Journal of Statistical Planning and Inference 8 (1983) 375–388
North-Holland

MINIMAL 2-COVERINGS OF A FINITE AFFINE SPACE BASED ON GF(2) *

Gyula KATONA

Hungarian Academy of Sciences, Budapest, Hungary

Jaya SRIVASTAVA

Colorado State University, Fort Collins, CO, USA

Received 28 December 1982
Recommended by Jeniffer Seberry

Abstract: Let EG$(m,2)$ denote the m-dimensional finite Euclidean space (or geometry) based on GF(2), the finite field with elements 0 and 1. Let T be a set of points in this space, then T is said to form a q-covering (where q is an integer satisfying $1 \leqslant q \leqslant m$) of EG$(m,2)$ if and only if T has a nonempty intersection with *every* $(m-q)$-flat of EG$(m,2)$. This problem first arose in the statistical context of factorial search designs where it is known to have very important and wide ranging applications. Evidently, it is also useful to study this from the purely combinatorial point of view. In this paper, certain fundamental studies have been made for the case when $q=2$. Let N denote the size of the set T. Given N, we study the maximal value of m.

AMS Subject Classification: 05B99, 05B15, 05B20.

Key words: Search design; Factorial design; Zero-one matrices; Coding theory.

1. Introduction

In this paper we shall restrict ourselves to the combinatorial aspects of this development. Researchers interested in the statistical context of the problem may kindly refer to the articles by Srivastava (1975, 1978).

Let L_m denote the set of the first m positive integers $\{1,\dots,m\}$. If $1 \leqslant w \leqslant m$, and $1 \leqslant h_1 < \cdots < h_w \leqslant m$, then $(h_1,\dots,h_w)$ is called a w-subset of L_m. Let $\bar{T}$ be an $(N \times m)$ matrix of zeros and ones. The columns of $\bar{T}$ will be indexed by the elements of L_m and will therefore, be numbered respectively columns $1,\dots,m$. Let L^m describe the class of all the 2^m possible subsets of L_m, including, of course, the empty set (which is denoted by $\emptyset$). Thus, $(h_1,\dots,h_w)$ is a typical member of L^m, where w and the h's are restricted as above. Next, we define an $(N \times 2^m)$ matrix Z, whose columns are indexed by the members of L^m. Without loss of generality, we shall

*This work was supported by the United States National Science Foundation Grant No. MCS77-22985.

assume that the indices of the columns of Z are, respectively,

$$\emptyset, (1), (2), \ldots, (m), (1,2), (1,3), \ldots, (1,m), (2,3), \ldots, (m-1,m),$$
$$(1,2,3), \ldots, (m-2,m-1,m), (1,2,3,4), \ldots, (1,2,\ldots,m).$$

The first column of Z (i.e. the one corresponding to $\emptyset$) has 0 everywhere. The next m columns of Z (i.e. those corresponding to the subsets $(1), \ldots, (m)$ of L_m) are respectively indentical to the corresponding columns of $\bar{T}$. In other words, the $(N \times m)$ submatrix of Z sitting in the m columns of Z after the first column, is $\bar{T}$. The other columns of Z are obtained from the columns of A in $\bar{T}$ as follows. For w, and $h_1, \ldots, h_w$ restricted as before, the column of Z corresponding to the member $(h_1, \ldots, h_w)$ of L^m is the sum (over GF(2)) of the columns of $\bar{T}$ corresponding to the indices $(h_1), \ldots, (h_w)$. For example, if $m \geqslant 4$, the column of Z corresponding to $(1,2,4)$ is the sum of the three columns of $\bar{T}$ corresponding to (1), (2) and (4) respectively.

Let T be obtained from $\bar{T}$ by interchanging 0 and 1. Then for statistical applications, T is a factorial design of the 2^m type, and the N rows of T represent the N treatment combinations to be used in the experiment.

Let A be the $(N \times 2^m)$ matrix with elements 1 and (-1) over the real field, obtained from Z by replacing 0 by 1, and 1 by (-1). Also, let us say that a given matrix M (over any given field F) has the property P_t (with t being a positive integer), if and only if every set of t columns of M is linearly dependent over F. It is well known that certain matrices with property P_t play a central role in the theory of factorial designs, and in coding theory. In the theory of factorial search designs, we are interested in the matrix A having the property P_t over the real field, for various values of t. Since, clearly, A is obtained from T, we wish to characterize the property P_t of A in terms of properties in T which could be checked relatively easily. It turns out that although this characterization problem is easy to explain and understand, it is difficult to solve. On the other hand, from the combinatorial angle, it is elegant, multi-aspected and rich in structure, and hence, its solution is justified in its own right.

In this paper, we study the case $t = 4$. From the point of view of statistical needs, this value of t is much too small. (A value of t of the order of $\frac{1}{2}m^2$, will perhaps be closer to practical needs in many cases.) However, the higher values of t can not be studied without first considering the lower values. Thus, the present series of papers (going up to $t \leqslant 8$) have a basic importance.

For later use, we now present some results which are either essentially obvious, or known (or both).

Definition 1.1. Let $G(g_1 \times g_2)$ and $G_0(g_{10} \times g_{20})$, be two (0, 1)-matrices such that $g_1 \geqslant g_{10}$ and $g_2 \geqslant g_{20}$. Then we say that G_0 is *hidden* in G if there exists a submatrix $G_1(g_{10} \times g_{20})$ of G, such that every row of G_0 is a row of G_1 and vice versa.

Definition 1.2. Let q be a positive integer. We shall denote by B_q the q-dimensional vector space over GF(2), whose elements are column vectors of size $(q \times 1)$. Let G and G_0 be as above with $g_{10} = q$, and $g_{20} = 2^q$. Then we say that B_q is *hidden*

in G if and only if G_0 is hidden in G and G_0 has, in some order, the vectors of B_q as its columns.

Theorem 1.1. *Let t be a positive integer. Then A has the property P_t iff every set of $(t-1)$ columns of Z (whose indices are distinct and do not include $\emptyset$) are linearly independent over the real field.*

Theorem 1.2. (1a) *The matrix A has property P_1.*

(1b) *Each of the following conditions is necessary and sufficient in order for A to have property P_2:* (i) *Only one column of Z has 0 everywhere.* (ii) *Only one column of A has 1 everywhere.* (iii) *All columns of Z are distinct.* (iv) *All columns of A are distinct.* (v) *The rank of $\bar{T}$ over* GF(2) *is m.* (vi) *In every $(N \times q)$ submatrix T^* of T_1 with $1 \leqslant q \leqslant m$, there exists a row with an odd number of zeros.* (vii) *The rows of $\bar{T}$, considered as points of* EG$(m,2)$, *constitute a* 1*-covering of* EG$(m,2)$.

(1c) *If A has property P_2, then A also has P_3.*

(1d) *If t is a positive integer, and a matrix M has property P_{t+1}, then it also has P_t.*

(1e) *Let $\bar{Z}$ be obtained from Z by interchanging* 0 *and* 1. *Then A has property P_t iff $\bar{Z}$ does.*

(1f) *Let G be a* $(0,1)$*-matrix such that the first row of G has* 1 *everywhere.* (i) *Suppose over the real field, G has the property P_{2t} but not P_{2t+1}. Then, over* GF(2), *G does not have property P_{2t}.* (ii) *G has P_{2t+1} over the reals if G has P_{2t} over the real field* ***and also*** *over* GF(2).

Theorem 1.3. *Let A have property P_2. Then each of the following conditions is necessary and sufficient for A to have the property P_4:*

(2a) *The rows of $\bar{T}$, considered as points of* EG$(m,2)$, *taken together, constitute a* 2*-covering of* EG$(m,2)$.

(2b) *The space B_2 is not hidden in Z.*

(2c) *The matrix Z has P_2 over the real field, and furthermore, satisfies one of the following conditions for every pair of nonzero columns:* (i) *The two sets of* 1*-coordinates (in the two columns of Z under consideration) do not contain each other.* (ii) *In the $(N \times 2)$-submatrix of Z, formed by the two columns, the set of the N rows includes the two row vectors* $(0,1)$ *and* $(1,0)$. (iii) *The two sets of* 1*-coordinates (in the two columns of Z under consideration) are not disjoint.* (iv) *In the $(N \times 2)$ submatrix of Z formed by the two columns, the set of N rows includes the row vector* $(1,1)$. (v) *In the $(N \times 2)$ submatrix of Z formed by the two columns, the set of the N rows includes the three row vectors* $(0,1)$, $(1,0)$ *and* $(1,1)$.

Proof (sketch only). (2a) This is established in Srivastava (1975, 1978).

(2b) If B_2 is hidden in Z, then there are four columns of Z which after rearrangement, constitute an $(N \times 4)$ matrix Z, in which the submatrix

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

is hidden. But the last three columns of Z_1 are obviously dependent. Hence, by Theorem 1.1, A does not have P_4. On the other hand, if A has P_4, then by (2a), $\bar{T}$ constitutes a 2-covering of EG$(m, 2)$. This in turn implies that B_2 is not hidden in Z.

(2c) (i) and (iii) follow directly from (2b). Also, (ii) is a restatement of (i), and (iv) of (iii). Finally, (v) follows from (i) and (iii). This completes the proof.

2. Designs for increasing m

In this section, we consider the question of obtaining designs with a higher value of m from those with a lower value of m.

Definition 2.1. A (0, 1) matrix $T(N \times m)$ is said to be a (*pure*) *search design of order* q for m factors, if the corresponding matrix A $(N \times 2^m)$ has property P_{2q}.

Suppose we are given a design $T(N \times m)$ of order 2. Below we give some results on obtaining a design T for $(m+1)$ factors and of order 2, using T.

Throughout this and related papers, we shall use the following notation. The symbol I_q will denote the $(q \times q)$ identity matrix, J_{pq} a $(p \times q)$ matrix with 1 everywhere, and 0_{pq} a $(p \times q)$ matrix with 0 everywhere. We shall write $J_{p1} = J_p = J$ and $0_{p1} = \mathbf{0}_p = \mathbf{0}$, if the value of p is clear from the context. If G_1 and G_2 are two matrices (or vectors) of the same size, then $G_1 \odot G_2$ will denote the Schur product of G_1 and G_2, so that $G_1 \odot G_2$ is of the same size as G_1 or G_2 and is obtained by multiplying the corresponding elements of G_1 and G_2. For two designs $T_1(N_1 \times m)$ and $T_2(N_2 \times m)$, the symbols

$$\begin{pmatrix} T_1 \\ T_2 \end{pmatrix} \quad \text{and} \quad T_1 + T_2$$

will both denote the designs with $(N_1 + N_2)$ treatments obtained by taking T_1 and T_2 together. Prime ($'$) will denote transpose (of a matrix) as usual.

Theorem 2.1. *Let* $\bar{T}_1(N_1 \times m)$ *and* $\bar{T}_2(N_2 \times m)$ *be two* (0, 1)*-matrices with* $\bar{T}_1' = [\mathbf{0}_m, I_m]$ *so that* $N_1 = 1 + m$. *Let* $\bar{T} = \bar{T}_1 + \bar{T}_2$. *Then a necessary and sufficient condition that* $\bar{T}$ *is a* 2*-covering of* EG$(m, 2)$ (*i.e. T is a search design of order* 2) *is that for every pair of nonzero* (0, 1)*-vectors* α *and* β *of size* $(m \times 1)$ *such that* $\alpha \odot \beta = \mathbf{0}_m$, *there exists a row* x *in* $\bar{T}_2$ *such that* $\alpha' x = \beta' x = 1$. (*Of course,* x *may depend upon the chosen values of* α *and* β.)

Proof. (a) *Sufficiency.* Let α_1, β_1 be a pair of distinct nonzero (0, 1)-vectors of size $(m \times 1)$. Let

$$\gamma_2 = \alpha_1 \odot \beta_1, \qquad \alpha_2 = \alpha_1 + \gamma_2, \qquad \beta_2 = \beta_1 + \gamma_2.$$

Then $\alpha_2 \odot \gamma_2 = \beta_2 \odot \gamma_2 = \alpha_2 \odot \beta_2 = \mathbf{0}_m$. Let $C_1, C_2 \in \mathrm{GF}(2)$. We must show that there is a row y in $\bar{T}$ such that $\alpha_1' y = C_1$, $\beta_1' y = C_2$. Four cases arise:

(i) $C_1 = C_2 = 0$. For this case, we can take $y = \mathbf{0}_m$, which is in $\bar{T}_1$.

(ii) $C_1 = 1$, $C_2 = 0$. *Two subcases arise:* $\alpha_2 = \mathbf{0}$ and $\alpha_2 \neq \mathbf{0}$. If $\alpha_2 \neq 0$, take a row y in I_m (which is in $\bar{T}_1$) such that $\alpha_2' y = 1$. Then clearly $\gamma_2' y = 0$, $\beta_2' y = 0$. Hence

$$\alpha_1' y = \alpha_2' y + \gamma_2' y = 1 \quad \text{and} \quad \beta_1' y = \beta_2' y + \gamma_2' y = 0.$$

Hence

$$\alpha_1' y = \alpha_2' y + \gamma_2' y = 1 \quad \text{and} \quad \beta_1' y = \beta_2' y + \gamma_2' y = 0.$$

If $\alpha_2 = \mathbf{0}$, then $\gamma_2 \neq \mathbf{0}$ since otherwise α would be $\mathbf{0}$. Similarly, $\beta_2 \neq 0$ since otherwise $\alpha_1 = \beta_1$. From the conditions of the theorem, there exists a row y in $\bar{T}_2$ such that $\beta_2' y = \gamma_2' y = 1$. But this gives $\alpha_1' y = 1$, $\beta_1' y = 0$.

(iii) $C_1 = 0$, $C_2 = 1$. Proof is similar to (ii).

(iv) $C_1 = C_2 = 1$. If $\gamma_2' \neq 0$, choose a row y in I_m such that $\gamma_2' y = 1$. This clearly does the job. If $\gamma_2 = 0$, then the conditions of the theorem ensure the existence of a $y \in T_2$, such that $\alpha_2' y = \beta_2' y = 1$, so that $\alpha_1' y = \beta_1' y = 1$.

(b) *Necessity.* Take α_1 and β_1 to be such that $\alpha_1 \odot \beta_1 = \gamma_2 = \mathbf{0}$. Clearly, there is no row $y \in \bar{T}_1$ which would give $\alpha_1' y = \beta_1' y = 1$. Now, suppose there is also no row $y \in \bar{T}_2$ such that $\alpha_1' y = \beta_1' y = 1$. Then clearly, $\bar{T}$ does not cover the $(m-2)$-flat whose equation is $\alpha_1' x = \beta_1' x = 1$. This completes the proof.

Theorem 2.2. (a) *Let q be a nonnegative integer and let $\bar{T}$ be a q-covering of* EG$(m,2)$. *Choose a particular column of $\bar{T}$ and interchange* 0 *and* 1 *in this column and let $\bar{T}^*$ be the matrix so obtained. Then $\bar{T}^*$ is also a q-covering of* EG$(m,2)$.

(b) *Let $\bar{T}$ be as in* (a). *By interchanging* 0 *and* 1 *in selected columns of $\bar{T}$, we can obtain a matrix $\bar{T}$ which has at least one row equal to $\mathbf{0}_m'$, and whose rows constitute (together) a q-covering of* EG$(m,2)$.

(c) *Let $\bar{T}$ be as in* (a), *let $G(m \times m)$ be a nonsingular matrix over* GF(2), *and let $\bar{T}_{01} = \bar{T}G$. Then $\bar{T}_{01}$ is a q-covering of* EG$(m,2)$.

(d) *Let $q \geqslant 1$. By using transformations as in* (b) *and* (c), *we can reduce $\bar{T}$ to a matrix $\bar{T}_{00}$ of the same size such that $\bar{T}_{00}$ contains $\bar{T}_1$ of Theorem* 2.1 *as a submatrix, and such that $\bar{T}_{00}$ constitutes a q-covering of* EG$(m,2)$.

Proof. (a) Without loss of generality, choose the first column of $\bar{T}$. For $q = 0$, the result is obvious. For $q \geqslant 1$ we proceed as follows. Take any $6m - q$)-flat and let its equation be

$$\sigma_{i1} x_1 + \cdots + \sigma_{im} x_m = C_i \quad (i = 1, \ldots, q).$$

As the C_i are varied, we obtain a parallel pencil of 2^q flats, all of which are (by assumption) covered by $\bar{T}$. If we interchange 0 and 1 in the first column of $\bar{T}$, then a typical row $(x_1^*, \ldots, x_m^*)$ of $\bar{T}$ will be changed to $(1 + x_1^*, \ldots, x_m^*)$. If $(x_1^*, \ldots, x_m^*)$ satisfies

$$\sigma_{i1} x_1 + \cdots + \sigma_{im} x_m = C_i,$$

then $(1+x_1^*,\ldots,x_m^*)$ satisfies the same equation but with C_i replaced by $C_i+\sigma_{i1}$. However, just as the vector $(C_1,\ldots,C_q)$ takes all the possible 2^q values as the C's are varied, so does $(C_1+\sigma_q,\ldots,C_q+\sigma_{q1})$. Hence, the pencil is still covered.

(b) This is obvious in view of (a).

(c) This follows since clearly, $\bar{T}$ and $\bar{T}G$ generate the same matrix Z.

(d) This follows from (b), (c) and Theorem 1.2 (condition 1b(v)).

Remark 2.1. In view of the above, it is clear that a 2-covering $\bar{T}^*$ is 'equivalent' to a covering $\bar{T}=\bar{T}_1+\bar{T}_2$, where $\bar{T}_1$ and $\bar{T}_2$ are as in Theorem 2.1. Thus, there is no loss of generality in restricting attention to the coverings of this type (i.e., $\bar{T}_1+\bar{T}_2$).

3. Bounds on m, given N

We first ask the question: given N, what is the maximum value that m can have so that T is a search design of order 2, i.e., A has property P_4. The development below could be made using the well known Sperner theorem, and related results, and also in terms of (0, 1)-matrices. For clarity of discussion, we follow the latter route in this first paper. Throughout this paper, for any matrix M, the symbol $w(M)$ will denote the number of nonzero elements in M. Also, M_c will denote the set of columns of M. Furthermore, if M_1 and M_2 are two matrices of the *same* size, then we shall say that M_2 is contained in M_1 (and M_1 contains M_2) if, and only if, $M_2=M_1\odot M_2$. Notice that if M_1 and M_2 are (0, 1)-matrices, then M_1 contains M_2 if, and only if, the set of nonzero cells of M_1 contains the set of nonzero cells of M_2.

Lemma 3.1. *Let T be of order 2. Consider Z. Suppose there is a $z\in Z_c$ such that $w(z)=\mu$, a nonnegative integer. Then*

(i) *the vectors $z^*\odot z$, when z^* varies over Z_c, are all distinct, and* (3.1)

(ii) $m\leqslant\mu$.

Also, equality can occur in (ii) *only if the set $\{z\odot z^* \mid z^*\in Z_c\}$ is the set of the 2^μ vectors (over* GF(2)*) contained in z.*

Proof. Suppose $z_1,z_2\in Z_c$, and $z_1\odot z=z_2\odot z$. Then $(z_1+z_2)\odot z=\mathbf{0}_m$. By Theorem 3 (Part 2c(i)), it follows that $(z_1+z_2)=\mathbf{0}$, or $z_2=z_2$. This proves (i). Also, clearly the set $\{z\odot z^* \mid z^*\in Z_c\}$ has 2^m elements, each $z^*\odot z$ is contained in z, and the number of distinct (0, 1)-vectors contained in z is 2^μ. Hence, $2^m\leqslant 2^\mu$, leading to (ii). The remaining statement of Lemma 3.1 is now obvious. This completes the proof.

We now derive another similar bound on m using $(z+J)$. Let z_1 and z_2 be $(m\times 1)$ vectors over GF(2) such that

$$z_1\odot(z+J)=z_2\odot(z+J). \tag{3.2}$$

Then we have $(z_1+z_2)\odot(z+J)=\mathbf{0}$, so that $(z_1+z_2)\odot z=(z_1+z_2)$. Hence, if z_1 and z_2 are distinct, we must have

$$z_1+z_2=z, \tag{3.3a}$$

$$(z_1\odot z)+(z_2\odot z)=z, \tag{3.3b}$$

$$(z_1\odot z)\odot(z_2\odot z)=\mathbf{0}. \tag{3.3c}$$

Notice that (3.3a,b) imply (3.2) and recall that Z_c is a vector space. Thus, if $z_1\in Z_c$, there is exactly one $z_2\in Z_c$ (with $z_2\neq z_1$) such that (3.2) holds. Hence, the 2^m columns of Z get divided into 2^{m-1} pairs, such that each of the two columns within a pair give the same Schur Product ($\odot$) when multiplied with $(z+J)$. Also, every such Schur Product is contained in $(z+J)$, and the number of distinct (0, 1)-vectors contained in $(z+J)$ is $2^{N-\mu}$. Hence, $2^{m-1}\leqslant 2^{N-\mu}$. We have proved

Lemma 3.2. *Suppose Z and z are as in Lemma* 3.1. *Then*

(i) $$m\leqslant N-\mu+1; \tag{3.4}$$

(ii) *equality holds in* (i) *only if for each vector z^* contained in $(z+J)$ there are exactly two columns z_1^* and z_2^* in Z, such that*

$$z^*=z_1^*\odot(z+J)=z_2^*\odot(z+J). \tag{3.5}$$

Next, we establish some connections with coding theory. Let

$$\psi_2(N,d) = \text{maximum number of (binary) code words of length } N \text{ such that the distance between a pair of distinct code words is at least } d, \tag{3.6}$$

$$\psi_2(N,d) = \text{maximum number of (binary) code words of length } N \text{ such that the distance between a pair of distinct code words is at least } d \text{ and at most } (N-d+1), \text{ and such that the set of code words is closed under additions over GF(2).} \tag{3.7}$$

Theorem 3.1. *Let $T(N\times m)$ be a search design of order* 2. *Then*

$$m\geqslant \max_d \min\,(d, N-d+1, \log_2\psi_2(N,d)). \tag{3.8}$$

Proof. Let d be defined by

$$d=\min_{y\neq\mathbf{0},\,y\in Z_c}(\min\,(w(y), N-w(y)+1)) \tag{3.9}$$

Then,

$$m\leqslant \min\,(d, N-d+1) \tag{3.10}$$

follows from Lemmas 3.1 and 3.2. Now, since Z is a vector space, it is clear that

any two different members of Z_c have a difference whose weight is between d and $(N-d+1)$. Hence, if the elements of Z_c are considered as code words, the distance between any distinct pair of them is between d and $(N-d+1)$. Since Z_c has 2^m elements, we therefore have

$$m \leqslant \log_2 \psi_2(N,d). \tag{3.11}$$

Since d depends upon Z and hence on T, combining (3.10) and (3.11), the inequality (3.8) is obtained.

Define

$$\lfloor \delta \rfloor = \text{largest integer less than or equal to (the real number) } \delta, \tag{3.12}$$

$$\lceil \delta \rceil = \text{smallest integer greater than or equal to (the real number) } \delta, \tag{3.13}$$

$$m(N,t) = \text{the maximum value of } N \text{ such that there exists a } (1,-1)\text{-matrix } A(N\times 2^m), \text{ defined as earlier, which has the property } P_t \text{ over the real field.} \tag{3.14}$$

Theorem 3.2. *We have*

$$\overline{\lim_{N\to\infty}} \frac{1}{N} m(N,4) \leqslant 0.2835. \tag{3.15}$$

Proof. Define for a real number δ, such that $(0 \leqslant \delta \leqslant \frac{1}{2})$, the quantity

$$\psi(\delta) = \overline{\lim_{N\to\infty}} \frac{1}{N} \log_2 \psi_1(N, \lfloor \delta N \rfloor). \tag{3.16}$$

Let $\phi(\delta)$ be a decreasing function which satisfies the condition

$$\psi(\delta) \leqslant \phi(\delta), \quad 0 \leqslant \delta \leqslant \tfrac{1}{2}. \tag{3.17}$$

Notice that $\psi(0) = 1 \leqslant \phi(0)$. Let ε be the (unique) solution to the equation

$$\varepsilon = \phi(\varepsilon). \tag{3.18}$$

We shall prove that

$$\overline{\lim_{N\to\infty}} \frac{1}{N} m(N,4) \leqslant \varepsilon. \tag{3.19}$$

From (3.6)–(3.8) we obtain

$$m(N,4) \leqslant \max_d \min\,(d, \log_2 \psi_1(N,d)), \tag{3.20}$$

and

$$\overline{\lim_{N\to\infty}} \frac{1}{N} m(N,4) \leqslant \lim_{N\to\infty} \max_d \min \left(\frac{d}{N}, \frac{1}{N} \log_2 \psi_1(N,d) \right)$$

$$\leqslant \overline{\lim_{N\to\infty}} \sup_\delta \min \left(\delta, \frac{1}{N} \log_2 \psi_1(N, \lfloor \delta N \rfloor) \right), \tag{3.21}$$

where throughout the supremum is taken over all values of δ satisfying $0 \leqslant \delta \leqslant \frac{1}{2}$. If the last expression is $\leqslant \varepsilon$, we are done. Suppose on the contrary that

$$\overline{\lim_{N\to\infty}} \sup_{\delta} \min\left(\delta, \frac{1}{N}\log_2 \psi_1(N, \lfloor \delta N \rfloor)\right) = \varepsilon^* > \varepsilon. \tag{3.22}$$

This implies that

$$\sup_{\delta} \min\left(\delta, \frac{1}{N}\log_2 \psi_1(N, \lfloor \delta N \rfloor)\right) > \tfrac{1}{4}(\varepsilon + 3\varepsilon^*), \tag{3.23}$$

for infinitely many N. In other words, there are an infinite number of values of N for each of which there exists a δ (possibly depending on N) such that

$$\min\left(\delta, \frac{1}{N}\log_2 \psi_1(N, \lfloor \delta N \rfloor)\right) > \tfrac{1}{2}(\varepsilon + \varepsilon^*). \tag{3.24}$$

But (3.24) give

$$\delta > \tfrac{1}{2}(\varepsilon + \varepsilon^*) \quad \text{and} \quad \frac{1}{N}\log_2 \psi_1(N, \lfloor \delta N \rfloor) > \tfrac{1}{2}(\varepsilon + \varepsilon^*).$$

Since $\psi_1(N, d)$ is a decreasing function of d, the inequality

$$\frac{1}{N}\log_2 \psi_1(N, \lfloor \tfrac{1}{2}(\varepsilon + \varepsilon^*)N \rfloor) > \tfrac{1}{2}(\varepsilon + \varepsilon^*)$$

follows immediately for infinitely many N. This, with (3.16), implies

$$\psi(\tfrac{1}{2}(\varepsilon + \varepsilon^*)) \geqslant \tfrac{1}{2}(\varepsilon + \varepsilon^*).$$

Hence, since $\psi(\delta)$ is also a decreasing function, we obtain

$$\psi(\varepsilon) \geqslant \tfrac{1}{2}(\varepsilon + \varepsilon^*) > \varepsilon_1$$

contradicting (3.17) and (3.18). Thus (3.22) cannot hold and (3.19) is proved. On the other hand, McEliece, Rodemich, Rumsey and Welch (1977) showed that (3.17) holds with

$$\phi(\delta) = H(\tfrac{1}{2} - \sqrt{\delta(1-\delta)}), \tag{3.25}$$

where H is the entropy defined by

$$H(\delta) = -\delta \log \delta - (1-\delta)\log(1-\delta). \tag{3.26}$$

Since the solution of

$$\delta = H(\tfrac{1}{2} - \sqrt{\delta(1-\delta)}), \tag{3.27}$$

is approximately $\delta = 0.2834\ldots$, the theorem is proved.

The above result gives an upper bound for $m(N, 4)$. Helgert and Stineff (1977) have collected the values of $B(n, d)$ for small values of N and d. Using their tables,

we computed the upper bounds given below on $m(N,4)$ for small values of N using Theorem 3.1:

$$\begin{array}{lcccccccccccc} N = & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ m(N,4) \leqslant & 2 & 2 & 2 & 3 & 3 & 3 & 4 & 4 & 4 & 4 & 5 & 5 \end{array} \tag{3.28}$$

Theorem 3.3. *Suppose every nonzero column of* $Z(N \times 2^m)$ *is of weight* $(\frac{1}{2}N)$. *Then for some integer* $\pi > 0$, *we have*

$$N = \pi 2^m. \tag{3.29}$$

Proof. Let z_1 and z_2 be two unequal columns of Z. Clearly, the weight $w(\lambda_1 z_1 + \lambda_2 z_2) = \frac{1}{2}N$, unless $\lambda_1 = \lambda_2 = 0$. Hence, it is easy to see that $w((z_1 + \lambda_1 \boldsymbol{J}) \odot (z_2 + \lambda_2 \boldsymbol{J})) = \frac{1}{4}N$, for all $\lambda_1, \lambda_2 \in \mathrm{GF}(2)$. If $\boldsymbol{a}_1, \boldsymbol{a}_2$ are the two columns of A corresponding to z_1 and z_2 in Z, then the above shows us that (over the real field) $\boldsymbol{a}_1' \boldsymbol{a}_2 = 0$. Hence, the columns of A are pairwise orthogonal and hence, independent over the real field. Thus $N \geqslant 2^m$. If $N = 2^m$, then A is clearly the Hadamard matrix of size $2^m \times 2^m$. If $N > 2^m$, then it is easy to show that A must consist of a few (say π) such matrices put together. This completes the proof.

4. Value of $m(N,4)$ for small n

We shall use Theorems 2.1 and 2.2 extensively. For a given N, $m(N,4)$ is the largest value of m such that there exists a search design $T(N \times m)$ or order 4. Similarly, let $N(m, 2q)$ be the minimum value of N, given m, such that there exists a search design of order q. Investigations on $m(N,4)$ and $N(m,4)$ are essentially equivalent.

For $m = 2$, Theorem 2.1 immediately gives $N_2 = 1$ and $\bar{T}_2 = (1,1)$, so that $N(2,4) = 4$.

For $m = 3$, clearly $N_2 > 1$. Also

$$\bar{T}_2 = \bar{T}_{20} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

does the job. Hence $6 \leqslant N(3,4) \leqslant 7$. Now

$$\bar{T}_{21} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

cannot do the job of $\bar{T}_2$ since the case $\alpha' = (1\ 0\ 0)$, $\beta' = (0\ 1\ 0)$ is not covered. Similarly,

$$\bar{T}_{22} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

will not work since $\alpha' = (1\ 0\ 0)$, $\beta' = (0\ 1\ 1)$ is left out. Thus, because of symmetry, it is clear that $N_2 > 2$. Hence $N(3,4) = 7$. Also, notice that a 3-rowed matrix whose one row is (1 1 1) and the other two rows are identical with any two rows of $\bar{T}_{20}$ will *not* work. For example,

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

does not work since the case $\alpha' = (0\ 1\ 0)$, $\beta' = (1\ 0\ 1)$ is left out. We have proved:

Theorem 4.1. *We have*

$$m(6,4) = 2, \qquad m(7,4) = 3. \tag{4.1}$$

Also, there is a unique (7×3) *matrix* $\bar{T}$ *(apart from a permutation of rows) and a unique* (7×8) *matrix* Z *(apart from a permutation of rows and columns) serving the case* $N = 7$, $m = 3$.

Consider the case $m = 4$. We show that $N(4,4) > 9$. Notice that like (4.1), follows from (3.28). However, a direct argument is instructive. It is $\bar{T}_1$ is (5×4). Consider a matrix $\bar{T}_{23}(4 \times 4)$ as a candidate for $\bar{T}_2$. Now, the weight of each column of $\bar{T}_1$ is 1. Also, Lemma 3.1 tells us that the weight of each column of Z (and hence of $\bar{T}$) must not be less than 4. Hence, the weight of each column of $\bar{T}_{23}$ must be at least 3. On the other hand, the rows of $\bar{T}_{23}$ must be such that we are able to cover each of the three cases

$$(\alpha' = (1\ 1\ 0\ 0),\ \beta' = (0\ 0\ 1\ 1)), \qquad (\alpha' = (1\ 0\ 1\ 0),\ \beta' = (0\ 1\ 0\ 1)),$$
$$(\alpha' = (1\ 0\ 0\ 1),\ \beta' = (0\ 1\ 1\ 0)).$$

It is easy to check that this implies that at least two rows of $\bar{T}_{23}$ must be distinct, and must be of weight 2, and must not add to (1 1 1 1). Now, assume for a moment that $\bar{T}_{23}$ has the rows (1 1 0 0) and (1 0 1 0); then the weight of the last column of $\bar{T}_{23}$ cannot exceed 2. This contradicts the earlier requirement that the weight of each column of $\bar{T}_{23}$ be at least 3. Similar is the situation with any other pair of vectors of weight 2 being the rows of $\bar{T}_{23}$. Hence $N(4,4) > 9$.

Next, we show that $N(4,4) = 10$. Let $\bar{T}_{24}(5 \times 4)$ be the candidate for $\bar{T}_2$. We shall determine the structure of $\bar{T}_{24}$ up to a permutation of rows and/or columns. From the preceeding argument, we can assume, without loss of generality, that the first and second rows of $\bar{T}_{24}$ are (1 1 0 0) and (0 1 1 0). Let $\bar{T}_{241}$ be the (3×4) matrix formed by the last three rows of $\bar{T}_{24}$. Now, the weight of any linear combination of columns of $\bar{T}$ must be at least 4. Hence, the weight of each column of $\bar{T}_{24}$ must be at least 3. This, in turn, implies that the 4th column of $\bar{T}_{241}$ is $(1\ 1\ 1)'$. Similarly, it is obvious that the sum of any two columns of $\bar{T}_{24}$ must be of weight at least 2. Hence, without loss of generality, the 3rd column of $\bar{T}_{241}$ is $(0\ 1\ 1)'$, and the first

column is either $(0\ 1\ 1)'$ or $(1\ 0\ 1)'$. Since $\bar{T}_{24}$ must cover the case $\alpha' = (0\ 0\ 1\ 0)$ and $\beta' = (1\ 0\ 0\ 1)$, we find that the first column of $\bar{T}_{241}$ is $(1\ 0\ 1)'$.

Let $r'(3 \times 1)$ be the second column of $\bar{T}_{241}$. Clearly, $r' \neq (0\ 0\ 0)'$. Also, the three cases when $\beta' = (1\ 1\ 0\ 0)$, $(0\ 1\ 1\ 0)$ and $(1\ 1\ 1\ 0)$ (α' being $(0\ 0\ 0\ 1)$ in each case) respectively knock out the values $(1\ 0\ 1)'$, $(0\ 1\ 1)'$ and $(1\ 1\ 0)'$ for r'. It is easily checked that the remaining four values of r' are permissible. Of these, the two values $(1\ 0\ 0)'$ and $(0\ 1\ 0)'$ lead to two values of $\bar{T}_2$ which are equivalent under permutation (or rows and/or columns). We have proved:

Theorem 4.2. *We have*

$$m(8,4) = m(9,4) = 3, \qquad m(10,4) = 4. \tag{4.2}$$

Also, there are three nonisomorphic (under permutations of rows and/or columns) solutions for $\bar{T}$; the corresponding (nonunique) matrices $\bar{T}_2$ being

$$\bar{T}_2 = \begin{bmatrix} 1&1&0&0 \\ 0&1&1&0 \\ 1&1&0&1 \\ 0&0&1&1 \\ 1&0&1&1 \end{bmatrix}, \begin{bmatrix} 1&1&0&0 \\ 0&1&1&0 \\ 1&1&0&1 \\ 0&1&1&1 \\ 1&1&1&1 \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} 1&1&0&0 \\ 0&1&1&0 \\ 1&0&0&1 \\ 0&0&1&1 \\ 1&1&1&1 \end{bmatrix}. \tag{4.3}$$

Next we consider $m = 5$. From (3.28), we obtain $N(5,4) \geqslant 14$. We prove that $N(5,4) = 14$ and obtain a $\bar{T}_2(8 \times 5)$ serving this case. However, we first note the following result which helps in obtaining a $\bar{T}_2$ for $(m+1)$ factors in case we are given a $\bar{T}_2$ for m factors.

Theorem 4.3. *Let $\bar{T}_{2,m}$ be an $(N_2 \times m)$ matrix such that $\bar{T}_2 = \bar{T}_{2,m}$ satisfies the conditions for $\bar{T}_2$ in Theorem* 2.1. *Also, let $K(m \times m)$ be a nonsingular matrix over* GF(2). *Let*

$$\bar{T}_{2,m+1} = \left[\begin{array}{c|c} \bar{T}_{2,m} & \mathbf{0}_{N_2} \\ \hline K & J_m \end{array}\right]. \tag{4.4}$$

Then $\bar{T}_2 = \bar{T}_{2,m+1}$ satisfies the condition for $\bar{T}_2$ in Theorem 2.1, *corresponding to $(m+1)$ factors.*

Proof. We use the notation of Theorem 2.1, but with $(m+1)$ factors. Consider α' and β'. Notice that both of them cannot have 1 in the $(m+1)$th position since otherwise $\alpha \odot \beta \neq \mathbf{0}$. Now, if both α and β have 0 in the $(m+1)$th position, then such a case is already covered by the structure of $\bar{T}_{2,m}$. The same is true if one of α and β (say, α) has 1 in the $(m+1)$th position, provided $w(\alpha) > 1$. We are left with the case when $w(\alpha) = 1$, so that $\alpha' = (0\ 0 \cdots 0\ 1)$. However, this case is also covered in view of Theorem 1.2 (1b(v),(vi)). This completes the proof.

Definition 4.1. Let $T_0(N_0 \times m)$ be a pure search design of order q for m factors. If there exists a row in T_0, such that the design $\bar{T}_0((N-1)\times m)$ obtained from T_0 by deleting this row is also of order q, then T_0 is said to be *unsaturated*. Otherwise, T_0 is called *saturated*. Also, T_0 is said to be *minimal* if and only if $N_0 = N(m, 2q)$. Clearly, 'minimal' implies 'saturated', but 'saturated' does not necessarily imply 'minimal'.

Notice that the designs $\bar{T}_{2,m+1}$ of (4.4) are not necessarily minimal or even saturated. However, K is at our disposal and can have one out of a rather large number of values. It is, therefore, sometimes possible to choose K in such a way that $\bar{T}_{2,m+1}$ is unsaturated so that some of its rows can be deleted, and the size of the design be reduced. This will be studied in later communications. Here, we illustrate the above by obtaining a design $\bar{T}(14\times 5)$ of order 2.

For the $\bar{T}_{2,4}$ of (4.4) (with $m=4$), we take the first matrix on the right hand side of (4.3). Notice that the rows 1, 3, 4 and 5 of this last matrix cover all cases of values of α and β except two cases, namely

$$(\alpha' = (1\ 1\ 0\ 0),\ \beta' = (0\ 0\ 1\ 1)) \quad \text{and} \quad (\alpha' = (0\ 1\ 0\ 0),\ \beta' = (0\ 0\ 1\ 0)),$$

which are covered by row no. 2. If we wish to cover these cases (for $m=5$) using a $\bar{T}_{2,5}$ as at (4.4), we need to choose K so as to cover, if possible, four values of α and β, namely

$$(\alpha' = (1\ 1\ 0\ 0\ 1),\ \beta' = (0\ 0\ 1\ 1\ 0)), \quad (\alpha' = (1\ 1\ 0\ 0\ 0),\ \beta' = (0\ 0\ 1\ 1\ 1)),$$
$$(\alpha' = (0\ 1\ 0\ 0\ 1),\ \beta' = (0\ 0\ 1\ 0\ 0)) \quad \text{and} \quad (\alpha' = (0\ 1\ 0\ 0\ 0),\ \beta' = (0\ 0\ 1\ 0\ 1)),$$

which are arrived at in an obvious manner from the two values of (α, β) mentioned in the previous sentence. It is easy to check that

$$K = \begin{bmatrix} 0\ 0\ 1\ 0 \\ 0\ 1\ 0\ 0 \\ 1\ 0\ 1\ 0 \\ 0\ 1\ 1\ 1 \end{bmatrix} \tag{4.5}$$

satisfies this requirement. Thus, a minimal design of order 2 with $m=5$ is given by the following 14 points:

$$\bar{T}' = \left[\begin{array}{c|ccccc|cccc|cccc} 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]. \tag{4.6}$$

That this design is not unique, is exemplified by the existence of the following non-

isomorphic minimal design:

$$\bar{T}' = \left[\begin{array}{c|ccccc|ccccccc} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{array}\right]. \tag{4.7}$$

References

Helgert, H.J. and R.D. Stineff (1977). Minimum distance bounds for binary linear codes. *IEEE Trans. Inf. Theory* 19.

McEliece, R.J., E.R. Rodemich, H.C. Rumsey, Jr. and L.R. Welch (1977). New upper bounds on the rate of a code, via the Delsarte-McWilliams inequalities. *IEEE Trans. Inf. Theory* 23.

Srivastava, J.N. (1975). Designs for searching nonnegligible effects. In: *A Survey of Statistical Design and Linear Models.* North-Holland, Amsterdam, 507–519.

Srivastava, J.N. (1978). On the Linear Independence of Sets of 2^q Columns of Certain $(1, -1)$ matrices with a group structure and its connection with finite geometries. In: D.A. Holton and J. Seberry, Eds., *Combinatorial Mathematics.* Springer, Berlin and Australian Academy of Science.