MATRICES AND EXISTENCE OF DESIGNS

Marshall Hall, Jr.

Emory University

1. Introduction.

A balanced incomplete block design D, briefly a design, will have parameters (v, b, r, k, λ) . For a particular design D the incidence matrix A is essentially a listing of points on blocks. The matrix $S = A^T A = (s_{ij})$ gives the size of block intersections where $s_{ij} = |B_i \cap B_i|$. Also the projection matrix $C = r(r - \lambda)I + \lambda kJ - rS$ is intimately related as $C = C^T$, $C^2 = r(r - \lambda)C$ and AC = 0. A principal minor of C must have a non-negative determinant. This excludes many possible choices of initial blocks. Section 2 describes these properties.

Section 3 treats automorphisms (or collineations) of designs. I conjecture that if a design D exists then a design with the same parameters will have a non-trivial automorphism.

Section 4 considers applications of codes to designs. Codes are a major tool, and in particular have led to a proof of the non-existence of a plane of order 10.

2. Matrices associated with a design.

Given a design $D(v, b, r, k, \lambda)$ the matrix associated with this is the *incidence* matrix A

$$A = [a_{ij}] \ i = 1, \dots, v, \quad j = 1, \dots, b$$
 (2.1)

where $a_{ij} = 1$ if the *i*th point is in the *j*th block and otherwise $a_{ij} = 0$. Thus the incidence matrix can be considered a detailed listing of points on blocks. Taking $J_{t,u}$ to be the t by u matrix of all 1's.

$$AJ_{bb} = rJ_{vb}, \quad J_{vv}A = kJ_{vb}, \quad AA^{T} = (r - \lambda)I + \lambda J_{vv}.$$
 (2.2)

The intersection matrix S is defined as

$$S = A^{T}A = [s_{ij}] i, j = 1...b$$
 (2.3)

where $s_{i,j} = |B_i \cap B_j|$. Relations on S are

$$S^{T} = S$$
, $SJ_{bb} = rkJ_{bb}$, $S^{2} = (r - \lambda)S + \lambda k^{2}J_{bb}$. (2.4)

A further matrix associated with the design D is the projection matrix C defined by

$$C = r(r - \lambda) I_b + \lambda k J_{bb} - rS. \tag{2.5}$$

Relations on C are

$$C^2 = r(r - \lambda)C$$
, $C = C^T$, $AC = 0$, $C = rank(b - v)$. (2.6)

Since C corresponds to a positive semi-definite quadratic form, every principal minor of C has a non-negative determinant.

This research was supported in part by NSF Grant No. DMS 8518824.

3. Automorphisms of designs.

An automorphism (or collineation) of a design D is a one-to-one mapping of points onto points and of blocks onto blocks which preserves incidence. If A is the incidence matrix of D, X the point mapping, Y the block mapping then

$$X^{-1}AY = A. (3.1)$$

If the design D is a symmetric block design with v = b, k = r, then A is a non-singular square matrix and

$$Y = A^{-1}XA \tag{3.2a}$$

from which it follows that trace Y = trace X and so the collineation fixes the same number of blocks as points. I have a conjecture:

Conjecture. If a design $D(v, b, r, k, \lambda)$ exists then a design with the same parameters exists with a non-identical automorphism.

This conjecture is true in all known cases. The projective plane of order 10 is the symmetric design D(111,11,1). For some time it has been known that it could have only the identical automorphism. But recently it has been shown by Clement Lam that the plane does not exist. Of the 81 designs (15,35,7,3,1) some have only the identical automorphism but others have non-trivial automorphisms.

For a design (28,42,15,10,5) it is not hard to show that for an automorphism α with $\alpha^p = 1$, for no prime $p \ge 5$ does an automorphism exist. But with $\alpha^3 = 1$. Tonchev and van Lint [4] have constructed a design. On the points $P, 1, \ldots, 27$ α fixes P and moves $1, \ldots, 27$ in 9 orbits of 3 points.

$$\alpha = (P)(1,2,3)(4,5,6)(7,8,9)(10,11,12)(13,14,15)$$

$$(16,17,18)(19,20,21)(22,23,24)(25,26,27).$$
(3.2b)

Here is the full design which they constructed

(28, 42, 15, 10, 5) Tonchev and van Lint

```
P 1 2 3 4 5 6
                    7
                                P 1 6 9 11 14 17 20 24 27
P 10 11 12 13 14 15 16 17 18
                                       7 12 15 18 21 22 25
P 19 20 21 22 23 24 25 26 27
                                P 3 5 8 10 13 16 19 23 26
Ρ
        3 10 11 12 19 20 21
                                2 3 6
                                       7 11 13 17 19 24 25
      5 6 13 14 15 22 23 24
Р
                                3 1 4
                                       8 12 14 18 20 22 26
P 7
        9 16 17 18 25 26 27
                                1 2 5 9 10 15 16 21 23 27
P
  1
      2 3 13 14 15 25 26 27
                                3 5 6 8 12 13 17 20 23 26
P 4
     5 6 16 17 18 19 20 21
                                1 6 4 8 10 13 18 21 24 27
P 7
     8 9 10 11 12 22 23 24
                                2 4 5 9 11 14 16 19 22 25
P 1
     2 3 16 17 18 22 23 24
                                1 4 8 9 12 13 17 19 23 25
     5 6 10 11 12 25 26 27
P 4
                                2 5 9 7 10 14 18 20 24 26
P 7 8 9 13 14 15 19 20 21
                                3 6 7 8 11 15 16 21 22 27
                                2 6 9 11 12 13 18 21 23 26
                                3 4 7 12 10 14 16 19 24 27
                                1 5 8 10 11 15 17 20 22 25
                                                            (3.3)
                                1 6 7 10 14 15 18 19 23 25
                                2 4 8 11 15 13 16 20 24 26
                                3 5 9 12 13 14 17 21 22 27
                                2 5 8 12 15 17 18 19 24 27
                                3 6 9 10 13 18 16 20 22 25
                                1 4 7 11 14 16 17 21 23 26
                                1 5 7 12 13 16 20 21 24 25
                               2 6 8 10 14 17 21 19 22 26
                                3 4 9 11 15 18 19 20 23 27
                                3 5 8 11 14 18 21 23 24 25
                                1 6 9 12 15 16 19 24 22 26
                               2 4 7 10 13 17 20 22 23 27
                                1 5 7 11 13 18 19 22 26 27
                               2 6 8 12 14 16 20 23 27 25
```

If a group G acts transitively and regularly on the points (and so also on the blocks) of a symmetric design, then D is completely determined given the points on a single block, say (x_1,\ldots,x_k) . We say $\Delta(x_1,x_2,\ldots,x_k)$ is the difference set. If G is abelian and written in additive form this means that any $d\neq 0$ is represented as $d=x_i-x_j,x_i,x_j\in \Delta$ exactly λ times. In general if D is given by an abelian difference set there will be further automorphisms of the shape $x\to tx$, where t is called the multiplier.

3 4 9 10 15 17 21 24 25 26

Multiplier Theorem 3.1. If p is a prime, (p, v) = 1 $p \mid k - \lambda$ and $p > \lambda$ then p is a multiplier of a difference set D given by $\Delta(x_1, \ldots, x_k)$.

A tempting case is the following:

A symmetric (81, 16, 3) design with a collineation α of order 13.

$$C_1 \qquad C_2 \qquad C_3 \qquad C_4 \qquad C_5 \qquad C_6$$

$$\alpha = (1, \dots, 13)(14, \dots, 26)(27, \dots, 39)(40, \dots, 52)(53, \dots, 65)(66, \dots, 78)(X)(Y)(Z)$$
(3.8)

A possible orbit matrix is the following:

$$C_1 \ C_2 \ C_3 \ C_4 \ C_5 \ C_6 \ X \ Y \ Z$$

$$B_1 \ 13 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1$$

$$B_2 \ 0 \ 13 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1$$

$$B_3 \ 0 \ 0 \ 13 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1$$

$$B_4(...B_{16}) \ 2 \ 2 \ 2 \ 3 \ 3 \ 3 \ 1 \ 0 \ 0 \ .$$

$$B_{17}(...B_{29}) \ 2 \ 2 \ 2 \ 3 \ 3 \ 3 \ 0 \ 1 \ 0$$

$$B_{30}(...B_{42}) \ 2 \ 2 \ 2 \ 3 \ 3 \ 3 \ 0 \ 0 \ 1$$

$$B_{43}(...B_{55}) \ 3 \ 3 \ 3 \ 4 \ 3 \ 0 \ 0 \ 0 \ 0$$

$$B_{56}(...B_{68}) \ 3 \ 3 \ 3 \ 0 \ 4 \ 3 \ 0 \ 0 \ 0$$

$$B_{69}(...B_{81}) \ 3 \ 3 \ 3 \ 0 \ 4 \ 0 \ 0 \ 0$$

This orbit matrix is entirely consistent, but as yet no one has been able to choose subscripts correctly to complete the design.

4. Applications of codes.

Let $q = p^t$, p a prime. We consider $F_q = GF(q)$ the finite field with q elements. Let A be the incidence matrix of design $D(v, b, r, k, \lambda)$. The $code\ C$ of D over F_q is defined to be the subspace of F_q^b spanned by the rows (a_{i1}, \ldots, a_{ib}) , $i = 1 \ldots v$ of A taken as vectors over F_q . Since $a_{ij} = 1$ or 0, this is certainly possible. The dimension of C will be s so that C contains q^s vector. The weight w(v) of a vector $v = (x_1, \ldots, x_b)$ is the number of $x_i \neq 0$. The weight distribution of C is A_0, A_1, \ldots, A_b where A_i is the number of codewords of weights i. The orthogonal dual code C^\perp is defined by

$$C^{\perp} = \{ w \mid (w, v) = 0 \, \forall v \in C \}.$$
 (4.1)

Here the inner product $(w, v) = w_1v_1 + w_2v_2 \dots + w_bv_b$. Clearly C^{\perp} is a vector space and it is easy to show that dim $C^{\perp} = b - \dim C$. Also $(C^{\perp})^{\perp} = C$. If $C_1 \cap C_2$ is the set of vectors common to C_1 and C_2 and $C_1 + C_2$ the vectors spanned by both C_1 and C_2 then it easily follows that

$$(C_1 \cap C_2)^{\perp} = C_1^{\perp} + C_2^{\perp} \qquad (C_1 + C_2)^{\perp} = C_1^{\perp} \cap C_2^{\perp}.$$
 (4.2)

The condition $p > \lambda$ seems to be superfluous, but is needed in all known proofs. There are a number of classes of known difference sets. The following is a somewhat unusual individual case with $(v, k, \lambda) = (133, 33, 8)$.

$$\Delta = (1,4,5,14,16,19,20,21,25,38,54,56,57,64,66,70,76,80,83,84,91,93,95,98,100,101,103,105,106,114,125,126,131).$$
(3.4)

Here G is the cyclic group of order 133. Here 5 is a multiplier, even though the condition $p > \lambda$ does not hold.

To construct a symmetric (41, 16, 6) design we assume a collineation α of order 5 fixing exactly one point and one block. Let the collineation on points be $\alpha = (x)(1,2,3,4,5)$ (6,7,8,9,10) ...(36,37,38,39,40) and on blocks $\alpha = (B_0)(B_1,B_2,B_3,B_4,B_5)$... $(B_{36},B_{37},B_{38},B_{39},B_{40})$. If a block B_i contains b_{ij} points from the *j*th orbit of points, the matrix $B = [b_{ij}]$ is the *orbit matrix*. Here one possible orbit matrix is

This table suggests a possible further collineation B of order 3 permuting (C_1, C_2, C_3) and (C_4, C_5, C_6) . In fact this works with B on points being

$$B = (x)(1,6,11)(2,7,12)(3,8,13)(4,9,14)(5,10,15)(16,21,26)$$

$$(17,22,27)(18,23,28)(19,24,29)(20,25,30)$$

$$(30)(32)(33)(34)(35)(36)(37)(38)(39)(40).$$
(3.6)

Representative blocks are

Along with the weight distribution of C is the weight enumerator $W_c(x, y)$

$$W_C(x,y) = A_0 x^b + A_1 x^{b-1} y + \ldots + A_x x^{b-i} y^i + \ldots + A_b y^b. \tag{4.3}$$

There is a remarkable result, due to Jesse MacWilliams which asserts that given the weight distribution of C the weight distribution of C^{\perp} is completely determined. This is given by the MacWilliams identity.

Theorem 4.1.

$$W_{C^{\perp}}(x,y) = \frac{1}{|C|} W_C(x + (q-1)y, x-y). \tag{4.4}$$

This identity is very powerful. For a code C coming from a design D there is a powerful result on C^{\perp} , over F_q , with $q = p^t$ and $p \mid (r - \lambda)$

Theorem 4.2. over F_q with $q = p^t$ and $p \mid r - \lambda$ then $C \cap C^{\perp}$ is of codimension 0 or 1 in C.

Proof: Let r_1, r_2, r_3 be any 3 rows of A. Then

$$(r_1, r_1) = r \equiv \lambda (r_1, r_2) = \lambda (r_1 - r_2, r_3) = \lambda - \lambda = 0 \pmod{p}.$$
 (4.5)

It now follows that the difference of any two rows of A is a vector of C^{\perp} and so $C \cap C^{\perp}$ is of codimension 0 or 1 in C. Combining them with the MacWilliams identity gives much information.

The projective plane of order 10 is a symmetric (111, 11, 1) design. It has recently been shown by Clement Lam that it does not exist. The proof depends on coding theory. In a major work in 1973, Jessie MacWilliams, Neil Sloane, and John Thompson [3] applied coding theory to the problem of existence of the plane. Let A be the incidence matrix of a plane. Then (4.6) $AA^T = B = 10I + J$ det $B = 11^2 \cdot 10^{110}$, det $A = \pm 11 \cdot 10^{55}$. Hence, over F_2 , A has rank at least 56 and so dim $C \ge 56$. Then dim $C^{\perp} \ge 55$. As dim $C + \dim C^{\perp} = 111$ it follows that dim C = 56, dim $C^{\perp} = 55$ and $C^{\perp} \subset C$. A word of C has weight $\equiv 0$, 3 (mod 4) and words of C^{\perp} have weight $\equiv 0$, (mod 4). Every row of A has weight 11 and so a word which is the sum of an odd number of rows will have weight $\equiv 3 \pmod{4}$ and the sum of an even number of rows will have weight \equiv 0(4). Trivially $A_0 = 1$ and using these facts $A_i = 0$, i = 1, ..., 10. Consider the configuration of a word W of weight $11 = \{P_1 \dots P_{11}\}$. Two of the points P_1, P_2 will lie on a line L. If L contains a point Q not in $P_1 ldots P_{11}$, then there will be 10 further lines through Q and at most 9 further points of W_{11} . Hence, there is a line L^* through Q with no points of W^{11} . But words of odd weight have an odd number of points in common, a conflict. Hence, there is no such Q and $W_{11}\{P_1 \dots P_{11}\}$ is a line. Thus, $A_{11} = 111$. Also the sum of all rows of A is $(11, 11, \dots, 11)$ or

 $(1,\ldots,1)$ over F_2 . Hence, $A_{111}=1$ and so $A_i=A_{111-i}$, counting complements. With these facts and the MacWilliams identity the complete weight distribution is determined by A_{12} , A_{15} , and A_{16} . A word W_{12} of weight $12(P_{11},\ldots,P_{12})$ will be such that a line through P_i meets W_{12} in an even number of points and so in at least one more P_j . Hence, the 11 lines through P_i use up the remaining 11 points of W_{12} . Hence, a W_{12} is an *oval*, every line meeting W_{12} in 0 or 2 points. A line will meet a $W_{15}(P_1 \ldots P_{15})$ in an odd number of points.

$$L \cap W_{15} = 11wt(L + W_{15}) = 4$$
 a conflict
 $L \cap W_{15} = 9wt(L + W_{15}) = 15 - 9 + 2 = 8$ a conflict
 $L \cap W_{15} = 7wt(L + W_{15}) = 15 - 7 + 4 = 12$, (4.6)

but here the oval of 12 points has L meeting it in 4 points, a conflict. Let there be b_1, b_3, b_5 lines meeting W_{15} in respectively 1, 3, or 5 points. Then

$$b_1 + b_3 + b_5 = 111$$

$$b_1 + 3b_3 + 5b_5 = 15 \cdot 11 = 165$$

$$3b_3 + 10b_5 = \frac{15 \cdot 14}{2} = 105.$$
(4.7)

The first of these counts the number of lines, the second the incidences of the 15 points on lines, the third the $\binom{15}{2}$ = 105 pairs of the 15 points. Solution of (4.7) is easily seen to be

$$b_1 = 90$$
 $b_3 = 15$ $b_5 = 6$.

Lemma. No one of $P_1 ldots P_{15}$ is on as many as 3 of the 6 lines containing 5 points.

Proof: Consider

$$P_1$$
 P_2 P_3 P_4 P_5 P_1 P_6 P_7 P_8 P_9 . P_1 P_{10} P_{11} P_{12} P_{13}

Here only P_{14} and P_{15} remain and so a 4th line with 5 points through P_1 is impossible. Thus, a further 5 point line will contain exactly 3 of $P_2 cdots P_{13}$ and so both of P_{14} and P_{15} . There are 3 such lines and this is a conflict, and the lemma is proved. As there are $6 \cdot 5 = 30$ incidences on the 5 point lines each of $P_1 cdots P_{15}$ will occur exactly twice. Thus, up to isomorphism these lines are

$$P_{1} P_{2} P_{3} P_{4} P_{5}$$

$$P_{1} P_{6} P_{7} P_{8} P_{9}$$

$$P_{2} P_{6} P_{10} P_{11} P_{12}$$

$$P_{3} P_{7} P_{10} P_{13} P_{14}$$

$$P_{4} P_{8} P_{11} P_{13} P_{15}$$

$$P_{5} P_{9} P_{12} P_{14} P_{15}$$

$$(4.8)$$

 P_1 must still appear with P_{10} , P_{11} , P_{12} , P_{13} , P_{14} , P_{15} in 3 point lines

$$P_1 P_{10}$$
 $P_1 P_{11}$. (4.9)
 $P_1 P_{12}$

 P_{10} has been with $P_{13} + P_{14}$ so the 3rd point of P_1 P_{10} is P_{15} . This yields similarly

$$P_1 P_{10} P_{15}$$

 $P_1 P_{11} P_{14}$. (4.10)
 $P_1 P_{12} P_{13}$

Similarly all 15–3 point lines are completely determined. Using a computer they showed that this configuration cannot be completed to a full plane, and conclude that $A_{15} = 0$.

In 1974 J.L. Carter showed that some of the six possible configurations for W_{16} are impossible. Clement Lam showed all of these impossible giving $A_{16} = 0$. Similarly he showed that $A_{12} = 0$. This fully determined the weight distribution and in particular $A_{19} = 24$, 675. A line intersects a W_{19} in 1, 3, or 5 points and suppose there are b_1 , b_3 , b_5 such lines. Then

$$b_1 + b_3 + b_5 = 111$$

$$b_1 + 3b_3 + 5b_5 = 11 \cdot 19 = 209$$

$$3b_3 + 10b_5 = \frac{19 \cdot 18}{2} = 171.$$
(4.11)

Solution here is $b_1 = 67$, $b_3 = 37$, $b_5 = 6$.

These are 64 possible configurations for the 6 5 point lines. Using the CRAY computer at the Institute for Defense Analyses in Princeton, all 64 cases have now been eliminated and we conclude that a plane of order 10 does not exist. The amount of computer time used was very large.

A design D(22, 33, 12, 8, 4) is of particular interest since this is the smallest number of points for which the existence is unknown [1]. Hamada and Kobayashi [2] have shown that the rows of S are of the following 4 types (apart from order)

The code C over F_2 will be doubly even with all weights multiples of 4, A_0 , A_4 , A_8 , A_{12} , A_{16} , A_{20} , A_{24} , A_{28} . We must have $A_{32}=0$ since in the remaining 33 rd column there will be a 1 and 11 further 1's in the row, contrary to the fact that any two words of C have an even number of positions where both are 1. Thus, if

 C^{\perp} has weight distribution $C_0, C_1, C_2, \ldots, C_{33}$ we will have $C_0 = 1, C_{33} = 1$, but also $C_1 = 0$, $C_2 = 0$. If $C_1 > 0$ there would be a column with no 1's and if $C_2 > 0$ we would have two identical columns contrary to Hamada and Kobayashi. Let $|C| = 2^s$. Using this and $C_1 = C_2 = 0$ we can solve for A_{12} , A_{16} , and A_{20} in terms of 2^s , A_4 , A_8 , A_{24} , A_{28} . In particular we have

$$2^{s-9}C_4 = -45 \cdot 2^{s-9} + 90 + 28s_4 + 5A_8 + 3A_{24} + 24A_{28}$$

$$2^{s-9}C_5 = -39 \cdot 2^{s-9} + 474 + 92s_4 + 5A_8 + 3A_{24} - 40A_{28}.$$
(4.13)

This leads to

$$2^{s-9}C_5 = 2^{s-9}C_4 + 6 \cdot 2^{s-9} + 384 + 64A_4 - 64A_{28}. \tag{4.14}$$

Since $C_{33} = 1$, $C_5 = C_{28} \ge A_{28}$. Hence, if $A_{28} \ge 6$ then $C_5 \ge 6$. But if $A_{28} < 6$ then (4.14) gives $2^{i-9}C^5 \ge 6 \cdot 2^{s-9}$ and so $C_5 \ge 6$ in either event.

A word of weight 5 in C^{\perp} corresponds to 5 columns of A in which every row has an even number of 1's, namely, 0, 2 or 4. Up to isomorphism there are 108 such configurations. Using the projection matrix and other arguments all but 13 of these starts have been eliminated. A start will give a 5 by 5 principal minor of 5. The 13 possibilities remaining are

An attempt to complete these minors to the full matrix S would involve a prohibitively large number of cases.

References

- 1. M. Hall, Jr., R. Roth, G.H.J. van Rees and S.A. Vanstone, *On designs* (22, 33, 12, 8, 4), Journal of Combinatorial Theory (Series A) 47 (1988), 157-175.
- 2. N. Hamada and Y. Kobayashi, On the block structure of a BIB design with parameters v = 22, b = 33, k = 8, $\lambda = 4$, J. Combinatorial Theory (Series A) 24 (1988), 75–83.
- 3. F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, On the existence of a projecture plane of order 10, J. Combinatorial Theory (Series A) 14 (1973), 66-78.
- 4. Tonchev and J. van Lint, Construction of a new design, (to appear).