

Williamson 等式の拡張

東女大 文理 山本幸一

1. n 次巡回行列は, 基本的巡回行列 $T = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$ の多

項式で, 逆巡回行列は, 巡回行列と基本的逆巡回行列 $R =$

$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \end{pmatrix}$ の積を言う. 巡回行列 A に対して $RA R = A^*$ であるから, AR は対称行列になる. また巡回行列 A, B に対して $(AR)B^* = B(AR) = B(AR)^*$ が成立つ. ゆえに 4 つの巡回行列 A, B, C, D から $4n$ 次の行列

$$H = \begin{pmatrix} AR & B & C & D \\ -B & AR & D^* & -C^* \\ -C & -D^* & AR & B^* \\ -D & C^* & -B^* & AR \end{pmatrix}$$

を作れば, それは条件

$$HH^* = (AA^* + BB^* + CC^* + DD^*) \otimes I_4$$

を満たす. もし A, B, C, D の成分が ± 1 なら

$$AA^* + BB^* + CC^* + DD^* = 4nI$$

が成立するならば H は $4n$ 次の Hadamard 行列を与える. これが Goethals-Seidel 型の Hadamard 行列と呼ばれるものと本質的に同一である.

2. 今 $A = \sum_{i=0}^{n-1} a_i T^i$, $B = \sum_{i=0}^{n-1} b_i T^i$, $C = \sum_{i=0}^{n-1} c_i T^i$, $D = \sum_{i=0}^{n-1} d_i T^i$ と置いて, それらの生成多項式 $F_1(x) = \sum_{i=0}^{n-1} a_i x^i$, $F_2(x) = \sum_{i=0}^{n-1} b_i x^i$, $F_3(x) = \sum_{i=0}^{n-1} c_i x^i$, $F_4(x) = \sum_{i=0}^{n-1} d_i x^i$ を定義すれば, 各係数が ± 1 なら

$$(1) \quad F_1(x)F_1(x^{-1}) + F_2(x)F_2(x^{-1}) + F_3(x)F_3(x^{-1}) + F_4(x)F_4(x^{-1}) \equiv 4n \pmod{x^n - 1}$$

が成立するならば Goethals-Seidel 型 Hadamard 行列が出来る.

$a_i = 1$ なる添数 i の集合を A とし, その濃度を $k_1 = \#A$ とし, $P_1(x) = \sum_{i \in A} x^i$ と置き, また B, C, D や k_2, k_3, k_4 及び $P_2(x), P_3(x), P_4(x)$ を同様に定義する. そして

$$T(x) = 1 + x + x^2 + \dots + x^{n-1}$$

とすれば

$$\begin{aligned} F_1(x)F_1(x^{-1}) &= (2P_1(x) - T(x))(2P_1(x^{-1}) - T(x)) \\ &\equiv 4P_1(x)P_1(x^{-1}) - 4P_1(1)T(x) + T(1)T(x) \\ &\equiv 4P_1(x)P_1(x^{-1}) - (4k_1 - n)T(x) \pmod{x^n - 1} \end{aligned}$$

だから, (1) は

$$(2) \quad P_1(x)P_1(x^{-1}) + P_2(x)P_2(x^{-1}) + P_3(x)P_3(x^{-1}) + P_4(x)P_4(x^{-1}) \equiv$$

$$\equiv n + \lambda T(x) \pmod{x^n - 1},$$

$$\lambda = k_1 + k_2 + k_3 + k_4 - n.$$

となる. 一般に $\{0, 1, 2, \dots, n-1\}$ の部分集合 P, Q について

$$x - y \equiv l \pmod{n}, \quad x \in P, y \in Q$$

の解の個数を $[P, Q]_l$ で表わせば, 条件(2) は $l \neq 0$ のとき

$$[A, A]_l + [B, B]_l + [C, C]_l + [D, D]_l = \lambda$$

となり, この事は A, B, C, D は“相補差集合”(supplementary difference set) を作ることを意味する.

3. 以下われわれは n が奇数の場合だけを考察する. Williamson 型の場合には (2) において $P_i(x) = P_i(x^{-1})$ が要求されている. もし $0 \in A \cap B \cap C \cap D$ を仮定すれば, k_1, k_2, k_3, k_4 が奇数, 従って λ も奇数となるから

$$\begin{aligned} P_1(x^2) + P_2(x^2) + P_3(x^2) + P_4(x^2) &\equiv P_1(x)^2 + P_2(x)^2 + P_3(x)^2 + P_4(x)^2 \\ &\equiv n + \lambda T(x) \equiv 1 + T(x) \equiv \sum_{i=1}^{n-1} x^i \equiv \sum_{i=1}^{n-1} x^{2i} \pmod{(2, x^n - 1)} \end{aligned}$$

となり, $i=1, 2, \dots, n-1$ に対して a_i, b_i, c_i, d_i のうち $+1$ に等しいものの個数は必ず奇数となる.

Goethals-Seidel 型の場合については, $0 \in A \cap B \cap C \cap D$ は困難に要求できるが, a_i, b_i, c_i, d_i のうちの $+1$ の個数に関しては特別な制限は出て来ない. しかし, われわれは $i \geq 1$ の時

(4) a_i, b_i, c_i, d_i のうち正のものは奇数個だけある:

$$a_i b_i c_i d_i = -1 \quad (i=1, 2, \dots, n-1)$$

ことを仮定するものとする。

そうすれば Williamson 型の場合と同様な変形が可能になる。
それを以下に示そう。

$i \geq 1$ のとき a_i, b_i, c_i, d_i の分布は

a_i	-	+	+	+	+	-	-	-
b_i	+	-	+	+	-	+	-	-
c_i	+	+	-	+	-	-	+	-
d_i	+	+	+	-	-	-	-	+

の 8 種類だけが可能であるが、そのような分布を示す添数 i の集合をこの順に $A_+, B_+, C_+, D_+, A_-, B_-, C_-, D_-$ で表わせば、 $\Omega = \{1, 2, \dots, n-1\}$ がこれら 8 個の部分集合に分割される。(たとえば

$$a_i = 1 \iff i \in A_- \cup B_+ \cup C_+ \cup D_+,$$

$$a_i = -1 \iff i \in A_+ \cup B_- \cup C_- \cup D_-.$$

であるから,

$$\begin{aligned} F_1(x) &= 1 + \sum_{i=1}^{n-1} a_i x^i = 1 + \sum_{m \in A_-} x^m + \sum_{m \in B_+} x^m + \sum_{m \in C_+} x^m + \sum_{m \in D_+} x^m \\ &\quad - \sum_{m \in A_+} x^m - \sum_{m \in B_-} x^m - \sum_{m \in C_-} x^m - \sum_{m \in D_-} x^m \\ &= 1 - S_A + S_B + S_C + S_D, \end{aligned}$$

但し $S_A = \sum_{m \in A_+} x^m - \sum_{m \in A_-} x^m$ 等, とする。故に (2) に戻って

記号 $\bar{S}_A = \sum_{m \in A_+} x^{-m} - \sum_{m \in A_-} x^{-m}$ 等を用いて

$$\begin{aligned}
 & F_1(x)F_1(x^{-1}) + F_2(x)F_2(x^{-1}) + F_3(x)F_3(x^{-1}) + F_4(x)F_4(x^{-1}) \\
 &= (1 - S_A + S_B + S_C + S_D)(1 - \bar{S}_A + \bar{S}_B + \bar{S}_C + \bar{S}_D) + (1 + S_A - S_B + S_C + S_D)(1 + \bar{S}_A - \bar{S}_B + \bar{S}_C + \bar{S}_D) \\
 &+ (1 + S_A + S_B - S_C + S_D)(1 + \bar{S}_A + \bar{S}_B - \bar{S}_C + \bar{S}_D) + (1 + S_A + S_B + S_C - S_D)(1 + \bar{S}_A + \bar{S}_B + \bar{S}_C - \bar{S}_D) \\
 &= (1 + 2S_A)(1 + 2\bar{S}_A) + (1 + 2S_B)(1 + 2\bar{S}_B) + (1 + 2S_C)(1 + 2\bar{S}_C) + (1 + 2S_D)(1 + 2\bar{S}_D) \\
 &\equiv 4n \pmod{x^n - 1}
 \end{aligned}$$

となる.

特に $x=1$ と置けば, $W_1 = \#A_+ - \#A_-$, $W_2 = \#B_+ - \#B_-$ 等について

$$(1 + 2W_1)^2 + (1 + 2W_2)^2 + (1 + 2W_3)^2 + (1 + 2W_4)^2 = 4n$$

をおこの際

$$W_1 + W_2 + W_3 + W_4 \equiv 0 \pmod{2}$$

が必要である.

定理 集合 $\{1, 2, \dots, n-1\}$ を 8 個の部分集合 $A_+, A_-, B_+, B_-, C_+, C_-, D_+, D_-$ に分解し, $A = A_+ \cup A_-$, $B = B_+ \cup B_-$, $C = C_+ \cup C_-$, $D = D_+ \cup D_-$ とし, e_m は $A_+ \cup B_+ \cup C_+ \cup D_+ \ni m$ のとき 1 を $A_- \cup B_- \cup C_- \cup D_- \ni m$ のとき -1 を表わすとする. この際

$$\begin{aligned}
 & N(1 + 2 \sum_{m \in A} e_m x^m) + N(1 + 2 \sum_{m \in B} e_m x^m) + N(1 + 2 \sum_{m \in C} e_m x^m) \\
 &+ N(1 + 2 \sum_{m \in D} e_m x^m) \equiv 4n \pmod{x^n - 1}
 \end{aligned}$$

が成立てば, $4n$ 次の Goethals-Seidel 型 Hadamard 行列を作ることが出来る. ここに N は相対ノルムを表わす, 即ち $Nf(x) =$

$f(x)f(x^{-1})$ とする.

この定理において部分集合 $A_+, A_-, \dots$ のどれかが自己同型 $x \rightarrow x^{-1}$ で不変である場合には $u_m = x^m + x^{-m}$ と書いて,
 A_0, B_0, C_0, D_0 はそれぞれ A, B, C, D を“半分に切った”集合とすれば, 古典的な Williamson 等式

$$\begin{aligned} (1 + 2 \sum_{m \in A_0} e_m u_m)^2 + (1 + 2 \sum_{m \in B_0} e_m u_m)^2 + (1 + 2 \sum_{m \in C_0} e_m u_m)^2 + (1 + 2 \sum_{m \in D_0} u_m u_m)^2 \\ \equiv 4n \pmod{x^n - 1} \end{aligned}$$

が現われる.

4. 前掲の公式

$$\begin{aligned} (1 + 2S_A)(1 + 2\bar{S}_A) + (1 + 2S_B)(1 + 2\bar{S}_B) + (1 + 2S_C)(1 + 2\bar{S}_C) \\ + (1 + 2S_D)(1 + 2\bar{S}_D) \equiv 4n \end{aligned}$$

に戻ってその左辺を変形すると, それは

$$\begin{aligned} (5) \quad S_A \bar{S}_A + S_B \bar{S}_B + S_C \bar{S}_C + S_D \bar{S}_D \\ + \frac{1}{2} (S_A + \bar{S}_A + S_B + \bar{S}_B + S_C + \bar{S}_C + S_D + \bar{S}_D) \equiv n-1 \end{aligned}$$

の形になる. たとえば

$$S_A \bar{S}_A = \sum_{\ell=0}^{n-1} \left([A_+, A_+]_{\ell} + [A_-, A_-]_{\ell} - [A_+, A_-]_{\ell} - [A_-, A_+]_{\ell} \right) x^{\ell}$$

であるから, (5) においてまず

$$\begin{aligned} S_A \bar{S}_A + S_B \bar{S}_B + S_C \bar{S}_C + S_D \bar{S}_D \\ = \#A_+ + \#A_- + \#B_+ + \#B_- + \#C_+ + \#C_- + \#D_+ + \#D_- + \\ + \sum_{\ell=1}^{n-1} X_{\ell} x^{\ell} - \sum_{\ell=1}^{n-1} Y_{\ell} x^{\ell} = n-1 + \sum_{\ell=1}^{n-1} (X_{\ell} - Y_{\ell}) x^{\ell} \end{aligned}$$

となる. ここに

$$(6) \begin{cases} X_\ell = [A_+, A_+]_\ell + [A_-, A_-]_\ell + [B_+, B_+]_\ell + [B_-, B_-]_\ell + [C_+, C_+]_\ell + \\ \quad + [C_-, C_-]_\ell + [D_+, D_+]_\ell + [D_-, D_-]_\ell, \\ Y_\ell = [A_+, A_-]_\ell + [A_-, A_+]_\ell + [B_+, B_-]_\ell + [B_-, B_+]_\ell + [C_+, C_-]_\ell + \\ \quad + [C_-, C_+]_\ell + [D_+, D_-]_\ell + [D_-, D_+]_\ell. \end{cases}$$

更に (5) の左辺の才 2 項では

$$\begin{aligned} & \frac{1}{2} (S_A + \bar{S}_A + S_B + \bar{S}_B + S_C + \bar{S}_C + S_D + \bar{S}_D) \\ &= \frac{1}{2} \sum_{\ell=1}^{n-1} \left([A_+]_\ell - [A_-]_\ell + [-A_+]_\ell - [-A_-]_\ell + [B_+]_\ell - [B_-]_\ell + [-B_+]_\ell - [-B_-]_\ell \right. \\ & \quad \left. + [C_+]_\ell - [C_-]_\ell + [-C_+]_\ell - [-C_-]_\ell + [D_+]_\ell - [D_-]_\ell + [-D_+]_\ell - [-D_-]_\ell \right) x^\ell \end{aligned}$$

となる。こゝで

$$\left. \begin{aligned} [P]_\ell &= [P, 0]_\ell = 1 & (\ell \in P \text{ のとき}) \\ &= 0 & (\ell \notin P \text{ のとき}) \end{aligned} \right\}$$

は P の特性函数を表わす記号である。上式と

$$[A_+]_\ell + [A_-]_\ell + [B_+]_\ell + [B_-]_\ell + [C_+]_\ell + [C_-]_\ell + [D_+]_\ell + [D_-]_\ell = 1,$$

$$[-A_+]_\ell + [-A_-]_\ell + [-B_+]_\ell + [-B_-]_\ell + [-C_+]_\ell + [-C_-]_\ell + [-D_+]_\ell + [-D_-]_\ell = 1$$

の各 $\frac{1}{2}$ 倍を加えて

$$\begin{aligned} & \frac{1}{2} (S_A + \bar{S}_A + S_B + \bar{S}_B + S_C + \bar{S}_C + S_D + \bar{S}_D) + T(x) - 1 \\ &= \sum_{\ell=1}^{n-1} \left([A_+]_\ell + [-A_+]_\ell + [B_+]_\ell + [-B_+]_\ell + [C_+]_\ell + [-C_+]_\ell + [D_+]_\ell + [-D_+]_\ell \right) x^\ell \\ &= \sum_{\ell=1}^{n-1} Z_\ell x^\ell, \end{aligned}$$

$$(7) \quad Z_\ell = [A_+]_\ell + [A_-]_\ell + [B_+]_\ell + [B_-]_\ell + [C_+]_\ell + [C_-]_\ell + [D_+]_\ell + [D_-]_\ell.$$

(6) と (7) で定義される数 X_ℓ, Y_ℓ, Z_ℓ について, (5) は

$$X_l - Y_l + Z_l = 1 \quad (l=1, 2, \dots, n-1)$$

と同値になる.

6. n が与えられた時, 我々の条件を満たす分割 $A_+, A_-, \dots$ を見付ける具体的手順は次のようになるであろう.

まず $4n$ を 4 つの奇数の平方和に分けて

$$4n = (1+2W_1)^2 + (1+2W_2)^2 + (1+2W_3)^2 + (1+2W_4)^2,$$

$$W_1 + W_2 + W_3 + W_4 \equiv 0 \pmod{2}$$

なるものとし, 次に

$$\begin{cases} a_+ - a_- = W_1, & b_+ - b_- = W_2, & c_+ - c_- = W_3, & d_+ - d_- = W_4, \\ a_+ + a_- + b_+ + b_- + c_+ + c_- + d_+ + d_- = n-1 \end{cases}$$

を満たす非負整数 $a_+, a_-, b_+, b_-, c_+, c_-, d_+, d_-$ を求める. ここで

$$\#A_+ = a_+, \#A_- = a_-, \#B_+ = b_+, \#B_- = b_-, \#C_+ = c_+, \#C_- = c_-, \#D_+ = d_+,$$

$$\#D_- = d_- \text{ を満足するような分割 } A_+, A_-, B_+, B_-, \dots \text{ を作る.}$$

これから 8 個の部分集合が与えられたとして, $l \not\equiv 0 \pmod{n}$

に対して, l を

A_+ の元と A_+ の元の差として表わす方法の数,

A_- " A_- "

B_+ " B_+ "

B_- " B_- "

C_+ " C_+ "

C_- " C_- "

$$D_+ \quad , \quad D_+ \quad //$$

$$D_- \quad // \quad D_- \quad //$$

の総計を X_l とする。また l を

A_+ の元と A_- の元の差として表わす方法の数,

$$B_+ \quad // \quad B_- \quad //$$

$$C_+ \quad // \quad C_- \quad //$$

$$D_+ \quad , \quad D_- \quad //$$

の総計を Y_l とする。さらに Z_l は

$$\left. \begin{array}{ll} l \in A_+ \cup B_+ \cup C_+ \cup D_+ & \text{のとき } 1 \\ -l \in A_+ \cup B_+ \cup C_+ \cup D_+ & \text{のとき } 1 \end{array} \right\} \text{と数えた総和}$$

とする。この時凡ての l について

$$X_l - Y_l + Z_l = 1$$

が成立すれば、分割 $A_+, A_-, B_+, B_-, C_+, C_-, D_+, D_-$ から Goethals-Seidel 型の Hadamard 行列が得られる。

7. ● $n=3$ とすると $12=1^2+1^2+1^2+3^2$ ぞ、 W_1, W_2, W_3, W_4 は
(順序を無視して) 2通りだけある。

$$W_1 = \begin{array}{cc} 0 & 0 \end{array}$$

$$W_2 = \begin{array}{cc} 0 & 0 \end{array}$$

$$W_3 = \begin{array}{cc} 0 & -1 \end{array}$$

$$W_4 = \begin{array}{cc} -2 & 1 \end{array}$$

それらから分割

$$A_+ = \emptyset$$

$$A_- = \emptyset$$

$$B_+ = \emptyset$$

$$B_- = \emptyset$$

$$C_+ = \emptyset$$

$$C_- = \emptyset$$

$$D_+ = \emptyset$$

$$D_- = \{1, 2\}$$

及び

$$A_+ = \emptyset$$

$$A_- = \emptyset$$

$$B_+ = \emptyset$$

$$B_- = \emptyset$$

$$C_+ = \emptyset$$

$$C_- = \{1\}$$

$$D_+ = \{2\}$$

$$D_- = \emptyset$$

を得る. 初めのものは Williamson 方程式に対応する. 後の方は等式

$$12 = 1^2 + 1^2 + (1-2x)(1-2x^2) + (1+2x^2)(1+2x)$$

に対応する.

● $n=5$ では $20 = 1^2 + 1^2 + 3^2 + 3^2$ であり, W_1, W_2, W_3, W_4 は:

$$W_1 \quad 0 \quad 0 \quad -1 \quad 0$$

$$W_2 \quad 0 \quad -1 \quad -1 \quad 0$$

$$W_3 \quad -2 \quad 1 \quad 1 \quad 1$$

$$W_4 \quad -2 \quad -2 \quad 1 \quad 1$$

の4種がある. 始の3つでは $a_+, a_-, b_+, b_-, c_+, c_-, d_+, d_-$ が一意的に決まる. 前例に対応して要處だけを表にまとめると次のようになる.

0	$\emptyset$	$\emptyset$	0	$\emptyset$	$\emptyset$
0	$\emptyset$	$\emptyset$	-1	$\emptyset$	1
-2	$\emptyset$	1, 4	1	2	$\emptyset$
-2	$\emptyset$	2, 3	-2	$\emptyset$	3, 4

-1	$\emptyset$	1	0	1	2
-1	$\emptyset$	2	0	$\emptyset$	$\emptyset$
1	3	$\emptyset$	1	3	$\emptyset$
1	4	$\emptyset$	1	4	$\emptyset$

0	1	4	0	$\emptyset$	$\emptyset$
0	$\emptyset$	$\emptyset$	0	$\emptyset$	$\emptyset$
1	2	$\emptyset$	1	1, 2	3
1	3	$\emptyset$	1	4	$\emptyset$

● $n=7$ について

$$28 = 1^2 + 1^2 + 1^2 + 5^2 = 3^2 + 3^2 + 3^2 + 1^2,$$

w_1	0	0	0	-1	-1	0	-1	0
w_2	0	0	-1	-1	1	1	1	-2
w_3	0	-1	-1	-1	1	1	-2	-2
w_4	2	-3	2	-3	1	-2	-2	-2

120

$$28=1^2+1^2+1^2+5^2.$$

0	*	*	*	*	*	*	*	*	*	*	*	*
0	*	*	1	2	1	2	1	2	1	2	1	3
0	16	25	3	4	3	6	4	3	6	4	5	4
2	34	*	56	*	45	*	56	*	35	*	26	*
	*	*	*	*	*	*	*	*	*	*	*	*
	1	5	1	5	*	*	*	*	*	*	*	*
	3	4	4	3	1	2	1	3				
	26	*	26	*	345	6	245	6				
0	*	*	*	*	*	*	*	*				
0	1	2	1	2	1	3	*	*				
-1	*	4	*	5	*	5	1	25				
-3	*	356	*	346	*	246	*	346				
0	1	2	1	2	1	3	1	3	1	6	1	6
-1	*	3	*	3	*	4	*	5	*	2	*	3
-1	*	5	*	6	*	6	*	6	*	4	*	4
2	46	*	45	*	25	*	24	*	35	*	25	*
	1	6	*	*	*	*	*	*	*	*	*	*
	*	3	1	24	1	25	*	1	*	1		
	*	5	*	5	*	3	*	2	*	6		
	24	*	36	*	46	*	345	6	345	2		
-1	*	1	*	1								
-1	*	2	*	2								
-1	*	4	*	5								
-3	*	356	*	346								

$$28=1^2+3^2+3^2+3^2.$$

-1	*	1	*	1	*	1	*	1	*	1	*	1
1	2	*	2	*	2	*	3	*	3	*	5	*
1	3	*	5	*	6	*	5	*	6	*	6	*
1	56	4	34	6	45	3	46	2	45	2	23	4
0	1	2	1	4	1	6	*	*	*	*	*	*
1	4	*	3	*	2	*	13	2	13	4	1	*
1	6	*	5	*	4	*	6	*	6	*	6	*
-2	*	35	*	26	*	35	*	45	*	25	4	235

-1	*	1	*	1	*	1
1	2	*	3	*	5	*
-2	*	36	*	24	*	24
-2	*	45	*	56	*	36

0	*	*	*	*
-2	*	13	*	16
-2	*	26	*	25
-2	*	45	*	34

$n=5$ の場合は 6 個の解のうち唯 1 個 (最初のも) が Williamson 型に属し, $n=7$ の場合は 44 個のうち唯 2 つ (最初と最後) が Williamson 型に属する.

8. Williamson 型の場合は $A_+, A_-, \dots$ がそれぞれに, 自己同型 $x \rightarrow x^{-1}$ で不変であり, 逆にその性質で特長づけられる. 今, $n=p$ を素数 ($p \equiv 1 \pmod{3}$) とし, 対応する剰余類乗法群の中で位数 3 の元 ω をとって $x \rightarrow x^\omega$ に対応する自己同型が, 各部分集合 $A_+, A_-, \dots$ を不変に保つとするとするならば, $p \equiv 1 \pmod{3}$ が必要である外に

$$4p = (1+6w_1)^2 + (1+6w_2)^2 + (1+6w_3)^2 + (1+6w_4)^2$$

$$w_1 + w_2 + w_3 + w_4 \equiv 0 \pmod{2}$$

が解けなければならない. これはまた「任意の自然数 > 1 は 4 個の五角数の和である」という Fermat 以来の推測に関連する. すなわち $n > 1$ ならば

$$n = \frac{3k_1^2 + k_2^2}{2} + \frac{3k_2^2 + k_3^2}{2} + \frac{3k_3^2 + k_4^2}{2} + \frac{3k_4^2 + k_1^2}{2},$$

k_1, k_2, k_3, k_4 のうち真であるものの数は偶数
 に解がある. そしてこのような分解様式を持つ部分集合 A_+ ,
 A_- , ... が存在するのではないかと思われる. Wallis の本に載
 せられてゐる $n=43$, $4n=1^2+1^2+1^2+13^2$, $w_1=w_2=w_3=0$, $w_4=2$ に対
 応する例は Williamson 自身の発見にかかわるものであって, こ
 の範疇に入る.

また $p=2^2+27b^2$ の形の場合 (2 が p の立方剰余) には,
 或は Gauss の和によるパラメータ表示を持つ無限系列が存
 在するかも知れない. $p=31, 43, 109, 127, 157, 223, 229, 277,$
 $283, \dots$ である. $p=67$ の場合は $4 \cdot 67 = 1^2 + 7^2 + 7^2 + 13^2$,
 $w_1=0, w_2=1, w_3=1, w_4=2$ だから, その計算を実行すれば 268
 次の Hadamard 行列が見付るかも知れない.