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

Sara Sasani, Priya Soundararajan

May 28, 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, denoted by $GH(G, r/s)$ 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. *Two Hadamard matrices H_{2^k}, H'_{2^k} are said to be equivalent to each other if one can be obtained from the other by the following operations:*
(i) Permutation of rows
(ii) Permutation of columns
(iii) Multiplication of a row(column) with -1

Definition 4. *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 5. *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 6. *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.

Lemma 7. *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 8. *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

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

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 9. *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 ones, and is a symmetric matrix. Then,

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

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

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

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 $1 \le i \le 8$. 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 lemma states for each $k \geq 1$, S_k has a subset U_k with k elements, with a specific property.

Lemma 10. *For each $k \geq 1$, 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 $b_i^{2^k} = [(b_i^{2^k})_j]$, $1 \le j \le 2^k$, 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 $i = 1$, $b_1^{2^k} = [(b_1^{2^k})_j] = [-(-1)^j]$.*

$$b_k^{2^k} = \left(\overbrace{1 \quad 1 \quad 1 \quad 1 \quad \ldots}^{2^{k-1}} \overbrace{-1 \quad -1 \quad -1 \quad -1 \quad \ldots}^{2^{k-1}} \right)$$

$$b^{2^k}_{k-1} = \left(\overbrace{1 \quad 1 \quad \dots}^{2^{k-2}} \overbrace{-1 \quad -1 \quad \dots}^{2^{k-2}} \overbrace{1 \quad 1 \quad \dots}^{2^{k-2}} \overbrace{-1 \quad -1}^{2^{k-2}} \right)$$

$$b^{2^k}_{k-2} = \left(\overbrace{1 \quad \dots}^{2^{k-3}} \overbrace{-1 \quad \dots}^{2^{k-3}} \overbrace{1 \quad \dots}^{2^{k-3}} \overbrace{-1 \quad \dots}^{2^{k-3}} \overbrace{1 \quad \dots}^{2^{k-3}} \overbrace{-1 \quad \dots}^{2^{k-3}} \overbrace{1 \quad \dots}^{2^{k-3}} \overbrace{-1 \quad \dots}^{2^{k-3}} \right)$$

$$\vdots$$

$$b^{2^k}_{1} = \left(\overbrace{1 \quad -1 \quad 1 \quad -1 \dots \quad 1 \quad -1 \quad 1 \quad -1}^{\textit{alternating +1's and -1's}} \right)$$

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 $b^{2^1}_1 = [-(-1)^j] = [1, -1] = a^2_2$.
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 $b^{2^1}_1 = [-(-1)^j] = [1, -1, 1, -1] = a^{2^2}_2$, and $b^{2^2}_2 = [(-1)^{q_j}] = [1, 1, -1, -1] = a^{2^2}_3$.
Therefore, $U_2 = \{a^{2^2}_3, a^{2^2}_2\}$.

Assume, for $n = k$, we have $U_k = \{b^{2^k}_1, \dots, b^{2^k}_k\}$ with desired properties. Let $n = k+1$. By the construction of S_k, we have the set $\{(b^{2^k}_1 | b^{2^k}_1), \dots, (b^{2^k}_k | b^{2^k}_k)\}$ is a subset of S_{k+1}. Moreover, for $1 \le i \le k$, we have

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

Hence, we have k elements of U_{k+1}. We also have that the first 2^k components of $b^{2^{k+1}}_{k+1}$ are one, and the rest are minus one. By constructure of S_{k+1}, this element is $b^{2^{k+1}}_{k+1} = a^{2^{k+1}}_{2^k+1} = (a^{2^k}_1 | -a^{2^k}_1)$ which make the last element of U_{k+1}. □

The rows of the Hadamard matrix H_{2^k} are permuted to obtain an equivalent Hadamard matrix $H^{'}_{2^k}$, such that the i^{th} row of $H^{'}_{2^k}$ is $b^{2^k}_i$. We use $S^{'}_k$ to denote the group of columns of $H^{'}_{2^k}$.

Lemma 11. *The first k elements of any two columns in the group $S^{'}_k$ are distinct.*

Proof. For the sake of clarity, we can impose an order on the elements of $S^{'}_k$. The i^{th} column of $H^{'}_{2^k}$ is expressed as $a^{'2^k}_i$ for each i, $1 \le i \le k$.
We want to prove that if $1 \le r \ne s \le 2^k$, $(a^{'2^k}_r)_j \ne (a^{'2^k}_s)_j$ for atleast one j, $1 \le j \le k$.

Toward a contradiction, suppose $r \neq s$ but $(a_r^{\prime 2^k})_j = (a_s^{\prime 2^k})_j$ for each $1 \leq j \leq k$.
$(a_r^{\prime 2^k})_k = (a_s^{\prime 2^k})_k \;\Rightarrow\; 1 \leq r\ ,\ s \leq 2^{k-1}$ or $2^{k-1}+1 \leq r\ ,\ s \leq 2^k$.
With out loss of generality, suppose $1 \leq r\ ,\ s \leq 2^{k-1}$.
Then, $(a_r^{\prime 2^k})_{k-1} = (a_s^{\prime 2^k})_{k-1} \;\Rightarrow\; 1 \leq r\ ,\ s \leq 2^{k-2}$ or $2^{k-2}+1 \leq r\ ,\ s \leq 2^{k-1}$.
With out loss of generality, suppose $1 \leq r\ ,\ s \leq 2^{k-2}$.
Continuing this way,
Since $(a_r^{\prime 2^k})_1 = (a_s^{\prime 2^k})_1$, we have $1 \leq r\ ,\ s \leq 2^{k-k} = 1$.

This is a contradiction because we have assumed that $r \neq s$. Hence, the first k elements of any two columns in $S_k^{'}$ are distinct. □

2 Construction of Generalized Hadamard matrices

A method presented in [1] illustrates a construction for $GH(G,n)$, where G is an elementary abelian group. This method can be extended by an isomorphism described in Proposition 15 construct a $GH(G,1)$, where G is the elementary abelian group of columns of a Hadamard matrix , $S_k^{'}$.

Proposition 12. *[1], There is a symmetric GH matrix of type 1 over every finite elementary abelian group G of order p^k, where p is a prime.*

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 polynomials of order less than or equal to $k-1$ with coefficients from $GF(2)$.
Addition is pointwise and multiplication is done modulo some primitive polynomial over $GF(2)$.
For each $k \geq 1$, let G_k denote the additive group of $GF(2^k)$.

$$G_k = \{v_i \;=\; v_{i1} + v_{i2}T + \ldots v_{ik}T^{k-1} | v_{ij} \in \{0,1\}\ \forall j, 1 \leq j \leq k\}$$

Addition of two polynomials v_i and v_j is defined as,

$$v_i + v_j = (v_{i1} + v_{j1}) + (v_{i2} + v_{j2})T + \ldots (v_{ik} + v_{jk})T^{k-1}$$

Remark 13. *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, and addition is changed to multiplication. G_k obtains another representation through the use of this isomorphism as:*

$$G_k = \{v_i \; = \; v_{i1} + v_{i2}T + \ldots v_{ik}T^{k-1} | v_{ij} \in \{-1,1\} \; \forall j, 1 \leq j \leq k\}$$

with the operation being pointwise multiplication, denoted by $\odot$,

$$v_i \odot v_j = (v_{i1} \cdot v_{j1}) + (v_{i2} \cdot v_{j2})T + \ldots (v_{ik} \cdot v_{jk})T^{k-1}$$

This representation of G_k finds use in the next proposition. Before that, we view an example of the construction.

Example 14. *GH matrix constructed over the additive group of $GF(2^3) = \mathbb{Z}/2\mathbb{Z}[T]/(T^3+T+1)$*
$GF(2^3) = \{0, 1, T, T+1, T^2, T^2+1, T^2+T, T^2+T+1\}$
$G_3(2^3) = \{(1+T+T^2), (-1+T+T^2), (1-T+T^2), (-1-T+T^2), (1+T-T^2), (-1+T-T^2), (1-T-T^2), (-1-T-T^2)\}$

The multiplication table for $GF(2^3)$:

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

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.

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

Proposition 15. *There is an isomorphism between the elements of the group $S_k^{'}$, with the operation of pointwise multiplication $*$, and the elementary abelian group G_k, also with the operation of pointwise multiplication $\odot$ formed using 12.*

Proof. Consider the mapping,

$$f : S_k^{'} \longrightarrow G_k$$
$$a_i^{'2^k} \mapsto (a_i^{'2^k})_1 \ + \ (a_i^{'2^k})_2 T^1 \ + \ (a_i^{'2^k})_3 T^2 \ldots (a_i^{'2^k})_k T^{k-1}$$

From *remark 13*, the mapping is well defined. To show that it is one-one, let
$f(a_i^{'2^k}) = f(a_j^{'2^k})$ for some $1 \leq i \neq j \leq 2^k$.
$\Rightarrow (a_i^{'2^k})_r = (a_j^{'2^k})_r$, for all $1 \leq r \leq k$.
Using *lemma 11*, $a_i^{'2^k} = a_j^{'2^k}$. Thus it is injective.
The number of elements in $S_k^{'}$ and G is 2^k, hence it is onto in addition to being one-one.
To show that the mapping is a homomorphism,

$$f(a_i^{'2^k} * a_j^{'2^k}) = ((a_i^{'2^k})_1 \cdot (a_j^{'2^k})_1) \ + \ ((a_i^{'2^k})_2 \cdot (a_j^{'2^k})_2) T^1 \ + \ldots ((a_i^{'2^k})_k (a_j^{'2^k})_k) T^{k-1}$$
$$= ((a_i^{'2^k})_1 \ + \ (a_i^{'2^k})_2 T^1 \ + \ldots (a_i^{'2^k})_k T^{k-1}) \odot ((a_j^{'2^k})_1 \ + \ (a_j^{'2^k})_2 T^1 \ + \ldots (a_j^{'2^k})_k T^{k-1})$$
$$= f(a_i^{'2^k}) \odot f(a_j^{'2^k})$$

$\Rightarrow$, the above arguments prove that f is an isomorphism. □

References

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