On Classification of Generalized Hadamard Matrices

Chked Sarami
Department of Mathematics & Computer Science
Fayetteville State University
Fayetteville, North Carolina, U.S.A.

Abstract - In this paper, we give an algorithm to list and classify generalized Hadamard matrices of a given order over an arbitrary elementary Abelian group. Generalized Hadamard matrices of order less than or equal to 16 over Abelian groups $Z_3, Z_4, Z_2 \times Z_2$ and $Z_5$ have been classified up to equivalence. We have shown that generalized Hadamard matrices of order 4, 8, and 12 over $EA(4)$ are unique up to equivalence.

Keywords: Hadamard matrices, generalized Hadamard matrices, symmetric nets.

1 Introduction

A $t$-$(v, k, \lambda)$ design $D = (X, B)$ is a set $X$ of $v$ points together with a collection $B$ of $b$ $k$-subsets of $X$ called blocks such that every $t$-subset of $X$ is contained in exactly $\lambda$ blocks. It follows that every $i$-subset of points ($i \leq t$) is contained in exactly $\lambda_i = \lambda \binom{v-i}{t-i}/\binom{v-i}{k-i}$ blocks [1], [3]. In particular, the total number of blocks is $\lambda_0 = b$. The number $\lambda_1$ of blocks that contain a given point is traditionally denoted by $r$. Two designs with the same parameters are isomorphic if there is a bijection between their point sets that maps the blocks of the first design into the blocks of the second design.

A parallel class in a $t$-$(mk, k, \lambda)$ design is a set of $m$ pairwise disjoint blocks. A resolution is a partition of the collection of blocks into disjoint parallel classes. A design is resolvable if it has a resolution. A resolvable design with a resolution $R$ is said to be affine resolvable or affine, if there is a constant $\mu \neq 0$ such that every two blocks that belong to different parallel classes of $R$ intersect in exactly $\mu$ points. An affine design admits only one resolution and $\mu = k/m = k^2/v$.

We recall that the dual design $D^*$ of $D$ is obtained by interchanging the roles of points and blocks in $D$. A symmetric $(\mu, m)$-net is a 1-$(\mu m^2, \mu m, \mu m)$ design $D$ such that both $D$ and $D^*$ are affine [1]. Therefore, the $\mu m^2$ points of $D$ can be partitioned into $\mu m$ disjoint (parallel) classes each containing $m$ points, so that any two points that belong to the same class do not occur together in any block, while any two points that belong to different classes occur together in exactly $\mu$ blocks. A symmetric $(\mu, m)$-net is class-regular if it admits a group of automorphisms $G$ of order $m$ (called group of bitranslations) that acts transitively (and hence regularly) on every point and block parallel class. The classical example of a class regular $(q^{n-2}, q)$-net, where $q$ is a prime power, is obtained from the affine design with parameters

$$v = q^n, k = q^{n-1}, \lambda = \frac{q^{n-1} - 1}{q - 1}, r = \frac{q^n - 1}{q - 1}$$

having as points and blocks the points and hyperplanes the $n$-dimensional affine space $AG(n, q)$ over $F_q$.

Let $G$ be an additive Abelian group of order $g$. Suppose $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in G^n$, we say $u$ and $v$ are difference-balanced if and only if each element of $G$ appears exactly $\lambda = n/g$ times in the set of components of $(x_1 - y_1, \ldots, x_n - y_n)$. A $(g, k; \lambda)$-difference matrix is a $k \times \lambda g$ matrix over $G$ in which any two distinct rows are difference-balanced. It is known that $k \leq g\lambda$. A generalized Hadamard matrix $GH(g, \lambda)$ is a $(g, \lambda g; \lambda)$-difference matrix. There are many existence, non-existence and construction theorems about these matrices (for surveys see [3], [5], [18]). An ordinary Hadamard matrix of order $4\lambda$ is corresponding to a $GH(2, 2\lambda)$ over $Z_2$. Generalized Hadamard matrices have connections with many combinatorial objects, such as three-weight extended-BCH codes, strongly regular graphs, affine resolvable and symmetric balanced incomplete block designs, orthogonal
arrays of strength two, affine, nets, and transversal designs [7], [12].

We say two generalized Hadamard matrices $H_1$ and $H_2$ are equivalent if and only if one can be obtained from the other by permutation of the rows and columns and a series of addition of elements of group independently of the rows and columns. To identify the equivalence of two generalized Hadamard matrices of order $n$ by a complete search is known to be an NP-hard problem.

Every generalized Hadamard matrix $GH(g, \lambda)$ determines a class-regular symmetric $(\mu, m)$-net with a group of bitranslations isomorphic to $G$. Conversely, every class-regular symmetric $(\mu, m)$-net with a group of bitranslations $G$ determines a generalized Hadamard matrix [1]. Two generalized Hadamard matrices are equivalent if their corresponding symmetric nets are isomorphic as designs [1]. Using classification of class-regular symmetric nets, it is shown that there are precisely two inequivalent generalized Hadamard matrices of order 9 over the group of order 3 [15], and 226 inequivalent generalized Hadamard matrices of order 16 over the elementary Abelian group of order 4, only one of these matrices base on a net in $AG(3,4)$ [10].

The number of non-isomorphic affine 2-designs with parameters (1) grows exponentially with $n$ for any prime power $q$ (cf. [13], [14]). It is likely that these designs yield an exponentially growing number of inequivalent generalized Hadamard matrices over the elementary Abelian group $EA(q^n)$.

The classification of Hadamard matrices has been done up to order 28. More precisely, there is a unique equivalence class of Hadamard matrices of each order 1; 2; 4; 8, and 12. The number of classes for orders 16, 20, 24 and 28 are 5, 3, 60 and 487, respectively. Since generalized Hadamard matrices have larger groups, the classification of such matrices is harder. In the next section, we give an algorithm to generate and classify generalized Hadamard matrices over a given elementary Abelian group. We classify generalized Hadamard matrices over Abelian groups of order less than or equal to 5, that is, $Z_3$, $Z_4$, $Z_2 \times Z_2$, and $Z_5$ of orders less than or equal to 16. We have proven the following results:

1. A $GH(g, \lambda)$ over $G$ is unique up to isomorphism in the following cases:

(a) $g = 3$, $G = Z_3$, $\lambda = 1, 2, 4$. (when $\lambda = 3$ there are two inequivalent $GH$-matrices [15])

(b) $g = 4$, $G = Z_2 \times Z_2$, $\lambda = 1, 2, 3$.

2. For $\lambda = 1, 2, 3$, there is no $GH(4, \lambda)$ matrix over $Z_4$.

The following table gives the list of generalized Hadamard matrices that have been classified so far. The orders enclosed in parenthesis are classified so far. The exponents represent the number of inequivalent generalized Hadamard matrices.

<table>
<thead>
<tr>
<th>Group</th>
<th>Classified orders</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Z_2$</td>
<td>$2^1, 4^1, 8^1, 12^1, 16^0, 20^1, 24^{10}, 28^{18}$</td>
</tr>
<tr>
<td>$Z_3$</td>
<td>$3^1, (6^1), 9^2, (12^1), 15^0$ (c.f. [6])</td>
</tr>
<tr>
<td>$Z_4$</td>
<td>$4^0, (8^0), 12^0, 16^{13}$ (c.f. [10])</td>
</tr>
<tr>
<td>$Z_2 \times Z_2$</td>
<td>$(4^1), (8^1), (12^1), 16^{226}$ (c.f. [10])</td>
</tr>
<tr>
<td>$Z_5$</td>
<td>$(5^1), (10^1), 15^0$ (c.f. [6]), $20^{\geq 1}$ (c.f. [4])</td>
</tr>
</tbody>
</table>

Non-existence of the generalized Hadamard matrices in the above table except for $GH(4, 2)$ over $Z_4$ can be proven using the following theorem:

**Proposition 1** [8] A $(g, 3, \lambda)$-difference matrix does not exist if $g \equiv 2(\text{mod} 4)$ and $\lambda$ is odd.

In the next section we describe a method to list the classify generalized Hadamard matrices over an arbitrary Abelian group.

2 Generating Generalized Hadamard Matrices

To construct a $GH(g, \lambda)$ over an Abelian group $G = \{a_1 = 0, \ldots, a_g\}$, we can always assume that the first row and column is zero (by adding a constant group element to the rows and columns of a $GH$-Matrix). A generalized Hadamard matrix in this form is said to be normalized. Now if $R$ is a row of such matrix of length $g\lambda$ then it must contain exactly each element of group $\lambda$ times. Therefore, without
loss of generality we can assume the first two rows of the matrix are as follows:

\[
\begin{bmatrix}
0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0
\end{bmatrix}
\]

Assuming the first entry of the third row is 0, we can easily show that there are exactly

\[
\prod_{i=1}^{g} \binom{g}{\lambda}
\]

possible rows that contain each element of group \(\lambda\) times. Now, suppose \(A\) is the set of rows which are difference-balanced with the second row. For large matrices \(|A|\) is very large and the classification will be problematic. To this end, we can permute these rows within the blocks

\[
\begin{bmatrix}
0 & \cdots & 0
\end{bmatrix}
\]

and the rows still remain difference-balanced. The group \(S_n^\lambda = S_\lambda \times \cdots \times S_\lambda\) acts on \(A\). Assume that \(G \setminus A = \{[r_i]\}_{i=1}^{g}\) is the complete set of orbit representatives of the action. For each \(r_i\), we consider a graph \(G_i\) with vertices \(X = A \setminus \{r_i\}\) and with the edge set

\[
E_i = \{\{x,y\} \in A : x \text{ and } y \text{ are difference-balanced with } r_i \text{ and each other}\}.
\]

If a \(GH(g,\lambda)\) matrix exists, then \(m_i\), the maximum clique number of the graph is \(g\lambda - 3\). By adding the first three rows to each clique we obtain a generalized hadamard matrix.

In the next section we describe how to classify the obtained generalized Hadamard matrices.

Let \(A\) be an \(m \times n\) matrix (with entries \(a_{ij}\)) and let \(B\) be a \(p \times q\) matrix. Then the Kronecker product of \(A\) and \(B\) is the \(mn \times mn\) block matrix

\[
A \otimes B = \begin{bmatrix}
a_{11}B & \cdots & a_{1n}B \\
\vdots & \ddots & \vdots \\
a_{m1}B & \cdots & a_{mn}B
\end{bmatrix}.
\]

For a permutation \(\pi \in S_n\) we define a permutation matrix \(A_{\pi} = [a_{ij} = \delta_{\pi(i)j}]_{n \times n}\) where \(\delta\) is the Kronecker delta function define as follows:

\[
\delta_{mn} = \begin{cases}
1 & m = n \\
0 & m \neq n
\end{cases}
\]

We can easily show that for the cyclic permutation \(\sigma_n = (1,2,\ldots,n)\), we have \(A_{\sigma_n} = A_{\sigma_n}^T\). Using mathematical induction and the properties of the Kronecker product we obtain:

**Lemma 2** Assume the Abelian group \(G\) with \(|G| = g\) is a direct product of cyclic groups as follows

\[
G = \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_n^{m_n}},
\]

where \(n, m_1, \ldots, m_n \in \mathbb{N}, p_1, \ldots, p_n\) are prime numbers. For \(i \in \mathbb{N}\), let \(\sigma_i = (1,2,\ldots,n)\). Then we have the following natural isomorphism

\[
G \cong \{(A_{i_{p_1^{m_1}}}^1 \otimes \cdots \otimes A_{i_{p_n^{m_n}}}^n) : i_{p_1^{m_1}} \in \{0,1,\ldots,p_1^{m_1} - 1\},
\]

\[
\forall i_{p_1^{m_1}} \in \{1,\ldots,n\} \},
\]

in which \(([i_1],\ldots,[i_n])\) is corresponded to the \(g \times g\) matrix \(A_{\sigma_n}^{i_{p_1^{m_1}}} \otimes \cdots \otimes A_{\sigma_n}^{i_{p_n^{m_n}}}\).

Given an \(H = GH(g,\lambda)\) over an abelian group \(G = \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_n^{m_n}}\) of order \(g\) we replace each entry of \(H\) by its corresponding \(g \times g\) matrix to get a \(g^2\lambda \times g^2\lambda\) binary matrix \(M(H)\). The resulting matrix is an incidence matrix of a class-regular symmetric \((\mu, m)\)-net.

**Example 3** These following matrices

\[
I = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]

\[
A = \begin{bmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]

\[
B = \begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{bmatrix}
\]

\[
C = \begin{bmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0
\end{bmatrix}
\]
form a multiplicative Abelian group, $G$ as follows:

$$G = (\{I, A, B, C = AB|A^2 = B^2 = (AB)^2 = I, AB = BA\}, \cdot) \cong E A (4).$$

In the following section, we present the obtained generalized Hadamard matrices. We have used the computer algebra system Magma [2] to list and classify the matrices.

3.1 Generalized Hadamard matrices over $\mathbb{Z}_3$

There is exactly one GH(3, 1) matrix over $\mathbb{Z}_3$ up to equivalence which corresponds to the multiplication table of $\mathbb{Z}_3$. A GH(3, 2) matrix over $\mathbb{Z}_3$ is also unique up to equivalency as follows:

$$GH(3, 2) = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 2 & 2 & 2 & 0 & 2 & 2 & 1 & 1 \\
0 & 0 & 1 & 1 & 2 & 2 & 2 & 0 & 2 & 2 & 1 & 1 \\
0 & 0 & 1 & 1 & 2 & 2 & 2 & 0 & 2 & 2 & 1 & 1 \\
0 & 0 & 1 & 1 & 2 & 2 & 2 & 0 & 2 & 2 & 1 & 1
\end{pmatrix}$$

There are exactly two GH(3, 3) matrices up to equivalence over $\mathbb{Z}_3$. They are the ones listed in [10]. There is a unique generalized Hadamard matrix of order 12 over $\mathbb{Z}_3$ up to equivalence as follows:

$$GH(3, 3) = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

3.2 Generalized Hadamard matrices over $\mathbb{Z}_4$

According to Proposition 1, there is no GH(4, $\lambda$) when $\lambda = 1, 3$. When $\lambda = 2$, we have 80 candidates for the third rows ($|A| = 80$) with the maximum clique number 2. Hence, there is no generalized Hadamard matrix of order 8. In this case we get the following maximal (4, 4; 2)-difference matrix:

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 2 & 3 & 3 & 1 & 1 \\
0 & 1 & 3 & 0 & 2 & 2 & 3 & 1 \\
0 & 3 & 3 & 2 & 1 & 1 & 0 & 2
\end{pmatrix}$$

3.3 Generalized Hadamard matrices over $\mathbb{Z}_2 \times \mathbb{Z}_2$

For $\lambda = 1, 2$ we have unique GH(4, $\lambda$) matrices up to equivalence as follows:

$$GH(4, 1) = \begin{pmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & w & w^2 \\
0 & w & w^2 & 1 \\
0 & w^2 & 1 & w
\end{pmatrix}$$

$$GH(4, 2) = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

The following is the unique GH(4, 3) over $\mathbb{Z}_2 \times \mathbb{Z}_2$:

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & w & w & w^2 & w^2 & w^2 & w^2 \\
0 & 0 & 0 & w & w & w & w^2 & w^2 & 1 & 1 & 1 & 1 \\
0 & 1 & w^2 & 0 & w & w^2 & w & w^2 & 1 & 1 & 1 & 1 \\
0 & 1 & w^2 & w^2 & 0 & 0 & 0 & 1 & w & w & w & w \\
0 & 0 & 1 & w^2 & 0 & w & w^2 & 0 & 1 & w & w & w \\
0 & 0 & 1 & w^2 & w^2 & 0 & w & w^2 & 1 & w & w & w \\
0 & 0 & 1 & w^2 & w^2 & w^2 & 0 & w & w^2 & 1 & w & w \\
0 & 0 & 1 & w^2 & w^2 & w^2 & w^2 & 0 & w & w^2 & 1 & w \\
0 & 0 & 1 & w^2 & w^2 & w^2 & w^2 & w^2 & 0 & w & w^2 & 1
\end{pmatrix}$$
Using the classification of class-regular (4,4)-nets Harada, Lam and Tonchev have shown that there are 226 inequivalent generalized Hadamard matrices of order 16 over $\mathbb{Z}_2 \times \mathbb{Z}_2$, one of those based on a net in AG(3,4) [10]. Many of the $F_4$-codes spanned by generalized Hadamard matrices of order 16 over the elementary Abelian of order 4 are self-orthogonal with respect to the Hermitian inner product and yield quantum error-correcting codes, including some codes with optimal parameters [10].

3.4 Generalized Hadamard matrices over $\mathbb{Z}_5$

For $n = 5, 10$ there are unique generalized Hadamard matrix of order $n$ up to isomorphism.

$\text{GH}(5, 1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 0 & 3 & 1 & 4 & 2 \\ 0 & 4 & 3 & 2 & 1 \end{pmatrix}$

$\text{GH}(5, 2) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 3 & 4 & 1 & 2 \\ 0 & 3 & 0 & 2 & 4 & 1 & 4 & 3 \\ 0 & 1 & 3 & 4 & 0 & 2 & 4 & 2 \\ 0 & 4 & 2 & 1 & 4 & 3 & 2 & 1 \\ 0 & 2 & 1 & 4 & 3 & 2 & 1 & 0 \\ 0 & 3 & 0 & 2 & 3 & 1 & 1 & 4 \\ 0 & 4 & 2 & 1 & 3 & 4 & 0 & 1 \\ 0 & 4 & 3 & 2 & 3 & 1 & 2 & 1 \end{pmatrix}$

References


