IEICE TRANS. FUNDAMENTALS, VOL.E95–A, NO.11 NOVEMBER 2012

PAPER Special Section on Signal Design and Its Applications in Communications

Some Properties of Binary Matrices and Quasi-Orthogonal Signals Based on Hadamard Equivalence*

Ki-Hyeon PARK[†a)], *Student Member and* **Hong-Yeop SONG**[†b)], *Nonmember*

SUMMARY We apply the Hadamard equivalence to all the binary matrices of the size $m \times n$ and study various properties of this equivalence relation and its classes. We propose to use HR-minimal as a representative of each equivalence class, and count and/or estimate the number of HR-minimals of size $m \times n$. Some properties and constructions of HR-minimals are investigated. Especially, we figure that the weight on an HR-minimal's second row plays an important role, and introduce the concept of Quasi-Hadamard matrices (QH matrices). We show that the row vectors of $m \times n$ QH matrices form a set of m binary vectors of length n whose maximum pairwise absolute correlation is minimized over all such sets. Some properties, existence, and constructions of Quasi-orthogonal sequences are also discussed. We also give a relation of these with cyclic difference sets. We report lots of exhaustive search results and open problems, one of which is equivalent to the Hadamard conjecture.

key words: *Hadamard equivalence, orthogonality, Quasi-orthogonal signal, Quasi-Hadamard matrix*

1. Introduction

A Hadamard matrix of order n (or, size $n \times n$) is defined as an $n \times n$ matrix with the entries $+1$ or -1 such that

$$H \cdot H^T = nI,$$

where I is the $n \times n$ identity matrix [6], [20]. One implication of the above is that the rows of a Hadamard matrix are orthogonal, and the set of rows form a set of orthogonal vectors of $+1$'s and -1's and all of the same length [20]. This is the key to their applications to the design of good error-correcting codes and CDMA cellular communication systems [2], [4], [7], [9]. After that, bandwidth and PAPR problems are issued using Hadamard matrix and *quasi-orthogonal signal set* that the correlation values among signals are near but not ensured as zero is considered in OFDM systems and IEEE standards. However, many theoretical topics about quasi-orthogonal signal set like the maximum size are still open.

Given a Hadamard matrix of order n, one can transform it into another by the following (Hadamard-preserving) operations [20]: multiplying a column (or a row, resp.) by -1; and/or permuting columns (or rows, resp.). The resulting matrix is also Hadamard, and it is said to be "equivalent" to the original. In general, one can easily produce many different matrices which are equivalent to a given one by applying any combination of the above Hadamard-preserving operations. On the other hand, it would be quite hard to check whether two given Hadamard matrices of the same size are Hadamard-equivalent [20]. The first elegant method for equivalence check is studied at [8]. And after that, there have been many results on the equivalence/inequivalence of Hadamard matrices [10]–[13], [16], [18]. We note that [11] and [12] calculated the number of inequivalent classes for sizes 24 and 28, which would have been impossible by computer, and very recently, [13] calculated the number partially for sizes 32.

This paper applies the Hadamard equivalence to general $m \times n$ binary matrices, and studies their equivalence classes for quasi-orthogonality. To do this, we define and use HR-minimal [14] as a representative of an equivalence class, and discuss its properties. One interesting result would be a characterization of binary matrices which are very similar to Hadamard matrices in the sense that the row vectors have minimum possible pairwise absolute correlation. We name these as Quasi-Hadamard matrices, and these include Hadamard matrices when $m = n$ and whenever an $n \times n$ Hadamard matrix exists. Some properties and existence of QH matrices are also discussed. Another special types of HR-minimals are H-minimals and symmetric H-minimals. These are also characterized in various ways and by computer.

Section 2 describes definition and notation that we use throughout the paper, including the Hadamard equivalence and the representative "HR-minimal" with some examples. Section 3 develops various properties and existence of HR-minimals. We will characterize the shape of them and identify some special properties of HR-minimals which determines orthogonality, and we define a special form for minimized absolute correlation called "Quasi-Hadamard matrices." Various properties of them are also discussed. Section 4 discusses various properties and the number of equivalent classes. We introduce HC-minimal and H-minimal, and investigate various properties of equivalence classes in terms of these representatives. Cyclic difference sets are used to construct systematically some HR-minimals and minimal QH matrices of square sizes. This relation is given at the end of Sect. 4. Some bounds, some exact number, and lots of exhaustive search results are also given in Sects. 3 and 4. Finally, Sect. 5 concludes this paper, with a list of

Manuscript received January 23, 2012.
Manuscript revised June 3, 2012.

[†]The authors are with Yonsei University, Korea.

*This paper is a full version of 2010 ISIT proceeding paper "Quasi-Hadamard Matrix" and 2011 IWSDA proceeding paper "Classification, Construction and Search of General Quasi-Orthogonal Binary Signal Sets".

a) E-mail: kh.park@yonsei.ac.kr
b) E-mail: hysong@yonsei.ac.kr

DOI: 10.1587/transfun.E95.A.1862

open problems.

2. Hadamard Equivalence on Binary Matrices

Hadamard matrices have entries from $\{+1, -1\}$. By setting up a suitable isomorphic relation, we may convert them over the binary field $\{0, 1\}$. This can be done by $x = (-1)^y \in \{+1, -1\}$ for $y \in \{0, 1\}$ or its inverse map. Throughout this paper, we consider binary matrices over $\{0, 1\}$, but the dot-product of two row vectors of a binary matrix will be calculated over the complex, after converting first each entry into $\{+1, -1\}$ by the above map. Then, in order to apply Hadamard equivalence to binary matrices, we change slightly the way it is described from the one in Introduction, which is essentially the same except it applies binary matrices over $\{0, 1\}$:

Definition 1 *Two $\{0, 1\}$-valued binary matrices A and B of the same size $m \times n$ are said to be Hadamard-equivalent, or simply, equivalent, and denoted by $A \sim B$, if one can be transformed into another by applying any combination of the following operations:*

1. [CC/CR] *complementing a column (or row); and/or*
2. [PC/PR] *permuting columns (or rows).*

We call these Hadamard-preserving operations also.

It is obvious that the binary relation defined in Definition 1 on the set of binary matrices of size $m \times n$ is indeed an equivalence relation. Note that there can be as many as $n! \times m! \times 2^{n+m}$ different binary matrices which are equivalent to a given one. Thus, any equivalence class can have up to so many members in it.

For Hadamard matrices, the key property is the orthogonality of its rows, and any Hadamard-preserving operations will preserve the orthogonality of its row vectors. Here, the orthogonality is checked by the dot-product of two rows (consisting of $+1$'s and -1's). For binary matrices over $\{0, 1\}$ with rows which are not orthogonal in general, we have to find some similar measure which would be preserved by the above operations and still useful in communication and coding problems. It turned out that it is the absolute value of the same dot-product: given two binary vectors $\mathbf{r}$ and $\mathbf{s}$ of length n, we define their absolute correlation as

$$Cor(\mathbf{r}, \mathbf{s}) \triangleq \left| \sum_i (-1)^{r(i)+s(i)} \right|, \tag{1}$$

where $r(i)$ is the i-th element of the binary vector $\mathbf{r}$. Observe that it is equal to $|A - D|$, where A is the number of agreements and D is the number of disagreements between the vectors $\mathbf{r}$ and $\mathbf{s}$.

Proposition 1 *The absolute correlation of the two rows of a $2 \times n$ binary matrix will be preserved by any Hadamard-preserving operation in* Definition 1.

proof. Recall that $Cor = |A - D|$. Note first that the values A and D will not be changed by any PR, PC, CC, and also the CR on both rows. Finally, CR on any one row will change the value A to D and D to A so that the absolute correlation remains the same. □

Corollary 1 *Two equivalent $m \times n$ binary matrices have the same profile of absolute correlations.*

We now define a map from the set of $m \times n$ binary matrices to the integers of the range from 0 to $2^{mn} - 1$ as follows:

Definition 2 *Let $A = (a(i, j))$ be an $m \times n$ binary matrix whose (i, j)-entry is $a(i, j)$, where $i = 1, 2, ..., m$ and $j = 1, 2, ..., n$. Then,*

$$\rho(A) \triangleq \sum_{i=1}^{m} \sum_{j=1}^{n} \left[a(i, j) 2^{n(m-i)+(n-j)} \right]. \tag{2}$$

The set of binary matrices of size $m \times n$ is in one-to-one correspondence with the set of binary vectors of length mn. Considering this relation and the fact that the binary vectors of length mn can be lexicographically ordered, we may summarize some important properties of the map ρ as follows:

Theorem 1 [14] *Let $\mathbf{S}$ be the set of binary matrices of size $m \times n$, and ρ be the map from $\mathbf{S}$ to the integers of the range from 0 to $2^{mn} - 1$ in* Definition 2. *Then, we have the following:*

1. Order property: *ρ induces a complete ordering. That is, exactly one of $\rho(A) < \rho(B)$, $\rho(A) > \rho(B)$ or $\rho(A) = \rho(B)$ must be true for any $A, B \in \mathbf{S}$.*
2. $1 - 1$ property: *ρ is one-to-one. That is, we have $\rho(A) = \rho(B)$ if and only if $A = B$ for any $A, B \in \mathbf{S}$.*
3. Existence of minimal element: *Any subset $\mathbf{S}_0$ of $\mathbf{S}$ must contain an element M_0, which we call the minimal matrix of $\mathbf{S}_0$, such that $\rho(M_0) < \rho(A)$ for any $A \in \mathbf{S}_0$. Furthermore, since ρ is one-to-one, such a minimal matrix is uniquely determined.*

Now, we are ready to define the representative of the equivalence class induced by the above equivalence relation:

Definition 3 *The minimal matrix of an equivalence class, which is uniquely determined as stated in* Theorem. 1, *is called the Hadamard-row minimal matrix, or* HR-minimal. *The ρ value of the HR-minimal is called the ρ value of the equivalence class.*

Example 1 *All* 16 *binary matrices of size 2×2 are shown in Fig. 1 with the color "black" and "white" denoting the value* 0 *and* 1 *respectively. We often use this coloring scheme to represent various binary matrices in this paper. Note that the matrices in Class A are not Hadamard, with the absolute correlation values between the two rows all*

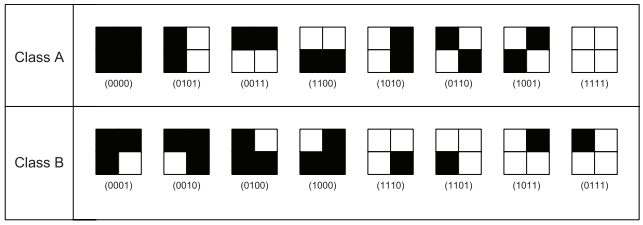

Fig. 1 All the 2×2 binary matrices in two equivalence classes.

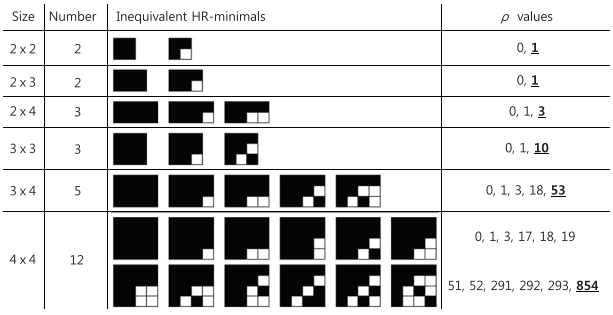

Fig. 2 Examples of the inequivalent HR-minimals.

equal to 2*. Class B contains all the equivalent Hadamard matrices of size* 2×2*. The matrix* $(abcd)$ *in Fig. 1 has the* ρ *value*

$$\rho((abcd)) = (abcd)_{(2)} = 2^3a + 2^2b + 2c + d.$$

Thus, Class A has the ρ *value* $0000_{(2)} = 0$*, and Class B has* $0001_{(2)} = 1$.

Example 2 *Figure 2 shows all the inequivalent HR-minimals of some small sizes. The number of inequivalent classes and their* ρ *values are shown also. We note that the examples with the maximum* ρ *values (those with underline) for a given size, which will be treated with a special attention in* Sect. 3*. For sizes* 2×2 *and* 4×4*, they are indeed Hadamard matrices. Note also that all the* 3×3 *HR-minimals are symmetric. For the size* 4×4*, only eight of them are symmetric.*

Remark 1 *The definition of HR-minimal is the same as the canonical form of a Hadamard matrix introduced in* [13], [16].

3. Properties HR-Minimals and Quasi-Hadamard Matrices

In this section, we will investigate some interesting properties of HR-minimals and identify some special ones as Quasi-Hadamard matrices. We first characterize the shape and structure of HR-minimals:

Theorem 2 *1. An HR-minimal is in, so called, a normalized form. That is, its top row and left-most column consist entirely of* 0*'s.*
2. In an HR-minimal of size $m \times n$*, the weight of the second row cannot exceed* $n/2$*. Furthermore, in its second row, all the* 0*'s come to the left of all the* 1*'s. In its second left-most column, all the* 0*'s come on top of all the* 1*'s.*
3. An HR-minimal is row-sorted, and also, column-sorted.

proof. **1)** If the top row contains a 1, then complement the column. The resulting matrix will have smaller ρ value. Similarly for a 1 at the left-most column.

2) Recall that the top row contains 0 only. If any 1 comes to the left of a 0 in the second row, then permute the columns so that all the 0's come to the left of all the 1's. The resulting matrix has a smaller ρ value. If the weight of the second row exceeds $n/2$, then complement the second row and permute the columns so that all the 0's come to the left of all the 1's. The property of the second column is proved similarly.

3) Obvious. □

Remark 2 *We believe that the weight of the second column of an* $m \times n$ *HR-minimal need not be upper bounded by* $m/2$*, though it is true for all the examples we have found by computer. It could be true that it cannot exceed* $m/2$*, and we leave this as an open problem.*

Remark 3 *Note that the converse of Item* 3 *in* Theorem 2 *is NOT true in general. See the examples A and B below:*

$$A = \begin{pmatrix} 000 \\ 011 \end{pmatrix} \sim \begin{pmatrix} 000 \\ 001 \end{pmatrix} = B.$$

Trivially A is not an HR-minimal although it is row-and-column-sorted.

A binary matrix may have multiple number of rows that are the same. If these rows are not adjacent then the rows are not sorted. Similarly for the same columns. This gives the following:

Corollary 2 *Two same rows of an HR-minimal must be adjacent. So must be its two same columns.*

If a not-all-zero row repeats more than the all-zero row at the top of an HR-minimal, then these rows can be moved to the top and some appropriate CCs will make them all-zero rows. The result will have smaller ρ value than the original, which is impossible.

Corollary 3 *In an HR-minimal, the number of repetitions of any row cannot exceed that of the all-zero row at the top.*

Remark 4 *We have conjectured that a similar statement to* Cor. 3 *must hold for the columns in an HR-minimal. It turned out that it is false by the following counter example of size* 6×6 *HR-minimal in which the* 4*-th and the* 5*-th columns are the same, (i.e., they repeat twice) but the left-most all-zero column repeats only once:*

$$\begin{pmatrix} 000000 \\ 000000 \\ 000001 \\ 000110 \\ 001110 \\ 010110 \end{pmatrix}$$

As long as all the rows are repeated the same number of times, the HR-minimality will be preserved. Similarly for the columns. For example in the following, B is obtained from A by repeating all the rows twice and all the columns three times:

$$A = \begin{pmatrix} 00 \\ 01 \end{pmatrix} \Longrightarrow \begin{pmatrix} 000000 \\ 000000 \\ 000111 \\ 000111 \end{pmatrix} = B. \tag{3}$$

Corollary 4 *(Linear Expanding Construction) Repeating each row k times and each column l times results in an HR-minimal of size $mk \times nl$ if we start with an HR-minimal of size $m \times n$.*

Corollary 5 *(Add-Zero-Row Operation) We obtain an $(m+1) \times n$ HR-minimal by adjoining the all-zero row to the top of an $m \times n$ HR-minimal.*

Note that repeating any other row not necessarily preserves the HR-minimality. A similar statement regarding the columns of HR-minimals turned out to be true, whose proof is not as simple as the above:

Theorem 3 *(Add-Zero-Column Operation) We obtain an $m \times (n+1)$ HR-minimal by adjoining the all-zero column to the left-most of an $m \times n$ HR-minimal.*

proof. Let A be an $m \times n$ HR-minimal and obtain the $m \times (n+1)$ matrix A' by adjoining the all-zero column to the left-most of A. Suppose that A' is not an HR-minimal. Then, there exists $H' \sim A'$ such that H' is HR-minimal and we must have $\rho(H') < \rho(A')$. Delete the left-most column of H' and call it H of the size $m \times n$. From the structure of H' and A', it is obvious that

$$\rho(H) < \rho(A). \tag{4}$$

If $H \sim A$, then (4) is impossible and therefore we are done.

Now we assume that $H \nsim A$. We now think of the operation which converts A' into the HR-minimal H'. Whatever the operation might be, the final form H' must have the shape and structure described by Theorem 2, Corollaries 2 and 3. Especially, we would like to concentrate on the all-zero added column on the left-most of A so that A' has at least two all-zero columns on the left. It is possible that they are relocated from the left-most to some other column positions by some PC, they become not-all-zero columns by some CR, some components may have been permuted by some PR, but they must be adjacent in the final form H'. Let's obtain H'' by deleting one of these columns from H'. We simply note that the deleted column from H' to obtain H'' is indeed the one that was originally adjoined to obtain A' from A (and possibly moved and/or changed to not-all-zero column). Therefore, it is obvious that $H'' \sim A$. Since A is an HR-minimal, we must have

$$\rho(A) \le \rho(H'').$$

We now claim that

$$\rho(H'') \le \rho(H).$$

To see this, simply observe that both H and H'' are the results of deleting a column from H'. When you delete the left-most all-zero column, you obtain H. When you delete the column described earlier, then you obtain H''.

Combining two inequalities above, we have $\rho(A) \le \rho(H)$, which is a desired contradiction to (4). □

Proposition 2 *If A is an $m \times n$ HR-minimal, then the $(m-1) \times n$ matrix B obtained by deleting the bottom row of A is also an HR-minimal.*

proof. If there is an operation on B that results in smaller ρ value than B, then the similar operation (with the bottom row of A included) on A will also results in smaller ρ value than A. □

Remark 5 *We have conjectured, similar to* Prop. 2*, that deleting the right-most column of an $m \times n$ HR-minimal gives an $m \times (n-1)$ HR-minimal. It turned out to be false by the counter example A of size 5×6 shown in the following. The 5×5 matrix B obtained by deleting the right-most column of A is not HR-minimal. We show also the equivalent HR-minimal C of this:*

$$A = \begin{pmatrix} 000000 \\ 000011 \\ 001100 \\ 010101 \\ 010110 \end{pmatrix} \Longrightarrow B = \begin{pmatrix} 00000 \\ 00001 \\ 00110 \\ 01010 \\ 01011 \end{pmatrix} \sim \begin{pmatrix} 00000 \\ 00001 \\ 00110 \\ 00111 \\ 01010 \end{pmatrix} = C.$$

Now we consider the absolute correlations given in (1) of all possible pairs of rows of a given HR-minimal. Since any HR-minimal is normalized, the top row must be the all-zero row. Let w be the weight of its second row. Then the absolute correlation of the top all-zero row and the second row becomes $|n-2w|$. We will show that this value is maximum over all possible pairs, though this maximum value could occur from some other pairs.

Theorem 4 *In an HR-minimal, the absolute correlation of the top two rows cannot be exceeded by that of any other pair of rows.*

proof. Let c be the absolute correlation of the top two rows of an HR-minimal A. If $c = n$, it implies the second row is also the all-zero row and we are done since n is the trivial maximum that cannot be exceeded by any pair. Thus, we may suppose a pair of rows (other than the top two rows) has the absolute correlation d with $c < d \le n$. The idea

is to permute the rows so that these two rows (with absolute correlation d) come at the top, and then normalize the result, and then permute the columns so that all the 0's come to the left of all the 1's in the second row. Since the weight of the column-sorted second row of B is smaller than A, the resulting matrix B has a smaller ρ value than A. □

Let w be the weight of the second row of an HR-minimal of size $m \times n$. From Theorem 2, we know that w cannot exceed $n/2$. Therefore, $w \leq (n-1)/2$ for odd n and $w \leq n/2$ for even n. Now, we have to distinguish two cases where n is doubly-even and it is singly-even when $m > 2$:

Proposition 3 *Let $n \equiv 2 \pmod 4$, and A be an HR-minimal of size $m \times n$ with $m \geq 2$. Denote by w the weight of the second row of A.* (a) *If $w = n/2$ (and hence n is even) then $m = 2$.* (b) *If $m > 2$, then $w \leq n/2 - 1$.*

proof. If $w = n/2$ then the absolute correlation of the top two rows is zero and this cannot be exceeded by any other pair. Therefore, all the rows are orthogonal with each other, and A must have rows of length which is a multiple of 4 if it contains at least 3 rows. If $m > 2$ then the value w cannot attain $n/2$ since the matrix cannot be a Hadamard matrix. [20]. □

Now, we would like to identify some special equivalence classes, whose representatives are quite similar to and generalization of Hadamard matrices:

Definition 4 *(Quasi-Hadamard Matrix)* (a) *An $m \times n$ equivalence class containing an HR-minimal A is called* Quasi-Hadamard class*, or* QH class*, if the weight w of the second row of A is ether $(n-1)/2$, $n/2$ or $n/2-1$ according to the values of n and m as follows:*

- *when n is odd, $w = (n-1)/2$ for all $m \geq 2$;*
- *when n is even, we have distinguish two cases:*
  - *when $n \equiv 0 \pmod 4$,*
    - *$w = n/2$ for all $m \geq 2$;*
  - *when $n \equiv 2 \pmod 4$,*
    - *$w = n/2$ for $m = 2$;*
    - *$w = n/2 - 1$ for all $m > 2$.*

(b) *All the matrices in the equivalence class containing such A are called* Quasi-Hadamard matrices*, or* QH matrices*. The representative HR-minimal A in the class is called the* minimal QH matrix. (c) *For all $n \geq 2$, the function $R_Q(n)$ is defined to be the maximum such that an $R_Q(n) \times n$ QH matrix exists.*

In the item (c) of Definition 4, the function $R_Q(n)$ is well-defined because of the following, which could be a corollary of Prop. 2:

Corollary 6 (a) *If A is an $m \times n$ minimal QH matrix then the $(m-1) \times n$ matrix obtained from A by deleting its bottom row is also a minimal QH matrix.* (b) *If there does not exist an $m \times n$ minimal QH matrix, then neither does an $(m+1) \times n$ minimal QH matrix.*

Remark 6
1. *When $m = 2$, there exists a unique $m \times n$ QH class for all $n \geq 2$. For $2 < m \leq R_Q(n)$, the number of inequivalent $m \times n$ QH classes could be 1 or more. Its exact behavior is an interesting open problem.*
2. *An $m \times n$ (minimal) QH matrix is indeed a (minimal) Hadamard matrix whenever $m = n$ and $n \equiv 0 \pmod 4$. Otherwise, it gives the set of m row vectors all of length n whose maximum pairwise absolute correlation is minimized over all possible m-sets of binary vectors of length n. This minimum value is either 2, 1, or 0, according to the values of n and m. Note that the minimal Hadamard matrix is the one with the minimum ρ value in its equivalence class.*

We now compare the ρ values of minimal QH matrices with those of all other HR-minimals of the same size. Since the second row of a minimal QH matrix has the largest weight, the ρ value is relatively larger than those of HR-minimals in any other non-QH classes. The following is a direct consequence of Definition 4:

Proposition 4 *An $m \times n$ minimal QH matrix has a larger ρ value than any other HR-minimals of non-QH classes of the same size.*

Remark 7
1. *When we consider the set of all the HR-minimals of size $m \times n$, and order them according to the ρ values in increasing order, then all the minimal QH matrices come at the end. Figure 2 shows this with the maximum ρ value in underline.*
2. *Assume an $n \times n$ Hadamard matrix exists. Since a Hadamard matrix is a very special QH matrix,* Prop. 4 *implies the following: the ρ value of an $n \times n$ minimal Hadamard matrix is larger than that of any HR-minimal which is not (equivalent to) a Hadamard matrix.*

We have done some series of computer search for the values of $R_Q(n)$ for $n \leq 18$ and the number of inequivalent $R_Q(n) \times n$ minimal QH matrices. The result is contained in Table 1. Here, the notation $R(w, n)$ generalizes $R_Q(n)$ and is defined in Defition 6. Note that the existence of (minimal) QH matrices of sizes 16×6, 16×10, and 16×17. Some examples of these sizes are shown in Fig. 3.

Based on the values of $R_Q(n)$ and the examples we have found by computer, we were able to find some interesting properties of minimal QH matrices and their equivalence classes. We will finish this section with some remarks and discussions on this.

The value $R_Q(n) \geq n$ seems to be true for most of n except when $n \equiv 1 \pmod 8$. We formulate this as a conjecture:

Conjecture 1 *There exists an $n \times n$ QH class for all the positive integers $n \geq 2$ except for $n \equiv 1 \pmod 8$.*

Table 1 The value of $R(w,n)$ and the number of $R(w,n)\times n$ inequivalent matrices with $\wp(\cdot)=w$.

	w=2	3	4	5	6	7	8
n=4	**4(1)**	-	-	-	-	-	-
5	**5(1)**	-	-	-	-	-	-
6	**16(1)**	2(1)	-	-	-	-	-
7	22(1)	**8(1)**	-	-	-	-	-
8	≥64	8(14)	**8(1)**	-	-	-	-
9	?	16(5)	**8(3)**	-	-	-	-
10	?	≥24	**16(3)**	2(1)	-	-	-
11	?	≥64	≥17	**12(1)**	-	-	-
12	?	?	≥64	13(1)	**12(1)**	-	-
13	?	?	?	≥16	**13(1)**	-	-
14	?	?	?	≥20	**≥16**	2(1)	-
15	?	?	?	≥64	≥17	**16(5)**	-
16	?	?	?	?	≥64	≥16	**16(5)**
17	?	?	?	?	?	≥20	**16(76)**
18	?	?	?	?	?	≥20	**≥20**
19	?	?	?	?	?	≥64	≥20

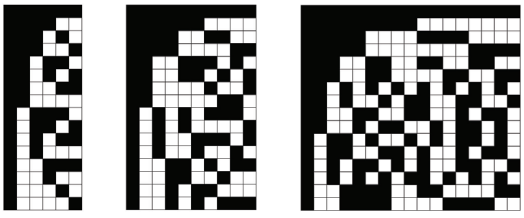

Fig. 3 Examples of 16×6, 16×10, and 16×17 minimal QH matrices.

Remark 8 *The truth of* Conjecture 1 *for* $n\equiv 0 \pmod 4$ *implies and is implied by the Hadamard Conjecture.*

When $n\equiv 2 \pmod 4$, the value $R_Q(n)$ seems to be "much" larger than n in the table. For example, $R_Q(6)=16$ implies that there exist a lot of inequivalent 6×6 minimal QH matrices. We just found that the number is 15 for size 6×6, and is 4718 for size 10×10. This number turned out to be huge for the sizes 14×14 and 18×18, for which more than 1 million inequivalent examples are found by computer.

Remark 9 *The repetition of rows and/or columns of a minimal QH matrix as in* Cor. 4 *does not in general result in a minimal QH matrix, though it results always in an HR-minimal of larger size. One example is shown in* (3) *where A is a minimal QH matrix, and, in fact, it is the minimal* 2×2 *Hadamard matrix shown in* Fig. 1*, but B is not.*

The $R_Q(n)$ can easily be lower bounded whenever a Hadamard matrix exists of size near n:

Proposition 5 *If an* $n\times n$ *Hadamard matrix exists, for* $n\geq 4$*, then* $R_Q(n)=n$*,* $R_Q(n-1)\geq n$ *and* $R_Q(n-2)\geq n$*.*

proof. It is well known that any $n\times n$ Hadamard matrix cannot be extended to $(n+1)\times n$ QH matrix. See [5] for example. This gives $R_Q(n)=n$ whenever an $n\times n$ Hadamard matrix exists. For the other two, simply delete the right-most column of the HR-minimal of an $n\times n$ Hadamard matrix once and then twice. The resulting matrices may not be an HR-minimal (recall Remark 5), but the pairwise absolute correlations is upper bounded by 1 and 2, respectively. Transform them into HR-minimals, which proves the bounds, since the absolute correlation profile is preserved. □

It seems to be true that $R_Q(n-1)=n$ whenever an $n\times n$ Hadamard matrix exists, which is still open. The bound $R_Q(n-2)\geq n$ in Prop. 5 seems to be very lose, and any tighter bound will be an interesting result.

Conjecture 2 *If an* $n\times n$ *Hadamard matrix exists, then* $R_Q(n-1)=n$*.*

Using Theorem 4, we can easily determine the maximum absolute correlation value of a given matrix A if we can find its HR-minimal. Otherwise, we have to check the absolute correlations of all the row-pairs of A.

Definition 5 *Given an* $m\times n$ *binary matrix* A*, we define* $\wp(A)$ *to be the weight of the second row of the HR-minimal of* A*.*

Given a binary matrix A, we denote by c_M the maximum over all the absolute correlations of the row-pairs of A. Consider the HR-minimal H of A. Then the absolute correlation of the top two rows of H must be c_M. Denote by w the weight of the second row of H. Then we see $n-2w=c_M$ or $w=(n-c_M)/2$. Thus, we have $\wp(A)=w$ if and only if $n-2w$ is the maximum absolute correlation of all the row-pairs of A. Note also that $\wp(A)$ is the value shared by all the matrices belonging to the equivalence class of A.

Definition 6 *We define* $R(w,n)$ *to be the maximum such that there exists an* $R(w,n)\times n$ *matrix* A *with* $w=\wp(A)$*.*

Given a length n, the fact that $R(w,n)=k$ implies that (1) there exists a $k\times n$ matrix A with $\wp(A)=w$ but (2) no $(k+1)\times n$ matrix B with $\wp(B)=w$. Note also that $R_Q(n)=R(n/2-1,n)$ if $n\equiv 2 \pmod 4$, and $R_Q(n)=R(\lfloor n/2\rfloor,n)$ otherwise. Now, We can determine $R(w,n)$ directly for some small values of w as in the following theorem.

Theorem 5
1. $R(0,n)=\infty$ *where* $n\geq 1$.
2. $R(1,n)=2^{n-1}$ *where* $n\geq 1$.
3. $R(n,2n)=2$ *where* n *is odd.*
4. $R(2^k,2^{k+1})=2^{k+1}$ *where* $k\geq 0$.
5. *(Hadamard conjecture)* $R(n,2n)=2n$ *where* n *is even.*

proof.

1. Every all-zero matrix is HR-minimal.
2. The HR-minimal matrix A of size $R(1,n)\times n$ with $\wp(A)=1$ must be of the form in which there should not be the same rows and no two rows are complementary of each other.
3. There cannot be three pair-wise orthogonal rows of length $2 \pmod 4$.

4. $2^k \times 2^k$ Hadamard matrix always exists for all $k \geq 0$.
5. Obvious. □

Next we give some bounds on $R(w, n)$. The proofs contain some constructions of new quasi-orthogonal sequences.

Theorem 6 *1.* $R(w, n) \leq R(w, n+1)$ *where* $w \geq 0$ *and* $n \geq 1$. *(Non-decreasing in n)*
2. $R(w, n) \leq R(w+1, n+1)$ *where* $w \geq 0$ *and* $n \geq 1$.
3. $R(w, n) \geq R(w+1, n)$ *where* $w \geq 0$ *and* $n \geq 1$. *(Non-increasing in w)*
4. $R(w, n) \geq \frac{2^{n-1}}{\sum_{i=0}^{w-1} \binom{n}{i}}$ *where* $w \geq 0$ *and* $n \geq 1$.*(Trivial bound)*
5. $R(\min(w_1 n_2, w_2 n_1), n_1 n_2) \geq R(w_1, n_1) R(w_2, n_2)$ *where* $w_1, w_2 \geq 0$ *and* $n_1, n_2 \geq 1$. *(Kronecker expansion)*
6. $R(\min(w_1, w_2), n_1 + n_2) \geq 2R(w_1, n_1) R(w_2, n_2)$ *where* $w_1, w_2 \geq 0$ *and* $n_1, n_2 \geq 1$. *(u+v expansion)*
7. $R(2^k, n) \geq 2^{k+1} R(2^k, n-2^k) \geq 2^{\frac{(k+1)n}{2^k} - (k+1)}$ *where* $n \geq 3 \cdot 2^k$, $n \equiv 0 \pmod{2^k}$ *and* $k \geq 0$.

proof.

1. Using Theorem 3, we can make $R(w, n) \times (n+1)$ matrix A with $w = \wp(A)$ given an $R(w, n) \times n$ matrix.
2. Deleting the rightmost column doesn't increase the absolute correlation more than 1.
3. Obvious by 1) and 2).
4. Given any binary vector $\mathbf{r}$ of length n, there could be at most $2\sum_{i=0}^{w-1} \binom{n}{i}$ vectors whose absolute correlation with $\mathbf{r}$ is at least $n-2w$. This number counts all the vectors in a Hamming distance $w-1$ or less from $\mathbf{r}$ and their complements. Therefore, if we have $R(w, n)$ binary vectors of length n whose pairwise absolute correlation is at most $n-2w$, then, since there are exactly 2^n binary vectors of length n, we have $2^n / R(w, n) \leq 2\sum_{i=0}^{w-1} \binom{n}{i}$.
5. Let A_1 as an $R(w_1, n_1) \times n$ matrix satisfying $\wp(A_1) = w_1$ and A_2 as an $R(w_2, n_2) \times n$ matrix satisfying $\wp(A_2) = w_2$. Now, we can make $R(w_1, n_1) R(w_2, n_2) \times n_1 n_2$ matrix $B = A_1 \otimes A_2$ when the symbol $\otimes$ is a Kronecker product using XOR operation instead multiplying. Next we choose a-th and b-th row of the B and calculate their absolute correlation. We can easily find that the value is not larger than $n_2(n_1 - 2w_1)$ if $a \equiv b \pmod{R(w_2, n_2)}$, and not larger than $n_1(n_2 - 2w_2)$ otherwise.
6. Let A_1 as an $R(w_1, n_1) \times n$ matrix satisfying $\wp(A_1) = w_1$ and A_2 as an $R(w_2, n_2) \times n$ matrix satisfying $\wp(A_2) = w_2$. We can make an $2R(w_1, n_1) R(w_2, n_2) \times (n_1 + n_2)$ matrix B with $\wp(B) = \min(w_1, w_2)$ as follows. Let $A_1^* = a_1(\lceil \frac{i}{2R(w_2, n_2)} \rceil, j)$ where $A_1 = a_1(i, j)$. The size of A_1^* is $2R(w_2, n_2) R(w_1, n_1) \times n_1$. Now, we can make a $2R(w_2, n_2) R(w_1, n_1) \times n_2$ matrix $C = \left[A_2^T | \sim A_2^T | A_2^T | \sim A_2^T | ... \right]^T$. Finally we construct B as $B = \left[A_1^* | C \right]$. Using the similar approach in Kronecker expansion, we can find that $\wp(B) = \min(w_1, w_2)$.
7. We start from the $2^{k+1} \times 2^{k+1}$ Hadamard matrix and use induction. At first, we let an $R(2^k, n-2^k) \times (n-2^k)$ matrix B with $\wp(B) = 2^k$. Let A as a $2^{k+1} R(2^k, n-2^k) \times 2^k$ matrix and $A = a(i, j) = h(\lceil \frac{i}{2R(2^k, n-2^k)} \rceil, j)$ where $H = h(i, j)$ is a $2^k \times 2^k$ Hadamard matrix. Now, we can make a $2^{k+1} R(2^k, n-2^k) \times n$ matrix $C = \left[A | \left[[A | \underline{0}] \oplus B_T \right] \right]$ where B_T is a $2^{k+1} R(2^k, n-2^k) \times n - 2^k$ matrix with the form as $B_T = \left[B^T | \sim B^T | B^T | \sim B^T | ... \right]^T$, $\underline{0}$ is a $2^{k+1} R(2^k, n-2^k) \times 2^k$ all-zero matrix, and $\oplus$ is XOR operation (or modulo 2 addition) of all elements of two matrices with the same size. Using the similar approach in Kronecker expansion, we can find that $\wp(C) = 2^k$. The last term of the inequality is a cumulated form by adopting this bound, started from the $2^{k+1} \times 2^{k+1}$ Hadamard matrix. □

We also have done computer search for $R(w, n)$ for some small w and n. Table 1 shows the result.

4. Properties of Equivalence Classes and H-Minimals

We will begin this section by considering the transpose of HR-minimals. We denote by A^T the transpose of the matrix A.

Definition 7 *If a binary matrix* A^T *is an HR-minimal (of some equivalence class) then we call A a Hadamard-column minimal matrix, or* HC-minimal. *If an HR-minimal is also an HC-minimal, it is called Hadamard-row-column minimal, or* H-minimal.

Remark 10 *An HR-minimal is not always an HC-minimal. Following show three examples of HR-minimals, all of which are not HC-minimals:*

$$\begin{pmatrix} 00000 \\ 00000 \\ 00001 \\ 00110 \\ 00110 \end{pmatrix}, \quad \begin{pmatrix} 00000 \\ 00001 \\ 00110 \\ 01010 \\ 01100 \end{pmatrix}, \quad \begin{pmatrix} 000000 \\ 000001 \\ 000110 \\ 001110 \end{pmatrix}. \tag{5}$$

This implies that not every equivalence class contains the H-minimal, though it always contains both an HR-minimal and an HC-minimal.

We denote by $N_E(m, n)$ the number of inequivalent classes of binary matrices of size $m \times n$. Note that this is the same as the number of inequivalent HR-minimals of the same size.

Proposition 6 (a) *For a given size* $m \times n$*, the number of HR-minimals is the same as that of HC-minimals.* (b) $N_E(m, n) = N_E(n, m)$ *for any positive integers m and n.*

proof. (a) Both of them is equal to the number of inequivalent classes of binary matrices of size $m \times n$. (b) The transpose of any $m \times n$ HC-minimal is an $n \times m$ HR-minimal. □

Proposition 7 $N_E(m, n)$ *is monotonically non-decreasing as m or n increases.*

Table 2 Number of inequivalent HR-minimals.

	n=1	2	3	4	5	6	7	8	9
m=1	**1**	*							
2	1	**2**							
3	1	2	**3**						
4	1	3	5	**12**					
5	1	3	6	18	**39**				
6	1	4	9	35	101	**388**			
7	1	4	11	54	228	1343	**8102**		
8	1	5	15	94	551	5083	53775	**656108**	
9	1	5	18	140	1221	18366	355773	8225529	**199727714**
10	1	6	23	224	2746	66524	2324945	101773978	?
11	1	6	27	326	5850	231189	14591376	?	?
12	1	7	34	495	12338	780372	87435412	?	?
13	1	7	39	699	24994	2526857	?	?	?
14	1	8	47	1012	49708	7884776	?	?	?
15	1	8	54	1397	95771	23655568	?	?	?
16	1	9	64	1955	180759	68431000	?	?	?
17	1	9	72	2634	332252	191016328	?	?	?
18	1	10	84	3579	598631	?	?	?	?
19	1	10	94	4728	1054614	?	?	?	?
20	1	11	108	6271	1823859	?	?	?	?
21	1	11	120	8132	3093591	?	?	?	?
22	1	12	136	10563	5160004	?	?	?	?

* We omit the case $m < n$ since $N_E(m,n) = N_E(n,m)$.

proof. Any $(m-1) \times n$ HR-minimal will induce an $m \times n$ HR-minimal by the add-zero-row in Cor. 5. Therefore, $N_E(m,n) \geq N_E(m-1,n)$ for any m. Similarly for n by the add-zero-column in Theorem. 3. □

Trivially, we have $N_E(1,n) = 1$ for all the positive integers n. For $m = 2$ and $m = 3$, we have the following:

Theorem 7

$$N_E(2,n) = \sum_{a=0}^{\lfloor n/2 \rfloor} 1 = \lfloor n/2 \rfloor + 1,$$

$$N_E(3,n) = \sum_{a=0}^{\lfloor n/2 \rfloor} \sum_{b=\lceil a/2 \rceil}^{\lfloor (n-a)/2 \rfloor} \sum_{c=\max(0,\, a-b)}^{\lfloor a/2 \rfloor} 1.$$

proof. Consider the case $m = 2$. By the item 2 in Theorem 2, any HR-minimal of size $2 \times n$ looks like the following:

$$\begin{array}{c} \underbrace{0\,0\,0\,\cdots\,0\,0\,0}_{n} \\ \underbrace{0\,\cdots\,0}_{n-a}\underbrace{1\,\cdots\,1}_{a} \end{array} \tag{6}$$

Furthermore, the value of a must be in the range $0 \leq a \leq \lfloor \frac{n}{2} \rfloor$, which proves the formula. The case $m = 3$ is proved in Appendix. □

Now, we derive an interesting corollary about the sequence of $N_E(3,n)$, whose proof is given also in Appendix.

Corollary 7 *$N_E(3,n)$ is essentially the same as the number of partitions of integer n into at most 4 parts.* [19]

Remark 11 *Corollary 7 gives another interpretation of the sequence in [19]. In fact, $N_E(2,n)$ is the same as the number of partitions of n into at most 2 parts. However, $N_E(4 = k, n)$ is not the same as the number of partitions of n into at most $8 = 2^{k-1}$ parts, in some complicated reasons.*

Table 3 Number of H-minimals.

	n=4	5	6	7	8
m=4	**12**	*			
5	18	**37**			
6	34	93	**318**		
7	53	197	968	**4624**	
8	90	448	3109	23518	**200127**
9	131	917	9549	118346	?
10	205	1913	29244	?	?
11	292	3728	85549	?	?
12	434	7285	?	?	?

* We omit the case $m < n$ since the numbers at size (m,n) and (n,m) are same.

We have performed an exhaustive search for all the HR-minimals of size $m \times n$ for some small m and n, and the result is shown in Table 2. The question marks in this table represent more than 200 million. We note that the values of $N_E(2,n)$ and $N_E(3,n)$ agree with those given in Theorem 7.

We have also performed an exhaustive search to find the number of different H-minimals, and shown the result in Table 3. We note that, except for the cases $(m,n) = (4,4), (4,5), (5,4)$ which are shown in underline in both tables, the number of $m \times n$ H-minimals is always less than that of $m \times n$ HR-minimals whenever $m, n \geq 4$. We will show this eventually in the following. We begin by the following proposition which is an easy case but with tedious checks.

Proposition 8 *If $m \leq 3$ or $n \leq 3$, then all the HR-minimals of size $m \times n$ are HC-minimals, and hence, H-minimals.*

proof. It is obviously true for any $1 \times n$ HR-minimals and any $2 \times n$ HR-minimals. Consider a $3 \times n$ HR-minimal in $(\mathrm{A}\cdot 1)$. We know from the proof of Theorem 7 that

$$\begin{cases} 0 \le a \le \lfloor n/2 \rfloor, \\ \lceil a/2 \rceil \le b \le \lfloor (n-a)/2 \rfloor, \\ \max(0, a-b) \le c \le \lfloor a/2 \rfloor. \end{cases} \tag{7}$$

Now, going through some similar process as in the proof of Theorem 7, we check that these conditions are necessary and sufficient for (A· 1) to be an HC-minimal. □

We now consider what would happen when we add the all-zero row (Cor. 5) on top of an HR-minimal which is not an HC-minimal.

Proposition 9 *The add-zero-row operation on top of an $m \times n$ HR-minimal A results in an $(m+1) \times n$ HR-minimal which is not an HC-minimal if A is not an HC-minimal.*

proof. We call the result B and suppose that B is an HC-minimal, and hence B^T is an HR-minimal. Let X^T be the HR-minimal in the class to which A^T belongs. We note that $A^T \neq X^T$ and hence $A \neq X$ but $A \sim X$. Now, the add-zero-column on X^T gives the $n \times (m+1)$ HR-minimal Y^T by Theorem 3. Then, observe that $B^T \sim Y^T$ since $A^T \sim X^T$. Since both B^T and Y^T are HR-minimals, we must have $B = Y$ and hence $A = X$, which is a contradiction. □

Remark 12 *It is obvious that the add-zero-column operation on the left-most of an $m \times n$ HR-minimal A results in an $m \times (n+1)$ HR-minimal which is not an HC-minimal if A is not an HC-minimal.*

Theorem 8 *Every $m \times n$ HR-minimal is an HC-minimal (and hence, H-minimal) if and only if $m \le 3$, $n \le 3$, or $(m, n) = (4, 4), (4, 5)$ or $(5, 4)$.*

proof. Prop. 8 shows every $m \times n$ HR-minimal is an HC-minimal for $m \le 3$ or $n \le 3$. By computer search, we conclude also that all the HR-minimals are HC-minimals for the sizes 4×4, 4×5, and 5×4, which are shown in both Tables 2 and 3 in underline. Now, assume that $m \ge 4$, $n \ge 4$ and $m + n \ge 10$, and we note the three examples of HR-minimals in (5), which are not HC-minimals, of sizes 5×5, 5×5 and 4×6, respectively. The add-zero-row operation (Cor. 5) k times on C will give a $(4+k) \times 6$ HR-minimal for all $k \ge 1$, which is not an HC-minimal by Prop. 9. All these can be extended to $(4+k) \times (6+l)$ HR-minimals by the add-zero-column operation in Theorem 3, which are neither HC-minimals since all the $(4+k) \times 6$ ones are not HC-minimals in the beginning. Similarly for the sizes $5 \times (5+l)$ using the first two examples in (5). □

We now concentrate on the diagonal entries in Tables 2 and 3 (shown in bold type). They represent the number of HR-minimals and H-minimals of square sizes, respectively. We have also done some search for symmetric H-minimals of square sizes, and the result is shown in Table 4 with various ratios.

It is obvious by the add-zero-row and add-zero-column operations that the the number of $n \times n$ H-minimals or symmetric H-minimals monotonically increases as n increases. It would be interesting in the future to determine how fast (or slowly) it increases as n increases.

Table 4 Number of H-minimals and symmetric H-minimals.

Size	NE	NH	NS	NH/NE	NS/NE	NS/NH
1×1	1	1	1	1.000	1.000	1.000
2×2	2	2	2	1.000	1.000	1.000
3×3	3	3	3	1.000	1.000	1.000
4×4	12	12	8	1.000	0.667	0.667
5×5	39	37	19	0.950	0.487	0.514
6×6	388	318	70	0.820	0.180	0.220
7×7	8102	4624	336	0.571	0.415	0.727
8×8	656108	200127	2675	0.305	0.041	0.134

- NE: Total Number of Equivalence Classes
- NH: Number of Classes containing H-minimal
- NS: Number of Classes containing Symmetric H-minimal

We will finish this section by summarizing this.

The all-zero matrix is an HR-minimal, HC-minimal, and symmetric H-minimal for all $n \times n$. The 2×2 matrix $(00; 01)$ can be extended to $n \times n$ with ρ value equal to 1 by add-zero-row and add-zero-column. They are all HR-minimals, HC-minimals, and symmetric H-minimals. There are many possibilities in this way to extend the size but they are all trivial in the sense that eventually the all-zero rows or all-zero columns dominate.

We now consider some non-trivial cases. Let I_v be the $v \times v$ identity matrix. Flip this matrix so that the diagonal comes in the other direction. Finally, complement the right-most column and the bottom row so that it becomes normalized. It is easy to check that the result is an HR-minimal with the weight of its second row equals to 2, and hence the pairwise absolute correlation of the rows is upper bounded by $v - 4$.

The above idea can be generalized to construct an $v \times v$ HR-minimal. For this we consider a cyclic (v, k, λ) difference set D [1], [3], [4], [20]. It is a k-subset of the integers mod v, such that the equation $x - y \equiv d \pmod{v}$ has exactly λ solution pairs (x, y), $x, y \in D$ for all the non-zero residues d mod v. It is well-known that the characteristic sequence $\{a_i\}$ of length v of a cyclic (v, k, λ) difference set D has two-level periodic autocorrelation all of whose out-of-phase values are the constant given as $v - 4(k - \lambda)$. This value is the dot-product of the sequence-vector of length v and any of its cyclically shifted versions [1], [3], [4], [20].

Consider a $v \times v$ matrix A given by the following:

1. Construct a cyclic (v, k, λ) difference set D and its characteristic sequence $\{a_i\}$ of length v.
2. Use the sequence $\{a_i\}$ of length v as a top row of the matrix A.
3. Fill the remaining rows of A by all the cyclic shifts of its top row.

Then, v rows of A form a set of v binary vectors of length v such that the pairwise dot-product is a constant $v - 4(k - \lambda)$. Therefore, the minimal matrix in the equivalence class containing A is an HR-minimal, whose second row has the weight $2(k - \lambda)$. This proves the following:

Proposition 10 *If a cyclic (v, k, λ) difference set exists, then*

there exists a $v \times v$ HR-minimal whose second row has the weight $2(k-\lambda)$, and all the pairwise absolute correlations of the rows are constant $|v-4(k-\lambda)|$.

We note that the top row of the identity matrix of size $v \times v$ earlier is a characteristic sequence of a trivial cyclic difference set, where $k = 1$ and $\lambda = 0$ and $D = \{0\}$.

The HR-minimal in the above proposition will be, in fact, a $v \times v$ minimal QH matrix if and only if $w = 2(k-\lambda)$ satisfies the condition in Definition 4 with $n = m = v$. One famous such case would be when the cyclic difference set has parameters $v = 4t-1$, $k = 2t-1$ and $\lambda = t-1$ for some integer t, and it is called a cyclic Hadamard difference set of length v. The connection between this with a cyclic Hadamard matrix of order $v+1$ is well-known [1], [3], [4], [15], [20]. If we use a cyclic Hadamard difference set D of length v in constructing the matrix A above, then the pairwise absolute correlation is a constant 1 and the minimal matrix in the equivalence class containing A is a minimal QH matrix of size $v \times v$. This proves the following:

Corollary 8 *If a cyclic Hadamard difference set of length v exists, then there exists a $v \times v$ minimal QH matrix.*

We note finally that the above $v \times v$ minimal QH matrix in Cor. 8 can be extended to a $(v+1)\times(v+1)$ minimal Hadamard matrix by adjoining the all-zero row at the top and all-zero column on the left-most. This is called a Hadamard matrix of "cyclic type."

5. Concluding Remarks

In this paper, we proposed a new problem on the classification of binary matrices with respect to the Hadamard equivalence. In the development, we have introduced HR-minimals and Quasi-Hadamard matrices, and investigated the properties of various equivalence classes of binary matrices.

A Quasi-Hadamard matrix of size $m \times n$ gives a set of m binary vectors of length n whose maximum pairwise absolute correlation is minimized over all the m-sets of such binary vectors.

We finish this paper with a list of some open problems for the readers:

1. Find a systematic construction for $m \times n$ HR-minimals or (minimal) QH matrices, other than indirectly using some cyclic difference sets. (Sect. 4)
2. The weight of the second left-most column of an $m \times n$ HR-minimal cannot exceed $m/2$. (Remark 2)
3. There exists an $n \times n$ minimal QH matrix for all $n \geq 2$ except for $n \equiv 1 \pmod 8$. (Conjecture 1)
4. If an $n \times n$ Hadamard matrix exists for $n \geq 4$, then $R_Q(n-1) = n$. (Conjecture 2)
5. Determine the value $R(w, n)$ for any w, n.
6. Determine the number of inequivalent $m \times n$ QH classes for $2 < m \leq R_Q(n)$.
7. Determine the value $N_E(m, n)$ for any $m > 3$. See Theorem 7 and Tables 2 and 3.
8. Determine the number of $n \times n$ H-minimals or symmetric H-minimals (Table 4). Or else, determine how fast they grow as n increases.

References

[1] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics, vol.182, Springer-Verlag, New York, 1971.
[2] M. Bossert, "Hadamard matrices and codes," in Encyclopedia of Telecommunications, ed. J.G. Proakis, vol.2, pp.929–935, John Wiley & Sos, 2003.
[3] C. Colbourn and J. Dinitz (editors) Handbook of Combinatorial Designs, 2nd ed., Chapman & Hall/CRC, 2007.
[4] S.W. Golomb and G. Gong, Sequence Design for Good Correlation, Cambridge University Press, 2005.
[5] G. Gong, S.W. Golomb, and H.-Y. Song, "A note on low correlation zone signal sets," IEEE Trans. Inf. Theory, vol.53, no.7, pp.2575–2581, July 2007.
[6] J. Hadamard, "Résolution d'une question relative aux déterminants," Bull. des Sciences Math., vol.2, pp.240–246, 1893.
[7] A. Hedayat and W.D. Wallis, "Hadamard matrices and their applications," The Annals of Statistics, vol.6, no.6, pp.1184–1238, 1978.
[8] B.D. McKay, "Hadamard equivalence via graph isomorphism," Discrete Mathmatics, vol.27, pp.213–214, 1979.
[9] K.J. Horadam, Hadamard matrices and their applications, Princeton University Press, 2007.
[10] H. Kimura, "Hadamard matrices of order 28 with automorphism groups of order two," J. Combin. Theory, A, vol.43, pp.98–102, 1986.
[11] H. Kimura, "New Hadamard matrix of order 24," Graphs Combin., vol.5, pp.235–242, 1989.
[12] H. Kimura, "Classification of Hadamard matrices of order 28," Discrete Math., vol.133, pp.171–180, 1994.
[13] H. Kharaghani and B. Tayfeh-Rezaie, "On the classification of hadamard matrices of order 32," J. Combinatorial Design, vol.18, no.5, pp.328–336, 2010.
[14] K.-H. Park and H.-Y. Song, "Hadamard equivalence of binary matrices," Proc. 2009 Asia-Pacific Conference on Communications, pp.454–458, Shanghai, China, 2009.
[15] H.-Y. Song and S.W. Golomb, "On the existence of cyclic Hadamard difference sets," IEEE Trans. Inf. Theory, vol.40, no.4, pp.1266–1268, July 1994.
[16] E. Spence, "Classification of Hadamard matrices of order 24 and 28," Discrete Math., vol.140, no.1-3, pp.185–243, 1995.
[17] D.R. Stinson, Cryptography, Theory and Practice, second ed., CRC Press, Chapman & HALL/CRC, 2002.
[18] N.J.A. Sloane, On-line Library of Hadamard Matrices, http://www.research.att.com/~njas/hadamard/index.html
[19] N.J.A. Sloane, A Handbook of Integer Sequences, Academic Press, 1973. (A001400 in The On-Line Encyclopedia of Integer Sequences, http://oeis.org)
[20] J.H. van Lint and R.M. Wilson, A Course in Combinatorics, Cambridge University Press, 1992.

Appendix A: Proof of the formula $N_E(3, n)$

Consider the case $m = 3$. Since any $3 \times n$ HR-minimal must have the top two rows described by Theorem 2, and can be reduced to a $2 \times n$ HR-minimal by Prop. 2, we have the following situation, including some integer variables a, b, and c:

$$\begin{array}{l} \underbrace{0\,0\,0\,0\,0\,0\,0\,\cdots\,0\,0\,0\,0\,0\,0\,0}_{n} \\ \underbrace{0\,0\,0\,\cdots\,0\,0\,0}_{n-a}\underbrace{1\,1\,1\,\cdots\,1\,1\,1}_{a} \\ \underbrace{0\,\cdots\,0}_{n-a-b}\underbrace{1\,\cdots\,1}_{b}\underbrace{0\,\cdots\,0}_{a-c}\underbrace{1\,\cdots\,1}_{c} \end{array} \quad (\mathrm{A}\cdot 1)$$

From the same reason as in the proof of Theorem 2, the values a, b, and c are restricted to the following:

$$\begin{cases} 0 \le a \le \lfloor \frac{n}{2} \rfloor \\ 0 \le b \le \lfloor \frac{n-a}{2} \rfloor \\ 0 \le c \le \lfloor \frac{a}{2} \rfloor \end{cases} \quad (\mathrm{A}\cdot 2)$$

Now, consider all the possible equivalent $3\times n$ matrices with the one in (A· 1). They are obtained by taking one of six permutations of three rows, complementing those columns with the top entry 1 if necessary, complementing the second and/or third rows, and then finally taking the column-permutation so that the final form looks like the following:

$$\begin{array}{l} \underbrace{0\,0\,0\,0\,0\,0\,0\,\cdots\,0\,0\,0\,0\,0\,0\,0}_{n} \\ \underbrace{0\,0\,0\,\cdots\,0\,0\,0}_{n-d}\underbrace{1\,1\,1\,\cdots\,1\,1\,1}_{d} \\ \underbrace{0\,\cdots\,0}_{n-d-e}\underbrace{1\,\cdots\,1}_{e}\underbrace{0\,\cdots\,0}_{d-f}\underbrace{1\,\cdots\,1}_{f} \end{array}. \quad (\mathrm{A}\cdot 3)$$

The values of d, e, and f are shown below in each cell of the table as a column, where the top row represents six permutations of three rows and the left-most column represents four CRs:

PRs \ CRs	-	3	2	23
(123)	a b c	a $n-a-b$ $a-c$	$n-a$ c b	$n-a$ $a-c$ $n-a-b$
(132)	$b+c$ $a-c$ c	$b+c$ $n-a-b$ b	$n-b-c$ c $a-c$	$n-b-c$ b $n-a-b$
(213)	a b $a-c$	a $n-a-b$ c	$n-a$ $a-c$ b	$n-a$ c $n-a-b$
(231)	$a+b-c$ c $a-c$	$a+b-c$ $n-a-b$ b	$n-a-b+c$ $a-c$ c	$n-a-b+c$ b $n-a-b$
(312)	$b+c$ $a-c$ b	$b+c$ $n-a-b$ c	$n-b-c$ b $a-c$	$n-b-c$ c $n-a-b$
(321)	$a+b+c$ c b	$a+b-c$ $n-a-b$ $a-c$	$n-a-b+c$ b c	$n-a-b+c$ $a-c$ $n-a-b$

In order for the $3\times n$ matrix in (A· 1) be an HR-minimal, the values d, e, and f in (A· 3) must satisfy the following:

- $d \ge a$,
- if $a = d$ then $e \ge d$, and
- if $a = d$ and $b = e$ then $f \ge c$.

Substituting the values of d, e, f in the above table into these conditions gives various new conditions for a, b, and c. For example, for the value $(d, e, f) = (b + c, a - c, c)$ in the cell of the table corresponding to no-CR and (132), we have:

- $b + c \ge a$, which is a new condition;
- if $b + c = a$, then $a - c \ge b$, which is always true;
- if $b + c = a$ and $a - c = b$, then $c \ge c$, which is always true.

Going through all the twenty-four cases, similarly, gives some more new conditions, all of which are compactly summarized as the following two:

$$\begin{cases} \lceil \frac{a}{2} \rceil \le b, \\ a - b \le c. \end{cases} \quad (\mathrm{A}\cdot 4)$$

Now, $N_E(3, n)$ is exactly the same as the number of different triples of (a, b, c) satisfying the conditions in (A· 2) and (A· 4). □

Appendix B: Proof of Cor.7

We can make an integer sequence $(n-a-b, b, a-c, c)$ from (A· 1). By the proof, in an HR-minimal the inequality $n - a - b \ge b \ge a - c \ge c \ge 0$ holds. So it becomes a kind of partitions of integer n into at most 4 parts. Moreover, two different $3 \times n$ HR-minimals have different sequence since a, b, and c can't be changed to make same sequence. Also, every partitions can make corresponding integer sequence and unique HR-minimal since the sorting condition $n - a - b \ge b \ge a - c \ge c \ge 0$ ensures $b + c \ge a$ and $b \ge c$. So there is a one to one correspondence between $3 \times n$ HR-minimals and partitions of integer n into at most 4 parts. □

Ki-Hyeon Park was born in Iksan, Republic of Korea, on July 9, 1984. He received the B.S. and the M.S. degree in Electrical and Electronic Engineering from the Yonsei University of Seoul, Korea, in 2007 and 2009, respectively. He is currently a Ph.D. student working in Coding and Crypto Lab (CCL) at Yonsei University. His area of research interest includes cryptography, coding theory, and combinatorial mathematics.

Hong-Yeop Song received his B.S. degree in Electronic Engineering from Yonsei University in 1984, MSEE and Ph.D. degrees from the University of Southern California, Los Angeles, CA, in 1986 and 1991, respectively, specializing in the area of communication theory and coding. He spent 2 years as a senior engineer at Qualcomm Inc., San Diego, CA, from 1994 to 1995, contributed to a team developing North American CDMA Standards for PCS and cellular air-interface systems. Finally, in the fall of 1995, he joined the Dept. of Electrical and Electronic Engineering at Yonsei University, Seoul, Korea, and is currently working as a professor. He visited Dr. G. Gong at University of Waterloo, Canada, in the year 2002. He is interested in Communication and Coding Theory, including error-correcting codes, PN sequences, and crypto algorithms. He is a senior member of IEEE, member of MAA(Mathematical Association of America), and domestic societies: IEEK, KICS, KIISC and KMS(Korean Mathematical Society).