

ある特殊な Williamson 等式

名工大 情報 沢出和江

1. R. Turyn[2]は 1972 年に Williamson 型 Hadamard 行列の無限系列を発見したが[3], それは奇数 n 次の特殊な形の Williamson 等式

$$1^2 + 1^2 + (1 + 2 \sum_{\nu \in A} e_{\nu} u_{\nu})^2 + (1 + 2 \sum_{\nu \in B} e_{\nu} u_{\nu})^2 = 4n \quad (1)$$

に基づくものである。ここに, ϵ は 1 の n 乗根, $u_{\nu} = \epsilon^{\nu} + \epsilon^{-\nu}$, $e_{\nu} = +1$ または -1 ; $A = \{l_1, l_2, \dots, l_r\}$ は $\Omega = \{1, 2, \dots, \frac{n-1}{2}\}$ の部分集合, B は A の余集合とする。

先に, 式(1)の中で最も特殊な場合で

- $n \equiv 1 \pmod{4}$ ならば

$$1^2 + 1^2 + (1 + 2u_1)^2 + (1 + 2 \sum_{\nu \neq 1} e_{\nu} u_{\nu})^2 = 4n$$

に解がない,

- $n \equiv 3 \pmod{4}$ ならば

$$1^2 + 1^2 + (1 - 2u_1)^2 + (1 + 2 \sum_{\nu \neq 1} e_{\nu} u_{\nu})^2 = 4n$$

に解がない

ことを喜安善市先生[1]より教えて戴いたことがこの研究の契機となり，その拡張を行なつて以下のことが得られた。

2. 式(1)は

$$f = \left(\frac{1}{2} + \sum_{\nu \in A} e_{\nu} u_{\nu} \right) + i \left(\frac{1}{2} + \sum_{\nu \in B} e_{\nu} u_{\nu} \right)$$

に対して

$$f \bar{f} = n - \frac{1}{2} \quad (2)$$

とも書けるが，記号を少し変えて

$$f = \sum_{\nu=0}^{n-1} \varepsilon_{\nu} \zeta^{\nu}, \quad \varepsilon_0 = \frac{1+i}{2}, \quad \varepsilon_{\nu} = \varepsilon_{-\nu} \in \{\pm 1, \pm i\} \quad (\nu \neq 0 \pmod{n})$$

とおくと，式(2)は

$$\sum_{\mu+\lambda \equiv \nu} \varepsilon_{\mu} \overline{\varepsilon_{\lambda}} = 0 \quad (\nu = 1, 2, \dots, n-1) \quad (3)$$

を意味する。

今，ordered pair を $(,)$ ，unordered pair を $[,]$ で記すことにすると，式(3)は $\nu \neq 0 \pmod{n}$ の時

- (i) $\mu + \lambda \equiv \nu$ の n 個の解は， $\mu \equiv \lambda \equiv \frac{\nu}{2}$ 以外は (μ, λ) ， (λ, μ) のように対となつてあらわれる；
- (ii) 対 $(0, \nu)$ ， $(\nu, 0)$ を別に取出し

$$\operatorname{sgn} \varepsilon_{\nu} = \begin{cases} 1 & (\varepsilon_{\nu} = 1 \text{ または } i \text{ のとき}) \\ -1 & (\varepsilon_{\nu} = -1 \text{ または } -i \text{ のとき}) \end{cases}$$

と定義すると

$$\varepsilon_0 \overline{\varepsilon_\nu} + \varepsilon_\nu \overline{\varepsilon_0} = \frac{\varepsilon_\nu + \overline{\varepsilon_\nu}}{2} + j \frac{\overline{\varepsilon_\nu} - \varepsilon_\nu}{2} = \operatorname{sgn} \varepsilon_\nu ;$$

(iii) さらに (i), (ii) 以外の対 $(\mu, \lambda), (\lambda, \mu)$ については

$$\varepsilon_\mu \overline{\varepsilon_\lambda} + \varepsilon_\lambda \overline{\varepsilon_\mu} = \begin{cases} \pm 2 & (\varepsilon_\mu \overline{\varepsilon_\lambda} \text{ が実数のとき}), \\ 0 & (\varepsilon_\mu \overline{\varepsilon_\lambda} \text{ が虚数のとき}); \end{cases}$$

以上 (i), (ii), (iii) より

$$\begin{aligned} 0 &= \varepsilon_{\frac{\nu}{2}} \overline{\varepsilon_{\frac{\nu}{2}}} + (\varepsilon_0 \overline{\varepsilon_\nu} + \varepsilon_\nu \overline{\varepsilon_0}) + \sum_{\substack{[\lambda, \mu] \\ \varepsilon_\mu \overline{\varepsilon_\lambda} = \pm 1}} (\varepsilon_\mu \overline{\varepsilon_\lambda} + \varepsilon_\lambda \overline{\varepsilon_\mu}) \\ &\equiv 1 + \operatorname{sgn} \varepsilon_\nu - 2 \left(\frac{n-3}{2} - N_\nu \right) \pmod{4}. \end{aligned} \quad (4)$$

ここで, N_ν は $\frac{n-3}{2}$ 個の $[\lambda, \mu]$ の中で, $\varepsilon_\mu \overline{\varepsilon_\lambda}$ が虚数であるものの個数である. 式(4)は

$$\operatorname{sgn} \varepsilon_\nu \equiv n + 2N_\nu \pmod{4} \quad (5)$$

を意味する.

一方, 別の表現をすれば, $N_\nu = \#\{(\lambda, \mu) \mid \lambda + \mu \equiv \nu, \lambda \in \pm A, \mu \in \pm B\}$

であるが,

$$\begin{aligned} N_\nu &\equiv 2r - N_\nu \\ &\equiv \#\{(\lambda, \mu) \mid \lambda + \mu \equiv \nu, \lambda \in \pm A\} - N_\nu \\ &\equiv \#\{(\lambda, \mu) \mid \lambda + \mu \equiv \nu, \lambda \in \pm A, \mu \equiv 0 \pmod{n}\} \\ &\quad + \#\{(\lambda, \mu) \mid \lambda + \mu \equiv \nu, \lambda \in \pm A, \mu \in \pm A\} \pmod{2}. \end{aligned} \quad (6)$$

A の特性函数を

$$\delta_A(\nu) = \begin{cases} 1 & \nu \in \pm A \text{ のとき} \\ 0 & \nu \notin \pm A \text{ のとき} \end{cases}$$

と定義する時，式(6)の最後の辺の才1項は $\delta_A(\nu)$ に等しく，才2項の集合には (λ, μ) と共に (μ, λ) も属するから才2項は一般に偶数で，唯 $\nu \equiv 2\lambda \pmod{n}$ なる $\lambda \in \pm A$ が存在する時だけは奇数になるので， A^* を $\{2\lambda_1, 2\lambda_2, \dots, 2\lambda_r\}$ の各要素の符号を適当に選んで Ω の部分集合ならしめたものとするとき才2項は法2に関して A^* の特性函数 $\delta_{A^*}(\nu)$ に合同である。

従って， $N_\nu \equiv \delta_A(\nu) + \delta_{A^*}(\nu) \pmod{2}$ で，定理1が得られる。

$$\text{定理1.} \quad e_\nu \equiv n + 2\delta_A(\nu) + 2\delta_{A^*}(\nu) \pmod{4}. \quad (7)$$

3. Ω の部分集合 A を互いに素な $A_+ = \{\nu \in A \mid e_\nu = 1\}$ と $A_- = \{\nu \in A \mid e_\nu = -1\}$ とに分割し， B についても同様とする。

§2で得た式(7)から，次の必要条件が導かれる。

定理2. n 次のWilliamson等式(1)が成立するならば，

1. $2n-1 = p_1 p_2 \cdots p_k d^2$ (p_i ($i=1, \dots, k$) は相異なる奇素数) と表わした時，各 i について， $p_i \equiv 1 \pmod{4}$.
2. 1.を満足する n について， $4n-2$ を2つの奇数 α, β の平方の和として書き表わす： $4n-2 = \alpha^2 + \beta^2$ ， $\alpha \equiv 1$,

$\beta \equiv 1 \pmod{4}$. このとき, $\alpha = 1 + 4W_1$, $\beta = 1 + 4W_2$ で決まる W_1, W_2 に対して

(i) $n \equiv 1 \pmod{4}$ の時, $S = \frac{1}{2}(W_1^2 + W_2^2)$ について

$$\#A_- = \#B_- = S, \quad \#A_+ = W_1 + S, \quad \#B_+ = W_2 + S;$$

(ii) $n \equiv 3 \pmod{4}$ の時, $S = \frac{1}{2}(W_1^2 + W_2^2 + W_1 + W_2)$ について

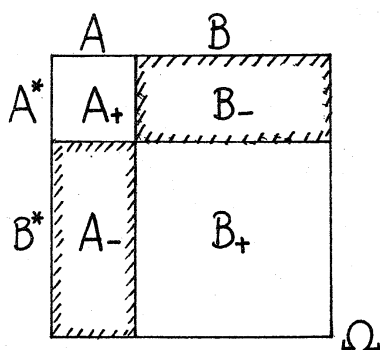
$$\#A_+ = \#B_+ = S, \quad \#A_- = S - W_1, \quad \#B_- = S - W_2.$$

(証明) 1. は $4n-2 = \alpha^2 + \beta^2$ が解を持つ為の, 即ち $2n-1$ が 2 平方和で表現出来る為の必要十分条件として明らかである.

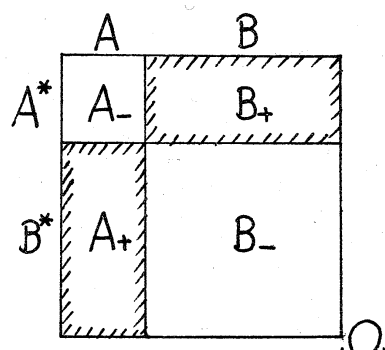
2. $n \equiv 1 \pmod{4}$ の時, 式(7)は $\nu \in \pm A$ について, $e_\nu \equiv 3 + 2\delta_{A^*}(\nu) \pmod{4}$ となり, $e_\nu = 1$ は $\nu \in \pm A^*$ と同値. 従って, $A_+ = A \cap A^*$.

同様にして図 1(a) を得る. 即ち

$$\begin{cases} A_+ = A \cap A^*, & A_- = A \cap B^*, \\ B_+ = B \cap B^*, & B_- = B \cap A^*. \end{cases}$$



(a) $n \equiv 1 \pmod{4}$ のとき.



(b) $n \equiv 3 \pmod{4}$ のとき.

図1. ベン図式.

n : 奇数より, $\#A = \#A^*$, $\#B = \#B^*$ であるから, 図1(a)より明らかのように

$$n \equiv 1 \pmod{4} \text{ ならば } \#A_- = \#B_-.$$

今, $S = \#A_- = \#B_-$ とおく. また仮定より, $W_1 = \#A_+ - \#A_-$, $W_2 = \#B_+ - \#B_-$. 従って

$$W_1 + W_2 = (r - 2S) + \left(\frac{n-1}{2} - r - 2S\right) = \frac{n-1}{2} - 4S$$

及び

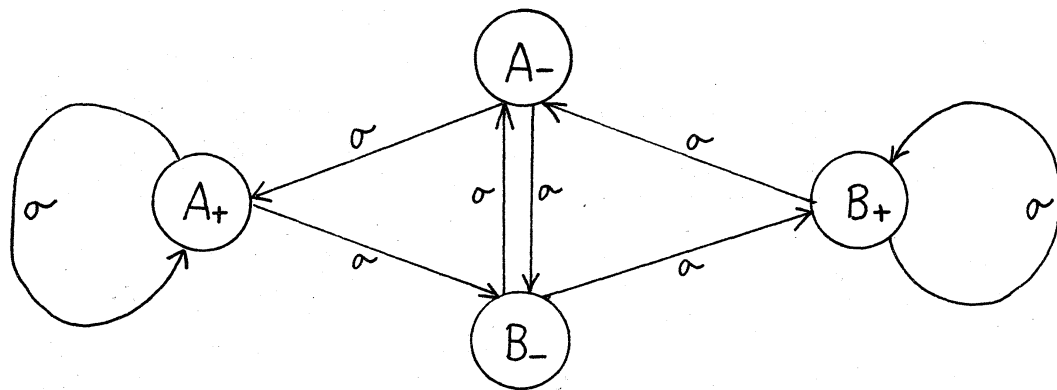
$$(1 + 4W_1)^2 + (1 + 4W_2)^2 = 4n - 2$$

より

$$W_1^2 + W_2^2 = 2S.$$

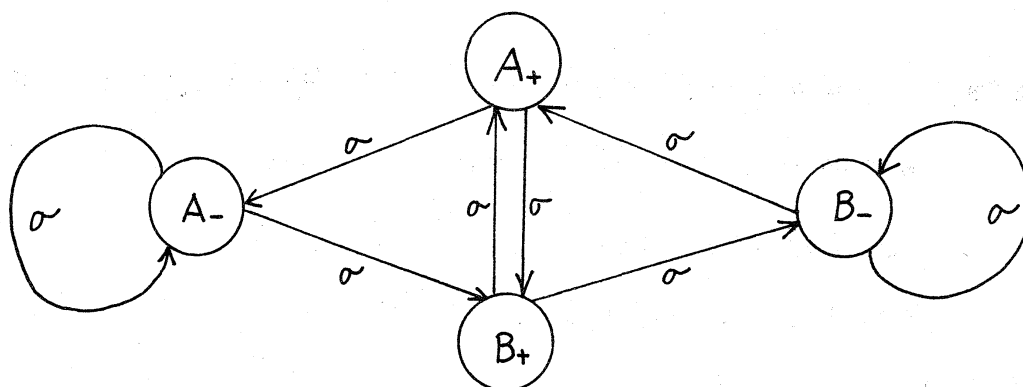
$n \equiv 3 \pmod{4}$ の場合も同様な方法で得られる.

定理2により, 与えられた n から得られる1組の α, β について, パラメータ $\#A_+, \#A_-, \#B_+, \#B_-$ が全て決定される.



(a) $n \equiv 1 \pmod{4}$ のとき

図2. 有向グラフ



(b) $n \equiv 3 \pmod{4}$ のとき

図2. (続き)

また

$$\sigma: \Omega \ni \nu \mapsto \nu^* \in \Omega, \quad \nu^* \equiv 2\nu \text{ 又は } -2\nu \pmod{n}$$

で σ を定義すると、式(7)から図2(a), (b)のような有向グラフが得られる。

4. 定理2とは逆に、パラメータ $\#A=r$ を持つ Williamson 等式の次数 n は、以下のように r によって決定されることも分かる。

定理3. $\#A=r$ なる Williamson 等式(1)が成立する次数 n は

$$4r+1 = c^2 + d^2$$

を満足する c, d について

$$n = 4r+2 - (c+d).$$

さらに

$$4r+2 - \sqrt{8r+1} \leq n \leq 4r+2 + \sqrt{8r+1}.$$

(証明) $b = \#A - \#B = r - (\frac{n-1}{2} - r) = 2r - \frac{n-1}{2}$ とおくと, 定理 2 より, $W_1 - W_2 = \pm(2r - \frac{n-1}{2}) = \pm b$. レたがって,

$$n = (4r+2) - (2b+1). \quad (8)$$

また, $a = 1 + 2(W_1 + W_2)$ とおくと

$$2n-1 = \frac{1}{2}\{(1+4W_1)^2 + (1+4W_2)^2\} = (1+2W_1+2W_2)^2 + 4(W_1-W_2)^2 = a^2 + 4b^2.$$

式(8)から

$$2n-1 = 2\{(4r+2) - (2b+1)\} - 1 = a^2 + 4b^2,$$

$$8r+2 = a^2 + (2b+1)^2,$$

$$4r+1 = \left(\frac{a+1}{2} + b\right)^2 + \left(\frac{-a+1}{2} + b\right)^2 = c^2 + d^2,$$

但し, $c = \frac{a+1}{2} + b$, $d = \frac{-a+1}{2} + b$. 従って,

$$c+d = 2b+1. \quad (9)$$

(8) 及び (9) より

$$n = (4r+2) - (c+d).$$

また一般に, $(c+d)^2 = 2(c^2+d^2) - (c-d)^2 \leq 8r+2-1 = 8r+1$.

$$\therefore 4r+2 - \sqrt{8r+1} \leq n \leq 4r+2 + \sqrt{8r+1}.$$

これは, n が r によって定まる限界内に入ることを示す.

定理 3 により, 喜安先生が示された $r=1$ に対しては, 次数 $n=3, 5, 7, 9$ の時のみ等式(1)の成立が可能で,

$$n \geq 11 \text{ ならば } 1^2 + 1^2 + (1 \pm 2u_2)^2 + (1 + 2 \sum_{\nu=2}^n e_\nu u_\nu)^2 = 4n \text{ に解がない}$$

ことが証明された。

また, $r=5, 8, 14, 17, \dots$ については, $4r+1$ を 2 平方和に表わすことが出来ない (定理 2 の 1.) ので, このようなパラメータを持つ等式 (1) は, 如何なる n をもってしても成立しないことに注意したい。

5. 定理 2 を適用して, 我々は $n \leq 37$ 及び $n=61$ について Williamson 等式 (1) の探索をすべて行なった。 $n \leq 35$ では充分手計算で間に合うが, $n=37$ と $n=61$ については計算機 (HITAC 8450) を使って run time それぞれ 2 秒と 10 分 43 秒を要した。 61 の場合は, 37 の探索に使用したアルゴリズムを改良した為, 計算時間が随分短縮されている。

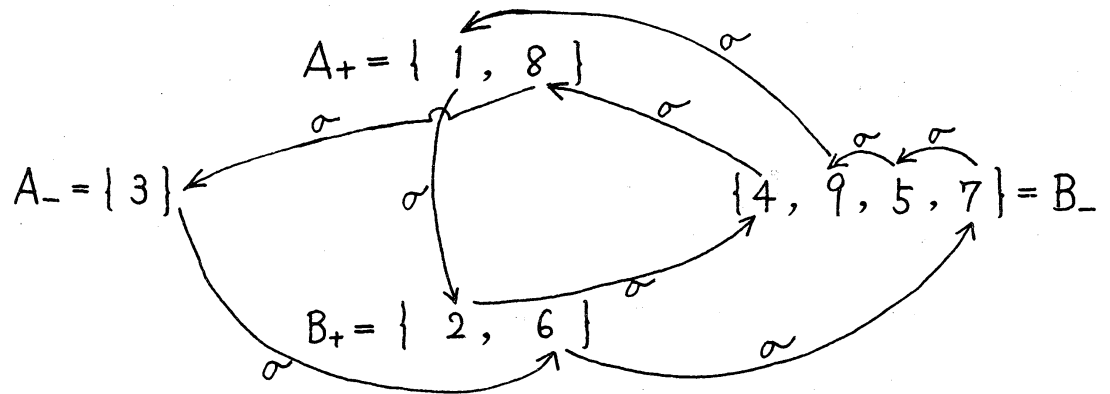
また, $n=37$ から飛ばして $n=61$ の計算を特に試みたのは, $n=61$ が 2 を原始根にもつ素数で, しかも $2n-1$ が素数中となり Turyn 型 [3] のものの存在することが分かっていると言う事にある。この時, § 3 の写像 σ が法 n では位数 $\frac{n-1}{2}$ の巡回群を生成する。即ち, 得られる有向グラフは長さが $\frac{n-1}{2}$ の周期を持つ唯一つの閉グラフで構成される為, 探索のアルゴリズムが中でも最も単純で計算機にのせ易かったからである。一般に n が素数のとき, n の既約剰余類の乗法群の中において -1 と 2 とで生成される部分群の位数を t とすると, 問題の有向グラフはそれぞれ長さ $\frac{t}{2}$ をもつ $\frac{n-1}{t}$ 個の閉グラフで構成される。

例として, 同じく 2 を原始根にもつ素数 19 の場合を挙げる.
19 次の Williamson 等式:

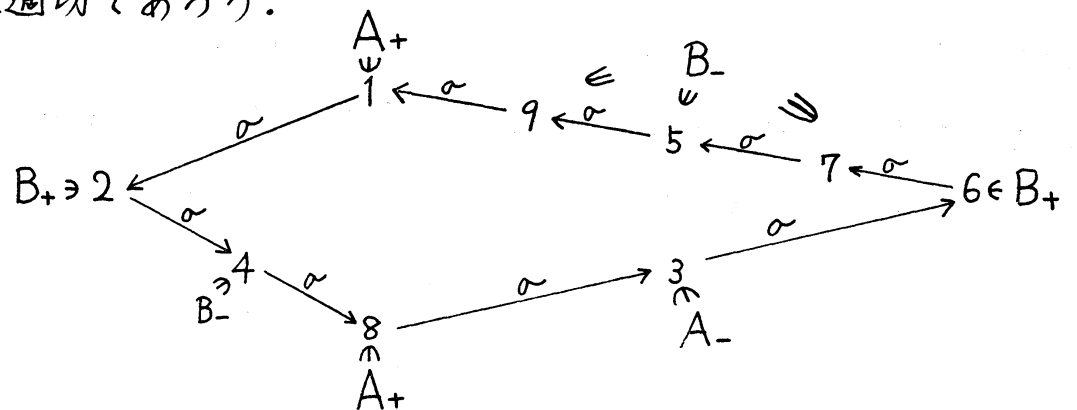
$$76 = 4 \cdot 19 = 1^2 + 1^2 + 5^2 + 7^2$$

$$= 1^2 + 1^2 + (1 + 2u_1 + 2u_8 - 2u_3)^2 + (1 + 2u_2 + 2u_6 - 2u_4 - 2u_5 - 2u_7 - 2u_9)^2$$

に対する有向グラフは



であるが, 閉グラフであることを明白にするには, 下図の方が適切であろう.



我々の現在迄の計算結果では, Williamson 等式 (I) で成立するのは, R. Turyn によって発見された系列に属するもののみで [4], 表 1 の通りである.

表1. $n < 100$ に対するパラメータ表.

$$(2n-1=a^2+b^2, r_1=\#A, r_2=\#B.)$$

$n \equiv 1 \pmod{4}$

n	2n-1	a	b	α	β	W_1	W_2	s	#A ₊	#A ₋	#B ₊	#B ₋	r_1	r_2	Result
1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	One solution
5	9	-3	0	-3	-3	-1	-1	1	0	1	0	1	1	1	One solution
9	17	1	4	-3	5	-1	1	1	0	1	2	1	1	3	One solution
13	25	5	0	5	5	1	1	1	2	1	2	1	3	3	None
		-3	4	-7	1	-2	0	2	0	2	2	2	2	4	One solution
17	33	-	-	-	-	-	-	-	-	-	-	-	-	-	-
21	41	5	4	1	9	0	2	2	2	2	4	2	4	6	One solution
25	49	-7	0	-7	-7	-2	-2	4	2	4	2	4	6	6	One solution
29	57	-	-	-	-	-	-	-	-	-	-	-	-	-	-
33	65	1	8	-7	9	-2	2	4	2	4	6	4	6	10	None
		-7	4	-11	-3	-3	-1	5	2	5	4	5	7	9	None
37	73	-3	8	-11	5	-3	1	5	2	5	6	5	7	11	One solution
41	81	9	0	9	9	2	2	4	6	4	6	4	10	10	-
45	89	5	8	-3	13	-1	3	5	4	5	8	5	9	13	-
49	97	9	4	5	13	1	3	5	6	5	8	5	11	13	-
53	105	-	-	-	-	-	-	-	-	-	-	-	-	-	-
57	113	-7	8	-15	1	-4	0	8	4	8	8	8	12	16	-
61	121	-11	0	-11	-11	-3	-3	9	6	9	6	9	15	15	One solution *
65	129	-	-	-	-	-	-	-	-	-	-	-	-	-	-
69	137	-11	4	-15	-7	-4	-2	10	6	10	8	10	16	18	-
73	145	1	12	-11	13	-3	3	9	6	9	12	9	15	21	-
		9	8	1	17	0	4	8	8	8	12	8	16	20	-
		-3	12	-15	9	-4	2	10	6	10	12	10	16	22	-
77	153	-	-	-	-	-	-	-	-	-	-	-	-	-	-
81	161	13	0	13	13	3	3	9	12	9	12	9	21	21	-
85	169	5	12	-7	17	-2	4	10	8	10	14	10	18	24	-
89	177	-	-	-	-	-	-	-	-	-	-	-	-	-	-
93	185	13	4	9	17	2	4	10	12	10	14	10	22	24	-
		-11	8	-19	-3	-5	-1	13	8	13	12	13	21	25	-
97	193	-7	12	-19	5	-5	1	13	8	13	14	13	21	27	-

* 山田美枝子氏が1979年に Shift register 列を使って発見されたもの。

表 1. (続き)

 $n \equiv 3 \pmod{4}$

n	2n-1	a	b	α	β	W_1	W_2	s	#A ₊	#A ₋	#B ₊	#B ₋	r ₁	r ₂	Result
3	5	1	2	1	-3	0	-1	0	0	0	0	1	0	1	One solution
7	13	-3	2	5	1	1	0	1	1	0	1	1	1	2	One solution
11	21	-	-	-	-	-	-	-	-	-	-	-	-	-	-
15	29	5	2	-3	-7	-1	-2	1	1	2	1	3	3	4	One solution
19	37	1	6	5	-7	1	-2	2	2	1	2	4	3	6	One solution
23	45	-3	6	9	-3	2	-1	3	3	1	3	4	4	7	None
27	53	-7	2	9	5	2	1	4	4	2	4	3	6	7	One solution
31	61	5	6	1	-11	0	-3	3	3	3	3	6	6	9	One solution
35	69	-	-	-	-	-	-	-	-	-	-	-	-	-	-
39	77	-	-	-	-	-	-	-	-	-	-	-	-	-	-
43	85	9	2	-7	-11	-2	-3	4	4	6	4	7	10	11	One solution
47	93	-7	6	13	1	3	0	6	6	3	6	6	9	12	One solution
51	101	-	-	-	-	-	-	-	-	-	-	-	-	-	-
55	109	1	10	9	-11	2	-3	6	6	4	6	9	10	15	One solution
59	117	-3	10	13	-7	3	-2	7	7	4	7	9	11	16	One solution
63	125	9	6	-3	-15	-1	-4	6	6	7	6	10	13	16	One solution
67	133	-11	2	13	9	3	2	9	9	6	9	7	15	16	One solution
71	141	5	10	5	-15	1	-4	7	7	6	7	11	13	18	One solution
75	149	-	-	-	-	-	-	-	-	-	-	-	-	-	-
79	157	-7	10	17	-3	4	-1	10	10	6	10	11	16	21	One solution
83	165	-11	6	17	5	4	1	11	11	7	11	10	18	21	One solution
87	173	-	-	-	-	-	-	-	-	-	-	-	-	-	-
91	181	13	2	-11	-15	-3	-4	9	9	12	9	13	21	22	One solution
95	189	9	10	1	-19	0	-5	10	10	10	10	15	20	25	One solution
99	197	-	-	-	-	-	-	-	-	-	-	-	-	-	-
103	205	1	14	13	-15	3	-4	12	12	9	12	16	21	28	One solution

この結果からは、問題の Williamson 等式の成り立つのは Turyn
 によって発見された系列に属するもののみであるのか否かが
 未だ分らない。また、等式(1)をさらに拡張して

$$1^2 + (1 + 2 \sum_{v \in A} e_v u_v)^2 + (1 + 2 \sum_{v \in B} e_v u_v)^2 + (1 + 2 \sum_{v \in C} e_v u_v)^2 = 4n$$

についてもパラメータを決定出来ないだろうかが今後の課題
 とするところである。

文 献

1. 喜安善市, 私信, 1980年1月.
2. R.J. Turyn, An infinite class of Williamson matrices, J. Combinatorial Theory Ser. A12 (1972), 319-321.
3. 山田美枝子, Turyn型 Williamson 行列について, 京都大学数理解析研究所講究録, 本号.
4. 山本章一, Williamson型 Hadamard 行列と shift register 列について, 大阪市立大学での「実験計画法とその関連分野」の研究集会予稿集, 1978年12月.