

Williamson형식의 하다마드 행렬의 탐색

연세대학교 전자공학과
컴퓨터응용 연구실

박찬형 . 송홍엽 . 박규태

▶ 하다마드 행렬의 정의

하다마드 행렬의 정의

하다마드 행렬의 존재에 관한 필요조건

open problem

▶ 현재까지 알려진 하다마드 행렬의 구성방법

Kronecker 곱

Payley 방법

Williamson 형식

▶ Williamson 형식의 하다마드 행렬의 탐색

탐색에 관한 필요조건

92차에서의 탐색

▶ 결론

▶ 하다마드 행렬의 정의

▷ 하다마드 행렬

크기 n 인 하다마드 행렬은 원소로 $+1$ 또는 -1 을 가지는 $n \times n$ 행렬이며 $HH^T = nI$ 이다.

▷ 하다마드 행렬의 존재에 관한 필요조건

$n \times n$ 하다마드 행렬 H 가 존재한다면,

$n = 1$, $n = 2$, 혹은, n 은 4의 배수이다.

▷ Open Problem

※ 모든 $4n$ 차 하다마드 행렬이 존재하는가?

※ 모든 $4n$ 차 Williamson 형식의 하다마드 행렬이 존재하는가?

▷ 하다마드 행렬이 존재하는 경우 Williamson 형식의 하다마드 행렬이 존재한다. (not yet completely proved and no counter-example is known)

4	4	k			104	$4 * 2 * 1$	K_{2*52}		204	$4 * 51$	P		304	$4^2 * 19$	K_{2*152}		404	$4 * 101$			
8	$4 * 2$	k			108	$4 * 27$	P		208	$4^2 * 13$	K_{2*104}		308	$4 * 77$	P		408	$4 * 2 * 5$	K_{2*204}		
12	$4 * 3$		P		112	$4^2 * 7$	K_{2*56}		212	$4 * 53$	P		312	$4 * 2 * 3$	P		412	$4 * 103$			
16	4^2	k			116	$4 * 29$		W	216	$4 * 2 * 2$	K_{2*108}		316	$4 * 79$	P		416	$4^2 * 2 *$	K_{2*208}		
20	$4 * 5$		P		120	$4 * 2 * 1$	K_{2*60}		220	$4 * 55$	P		320	$4^3 * 5$	K_{2*160}		420	$4 * 105$	P		
24	$4 * 2 * 3$	K_{2*12}			124	$4 * 31$	P		224	$4^2 * 2 *$	K_{2*112}		324	$4 * 81$		W	424	$4 * 2 * 5$	K_{2*212}		
28	$4 * 7$		P		128	$4^3 * 2$	K		228	$4 * 57$	P		328	$4 * 2 * 4$	K_{2*164}		428	$4 * 107$			
32	$4^2 * 2$	k			132	$4 * 33$	P		232	$4 * 2 * 2$		K_{2*116}	332	$4 * 83$	P		432	$4^2 * 27$	K_{36*12}		
36	$4 * 9$		P		136	$4 * 2 * 1$	K_{2*68}		236	$4 * 59$		W	336	$4^2 * 21$	K_{12*28}		436	$4 * 109$			
40	$4 * 2 * 5$	K_{2*20}			140	$4 * 35$	P		240	$4^2 * 15$	K_{12*20}		340	$4 * 85$	P		440	$4 * 2 * 5$	K_{2*220}		
44	$4 * 11$	P			144	$4^2 * 9$	K_{2*72}		244	$4 * 61$	P		344	$4 * 2 * 4$	P		444	$4 * 111$	P		
48	$4^2 * 3$	K_{2*24}			148	$4 * 37$	P		248	$4 * 2 * 3$	K_{2*124}		348	$4 * 87$	P		448	$4^3 * 7$	K_{2*224}		
52	$4 * 13$		P		152	$4 * 2 * 1$	K_{2*76}		252	$4 * 63$	P		352	$4^2 * 2 *$	K_{2*176}		452	$4 * 113$			
56	$4 * 2 * 7$	K_{2*28}			156	$4 * 39$		W	256	4^4	K		356	$4 * 89$		W	456	$4 * 2 * 5$	K_{2*228}		
60	$4 * 15$		P		160	$4^2 * 2 *$	K_{2*80}		260	$4 * 65$		W	360	$4 * 2 * 4$	K_{2*180}		460	$4 * 115$	P		
64	4^3	k			164	$4 * 41$	P		264	$4 * 2 * 3$	K_{2*132}		364	$4 * 91$	P		464	$4^2 * 29$	P		
68	$4 * 17$		P		168	$4 * 2 * 2$	K_{2*84}		268	$4 * 67$		W	368	$4^2 * 23$	P		468	$4 * 117$	P		
72	$4 * 2 * 9$	K_{2*36}			172	$4 * 43$		W	272	$4^2 * 17$	K_{2*136}		372	$4 * 93$		W	472	$4 * 2 * 5$			
76	$4 * 19$		P		176	$4^2 * 11$	K_{2*88}		276	$4 * 69$	P		376	$4 * 2 * 4$		K_{2*188}	476	$4 * 119$			
80	$4^2 * 5$	K_{2*40}			180	$4 * 45$	P		280	$4 * 2 * 3$	K_{2*140}		380	$4 * 95$	P		480	$4^2 * 2 *$	K_{2*240}		
84	$4 * 21$	P			184	$4 * 2 * 2$		K_{2*92}	284	$4 * 71$	P		384	$4^3 * 2 *$	K_{2*192}		484	$4 * 121$	P		
88	$4 * 2 * 1$	K_{2*44}			188	$4 * 47$		W	288	$4^2 * 2 *$	K_{2*144}		388	$4 * 97$	P		488	$4 * 2 * 6$	K_{2*244}		
92	$4 * 23$			W	192	$4^3 * 3$	K_{2*96}		292	$4 * 73$		W	392	$4 * 2 * 4$	K_{2*196}		492	$4 * 123$	P		
96	$4^2 * 2 *$	K_{2*48}			196	$4 * 49$	P		296	$4 * 2 * 3$	K_{2*148}		396	$4 * 99$	P		496	$4^2 * 31$	K_{2*248}		
100	$4 * 25$		P		200	$4 * 2 * 2$	K_{2*100}		300	$4 * 75$	P		400	$4^2 * 25$	K_{2*200}		500	$4 * 125$	P		

현재까지 알려지지 않은 가장 작은 크기의 하다마드 행렬은 크기 428인 하다마드 행렬이다.

▶ 현재까지 알려진 Construction 방법

▷ Kronecker Product

H_m : 크기 m 인 하다마드 행렬.

H_n : 크기 n 인 하다마드 행렬.

$H_m \otimes H_n$ 은 크기 $n \times m$ 인 하다마드 행렬이다.

ex) $H_2 \otimes H_4 =$

+	+	+	+	+	+	+	+
+	-	+	-	+	-	+	-
+	+	-	-	+	+	-	-
+	-	-	+	+	-	-	+
+	+	+	+	-	-	-	-
+	-	+	-	-	+	-	+
+	+	-	-	-	-	+	+
+	-	-	+	-	+	+	-

▷Payley Type

정의) Conference Matrix C

대각선은 0 으로 채워지고, 다른 부분은 ± 1 의 값을 가지며 다음을 만족한다. $CC^T = (n-1)I$

※Type 1

만약 $n \equiv 0 \pmod{4}$ 이고, 크기 n 인 conference matrix C 가 존재한다면, $I + C$ 는 하다마드 행렬이다.

ex) $n = 4$ 인 Payley Type 1 하다마드 행렬

+	+	+	+
-	+	-	+
-	+	+	-
-	-	+	+

※ Type 2 : 만약 $n \equiv 2 \pmod{4}$ 이고, 크기 n 인 conference matrix C 가 존재한다면,

$$H = \begin{pmatrix} I + C & -I + C \\ -I + C & -I - C \end{pmatrix}$$
는 크기 $2n$ 인 하다마드 행렬이다.

ex) $n = 6$ 인 Payley Type 2 하다마드 행렬

+	+	+	+	+	+	-	+	+	+	+	+
-	+	-	+	-	+	-	-	-	+	-	+
-	-	+	+	+	-	-	-	-	+	+	-
-	+	+	+	-	-	-	+	+	-	-	-
-	-	+	-	+	+	-	-	+	-	-	+
+	-	+	+	-	+	+	-	+	+	-	-
-	+	+	+	+	+	-	-	-	-	-	-
-	-	-	+	-	+	+	-	+	-	+	-
-	-	-	+	+	-	+	+	+	-	-	+
-	+	+	-	-	-	+	-	-	-	+	+
-	-	+	-	-	+	+	+	-	+	-	-
+	-	+	+	-	-	-	+	-	-	+	-

▷ Williamson Type

$n \times n$ 행렬 A_i , $i = 1, 2, 3, 4$ 가 ± 1 을 원소로 가지며, 순환 대칭적이고 (circulant symmetric)

$$A_1^2 + A_2^2 + A_3^2 + A_4^2 = 4nI_n \quad \text{--- (1)}$$

를 만족할 때, 다음과 같이 정의된 크기 $4n$ 인 행렬 H 는 하다마드 행렬이다.

$$H = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ -A_2 & A_1 & -A_4 & A_3 \\ -A_3 & A_4 & A_1 & -A_2 \\ -A_4 & -A_3 & A_2 & A_1 \end{pmatrix}$$

--- (2)

ex) 크기 12인 Williamson 형식의 하다마드 행렬

+	+	+	-	+	+	-	+	+	-	+	+
+	+	+	+	-	+	+	-	+	+	-	+
+	+	+	+	+	-	+	+	-	+	+	-
+	-	-	+	+	+	+	-	-	-	+	+
-	+	-	+	+	+	-	+	-	+	-	+
-	-	+	+	+	+	-	-	+	+	+	-
+	-	-	-	+	+	+	+	+	+	-	-
-	+	-	+	-	+	+	+	+	-	+	-
-	-	+	+	+	-	+	+	+	-	-	+
+	-	-	+	-	-	-	+	+	+	+	+
-	+	-	-	+	-	+	-	+	+	+	+
-	-	+	-	-	+	+	+	-	+	+	+

▶ Williamson 형식의 하다마드 행렬의 Search

크기 428인 Williamson형식의 하다마드 행렬을 search하기 위해 Williamson 형식에 대한 여러가지 필요조건을 사용한다. 그 조건들을 이용하여 search 알고리즘을 제안하며, 그 알고리즘을 사용하여 92차의 Williamson 형식의 하다마드 행렬을 전영역 탐색하고, 이를 기반으로 428차 Williamson형식의 하다마드 행렬에 대한 탐색 가능성을 조사한다.

▷필요조건 1. $A_i (i = 1, 2, 3, 4)$ 는 식(1)을 만족하며

원소가 ± 1 이고, 순환대칭인 $n \times n$ 행렬이라 하자. s_i 를 A_i 의 한 행의 모든 원소의 합이라 두면, 다음을 만족한다.

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

(2)

▷필요조건 2. A_i ($i = 1, 2, 3, 4$)행렬의 같은 행과 열에 있는 4개의 원소의 합은 $+2$ 또는 -2 가 되어야 한다.

▶ Williamson 형식의 92차 하다마드행렬 탐색
($92 = 4 \times 23$)

$s_1^2 + s_2^2 + s_3^2 + s_4^2 = 4n$ 을 만족하는 정수해 s_1, s_2, s_3, s_4 를 구한다. 정수해는 $(\pm 7, \pm 5, \pm 3, \pm 3)$ 과 $(\pm 9, \pm 3, \pm 1, \pm 1)$ 이 있다. 이는 각각 2^4 개의 경우이지만 실제로는 부호가 한가지로 고정되어 $(7, -5, 3, 3)$ 과 $(-9, 3, -1, -1)$ 의 두 가지만이 가능하다. 이로부터 탐색해야하는 수열의 개수가 줄어들게 된다.

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

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

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

길이 23의 $\{\pm 1\}$ binary word 중에서 첫 번째 원소를 +1로 고정시키고, 22개의 원소를 길이 11으로 대칭적으로 구성하되, 첫째 word는 합이 7, 둘째는 합이 -5, 셋째와 넷째는 합이 3이 되는 경우만을 택한다.

$$\text{경우의수} : \binom{11}{7} \binom{11}{4} \binom{11}{6} \binom{11}{6} \doteq 2.32 \times 10^{10}$$

이로부터 23×23 행렬 4개를 구성하고, 식(2)와 같이 크기

$4n = 92$ 인 행렬을 구성하여, 하다마드행렬인지 확인한다.

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

1 1 1 1 0 0 0 0 1 0 1 0 0 0 0 0 1 1 0 1 0 1 1 0 1 0 1 1 1 0 1 1 0 1 0 1 0 0 1 1 1 0 0 1	1 1 0 1 1 0 0 1 0 1 0 0 1 1 1 0 0 0 0 0 1 0 1 1 1 0 0 1 0 1 0 1 1 1 0 1 1 0 0 1 1 1 0 0	1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 0 0 0 1 0 1 0 0 0 0 1 1 1 1 1 1 1 0 0 1 1 1 1 1 0 0 0 1 0	0 1 1 1 0 0 1 1 0 1 0 0 0 1 1 0 1 0 1 0 0 0 1 1 1 1 0 1 1 0 0 0 1 0 1 0 0 1 1 1 1 1 0 0
1 1 1 0 1 0 0 0 1 1 0 0 1 0 1 1 0 0 0 0 1 0 0 1 1 1 1 0 1 1 1 0 0 0 0 1 1 0 1 0 0 1 1 1	1 1 0 1 1 0 0 0 1 0 1 1 1 0 0 1 0 0 0 0 1 0 1 0 1 1 1 1 0 0 0 1 1 0 1 0 1 0 0 1 1 0 1 1	1 0 1 0 1 0 0 1 1 1 0 1 0 0 0 0 0 1 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 0 0 0 0 1 1 1 1 1 0 1	0 0 1 1 0 1 1 1 1 0 0 0 0 0 0 0 1 1 1 0 0 1 1 1 0 1 0 1 0 1 1 0 1 0 0 0 1 1 0 1 0 1 1 1
1 1 0 1 1 1 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 1 0 1 1 0 1 1 0 0 1 1 1 1 1 0 0 0 1 1 0 1 0 1	1 1 0 0 0 1 1 0 0 1 1 0 0 1 0 0 1 1 1 0 0 0 0 0 1 0 1 0 1 1 1 1 1 0 0 1 1 0 1 0 1 0 1 1	1 0 0 0 1 0 1 0 1 1 1 1 1 0 0 1 0 0 0 1 0 0 1 1 0 1 0 0 1 1 1 1 0 0 1 1 0 1 1 1 0 0 1 0	Total_CPU_time[Min] = 23.079785

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

None.

$$\text{Total_CPU_time[Min]} = 18.00$$

▶ 결론

Paley Type이나 Kronecker 방법에 의해 만들어지지 않는 크기의 하다마드 행렬에 대해 Williamson형식의 예를 찾아 보고자 하였다. 92차에서는 약 40분의 CPU시간으로 전영역 탐색을 마칠 수 있었다.

428차의 하다마드 행렬은 그 존재의 유무가 밝혀지지 않은 상태로 탐색의 과정이 필요한 부분이다. 그러나, 위에서 찾은 조건만을 가지고 현재의 CPU속도로 크기 428에서 전 영역 탐색을 한다는 것은 불가능해 보인다. 전 영역의 탐색이 불

가능하면 부분탐색도 의미가 있을 것이다.