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

Sara Sasani, Priya Soundararajan

May 27, 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 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. *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 Introduction to the group D^{2^k}

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 two matrices 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 follows:*

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

1.1 Sylvester's construction

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 follows

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

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

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

Now, we introduce a notation which is useful.

Notation 5. *For each $k \geq 1$, let S_k be the set of rows of H_{2^k}; i.e.,*

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

Note that S_k has 2^k elmements.

By using this notation, we have

- For $1 \leq i \leq 2^k$, $a_i^{2^{k+1}} = (a_i^{2^k} | a_i^{2^k})$; and
- For $2^k + 1 \leq i \leq 2^{k+1}$, $a_i^{2^{k+1}} = (a_{imod2^k}^{2^k} | -a_{imod2^k}^{2^k})$.

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

Theorem 6. *The rows of H_{2^k} form an elemetary abelian group of order 2^k, for each $k \geq 1$. The operation of this group is componentwise multiplication.*

Proof. S_k has associativity and commutativity because the componentwise multiplication of real vectors is commutative and associative. The first element of S_k includes only ones because of the first row of H_2, $[1, 1]$, and the property of the Kronecker product.
This element is the identity element of S_k. On the other hand, since the rows or elements, we are dealing with, include only ±1, the inverse of each element is itself. In fact, the order of each element 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 component-wise 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.

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 elements 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 $k \geq 1$. □

Remark 7. *Note that H_2 is a symmetric Hadamard matrix, so $H_2 = H_2^T$ Then H_{2^k} is also symmetric because it is constructed by repetitions of Kronecker product of H_2 with itself (k-1) times. Thus 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

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

For each i, we can replace $a_i^{2^k}$ with $D_i = diag(a_i^{2^k})$, a diagonal matrix having $a_i^{2^k}$ on its diagonal. Now, let's make a new set called T_k as follow

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

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 8. *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

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

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

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

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

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

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

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

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

Then the multiplication tables of S_3 and T_3 are the same if i refers to both $D_i^{2^3}$ and $a_i^{2^3}$, for each $1 \leq i \leq 8$. 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 $k \geq 1$, S_k has a subset U_k with k elements with a specific property. We will use U_k in the next section.

Lemma 9. *For each $k \geq 1$, there is a subset U_k of S_k with k elements satisfying the following condition:*

- *For each $1 \leq i \leq k$, there is an element $b_i^{2^k} = [(b_i^{2^k})_j]$, $1 \leq j \leq 2^k$, in U_k such that:*
  - *If $i > 1$, $b_i^{2^k} = [(b_i^{2^k})_j] = [(-1)^{q_j}]$, where q_j is $[j/2^i]$; and*
  - *if $i = 1$, $b_1^{2^k} = [(b_1^{2^k})_j] = [-(-1)^j]$.*

$$b_k^{2^k} = \begin{pmatrix} \overbrace{1 \quad 1 \quad 1 \quad 1 \quad \ldots}^{2^{k-1}} \overbrace{-1 \quad -1 \quad -1 \quad -1 \quad \ldots}^{2^{k-1}} \end{pmatrix}$$

$$b_{k-1}^{2^k} = \begin{pmatrix} \overbrace{1 \quad 1 \quad \ldots}^{2^{k-2}} \overbrace{-1 \quad -1 \quad \ldots}^{2^{k-2}} \overbrace{1 \quad 1 \quad \ldots}^{2^{k-2}} \overbrace{\quad -1 \quad -1}^{2^{k-2}} \end{pmatrix}$$

$$b_{k-2}^{2^k} = \begin{pmatrix} \overbrace{1 \quad \ldots}^{2^{k-3}} \overbrace{-1 \quad \ldots}^{2^{k-3}} \overbrace{1 \quad \ldots}^{2^{k-3}} \overbrace{-1 \quad \ldots}^{2^{k-3}} \overbrace{1 \quad \ldots}^{2^{k-3}} \overbrace{-1 \quad \ldots}^{2^{k-3}} \overbrace{1 \quad \ldots}^{2^{k-3}} \overbrace{-1 \quad \ldots}^{2^{k-3}} \end{pmatrix}$$

$$\vdots$$

$$b_1^{2^k} = \left(\overbrace{1 \quad -1 \quad 1 \quad -1 \ldots \quad 1 \quad -1 \quad 1 \quad -1}^{\text{alternating +1's and -1's}} \right)$$

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 only be 1. We have $b_1^{2^1} = [-(-1)^j] = [1, -1] = a_2^2$.
Hence, $U_1 = \{a_2^2\}$.
If $n = 2$, then U_2 has two elements and i can take values 1 and 2. We have $b_1^{2^1} = [-(-1)^j] = [1, -1, 1, -1] = a_2^{2^2}$, and $b_2^{2^2} = [(-1)^{q_j}] = [1, 1, -1, -1] = a_3^{2^2}$.
Therefore, $U_2 = \{a_3^{2^2}, a_2^{2^2}\}$.

Assume, for $n = k$, we have $U_k = \{b_1^{2^k}, \ldots, b_k^{2^k}\}$ with desired properties. Let $n = k+1$. By the construction of S_k, we have the set $\{(b_1^{2^k} | b_1^{2^k}), \ldots, (b_k^{2^k} | b_k^{2^k})\}$ is a subset of S_{k+1}. Moreover, for $1 \leq i \leq k$, we have

$$b_i^{2^{k+1}} = (b_i^{2^k} | b_i^{2^k})$$

Hence, we have k elements of U_{k+1}. We also have that the first 2^k components of $b_{k+1}^{2^{k+1}}$ are one, and the rest are minus one. By constructure of S_{k+1}, this element is $b_{k+1}^{2^{k+1}} = a_{2^k+1}^{2^{k+1}} = (a_1^{2^k} | -a_1^{2^k})$ which make the last element of U_{k+1}. □

The subset U_k mentioned in lemma (9), has more specific properties. In the following lemma, we use U_k to build a matrix.

Lemma 10. *For each $k \geq 1$, suppose U_k is the subset of S_k mentioned in the last lemma, and construct a matrix UG_{2^k} in the following way:*

- *the element $b_i^{2^k}$ of the set U_k is the ith row of UG_{2^k}.*

Then, this matrix has the following properties:

- *The order of UG_{2^k} is k to 2^k;*
- *All 2^k columns of UG_{2^k} are distinct;*

Proof. For each k, consider the matrix UG_{2^k}. Since U_k has k elements which are the rows of UG_{2^k}, and since each element of U_k has 2^k components, the order of UG_{2^k} is k to 2^k.
Now, suppose UC_k is the set of culomns of UG_{2^k}; i.e.,

$$UC_k = \{u_i^{2^k}; u_i^{2^k} \textit{ is the ith column of } UG_{2^k}\}$$

We want to prove $u_r^{2^k} = [(u_r^{2^k})_j]$ and $u_s^{2^k} = [(u_s^{2^k})_j]$ are distinct if $r \neq s$, where $1 \leq r \neq s \leq 2^k$, and $1 \leq j \leq k$.

Toward a contradiction, suppose $r \neq s$ but $u_r^{2^k} = u_s^{2^k}$. Since $u_r^{2^k} = u_s^{2^k}$, then $(u_r^{2^k})_j = (u_s^{2^k})_j$ for each $1 \leq j \leq k$. We have $(u_r^{2^k})_k = (u_s^{2^k})_k$ implies $1 \leq r\ ,\ s \leq 2^{k-1}$ or $2^{k-1}+1 \leq r\ ,\ s \leq 2^k$. With out loss of generality, suppose $1 \leq r\ ,\ s \leq 2^{k-1}$.
Next, we have $(u_r^{2^k})_{k-1} = (u_s^{2^k})_{k-1}$ implies $1 \leq r\ ,\ s \leq 2^{k-2}$ or $2^{k-2}+1 \leq r\ ,\ s \leq 2^{k-1}$. With out loss of generality, suppose $1 \leq r\ ,\ s \leq 2^{k-2}$. If we continue in this way, we have last step as follow:

- Since $(u_r^{2^k})_1 = (u_s^{2^k})_1$, we have $1 \leq r\ ,\ s \leq 2^{k-k} = 1$.

This is a contradiction because we suppose $r \neq s$; so, $u_r^{2^k} \neq u_s^{2^k}$. Hence, all columns of UG_{2^k} are distinct. □

Now, consider the following lemma which is about the set UC_k mentioned in the lemma (10).

Lemma 11. *For each $k \geq 1$, the set UC_k, the set of culomns of UG_{2^k}, is an elementary abelian group of order 2^k under componentwise multiplication.*

Proof. For each $k \geq 1$, from lemma (9), the rows of H_{2^k} can be permuted so that the i^{th} row of H'_{2^k} is $b_i^{2^k}$. Then the matrix UG_{2^k} is a submatrix of H'_k; i.e., the matrix UG_{2^k} form the first k rows of H'_{2^k}. By remark 7, the columns of H_{2^k} form an elementary abelian group under componentwise multiplication. Therefore, the columns of H'_{2^k} also form an elementary abelian group under componentwise multiplication. This implies that UC_k is an elementary group under componentwise multiplication. By previous lemma, the order of this group is 2^k. □

In the following lemma, we prove the existence of an isomorphism between S_k and UC_k.

Lemma 12. *For each $k \geq 1$, there is an isomorphism Φ from S_k to UC_k defined as follow.*

- $\Phi(a_i^{2^k}) = u_i^{2^k}$*, where* $1 \leq i \leq 2^k$.

Proof. For each $k \geq 1$, since the matrix UG_{2^k} forms the first k rows of H'_{2^k}, we can map each column of UG_{2^k} to each column of H'_{2^k}, in the natrual way. Hence, if

$$S'_k = \{a_i'^{2^k} : a_i'^{2^k} \text{ } is\ the\ ith\ row\ of\ H'_{2^k}\ ,\ for\ each\ 1 \leq i \leq 2^k\},$$

then let σ from S'_k to UC_k be the following mapping:

$$\sigma(a_i'^{2^k}) = u_i^{2^k},\ for\ each\ 1 \leq i \leq 2^k.$$

By considering the componentwise multiplicetion, this is an isomorphism. To complete the proof, we need the isomorphism σ from S_k to S'_k defined as follow:

$$\phi(a_i^{2^k}) = a_i'^{2^k},\ for\ each\ 1 \leq i \leq 2^k.$$

Indeed, σ is an isomorphism. Since H_{2^k} is symmetric, the set S_K can be consider as the set of columns of H_{2^k} as well, and σ can be considered as a permutation of the components of each $a_i^{2^k}$. Since the multiplication is componentwise, σ prevers the operations, and it is an isomorphism. Then our desied isomorphism is

$$\Phi = \phi \circ \sigma.$$

□

2 Construction of Generalized Hadamard matrices

In this section, we start with a preposition and use it to introduced a new class of generalized Hadamard matrix.

Proposition 13. *[1], There is a symmetric GH matrix of type 1 over every finite elementary abelian group G of order p^k.*

Proof. 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.

□

We now focus on Galois field of order 2^k, $GF(2^k)$. For a specific k, the elements of $GF(2^k)$ are polynomails of order less than or equal to $k-1$ with coefficients from $GF(2)$. For each $k \geq 1$, let G_k be the additive group of $GF(2^k)$. Multiplication of the elements in the field is done modulo some primitive polynomial over $GF(2)$.

We can use vector of length k as an expression of elements of $GF(2^k)$ in the following way:

$$v_i^{2^k} = \begin{pmatrix} v_{i1}^{2^k} & v_{i2}^{2^k} & \ldots & v_{ik}^{2^k} \end{pmatrix} \simeq v_{i1}^{2^k} + v_{i2}^{2^k} x + \ldots + v_{i(k-1)}^{2^k} x^{k-2} + v_{ik}^{2^k} x^{k-1} \tag{1}$$

The additive group of $GF(2)$ is isomorphic to the multiplicative group of $\{1, -1\}$ with the usual operation of multiplication. By this isomorphism, 1 is mapped to -1, 0 is mapped to 1, the addition is changed to componentwise multiplication. Thus, the elementary abelian group G_k can be now be seen to consist of elements of the form

$$G_k = \{v_i^{2^k} = \begin{pmatrix} v_{i1}^{2^k} & v_{i2}^{2^k} & \ldots & v_{ik}^{2^k} \end{pmatrix} : \ v_{i1}^{2^k}, v_{i2}^{2^k}, \ldots, v_{ik}^{2^k} \in \{-1, 1\}, \ 1 \leq i \leq 2^k\}$$

, and the operation being pointwise multiplication. It is really useful to make an specific structure for each element of G_k, which is done in the following remark.

Remark 14. *For each $k \geq 1$, the elements of G_k are as followed*

$$G_k = \{0, 1, T, T+1, T^2, T^2+1, T^2+T, \ldots, T^{k-1} + T^{k-2} + \ldots + T + 1\} = \{g_1^{2^k}, \ldots, g_{2^k}^{2^k}\}.$$

Note that in this set, the polynomails have an specific order which is important for us. For two arbitrary distinct polynomails $g_r^{2^k}$ and $g_s^{2^k}$, we have $r < s$ if the degree of polynomail $g_s^{2^k}$ is strictly greater than the degree of $g_r^{2^k}$ or in the case of equality for some $0 \le t \le \deg(g_r^{2^k})(= \deg(g_s^{2^k}))$ we have for each $t < e \le \deg(g_r^{2^k})$ both polynomials $g_r^{2^k}$ and $g_s^{2^k}$ include T^e or both does not include T^e, and $g_s^{2^k}$ includes T^t but $g_r^{2^k}$ does not include T^t. As before, we change this polynomail to vector of lenght k with components from $\{1,-1\}$. Let the following set be the elements of G_k with vector as their expression

$$G_k = \{v_i^{2^k} = \begin{pmatrix} v_{i1}^{2^k} & v_{i2}^{2^k} & \ldots & v_{ik}^{2^k} \end{pmatrix} : \; v_{i1}^{2^k}, v_{i2}^{2^k}, \ldots, v_{ik}^{2^k} \in \{-1,1\}, \; 1 \le i \le 2^k\}$$

, where $v_i^{2^k}$ referes to $g_i^{2^k}$ by the map define in equation (1) in the form of ± 1-vector. Now, we want to apply the order for $v_i^{2^k}$. For two arbitrary vectors $v_r^{2^k}$ and $v_s^{2^k}$, we have $r < s$ if $i_r < i_s$, where i_r and i_s are the largest numbers between 1 and k such that $v_{ri_r}^{2^k}$ and $v_{si_s}^{2^k}$ are equal; or in the case of equality $i_r = i_s$, for some $0 \le t \le i_s$ we have for each $t < e \le i_s$ both $v_{re}^{2^k}$ and $v_{se}^{2^k}$ are equal to -1 , and $v_{st}^{2^k}$ is equal to -1 but $v_{rt}^{2^k}$ is equal to one.

In the following example which is about the construction of $GH(2^3,1)$ over $GF(2^3)$, the ordering menteioned in remark (14) is preserved.

Example 15. *GH matrix constructed over $GF(2^3) = \mathbb{Z}/2\mathbb{Z}[T]/(T^3+T+1)$*
$GF(2^3) = \{0, 1, T, T+1, T^2, T^2+1, T^2+T, T^2+T+1\}$
$G(2^3) = \{(1,1,1), (-,1,1), (1,-,1), (-,-,1), (1,1,-), (-,1,-), (1,-,-), (-,-,-)\}$

Then the multiplication table is as followed.

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

, or

$$\begin{pmatrix}
(1,1,1) & (1,1,1) & (1,1,1) & (1,1,1) & (1,1,1) & (1,1,1) & (1,1,1) & (1,1,1) \\
(1,1,1) & (-,1,1) & (1,-,1) & (-,-,1) & (1,1,-) & (-,1,-) & (1,-,-) & (-,-,-) \\
(1,1,1) & (1,-,1) & (1,1,-) & (1,-,-) & (-,-,1) & (-,1,1) & (-,-,-) & (-,1,-) \\
(1,1,1) & (-,-,1) & (1,-,-) & (-,1,-) & (-,-,-) & (1,1,-) & (-,1,1) & (1,-,1) \\
(1,1,1) & (1,1,-) & (-,-,1) & (-,-,-) & (1,-,-) & (1,-,1) & (-,1,-) & (-,1,1) \\
(1,1,1) & (-,1,-) & (-,1,1) & (1,1,-) & (1,-,1) & (-,-,-) & (-,-,1) & (1,-,-) \\
(1,1,1) & (1,-,-) & (-,-,-) & (-,1,1) & (-,1,-) & (-,-,1) & (1,-,1) & (1,1,-) \\
(1,1,1) & (-,-,-) & (-,1,-) & (1,-,1) & (-,1,1) & (1,-,-) & (1,1,-) & (-,-,1)
\end{pmatrix}$$

It is easy to see that the set $1 \leqslant i \neq j \leqslant 2^k$, $\{h_{il} \cdot h_{jl}^{-1} : 1 \leqslant l \leqslant 2^k\}$ *includes every element of* G_k *once.*

Lemma 16. *For each* $k \geq 1$*, consider two groups*

$$G_k = \{v_i^{2^k} = \begin{pmatrix} v_{i1}^{2^k} & v_{i2}^{2^k} & \dots & v_{ik}^{2^k} \end{pmatrix} : v_{i1}^{2^k}, v_{i2}^{2^k}, \dots, v_{ik}^{2^k} \in \{-1,1\},\ 1 \leq i \leq 2^k\}$$

and

$$UC_k = \{u_i^{2^k}; u_i^{2^k}\ is\ the\ ith\ column\ of\ UG_{2^k}\}.$$

For each i between 1 *and* 2^k*, we have* $v_i^{2^k t} = u_i^{2^k}$*.*

Proof. For each $k \geq 1$, lemma (10) and (11) prove that the elements of two groups G_k and UC_k are the same; i.e., both groups include vectors (or columns) of lenght k having $\{1,-1\}$ as their componenets. To prove the lemma, it is sufficient to show that both groups have the same order for index. Consider two arbitrary elements $v_r^{2^k}$ and $v_s^{2^k}$, we have $v_r^{2^k t} = [u_m^{2^k}]^T$ and $v_s^{2^k t} = [u_n^{2^k}]^T$ for some n and m between 1 and 2^k. If we prove that $r < s$ implies $m < n$, then since r, s, m, *and* n were arbitrary, we are done. Now, suppose $r < s$, then by remark (14), we have two following case:

- $i_r < i_s$, where i_r and i_s are the largest numbers between 1 and k such that $v_{ri_r}^{2^k}$ and $v_{si_s}^{2^k}$ are equal to -1 respectivly; or
- $i_r = i_s$, and for some $0 \leq t \leq i_s$ and each $t < e \leq i_s$, both $v_{re}^{2^k}$ and $v_{se}^{2^k}$ are equal, and $v_{st}^{2^k}$ is equal to -1 but $v_{rt}^{2^k}$ is equal to one.

For the rest of the proof, you should consider the constructure of UG_k. Now, consider the first case. If $i_s = y$, then n should be between $2^{y-1}+1$ and 2^y. Since $i_r < i_s$, we have $m < 2^{y-1}+1$. Hence, $m < n$. For the second case with $i_r = i_s = y$, for t with $0 \leq t \leq i_s$, and for each e between t and i_s, we have both $v_{re}^{2^k}$ and $v_{se}^{2^k}$ are equal. This equality send both m and n to the same partition. We also have $v_{st}^{2^k}$ is equal to -1 but $v_{rt}^{2^k}$ is equal to one. This puts n after m. Hence, $m < n$. □

Result 17. *For each* $k \geq 1$*, there is an isomorphism* Θ *between two groups* G_k *and* UC_k*.*

Proof. For each $k \geq 1$, lemma (10) and (11) prove that the elements of two groups G_k and UC_k are the same; i.e., both groups include vectors (or columns) of lenght k having $\{1,-1\}$ as their componenets. By the order introduced in remark (14), we can define an isomorphism Θ from G_k to UC_k as followed.

$$\Theta(v_i^{2^k}) = v_i^{2^k t} = u_i^{2^k},\ for\ each\ 1 \leq i \leq 2^k.$$

Indeed, this map change a vector or row to a column by using the transpose of the vector or row. This isomorphism is well-defined if the ordering of the set UC_k and G_k are the same. Indeed, because of the structure of UC_k the ordering of the set UC_k and G_k are the same, and this isomorphism is well-defined. □

Result 18. *The group of columns UC_k of UG_{2^k} under pointwise multiplication $*$ is isomorphic to the elementary abelian group G obtained through the construction in 13, also under pointwise multiplication $\odot$.*

Proof. $G = \{v_i : v_i = \{v_{i1}, v_{i2}, \ldots, v_{ik}\}$ where $v_{ij} \in \{-1, 1\}, 1 \le j \le k\}$

The mapping $f : UC_k \to G$, $f(u_i^{2^k}) = v_j : v_{jl} = u_{il}^{2^k}\ \forall 1 \le l \le k$ is well defined, because all the 2^k possibilities of filling up k spaces with 1 and -1 are included in G_k. Each column is mapped to a unique vector so the mapping is one-one. Since $|V_k| = |S_k| = 2^k$, the mapping is onto as well. We now prove that the group operation is preserved over the mapping. Here $\cdot$ represents usual multiplication of real numbers.

For some $i, j:\ 1 \le i, j \le 2^k$
$f(a_i^{2^k} * a_j^{2^k}) = v_x :\ v_{xl} = (a_{il}^{2^k} \cdot a_{jl}^{2^k})\ \forall\ 1 \le l \le k$
Let $f(a_i^{2^k}) = v_y\ for\ some\ 1 \le y \le 2^k$, and $f(a_j^{2^k}) = v_z\ for\ some\ 1 \le z \le 2^k$,then
$v_{yl} = a_{il}^{2^k}\ \forall\ 1 \le l \le k$ and $v_{zl} = a_{jl}^{2^k}\ \forall 1 \le l \le k$, so
$v_{xl} = v_{yl} \cdot v_{zl}\ \forall\ 1 \le l \le k, \Rightarrow v_x = v_y \odot v_z$
$\Rightarrow f(a_i^{2^k} * a_j^{2^k}) = f(a_i^{2^k}) \odot f(a_j^{2^k})$
Hence f is a homomorphism. Thus f is an isomorphism.

□

This isomorphism can be used to obtain $GH(2^k, 1)$ over D_k, using the construction described in Proposition 10.

Now, we want to review an example of the last theorem for the case $k = 3$.

Example 19. *For this case, we have*

$$G = \{[111], [11-], [1-1], [1--], [-11], [-1-], [--1], [---]\}$$

, and the first 3 rows of H'_{2^3} is as follows

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

By the proof of last theorem, we map each element of G_k to one column in S_k. This mapping is an isomorphism.

References

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