Hadamard Equivalence on Binary Matrices

- new combinatorial problem

Ki-Hyeon Park and Hong-Yeop Song
hysong@yonsei.ac.kr

Coding and Crypto Lab
School of Electrical and Electronic Engineering
Yonsei University

December 16-19
2009 Joint meeting of AMS-KMS
Ewha Womans University
Seoul, Korea

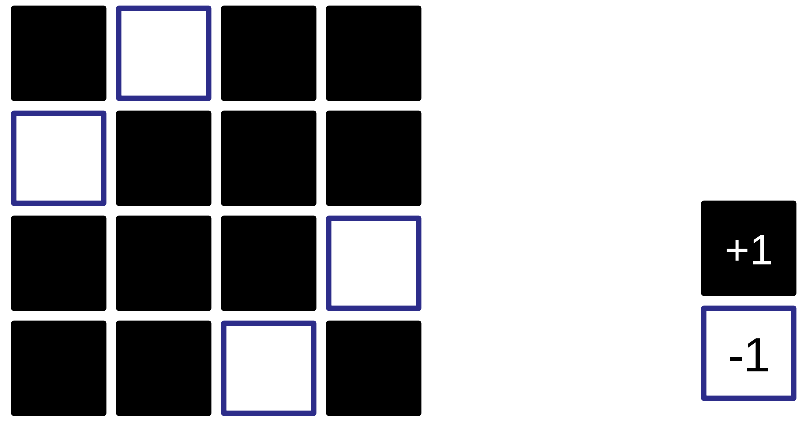
In this talk

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- **Introduction**
  - Hadamard Matrix
  - Hadamard Equivalence
- **Main Results**
  - Classification of binary matrices
  - Pseudo-Hadamard matrices
  - Some Theorems and a Conjecture
  - Result of Exhaustive Search and More
- **Concluding Remarks**
  - More Conjectures and Open Problems

Hadamard Matrix

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111



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

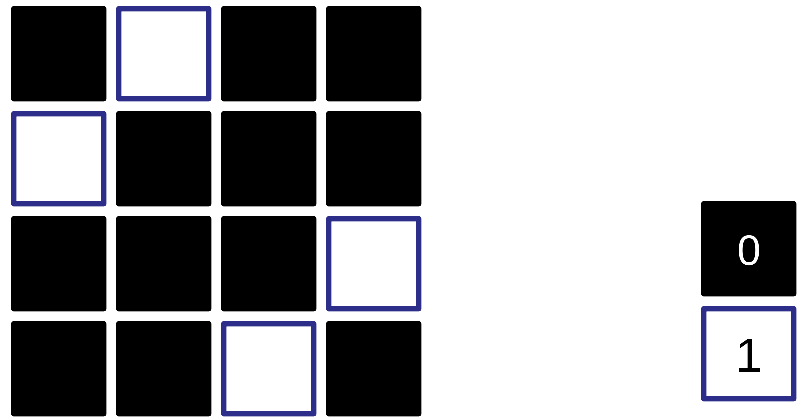
$$H\,H^T = n\,I,$$

where I is the $n \times n$ identity matrix.

- **Hadamard Conjecture:** There exists a Hadamard matrix of order every multiple of 4.

Hadamard Matrix over {0, 1}

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111



- A Hadamard matrix can be represented as a binary matrix over {0,1}.

- In this talk, we consider the binary matrices over {0,1} .

Studies on Hadamard Matrices

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- **Hadamard matrix is widely used in communications and signal processing engineering:**
  - Orthogonal Channelization in CDMA communication systems
  - Construction of orthogonal signals and LCZ/ZCZ signals
  - Hadamard Transform is widely used in image processing

- **Theoretical/Mathematical research on Hadamard matrices:**
  - Existence/Constructions
  - Classification/Equivalence

- **This paper is to study the classification of binary matrices in terms of Hadamard equivalence**

Hadamard Equivalence on Binary Matrices

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- **Definition 1 (Hadamard-preserving operation)**
  - PC/PR: Permuting columns (PC) / rows (PR)
  - CC/CR: Complementing a column (CC) / a row (CR)

- **Definition 2 (Hadamard Equivalence)**

  Two binary matrices of the same size are said to be hadamard-equivalent if one can be converted to the other by some combinations of the hadamard-preserving operations.

- **Hadamard-equivalent binary matrices have the same correlation property (in absolute value).**
  - We use the alphabet {0,1}, so the correlation is calculated as the difference between the number of agreements and that of disagreements of the components.

Number of inequivalent Hadamard matrices

1000000100000110000101000111100100010110011101010011111010000011100010010011011010110111101100011010010111011100110010101011111111

Size	Number	Reference
1, 2, 4, 8, 12	1	
16	5	
20	3	
24	60	Kimura, 1989
28	487	Kimura, 1994
>32	Unknown	

Integer Representation of Binary Matrices

100000010000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

- **Definition 3**: Let $A = (a_{ij})$ be an $m \times n$ binary matrix where $i = 1, 2, \ldots, \mathrm{m}$ and $j = 1, 2, \ldots, \mathrm{n}$. We define a map ρ as

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

- **Example:**

$$\rho\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} = \begin{matrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix}$$
$$= 0000001101010110_{(2)} = 854.$$

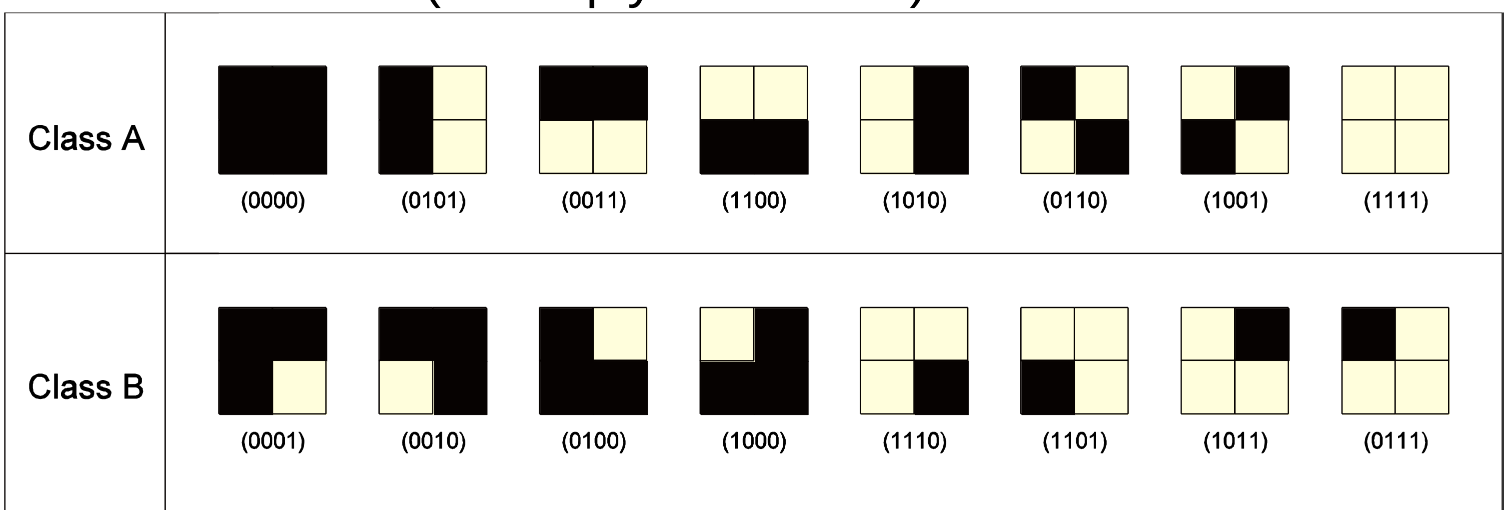
- **Proposition 1:** Let A and B be two binary matrices of the same size. Then,

$$\rho(A) = \rho(B) \text{ if and only if } A = B.$$

Representation of equivalence Class

1000000100000011000010100011110010001011001110101001111101000011100010010011011010110111101100011010010111011100110010101011111

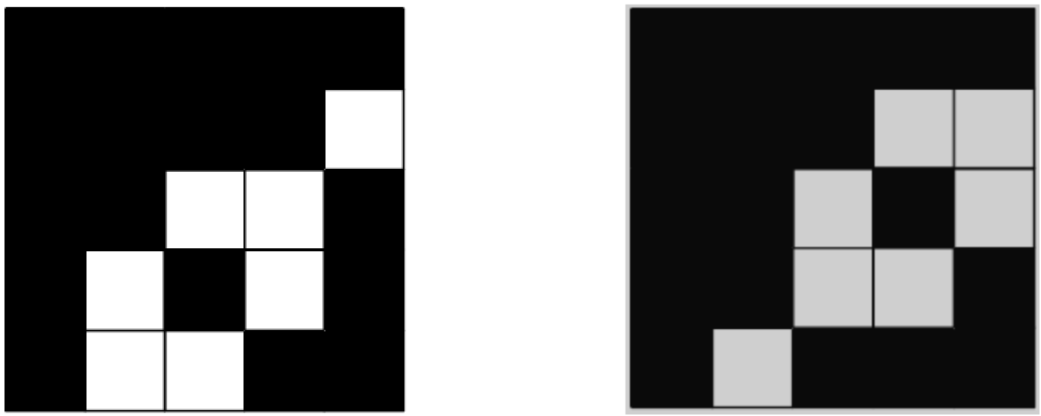
- **Definition 4: (HR-minimal, HC-minimal, H-minimal)**
  - A binary matrix A is a Hadamard-row-minimal matrix (or simply HR-minimal) if $\rho(A) \leq \rho(B)$ for all B which are hadamard-equivalent with A
  - A binary matrix A is a Hadamard-column-minimal matrix (or simply HC-minimal) if A^T is an HR-minimal
  - If a matrix is both HR-minimal and HC-minimal, it is a Hadamard-minimal matrix (or simply H-minimal)



HR-minimal and HC-minimal

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

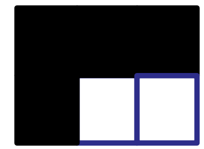
- These two matrices are hadamard-equivalent:



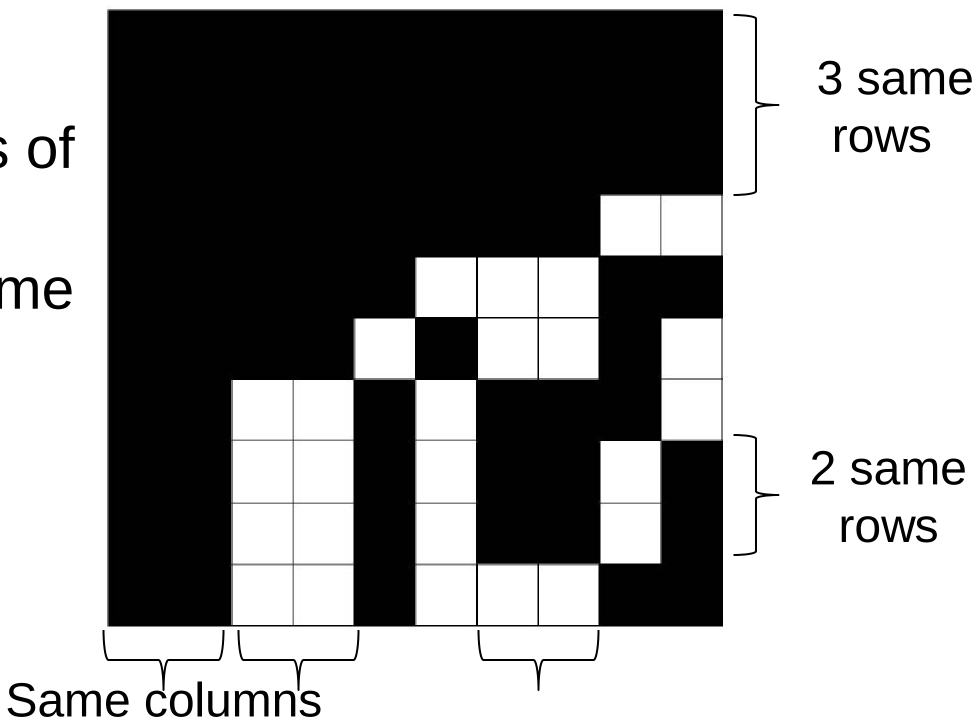
- Left one is HR-minimal but not HC-minimal. Note that it is column-sorted.
- An HR-minimal is not always an HC-minimal, and vice versa.
- The above shows the smallest size of the class with no H-minimal.

Properties of HR-minimals

- **Proposition 2:** An HR-minimal is row-sorted, and also, column-sorted. The converse is not true in general.



- **Corollary 1:** Two same rows of an HR-minimal must be adjacent. So must be two same columns.

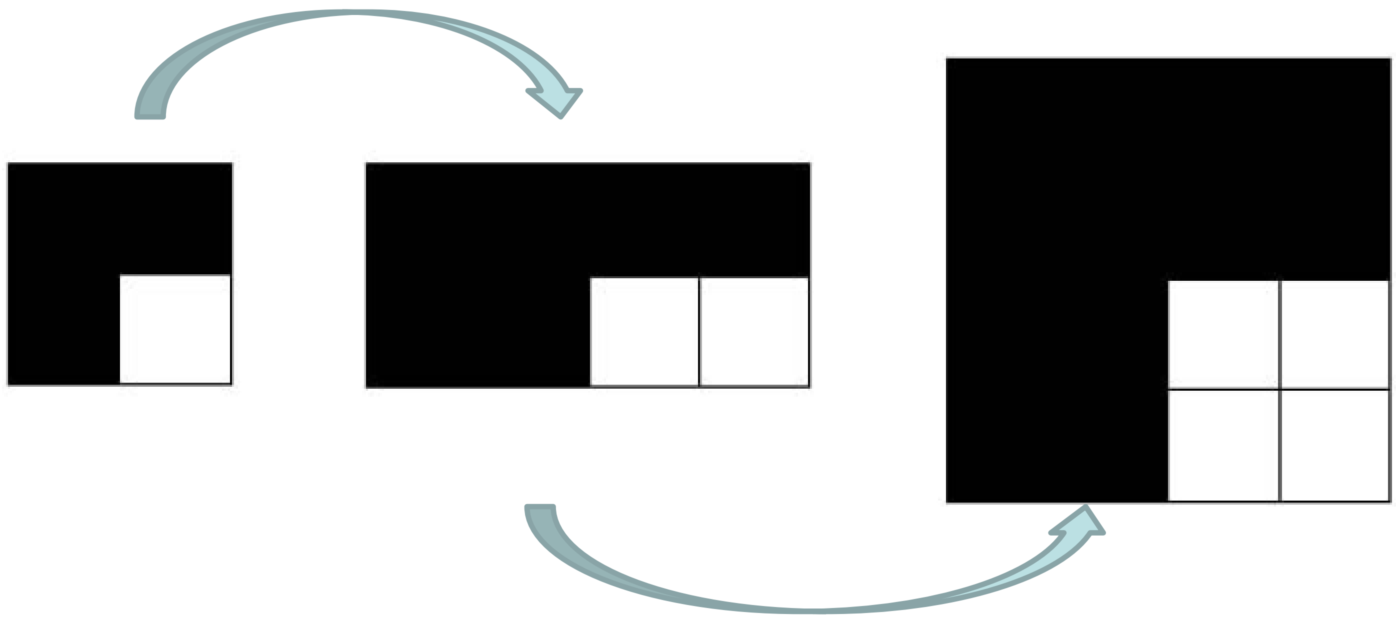


Properties of HR-minimals

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- **Theorem 1 (Linear Expanding Construction)**: Let $A = (a_{ij})$ be an $m \times n$ HR-minimal, and k and l be positive integers. Then $B = (b_{ij})$ of size $km \times ln$ is also an HR-minimal, where

$$b_{ij} = a_{\lfloor \frac{i+k-1}{k} \rfloor \lfloor \frac{j+l-1}{l} \rfloor}$$

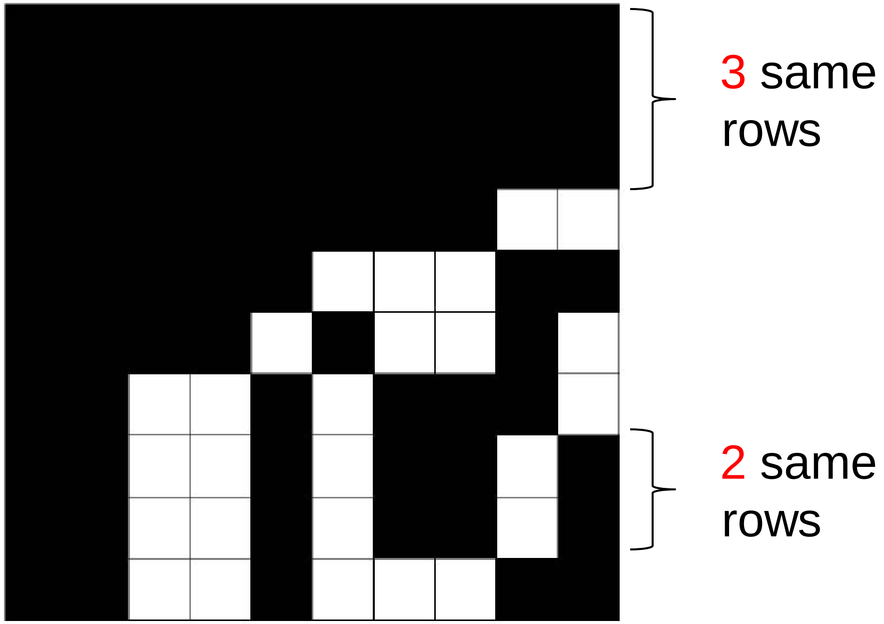


Properties of HR-minimals

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

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

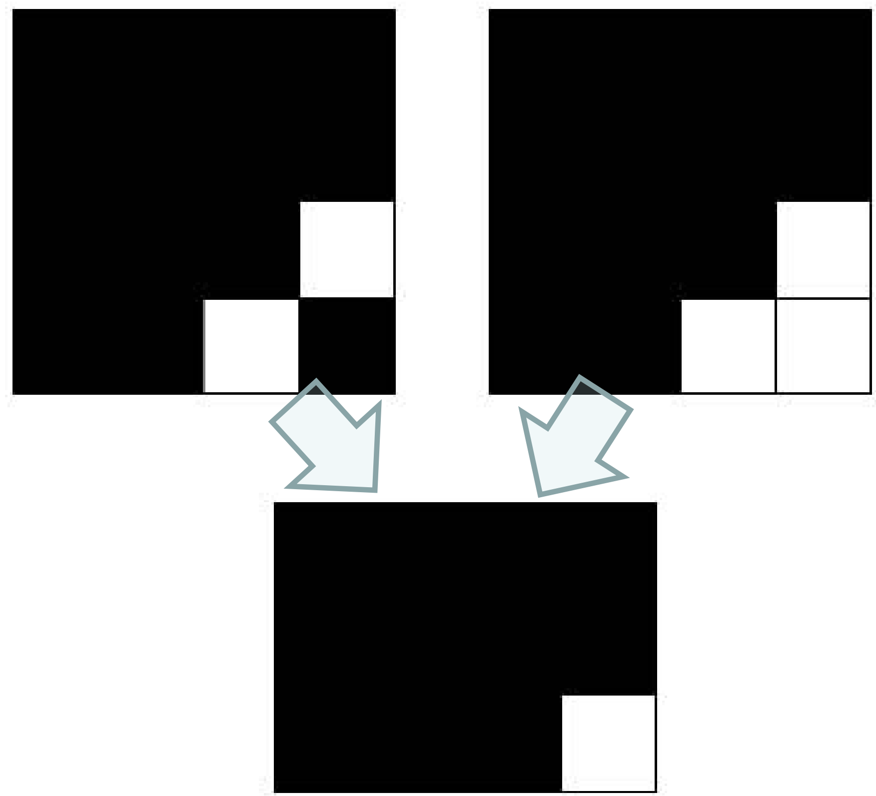
- **Corollary 2 (All-zero-row Adjoining Construction):** We can construct an $(m+1) \times n$ HR-minimal by adjoining the all-zero row at the top of an $m \times n$ HR-minimal.



- Repeating any other row not necessarily preserves the HR-minimality.

Properties of HR-minimals

- **Proposition 4:** If A is an $m \times n$ HR-minimal, then the $(m\text{-}1) \times n$ matrix obtained by deleting the bottom row of A is also an HR-minimal.



A Theorem toward Hadamard Conjecture

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

Theorem 2: Fix a positive integer n and consider the set S_n of all the HR-minimals of size $n \times n$. Let $A \in S_n$. Then the following holds:

① The weight of the second row of A is upper bounded by:

a. 1 when $n = 2$,

b. $(n\text{-}1)/2$ when $n \equiv 1 \bmod 2$,

c. $(n\text{-}2)/2$ when $n \equiv 2 \bmod 4$ except for $n = 2$, and

d. $n/2$ when $n \equiv 0 \bmod 4$.

② For $n \equiv 0 \bmod 4$, if the matrix A which attains the upper bound above on the weight of its second row, then it must be a Hadamard matrix, and conversely for the HR-minimal of any Hadamard matrix.

Second Row of HR-minimals

- If the weight is w, then the correlation of the top row (= all-zero-row) and itself becomes:

  $$\#\text{Agreements} - \#\text{Disagreements} = n - 2w.$$

- Note that the value $|n - 2w| = C_{max}$ is maximum (in absolute value) over the correlations of all possible pairs of rows of the HR-minimal.
- Therefore, the HR-minimal A with largest weight in its second row gives a set of row vectors with the lowest possible pairwise correlations.
- **Definition 5 (Pseudo-Hadamard Matrix)**

  An $n \times n$ HR-minimal A is called as pseudo-hadamard matrix (PH matrix) of order n if the weight of its second row attains the upper bound in Theorem 2. So are all its hadamard-equivalent matrices.

Existence of PH Classes

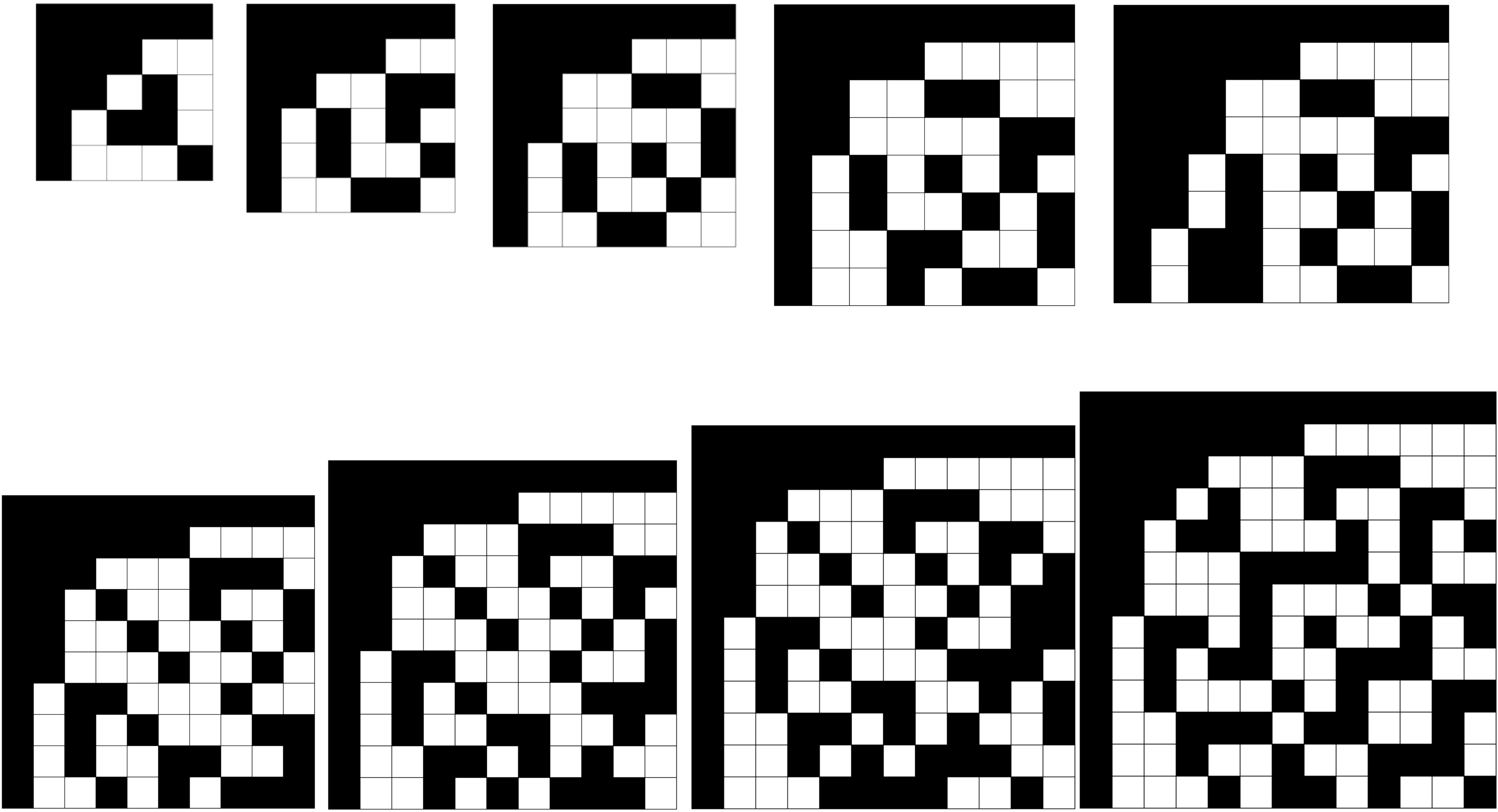
1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- Note that the pseudo-hadamard matrix is a hadamard matrix when $n \equiv 0 \bmod 4$.
- It is a generalized concept of hadamard matrices to the orders $n \neq 0 \bmod 4$.
- The result of computer search for some small values of n is shown here. Observe that there does not exist a pseudo-hadamard matrix of order 9.

Order	Number of inequivalent PHCs
3	1
4	1
5	1
6	15
7	1
8	1
9	0
10	4718
11	1
12	1
13	1
14	> 1,000,000
15	5
16	5

Examples of PH Matrices

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111



Main Conjecture

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

Conjecture 1: There exists a pseudo-Hadamard matrix of all positive orders n except for n=9.

- The truth of this conjecture for $\boldsymbol{n \equiv 0 \bmod 4}$ implies and implied by the Hadamard Conjecture.

Number of Equivalence Classes

1000000100000011000010100011110010001011001110101001111101000011100010010011011010110111101100011010010111011100110010101011111111

- **Definition 5:** We denote by $N_E(m, n)$ the number of equivalence classes of binary matrices of the size $m \times n$.

- **Proposition 5:**
  - For a given size $m \times n$, the number of HR-minimals is the same as that of HC-minimals.
  - $N_E(m, n) = N_E(n, m)$ for any positive integers m and n.

- **Corollary 3 (of Corollary 2):** $N_E(m, n)$ is monotonically non-decreasing as m and n increases.

Some Formula

10000001000000110000101000111100100010110011101010011111010000111000100100110110101101111011000

Theorem 3:

$$N_E(1,n) = 1$$

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

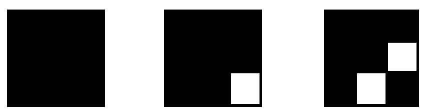
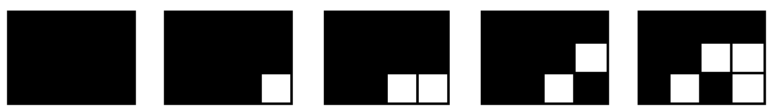
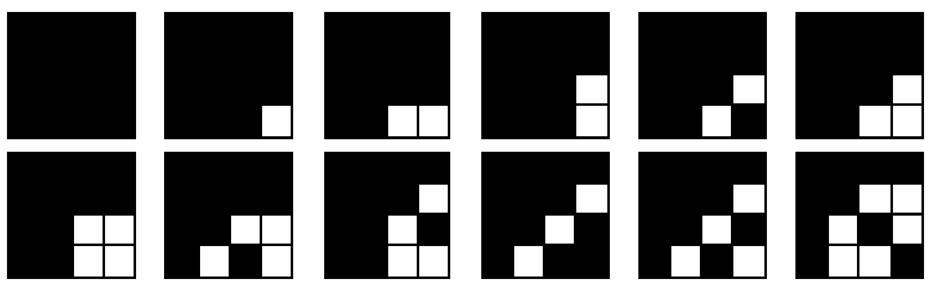
$$N_E(3,n) = \sum_{a=0}^{\lfloor \frac{n}{2} \rfloor} \sum_{b=\lfloor \frac{a}{2} \rfloor}^{\lfloor \frac{n-a}{2} \rfloor} \sum_{c=\max(0,a-b)}^{\lfloor \frac{a}{2} \rfloor} 1$$

m \ n	1	2	3
1	1	1	1
2	1	2	2
3	1	2	3
4	1	3	5
5	1	3	6
6	1	4	9
7	1	4	11
8	1	5	15
9	1	5	18
10	1	6	23
11	1	6	27
12	1	7	34
13	1	7	39
14	1	8	47
15	1	8	54
16	1	9	64
17	1	9	72
18	1	10	84
19	1	10	94
20	1	11	108

Some Exhaustive Search

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

All the HR-minimals of small sizes

Size	Inequivalent Minimal Matrices	Number
2 x 2		2
2 x 3		2
2 x 4		3
3 x 3		3
3 x 4		5
4 x 4		12

Total Number of the Equivalence Classes

m \ n	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2	1	**2**	2	3	3	4	4	5
3	1	2	**3**	5	6	9	11	15
4	1	3	5	**12**	18	**35**	**54**	**94**
5	1	3	6	18	**39**	**101**	**228**	**551**
6	1	4	9	**35**	**101**	**388**	**1343**	**5083**
7	1	4	11	**54**	**228**	**1343**	**8102**	**53775**
8	1	5	15	**94**	**551**	**5083**	**53775**	**656108**
9	1	5	18	**140**	**1221**	**18366**	**355773**	
10	1	6	23	**224**	**2746**	**66524**		
11	1	6	27	**326**	**5850**	**231189**		
12	1	7	34	**495**	**12338**	**780372**		
13	1	7	39	**699**	**24994**			
14	1	8	47	**1012**	**49708**			
15	1	8	54	**1397**	**95771**			
16	1	9	64	**1955**	**180759**			

Total Number of H-minimals

m \ n	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2	1	2	2	3	3	4	4	5
3	1	2	3	5	6	9	11	15
4	1	3	5	12	18	**34**	**53**	**90**
5	1	3	6	18	37	**93**	**197**	**448**
6	1	4	9	**34**	**93**	318	**968**	**3109**
7	1	4	11	**53**	**197**	**968**	4624	**23518**
8	1	5	15	**90**	**448**	**3109**	**23518**	200127
9	1	5	18	**131**	**917**	**9549**	**118346**	
10	1	6	23	**205**	**1913**	**29244**		
11	1	6	27	**292**	**3728**	**85549**		
12	1	7	34	**434**	**7285**			
13	1	7	39					
14	1	8	47					
15	1	8	54					
16	1	9	64					

Various ratios of H-minimals

10000001000000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

Size	Total No. of Eq. Classes (T)	No. of Classes containing H-minimal (H)	No. of Classes containing Symmetric H-minimal (S)	Ratio of H/T(%)	Ratio of S/T(%)	Ratio of S/H(%)
1x1	1	1	1	**100**	**100**	**100**
2x2	2	2	2	**100**	**100**	**100**
3x3	3	3	3	**100**	**100**	**100**
4x4	12	12	8	**100**	66.67	66.67
5x5	39	37	19	94.87	48.72	51.35
6x6	388	318	70	81.96	18.04	22.01
7x7	8102	4624	336	57.07	4.147	7.266
8x8	656108	200127	2675	30.50	0.4077	1.337

- Is the number going to increase monotonically?
  - Will it ever touch the value 0? - No, because of the all-zero matrix.
- Is the ratio going to decrease down to zero indefinitely?

Properties of H-minimals

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- **Proposition 6**: If A is an HR-minimal but not HC-minimal, then the matrix obtained by adjoining the all-zero-row at the top of A is (still an HR-minimal) but not an HC-minimal either.

- **Theorem 4:** Every equivalence class of size $m \times n$ contains H-minimal if and only if $m \leq 3$, $n \leq 3$, 4×4, 4×5, or 5×4.

Concluding Remarks

- We propose:
  - A new problem on the classification of binary matrices in terms of the Hadamard equivalence.
  - Canonical forms that represent the equivalence classes.
  - Properties of HR-minimals and H-minimals.
  - Definition of Pseudo-Hadamard matrix
- We perform exhaustive search to determine the number of **equivalence classes** (and **H-minimals**, and also **pseudo-hadamard matrix classes**) of some small sizes.
- We leave some unsolved problems. One of them is related with the Hadamard conjecture:

For n which is a multiple of 4,

the set of all the HR-minimals of size $n \times n$

contains a Hadamard matrix.