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & & 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 & & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 1 & \cdots & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & & 1 & 1 & 1 & \cdots & 1 \end{pmatrix}$$

and C is the kernel.

Since A is the incidence matrix of a projective plane, we know that $AA^T = nI + J$; hence

$$AA^T = \begin{pmatrix} M & B \\ B^T & C \end{pmatrix} \begin{pmatrix} M^T & B \\ B^T & C^T \end{pmatrix}$$

$$= \begin{pmatrix} MM^T + BB^T & MB + BC^T \\ B^TM^T + CB^T & B^TB + CC^T \end{pmatrix} = nI + J$$

Equating the $(2,2)$ blocks, we have $B^TB + CC^T = nI_{n^2} + J_{n^2}$. Now noting that

$$B^TB = \begin{pmatrix}
\begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \cdots & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} \\
\begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} & \cdots & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} \\
\vdots & \vdots & \ddots & \vdots \\
\begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \cdots & \begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix}
\end{pmatrix},$$

$$\text{in block form } BB^T = \begin{pmatrix} \mathrm{J}_n & 0 & \cdots & 0 \\ 0 & \mathrm{J}_n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathrm{J}_n \end{pmatrix}$$

it follows that

$$CC^T = \left(\begin{array}{cccccccccccccc}
n & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 & & 1 & 1 & \cdots & 1 \\
0 & n & \cdots & 0 & 1 & 1 & \cdots & 1 & \cdots & 1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & n & 1 & 1 & \cdots & 1 & & 1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 & n & 0 & \cdots & 0 & & 1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 & 0 & n & \cdots & 0 & \cdots & 1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1 & 0 & 0 & \cdots & n & & 1 & 1 & \cdots & 1 \\
 & \vdots & & & & \vdots & & & \ddots & & \vdots & & \\
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & & n & 0 & \cdots & 0 \\
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & \cdots & 0 & n & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & & 0 & 0 & \cdots & n
\end{array}\right),$$

$$\text{in block form } CC^T = \begin{pmatrix} n\mathrm{I}_n & \mathrm{J}_n & \cdots & \mathrm{J}_n \\ \mathrm{J}_n & n\mathrm{I}_n & \cdots & \mathrm{J}_n \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{J}_n & \mathrm{J}_n & \cdots & n\mathrm{I}_n \end{pmatrix}.$$

Since P is a permutation matrix, $P^{-1} = P^T$. So for $C = [P_{ij}]$, we get

$$C^T = [P_{ij}^T]^T = [Pji^T] = [P_{ji}^{-1}] = C^*.$$

Hence $CC^* = nI \bmod J$, hence C is a $GPH(n,n)$.

Note that the kernel is not unique but, for a given anchor, the different possible kernels are equivalent (as GPH matrices). It can depend upon the order of the points $p_1, \cdots, p_n$ (order of the columns), the lines $\ell_1, \cdots, \ell_n$ (order of the rows), or the order of $p_{ni+1}, \ldots, p_{n(i+1)}$ (multiplication of a row by an element of S_n) or $\ell_{ni+1}, \ldots, \ell_{n(i+1)}$

(multiplication of a column by an element of S_n). However, different anchors may give inequivalent kernels.

Example 32. The following matrix is an incidence matrix of the Fano plane, described in Example 11, with flag $(1, \langle 1, 2, 4\rangle)$ as the anchor.

$$\left(\begin{array}{ccc|cccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right)$$

The kernel is

$$\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right).$$

We can replace the permutation blocks with representatives from the group $Z_2 = \{e, a\}$ to get the following $GH(2, Z_2)$:

$$\begin{pmatrix} e & e \\ e & a \end{pmatrix}$$

Using the natural group isomorphism from Z_2 into $\{1, -1\}$ we get the Hadamard matrix

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Example 33. The following matrix is a flag form of the projective plane of order 3.

$$\left(\begin{array}{cccc|ccccccccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
\hline
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0
\end{array}\right).$$

The kernel is

$$\left(\begin{array}{ccc|ccc|ccc}
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
\hline
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0
\end{array}\right),$$

which can be represented by the following $GH(3, C_3)$ where C_3 is the cyclic group $\{e, \gamma, \gamma^2\}$:

$$\begin{pmatrix}
e & e & e \\
e & \gamma & \gamma^2 \\
e & \gamma^2 & \gamma
\end{pmatrix}.$$

Example 34. The following is a flag form of the projective plane of order 4.

$$
\left(\begin{array}{ccccc|cccccccccccccccc}
1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
\hline
0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&1&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
0&0&1&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&0&1&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&1&0\\
0&0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&0&1&0&0&1&0&0&1&0&0&1&0&0&0\\
0&0&0&1&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&1&0\\
0&0&0&1&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&1&0&0&1&0&0&0&0&0&1&1&0&0&0\\
0&0&0&1&0&0&0&0&1&1&0&0&0&0&0&1&0&0&1&0&0\\
0&0&0&0&1&1&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&1&0&0&1&0&1&0&0&0\\
0&0&0&0&1&0&0&1&0&1&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&1&0&0&0&1&0&1&0&0&1&0&0&0&0&0&1&0
\end{array}\right)
$$

The kernel is

$$\left(\begin{array}{cccc|cccc|cccc|cccc}
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
\hline
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&1&0&0&1&0&0&0&0&0&0&1&0&0&1&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&0&1&0&0&1&0&0&1&0&0&1&0&0&0\\
\hline
1&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0\\
0&1&0&0&0&0&0&1&0&0&1&0&1&0&0&0\\
0&0&1&0&1&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&1&0&1&0&0&1&0&0&0&0&0&1&0\\
\hline
1&0&0&0&0&0&0&1&0&1&0&0&0&0&1&0\\
0&1&0&0&0&0&1&0&1&0&0&0&0&0&0&1\\
0&0&1&0&0&1&0&0&0&0&0&1&1&0&0&0\\
0&0&0&1&1&0&0&0&0&0&1&0&0&1&0&0
\end{array}\right)$$

which is also representable by

$$\begin{pmatrix} e & e & e & e \\ e & a & b & ab \\ e & b & ab & a \\ e & ab & a & b \end{pmatrix},$$

a $GH(4, G)$ where G is the Klein-4 group $\{a, b | a^2 = 1, b^2 = 1, ab = ba\}$.

Lemma 12. *If Π is a plane with kernel $GPH(n, n)$ and $s \in S_n$ is a permutation which commutes with every element in the $GPH(n, n)$, then we can associate with it a (p, ℓ)-collineation, where (p, ℓ) is the anchor.*

Proof. We define the map α as follows: points $p_0, \ldots, p_n$ will all map to themselves, i.e. $\alpha(p_0) = p_0$, etc.. Points $p_{ni+1}, \ldots, p_{n(i+1)}$ will be mapped according to the permutation s, i.e. $\alpha(p_{ni+j}) = p_{ni+s(j)}$.

This will induce a similar map on the lines. So lines $\ell_0, \ldots, \ell_n$ will all map to themselves, and $\alpha(\ell_{ni+j}) = \ell_{ni+s(j)}$.

All incidences with the points $p_0, \ldots, p_n$ are preserved, since a line in the set $\{\ell_{ni+1}, \ldots, \ell_{n(i+1)}\}$ maps to another line in that set, incidences with lines $\ell_0, \ldots, \ell_n$ are similarly preserved. Now consider the incidence of points $p_{nk+1}, \ldots, p_{n(k+1)}$ and lines $\ell_{nm+1}, \ldots, \ell_{n(m+1)}$. The incidence is given by the (k, m) element of $GPH(n, n)$, say g. Reordering the points according to the permutation s is the same as multiplication on the left by s, and reordering the lines according to the permutation s is the same as multiplication on the right by s^{-1}. Since s commutes with g, we get that $sgs^{-1} = g$. So if $p_{nk+i} \in \ell_{nm+j}$ then $\alpha(p_{nk+i}) \in \alpha(\ell_{nm+j})$.

This gives a central collineation with center p and axis ℓ. □

Theorem 13. *[39] If the kernel of a projective plane $PP(n)$, with anchor (p, ℓ), forms a generalised Hadamard matrix $GH(n, G)$, where $|G| = n$, then this $PP(n)$ is (p, ℓ)-transitive.*

Proof. Let Π be a projective plane of order n whose kernel is a $GH(n, G)$; $|G| = n$, when anchored at (p, ℓ). Let $s \in S$, where S is the group associated with G described in Lemma 10. From Lemma 12, there is a collineation associated with s. Since $|G| = n$, G is a transitive subgroup of S_n, and hence S is a transitive group, and we can get such a collineation for each element, Π is (p, ℓ)-transitive. □

Corollary 14. *If a projective plane $PP(n)$ has a flag form such that the kernel is a generalised Hadamard matrix of index 1, then it is of Lenz class at least II.*

Converse to Theorem 13:

Theorem 15. *If a projective plane $PP(n)$ is (p, ℓ)-transitive for flag (p, ℓ), then it has a kernel that is a $GH(n, G)$ where $|G| = n$.*

Proof. Suppose $PP(n)$ is (p, ℓ)-transitive. Arrange the incidence matrix with anchor (p, ℓ) having kernel C, a $GPH(n, n)$ in normalised form. Let α be a permutation in the group of (p, ℓ)-collineations, we can associate with it a permutation $s \in S_n$. Let s be the permutation which takes points $p_{n+1}, \ldots, p_{2n}$ to points $\alpha(p_{n+1}), \ldots, \alpha(p_{2n})$. Since the kernel is normalised, there is an identity matrix in the $(1, i)$-entry of C. So, s is also be the action of α on lines $\ell_{ni+1}, \ldots, \ell_{n(i+1)}$. Since s is the action on lines $\ell_{n+1}, \ldots, \ell_{2n}$, and since there is an identity matrix in the $(j, 1)$-entry of C, s is the action on points $p_{nj+1}, \ldots, p_{n(j+1)}$. Since incidence is preserved, for every entry g of C, $sgs^{-1} = g$. So g is in the centralizer of the group generated by the permutations s. So by Lemma 11, the elements of $GPH(n, n)$ are from a group of order n. So the $GPH(n, n)$ is a $GH(n, G)$ where G is isomorphic to the group of (p, ℓ)-collineations. □

Example 35. We now take another look at the kernel of the matrix given in Example 32. The Fano plane, along with all Desarguesian planes, are known to be (p, ℓ)-transitive for all p and ℓ. Hence we would expect to get a GH, as we did. Similarly with Example 33, and Example 34 .

3.1.1 Latin squares and flag form

There is an easy way to build a set of mutually orthogonal Latin squares from the flag form of the incidence matrix of a projective plane [14] [51]. To each column beyond the first in the normalised kernel, we associate a Latin square whose ith row is the ith permutation of that column acting on $\left[\begin{array}{ccc} 1 & \cdots & n \end{array}\right]$.

Example 36. Using the kernel from Example 34, we can form the following set of MOLS:

$$\left|\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array}\right|, \quad \left|\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{array}\right|, \quad \left|\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{array}\right|.$$

3.2 The anti-flag form of the incidence matrix

We introduce here a second nice form of the incidence matrix. First, pick an anti-flag (p_0, ℓ_0). Let $\ell_1, \ldots, \ell_{n+1}$ be the $n+1$ lines on p_0, and we let $p_1, \ldots, p_{n+1}$ be the $n+1$ points on ℓ_0 such that p_i is on ℓ_i for $i = 1, \ldots, n+1$ (ℓ_i must meet ℓ_0 at a unique point). Now, for $j = 1, \ldots, n-1$, ℓ_j has $n-1$ more points on it, other than p_0 and p_i. And, since all the lines $\ell_1, \ldots, \ell_{n+1}$ already meet (at point p_1), these are all distinct. So arrange the points so that $p_{(n+2)+(i-1)(n-1)}, \ldots, p_{(n+1)+(i)(n-1)}$ are the other $n-1$

points of ℓ_i. Similarly, the lines $\ell_{(n+2)+(i-1)(n-1)}, \ldots, \ell_{(n+1)+(i)(n-1)}$ are the other $n-1$ lines through p_i.

Now for $i, j = 0, \ldots, n-1$, the submatrix consisting of the rows indexed by

$$(n+2) + i(n-1), \ldots, (n+1) + (i+1)(n-1)$$

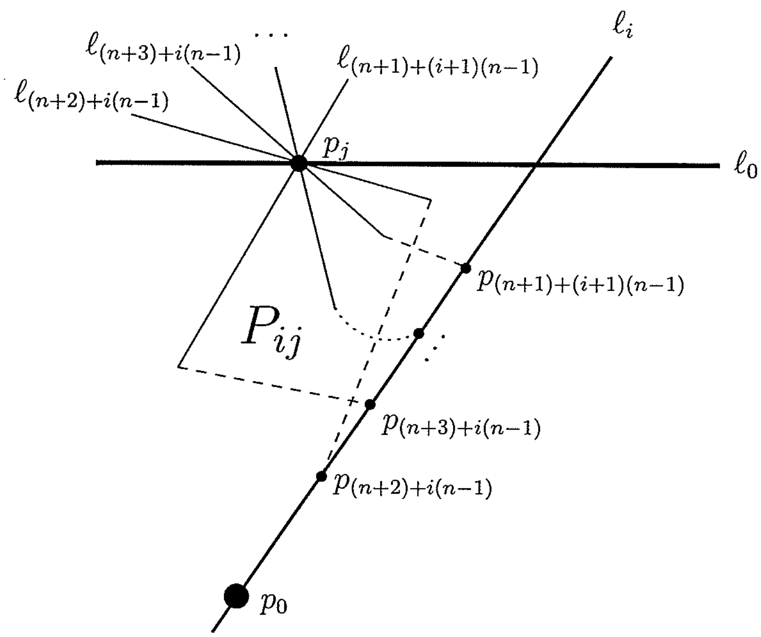
and columns indexed by

$$(n+2) + j(n-1), \ldots, (n+1) + (j+1)(n-1)$$

is either an $(n-1) \times (n-1)$ permutation, or (if $i = j$) it is a matrix of all 0's. The points $p_{(n+2)+i(n-1)}, \ldots, p_{(n+1)+(i+1)(n-1)}$ are all on the line ℓ_i, the lines $\ell_{(n+2)+j(n-1)}, \ldots, \ell_{(n+1)+(j+1)(n-1)}$ all must meet ℓ_i in some point. If $i = j$, then these lines will all meet ℓ_i at the same point, p_i, and so the submatrix considered will be a matrix of all 0's. If $i \neq j$, then each of the lines $\ell_{(n+2)+j(n-1)}, \ldots, \ell_{(n+1)+(j+1)(n-1)}$ must meet ℓ_i in one of the points $p_{(n+2)+i(n-1)}, \ldots, p_{(n+1)+(i+1)(n-1)}$. Since it must be a distinct point for each line (the lines all meet at point p_j), then the submatrix is a $(n-1) \times (n-1)$ permutation. For $i \neq j$, see Figure 3.2.

We will refer to the anti-flag (p_0, ℓ_0) as the *anchor* of this form and the submatrix consisting of rows $n+2, \ldots, n^2+n$ and columns $n+2, \ldots, n^2+n$ will be referred to as the *cokernel*.

Figure 3.3: Permutations in anti-flag form



Theorem 16. *The cokernel, C, of a projective plane is a $GPW(n+1, n; n-1)$.*

Proof. View the above matrix in block form,

$$A = \begin{pmatrix} M & B \\ B^T & C \end{pmatrix},$$

where $M = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 1 \end{pmatrix}$,

$$B = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & & 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 & & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 1 & \cdots & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & & 1 & 1 & 1 & \cdots & 1 \end{pmatrix}$$

Figure 3.4: Incidence matrix in anti-flag form

$$
\left(\begin{array}{cccccc|ccccc}
0 & 1 & 1 & 1 & \cdots & 1 & 0\ 0\ \cdots\ 0 & 0\ 0\ \cdots\ 0 & 0\ 0\ \cdots\ 0 & & 0\ 0\ \cdots\ 0 \\
1 & 1 & 0 & 0 & \cdots & 0 & 1\ 1\ \cdots\ 1 & 0\ 0\ \cdots\ 0 & 0\ 0\ \cdots\ 0 & & 0\ 0\ \cdots\ 0 \\
1 & 0 & 1 & 0 & \cdots & 0 & 0\ 0\ \cdots\ 0 & 1\ 1\ \cdots\ 1 & 0\ 0\ \cdots\ 0 & & 0\ 0\ \cdots\ 0 \\
1 & 0 & 0 & 1 & \cdots & 0 & 0\ 0\ \cdots\ 0 & 0\ 0\ \cdots\ 0 & 1\ 1\ \cdots\ 1 & \cdots & 0\ 0\ \cdots\ 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\ \vdots\ \ddots\ \vdots & \vdots\ \vdots\ \ddots\ \vdots & \vdots\ \vdots\ \ddots\ \vdots & & \vdots\ \vdots\ \ddots\ \vdots \\
1 & 0 & 0 & 0 & \cdots & 1 & 0\ 0\ \cdots\ 0 & 0\ 0\ \cdots\ 0 & 0\ 0\ \cdots\ 0 & & 1\ 1\ \cdots\ 1 \\
\hline
0 & 1 & 0 & 0 & \cdots & 0 & & & & & \\
0 & 1 & 0 & 0 & \cdots & 0 & 0 & P_{12} & P_{13} & \cdots & P_{1n} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & & & & \\
0 & 1 & 0 & 0 & \cdots & 0 & & & & & \\
 & & & & & & & & & & \\
0 & 0 & 1 & 0 & \cdots & 0 & & & & & \\
0 & 0 & 1 & 0 & \cdots & 0 & P_{21} & 0 & P_{23} & \cdots & P_{2n} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & & & & \\
0 & 0 & 1 & 0 & \cdots & 0 & & & & & \\
 & & & & & & & & & & \\
0 & 0 & 0 & 1 & \cdots & 0 & & & & & \\
0 & 0 & 0 & 1 & \cdots & 0 & P_{31} & P_{32} & 0 & \cdots & P_{3n} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & & & & \\
0 & 0 & 0 & 1 & \cdots & 0 & & & & & \\
 & & & \vdots & & & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 & & & & & \\
0 & 0 & 0 & 0 & \cdots & 1 & P_{n1} & P_{n2} & P_{n3} & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & & & & \\
0 & 0 & 0 & 0 & \cdots & 1 & & & & &
\end{array}\right)
$$

and C is the cokernel.

Since A is the incidence matrix of a projective plane, $AA^T = nI + J$; hence

$$AA^T = \begin{pmatrix} M & B \\ B^T & C \end{pmatrix} \begin{pmatrix} M^T & B \\ B^T & C^T \end{pmatrix}$$

$$= \begin{pmatrix} MM^T + BB^T & MB + BC^T \\ B^TM^T + CB^T & B^TB + CC^T \end{pmatrix}$$

Equating the $(2,2)$ block entries, we obtain $B^TB + CC^T = nI_{n^2-1} + J_{n^2-1}$. Now noting that

$$B^TB = \begin{pmatrix}
\begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \cdots & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} \\
\begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} & \cdots & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} \\
\vdots & \vdots & \ddots & \vdots \\
\begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \cdots & \begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix}
\end{pmatrix}$$

in block form $BB^T = \begin{pmatrix} J_{n-1} & 0 & \cdots & 0 \\ 0 & J_{n-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_{n-1} \end{pmatrix}$.

we see that

$$CC^T = \begin{pmatrix}
n & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 & & 1 & 1 & \cdots & 1 \\
0 & n & \cdots & 0 & 1 & 1 & \cdots & 1 & \cdots & 1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & n & 1 & 1 & \cdots & 1 & & 1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 & n & 0 & \cdots & 0 & & 1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 & 0 & n & \cdots & 0 & \cdots & 1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1 & 0 & 0 & \cdots & n & & 1 & 1 & \cdots & 1 \\
 & \vdots & & & & \vdots & & & \ddots & & \vdots & & \\
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & & n & 0 & \cdots & 0 \\
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & \cdots & 0 & n & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & & 0 & 0 & \cdots & n
\end{pmatrix}.$$

$$\text{in block form } CC^T = \begin{pmatrix}
n\mathrm{I}_{n-1} & \mathrm{J}_{n-1} & \cdots & \mathrm{J}_{n-1} \\
\mathrm{J}_{n-1} & n\mathrm{I}_{n-1} & \cdots & \mathrm{J}_{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
\mathrm{J}_{n-1} & \mathrm{J}_{n-1} & \cdots & n\mathrm{I}_{n-1}
\end{pmatrix}.$$

For a permutation P, $P^{-1} = P^T = P^*$, and also $0^T = 0^*$. Hence if $C = [P_{ij}]$, we get $C^T = [P_{ij}^T]^T = [P_{ji}^T] = [P_{ji}^*] = C^*$. Hence $CC^* = nI \bmod J$, or C is a $GPW(n+1, n; n-1)$. $\square$

Example 37. The following is the incidence matrix of the Fano plane in antiflag form:

$$\left(\begin{array}{cccc|ccc}
0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 \\
\hline
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0
\end{array}\right).$$

Its cokernel is

$$\left(\begin{array}{c|c|c}
0 & 1 & 1 \\
\hline
1 & 0 & 1 \\
\hline
1 & 1 & 0
\end{array}\right).$$

Example 38. The following is the incidence matrix of a projective plane of order 3 in antiflag form.

$$\left(\begin{array}{ccccc|cccccccc}
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
\hline
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0
\end{array}\right).$$

Its cokernel is

$$\left(\begin{array}{cc|cc|cc|cc}
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
\hline
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
\hline
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0
\end{array}\right).$$

This is a $GW(4,3,Z_2)$ where Z_2 is $\{e,a\}$, the cyclic group of order 2

$$\begin{pmatrix}
0 & e & e & e \\
e & 0 & e & a \\
e & a & 0 & e \\
e & e & a & 0
\end{pmatrix}.$$

Using the natural isomorphism form Z_2 into $\{1,-1\}$ we get the following $W(4,3)$:

$$\begin{pmatrix}
0 & 1 & 1 & 1 \\
1 & 0 & 1 & -1 \\
1 & -1 & 0 & 1 \\
1 & 1 & -1 & 0
\end{pmatrix}.$$

Example 39. The following is the projective plane of order 4 in antiflag form.

$$
\left(\begin{array}{cccccc|ccccccccccccccc}
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
\hline
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0
\end{array}\right).
$$

Its cokernel is:

$$
\left(\begin{array}{ccc|ccc|ccc|ccc|ccc}
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
\hline
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0
\end{array}\right)
$$

which is simply the following $GW(5,4,C_3)$ where C_3 is $\{e,\gamma,\gamma^2\}$, the cyclic group of order 3:

$$\begin{pmatrix} 0 & e & e & e & e \\ e & 0 & e & \gamma & \gamma^2 \\ e & e & 0 & \gamma^2 & \gamma \\ e & \gamma & \gamma^2 & 0 & e \\ e & \gamma^2 & \gamma & e & 0 \end{pmatrix}.$$

Theorem 17. *If Π is a plane with cokernel $GPW(n+1,n,n-1)$ and $s \in S_{n-1}$ is a permutation which commutes with every element in the $GPW(n+1,n,n-1)$, then there is a (p,ℓ)-collineation which can be associated with s, where (p,ℓ) is the anchor.*

Proof. We define the map α as follows: points $p_0,\ldots,p_{n+1}$ will all map to themselves, i.e. $\alpha(p_0)=p_0$, etc.. Points $p_{(n+2)+(i-1)(n-1)},\ldots,p_{(n+1)+(i)(n-1)}$ will be mapped according to the permutation s. Hence $\alpha(p_{(n+1)+(i-1)(n-1)+j}) = p_{(n+1)+(i-1)(n-1)+s(j)}$.

This will induce a similar map on the lines: lines $\ell_0,\ldots,\ell_{n+1}$ will all map to themselves, and $\alpha(\ell_{(n+1)+(i-1)(n-1)+j}) = \ell_{(n+1)+(i-1)(n-1)+s(j)}$.

All incidences with points $p_0,\ldots,p_{n+1}$ are preserved, since a line in the set $\{\ell_{(n+2)+(i-1)(n-1)},\ldots,\ell_{(n+1)+(i)(n-1)}\}$ maps to another line in that set, incidences with lines $\ell_0,\ldots,\ell_n$ are similarly preserved. Now consider the incidence of points $p_{(n+2)+(k-1)(n-1)},\ldots,p_{(n+1)+(k)(n-1)}$ and lines $\ell_{(n+2)+(m-1)(n-1)},\ldots,\ell_{(n+1)+(m)(n-1)}$. The incidence is given by the (k,m) element of $GPW(n+1,n,n-1)$, say g.

Reordering the points according to the permutation s corresponds to multiplication on the left by s, and reordering the lines according to the permutation s corresponds to multiplication on the right by s^{-1}. Since s commutes with g, we get that $sgs^{-1} = g$. So if $p_{(n+1)+(k-1)(n-1)+j} \in \ell_{(n+1)+(m-1)(n-1)+j}$ then $\alpha(p_{(n+1)+(k-1)(n-1)+j}) \in \alpha(\ell_{(n+1)+(m-1)(n-1)+j})$.

This gives a central collineation with center p and axis ℓ. □

Theorem 18. *If the cokernel of a projective plane $PP(n)$, with anchor (p, ℓ), forms a generalised weighing matrix $GW(n+1, n, G)$, where $|G| = n-1$, then this $PP(n)$ is (p, ℓ)-transitive.*

Proof. Let Π be a projective plane of order n whose kernel is a $GW(n+1, n, G)$; $|G| = n-1$, when anchored at (p, ℓ). Let $s \in S$, where S is the group associated with G described in Lemma 10. From Lemma 17, there is a collineation associated with s. Since $|G| = n-1$, G is a transitive subgroup of S_{n-1}, hence S is a transitive group, and we can get such a collineation for each element of S, Π is (p, ℓ)-transitive. □

Corollary 19. *If a projective plane $PP(n)$ has an antiflag form whose cokernel is a generalised weighing matrix of index 1, then it cannot be of Lenz-Barlotti class* I.1, II.1, III.1, IVa.1, IVb.1, V *or* VII.1.

Converse to Theorem 18:

Theorem 20. *If a projective plane $PP(n)$ is (p, ℓ)-transitive for anti-flag (p, ℓ), then it has a cokernel that is a $GW(n+1, n, G)$ where $|G| = n-1$.*

Proof. Suppose $PP(n)$ is (p,ℓ)-transitive. Arrange the incidence matrix with anchor (p,ℓ) having cokernel C, a $GPW(n+1,n,n-1)$ in normalised form. We further assume that the $(2,3)$-entry is also an identity matrix. (If it were not, we could multiply each column by the inverse of that entry, then multiply the first row by the element to get a normalised form with an identity matrix in the $(2,3)$-entry.)

Let α be a collineation in the group of (p,ℓ)-collineations. We can associate with this collineation a permutation $s \in S_{n-1}$, which takes points $p_{(n+2)},\ldots,p_{2n}$ to points $\alpha(p_{(n+2)}),\ldots,\alpha(p_{2n})$. Since the cokernel is normalised, s must also be the action of α on lines $\ell_{(n+2)+(i-1)(n-1)},\ldots,\ell_{(n+1)+(i)(n-1)}$, for $i=2,\ldots,n+1$. Since there is an identity matrix in the $(2,3)$-entry, s is also the action on the points $p_{(n+2)+(n-1)},\ldots,p_{(n+1)+(2)(n-1)}$. This implies s is the action on the lines $\ell_{(n+2)},\ldots,\ell_{2n}$, hence s is the same action on the points $p_{(n+2)+(i-1)(n-1)},\ldots,p_{(n+1)+(i)(n-1)}$ for $i=2,\ldots,n+1$. Let S be the set of all such permutations.

Since incidence is preserved, for every non zero entry g of C, $sgs^{-1}=g$. So g is in the centralizer of the group generated by the permutations in S. So by Lemma 11, the elements of $GPW(n+1,n,n-1)$ are from a group of order $n-1$. So the $GPW(n+1,n,n-1)$ is a $GW(n+1,n,G)$ where G is isomorphic to the group of (p,ℓ)-collineations. $\square$

Example 40. The matrix in Example 38 show that there exists exactly one nontrivial (p, ℓ)-collineation of the plane. The matrix in Example 39 shows that there exist two nontrivial (p, ℓ)-collineation of the plane of order 4.

In Example 37, we note that any collineation in this plane that fixes a line and a point not on the line will be the identity.

3.3 Relating flag form and anti-flag form

Given a projective plane Π of order n, let K be the normalised kernel of a flag form of the incidence matrix of Π. Let C be the normalised cokernel of an anti-flag ordering of Π. The core of K is an $(n-1) \times (n-1)$ array of $n \times n$ matrices, and the core of C is an $n \times n$ array of $(n-1) \times (n-1)$ matrices. By choosing the appropriate anchors for C and K, we can draw a nice correspondence between their cores. If the incidence matrix of Π is in flag form, the point line pair (p_1, ℓ_1) is an anti-flag, and we shall use that pair as our anchor for anti-flag form.

First, assume that the incidence matrix A of the plane Π is in flag form with a normalised kernel. (We have points labelled $p_0, \ldots, p_{n^2+n}$ and lines labelled $\ell_0, \ldots, \ell_{n^2+n}$.) Let $\widehat{A}$ be the incidence matrix of Π in antiflag form with anchor (p_1, ℓ_1). We will describe a new ordering of points indicated as $\widehat{p}_0, \ldots, \widehat{p}_{n^2+n}$; lines as $\widehat{\ell}_0, \ldots, \widehat{\ell}_{n^2+n}$.

So $(\widehat{p}_0, \widehat{\ell}_0)$ is (p_1, ℓ_1). Now $\widehat{p}_1, \widehat{p}_2, \ldots, \widehat{p}_{n+1}$ are the points on ℓ_1; hence so also are $p_0, p_{n+1}, p_{n+2}, \ldots, p_{2n}$ (such lists are given to mean in respective order, in other words, $\widehat{p}_1 = p_0$, $\widehat{p}_2 = p_{n+1}, \dots$ etc.). Similarly, the lines $\widehat{\ell}_1, \widehat{\ell}_2, \dots, \widehat{\ell}_{n+1}$ are the lines $\ell_0, \ell_{n+1}, \ell_{n+2}, \dots, \ell_{2n}$. This ordering agrees with the antiflag form: the $(\widehat{1}, \widehat{1})$ entry is a 1 (since A was in flag form) and the $\widehat{\ell}_2, \dots, \widehat{\ell}_{n+1}$ by $\widehat{p}_2, \dots, \widehat{p}_{n+1}$ submatrix is the identity matrix from the (1,1) block entry of the normalised kernel of A.

Now $\widehat{p}_{n+2}, \widehat{p}_{n+3}, \dots, \widehat{p}_{2n}$ will be the points on the line ℓ_0 $(\widehat{\ell}_1)$ other than p_0 and p_1 ($\widehat{p}_1$ and $\widehat{p}_0$), that is, $p_2, p_3, \dots, p_n$. Similarly, $\widehat{\ell}_{n+2}, \widehat{\ell}_{n+3}, \dots, \widehat{\ell}_{2n}$ will be the lines $\ell_2, \ell_3, \dots, \ell_n$.

For $i = 1, \dots, n$, $\widehat{p}_{(n+2)+i(n-1)}, \widehat{p}_{(n+2)+i(n-1)+1}, \dots, \widehat{p}_{(n+1)+(i+1)(n-1)}$ will be the points on the line $\widehat{\ell}_{i+1}$ (the line ℓ_{n+i} of A). Since this line was in the first row of blocks of the normalised kernel (consisting of identities), these will be the points

$$p_{2n+i}, p_{3n+i}, \dots, p_{n^2+i}\,.$$

Similarly the lines $\widehat{\ell}_{(n+2)+i(n-1)}, \widehat{\ell}_{(n+2)+i(n-1)+1} \dots, \widehat{\ell}_{(n+1)+(i+1)(n-1)}$ are

$$\ell_{2n+i}, \ell_{3n+i}, \dots, \ell_{n^2+i}\,.$$

Note that the cokernel of $\widehat{A}$ is already normalised. Consider the first row of blocks of the cokernel, representing the lines $\widehat{\ell}_{n+2}, \dots .\widehat{\ell}_{2n}$ which are $\ell_2, \dots, \ell_n$. Since the point p_{2n+i} is on the line ℓ_2, p_{3n+i} is on ℓ_3, etc. the submatrices $\widehat{\ell}_{n+2}, \widehat{\ell}_{n+3}, \dots, \widehat{\ell}_{2n}$ by $\widehat{p}_{(n+2)+i(n-1)}, \dots, \widehat{p}_{(n+1)+(i+1)(n-1)}$ (for $i = 1, 2, \dots, n$) are identity matrices. Hence the first row of blocks of the cokernel is in normalised form. Similarly, the first column of blocks of the cokernel is also in normalised form.

Now compare the core of the kernel of A with the core of the cokernel of $\widehat{A}$. Consider the (i, j) entry of the (h, k) block of the core of the cokernel of $\widehat{A}$. This is the position representing whether or not the point $\widehat{p}_{(n+1)+k(n-1)+j}$ is on the line $\widehat{\ell}_{(n+1)+h(n-1)+i}$, which is whether or not the point $p_{(j-1)n+k}$ is on the line $\ell_{(i-1)n+h}$, which is represented by the (h, k) position of the (i, j) block of the core of the kernel of A.

This process can also be done in reverse, starting with an anti-flag form and reordering to a flag form (picking the flag $(\widehat{p}_1, \widehat{\ell}_1)$ as the anchor). I.e. Reverseing the process in $\widehat{A}$ will result in A. In this manner, every kernel has an associated cokernel.

Rearrangements of block matrices in this manner, having the (i, j) entry of the (h, k) block as the (h, k) entry of the (i, j) block, have been studied by Craigen in [28]. He found the following: If the core of a matrix $GH = GH(n, G)$, where G is a group of permutation matrices of order n, then the result is the core of a $GPW(n+1, n, n-1) = GPW$, which is developed over G. Moreover, GPW is a $GW(n+1, n, H)$ with $|H| = n-1$ iff GH is group developed over H.

Theorem 21. *There is a plane* Π *of Lenz-Barlotti class* II.2 *only if there is a* $GH(n, G)$ *(*$|G| = n$*) whose core is group developed.*

Proof. Let Π be a plane of Lenz-Barlotti class II.2 and let A be the flag form of the incidence matrix of Π where the anchor is the flag (p_0, ℓ_0) such that Π is (p_0, ℓ_0)-

transitive. Let (p_1, ℓ_1) be the antiflag pair such that Π is (p_1, ℓ_1)-transitive.

By Lemma 15, there is a group G of order n such that the kernel of A is a $GH(n, G)$. By Theorem 20, there is a group H of order $n-1$ such that the associated cokernel is a $GW(n+1, n-1, H)$. From [28] the associated $GPW(n+1, n, n-1)$ of a $GH(n, G)$ is a $GW(n+1, n, H)$ iff the core of the $GH(n, G)$ is group developed (developed over H). □

Example 41. There are 4 planes of order 9 [69]. They are the Desarguesian plane (of Lenz-Barlotti class VII.2), the left and right nearfield planes (class IVb.3 and IVa.3), and the Hughes plane (class I.1). The nearfield planes of order 9 are also known as the Hall planes [19].

The following matrix corresponds with the kernel of the Desarguesian projective plane of order 9 in flag form. It is a $GH(9, G)$ where $G = \{x, y | x^3 = 1, y^3 = 1, xy = yx\}$.

$$\begin{pmatrix}
e & e & e & e & e & e & e & e & e \\
e & x & y & xy^2 & x^2y^2 & x^2 & y^2 & x^2y & xy \\
e & xy & x & y & xy^2 & x^2y^2 & x^2 & y^2 & x^2y \\
e & x^2y & xy & x & y & xy^2 & x^2y^2 & x^2 & y^2 \\
e & y^2 & x^2y & xy & x & y & xy^2 & x^2y^2 & x^2 \\
e & x^2 & y^2 & x^2y & xy & x & y & xy^2 & x^2y^2 \\
e & x^2y^2 & x^2 & y^2 & x^2y & xy & x & y & xy^2 \\
e & xy^2 & x^2y^2 & x^2 & y^2 & x^2y & xy & x & y \\
e & y & xy^2 & x^2y^2 & x^2 & y^2 & x^2y & xy & x
\end{pmatrix}$$

We see that the core of this kernel is group developed (displaying the division table representation of the cyclic group of order 8 with generator ω). The associated cokernel is as follows:

$$\begin{pmatrix}
0 & e & e & e & e & e & e & e & e & e \\
e & 0 & e & \omega^4 & \omega & \omega^7 & \omega^6 & \omega^5 & \omega^2 & \omega^3 \\
e & \omega^4 & 0 & e & \omega^6 & \omega & \omega^7 & \omega^3 & \omega^5 & \omega^2 \\
e & e & \omega^4 & 0 & \omega^7 & \omega^6 & \omega & \omega^2 & \omega^3 & \omega^5 \\
e & \omega^5 & \omega^2 & \omega^3 & 0 & e & \omega^4 & \omega & \omega^7 & \omega^6 \\
e & \omega^3 & \omega^5 & \omega^2 & \omega^4 & 0 & e & \omega^6 & \omega & \omega^7 \\
e & \omega^2 & \omega^3 & \omega^5 & e & \omega^4 & 0 & \omega^7 & \omega^6 & \omega \\
e & \omega & \omega^7 & \omega^6 & \omega^5 & \omega^2 & \omega^3 & 0 & e & \omega^4 \\
e & \omega^6 & \omega & \omega^7 & \omega^3 & \omega^5 & \omega^2 & \omega^4 & 0 & e \\
e & \omega^7 & \omega^6 & \omega & \omega^2 & \omega^3 & \omega^5 & e & \omega^4 & 0
\end{pmatrix}.$$

Example 42. The following matrix is the kernel of a flag form of the (right) nearfield plane of order 9 (Since the incidence matrix of the left nearfield plane is the transpose that of the right nearfield plane, it is omitted). It is another $GH(9, G)$, where G is the same group defined in Example 41.

$$\begin{pmatrix}
e & e & e & e & e & e & e & e & e \\
e & x^2 & x & y^2 & x^2y^2 & xy^2 & y & x^2y & xy \\
e & x & x^2 & y & xy & x^2y & y^2 & xy^2 & x^2y^2 \\
e & y & y^2 & x^2 & xy^2 & xy & x & x^2y^2 & x^2y \\
e & xy & x^2y^2 & x^2y & x^2 & y^2 & xy^2 & y & x \\
e & x^2y & xy^2 & x^2y^2 & y & x^2 & xy & x & y^2 \\
e & y^2 & y & x & x^2y & x^2y^2 & x^2 & xy & xy^2 \\
e & xy^2 & x^2y & xy & y^2 & x & x^2y^2 & x^2 & y \\
e & x^2y^2 & xy & xy^2 & x & y & x^2y & y^2 & x^2
\end{pmatrix}$$

Note that its core is group developed, over the quaternion group, H, of eight elements.

The associated cokernel is

$$\begin{pmatrix}
0 & e & e & e & e & e & e & e & e & e \\
e & 0 & e & B^2 & B^3 & C & CB^3 & B & CB & CB^2 \\
e & B^2 & 0 & e & CB^3 & B^3 & C & CB^2 & B & CB \\
e & e & B^2 & 0 & C & CB^3 & B^3 & CB & CB^2 & B \\
e & B & CB & CB^2 & 0 & e & B^2 & B^3 & C & CB^3 \\
e & CB^2 & B & CB & B^2 & 0 & e & CB^3 & B^3 & C \\
e & CB & CB^2 & B & e & B^2 & 0 & C & CB^3 & B^3 \\
e & B^3 & C & CB^3 & B & CB & CB^2 & 0 & e & B^2 \\
e & CB^3 & B^3 & C & CB^2 & B & CB & B^2 & 0 & e \\
e & C & CB^3 & B^3 & CB & CB^2 & B & e & B^2 & 0
\end{pmatrix}$$

where $H = \{B, C | B^4 = 1\ C^4 = 1\ C^2 = B^2\ BC = CB^3\}$.

Example 43. The following is a $GPH(9,9)$ which is a kernel of the Hughes plane of order 9.

$$\begin{pmatrix}
e & e & e & e & e & e & e & e & e \\
e & x^3 & xy^4 & x^7y^4 & x^4y^4 & y^2x^8 & y^2x^2 & y^2x^5 & x^6 \\
e & x^8y^2 & x^4y^2 & y^4x^5 & x^2y^2x & xy^3x & y^2x^2y & yx^8y^2 & y^4x \\
e & x^2y^2 & x^2y^2x & x & y^4x^8 & y^4x^7y & y & x^2y^3 & y^4x^7y \\
e & x^5y^2 & y^4x^2 & x^2y^2x & x^7 & y^5x & x^7y^5 & x^4y^5xy^4 & y^4x^4 \\
e & yx^2y & x^7y^2 & x^2y^4x^4 & x^2 & y^5 & yx^2 & y^4x^8y^3 & y^4x^8y^4 \\
e & x^2y^4x^5 & x^2y^4x^4 & x^8 & xy^2 & xy^3 & x^8y & x^5y^3x^2 & y^4x^5y^4 \\
e & x^2y^4x^8 & x^5 & x^4y^2 & x^2y^4x^4 & y^3x^7 & x^4y^5xy^4 & y^3x^2y^4 & y^4x^2y^4 \\
e & x^6 & y^2x^8 & y^2x^2 & y^2x^5 & xy^4 & x^7y^4 & x^7y^4 & x^3
\end{pmatrix}$$

Where x is the permutation $(1, 5, 7, 3, 4, 9, 2, 6, 8)$ and y is $(1, 4)(2, 5)(3, 6)(7, 8, 9)$. It is interesting to note that this differs from the presentation of the Hughes plane found in [47], since the permutations x and y generate a subgroup of order 162, whereas the permutations found in [47] generate all of S_9. The group generated by x and y has a three element center (generated by $(1, 3, 2)(4, 6, 5)(7, 9, 8)$, found using Groups and Graphs [68]). This indicates that there are two non-trivial (p, ℓ)-collineations where (p, ℓ) is the anchor associated with this kernel.

The following $GPW(10, 9, 8)$ matrix is the cokernel of the antiflag from of the Hughes plane associated with the above kernel.

$$\begin{pmatrix}
0 & e & e & e & e & e & e & e & e & e \\
e & 0 & A & B & C & D & E & F & G & H \\
e & B & 0 & A & E & C & D & H & F & G \\
e & A & B & 0 & D & E & C & G & H & F \\
e & S & T & U & 0 & V & W & X & Y & Z \\
e & U & S & T & W & 0 & V & Z & X & Y \\
e & T & U & S & V & W & 0 & Y & Z & X \\
e & \mathfrak{A} & \mathfrak{B} & \mathfrak{C} & \mathfrak{D} & \mathfrak{E} & \mathfrak{F} & 0 & \mathfrak{G} & \mathfrak{H} \\
e & \mathfrak{C} & \mathfrak{A} & \mathfrak{B} & \mathfrak{F} & \mathfrak{D} & \mathfrak{E} & \mathfrak{H} & 0 & \mathfrak{G} \\
e & \mathfrak{B} & \mathfrak{C} & \mathfrak{A} & \mathfrak{E} & \mathfrak{F} & \mathfrak{D} & \mathfrak{G} & \mathfrak{H} & 0
\end{pmatrix}$$

The permutations as follows:

$A = (1, 8)(2, 4, 3)(5, 6)$ $\quad S = (1, 7, 2, 3, 6, 8, 4)$ $\quad \mathfrak{A} = (1, 3, 7, 5, 2, 8, 6)$

$B = (2, 7, 4, 6)(3, 5)$ $\quad T = (1, 6, 7, 8, 3)(2, 5, 4)$ $\quad \mathfrak{B} = (1, 4, 5)(3, 8, 7)$

$C = (1, 4, 8, 7, 3, 6)$ $\quad U = (1, 5, 8, 2)(3, 4, 7, 6)$ $\quad \mathfrak{C} = (1, 2, 6, 4, 8, 5, 7)$

$D = (1, 2, 8, 5)(4, 7, 6)$ $\quad V = (1, 8)(2, 6)(3, 7, 4, 5)$ $\quad \mathfrak{D} = (1, 5, 4, 6, 8, 2, 3)$

$E = (1, 3, 8, 6, 7)(2, 5)$ $\quad W = (2, 4, 3)(5, 7)$ $\quad \mathfrak{E} = (1, 7, 8, 4, 2)(3, 5, 6)$

$F = (1, 6, 8, 3, 7, 5, 4, 2)$ $\quad X = (1, 2, 7, 3, 8, 5, 6)$ $\quad \mathfrak{F} = (1, 6, 5, 8, 3, 4)(2, 7)$

$G = (1, 5, 7, 8, 2, 6, 3, 4)$ $\quad Y = (1, 3, 5)(4, 8, 6)$ $\quad \mathfrak{G} = (1, 8)(2, 5, 3, 6)(4, 7)$

$H = (1, 7, 2, 3)(4, 5, 8)$ $\quad Z = (1, 4, 6, 5, 2, 8, 7)$ $\quad \mathfrak{H} = (2, 4, 3)(6, 7)$

3.4 Baer subplane form of the incidence matrix

There is a third interesting form of the incidence matrix of a projective plane that has a Baer subplane. Let Π be a projective plane of square order (Π is a $PP(n^2)$) which has a Baer subplane Π' (Π' is a $PP(n)$).

We can organize the incidence matrix of Π as follows. We let the first n^2+n+1 points and lines be those of Π'. Now each point p_i, $i \in \{1 \ldots n^2+n+1\}$, is already incident with $n+1$ lines, and will be incident with n^2-n other lines. Hence let $\ell_{n^2+n+1+(i-1)(n^2-n)}, \ell_{n^2+n+1+(i-1)(n^2-n)+1}, \ldots, \ell_{n^2+n+1+i(n^2-n)}$ be the n^2-n lines on p_i. Similarly, let $p_{n^2+n+1+(i-1)(n^2-n)}, p_{n^2+n+1+(i-1)(n^2-n)+1}, \ldots, p_{n^2+n+1+i(n^2-n)}$ be the n^2-n points on ℓ_i.

The submatrix with rows

$$r_{n^2+n+2+(i-1)(n^2-n)}, \ldots, r_{n^2+n+1+i(n^2-n)}$$

and columns

$$c_{n^2+n+2+(j-1)(n^2-n)}, \ldots, c_{n^2+n+1+j(n^2-n)}$$

corresponds to the points (outside of Π') on ℓ_i and the lines (outside of Π') on p_j. If p_j is on ℓ_i, then this submatrix is a matrix of all 0's, otherwise, since each line on p_j must meet ℓ_i in some point, it is an $(n^2-n) \times (n^2-n)$ permutation matrix. Hence we can view the submatrix of $r_{n^2+n+2} \ldots r_{n^4+n^2+1}$ and $c_{n^2+n+2} \ldots c_{n^4+n^2+1}$ as a $GPW(n^2+n+1, n^2, n^2-n)$. We refer to this as the *Baer-kernel.*

To see this, we can view the incidence matrix of Π in block form.

$$A = \begin{pmatrix} M & B \\ B^T & K \end{pmatrix}$$

where M is the incidence matrix of the subplane Π',

$$B = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 & & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 1 & \cdots & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & & 1 & 1 & 1 & \cdots & 1 \end{pmatrix}$$

and K is the Baer-kernel.

Since A is the incidence matrix of a projective plane, we know that $AA^T = nI + J$; hence

$$AA^T = \begin{pmatrix} M & B \\ B^T & K \end{pmatrix} \begin{pmatrix} M^T & B \\ B^T & K^T \end{pmatrix}$$

$$= \begin{pmatrix} MM^T + BB^T & MB + BK^T \\ B^T M^T + KB^T & B^T B + KK^T \end{pmatrix} = nI + J$$

Equating the $(2,2)$ blocks, we have $B^T B + KK^T = nI_{n^4-n} + J_{n^4-n}$. Now noting that

$$B^TB = \begin{pmatrix}
\begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \cdots & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} \\
\begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} & \cdots & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} \\
\vdots & \vdots & \ddots & \vdots \\
\begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \begin{matrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{matrix} & \cdots & \begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix}
\end{pmatrix}$$

we see that

$$KK^T = \begin{pmatrix}
\begin{matrix} n & 0 & \cdots & 0 \\ 0 & n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & n \end{matrix} & \begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} & \cdots & \begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} \\
\begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} & \begin{matrix} n & 0 & \cdots & 0 \\ 0 & n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & n \end{matrix} & \cdots & \begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} \\
\vdots & \vdots & \ddots & \vdots \\
\begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} & \begin{matrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{matrix} & \cdots & \begin{matrix} n & 0 & \cdots & 0 \\ 0 & n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & n \end{matrix}
\end{pmatrix}$$

.

So KK^T is a $GPW(n^2+n+1, n^2, n^2-n)$.

Moreover, the (0,1)-complement of this matrix is the incidence matrix of a projective plane of order n (In fact, it is the transpose of M). If there is 1 in the (i,j)-entry of M, then p_i is on ℓ_j. Considering the (j,i)-block entry of K, since p_i is on ℓ_j, this must be a block of 0's.

Example 44. The following is the incidence matrix of $PP(4)$. It has a subplane of order 2, so when it is organized as described above we get a $GPW(2^2+2+1, 2^2, 2^2-2) = GPW(7,4,2)$.

$$\left(\begin{array}{ccccccc|cccccccccccccc}
1&1&0&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&1&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\
0&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\
1&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
\hline
1&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0&1&0&0&0\\
1&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0&1&0&0\\
0&1&0&0&0&0&0&0&0&0&0&1&0&0&1&1&0&0&0&1&0\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&1\\
0&0&1&0&0&0&0&1&0&0&0&0&0&1&0&1&0&0&1&0&0\\
0&0&1&0&0&0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&0\\
0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&1&0\\
0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&1\\
0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&0&0&1&0&1&0\\
0&0&0&0&1&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&1&0&1&0&1&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&1&0&1&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&0&1&1&0&0&1&1&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&1&0&1&1&0&0&1&0&0&1&0&0&0&0&0
\end{array}\right)$$

whose Baer-kernel is

$$\left(\begin{array}{cc|cc|cc|cc|cc|cc|cc}
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
\hline
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
\hline
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
\hline
1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
\hline
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0
\end{array}\right).$$

This corresponds with the following $GW(7,4,C_2)$.

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & - & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & - & 0 \\
0 & 1 & 0 & 0 & - & - & 1 \\
1 & 0 & - & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & - & 0 & 0 & - \\
1 & - & 1 & 0 & 1 & 0 & 0
\end{pmatrix}$$

Example 45. This example is found in [82], and is attributed to David Glynn.

Let G be the group found in Example 24, with generators

$$x = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0
\end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

Then the matrix $circ(0 \quad x^2y \quad 1 \quad y \quad 0 \quad 1 \quad 1 \quad xy \quad x^2y \quad xy \quad 0 \quad y \quad 0)$ is a $GW(13,9,G)$, which is the Baer-kernel of the Hughes plane of order 9.

Chapter 4

Related Constructions

4.1 Power Hadamard matrices

A technique developed by Robert Craigen and Roger Woodford gives rise to the possibility of finding generalised Hadamard matrices from Butson Hadamard matrices.

Lemma 22. *If $n_1, n_2, \ldots, n_k$ are pairwise relatively prime, and there exists $BH(h, n_1)$, $BH(h, n_2)$, …, $BH(h, n_k)$ then there exists a $PH(h, \Phi_{n_1}\Phi_{n_2}\cdots\Phi_{n_k})$*

The proof of the above lemma requires the solution to systems of modular equations, which are guaranteed if the moduli are relatively prime. It is possible to have solutions when the moduli are not relatively prime as well. However, in the case of $n_1 = 2$, $n_2 = 4$ and $h = 4n$ where n is odd, this will not be possible.

Theorem 23. *There is no $PH(4n, (1+x)(1+x^2))$ if n is odd.*

Proof. Suppose such a PH existed. Then, since $x = -1$ is a zero of $(1+x)(1+x^2)$, replacing x^a with $(-1)^a$ in our matrix gives a Hadamard matrix H. Similarly, replacing x^a with $(-i)^a$ gives a Butson Hadamard matrix over 4'th roots of unity, B. We can organize the columns of the PH in such a way that the first three rows of H would have the following form:

$$\left(\begin{array}{cccc|cccc|cccc|cccc}
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & -1 & -1 & \cdots & -1 & -1 & -1 & \cdots & -1 \\
1 & 1 & \cdots & 1 & -1 & -1 & \cdots & -1 & 1 & 1 & \cdots & 1 & -1 & -1 & \cdots & -1 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}\right)$$

If in some position PH has the entry x^a where $a \equiv 0 \pmod 4$ then H would have a 1 in that position and B would also have a 1 in that position. If PH had a x^b where $b \equiv 1 \pmod 4$, H would have a -1 and B would have a $-i$. If PH had a x^c where $c \equiv 2 \pmod 4$, H would have a 1 and B would have a -1.If PH had a x^d where $d \equiv 3 \pmod 4$, H would have a -1 and B would have a i. So we can see that each of the four types of columns of H, listed above, would give rise to four different types of columns of B, giving a total of 16, as listed below. Let a be the number of columns of type $\begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \end{pmatrix}$, let b be the number of columns of type $\begin{pmatrix} 1 \\ 1 \\ -1 \\ \vdots \end{pmatrix}$, etc..

$$\begin{array}{cccc|cccc|cccc|cccc}
a & b & c & d & e & f & g & h & s & t & u & v & w & x & y & z \\
\\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & i & i & -i & -i & i & i & -i & -i \\
1 & -1 & 1 & -1 & i & -i & i & -i & 1 & -1 & 1 & -1 & i & -i & i & -i \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}$$

Since H is a Hadamard matrix,

$a+b+c+d=e+f+g+h=s+t+u+v=w+x+y+z=n$

Let $R_i, i=i,2,3$ be the i'th row of B. Since B is a Butson Hadamard matrix $(R_1)((R_2)^*)^T=0$. From this we get

$a+b+e+f=c+d+g+h=s+t+w+x=u+v+y+z=n.$

From $(R_1)((R_3)^*)^T=0$,

$a+c+s+u=b+d+t+v=e+g+w+y=f+h+x+z=n,$

and from $(R_2)((R_3)^*)^T=0$,

$a+d+w+z=b+c+x+y=f+g+s+v=e+h+t+u=n.$

Now since $a+b+c+d=c+d+g+h$ we get $a+b=g+h$, similarly we get

$$\begin{array}{lll}
c+d=e+f & s+t=y+z & u+v=w+x \\
a+c=t+v & b+d=s+u & e+g=x+z \\
f+h=w+y & b+c=w+z & a+d=x+y \\
s+v=e+h & f+g=t+u &
\end{array}$$

and, from these, $b+c+2d+x+y+2z=w+z+x+y+2d+2z=n+2(d+z)$. Also, $t+v+f+h+g+h+u+v=f+g+t+u+2h+2v=t+u+t+u+2h+2v=2(t+u+h+v)$.

Now we get $(b+d+t+v)+(f+h+x+z)+(g+h+c+d)+(u+v+y+z)=4n$. Subtracting $t+v+f+h+g+h+u+v$ we get $b+d+x+z+c+d+y+z=b+c+2d+x+y+2z=4n-2(t+u+h+v)$.

Hence $n+2(d+z)=4n-2(t+u+h+v)$ but the left hand side is odd if n is odd, and the right hand side is always even. This is a contradiction. $\square$

Theorem 24. *There are no projective planes of order $n=4m$, m odd, that is (p,ℓ)-transitive ($p\in\ell$) where the group of (p,ℓ)-collineations is equivalent to the cyclic* *group.*

Proof. Suppose Π is a plane of order n which was (p, ℓ)-transitive $(p \in \ell)$, whose group of (p, ℓ)-collineations was the cyclic group. By Lemma 15, there is a $GH(n, G)$ where G is the cyclic group (say generated by g). By replacing the generator g with x, we would get a $PH(n, x^n - 1)$. Since $x^n - 1 = (1 + x)(1 + x^2)g(x)$, we would also have a $PH(n, (1 + x)(1 + x^2))$. Hence by Theorem 23, no planes of this type can exist. □

4.2 Latin squares

It is possible to use certain power Hadamard matrices to give sets of mutually orthogonal Latin squares. It is known that for n the matrix

$$circ(\; 1 \quad x \quad x^4 \quad x^9 \quad x^{16} \quad \ldots \quad x^{(n-1)^2} \;)$$

where the powers are taken $\mod n$ will give a $PH(n, \Phi_n)$ if n is odd and a $PH(n, \Phi_{2n})$ if n is even. In the case where n is odd, the inner product of certain pairs of rows give the full cyclotomic polynomial. In that case, those two rows will correspond to a Latin square, as follows.

Given a $PH(n, f(x)) = [a_{ij}]$, we define $R_i * R_j = [b_1, b_2, \cdots, b_n]$ where each element is in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ and $b_k = a_{ik} \cdot a_{jk}^{-1}$. If all elements of $R_i * R_j$ are distinct, then the following construction gives a Latin square. Let x be the right shift permutation matrix, so

$$x = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}, \text{ and let } d = \begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix}.$$

The k'th row of the Latin square L_{ij} is defined to be $[db_k]$.

Example 46. In the case where $n = 5$, we have the matrix

$$\begin{pmatrix} 1 & x & x^4 & x^4 & x \\ x & 1 & x & x^4 & x^4 \\ x^4 & x & 1 & x & x^4 \\ x^4 & x^4 & x & 1 & x \\ x & x^4 & x^4 & x & 1 \end{pmatrix}$$

So $R_1 * R_5 = \begin{pmatrix} x^{-1} & x^{-3} & 1 & x^3 & x \end{pmatrix}$

Reducing the powers $\bmod 5$, gives

$\begin{pmatrix} x^4 & x^2 & 1 & x^3 & x \end{pmatrix}$, hence

$$L_{1,5} = \begin{bmatrix} 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix}.$$

Lemma 25. *If m is odd and r is relatively prime to m then the set*

$$\{a^2 - (a+r)^2 \pmod m | a \in \{0, \dots, m-1\}\}$$

contains m distinct elements.

Proof. If two elements were congruent then (since r and 2 are invertible $\mod m$)

$$a^2 - (a+r)^2 \equiv b^2 - (b+r)^2$$

$$-r(2a+r) \equiv -r(2b+r)$$

$$2a+r \equiv 2b+r$$

$$2a \equiv 2b$$

$$a \equiv b$$

□

Corollary 26. *If m is odd, then using $PH(m, \Phi_m)$, there will be a Latin square associated with $R_i * R_j$ if $j-i$ is relatively prime to m.*

Knowing which inner products give us Latin squares, we can now look at which pairs would be orthogonal.

Theorem 27. *If m is odd, then using $PH(m, \Phi_m)$, the Latin squares associated with $R_i * R_k$ and $R_j * R_k$ will be orthogonal if $j-i$ is relatively prime to m.*

Proof. We show that the positions in L_{ik} which contain a 1 form a transversal in L_{jk} (i.e. in L_{jk}, each of those entries are distinct). Since all the rows are a shift of the row $\begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix}$, the positions corresponding to any entry in L_{ik} will form a transversal in L_{jk}. Hence L_{ik} and L_{jk} will be orthogonal.

In row z of L_{ik}, there will be a 1 in the a'th column if the z'th entry of $R_i * R_j$ is x^{a-1}. If the z'th entry of $R_j * R_k$ were x^b, then there would be a 1 in the $(b+1)$'st column of L_{jk}. Hence there would be an $(a-b) \mod m$ in the a'th column of the z'th row of L_{jk}.

Since the z'th entry of $R_i * R_j$ is x^{a-b-1}, the positions corresponding to 1's in L_{ik} will form a transversal in L_{jk} if the elements of $R_i * R_j$ are distinct. By Lemma 25, these will be distinct when $j-i$ is relatively prime to m. $\square$

Example 47. In order 5 (from Example 46), we get $R_1 * R_2 = \begin{pmatrix} x^4 & x & x^3 & 1 & x^2 \end{pmatrix}$. Comparing the 1's in $L_{1,5}$ (indicated by circles), we see the corresponding entry in row i, $i = 1, \ldots, 5$ of $L_{2,5}$ (indicated by squares) is one more than the power of the i'th entry of $R_1 * R_2$.

$$L_{1,5} = \begin{bmatrix} 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix} \qquad L_{2,5} = \begin{bmatrix} 1 & 2 & 3 & 4 & \boxed{5} \\ 5 & 1 & \boxed{2} & 3 & 4 \\ \boxed{4} & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & \boxed{1} & 2 \\ 2 & \boxed{3} & 4 & 5 & 1 \end{bmatrix}$$

Similarly $R_2 * R_1 = \begin{pmatrix} x & x^4 & x^2 & 1 & x^3 \end{pmatrix}$. For the 1's in $L_{2,5}$ (indicated by circles), the corresponding entry in row i, $i = 1, \ldots, 5$ of $L_{1,5}$ (indicated by squares) is one more than the power of the i'th entry of $R_2 * R_1$.

$$L_{1,5} = \begin{bmatrix} \boxed{2} & 3 & 4 & 5 & 1 \\ 4 & \boxed{5} & 1 & 2 & 3 \\ 1 & 2 & \boxed{3} & 4 & 5 \\ 3 & 4 & 5 & \boxed{1} & 2 \\ 5 & 1 & 2 & 3 & \boxed{4} \end{bmatrix} \qquad L_{2,5} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix}$$

In this manner, we are able to construct sets of mutually orthogonal Latin squares of size equal to one less than the smallest prime in the prime power decomposition of m. The McNeish bound is a constructive lower bound for sizes of sets of MOLS [47]. This will meet the McNeish bound for square free m's, but will give Latin squares all of whose rows are shifts of the same starting row.

Example 48. In order 15, we use the matrix

$$\mathrm{circ}(\ 1\ \ x\ \ x^4\ \ x^9\ \ x\ \ x^{10}\ \ x^6\ \ x^4\ \ x^4\ \ x^6\ \ x^{10}\ \ x\ \ x^9\ \ x^4\ \ x\ ).$$

In this case we find a pair of orthogonal Latin squares which correspond to $R_1 * R_{15}$ and $R_2 * R_{15}$:

$$\begin{bmatrix}
2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 \\
4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 \\
6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 \\
8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 \\
5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 \\
7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 \\
9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14
\end{bmatrix},$$

and

$$\begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 \\
9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 \\
6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 \\
10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\
3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 \\
7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 \\
11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\
4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 \\
8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
12 & 13 & 14 & 15 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11
\end{bmatrix}$$

Example 49. In order 35, a set of 4 mutually orthogonal Latin squares can be constructed from the following row vectors ($\mathfrak{R}_1, \ldots, \mathfrak{R}_4$), each entry represents a row of the Latin square:

$$\mathfrak{R}_1 = \begin{array}{llllllllllll}
(x^{34} & x^{32} & x^{30} & x^{28} & x^{26} & x^{24} & x^{22} & x^{20} & x^{18} & x^{16} & x^{14} & x^{12} \\
x^{10} & x^{8} & x^{6} & x^{4} & x^{2} & 1 & x^{33} & x^{31} & x^{29} & x^{27} & x^{25} & x^{23} \\
x^{21} & x^{19} & x^{17} & x^{15} & x^{13} & x^{11} & x^{9} & x^{7} & x^{5} & x^{3} & x\ ) &
\end{array}$$

$$\mathfrak{R}_2 = \begin{array}{llllllllllll}
(1 & x^{31} & x^{27} & x^{23} & x^{19} & x^{15} & x^{11} & x^{7} & x^{3} & x^{34} & x^{30} & x^{26} \\
x^{22} & x^{18} & x^{14} & x^{10} & x^{6} & x^{2} & x^{33} & x^{29} & x^{25} & x^{21} & x^{17} & x^{13} \\
x^{9} & x^{5} & x & x^{32} & x^{28} & x^{24} & x^{20} & x^{16} & x^{12} & x^{8} & x^{4}\ ) &
\end{array}$$

$$\mathfrak{R}_3 = \begin{array}{llllllllllll}
(x^{3} & x^{32} & x^{26} & x^{20} & x^{14} & x^{8} & x^{2} & x^{31} & x^{25} & x^{19} & x^{13} & x^{7} \\
x & x^{30} & x^{24} & x^{18} & x^{12} & x^{6} & 1 & x^{29} & x^{23} & x^{17} & x^{11} & x^{5} \\
x^{34} & x^{28} & x^{22} & x^{16} & x^{10} & x^{4} & x^{33} & x^{27} & x^{21} & x^{15} & x^{9}\ ) &
\end{array}$$

$$\mathfrak{R}_4 = \begin{pmatrix} x^8 & 1 & x^{27} & x^{19} & x^{11} & x^3 & x^{30} & x^{22} & x^{14} & x^6 & x^{33} & x^{25} \\ x^{17} & x^9 & x^1 & x^{28} & x^{20} & x^{12} & x^4 & x^{31} & x^{23} & x^{15} & x^7 & x^{34} \\ x^{26} & x^{18} & x^{10} & x^2 & x^{29} & x^{21} & x^{13} & x^5 & x^{32} & x^{24} & x^{16} \end{pmatrix}$$

4.3 Hadamard matrices from collineations

Hughes [59] shows that if a projective plane of order $n \equiv 2 \pmod 4$ has an even order collineation, then $n = 2$. We adapt his technique to get Hadamard matrices of order $\frac{q^2-1}{2}$ for certain prime powers q.

Let α be a central collineation of order 2 of a projective plane Π of order n. If n is odd then α must be a homology, and if n is even then α must be an elation. In both cases we can use α to define a weighing matrix.

If n is even, and α is a (p, ℓ)-collineation, let $q_1, q_2, \ldots, q_n$ be the n points on ℓ other than p. Let m_1, m_2, $\ldots$, m_n be the n lines on p other than ℓ. Let $x_{(i,1)}$, $x^\alpha_{(i,1)}$, $x_{(i,2)}$, $x^\alpha_{(i,2)}$, $\ldots$, $x_{(i,t)}$, $x^\alpha_{(i,t)}$ be the n points on line m_i other than p where $t = \frac{n}{2}$. Let $w_{(i,1)}$, $w^\alpha_{(i,1)}$, $w_{(i,2)}$, $w^\alpha_{(i,2)}$, $\ldots$, $w_{(i,t)}$, $w^\alpha_{(i,t)}$ be the n lines through point q_i other than ℓ.

In the case where n is odd, and α is a (p, ℓ)-collineation, we let $q_1, q_2, \ldots, q_n, q_{n+1}$ be the n+1 points on ℓ. Let $m_1, m_2, \ldots, m_n$, m_{n+1} be the n+1 lines on p. Let $x_{(i,1)}$, $x^\alpha_{(i,1)}$, $x_{(i,2)}$, $x^\alpha_{(i,2)}$, $\ldots$, $x_{(i,t)}$, $x^\alpha_{(i,t)}$ be the n-1 points on line m_i other than q_i and p where $t = \frac{n-1}{2}$. Let $w_{(i,1)}$, $w^\alpha_{(i,1)}$, $w_{(i,2)}$, $w^\alpha_{(i,2)}$, $\ldots$, $w_{(i,t)}$, $w^\alpha_{(i,t)}$ be the n-1 lines through point q_i other than m_i and ℓ.

We index rows and columns of a square matrix by pairs (i,j), in the even case $1 \le i \le n$ and $1 \le j \le \frac{n}{2} = t$, and in the odd case $1 \le i \le n+1$ and $1 \le j \le \frac{n-1}{2} = t$. We define W, a $\{0,1,-1\}$-matrix by

$$W = [a_{(i,j)(r,s)}] \text{ where } a_{(i,j)(r,s)} = \begin{cases} 1 & \text{if } x_{(i,j)} \in w_{(r,s)} \\ -1 & \text{if } x^{\alpha}_{(i,j)} \in w_{(r,s)} \\ 0 & \text{otherwise} \end{cases}$$

In the case where n is even, W is a $W(\frac{n^2}{2}, n)$, and in the case where n is odd, W is a $W(\frac{n^2-1}{2}, n)$, as we now demonstrate.

To see that W is a weighing matrix, we show that any two distinct rows are orthogonal. First, we consider rows indexed by (i,k), for a fixed i and $k = 1,\ldots,t$; we say these rows are in the same block. The rows of this block represent points on line m_i, so for any line other than m_i, no more than one of these points can be on it, hence the rows in any block are disjoint, in the sense that no two will have non-zero entries in the same column.

Now consider two rows from differing blocks, say rows (i,y) and (j,z) where $i \neq j$. The only columns in which both rows could have non-zero entries are those columns that correspond to lines $x_{(i,y)}x_{(j,z)}$, $x^{\alpha}_{(i,y)}x_{(j,z)}$, $x_{(i,y)}x^{\alpha}_{(j,z)}$ or $x^{\alpha}_{(i,y)}x^{\alpha}_{(j,z)}$. Since $(x_{(i,y)}x_{(j,z)})^{\alpha} = x^{\alpha}_{(i,y)}x^{\alpha}_{(j,z)}$ exactly one of these lines will be some $w_{(r,s)}$, representing some column. Similarly, since $(x^{\alpha}_{(i,y)}x_{(j,z)})^{\alpha} = x_{(i,y)}x^{\alpha}_{(j,z)}$, exactly on of these lines will be some representing some column. Suppose that $w_{(r,s)} = x_{(i,y)}x_{(j,z)}$ and $w_{(t,u)} = x^{\alpha}_{(i,y)}x_{(j,z)}$. Then the (i,y)'th row would have a 1 both column (r,s) and column

(t,u), and the (j,z)'th row will have a 1 in column (r,s) and a -1 in column (t,u). A similar situation will occur for all other choices of $w_{(t,u)}$ and $w_{(r,s)}$. Hence the inner product of these two rows will be zero.

To see that the weight of W is n, consider a point $x_{(i,j)}$. This point is not on ℓ, so each of the $n+1$ lines on it meet ℓ. Each line, except the line that passes through p, is either $w_{(r,s)}$ or $w^{\alpha}_{(r,s)}$. Each of those n lines is represented by some column, hence the row (i,j) will have a 1 or a -1, so every row will have n non-zero entries.

We now have a weighing matrix where the rows of a block are disjoint, so we can sum all the rows of a block and preserve orthogonality. Further, if there exists an $H(t)$, then we can multiply (on the left) by the matrix $\begin{pmatrix} H(t) & 0 & \cdots & 0 \\ 0 & H(t) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & H(t) \end{pmatrix}$. This has the effect of combining rows within a block.

Example 50. The matrix $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$ would have blocks of size 2, so using $H(2) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ we replace the first row with the sum of the first and second rows, and replace the second row with the difference of the first and second rows, similarly with the third and forth rows to get $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$.

(Due to Hughes [59]) In the case where n is even, for $n \geq 3$ adding the rows in a block would result in 3 rows of a Hadamard matrix. Hence $\frac{n^2}{2} \equiv 0 \pmod 4$, implying

$n \equiv 0 \pmod 4$.

In the odd case, if an $H(t)$ exists, then combining the rows would result in a $W(\frac{n^2-1}{2}, \frac{n^2-n}{2})$. In the Desarguesian case, we can do better, and find an $H(\frac{n^2-1}{2})$. To do this, we find a skew $W = W(\frac{n^2-1}{2}, n)$, then add ones to the diagonal. Hence when the rows are combined, the result will be a Hadamard matrix.

The following theorem uses the fact that the core of the kernel of a Desarguesion plane Π can be expressed as $circ(1, \beta, \beta^2, \ldots, \beta^{q-2})$ where β generates the multiplicative group of the associated field, and where entries are considered as elements of the additive group. To see this, we use the associated Latin squares as found in [59]. Suppose Π is constructed using the field F. Then for each non-zero element of F, β^a, the Latin square is the addition table of $x\beta^a + y$, hence each row permutes $x\beta^a$ into $x\beta^a + y$, hence are equivalent to additive elements of F. Also, since $(\beta^{i+1})(\beta^a) + y = (\beta^i)(\beta^{a+1}) + y$, we see that the core will be back circulant. To find a circulant core, we simple take to rows in reverse order.

Theorem 28. *If Π is a Desarguesian projective plane of odd order q, then there exists a skew $W(\frac{q^2-1}{2}, q)$, with a decomposition into $\frac{q-1}{2} \times \frac{q-1}{2}$ blocks such that the rows of each block are disjoint.*

Proof. Consider the antiflag form of Π, whichcomes from a rearrangement of the core of the kernel $circ(1, \beta, \beta^2, \ldots, \beta^{q-2})$ as described above.

From Section 3.3 the antiflag form of Π will have elements from the cyclic group of order $q-1$, generated by ω. Since $1+\beta^{\frac{q-1}{2}}=0$, the associated antiflag form will have a core with the property that when there is an ω^a in the (i,j) position there is an $\omega^{\frac{q-1}{2}+a}$ in the (j,i) position.

A homology α of order two would be derived in this case from the element $\omega^{\frac{q-1}{2}}$ by the following mapping: the element ω^a would be mapped to the element $\omega^{\frac{q-1}{2}+a}$. Let $\frac{q-1}{2}=m$ and consider a rearrangement of a division table as follows:

$\div$	$1 \quad \omega^m$	$\omega \quad \omega^{m+1}$	$\omega^2 \quad \omega^{m+2}$	$\cdots$	$\omega^{m-1} \quad \omega^{2m-1}$
1 ω^m					
ω^{2m-1} ω^{m-1}					
ω^{2m-2} ω^{m-2}					
$\vdots$ $\vdots$					
ω^{m+2} ω^2					
ω^{m+1} ω					

This arrangement gives a symmetric table, with elements paired with their image under α. As in Section 2.5, we can associate each element with a permutation matrix $\mathfrak{A}(\omega^a)=[a_{ij}]$, where

$$a_{ij}=\begin{cases} 1 & \text{if } C_G(i,j)=g \\ 0 & \text{otherwise.} \end{cases}$$

Replacing the elements in the antiflag form matrix with their associated permutations is still an antiflag form of Π, C, although no longer normalized. If for the previous construction we choose for $x_{(i,j)}$ or $w_{(i,j)}$ the first element of the pair, then this has the same effect as mapping the cokernel into a $\{0, 1, -1\}$-matrix via

$$a_{ij} = \begin{cases} 1 & \text{if the}(2i-1, 2i) \times (2j-1, 2j) \text{ submatrix of C is } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ -1 & \text{if the}(2i-1, 2i) \times (2j-1, 2j) \text{ submatrix of C is } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 0 & \text{otherwise.} \end{cases}$$

Hence when an element ω^a has a 1, (respectively -1) then $\omega^{\frac{q-1}{2}+a}$ will have a -1, (respectively 1). Since the first row and first column will not be skew under these conditions, however, multiplying the first m rows by -1 will result in a skew weighing matrix. $\square$

Theorem 29. *For q a prime power, if there exists a Hadamard matrix of order $\frac{q-1}{2}$, then there is a Hadamard matrix of order $\frac{q^2-1}{2}$.*

Example 51. Consider the case of the projective plane Π of order 5. The flag from of Π is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & e & \beta & \beta^2 & \beta^3 \\ 1 & \beta^3 & e & \beta & \beta^2 \\ 1 & \beta^2 & \beta^3 & e & \beta \\ 1 & \beta & \beta^2 & \beta^3 & e \end{pmatrix}$$

and its antiflag form is

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^3 & \omega^2 \\ 1 & \omega^2 & 0 & 1 & \omega & \omega^3 \\ 1 & \omega^3 & \omega^2 & 0 & 1 & \omega \\ 1 & \omega & \omega^3 & \omega^2 & 0 & 1 \\ 1 & 1 & \omega & \omega^3 & \omega^2 & 0 \end{pmatrix}$$

Considering the following rearranged division table for the group in the above matrix:

$\div$	1	ω^2	ω	ω^3
1	1	ω^2	ω	ω^3
ω^2	ω^2	1	ω^3	ω
ω^3	ω	ω^3	ω^2	1
ω	ω^3	ω	1	ω^2

We get the following symmetric weighing matrix

$$\begin{pmatrix}
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & -1 & 0 & -1 & 0 & -1 & 0 & -1 & 0 & -1 \\
-1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & -1 & -1 & 0 \\
0 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & -1 & 0 & 0 & 1 \\
-1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & -1 & 0 \\
-1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 1 & 0 \\
-1 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\
-1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 0 & 0 \\
0 & 1 & 0 & -1 & 1 & 0 & -1 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}.$$

We add 1's along the diagonal, to get

$$\begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & -1 & 0 & -1 & 0 & -1 & 0 & -1 & 0 & -1 \\
-1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 & -1 & 0 \\
0 & 1 & 0 & 1 & 0 & -1 & 1 & 0 & -1 & 0 & 0 & 1 \\
-1 & 0 & -1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & -1 & 1 & 0 & -1 & 0 \\
-1 & 0 & 0 & -1 & -1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & -1 & 0 & 0 & 1 & 0 & 1 & 0 & -1 & 1 & 0 \\
-1 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 & 0 & -1 \\
-1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 1 & 0 \\
0 & 1 & 0 & -1 & 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1
\end{pmatrix}.$$

Multiplying by $\begin{pmatrix} H(2) & 0 & 0 \\ 0 & H(2) & 0 \\ 0 & 0 & H(2) \end{pmatrix}$ where $H(2) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to get

$$\begin{pmatrix}
1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\
-1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\
-1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\
-1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\
-1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \\
-1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\
-1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\
-1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \\
-1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\
-1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1
\end{pmatrix},$$

which is an $H(12)$.

4.4 Impact of the flag and antiflag forms on the Lenz Barlotti classification

There are some known existence and non-existence results in generalised Hadamard matrices and generalised weighing matrices. We can use these results, along with results from Chapter 3 to get restriction of the possible planes for particular orders. We consider the question of existence for projective planes of orders less than 100, and give a table with the restrictions implied by these results, along with the result from Theorem 24.

In the table in Figure 4.1, we use the following abbreviations:

(BR) The Bruck-Ryser theorem states the non-existence of particular orders of projective planes. [59]

(deL) Paper by de Launey state the non-existence of certain generalised Hadamard matrices. [39]

(H) If $n > 2$, then a projective plane of order $n \equiv 2 \bmod 4$ has no collineations of even order, hence cannot be of Lenz class II.[59]

(Lam) An exhaustive search shows the non-existence of a plane of order 10. [70]

(gpw) Theorem 20, along with non-existence results in [39] imply the non-existence of planes of Lenz-Barlotti class I.1, II.1, III.1, IVa.1, IVb.1, V or VII.1.

(res) Theorem 24 gives restrictions on the possibility of planes of Lenz class II^+.

E($\mathfrak{L}$) means excludes Lenz class II (or greater).

R($\mathfrak{L}$) means restricted Lenz class II (or greater).

E($\mathfrak{B}$) means excludes Lenz-Barlotti classes I.1, II.1, III.1, IVa.1, IVb.1, V or VII.1.

Figure 4.1: Planes of order less than 100

order	comments
2	prime
3	prime
4	prime power
5	prime
6	does not exist (BR)
7	prime
8	prime power
9	prime power
10	does not exist (Lam)
11	prime
12	unknown
13	prime
14	does not exist (BR)
15	E($\mathfrak{L}$) (deL)
16	prime power
17	prime
18	E($\mathfrak{L}$) (H)
19	prime
20	R($\mathfrak{L}$) (res) and E($\mathfrak{B}$) (gpw)
21	does not exist (BR)
22	does not exist (BR)
23	prime
24	unknown
25	prime power
26	E($\mathfrak{L}$) (H) and E($\mathfrak{B}$) (gpw)
27	prime power
28	R($\mathfrak{L}$) (res) and E($\mathfrak{B}$) (gpw)
29	prime
30	does not exist (BR)
31	prime
32	prime power
33	does not exist (BR)
34	E($\mathfrak{L}$) (H) and E($\mathfrak{B}$) (gpw)
35	E($\mathfrak{L}$) (deL)
36	R($\mathfrak{L}$) (res)
37	prime
38	does not exist (BR)
39	unknown
40	E($\mathfrak{B}$) (gpw)
41	prime
42	does not exist (BR)
43	prime
44	R($\mathfrak{L}$) (res)
45	E($\mathfrak{L}$) (deL)
46	does not exist (BR)
47	prime
48	unknown
49	prime power
50	E($\mathfrak{L}$) (H) and E($\mathfrak{B}$) (gpw)

order	comments
51	E($\mathfrak{L}$) (deL)
52	R($\mathfrak{L}$) (res) and E($\mathfrak{B}$) (gpw)
53	prime
54	does not exist (BR)
55	unknown
56	E($\mathfrak{B}$) (gpw)
57	does not exist (BR)
58	E($\mathfrak{L}$) (H) and E($\mathfrak{B}$) (gpw)
59	prime
60	R($\mathfrak{L}$) (res)
61	prime
62	does not exist (BR)
63	unknown
64	prime power
65	E($\mathfrak{L}$) (deL)
66	does not exist (BR)
67	prime
68	R($\mathfrak{L}$) (res)
69	does not exist (BR)
70	does not exist (BR)
71	prime
72	unknown
73	prime
74	E($\mathfrak{L}$) (H)
75	E($\mathfrak{L}$) (deL)
76	R($\mathfrak{L}$) (res)
77	does not exist (BR)
78	does not exist (BR)
79	prime
80	unknown
81	prime power
82	E($\mathfrak{L}$) (H) and E($\mathfrak{B}$) (gpw)
83	prime
84	R($\mathfrak{L}$) (res)
85	E($\mathfrak{L}$) (deL)
86	does not exist (BR)
87	E($\mathfrak{L}$) (deL)
88	E($\mathfrak{B}$) (gpw)
89	prime
90	does not exist (BR)
91	E($\mathfrak{L}$) (deL)
92	R($\mathfrak{L}$) (res) and E($\mathfrak{B}$) (gpw)
93	does not exist (BR)
94	does not exist (BR)
95	E($\mathfrak{L}$) (deL)
96	E($\mathfrak{B}$) (gpw)
97	prime
98	E($\mathfrak{L}$) (H)
99	E($\mathfrak{L}$) (deL)

Chapter 5

Projective Spaces and Codes

The work for this chapter was originally done under the supervison of Lynn Batten. With the exception of Section 5.3, most of the results are to appear in a paper coauthored with Lynn Batten [7].

5.1 Skew arcs

Recall from Chapter 1 the definition of a projective space. We consider here only geometries over $GF(2)$. All lines in $PG(m,2)$ have 3 points and all subspaces of dimension two are Fano planes.

Definition 18. We define a *skew arc* S to be a set of points in $PG(m,2)$ such that:

1. S does not contain all points of a line.
2. Given any four distinct points of S, say s_1, s_2, s_3 and s_4, the third point on the line containing s_1 and s_2 is not on the line containing s_3 and s_4.

In the Fano plane, the maximum number of points that can satisfy the conditions of a skew arc is 3 therefore there are no more than 3 points of a skew arc on any plane. A set of points which satisfies condition 1 is called an *arc*. We call 4 points that satisfy condition 1 but not condition 2 of the above definition a *planar quadrangle.*

We can coordinatize the points of $PG(m, 2)$ with the nonzero $(m+1)$-*tuples* of zeros and ones.

Example 52. The following 8 points in $PG(5, 2)$ form a skew arc: $(1,0,0,0,0,0)$, $(0,1,0,0,0,0)$, $(0,0,1,0,0,0)$, $(0,0,0,1,0,0)$, $(0,0,0,0,1,0)$, $(0,0,0,0,0,1)$, $(1,1,1,1,0,0)$, $(0,0,1,1,1,1)$.

Using the coordinates, the third point on a line containing points a_1 and a_2 is $a_1 + a_2$.

Definition 19. Given a set of points S in $PG(m, 2)$, we define the set $\widetilde{S}$ as $\{s_1 + s_2 | s_1, s_2 \in S, s_1 \neq s_2\}$.

We note that by the definition of a skew arc that there must be a unique point in $\widetilde{S}$ for each pair of distinct points in S. So if S is a skew arc with k points, then the size of $\widetilde{S}$ will be $\frac{k(k-1)}{2}$ and $S \cup \widetilde{S}$ will have $\frac{k(k+1)}{2}$ elements. This last equation, $|S \cup \widetilde{S}| = \frac{k(k+1)}{2}$, is a necessary and sufficient condition for S to be a skew arc.

We use the coordinatization of points to draw a correspondence between skew arcs and codes of minimum distance 5.

Example 53. If S is the skew arc given in example 52 then $\widetilde{S} = \{(1,1,0,0,0,0),$

$(1,0,1,0,0,0)$, $(1,0,0,1,0,0)$, $(1,0,0,0,1,0)$, $(1,0,0,0,0,1)$, $(0,1,1,0,0,0)$,

$(0,1,0,1,0,0)$, $(0,1,0,0,1,0)$, $(0,1,0,0,0,1)$, $(0,0,1,1,0,0)$, $(0,0,1,0,1,0)$,

$(0,0,1,0,0,1)$, $(0,0,0,1,1,0)$, $(0,0,0,1,0,1)$, $(0,0,0,0,1,1)$, $(0,1,1,1,0,0)$,

$(1,0,1,1,0,0)$, $(1,1,0,1,0,0)$, $(1,1,1,0,0,0)$, $(1,1,1,1,1,0)$, $(1,1,1,1,0,1)$,

$(1,0,1,1,1,1)$, $(0,1,1,1,1,1)$, $(0,0,0,1,1,1)$, $(0,0,1,0,1,1)$, $(0,0,1,1,0,1)$,

$(0,0,1,1,1,0)$, $(1,1,0,0,1,1)\}$.

We see that $\widetilde{S}$ has 28 points, all which are distinct from the 8 points of S. So $S \cup \widetilde{S}$ has 36 points, as expected.

5.2 Codes

We now show the relation between skew arcs and binary linear codes.

Definition 20. A (binary) *codeword of length* n is a binary n-tuple. We say the *distance* between two codewords (of the same length) is the number of positions in which they differ. A *code* is a collection of codewords and the *distance of a code* is the minimum distance over all pairs of codewords.

A $[n, k, d]$ *binary linear code* is a code having distance d with 2^k codewords, which are binary *n-tuples*, such that the sum of any two codewords is also a codeword. This implies the code is a subspace of dimension k of $GF(2)^n$. The *dual space* of C is the set of all vectors which are orthogonal to all the vectors in C, which is also a subspace of $GF(2)^n$.

We can associate with a linear code a parity check matrix H of size $(n-k) \times n$, whose rows are a basis of the dual space of the code. If H is the *parity check matrix* of the code C then $C = \{x|Hx^T = 0\}$.

Lemma 30. *If H is the parity check matrix of a code C then C has distance at least d iff any $d-1$ columns of H are linearly independent. [74]*

Lemma 31. *Let S be a skew arc in $PG(m, 2)$ with n points. Let H be a matrix whose columns are the elements of S, where each element of S is expressed as a binary vector. Then H is the parity check matrix of an $[n, n-(m+1), 5]$ code.*

Proof. No two columns of H are dependent since all of the columns are distinct. No three columns are dependent by part 1 of Definition 18. No four columns are dependent by part 2 of Definition 18. $\square$

Observe that the converse of Lemma 31 is also true - the columns of a parity check matrix of a code with distance at least 5 will form a skew arc; the fact that no three columns are dependent is sufficient to satisfy part 1 of Definition 18, and the fact that no three columns are dependent is sufficient to satisfy part 2 of Definition 18.

Example 54. Using the skew arc given in Example 52, we form

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix},$$

the parity check matrix of an $[8,2,5]$ code whose 4 codewords are the vectors comprising the null space of H, namely $[0,0,0,0,0,0,0,0,0]$, $[1,1,1,1,0,0,1,0]$, $[0,0,1,1,1,1,0,1]$, $[1,1,0,0,1,1,1,1]$.

5.3 Some basics about skew arcs

Definition 21. Given a skew arc S we define $\widehat{S}$ as $\{s|\exists s_1, s_2, s_3 \in S$ such that for some x, $\{x, s_1, s_2\}$ and $\{x, s_3, s\}$ are lines $\}$. Also, $\widehat{S} = \{s_1 + s_2 + s_3 | s_1, s_2, s_3 \in S$, $s_1 \neq s_2 \neq s_3 \neq s_1\}$

Note that $\widehat{S} \cap S = \varnothing$, since if an element $s_1 + s_2 + s_3$ were also in S, then $s_1 + (s_1 + s_2 + s_3) = s_2 + s_3$, and S would not be a skew arc.

We call a skew arc S *maximal* if there is no skew arc S' such that $S \subsetneq S'$.

Lemma 32. *A skew arc S in $PG(m,2)$ is maximal iff $S \cup \widetilde{S} \cup \widehat{S} = PG(m,2)$.*

Proof. Suppose $S \cup \widetilde{S} \cup \widehat{S} = PG(m,2)$, if S is not maximal then there exists $p \in PG(m,2)$ ($p \notin S$) such that $S \cup \{p\}$ is a skew arc. If $p \in \widetilde{S}$ then $S \cup \{p\}$ would contain a line, violating condition 1 of Definition 18. If $p \in \widehat{S}$ then $S \cup \{p\}$ would contain 4 points which violated condition 2 of Definition 18.

Suppose S is maximal, then for every $p \neq S$, $S \cup \{p\}$ is not a skew arc. If $S \cup \{p\}$ fails condition 1, then $p \in \widetilde{S}$. If $S \cup \{p\}$ fails condition 2, then $p \in \widehat{S}$. □

Lemma 33. *If $m \geq 4$, then all maximal skew arcs in $PG(m, 2)$ will intersect any hyperplane.*

Proof. Suppose there was a maximal skew arc S with k points and a disjoint hyperplane H. Since any line with two points of $PG(m, 2)\backslash H$ must meet in H, we know that $\widetilde{S} \subseteq H$. Every point in $\widehat{S}$ is the third point on a line through a point of $\widetilde{S}$ and a point of S. Since $S \subset PG(m, 2)\backslash H$, it follows that $\widehat{S} \subset PG(m, 2)\backslash H$. By maximality, we get that $\widetilde{S} = H$. By comparing the sizes we get

$$\frac{k(k-1)}{2} = 2^{m-1} - 1.$$

So

$$4k^2 - 4k = 2^{m+2} - 8$$

$$(2k-1)^2 = 2^{m+2} - 7.$$

This is a Diophantine equation of the form $2^n = x^2 + 7$ which is known to have integral solutions only when $n = 3, 4, 5, 7, 15$ [76].

We can eliminate certain cases by noting that the size of S must be divisible by 3. To see this, simply let p be a point of $\widehat{S} \subset PG(m, 2)\backslash H$. For every point a in S, we know that $p + a$ is in H so it must be the (unique) sum of two points of S, say b and c. Now since $p+a = b+c$ we get $p+b = a+c$ and $p+c = a+b$. This will induce a partition on the points of S where the size of each part is 3. Hence S is divisible by 3.

Hence the only solutions to the above Diophantine equation that give viable solutions to a skew arc that is disjoint from a hyperplane are $k = 3$ in $PG(2, 2)$ and $k = 6$ in $PG(4, 2)$. □

Example 55. The skew arc of size 3 in the Fano plane is contained in the complement of a hyperplane (hyperplanes in PG(2,2) are simply lines).

Example 56. The skew arc of size 6 in $PG(4, 2)$ given by the points $(1, 0, 0, 0, 0)$, $(0, 1, 0, 0, 0)$, $(0, 0, 1, 0, 0)$, $(0, 0, 0, 1, 0)$, $(0, 0, 0, 0, 1)$, and $(1, 1, 1, 1, 1)$ is contained in the complement of a hyperplane: these points all miss the hyperplane described by $x_1 + x_2 + x_3 + x_4 + x_5 = 0$.

It is known that the maximum size of an arc in $PG(m, 2)$ is 2^m, and these points are the complement of a hyperplane.

Corollary 34. *A maximal skew arc cannot be derived by deleting points from a maximum arc.*

Proof. A maximal arc is contained in the complement of a hyperplane. □

5.4 Some skew arc constructions

There are several known constructions for arcs [16] [17] [18] [22] [24] [57]. For example, given an arc of size k in $PG(m, 2)$, an arc of size $2k$ can be constructed in $PG(m+1, 2)$. Essentially, if A is an arc in $PG(m, 2)$ then we can embed $PG(m, 2)$ into $PG(m+1, 2)$, pick a point outside of the embedded $PG(m, 2)$, say p. Then $B = A \cup \{a + p | a \in A\}$ is an arc in $PG(m + 1, 2)$.

We attempted to find something similar to the above construction for skew arcs, leading us to the following result, which unfortunately requires two separate skew arcs to start with.

Theorem 35. *If, in $PG(m, 2)$, there are two skew arcs S_1 and S_2 of sizes k_1 and k_2 respectively such that $(S_1 \cup \widetilde{S_1}) \cap (S_2 \cup \widetilde{S_2}) = \varnothing$ then there exists a skew arc of size $k_1 + k_2 + 1$ in $PG(m + 1, 2)$.*

Proof. We embed a copy of $PG(m, 2)$ into $\Pi = PG(m + 1, 2)$ via an isomorphism with a hyperplane H of Π. Let $p \in \Pi \backslash H$.

We define $\vec{S_2^p}$ as $\{s_i + p | s_i \in S_2\}$. Now let $S = S_1 \cup \vec{S_2^p} \cup \{p\}$. We claim that S a skew arc.

First, we claim S contains no lines. Since $S \cap H$ contains only elements of S_1, which is itself a skew arc, there are no lines of H in S. We consider lines that will have one point in H and two in $\Pi \backslash H$. The point p will not be on a line with a point of $\vec{S_2^p}$ and a point of S_1 since $S_1 \cap S_2 = \varnothing$. Two points of $\vec{S_2^p}$ will not be on a line with a point of S_1 since $S_1 \cap \widetilde{S}_2 = \varnothing$. Since all lines of Π meet H, S satisfies condition 1 of Definition 18.

Now to see that there are no planar quadrangles in S we check that all sums of two elements of S are distinct. Since H is a hyperplane, the sum of any two elements in H will be in H, and also the sum of two elements in $\Pi \backslash H$ will be in H. The sum of an element from H and one from $\Pi \backslash H$ cannot be in H since if H contains two points of a line, it contains the whole line. Hence the only way for an element of $\widetilde{S}$ to be in H is for it to be either the sum of two elements that are both from S_1 or the sum of two elements both from $\vec{S_2^p} \cup \{p\}$.

Two elements from S_1 have their sum in $\widetilde{S}_1$ and two elements of $\vec{S_2^p}$ have their sum in $\widetilde{S}_2$. Also, p and any element from $\vec{S_2^p}$ will have their sum in S_2. Hence an element of $\widetilde{S} \cap H$ is the sum of two elements of S in only one way.

For sums in $\Pi \backslash H$, we look at the sum of two elements of S, one in H, the other in $\Pi \backslash H$. There are two types, $a + p$ and $a + b$ where $a \in S_1$ and $b \in \vec{S_2^p}$. A point of type $a + p$ and a point of type $a + b$ are distinct since $\widetilde{S}_1 \cap S_2 = \varnothing$. Two points of type $a + b$, where the a's and b's are distinct, will be distinct since $\widetilde{S}_1 \cap \widetilde{S}_2 = \varnothing$. If the a's are not distinct, then two sums of type $a + b$ will be distinct simply because the b's are distinct. If the b's are not distinct, then two sums of type $a + b$ will be distinct since the a's are. Two sums of type $a+p$ will also be distinct since the a's are. Hence S satisfies condition 2 of Definition 18. $\square$

In terms of codes, this construction is similar to the inverted Y1 construction [49], and a condition similar to that of Theorem 35 was given in [23].

Example 57. Let S_1 be the skew arc in Example 52, we can let $S_2 = \{(1,0,1,0,1,1), (0,1,1,1,0,1)\}$. Since $\widetilde{S_2} = \{(1,1,0,1,1,0)\}$, we can check (from Example 53) that $(S_1 \cup \widetilde{S_1}) \cap (S_2 \cup \widetilde{S_2}) = \varnothing$. We embed $PG(5,2)$ into $PG(6,2)$ by identifying each element of $PG(5,2)$ with the element of $PG(6,1)$ having its last coordinate zero. (E.g. $(1,0,0,0,0,0)$ in $PG(5,2)$ becomes identified with $(1,0,0,0,0,0,0)$ in $PG(6,2)$.) Now using $(0,0,0,0,0,0,1)$ as p we get a skew arc with 11 points in $PG(6,2)$, namely $(1,0,0,0,0,0,0)$, $(0,1,0,0,0,0,0)$, $(0,0,1,0,0,0,0)$, $(0,0,0,1,0,0,0)$, $(0,0,0,0,1,0,0)$, $(0,0,0,0,0,1,0)$, $(1,1,1,1,0,0,0)$, $(0,0,1,1,1,1,0)$, $(0,0,0,0,0,0,1)$, $(1,0,1,0,1,1,1)$, $(0,1,1,1,0,1,1)$.

Corollary 36. *If there are, in $PG(m,2)$, $n+1$ skew arcs S_0, S_1, …, S_n of sizes k_0, k_1, …, k_n respectively such that $(S_i \cup \widetilde{S_i}) \cap (S_j \cup \widetilde{S_j}) = \varnothing$ for $i \neq j$; $i,j = 0,\dots,n$ then there exist a skew arc of size $k_0 + k_1 + \cdots + k_n + n$ in $PG(m+n,2)$.*

Proof. We can embed $PG(m,2)$ into $PG(m+1,2)$ as above and use S_0 with S_1 to construct a new skew arc S with Theorem 35. From the proof, we can see that since all points of $\widetilde{S}$ that intersect the original $PG(m,2)$ are either in $\widetilde{S}_0$, S_1, or $\widetilde{S}_1$, hence $(S \cup \widetilde{S}) \cap (S_i \cup \widetilde{S}_i) = \varnothing$ for $i = 2 \dots n$. We continue in this manner $n-1$ times. $\square$

Example 58. Using S_1 and S_2 as in Example 57 and

$S_3 = \{(1,1,0,1,1,1),(0,1,1,1,1,0)\}$, we get

$$\{(1,0,0,0,0,0,0,0),(0,1,0,0,0,0,0,0),(0,0,1,0,0,0,0,0),$$
$$(0,0,0,1,0,0,0,0),(0,0,0,0,1,0,0,0),(0,0,0,0,0,1,0,0),$$
$$(1,1,1,1,0,0,0,0),(0,0,1,1,1,1,0,0),(0,0,0,0,0,0,1,0),$$
$$(1,0,1,0,1,1,1,0),(0,1,1,1,0,1,1,0),(1,1,0,1,1,1,0,1),$$
$$(0,1,1,1,1,0,0,1),(0,0,0,0,0,0,0,1)\},$$

a skew arc in $PG(7,2)$ with 14 points.

Chen [23] did something similar, using three sets to construct a skew arc, increasing the dimension by two. We have shown in Corollary 36 that this can be generalised, with any number of skew arcs in the original projective space. This led us to raise the question of whether an additional dimension is needed for each additional set. One answer we have found is that, with some other conditions, a construction requiring fewer dimensions may be obtained.

For this, we introduce some new notation. If A and B are disjoint subsets of $PG(m,2)$ then $A+B = \{a+b | a \in A, b \in B\}$. Alternately this can be viewed as the set $\{x | \exists a \in A, \exists b \in B$ and $\{a, b, x\}$ is a line$\}$.

Theorem 37. *If there are, in $PG(m, 2)$, four skew arcs S_0, S_1, S_2 and S_3 of sizes k_0, k_1, k_2 and k_3 respectively such that $(S_i \cup \widetilde{S_i}) \cap (S_j \cup \widetilde{S_j}) = \varnothing$ for $i \neq j$; $i, j = 0, 1, 2, 3$ and there is a point d in $PG(m, 2)$ such that $d \notin S_i$, $d \notin S_i + S_j$, $i \neq j$, $d \notin S_i + S_j + S_k$ for distinct $i, j, k \in \{0, 1, 2, 3\}$ and $d \notin S_0 + S_1 + S_2 + S_3$, then there exists a skew arc of size $k_0 + k_1 + k_2 + k_3 + 3$ in $PG(m + 2, 2)$.*

Proof. We embed $PG(m, 2)$ into $\Pi = PG(m + 2, 2)$ via an isomorphism with a subspace H of Π. Let M_1, M_2, and M_3 be the hyperplanes of Π containing H. We pick $p_1 \in M_1 \backslash H$, $p_2 \in M_2 \backslash H$ and let $p_3 = p_1 + p_2 + d$. Note that $p_3 \in M_3 \backslash H$.

Now $S = S_0 \cup S_1^{\vec{p_1}} \cup \{p_1\} \cup S_2^{\vec{p_2}} \cup \{p_2\} \cup S_3^{\vec{p_3}} \cup \{p_3\}$ is the required skew arc, which we now show.

For $i = 1, 2, 3$, $S \cap M_i$ is constructed exactly as in Theorem 35. So there are no lines in H, nor in each M_i. We now check that there are no lines that have one point in each of the M_i's.

A line intersecting all of the M_i's would have one point in each $M_i \backslash H$. Let these three points be $a + p_1$, $b + p_2$, and $c + p_3$, where $a \in S_1 \cup \{0\}$, $b \in S_2 \cup \{0\}$, and $c \in S_3 \cup \{0\}$ (where $0 + p_i$ would simply be the point p_i). If these three points were on a line then $a + p_1 + b + p_2 + c + p_3 = 0$; hence $a + b + c + d = 0$, so $d = a + b + c$. If all three of a, b, and c were 0 then it would follow that $d = 0$, which is a contradiction, since 0 does not represent any point in the geometry. Since $d = a + b + c$ and $d \neq 0$ we know that $d \in S_1$, S_2, S_3, $S_1 + S_2$, $S_1 + S_3$, $S_2 + S_3$, or $S_1 + S_2 + S_3$.

From the proof of Theorem 35, no planar quadrangle is contained in a single M_i. All that is left to check is that the sum of two elements from $M_i \backslash H$ is not the sum of two elements of H or of two elements of $M_j \backslash H$ (for $i \neq j$, $i, j \in \{1, 2, 3\}$), and that the sum of an element from $M_1 \backslash H$ with an element of $M_2 \backslash H$ is not the sum of an element in $M_3 \backslash H$ and an element of H.

As in the proof of Theorem 35, we notice that the sum of two elements of $S \cap H$ is in $S_0 \cup \widetilde{S_0}$ and the sum of two elements of $S \cap M_i \backslash H$ (for $i \in \{1, 2, 3\}$) is in $S_i \cup \widetilde{S_i}$, they must be distinct.

Now let us consider $a+p_1$ to be an element of $S \cap M_1 \backslash H$ where $a \in S_1 \cup \{0\}$, $b+p_2$ an element of $S \cap M_2 \backslash H$ where $b \in S_2 \cup \{0\}$, and $c+p_3$ an element of $S \cap M_3 \backslash H$ where $c \in S_3 \cup \{0\}$. Let $z \in S \cap H$. If the sum of $a+p_1$ and $b+p_2$ were not distinct from the sum of $c+p_3$ and z, then we would have $a+b+c+d+z = 0$, hence $d = a+b+c+z$. This would imply that $d \in S_0$, $S_0 + S_1$, $S_0 + S_2$, $S_0 + S_3$, $S_0 + S_1 + S_2$, $S_0 + S_1 + S_3$, $S_0 + S_2 + S_3$, or $S_0 + S_1 + S_2 + S_3$. $\square$

Example 59. To emphasize the necessity of d in the above proof, we consider the following skew arcs. Let

$$S_0 = \{(1,0,0,0,0,0),(0,1,0,0,0,0),(0,0,1,0,0,0),(0,0,0,1,0,0),$$
$$(0,0,0,0,1,0),(0,0,0,0,0,1),(1,1,1,1,0,0)\},$$
$$S_1 = \{(1,0,1,0,1,0),(0,1,0,1,0,1),(1,1,0,0,1,1)\},$$
$$S_2 = \{(1,0,0,0,1,1),(0,1,1,0,1,0),(1,1,0,1,0,1)\} \text{ and}$$
$$S_3 = \{(1,0,0,1,0,1),(0,1,0,0,1,1)\}.$$

Now $(S_i \cup \widetilde{S}_i) \cap (S_j \cup \widetilde{S}_j) = \varnothing$ for $i \neq j$, but there is no 18 point skew arc in $PG(7,2)$. [15] Hence no such skew arc can be constructed from these skew arcs having 18 points.

Example 60. Let S_0 be the skew arc given in Example 52, let

$$S_1 = \{(1,0,1,0,1,1),(0,1,1,1,0,1)\},$$
$$S_2 = \{(1,1,0,1,1,1),(0,1,1,1,1,0)\} \text{ and}$$
$$S_3 = \{(0,1,0,1,0,1),(1,0,1,0,1,0)\}.$$

Then $d = (1,0,1,1,0,0)$ satisfies the conditions of Theorem 37. This gives us a skew arc with 17 points in $PG(7,2)$, which is maximum [15]. If we choose p_1 to be $(0,0,0,0,0,0,1,0)$, and p_2 to be $(0,0,0,0,0,0,0,1)$, then our construction give the following skew arc :

$(1,0,0,0,0,0,0,0)$, $(0,1,0,0,0,0,0,0)$, $(0,0,1,0,0,0,0,0)$, $(0,0,0,1,0,0,0,0)$, $(0,0,0,0,1,0,0,0)$, $(0,0,0,0,0,1,0,0)$, $(1,1,1,1,0,0,0,0)$, $(0,0,1,1,1,1,0,0)$, $(0,0,0,0,0,0,1,0)$, $(1,0,1,0,1,1,1,0)$, $(0,1,1,1,0,1,1,0)$, $(1,1,0,1,1,1,0,1)$, $(0,1,1,1,1,0,0,1)$, $(0,0,0,0,0,0,0,1)$, $(1,0,1,1,0,0,1,1)$, $(1,1,1,0,0,1,1,1)$, $(0,0,0,1,1,0,1,1)$.

5.5 Codes and constructions

We turn our attention now to a known class of codes: BCH codes [74]. Each element of $GF(2^n)$ can be expressed as an n length vector over $GF(2)$. The matrix H is a $\{0,1\}$-matrix written in terms of elements of $GF(2^n)$, each representing its vector expansion as a column. If α is primitive in $GF(2^n)$ it is known that the parity check matrix of the BCH code with distance $d \geq 5$ can be taken to be the following $2n \times 2^n - 1$ matrix .

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^i & \cdots & \alpha^{(2^n-2)} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3i} & \cdots & \alpha^{3(2^n-2)} \end{bmatrix}$$

Since the columns of H are $2n$ length vectors over $GF(2)$, we can view them as points of $PG(2n-1,2)$ and we will refer to the set of these points (which is a skew arc - see comment following Lemma 31) as B_n. Also, we can view all points in $PG(2n-1,2)$ as 2-tuples over $GF(2^n)$ as well as $2n$-tuples over $GF(2)$.

Wishing to use the skew arcs B_n in constructions, we discovered the following theorem which gives a characterization of $B_n \cup \widetilde{B_n}$ looks like in $PG(2n-1,2)$.

Theorem 38. *For $x \neq 0$, $x \in GF(2^n)$, the set $M_x = \{x^3 + a^3 + b^3 | a + b = x\}$ is a subgroup of the additive group of $GF(2^n)$ with $[GF(2^n) : M_x] = 2$.*

Proof. Suppose $a + b = x$ and $c + d = x$. Then

$$\begin{aligned} x^3 + a^3 + b^3 + x^3 + c^3 + d^3 &= a^3 + b^3 + c^3 + d^3 \\ &= a^3 + b^3 + x^3 + c^2 d + c d^2 \\ &= x^3 + a^3 + b^3 + c^2(a + b + c) + c(a^2 + b^2 + c^2) \\ &= x^3 + (a^3 + ca^2 + c^2 a + c^3) + (b^3 + cb^2 + c^2 b + c^3) \\ &= x^3 + (a + c)^3 + (b + c)^3. \end{aligned}$$

Since $(a + c) + (b + c) = a + b = x$, we see that the sum of two elements of M_x is in M_x. Hence M_x is closed under addition.

There are exactly 2^{n-1} pairs of elements that sum to x. Suppose again we have $a + b = x$ and $c + d = x$, then $d = a + b + c$. Now if $x^3 + a^3 + b^3 = x^3 + c^3 + d^3$ then

$$\begin{aligned} a^3 + b^3 &= c^3 + (a + b + c)^3 \\ a^3 + b^3 &= a^3 + b^3 + a^2 b + a^2 c + ab^2 + b^2 c + ac^2 + bc^2. \end{aligned}$$

Hence we would have

$$a^2b + a^2c + ab^2 + b^2c + ac^2 + bc^2 = 0$$

$$a^2(b + c) + a(b + c)^2 = bc(b + c)$$

$$a^2 + ab = bc + ac$$

$$a(a + b) = c(a + b)$$

$$a = c.$$

Hence each pair of elements which sum to x gives a distinct element of M_x, so $[GF(2^n) : M_x] = 2$. □

Let $M_x + x^3 = N_x = \{a^3 + b^3 | a + b = x\}$. If n is even we let $t = (2^n - 1)/3$. Recall that α is a primitive element in $GF(2^n)$. Since n is even, $GF(2^n)$ contains a subfield of order 4 which will contain the elements $\{0, 1, \alpha^t, \alpha^{2t}\}$. Hence $1 + \alpha^t + \alpha^{2t} = 0$. So for $x \in GF(2^n)$ $x = x\alpha^t + x\alpha^{2t}$. Since $x^3 = (x\alpha^t)^3 = (x\alpha^{2t})^3$, we can see that $0 \in N_x$ and hence $N_x = M_x$. If n is odd, 3 and $2^n - 1$ are relatively prime, so $a^3 \neq b^3$ if $a \neq b$ for $a, b \in GF(2^n)$. So $0 \notin N_x$. Hence N_x must be the other coset of M_x. So for any element y in $GF(2^n)$, all points in $B_n \cup \widetilde{B_n}$, as 2-tuples over $GF(2^n)$, which have y in the first coordinate have either y^3 or $a^3 + b^3$, where $a + b = y$, in the second. Hence $B_n \cup \widetilde{B_n} = \{(y, z) | z \in N_y\}$.

We introduce now a small skew arc to be used along with the BCH codes in constructions. It has 7 points: $(0, x_2+y_2+z_2)$, (x_1, x_2), (x_1, x_2+z_2), (y_1, y_2), (y_1, y_2+x_2), (z_1, z_2), (z_1, z_2+y_2), where $\{x_1, y_1, z_1\}$ and $\{x_2, y_2, z_2\}$ generate 8 element additive subgroups (not necessarily different) of $GF(2^n)$ for $n \geq 3$. We call this skew arc A_3, since the code it gives via Lemma 31 is isomorphic to that given by B_3 (i.e., the BCH code of length 7).

We see that $A_3 \cup \widetilde{A_3}$ takes the following form, which is similar to the form of $B_n \cup \widetilde{B_n}$. Elements whose first element, taken as a 2-tuple over $GF(2^n)$, is 0 have as their second element one of $\{x_2 + y_2 + z_2, x_2, y_2, z_2\}$ (which is a coset of a 4 element subgroup of the group generated by x_2, y_2, z_2). Elements whose first element is x_1 have as second element one of $\{x_2, x_2 + z_2, y_2 + z_2, y_2\}$ (again a coset), etc.

Let α be a primitive element in $GF(2^4)$, where $x^4 + x + 1$ is the generating polynomial, and let $\{x_1, y_1, z_1\}$ be $\{\alpha^{10}, \alpha^9, \alpha^6\}$ and $\{x_2, y_2, z_2\}$ be $\{\alpha^2, \alpha^8, \alpha^{10}\}$. This skew arc and B_4 do not satisfy the conditions of Theorem 35, so we alter it by adding α^{13} to the second element of each column that has a first element α^{10} or α^6. We then get the following skew arc in $PG(7, 2)$ with 7 points: $\{(0, \alpha^5)$, $(\alpha^{10}, \alpha^{14})$, $(\alpha^{10}, \alpha^{11})$, $(\alpha^9, 1)$, (α^9, α^8), (α^6, α^9), $(\alpha^6, \alpha^{12})\}$

Now A_3 as given above and B_4 satisfy the conditions of Theorem 35. Hence, since A_3 (of size 7) and B_4 (of size 15) are disjoint skew arcs in $PG(7, 2)$ satisfying the conditions of Theorem 35 we can construct a skew arc of size 23 in $PG(8, 2)$ which gives rise to a $[23, 14, 5]$ code.

This gives a nice construction of the Wagner code [84], answering Research Problem 18.3 of [74], but unfortunately this approach does not extend well. It works mostly because A_3 is small. Also, constructing with B_n when $n > 4$ gives codes too small to be considered interesting.

Appendix A

Examples

For planes of small orders, we give a representation of the plane by the kernel, and again by the cokernel. Also, for odd orders, we give the weighing matrix build from the construction in Theorem 28 and if applicable, the Hadamard matrix from Theorem 29. We use the standard convention of representing a -1 by a $-$ in Hadamard and weighing matrices.

A.1 Plane of order 2 - the Fano plane

Kernel $(GH(2, G))$:

$$\begin{pmatrix} e & e \\ e & a \end{pmatrix}$$

where $G = Z_2 = \{e, a\}$.

Cokernel $(GW(3, G))$:

$$\left(\begin{array}{c|c|c} 0 & 1 & 1 \\ \hline 1 & 0 & 1 \\ \hline 1 & 1 & 0 \end{array}\right)$$

where $G = \{1\}$.

A.2 plane of order 3

Kernel ($GH(3, G)$):

$$\begin{pmatrix} e & e & e \\ e & \gamma & \gamma^2 \\ e & \gamma^2 & \gamma \end{pmatrix}$$

where $G = C_3 = \{e, \gamma, \gamma^2\}$.

Cokernel ($GW(4, 3, G)$):

$$\begin{pmatrix} 0 & e & e & e \\ e & 0 & e & a \\ e & a & 0 & e \\ e & e & a & 0 \end{pmatrix}$$

where $G = Z_2 = \{e, a\}$.

Skew symmetric weighing matrix:

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ - & 0 & 1 & - \\ - & - & 0 & 1 \\ - & 1 & - & 0 \end{pmatrix}.$$

Hadamard matrix:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ - & 1 & 1 & - \\ - & - & 1 & 1 \\ - & 1 & - & 1 \end{pmatrix}.$$

A.3 plane of order 4

Kernel ($GH(4, G)$):

$$\begin{pmatrix} e & e & e & e \\ e & a & b & ab \\ e & b & ab & a \\ e & ab & a & b \end{pmatrix}$$

where $G = \{a, b | a^2 = 1, b^2 = 1, ab = ba\}$.

Cokernel (GW(5,4,G)):

$$\begin{pmatrix} 0 & e & e & e & e \\ e & 0 & e & \gamma & \gamma^2 \\ e & e & 0 & \gamma^2 & \gamma \\ e & \gamma & \gamma^2 & 0 & e \\ e & \gamma^2 & \gamma & e & 0 \end{pmatrix}.$$

where $G = C_3 = \{e, \gamma, \gamma^2\}$.

Baer-kernel ($GW(7,4,2)$):

$$\begin{pmatrix} 0 & e & e & e & 0 & e & 0 \\ 0 & 0 & e & a & e & 0 & e \\ e & 0 & 0 & e & e & a & 0 \\ 0 & e & 0 & 0 & a & a & e \\ e & 0 & a & 0 & 0 & e & e \\ e & e & 0 & a & 0 & 0 & a \\ e & a & e & 0 & e & 0 & 0 \end{pmatrix}$$

where $G = Z_2 = \{e, a\}$.

A.4 plane of order 5

Kernel ($GH(5, G)$):

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^4 & \beta^3 \\ 1 & \beta^3 & \beta & \beta^2 & \beta^4 \\ 1 & \beta^4 & \beta^3 & \beta & \beta^2 \\ 1 & \beta^2 & \beta^4 & \beta^3 & \beta \end{pmatrix}$$

where $G = \{1, \beta, \beta^2, \beta^3, \beta^4\}$.

Cokernel($GW(6, 4, G)$):

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^3 & \omega^2 \\ 1 & \omega^2 & 0 & 1 & \omega & \omega^3 \\ 1 & \omega^3 & \omega^2 & 0 & 1 & \omega \\ 1 & \omega & \omega^3 & \omega^2 & 0 & 1 \\ 1 & 1 & \omega & \omega^3 & \omega^2 & 0 \end{pmatrix}$$

where $G = \{1, \omega, \omega^2, \omega^3\}$

Skew symmetric weighing matrix:

$$\begin{pmatrix}
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & - & 0 & - & 0 & - & 0 & - & 0 & - \\
- & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & - & - & 0 \\
0 & 1 & 0 & 0 & 0 & - & 1 & 0 & - & 0 & 0 & 1 \\
- & 0 & - & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & - \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & - & 1 & 0 & - & 0 \\
- & 0 & 0 & - & - & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & - & 0 & 0 & 1 & 0 & 0 & 0 & - & 1 & 0 \\
- & 0 & 0 & 1 & 0 & - & - & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & - & 0 & 0 & 1 & 0 & 0 & 0 & - \\
- & 0 & 1 & 0 & 0 & 1 & 0 & - & - & 0 & 0 & 0 \\
0 & 1 & 0 & - & 1 & 0 & - & 0 & 0 & 1 & 0 & 0
\end{pmatrix}.$$

Hadamard matrix:

$$\begin{pmatrix}
1 & 1 & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - \\
1 & - & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
- & 1 & 1 & 1 & 1 & - & 1 & 1 & - & - & - & 1 \\
- & - & 1 & - & 1 & 1 & - & 1 & 1 & - & - & - \\
- & 1 & - & 1 & 1 & 1 & 1 & - & 1 & 1 & - & - \\
- & - & - & - & 1 & - & 1 & 1 & - & 1 & 1 & - \\
- & 1 & - & - & - & 1 & 1 & 1 & 1 & - & 1 & 1 \\
- & - & 1 & - & - & - & 1 & - & 1 & 1 & - & 1 \\
- & 1 & 1 & 1 & - & - & - & 1 & 1 & 1 & 1 & - \\
- & - & - & 1 & 1 & - & - & - & 1 & - & 1 & 1 \\
- & 1 & 1 & - & 1 & 1 & - & - & - & 1 & 1 & 1 \\
- & - & 1 & 1 & - & 1 & 1 & - & - & - & 1 & -
\end{pmatrix}.$$

A.5 plane of order 7

Kernel $(GH(7,G))$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^3 & \beta^2 & \beta^6 & \beta^4 & \beta^5 \\ 1 & \beta^5 & \beta & \beta^3 & \beta^2 & \beta^6 & \beta^4 \\ 1 & \beta^4 & \beta^5 & \beta & \beta^3 & \beta^2 & \beta^6 \\ 1 & \beta^6 & \beta^4 & \beta^5 & \beta & \beta^3 & \beta^2 \\ 1 & \beta^2 & \beta^6 & \beta^4 & \beta^5 & \beta & \beta^3 \\ 1 & \beta^3 & \beta^2 & \beta^6 & \beta^4 & \beta^5 & \beta \end{pmatrix}$$

where $G = \{1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6\}$

Cokernel $(GW(8,7,G))$:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega^2 & \omega & \omega^4 & \omega^5 & \omega^3 \\ 1 & \omega^3 & 0 & 1 & \omega^2 & \omega & \omega^4 & \omega^5 \\ 1 & \omega^5 & \omega^3 & 0 & 1 & \omega^2 & \omega & \omega^4 \\ 1 & \omega & \omega^4 & \omega^5 & \omega^3 & 0 & 1 & \omega^2 \\ 1 & \omega^2 & \omega & \omega^4 & \omega^5 & \omega^3 & 0 & 1 \\ 1 & 1 & \omega^2 & \omega & \omega^4 & \omega^5 & \omega^3 & 0 \end{pmatrix}$$

where $G = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$

Skew symmetric weighing matrix:

$$
\begin{pmatrix}
0&0&0&1&0&0&1&0&0&1&0&0&1&0&0&1&0&0&1&0&0&1&0&0\\
0&0&0&0&0&-&0&0&-&0&0&-&0&0&-&0&0&-&0&0&-&0&0&-\\
0&0&0&0&-&0&0&-&0&0&-&0&0&-&0&0&-&0&0&-&0&0&-&0\\
-&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&-&0&0&0&-&-&0&0\\
0&0&1&0&0&0&0&0&-&0&1&0&1&0&0&-&0&0&0&-&0&0&0&1\\
0&1&0&0&0&0&0&-&0&1&0&0&0&0&-&0&0&1&-&0&0&0&1&0\\
-&0&0&-&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&-&0&0&0&-\\
0&0&1&0&0&1&0&0&0&0&0&-&0&1&0&1&0&0&-&0&0&0&-&0\\
0&1&0&0&1&0&0&0&0&0&-&0&1&0&0&0&0&-&0&0&1&-&0&0\\
-&0&0&0&0&-&-&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&-&0\\
0&0&1&0&-&0&0&0&1&0&0&0&0&0&-&0&1&0&1&0&0&-&0&0\\
0&1&0&-&0&0&0&1&0&0&0&0&0&-&0&1&0&0&0&0&-&0&0&1\\
-&0&0&0&-&0&0&0&-&-&0&0&0&0&0&1&0&0&0&0&1&0&1&0\\
0&0&1&-&0&0&0&-&0&0&0&1&0&0&0&0&0&-&0&1&0&1&0&0\\
0&1&0&0&0&1&-&0&0&0&1&0&0&0&0&0&-&0&1&0&0&0&0&-\\
-&0&0&0&1&0&0&-&0&0&0&-&-&0&0&0&0&0&1&0&0&0&0&1\\
0&0&1&1&0&0&-&0&0&0&-&0&0&0&1&0&0&0&0&0&-&0&1&0\\
0&1&0&0&0&-&0&0&1&-&0&0&0&1&0&0&0&0&0&-&0&1&0&0\\
-&0&0&0&0&1&0&1&0&0&-&0&0&0&-&-&0&0&0&0&0&1&0&0\\
0&0&1&0&1&0&1&0&0&-&0&0&0&-&0&0&0&1&0&0&0&0&0&-\\
0&1&0&1&0&0&0&0&-&0&0&1&-&0&0&0&1&0&0&0&0&0&-&0\\
-&0&0&1&0&0&0&0&1&0&1&0&0&-&0&0&0&-&-&0&0&0&0&0\\
0&0&1&0&0&-&0&1&0&1&0&0&-&0&0&0&-&0&0&0&1&0&0&0\\
0&1&0&0&-&0&1&0&0&0&0&-&0&0&1&-&0&0&0&1&0&0&0&0
\end{pmatrix}.
$$

A.6 plane of order 8

Kernel ($GH(8, G)$):

$$
\begin{pmatrix}
1&1&1&1&1&1&1&1\\
1&a&b&c&ab&bc&abc&ac\\
1&ac&a&b&c&ab&bc&abc\\
1&abc&ac&a&b&c&ab&bc\\
1&bc&abc&ac&a&b&c&ab\\
1&ab&bc&abc&ac&a&b&c\\
1&c&ab&bc&abc&ac&a&b\\
1&b&c&ab&bc&abc&ac&a
\end{pmatrix}.
$$

where $G = \{abc|a^2 = b^2 = c^2 = 1; xy = yx \text{ for generators } x, y\}$

Cokernel $(GW(9,8,G))$:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & g & g^2 & g^3 & g^6 & g^4 & g^5 \\ 1 & 1 & 0 & g^3 & g^6 & g & g^2 & g^5 & g^4 \\ 1 & g & g^3 & 0 & g^4 & 1 & g^5 & g^2 & g^6 \\ 1 & g^2 & g^6 & g^4 & 0 & g^5 & 1 & g & g^3 \\ 1 & g^3 & g & 1 & g^5 & 0 & g^4 & g^6 & g^2 \\ 1 & g^6 & g^2 & g^5 & 1 & g^4 & 0 & g^3 & g \\ 1 & g^4 & g^5 & g^2 & g & g^6 & g^3 & 0 & 1 \\ 1 & g^5 & g^4 & g^6 & g^3 & g^2 & g & 1 & 0 \end{pmatrix}.$$

where $G = C_7 = \{1, g, g^2, g^3, g^4, g^5, g^6\}$.

A.7 planes of order 9

There are four known planes of order 9, the Desarguesian plane, the left and right nearfield planes, and the Hughes plane.

A.7.1 Desarguesian plane

Kernel ($GH(9,G)$);

$$\begin{pmatrix} e & e & e & e & e & e & e & e & e \\ e & x & y & xy^2 & x^2y^2 & x^2 & y^2 & x^2y & xy \\ e & xy & x & y & xy^2 & x^2y^2 & x^2 & y^2 & x^2y \\ e & x^2y & xy & x & y & xy^2 & x^2y^2 & x^2 & y^2 \\ e & y^2 & x^2y & xy & x & y & xy^2 & x^2y^2 & x^2 \\ e & x^2 & y^2 & x^2y & xy & x & y & xy^2 & x^2y^2 \\ e & x^2y^2 & x^2 & y^2 & x^2y & xy & x & y & xy^2 \\ e & xy^2 & x^2y^2 & x^2 & y^2 & x^2y & xy & x & y \\ e & y & xy^2 & x^2y^2 & x^2 & y^2 & x^2y & xy & x \end{pmatrix}$$

where $G = \{x, y | x^3 = 1, y^3 = 1, xy = yx\}$.

Cokernel (GW(10,9, G)):

$$\begin{pmatrix}
0 & e & e & e & e & e & e & e & e & e \\
e & 0 & e & \omega^4 & \omega & \omega^7 & \omega^6 & \omega^5 & \omega^2 & \omega^3 \\
e & \omega^4 & 0 & e & \omega^6 & \omega & \omega^7 & \omega^3 & \omega^5 & \omega^2 \\
e & e & \omega^4 & 0 & \omega^7 & \omega^6 & \omega & \omega^2 & \omega^3 & \omega^5 \\
e & \omega^5 & \omega^2 & \omega^3 & 0 & e & \omega^4 & \omega & \omega^7 & \omega^6 \\
e & \omega^3 & \omega^5 & \omega^2 & \omega^4 & 0 & e & \omega^6 & \omega & \omega^7 \\
e & \omega^2 & \omega^3 & \omega^5 & e & \omega^4 & 0 & \omega^7 & \omega^6 & \omega \\
e & \omega & \omega^7 & \omega^6 & \omega^5 & \omega^2 & \omega^3 & 0 & e & \omega^4 \\
e & \omega^6 & \omega & \omega^7 & \omega^3 & \omega^5 & \omega^2 & \omega^4 & 0 & e \\
e & \omega^7 & \omega^6 & \omega & \omega^2 & \omega^3 & \omega^5 & e & \omega^4 & 0
\end{pmatrix}$$

where $G = C_8 = \{\omega | \omega^8 = 1\}$.

Skew symmetric weighing matrix:

$$\begin{pmatrix}
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-\\
0&0&0&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0\\
0&0&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0&0&-&0&0\\
-&0&0&0&0&0&0&0&1&0&0&0&-&0&0&0&0&0&0&-&0&1&0&0&0&0&1&0&0&0&0&1&0&0&-&0&0&-&0&0\\
0&0&0&1&0&0&0&0&0&0&0&-&0&0&0&1&0&0&-&0&1&0&0&0&0&1&0&0&0&0&1&0&0&-&0&0&-&0&0&0\\
0&0&1&0&0&0&0&0&0&0&-&0&0&0&1&0&0&-&0&0&0&0&0&-&1&0&0&0&0&1&0&0&-&0&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0&-&0&0&0&1&0&0&-&0&0&0&0&0&-&0&0&0&0&-&1&0&0&0&0&0&0&1&0&0&1&0\\
-&0&0&0&-&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&-&0&1&0&0&0&-&0&0&0&0&0&1&0&0&-&0\\
0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&-&0&1&0&0&0&0&-&0&1&0&0&0&-&0&0&0&0&0&1&0&0&-&0&0\\
0&0&1&0&0&0&1&0&0&0&0&0&0&0&-&0&1&0&0&0&0&-&0&0&0&0&0&-&0&0&0&1&0&1&0&0&-&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&-&0&0&0&0&0&-&-&0&0&0&0&0&-&0&0&0&1&0&1&0&0&0&0&0&0&1\\
-&0&0&0&1&0&0&0&-&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&-&0&0&-&0&0&-&0&0&0&0&0&1\\
0&0&0&1&0&0&0&-&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&-&0&0&-&0&0&-&0&0&0&0&0&1&0\\
0&0&1&0&0&0&-&0&0&0&1&0&0&0&0&0&0&0&0&-&1&0&0&0&0&-&0&0&-&0&0&0&0&0&0&1&0&1&0&0\\
0&1&0&0&0&-&0&0&0&1&0&0&0&0&0&0&0&0&-&0&0&0&0&-&-&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0\\
-&0&0&0&0&0&0&1&0&0&-&0&0&-&0&0&0&0&0&0&1&0&0&0&-&0&0&0&0&0&0&-&0&1&0&0&0&0&1&0\\
0&0&0&1&0&0&1&0&0&-&0&0&-&0&0&0&0&0&0&0&0&0&0&-&0&0&0&1&0&0&-&0&1&0&0&0&0&1&0&0\\
0&0&1&0&0&1&0&0&-&0&0&0&0&0&0&1&0&0&0&0&0&0&-&0&0&0&1&0&0&-&0&0&0&0&0&-&1&0&0&0\\
0&1&0&0&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&-&0&0&0&1&0&0&-&0&0&0&0&0&-&0&0&0&0&-\\
-&0&0&0&0&-&0&0&0&0&0&1&0&0&-&0&-&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&-&0&1&0&0\\
0&0&0&1&-&0&0&0&0&0&1&0&0&-&0&0&0&0&0&1&0&0&0&0&0&0&0&-&0&1&0&0&0&0&-&0&1&0&0&0\\
0&0&1&0&0&0&0&1&0&1&0&0&-&0&0&0&0&0&1&0&0&0&0&0&0&0&-&0&1&0&0&0&0&-&0&0&0&0&0&-\\
0&1&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&-&0&0&0&0&0&-&-&0&0&0&0&0&-&0\\
-&0&0&0&0&0&-&0&0&-&0&0&0&0&0&1&1&0&0&0&-&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&-\\
0&0&0&1&0&-&0&0&-&0&0&0&0&0&1&0&0&0&0&-&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&-&0\\
0&0&1&0&-&0&0&0&0&0&0&1&0&1&0&0&0&0&-&0&0&0&1&0&0&0&0&0&0&0&0&-&1&0&0&0&0&-&0&0\\
0&1&0&0&0&0&0&1&0&0&1&0&1&0&0&0&0&-&0&0&0&1&0&0&0&0&0&0&0&0&-&0&0&0&0&-&-&0&0&0\\
-&0&0&0&0&0&0&-&0&1&0&0&0&0&1&0&0&0&0&1&0&0&-&0&0&-&0&0&0&0&0&0&1&0&0&0&-&0&0&0\\
0&0&0&1&0&0&-&0&1&0&0&0&0&1&0&0&0&0&1&0&0&-&0&0&-&0&0&0&0&0&0&0&0&0&0&-&0&0&0&1\\
0&0&1&0&0&-&0&0&0&0&0&-&1&0&0&0&0&1&0&0&-&0&0&0&0&0&0&1&0&0&0&0&0&0&-&0&0&0&1&0\\
0&1&0&0&-&0&0&0&0&0&-&0&0&0&0&-&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&-&0&0&0&1&0&0\\
-&0&0&0&0&0&1&0&0&0&0&-&0&1&0&0&0&-&0&0&0&0&0&1&0&0&-&0&-&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&1&0&1&0&0&0&0&-&0&1&0&0&0&-&0&0&0&0&0&1&0&0&-&0&0&0&0&0&1&0&0&0&0&0&0&0&-\\
0&0&1&0&1&0&0&0&0&-&0&0&0&0&0&-&0&0&0&1&0&1&0&0&-&0&0&0&0&0&1&0&0&0&0&0&0&0&-&0\\
0&1&0&0&0&0&0&-&-&0&0&0&0&0&-&0&0&0&1&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&-&0&0\\
-&0&0&0&0&1&0&0&0&0&1&0&0&0&0&-&0&0&-&0&0&-&0&0&0&0&0&1&1&0&0&0&-&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&-&0&0&-&0&0&-&0&0&0&0&0&1&0&0&0&0&-&0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&0&-&1&0&0&0&0&-&0&0&-&0&0&0&0&0&0&1&0&1&0&0&0&0&-&0&0&0&1&0&0&0&0&0\\
0&1&0&0&0&0&-&0&0&0&0&-&-&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0&0&-&0&0&0&1&0&0&0&0&0&0
\end{pmatrix}$$

Hadamard matrix:

$$
\left(\begin{array}{*{40}{c}}
1&1&1&1&1&-&-&-&1&-&-&-&1&-&-&-&1&-&-&-&1&-&-&-&1&-&-&-&1&-&-&-&1&-&-&-&1&-&-&- \\
1&-&1&-&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1 \\
1&1&-&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&- \\
1&-&-&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1&1&-&1&1 \\
-&1&1&1&1&1&1&1&1&-&-&-&-&1&1&1&-&-&-&-&1&1&-&-&1&1&1&-&1&1&1&1&-&-&-&1&-&-&1&1 \\
-&-&1&-&1&-&1&-&1&1&-&1&-&-&1&-&1&-&1&-&-&1&1&-&1&-&1&1&-&1&-&1&-&1&-&-&1&-&-&1 \\
-&-&-&1&1&1&-&-&1&1&1&-&-&-&-&1&1&1&-&-&1&1&1&1&-&1&1&1&-&-&1&1&1&-&-&-&-&-&-&- \\
-&1&-&-&1&-&-&1&1&-&1&1&-&1&-&-&-&1&1&-&-&1&-&1&-&-&1&-&1&-&-&1&1&1&-&1&1&-&1&- \\
-&1&1&1&-&1&1&1&1&1&1&1&1&-&-&-&1&1&1&-&-&-&-&-&1&1&-&-&-&-&1&1&1&1&1&1&-&-&-&1 \\
-&-&1&-&-&-&1&-&1&-&1&-&1&1&-&1&1&-&1&1&1&-&1&-&-&1&1&-&1&-&-&1&-&1&-&1&-&1&-&- \\
-&-&-&1&-&-&-&1&1&1&-&-&1&1&1&-&-&1&1&1&1&1&-&-&1&1&1&1&-&-&-&-&-&-&1&1&1&-&-&- \\
-&1&-&-&-&1&-&-1&1&-&-&1&1&-&1&1&-&-&1&-&-&1&1&-&-&1&-&1&1&-&1&-&1&-&-&1&1&1&-&1 \\
-&1&1&1&1&-&-&-&-&1&1&1&1&1&1&1&1&1&-&-&1&1&1&-&-&-&-&-&-&-&-&1&-&-&1&1&1&1&1&1 \\
-&-&1&-&1&1&-&1&-&-&1&-&1&-&1&-&-&1&1&-&1&-&1&1&1&-&1&-&-&1&-&-&1&-&-&1&-&1&-&1 \\
-&-&-&1&1&1&1&-&-&-&-&1&1&1&-&-&1&1&1&1&-&1&1&1&1&1&-&-&1&-&-&-&-&-&-&-&-&-&1&1 \\
-&1&-&-&1&-&1&1&-&1&-&-&1&-&-&1&-&1&-&1&-&-&1&-&-&1&1&-&1&1&-&1&1&-&1&-&1&-&-&1 \\
-&1&1&1&1&1&1&1&-&-&-&1&-&-&1&1&1&1&1&1&1&-&-&-&-&1&1&1&-&-&-&-&1&1&-&-&1&1&1&- \\
-&-&1&-&-&1&-&1&-&1&-&-&1&-&-&1&1&-&1&-1&1&1&-&1&-&-&1&-&1&-&1&-&-&1&1&-&1&-&1&1 \\
-&-&-&1&-&-&1&1&1&-&-&-&-&-&-&-&1&1&-&-&1&1&1&-&-&-&-1&1&1&1&-&-&1&1&1&1&-&1&1&1 \\
-&1&-&-&1&-&-&1&1&1&-&1&1&-&1&-&1&-&-&1&1&-&1&1&-&1&-&-&-&1&1&-&-&1&-&1&-&-&1&- \\
-&1&1&1&-&-&1&1&1&1&1&1&-&-&-&1&-&1&1&1&1&1&1&1&1&-&-&-&1&1&1&-&-&-&-&-&1&1&-&- \\
-&-&1&-&1&-&-&1&-&1&-&1&-&1&-&-&-&-&1&-&1&-&1&-&1&1&-&1&1&-&1&1&1&-&1&-&-&1&1&- \\
-&-&-&1&-&-&-&-&-&-&1&1&1&-&-&-&-&-&-&1&1&1&-&-&1&1&1&-&-&1&1&1&1&1&-&-&1&1&1&1 \\
-&1&-&-&1&-&1&-&1&-&-&1&1&1&-&1&-&1&-&-&1&-&-&1&1&-&1&1&-&-&1&-&-&1&1&-&-&1&-&1 \\
-&1&1&1&-&-&-&1&-&-&1&1&1&1&1&1&1&-&-&-&-&1&1&1&1&1&1&1&1&1&-&-&1&1&1&-&-&-&-&- \\
-&-&1&-&-&1&-&-&1&-&-&1&-&1&-&1&1&1&-&1&-&-&1&-&1&-&1&-&-&1&1&-&1&-&1&1&1&-&1&- \\
-&-&-&1&1&-&-&-&-&-&-&-&-&-&1&1&1&1&1&-&-&-&-&1&1&1&-&-&1&1&1&1&-&1&1&1&1&1&-&- \\
-&1&-&-&1&1&-&1&1&-&1&-&1&-&-&1&1&-&1&1&-&1&-&-&1&-&-&1&-&1&-&1&-&-&1&-&-&1&1&- \\
-&1&1&1&-&-&-&-&1&1&-&-&1&1&1&-&1&1&1&1&-&-&-&1&-&-&1&1&1&1&1&1&1&-&-&-&-&1&1&1 \\
-&-&1&-&1&-&1&-&-&1&1&-&1&-&1&1&-&1&-&1&-&1&-&-&1&-&-&1&1&-&1&-&1&1&-&1&-&-&1&- \\
-&-&-&1&1&1&-&-&1&1&1&1&-&1&1&1&-&-&1&1&1&-&-&-&-&-&-&-&1&1&-&-&1&1&1&-&-&-&-&1 \\
-&1&-&-&-&1&1&-&-&1&-&1&-&-&1&-&1&-&-&1&1&1&-&1&1&-&1&-&1&-&-&1&1&-&1&1&-&1&-&- \\
-&1&1&1&1&1&1&-&-&-&-&-&1&1&-&-&-&-&1&1&1&1&1&1&-&-&-&1&-&1&1&1&1&1&1&1&1&-&-&- \\
-&-&1&-&1&-&1&1&1&-&1&-&-&1&1&-&1&-&-&1&-&1&-&1&-&1&-&-&-&-&1&-&1&-&1&-&1&1&-&1 \\
-&-&-&1&-&1&1&1&1&1&-&-&1&1&1&1&-&-&-&-&-&-&1&1&1&-&-&-&-&-&-&1&1&1&-&-&1&1&1&- \\
-&1&-&-&-&-&1&-1&-&1&1&-&-&1&-&1&1&-&1&-&1&-&-&1&1&1&-&1&-&1&-&-&1&-&-&1&1&-&1&1 \\
-&1&1&1&1&1&-&-&1&1&1&-&-&-&-&-&-&-&-&1&-&-&1&1&1&1&1&1&1&-&-&-&-&1&1&1&1&1&1&1 \\
-&-&1&-&-&1&1&-&1&-&1&1&1&-&1&-&-&1&-&-&1&-&-&1&-&1&-&1&1&1&-&1&-&-&1&-&1&-&1&- \\
-&-&-&1&1&1&1&1&-&1&1&1&1&1&-&-&1&-&-&-&-&-&-&-&-&-&1&1&1&1&1&-&-&-&-&1&1&1&-&- \\
-&1&-&-&-&1&-&1&-&-&1&-&-&1&1&-&1&1&-&1&1&-&1&-&1&-&-&1&1&-&1&1&-&1&-&-&1&-&-&1
\end{array}\right)
$$

A.7.2 right nearfield plane

We include only the right nearfield plane, since the matrices for the left nearfield can be found from the matrices for the right nearfield (by transposition of the incidence matrix).

Kernel $(GH(9,G))$

$$\begin{pmatrix}
e & e & e & e & e & e & e & e & e \\
e & x^2 & x & y^2 & x^2y^2 & xy^2 & y & x^2y & xy \\
e & x & x^2 & y & xy & x^2y & y^2 & xy^2 & x^2y^2 \\
e & y & y^2 & x^2 & xy^2 & xy & x & x^2y^2 & x^2y \\
e & xy & x^2y^2 & x^2y & x^2 & y^2 & xy^2 & y & x \\
e & x^2y & xy^2 & x^2y^2 & y & x^2 & xy & x & y^2 \\
e & y^2 & y & x & x^2y & x^2y^2 & x^2 & xy & xy^2 \\
e & xy^2 & x^2y & xy & y^2 & x & x^2y^2 & x^2 & y \\
e & x^2y^2 & xy & xy^2 & x & y & x^2y & y^2 & x^2
\end{pmatrix}$$

where $G = \{x, y | x^3 = 1, y^3 = 1, xy = yx\}$.

Cokernel (GW(10,9,G));

$$\begin{pmatrix}
0 & e & e & e & e & e & e & e & e & e \\
e & 0 & e & B^2 & B^3 & C & CB^3 & B & CB & CB^2 \\
e & B^2 & 0 & e & CB^3 & B^3 & C & CB^2 & B & CB \\
e & e & B^2 & 0 & C & CB^3 & B^3 & CB & CB^2 & B \\
e & B & CB & CB^2 & 0 & e & B^2 & B^3 & C & CB^3 \\
e & CB^2 & B & CB & B^2 & 0 & e & CB^3 & B^3 & C \\
e & CB & CB^2 & B & e & B^2 & 0 & C & CB^3 & B^3 \\
e & B^3 & C & CB^3 & B & CB & CB^2 & 0 & e & B^2 \\
e & CB^3 & B^3 & C & CB^2 & B & CB & B^2 & 0 & e \\
e & C & CB^3 & B^3 & CB & CB^2 & B & e & B^2 & 0
\end{pmatrix}$$

where $G = \{B, C | B^4 = 1 \; C^4 = 1 \; C^2 = B^2 \; BC = CB^3\}$.

A.7.3 Hughes plane

Kernel $GPH(9,9)$

$$\begin{pmatrix}
e & e & e & e & e & e & e & e & e \\
e & x^3 & xy^4 & x^7y^4 & x^4y^4 & y^2x^8 & y^2x^2 & y^2x^5 & x^6 \\
e & x^8y^2 & x^4y^2 & y^4x^5 & x^2y^2x & xy^3x & y^2x^2y & yx^8y^2 & y^4x \\
e & x^2y^2 & x^2y^2x & x & y^4x^8 & y^4x^7y & y & x^2y^3 & y^4x^7y \\
e & x^5y^2 & y^4x^2 & x^2y^2x & x^7 & y^5x & x^7y^5 & x^4y^5xy^4 & y^4x^4 \\
e & yx^2y & x^7y^2 & x^2y^4x^4 & x^2 & y^5 & yx^2 & y^4x^8y^3 & y^4x^8y^4 \\
e & x^2y^4x^5 & x^2y^4x^4 & x^8 & xy^2 & xy^3 & x^8y & x^5y^3x^2 & y^4x^5y^4 \\
e & x^2y^4x^8 & x^5 & x^4y^2 & x^2y^4x^4 & y^3x^7 & x^4y^5xy^4 & y^3x^2y^4 & y^4x^2y^4 \\
e & x^6 & y^2x^8 & y^2x^2 & y^2x^5 & xy^4 & x^7y^4 & x^7y^4 & x^3
\end{pmatrix}$$

Where x is the permutation $(1,5,7,3,4,9,2,6,8)$ and y is $(1,4)(2,5)(3,6)(7,8,9)$, which generate a subgroup of S_9 of order 162.

Cokernel $GPW(10,9,8)$:

$$\begin{pmatrix}
0 & e & e & e & e & e & e & e & e & e \\
e & 0 & A & B & C & D & E & F & G & H \\
e & B & 0 & A & E & C & D & H & F & G \\
e & A & B & 0 & D & E & C & G & H & F \\
e & S & T & U & 0 & V & W & X & Y & Z \\
e & U & S & T & W & 0 & V & Z & X & Y \\
e & T & U & S & V & W & 0 & Y & Z & X \\
e & \mathfrak{A} & \mathfrak{B} & \mathfrak{C} & \mathfrak{D} & \mathfrak{E} & \mathfrak{F} & 0 & \mathfrak{G} & \mathfrak{H} \\
e & \mathfrak{C} & \mathfrak{A} & \mathfrak{B} & \mathfrak{F} & \mathfrak{D} & \mathfrak{E} & \mathfrak{H} & 0 & \mathfrak{G} \\
e & \mathfrak{B} & \mathfrak{C} & \mathfrak{A} & \mathfrak{E} & \mathfrak{F} & \mathfrak{D} & \mathfrak{G} & \mathfrak{H} & 0
\end{pmatrix}$$

The permutations as follows:

$A = (1,8)(2,4,3)(5,6)$

$B = (2,7,4,6)(3,5)$

$C = (1,4,8,7,3,6)$

$D = (1,2,8,5)(4,7,6)$

$E = (1,3,8,6,7)(2,5)$

$F = (1,6,8,3,7,5,4,2)$

$G = (1,5,7,8,2,6,3,4)$

$H = (1,7,2,3)(4,5,8)$

$S = (1,7,2,3,6,8,4)$

$T = (1,6,7,8,3)(2,5,4)$

$U = (1,5,8,2)(3,4,7,6)$

$V = (1,8)(2,6)(3,7,4,5)$

$W = (2,4,3)(5,7)$ $\mathfrak{A} = (1,3,7,5,2,8,6)$ $\mathfrak{E} = (1,7,8,4,2)(3,5,6)$

$X = (1,2,7,3,8,5,6)$ $\mathfrak{B} = (1,4,5)(3,8,7)$ $\mathfrak{F} = (1,6,5,8,3,4)(2,7)$

$Y = (1,3,5)(4,8,6)$ $\mathfrak{C} = (1,2,6,4,8,5,7)$ $\mathfrak{G} = (1,8)(2,5,3,6)(4,7)$

$Z = (1,4,6,5,2,8,7)$ $\mathfrak{D} = (1,5,4,6,8,2,3)$ $\mathfrak{H} = (2,4,3)(6,7)$

A different kernel (found in [47])

$$\begin{pmatrix} e & e & e & e & e & e & e & e & e \\ e & a_1 & b_1 & c_1 & d_1 & e_1 & f_1 & g_1 & h_1 \\ e & a_2 & b_2 & c_2 & d_2 & e_2 & f_2 & g_2 & h_2 \\ e & a_3 & b_3 & c_3 & d_3 & e_3 & f_3 & g_3 & h_3 \\ e & a_4 & b_4 & c_4 & d_4 & e_4 & f_4 & g_4 & h_4 \\ e & a_5 & b_5 & c_5 & d_5 & e_5 & f_5 & g_5 & h_5 \\ e & a_6 & b_6 & c_6 & d_6 & e_6 & f_6 & g_6 & h_6 \\ e & a_7 & b_7 & c_7 & d_7 & e_7 & f_7 & g_7 & h_7 \\ e & a_8 & b_8 & c_8 & d_8 & e_8 & f_8 & g_8 & h_8 \end{pmatrix}$$

The permutations as follows:

$a_1 = (1,8,5,2)(3,7,6)(4,9)$ $a_2 = (1,9,3)(2,7)(4,8)(5,6)$ $a_3 = (1,5,7,4)(2,3,8)(6,9)$

$b_1 = (1,4,2,6,5,7,3,9,8)$ $b_2 = (1,7,8,6)(2,9)(3,5,4)$ $b_3 = (1,8,4,9,7,5,6,3,2,1)$

$c_1 = (1,9,3,8,2,7,5,6,4)$ $c_2 = (1,2,6,8)(3,4,5)(7,9)$ $c_3 = (1,3)(2,9,4,7,6)(5,8)$

$d_1 = (1,6,2,8,3,4,5,9,7)$ $d_2 = (1,4,2,5)(3,6,7)(8,9)$ $d_3 = (1,9,3,5,4,8,7,2,6)$

$e_1 = (1,7,2,9,5,8,4,3,6)$ $e_2 = (1,5,7,4)(2,3,8)(6,9)$ $e_3 = (1,4,6,8,9)(2,5)(3,7)$

$f_1 = (1,5)(2,3)(4,8,9,6,7)$ $f_2 = (1,3,9)(2,4,6)(5,8,7)$ $f_3 = (1,7)(2,8,6,5,9)(3,4)$

$g_1 = (1,3)(2,5,4,6,9)(7,8)$ $g_2 = (1,6,4,7)(2,8,3)(5,9)$ $g_3 = (1,2,4,5,3,6,7,9,8)$

$h_1 = (1,2,4,7,9)(3,5)(6,8)$ $h_2 = (1,8,5,2)(3,7,6)(4,9)$ $h_3 = (1,6,4,2,7,8,3,9,5)$

$a_4 = (1,4,2,5)(3,6,7)(8,9)$

$b_4 = (1,3)(2,8,7,9,5)(4,6)$

$c_4 = (1,6,5,9,2,4,8,3,7)$

$d_4 = (1,5,8,6,9)(2,3)(4,7)$

$e_4 = (1,9,3,4,5,6,2,7,8)$

$f_4 = (1,2)(3,5)(4,9,7,6,8)$

$g_4 = (1,8,5,7,2,6,3,9,4)$

$h_4 = (1,7,5,4,3,8,2,9,6)$

$a_5 = (1,7,8,6)(2,9)(3,5,4)$

$b_5 = (1,6,2,5,9)(3,8)(4,7)$

$c_5 = (1,4,6,7,3,2,8,9,5)$

$d_5 = (1,3)(2,4,9,6,8)(5,7)$

$e_5 = (1,2,6,4,8,5,3,9,7)$

$f_5 = (1,8)(2,7,9,4,5)(3,6)$

$g_5 = (1,9,3,7,6,5,8,4,2)$

$h_5 = (1,5,6,9,8,7,2,3,4)$

$a_6 = (1,6,4,7)(2,8,3)(5,9)$

$b_6 = (1,9,3,6,7,2,4,8,5)$

$c_6 = (1,5,7,8,4,2,3,9,6)$

$d_6 = (1,2,7,9,4,6,5,3,8)$

$e_6 = (1,8,7,6,3,5,4,9,2)$

$f_6 = (1,4)(2,5,6,9,8)(3,7)$

$g_6 = (1,7,5,2,9)(3,4)(6,8)$

$h_6 = (1,3)(2,6)(4,5,8,9,7)$

$a_7 = (1,2,6,8)(3,4,5)(7,9)$

$b_7 = (1,5,8,2,3,7,6,9,4)$

$c_7 = (1,8,7,4,9)(2,5)(3,6)$

$d_7 = (1,7,8,5,6,4,3,9,2)$

$e_7 = (1,3)(2,4)(5,9,8,6,7)$

$f_7 = (1,6)(2,9,5,4,7)(3,8)$

$g_7 = (1,4,8,9,6,2,7,3,5)$

$h_7 = (1,9,3,2,8,4,6,5,7)$

$a_8 = (1,3,9)(2,4,6)(5,8,7)$

$b_8 = (1,2,7)(3,4,5)(6,8,9)$

$c_8 = (1,7,2)(3,5,4)(6,9,8)$

$d_8 = (1,8,4)(2,9,5)(3,7,6)$

$e_8 = (1,6,5)(2,8,3)(4,7,9)$

$f_8 = (1,9,3)(2,6,4)(5,7,8)$

$g_8 = (1,5,6)(2,3,8)(4,9,7)$

$h_8 = (1,4,8)(2,5,9)(3,6,7)$

Baer-kernel($GW(13,9,G)$):

$$\begin{pmatrix}
0 & x^2y & 1 & y & 0 & 1 & 1 & xy & x^2y & xy & 0 & y & 0 \\
0 & 0 & x^2y & 1 & y & 0 & 1 & 1 & xy & x^2y & xy & 0 & y \\
y & 0 & 0 & x^2y & 1 & y & 0 & 1 & 1 & xy & x^2y & xy & 0 \\
0 & y & 0 & 0 & x^2y & 1 & y & 0 & 1 & 1 & xy & x^2y & xy \\
xy & 0 & y & 0 & 0 & x^2y & 1 & y & 0 & 1 & 1 & xy & x^2y \\
x^2y & xy & 0 & y & 0 & 0 & x^2y & 1 & y & 0 & 1 & 1 & xy \\
xy & x^2y & xy & 0 & y & 0 & 0 & x^2y & 1 & y & 0 & 1 & 1 \\
1 & xy & x^2y & xy & 0 & y & 0 & 0 & x^2y & 1 & y & 0 & 1 \\
1 & 1 & xy & x^2y & xy & 0 & y & 0 & 0 & x^2y & 1 & y & 0 \\
0 & 1 & 1 & xy & x^2y & xy & 0 & y & 0 & 0 & x^2y & 1 & y \\
y & 0 & 1 & 1 & xy & x^2y & xy & 0 & y & 0 & 0 & x^2y & 1 \\
1 & y & 0 & 1 & 1 & xy & x^2y & xy & 0 & y & 0 & 0 & x^2y \\
x^2y & 1 & y & 0 & 1 & 1 & xy & x^2y & xy & 0 & y & 0 & 0
\end{pmatrix}$$

where $x = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$, and $y = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$.

Bibliography

[1] E. Ademaj, *On the classification of projective planes of order 15 with a Frobenius group of order 30 as a collineation group*, Archiv der Mathematik, 45 (1985), pp. 86–96.

[2] E. Artin, *Geometric Algebra*, Interscience Tracts in Pure and Applied Mathematics, Interscience Publishers, Inc, New York, 1957.

[3] E. Assmus, Jr and J. Key, *Affine and projective planes*, Discrete Mathematics, 83 (1990), pp. 161–187.

[4] ——, *Translation planes and derivation sets*, Journal of Geometry, 37 (1990), pp. 3–16.

[5] ——, *Hadamard matrices and their designs: A coding theory approach*, Transactions of the American Mathematical Society, 330 (1992), pp. 269–293.

[6] A. Barlotti, *Le possibili configurazioni del sistema delle coppie punto-retta* (a, a) *per cui un piano grafico risulta* (a, a)*-transitivo.*, Boll. Un. Mat. Ital., 12

(1957), pp. 212–226.

[7] L. Batten and M. Davidson, *Skew arcs and Wagners [23,14,5] code.* to appear in Journal of Combinatorial Mathematics and Combinatorial Computing.

[8] L. Batten, M. Davidson, and L. Storme, *An analysis of Chen's construction of minimum distance five codes*, IEEE Trans. Inform. Theory, 46 (2000), pp. 505–511.

[9] L. M. Batten, *The combinatorics of points and lines*, Congressus Numerantium, 75 (1990), pp. 51–62.

[10] ——, *Combinatorics of finite geometries*, Cambridge University Press, second ed., 1997.

[11] J. H. Beder, *Conjectures about Hadamard matrices*, Journal of Statistical Planning and Inference, 72 (1998), pp. 7–14.

[12] A. Beutelspacher and U. Rosenbaum, *Projective Geometry from foundations to applications*, Cambridge University press, United Kingdom, 1998.

[13] A. Bonisoli, *On collineation groups of finite planes.* preprint.

[14] S. Bourn, *A canonical form for incidence matrices of finite projective planes and their associated latin squares and planar ternary rings*, in Combinatori-

cal Mathematics X, L. Casse, ed., no. 1036 in Lecture Notes in Mathematics, Springer-Verlag, 1982, pp. 111–120.

[15] A. Brouwer and T. Verhoeff, *An updated table of minimun-distance bounds for binary linear codes*, IEEE Transactions on Information Theory, 39 (1993), pp. 662–677.

[16] A. A. Bruen, L. Haddad, and D. L. Wehlau, *Binary codes and caps*, J. Combin. Des., 6 (1998), pp. 275–284.

[17] A. A. Bruen and D. L. Wehlau, *Codes, caps, graphs coloring and line-free sets in projective space.* talk given at 'Combinatorics 96' in Assisi, Italy.

[18] ——, *Long binary linear codes and large caps in projective space*, Des. Codes. Cryptogr., 17 (1999), pp. 37–60.

[19] F. Buetkenhout, *Handbook of Incidence Geometry*, Elsevier, Netherlands, 1995.

[20] A. Butson, *Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences*, Canadian Journal of Mathematics, 15 (1963), pp. 42–48.

[21] A. T. Butson, *Generalized Hadamard matrices*, Proceedings of the American Mathematics Society, 13 (1962), pp. 894–898.

[22] P. Ceccherini and G. Tallini, *Codes, caps and linear spaces*, London Math. Soc. Lecture Notes Ser., 49 (1981), pp. 72–80.

[23] C. L. Chen, *Construction of some binary linear codes of minimum distance five*, IEEE Trans. Inform. Theory, 37 (1991), pp. 1429–1432.

[24] W. E. Clark, *Blocking sets in finite projective spaces and uneven binary codes*, Discrete Mathematics, 94 (1991), pp. 65–68.

[25] C. J. Colbourn and J. H. Dinitz, *Mutually othogonal latin squares: A brief survey of constructions*, Journal of Statistical Planning and Inference, 95 (2001), pp. 9–48.

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

[27] H. Coxeter, *Projective Geometry*, University of Toronto Press, Canada, second ed., 1974.

[28] R. Craigen, *Constructions for Orthogonal Matrices*, PhD thesis, University of Waterloo, 1991.

[29] ——, *Equivalence classes of inverse orthogonal and unit Hadamard matrices*, Bulletin of The Australian Mathematical Society, 44 (1991), pp. 109–115.

[30] ——, *Weighing matrices from generalized Hadamard matrices by 2-adjugation*, Journal of Combinatorial Mathematics and Combinatorial Computing, 10 (1991), pp. 193–200.

[31] ——, *Matrices equivalent to their transpose by permautation*, Congressus Numeranitium, 86 (1992), pp. 33–41.

[32] ——, *Trace, symmetry and orthogonality*, Canadian Mathematical Bulletin, 37 (1994), pp. 461–467.

[33] R. Craigen and W. Wallis, *Hadamard matrices: 1893-1993*, Congressus Numeranitium, 97 (1993), pp. 99–129.

[34] R. Craigen and R. Woodford, *Power Hadamard matrices.* to appear in Discrete Mathematics, 2005.

[35] T. Czerwinski, *On finite projective planes with a single* (p, l) *transitivity*, Journal of Combinatorial Theory, Series A, 48 (1988), pp. 136–138.

[36] A. Davydov and L. Tombak, *Quasiperfect linear binary codes with distance 4 and complete caps in projective geometry*, Problems of Information Transmission, 25 (1990), pp. 265–275.

[37] J. Dawson and W. de Laŭney, *A note on the construction of* $GH(4tq; EA(q))$ *for* $t = 1, 2$, Australasian Journal of Combinatorics, 6 (1992), pp. 177–186.

[38] W. de Launey, *Generalised Hadamard matrices whose rows and columns form a group*, Lecture Notes in Mathematics, (1983), pp. 154–176.

[39] ——, *On the non-existence of generalised weighing matrices*, Ars Combinatoria, 17 (1984), pp. 117–132.

[40] ——, *A survey of generalised Hadamard matrices and difference matrices $D(k, \lambda; G)$ with large k*, Utilitas Mathematica, 30 (1986), pp. 5–29.

[41] ——, *GBRD's: Some new constructions for difference matrices, generalised Hadamard matrices and balanced generalised weighing matrices*, Graphs and Combinatorics, 5 (1989), pp. 125–135.

[42] ——, *Circulant $GH(p^2; z_p)$ exist for all primes p*, Graphs and Combinatorics, 8 (1992), pp. 317–321.

[43] ——, *Generalised Hadamard matrices which are developed modulo a group*, Discrete Mathematics, 104 (1992), pp. 49–65.

[44] W. de Launey and J. E. Dawson, *An asymptotic result on the existence of generalised Hadamard matrices*, Journal of Combinatorial Theory Series A, 65 (1994), pp. 158–163.

[45] W. de Launey and p. Vijay Kumar, *On circulant generalised Hadamard matrices of prime order.* preprint.

[46] P. Dembowski, *Finite Geometries*, Springer-Verlag, New York, 1968.

[47] J. Dénes and A. Keedwell, *Latin Squares and Their Applications*, Academic Press, New York, 1974.

[48] P. Dey and J. Hayden, *On symmetric incidence matrices of projective planes*, Designs, Codes and Cryptography, 6 (1995), pp. 179–188.

[49] Y. Edel, *Inverting construction Y1.* preprint.

[50] A. Geramita and J. Seberry, *Orthogonal Designs: Quadratic forms and Hadamard matrices*, Lecture notes in pure and applied mathematics, Marcel Dekker Inc., New York and Basel, 1979.

[51] D. S. Gunderson, *Finite projective planes and applications in combinatorics.* Unpublished manuscript.

[52] J. Hadamard, *Resolution d'une question relative aux determinants*, Bull. Des Sciences Math., (1893), pp. 240–246.

[53] M. Hall Jr., *Combinatorial Theory*, Blaisdell Publishing Company, Waltham, Massachusetts, 1967.

[54] M. Hall, Jr., *Ternary and binary codes for a plane of order 12*, Journal of Combinatorial Theory, Series A, 36 (1984), pp. 183–203.

[55] M. Hall, Jr. and R. Roth, *On a conecture of R. H. Bruck*, Journal of Combinatorial Theory, Series A, 37 (1984), pp. 22–31.

[56] A. Hedayat and W.T.Federer, *An application of group theory to the existence and nonextence of orthogonal latin squares*, Biometrika, 56 (1969), pp. 547–551.

[57] R. Hill, *Caps and codes*, Discrete Mathematics, 22 (1978), pp. 111–137.

[58] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, second ed., 1998.

[59] D. R. Hughes and F. C. Piper, *Projective Planes*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1973.

[60] ——, *Design Theory*, Cambridge University Press, Cambridge, 1985.

[61] N. Ito, *On generalized Hadamard subsets*, Journal of Algebra, 223 (2000), pp. 601–609.

[62] W.-A. Jackson and P. R. Wild, *On GMW designs and cyclic Hadamard designs*, Designs. Codes and Cryptography, 10 (1997), pp. 185–191.

[63] Z. Janko and T. V. Trung, *The full collineation group of any projective plane of order 12 is {2,3} -group*, Geometriae Dedicata, 12 (1982), pp. 101–110.

[64] ——, *A generalization of a result of L. Baumert and M. Hall about projective planes of order 12*, Journal of Combinatorial Theory, Series A, 32 (1982), pp. 378–385.

[65] ——, *On projective planes of order 12 with an automorphism of order 13*, Geometriae Dedicata, 12 (1982), pp. 87–99.

[66] ——, *Projective planes of order 12 do not have a four group as a collineation group*, Journal of Combinatorial Theory, Series A, 32 (1982), pp. 401–404.

[67] B. C. Kestenband, *Correlations whose squares are perspectivities*, Geometriae Dedicata, 33 (1990), pp. 289–315.

[68] B. Kocay, *Groups and graphs.* Software package.

[69] C. Lam, G. Kolesova, and L. Thiel, *A computer search for finite projective planes of order 9*, Discrete Mathematics, 92 (1991), pp. 187–195.

[70] C. Lam, L. Thiel, and S. Swiercz, *The non-existence of finite projective planes of order 10*, Canadian Journal of Mathematics, 41 (1989), pp. 1117–1123.

[71] H. Lenz, *Kleiner desarguesscher satz und dualitt in projektiven ebenen.*, Jberr. Deutsch. Math. Verein., 57 (1954), pp. 20–31.

[72] J. Q. Longyear, *Certain m.o.l.s. as groups*, Proceedings of the American Mathematical Society, 36 (1972), pp. 379–384.

[73] P. Lorimer, *Some of the finite projective planes*, The Mathematical Intelligencer, 5 (1983), pp. 41–50.

[74] F. MacWilliams and N. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, The Netherlands, 1977.

[75] R. J. Mihalek, *Projective Geometry and Algebraic Structures*, Academic Press, United Kingdom, 1972.

[76] Nagell, *The diophantine equation* $x^2+7 = 2^n$, Ark. Mat., 4 (1961), pp. 185–187.

[77] T. Ostrom, *Finite Translation Planes*, vol. 158 of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1970.

[78] L. J. Paige and C. Wexler, *A canonical form for the incidence matrices of finite projective planes and their associated latin squares*, Portugaliae Math., 12 (1953), pp. 105–112.

[79] A. R. Prince, *Projecitve planes of order 12 and* $PG(3,3)$, Discrete Mathematics, 208/209 (1999), pp. 477–483.

[80] D. P. RAJKUNDLIA, *Some techniques for constucting infinite families of BIBD's*, Discrete Mathematics, 44 (1983), pp. 61–96.

[81] G. RINALDI AND F. ZIRONI, *Complete unital-derived arcs in the Hall plane of order 9*, Bulletin of the ICA, 36 (2002), pp. 29–36.

[82] J. SEBERRY, *Some remarks on generalized Hadamard matrices and theorems of Rajkundlia on SBIBDS*, Lecture Notes in Mathematics, 748 (1978), pp. 154–164.

[83] F. W. STEVENSON, *Projective Planes*, W.H. Freeman and Company, United States of America, 1972.

[84] T. J. WAGNER, *A search technique for quasi-perfect codes*, Information and control, 9 (1966), pp. 94–99.

[85] A. WINERHOF, *On the non-existence of generalized Hadamard matrices*, Journal of Statistical Planning and Inference, 84 (2000), pp. 337–342.

[86] Y. ZHANG, L. DUAN, Y. LU, AND Z. ZHENG, *Construction of generalized Hadamard matrices* $D(r^m(r+1), r^m(r+1); p)$, Journal of Statistical Planning and Inference, 104 (2002), pp. 239–258.