Filomat 34:3 (2020), 815–834
https://doi.org/10.2298/FIL2003815F

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

An Infinite Family of Hadamard Matrices Constructed From Paley Type Matrices

Adda Farouk[a], Qing-Wen Wang[a]

[a]*International Research Center for Tensors and Matrix Theory of Shanghai University. 99 Shangda Road, Shanghai, 200444, P.R. China.*

Abstract. An $n \times n$ matrix whose entries are from the set $\{1, -1\}$ is called a Hadamard matrix if $HH^\top = nI_n$. The Hadamard conjecture states that if n is a multiple of four then there always exists Hadamard matrices of this order. But their construction remain unknown for many orders. In this paper we construct Hadamard matrices of order $2q(q+1)$ from known Hadamard matrices of order $2(q+1)$, where q is a power of a prime number congruent to 1 modulo 4. We show then two ways to construct them. This work is a continuation of U. Scarpis' in [7] and Dragomir-Ž. Dokovič's in [10].

1. Introduction

Hadamard matrices can be defined as $\{1, -1\}$ matrices for which the inner product of any pair of distinct rows (or columns respectively) is 0. There are many applications in signal processing, coding, cryptography, etc (see [1]). Finding Hadamard matrices has been an elusive problem which has remained unsolved for one and a half century, and was discussed by many mathematicians. J.J. Sylvester was the first to define such matrices in 1839 [16] of orders $2^m, m \in \mathbb{N}$, using Kronecker products. Then J.S. Hadamard proved the existence of such matrices of orders $n = 2$ and $n = 4k$, for every $k \in \mathbb{N}^*$. But no construction is known for all possible orders.

Many mathematicians have attempted to solve this problem. For instance, Paley constructed them using finite fields $\mathbb{F}_q$ for $n = q + 1$ or $n = 2(q + 1)$ when $q \equiv 3(mod\ 4)$, $q \equiv 1(mod\ 4)$, respectively (see [2, 9]). J. Williamson, J.M. Goethales and J.J. Seidel constructed Hadamard matrices for different orders (see [13, 14]). Using *Orthogonal designs* (see [4]), the constructions of Williamson and Goethales and Seidel led to the obtainment of many orders of Hadamard matrices. Latest orders revealed are 1004 in [11] and 764 in [12]. U. Scarpis, by using Hadamard matrices of order $n = p + 1$ with $p \equiv 3(mod\ 4)$ a prime number, constructed a larger matrix of order pn in [7, 8]. This work was generalized by Dragomir-Ž. Dokovič in [10] recently.

Hadamard matrices are invariant under row or column permutations as well as multiplication by -1. Thus, they are partitioned naturally into equivalence classes, each containing a *normalised Hadamard matrix* (a Hadamard matrix whose first row and column consist of 1's only). However, the classification of

2010 *Mathematics Subject Classification*. 15B34; 05B20
Keywords. Hadamard matrices, Scarpis constructions, Paley constructions.
Received: 06 November 2019; Revised: 21 November 2019; Accepted: 05 December 2019
Communicated by Dragana Cvetković Ilić
Corresponding author: Qing-Wen Wang
This research is supported by the Natural Science Foundation of China (11971294, 11571220).
Email addresses: adda-farouk@hotmail.com (Adda Farouk), wqw@t.shu.edu.cn (Qing-Wen Wang)

Hadamard matrices by equivalence has been a considerable challenge. Hadamard matrices have been constructed, but complete lists are available only for a few small orders. There is only one equivalence class for Hadamard matrices of sizes $n = 1, 2, 4, 8, 12$, five equivalence classes for $n = 16$, three for $n = 20$, 60 for $n = 24$ and 487 for $n = 28$ (see [6, 15]). From the lower bound $n = 40$ the number grows rapidly (see [17, 18]).

This paper aims to construct a family of Hadamard matrices of size $2q(q + 1)$ from a known Hadamard matrix of size $2(q + 1)$, where q is a power of a prime number $q \equiv 1(mod\ 4)$.

The rest of this paper is organized as follows. In Section 2, we construct a qn-Hadamard matrix where q is a power of a prime number congruent to 1 modulo 4 and $n = 2(q + 1)$. In Section 3, we give a matrix-like form to Scarpis constructions by the use of permutations matrices. This construction is of complexity at most $O(t^3)$, where t is the prime power. We show that Scarpis Hadamard matrices may be different under a choice of bijections. In the last section, we give a conclusion and propose an open problem.

Now we recall some definitions and notations. We denote the set of all $n \times n$ Hadamard matrices by $\mathcal{H}_n$. The i-th row of a matrix A is denoted by $\mathbf{a}_i$. $A^\top$ denotes the transpose matrix of A.

Two vectors are orthogonal if their inner product (or dot product) is 0 (i.e., taking $\mathbf{x} = (x_i), \mathbf{y} = (y_i)$ two vectors of same size $1 \times n$, they are orthogonal if $< \mathbf{x}, \mathbf{y} >:= \sum_{i=1}^{n} x_i y_i = \mathbf{x}\mathbf{y}^\top = 0$).

The Kronecker (or tensor) product $X \otimes Y$ of two matrices $X = (x_{ij})$ and Y is the block matrix $X \otimes Y = (x_{ij}Y)$. $\mathbf{J}_m$ denotes the row vector whose m entries are 1. $O_{m,p}$ is the zero matrix of size $m \times p$, and I_n is the identity matrix of order n. For two matrices A and B, we define that

$$A \oplus B := \begin{bmatrix} A & O \\ O & B \end{bmatrix}.$$

By deleting the first row and column of a *normalized Hadamard matrix* H, we obtain a matrix where the inner product of every two of its rows (or columns resp) gives -1. This matrix is called the *Core* of H.

Let α be the bijection

$$\alpha : \{1, 2, ..., q\} \to \mathbb{F}_q$$

such that, $\mathbf{a}(x)$ represents the t-th row $\mathbf{a}_t$ of the matrix A whenever $x = \alpha(t)$.
Throughout l, q denote two prime powers such that $l \equiv 3(mod\ 4)$, $q \equiv 1(mod\ 4)$, respectively, and $n = 2(q + 1)$ for the rest of this paper.
In [10] Dragomir-Ž.Dokovič considers transformations, which we denote by $\Phi_{l,\alpha}$, to define the $l(l + 1)$-Hadamard matrices. It can also be presented as

$$\Phi_{l,\alpha} : \mathcal{H}_{l+1} \to \mathcal{H}_{l(l+1)}$$

and $\Phi_{l,\alpha}(H)$ is a $l(l + 1)$-Hadamard matrix.

Note that the multiplicative group of permutation matrices of size n, is group isomorphic to the symmetric group $\mathbb{S}_n$ by corresponding to each $\pi \in \mathbb{S}_n$ the permutation matrix $P_\pi = [\delta(\pi(i), j)]$, where

$$\delta(i, j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}.$$

It is generated by transposition matrices which are permutations that switch only two rows (or two columns). On the other hand, $\mathbb{S}_n$ can also be represented as the group of all bijections from $\mathbb{F}_d$ to $\mathbb{F}_d$ equiped with morphisms composition law, when d is a power of a prime number.

2. Construction of *qn*-Hadamard Matrices

In this section, we first recall Paley's Theorem which is used as a generator of input matrices used in this construction, then we construct a *qn*-Hadamard Matrix.

A quadratic character χ is a map defined on the cyclic group $\mathbb{F}_q^*$ by $\chi(x) = 1$ if x is quadratic residue (i.e., there exists $y \in \mathbb{F}_q^*$ such that $y^2 = x$) and $\chi(x) = -1$ otherwise. It's extended to $\mathbb{F}_q$ by setting $\chi(0) = 0$.

Theorem 2.1 (Paley). *For q an odd prime power, and an ordering $g_0 = 0, g_1, ..., g_{q-1} \in \mathbb{F}_q$ of $\mathbb{F}_q$, set $Q = \chi[(g_i - g_j)]_{0\le i,j\le q}$. Let S be a matrix of the form*

$$S = \begin{bmatrix} 0 & \mathbf{1} \\ \mathbf{1}^\top & Q \end{bmatrix}$$

where $\mathbf{1}$ is the all-1s string. Then we have the following:

(1) *If $q \equiv 3 (mod\ 4)$, then*

$$P_q = \begin{bmatrix} 1 & \mathbf{1} \\ \mathbf{1}^\top & Q + I_q \end{bmatrix}$$

is a Hadamard matrix of order $(q + 1)$ called the Paley Type I Hadamard matrix.

(2) *If $q \equiv 1 (mod\ 4)$, then*

$$P'_q = \begin{bmatrix} S + I_{q+1} & S - I_{q+1} \\ S - I_{q+1} & -S - I_{q+1} \end{bmatrix}$$

is a Hadamard matrix of order $2(q + 1)$ called the Paley Type II Hadamard matrix.

Note that Q is skew-symmetric ($Q^\top = -Q$) when $q \equiv 3 (mod\ 4)$ and symmetric when $q \equiv 1 (mod\ 4)$.

In [10] the author uses *Core* rows for the construction, in such way that any Hadamard matrix of order $l+1$ can be used as an input matrix. But here, Core rows are incompatible to the construction, then we need to use a sub-matrix extracted from it. This last sub-matrix must verify some conditions and therefore it is extracted from a particular Hadamard matrix. In the following lemmas, we will discuss the nature of such Hadamard matrices, by giving the conditions and by describing their existence.

Lemma 2.1. *For every normalized Hadamard matrix $H = (h_{ij})$ of order n there exists an equivalent normalized Hadamard matrix $H' = (h'_{ij})$ containing a row i (or a column j resp)of the form $(1, -1, 1, ..., 1, -1, ..., -1)$.*

Proof. By [8] every row or column of H differs in $\frac{n}{2}$ position except the first row (or column resp) so there are as many 1s in every such row or column as -1s. Then, applying at most $n - 1$ permutations on rows (or columns resp) we can obtain H'. □

Lemma 2.2. *Let $q \equiv 1 (mod\ 4)$ a power of a prime number. Then there exists a normalized Hadamard matrix of order $2(q + 1)$ with second column $(1, -1, 1, ..., 1, -1, ..., -1)$ and satisfies the following:*

(1) By deleting the first two rows and columns respectively and using a column permutation N, we get a matrix $T = \begin{bmatrix} C \\ D \end{bmatrix}$ such that C and D are of size $q \times 2q$ satisfying the following:

i. For each row of C, the sum of the first q entries is -1, and the sum of the remaning q entries is also -1.

ii. For each row of D, the sum of the first q entries is 1, and the sum of the remaning q entries is -1.

(2) *We denote by* $\overline{T}$ *the matrix obtained by deleting the first two rows only. Then, there exists a column permutation matrix* M *that rearranges the rows of* $\overline{T}$ *in such away that any two consecutive entries appear as the elements of the set* $\mathcal{A} = \{(1,1),(-1,-1),(1,-1),(-1,1)\}$*, where each row contains as many* $(1,1)$*s as* $(-1,-1)$*s and as many* $(-1,1)$*s as* $(1,-1)$*s.*

Proof. It follows from Theorem 1 that we can construct the following matrix

$$P'_q = \begin{bmatrix} 1 & 1 & \mathbf{J}_q & \mathbf{J}_q \\ 1 & -1 & -\mathbf{J}_q & \mathbf{J}_q \\ \mathbf{J}_q{}^\top & \mathbf{J}_q{}^\top & Q - I_q & -Q - I_q \\ \mathbf{J}_q{}^\top & -\mathbf{J}_q{}^\top & Q + I_q & Q - I_q \end{bmatrix}.$$

By deleting its first two rows and columns we obtain

$$T = \begin{bmatrix} Q - I_q & -Q - I_q \\ Q + I_q & Q - I_q \end{bmatrix}.$$

The quadratic character gives as many 1s as −1s over any finite field. Then, the statement i. follows from the first q rows of T and the statement ii. follows from the second respectively, and $N = I_{2q}$. We obtain consequently the first result.
By deleting the first two rows of P'_q we obtain

$$\overline{T} = \begin{bmatrix} \mathbf{J}_q{}^\top & \mathbf{J}_q{}^\top & Q - I_q & -Q - I_q \\ \mathbf{J}_q{}^\top & -\mathbf{J}_q{}^\top & Q + I_q & Q - I_q \end{bmatrix}.$$

Now, we multiply $\overline{T}$ by a column permutation matrix that puts every $(i+2)$-th column side to the $(q+i+1)$-th column, when $i \in \{1,..,q\}$. Let's denote the resulted matrix by H'. As the quadratic character gives as many 1s as −1s, then H' contains as many $(-1,1)$s as $(1,-1)$s, one $(1,1)$ and one $(-1,-1)$ in every row of the first q rows, as many $(1,1)$s as $(-1,-1)$s, one $(1,-1)$ and one $(-1,1)$ in every row of the last q rows. Hence, the second result of the lemma follows. Therefore, P'_q satisfies (1) and (2) of Lemma 2. □

We describe a procedure whose input is a Hadamard matrix A of order $n = 2(q+1)$ that satisfies (1) and (2) of Lemma 2, and output is a Hadamard matrix B of order qn. So, we obtain

$$\Psi_{q,\alpha} : \overline{\mathcal{H}}_n \to \mathcal{H}_{qn}$$

where $\overline{\mathcal{H}}_n$ is the set of all Hadamard matrices of order n that satisfies the conditions in Lemma 2. $\Psi_{q,\alpha}$ generates a family of Hadamard matrices which depends on variation of the bijections α, and whose orders depend on variation of q prime powers. Thus, we obtain the following.

Theorem 2.2 (*qn*-Hadamard construction). *Let* $q \equiv 1 (mod\ 4)$ *be a prime power. Suppose that an order* $n = 2(q+1)$ *Hadamard matrix* A *satisfies the properties of Lemma 2. Then there exists a Hadamard matrix of order* $qn = 2q(q+1)$.

Proof. The proof includes two parts. We first show how to construct a square matrix noted here by B from the given Hadamard matrix A of order n. Then we show that B satisfies row orthogonality requirement (Columns orthogonality requirement can be obtained evidently since if $BB^\top = qnI_{qn}$, then $B^\top B = qnI_{qn}$).

Matrix construction:

Step 1. Let A be a Hadamard matrix of size $2(q+1) \times 2(q+1)$ with $a_{11} = 1$, if not, we take $-A$ and let $\mathbf{J}$ be a row vector that consists of q ones.

Step 2. For each $i = \{2,3,...,n\}$ if $a_{1i} = -1$, we multiply the column i by -1. Then, we obtain a first row of ones similarly if $a_{i1} = -1$. Hence, we obtain an equivalent normalized matrix A'.

Step 3. Permuting A' rows, we obtain A'' a normalized Hadamard matrix with the second column $(1,-1,1,...,1,-1,...,-1)$ as shown in Lemma 1.

Step 4. The matrix obtained by deleting first two rows of A'' is $\overline{T}$. We define

$$B_0 = \overline{T}M \otimes \mathbf{J},$$

where M is the permutation matrix from (2) of Lemma 2.

Step 5. By deleting the first two columns of $\overline{T}$ we obtain a matrix T'. Using the permutation matrix N defined as in (1) of Lemma 2, we get a matrix $T = T'N$ of size $2q \times 2q$. We divide T into C, the first q rows and D, the last q rows. The inner product of two rows of C (or two rows of D resp) is -2. While, the inner product of one row of C and another from D is 0.

Step 6. We partition B into $q+1$ block matrices of sizes $2q \times qn$

$$B = \begin{bmatrix} B_0 \\ B_1 \\ . \\ . \\ . \\ B_q \end{bmatrix}.$$

Then, for each $r \in \{1,2,...,q\}$ we partition B_r into $2n$ blocks of size $q \times q$ such that

$$B_r = \begin{bmatrix} {B^{[1]}}_{r,0} & {B^{[1]}}_{r,1} & ... & {B^{[1]}}_{r,q} \\ {B^{[2]}}_{r,0} & {B^{[2]}}_{r,1} & ... & {B^{[2]}}_{r,q} \end{bmatrix}.$$

Let ${B^{[1]}}_{r,0} = \mathbf{J}^T \otimes \mathbf{c}_r$ and ${B^{[2]}}_{r,0} = \mathbf{J}^T \otimes \mathbf{d}_r$. Next we define ${B^{[1]}}_{r,i}$, ${B^{[2]}}_{r,i}$ for $i \in \{1,2,...,q\}$.

Step 7. For each r, i, we specify the rows of the block matrices ${B^{[1]}}_{r,i}$ and ${B^{[2]}}_{r,i}$ as follows.

- rows of ${B^{[1]}}_{r,i}$ will be $\mathbf{c}(\alpha_i\alpha_r + \alpha_k)$ with $k \in \{1,2,...,q\}$,
- rows of ${B^{[2]}}_{r,i}$ will be $\mathbf{d}(\alpha_i\alpha_r + \alpha_k)$ with $k \in \{1,2,...,q\}$.

This completes the definition of B of size $2q(q+1) \times 2q(q+1)$.

Orthogonality verification:

1. Two distinct rows of B_0 are orthogonal by the fact that the tensor product preserves rows orthogonality.
2. If we take two distinct rows of B_r, then we must investigate 3 different cases.

   (i) Two rows l, k from ${B^{[1]}}_r$, the dot product gives

   $$\mathbf{c}_r{\mathbf{c}_r}^\top + \sum_{t=1}^{q} \mathbf{c}(\alpha_i\alpha_r + \alpha_k)\mathbf{c}(\alpha_i\alpha_r + \alpha_l)^\top = 2q - 2q = 0.$$

   Because, $\mathbf{c}_i{\mathbf{c}_j}^\top = -2$, if $i \neq j$, and multiplying a row by itself give its length $2q$. The verification is similar if they are taken from ${B^{[2]}}_r$.

   (ii) Taking the l-th row of ${B^{[1]}}_r$ and the k-th row of ${B^{[2]}}_r$, we have

   $$\mathbf{c}_l{\mathbf{d}_k}^\top + \sum_{t=1}^{q} \mathbf{c}(\alpha_i\alpha_r + \alpha_k)\mathbf{d}(\alpha_i\alpha_r + \alpha_l)^\top = 0,$$

   by the construction of T.

3. A row of B_0 and another from B_r, $r \neq 0$:
   k-th row of B_0 has the form $[\bar{\mathbf{t}}_k \otimes \mathbf{J}]$ and the a-th row of B_r has the form

$$[\mathbf{c}_r \ \mathbf{c}(\alpha_1\alpha_r + \alpha_b) \ ... \ \mathbf{c}(\alpha_q\alpha_r + \alpha_b)] \tag{1}$$

   or

$$[\mathbf{d}_r \ \mathbf{d}(\alpha_1\alpha_r + \alpha_b) \ ... \ \mathbf{d}(\alpha_q\alpha_r + \alpha_b)], \tag{2}$$

   where $b = a(mod\ q) + 1$.

   Considering (2.1), the inner product of the two rows is the result of summing the terms obtained from the following:

$$\bar{t}_{k\,1}\sum_{u=1}^{q} c_{r\,u} + \bar{t}_{k\,2}\sum_{u=q+1}^{2q} c_{r\,u} = -(\bar{t}_{k\,1} + \bar{t}_{k\,2}).$$

   For $0 < v < q$,

$$\bar{t}_{k\,2v+1}\sum_{u=1}^{q}[\mathbf{c}(\alpha_v\alpha_r + \alpha_b)]_u + \bar{t}_{k\,2v+2}\sum_{u=q+1}^{2q}[\mathbf{c}(\alpha_v\alpha_r + \alpha_b)]_u = -(\bar{t}_{k\,2v+1} + \bar{t}_{k\,2v+2}).$$

   Here, $[\mathbf{c}(\alpha_i\alpha_r + \alpha_l)]_u$ are components of the row $\mathbf{c}(\alpha_i\alpha_r + \alpha_l)$, and we obtain $-(\bar{t}_{k\,1} + \bar{t}_{k\,2}), -(\bar{t}_{k\,3} + \bar{t}_{k\,4}), ..., -(\bar{t}_{k\,2q+1} + \bar{t}_{k\,2q+2})$. In sum, we get $-\sum_{v=1}^{n}\bar{t}_{k\,v} = 0$, and hence, the orthogonality is shown.
   Similarly, considering (2.2) we have

$$\bar{t}_{k\,1}\sum_{u=1}^{q} d_{l\,u} + \bar{t}_{k\,2}\sum_{u=q+1}^{2q} d_{l\,u} = \bar{t}_{k\,1} - \bar{t}_{k\,2}$$

   and for $0 < v < q$:

$$\bar{t}_{k\,2v+1}\sum_{u=1}^{q}[\mathbf{d}(\alpha_v\alpha_r + \alpha_b)]_u + \bar{t}_{k\,2v+2}\sum_{u=q+1}^{2q}[\mathbf{d}(\alpha_v\alpha_r + \alpha_b)]_u = \bar{t}_{k\,2v+1} - \bar{t}_{k\,2v+2}$$

   yielding the terms $(\bar{t}_{k\,1} - \bar{t}_{k\,2}), (\bar{t}_{k\,3} - \bar{t}_{k\,4}), ..., (\bar{t}_{k\,2q+1} - \bar{t}_{k\,2q+2})$. If $\bar{t}_{k\,2v+1} = -\bar{t}_{k\,2v+2} = 1$, the v-th term has the value 2, if $\bar{t}_{k\,2v+1} = -\bar{t}_{k\,2v+2} = -1$, then it yields -2. But by part 2 of Lemma 2, we have as many $(1, -1)$s as $(-1, 1)$s. Therefore, the inner product of the two rows is zero, i.e,

$$\sum_{v=0}^{q}\bar{t}_{k\,2v+1} - \sum_{v=1}^{q+1}\bar{t}_{k\,2v} = 0$$

   implying the orthogonality follows.

4. Lastly, a row from B_r and another from B_s with $r, s \neq 0$ and $r \neq s$:

   (i) If one is from $B^{[1]}{}_r$ and another from $B^{[2]}{}_s$, the inner product of the two rows is equal to

$$\mathbf{c}_r\mathbf{d}_s{}^{\top} + \sum_{t=1}^{q}\mathbf{c}(\alpha_t\alpha_r + \alpha_k)\mathbf{d}(\alpha_t\alpha_s + \alpha_l)^{\top},$$

   the result evidently is 0 (as mentioned in **Step 5.**).

(ii) If they are from the same upper indexed block $B^{[1]}$, the product gives

$$\mathbf{c}_r\mathbf{c}_s{}^{\top} + \sum_{t=1}^{q} \mathbf{c}(\alpha_t\alpha_r + \alpha_k)\mathbf{c}(\alpha_t\alpha_s + \alpha_l)^{\top}$$

For every $t \in \{1, ..., q\}$, the product $\mathbf{c}(\alpha_t\alpha_r + \alpha_k)\mathbf{c}(\alpha_t\alpha_s + \alpha_l)^{\top}$ is equal to -2 except in one case t' such that $\alpha_{t'} = (\alpha_l - \alpha_k)(\alpha_r - \alpha_s)^{-1}$ where it is equal to $2q$. Thus, the total sum is equal to zero (as in case 2. (i)). Similar computations are concluded considering two rows of $B^{[2]}$.

We have shown that B is qn-Hadamard matrix, and this completes the proof. □

By using Paley's type II Hadamard matrices P'_q we can always find an input Hadamard matrix of size $2(q + 1)$. Therefore, we obtain the following Corollary.

Corollary 2.1. *Suppose that $q \equiv 1(mod\ 4)$ is a prime power. Then there exists a Hadamard matrix of size $2q(q + 1)$.*

3. Other Form for Scarpis Hadamard matrices

In this section we propose another matrix shape of Scarpis constructions when $q \equiv 1(mod\ 4)$ or $l \equiv 3(mod\ 4)$. It is much easier to implement on programming devices, as it's based on rows permutations of the input matrix, insertion of matrices of orders less or equal to the order of the input matrix, and the computation of powers of a generator over a finite field. Hence, the construction is of a complexity that do not exceed $O(m^3)$, where $m \in \{l, q\}$.

We start by defining the shift permutation matrix:

$$U_d = \begin{bmatrix} 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & ... & \vdots \\ 1 & 0 & 0 & & 0 \end{bmatrix}.$$

U_d is of order d, and ${U_d}^d = I_d$.

Let's take the bijection α as:

$$\alpha(i) = \begin{cases} 0 & if \quad i = 1, \\ \gamma^{i-1} & if \quad i \in \{2, ..., l\}(or\{2, ...q\}) \end{cases}$$

where γ is a primitive root of the unity of $\mathbb{F}_l$ (or $\mathbb{F}_q$ respectively).

When l (or q) is a prime number, the field $\mathbb{F}_l$ (or $\mathbb{F}_q$) is the same as the quotient ring $\mathbb{Z}/l\mathbb{Z} = \{0, 1, 2, .., l-1\}$ (or $\mathbb{Z}/q\mathbb{Z} = \{0, 1, 2, .., q-1\}$, respectively). Therefore, we can define the matrix

$$V_l = \begin{bmatrix} \delta(\alpha(i) + 1, j) \end{bmatrix},$$

where V_l is the permutation matrix correspond to α, taking α as a permutation of $\{0, ..., l-1\}$. Similarly, we define V_q.

On the other hand, if $l = p^d$ (a power $d \neq 1$ of a prime number p), then the field $\mathbb{F}_l$ is isomorphic to $\mathbb{F}_p[z]/\langle f\rangle$ by a field homomorphism $s(x) = f_x(z)$, where $\mathbb{F}_p[z]$ is the polynomial ring over $\mathbb{F}_p$, and $\langle f\rangle$ is the ideal generated by an irreducible polynomial f of degree d (see Chapter 2 in [3]). We define the set mapping

$$t: \begin{array}{ccc} \mathbb{F}_p[z]/\langle f\rangle & \rightarrow & \mathbb{Z}/l\mathbb{Z} \\ f_x(z) & \rightarrow & f_x(p) \end{array}.$$

Clearly, t is a bijection. If we take $a_0, a_1, ..., a_{d-1} \in \mathbb{F}_p$, then $\sum_{i=0}^{d-1} a_i p^i = 0$ implies that the a_is are all identical to 0, then the injectivity follows, and so, surjectively (as the two sets have the same cardinality).
Taking $\Delta(i) = t \circ s \circ \alpha(i)$, we define the permutation matrix correspond to α by

$$V_l = \left[\ \delta(\Delta(i) + 1, j) \ \right].$$

In the same way we can define V_q when $q = p'^{d'}$, respectively.

Using these matrices and a Hadamard matrix of order $(l + 1)$ or $2(q + 1)$ we can define Scarpis matrix. We elaborate the constructions of the new form in the following proposition.

Proposition 3.1. *Let H be a normalized Hadamard matrix. Then the following holds:*

(1) For $l \equiv 3 (mod\ 4)$ a prime power, H of size $l + 1$, has a Core C. Taking

$$B_0 = H' \otimes \mathbf{J}_l,$$

where H' is the matrix obtained by deleting the first row of H, and

$$B = \left[\begin{array}{c|c|ccc} & \mathbf{J}_l{}^\top \otimes \mathbf{c}_1 & S_lC & ... & S_l{}^{l-2}C & C \\ & \mathbf{J}_l{}^\top \otimes \mathbf{c}_2 & S_lU_lC & ... & S_l{}^{l-2}U_lC & U_lC \\ \mathbf{J}_l{}^\top \otimes C & \vdots & \vdots & \vdots & ... & \vdots \\ & \mathbf{J}_l{}^\top \otimes \mathbf{c}_l & S_lU_l{}^{l-1}C & ... & S_l{}^{l-2}U_l{}^{l-1}C & U_l{}^{l-1}C \end{array}\right]$$

where $S_l = V_l{}^{-1}(1 \oplus U_{l-1})V_l$.Then,

$$\Phi = \left[\begin{array}{c} B_0 \\ B \end{array}\right]$$

is a Hadamard matrix of order $l(l + 1)$.

(2) For $q \equiv 1 (mod\ 4)$ a prime power, H is of order $2(q+1)$ whose second column is in the form $(1, -1, 1, ..., 1, -1, ..., -1)$. Then if H verifies (1) and (2) of Lemma 2 for some permutation matrices N and M, respectively, the matrix:

$$\Psi = \left[\begin{array}{c} B'_0 \\ B' \end{array}\right]$$

where $B'_0 = \overline{T}M \otimes \mathbf{J}_q$, with $\overline{T}$ the matrix obtained by deleting the first two rows of H, and

$$B' = \left[\begin{array}{c|c|ccc} & \widetilde{T}_1 & \widetilde{S}_qT & ... & \widetilde{S}_q{}^{q-2}T & T \\ & \widetilde{T}_2 & \widetilde{S}_q\widetilde{U}_qT & ... & \widetilde{S}_q{}^{q-2}\widetilde{U}_qT & \widetilde{U}_qT \\ \mathbf{J}_q{}^\top \otimes T & \vdots & \vdots & \vdots & ... & \vdots \\ & \widetilde{T}_q & \widetilde{S}_q\widetilde{U}_q{}^{q-1}T & ... & \widetilde{S}_q{}^{q-2}\widetilde{U}_q{}^{q-1}T & \widetilde{U}_q{}^{q-1}T \end{array}\right]$$

where $\widetilde{U_q} = I_2 \otimes U_q$, $\widetilde{S}_q = I_2 \otimes (V_q{}^{-1}(1 \oplus U_{q-1})V_q)$, $T = T'N$ such that, T' is the matrix obtained by deleting the first two rows and columns of H, and $\widetilde{T}_i = \begin{pmatrix} \mathbf{J}_q{}^\top \otimes \mathbf{t}_i \\ \mathbf{J}_q{}^\top \otimes \mathbf{t}_{q+i} \end{pmatrix}$, is a Hadamard matrix.

Proof. We prove the first case of the proposition, and the second case can be concluded similarly. Using a construction obtained via the bijection α, we denote by $\overline{B}$ the matrix

$$\left[\begin{array}{c} B_1 \\ \vdots \\ B_l \end{array}\right] \tag{3}$$

constructed as in Theorem 1 in [10]. The first form above is revealed using rows permutations on $\overline{B}$. We permute the rows of $\overline{B}$ in a way to obtain

$$\widehat{B} = \begin{bmatrix} \Gamma_1 \\ \vdots \\ \Gamma_l \end{bmatrix} \tag{4}$$

where each Γ_k is a $l \times l(l+1)$ matrix of rows $[\mathbf{c}_r \ \mathbf{c}(\alpha_1\alpha_r + \alpha_k) \ ... \ \mathbf{c}(\alpha_q\alpha_r + \alpha_k)]$ with $r \in \{1, ..., l\}$. Thus we have, for $k = 1$:

$$\Gamma_1 = \left[\begin{array}{c|c|ccc} & i=1 & & & \\ \hline \mathbf{c}_1 & \mathbf{c}(\alpha_1) & \mathbf{c}(\alpha_1) & ... & \mathbf{c}(\alpha_1) \\ \mathbf{c}_2 & \mathbf{c}(\alpha_1) & \mathbf{c}(\alpha_2\alpha_2) & ... & \mathbf{c}(\alpha_l\alpha_2) \\ \mathbf{c}_3 & \mathbf{c}(\alpha_1) & \mathbf{c}(\alpha_2\alpha_3) & ... & \mathbf{c}(\alpha_l\alpha_3) \\ \vdots & \vdots & \vdots & ... & \vdots \\ \mathbf{c}_l & \mathbf{c}(\alpha_1) & \mathbf{c}(\alpha_2\alpha_l) & ... & \mathbf{c}(\alpha_l\alpha_l) \end{array}\right],$$

which is equal to:

$$\left[\begin{array}{c|c|cccc} & i=1 & & & & \\ \hline \mathbf{c}_1 & \mathbf{c}_1 & \mathbf{c}_1 & \mathbf{c}_1 & ... & \mathbf{c}_1 \\ \mathbf{c}(\gamma) & \mathbf{c}_1 & \mathbf{c}(\gamma^2) & \mathbf{c}(\gamma^3) & ... & \mathbf{c}(\gamma) \\ \mathbf{c}(\gamma^2) & \mathbf{c}_1 & \mathbf{c}(\gamma^3) & \mathbf{c}(\gamma^4) & ... & \mathbf{c}(\gamma^2) \\ \vdots & \vdots & \vdots & \vdots & ... & \vdots \\ \mathbf{c}(1) & \mathbf{c}_1 & \mathbf{c}(\gamma) & \mathbf{c}(\gamma^2) & ... & \mathbf{c}(1) \end{array}\right].$$

Starting from the $2l+1$-th column, every l columns of Γ_1 present the columns of the Core C, in which the rows are exchanging positions following a shifting over the finite field $\mathbb{F}_l$. That to say that every such l columns become S^tC, where $S = {V_l}^{-1}(1 \oplus U_{l-1})V_l$, and $t \in \{1, ..., l-1\}$. Hence, Γ_1 is also equal to

$$\left[\begin{array}{c|c|cccc} C & {\mathbf{J}_l}^\top \otimes \mathbf{c}_1 & S_lC & {S_l}^2C & ... & {S_l}^{l-2}C \quad C \end{array}\right].$$

When $k \neq 1$, we have

$$\Gamma_k = \left[\begin{array}{c|c|ccc} & i=1 & & & \\ \hline \mathbf{c}_1 & \mathbf{c}(\alpha_k) & \mathbf{c}(\alpha_k) & ... & \mathbf{c}(\alpha_k) \\ \mathbf{c}_2 & \mathbf{c}(\alpha_k) & \mathbf{c}(\alpha_2\alpha_2 + \alpha_k) & ... & \mathbf{c}(\alpha_l\alpha_2 + \alpha_k) \\ \mathbf{c}_3 & \mathbf{c}(\alpha_k) & \mathbf{c}(\alpha_2\alpha_3 + \alpha_k) & ... & \mathbf{c}(\alpha_l\alpha_3 + \alpha_k) \\ \vdots & \vdots & \vdots & ... & \vdots \\ \mathbf{c}_l & \mathbf{c}(\alpha_k) & \mathbf{c}(\alpha_2\alpha_l + \alpha_k) & ... & \mathbf{c}(\alpha_l\alpha_l + \alpha_k) \end{array}\right].$$

Proceeding as before, the matrix Γ_k is equal to:

$$\left[\begin{array}{c|c|cccc} C & {\mathbf{J}_l}^\top \otimes \mathbf{c}(\alpha_k) & S_l\overline{C} & {S_l}^2\overline{C} & ...{S_l}^{q-2}\overline{C} & \overline{C} \end{array}\right],$$

where

$$\overline{C} = \begin{bmatrix} \mathbf{c}_{((1+a)(\mod l)+1)} \\ \mathbf{c}_{((2+a)(\mod l)+1)} \\ \vdots \\ \mathbf{c}_{((l+a)(\mod l)+1)} \end{bmatrix} = {U_l}^aC$$

such that, $a = \alpha_k$ if l is a prime number, and $a = \Delta(k)$ otherwise. Then, Γ_k is identical to

$$\left[\begin{array}{c|c|cccc} C & \mathbf{J}_l{}^{\top} \otimes \mathbf{c}_a & S_l U_l{}^a C & S_l{}^2 U_l{}^a C & \ldots & S_l{}^{l-2} U_l{}^a C \quad U_l{}^a C \end{array}\right].$$

Note that S_l and U_l cannot permute.

Finally, we rearrange the rows of $\widehat{B}$ following the permutation $V_l \otimes I_l$, and we get B as defined in the proposition above. B_0 is the same as the one defined in Theorem 1 in [10].

For the second case by using C and D defined in the construction of Theorem 2, and proceeding similarly we obtain $\widetilde{S_q}$ and $\widetilde{U_q}$.
□

Taking a Scarpis construction obtained via an arbitrary bijection, then the results in Proposition 1 lead to the following.

Proposition 3.2. *(1) Let β be any bijection from $\{1, ..., l\}$ to $\mathbb{F}_l$, and H be a normalized Hadamard matrix of order $l+1$. Then, $\Phi_{l,\beta}(H)$ is equivalent to*

$$\Phi_\beta = \left[\begin{array}{c} B_{0,\beta} \\ B_\beta \end{array}\right],$$

where $B_{0,\beta} = H'P \otimes \mathbf{J}$, $P = 1 \oplus P_\beta$ for some permutation matrix P_β depending on the choice of β, and

$$B_\beta = \left[\begin{array}{c|c|ccc} & \mathbf{J}_l{}^{\top} \otimes \mathbf{c}_1 & S_l C & \ldots & S_l{}^{l-2} C \quad C \\ & \mathbf{J}_l{}^{\top} \otimes \mathbf{c}_2 & S_l U_l C & \ldots & S_l{}^{l-2} U_l C \quad U_l C \\ \mathbf{J}_l{}^{\top} \otimes P_\beta C & \vdots & \vdots & \vdots \quad \ldots & \vdots \\ & \mathbf{J}_l{}^{\top} \otimes \mathbf{c}_l & S_l U_l{}^{l-1} C & \ldots & S_l{}^{l-2} U_l{}^{l-1} C \quad U_l{}^{l-1} C \end{array}\right].$$

(2) Same result can be obtained for $\Psi_{q,\beta}(H)$ by taking an appropriate Hadamard matrix H, and a permutation β acting on $\{1, .., q\}$. In this case, we use $\widetilde{P} = (1 \oplus P_\beta) \otimes I_2$ and $\widetilde{P_\beta} = I_2 \otimes P_\beta$ instead of P and P_β, respectively.

Proof. Let β be a bijection from $\{1, ..., l\}$ to $\mathbb{F}_l$, and

$$\sigma : \begin{array}{ccc} \mathbb{F}_l & \to & \mathbb{F}_l \\ \beta_i & \to & \alpha_i \end{array}.$$

It is easy to see that σ is a one-to-one and onto, and the equation $\sigma(x) = a$ has a unique solution for each $a \in \mathbb{F}_l$. Then, σ is a bijection of $\mathbb{F}_l$, and then a permutation of $\mathbb{S}_l$. Let P_β denotes its corresponded permutation matrix.

Taking same assumptions as in Proposition 1, let's define $\overline{B}_\beta$ as in (3.1) via the bijection β. Let also $\widehat{B}_\beta$ denote the matrix obtained as in (3.2) from $\overline{B}_\beta$ following a permutation matrix that we denote it by $\widehat{P}$. Then let t be the integer such that, $\beta_t = 0$. Hence, Γ_t is the block matrix

$$\left[\begin{array}{cccc|c|cc} & & & & i=t & & \\ \hline \mathbf{c}_1 & \mathbf{c}(\beta_1\beta_1) & \mathbf{c}(\beta_2\beta_1) & \ldots & \mathbf{c}(0) & \ldots & \mathbf{c}(\beta_l\beta_1) \\ \mathbf{c}_2 & \mathbf{c}(\beta_1\beta_2) & \mathbf{c}(\beta_2\beta_2) & \ldots & \mathbf{c}(0) & \ldots & \mathbf{c}(\beta_l\beta_2) \\ \vdots & \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ \hline \mathbf{c}_t & \mathbf{c}(0) & \mathbf{c}(0) & \ldots & \mathbf{c}(0) & \ldots & \mathbf{c}(0) \\ \hline \vdots & \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ \mathbf{c}_l & \mathbf{c}(\beta_1\beta_l) & \mathbf{c}(\beta_2\beta_l) & \ldots & \mathbf{c}(0) & \ldots & \mathbf{c}(\beta_l\beta_l) \end{array}\right].$$

Multiplying $\widehat{B_\beta}$ by a column permutation $\mathcal{Q} = [P \otimes I_l]$, for $P = 1 \oplus P_\beta$, Γ_t becomes equivalent to

$$\Gamma_t\mathcal{Q} = \begin{bmatrix} \mathbf{c}_1 & \mathbf{c}_1 & \mathbf{c}(\alpha_2\beta_1) & ... & \mathbf{c}(\alpha_l\beta_1) \\ \mathbf{c}_2 & \mathbf{c}_1 & \mathbf{c}(\alpha_2\beta_2) & ... & \mathbf{c}(\alpha_l\beta_2) \\ \mathbf{c}_3 & \mathbf{c}_1 & \mathbf{c}(\alpha_2\beta_3) & ... & \mathbf{c}(\alpha_l\beta_3) \\ \vdots & \vdots & \vdots & ... & \vdots \\ \mathbf{c}_l & \mathbf{c}_1 & \mathbf{c}(\alpha_2\beta_l) & ... & \mathbf{c}(\alpha_l\beta_l) \end{bmatrix}.$$

$\mathcal{Q}$ involves also columns permutations on the other Γ_ts that permute their columns such that, for each $\beta_k \neq 0$, the block Γ_k becomes

$$\Gamma_k\mathcal{Q} = \begin{bmatrix} \mathbf{c}_1 & \mathbf{c}(\beta_k) & \mathbf{c}(\alpha_2\beta_1 + \beta_k) & ... & \mathbf{c}(\alpha_l\beta_1 + \beta_k) \\ \mathbf{c}_2 & \mathbf{c}(\beta_k) & \mathbf{c}(\alpha_2\beta_2 + \beta_k) & ... & \mathbf{c}(\alpha_l\beta_2 + \beta_k) \\ \mathbf{c}_3 & \mathbf{c}(\beta_k) & \mathbf{c}(\alpha_2\beta_3 + \beta_k) & ... & \mathbf{c}(\alpha_l\beta_3 + \beta_k) \\ \vdots & \vdots & \vdots & ... & \vdots \\ \mathbf{c}_l & \mathbf{c}(\beta_k) & \mathbf{c}(\alpha_2\beta_l + \beta_k) & ... & \mathbf{c}(\alpha_l\beta_l + \beta_k) \end{bmatrix}.$$

Moreover, multiplying $\mathcal{Q}$ on the right of $\Phi_{l,\beta}(H)$ involves also columns permutations on B_0, that results $H'P \otimes \mathbf{J}$.

If we permute the rows of Γ_t following P_β, then we obtain

$$P_\beta\Gamma_t\mathcal{Q} = \begin{bmatrix} \mathbf{c}(\beta_1) & \mathbf{c}_1 & \mathbf{c}_1 & \mathbf{c}_1 & ... & \mathbf{c}_1 \\ \mathbf{c}(\beta_2) & \mathbf{c}_1 & \mathbf{c}(\gamma^2) & \mathbf{c}(\gamma^3) & ... & \mathbf{c}(\gamma) \\ \mathbf{c}(\beta_3) & \mathbf{c}_1 & \mathbf{c}(\gamma^3) & \mathbf{c}(\gamma^4) & ... & \mathbf{c}(\gamma^2) \\ \vdots & \vdots & \vdots & \vdots & ... & \vdots \\ \mathbf{c}(\beta_q) & \mathbf{c}_1 & \mathbf{c}(\gamma) & \mathbf{c}(\gamma^2) & ... & \mathbf{c}(1) \end{bmatrix}.$$

So, to deduce (1), we use similar row permutations on the blocks Γ_k, for each $k \in \{1, ..., l\}$, followed by permutations of the blocks Γ_k following $P_\beta \otimes I_l$, and consequently the Scarpis matrix constructed via β way is equivalent to the form

$$\Phi_\beta = \mathcal{P}\Phi_{l,\beta}(H)\mathcal{Q} = \left[\begin{array}{c|ccccc} & \multicolumn{5}{c}{H'P \otimes \mathbf{J}} \\ \hline & {\mathbf{J}_l}^\top \otimes \mathbf{c}_1 & S_lC & ... & {S_l}^{l-2}C & C \\ & {\mathbf{J}_l}^\top \otimes \mathbf{c}_2 & S_lU_lC & ... & {S_l}^{l-2}U_lC & U_lC \\ {\mathbf{J}_l}^\top \otimes P_\beta C & \vdots & \vdots & \vdots & ... & \vdots \\ & {\mathbf{J}_l}^\top \otimes \mathbf{c}_l & S_l{U_l}^{l-1}C & ... & {S_l}^{l-2}{U_l}^{l-1}C & {U_l}^{l-1}C \end{array}\right],$$

where $\mathcal{P} = I_l \oplus [(P_\beta \otimes I_l)(I_l \otimes P_\beta)\widehat{P}]$. Taking same steps for the case $\Psi_{q,\beta}(H)$ we obtain the results in (2). □

From Proposition 2 we conclude that two Scarpis Hadamard matrices can be inequivalent under a different choice of bijections, and it divides them into $n!$ classes, hereby they can be classified in a more compatible way. If we take for example $l = 3$, then we have only 1 class of order 12 Hadamard matrices. But Proposition 2 states that we have $3! = 6$ classes. Thus, this classification can be more specific.

The *binary Hadamard matrix* is the matrix $A = \frac{J - H}{2}$, where J is the all one's array of size $m \times m$ and H a Hadamard matrix of order m. The vector subspace over $\mathbb{F}_2$ generated by the rows of A is called the *(binary) Hadamard code*, and the dimension of its image is its *binary rank*.

The matrices obtained by the new construction Ψ are of orders not divisible by 8, and then of a maximal binary rank $qn - 1$ (see [5]). Hence, they generate Hadamard codes with length $2^{t-1} \cdot q(q + 1)$ of all

possible ranks, for every $t \geq 2$, (see Theorems 2, 3 in [19]).

Finally, the first Hadamard matrices obtained using the construction Ψ are of orders 60, when $q = 5$ a prime number, and 180 for $q = 9$ a power of prime number. Using Paley type II matrix of order $12 = 2 \cdot (5 + 1)$ as input, we can present an example of order 60 based on Proposition 1 for $q = 5$. The example is performed by MATLAB in the Appendix of this paper.

4. Conclusion

We gave an analogue of Scarpis' theorem on Hadamard matrices of size $l(l+1)$ that construct Hadamard matrices of size $2q(q+1)$. Moreover, another form was deduced for these matrices in both cases. We noticed that this family of matrices can be variant under different choice of bijections. So, we extended the second form to a family of matrices defined in function of permutation matrices. As $2q(q + 1)$ is not divisible by 8, we became interested in the obtained matrices in the construction of Hadamard codes.

To conclude this paper, we propose an open problem: how to obtain a recursion that uses a Hadamard matrix of order m to construct Hadamard matrices of order qm, where q is a power of a prime number chosen randomly?

Acknowledgements We would like to thank Vehbi Paksoy for his comments that helped to improve the presentation of this paper.

References

[1] K.J. Horadam, Hadamard matrices and their applications, Princeton University Press, Princeton. NJ, 2007.
[2] S.S. Agaian, Hadamard matrices and their applications, LNM 1168. Springer, Berlin, 1985.
[3] R. Lidl, H, Niederreiter, P.M. Cohn, Finite fields, Cambridge University Press, Transferred to degital printing in 2003.
[4] Jennifer Seberry, Orthogonal designs, Hadamard matrices quadratic forms and algebra, Springer, Cham, 2017.
[5] E. F. Assmus Jr. and J. D. Key, Designs and their codes, Cambridge University Press, Great Britain, 1992.
[6] A.S. Hedayat, W. D. Wallis, Hadamard matrices and their applications, Ann. Statist. 6 (1978) 1184–1238.
[7] U. Scarpis, Sui determinanti di valore massimo [On determinants of maximal value], Rendic R Istit Lombardo Sci Lett, 31 (1898) 1441–1446.
[8] W. Orrick, Maximal determinant blog, Hadamard matrices: the construction of Scarpis; 2012 Nov 17, Available from: http://willorrick.wordpress.com/2012/11/17/.
[9] Paley Reac, On orthogonal matrices, J Math Phys, 12 (1933) 311–320.
[10] Dragomir-Ž. Dokovič, Generalization of Scarpis' theorem on Hadamard matrices, Linear and Multilinear Algebra, 65 (2017) 1985–1987.
[11] Dragomir-Ž. Dokovič, Oleg Golubitsky, Ilias S. Kotsireas, Some new orders of Hadamard and skew-Hadamard matrices, Journal of Combinatorial Designs, 22(6) (2014) 270–277.
[12] Dragomir-Ž. Dokovič, Note: Hadamard matrices of order 764 exist, Combinatorica, 28(4) (2008) 487–489.
[13] J. Williamson, Hadamard's determinant theorem and sum of four squares, Duke Math, 11 (1944) 65–81.
[14] J.M. Goethals, J.J. Seidel, A Skew Hadamard matrix of order 36, Cambridge Core, (1969) 343–344.
[15] J. Cooper, J. Milas, W.D. Wallis, Hadamard equivalence, Combinatorial Mathematics, Lecture Notes in Mathematics, Springer-Verlag, Berlin, Heidelberg, New York. 686 (1978) 126–135.
[16] J. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions and tesselated pavements in two or more colours, with applications to Newton's rule, Ornamental tile work and the theory of numbers, Phil. Mag, 34 (1867) 461–475.
[17] W. Orrick, Switching operations for Hadamard matrices, http://www.arxiv.org/abs/math.
[18] A. Mohammadian & B. Tayfeh-Rezaie, Hadamard matrices with few distinct types, Linear and Multilinear Algebra, 67 (2019) 1596–1605.
[19] Kevin T. Phelps, Josep Rif'a, Merc'e Villanueva, Hadamard Codes of Length $2^t \cdot s$ (s Odd), Rank and Kernel, M. Fossorier et al. (Eds.): AAECC 2006, LNCS 3857, (2006) 328–337.

Appendix

Here, we use MATLAB program to apply the results obtained in this paper. Inputting a Paley type II matrix of order 12, we can present an example of order 60 based on Proposition 1 for $q = 5$. In the implementation, by H we denote the output Scarpis matrix, $q = p^r$, and we define the functions:

- $Paley1(p, r) = P'_{p^r}$, returns the Paley type II Hadamard matrix of order $2(q + 1)$. The function is of a complexity $O(q^2)$.
- $TCore(P'_{p^r})$ gives T and $T'M$ (defined in Lemma 2). For any two suitable matrices A and B, $insertA - B(A, B) = \begin{bmatrix} A & B \end{bmatrix}$. $insertA(A, B) = \begin{bmatrix} A \\ B \end{bmatrix}$. Each of this functions is of a complexity $O(q)$.
- Instead of using the matrix product to compute the product of permutations, we use the corresponding composition law over $\mathbb{S}_q$, to reduce the complexity. So, to define a permutation, we take the row vector $X = (\pi(1), ..., \pi(q))$ instead of the matrix $P = [\delta(\pi(i), j)]$. Hence, the product of two matrices A and B associated to the permutations X and Y, can be done using the following function:

```
function [circ]= circ(X,Y)
  K=size(X);
  q=K(1,2);
        for(i=1:q)
            Z(i)= Y(X(i));
        end
  circ=Z;
end
```

  It returns the row vector $Y \circ X$ corresponded to the matrix AB. Clearly, the function is of a complexity $O(q)$.

- $Alpha(r, p) = V_{p^r}$ is a vector that represent a permutation of $\{1, ..., q\}$ following α. Considering a known generator of the multiplicative group, the function is of a complexity $O(q)$.
- $Perms(V_{p^r}) = L$ is a function that define shift permutations U_{p^r}, then use V_{p^r} to compute $S = V_{p^r}^{\top}(1 \oplus U_{p^r-1})V_{p^r}$ and its powers. It returns a tensor L such that $L(i, :, j)$ is a permutation of $\{1, .., q\}$ following $S^i U_{p^r}^j$. This function is of a complexity $O(q^3)$.
- $KronPerms(L) = Q$ is a function that returns a tensor Q such that,

$$Q(i, :, j) = [L_{i,1,j}, ..., L_{i,q,j}, L_{i,1,j} + q, ..., L_{i,q,j} + q].$$

  Then of a complexity $O(q^2)$.

- $PermMat(Q, T) = R$ is a function that return a tensor R such that, $R(:, :, i, j)$ present a row permutation of T following the permutation $Q(i, :, j)$, and then of a complexity $O(q^3)$.

$\Psi_{5,\alpha}(P'_5)$:

```
clear;
clc;
%entries_____________________________________
p=5;
r= 1;
%entry matrix_____________________________________________
```

```
[PAL1]=Paley1(p,r);
[ST,T]=Tcore(PAL1);
%Help_____________________________________________________
K=size(T);
m=K(1,1);
J=ones(m/2);
JT=J(:,1);
J=J(1,:);
%permutations_____________________________________________
[U]=Alpha(r,p);
[L]=Perms(U);
[Q]=KronPerms(L);
[R]=PermMat(Q,T);
%B0_______________________________________________
  B0=kron(ST,J);
%BR_______________________________________________
  B=kron(JT,T);
[L]=InsertA(kron(JT,T(1,:)),kron(JT,T((m/2)+1,:)));
for(j=2:m/2)
[A]=InsertA(kron(JT,T(j,:)),kron(JT,T(m/2+j,:)));
[L]=InsertA(L,A);
end
[B]=InsertA_B(B,L);


  for(i=1:m/2-1)
       for(j=1:m/2-1)
         [BR]=InsertA(BR,R(:,:,i,j));
       end
[B]=InsertA_B(B,BR);
  end
% %final result_____________________________________________
n=2*p^r*(p^r+1)
[H]=InsertA(B0,B);
H=diag(H(:,1))*H*diag(H(1,:))
%%Verification_____________________________________________
if (H*transpose(H)==n*eye(n))
    fprintf('H is a Hadamard matrix');
end
```

Results:

```
n = 60
H =
Columns 1 through 13
     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	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	−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	−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	−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	−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	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	−1	1	−1	1	1	−1	−1	−1	1	−1	−1
1	−1	−1	1	−1	1	−1	−1	1	1	−1	1	1

```
Columns 14 through 26
   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    -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    -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    -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    -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     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     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     1    -1    -1     1     1     1     1    -1     1    -1    -1
  -1     1    -1     1     1    -1    -1     1    -1     1    -1    -1    -1

Columns 27 through 39
   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     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     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    -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     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    -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    -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     1     1     1    -1     1    -1    -1    -1    -1    -1     1
   -1    -1     1     1     1    -1     1     1    -1     1     1    -1    -1

Columns 40 through 52

    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     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     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     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     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    -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    -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     1    -1    -1     1    -1    -1     1     1    -1     1    -1
   1     1    -1     1    -1     1    -1     1     1     1    -1    -1    -1

Columns 53 through 60
   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     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
-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    -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
 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
```

H is a Hadamard matrix.