1000000100000011000010100011110010001011001110101001111101000011100010010011011010110111101100011010010111011100110010101011111

Classification, Construction and Search of General Quasi-Orthogonal Binary Signal Sets

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

Yonsei University, Seoul, Korea

2011 International Workshop on Signal Design and its Applications (IWSDA 2011)

October 10~14, 20110
Guilin, China

1000000100000011000010100011110010001011001110101001111101000011100010010011011010110111101100011010010111011100110010101011111

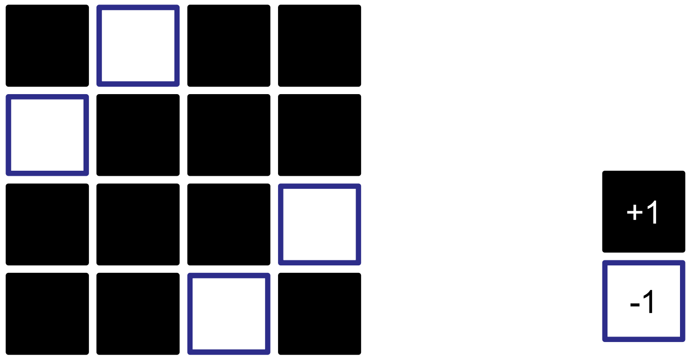
Orthogonal Signals and Hadamard Matrix

1000000100000011000010100011110010001011001110101001111101000011100010010011011010110111101100011010010111011100110010101011111

- 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

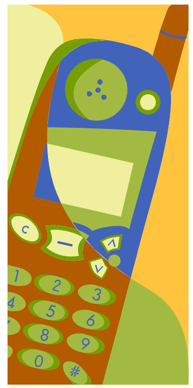
$$H\,H^T = n\,I,$$

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



- **Orthogonality:** Inner product of any row vector pairs are zero → Side signals give no interference to main signal receiver

- **Orthogonal signal set is widely used in communications and signal processing engineering:**
  - Orthogonal channelization in CDMA communications
  - Construction of orthogonal signals for OFDM, OFDMA
  - Construction of GOOD error-correcting codes

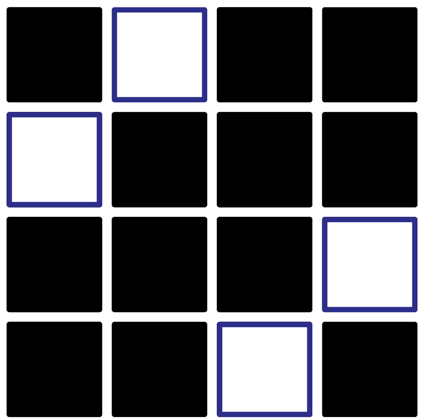


Hadamard Equivalence

Definition 1 (Hadamard Equivalence)

Two **binary matrices** of the same size are said to be hadamard-equivalent (or just **equivalent**) if one can be converted to the other by some combinations of the following hadamard-preserving operations:

- CC/CR: Complementing a column (CC) / a row (CR)
- PC/PR: Permuting columns (PC) / rows (PR)



Size	# inequivalent Hadamard matrices	Reference
1, 2, 4, 8, 12	1	
16	5	
20	3	
24	60	Kimura, 1989
28	487	Kimura, 1994
32	≥13,707,126	Kharaghani, 2010

Absolute correlation is preserved

1000000100000011000010100011110010001011001110101001111110100001110001001001101101011011110110001101001011101110011001010101111111

- Give two **binary vectors** $\underline{r}$ and $\underline{s}$ of length n, their absolute correlation is given as

$$C(\underline{r},\underline{s}) = \left|\sum_i (-1)^{r(i)+s(i)}\right| = |A-D|$$

where A is the number of agreements and D is the number of disagreements between $\underline{r}$ and $\underline{s}$.

Remark 1. The absolute correlation of the two rows of a 2 x n binary matrix will be preserved by any Hadamard-preserving operation.

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

Integer Representation of Binary Matrices

10000001000000110000010100011110010001011001110101001111101000011100010010011011010110111101100011010010111011100110010101011111 11

Definition 2: 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:

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

- **Note that the map ρ is bijective**

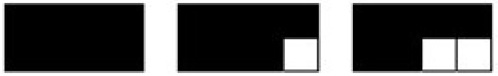
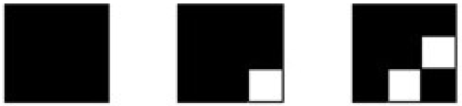
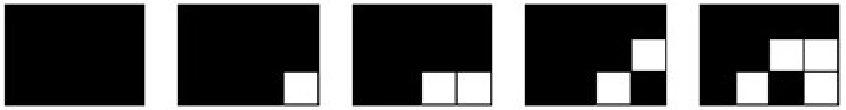
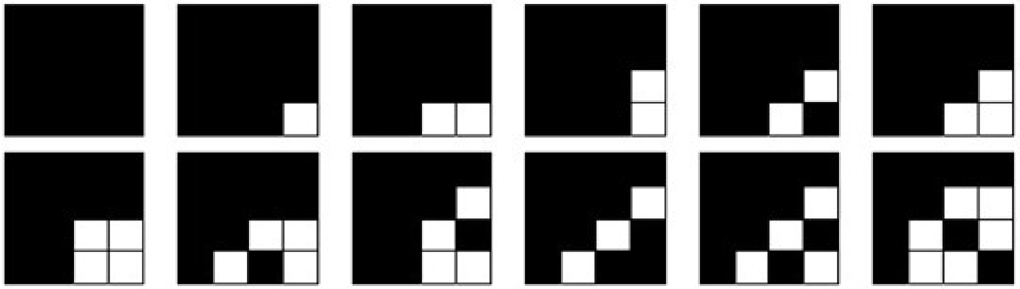
Definition 3. The minimal matrix of an equivalence class is called the **Hadamard-row minimal matrix**, or **HR-minimal**. Its ρ value is called the ρ value of the equivalence class.

Example 1: 2 x 2 binary matrices

1000000100000011000001010001111001000101100111010100111111010000111000100100110110101101111011000110100101110111001100101010111111

Example 2: some more

1000000100000011000010100011110010001011001110101001111110100001110001001001101101011011110110001101001011101110011001010101111111

Size	Number	Inequivalent HR-minimals	ρ values
2 x 2	2		0, **1**
2 x 3	2		0, **1**
2 x 4	3		0, 1, **3**
3 x 3	3		0, 1, **10**
3 x 4	5		0, 1, 3, 18, **53**
4 x 4	12		0, 1, 3, 17, 18, 19 51, 52, 291, 292, 293, **854**

Shape/Properties of HR-minimals

10000001000000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

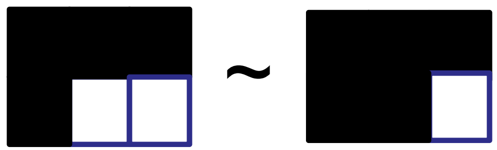
Theorem 2.

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

   Remark 1. It seems to be true that the weight of the second column of an $m \times n$ HR-minimal cannot exceed $m/2$. (open)

3) An HR-minimal is row-sorted and column-sorted.

   Remark 2. Its converse is not true.



Shape / Properties of HR-minimals

10000001000000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

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

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

Remark : Similar statement for the columns is **not true** in general.

Corollary 4 (Add-zero-row): 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.

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

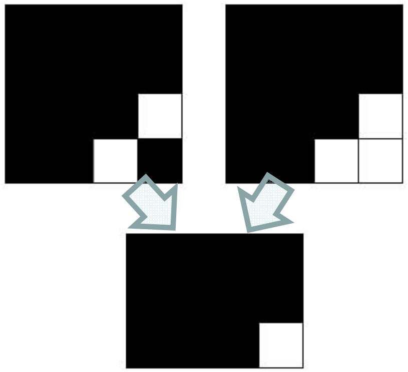
Shape/Properties of HR-minimals

1000000100000011000010100011110010001011001110101001111101000011100010010011011010110111101100011010010111011100110010101010111111

Theorem 3 (Add-zero-column): We can construct an $m \times (n+1)$ HR-minimal by adjoining the all-zero-column at the left-most of an $m \times n$ HR-minimal.

Proposition 2: 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.

Remark 5. Deleting the right-most column of an HR-minimal does not in general result in an HR-minimal.



000000		00000		00000		00000
000011		00001		00001		00001
001100	→	00110	~	01010	~	00110
010101		01010		00110		00111
010110		01011		00111		01010

Weight of the second row of HR-minimal

10000001000000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

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

  #Agreements - #Disagreements = $n - 2w$.

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.

- Therefore, the HR-minimal A with largest weight in its second row gives a set of row vectors with the lowest possible pair-wise correlations.

O-number and $R(w, n)$

10000001000000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

Definition 4 (o-number): We define the o-number of an $m \times n$ binary matrix A, or $\wp(A)$, as the weight of the second row of the HR-minimal of A.

Remark : In other word, $\wp(A)$ is $(n - C_M)/2$ where C C_M is the maximum absolute correlation of rows of A.

Definition 5 (Maximum size): We define $R(w, n)$ as the value satisfying that $R(w, n) \times n$ binary matrix with the o-number is w exists but $R(w, n)+1 \times n$ binary matrix with the o-number is w does not exist.

Remark : $R(w, n)$ give the maximum size of signal set with the maximum absolute correlation value of two arbitrary vectors are bounded to n-2w

Some Properties about $R(w, n)$

100000010000001100000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

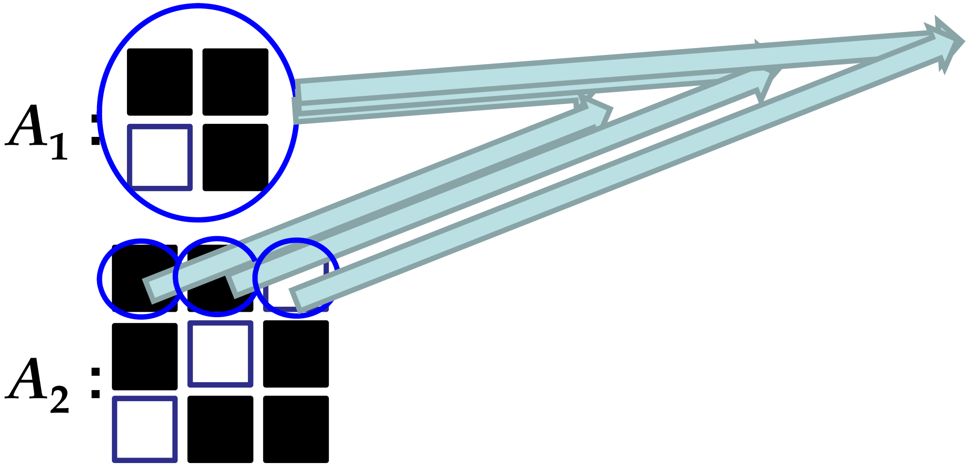
- **Theorem 5: Exact value of some $R(w, n)$**
  - $R(0, n) = \infty$ (ex: all-zero matrix)
  - $R(1, n) = 2^{n-1}$
  - $R(k, 2k) = 2$ where $k \geq 0$, $k \equiv 2 \bmod 4$
  - $R(2^k, 2^{k+1}) = 2^{k+1}$ where $k \geq 0$

- **Theorem 6: Bound of some $R(w, n)$**
  - $R(w, n+1) \geq R(w, n)$ where $w \geq 0$, $n \geq 1$
  - $R(w\text{-}1, n\text{-}1) \geq R(w, n)$ where $w \geq 1$, $n \geq 2$
  - $R(w\text{-}1, n) \geq R(w, n)$ where $w \geq 1$, $n \geq 1$
  - $R(w, n) \geq \dfrac{2^{n-1}}{\sum_{i=0}^{w-1}\binom{n}{i}}$ where $w \geq 1$, $n \geq 1$
  - $R(\min(w_1 n_2, w_2 n_1), n_1 n_2) \geq R(w_1, n_1)R(w_2, n_2)$
    where $w_1, w_2 \geq 0$, $n_1, n_2 \geq 1$
  - $R(\min(w_1, w_2), n_1+n_2) \geq 2R(w_1, n_1)R(w_2, n_2)$
    where $w_1, w_2 \geq 0$, $n_1, n_2 \geq 1$ (not in paper)

The Construction

10000001000000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

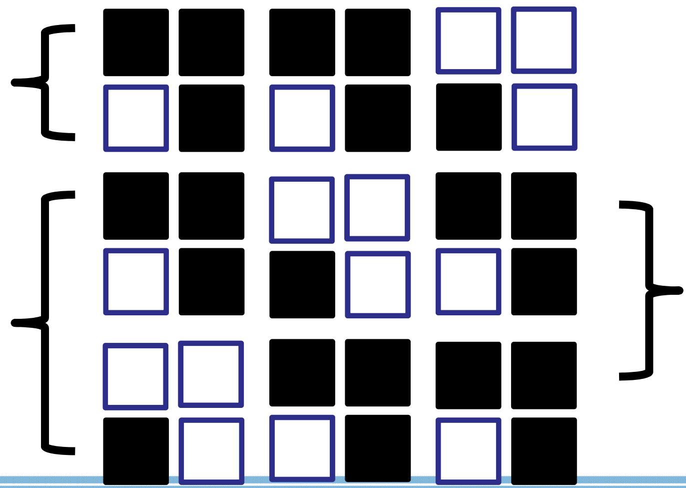
- A_1 : $m_1 \times n_1$ **binary matrix,** $\wp(A_1)=w_1$
- A_2 : $m_2 \times n_2$ **binary matrix,** $\wp(A_2)=w_2$
- $B=A_1 \otimes A_2$ **where** $\otimes$ **means Kronecker product**
  - So, the size of B is $m_1 m_2 \times n_1 n_2$
- **And,** $\wp(B) \geq$ **min**$(w_1 n_2, w_2 n_1)$
- **Example:**



Proof

100000010000001100000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- Let $i \neq j$ and $1 \leq i, j \leq m_1 m_2$.
- If $i \neq j \bmod m_2$, the correlation of i-th and j-th row of B is sum of n_2 term of the correlation of $i \bmod m_2$, $j \bmod m_2$ row of A_1. The value is positive or negative, and the absolute correlation of A_1 rows can't exceed n_1-2w_1, so the absolute value can't exceed $n_1 n_2 - 2 w_1 n_2$.
- If $i \equiv j \bmod m_2$, the i-th and j-th rows are n_1-column repeated version of A_2. So the absolute correlation value can't exceed $n_1(n_2 - 2w_2) = n_1 n_2 - 2 w_2 n_1$.
- So the maximum correlation ≥ max($n_1 n_2 - 2 w_1 n_2$, $n_1 n_2 - 2 w_2 n_1$) and $\wp(B) \geq$ min($w_1 n_2$, $w_2 n_1$).



Second Construction (Not in paper)

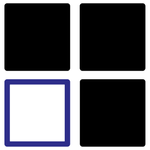
1000000100000011000010100011110010001011001110101001111110100001110001001001101101011011110110001101001011101110011001010101111111

- A_1 : $m_1 \times n_1$ binary matrix, $\wp(A_1)=w_1$
- A_2 : $m_2 \times n_2$ binary matrix, $\wp(A_2)=w_2$
- $A_1\{m_2\}$: $(2m_1m_2) \times n_1$ binary matrix, $2m_2 \times 1$ scaled form of A_1
- $\sim A_2$: $m_2 \times n_2$ binary matrix and all elements are inverted from A_2
- $$B=\left(\begin{array}{c|c} A_1\{m_2\} & \left.\begin{array}{c} \left.\begin{array}{c} A_2 \\ \sim A_2 \end{array}\right\} \\ \left.\begin{array}{c} A_2 \\ \sim A_2 \end{array}\right\} \\ \vdots \\ \left.\begin{array}{c} A_2 \\ \sim A_2 \end{array}\right\} \end{array}\right\} (m_1 \text{ groups}) \end{array}\right)$$ $(2m_1m_2) \times (n_1+n_2)$ binary matrix, $\wp(B) = \min(w_1, w_2)$

Second Construction : Example

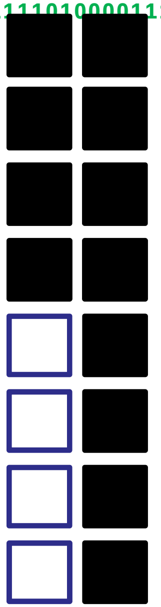
100000001000000110000010100011110010001011001110101001111101000011100010010011011010110111101100011010010111011100110010101011111

A_1 :

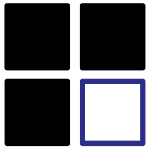


$\wp(A_1)=1$

A_1^{*m2} :

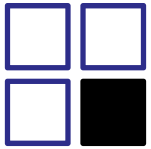


A_2 :



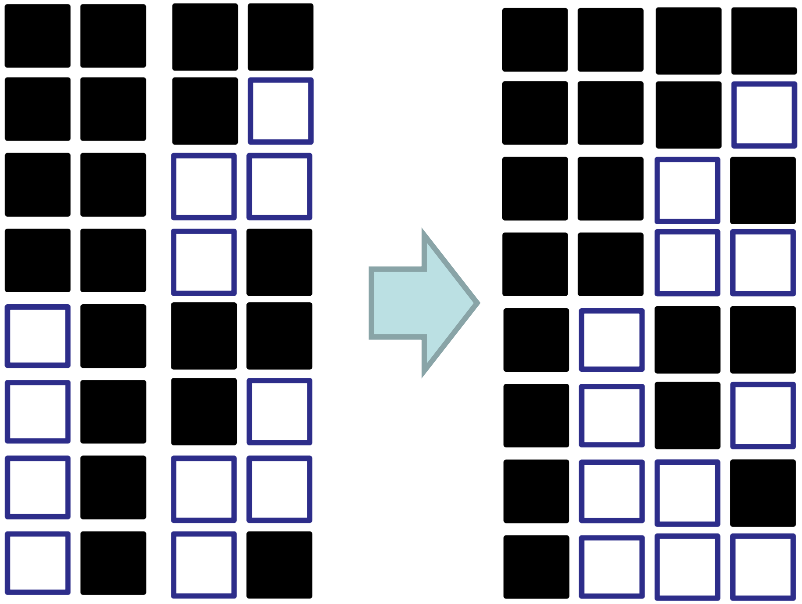
$\wp(A_2)=1$

$\sim A_2$:



HR-minimal:

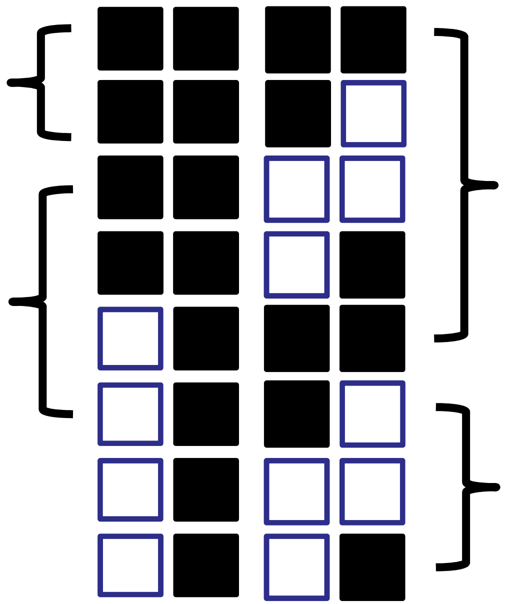
B :



$\wp(B) = \min(1, 1) = 1$

Proof

- If $i \neq j \bmod m_2$, the correlation of i-th and j-th row of B is sum of at most n_1 (left part) and the value that can't exceed n_2-$2w_2$ (right part), so the absolute value can't exceed $n_1+n_2-2w_2$.
- If $i \equiv j \bmod 2m_2$, the absolute correlation of i-th and j-th row of B is sum of the value that can't exceed n_1-$2w_1$ (left part) and at most n_2 (right part), so the absolute value can't exceed $n_1+n_2-2w_1$.
- If $i \equiv j \bmod m_2$ but $i \neq j \bmod 2m_2$, There are n_2 disagreements at right part, and there are at least w_1 agreements at right part. So the absolute correlation = |# Disagreements - # Agreements| ≤ | $n_2+(n_1-w_1)-w_1$ | = $n_1+n_2-2w_1$.



Exhaustive Search for $R(w, n)$

n \ w	w=2	3	4	5	6	7	8
n=4	**4(1)**	-	-	※ $R(w, n)$ (# of inequivalent matrices)			
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)**

Any question ?