A Note on Classification of Binary Signal Set in the View of Hadamard Equivalence

Ki-Hyeon Park and Hong-Yeop Song

Coding and Crypto Lab
Yonsei University, Seoul, KOREA

The Fourth International Workshop on Signal Design and its Application in Communications (IWSDA'09)
Fukuoka International Congress Center in Fukuoka, Japan
October 19-23, 2009

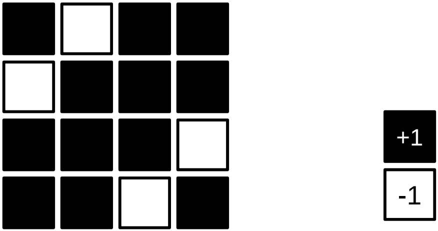
Contents

In this talk

- A Brief Review about the Hadamard Equivalence
- Basic Definitions and Theorems
- Proposed Scheme and its Applications
- Some New Problems and Concluding Remarks

A Brief Review about the Hadamard Equivalence

Hadamard Matrix



- 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

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

where I is the $n \times n$ identity matrix.
- In other word, the rows of a Hadamard matrix are orthogonal

Studies on Hadamard Matrices

- Hadamard matrix is widely used in communication and signal processing:
  - 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/Inequivalence
- This paper is to study on how to check equivalence of two Hadamard matrices EFFICIENTLY, and generalize this idea to binary matrices in general

Hadamard Equivalence

- If H is a Hadamard matrix, then the matrix that is the result of applying following operations to H is also a Hadamard matrix:
  - Multiply -1 to all elements of some rows (row complement)
  - Multiply -1 to all elements of some columns
  - Row permutation (Exchange the position of rows)
  - Column permutation
- These operations are called as 'Hadamard-preserving operation'.
- If a Hadamard matrix B can be obtained by applying Hadamard-preserving operations to H, then we say H and B are Hadamard-equivalent

Number of Inequivalent Matrices

The size of matrices	Number of Inequivalent Hadamard Matrices
1,2,4,8,12	1
16	5
20	3
24	60
28	487
≥ 32	Unknown

Integer Representation of a Binary Matrix

Definition

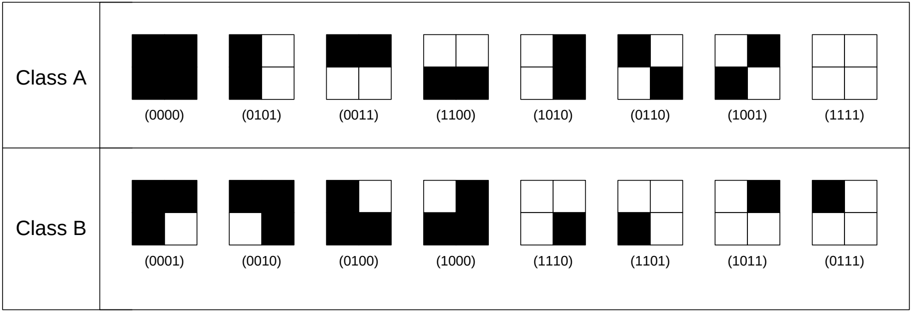
Let $A = (a_{ij})$ be an $m \times n$ binary matrix, where $i = 1, 2, ..., m$ and $j = 1, 2, ..., n$. Then,

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

Example:

$$\rho \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} = 0101\ 0110\ 1001\ 1110_{(2)} = 22174$$

Minimal Matrix - Example

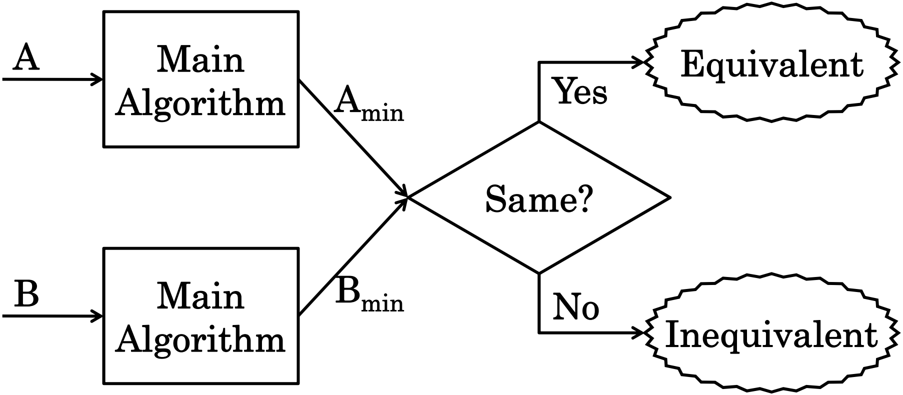


Description of the Proposed Scheme

To Check Equivalence/Inequivalence

- Two binary matrices are Hadamard-equivalent if they belong to the same class
- An equivalence class has only one minimal matrix
- Find the minimal matrices of (classes of) two binary matrices in question, and then see if they are the same or not
- How to find it?

Equivalence Check by Using Main Algorithm



Complexity of the Proposed Scheme

Theorem

1. *All elements in the first row and the first column of a minimal matrix are zero.*
2. *Given a binary matrix H and its minimal matrix L, there exist permutation matrices P_r and P_c (not necessarily unique) such that*
$$L = N(P_r H P_c). \tag{2}$$
3. *When P_r and the first column of P_c are known, the remaining columns of P_c can be determined in* (2).

- Checking whole P_r and the first column of $P_c = \mathcal{O}(m!n)$
- Determining $P_c = \mathcal{O}(nlogn)$ using Quicksort
- Overall complexity: $\mathcal{O}((m!)n^2 logn)$

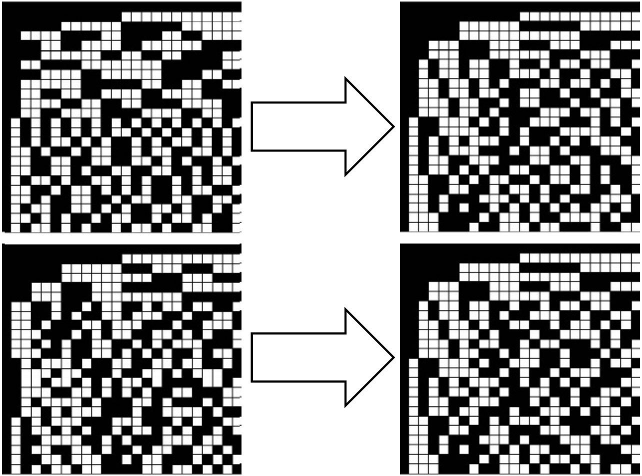
Some Applications of the Proposed Scheme

Problem	Result	CPU Time
20×20 Williamson - apply HPOs randomly	All equivalent decision	40 seconds for each
All 24×24 inequivalent Hadamard matrices	All inequivalent decision	3 to 15 minutes for each
60×60 Paley I/II	Inequivalent decision	I: 30 hours, II: 3 hours
Various size of random binary matrices	Successful decisions	Less than 1 second when size < 50

Examples of Order 24

Two Hadamard matrices of order 24

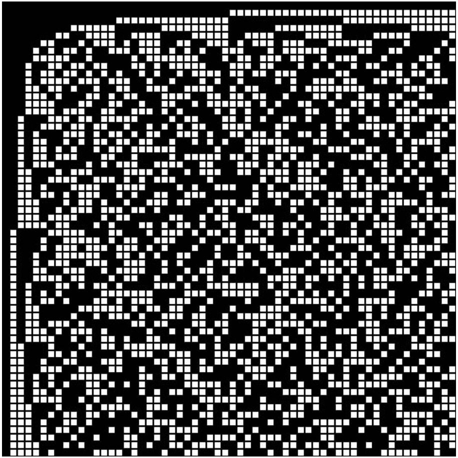
Their minimal matrices



Examples of Order 60

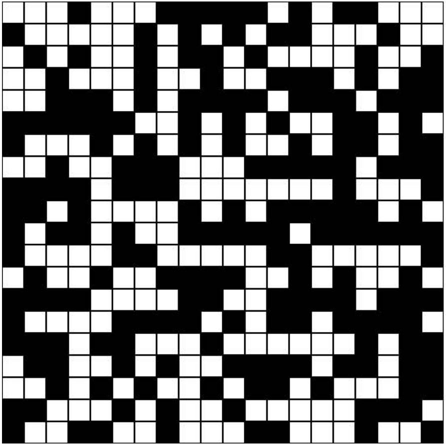
Minimal Matrices of Payley type I and II

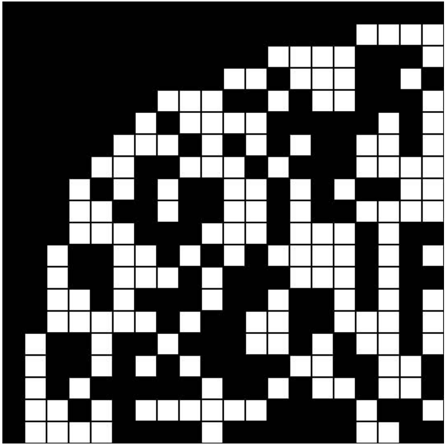
$\Longrightarrow$ This shows they are inequivalent.



Examples of General Binary Matrix

Minimal Matrix of a Random Binary Matrix of Size 20





Fast Algorithm (Not in the Paper)- Basic Idea

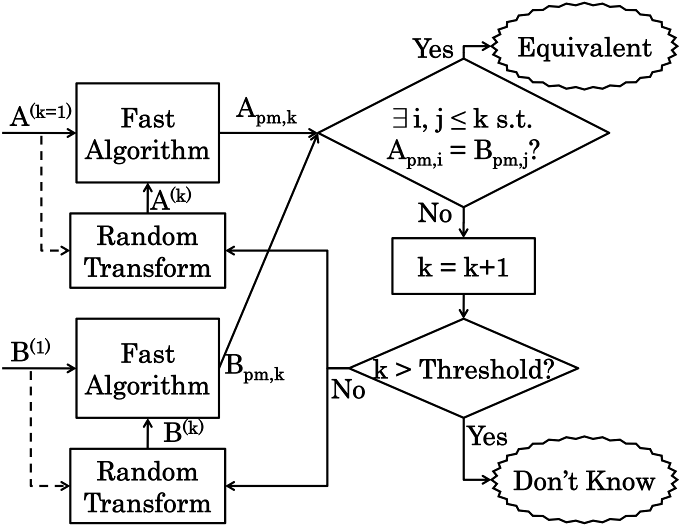
- Calculation time highly depends on the matrices, For example, 32×32 Kronecker type matrix takes too long time to get output by the main algorithm
- When progress is slower, the minimal matrix gets out faster, and almost all matrices' minimal matrix is found at very early time
  - For example, 60×60 Payley II took 3 hours to finish
  - But the time when the minimal matrix is found is about 2 minutes after the algorithm started
  - And Payley I's time, which took 30 hours, was only 15 seconds
- So if two matrices are equivalent, same minimum may be found in reasonably short time

Fast Algorithm

- Step 1. Operate the main algorithm with A
- Step 2. When certain time (threshold time) passes, stop and get the minimal matrix stored

- We can't assure the result becomes the minimal matrix if algorithm is not completed
- But it may be with high probability when the threshold time is sufficiently long
- We call the result of the Fast Algorithm as pseudo-minimal matrix

Equivalence Check by Using Fast Algorithm



Conclusion and Future Work

- We propose an efficient scheme to check Hadamard-equivalence of binary matrices
- We show the results of this scheme for some Hadamard matrices and binary matrices
- We also propose some basic theorems about the minimal matrix (in the paper)

- Generalization of the problem - numer of inequivalent Hadamard matrix - to the set of $m \times n$ binary matrices (especially all sizes) could lead to new and interesting combinatorial problems