Search for Hadamard matrices of Williamson type

Yonsei University Electronics engineering
Computer Application Lab

Chan-Hyoung Park, Hong-Yeop Song, Kyu-Tae Park

Contents

Introduction

- Hadamard matrix

  Hadanard matrix of order n is defined as $n \times n$ matrix with entries +1 or -1 such that $HH^T = nI$

- Necessary condition for existence of Hadamard matrices

  If there exists a Hadamard matrix of order n,

  $n = 1$, $n = 2$ *or* $n = 0 \pmod 4$

Relation between Hadamard matrix and ECC

- Any Hadamard matrix H_n of order n constructs an **Orthogonal code** of length n.
- Any Hadamard matrix H_n of order n constructs an **Biorthogonal code** of length n.
- For the given normalized Hadamard matrix, delete the first column. Then each rows construct **Simplex code**.

Open Problem

- For all $4n$ does a Hadamard matrix exist?
- For all $4n$ does a Williamson type Hadamard matrix exist?
- Order 428 is the least order of which no Hadamard matrix is known.

Constructions

- Sylvester type
  - H_n: Hadamard matrix of order n
  - H_m: Hadamard matrix of order m

$H_m \otimes H_n$ is a Hadamard matrix of of order $m \times n$

Constructions

- Paley type

  p : *prime number* , $q = p^k$, $k = 1,2,3,\ldots$

  - Type1

    If $q \equiv 3 \pmod 4$, then a Hadamard matrix of order $q+1$ exists.

  - Type2

    If $q \equiv 1 \pmod 4$, then a Hadamard matrix of order $2(q+1)$ exists.

Constructions

- Williamson type
  - If $n \times n$ matrices $A_i, i = 1,2,3,4$ with entries ± 1 are symmetric circulant and satisfy

$$A_1^2 + A_2^2 + A_3^2 + A_4^2 = 4nI_n \qquad (1)$$

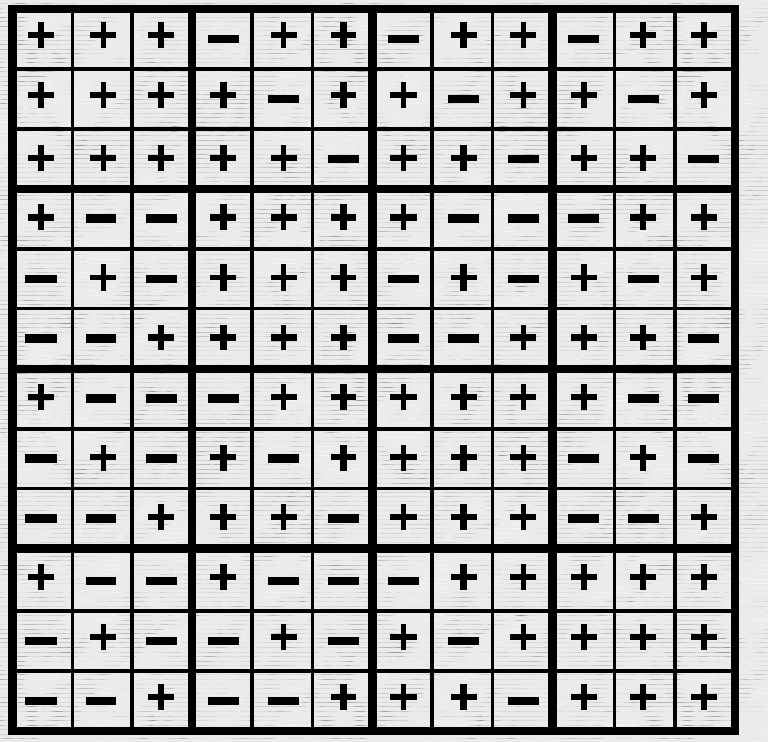
then H_{4n} is a Hadamard matrix

$$H_{4n} = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ -A_2 & A_1 & -A_4 & A_3 \\ -A_3 & A_4 & A_1 & -A_2 \\ -A_4 & -A_3 & A_2 & A_1 \end{pmatrix}$$

Constructions

Example)

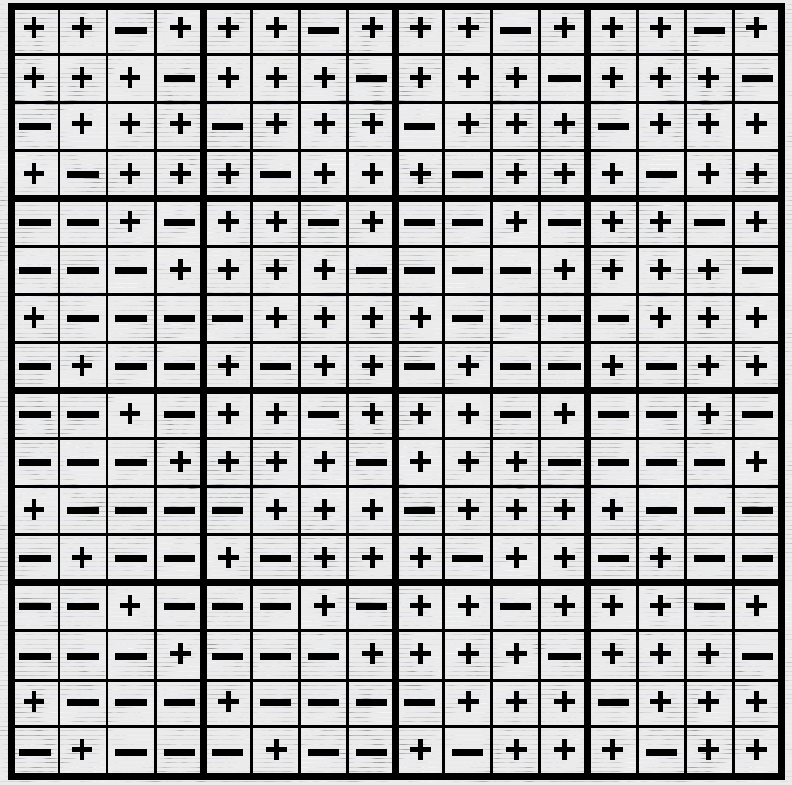
$n = 3, \quad 4n = 12$



Constructions

Example)

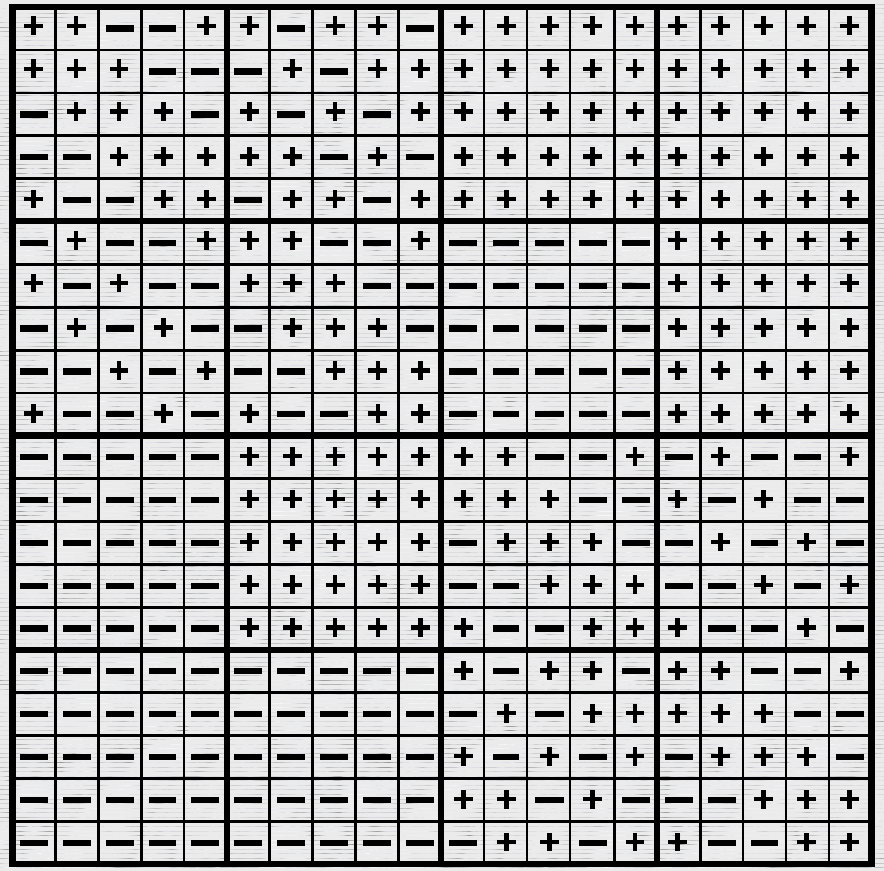
$n = 4, \quad 4n = 16$



Constructions

Example)

$n = 5, \quad 4n = 20$



A table

4	4	k			56	4*2*7		k		108	4*27		p	
8	4*2	k			60	4*15		p		112	$4^2 * 7$		k	
12	4*3		p		64	4^3	k			116	4*29			W
16	4^2	k			68	4*17		p		120	4*2*15		k	
20	4*5		p		72	4*2*9		k		124	4*31		p	
24	4*11		k		76	4*19		p		128	$4^3 * 2$	k		
28	4*7		p		80	$4^2 * 5$		k		132	4*33		p	
32	$4^2 * 2$	k			84	4*21		p		136	4*2*17		k	
36	4*9		p		88	4*2*11		k		140	4*35		p	
40	4*2*5		k		92	4*23			W	144	$4^2 * 9$		k	
44	4*11		p		96	$4^2 * 2 * 3$		k		148	4*37		p	
48	$4^2 * 3$		k		100	4*25		p		152	4*2*19		k	
52	4*13		p		104	4*2*13		k		156	4*39			w

A table

160	4^2*2*5		k		212	4*53		p		264	4*2*33		k	
164	4*41		p		216	4*2*27		k		268	4*67			W
168	4*2*21		k		220	4*55		p		272	4^2*17		k	
172	4*43			W	224	4^2*2*7		k		276	4*69		p	
176	4^2*11		k		228	4*57		p		280	4*2*35		k	
180	4*45		p		232	4*2*29			k	284	4*71		p	
184	4*2*23			k	236	4*59			W	288	4^2*2*9		k	
188	4*47			W	240	4^2*15		k		292	4*73			W
192	4^3*3		k		244	4*61		p		296	4*2*37		k	
196	4*49		p		248	4*2*31		k		300	4*75		p	
200	4*2*25		k		252	4*63		p		304	4^2*19		k	
204	4*51		p		256	4^4	k			308	4*77		p	
208	4^2*13		k		260	4*65			W	312	4*2*39		p	

A table

316	4*79		p		368	4^2*23		p		420	4*105		p	
320	4^3*5		k		372	4*93			W	424	4*2*53		k	
324	4*81			W	376	4*2*47			k	428	4*107			
328	4*2*41		k		380	4*95		p		432	4^2*27		k	
332	4*83		p		384	4^3*2*3		k		436	4*109			
336	4^2*21		k		388	4*97		p		440	4*2*55			
340	4*85		p		392	4*2*49		k		444	4*111			
344	4*2*43		p		396	4*99		p		448	4^3*7			
348	4*87		p		400	4^2*25		k		452	4*113			
352	4^2*2*11		k		404	4*101			W	456	4*2*57			
356	4*89			W	408	4*2*51		k		460	4*115			
360	4*2*45		k		412	4*103			W	464	4^2*29			
364	4*91		p		416	4^2*2*13		k		468	4*117			

Search for Hadamard matrices of Williamson type

1. To search the Williamson type Hadamard matrix , we use some **Necessary conditions.**
2. Using this Necessary conditions, suggest a search algorithm.
3. Using this algorithm, fully search the Williamson type Hadamard matrices of order 92.
4. Based on the search for order 92, consider the possibility of search for Williamson type Hadamard matrix of order 428.

Necessary Conditions

- Necessary condition 1
  - $n \times n$ symmetric circulant matrices A_i $(i = 1,2,3,4)$ with entries ± 1 satisfy equation (1) and let s_i be the sum of all entries of one row in A_i . Then,

$$s_1^2 + s_2^2 + s_3^2 + s_4^2 = 4n$$

- Necessary condition 2
  - Sum of four entries in the same row and column of A_i $(i = 1,2,3,4)$ is +2 or −2

Cases for order 92

1. Find s_1, s_2, s_3, s_4 satisfying Necessary condition 1.

   $(\pm 7, \pm 5, \pm 3, \pm 3)$ $(\pm 9, \pm 3, \pm 1, \pm 1)$

2. We consider two CASES.

   $CASE\ 1: \quad (s_1, s_2, s_3, s_4) = (7, -5, 3, 3)$

   $CASE\ 2: \quad (s_1, s_2, s_3, s_4) = (-9, 3, -1, -1)$

- Other cases can be constructed by CASE1 and CASE2.

Cases for order 92

CASE 1: $(s_1, s_2, s_3, s_4) = (7, -5, 3, 3)$

1. Set the first element $+1$ and construct two palindromic pair with other 22-element.

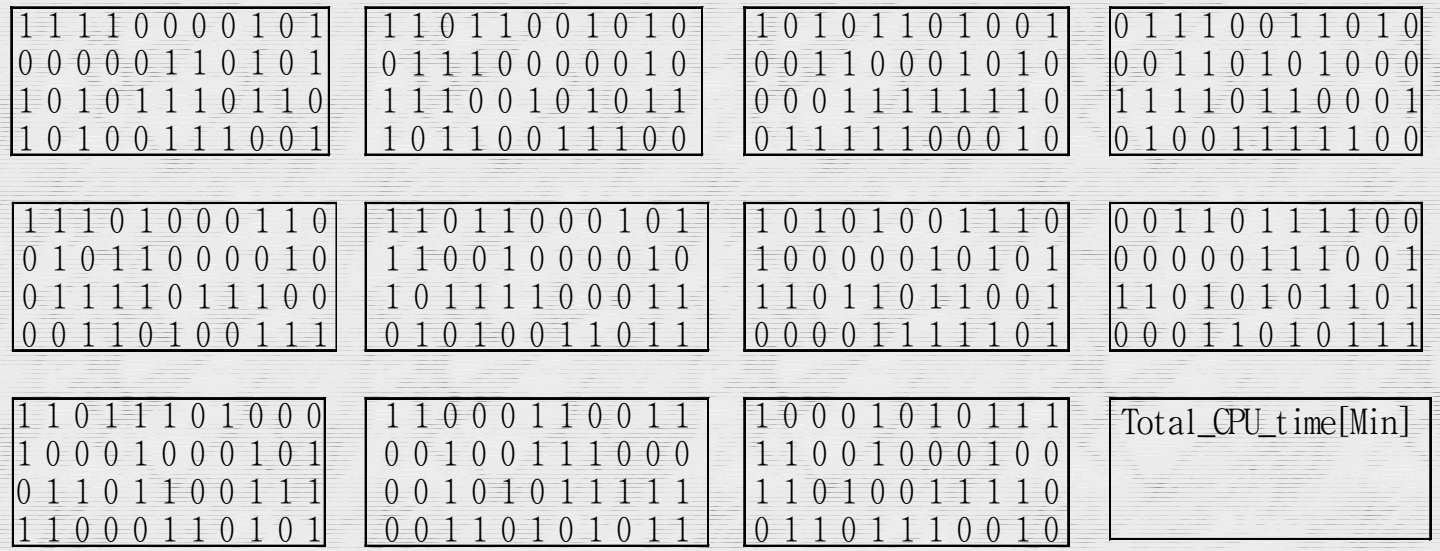
1	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{11}	b_{10}	b_9	b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1

2. Select four candidate satisfying $(s_1, s_2, s_3, s_4) = (7, -5, 3, 3)$

3. Construct (A_1, A_2, A_3, A_4) and check four matrix construct a Hadamard matrix.

Cases for order 92

CASE 1: $(s_1, s_2, s_3, s_4) = (7, -5, 3, 3)$



CASE 2: $(s_1, s_2, s_3, s_4) = (-9, 3, -1, -1)$

None. Total_CPU_Time[Min] =18.07

Cases for order 428

- Each expected time is compared with the cases for order 92

$$s \quad s \quad s \quad s_4) = \; - \quad - \quad - \quad)$$

$$Cand = \quad 0 \qquad \times 10^{44}$$

$$eed \qquad ear \qquad e \qquad = \qquad \times \quad ^{32} \; Year]$$

$$s \quad s \quad s \quad s_4) = \qquad - \quad - \;)$$

$$Cand = \qquad \times 10^{44}$$

$$eed \qquad ear \qquad e \qquad = \qquad \times \quad ^{32} \; Year]$$

Cases for order 428

$$s \quad s \quad s \quad s_4) = \quad - \quad - \quad)$$

$$Cand = \quad 1 \quad \times 10^{44}$$

$$eed \qquad ear \qquad e \quad = \qquad \times \quad ^{32} \; Year]$$

$$CASE\ 4: \quad (s_1, s_2, s_3 \; s_4) = \; - \quad - \quad)$$

$$Num\_Cand = 3.25801 \times 10^{44}$$

$$Expected\_Search\_Time = 2.9822 \times 10^{32}\ [Year]$$

Cases for order 428

$$CASE\ 5: \quad (s_1, s_2, s_3, s_4) = (-17,11,3,3)$$

$$Num\_Cand = 3.5086 \times 10^{44}$$

$$Expected\_Search\_Time = 3.2116 \times 10^{32}\ [Year]$$

$$CASE\ 6: \quad (s_1, s_2, s_3, s_4) = (19,7,3,3)$$

$$Num\_Cand = 4.0700 \times 10^{44}$$

$$Expected\_Search\_Time = 3.7254 \times 10^{32}\ [Year]$$

Conclusion

- For the order of which Hadamard matrix can not be constructed by Paley type and Sylvester type, we want to search Hadamard matrix using Williamson method. In order 92 it took 41.149 minute.
- It is necessary to search the Hadamard matrix of order 428, because no Hadamard matrix is Known in order 428. it is impossible to fullly search because too many candidate. But partially searching is meaning.