submatrix whose completion cannot have a big enough determinant, so that we end up with a list of elements of $\overline{\mathcal{M}_n}^{(1)}$ with determinant $\geq d$.

There are only finitely many such matrices, since all new entries will have magnitude strictly less than n by Theorem 4.4. However finitely many can still be a very large number, so we also apply an ordering on our candidates, so that the computer does not generate M-matrices which are equivalent to those already generated, but which are higher up in the ordering.

Step 2) We discard each matrix whose determinant is not a perfect square (since $\det M = \det RR^T = \det R \det R^T = \det R \det R = (\det R)^2$).

11.3. Step 1 in detail

Our working solution is based upon the method described in [**CKM**].

We will need their

THEOREM 11.1. *(i) Let*

$$M(D_r) = \begin{pmatrix} D_r & B \\ B^T & A \end{pmatrix}$$

be an $m \times m$ symmetric, positive-definite matrix where D_r is an $r \times r$ matrix with $r \leq m \leq n$; $B = (b_{ij})$ is an $r \times (m-r)$ matrix; $A = (a_{ij})$ is an $(m-r) \times (m-r)$ matrix; satisfying $a_{ii} = n$, $|a_{ij}| \geq 1$, $|b_{ij}| \geq 1$, for $i \neq j$.

(ii) Let

$$0 \leq d^* = \det \begin{pmatrix} D_r & g^* \\ g^{*T} & 1 \end{pmatrix} = \max_{g \in G} \left\{ \det \begin{pmatrix} D_r & g \\ g^T & 1 \end{pmatrix} \right\},$$

where $G = \{g = (g_1, g_2, \ldots, g_r)^T : |g_i| \geq 1, i = 1, 2, \ldots, r\}$.

Then

$$\det M(D_r) \leq (n-1)^{m-r-1}[(n-1)\det D_r + (m-r)d^*]$$

and equality is attained when

$$M^*(D_r) = \begin{pmatrix} D_r & g^* & g^* & \cdots & g^* \\ g^{*T} & n & 1 & \cdots & 1 \\ g^{*T} & 1 & n & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g^{*T} & 1 & 1 & \cdots & n \end{pmatrix}.$$

PROOF: See [**MK**]

Choose the target d. It should be bigger than any known lower bound, and less than or equal to the known upper bound. Obviously, the bigger d is, the smaller the search space.

We build up our candidate M-matrix out of a nested sequence of square submatrices:

$$(m_{11}), \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}, \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix}, \begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{pmatrix}$$

We use Theorem 11.1 in the following manner.

Suppose we have D_{r-1}. We create D_r by placing D_{r-1} in the top left hand corner and filling in the remaining entries so that D_r is symmetric.

We then put our D_r in the top left hand corner of an $(r+1) \times (r+1)$ matrix, put a '1' in the bottom right hand corner, calling the leftover column vector g, as in:

$$\begin{pmatrix} D_r & g \\ g^T & 1 \end{pmatrix}$$

Now we vary over all possible vectors g's, and select the one for which this matrix has maximum determinant. Call that vector g^* and denote the maximum determinant d^*.

Calculate the number $test = (n-1)^{n-r-1}[(n-1)\det D_r + (n-r)d^*]$.

If $test < d$, we discard this D_r.
If $test > d$, we keep this D_r.
If $test = d$, we include the $n \times n$ matrix

$$M^*(D_r) = \begin{pmatrix} D_r & g^* & g^* & \cdots & g^* \\ g^{*T} & n & 1 & \cdots & 1 \\ g^{*T} & 1 & n & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g^{*T} & 1 & 1 & \cdots & n \end{pmatrix}$$

in our set of possible M-matrices.

We repeat this procedure for every possible completion D_r of our D_{r-1}. We then iterate this whole process through $r = 1, 2, 3, \ldots, n$.

So far, so good. This method alone, however produces a swath of duplicate solutions, in the following sense.

Consider the matrix

$$\begin{pmatrix} n & 1 & 1 & -3 & \cdots & 1 \\ 1 & n & 1 & 1 & \cdots & 1 \\ 1 & 1 & n & 1 & \cdots & 1 \\ -3 & 1 & 1 & n & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & n \end{pmatrix}$$

Exchanging column 4 with column 3 gives

$$\begin{pmatrix} n & 1 & -3 & 1 & \cdots & 1 \\ 1 & n & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & n & \cdots & 1 \\ -3 & 1 & n & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & n \end{pmatrix}$$

Then exchanging row 4 with row 3 gives

$$\begin{pmatrix} n & 1 & -3 & 1 & \cdots & 1 \\ 1 & n & 1 & 1 & \cdots & 1 \\ -3 & 1 & n & 1 & \cdots & 1 \\ 1 & 1 & 1 & n & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & n \end{pmatrix}$$

Hence the first and last of these matrices are equivalent. To avoid duplicating work we want to generate as few of the members of a given equivalence class as possible, preferably only one. So we have another Equivalence/Ordering Problem.

11.4. The Ordering

We want to define an equivalence on M-matrices. Since M-matrices are symmetric, we need operations which preserves symmetry. We define a class of operations which achieve this aim by simultaneously permuting rows and columns.

DEFINITION 16. SymSwap_{ij} is the operation acting on a matrix which has the combined effect of

- exchanging row i with row j, and
- exchanging column i with column j,

where $i, j \in \{1, 2, \ldots, n\}$ and n is the order of the matrix.

Then we can permute the entries of a symmetric matrix in such a way as to move an entry anywhere in the matrix to any other desired position, by

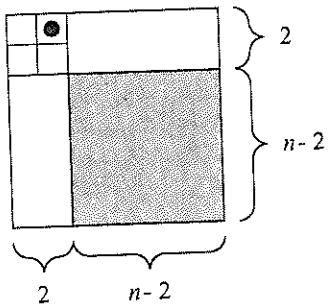
moving the given entry into the correct row and column using a choice of SymSwaps.

DEFINITION 17. $A \in \mathcal{M}^{(1)}$ is *equivalent* to $B \in \mathcal{M}^{(1)}$ provided that A can be obtained from B by performing a finite number of SymSwaps.

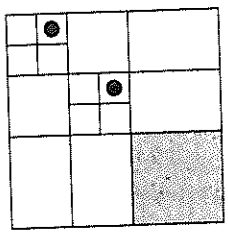
The paper [**CKM**] describes the following partial ordering.

Note(1) Throughout this description I will refer to 'the maximal element' of various submatrices. In fact such a maximal element is not necessarily unique, which is why we only have a partial ordering. At such points an arbitrary choice is being made. However for clarity I will not refer to the non-uniqueness explicitly in what follows. Note(2) When I refer to putting elements in a given position, I always mean by performing a finite number of SymSwaps.

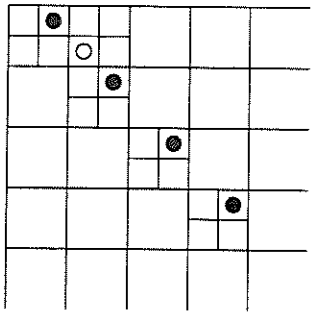
To generate a maximal representative matrix of a given matrix, with respect to the partial ordering, proceed as follows. Put the maximal off-diagonal element of the matrix in the (1,2) position. (A maximal element is an entry with largest absolute value.) This fixes rows 1 and 2, and they may henceforth only be permuted amongst each other. Likewise for columns 1 and 2.



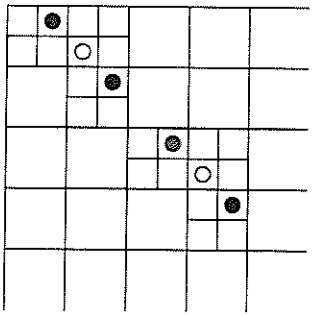
Now put the maximal off-diagonal element of the shaded two by two submatrix in the (3,4) position. That fixes rows 3 and 4, so that they may henceforth only be permuted amongst each other. Likewise for columns 3 and 4.



Continue in this way to the last available pair of rows/columns. Now consider the 2×2 block consisting of elements in the (1,3), (1,4), (2,3), (2,4) positions. By permuting rows/columns 1&2 within themselves and rows/columns 3&4 within themselves, put the maximal element of that 2x2 block in the (2,3) position.



Next consider the 2x2 block consisting of elements in the (5,7), (5,8), (6,7), (6,8) positions. By permuting rows/columns 5&6 within themselves and rows/columns 7&8 within themselves, put the maximal element of that 2x2 block in the (6,7) position.



Continue in this way to the last available 4-tuple of rows/columns.

Note: We never actually order the matrices. What we do is to throw out (or never generate in the first place) any submatrices which would lead to an M which is submaximal in the partial ordering.

11.5. Mysterious Missing M-Matrices

We have implemented the procedure of [**CKM**], so far only allowing for modifications of $E^{(1)}$ in the first two rows (and columns). Curiously, in the 17×17 and 21×21 cases, we have been able to find M-matrices which match all of the criteria that the authors of [**CKM**] specify, but which are not in their putative complete list.

Here are their criteria as stated for the 21×21 case:

(i) $M = (m_{ij}) : m_{ii} = 21, m_{ij} \equiv 1 \mod 4, i \neq j; i, j = 1, 2, ..., 21$
(ii) M is symmetric, positive definite
(iii) $\det M \geq 20^{18}.(116)^2$
(iv) $\det M$ is the square of an integer

Here are our extra 21×21 matrices (both with determinant $20^{18}.116^2$):

$$M_{21;1,5} = \begin{pmatrix} 21 & 5 & -3 & -3 & -3 & -3 & -3 & 1 & \cdots & 1 \\ 5 & 21 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 21 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 21 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 21 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 1 & 21 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 1 & 1 & 21 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 21 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 21 \end{pmatrix} \tag{136}$$

and

$$M_{21;1,0,2} = \begin{pmatrix} 21 & -7 & -3 & -3 & 1 & \cdots & 1 \\ -7 & 21 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 21 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 21 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 1 & 21 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & 1 & \cdots & 21 \end{pmatrix} \tag{137}$$

And here are our extra 17x17 matrices (both with determinant $16^{14}.80^2$):

$$M_{17;2,2} = \begin{pmatrix} 17 & 5 & 5 & -3 & -3 & 1 & \cdots & 1 \\ 5 & 17 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 5 & 1 & 17 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 17 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 17 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 1 & 1 & 17 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 17 \end{pmatrix} \tag{138}$$

and

(139)

$$M_{17;-3's} = \begin{pmatrix} 17 & 1 & 1 & -3 & -3 & -3 & -3 & -3 & -3 & 1 & \cdots & 1 \\ 1 & 17 & -3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & -3 & 17 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 17 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 17 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 1 & 17 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 1 & 1 & 17 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 1 & 1 & 1 & 17 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 17 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 17 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 17 \end{pmatrix}$$

So far we've only implemented the ordering described above up to modifications in the first two rows, since more than this gives a combinatorial explosion in number of cases. We hope to make some improvement in the ordering scheme described to handle this.

We note that we have tried to decompose $M_{17;2,2}$ under the assumption that $M_{17;2,2} = RR^T = R^TR$, and, providing that our program is correct, this decomposition is not possible. It might however be the case that $M_{17;2,2} = RR^T$ for some R, and that R^TR equals some other M-matrix with the same eigenvalues. We have checked and ruled this out for one possible pairing of M-matrices (the first step of this check is described in detail in Section 12.4 of the next chapter). Since we cannot find all M-matrices for sure, we cannot rule out for certain $M_{17;2,2}$ decomposing yet.

We further note that in all known cases of maximal decompositions, $M = RR^T = R^TR$.

CHAPTER 12

The Grammian Method: The Decomposition Algorithm

12.1. Finding Constraints on R

We extract from our M-matrices constraints on the possible matching R-matrices, and then conduct a tree search of possible decompositions $M = RR^T$ for $R \in \mathcal{R}$.

We make the key observation:

THEOREM 12.1. *Let A and B be invertible square matrices. Then the eigenvalues for the matrix AB are the same as those for the matrix BA.*

PROOF: Suppose $ABv = \lambda v$. Then

$$BA(A^{-1}v) = A^{-1}ABA(A^{-1}v) = A^{-1}ABv = A^{-1}\lambda v = \lambda(A^{-1}v). \qquad \square$$

So for two matrices A and B in our candidate set which have the same eigenvalues, it is at least possible that

$$A = RR^T \text{ and } B = R^T R$$

for some $R \in \mathcal{R}$. We need to test for this possibility. In the case that there is only one M-matrix for a given set of eigenvectors, we know that if it does decompose, we can use a similarity transform to show that we can find an R such that

$$M = RR^T = R^T R. \tag{140}$$

This means that we are able to produce a natural pairing of an M-matrix A with either another M-matrix B with the same eigenvalues, or else with itself as its own transpose, in such a way as to be able to extract much more information than we could get by using A alone. Assume

$$A = (a_{ij}) = RR^T \text{ and } B = (b_{ij}) = R^T R. \tag{141}$$

(with A possibly equal to B). We are able to extract from our pair of M-matrices some linear constraints, some quadratic constraints and some

determinant constraints. We begin with an obvious linear constraint. Let

$$R = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \\ \vdots \\ \mathbf{r}_n \end{pmatrix} = \begin{pmatrix} \mathbf{c}_1 & \mathbf{c}_2 & \dots & \mathbf{c}_n \end{pmatrix} \tag{142}$$

Then

$$\boxed{a_{ij} = \mathbf{r}_i.\mathbf{r}_j \text{ and } b_{ij} = \mathbf{c}_i.\mathbf{c}_j} \tag{143}$$

This means that we are able to produce restrictions on what the sums of blocks of unknown $\mathbf{r}_i$'s must be.

For example if the upper left hand corner of A looks like:

$$\begin{pmatrix} 17 & -3 & 1 & \dots \\ -3 & 17 & -3 & \dots \\ 1 & -3 & 17 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \tag{144}$$

and we have already built

$$\begin{aligned} \mathbf{r}_1 = &\ (1, \ -, \ -, \ 1,1, \ -,-, \ -,-,-, \ 1,1,1, \ 1,1,1,1), \\ \mathbf{r}_2 = &\ (-, \ -, \ 1, \ -,-, \ -,-, \ 1,1,1, \ -,-,-, \ 1,1,1,1), \end{aligned}$$

then our new row $\mathbf{r}_3$ is broken naturally into blocks as indicated by semicolons.

$\mathbf{r}_3 =$ (a; b; c; d,e; f,g; h,i,j; k,l,m; n,o,p,q).

Defining $D = d+e$, $F = f+g$, $H = h+i+j$, $K = k+l+m$, $N = n+o+p+q$, and since from the fragment of the matrix A shown above we must have $\mathbf{r}_1.\mathbf{r}_3 = 1$ and $\mathbf{r}_2.\mathbf{r}_3 = -3$, we obtain the following set of simultaneous linear Diophantine equations.

$$\begin{aligned} 1 &= \ a \ -b \ -c \ +D \ -F \ -H \ +K \ +N, \\ -3 &= -a \ -b \ +c \ -D \ -F \ +H \ -K \ +N. \end{aligned}$$

Applying the inequalities gives a list of possible new $\mathbf{r}_3$'s to try.

To derive our other constraints, write

$$R = \begin{pmatrix} 1 & \mathbf{y}^T \\ \mathbf{x} & R' \end{pmatrix}, \ R^T = \begin{pmatrix} 1 & \mathbf{x}^T \\ \mathbf{y} & R'^T \end{pmatrix}, \ A = \begin{pmatrix} n & \mathbf{a}^T \\ \mathbf{a} & A' \end{pmatrix}, \ B = \begin{pmatrix} n & \mathbf{b}^T \\ \mathbf{b} & B' \end{pmatrix} \tag{145}$$

where $\mathbf{x}$, $\mathbf{y}$, $\mathbf{a}$ and $\mathbf{b}$ are $(n-1) \times 1$ column vectors and R', A' and B' are $(n-1) \times (n-1)$ square matrices.

Multiplying out $A = RR^T$ and $B = R^T R$ gives

$$A = \begin{pmatrix} n & \mathbf{x}^T + \mathbf{y}^T R'^T \\ \mathbf{x} + R'\mathbf{y} & \mathbf{x}\mathbf{x}^T + R'R'^T \end{pmatrix}$$

$$B = \begin{pmatrix} n & \mathbf{y}^T + \mathbf{x}^T R' \\ \mathbf{y} + R'^T\mathbf{x} & \mathbf{y}\mathbf{y}^T + R'^T R' \end{pmatrix}$$

Equating entries in the top right hand corners gives

$$\mathbf{a}^T = \mathbf{x}^T + \mathbf{y}^T R'^T, \tag{146}$$

$$\mathbf{b}^T = \mathbf{y}^T + \mathbf{x}^T R'. \tag{147}$$

Multiplying on the right hand side of these equations by $\mathbf{x}$ and $\mathbf{y}$ respectively gives

$$\begin{aligned} \mathbf{a}^T\mathbf{x} &= \mathbf{x}^T\mathbf{x} + \mathbf{y}^T R'^T\mathbf{x} \\ &= (n-1) + \mathbf{y}^T R'^T\mathbf{x}, \end{aligned}$$

and

$$\begin{aligned} \mathbf{b}^T\mathbf{y} &= \mathbf{y}^T\mathbf{y} + \mathbf{x}^T R'\mathbf{y} \\ &= (n-1) + \left(\mathbf{y}^T R'^T\mathbf{x}\right)^T. \end{aligned}$$

Then noticing that $\mathbf{y}^T R'^T\mathbf{x}$ is just a number, and is thus equal to its transpose, we get

$$\boxed{\mathbf{a}^T\mathbf{x} = \mathbf{b}^T\mathbf{y}} \tag{148}$$

Now equating entries in the bottom right hand corners we have

$$A' = \mathbf{x}\mathbf{x}^T + R'R'^T \tag{149}$$

$$B' = \mathbf{y}\mathbf{y}^T + R'^T R' \tag{150}$$

Then multiplying (149) by $\mathbf{x}$ on the right and $\mathbf{x}^T$ on the left, and using (147) and (148) gives

$$\begin{aligned} \mathbf{x}^T A'\mathbf{x} &= (n-1)^2 + \left(\mathbf{x}^T R'\right)\left(R'^T\mathbf{x}\right) \\ &= (n-1)^2 + \left(\mathbf{b}^T - \mathbf{y}^T\right)(\mathbf{b} - \mathbf{y}) \\ &= n(n-1) + \mathbf{b}^T\mathbf{b} - 2\mathbf{b}^T\mathbf{y} \\ &= n(n-1) + \mathbf{b}^T\mathbf{b} - 2\mathbf{a}^T\mathbf{x}. \end{aligned}$$

Similarly we can produce

$$\mathbf{y}^T B'\mathbf{y} = n(n-1) + \mathbf{a}^T\mathbf{a} - 2\mathbf{b}^T\mathbf{y}. \tag{151}$$

We have found the quadratic constraints

$$\boxed{\begin{aligned}\mathbf{x}^T A'\mathbf{x} + 2\mathbf{a}^T\mathbf{x} - \mathbf{b}^T\mathbf{b} - n(n-1) &= 0,\\ \mathbf{y}^T B'\mathbf{y} + 2\mathbf{b}^T\mathbf{y} - \mathbf{a}^T\mathbf{b} - n(n-1) &= 0.\end{aligned}} \tag{152}$$

We are not yet finished with (149) and (150). We can also use them to get the determinantal constraints

$$\boxed{\det(A' - \mathbf{x}\mathbf{x}^T) = (\det R')^2 = \det(B' - \mathbf{y}\mathbf{y}^T)} \tag{153}$$

Note that since R' is unknown, the constraint here is perfect squareness, not equality with some known square.

Here is a summary of all the constraints we have gleaned:

12.2. Summary of Constraints on R

$$a_{ij} = \mathbf{r_i}.\mathbf{r_j} \text{ and } b_{ij} = \mathbf{c_i}.\mathbf{c_j} \tag{154}$$

$$\mathbf{a}^T\mathbf{x} = \mathbf{b}^T\mathbf{y} \tag{155}$$

$$\det(A' - \mathbf{x}\mathbf{x}^T) = \det(B' - \mathbf{y}\mathbf{y}^T) \tag{156}$$

$$\mathbf{x}^T A'\mathbf{x} + 2\mathbf{a}^T\mathbf{x} - \mathbf{b}^T\mathbf{b} - n(n-1) = 0 \tag{157}$$

$$\mathbf{y}^T B'\mathbf{y} + 2\mathbf{b}^T\mathbf{y} - \mathbf{a}^T\mathbf{a} - n(n-1) = 0 \tag{158}$$

$$\det(A' - \mathbf{x}\mathbf{x}^T) = \text{ a perfect square} \tag{159}$$

$$\det(B' - \mathbf{y}\mathbf{y}^T) = \text{ a perfect square} \tag{160}$$

12.3. Searching for R

Overview:
At each stage we use those equations which involve $\mathbf{x}$ (resp. $\mathbf{y}$) to generate a list of possible $\mathbf{x}$'s (resp. $\mathbf{y}$'s). We then check against the constraints which couple the two to generate a list of possible pairs $(\mathbf{x}, \mathbf{y})$.

We take the first pair, put it in our R-matrix, and generate the new sub-problem. We repeat this process until we have either constructed the whole R-matrix, or until one of our constraints has no solution. At such a point we backtrack to our last arbitrary choice of $(\mathbf{x}, \mathbf{y})$, and continue from there.

We search the entire tree of possibilities in this manner, to either produce a list of solutions or a proof that none exist. In most instances in the literature, this method is only being used as a proof of non-existence.

We have made the empirical observation, based on trials so far, that when a solution (i.e. an R-matrix such that $A = RR^T$ and $B = R^T R$) does not exist the program usually hits a wall within the first few levels, and so finishes very quickly. So far the exceptions seem to be when we've tried it on an $n \equiv 3 \pmod 4$ case, when it has often got very deep into the structure before backtracking. This deserves further investigation.

If we have produced a plurality of solutions, we check to see if these are unique up to equivalence. It would be nice to have fast algorithm to do this, but at the moment we just try permutations of rows and columns to see if we can transform members of the list into each other.

More detail:
The first step is distinct from all the others in that we don't have any previous rows/columns of R to use, so we can't use constraints (154). So we always begin with the quadratic constraints (157) and (158). Also, the entry in the top left hand corner of R hasn't been defined yet. Without loss of generality we choose it to be '1'.[1].

Here is the first step of a particular example carried out by hand, with comments upon technical difficulties and opportunities segued in at the end:

[1]Since R is always multiplied by R^T it's overall sign is irrelevant, hence we can choose it to be anything we want. We can use this freedom to fix the entry in the (1,1) position

12.4. The Quadratic Constraints: an Example

$$A = \begin{pmatrix} 17 & -3 & -3 & -3 & -3 & -3 & -3 & -3 & -3 & 1 & \cdots & 1 \\ -3 & 17 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 17 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 17 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 17 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 1 & 17 & 1 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 1 & 1 & 17 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 1 & 1 & 1 & 17 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 17 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 17 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 17 \end{pmatrix} \qquad B = \begin{pmatrix} 17 & 5 & 5 & -3 & -3 & 1 & \cdots & 1 \\ 5 & 17 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 5 & 1 & 17 & 1 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 17 & 1 & 1 & \cdots & 1 \\ -3 & 1 & 1 & 1 & 17 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 1 & 1 & 17 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 17 \end{pmatrix}$$

$$A = \begin{pmatrix} 17 & \mathbf{a}^T \\ \mathbf{a} & A' \end{pmatrix} \qquad B = \begin{pmatrix} 17 & \mathbf{b}^T \\ \mathbf{b} & B' \end{pmatrix}$$

Apply first (157) and (158)

$$\mathbf{x}^T A' \mathbf{x} + 2\mathbf{a}^T \mathbf{x} - n(n-1) - \mathbf{b}^T \mathbf{b} = 0$$

$$\mathbf{b}^T \mathbf{b} = 80$$

$$\mathbf{x}^T A' \mathbf{x} + 2\mathbf{a}^T \mathbf{x} = 352$$

$$\mathbf{y}^T B' \mathbf{y} + 2\mathbf{b}^T \mathbf{y} - n(n-1) - \mathbf{a}^T \mathbf{a} = 0$$

$$\mathbf{a}^T \mathbf{a} = 80$$

$$\mathbf{y}^T B' \mathbf{y} + 2\mathbf{b}^T \mathbf{y} = 352$$

Now write:

$$\mathbf{a} = -4(\mathbf{e}_1 + \cdots + \mathbf{e}_8) + \mathbf{1}_{16} \qquad \mathbf{b} = 4(\mathbf{e}_1 + \mathbf{e}_2) - 4(\mathbf{e}_3 + \mathbf{e}_4) + \mathbf{1}_{16}$$

$$A' = \mathbf{1}_{16}\mathbf{1}_{16} + 16\,\mathbf{I} \qquad B' = \mathbf{1}_{16}\mathbf{1}_{16} + 16\,\mathbf{I}$$

Substitute and tidy up (noting that $\mathbf{x}^T \mathbf{1}_{16} = \mathbf{1}_{16}^T \mathbf{x} = (x_1 + \cdots + x_{16})$, completing the square, and using the facts $\mathbf{e}_j^T \mathbf{x} = x_j$ and $\mathbf{x}^T \mathbf{x} = 16$) to get

$$\boxed{97 + 8(x_1 + \cdots + x_8) = (\mathbf{x}^T \mathbf{1}_{16} + 1)^2} \qquad \boxed{\begin{array}{c} 97 + 8(-y_1 - y_2 + y_3 + y_4) \\ = (\mathbf{y}^T \mathbf{1}_{16} + 1)^2 \end{array}}$$

We need to find candidate $\mathbf{x}$'s and $\mathbf{y}$'s which satisfy these equations. I will just do the calculation for the $\mathbf{y}$'s.

Each y_i may take the value 1 or -1. So we have the following table of possibilities:

$-y_1 - y_2 + y_3 + y_4$	$97 + 8(-y_1 - y_2 + y_3 + y_4)$
-4	65
-2	$81 = 9^2$
0	97
2	113
4	129

Since in this case 81 is the only square, we only need to look for the y_i's corresponding to $-y_1 - y_2 + y_3 + y_4 = -2$.

Since y_1 and y_2 naturally group together, and y_3 and y_4 naturally group together, there are essentially only two possibilities, where we follow the convention that where we have an arbitrary choice we place 1's to the left and $-$'s to the right:

y_1	y_2	y_3	y_4
1	1	1	$-$
1	$-$	$-$	$-$

We require that

$$\begin{aligned}(\mathbf{y}^T\mathbf{1}_{16} + 1)^2 =& 97 + 8(-y_1 - y_2 + y_3 + y_4)\\ =& 81\end{aligned}$$

so that

$$\mathbf{y}^T\mathbf{1}_{16} + 1 = \pm 9$$

which implies that

$$\mathbf{y}^T\mathbf{1}_{16} = \begin{cases} -10 \\ 8 \end{cases}$$

so that we now have possible $\mathbf{y}^T$ vectors:

y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8	y_9	y_{10}	y_{11}	y_{12}	y_{13}	y_{14}	y_{15}	y_{16}
1	1	1	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
1	1	1	$-$	1	1	1	1	1	1	1	1	1	$-$	$-$	$-$
1	$-$	$-$	$-$	1	1	1	1	1	1	1	1	1	1	$-$	$-$
1	$-$	$-$	$-$	1	1	1	1	1	1	1	1	1	1	1	$-$

We then go back and do the same thing for the $\mathbf{x}$'s. So then we can make a list of all possible pairings of $\mathbf{x}$-vectors and $\mathbf{y}$-vectors that satisfy

$$\det(A' - \mathbf{x}\mathbf{x}^T) = (\det R')^2 = \det(B' - \mathbf{y}\mathbf{y}^T).$$

Using each of these pairs in turn we can begin our tree search.

12.5. Comments

In subsequent steps there are also the linear constraints (155). The program in its current incarnation first finds solutions for the quadratic equations (157) and (158), and then checks them against the linear equations. The method of 'solving' the quadratics is simply to enumerate possibilities and exclude those which don't work.

Alternatively (after the first row and column are built), we could try solving the linear equations first and checking against the quadratic.

At the moment we don't really know which order is better per se., since we don't know how sharply our various constraints prune the possibilities back. We also don't know how much overlap there is between exclusions due to the various constraints. It is not clear how we could do this theoretically at this point. For this reason it is our intention to rewrite the code in C and run some diagnostics, to see where it spends most of its time.

One reason why it might be very much more sensible to solve for linear constraints first, and then just check against the quadratic [2], is that more is known about solving linear systems of Diophantine equations than is known about solving quadratic Diophantine equations in many variables.

Much work has been done in recent years on solving linear systems of Diophantine equations (subject to inequalities). References are [**A**], [**AC**], citeGLS and [**Sc**]. We hope to utilize these techniques in a new version of our algorithm.

We comment that [**CKM**] use the quadratic technique outlined above to prove that certain matrices do not decompose, but that they say very little about how they do produce a decomposition when one exists.

Furthermore, we note that in order to create an efficient decomposition algorithm, we need to solve our old familiar problem of ordering/equivalence, in the context of R-matrices, so that when we're decomposing we don't produce swathes of duplicates of the one R-matrix. Whilst it is easy to define a total ordering, any such we can think of is very difficult to implement. By contrast a partial ordering is harder to define sensibly, and is less efficient in the sense that it allows duplication, but may be much easier to implement efficiently. Once again, we have a trade-off. Our current program does implement a partial ordering based on the lexicographical ordering to cut some duplication, but there is much room for improvement. Our hope is to greatly improve this, perhaps by incorporating some of the ideas of Brendan McKay, [**M, M1, M2, BKMS**].

[2] Of course it would be nice to have some sleek technique for solving (where 'solving' means coming up with a prescription to list all solutions) both directly. My expectation is that that would be very difficult, and maybe not faster than just checking.

CHAPTER 13

Concluding Remarks

13.1. Conclusion

There is much work to be done on the Hadamard maximal determinant problem, and related problems. The four general bounds found by Hadamard, Barba, Wojtas and Ehlich [**H, Ba, Wo, E1, E2, EZ**] provide a framework from within to consider the state of knowledge. The infinite families provided by researchers such as Sylvester, Paley and Brouwer [**S, Pa, B**] demonstrate that at least in these cases there is a structure to be uncovered. We want to know, are these known families slender threads of order that run through a terrain of constrained randomness, or is there a general predictable pattern to be revealed?

With respect to the Hadamard Conjecture (by Paley [**Pa**]) that there exists a Hadamard matrix of order n for all n divisible by four, it is very striking that the number of inequivalent Hadamard matrices appears to increase very rapidly [**S12**] with n, and yet so far no one has been able to prove that we can always find even one Hadamard matrix.

I note that all proofs of maximal determinants that I am aware of are constructive, in the sense that they involve providing a recipe for exhibiting a maximal matrix. There are no proofs of the form, 'There exists a ...'. Is this a necessary outcome of the nature of the problem?

The very bad exponential growth of the problem presents difficulties in getting data experimentally, and the mod four dependence of the results compounds this issue by separating results in comparable cases by a large computational leap. Also, the higher the order the more widely spaced the known values become.

The Hadamard maximal determinant problem belongs to the class of problems which are easy to state and hard(?) to solve. The vast majority of the known results have been based on either intricate (as in the Brouwer construction) or else computationally arduous (as in the Grammian method) uses of elementary techniques primarily of abstract and linear algebra. And there's no evidence that the fruits of these techniques have been exhausted. I am sure that more particular values of $g(n)$ can be found and proven with existing techniques. It is also quite likely that further constructions for special families of solutions may be found with some ingenuity. What is not

clear to me is what a general solution of the problem would or could look like.

Following is a list of ideas for further research, most of them aimed at generating more data.

13.2. Ideas for further research

i. Rewrite the 'Grammian Method' programs in a compiled language such as 'C', reordering the application of the constraints in such a way as to prune the search tree more severely. Within the Decomposition program, utilize the ideas of researchers such as Karen Aardal et al. [**A**], into efficient solving of linear systems of Diophantine equations. With respect to the equivalence issues that arise in both the Decomposition and the M-matrix program, consider implementing the ideas of Brendan McKay [**M**]. Also consider combining the two programs into one for further gains in efficiency. Another possibility would be to take advantage of parallelizing the algorithms, so that they might be run on several machines at once, thus making better use of computer resources. My expectation is that these methods should be able to prove the maximal value for $n = 15$, verify the results for $n = 17$ and 21, the published results for which in [**MK**] and [**CKM**] we found to be incomplete, find the maximal value for $n = 19$, confirm or disconfirm our guessed value for $n = 29$, and possibly make even further inroads into unknown territory.

ii. Investigate by means of random/semi-random computer searches, the entire spectrum of determinants available to an $n \times n$ matrix with ± 1 entries. Investigate both with respect to which numbers are allowed, and how frequently they occur. The former investigation may be more computationally accessible, since its memory requirements, though still substantial, are likely to be less than the latter. With respect to the latter, graph the determinants against their frequency, and see whether the histograms thus produced can be well approximated by curves predicted by random matrix theory. If so, try to see whether the deviation from the curve can be predicted by any number theoretic properties of the values of n for which the histogram is noticeably above or below the predicted curve. Might the Hadamard bound, $n^{n/2}$, have particularly nice divisibility properties, for instance, which ensure that it occurs even when determinants close to it do not? Alternatively, if random matrix theory does not predict the shape of our histograms, try to explain why not, and possibly use curve-fitting techniques to try to find out what the dominating distribution is.

iii. Further investigate the spectrum of available determinants, possibly in the context of binary matrices of order m by regarding the determinant as a kind of generalized (in the sense that negatives are allowed)

integer partition with at most m parts, derived from the cofactor expansion. The allowable entries in the partition come from allowable determinants of binary matrices of lower orders. Such an approach was used by Craigen in [**Cr**] to show that certain determinantal values close to the maximal value were not obtainable in a binary matrix of order 7. Also, read up on the early work of Sylvester [**S**], who seems to have also used integer partitions. Further in this regard, calculate minors of known maximal matrices to at least four orders down from the matrix size, to check whether any recurrences with modulo four dependency may be observed.

iv. Consider arbitrary square $\{0,1\}$ matrices as incidence matrices of a directed graph? Does a high determinant correspond to any important property of graphs, and can graph theory tell us anything about graphs/matrices with high determinant?

v. Consider a hill-climbing or random search for large determinants that works by, instead of modifying entries in some ± 1 matrix, starting with a known orthogonal or close to orthogonal matrix with low determinant and arbitrary entries (for instance a multiple of the identity matrix of some given size) and then giving it random rotational kicks about the axes, and after each kick approximating each real entry with the closest of $-1, 0$ or 1 simply by taking the sign of that entry. Also calculate what rotations, broken up into rotations about the axes in some order, are required to produce known maximal matrices from some natural starting point, and see if any pattern can be observed.

vi. Look up the proof of Theorem 4.9, which states that under certain conditions the matrix $nI + J$, where I is the $n \times n$ identity matrix and J is the $n \times n$ matrix of all 1's, decomposes in the form AA^T for A a matrix with rational entries. See whether we can modify it for matrices of the form $(n-1)I + J$, especially when $n \equiv 1$ modulo 4, and whether the method of proof could give any insight if further restrictions were placed on the rational entries of A, for instance that they must be between -1 and 1 in magnitude.

vii. Consider 'M-matrices' of the form AXA^T and A^TXA, for some fixed X in the middle. This was suggested to my collaborator Will by Dr Brendan McKay. It corresponds to maximizing the volume of a parallelepiped in $\mathbb{R}^n$ under a different (inner product) norm to the standard Euclidean one.

viii. Investigate what happens when you apply the Brouwer construction starting with a matrix which is not quite Hadamard. See if a small change in the input produces a small or a large change in the usefulness of the output. This might be of use in the $n \equiv 1 \pmod 4$ cases for which n is not a sum of two consecutive squares. Also, try to understand more deeply the motivation for the use of finite fields in the original Brouwer construction, and whether the algorithm might be

modified to deal with cases in which n *is* the sum of two squares, but such that the smaller one does *not* arise from taking a power of an odd prime.

Part D

Postlude

Bibliography

[A] Karen Aardel, Cor Hurkens, Arjen K. Lenstra, Solving a system of diophantine equations with lower and upper bounds on the variables, Report UU-CS-1998-36, Department of Computer Science, Utrecht University, 1998. http://www.cs.uu.nl/research/techreps

[AC] F. Ajili and E. Contejean, Avoiding slack Variables in the Solving of Linear Diophantine Equations and Inequations, *Theoret. Comput.Sci.* **173** (1997), 183–208.

[B] A. E. Brouwer, An infinite series of symmetric designs, *Math. Centrum Amsterdam Report ZW* **202/83** (1983).

[Ba] G. Barba, Intorno al teorema di Hadamard sui determinanti a valore massimo, Giorn. Mat. Battaglini 71 (1933) 70-86.

[Be] V. Belevitch, Conference Networks and Hadamard Matrices, *Ann. Soc. Scientifique Bruxelles*, **82** (I) (1968) 13–32.

[Bi] Stephen Bilaniuk Champlain College H12 Trent University course notes for Mathematics 426H–Geometry III: Topics in Geometry www.trentu.ca/academic/math/sb/426H/pcpp-02-chapter1.pdf

[Br] Proofs and Confirmations: The Story of the Alternating Sign Matrix Conjecture, Cambridge University Press, 1999. David M Bressoud

[BC] J. Brenner and L. Cummings, The Hadamard Maximum Determinant Problem, *Am. Math. Month.* **79** (1972) 626–630.

[BGH] L. D. Baumert, S. Golomb, and M. Hall Jr., Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.* **68** (1962) 237–238.

[BHH] W. G. Bridges, M. Hall Jr., and J. L. Hayden, Codes and designs, *J. Combin. Theory, Ser. A* **31** (1981) 155–174.

[BKMS] F. Bussemaker, I. Kaplansky, BD McKay and JJ Seidel, Determinants of Matrices of the Conference Type, *Linear Algebra and its Applications* **261** (1997) 275–292

[C1] J. H. E. Cohn, Determinants with elements ± 1 *Journal London Math. Soc.* **42** (1967) 436-442

[C2] J. H. E. Cohn, On determinants with elements ± 1, II, *Bull. London Math. Soc.* **21** (1989) 36–42.

[C3] J. H. E. Cohn, Almost D-optimal designs, *Utilitas Math.* **57** (2000) 121–128.

[C] R. Courant *Differential and Integral Calculus, Volume II* Blackie and Son Limited, London and Glasgow 1936.

[Ca] Alan J Cain MathEnomIcon http://www.cenius.net/refer/articles/b/~balancedincompleteblockdesign_ency.asp

[CF] Michael Clausen, Albrecht Fortenbacher, *J. Symbolic Computation* 8 (1989) 201–216

[Ch] Comb. Structures Lecture Notes on Block Designs http://www-math.cudenver.edu/~wcherowi/courses/m6406/cslnb.html

[Cr] R. Craigen, The Range of the Determinant Function on the Set of $n \times n$ (0,1)-Matrices, *JCMCC* **8** (1990) 161–171

[CK] T. Chadjipantelis and S. Kounias, Supplementary difference sets and D-optimal designs for $n \equiv 2 \bmod 4$, *Discrete Math.* **57** (1985) 211–216.

[CKM] T. Chadjipantelis, S. Kounias and C. Moyssiadis, The maximal determinant of 21×21 $(+1,-1)$-matrices and D-optimal designs, *J. Stat. Plann. Inference* **16** (1987) 167–178.

[D] P. Delsarte, J.-M. Goethals, and J.J. Seidel, Orthogonal Matrices with zero diagonal II., *Canad, J, Math.*, **23** (1971) 816–832.

[E1] H. Ehlich, Determinantenabschätzungen für binäre Matrizen, *Math. Zeitschr.* **83** (1964) 123–132.

[E2] H. Ehlich, Determinantenabschätzungen für binäre Matrizen mit $n \equiv 3 \bmod 4$, *Math. Zeitschr.* **84** (1964) 438–447.

[EZ] H. Ehlich und K. Zeller, Binäre matrizen, *Z. Angew. Math. Mech.* **42** (1962) T20–T21

[EM] H. Enomoto and M. Miyamoto, On maximal weights of Hadamard matrices, *J. Combin. Theory Ser. A* **29** (1980) 94–100.

[FK1] N. Farmakis and S. Kounias, The excess of Hadamard matrices and optimal designs, *Discrete MAth.* **67** (1987) 165–176.

[FK2] N. Farmakis and S. Kounias, The excess of Hadamard matrices, *Discrete Math.* **68** (1988) 59–69.

[GK1] Z. Galil and J. Kiefer, D-optimum weighing designs, *Ann. Stat.* **8** (1980) 1293–1306.

[GK2] Z. Galil and J. Kiefer, Construction methods for d-optimum weighing designs when $n \equiv 3 (\bmod 4)$, *Ann. Stat.* **10** (1982) 502–510.

[GLS] M. Grötschel, L. Lovász and A. Schrijiver, Geometric Algorithms amd Combinatorial Optimization, Berlin, New York: Springer Verlag 1993.

[H] J. Hadamard, Resolution d'une question relative aux determinants, *Bull. des Sci. Math.* **17** (1893) 240–246.

[Ha] M. Hall, Jr. Combinatorial Theory. 2nd edn. New York: Wiley (1986)

[HK] W.H.Holzmann, H. Kharaghani, *A D-Optimal Design of order 150* **190** (1998) 265–269

[HSS] A.S. Hedayat, N.J.A. Sloane, John Stufken, *Orthogonal Arrays: Theory and Applications*,Springer Series in Statistics, Springer-Verlag New York, 1999.

[JJ] J. Johnson, Plackett-Burman designs using galois fields, Unpublished report (see `http://www.ibiblio.org/smiley/expdesign`).

[Ko] C. Koukouvinos, On almost D-optimal first order saturated designs and their efficiency, *Utilitas Mathematica* **52** (1997) 113–121.

[Ka] W. Kahan, Chió's trick for linear equations with integer coefficients, Unpublished lecture notes (see `http://www.cs.berkeley.edu/~wkahan/MathH110/` (as of Nov. 2001)).

[Kh] H. Kharaghani, A construction of D-optimal designs for $n \equiv 2 \bmod 4$, *J. Combin. Theory, Ser. A* **46** (1987) 156–158.

[KMS] C. Koukouvinos, M. Mitrouli and J. Seberry, Bounds on the maximum determinant for $(1, -1)$ matrices, *Bull ICA* **29** (2000) 39–48.

[KKS] C. Koukouvinos, S. Kounias and J. Seberry, Supplementary difference sets and optimal designs, Discrete Math. 88 (1991) 49-58.

[L] C.W.H. Lam, The Search for a Finite Projective Plane of Order 10 *American Mathematical Monthly* textbf98 (1991) 305–318.

[LTS] C.W.H. Lam, L.H. Theil, and S. Swiercz, The nonexistence of a finite projective plane of order 10. *Canadian J. Math* **41** (1989) 1117–1123.

[M] Brendan D McKay, Isomorph-free Exhaustive Generation, unpublished talk at the University of Melbourne Mathematics and Statistics Department, 2002.

[M1] B. D. McKay, Computing automorphisms and canonical labellings of graphs, *Combinatorial Mathematics, Lecture Notes in Mathematics*, 686, Springer-Verlag, Berlin, 1978.

[M2] B. D. McKay, Hadamard equivalence via graph isomorphism, *Discrete Mathematics*, **27** (1979) 213–216.

[Me] Madan Lal Mehta, *Matrix Theory: Selected Topics and Useful Results*, les éditions de physique 1977.

[Mey] Carl D. Meyer, *Matrix Analysis and Applied Linear Algebra*, SIAM (The Society for Industrial and Applied Mathematics) 2000.

[MK] C. Moyssiadis and S. Kounias, The exact D-optimal first order saturated design with 17 observations, *J. Stat. Plann. Inference* **7** (1982) 13–27.

[MS] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North Holland 1978.

[NR] M. G. Neubauer and A. J. Radcliffe, The maximum determinant of (± 1)-matrices, *Linear Algebra Appl.* **257** (1997) 289–306.

[O] W.P.Orrick. `http://www.ms.unimelb.edu.au/~worrick`

[P] S. E. Payne, On maximising $\det(A^T A)$, *Discrete Mathematics* **10** (1974) 145–158.

[Pa] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933) 311–320.

[Pas] Diagram Geometries by Antonio Pasini, Oxford Science Publications, Oxford University Press, 1994 ... a review on the web thereof

[R] D. Raghavarao, Some optimum weighing designs, *Ann. Math. Statist.* **30** (1959) 295–303.

[S] J. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers, *London Edinburgh and Dublin Philos. Mag. and J. Sci.* **34** (1867) 461–475.

[Sc] A. Schrijver, Theory of Linear and Integer Programming, Chichester; New York: Wiley, 1986.

[Sl] N.J.A. Sloane, My Favorite Integer Sequences `www.research.att.com/~njas/doc/sg.pdf`

[Sl2] N.J.A. Sloane, The Online Encyclopedia of Integer Sequences, `http://www.research.att.com/~njas/sequences/`

[So] B. Solomon. These references are to matrices found by Bruce Soloman, using a program which had it's genesis in work with R. Dowdeswell, and earlier still with M. Neubauer and K. Turner. Some matrices were communicated privately to my collaborator Will Orrick. Others were published on the web page `http://www.imrryr.org/~elric/matrix/`, of R. Dowdeswell, M. Neubauer, B. Solomon and K. Turner.

[Sm] Warren D. Smith, Studies in Computational Geometry Motivated by Mesh Generation, Ph. D. dissertation, Princeton University (1988).

[Sp] E. Spence, Skew-Hadamard matrices of the Goethals-Seidel type, Canad. J. Math. 27 (1975) 555-560.

[V] T. Van Trung, The existence of symmetric block designs with parameters $(41, 16, 6)$ and $(66, 26, 10)$, *J. Combin. Theory, Ser. A* **33** (1982) 201–204.

[W] J. Williamson, Determinants whose elements are 0 and 1, *Amer. Math. Monthly* **53** (1946) 427–434.

[W2] J. Williamson, Hadamard's Determinant Theorem and the sum of four squares. *Duke Math. J.*, **11** 65–81.

[Wa] W.D. Wallis, *Combinatorial Designs*, marcel Dekker, Inc., 270 Madison Avenue, New York, New York, 1988.

[We] Eric Weisstein's World of Mathematics `http://www.mathworld.wolfram.com/`

[Wel] T.A. Welsh. These references are to matrices found by Trevor Welsh, and communicated privately to my collaborator Will Orrick. Those currently up to date are available at `http://www.ms.unimelb.edu.au/~worrick/maxdet`

[Wh] A.L. Whiteman, A family of D-optimal designs, *Ars Combinatoria*, **30** (1990), 23-26.

[Wo] W. Wojtas, On Hadamard's inequality for the determinants of order non-divisible by 4, Colloq. Math. 12 (1964) 73-83.

[Y1] C. H. Yang, Some designs for maximal $(+1, -1)$-determinant of order $n \equiv 2 \pmod 4$, *Math. Comput.* **20** (1966) 147–148.

[Y2] C. H. Yang, On designs of maximal $(+1, -1)$-matrices of order $n \equiv 2 \pmod 4$, *Math. Comput.* **22** (1968) 174–180.

[Y3] C. H. Yang, On designs of maximal $(+1, -1)$-matrices of order $n \equiv 2 \pmod 4$. II, *Math. Comput.* **23** (1969) 201–205.

[Y4] C. H. Yang, Maximal binary matrices and sum of two squares, *Math. Comput.* **30** (1976), 148–153.

[Y5] C. H. Yang, A construction of maximal $(+1, -1)$-matrix of order 54, *Bull. Amer. Math. Soc.* **72** (1966) 293.

APPENDIX A

Properties of Matrices & Determinants

1.1. Properties of the Determinant Function

Here is a selection of properties of the determinant function. Particularly useful in many of our calculations is the Rank-One Update theorem, which means that given the determinant of some arbitrary $n \times n$ matrix A, we can calculate the determinant of $A + B$, where B is some other $n \times n$ matrix of rank equal to one. Most of this material comes from [**Mey**].

DEFINITION 18. Let $A = (a_{ij})$ be an arbitrary $n \times n$ matrix. Then the *determinant* of A is defined to be

$$\det A = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)},$$

where S_n is the set of all permutation of n elements.

LEMMA A.1. *(From* [**Mey**, p 494] *or* [**Me**].*) The determinant of a square matrix is the product of it's eigenvalues; i.e. for $A = (a_{ij})$ an $n \times n$ matrix with eigenvalues $\lambda_1, .., \lambda_n$,*

$$\sum_{i=1}^{n} a_{ii} = \sum_{i=1}^{n} \lambda_i$$

PROOF: Let $\det(A - \lambda I) = 0$ be the characteristic equation of A, with roots (eigenvalues) $\lambda_1, .., \lambda_n$. The result is obtained easily enough by comparing the results of two different ways of calculating the coefficients of λ^{n-1}:

Consider $A - \lambda I$. Calculating the determinant using the definition involves taking products of n elements in such a way that you never take more than one element from any given row or column.

To get λ^{n-1} you need to take $n - 1$ entries on the diagonal, but then having taken $n - 1$ of them you have to take the n^{th} one as well since that's the only valid possibility left to make up the product.

Hence we're looking for the coefficient of λ^{n-1} in

$$(a_{11} - \lambda)(a_{22} - \lambda)...(a_{nn} - \lambda),$$

which is

$$\sum_{i=1}^{n} a_{ii}. \tag{161}$$

Alternatively we know that

$$\det(A - \lambda I) = (\lambda_1 - \lambda)(\lambda_2 - \lambda)...(\lambda_n - \lambda),$$

so that the coefficient of λ^{n-1} is

$$\sum_{i=1}^{n} \lambda_i. \tag{162}$$

Equating (161) and (162) gives the result. □

LEMMA A.2. *(From* [**Mey**, p 494]*) The trace of a square matrix is the sum of it's eigenvalues.*

THEOREM A.3. [Rank-One Update Theorem] *(From* [**Mey**, p 475].*) If A is an $n \times n$ non-singular matrix, and $\mathbf{c}$ and $\mathbf{d}$ are $n \times 1$ column vectors, then*

$$\det(A + \mathbf{c}\mathbf{d}^T) = (\det A)(1 + \mathbf{d}^T A^{-1}\mathbf{c}).$$

THEOREM A.4. [Block Determinant Theorem]*(From* [**Mey**, p 475].*) If A and D are square matrices, then*

$$\begin{aligned} \det \begin{pmatrix} A & B \\ C & D \end{pmatrix} &= \det(A) \det(D - CA^{-1}B) && \text{when } A^{-1} \text{ exists,} \\ &= \det(D) \det(A - BD^{-1}C) && \text{when } D^{-1} \text{ exists,.} \end{aligned}$$

1.2. Properties of Matrices

The following is a collection of mostly well-known definitions and facts about matrices. Many are sourced from 'Eric Weisstein's World of Mathematics [**We**].

DEFINITION 19. An $n \times n$ matrix H with ± 1 entries, such that

$$HH^T = nI_n \tag{163}$$

is called a *Hadamard* matrix.

Note that this definition implies that the rows of H are orthogonal. We could as easily have used the columns, since (163) implies that $\frac{1}{n}H^T = H^{-1}$, so that

$$H^T H = nI_n. \tag{164}$$

DEFINITION 20. (From [**We**].) A matrix, M, with complex entries is called *Hermitian* provided that

$$M = M^\dagger, \tag{165}$$

where $M^\dagger$ is the complex conjugate transpose of M.

LEMMA A.5. *(From* [**We**].*) An integer or real matrix is Hermitian if and only if it is symmetric.*

DEFINITION 21. (From [**We**].) An $n \times n$ Hermitian matrix, M, is called *positive definite* provided that

$$\mathbf{x}^T M \mathbf{x} > 0$$

for all $\mathbf{x} \neq \mathbf{0}$ in $\mathbb{R}^n$.

LEMMA A.6. *(From* [**We**].*)*

- *Positive definiteness of a matrix M is equivalent to the requirement that all the eigenvalues of M are positive.*
- *Positive definiteness of a matrix M is equivalent to the requirement that the determinants associated with all upper-left submatrices are positive.*
- *The determinant of a positive definite matrix is positive, but the converse does not necessarily hold.*

We define our own terminology for the following matrix operation.

DEFINITION 22. A *SymSwap* is the operation of simultaneously permuting a pair of rows and the corresponding pair of columns in some square matrix. i.e. Under SymSwap_{ij},

$$\begin{pmatrix} & a_{1i} & \cdots & a_{1j} & \\ & \vdots & & \vdots & \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{j1} & \cdots & a_{ji} & \cdots & a_{jj} & \cdots & a_{jn} \\ & \vdots & & \vdots & \\ & a_{ni} & \cdots & a_{nj} & \end{pmatrix} \rightarrow \begin{pmatrix} & a_{1j} & \cdots & a_{1i} & \\ & \vdots & & \vdots & \\ a_{j1} & \cdots & a_{jj} & \cdots & a_{ji} & \cdots & a_{jn} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{ii} & \cdots & a_{in} \\ & \vdots & & \vdots & \\ & a_{nj} & \cdots & a_{ni} & \end{pmatrix}.$$

APPENDIX B

The Fischer-Lieb and other Inequalities

All theorems in this section were sourced from [**Me**].

THEOREM B.1. *[Hadamard] If A is Hermitian positive semi-definite, then*

$$\det A \leq a_{11}a_{22}...a_{nn} \tag{166}$$

PROOF: Suppose $a_{ii} = 0$ for some i. Then since all the principal minors of a positive semi-definite matrix are themselves positive semi-definite (and remembering that a Hermitian matrix is symmetric), we have for any j

$$\begin{vmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{vmatrix} = a_{ii}a_{jj} - a_{ij}a_{ji} = -a_{ij}^2 \geq 0$$

implies $a_{ij} = 0$ for all j. Hence we have a whole row of zeros, and $\det A = 0$. So the inequality (166) is trivial.

So assume $a_{ii} > 0$ for all i. Define a new matrix $C = (c_{ij})$, where

$$c_{ij} = \frac{a_{ij}}{\sqrt{a_{ii}a_{jj}}}.$$

For $\mathbf{x}$ any vector, define a new vector $\mathbf{y}$ by

$$y_i = x_i\sqrt{a_{ii}}.$$

Let the eigenvalues of C be $\lambda_1, \lambda_2, ..., \lambda_n$.

Since $\sum_{i=1}^n \lambda_i = \sum_{i=1}^n c_{ii} = \sum_{i=1}^n \frac{a_{ii}}{\sqrt{a_{ii}a_{ii}}} = \sum_{i=1}^n 1 = n$, where I have used Lemma A.1, we have that

$$\left(\frac{1}{n}\sum_{i=1}^n \lambda_i\right)^n = 1. \tag{167}$$

We calculate that from A positive semi-definite we have, for all $\mathbf{x}$,

$$0 \leq \mathbf{x}^\dagger A\mathbf{x} = \mathbf{y}^\dagger C\mathbf{y}$$

which implies C is also positive semi-definite. Hence $\lambda_i \geq 0$ for all i, so that

$$0 \leq \det C = \prod_{i=1}^n \lambda_i \leq \left(\frac{1}{n}\sum_{i=1}^n \lambda_i\right)^n = 1, \tag{168}$$

where the last inequality is obtained by using the fact that the geometric mean is less than or equal to the arithmetic mean of a set of non-negative real numbers, and the last equality follows from (167).

Now since C is obtained from A by multiplying each row i by $\frac{1}{\sqrt{a_{ii}}}$ and each column j by multiplying each column j by $\frac{1}{\sqrt{a_{jj}}}$,

$$\det C = \frac{\det A}{a_{11}a_{22}...a_{nn}} \tag{169}$$

Substituting (169) into (168) gives the desired inequality. □

We state Holder's Inequality without proof:

THEOREM B.2 (Holder's Inequality). *If $\alpha, \beta, ..., \gamma$ are real positive numbers such that $\alpha + \beta + ... + \gamma = 1$, and $(a_j), (b_j), ..., (l_j)$ are sets of n complex numbers each, then*

$$\left|\sum_{j=1}^{n} a_j^{\alpha} b_j^{\beta} ... l_j^{\lambda}\right| \leq \left(\sum_{j=1}^{n} |a_j|\right)^{\alpha} \left(\sum_{j=1}^{n} |b_j|\right)^{\beta} ... \left(\sum_{j=1}^{n} |l_j|\right)^{\lambda}.$$

Taking $\alpha = \beta = ... = \lambda = \frac{1}{n}$ and

$$\begin{array}{cccc} a_1 = x_1, & b_1 = x_2, & \ldots, & l_1 = x_n, \\ a_2 = y_1, & b_2 = y_2, & \ldots, & l_2 = y_n, \\ \vdots & \vdots & & \vdots \end{array}$$

Holder's Inequality gives

COROLLARY B.3.

$$\prod_{j=1}^{n}(x_j + y_j + ...)^{\frac{1}{n}} \geq \prod_{j=1}^{n} x_j^{\frac{1}{n}} + \prod_{j=1}^{n} y_j^{\frac{1}{n}} + ... \tag{170}$$

for x_j, y_j,... real and positive.

THEOREM B.4. *Let A and B be $n \times n$ Hermitian positive semi-definite matrices. Then*

$$(\det(A+B))^{\frac{1}{n}} \geq (\det A)^{\frac{1}{n}} + (\det B)^{\frac{1}{n}}$$

PROOF: Assume without loss of generality that $A + B$ is a diagonal matrix. (Otherwise just diagonalize it, which leaves the determinant unchanged.) Then

$$\begin{aligned} (\det(A+B))^{\frac{1}{n}} &= \prod_{i=1}^{n}(a_{ii} + b_{ii})^{\frac{1}{n}} \\ &\geq \prod_{i=1}^{n} a_{ii}^{\frac{1}{n}} + \prod_{i=1}^{n} b_{ii}^{\frac{1}{n}} \qquad \text{by Holder's Inequality, Corollary B.3} \\ &\geq (\det A)^{\frac{1}{n}} + (\det B)^{\frac{1}{n}} \qquad \text{by Theorem B.1} \end{aligned}$$

□

THEOREM B.5 (Fischer-Lieb). *Let A be an $n \times n$ Hermitian positive semi-definite matrix in the partitioned form*

$$A(n,n) = \begin{pmatrix} P(n-k, n-k) & Q(n-k,k) \\ Q^\dagger(k, n-k) & S(k,k) \end{pmatrix}$$

Then

$$\det A \leq \det P \det S \tag{171}$$

PROOF: Let D be the diagonal matrix with $d_{11} = .. = d_{n-k,n-k} = -1$ and $d_{n-k+1,n-k+1} = .. = d_{n,n} = 1$. Define $B = DAD$. Then

$$B = \begin{pmatrix} P & -Q \\ -Q^\dagger & S \end{pmatrix}$$

is also Hermitian positive semi-definite with the same eigenvalues as A (and hence the same determinant). We have

$$\begin{aligned} 2(\det P \det S)^{\frac{1}{n}} &= (2^n \det P \det S)^{\frac{1}{n}} \\ &= (\det 2P \det 2S)^{\frac{1}{n}} \\ &= (\det(A+B))^{\frac{1}{n}} \\ &\geq (\det A)^{\frac{1}{n}} + (\det B)^{\frac{1}{n}} \qquad \text{by Theorem B.4} \\ &= 2(\det A)^{\frac{1}{n}} \end{aligned}$$

and (171) follows. □

APPENDIX C

Designs

The purpose of these appendices on Designs and Geometry is twofold. Firstly it is to provide a familiarity with much of the language in terms of which the problem of finding maximal matrices is often described in the literature. For instance the Brouwer's paper [**B**]*, which is the topic of Chapter 6, was written in terms of finding designs with given specifications, not in terms of maximizing a determinant. The second purpose is to provide a gateway to similar problems to the one I have been tackling. One hopes that by comparison new perspectives and approaches can be found which may be of benefit in either or both directions.*

For some people the principal focus of the maximal determinant problem is not to find the *number* which is the maximal determinant of a $\{0,1\}$ or a $\{\pm 1\}$ matrix of a given size — the important thing is to find the corresponding *matrix.*

Amongst these are experimental scientists, for such matrices have application in experimental design. For this reason matrices $A \in \mathcal{A}_n$ or $\mathcal{B}_n$ are often called *designs.* The useful matrix $M = AA^T$ (which I have termed the *Grammian,* $G(A)$) is called the *information* matrix.

In the various applications there are several measures of optimality of the design, including maximizing the determinant. A design with maximal determinant is called $D - optimal$.

In some situations the matrices used are not square. In this case for D-optimal designs the design A is chosen such that the information matrix AA^T has maximal determinant. To distinguish between cases in which A is or is not square, the situation in which it is square is called *saturated.*

One of the simplest interpretations of designs are as *weighing designs.* I provide a brief motivation for these; more details can be found in [**MS**]. Another type of design, also used experimentally but with an additional interpretation in terms of finite geometries, is the *block design.* Block designs constitute an example of a general *combinatorial design,* which latter is defined by Wallis in [**Wa**] to be 'a way of selecting subsets from a finite set in such a way that some specified conditions are satisfied. ..[the conditions] tend to involve *incidence*: set membership, set intersection, and so on.' More information on block designs and many other kinds of design can be found in [**Wa**].

APPENDIX D

Weighing Designs

Suppose we want to weigh some very light objects, so light that the error we make in each measurement is comparable to the weight of the objects. One way to get around this problem is to weigh various combinations of objects at once, and then calculate the weights of the individual objects.

Consider the following order seven binary matrix, which comes from taking the eight by eight Hadamard matrix of the Sylvester construction, removing the first row and column and exchanging 1's for -1's and 0's for 1's, as in Chapter 3.

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

It can be regarded as a recipe for weighing seven objects of unknown weights $a, b, c, .., g$, as in the scheme:

$$\begin{array}{ccccccccccccccc} a & & & + & c & & & + & e & & & + & g & = & \text{1st weighing} \\ & & b & + & c & & & & & + & f & + & g & = & \text{2nd weighing} \\ a & + & b & & & & & + & e & + & f & & & = & \text{3rd weighing} \\ & & & & & & d & + & e & + & f & + & g & = & \text{4th weighing.} \\ a & & & + & c & + & d & & & + & f & & & = & \text{5th weighing} \\ & & b & + & c & + & d & + & e & & & & & = & \text{6th weighing} \\ a & + & b & & & + & d & & & & & + & g & = & \text{7th weighing} \end{array}$$

Then since the matrix of coefficients (the design) has non-zero determinant, we can solve for $a, b, .., g$. In this case if the original variance from weighing the objects separately was σ^2, then the new, reduced variance is $\frac{7\sigma^2}{16}$ [**MS**, p 53].

In general if there are n objects to be weighed in n weighings and a Hadamard matrix of order $n+1$ exists, then using this method reduces the variance from σ^2 to $\frac{4n}{(n+1)^2}\sigma^2$, [**MS**, p 53], which in some sense is best possible using one weighing pan.

If our scale has two weighing pans (so that we can form differences as well as sums), then we can do even better.

For instance the order four Hadamard matrix which comes from the Sylvester construction can be used directly to produce the weighing scheme

$$\begin{array}{rcrcrcrl} a & + & b & + & c & + & d & = \text{1st weighing} \\ a & - & b & + & c & - & d & = \text{2nd weighing} \\ a & + & b & - & c & - & d & = \text{3rd weighing'} \\ a & - & b & - & c & + & d & = \text{4th weighing} \end{array}$$

for four objects of unknown weight a, b, c and d.

In this case the variance is reduced from σ^2 to $\frac{\sigma^2}{4}$, [**MS**, p 53].

These techniques are of particular use to chemists weighing very light elements, but can also be used in a plethora of other measurement problems, including those of carefully measuring lengths, voltages, resistances, concentrations of chemicals and frequency spectra.

This description has been taken almost entirely from [**MS**, p 52–53].

APPENDIX E

Block Designs

5.1. Motivation and Definitions

The theory of block designs was developed (largely by R.A. Fisher and F. Yates in the early 1930's) to deal with experimental situations in which there are many variables interacting in unpredictable ways, and when there are insufficient resources to take measurements over every possible combination of inputs, so that it is desirable to select some combination of inputs to measure, in such a way that there is no a priori bias in the design towards a particular outcome. The theory was developed in the context of agricultural experiments, and the terminology reflects the origins of the work. The material in this section is taken from [**Wa**] and [**Ch**]. I originally also used the reference [**Ca**], which is a web reference which has unfortunately been taken down.

A BALANCED INCOMPLETE BLOCK DESIGN (BIBD) consists of

- A set X consisting of v *varieties*, where $v \geq 2$,
- A set Y consisting of b subsets of X, called *blocks*,

subject to the rules:

i. there are k varieties in each block, $v > k > 0$;
ii. there are r blocks containing any given variety, $r > 0$;
iii. there are λ blocks containing any given pair of varieties, $\lambda > 0$.

It may be denoted a (v, b, r, k, λ) design.

A BIBD may be pictured, as in Fig 1 as b blocks of land, over each of which the conditions are fairly even, in which are planted v varieties of grain.

"Balanced" refers to the constancy of k and λ. It's consequence is that the probability of any two varieties being compared (i.e. being in the same block) is the same for all pairs. "Incomplete" refers to the fact that not all varieties appear in all blocks.

The parameters of a BIBD turn out not to be independent:

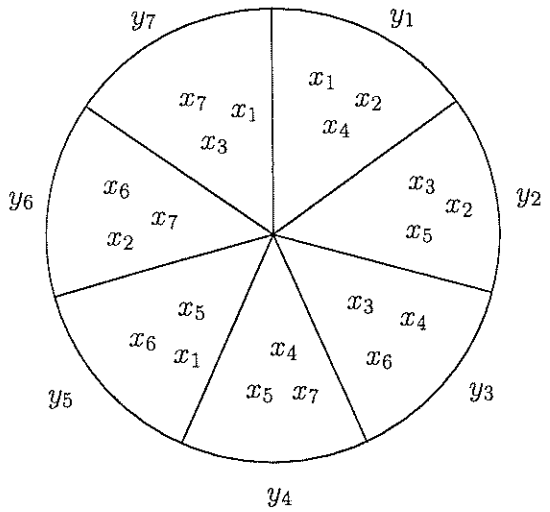


FIGURE 1. A $(7,7,3,3,1)$-design with blocks $y_1, \ldots, y_7$ and varieties $x_1, \ldots, x_7$.

THEOREM E.1. *Given a (v,b,r,k,λ)-design,*

$$bk = vr$$
$$r(k-1) = \lambda(v-1).$$

PROOF: We count the set of pairs (x,y), where x is a variety and y is a block containing x in two different ways. There are v possible values for x, and since r each appears in r blocks, vr counts the number of these pairs. On the other hand, there are b blocks and each contains k varieties, so bk also counts the number of these pairs. Hence we have shown the first equation.

For the second equation, fix a particular variety, say p, and count the number of pairs of varieties (p,y), where p and y appear in some block together and if the pair occurs more than once it is multiply counted. There are $v-1$ possible choices for each y and each pair will occur in λ blocks together, so there are $\lambda(v-1)$ such pairs. On the other hand, p appears in r blocks and can be paired with $k-1$ other elements in such a block, so $r(k-1)$ also counts such pairs. So we have shown the second equation. □

The convention is to take the three independent variables of a BIBD to be v, k and λ.

DEFINITION 23. An SBIBD, or *symmetric balanced incomplete block design*, is a BIBD such that $b = v$ (and hence $k = r$).

SBIBD's are also called *square* or *projective* BIBD's. The term "symmetric" may be misleading in the matrix context, since the matrix interpretation of BIBD's comes from taking their incidence matrices, and the incidence matrix of an SBIBD will not in general be symmetric.

SBIBD's are typically denoted (v,k,λ)-designs.

DEFINITION 24. A $t-(v,b,r,k,\lambda)-$*design* is a generalization of a (v,b,r,k,λ)-design in which the rule: "each pair of varieties appear in exactly λ blocks" is replaced by the rule, "each t-tuple of varieties appear in exactly λ blocks".

Hence a BIBD may also be denoted a $2-(v,b,r,k,\lambda)$-design.

5.2. Incidence Matrices of Block Designs

Block designs can be expressed as matrices by taking their incidence matrices. A (v,b,r,k,λ) design is identified with a $v \times b$ incidence matrix, $A = (a_{ij})$, of zeros and ones with rows labelled by the varieties and columns by the blocks.

$$a_{ij} = \begin{cases} 1, & \text{variety } x_i \text{ is incident with block } y_j, \\ 0, & \text{variety } x_i \text{ is not incident with block } y_j. \end{cases}$$

Example: The $(7,7,3,3,1)$-design above has incidence matrix:

(172)
$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{array} \begin{array}{c} \begin{array}{ccccccc} y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y_7 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

The incidence matrix of a (v,b,r,k,λ)-design has the property that the number of "1's" per row is r. The number of "1's" per column is k. For any pair of rows, the number of "1's" in the same column is λ.

We can express this in matrix notation:

THEOREM E.2. *If A is the incidence matrix of a (v,b,r,k,λ)-design, then*

$$AJ = rJ, \tag{173}$$

$$JA = kJ, \tag{174}$$

$$AA^T = (r-\lambda)I + \lambda J; \tag{175}$$

where I is the $v \times v$ identity matrix and J is the $v \times v$ matrix of all 1's.

This form (175) is reminiscent of $E^{(1)}$, in the chapter on the M-Method. However in that case we were dealing with $\{\pm 1\}$ matrices and here we have $\{0,1\}$ matrices. It would be interesting to see if there is a connection though.

5.3. A Connection with Hadamard Matrices

The existence of an SBIBD with certain parameters implies the existence of a Hadamard matrix, and vice versa.

THEOREM E.3. *(From* [**Ch**].*) The existence of a* (v, k, λ)*-design with parameters*

$$(4m-1, 2m-1, m-1) \text{ or } (4m-1, 2m, m)$$

is equivalent to the existence of a Hadamard matrix of order $4m$.

We have two (reversible) constructions, taken from [**Ch**], which take Hadamard matrices of order $4m$, and yield SBIBD's of the parameters of Theorem E.3.

Let H be a Hadamard matrix of order $4m$. Normalize the first row and column to be all 1's, then remove them. We are left with an order $4m-1$ matrix, T, say, such that

$$TJ = JT^T = -J \text{ and } TT^T = 4tI - J$$

- Define
$$U = \frac{1}{2}(T + J).$$
Then $UU^T = mI + (m-1)J$ and U is the incidence matrix of a $(4m-1, 2m-1, m-1)$ SBIBD.
- Define
$$V = \frac{1}{2}(J - T).$$
Then V is the incidence matrix of a $(4m-1, 2m, m)$ SBIBD.

APPENDIX F

Designs as Geometry

We segue from applications to soil and wind into pure geometry.

In some sense the most elementary geometries are *incidence geometries*. The study of such geometries consists of the neglect of properties such as angle, length and in-between-ness, in favour of the consideration of *incidence properties* such as "this point lies on this line", or, "this line passes through this point". To reflect the symmetry here, we will write "this point is *incident* with this line", or, "this line is *incident* with this point".

Incidence geometry generalizes not only projective and affine geometry but also the geometries induced on such spaces when some additional structure (eg. a quadratic form) is given. They provide an appropriate framework for studying not only the classical *finite geometries* but also *matroids*, *coding theory* (in the sense of error-correcting codes rather than cryptography) and *designs*.

We note that incidence geometry fits into two algebraic frameworks. One is *linear algebra*, through the notion of division ring or through the use of incidence or adjacency matrices; the other is *group theory*, presenting the study of geometries as that of their automorphism groups.

I will give the barest definitional framework, from which may hopefully be gleaned the strong relation with designs.

DEFINITION 25. An *incidence structure* is a triple $(\mathcal{P}, \mathcal{L}, \mathcal{I})$, consisting of a set $\mathcal{P}$ of *points* (or *varieties*), a set $\mathcal{L}$ of *lines* (or *blocks*), and a relation $\mathcal{I}$ of *incidence* between elements of $\mathcal{P}$ and elements of $\mathcal{L}$.

DEFINITION 26. A *configuration* is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ satisfying the following axioms:

i. Any two distinct points are incident with at most one line.
ii. Any two distinct lines are incident with at most one point.

DEFINITION 27. An *affine plane* is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$, such that $\mathcal{P}$ and $\mathcal{L}$ are non-empty sets, and satisfying the following axioms:

i. Any two distinct points are incident with a unique line.
ii. Given a point P and a line l not incident with P, there is a unique line m incident with P which has no point in common with l.

iii. There exists a *triangle*, i.e. there exists three points which are not incident with the same line.

An affine plane of n^2 points is said to have *order* n. It corresponds to a symmetric $(n^2, n, 1)$ BIBD.

Two lines in an affine plane are said to be *parallel* if they have no point in common, i.e. if they do not *intersect*.

DEFINITION 28. A *projective plane* is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ such that $\mathcal{P}$ and $\mathcal{L}$ are non-empty sets, and satisfying the following axioms:

i. Any two distinct points are incident with a unique line.
ii. Any two distinct lines are incident with a unique point.
iii. There exists a *quadrangle*, i.e. there exists four points of which no three of are incident with the same line.

A projective plane of n^2+n+1 points is said to have *order* n. It corresponds to a symmetric $(n^2+n+1, n+1, 1)$ BIBD.

Affine and projective planes are closely related to each other in that we can always build one from the other by either adding (to go from affine to projective) or deleting, a line. Affine and projective planes of *order* n always exist for $n = p^r$, p prime. It is conjectured that these are the only possible projective planes. See [**Sl2**], [**L**] and [**LTS**].

To move from the language of designs to that of incidence geometries, call varieties *points* and blocks *lines*. If we try this with the incidence matrix (172) of the $(7, 3, 1)$ SBIBD figured in the previous section, and try to draw what we get, we find we have a picture of the smallest possible projective plane, the Fano Plane.

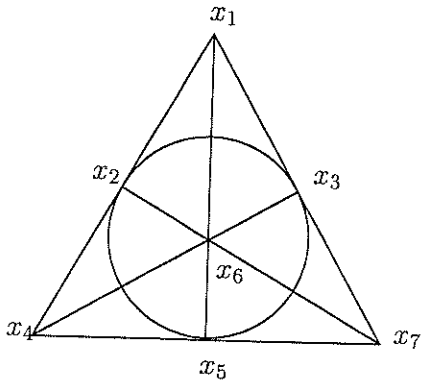


FIGURE 1. The Fano plane

Another notable equivalence between SBIBD's and projective planes is that between the SBIBD with parameters $(111, 11, 1)$ and a Finite Projective Plane of Order 10. The non-existence of both was proven by means of an

exhaustive computer search, the magnitude of which was such to rival the proof of the four-colour theorem. See [**LTS**] for the original article and [**L**] for a general exposition of the problem and the method.

This appendix is a synthesis of material from [**Bi**], [**Pas**] and [**We**].