A note on Hadamard arrays

Joan Cooper

Let \( v = 4k + 1 \) 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) \( X_i \ast X_j = 0 \), \( i \neq j \), \( i, j = 1, 2, 3, 4 \);

(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, \( \ast \), of two matrices \( A = \{a_{ij}\} \) and \( B = \{b_{ij}\} \) which are the same size is given by

\[
A \ast B = \{a_{ij}b_{ij}\}.
\]

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

Received 1 August 1973. Communicated by Jennifer R.S. Wallis.
of all 1's will be $J$.

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

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

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

$$A_1 \^\wedge A_2 = [x_1, \ldots, x_g] \^\wedge [y_1, \ldots, y_t] = [x_1^{A_2}, \ldots, x_g^{A_2}].$$

Let $v = mk + 1 = p^a$ (a prime power). Let $x$ be a primitive element of $F = GF(v)$ 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

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

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

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

$$X = \left[ \begin{array}{c} k-1 \\
\wedge \quad b \cdot C_g \\
s=0 \end{array} \right]$$

will mean the matrix $X$ which is a summation of the incidence matrices of the cosets. That is
Hadamard arrays

\[ X = \left[ \begin{array}{c} k-1 & b, C_s \end{array} \right] = \sum_{s=0}^{k-1} b_s [C_s] , \]

\( b_s \in \mathbb{Z} \), 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:

\[ C_i = \{ x^{kj+i} : 0 \leq j \leq m-1 \} , \]
\[ C_i^T = \{ -x^{kj+i} : 0 \leq j \leq m-1 \} . \]

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

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

- (ii) \( C_i \wedge C_l = m(0) \sum_{s=0}^{k-1} a_s C_s \) 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]. \( C_i \cap C_j = m(0) \) if and only if \( C_i = C_j^T \).

LEMMA 5 [1]. If

(i) \( C_i \neq C_i^T \) in \( C_i \cap C_j \) then

\[
\sum_{s=0}^{k-1} a_s C_s \quad \text{if and only if} \quad C_i = C_i^T.
\]

(ii) \( C_i = C_i^T \) in \( C_i \cap C_j \) then

\[
\sum_{s=0}^{k-1} a_s C_s = m(0) \quad \text{if and only if} \quad C_i = C_i^T.
\]

Method of partitioning \( GF(\nu) \)

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

\[
X_i \cdot X_j = 0, \quad i \neq j, \quad i, j = 1, 2, 3, 4;
\]

\[
\sum_{i=1}^{4} X_i X_i^T = \nu I_\nu.
\]

We show for \( \nu = mk + 1 = p^\alpha \) \((p \text{ a prime})\) with \( m \) even and \( \nu_1 \neq \nu_j \) it is not possible to get

\[
\sum_{i=1}^{4} X_i X_i^T = \nu I_\nu.
\]

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

Let

\[
X_i = \left[ \sum_{s=0}^{k-1} a_s C_s \right], \quad i = 1, 2, 3, 4,
\]

and suppose exactly one of \( a_1, a_2, a_3, a_4 \) is 1 or -1 and I
belongs to one of the $X_i$'s.

Then

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

is not possible.

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

$$X_1 = \left[ \begin{array}{c} k-1 \\ \vdots \\ s = 0 \end{array} \right] a_{1_s} C_s \& \{0\} \right]$$

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

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

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

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

$$X_1^2 = \sum_{s=0}^{k-1} a_{1_s}^2 [C_s]^2 + 2 \sum_{s=0}^{k-1} a_{1_s} [C_s] + 2 \sum_{s=0}^{k-1} a_{1_s} [C_s] + I.$$ For $i = 2, 3, 4$,

$$X_i^2 = \sum_{s=0}^{k-1} a_{i_s}^2 [C_s]^2 + 2 \sum_{s=0}^{k-1} a_{i_s} [C_s] + 2 \sum_{s=0}^{k-1} a_{i_s} [C_s] + I.$$
\[
\sum_{i=1}^{k-1} x_i^2 = \sum_{i=1}^{k-1} x_i^2
\]
from the conditions of the theorem

\[
= \sum_{s=0}^{k-1} [C_s]^2
\]

\[
+ 2 \sum_{i=1}^{k-1} \left( \sum_{s=0}^{k-1} a_i s [C_s] [C_i] \right) + 2 \sum_{s=0}^{k-1} a_{s+1} [C_s] + I ;
\]

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

\[
+ 2 \sum_{i=1}^{k-1} \left( \sum_{s=0}^{k-1} a_i s [C_s] \right) \left( \sum_{j=0}^{k-1} b_j [C_j] \right)
\text{ by Theorem 2 (i)}
\]

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

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

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

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 \(\sum_{i=1}^{k-1} x_i^2 = \nu I \) 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 \(\nu = 9, 11, 17, \ldots\), \(m\) cannot be odd, by a result in [2]. We have just shown \(m\) cannot be even. So it is impossible to partition \(\text{GF}(\nu)\) by the method of [2] in order to construct Hadamard arrays, for those values of \(\nu\).

References


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