Generalized Hadamard matrices $GH(2^k,1)$ over an elementary abelian group

Sara Sasani, Priya Soundararajan

July 14, 2014

Abstract

To find Generalized Hadamard matrices $GH(2^k,1)$ for $k \geq 3$ on the multiplicative group consisting of diagonal matrices each having as its diagonal one row of $H(2^k)$ (a Hadamard matrix of order 2^k) which we can denote as $\{D_1, D_2, \ldots, D_{2^k}\}$.

Definition 1. *An nxn ($\pm$1)-matrix H is a Hadamard matrix if $HH^T = nI$(i.e its rows are pairwise orthogonal). H_n denotes a Hadamard matrix of order n.*

If H is a Hadamard matrix, then H^T is also a Hadamard matrix.

Definition 2. *[1] If G is a finite group of order s, then a square matrix $H = [h_{ij}]$ of order r with elements from G is called a Generalized Hadamard matrix of type r/s if:*

(i) For each $1 \leqslant i \neq j \leqslant r$, $\{h_{ik}h_{jk}^{-1} : 1 \leqslant k \leqslant r\}$ includes r/s copies of every element of G.
(ii) H^T has the property (i).

Definition 3. *[2] A finite abelian group G of order n is said to be an elementary abelian group if each element of G has order p, where p is a prime.*

1 Introductio to a Group

In this section, we are going to construct an elementary abelian group of order 2^k, for each $k \geq 1$. The elements of these groups are diagonal matrices having order 2. At first, we review a definition.

Definition 4. *If $M = [m_{ij}]$ and $N = [n_{ij}]$ are tow matrix of order m and n respectivley, then the Kronecker product of M and N, denoted by $M \otimes N$, is a matrix of order nm which is defined as follow:*

$$M \otimes N = [m_{ij}N]$$

For this purpose, we choose specific Hadamard matrices. For $k=1$, we start with the following Hadamard matrix of order 2^1 and call it H_2:

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}$$

For $k=2$, define H_{2^2} as follow

$$H_{2^2} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix}$$

For $k \geq 3$, we define H_{2^k} as follow

$$H_{2^k} = H_2 \otimes H_{2^{k-1}}$$

The rows of these matrices have some properties mentioned in the following theorem.

Theorem 5. *The rows of H_{2^k} form an elemetary abelian group of order 2^k, for each $k \geq 1$. The multiplication of this group is componentwise multiplication.*

Proof. For each $k \geq 1$, let S_k be the set of rows of H_{2^k}; i.e.,

$$S_k = \{a_i^{2^k} : a_i^{2^k} \; is \; the \; ith \; row \; of \; H_{2^k}\;, \; for \; each \; 1 \leq i \leq 2^k\}$$

Note that S_k has 2^k elmements. Then S_k has associativity and commutativity properties because the componentwise multiplication of rows or real vectors is commutative and associative. Moreover, the first element of S_k includes only one because of the fisrt row of H_2, $[1,1]$, the first row of H_2^2, $[1,1,1,1]$, and the property of Kronecker product. Then so this element is the identity element of S_k. On the other hand, since the rows or elements, we are dailing with, include only ± 1, the inverse of each element is itself. In fact, the order of each elemetnt is two. Therefore, for each $k \geq 1$, S_k is a set with the properties associativity, inverse element, and identity. We use induction to prove closure.

Let $n=1$. Then, $S_1 = \{a_1^2, a_2^2\} = \{[1,1],[1,-1]\}$. If we denote componentwise multiplication by $*$, then we have

$$a_1^2 * a_1^2 = a_1^2$$
$$a_2^2 * a_1^2 = a_2^2$$
$$a_2^2 * a_2^2 = a_1^2$$

Therefore, the set S_1 is closed under componentwise multiplication. Since the structure of first two matrix is different, we consider two base cases for this proof. Now, let $n=2$. Then, $S_2 = \{a_1^{2^2}, a_2^{2^2}, a_3^{2^2}, a_4^{2^2}\} = \{[1,1,1,1],[1,1,-1,-1],[1,-1,1,-1],[1,-1,-1,1]\}$, then we have

$$a_1^{2^2} * a_1^{2^2} = a_1^{2^2}$$

$$a_1^{2^2} * a_2^{2^2} = a_2^{2^2}$$
$$a_1^{2^2} * a_3^{2^2} = a_3^{2^2}$$
$$a_1^{2^2} * a_4^{2^2} = a_4^{2^2}$$
$$a_2^{2^2} * a_2^{2^2} = a_1^{2^2}$$
$$a_2^{2^2} * a_3^{2^2} = a_4^{2^2}$$
$$a_2^{2^2} * a_4^{2^2} = a_3^{2^2}$$
$$a_3^{2^2} * a_3^{2^2} = a_1^{2^2}$$
$$a_2^{2^2} * a_4^{2^2} = a_2^{2^2}$$

Assume, for $n = k$, we have S_k is closed under componentwise multiplication. Let $n = k+1$. Then we have

$$H_{2^{k+1}} = H_2 \otimes H_{2^k} = \begin{pmatrix} H_{2^k} & H_{2^k} \\ H_{2^k} & -H_{2^k} \end{pmatrix}$$

Let $a_i^{2^{k+1}}$ and $a_j^{2^{k+1}}$ be two arbitrary element of S_{k+1}. Since the set of rows of Hadamard matrix H_{2^k}, S_k, is closed under componentwise multiplication, we have

- If $1 \leq i \neq j \leq 2^k$, then $a_i^{2^{k+1}} * a_j^{2^{k+1}} = a_r^{2^{k+1}}$, for some $1 \leq r \leq 2^k$.
- If $2^k + 1 \leq i \neq j \leq 2^{k+1}$, then $a_i^{2^{k+1}} * a_j^{2^{k+1}} = a_r^{2^{k+1}}$, for some $1 \leq r \leq 2^k$.
- If $1 \leq i \leq 2^k$ and $2^k + 1 \leq j \leq 2^{k+1}$, then $a_i^{2^{k+1}} * a_j^{2^{k+1}} = a_r^{2^{k+1}}$, for some $2^k + 1 \leq r \leq 2^{k+1}$.

Hence, the rows of H_{2^k} form an elemetary abelian group of order 2^k, for each $k \geq 1$. $\square$

Remark 6. *Note that H_2 and H_{2^2} are symmetric Hadamrd matrix, so $H_2 = H_2^T$ and $H_{2^2} = H_{2^2}^T$. Then H_{2^k} is also symmetric because it is constructed by repetitions of Kronecker product of H_2 with H_{2^2}. This means that The columns of H_{2^k} form the same elemetary abelian group S_k of order 2^k, for each $k \geq 1$.*

For each k, we have

$$S_k = \{a_i^{2^k} : a_i^{2^k} \text{ is the ith row of } H_{2^k}\ ,\ for\ each\ 1 \leq i \leq 2^k\}$$

For each i, we can replace a_i with $D_i = diag(a_i)$, a diagonal matrix having a_i on its diagonal. Now, let make a new set called T_k as follow

$$T_k = \{D_i^{2^k} : D_i^{2^k} \text{ is a diagonal matrix having } a_i^{2^k} \text{ on its diagonal}\ ,\ for\ each\ 1 \leq i \leq 2^k\}$$

By using matrix multiplication, T_k is also an elemetary abelian group of order 2^k isomorphic to S_k, for each $k \geq 1$.

Now, see an example for the case $k = 3$.

Example 7. *let $k=3$. Then we have*

$$H_{2^k} = H_{2^3} = H_2 \otimes H_{2^2}$$

So

$$H_{2^3} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & - & - & 1 & 1 & - & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - \end{pmatrix}$$

The first row of this matrix includes only one, and it is a symmetric matrix. Then we have

$$S_3 = \{a_1^{2^3}, a_2^{2^3}, \ldots, a_8^{2^3}\}$$

, where

$$a_1^{2^3} = [1,1,1,1,1,1,1,1]$$
$$a_2^{2^3} = [1,1-,-,1,1-,-]$$
$$a_3^{2^3} = [1,-,1,-,1,-,1,-]$$
$$a_4^{2^3} = [1,-,-,1,1,-,-,1]$$
$$a_5^{2^3} = [1,1,1,1,-,-,-,-]$$
$$a_6^{2^3} = [1,1,-,-,-,-,1,1]$$
$$a_7^{2^3} = [1,-,1,-,-,1,-,1]$$
$$a_8^{2^3} = [1,-,-,1,-,1,1,-]$$

, and

$$T_3 = \{D_1^{2^3}, D_2^{2^3}, \ldots, D_8^{2^3}\}$$

, where

$$D_1^{2^3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$D_2^{2^3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & - & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & - & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & - & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \end{pmatrix}$$

$$D_3^{2^3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & - & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & - & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & - & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \end{pmatrix}$$

$$D_4^{2^3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & - & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & - & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & - & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & - & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$D_5^{2^3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & - & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & - & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & - & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \end{pmatrix}$$

$$D_6^{2^3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & - & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & - & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & - & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & - & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$D_7^{2^3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & - & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & - & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & - & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & - & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$D_8^{2^3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & - & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & - & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & - & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \end{pmatrix}$$

Then the multiplication tables of S_3 and T_3 are the same if i referes to both D_i and a_i, for each $1 \le i \le 8$. Hence, we have

*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
2	*2*	*1*	*4*	*3*	*6*	*5*	*8*	*7*
3	*3*	*4*	*1*	*2*	*7*	*8*	*5*	*6*
4	*4*	*3*	*2*	*1*	*8*	*7*	*6*	*5*
5	*5*	*6*	*7*	*8*	*1*	*2*	*3*	*4*
6	*6*	*5*	*8*	*7*	*2*	*1*	*4*	*3*
7	*7*	*8*	*5*	*6*	*3*	*4*	*1*	*2*
8	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*

The following theorem states for each $k \ge 1$, S_k has a subset U_k with k elements with an specific property. We will use U_k in the next section.

Theorem 8. *For each $k \ge 1$, there is a subset U_k of S_k with k elements satisfying the following condition:*

- *For each $1 \le i \le k$, there is an element $b_k^i = [(b_k^i)_j]$, $1 \le j \le 2^k$, in U_k such that:*
  - *For each $i > 1$, $b_k^i = [(b_k^i)_j] = [(-1)^{q_i}]$, where q_i is the quotient when dividing j by 2^{i-1}; and*
  - *For $i = 1$, $b_k^1 = [(b_k^1)_j] = [-(-1)^j]$.*

Proof. We use induction for this proof. We have two base cases $n = 1$ and $n = 2$. Let $n = 1$, then U_1 has one element, and i can be only 1. We have $b_1^1 = [-(-1)^j] = [1, -1]$ which is equal to a_2^2. Hence, $U_1 = \{a_2^2\}$. Let $n = 2$, then U_2 has two elements, and i can be 1 and 2. We have $b_2^1 = [-(-1)^j] = [1, -1, 1, -1]$ which is equal to $a_3^{2^2}$, and $b_2^2 = [(-1)^{q_i}] = [1, 1, -1, -1]$ which is equal to $a_2^{2^2}$. Therefore, $U_2 = \{a_3^{2^2}, a_2^{2^2}\}$.

Assume, for $n = k$, we have $U_k = \{b_k^1, \ldots, b_k^k\}$ with desired properties. Let $n = k+1$. By the construction of S_k, we have the set $\{(b_k^1 | b_k^1), \ldots, (b_k^k | b_k^k)\}$ is a subset of S_{k+1}. Moreover, for $1 \leq i \leq k$, we have

$$b_{k+1}^i = (b_k^i | b_k^i)$$

Hence, we have k elements of U_{k+1}. We also have that the first 2^k components of b_{k+1}^{k+1} are one, and the rest are minus one. By constructure of S_{k+1}, this element is $a_{2^k+1}^{2^{k+1}}$ which is the last element of U_{k+1}. $\square$

2 Introduction

According to Proposition 1.5 in [1], there is a symmetric GH matrix of type 1 over every finite elementary abelian group G of order p^k. The GH matrix is constructed as follows:
G, the elementary abelian group of prime power order p^k is taken to be the additive group of the field $F = GF(p^k)$. A multiplication table for the field constitutes the elements of the GH matrix of type 1 over G.
An example of GH matrix constructed over $GF(2^3) = \mathbb{Z}/2\mathbb{Z}[T]/(T^3+T+1)$

$GF(2^3) = \{0, 1, T, T+1, T^2, T^2+1, T^2+T, T^2+T+1\}$ is

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & T & T+1 & T^2 & T^2+1 & T^2+T & T^2+T+1 \\
0 & T & T^2 & T^2+T & T+1 & 1 & T^2+T+1 & T^2+1 \\
0 & T+1 & T^2+T & T^2+1 & T^2+T+1 & T^2 & 1 & T \\
0 & T^2 & T+1 & T^2+T+1 & T^2+T & T & T^2+1 & 1 \\
0 & T^2+1 & 1 & T^2 & T & T^2+T+1 & T+1 & T^2+T \\
0 & T^2+T & T^2+T+1 & 1 & T^2+1 & T+1 & T & T^2 \\
0 & T^2+T+1 & T^2+1 & T & 1 & T^2+T & T^2 & T+1
\end{pmatrix}$$

It is easy to see that the set $1 \leqslant i \neq j \leqslant r$, $\{h_{ik} - h_{jk} : 1 \leqslant k \leqslant r\}$ includes every element of G once.
The elements of the $GF(2^k)$ can also be written in the form of vectors over $GF(2)$

$$\begin{pmatrix} a_0 & a_1 & a_{k-1} & a_k \end{pmatrix}$$

where $a_0, a_1, \ldots GF(2)$. The additive group of $GF(2)$ is isomorphic to the multiplicative group of $\{1, -1\}$ with the usual operation of multiplication. Thus, the elementary abelian group G can be now be seen to consist of elements of the form

$$\begin{pmatrix} a_0 & a_1 & a_{k-1} & a_k \end{pmatrix}$$

where $a_0, a_1, \ldots \{-1, 1\}$, and the operation being pointwise multiplication.

We prove this by induction:
Let the statement hold true for order = 2^k,
Let $a_i^{2^k}$ i $\geq$1 represent a row of length 2^k, of alternating segments of +1's and -1's, with the length of each segment being 2^{k-i}, and the number of segments of each type being 2^{i-1}, and let $a_0^{2^k}$ represent the row of all ones.
By our assumption, H_2^k contains ..
From the construction, it can be seen that $a_i^{2^k}|a_i^{2^k} = a_{i+1}^{2^{k+1}}, for i \geq 1$.
$a_1^{2^{k+1}} = a_0^{2^k}|-a_0^{2^k}$, and $a_0^{2^{k+1}} = a_0^{2^k}|a_0^{2^k}$, which is true from the construction.
Let a Hadamard matrix of order 2^k contain rows of the above type. Then, a Hadamard matrix of order 2^k+1 as obtained from the construction in sectionx has a first row as all ones.

A Hadamard matrix of order 2^k can be normalized so that the first row consists of all ones, which is implicitly true from the construction described in sectionx

By the classification of finitely generated abelian groups, every elementary abelian group must be of the form $\mathbb{Z}/2\mathbb{Z}^k$, and thus the elementary abelian group G is isomorphic to $-1, 1^k$ (Since the group -1,1 with ordinary multiplication is isomorphic to $\mathbb{Z}/2\mathbb{Z}$)

References

[1] DAVID A. DRAKE, *Partial λ geometries and Generalized Hadamard matrices over groups* Can.J.Math.(1979), pp. 617-627

[2]