Pacific Journal of Mathematics

ON THE NUMBER OF ABSOLUTE POINTS OF A CORRELATION

ALAN JEROME HOFFMAN, MORRIS NEWMAN,
ERNST GABOR STRAUS AND OLGA TAUSSKY

Vol. 6, No. 1 November 1956

ON THE NUMBER OF ABSOLUTE POINTS OF A CORRELATION

A. J. HOFFMAN, M. NEWMAN, E. G. STRAUS AND O. TAUSSKY

1. Introduction. In 1948, R. W. Ball [2] presented methods for obtaining information about the number of absolute points of a correlation of a finite projective plane in which neither the theorem of Desargues nor any other special property (except, of course, the existence of the correlation) is assumed. This work was, in a sense, a continuation of an earlier investigation by R. Baer [1] of the case that the correlation is a polarity.

We shall show how, using an incidence-matrix approach[1], one may obtain the principal results of [2] somewhat more directly. Some of the results are strengthened. In addition, our method is sufficiently general to apply at once to the so-called symmetric group divisible designs, a class of combinatorial configurations including the finite projective planes. For simplicity, we shall present our main discussion in the language of planes, reserving to the end indications of the generalization.

As pointed out in §§ 3 and 4 the geometric problem with which we are concerned leads naturally to the question: What are the irreducible polynomials whose roots are roots of natural numbers? This question is treated in the following section.

2. Polynomials whose roots are roots of natural numbers. Let $f(x)$ be an irreducible polynomial with integral coefficients and let one of its roots be $z=n^{1/k}\zeta$, (n, k natural numbers, ζ a root of unity). Clearly z satisfies the equation

$$z^k/n=\zeta^k=\zeta_h \tag{1}$$

for some h, where from now on we use ζ_h to denote a primitive hth root of unity. From (1) we see that $\Phi_h(z^k/n)=0$, where Φ_h is the cyclotomic polynomial of order h. Hence

$$f(x)\mid n^{\varphi(h)}\Phi_h(x^k/n)\,. \tag{2}$$

The problem is therefore reduced to that of finding the irreducible factors of $\Phi_h(x^k/n)$ for arbitrary positive integers h, k, n. It will suffice

Received August 16, 1954. The work of the first two authors was supported (in part) by the Office of Naval Research.

[1] Arithmetic properties of the incidence matrix have been exploited with conspicuous success ([4], [5]). In this paper we study its characteristic polynomial.

for our purpose here to consider only the reducibility of $\Phi_h(x^2/n)$ (that is the case $k=2$). The general case is settled in the note following this paper [9].

If $n^{\varphi(h)}\Phi_h(x^2/n)$ is divisible by an irreducible polynomial $g(x)$, then $g(x)$ is not a polynomial in x^2. Hence $g(-x)$, which also divides $n^{\varphi(h)}\Phi_h(x^2/n)$, is different from $g(x)$ and is irreducible. Therefore,

$$n^{\varphi(h)}\Phi_h(x^2/n) = \pm g(x)g(-x)\,, \tag{3}$$

for $g(x)g(-x)$ is a polynomial in x^2, and $n^{\varphi(h)}\Phi_h(x^2/n)$ is irreducible in x^2. Then by (3), $\sqrt{n}\zeta_h$ or $-\sqrt{n}\zeta_h$ is a root of $g(x)$; thus $\zeta_h=(\pm\sqrt{n}\zeta_h)^2/n$ is in the splitting field for $g(x)$. Thus the splitting field for $g(x)$ contains the hth roots of unity; but by (3), the degree of this splitting field is $\varphi(h)$. Therefore the splitting field for $g(x)$ is the same as $R(\zeta_h)$. Conversely since $\sqrt{n}\zeta_h$ is a root of $\Phi_h(x^2/n)$, $\sqrt{n}\zeta_h \in R(\zeta_h)$ implies that $\Phi_h(x^2/n)$ is reducible. We are thus led to the following lemma:

LEMMA 1. *The polynomial $\Phi_h(x^2/n)$ is reducible if and only if $\sqrt{n}\zeta_h$ is contained in $R(\zeta_h)$.*

LEMMA 2. *The polynomial $\Phi_h(x^2/n)$ where $n=n^{*2}n'$, n' squarefree, is reducible if and only if $n'|h$ and one of the following conditions holds*:

(a) $h\equiv 1 \pmod 2$ *and* $n'\equiv 1 \pmod 4$;
(b) $h\equiv 2 \pmod 4$ *and* $n'\equiv 3 \pmod 4$;
(c) $h\equiv 4 \pmod 8$ *and* $n'\equiv 0 \pmod 2$.

Proof. We first list for convenience several facts to which we shall make reference in the course of this proof and subsequently.

(i) The discriminant of a subfield of an algebraic number field divides the discriminant of the whole field [7, p. 95, Satz 39].

(ii) The discriminant of $R(\sqrt{m})$, m a squarefree integer, is $4m$ if $m\equiv 2, 3 \pmod 4$, and m if $m\equiv 1 \pmod 4$ [7, p. 157, Satz 95].

(iii) The discriminant of the field of the mth roots of unity is divisible only by primes which divide m [7, p. 146, Satz 88].

(iv)
$$\sum_{j=0}^{m-1}\zeta_m^{j^2} = \begin{cases} (1+i)\sqrt{m} & \text{if } m\equiv 0 \pmod 4 \\ \sqrt{m} & \text{if } m\equiv 1 \pmod 4 \\ i\sqrt{m} & \text{if } m\equiv 3 \pmod 4 \end{cases}$$

[8, p. 177, Theorem 99].

(v) If $(r, s)=1$, then $\zeta_r\zeta_s$ is a primitive rsth root of unity.

(vi) If m is odd and squarefree, $m|r$ then $\{(-1)^{(m-1)/2}m\}^{1/2} \in R(\zeta_r)$ (This can be shown in a variety of ways: for example, from (iv) or from (i), (ii), (iii)).

We now turn to the proof proper. We first prove the necessity. Assume $\Phi_h(x^2/n)$ is reducible; that is, by Lemma 1,

$$(4) \qquad \sqrt{n'\zeta_h} \in R(\zeta_h) .$$

Therefore $\sqrt{n'} \in R(\sqrt{\zeta_h})$, so by (i), (ii), (iii), n' is the product of primes each of which divides $2h$. If h is even, then $n'|h$. If h is odd, then since $\varphi(2h)=\varphi(h)$, we have $R(\sqrt{\zeta_h})=R(\zeta_h)$, so that by (i), (ii) and (iii) we have again $n'|h$. Next,

(a) Assume h odd. Then $\sqrt{\zeta_h} \in R(\zeta_h)$, so that (4) implies $n' \in R(\zeta_h)$. Further n' is odd, since $n'|h$, so either $n' \equiv 1 \pmod 4$ or $n' \equiv 3 \pmod 4$. But we cannot have $n' \equiv 3 \pmod 4$, for, by (ii), (i), and (iii), this would imply $2|h$.

(b) Assume $h \equiv 2 \pmod 4$. Then, since $\varphi(2h) > \varphi(h)$, it follows that $\sqrt{\zeta_h} \notin R(\zeta_h)$, so $\sqrt{n'\zeta_h} \in R(\zeta_h)$ implies $\sqrt{n'} \notin R(\zeta_h)$. If n' is odd, this implies $n' \equiv 3 \pmod 4$, by the fact that $n'|h$ and (vi). Further n' cannot be even. If n' were even, write $n'=2n''$. There are two cases: $n'' \equiv 1 \pmod 4$, $n'' \equiv 3 \pmod 4$. If $n'' \equiv 1 \pmod 4$, then $\sqrt{n'\zeta_h} = \sqrt{2}\sqrt{n''}\sqrt{\zeta_h} \in R(\zeta_h)$ implies $\sqrt{2}\sqrt{\zeta_h} \in R(\zeta_h)$, since $\sqrt{n''} \in R(\zeta_h)$ by the fact that $n''|h$ and (vi). But this means $\sqrt{2} \in R(\zeta_h)$, which is impossible. For $R(\sqrt{\zeta_h})$ contains i; and if it also contains $\sqrt{2}$, it would contain $\zeta_8=(1+i)/\sqrt{2}$. By (v), it follows that $R(\sqrt{\zeta_h})$ would then contain a primitive $8(h/2)=4h$th root of unity; therefore the degree of $R(\zeta_h)$ would be at least $\varphi(4h) > \varphi(2h)$; the actual degree of $R(\sqrt{\zeta_h})$.

If $n'' \equiv 3 \pmod 4$, then $\sqrt{n''\zeta_h} \in R(\zeta_h)$, for $i\sqrt{n''} \in R(\zeta_h)$ by the fact that $n''|h$ and (vi), and it is easy to see (for example by (v)) that $i\sqrt{\zeta_h} \in R(\zeta_h)$. Therefere $\sqrt{n''\zeta_h} = (i\sqrt{n''})(-i\sqrt{\zeta_h}) \in R(\zeta_h)$. Hence, $\sqrt{2} \in R(\zeta_h)$, and a fortiori $\sqrt{2} \in R(\sqrt{\zeta_h})$, and the preceding argument applies.

(c) Assume finally $h \equiv 4 \pmod 8$. Then n' cannot be odd. For since $R(\zeta_h)$ contains i, and $n'|h$, we learn from (vi) that $\sqrt{n'} \in R(\zeta_h)$. Therefore, $\sqrt{n'\zeta_h} \in R(\zeta_h)$ implies $\sqrt{\zeta_h} \in R(\zeta_h)$, which is impossible, since $\varphi(2h) > \varphi(h)$.

It remains to show that if $h \equiv 0 \pmod 8$, then $\sqrt{n'\zeta_h} \notin R(\zeta_h)$ for any n'. The argument used in (c) shows that n' cannot be odd. If n' were even, $n'=2n''$, then since $\zeta_8=(1+i)/\sqrt{2}$ and $i \in R(\zeta_h)$, we have $\sqrt{2} \in R(\zeta_h)$. Hence $\sqrt{n'\zeta_h} = \sqrt{2n''\zeta_h} \in R(\zeta_h)$ implies $\sqrt{n''\zeta_h} \in R(\zeta_h)$. Then we may use the argument just given to cover the case in which n' is odd. Hence we cannot have $h \equiv 0 \pmod 8$.

The sufficiency is established simply by constructing $g(x)$ of (3). We first prove that in cases (a), (b)

$$(5) \qquad z = n^*\zeta_h \sum_{j=0}^{n'-1} \zeta_h^{hj^2/n'} = \frac{n^*n'}{h}\zeta_h \sum_{j=0}^{h-1} \zeta_h^{hj^2/n'}$$

is a zero of $\Phi_h(x^2/n)$. Since $\zeta_h^{h/n'}$ is a primitive n'th root of unity we obtain from (iv):

$$\text{in case (a)} \quad z=n^*\sqrt{n'}\zeta_h=\sqrt{n}\,\zeta_h=\text{a zero of } \Phi_h(x^2/n)\,;$$

$$\text{in case (b)} \quad z=n^*\sqrt{n'}i\zeta_h=\sqrt{n}\,\zeta_1\zeta_h=\text{a zero of } \Phi_h(x^2/n)\,.$$

In case (c) we have

$$(6) \qquad z=\frac{1}{2}n^*\zeta_h\sum_{j=0}^{2n'-1}\zeta_h^{hj^2/2n'}=\frac{1}{2}n^*\sqrt{2n'}(1+i)\zeta_h=n^*\sqrt{n'}\zeta_8\zeta_h\,,$$

a zero of $\Phi_h(x^2/n)$. The conjugates $z^{(l)}$ of z in $R(\zeta_h)$ are now obtained simply by substituting ζ_h^l for ζ_h in (5) or (6) where $(l,h)=1$. Thus we obtain

$$g(x)=\prod_{\substack{l=1\\(l,h)=1}}^{h-1}(x-z^{(l)})\,.$$

Later on we shall need the sum of the $z^{(l)}$. We therefore establish the following lemma:

LEMMA 3. *If* (3) *holds, then the sum of the roots of* $g(x)$ *is*

(a) $\pm n^*n'$ *if* $h\not\equiv 0 \pmod 4$ *and squarefree,*

(b) 0 *if* $h\not\equiv 0 \pmod 4$ *and* h *is not squarefree,*

(c) $\pm n^*n'$ *if* $h\equiv 0 \pmod 4$ *and* $h/4$ *is odd and squarefree,*

(d) 0 *if* $h\equiv 0 \pmod 4$ *and* $h/4$ *is odd and not squarefree.*

Proof. Let us first note that, by Lemma 2, the foregoing enumeration accounts for all cases in which $n^{\varphi(h)}\Phi_h(x^2/n)$ may be reducible. Also, the $\pm$ in (a) and (c) is to be expected, since we are clearly unable to distinguish between $g(x)$ and $g(-x)$.

We now set $h=2^e p_1^{e_1}\cdots p_k^{e_k}$, $n'=2^\varepsilon p_1^{\varepsilon_1}\cdots p_k^{\varepsilon_k}$ where $\varepsilon, \varepsilon_i=0,1$; and write $h_0=2^e$, $h_i=p_i^{e_i}$; $n_0'=2^\varepsilon$, $n_i'=p_i^{\varepsilon_i}$; $\zeta_{(0)}=\zeta_{h_0}$, $\zeta_{(j)}=\zeta_{h_j}$.

Then $\zeta_h=\zeta_{(0)}\zeta_{(1)}\cdots\zeta_{(k)}$ and its conjugates ζ_h^l are the products of the conjugates $\zeta_{(0)}^{l_0}, \zeta_{(1)}^{l_1}, \cdots, \zeta_{(k)}^{l_k}$ where $l=l_i \pmod{h_i}$. Cases (a), (b) of this lemma correspond to cases (a), (b) of Lemma 2. Here $\zeta_0=\pm 1$ so that we obtain from (5)

$$(7) \qquad \sum z^{(l)}=\pm n^*\sum_{j=0}^{n'-1}\prod_{i=1}^{k}\sum_{\substack{l_i=1\\(l_i,p_i)=1}}^{h_i-1}\zeta_{(l)}^{l_i[hj^2/n'+1]}\,.$$

As j runs from 0 to $n'-1$ its residues (mod n_i') run independently from 0 to $n_i'-1$; hence we can write

$$(8)\qquad a=\sum z^{(l)}=\pm n^*\prod_{i=1}^{k}\sum_{j_i=0}^{n_i'-1}\sum_{\substack{l_i=1\\(l_i,\,p_i)=1}}^{h_i-1}\zeta_{(i)}^{l_i[h_ij_i^2/n'+1]}=\pm n^*a_1\cdots a_k\,.$$

In order to evaluate the a_i we first observe that the sum of the primitive mth roots of unity

$$(9)\qquad \sum_{\substack{l=1\\(l,m)=1}}^{m-1}\zeta_m^l=\mu(m)\,.$$

This is seen most simply by observing that

$$\Phi_m(x)=\prod_{d\mid m}(x^d-1)^{\mu(m/d)}=x^{\varphi(m)}-\mu(m)x^{\varphi(m)-1}+\cdots\,.$$

Now for $h_i>n_i'$ we have $\zeta_{(i)}^{[h_ij^2/n'+1]}$ a primitive h_ith root of unity and therefore

$$(10)\qquad a_i=\sum_{j_i=0}^{n_i'-1}\sum_{\substack{l_i=1\\(l_i,\,p_i)=1}}^{h_i-1}\zeta_{(i)}^{l_i[h_ij_i^2/n'+1]}=\sum_{j_i=0}^{n_i'-1}\mu(h_i)=n_i'\mu(h_i)\,.$$

For $h_i=n_i'$ we have h/n' relatively prime to p_i so that

$$(11)\qquad \sum_{j_i=0}^{n_i'-1}\zeta_{(i)}^{h_ij_i^2/n'}=\pm\sum_{j_i=0}^{n_i'-1}\zeta_{(i)}^{j_i^2}=\pm\begin{cases}\sqrt{p_i} & \text{if } p_i\equiv 1 \pmod 4\\ i\sqrt{p_i} & \text{if } p_i\equiv 3 \pmod 4\,.\end{cases}$$

Where the sign depends on whether h/n' is or is not a quadratic residue (mod p_i). Similarly

$$(12)\qquad \sum_{j_i=0}^{n_i'-1}\zeta_{(i)}^{l_ij_i^2}=\left(\frac{l_i}{p_i}\right)\sum_{j_i=0}^{n_i'-1}\zeta_{(i)}^{j_i^2}\,,\qquad \left(\frac{l_i}{p_i}\right)=\text{Legendre symbol.}$$

From (11) and (12) we obtain

$$(13)\qquad a_i=\pm\sum_{\substack{l_i=1\\(l_i,\,p_i)=1}}^{n_i'-1}\left(\frac{l_i}{p_i}\right)\zeta_{(i)}^{l_i}\sum_{j_i=0}^{n_i'-1}\zeta_{(i)}^{j_i^2}\,.$$

Now

$$(14)\qquad \sum\left(\frac{l_i}{p_i}\right)\zeta_{(i)}^{l_i}=\sum_1\zeta_{(i)}^{s}-\sum_2\zeta_{(i)}^{t}\,,$$

where $\sum_1$ ranges over those s in $1,\cdots,p_i-1$ which are quadratic residues (mod p_i) and $\sum_2$ ranges over those t in $1,\cdots,p_i-1$, which are quadratic nonresidues (mod p_i). According to (9)

$$(15)\qquad \sum_1\zeta_{(i)}^{s}+\sum_2\zeta_{(i)}^{t}=\mu(p_i)=-1$$

and obviously

$$\sum_{j_i=0}^{n_i'-1} \zeta_{(i)}^{j_i^2} = 1 + 2\sum_1 \zeta_{(i)}^{s} . \tag{16}$$

Combining (15) and (16) we have

$$\sum_1 \zeta_{(i)}^{s} - \sum_2 \zeta_{(i)}^{t} = \sum_{j_i=0}^{n_i'-1} \zeta_{(i)}^{j_i^2} \tag{17}$$

Substitution in (13) now yields

$$a_i = \pm\left(\sum_{j_i=0}^{n_i'-1} \zeta_{(i)}^{j_i^2}\right)^2 = \pm p_i = \mp n_i' \mu(h_i) . \tag{18}$$

From (8), (10) and (18) we now obtain

$$a = \pm n^* n' \mu(h) , \tag{19}$$

which proves cases (a), (b). In cases (c), (d) we have case (c) of Lemma (2) and therefore equation (6) obtains. We now have $a = \pm n^* a_0 a_1 \cdots a_k$ where $a_1, \cdots, a_k$ are the same as in (10) and (18). The only new factor is according to (6)

$$a_0 = \frac{1}{2} \sum_{\substack{l_0=1 \\ l_0 \text{ odd}}}^{3} \sum_{j_0=0}^{3} \zeta_{(0)}^{l_0[h_0 j_0^2/4+1]} . \tag{20}$$

If $h_0 > 4$ then, as in (10), we obtain

$$a_0 = 2\mu(h_0) = n_0 \mu(h_0) = n_0 \mu(h_0/2) = 0 . \tag{21}$$

If $h_0 = 4$ then $\zeta_{(0)} = i$ and

$$a_0 = \frac{1}{2}[\zeta_{(0)} + \zeta_{(0)}^2 + \zeta_{(0)}^5 + \zeta_{(0)}^{10} + \zeta_{(0)}^3 + \zeta_{(0)}^6 + \zeta_{(0)}^{15} + \zeta_{(0)}^{30}] = -2 = n_0 \mu(h_0/2) . \tag{22}$$

Thus, finally, in cases (c), (d)

$$a = \pm n^* n' \mu(h/2) \tag{23}$$

which proves these cases.

3. The incidence matrix. We assume that we have a finite projective plane Π with $n+1$ points on a line, $n > 1$, and consequently $N = n^2 + n + 1$ points in the plane. We further assume that the plane admits a correlation ρ, that is a one-to-one mapping of the set of points of Π onto the set of lines of Π, together with a one-to-one mapping of the set of lines of Π onto the set of points of Π such that a point is on a line if and only if the image of the point is on the image of the line.

Our attack on the study of the number of absolute points of a correlation, that is, the set of points each of which lies on its image, is based on the following:

LEMMA 4. *Let ρ be a correlation of a finite projective plane Π, and let the points $P_1, \cdots, P_N$ and lines $l_1, \cdots, l_N$ of Π be so numbered that $\rho P_i = l_i$ $(i=1, \cdots, N)$. Let $A=(a_{ij})$ be a square matrix of order N defined by the rule $a_{ij}=1$ if P_i is on l_j, and 0 otherwise, and let $P=(p_{ij})$ be a permutation matrix defined by $p_{ij}=1$ if $\rho^2 P_i = P_j$, and 0 otherwise. Then if A^T denotes the transpose of A, we have* (i) *$A^T=PA$, and* (ii) *the number of absolute points of ρ is* tr A (the trace of A).

Proof. The second part of the lemma is immediate. To prove (i), observe that the (i,j)th element of A^T is $1 \Leftrightarrow a_{ji}=1 \Leftrightarrow P_j$ is on $l_i \Leftrightarrow l_j = \rho P_j$ is on $\rho l_i = \rho^2 P_i$. But from the definition of P, the (i,j)th element of PA, is $1 \Leftrightarrow \rho^2 P_i$ is on l_j. Hence $A^T=PA$.

Of course, it is also true that if A is an incidence matrix of a finite projective plane, and there exists a permutation matrix $P=(p_{ij})$ such that $A^T=PA$, then the mappings $P_i \to l_i$; $l_i \to P_j$, where $p_{ij}=1$, define a correlation.

Because of (ii), it is clear that knowledge of the eigenvalues of A will contribute to the solution of our problem. Now, $A^T=PA$ implies A is normal. For if $A^T=PA$, then $A=A^TP^T$. Hence $AA^T=A^TP^TPA=A^TA$. Thus the eigenvalues of AA^T are the squares of the moduli of the eigenvalues of A. But the eigenvalues of AA^T can easily be computed from the fact that the incidence properties of a plane imply

$$AA^T = nI + J \tag{24}$$

where I is the identity matrix and J is the matrix every element of which is unity [4]. The eigenvalues of AA^T are

$$(n+1)^2, n, n, \cdots, n\ . \tag{25}$$

But by (24), $n+1$ is an eigenvalue of A with $(1, 1, \cdots, 1)$ as corresponding eigenvector; hence the eigenvalues of A are

$$n+1, \sqrt{n}\,e^{i\alpha_1}, \sqrt{n}\,e^{i\alpha_2}, \cdots, \sqrt{n}\,e^{i\alpha_{N-1}} \tag{26}$$

Let the permutation P split up into cycles of length $d_1, d_2, \cdots, d_r$; $d_1+d_2+\cdots+d_r=N$. Then the eigenvalues of P are the d_1th roots of unity, the d_2th roots of unity, $\cdots$, and the d_rth roots of unity. If we write out these eigenvalues of P as

$$1, e^{i\theta_1}, e^{i\theta_2}, \cdots, e^{i\theta_{N-1}} \tag{27}$$

then it follows from $A^TA^{-1}=P$, the normality of A, (26), and (27) that

$$e^{-i\theta_j}=e^{2i\alpha_j} \qquad j=1, 2, \cdots, N-1. \tag{28}$$

These elementary considerations alone suffice to prove the following:

THEOREM 1 (see [2, Theorem 2.1] and [1, Theorem 4]). *If* $n=n^{*2}n'$, *where* n' *is squarefree, and* M *is the number of absolute points of* ρ, *then* $M\equiv 1 \pmod{n^*n'}$.

Proof. By (26) and Lemma 4, we have

$$M=n+1+\sqrt{n}\,t\,, \tag{29}$$

where $t=\sum_{j=1}^{N-1}e^{i\alpha_j}$ is an algebraic integer, by (27) and (28). Therefore, $(M-(n+1))^2\equiv 0 \pmod{n}$, which implies the theorem.

4. The characteristic polynomial. By virtue of (26), the characteristic polynomial of A may be written

$$(x-(n+1))Q(x)\,, \tag{30}$$

where $Q(x)=(x-\sqrt{n}\,e^{i\alpha_1})(x-\sqrt{n}\,e^{i\alpha_2})\cdots(x-\sqrt{n}\,e^{i\alpha_{N-1}})$. Then since $N-1=n^2+n$ is even, we have

$$Q(x)Q(-x)=(x^2-ne^{2i\alpha_1})(x^2-ne^{2i\alpha_2})\cdots(x^2-ne^{2i\alpha_{N-1}})\,. \tag{31}$$

From (27), the fact that the complex conjugate of a dth root of unity is a dth root of unity, and the definition of $d_1, d_2, \cdots, d_r$, we may write the characteristic polynomial of P as

$$\prod_{i=1}^{r}(x^{d_i}-1)=(x-1)(x-e^{-i\theta_1})(x-e^{-i\theta_2})\cdots(x-e^{-i\theta_{N-1}})\,. \tag{32}$$

In (22), replace x by x^2/n and multiply both sides by n^N. There results

$$\prod_{i=1}^{r}(x^{2d_i}-n^{d_i})=(x^2-n)(x^2-ne^{-i\theta_1})\cdots(x^2-ne^{-i\theta_{N-1}})\,. \tag{33}$$

Comparing (33) and (31) we deduce

$$\frac{1}{x^2-n}\prod_{i=1}^{r}(x^{2d_i}-n^{d_i})=Q(x)Q(-x)\,, \tag{34}$$

so that the irreducible factors of $Q(x)$ are of the type discussed in §2.

5. The number of absolute points of ρ. In this section we apply the results of §2 to present criteria sufficient to insure that $M=n+1$. If we write

$$Q(x)=x^{N-1}+ax^{N-2}+bx^{N-3}+\cdots,$$

Then by (30), $M=n+1-a$.

We wish to prove that, under certain circumstances, $a=0$, and this will certainly hold if every irreducible factor of the left side of (34) is a polynomial in x^2. These factors are the irreducible factors of $\Phi_h(x^2/n)$, $h|d_i$, which were investigated in § 2.

On the basis of Lemma 2, we can assert the following.

THEOREM 2. *If, for each divisor of the orders $d_1, d_2, \cdots, d_r$ of the cycles of P, none of the conditions of Lemma 2 holds, then $M=n+1$. In particular* (see [2]), *$M=n+1$ if n' and $d=$*l.c.m.$\{d_i\}$ *satisfy one of the following*:

(a) $n' \nmid d$;

(b) $2n' \nmid d$ *and* $n' \not\equiv 1 \pmod 4$;

(c) *there exist odd primes p and q such that* $p \equiv q \pmod{2d}$ *and* $(n'/p)(n'/q)=-1$, *where (a/b) is the generalized Legendre-Jacobi symbol*;

(d) $d=1, 2$, *or* p^k, *where p is a prime* $\equiv 3 \pmod 4$, *k a positive integer*, $n'>1$.

Proof. The principal statement is an immediate consequence of Lemma 2.

Proof of (a): Since $n' \nmid d$ implies $n' \nmid h$ for any $h|d_i$, the irreducibility of each $\Phi_h(x^2/n)$ follows from Lemma 2.

Proof of (b): Assume (b) false. Then by virtue of (a), we may assume there exists a positive integer h such that for some d_i we have $n'|h|d_i$, and $\Phi_h(x^2/n)$ reducible. If h is odd, then we obtain the contradiction $n' \equiv 1 \pmod 4$ by Lemma 2. If h is even, then n' must be even, otherwise $2n'|h$. But by Lemma 2 (c), n' even implies $h \equiv 0 \pmod 8$, hence we are forced to the contradiction $2n'|h$.

Proof of (c): We have $(n'/p)(n'/q)=-1$. Assume $\Phi_h(x^2/n)$ reducible for some $h|d$. Then if h is odd, $n' \equiv 1 \pmod 4$, thus $(n'/p)=(p/n')$, $(n'/q)=(q/n')$, by the quadratic reciprocity law. Hence $-1=(n'/p)(n'/q)=(p/n')(q/n')$. But $p \equiv q \pmod{2d}$ implies $p \equiv q \pmod{n'}$, since $n'|h|d$. Therefore $(p/n')=(q/n')$. Combined with $-1=(p/n')(q/n')$, this yields a contradiction.

Now let h be even, $h \equiv 2 \pmod 4$. Then by Lemma 2 (b), $n' \equiv 3 \pmod 4$. By the quadratic reciprocity law

$$-1=(n'/p)(n'/q)=(-1)^{(p+q-2)/2}$$

implies $p+q \equiv 0 \pmod 4$.

But $p \equiv q \pmod{2d}$ implies $p-q \equiv 0 \pmod 4$, since $h|d$. Therefore, $2p \equiv 0 \pmod 4$, contrary to the fact that p is an odd prime.

Finally, let $h \equiv 0 \pmod 4$. Then by Lemma 2 (c), n' is even. Write $n' = 2n''$. Then

$$-1 = (n'/p)(n'/q) = (2/p)(2/q)(n''/p)(n''/q) = (n''/p)(n''/q) ,$$

since $p \equiv q \pmod 8$. If $n'' \equiv 1 \pmod 4$, we obtain a contradiction as in the first case considered above. If $n'' \equiv 3 \pmod 4$, we obtain a contradiction as in the second case. Note that the hypothesis $p \equiv q \pmod d$ (instead of $p \equiv q \pmod{2d}$) is sufficient in all cases except when simultaneously $n' \equiv 3 \pmod 4$ and $d \not\equiv 0 \pmod 4$.

Proof of (d): If $d=1$ (see [1, Theorem 6]) or $d=2$, then the only $h|d$ are $h=1$ or $h=2$. If $h=1$ we cannot have $n'|h$. If $h=2$, then $n'|h$ implies $n'=2$, contrary to Lemma 2 (b). If $d=p^k$, p a prime $\equiv 3 \pmod 4$, then $h|d$ implies h is also of this form. Assume now $\Phi_h(x^2/n)$ reducible. Since $n'|h$, $n'=p$. By Lemma 2 (b), this implies h is even, a contradiction.

Even in case one or more of the polynomials $n^{\varphi(h)}\Phi_h(x^2/n)$ where h divides some d_i is reducible, we may still obtain information about M. We can use the results of Lemma 3 as follows. Let $d_1, \cdots, d_r$ be the lengths of the disjoint cycles of P. For each $i=1, \cdots, r$ let k_i be defined as follows:

(i) if $n' \equiv 1 \pmod 4$, let k_i be the number of divisors of d_i each of which is odd, squarefree and a multiple of n';

(ii) if $n' \equiv 3 \pmod 4$, let k_i be the number of divisors of d_i each of which is even, squarefree and a multiple of n';

(iii) if $n' \equiv 2 \pmod 4$, let k_i be the number of divisors of d_i each of which is a multiple of n', and of the form $4t$, t odd and squarefree. Then we have the following theorem.

THEOREM 3. *If k_i is defined as above, then $M = n+1+sn^*n'$, where $-\sum_{i=1}^{r} k_i \leqq s \leqq \sum_{i=1}^{r} k_i$. Further, $s \equiv \sum_{i=1}^{r} k_i \pmod 2$.*

Proof. All that remains to be verified is the second sentence, which follows immediately from the fact that the sum of the roots of $Q(x)$ in (34) is the sum of $\sum k_i$ numbers $\pm n^*n'$.

6. In this section, we compare the number of absolute points of ρ^j, where j is any number prime to twice the order of ρ^2, with the number of absolute points of ρ. The results obtained coincide with those of [2], so we shall merely sketch the present approach.

The index j in what follows is an integer prime to twice the order of $\rho^2 = 2d$. Let M_j be the number of absolute points of ρ^j, so that $M_1 = M$ in our previous notation. If we let $j = 2c+1$, then $P^{-c}A$ is an incidence matrix for Π that bears the same relation to ρ^j that A does

to ρ. In particular, $M_j = \operatorname{tr} P^{-c}A$. Referring back to (26), (27), and (28), we see that

$$M_1 = n+1+\sqrt{n}(e^{i\alpha_1}+\cdots+e^{i\alpha_{N-1}}) ,$$

$$M_j = n+1+\sqrt{n}(e^{ij\alpha_1}+\cdots+e^{ij\alpha_{N-1}}) .$$

But from Theorem 1, $n^{-1/2}(M_1-(n+1))$ is of the form $u\sqrt{n'}$, where u is a rational integer. Further, if m is the least common multiple of the orders of the α's, then $n^{-1/2}(M_j-(n+1))$ is the image of $u\sqrt{n'}$ under the automorphism of $R(\zeta_m)$ which sends $\zeta_m \to \zeta_m^j$.

Now $m=d$ if d is odd, $m=2d$ if d is even. In either case, however, the indices j considered correspond biuniquely to all automorphisms of $R(\zeta_m)$. Thus, if $M_1 \neq n+1$ (so that we know $\sqrt{n'} \in R(\zeta_m)$), we have

$M_j = M_1$ if the automorphism $\zeta_m \to \zeta_m^j$ fixes $\sqrt{n'}$,

$M_j = 2(n+1)-M_1$ the automorphism $\zeta_m \to \zeta_m^j$ sends $\sqrt{n'}$ into $-\sqrt{n'}$.

One may use the Gauss sums of Lemma 2(iv) to show explicitly that in general

$$M_j = (n'/j)(M_1-(n+1))+(n+1) ,$$

where (n'/j) is defined to be 1 if $(j, n') > 1$. Among other things, this formula includes the equation $M_j = M_1$ if n is a square.

7. **We now show** how the preceding results may be extended to symmetric group divisible designs. (See [3] and [6] for a definition and discussion of the interesting properties of these designs.) For our purpose, it is appropriate to employ the following:

DEFINITION. A *symmetric group divisible design* Δ is a combinatorial configuration consisting of a set with v elements and v distinguished subsets such that

(i) each subset is incident with exactly k elements, and

(ii) the subsets can be partitioned into g groups, each group containing s subsets ($gs=v$), such that two distinct subsets in the same group have exactly λ_1 elements in common, two subsets in different groups have exactly λ_2 elements in common.

We assume that the design Δ admits a correlation ρ; that is, a one-to-one mapping of the elements of Δ onto the distinguished subsets of Δ, together with a one-to-one mapping of the subsets onto the elements such that an element is in a subset if and only if the image of the element contains the image of the subset. Now the existence of ρ implies that in the definition given above, we may interchange, in (i) and (ii) the words subset and element. Number the elements $E_1, E_2, \cdots, E_v$ such

that $E_1, E_2, \cdots, E_s$ are the elements of the first group, $E_{s+1}, E_{s+2}, \cdots, E_{2s}$ are the elements of the second group, and so on. Number the subsets $S_1, S_2, \cdots, S_v$ so that $\rho E_i = S_i$. Define the incidence matrix $A=(a_{ij})$ of order v, by the stipulation $a_{ij}=1$ if E_i is in S_j, 0 otherwise, and the permutation matrix $P=(p_{ij})$ such that $p_{ij}=1$ if and only if $\rho^2 E_i = E_j$. Then as in the case of planes, we have

$$A^T = PA, \text{ so } A \text{ is normal. Further} \tag{35}$$

$$AA^T = (k-\lambda_1)I + (\lambda_1-\lambda_2)K + \lambda_2 J\ , \tag{36}$$

where I and J are as before, and K is the direct sum of g matrices of order s each of which consists entirely of 1's.

Our object, as before, is to obtain a count on the number of absolute points of $\rho = \operatorname{tr} A = M$.

Since the vector $(1, 1, \cdots, 1)$ is an eigenvector of A and A^T corresponding to the eigenvalue k, and is also an eigenvector of K with eigenvalue s, we have from (27) that $k^2-\lambda_2 v = k-\lambda_1+s(\lambda_1-\lambda_2)$. Hence, we may compute [1] that

$$|AA^T - xI| = (k^2-x)[k+\lambda_1+s(\lambda_1-\lambda_2)-x]^{g-1}(k-\lambda_1-x)^{v-g}\ . \tag{37}$$

Henceforth, let us assume $v > g > 1$. This is no restriction for the combinatorial configurations apparently so excluded are realized by allowing $\lambda_1=\lambda_2$. (Indeed, the case $\lambda_1=\lambda_2$ with the further trivial restrictions $v > k > \lambda_1=\lambda_2 > 0$ is an important class of designs known as balanced symmetric incomplete block designs. Further, $\lambda_1=\lambda_2=1$ characterizes finite projective planes.)

Because A is normal, the eigenvalues of AA^T are the squares of the moduli of the eigenvalues of A. Hence, by (37), the eigenvalues of A are

$$k, \sqrt{n_1}e^{i\alpha_1}, \sqrt{n_1}e^{i\alpha_2}, \cdots, \sqrt{n_1}e^{i\alpha_{g-1}}, \sqrt{n_2}e^{i\alpha_g}, \cdots, \sqrt{n_2}e^{i\alpha_{v-1}}\ ,$$

where $n_1 = k-\lambda_1+s(\lambda_1-\lambda_2)$, $n_2 = k-\lambda_1$.

On the other hand, if P is a product of disjoint cycles of lengths $d_1, d_2, \cdots, d_r$, $d_1+\cdots+d_r=v$, then the eigenvalues of P are the d_1th roots of unity, the d_2th roots of unity, $\cdots$, the d_rth roots of unity, namely

$$1, e^{i\theta_1}, e^{i\theta_2}, \cdots, e^{i\theta_{v-1}}\ . \tag{38}$$

Now by (35) and (36) we have

$$A^2 = (k-\lambda_1)P^T + (\lambda_1-\lambda_2)P^T K + (\lambda_1-\lambda_2)J\ . \tag{39}$$

Further, each of A, P^T, K, J commutes with the three others (for example, to check that P^T commutes with K multiply (39) on the left and right

by P and apply (35)). Hence all four of these normal matrices can be simultaneously diagonalized. Let us imagine then that (39) is in diagonal form, and examine the diagonal elements. Note that one eigenvalue of J is v, the rest are 0, and that g eigenvalues of K are s, the rest are 0. Clearly, then, we have

$$
\begin{aligned}
k^2 &= (k-\lambda_1)\cdot 1 + (\lambda_1-\lambda_2)\cdot s + \lambda_2 \cdot v \ , \\
n_1 e^{2i\alpha_t} &= (k-\lambda_1)e^{-i\theta j_t} + (\lambda_1-\lambda_2)se^{-i\theta j_t}
\end{aligned} \tag{40}
$$

for $t=1, 2, \cdots, g-1$ and some $g-1$ indices j_t in the set $1, \cdots, v-1$, and also

$$
n_2 e^{2i\alpha_\mu} = (k-\lambda_1)e^{-i\theta j_\mu} \tag{41}
$$

for $u=g, g+1, \cdots, v-1$, and $\{j_\mu\}$ the indices in $1, 2, \cdots, v-1$ not in $\{j_t\}$.

We contend that the $e^{-i\theta_j}$ appearing in (40) can be partitioned into classes, each class consisting of a conjugate set of roots of unity. For the characteristic polynomial of P^TK is $(x-\zeta)x^{v-g}f(x)$, where

$$
f(x) = \prod_{t-1}^{g-1} (x - se^{-i\theta j_t}) \ . \tag{42}
$$

But since P^TK has rational coefficients, its characteristic polynomial is rational, hence $f(x)$ has rational coefficients. Let $h(x)=s^{\varphi(h)}\Phi_h(x/s)$ be the irreducible polynomial satisfied by $se^{-i\theta j_1}$; that is, $e^{-i\theta j_1}$ is a primitive hth root of unity. Then $h(x)$ and $f(x)$ have a root in common, so, by the irreducibility of $h(x)$, the set of roots of $f(x)$ contains all roots of $h(x)$, namely all numbers $s\zeta_h$. Divide $f(x)$ by $h(x)$, apply the same argument to the quotient, and continue. This verifies our statement.

We may now imitate our previous polynomial construction in § 4 for the case of planes as follows: If the characteristic polynomial of A is written as $(x-k)Q(x)$ and the characteristic polynomial of P as $\prod_{i=1}^{r} \Phi_{d_i}(x)$, then from the foregoing we have

$$
\pm Q(x)Q(-x) = n_1^{g-1} n_2^{v-g} \prod_i \Phi_{h_i}(x^2/n_1) \prod_j \Phi_{h_j}(x^2/n_2) \tag{43}
$$

where the h_i and h_j are divisors of the cycle lengths $d_1, d_2, \cdots, d_r$, $\sum_i \varphi(h_i)=g-1$, $\sum_j \varphi(h_j)=v-g$. One can then proceed from (43) by the techniques previously used in studying the consequences of (34).

REFERENCES

1. R. Baer, *Polarities in finite projective planes*, Bull. Amer. Math. Soc., **52** (1946), 77–93.

2. R. W. Ball, *Dualities of finite projective planes*, Duke. Math. J., **15** (1948), 929.

3. R. C. Bose and W. S. Connor, *Combinatorial properties of group divisible incomplete block designs*, Ann. Math. Stat., **23** (1952), 367.
4. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Canad. J. Math., **1** (1949), 88.
5. S. Chowla and H. J. Ryser, *Combinatorial problems*, Canad. J. Math., **2** (1950), 93.
6. W. S. Connor, *Some relations among the blocks of symmetrical group divisible designs*, Ann. Math. Stat., **23** (1952), 602.
7. O. Hilbert, *Gesammelte Abhandlungen*, Vol. 1, Berlin, 1932.
8. T. Nagell, *Introduction to number theory*, Uppsala, 1951.
9. E. G. Straus and O. Taussky, *Remark on the preceding paper. Algebraic equations satisfied by roots of natural numbers*, Pacific J. Math., **6** (1956), 000.

NATIONAL BUREAU OF STANDARDS
UNIVERSITY OF CALIFORNIA, LOS ANGELES

PACIFIC JOURNAL OF MATHEMATICS

Printed in Japan by Kokusai Bunken Insatsusha
(International Academic Printing Co., Ltd.), Tokyo, Japan

Pacific Journal of Mathematics
Vol. 6, No. 1 November, 1956