Hadamard Equivalence of Binary Matrices

Ki-Hyeon Park and Hong-Yeop Song

Coding and Crypto Lab
Yonsei University, Seoul, KOREA

The 15th Asia-Pacific Conference on Communications (APCC 2009)
Regal Shanghai East Asia Hotel
October 8-10, 2009

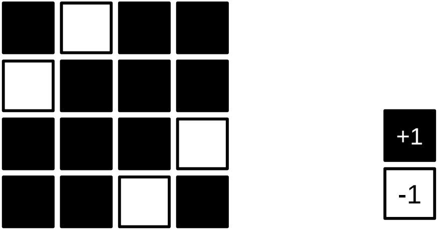
Contents

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
  - 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

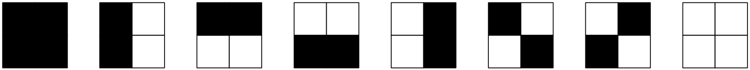
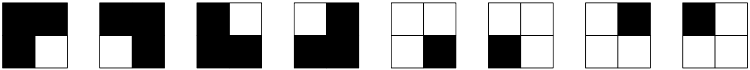
Let $A = (a_{ij})$ be an $m \times n$ binary matrix, where $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. Then,

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

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

Class A 	(0000)	(0101)	(0011)	(1100)	(1010)	(0110)	(1001)	(1111)
Class B 	(0001)	(0010)	(0100)	(1000)	(1110)	(1101)	(1011)	(0111)

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?

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).

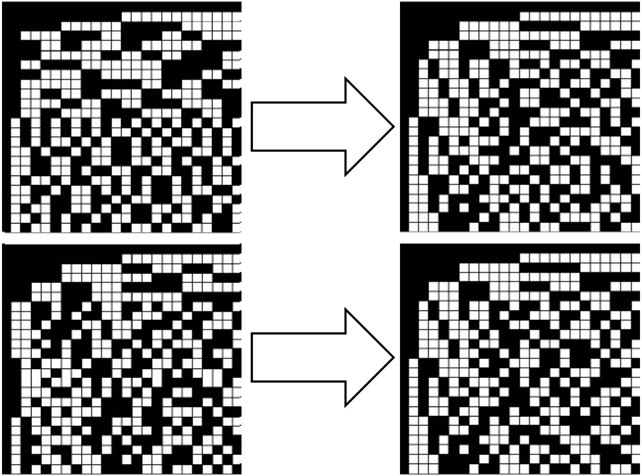
- Checking whole P_r and the first column of $P_c = \mathcal{O}(m!n)$
- Determining $P_c = \mathcal{O}(nlogn)$ using Quicksort
- Overall complexity: $\mathcal{O}((m!)n^2 logn)$

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
32×32 Sylvester / Kronecker	Equivalent Decision by Fast check method	Approximately 100 days

Examples of Order 24

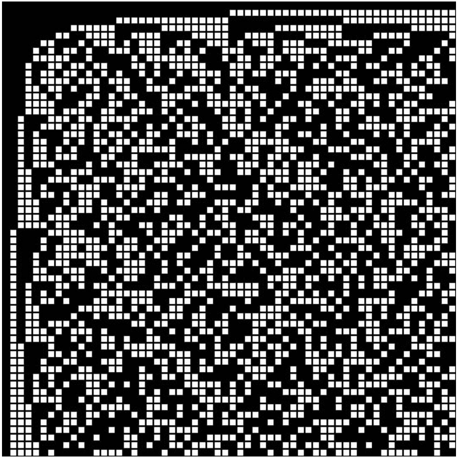
Two Hadamard matrices of order 24 | Their minimal matrices



Examples of Order 60

Minimal Matrices of Payley type I and II

$\Longrightarrow$ This shows they are inequivalent.



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 2×2 binary matrices
- We also propose a faster version (in the paper)

- Generalization of this idea to the set of $m \times n$ binary matrices
- Could lead to new and interesting combinatorial problems