CIRCULANT WEIGHING MATRICES

by

Richard Martin Hain

A thesis submitted to the
Australian National University
for the Master of Science Degree
February, 1977

ACKNOWLEDGEMENTS

I wish to thank Dr L.G. Kovács for the help and encouragement he gave me; always suggesting a sharper result or a better way of expressing a concept. I also wish to thank Dr Jennifer Wallis for her encouragement and her continual interest in my work, and her student Peter Eades who together with Laci and Jennie provided a stimulating atmosphere within which to work.

I would also like to acknowledge the support of the Australian Government and the Australian National University, for the support and the facilities without which the writing of this thesis would not have been possible.

I extend special thanks to Mrs Barbara Geary who did an excellent job with the typing and who ably coped with the myriad of tasks caused by my absence overseas.

ABSTRACT

Circulant weighing matrices are matrices with entries in $\{-1, 0, 1\}$ where the rows are pairwise orthogonal and each successive row is obtained from the previous row by a fixed cyclic permutation. They are useful in solving problems where it is necessary to determine as accurately as possible, the "weight" of n "objects" in n "weighings". They have also been successfully used to improve the performance of certain optical instruments such as spectrometers and image scanners.

In this thesis I discuss the basic properties of circulant weighing matrices, prove most of the known existence results known to me at the time of writing this thesis and classify the circulant weighing matrices with precisely four nonzero entries in each row. The problem of classifying all circulant weighing matrices is related to the "cyclic projective plane problem". This relationship is established and I have devoted the final chapter of this thesis to cyclic projective planes and their relationship to circulant weighing matrices. The final theorem in this thesis yields information about equations of the kind $xy^{-2} = a$ in cyclic projective planes.

CONTENTS

CHAPTER I

HISTORY AND APPLICATIONS

When I first learned that some mathematicians spend their time studying matrices with entries from $\{-1, 0, 1\}$, my reaction was like that of a young upperclass lady to the local sanitary can collector!

Aren't matrices passê? What kind of mathematicians are these that haven't heard of linear transformations?

Why study matrices with entries in $\{-1, 0, 1\}$? How does such a study relate to the total intrastructure of mathematics?

Specifically we are interested in *weighing matrices*; orthogonal integer matrices with entries $0, 1$ or -1 which have the same number of zeros in each row. Historically the study of such matrices began with the work of James Sylvester in 1876 and Jacques Hadamard in 1893. In 1893 Hadamard [12] showed that the absolute value of an $n \times n$ determinant, all of whose entries were complex and lay within the unit disc, is no greater than $n^{\frac{1}{2}n}$. Hadamard then showed that if such a determinant attained the bound, then all the entries lie on the perimeter of the unit disc (that is, the unit circle) and the rows of the determinant are pairwise orthogonal. Thus in the case when all the entries of the determinant are real, the entries must all be either -1 or 1 and in this case Hadamard showed that either $n = 2$ or n is divisible by four. Sylvester [26] had already constructed a family of real $n \times n$ determinants with these properties when n was a power of two.

Real $n \times n$ matrices whose determinants have the above properties are called *Hadamard matrices* and are examples of weighing matrices.

Weighing matrices also arise naturally in a practical context. Suppose we have a balance which records the difference in weight between the right and the left pans. How can we determine the weight of n objects as accurately as possible in n weighings?

As an example, suppose that we have two objects of weights x_1 and x_2. Let e be the error made each time the balance is used. We suppose that e is a random variable with zero mean and variance σ^2. Make two measurements, the first with both the objects in the left pan and the second with one object in each pan. If e_1 and e_2 are the errors made in the first and second weighings respectively and if y_1 and y_2 are the first and second measurements respectively, then

(1.1) $$y_1 = x_1 + x_2 + e_1 ,$$

(1.2) $$y_2 = x_1 - x_2 + e_2 .$$

Equations (1.1) and (1.2) can be solved easily to give us estimates of x_1 and x_2. The distributions of the estimates obtained for x_1 and x_2 using this procedure have variance $\sigma^2/2$ while the variance of the distributions of the estimates of x_1 and x_2 obtained by weighing each object separately have variance σ^2.

Equations (1.1) and (1.2) may be written

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = W \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

where

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

Notice that W is a 2×2 Hadamard matrix.

In general, given an $n \times n$ weighing matrix W whose ijth entry is w_{ij}, we can define a weighing proceedure for weighing n objects in n weighings as follows. If $w_{ij} = 1$, place object j on the left pan for the *i*th weighing; if $w_{ij} = -1$, place object j on the right pan for the *i*th weighing; and if $w_{ij} = 0$, object j is not weighed in weighing i .

If we suppose that the error made each time the balance is used is a random variable e with zero mean and variance σ^2 and if W has precisely k nonzero entries in each row, then the variance of the distribution of the estimates of the weights each have variance σ^2/k . The fact that W has pairwise orthogonal rows and the same number of zeros in each row means that the resulting equations are easy to solve for the individual estimates of the weights.

This same method can be applied to measuring lengths, voltages and resistances. Apparently the "best" $n \times n$ weighing matrices are those which have the least number of zeros in each row.

Weighing matrices have also been used to improve the performance of optical instruments such as spectrometers. Spectrometers measure the intensity of a dispersed spectrum at a finite number (n say) of wavelengths.

According to Ibbett, Aspinall and Grainger [15], these n measurements are either made by one detector which scans a screen, making the n measurements sequentially or else the n measurements are made simultaneously by a detector with spatial resolution. The first method has the disadvantage of not being able to compensate for variations in the intensity of the signal, while the second approach suffers the disadvantage of a lower signal to noise ratio (Ibbett *et al* [15]).

Both Decker and Harwitt [6], and Ibbett *et al* [15] proposed a modification of the second system which improves the signal to noise ratio. This method I will illustrate by the following example.

Suppose we wish to measure the intensities x_1 and x_2 of two light beams with wavelengths λ_1 and λ_2 . As with weighing two objects the best approach is to measure their combined intensities (x_1+x_2) and the difference between their intensities (x_1-x_2) . This can be achieved by making a square mask as depicted in Figure 1.3.

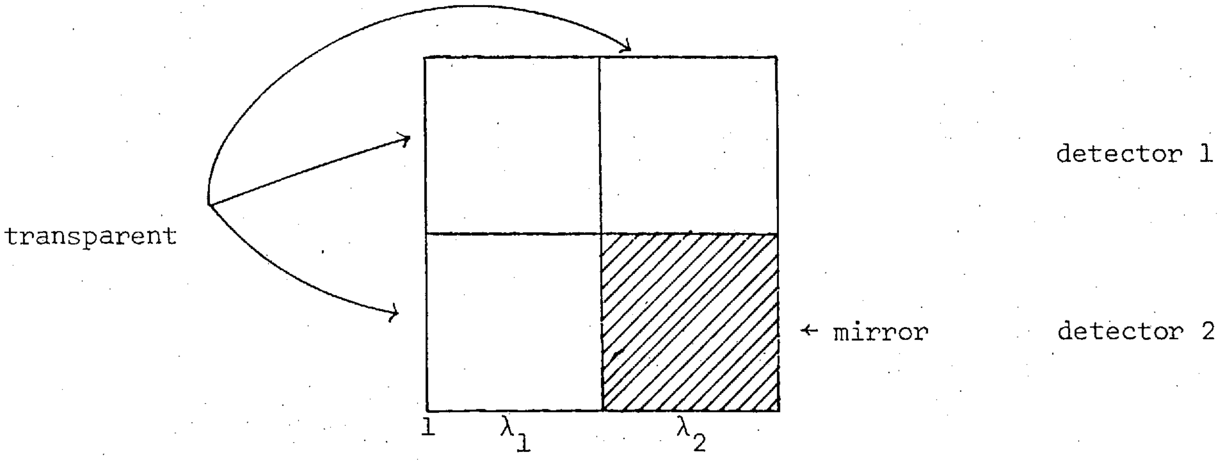


FIGURE 1.3

The bottom right hand quarter of the mask is a mirror and the other three quarters are transparent.

If the mask is positioned so that the light of wavelength λ_1 is incident with the left hand side of the mask, while the light of wavelength λ_2 is incident with the right hand side of the mask, then the detectors can be arranged so that the measurements

$$y_1 = x_1 + x_2 + e_1 \, , \quad y_2 = x_1 - x_2 + e_2 \tag{1.4}$$

can be made $(e_1$ and e_2 are the errors made when measuring $x_1 + x_2$ and $x_1 - x_2$ respectively$)$.

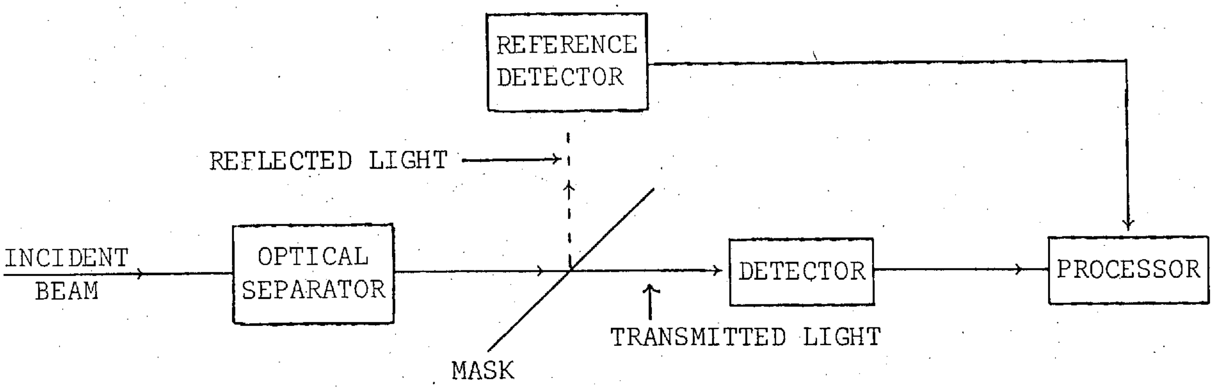


FIGURE 1.5 (after Sloane and Harwitt [24])

As in the case of the weighing problem, the variance of the distributions of the estimates of x_1 and x_2 as measured above is half the variance of the distribution of the estimates of x_1 and x_2 when measured separately.

In general, we can use an $n \times n$ weighing matrix W to define a proceedure for measuring the intensities x_i $(i = 1, \ldots, n)$ of n light beams of wavelengths $\lambda_1, \lambda_2, \ldots, \lambda_n$ as follows. First make a square $n \times n$ mask which is divided into n^2 unit squares, each of whose edges are parallel to one of the edges of the mask and such that the ijth unit square is transparent, opaque or a mirror according to whether the ijth entry w_{ij} of W is 1, 0 or -1 (see Figure 1.6).

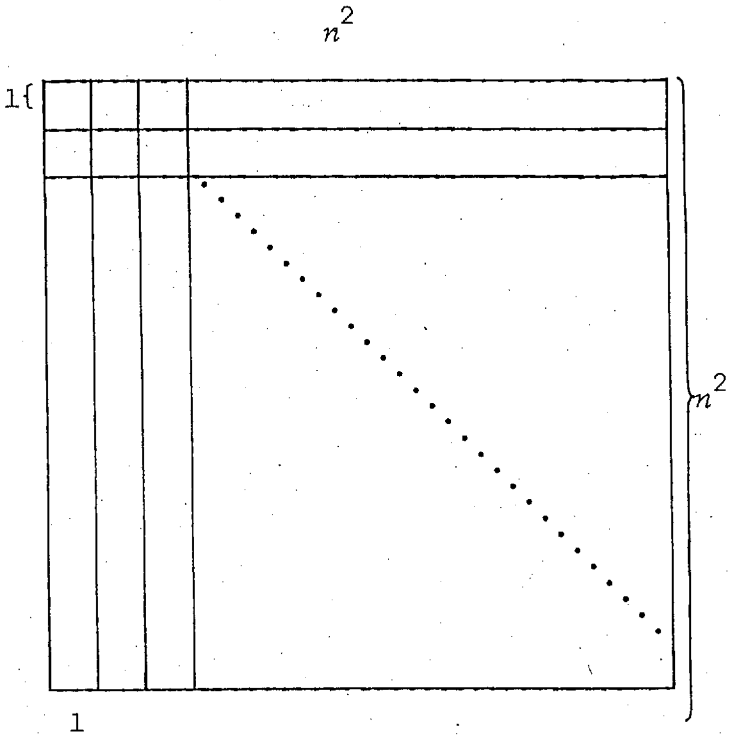


FIGURE 1.6

Now arrange the mask so that the light of wavelength λ_j is incident with the jth column of subsquares of the mask. The intensity of the light beam incident with the ijth subsquare of the mask is thus multiplied by

w_{ij} . By arranging the detectors as in Figure 1.5, the measurements

$$\sum_{j=1}^{n} w_{ij}x_j \quad (i = 1, \ldots, n)$$

can be made.

Another application of integer matrices is in modern communications theory. Student numbers, files stored in a computer and signals sent through space are all examples of information encoded into "words"; strings of symbols belonging to an "alphabet".

As an example, consider the code where the alphabet consists of the two letters 0 and 1 and all the words have length n . If we consider the set $\{0, 1\}$ as the field GF(2) of two elements, our code is a vector space of dimension n over GF(2) .

In practical situations, codewords are subject to "noise"; a codeword may be altered while travelling from its source to its destination. To reduce the effect of noise, we can introduce a redundancy into a code. A primitive error check in the above example would be to place a 0 at the end of each word if 1 occurred an even number of times in the codeword and a 1 if 1 occurred an odd number of times. That is, multiply each codeword on the right by the matrix

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

The resulting code is then an n dimensional subspace of the $n + 1$ dimensional vector space $\mathrm{GF}(2)^{n+1}$ over GF(2) . If one error occurs during the transmission of a codeword, then the resulting word is not a codeword. This code is an example of a 1-error detection code.

It is convenient to define a metric on the vector space $\mathrm{GF}(2)^m$. For an element x of $\mathrm{GF}(2)^m$, define the *weight of* x to be the number of times 1 occurs in x. Define the distance between two elements x and y of $\mathrm{GF}(2)^m$ as the weight of $x - y$.

Let r be a positive integer and suppose that we could find a subspace W of $\mathrm{GF}(2)^{n+r}$ of dimension n and an integer e such that no two elements of W were closer than $2e + 1$. If fewer than e errors were made during the transmission of a codeword, then there would be no confusion as to the codeword sent. Such a code is called an *e-error correcting code* and r is called the *redundancy* of the code. The *rate* of the code is defined as the quotient $n/(n+r)$ and when the redundancy is zero, we say that the rate of the code is at *capacity*.

What has this to do with integer matrices? If such a subspace as described above exists, then there is a linear injection

$$\varphi : \mathrm{GF}(2)^n \to \mathrm{GF}(2)^{n+r}$$

where the image of φ is the subspace W. By choosing the appropriate bases for $\mathrm{GF}(2)^n$ and $\mathrm{GF}(2)^{n+r}$, we may assume that φ has a matrix in the form

$$(I|A)$$

where I is the $n \times n$ identity matrix and A is an $n \times r$ integer matrix. The search for "good" codes then becomes a search for the right integer matrices A.

For example, if there is a Hadamard matrix of order n, then there is an $n/4$ error correcting code whose rate is $\frac{1}{2}$ (see Berlekamp [4], pp. 316-317).

For a more detailed account of coding theory, consult either Berlekamp [4] or van Lint [16].

Unfortunately we have not the time nor space to explore these applications more fully. We must away and begin the study of our *abstract nonsense*.

CHAPTER II

BASIC PROPERTIES

Here the mathematics begins. In this chapter much of the language and notation used in this thesis will be introduced. Hopefully sufficient motivation and examples will be provided to make the contents of this chapter palatable.

A *weighing matrix* of order n and weight k is an $n \times n$ matrix W with entries in $\{-1, 0, 1\}$ such that

$$WW^t = kI$$

where W^t denotes the transpose of W and I denotes the $n \times n$ identity matrix. Such a matrix has k non zero entries in each row.

If W is a non zero weighing matrix, then the weight k is a nonzero integer and W is invertible with inverse $k^{-1}W^t$. Consequently, if W is a weighing matrix, then $W^tW = kI$ and it is easy to see that each column of W contains precisely k nonzero entries. Furthermore, it is easy to see that the transpose of a weighing matrix of weight k is also a weighing matrix of weight k.

(2.1) EXAMPLE. The matrix

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

is a weighing matrix of order 6 and weight 4.

An $n \times n$ matrix A whose ijth entry is a_{ij} is *circulant* if $a_{ij} = a_{0,j-i}$ for all $i, j \in \{1, 2, \ldots, n\}$ (reduce $j - i$ modulo n).

According to Muir [17], circulant systems of linear equations were first considered by E. Catalan in 1846.

(2.2) EXAMPLE. The matrix

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

is a circulant matrix.

A circulant matrix is completely determined by its 0th row. Let $\langle x \rangle$ be a cyclic group of order n with distinguished generator x and let R be a ring with 1. Regard each element of the group ring $R\langle x \rangle$ as function α from the group $\langle x \rangle$ to the ring R $(\alpha : x^i \mapsto \alpha(x^i))$.

Consider the set of all circulant $n \times n$ matrices over R. There is a one to one correspondence between these matrices and the elements of the group ring $R\langle x \rangle$. The element of the group ring corresponding to the circulant matrix A is called the *Hall polynomial* of A and is defined as the function from $\langle x \rangle$ to R whose value at x^i is a_{0i}. It is usual to embed $\langle x \rangle$ in $R\langle x \rangle$ by identifying each element g of $\langle x \rangle$ with the characteristic function of the singleton $\{g\}$; with that identification the Hall polynomial of A is

$$\sum_{i=0}^{n-1} a_{0i} x^i .$$

(2.3) EXAMPLE. The circulant matrix

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

has Hall polynomial $1 + 2x + 3x^2$.

Denote by $\mathrm{M}_n(R)$ the R-algebra of all $n \times n$ matrices over R. Denote by P the $n \times n$ circulant matrix with Hall polynomial x. That is

$$P = \begin{pmatrix} 0 & 1 & 0 & & \cdots & & 0 \\ 0 & 0 & 1 & & \cdots & & 0 \\ 0 & 0 & 0 & 1 & \cdots & & 0 \\ \vdots & & & & & & \vdots \\ & & & & & & 0 \\ 0 & & & & \cdots & 0 & 1 \\ 1 & 0 & 0 & & \cdots & & 0 \end{pmatrix} .$$

PROPOSITION 1. *An $n \times n$ matrix commutes with P if and only it is a circulant matrix.*

Proof. Let A be an $n \times n$ matrix over R whose ijth entry is a_{ij} . The ijth entry $(AP)_{ij}$ of AP is given by

$$\sum_k a_{ik}p_{kj} = a_{i,j-1} .$$

Similarly, the ijth entry $(PA)_{ij}$ of PA is $a_{i+1,j}$.

If A is circulant, then

$$a_{i,j-1} = a_{0,j-i-1} = a_{i+1,j}$$

for all $i, j \in \{1, 2, \ldots, n\}$. That is $(AP)_{ij} = (PA)_{ij}$ for all i and j . Therefore $AP = PA$.

Conversely if $AP = PA$, then $a_{i,j-1} = a_{i+1,j}$ for all ij . A simple argument shows that $a_{ij} = a_{0,j-i}$ for all i, j ; that is A is circulant. //

Thus the $n \times n$ circulant matrices form an R-algebra, namely the centraliser of P in $\mathrm{M}_n(R)$. Let $C(P)$ denote the centraliser of P in $\mathrm{M}_n(R)$.

PROPOSITION 2. *There is an R-algebra isomorphism*

$$\varphi : C(P) \to R\langle x \rangle .$$

Proof. Let $\varphi : C(P) \to R\langle x \rangle$ be the map taking a circulant matrix to its Hall polynomial. As previously remarked, φ is a bijection.

It is clear that φ is an R-module isomorphism. We need only show that $\varphi(AB) = \varphi(A)\varphi(B)$ (where A and B are elements of $C(P)$). That is we have to show that the Hall polynomial of the product of two circulant matrices is the product of their Hall polynomials.

Let A and B be circulant matrices whose ijth entries are a_{ij} and b_{ij} respectively.

The ith entry of the 0th row of AB is $\sum_{k=0}^{n-1} a_{0k}b_{kj}$. Thus the Hall polynomial of AB is

$$\sum_{i=0}^{n-1}\left(\sum_{k=0}^{n-1} a_{0k}b_{ki}\right)x^i \text{ .}$$

Now

$$\begin{aligned}
\varphi(A)\varphi(B) &= \left(\sum_{k=0}^{n-1} a_{0k}x^k\right)\left(\sum_{j=0}^{n-1} b_{0j}x^j\right) \\
&= \sum_{k=0}^{n-1}\left(\sum_{j=0}^{n-1} a_{0k}b_{0j}x^{k+j}\right) \\
&= \sum_{k=0}^{n-1}\left(\sum_{j=0}^{n-1} a_{0k}b_{k,k+j}x^{k+j}\right) \quad \left(\text{since } AB \text{ is circulant, } b_{0j} = b_{k,k+j}\right) \\
&= \sum_{k=0}^{n-1}\left(\sum_{j=0}^{n-1} a_{0k}b_{kj}x^j\right) \\
&= \sum_{j=0}^{n-1}\left(\sum_{k=0}^{n-1} a_{0k}b_{kj}\, x^j\right) \\
&= \varphi(AB) \text{ .} \qquad //
\end{aligned}$$

One interesting consequence of this result is that every circulant matrix over R is a "polynomial" in P . If A is a circulant matrix, then

$$\begin{aligned}\varphi(A) &= \sum_{i=0}^{n-1} a_{0i}x^{i} \\ &= \sum_{i=0}^{n-1} a_{0i}\varphi(P)^{i} . \\ &= \varphi\left(\sum_{i=0}^{n-1} a_{0i}P^{i}\right) .\end{aligned}$$

Since φ is a bijection, it follows that

$$A = \sum_{i=0}^{n-1} a_{0i}P^{i} .$$

This result is also easily proved by direct computation. (See, for example, Newman [21], p. 184.)

(2.4) EXAMPLE. The circulant matrix

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

is equal to $I + 2P + 3P^2$.

From this point, we will restrict our attention to the case when the ring R is the ring of integers $\mathbb{Z}$.

A *circulant weighing matrix* is a weighing matrix which is circulant.

The following test is often useful when determining whether or not a circulant matrix is a weighing matrix.

(2.5). If A is a circulant matrix with Hall polynomial α , then AA^t is a scalar matrix if and only if

$$\sum_{g,h\in\langle x\rangle}\sum \alpha(g)\alpha(h)gh^{-1} \in \mathbb{Z} .$$

(2.6). The negative of a circulant weighing matrix is also a circulant weighing matrix. It is convenient to consider only one of each such pair, so *we make the convention that in each row of a circulant weighing matrix,* 1 *occurs at least as often as* -1 . The next lemma will imply among other things, that this convention achieves the desired selection.

LEMMA 3 (Stanton and Mullin [25]). *If k is the weight of a circulant weighing matrix, then $k = s^2$ where s is a nonnegative integer and the number of times* 1 *occurs in each row is* $\frac{1}{2}s(s+1)$.

Proof. Suppose that A is a circulant weighing matrix of order n and weight k . Let J be the $n \times n$ matrix where each entry is 1 . Let s be the row sum of A . It is easy to see that s is also the column sum of A and that

$$AJ = A^tJ = sJ \ .$$

Now

$$\begin{aligned}(AA^t)J &= (kI)J \\ &= kJ\end{aligned}$$

while

$$\begin{aligned}A(A^tJ) &= A(sJ) \\ &= s^2J \ .\end{aligned}$$

Therefore

$$(k-s^2)J = 0$$

which implies

$$k = s^2 \ .$$

Let l be the number of times 1 occurs in each row of A . The number of times -1 occurs in each row is then $s^2 - l$ and so the row sum s is $l - (s^2-l)$. That is

$$l = \tfrac{1}{2}s(s+1) \ . \qquad //$$

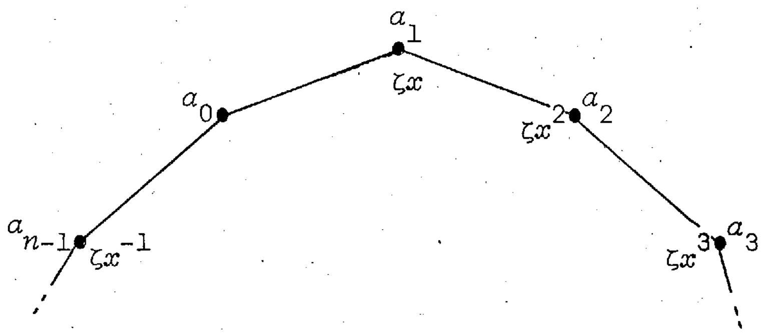
(2.7). Combining the result of Lemma 3 and the convention (2.6), it is easy to see that if A is a nonzero circulant weighing matrix, then $-A$ is not a circulant weighing matrix.

A Geometric Visualisation

Let us return to the cyclic group $\langle x\rangle$ of order n with distinguished generator x. If we think of x as a rotation by $2\pi/n$ of an oriented regular n-gon with a distinguished vertex ζ, we can associate each element g of $\langle x\rangle$ with the vertex ζg of the polygon. The elements of $\mathbb{Z}\langle x\rangle$ are then in one to one correspondence with the integer weighted, oriented, regular n-gons with distinguished vertex, so that the polygon with weight a_i at vertex ζx^i for each i corresponds to the element

$$\sum_{i=0}^{n-1} a_i x^i$$

of $\mathbb{Z}\langle x\rangle$.



This is a useful visualisation of circulant weighing matrices which should be kept in mind when reading the proof of Theorem 8.

Equivalence of Circulant Matrices

When trying to determine all circulant weighing matrices of a given order, it is useful to introduce some notion of equivalence of circulant matrices. Roughly speaking, two circulant matrices are equivalent when one can be obtained from the other by the "obvious" constructions.

To make this more precise, consider the split extension $\mathrm{Hol}\langle x\rangle$ of $\langle x\rangle$ by its automorphism group $\mathrm{Aut}\langle x\rangle$ (defined by the natural action of $\mathrm{Aut}\langle x\rangle$ on $\langle x\rangle$). This is known as the holomorph of $\langle x\rangle$ and is usually considered as a subgroup of the symmetric group of all permutations of the set of elements of $\langle x \rangle$, as follows. If $g, h \in \langle x \rangle$, $\tau \in \mathrm{Aut}\langle x \rangle$ $(\tau : g \to g^{\tau})$, and $(\tau, h) \in \mathrm{Hol}\langle x \rangle$, then $(\tau, h) : g \to g^{\tau}h$. We may regard $\mathrm{Hol}\langle x \rangle$ as acting on $Z\langle x \rangle$ so that (τ, h) takes each α in $Z\langle x \rangle$ to the composite map $(\tau, h)^{-1}\alpha$.

$$\begin{tikzcd}
\langle x \rangle \arrow[r, "(\tau{,}h)^{-1}"] \arrow[dr, "\alpha^{\tau}h"'] & \langle x \rangle \arrow[d, "\alpha"] \\
 & Z
\end{tikzcd} .$$

Thus for each α in $Z\langle x \rangle$,

$$\alpha^{\tau}h = \sum_{g} \alpha\left[g(\tau, h)^{-1}\right]g$$

$$= \sum_{g} \alpha(g)g^{\tau}h \; .$$

We see, using the test (2.5), that if A is a circulant weighing matrix with Hall polynomial α and if (τ, h) is in $\mathrm{Hol}\langle x \rangle$, then the circulant matrix with Hall polynomial $\alpha^{\tau}h$ is also a weighing matrix, with the same weight as A.

Let A and B be two $n \times n$ circulant matrices with Hall polynomials α and β respectively. We define A and B to be equivalent if and only if $\alpha = \beta^{\tau}h$ for some $(\tau, h) \in \mathrm{Hol}\langle x \rangle$.

(2.8) EXAMPLE. It is straightforward if tedious to check that the circulant matrices of order 13 with Hall polynomials

$$x^{2} + x^{4} + x^{5} + x^{6} - x^{7} - x^{8} + x^{10} - x^{11} + x^{12}$$

and

$$x^{2} - x^{4} + x^{5} + x^{6} + x^{7} + x^{8} - x^{10} + x^{11} - x^{12}$$

are inequivalent circulant weighing matrices.

(This notion of equivalence of circulant matrices was suggested to me by L.G. Kovács.)

Extending Circulant Matrices

As before, let $\langle x\rangle$ be a cyclic group of order n with distinguished generator x, and A a circulant matrix of order n with Hall polynomial α in $\mathbb{Z}\langle x\rangle$. Let $\langle y\rangle$, m, y, B and β be defined similarly. If m and n are coprime, the direct product of $\langle x\rangle$ and $\langle y\rangle$ is cyclic of order mn and xy may be taken as a convenient generator for it: thus $\langle x\rangle$ and $\langle y\rangle$ are embedded in $\langle xy\rangle$ and $\mathbb{Z}\langle x\rangle$, $\mathbb{Z}\langle y\rangle$ in $\mathbb{Z}\langle xy\rangle$. It is easily seen that the Kronecker product $A\otimes B$ may be considered as a circulant matrix with Hall polynomial $\alpha\beta$ (in $\mathbb{Z}\langle xy\rangle$).

Moreover, if both A and B are weighing matrices, then so is $A\otimes B$, and its weight is the product of the weights of A and B (Geramita, Geramita and Wallis [10]).

Another useful construction suggested to me by Peter Eades is the following. If t is any positive integer, the cyclic group $\langle z\rangle$ of order nt has a unique (cyclic subgroup of order n, namely $\langle z^t\rangle$: we may identify this with $\langle x\rangle$ so that $x = z^t$. Construct a circulant matrix A_t of order nt by replacing each entry a_{ij} of A by the $t\times t$ scalar matrix $a_{ij}I$. The Hall polynomial of A_t is α regarded as an element of $\mathbb{Z}\langle z\rangle$ after substituting z^t for x.

(2.9) EXAMPLE. The 4×4 circulant weighing matrix

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

can be extended to an 8×8 circulant weighing matrix

$$A_2 = \begin{bmatrix} -1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & -1 \end{bmatrix} .$$

If A is a circulant weighing matrix, then A_t is also a circulant weighing matrix.

If A and A' are inequivalent circulant weighing matrices of order n, then A_t and A'_t are inequivalent circulant matrices and if B is a circulant weighing matrix whose order is prime to n, then $A \otimes B$ and $A' \otimes B$ are inequivalent.circulant matrices. The first assertion is easy to check, while the second is a special case of the following lemma.

LEMMA 4. *Suppose that* A, A' *are nonzero circulant weighing matrices of order* n *and that* B, B' *are nonzero circulant weighing matrices of order* m. *Suppose that* m *and* n *are coprime.*

If $A \otimes B$ *is equivalent to* $A' \otimes B'$, *then* A *is equivalent to* A' *and* B *is equivalent to* B'.

Proof. As above, let $\langle x \rangle$, $\langle y \rangle$ be cyclic groups of orders n, m respectively with distinguished generators x, y respectively.

If

$$\left.\begin{aligned} \alpha &= \sum_g \alpha(g)g \\ \alpha' &= \sum_g \alpha'(g)g \end{aligned}\right\} \quad g \in \langle x \rangle ,$$

$$\left.\begin{aligned} \beta &= \sum_h \beta(h)h \\ \beta' &= \sum_h \beta'(h)h \end{aligned}\right\} \quad h \in \langle y \rangle$$

are the Hall polynomials of A, A', B, B' respectively, then $A \otimes B$ and

$A' \otimes B'$ have Hall polynomials $\alpha\beta$ and $\alpha'\beta'$ respectively where

$$\alpha\beta = \sum_{g,h\in\langle x\rangle}\sum \alpha(g)\beta(h)gh \quad\text{and}\quad \alpha'\beta' = \sum_{g,h\in\langle x\rangle}\sum \alpha'(g)\beta'(h)gh \ .$$

If $A \otimes B$ and $A' \otimes B'$ are equivalent, then there is an automorphism τ of $\langle xy \rangle$ and $a \in \langle x \rangle$ and $b \in \langle y \rangle$ such that

$$\alpha\beta = (\alpha'\beta')^{\tau}ab \ .$$

Since $\langle xy \rangle$ is the direct product of its unique subgroup $\langle x \rangle$ of order n and its unique subgroup $\langle y \rangle$ of order m, it follows that if ψ and φ are the restrictions of τ to $\langle x \rangle$ and $\langle y \rangle$ respectively, then

$$(gh)^{\tau} = g^{\psi}g \quad \text{for all } g \in \langle x \rangle \text{ and } h \in \langle y \rangle \ .$$

Therefore

(2.10) $$\alpha'(g)\beta'(h) = \alpha\left(g^{\psi}a\right)\beta\left(h^{\varphi}b\right)$$

for all $g \in \langle x \rangle$ and $h \in \langle y \rangle$.

Since $A' \neq 0$, we can choose g in $\langle x \rangle$ such that $\alpha'(g) \neq 0$.

Since $\alpha'(g) = 1$ or -1 and $\alpha'\left(g^{\psi}a\right) = -1, 0$ or 1 , we have either

(1) $\alpha\left(g^{\psi}a\right) = \alpha'(g)$, or

(2) $\alpha\left(g^{\psi}a\right) = -\alpha'(g)$, or

(3) $\alpha\left(g^{\psi}a\right) = 0$.

Case 1. Using equation (2.10), we see that if $\alpha\left(g^{\psi}a\right) = \alpha'(g)$, then $\beta\left(h^{\varphi}b\right) = \beta'(h)$ for all $h \in \langle y \rangle$ and so $\beta^{\varphi}b = \beta'$. Thus B is equivalent to B' .

Since $B' \neq 0$, we can find $h \in \langle y \rangle$ such that $\beta'(h) \neq 0$ and it follows that $\alpha\left(g^{\psi}a\right) = \alpha'(g)$ for all $g \in \langle x \rangle$; that is $\alpha^{\psi}a = \alpha'$ and A is equivalent to A' .

Case 2. Using equation (2.10), we see that if $\alpha\left(g^{\psi}a\right) = -\alpha'(g)$ then $\beta^{\varphi}b = -\beta'$, that is, B is equivalent to $-B'$ and so $-B$ is a circulant weighing matrix. But by (2.7), the negative of a nonzero circulant weighing matrix cannot be a circulant weighing matrix. This contradiction shows this case is vacuous.

Case 3. Again by Equation (2.10), if $\alpha\left(g^{\psi}a\right) = 0$ and $\alpha'(g) \neq 0$, then $B' = 0$, contrary to our assumptions. //

CHAPTER III

EXISTENCE

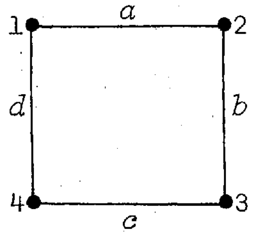
So far we have not worried too much about whether our principal objects of study (circulant weighing matrices) exist in any abundance. The time has now come to rectify this situation.

The material in the following section should be familiar, but is included because projective planes become the principal object of study in Chapter IV.

Projective Planes

An *incidence structure* is a triple $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ where $\mathcal{P}$ and $\mathcal{B}$ are sets and $\mathcal{I}$ is a subset of $\mathcal{P} \times \mathcal{B}$. The elements of $\mathcal{P}$ are called *points*, the elements of B are called *blocks* and the elements of $\mathcal{I}$ are called *flags*. Usually we shall write pIB instead of (p, B) for an element of $\mathcal{I}$ and we shall say that the point p is *incident* with the block B.

A square is an example of an incidence structure:



$P = \{1, 2, 3, 4\}$,

$B = \{a, b, c, d\}$,

$I = \{(1, a), (2, a), (2, b), (3, b), (3, c), (4, c), (4, d), (1, d)\}$.

The vertices of the square are the points, the edges are the blocks and the incidence relation is containment; that is pIB if and only if $p \in B$.

Often we shall "bastardise" our definition and identify each block with the set of points incident with it. In the cases we are interested in this should not lead to any confusion.

A *projective plane* is an incidence structure $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ which satisfies the following three axioms.

(I) For each pair of distinct points, there is a unique block which is incident with both points.

(II) For each pair of distinct blocks, there is a unique point which is incident with both blocks.

(III) There is at least one set of four distinct points such that no three of these points are incident with the same block.

The blocks of a projective plane are usually called *lines*.

(3.1). The most common examples of projective planes arise in the following way. Let F be a field and V a three dimensional vector space over F. Consider the one dimensional subspaces of V as points and the two dimensional subspaces of V as lines. If we interpret the point p being incident with the line l as meaning that p is a subspace of l, then the resulting incidence structure is a projective plane. Note however that not all projective planes arise in the above manner. For examples of such planes see either Dembowski [7] or Hughes and Piper [14].

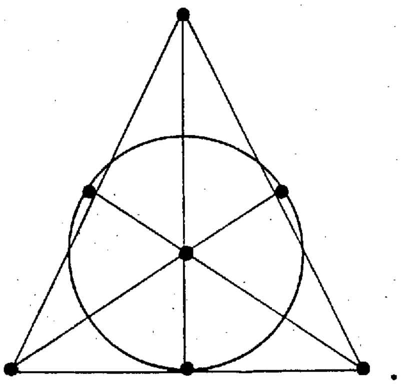
It is convenient to introduce a notion of isomorphism of incidence structures. Define the incidence structures $(\mathcal{P}_1, \mathcal{B}_1, \mathcal{I}_1)$ and $(\mathcal{P}_2, \mathcal{B}_2, \mathcal{I}_2)$ to be *isomorphic* if there are bijections $\varphi : \mathcal{P}_1 \to \mathcal{P}_2$ and $\psi : \mathcal{B}_1 \to \mathcal{B}_2$ such that $p\mathcal{I}B$ if and only if $(\varphi p)\mathcal{I}(\psi B)$ for all $p \in \mathcal{P}_1$ and $B \in \mathcal{B}_1$.

It is easy to show that all projective planes which can be constructed from a three dimensional vector space over a given field are isomorphic. Such a projective plane is called a *Desarguesian projective plane* and we denote the Desarguesian projective plane constructed from the vector space V by $\mathcal{P}V$.

For a set Y, denote the cardinality of Y by $|Y|$. It is not hard to show that if (P, B, I) is a projective plane, then the number of points incident with each line is fixed and equals the number of lines incident with each point. (Axiom III is needed to prove this fact.) It is easy to deduce from this fact that $|P| = |B|$.

When $|P|$ is finite, we say that the projective plane is finite and we define the *order* of a finite projective plane to be the integer one less than the number of points incident with each line.

The following self explanatory diagram represents a projective plane of order two:



If F is a finite field and V a three dimensional vector space over F , then the Desarguesian projective plane constructed from V has order $|F|$.

It is well known that the order of a finite field is always a prime power and conversely, given a prime power q , we can construct a field of order q . (See, for example, Birkhoff and Mac Lane [5].) Thus for each prime power q , there is a Desarguesian projective plane of order q .

We now have to justify the introduction of this seemingly unrelated material. First a definition.

A *cyclic projective plane* is a finite projective plane (P, B, I) which admits a cyclic group C of automorphisms which acts sharply transitively on P . That is, given two distinct elements a and b of P , there is precisely one element of C which takes a to b .

LEMMA 5 (Singer 1938, [23]). *Every finite Desarguesian projective* *plane is cyclic.*

Proof. Let F be a finite field and F_3 the cubic extension of F. The field F_3 is a three dimensional vector space V over F.

The elements of the multiplicative group $F_3^{\#}$ of F_3 may be thought of as a subgroup of the group of linear automorphisms of V by identifying the element f of F_3 with the linear transformation which takes the element e of F_3 to ef.

It is easy to see that each linear automorphism of V induces an automorphism of the projective plane PV. Thus there is a homomorphism from the multiplicative group $F_3^{\#}$ of F_3 into the automorphism group of PV. It is easy to show that the element f of $F_3^{\#}$ acts trivially on PV if and only if f is an element of the multiplicative group $F^{\#}$ of F.

Since the multiplicative group of a finite field is cyclic, it follows that the automorphism group of PV contains a cyclic subgroup isomorphic to the factor group $F_3^{\#}/F^{\#}$.

It is not hard to show that this cyclic group acts sharply transitively on PV. Since all Desarguesian projective planes of a given order are isomorphic, we have proved the lemma. //

An Inequality

We are now at the watershed of projective geometry and the study of circulant weighing matrices. In their paper [10], Geramita, Geramita and Wallis prove that if n is odd and if there is a weighing matrix of order n and weight k, then

$$(n-k)^2 - (n-k) \geq n - 1$$

and if $(n-k)^2 - (n-k) = n - 1$, then there is a projective plane of order

$n - k - 1$.

Here I prove a slight variation; namely, if n is odd and if there is a *circulant* weighing matrix of order n and weight k , then

$$(n-k)^2 - (n-k) \geq n - 1$$

and if $(n-k)^2 - (n-k) = n - 1$, then there is a *cyclic* projective plane of order $n - k - 1$.

In a later paper [28], Wallis and Whiteman prove the converse; given a cyclic projective plane of order q , we can construct a circulant weighing matrix of order $q^2 + q + 1$ and weight q^2 .

The proof of the Geramita, Geramita and Wallis inequality will be given immediately while L.G. Kovács' elegant proof of the Wallis-Whiteman theorem will be given in the next chapter.

First a lemma.

LEMMA 6. *Suppose that* C *is a cyclic group of order* n .

If Z *is a subset of* C *which meets each of its translates* Zg $(g \in C)$ *in at least one point, then*

$$|Z|^2 - |Z| \geq n - 1 .$$

If $|Z|^2 - |Z| = n - 1$ *, then* C *is a cyclic projective plane whose lines are the translates* Zg $(g \in C)$ *of* Z .

Proof. Observe that the group C acts sharply transitively on itself (by left multiplication). It follows that for each element z of Z there are precisely $|Z|$ elements g of C such that $z \in Z \cap Zg$.

Consider the set of ordered pairs (z, g) where $g \in C$ and $z \in Z \cap Zg$. By counting this set along "horizontal slices" then "vertical slices", we have

$$\sum_g |Z \cap Zg| = |Z|^2 . \tag{3.2}$$

Now when $g = 1$, we have $|Z \cap Zg| = |Z|$ while $|Z \cap Zg| \geq 1$ when $g \neq 1$. Therefore

$$|Z|^2 \geq |Z| + n - 1 .$$

That is $|Z|^2 - |Z| \geq n - 1$.

If $|Z|^2 = |Z| + n - 1$, then it is easy (using (3.2)) to see that for all nontrivial elements g of C , $|Z \cap Zg| = 1$. By counting the ordered pairs $(\{a, b\}, g)$ where $g \in C$ and where $\{a, b\}$ is a two element subset of C contained in Zg , it is easy to show that each pair of distinct elements of C lie in a unique translate of Z . That is C is a cyclic projective plane whose lines are the translates Zg of Z . //

THEOREM 7. *If there is a circulant weighing matrix of order* n *and if* n *is odd then*

$$(n-k)^2 - (n-k) \geq n - 1 .$$

If $(n-k)^2 - (n-k) = n - 1$ *, then there is a cyclic projective plane of order* $n - k - 1$.

Proof. Suppose that A is a circulant weighing matrix of order n and weight k with Hall polynomial α . Let

$$Z = \{g \in \langle x \rangle \mid \alpha(g) = 0\}$$

and notice that $|Z| = n - k$.

If n is odd, then using test (2.5) it is not hard to show that Z meets each of its distinct translates Zg (that is g is a nontrivial element of $\langle x \rangle$) in an odd number of points. In particular, $|Z \cap Zg| \geq 1$ for all elements g of $\langle x \rangle$.

Applying Lemma 6, we have

$$|Z|^2 - |Z| \geq n - 1 ;$$

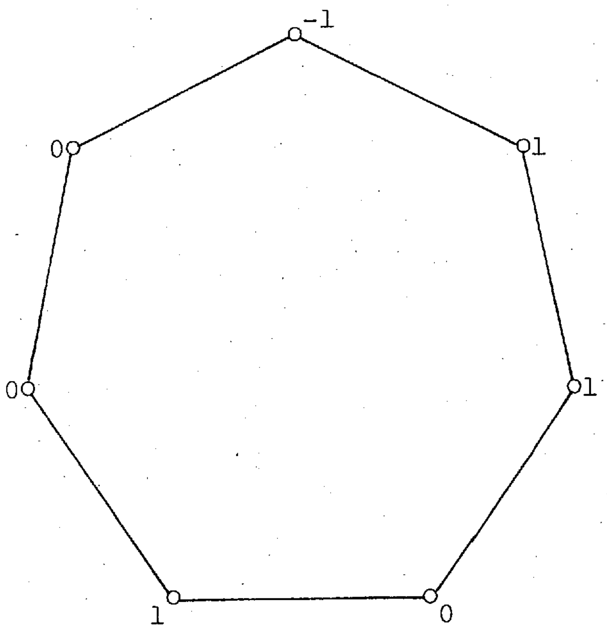
that is $(n-k)^2 - (n-k) \geq n - 1$.

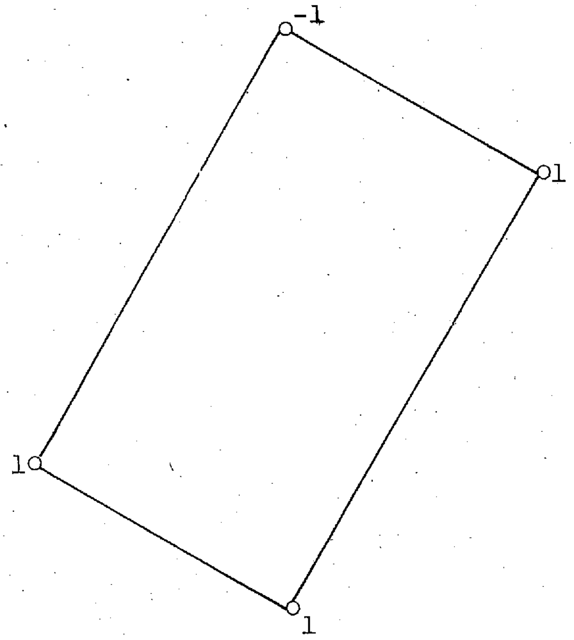
If $(n-k)^2 - (n-k) = n - 1$, then by Lemma 6, the cyclic group $\langle x \rangle$ admits a cyclic projective plane structure where the lines are the translates Zg of Z $(g \in \langle x \rangle)$. The order of this projective plane is $|Z| - 1$ which is equal to $n - k - 1$. //

The Geramita, Geramita, Wallis inequality is not valid when n is even. The matrix in Example (2.1) is a circulant weighing matrix for which $(n-k)^2 - (n-k) = 2$ while $n - 1$ is 5 .

Circulant Weighing Matrices of Weight 4

As we have seen, the weight of a circulant weighing matrix is always a square. It is easy to see that all circulant weighing matrices of weight 1 are equivalent to the identity matrix of the same order. Recall from Chapter 2 that the integer circulant matrices of order n are in a one to one correspondence with the integer weighted, oriented, regular n-gons with distinguished vertex. The following theorem shows that all circulant weighing matrices of weight 4 correspond to weighted polygons where all the weight lies either on an inscribed rectangle or on an inscribed regular heptagon. This implies that the order of a circulant weighing matrix of weight 4 must be divisible by 2 or 7 .





The converse is also true. Given $n \geq 4$, if n is divisible by either 2 or 7 , then there is a circulant weighing matrix of order n and weight 4 .

THEOREM 8 (Eades and Hain [9]). *Suppose that* $\langle x \rangle$ *is a cyclic group of order* n *with generator* x .

If n *is divisible by* 7 , *then the circulant matrix of order* n *with Hall polynomial* $-1 + x^{n/7} + x^{2n/7} + x^{4n/7}$ *is a weighing matrix.*

If n *is even, if* d *is a positive divisor of* $\frac{1}{2}n$ *and* $d \neq \frac{1}{2}n$, *then the circulant matrix with Hall polynomial* $-1 + x^{d} + x^{\frac{1}{2}n} + x^{d+\frac{1}{2}n}$ *is a weighing matrix.*

Each circulant weighing matrix of order n *and weight* 4 *is equivalent to one and only one of the matrices mentioned above.*

COROLLARY 9 (Eades and Hain [9]). *For a positive integer* m , *define* $\Delta(m)$ *to be the number of (positive) divisors of* m *(including* 1 *but excluding* m *).*

The number of equivalence classes of circulant weighing matrices of order n *and weight* 4 *is*

$$\begin{aligned} 0 &\quad \textit{if } n \textit{ is odd and } 7 \nmid n \,, \\ 1 &\quad \textit{if } n \textit{ is odd and } 7 \mid n \,, \\ \Delta(\tfrac{1}{2}n) &\quad \textit{if } n \textit{ is even and } 7 \nmid n \,, \\ \Delta(\tfrac{1}{2}n) + 1 &\quad \textit{if } n \textit{ is even and } 7 \mid n \,. \end{aligned}$$

Proof of Theorem 8. Using test (2.5), it is straightforward to check that the circulant matrices with Hall polynomials $-1 + x^{d} + x^{d+\frac{1}{2}n} + x^{\frac{1}{2}n}$ (when n is even and $d \mid \frac{1}{2}n$, $d \neq \frac{1}{2}n$) and $-1 + x^{n/7} + x^{2n/7} + x^{4n/7}$ (when $n \mid 7$) are weighing matrices of weight 4 .

For a positive integer m , define $D(m)$ to be the set of positive divisors d of m where $d \neq m$.

Put

$$\alpha = -1 + x^{n/7} + x^{2n/7} + x^{4n/7} \quad (7 \mid n)$$

and

$$\beta_{d} = -1 + x^{d} + x^{\frac{1}{2}n} + x^{\frac{1}{2}n+d}$$

(n is even and $d \in D(\frac{1}{2}n)$).

Given an integer n , define S to be the set of those polynomials α, β_d which "make sense" for that n . That is, $S = \emptyset$ when n is odd and $7 \nmid n$, $S = \{\alpha\}$ when n is odd and $7 | n$, $S = \{\beta_d \mid d \in D(\frac{1}{2}n)\}$ when n is even but $7 \nmid n$ and $S = \{\alpha\} \cup \{\beta_d \mid d \in D(\frac{1}{2}n)\}$ when n is even and $7 | n$.

For each n we have to show that if the circulant matrices with Hall polynomials γ, δ in S are equivalent, then $\gamma = \delta$.

Since each row of a circulant weighing matrix of weight 4 contains precisely one -1 and since $\gamma(1) = -1$ for all $\gamma \in S$, the circulant matrices with Hall polynomials γ, δ ($\in S$) are equivalent if and only if there is an automorphism τ of $\langle x \rangle$ such that $\gamma = \delta^\tau$.

We shall exploit the trivial fact that if G is a group and τ an automorphism of G , then each element g of G has the same order as its image g^τ under τ .

If n is divisible by 14 and $d \in D(\frac{1}{2}n)$, then the circulant matrices with Hall polynomials α, β_d cannot be equivalent because β_d takes the value 1 on the element of order 2 in $\langle x \rangle$, while α takes the value 1 only on elements of order 7 in $\langle x \rangle$.

If n is even and $d \in D(\frac{1}{2}n)$, then x^d is congruent to $x^{d+\frac{1}{2}n}$ modulo $\langle x^{\frac{1}{2}n} \rangle$ and these elements have order $n/2d$ ($\neq 1$) modulo $\langle x^{\frac{1}{2}n} \rangle$, while the other two elements, 1 and $x^{\frac{1}{2}n}$, have order 1 modulo $\langle x^{\frac{1}{2}n} \rangle$.

Consequently, if $d, d' \in D(\frac{1}{2}n)$ and τ is an automorphism of $\langle x \rangle$ such that $(\beta_d)^\tau = \beta_{d'}$, then x^d and $x^{d'}$ have the same order modulo $\langle x^{\frac{1}{2}n} \rangle$; that is $n/2d = n/2d'$. Therefore $d = d'$ and $\beta_d = \beta_{d'}$.

Thus we have shown that a circulant weighing matrix of order n and weight 4 can be equivalent to at most one of the circulant matrices with Hall polynomial in S .

From the following lemma we will deduce that all circulant weighing matrices of weight 4 are either "rectangular" or "heptagonal".

LEMMA 10 (Eades and Hain [9]). *Suppose that C is a cyclic group of order n and that Z is a subset of C containing exactly four elements.*

If the size of the intersection of Z with each of its translates Zg $(g \in C)$ is even, then

EITHER *n is even and some translate of Z is of the form*

$\{1, y, v, yv\}$ where $y, v \in C$ and v has order 2

(and we say that Z is a rectangle),

OR *n is divisible by 7 and some translate of Z is of*

the form $\{1, u, u^2, u^4\}$ where u has order 7 in C

(and we say that Z is heptagonal).

Proof. Since we are only determining Z up to a translation, we can without loss of generality assume that Z contains 1 . There are two possible cases; namely

(1) there is a nontrivial element y of G such that $Z = Zy$;

(2) for all nontrivial elements g of C we have $Z \neq Zg$.

For a set X , denote the cardinality of X by $|X|$.

Case 1. Let y be the nontrivial element of C such that $Z = Zy$. Since $1 \in Z$, it follows that $y \in Z$ and $y^{-1} \in Z$. Either $y^2 = 1$ $(y = y^{-1})$ or $y \neq y^{-1}$.

Let $Z = \{1, y, z, w\}$. If $y = y^{-1}$, then since $Z = Zy$, $w = zy$. That is $Z = \{1, y, z, yz\}$ where $y^2 = 1$. Now Z is a rectangle.

If $y \neq y^{-1}$, then $Z = \{1, y, y^{-1}, z\}$. Since $Z = Zy$ and $y \neq 1$, it follows that $z = y^2$ and $y^{-1} = zy$. That is $z = y^2 = y^{-2}$. Thus

$Z = \{1, y, y^2, y^3\}$ and $y^4 = 1$, so Z is a rectangle (in fact a "square"!).

Case 2. In this case $|Z \cap Zg| = 0$ or 2 for all nontrivial elements g of C. We divide this case into the following subcases;

(2a) there is an element y of Z such that $y^2 \neq 1$ and $y^{-1} \in Z$;

(2b) for all elements g of Z such that $g^2 \neq 1$, the element g^{-1} is not in Z.

Case 2a.

(2a.1) Let $Z = \{1, y, y^{-1}, w\}$. Since $Z \cap Zy \neq \emptyset$, $|Z \cap Zy| = 2$. But $1, y \in Z \cap Zy$, therefore $y^{-1} \neq y^2$ $(y^3 \neq 1)$, $w \neq y^2$ and $y^{-1} \neq wy$ $(w \neq y^{-2})$.

Now $Z \cap Zy^2 \neq \emptyset$, thus $|Z \cap Zy^2| = 2$. By (2a.1), $1 \neq y^3$, $1 \neq wy^2$ and by assumption, $1 \neq y^2$. Thus $1 \notin Z \cap Zy^2$.

Suppose $y^4 = 1$. Then, by (2a.1), $Z \cap Zw \neq \emptyset$; so $|Z \cap Zw| = 2$. Thus either $w^2 = y$, or $w^2 = y^3$. But then $|Z \cap Zw^3| = 1$; hence $y^4 \neq 1$.

Since $y^2 \neq 1$, $w \neq wy^2$ and by (2a.1), $w \neq y^2$. The only remaining possibilities are that either $w = y^3$ and $y^{-1} = wy^2$ (that is $w = y^3$ and $y^6 \neq 1$), or $wy^2 = y^{-1}$ and $w = y^3$ (that is $w = y^{-3}$ and $y^6 \neq 1$).

Because of the symmetry of the situation, we need only consider the first of these cases. Since $Z \cap Zy^3 \neq \emptyset$, it follows by a straightforward argument that $y^7 = 1$ and $Z = \{1, y^{-1}, y, y^3\}$. Thus Z is heptagonal.

Case 2b.

Here if $g \in Z$ and $g^2 \neq 1$, then $g^{-1} \in Z$. Since $Z \cap Zg \neq \emptyset$, it follows that $|Z \cap Zg| = 2$. As $\langle x \rangle$ has at most one element of order 2 , there is an element, say y , in Z such that $y^2 \neq 1$.

If $y^2 \in Z$ then $1, y, y^{-1} \in Zy^{-1}$ so the translate Zy^{-1} of Z has been dealt with under case 2a. Thus we may assume $y^2 \notin Z$. Of course we also have $y^{-1} \notin Z$, and as $Z \cap Zy \neq \emptyset$, it follows that $|Z \cap Zy| = 2$. Thus one may derive that $Z = \{1, y, w, wy\}$ for some w .

A similar straightforward but tedious argument concerning $Z \cap Zwy^{-1}$ and $Z \cap Zw^{-1}y^{-1}$ now leads to a contradiction, showing that his case is vacuous.

This completes the proof of the lemma. //

It is clear that every circulant weighing matrix of weight 4 is equivalent to a circulant matrix whose Hall polynomial takes the value -1 on $1 \; (\in \langle x \rangle)$.

Suppose that γ is the Hall polynomial of a circulant weighing matrix A of weight 4 and that $\gamma(1) = -1$. Using test (2.5) it is easy to show that $\sum_{g} \gamma(g)\gamma(gh)$ is 0 when $h \neq 1$ and 4 when $h = 1$.

Let $Z = \{g \in \langle x \rangle : \gamma(g) \neq 0\}$. It is also easy to show that Z meets each of its translates $Zg \;\; (g \in \langle x \rangle)$ in an even number of points and that Z contains exactly 4 elements. Thus Z satisfies the conditions of Lemma 10. Therefore either the order of $\langle x \rangle$ is congruent to 0 mod 7 and Z is a translate of $\{1, y, y^2, y^4\}$ where y is an element of order 7 in $\langle x \rangle$ or the order of $\langle x \rangle$ is even and Z is a translate of $\{1, z, u, zu\}$ where u is an element of order 2 in $\langle x \rangle$.

It is straightforward to show that, as $\gamma(1) = -1$, in the first case $\gamma = -1 + y + y^2 + y^4$ (and we say that n is *heptagonal*) and in the second case $\gamma = -1 + z + u + zu$ (and we say that u is *rectangular*).

It is worth pointing out that there is a slightly more direct proof of this fact, but the full strength of Lemma 10 is required to prove Theorem 11.

Our final task in the proof of Theorem 8 is to show that every circulant weighing matrix of weight 4 is equivalent to at least one at the circulant weighing matrices whose Hall polynomial lies in S.

Recall that if C is a cyclic group, then the automorphism group of C acts transitively on the elements of any given order in C.

If A is a heptagonal circulant weighing matrix with Hall polynomial $-1 + y + y^2 + y^4$ where y has order 7 in $\langle x \rangle$ and if τ is the automorphism at $\langle x \rangle$ taking y to $x^{n/7}$, then

$$\left(-1+y+y^2+y^4\right)^\tau = -1 + x^{n/7} + x^{2n/7} + x^{4n/7} \; (= \alpha)$$

and therefore every heptagonal circulant weighing matrix of order n is equivalent to the circulant matrix with Hall polynomial α.

When A is a rectangular circulant weighing matrix, the order n of $\langle x \rangle$ is even. Let y be an element of $\langle x \rangle$ which is not congruent to 1 modulo $\langle x^{\frac{1}{2}n} \rangle$. Let $n/2d$ be the (common) order of y and $yx^{\frac{1}{2}n}$ modulo $\langle x^{\frac{1}{2}n} \rangle$. It is easy to see that either y or $yx^{\frac{1}{2}n}$ has order n/d in $\langle x \rangle$. Since x^d has order n/d in $\langle x \rangle$, there is an automorphism τ of $\langle x \rangle$ such that either $\left(x^d\right)^\tau$ is $yx^{\frac{1}{2}n}$ or y. That is

$$\left(-1+x^d+x^{\frac{1}{2}n}+x^{d+\frac{1}{2}n}\right)^\tau = -1 + y + x^{\frac{1}{2}n} + yx^{\frac{1}{2}n} .$$

Thus if A is a rectangular circulant weighing matrix, then A is equivalent to one of the circulant matrices with Hall polynomial β_d where $d \in D(\frac{1}{2}n)$. This completes the proof of Theorem 8. //

Reduction Theorems

In Chapter 2 we used the fact that a cyclic group of order n can be embedded in a cyclic group of order nt to show that if there is a circulant weighing matrix of order n and weight k , then there is a circulant weighing matrix of order nt and weight k . In this section we essentially do the opposite.

Let $\langle x \rangle$ be a cyclic group of order nt with distinguished generator x . The subgroup $\langle x^t \rangle$ of $\langle x \rangle$ is cyclic of order n . We may choose x^t as a convenient generator for $\langle x^t \rangle$. The homomorphism φ from $\langle x \rangle$ to $\langle x^t \rangle$ which takes x to x^t induces a map φ_* from the circulant (but not necessarily weighing) matrices of order nt to the circulant matrices of order n in the following way: the map φ_* takes the circulant matrix of order nt with Hall polynomial

$$\sum_{i=0}^{nt-1} \alpha_i x^i$$

to the circulant matrix of order n with the Hall polynomial

$$\sum_{i=0}^{nt-1} \alpha_i x^{ti} \quad (\in Z\langle x^t \rangle) \; .$$

Notice that $x^{ti} = x^{tj}$ if and only if $i \equiv j$ modulo n . Thus

$$\sum_{i=0}^{nt-1} \alpha_i x^{ti} = \sum_{i=0}^{n-1} \left(\sum_{j \equiv i(n)} \alpha_j \right) x^{ti} \; .$$

It is easy to verify that if A is a circulant matrix such that AA^t is a scalar matrix, then $(\varphi_* A)(\varphi_* A)^t$ is also a scalar matrix.

(3.3) Of interest here is the case when A is a circulant weighing matrix of order $2n$ with Hall polynomial

$$\sum_{i=0}^{2n-1} \alpha_i x^i$$

where the subset $\left\{ x^i \mid \alpha_i \neq 0 \right\}$ of $\langle x \rangle$ is a union of cosets of the subgroup $\langle x^n \rangle$ of $\langle x \rangle$. In this case it is easy to see that $\frac{1}{2}\varphi_* A$ is a circulant weighing matrix with Hall polynomial

$$\tfrac{1}{2}\sum_{i=0}^{2n-1} \alpha_i x^{2i} .$$

If A has weight k, then

$$\left(\sum_{i=0}^{2n-1} \alpha_i x^{i}\right)\left(\sum_{i=0}^{2n-1} \alpha_i x^{-i}\right) = k .$$

Thus

$$\left(\tfrac{1}{2}\sum_{i=0}^{2n-1} \alpha_i x^{2i}\right)\left(\tfrac{1}{2}\sum_{i=0}^{2n-1} \alpha_i x^{-2i}\right) = \tfrac{1}{4}k$$

and $\frac{1}{2}\varphi_* A$ has weight $\frac{1}{4}k$.

THEOREM 11 [9]. *(a) If there is a circulant Hadamard matrix of order* n, *then* $n \equiv 0$ **modulo** 4 *and there is a circulant weighing matrix of order* $\frac{1}{2}n$ *and weight* $n/4$.

(b) If there is a circulant weighing matrix of order n *and weight* $n - 2$, *then either* $n = 3$ *or* $n \equiv 2$ modulo 4 *and there is a circulant weighing matrix of order* $\frac{1}{2}n$ *and weight* $(n-2)/4$.

(c) If there is a circulant weighing matrix of order n *and weight* $n - 4$ *then either* $n = 5$ *or* $n = 13$, *or* $n \equiv 0$ modulo 4 *and there is a circulant weighing matrix of order* $\frac{1}{2}n$ *and weight* $(n-4)/4$.

Proof. *(a)* It is well known that the order of a Hadamard matrix is congruent to 0 modulo 4 (Paley, [22]). If A is a Hadamard matrix of order n, then there are no zeros in any row of A. Using (3.3) we see that $\frac{1}{2}\varphi_* A$ is a circulant weighing matrix of order $\frac{1}{2}n$ and weight $n/4$.

(c) If A is a circulant weighing matrix of order n and weight $n - 4$ and if n is odd, then by Theorem 7 we have

$$4^2 - 4 \geq n - 1 .$$

That is $n \leq 13$. By Lemma 3, $n - 4$ is a square, so n is either 5 or 13.

If A is a circulant weighing matrix of order n and weight $n - 4$ and if n is even then $n - 4$ is an even square and is thus congruent to

0 modulo 4 . That is $n \equiv 0$ modulo 4 .

If also $n \equiv 0$ modulo 7 , then $n \equiv 0$ modulo 28 and there is an integer l such that $n - 4 = 28l - 4$ and so $(n-4)/4 \equiv 6$ modulo 7 . But $(n-4)/4$ is a square while 6 is not a quadratic residue modulo 7 , therefore $n \not\equiv 0$ modulo 7 .

If α is the Hall polynomial of A and $Z = \{g \in \langle x \rangle \mid \alpha(g) = 0\}$, then it is easy to check that Z satisfies the conditions of Lemma 10. Since $n \not\equiv 0$ modulo 7 , it follows that Z is a translate of $\{1, y, v, vy\}$ where $y \not\equiv 1$ modulo $\langle x^{\frac{1}{2}n} \rangle$. That is Z is a union of cosets of $\langle x^{\frac{1}{2}n} \rangle$ in $\langle x \rangle$. Therefore, by (3.3), $\frac{1}{2}\varphi_* A$ is a circulant weighing matrix of order $\frac{1}{2}n$ and weight $(n-4)/4$.

(b) The proof of *(b)* is similar to the proof of *(c)* but is much simpler. The proof will not be given. //

There is one more result regarding the existence of circulant weighing matrices. I state this theorem without proof.

THEOREM (Stanton and Mullin [25]). *If W is a circulant weighing matrix of order n and weight $n - 1$ then either $n = 1$ and W is the 1×1 zero matrix, or $n = 2$ and W is equivalent to the 2×2 identity matrix.*

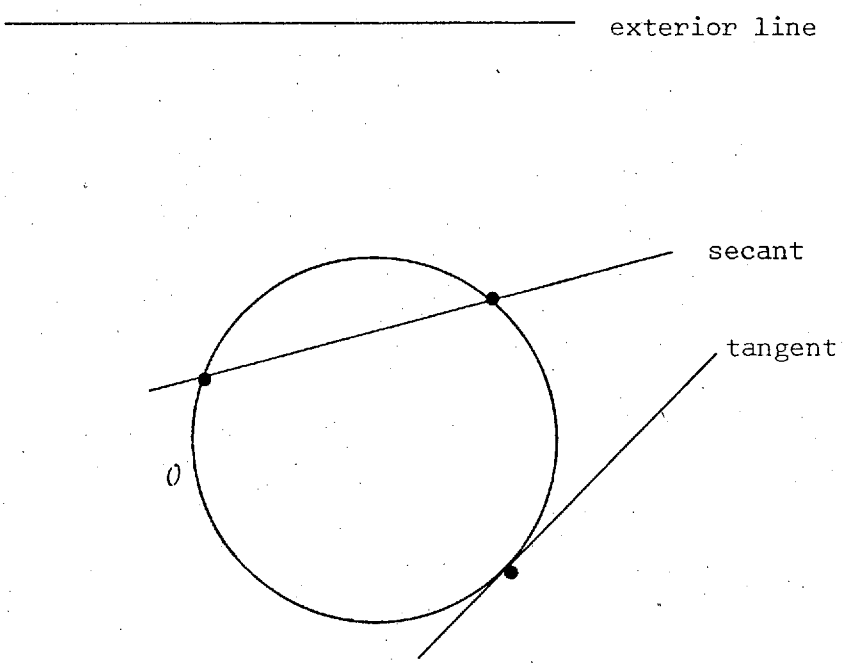
CHAPTER IV

OVALS IN CYCLIC PROJECTIVE PLANES

Welcome to Chapter IV. In this chapter I develop the interconnection between cyclic projective planes and circulant weighing matrices and give L.G. Kovács' proof of the Wallis-Whiteman theorem. Later in the chapter I exploit certain geometric facts about ovals in finite projective planes to establish results about equations of the kind $xy^{-2} = a$ "in" cyclic projective planes.

Ovals in Finite Projective Planes

Let Π be a finite projective plane of order q. An *oval* O in the finite projective plane Π is a set of $q + 1$ points of Π such that each line l of Π is incident with at most two points of O. A line l of Π is called a *secant*, *tangent* or *exterior line* (to O) according to whether l is incident with 2, 1 or 0 points of O.



If l is a tangent to the oval O and l meets O and the point x, then we say that l is a tangent to O at x. The following well known lemma shows that ovals in finite projective planes possess some of the properties of circles in the Euclidean plane.

LEMMA 12. *Every oval in a finite projective plane has a unique tangent at each of its points.*

Proof. Let O be an oval in a finite projective plane of order q and let x be an element of O. Since O contains $q + 1$ elements and since no three points of O are collinear, it follows that there are q secants of O which are incident with x. But in a projective plane of order q there are precisely $q + 1$ lines incident with each point. Therefore there is a unique line incident with x which is not a secant to O; that is, there is a unique tangent to O at x. //

The next lemma is well known (see Dembowski [7], p. 148). It demonstrates that the analogy between ovals in finite projective planes and circles in the Euclidean plane breaks down in the case when the projective plane has even order but remains intact when the projective plane is of odd order.

LEMMA 13. *(a) No three tangents of an oval in a finite projective plane of* odd *order are concurrent.*

(b) All the tangents of an oval in a finite projective plane of even order are coincident at one point. (This point is called the *knot* of the oval.)

Proof. Let O be an oval in a projective plane of order q where q is odd. Let x be a point which does not lie on O.

Since O is the disjoint union of the sets $O \cap m$ where m ranges through the lines incident with x, and since O contains an even number of points, it follows that x is incident with an even number of tangents of O. Consequently, if l is the tangent to O at the point z $(z \in O)$, then each point y on l distinct from z lies on at least one other tangent to O. There are q such points and q tangents to O distinct from l . Therefore each point on l not on O lies on precisely two tangents of O and thus no three tangents of O are coincident.

(b) Let O be an oval in a projective plane of order q where q is even. Since there are precisely $q + 1$ tangents of O (Lemma 12) and since each point in the projective plane is incident with precisely $q + 1$ lines, to show that all the tangents of O are coincident, it suffices to show that each point incident with a secant of O is incident with at most one tangent to O .

Let x be a point not on O which lies on a secant l of O . Since O contains an odd number of points and since O may be written as the disjoint union of the sets $O \cap m$ where m ranges through the lines containing x , it follows that x lies on at least one tangent of O . If x is an element of $O \cap l$, then by Lemma 12, x lies on precisely one tangent of O . But since there are $q + 1$ tangents to O and $q + 1$ points on the secant l , it follows that each point on l is incident with precisely one tangent of O . Thus each point which is incident with a secant of O is incident with precisely one tangent of O . //

It is absurd discussing the properties of ovals any further without knowing whether examples of such creatures exist. In the next theorem I will prove that each finite cyclic projective plane possesses an "abundance" of ovals. Preceding this theorem is a discussion of "coordinatising" cyclic projective planes.

(4.1) Let Π be a cyclic projective plane and C a cyclic sharply transitive group of automorphisms of Π . We can identify the points of Π with the elements of C by choosing a point p of Π and then associating the element g of C with the point pg of Π . Since C acts sharply transitively on Π , this is a well defined one to one correspondence between the elements of C and the points of Π . Each line l of Π can be identified with the subset $\Phi(l)$ of C defined by

$$\Phi(l) = \{g \mid g \in C \text{ and } pg \text{ is incident with } l\} .$$

Observe that if x is an element of C, then the line lx corresponds to the subset $\Phi(lx)$ of C.

It is now easy to see that we have defined a projective plane structure on C; the points are the elements of C, the lines are the subsets $\Phi(l)$ of C where l is a line of Π, and where "the point x is incident with the line L" is interpreted as "x is an element of L". In fact the group C acting by right multiplication on itself $(g : x \mapsto xg)$ is a cyclic sharply transitive automorphism group of the projective plane C. Thus C is a cyclic projective plane. Let Φ be the map from the projective plane Π to the projective plane C defined by

$$\Phi : pg \mapsto g \ , \quad g \in C \ ,$$

and

$$\Phi : l \mapsto \Phi(l)$$

where l is a line of Π. It is clear that Φ is a projective plane isomorphism and further, the diagram

$$\begin{tikzcd}
\Pi \arrow[r, "x"] \arrow[d, "\Phi"'] & \Pi \arrow[d, "\Phi"] \\
C \arrow[r, "x"'] & C
\end{tikzcd}$$

commutes for all elements x of C.

One final observation before moving on to Theorem 13. Notice that if Π is a finite cyclic projective plane, then C must act transitively on the set of lines of Π. To see this, let l be a line and let H be the stabiliser of l in C (that is, $H = \{g : g \in G \text{ and } lg = g\}$). Recall that if K is a group acting on a set Ω, then for each element ω of Ω,

$$(4.2) \qquad |K| = |\omega^K| \, |K_\omega|$$

where ω^K is the orbit of ω in Ω under K and K_ω is the stabiliser of

ω in K and as before, $|X|$ denotes the cardinality of the set X.

Let a be a point incident with l. Since C acts sharply transitively on Π, it follows from (4.2) that the stabiliser of a in H is trivial and that the length of each orbit of H on l is $|H|$. Thus $|H|$ divides $|l|$, but $|H|$ divides $|C|$ and therefore $|H|$ divides the greatest common divisor of $|l|$ and $|C|$. If n is the order of Π, then it is well known that $|\Pi| = n^2 + n + 1$ and since C acts sharply transitively on Π it follows from (4.2) that $|C| = n^2 + n + 1$. But $|l| = n + 1$ and therefore the greatest common divisor of $|l|$ and $|C|$ is 1. Therefore $|H| = 1$, so the stabiliser of a line in C is trivial and using (4.2) it is easy to see that C must act transitively on the lines of Π.

(4.3). Consequently we may specify the cyclic projective plane structure on C by specifying just one line L of C. The other lines are then the translates Lg of L where $g \in C$. It is easy to check that if a is a nontrivial element of C, then there is a unique ordered pair (x, y) of elements of L such that $xy^{-1} = a$. (Indeed, $\{x\} = L \cap La$ and $\{y\} = L \cap La^{-1}$.)

(4.4). Conversely, if C is any cyclic group and L is any subset of C with the property that for each nontrivial element a of C, there is a unique ordered pair (x, y) of elements of L such that $xy^{-1} = a$, then C admits a cyclic projective plane structure; the points are the elements of C and the lines are the translates Lg of L $(g \in C)$. Such a pair (C, L) is called a *planar cyclic difference set.*

THEOREM 14. *If* Π *is a finite cyclic projective plane and if* C *is a cyclic sharply transitive group of automorphisms of* Π, *then there is an oval* 0 *in* Π *such that* 0 *meets each of its translates* $0g$ $(g \neq 1$, $g \in C)$ *in precisely one point.*

Proof. In view of (4.3) and (4.4), we need only show that if (C, L)

is a cyclic planar difference set, then C contains a subset O such that $|O \cap Lg| \leq 2$ for all elements g of C and $|O \cap Og| = 1$ for all nontrivial elements g of C.

Denote the set $\{g^{-1} : g \in L\}$ by L^{-1}. I claim that L^{-1} is such a subset. If there is an element g of C such that $|L^{-1} \cap Lg| \geq 3$, then there are distinct elements x, y, z of L such that

$$\{xg, yg, zg\} \subseteq L^{-1} \cap Lg .$$

Since $\{xg, yg, zg\} \subseteq L^{-1}$ and $\{x, y, z\} \subseteq L$, it follows that the set $\{x, y, z, x^{-1}g^{-1}, y^{-1}g^{-1}, z^{-1}g^{-1}\}$ is contained in L. Now

$$\left(y^{-1}g^{-1}\right)\left(x^{-1}g^{-1}\right)^{-1} = xy^{-1} \ (\neq 1 \text{ since } x \neq y)$$

and since (C, L) is a planar cyclic difference set, it follows that $x = y^{-1}g^{-1}$. That is

$$(4.5) \qquad xy = g^{-1} .$$

But

$$\left(y^{-1}g^{-1}\right)\left(z^{-1}g^{-1}\right)^{-1} = zy^{-1} \ (\neq 1 \text{ since } x \neq y)$$

and since (C, L) is a cyclic difference set, it follows that $z = y^{-1}g^{-1}$. That is

$$(4.6) \qquad yz = g^{-1} .$$

Together (4.5) and (4.6) imply $x = z$, contrary to our assumption, that x, y, z are distinct elements of L. Therefore $|L^{-1} \cap Lg| \leq 2$ for all elements g of C. From (4.3) and (4.4) it follows that if g is a nontrivial element of C, then $|L \cap Lg| = 1$. Now

$$L^{-1} \cap L^{-1}g = \left(L \cap Lg^{-1}\right)^{-1} ,$$

thus $|L^{-1} \cap L^{-1}g| = 1$ for all nontrivial elements g of C. //

The Wallis-Whiteman Theorem

Here at last is the elusive Wallis-Whiteman Theorem. It follows a technical lemma.

LEMMA 15 (L.G. Kovács, private communication, 1976). *If* Π *is a finite projective plane of order* q *and* O *and* O' *are ovals in* Π *, then*

$$\sum_{l} (|O \cap l|-1)(|O' \cap l|-1) = q(|O \cap O'|-1) .$$

(*The summation* $\sum_{l}$ *is taken over all lines* l *in* Π *.*)

Proof.

$$(4.7)\quad \sum_{l} (|O \cap l|-1)(|O' \cap l|-1)$$

$$= \sum_{l} |O \cap l||O' \cap l| - \sum_{l} |O \cap l| - \sum_{l} |O' \cap l| + \sum_{l} 1 .$$

Let S, T, E be the set of secants of O , tangents of O and exterior lines of O respectively. Since S, T and E are disjoint and together contain all the lines of Π , it follows that

$$\sum_{l} |O \cap l| = \sum_{l \in S} |O \cap l| + \sum_{l \in T} |O \cap l| + \sum_{l \in E} |O \cap l|$$

$$= 2|S| + |T| .$$

By Lemma 12, $|T| = q + 1$ and since each secant of O is determined by a unique pair of distinct elements of O , it follows that $|S| = \frac{1}{2}q(q+1)$.

Thus

$$(4.8)\quad \sum_{l} |O \cap l| = q + 1 + q(q+1)$$

$$= (q+1)^2 .$$

Similarly $\sum_{l} |O' \cap l| = (q+1)^2$.

The key to the lemma is to notice that because for each line l in Π there are $|O' \cap l|$ points p in O' such that $p \in l$, then

(4.9) $$\sum_{l} |O \cap l||O' \cap l| = \sum_{p \in O'} \sum_{l \ni p} |O \cap l|$$

($\sum_{l \ni p}$ denotes the summation over all lines l of Π which contain p).

Next, since each point p of O is incident with q secants of O and 1 tangent of O, it follows that

(4.10) for all $p \in O$,

$$\sum_{l \ni p} |O \cap l| = 2q + 1 .$$

If p is a point not in O, then O is the disjoint union of the sets $O \cap l$ where l ranges through the lines containing p. Therefore

(4.11) $\sum_{l \ni p} |O \cap l| = q + 1$ for all points p not in O.

Let $O' \backslash O = \{p : p \in O' \text{ and } p \notin O\}$.

$$\begin{aligned}\sum_{l} |O \cap l||O' \cap l| &= \sum_{p \in O'} \sum_{l \ni p} |O \cap l| \quad (4.9)\\ &= \sum_{p \in O' \backslash O} \sum_{l \ni p} |O \cap l| + \sum_{p \in O \cap O'} \sum_{l \ni p} |O \cap l|\\ &= |O' \backslash O|(q+1) + |O \cap O'|(2q+1) \quad (4.10) \text{ and } (4.11)\\ &= (q+1-|O \cap O'|)(q+1) + |O \cap O'|(2q+1)\\ &= (q+1)^2 + |O \cap O'|q .\end{aligned}$$

That is

(4.12) $$\sum_{l} |O \cap l||O' \cap l| = (q+1)^2 + |O \cap O'|q .$$

Finally we return to (4.7).

$$\sum_{l} (|O \cap l|-1)(|O' \cap l|-1) = (q+1)^2 + |O \cap O'|q - 2(q+1)^2 + q^2 + q + 1$$

(4.7), (4.8), (4.12)

$$= q(|O \cap O'|-1) . \qquad //$$

THEOREM 16 (Wallis-Whiteman [28]). *If there is a finite cyclic projective plane of order* q , *then there is a circulant weighing matrix of order* $q^2 + q + 1$ *and weight* q^2 .

Proof (L.G. Kovács, private communication, 1976). If Π is a cyclic projective plane of order q and C a cyclic sharply transitive group of automorphisms of Π, then by Theorem 14, Π contains an oval O such that $|O \cap Og| = 1$ for all nontrivial elements g of C. Let L be a line in Π. Define an n by n matrix A, where $n = q^2 + q + 1$, by defining its ijth entry a_{ij} to be $|Ox^i \cap Lx^j| - 1$.

Now

$$\begin{aligned} a_{ij} &= |Ox^i \cap Lx^j| - 1 \\ &= |(O \cap Lx^{j-i})x^i| - 1 \\ &= |O \cap Lx^{j-i}| - 1 \\ &= a_{0,j-i} . \end{aligned}$$

That is, A is a circulant matrix. Since O is an oval, it follows that A is a circulant matrix with entries in $\{-1, 0, 1\}$. It remains to show that $AA^t = q^2I$.

The ijth entry of AA^t is $\sum_{k=0}^{n-1} a_{ik}a_{jk}$. Applying Lemma 15 we have

$$\begin{aligned} \sum_{k=0}^{n-1} a_{ik}a_{jk} &= \sum_{k=0}^{n-1} (|Ox^i \cap Lx^k|-1)(|Ox^j \cap Lx^k|-1) \\ &= \sum_{l} (|Ox^i \cap l|-1)(|Ox^j \cap l|-1) \\ &= q^2(|Ox^i \cap Ox^j|-1) \\ &= q(|Ox^{j-i} \cap O|-1) \\ &= \begin{cases} q & \text{when } i = j \\ 0 & \text{when } i \neq j . \end{cases} \end{aligned}$$

Thus

$$AA^t = q^2I$$

and A is a circulant weighing matrix of order $q^2 + q + 1$ and weight q^2 . //

REMARK. If in the proof of the preceding theorem we identify the projective plane Π with the cyclic difference set (C, L) and let O be the oval L^{-1} (as in the proof of Theorem 14), then

$$A = B^2 - J$$

where B is the matrix whose ijth entry b_{ij} is given by

$$b_{ij} = \begin{cases} 1 & \text{if } x^i \in Lx^j \\ \\ 0 & \text{if } x^i \notin Lx^j \end{cases}$$

and where J is the matrix whose every entry is 1 . The matrix B is an incidence matrix of the projective plane Π .

To see that $A = B^2 - J$, notice that $b_{ik}b_{kj} = 1$ if and only if $x^i \in Lx^k$ and $x^k \in Lx^j$, that is when $x^k \in L^{-1}x^i \cap Lx^j$. Thus

$$\sum_{k=0}^{n-1} b_{ik}b_{kj} = |L^{-1}x^i \cap Lx^j|$$

and it follows that

$$a_{ij} = |L^{-1}x^i \cap Lx^j| - 1 .$$

That is $A = B^2 - J$. //

POSTSCRIPT. In a draft of a thesis which he intends to submit for a PhD at the University of Adelaide, David Glynn has given a proof of a more general theorem. Roughly speaking it asserts that if Π and Π' are two cyclic projective planes of order q , then we can find an incidence matrix A of Π and an incidence matrix B of Π' such that $AB - J$ is a circulant weighing matrix of order $q^2 + q + 1$ and weight q^2 . The proof of this theorem uses similar techniques to Kovács proof of the Wallis-

Whiteman Theorem.

Equations in Finite Cyclic Projective Planes

By now it should be apparent that the problem of finding all circulant weighing matrices and the problem of finding all finite cyclic projective planes are intimately related (via Theorems 7 and 16). According to Dembowski [7], there is good evidence to suggest that the order of a finite cyclic projective plane is always a prime power.

In this section of the thesis, I shall intentionally blur the distinction between a cyclic projective plane and the associated planar cyclic difference set given by (4.3) and (4.4). Thus I can refer to ovals and lines etc. in planar difference sets. By an equation in a cyclic projective plane, I shall mean an equation in the associated cyclic difference set. For example, if Π is a cyclic projective plane and (C, L) is the associated planar cyclic difference set (given by (4.3)), then for a nontrivial element a of C, the equation

$$xy^{-1} = a$$

has a unique solution (x, y) with x and y elements of L (see (4.3) and (4.4)).

LEMMA 17. *If* (C, L) *is a planar cyclic difference set where* $1 \in L$, *then* L^{-1} *is an oval and for each point* x *in* L, *the tangent to* L^{-1} *at the point* x^{-1} *is the line* Lx^{-2}.

Proof. The fact that L^{-1} is an oval follows immediately from Theorem 14. We have to show that for each point x in L,

$$L^{-1} \cap Lx^{-2} = \{x^{-1}\} .$$

Since $x \in L$, it follows that $x^{-1} \in Lx^{-2}$ and $x^{-1} \in L^{-1}$. That is $x^{-1} \in L^{-1} \cap Lx^{-2}$. If there is a point y in L such that

$$\{x^{-1},\ yx^{-2}\} \subseteq L^{-1} \cap Lx^{-2}\ ,$$

then $x^2y^{-1} \in L$ and so

$$\{x,\ y,\ x^2y^{-1}\} \subseteq L\ .$$

But $(x^2y^{-1})x^{-1} = xy^{-1}$ and since $(C,\ L)$ is a planar cyclic difference set, either $xy^{-1} = 1$ or $x^2y^{-1} = x$. In either case $\{x^{-1},\ yx^{-2}\} = \{x^{-1}\}$. //

The following theorem now gives us information about equations of the kind $xy^{-2} = a$.

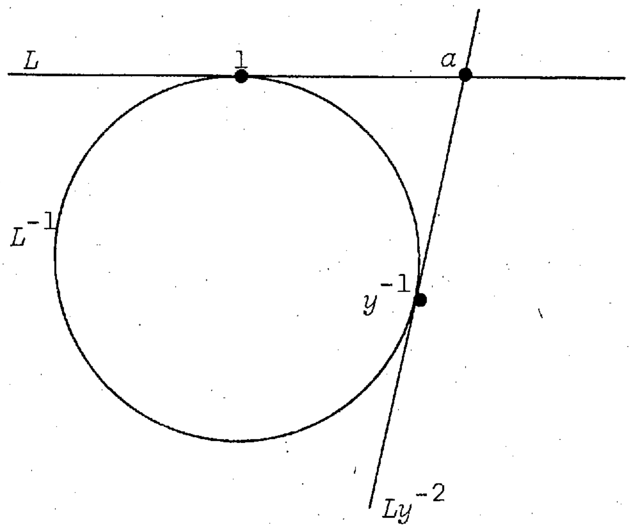
THEOREM 18. *(i) If* $(C,\ L)$ *is a planar cyclic difference set of odd order if* $1 \in L$ *and if* a *is a nontrivial element of* L *, then the equation*

$$xy^{-2} = a$$

has a unique solution $(x,\ y)$ *with* x *and* y *elements of* L *and* $y \neq 1$.

(ii) If $(C,\ L)$ *is a planar cyclic difference set of even order and if* $1 \in L$ *, then*

$$|\{xy^{-2}\ :\ x,\ y \in L \ \text{ and } \ y \neq 1\} \cap L| = 1\ .$$



(i) If a is a nontrivial element of L, then by Lemma 13 *(a)* there is a point y^{-1} in L^{-1}, $y \neq 1$, such that the tangent to L^{-1} at y^{-1} meets L at a. By Lemma 17, this tangent is Ly^{-2}.

Therefore

$$a = L \cap Ly^{-2} .$$

Since $y \neq 1$ and since $|C| \equiv 1 \bmod 2$, it follows that $y^{-2} \neq 1$ and thus $L \neq Ly^{-2}$. Therefore there is a unique element x of L such that

$$\{a\} = \{xy^{-2}\} = L \cap Ly^{-2} .$$

(ii) By Lemma 13 *(b)*, all the tangents of L^{-1} intersect at a single point. Let this point be a. If x and y are elements of L and $y \neq 1$ then $xy^{-2} \in Ly^{-2}$. The line Ly^{-2} is the tangent to L^{-1} at y^{-1}, so if $xy^{-2} \in L$, then $xy^{-2} = a$. Thus

$$\{xy^{-2} : x, y \in L \text{ and } y \neq 1\} \cap L = \{a\} . \qquad //$$

Postscript

I do not know whether Theorem 18 provides any nontrivial information about cyclic projective planes. So far I have not been able to produce a stronger result. However it appears plausible that combined with the Hall Multiplier Theorem (see Baumert [3]), Theorem 18 may provide some new information about the number of primes which may divide the order of a cyclic difference set. (Hopefully one can show there is only one prime dividing the order of the difference set!)

Thank you for reading my thesis.

REFERENCES

[1] E. Artin, *Geometric Algebra* (Interscience Tracts in Pure and Applied Mathematics, 3. Interscience, New York, London, 1957).

[2] Reinhold Baer, *Linear Algebra and Projective Geometry* (Academic Press, New York, London, 1952).

[3] Leonard D. Baumert, *Cyclic Difference Sets* (Lecture Notes in Mathematics, 182. Springer-Verlag, Berlin, Heidelberg, New York, 1971).

[4] Elwyn R. Berlekamp, *Algebraic Coding Theory* (McGraw-Hill, New York, St. Louis, San Francisco, Toronto, London, Sydney, 1968).

[5] Garrett Birkhoff and Saunders Mac Lane, *A Survey of Modern Algebra* (Macmillan, New York, 1941).

[6] John A. Decker, Jr., and Martin O. Harwitt, "Sequential encoding with multislit spectrometers", *Appl. Optics* 7 (1968), 2204-2209.

[7] P. Dembowski, *Finite Geometries* (Ergebnisse der Mathematik und ihrer Grenzgebiete, 44. Springer-Verlag, Berlin, Heidelberg, New York, 1968).

[8] Jean Dieudonne, *La Geometrie des Groupes Classique* (Ergebnisse der Mathematik und ihrer Grenzgebiete, 5. Springer-Verlag, Berlin, Heidelberg, New York, 1955).

[9] Peter Eades and Richard M. Hain, "On circulant weighing matrices", *Ars. Combin.* (to appear).

[10] Anthony V. Geramita, Joan Murphy Geramita, Jennifer Seberry Wallis, "Orthogonal designs", *J. Lin. Multlin. Algebra* 3 (1975/76), 281-306.

[11] Anthony V. Geramita and Jennifer Seberry Wallis, "Orthogonal designs III: weighing matrices", *Utilitas Math.* 6 (1974), 209-236.

[12] J. Hadamard, "Resolution d'une question relative aux determinants", *Darboux Bull.* (2) 17 (1893), 240-246.

[13] Paul R. Halmos, "How to write mathematics", *Enseignement Math.* 16 (1970), 123-152. See also: Norman E. Steenrod, Paul R. Halmos, Menahem M. Schiffer, Jean A. Dieudonne, *How to Write Mathematics* (Amer. Math. Soc., Providence, Rhode Island, 1973).

[14] D.R. Hughes, F.C. Piper, *Projective Planes* (Graduate Texts in Mathematics, 6. Springer-Verlag, New York, Heidelberg, Berlin, 1973).

[15] R.N. Ibbett, D. Aspinall, and J.F. Grainger, "Real-time multiplexing of dispersed spectra in any wavelength region", *Appl. Optics* 7 (1968), 1089-1903.

[16] Jacobus H. van Lint, *Coding Theory* (Lecture Notes in Mathematics, 201. Springer-Verlag, Berlin, Heidelberg, New York, 1971).

[17] Thomas Muir, *The Theory of Determinants in the Historical Order of Development.* Volume Two: *The Period* 1841 *to* 1860 (St. Martin's Press, 1911. Reprinted Dover, New York, 1960).

[18] R.C. Mullin, "A note on balanced weighing matrices", *Combinatorial Mathematics* III (Proc. Third Australian Conf., University of Queensland, 1974. Lecture Notes in Mathematics, 452, 28-41. Springer-Verlag, Berlin, Heidelberg, New York, 1975).

[19] R.C. Mullin and R.G. Stanton, "Group matrices and balanced weighing designs", *Utilitas Math.* 8 (1975), 277-301.

[20] R.C. Mullin and R.G. Stanton, "Balanced weighing matrices and group divisible designs", *Utilitas Math.* 8 (1975), 303-310.

[21] Morris Newman, *Integral Matrices* (Pure and Applied Mathematics, 45. Academic Press, New York and London, 1972).

[22] R.E.A.C. Paley, "On orthogonal matrices", *J. Math. Massachusetts* 12 (1933), 311-320.

[23] James Singer, "A theorem in finite projective geometry and some applications to number theory", *Trans. Amer. Math. Soc.* 43 (1938), 377-385.

[24] Neil J.A. Sloane and Martin Harwitt, "Masks for Hadamard transform optics, and weighing designs", *Appl. Optics* 15 (1976), 107-114.

[25] R.G. Stanton and R.C. Mullin, "On the nonexistence of a class of circulant balanced weighing matrices", *SIAM J. Appl. Math.* 30 (1976), 98-102.

[26] James Joseph Sylvester, "Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers", *Philos. Mag.* 34 (1867), 461-475. See also: *The Collected Mathematical Papers of James Joseph Sylvester*, Volume II (1854-1873), 615-628 (Chelsea, New York, 1973).

[27] Richard J. Turyn, "Sequences with small correlation", *Error Correcting Codes* (Proc. Sympos. Math. Res. Center, Madison, Wis., 1968, 195-228. John Wiley & Sons, New York, 1968).

[28] Jennifer Seberry Wallis and Albert Leon Whiteman, "Some results on weighing matrices", *Bull. Austral. Math. Soc.* 12 (1975), 433-447.