BULL. AUSTRAL. MATH. SOC. 05B20
VOL. 10 (1974), 15-21. (05B99), (12C20)

A note on Hadamard arrays

Joan Cooper

Let $v = mk + 1$ be a prime power; we show for m even it is not possible to partition the Galois field $GF(v)$ to give four $(0, 1, -1)$ matrices X_1, X_2, X_3, X_4 satisfying:

(i) $X_i * X_j = 0$, $i \neq j$, $i, j = 1, 2, 3, 4$;

(ii) $\sum_{i=1}^{4} X_i$ is a $(1, -1)$ matrix;

(iii) $\sum_{i=1}^{4} X_i X_i^T = vI_v$.

Thus this method of partitioning the Galois field $GF(v)$, into four matrices satisfying the above conditions, cannot be used to find Baumert-Hall Hadamard arrays $BH[4v]$ for $v = 9, 11, 17, 23, 27, 29, \ldots$.

Terminology and definitions

A $4n \times 4n$ Hadamard array, H , is a square matrix of order $4n$ with elements $\pm A, \pm B, \pm C, \pm D$ each repeated n times in each row and column. Assuming the indeterminants A, B, C, D commute, the row vectors of H must be orthogonal.

The Hadamard product, $*$, of two matrices $A = (a_{ij})$ and $B = (b_{ij})$ which are the same size is given by

$$A * B = (a_{ij}b_{ij}) .$$

The identity matrix will be represented as I and the $v \times v$ matrix

Received 1 August 1973. Communicated by Jennifer R.S. Wallis.

https://doi.org/10.1017/S0004972700040570 Published online by Cambridge University Press

of all 1's will be J .

The symbol & represents the result from adjoining two sets with repetition remaining; that is,

$$\{x_1, \ldots, x_s\} \ \& \ \{y_1, \ldots, y_t\} = [x_1, \ldots, x_s, y_1, \ldots, y_t] .$$

Where repetition occurs the elements resulting from such an adjunction will be called a collection and denoted by square brackets [ ] .

A binary composition $\wedge$ of two sets will be defined as

$$\begin{aligned} A_1 \wedge A_2 &= [x_1, \ldots, x_s] \wedge [y_1, \ldots, y_t] \\ &= [x_1+A_2, \ldots, x_s+A_2] . \end{aligned}$$

Let $v = mk + 1 = p^\alpha$ (a prime power). Let x be a primitive element of $F = \mathrm{GF}(v)$ and write $G = \{z_1, \ldots, z_{v-1}\}$ for the multiplicative cyclic group of order $v - 1$ generated by x .

Choose the cosets C_i of G by

$$C_i = \{x^{kj+i} : 0 \le j \le m-1\} \quad 0 \le i \le k-1 ,$$

where the order of C_i is m and its index k .

Now let $D_i = (d_{jl})$ be the incidence matrix of the coset C_i . $D_i = (d_{jl})$ is defined as

$$d_{jl} = \begin{cases} 1 & \text{if } z_l - z_j \in C_i , \\ 0 & \text{otherwise.} \end{cases}$$

We will denote D_i by $[C_i]$.

As $G = C_0 \cup C_1 \cup \ldots \cup C_{k-1} = F \backslash \{0\}$, its incidence matrix is $J - I$ and the incidence matrix of F is J .

Therefore the incidence matrix of $\{0\}$ will be I .

$X = \left[\mathop{\&}\limits_{s=0}^{k-1} b_s C_s \right]$ will mean the matrix X which is a summation of the incidence matrices of the cosets. That is

https://doi.org/10.1017/S0004972700040570 Published online by Cambridge University Press

(1) $$X = \left[\mathop{\&}_{s=0}^{k-1} b_s C_s \right] = \sum_{s=0}^{k-1} b_s [C_s] ,$$

$b_s \in Z$, the integers. Note from the definition of a binary composition

$$\{0\} \wedge C_i = C_i .$$

We will define the transpose of a coset C_i^T by:

$$C_i = \{x^{kj+i} : 0 \le j \le m-1\} ,$$

$$C_i^T = \{-x^{kj+i} : 0 \le j \le m-1\} .$$

LEMMA 1 [1]. *If* m *is even,* $C_i^T = C_i$ *; and if* m *is odd,* $C_i^T = C_{i+\frac{1}{2}k}$.

THEOREM 2 [1]. *If* C_i *and* C_l *are two cosets of order* m *and index* k *of the group* G *, then the binary composition of* C_i *and* C_l *is given by:*

(i) $C_i \wedge C_l = \mathop{\&}_{s=0}^{k-1} a_s C_s$ *if zero does not occur;*

(ii) $C_i \wedge C_l = m\{0\} \mathbin{\&} \mathop{\&}_{s=0}^{k-1} a_s C_s$ *if zero does occur;*

where the a_s *are integers giving multiplicities.*

LEMMA 3. *If*

(i) zero does not occur in $C_i \wedge C_l$ *then*

$$\sum_{s=0}^{k-1} a_s = m ;$$

(ii) zero does occur in $C_i \wedge C_l$ *then*

$$\sum_{s=0}^{k-1} a_s = m - 1 .$$

LEMMA 4 [1]. $C_i \wedge C_l = m\{0\} \;\&\; \mathop{\&}_{s=0}^{k-1} a_s C_s$ *if and only if* $C_l = C_i^T$.

LEMMA 5 [1]. *If*

(i) $C_l \neq C_i^T$ *in* $C_i \wedge C_l$ *then*

$$\mathop{\&}_{p=0}^{k-1} C_{i+p} \wedge C_{l+p} = \mathop{\&}_{s=0}^{k-1} mC_s \; ;$$

(ii) $C_l = C_i^T$ *in* $C_i \wedge C_l$ *then*

$$\mathop{\&}_{p=0}^{k-1} C_{i+p} \wedge C_{l+p} = km\{0\} \;\&\; \mathop{\&}_{s=0}^{k-1} (m-1)C_s \; .$$

Method of partitioning GF(v)

The incidence matrices $[C_i]$ of the cosets C_i and the identity matrix I are partitioned into four (0, 1, -1) matrices X_1, X_2, X_3, X_4 such that

$$X_i * X_j = 0 \; , \quad i \neq j \; , \quad i, j = 1, 2, 3, 4 \; ;$$

$$\sum_{i=1}^{4} X_i X_i^T = vI_v \; .$$

We show for m even with $X_i * X_j = 0$ it is not possible to get $\sum_{i=1}^{4} X_i X_i^T = vI_v$.

THEOREM 6. *Let* $v = mk + 1 = p^\alpha$ *(*p *a prime) with* m *even. Further suppose* C_i *are cosets of order* m *defined above.*

Let

$$X_i = \left[\mathop{\&}_{s=0}^{k-1} a_{i_s} C_s\right] , \quad i = 1, 2, 3, 4 \; ,$$

and suppose exactly one of $a_{1_s}, a_{2_s}, a_{3_s}, a_{4_s}$ *is* 1 *or* -1 *and* I

belongs to one of the X_i*'s* .

Then

$$\sum_{i=1}^{4} X_i X_i^T = vI_v$$

is not possible.

Proof. Without loss of generality let I occur in X_1 .

$$X_1 = \left[\mathop{\&}_{s=0}^{k-1} a_{1_s} C_s \ \& \ \{0\}\right]$$

$$= \sum_{s=0}^{k-1} a_{1_s} [C_s] + I \quad \text{from (1);}$$

for $i = 2, 3, 4$,

$$X_i = \sum_{s=0}^{k-1} a_{i_s} [C_s] .$$

Since m is even from Lemma 1,

$$C_i^T = C_i \ ;$$

thus $X_i X_i^T$ becomes X_i^2 for all i and we have

$$X_1^2 = \left(\sum_{s=0}^{k-1} a_{1_s} [C_s] + I\right)^2 ,$$

$$X_i^2 = \left(\sum_{s=0}^{k-1} a_{i_s} [C_s]\right)^2 , \quad i \neq 1 ,$$

$$X_1^2 = \sum_{s=0}^{k-1} a_{1_s}^2 [C_s]^2 + 2 \sum_{s=0}^{k-1} \sum_{p=s+1}^{k-1} a_{1_s} a_{1_p} [C_s][C_p] + 2 \sum_{s=0}^{k-1} a_{1_s} [C_s] + I .$$

For $i = 2, 3, 4$,

$$X_i^2 = \sum_{s=0}^{k-1} a_{i_s}^2 [C_s]^2 + 2 \sum_{s=0}^{k-1} \sum_{p=s+1}^{k-1} a_{i_s} a_{i_p} [C_s][C_p] .$$

Now

$$\sum_{i=1}^{4} X_i X_i^T = \sum_{i=1}^{4} X_i^2$$

$$= \sum_{s=0}^{k-1} [C_s]^2 \quad \text{from the conditions of the theorem}$$

$$+ 2 \sum_{i=1}^{4} \left\{ \sum_{s=0}^{k-1} \sum_{p=s+1}^{k-1} a_{i_s} a_{i_p} [C_s][C_p] \right\} + 2 \sum_{s=0}^{k-1} a_{1_s} [C_s] + I \ ;$$

$$\sum_{i=1}^{4} X_i^2 = kmI + (m-1) \sum_{s=0}^{k-1} [C_s] \quad \text{from Lemma 5}$$

$$+ 2 \sum_{i=1}^{4} \left\{ \sum_{s=0}^{k-1} \sum_{p=s+1}^{k-1} a_{i_s} a_{i_p} \left(\sum_{j=0}^{k-1} b_j [C_j] \right) \right\} \quad \text{by Theorem 2 } (i)$$

$$(b_j\text{'s depend on } s \text{ and } p)$$

$$+ 2 \sum_{s=0}^{k} a_{1_s} [C_s] + I \ ,$$

$$(2) \qquad \sum_{i=1}^{4} X_i^2 = (km+1)I + (m-1) \sum_{s=0}^{k-1} [C_s] + 2 \sum_{j=0}^{k-1} d_j [C_j] \ ,$$

where d_j comes from collecting all the cosets together from the third and fourth terms of the equation above.

It can be easily seen that it is not possible to get $\sum_{i=1}^{4} X_i^2 = vI_v$ as $m - 1$ is odd and the 2 in front of the last term of equation (2) gives all the cosets from this term an even number of times.

For $v = 9, 11, 17, \ldots$, m cannot be odd, by a result in [2]. We have just shown m cannot be even. So it is impossible to partition $GF(v)$ by the method of [2] in order to construct Hadamard arrays, for those values of v .

References

[1] Joan Cooper, "A binary composition for collections and sets", *Proc. First Austral. Conf. Combinatorial Math., Newcastle,* 1972, 145-161 (TUNRA, Newcastle, 1972).

https://doi.org/10.1017/S0004972700040570 Published online by Cambridge University Press

[2] Joan Cooper and Jennifer Wallis, "A construction for Hadamard arrays", *Bull. Austral. Math. Soc.* 7 (1972), 269-277.

[3] David C. Hunt and Jennifer Wallis, "Cyclotomy, Hadamard arrays and supplementary difference sets", *Proc. Second Manitoba Conf. Numerical Mathematics*, October 1972, 351-381 (Congressus Numerantium, 7. University of Manitoba, Winnipeg, 1972).

[4] Thomas Storer, *Cyclotomy and difference sets* (Lectures in Advanced Mathematics, 2. Markham, Chicago, Illinois, 1967).

Department of Mathematics,
University of Newcastle,
Newcastle,
New South Wales.