《科学研究費補助金（総合研究Ａ）研究集会報告集》

代数的組合せ論
報告集

1989年11月28日～30日

於 甲 南 大 学

ま　え　が　き

この報告集は、１９８９年11月28日～30日の３日間、甲南大学理学部に於て行なわれた研究集会、「代数的組合せ論」の講演記録である。

集会はJ. Seberry、 R. G. Stanton両教授を迎え、多数の参加者を得て、盛会であった。会場の御世話、会の運営には、甲南大学伊藤昇教授、大阪教育大学大山豪、伊藤達郎両教授、鈴木寛氏にたいへん御世話になった。これら、集会に御協力戴いた方々に深く感謝致します。

なお、研究集会の諸経費、この報告集の作成経費は、文部省科学研究費総合研究A（代表者　京都大学土方弘明教授）に依った。

１９８９年12月

木　村　　　浩

目　　　次

1. Mutually Balanced Nested Designs 1

藤　原　　良（筑波大・社工）

栗　木　進　二（東京理科大・理）

2. Hamming Scheme と Riemann 面のアナロジー 13

松　本　　真（東大・理）

3. Nearly Triply Regular Symmetric 2-designs 23

伊　藤　　昇

B. Raposa（Ateneo de Manila University）

4. On the Products of Hadamard Matrices, Williamson Matrices and other Orthogonal Matrices using M-structure 29

J. Seberry（University of New South Wales）

山　田　美枝子（東女大・理）

5. Toward the Classification of Distance-Transitive Graphs of Affine Type 57

横　山　和　弘（富士通・国際研）

6. Intersection Diagrams of Distance-regular Graphs 61

野　村　和　正（東京医科歯科大）

7. Factor Sets Associated with Regular Colliniation Groups 71

平　峰　　豊（阪大・教養）

8. The Splitting Fields. of association Schemes 80

宗　政　昭　弘（大阪教育大）

9. On Spherical t-designs (a survey) 88

坂　内　英　一（九大・理）

10. Application of a Circle Theorem in Graphics 102

R, G. Stanton (University of Manitoba)

11. Codes on an Algebraic Curve 117

安 藤 清(日本医大)

水 野 弘 文(電通大)

12. 有限体の符号による二次形式の構成 125

小 関 道 夫(弘前大・理)

Mutually Balanced Nested Designs

R. Fuji-Hara and S. Kuriki

Abstract

A mutually balanced nested design of strength t is introduced. It is shown that such a nested design is equivalent to a balanced array of strength t. Some recurrsive constructions are given for a mutually balanced nested design of strength 2. Some constructions are also given for a balanced incomplete array of strength 2 which are based on a mutually balanced nested design.

1. Introduction

Let $\mathcal{S}$ be a set $\{1,2,\ldots,s\}$ of s symbols and let $\mathbf{X}$ be the set of all t-dimensional vectors with elements from $\mathcal{S}$. A *balanced array* of strength t with s symbols is a $v \times b$ array $\mathbf{A}$ whose elements are from $\mathcal{S}$ satisfying the following conditions:

(i) in any t-rowed subarray $\mathbf{A}_0$ of $\mathbf{A}$, the number of columns of $\mathbf{A}_0$ which are equal to $\mathbf{x}$ is $\mu(\mathbf{x})$ for any $\mathbf{x} \in \mathbf{X}$,

(ii) for any permutation matrix $\mathbf{P}$ of order t and for any $\mathbf{x} \in \mathbf{X}$, $\mu(\mathbf{Px}) = \mu(\mathbf{x})$.

Such an array is denoted by $BA_\mu(t,s;v)$. If $\mu(\mathbf{x}) = \mu(\mathbf{y})$ for every $\mathbf{x},\mathbf{y} \in \mathbf{X}$, then the array is called an *orthogonal array* of strength t with s symbols.

A balanced array was first introduced and studied by Chakravarti [1,2] in connection with some class of statistical designs. Many authors (e.g. [4-7]) have researched such an array. Kuriki and Fuji-Hara [4] defined an (r,λ)-design with mutually balanced nested subdesigns which is equivalent to a balanced array of strength two. For strength $t(\geq 2)$, we introduce a nested design of strength t satisfying some conditions in Section 3 and show that such a nested design is equivalent to a balanced array of strength t. We give some recurrsive constructions of a nested design of strength 2. Gill [3] generalized a balanced array to a balanced incomplete array and gave a construction of a balanced incomplete array of strength 2 there. As an application of results obtained in Section 3, we give some constructions of a balanced incomplete array of strength 2 which are based on a nested design in Section 4.

2. Balanced arrays

Let $W_t^s = \{(d_1, d_2, \ldots, d_s); d_i \geq 0, \sum_{i=1}^s d_i = t\}$. For $\mathbf{d} = (d_1, d_2, \ldots, d_s) \in W_t^s$, let $\mathbf{X_d}$ be the set of all t-dimensional vectors which contain each symbol $i \in S$ in d_i positions. If A is a balanced array of strength t with s symbols, then $\mu(\mathbf{x}) = \mu(\mathbf{y})$ holds for $\mathbf{x}, \mathbf{y} \in \mathbf{X_d}$. Obviously, if $\mathbf{x} \in \mathbf{X_d}$, then $\mathbf{X_d} = \{\mathbf{Px}$; for every permutation matrix $\mathbf{P}\}$. Therefore, we can rewrite the conditions (i) and (ii) given in Section 1 for a balanced array as follows:

$C(t, \mathbf{d})$: in any t-rowed subarray $\mathbf{A}_0$ of $\mathbf{A}$, the number of columns of $\mathbf{A}_0$ which are equal to $\mathbf{x} \in \mathbf{X_d}$ is $\nu_t(\mathbf{d})$.

If $C(t, \mathbf{d})$ are satisfied for every $\mathbf{d} \in W_t^s$, then $\mathbf{A}$ is a balanced array of strength t with s symbols. Throughout this paper, we use the conditions $C(t, \mathbf{d})$ for a balanced array instead of usual conditions given in Section 1. Note that $C(0, \mathbf{O})$ is always satisfied and $\nu_0(\mathbf{O})$ is the number of columns of $\mathbf{A}$.

Lemma 2.1. *In an array with elements from S, if s conditions in the $s+1$ conditions $C(t-1, \mathbf{d}), C(t, \mathbf{d}+\mathbf{e}_1), C(t, \mathbf{d}+\mathbf{e}_2), \ldots, C(t, \mathbf{d}+\mathbf{e}_s)$ are satisfied, then the remaining condition is also satisfied, where $\mathbf{d} \in W_{t-1}^s$ and $\mathbf{e}_i$ denotes an s-dimensional vector with unity in the i th position and zero in all other positions.*

Proof. Let $\mathbf{A}$ be an array with elements from S. Consider a $(t-1)$-rowed subarray $\mathbf{A}_0$ of $\mathbf{A}$ and a t-rowed subarray $\mathbf{A}_1$ of $\mathbf{A}$ containing $\mathbf{A}_0$ as the first $t-1$ rows. For $\mathbf{x} \in \mathbf{X_d}$, $\mathbf{d} \in W_{t-1}^s$, the number of columns of the subarray $\mathbf{A}_1$ which are equal to $[\mathbf{x}|i]$ is denoted by $\alpha([\mathbf{x}|i])$ for each $i \in \mathcal{S}$, where $[\mathbf{a}|\mathbf{b}]$ denotes the jaxtaposition of two vectors $\mathbf{a}$ and $\mathbf{b}$. In the subarray $\mathbf{A}_0$, the number of columns which are equal to $\mathbf{x}$ is denoted by $\beta(\mathbf{x})$. Since the vectors $[\mathbf{x}|1], [\mathbf{x}|2], \ldots, [\mathbf{x}|s]$ are all distinct,

$$\beta(\mathbf{x}) = \alpha([\mathbf{x}|1]) + \alpha([\mathbf{x}|2]) + \cdots + \alpha([\mathbf{x}|s])$$

holds.

Now we assume that the following s conditions are satisfied:

$$C(t-1, \mathbf{d}), C(t, \mathbf{d}+\mathbf{e}_1), \ldots, C(t, \mathbf{d}+\mathbf{e}_{s-1}),$$

then $\beta(\mathbf{x}) = \nu_{t-1}(\mathbf{d})$, $\alpha([\mathbf{x}|1]) = \nu_t(\mathbf{d}+\mathbf{e}_1), \ldots, \alpha([\mathbf{x}|s-1]) = \nu_t(\mathbf{d}+\mathbf{e}_{s-1})$ and the numbers are independent of choice of $\mathbf{A}_0$ and $\mathbf{A}_1$. Hence, $\alpha([\mathbf{x}|s])$ is determined uniquely and the number is independent of choice of $\mathbf{A}_0$ and $\mathbf{A}_1$. Therefore, the remaining condition $C(t, \mathbf{d}+\mathbf{e}_s)$ is also satisfied.

For other cases of the assumption, we can prove the statement of this lemma by the similar technique. □

As an immediate consequence of Lemma 2.1, we have:

Lemma 2.2. *In an array with elements from $\mathcal{S}$, if $C(t, \mathbf{f})$ are satisfied for every $\mathbf{f} \in W_t^s$, then $C(t-1, \mathbf{d})$ are also satisfied for every $\mathbf{d} \in W_{t-1}^s$.*

Lemma 2.2 implies that if $\mathbf{A}$ is a balanced array of strength t with s symbols, then $\mathbf{A}$ is also a balanced array of strength $t-1$ with s symbols. Furthermore, by the proof of Lemma 2.1, in a balanced array of strength t with s symbols,

$$\nu_k(\mathbf{d}) = \sum_{i=1}^{s} \nu_{k+1}(\mathbf{d}+\mathbf{e}_i)$$

hold for every $\mathbf{d} \in W_k^s$, $k < t$.

Now we clarify the conditions to be a balanced array which used in succeeding sections.

Lemma 2.3. *In a balanced array* $\mathbf{A}$ *of strength* $t-1$ *with* s *symbols, if* $C(t, \mathbf{d})$ *are satisfied for every* $\mathbf{d} = (d_1, d_2, \ldots, d_s) \in W_t^s$ *such that* $d_s = 0$*, then* $\mathbf{A}$ *is also a balanced array of strength* t *with* s *symbols.*

Proof. We will show that $C(t, \mathbf{g})$ are satisfied for every $\mathbf{g} = (g_1, g_2, \ldots, g_s) \in W_t^s$ by induction on g_s.
Since $\mathbf{A}$ is a balanced array of strength $t-1$ with s symbols, $C(t-1, \mathbf{f})$ are satisfied for every $\mathbf{f} = (f_1, f_2, \ldots, f_s) \in W_{t-1}^s$. For every $\mathbf{f} \in W_{t-1}^s$ such that $f_s = 0$, each of vectors $\mathbf{f}+\mathbf{e}_1, \ldots, \mathbf{f}+\mathbf{e}_{s-1}$ does not contain the symbol s. Hence, by the conditions of this lemma, $C(t, \mathbf{f}+\mathbf{e}_1), \ldots, C(t, \mathbf{f}+\mathbf{e}_{s-1})$ are satisfied. Therefore, by Lemma 2.1, $C(t, \mathbf{f}+\mathbf{e}_s)$ is also satisfied. This implies that $C(t, \mathbf{g})$ are satisfied for every $\mathbf{g} \in W_t^s$ such that $g_s = 1$.
The remaining part of induction is straightforward, so omitted here. □

By use of Lemma 2.3, noting that $C(0, \mathbf{O})$ is always satisfied, we have the following:

Theorem 2.4. *In an array* $\mathbf{A}$ *with elements from* S*, if* $C(k, \mathbf{d})$ *are satisfied for every* $\mathbf{d} = (d_1, d_2, \ldots, d_s) \in W_k^s$ *such that* $d_s = 0$*,* $1 \le k \le t$*, then* $\mathbf{A}$ *is a balanced array of strength* t *with* s *symbols.*

3. Mutually Balanced Nested Designs

Let V be a v-set (called *points* or *varieties*) and $\mathcal{B}$ be a collection of subsets of V (called *blocks*). Then the pair $(V, \mathcal{B})$ is called a *design*. A *t-wise balanced design* $S_\lambda(t, K; v)$ is a design $(V, \mathcal{B})$ satisfying the following condition:

for any t-subset T of V, the number of blocks containing T
is λ which is independent of the t-subset T chosen.

If, for any u-subset U $(u \le t)$ of V, the number of blocks containing U is constant (say, λ_u) which is independent of the u-subset U chosen, then the design is called a *regular t-wise balanced design* $R_{\boldsymbol{\lambda}}(t, K; v)$, where K denotes the set of block sizes of $\mathcal{B}$ and $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_t)$. In the case $t = 2$, the designs are called a *pairwise balanced design* and a *regular pairwise balanced design* (or an (r, λ)-*design*, where $r = \lambda_1$ and $\lambda = \lambda_2$), respectively.

Let $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$ and $\mathcal{B}' = \{B'_1, B'_2, \ldots, B'_b\}$. If $B'_j \subseteq B_j$ for $1 \leq j \leq b$, then $(V, \mathcal{B}')$ is called a *subdesign* of a design $(V, \mathcal{B})$. Note that B'_j can be the empty set. Suppose that there exist s subdesigns $(V, \mathcal{B}^{(i)})$, $i = 1, 2, \ldots, s$, of $(V, \mathcal{B})$, such that $\bigcup_{i=1}^{s} B_j^{(i)} = B_j$ and $B_j^{(i)} \cap B_j^{(i')} = \phi$ if $i \neq i'$, for $1 \leq j \leq b$, where $\mathcal{B}^{(i)} = \{B_1^{(i)}, B_2^{(i)}, \ldots, B_b^{(i)}\}$. For convenience, we may write a block B of $\mathcal{B}$ as $B = \{B^{(1)}; B^{(2)}; \ldots; B^{(s)}\}, B^{(i)} \in \mathcal{B}^{(i)}$. If the subdesigns satisfy the following conditions:

(i) each subdesign $(V, \mathcal{B}^{(i)})$ is an (r_i, λ_i)-design,

(ii) for any distinct points $x, y \in V$, the number of blocks $B = \{B^{(1)}; B^{(2)}; \ldots; B^{(s)}\} \in \mathcal{B}$ which contain x in $B^{(i)}$ and y in $B^{(h)}$ is exactly λ_{ih},

then we call it an (r, λ)-*design with mutually balanced nested subdesigns.* Kuriki and Fuji-Hara [4] defined the design and proved that an (r, λ)-design with mutually balanced nested s subdesigns is equivalent to a balanced array of strength 2 with $s + 1$ symbols.

Here we generalize an (r, λ)-design with mutually balanced nested subdesigns to strength t. For $\mathbf{d} = (d_1, d_2, \ldots, d_s) \in W_k^s$, let $S_1, S_2, \ldots, S_s$ be mutually disjoint subsets of V such that $|S_i| = d_i$. Then we consider the following condition:

$L(k, \mathbf{d})$: the number of blocks $B = \{B^{(1)}; B^{(2)}; \ldots; B^{(s)}\} \in \mathcal{B}$ such that each $S_i \subset B^{(i)}$ is exactly $\eta_k(\mathbf{d})$ which is independent of choice of $S_1, S_2, \ldots, S_s$.

If $L(k, \mathbf{d})$ are satisfied for every $\mathbf{d} \in W_k^s$, $1 \leq k \leq t$, then $(V, \mathcal{B})$ is called a *mutually balanced nested design* (MBND) of strength t. Such a design is denoted by $M_{\boldsymbol{\eta}}(t, s; v)$, $\boldsymbol{\eta} = \{\eta_1, \eta_2, \ldots, \eta_t\}$, where each η_k is an index function from W_k^s to nonnegative integers and $v = |V|$. Note that $L(0, \mathbf{O})$ is always satisfied and $\eta_0(\mathbf{O})$ is the number of blocks. If $L(2, 2\mathbf{e}_i)$ is satisfied, then the i th subdesign is a pairwise balanced design. If $L(1, \mathbf{e}_i)$ and $L(2, 2\mathbf{e}_i)$ are satisfied, then the i th subdesign is an (r, λ)-design such that $r = \eta_1(\mathbf{e}_i)$ and $\lambda = \eta_2(2\mathbf{e}_i)$.

The conditions of the definition of a MBND do not mension about the original big design $(V, \mathcal{B})$.

Lemma 3.1. *A mutually balanced nested design $M_\eta(t, s; v)$ $(V, \mathcal{B})$ is also a regular t-wise balanced design with parameters*

$$\lambda_k = \sum_{\mathbf{d} \in W_k^s} \binom{k}{d_1, d_2, \ldots, d_s} \eta_k(\mathbf{d})$$

for $1 \le k \le t$, where $\mathbf{d} = (d_1, d_2, \ldots, d_s)$ and $\binom{k}{d_1, d_2, \ldots, d_s}$ denotes the multinomial coefficient.

Proof. Consider a k-subset U of V for $1 \le k \le t$. The number of partition of U into $U_1, U_2, \ldots, U_s$ such that $|U_i| = d_i$ is $\binom{k}{d_1, d_2, \ldots, d_s}$. For each partition, the number of blocks $B = \{B^{(1)}; B^{(2)}; \ldots; B^{(s)}\} \in \mathcal{B}$ such that each $U_i \subset B^{(i)}$ is $\eta_k(\mathbf{d})$. Therefore, the number of blocks of $\mathcal{B}$ containing U is

$$\sum_{\mathbf{d} \in W_k^s} \binom{k}{d_1, d_2, \ldots, d_s} \eta_k(\mathbf{d}),$$

which is independent of the k-subset U chosen. Hence $(V, \mathcal{B})$ is a regular t-wise balanced design. □

Now we show that a MBND of strength t with s subdesigns is equivalent to a balanced array of strength t with $s + 1$ symbols.

Theorem 3.2. *There exists a mutually balanced nested design $M_\eta(t, s; v)$ if and only if there exists a balanced array $BA_\mu(t, s + 1; v)$ such that*

$$\mu(\mathbf{x}) = \sum_{h=0}^{t-k} (-1)^h \binom{t-k}{h} \sum_{i_1=1}^{s} \cdots \sum_{i_h=1}^{s} \eta_{k+h}(\mathbf{d} + \mathbf{e}_{i_1} + \cdots + \mathbf{e}_{i_h}) \tag{3-1}$$

for a t-dimensional vector $\mathbf{x}$ containing each symbol $i \in S$ in d_i positions and the symbol $s + 1$ in the remaining positions, where $\mathbf{d} = (d_1, d_2, \ldots, d_s) \in W_k^s$, $0 \le k \le t$, and $\binom{t-k}{h}$ denotes the binomial coefficient.

Proof. Suppose that $(V, \mathcal{B})$ is a $M_\eta(t, s; v)$. Let $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$, $b = \eta_0(\mathbf{O})$. Each block is partitioned into s subblocks, i.e., $B_j = \{B_j^{(1)}; B_j^{(2)}; \ldots; B_j^{(s)}\}$, for $1 \leq j \leq b$. From the blocks, we define a $v \times b$ array $\mathbf{A} = [a_{xj}]$ as

$$a_{xj} = \begin{cases} i, & \text{if a point } x \text{ of } V \text{ occurs } B_j^{(i)}, \\ s+1, & \text{otherwise.} \end{cases}$$

For $\mathbf{d} = (d_1, d_2, \ldots, d_s) \in W_k^s$, $1 \leq k \leq t$, let $S_1, S_2, \ldots, S_s$ be mutually disjoint subsets of V such that $|S_i| = d_i$. Since $(V, \mathcal{B})$ is a $M_\eta(t, s; v)$, the number of blocks $B = \{B^{(1)}; B^{(2)}; \ldots; B^{(s)}\} \in \mathcal{B}$ such that each $S_i \subset B^{(i)}$ is $\eta_k(\mathbf{d})$ which is independent of choice of $S_1, S_2, \ldots, S_s$. Hence, in the array $\mathbf{A}$, $C(k, \mathbf{d}')$ is satisfied for $\mathbf{d}' = (d_1', d_2', \ldots, d_{s+1}') \in W_k^{s+1}$ such that $d_i' = d_i, i = 1, 2, \ldots, s$, and $d_{s+1}' = 0$. Therefore, by Theorem 2.4, $\mathbf{A}$ is a balanced array of strength t with $s+1$ symbols.

Conversely, suppose that $\mathbf{A}$ is a $BA_\mu(t, s+1; v)$. Correspond points of a v-set V to rows of $\mathbf{A}$ and blocks of a collection $\mathcal{B}$ to columns of $\mathbf{A}$. Each block of $\mathcal{B}$ consists of points of V corresponding to entries $1, 2, \ldots, s$ of $\mathbf{A}$. For each block $B_j \in \mathcal{B}$, $1 \leq j \leq b$, we partition B_j into s subblocks $B_j^{(1)}, B_j^{(2)}, \ldots, B_j^{(s)}$ such that $B_j^{(i)}$ consists of points with the entry i. For $\mathbf{d}' = (d_1', d_2', \ldots, d_{s+1}') \in W_k^{s+1}$ such that $d_{s+1}' = 0$, $1 \leq k \leq t$, let $\mathbf{y}$ be a k-dimensional vector containing each symbol $i \in S$ in d_i' positions. Since $\mathbf{A}$ is a $BA_\mu(t, s+1; v)$, in any k-rowed subarray $\mathbf{A}_0$ of $\mathbf{A}$, the number of columns of $\mathbf{A}_0$ which are equal to $\mathbf{y}$ is $\nu_k(\mathbf{d}')$. From the definition of the design $(V, \mathcal{B})$, $L(k, \mathbf{d})$ is satisfied for $\mathbf{d} = (d_1, d_2, \ldots, d_s) \in W_k^s$ such that $d_i = d_i', i = 1, 2, \ldots, s$. Therefore, $(V, \mathcal{B})$ is a $M_\eta(t, s; v)$.

Finally, we show (3.1) by induction on k. In the case $k = t$, $\mathbf{x}$ does not contain the symbol $s+1$. Hence $\mu(\mathbf{x}) = \eta_t(\mathbf{d})$ holds.

Assuming that (3.1) holds for $k = u+1, u+2, \ldots, t$, we will show that (3.1) holds for $k = u$. Since $\mu(\mathbf{x}) = \mu(\mathbf{Px})$ for any permutation matrix $\mathbf{P}$ of order t, we may assume that, without loss of generality, $\mathbf{x}$ contains the symbol $s+1$ in the last $t - u$ positions, i.e., $\mathbf{x} = [\mathbf{x}^* | s+1 \ldots s+1]$, where $\mathbf{x}^*$ is a u-dimensional vector containing each symbol $i \in \mathcal{S}$ in d_i positions for $\mathbf{d} \in W_u^s$. Then, we have

$$\mu(\mathbf{x}) = \mu([\mathbf{x}^*|s+1\ldots s+1])$$

$$= \eta_u(\mathbf{d}) - \sum_{p=1}^{t-u} \binom{t-u}{p} \sum_{i_1=1}^{s} \cdots \sum_{i_p=1}^{s} \mu([\mathbf{x}^*|i_1 \ldots i_p s+1 \ldots s+1]). \quad (3\text{-}2)$$

Applying the assumption to (3.2), we have

$$\mu(\mathbf{x}) = \eta_u(\mathbf{d}) - \sum_{p=1}^{t-u} \binom{t-u}{p} \sum_{i_1=1}^{s} \cdots \sum_{i_p=1}^{s} \sum_{l=0}^{t-u-p} (-1)^l \binom{t-u-p}{l}$$

$$\sum_{i_{p+1}=1}^{s} \cdots \sum_{i_{p+l}=1}^{s} \eta_{u+p+l}(\mathbf{d} + \mathbf{e}_{i_1} + \cdots + \mathbf{e}_{i_p} + \cdots + \mathbf{e}_{i_{p+1}} + \cdots + \mathbf{e}_{i_{p+l}})$$

$$= \eta_u(\mathbf{d}) - \sum_{p=1}^{t-u} \binom{t-u}{p} \sum_{h=p}^{t-u} (-1)^{h-p}$$

$$\binom{t-u-p}{h-p} \sum_{i_1=1}^{s} \cdots \sum_{i_h=1}^{s} \eta_{u+h}(\mathbf{d} + \mathbf{e}_{i_1} + \cdots + \mathbf{e}_{i_h})$$

$$= \eta_u(\mathbf{d}) - \sum_{h=1}^{t-u} (-1)^h \binom{t-u}{h} \sum_{p=1}^{h} (-1)^p \binom{h}{p} \sum_{i_1=1}^{s} \cdots \sum_{i_h=1}^{s} \eta_{u+h}(\mathbf{d} + \mathbf{e}_{i_1} + \cdots + \mathbf{e}_{i_h})$$

$$= \eta_u(\mathbf{d}) + \sum_{h=1}^{t-u} (-1)^h \binom{t-u}{h} \sum_{i_1=1}^{s} \cdots \sum_{i_h=1}^{s} \eta_{u+h}(\mathbf{d} + \mathbf{e}_{i_1} + \cdots + \mathbf{e}_{i_h})$$

$$= \sum_{h=0}^{t-u} (-1)^h \binom{t-u}{h} \sum_{i_1=1}^{s} \cdots \sum_{i_h=1}^{s} \eta_{u+h}(\mathbf{d} + \mathbf{e}_{i_1} + \cdots + \mathbf{e}_{i_h}).$$

Therefore, (3.1) holds for $k = u$. □

In the case $t = 2$, we give two recurrsive constructions of a $M_{\boldsymbol{\eta}}(2, s; v)$. Constructions are shown for only $t = 2$. However, it is not difficult to generalize the constructions to any integer t.

Theorem 3.3. *If there exists a $M_{\boldsymbol{\eta}}(2, s; v)$ with the set of block sizes K and if there exist (r', λ')-designs with v' varieties for all v' in K, then there exists a $M_{\boldsymbol{\eta}'}(2, s; v)$ such that*

$$\eta_1'(\mathbf{e}_i) = r'\eta_1(\mathbf{e}_i), \qquad i = 1, 2, \ldots, s,$$

and

$$\eta_2'(\mathbf{e}_i + \mathbf{e}_j) = \lambda'\eta_2(\mathbf{e}_i + \mathbf{e}_j), \qquad i, j = 1, 2, \ldots, s.$$

Proof. Let $(V, \mathcal{B})$ be a $M_{\boldsymbol{\eta}}(2, s; v)$ with block sizes K and let $B = \{B^{(1)}; B^{(2)}; \ldots; B^{(s)}\} \in \mathcal{B}$ such that $|B| = v'$. From the assumption, there exists an (r', λ')-design $(V', \mathcal{E})$ with $v' \in K$ varieties. Relabeling V' by varieties of B, we construct a design $(B, \mathcal{E}_B)$. Then we partition each block of $\mathcal{E}_B$ by the following way:

$$E = \{E^{(1)}; E^{(2)}; \ldots; E^{(s)}\} \in \mathcal{E}_B \quad \text{if and only if} \quad E^{(i)} \subseteq B^{(i)}.$$

Applying this method for each block B of $\mathcal{B}$, we construct a new design $(V, \mathcal{B}')$. We will show that it is also a MBND. Consider each new subdesign $(V, \mathcal{B}^{(i)\prime})$, where $\mathcal{B}^{(i)\prime}$ denotes a collection of i th subblocks of $\mathcal{B}'$. For any point x of V, if $B^{(i)}$ contains x, then x is contained in r' blocks of $\mathcal{E}_B^{(i)}$. Furthermore, for any pair of distinct points x and y of V, if $B^{(i)}$ contains $\{x, y\}$, then the pair is contained in λ' blocks of $\mathcal{E}_B^{(i)}$, where $\mathcal{E}_B^{(i)}$ denotes a collection of i th subblocks of $\mathcal{E}_B$. Hence $(V, \mathcal{B}^{(i)\prime})$ is an $(r'\eta_1(\mathbf{e}_i), \lambda'\eta_2(2\mathbf{e}_i))$-design.
Next consider the condition $L(2, \mathbf{e}_i + \mathbf{e}_j)$ about the new design $(V, \mathcal{B}')$. For distinct points x and y of V such that $x \in B^{(i)}$ and $y \in B^{(j)}$, the number of blocks of $\mathcal{E}_B$ such that $x \in E^{(i)}$ and $y \in E^{(j)}$ is λ'. So $\eta_2'(\mathbf{e}_i + \mathbf{e}_j) = \lambda'\eta_2(\mathbf{e}_i + \mathbf{e}_j)$ holds. Therefore, $(V, \mathcal{B}')$ is a MBND. □

Corollary 3.4. *If there exists a $M_{\boldsymbol{\eta}}(2, s; v)$ with the set of block sizes K and if there exist $(r, 1)$-designs with v' varieties for some v' in K, then there exists a new $M_{\boldsymbol{\eta}'}(2, s; v)$ with more blocks and the different set of block sizes.*

Proof. By the same way as Theorem 3.3, we can embed small $(r', 1)$-designs with v' varieties if $v' \in K$. It is easy to see that the condition $L(2, \mathbf{e}_i + \mathbf{e}_j)$ about the new design is satisfied. However $L(1, \mathbf{e}_i)$ is usually not satisfied. To satisfy the condition, we add some new blocks such that the i th subblock consists only one point and the remaining subblocks are empty, $\{\phi; \ldots; \phi; x; \phi; \ldots; \phi\}$ for a suitable point x of V, until $L(1, \mathbf{e}_i)$ is satisfied. □

4. Balanced Incomplete Array

A *balanced incomplete array* of strength t with s symbols and d blanks is a $v \times b$ array $\mathbf{A}$ whose elements are from S satisfying the following conditions:

(i) every row has exactly d blanks,

(ii) in any t-rowed subarray $\mathbf{A}_0$ of $\mathbf{A}$, the number of columns of $\mathbf{A}_0$ which are equal to $\mathbf{x}$ is $\mu(\mathbf{x})$ for any $\mathbf{x} \in \mathbf{X}$,

(iii) for any permutation matrix $\mathbf{P}$ of order t and for any $\mathbf{x} \in \mathbf{X}$, $\mu(\mathbf{Px}) = \mu(\mathbf{x})$.

Here, the vector $\mathbf{x}$ in the conditions (ii) and (iii) does not contain any blank. Such an array is denoted by $BIA_\mu(t, s, d; v)$. Note that a $BIA_\mu(t, s, d; v)$ is not always of strength $t - 1$. By deleting i symbols of a $BA_\mu(t, s; v)$, a $BIA_\mu(t, s - i, d; v)$ is obtained for a suitable d. Gill [3] defined a balanced incomplete array and he gave a construction of such an array of strength 2 there.

Using the conditions $L(k, \mathbf{d})$ in Section 3, we characterize a balanced incomplete array.

Theorem 4.1. *A $BIA_\mu(t, s, d; v)$ is equivalent to a design $(V, \mathcal{B})$ with s subdesigns satisfying the following conditions:*

(i) *for any point $x \in V$, x is contained in exactly $b - d$ blocks of $\mathcal{B}$,*

(ii) *$L(t, \mathbf{d})$ are satisfied for every $\mathbf{d} \in W_t^s$,*

where $v = |V|$ and $b = |\mathcal{B}|$.

Proof. We define the similar correspondence to Theorem 3.2 between a incomplete array with s symbols and a design $(V, \mathcal{B})$ with s subdesigns replacing the symbol $s+1$ of a balanced array in Theorem 3.2 to blank. Then, every row of the incomplete array has exactly d blanks if and only if any point $x \in V$ is contained in exactly $b-d$ blocks of $\mathcal{B}$. Futhermore, it is obvious that two conditions $C(t, \mathbf{d})$ and $L(t, \mathbf{d})$ are equivalent for every $\mathbf{d} \in W_t^s$. Then $\mu(\mathbf{x}) = \eta_t(\mathbf{d})$ holds for a t-dimensional vector $\mathbf{x}$ containing each symbol $i \in S$ in d_i positions, where $\mathbf{d} = (d_1, d_2, \ldots, d_s)$. □

In the case $t=2$, we have $W_2^s = \{\mathbf{e}_i + \mathbf{e}_j; i, j = 1, 2, \ldots, s\}$. Hence Theorem 4.1 yields:

Corollary 4.2. *A $BIA_\mu(2, s, d; v)$ is equivalent to a design $(V, \mathcal{B})$ with s subdesigns satisfying the conditions:*

(i) *for any point $x \in V$, x is contained in exactly $b-d$ blocks of $\mathcal{B}$,*

(ii) *each subdesign $(V, \mathcal{B}^{(i)})$ is a pairwise balanced design $S_\lambda(2, K; v)$ such that $\lambda = \eta_2(2\mathbf{e}_i)$,*

(iii) *for any distinct points $x, y \in V$, the number of blocks $B = \{B^{(1)}; B^{(2)}; \ldots; B^{(s)}\} \in \mathcal{B}$ such that $x \in B^{(i)}$ and $y \in B^{(j)}$ is $\eta_2(\mathbf{e}_i + \mathbf{e}_j)$,*

where $b = |\mathcal{B}|$ and $B^{(i)}$ denotes the i th subblock of $B \in \mathcal{B}$.

In order to construct a $BIA_\mu(2, s, d; v)$, we apply a pairwise balanced design instead of an (r, λ)-design to the constructions given in Theorems 3.3 and 3.4 and to satisfy the condition (i) of Corollary 4.2, we add some blocks containing only one point.

Theorem 4.3. *If there exists a $M_\eta(2, s; v)$ with the set of block sizes K and if there exist pairwise balanced designs $S_{\lambda'}(2, K'; v')$ for all v' in K, then there exists a $BIA_\mu(2, s, d; v)$ such that*

$$\mu([ij]) = \lambda' \eta_2(\mathbf{e}_i + \mathbf{e}_j), \quad i, j = 1, 2, \ldots, s,$$

for a suitable d.

Theorem 4.4 *If there exists a $M_{\eta}(2,s;v)$ with the set of block sizes K and if there exist pairwise balanced designs $S_1(2,K';v')$ for some v' in K, then there exists a $BIA_{\mu}(2,s,d;v)$ such that*

$$\mu([ij]) = \eta_2(\mathrm{e}_i + \mathrm{e}_j), \quad i,j = 1,2,\ldots,s,$$

for a suitable d.

Note that a $BIA_{\mu}(2,s,d;v)$ constructed by Gill [3] is always a balanced array of strength 2 with $s+1$ symbols.

References

1. I.M. Chakravarti, Fractional replication in asymmetrical factorial designs and partially balanced arrays, *Sankhyā* 17 (1956) 143-164.
2. I.M. Chakravarti, On some methods of construction of partially balanced arrays, *Ann. Math. Statist.* 32 (1961) 1181-1185.
3. P.S. Gill, Balanced incomplete arrays, *J. Statist. Plann. Inference* 14 (1986) 179-185.
4. S. Kuriki and R. Fuji-Hara, Balanced arrays of strength two and nested (r,λ)-designs, submitted for publication.
5. J.A. Rafter and E. Seiden, Contributions to the theory and construction of balanced arrays, *Ann. Statist.* 2 (1974) 1256-1273.
6. J.N. Srivastava, Some general existence conditions for balanced arrays of strength t and 2 symbols, *J. Combin. Theory Ser.* A 13 (1972) 198-206.
7. J.N. Srivastava and D.V. Chopra, Balanced arrays and orthogonal arrays, in: J.N. Srivastava et al., eds., *A Survey of Combinatorial Theory* (North-Holland, Amsterdam, 1973) 411-428.

R. Fuji-Hara
Institute of Socio-Economic Planning
University of Tsukuba
Tsukuba City, Ibaraki 305, Japan

S. Kuriki
Department of Applied Mathematics
Science University of Tokyo
1-3 Kagurazaka, Shinjuku-ku, Tokyo 162, Japan

An Analogy Between Locally Hamming Graphs and Riemann Surfaces.

Makoto Matsumoto
Department of Mathematics
Faculty of Science, University of Tokyo
Hongo, Bunkyo-ku Tokyo, 113 Japan

December 16, 1989

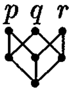
Abstract

A locally hamming graph is an undirected simple graph locally isomorphic to a hamming scheme. It was known that every locally hamming graph has a covering which is a hamming scheme. This paper proves the universality of this covering, through which we obtain 1-to-1 correspondence of Galois type between conjugate classes of discrete subgroups of the automorphic group of the r-dimensional hamming scheme and isomorphic classes of r-dimensional locally hamming graphs, analogously to the case of a Riemann surface and its fundamental group.

1 Locally Hamming Graphs and Coverings

In this paper all graphs are undirected, simple, and connected. For a graph G, $V(G)$ denotes the vertex set and $E(G)$ denotes the edge set of G. For a finite set V, $\#(V)$ denotes the cardinality of V. By $H(r)$ we denote the r-dimensional hamming scheme for $r \geq 1$; that is, $H(r)$ is such a graph that its vertex set is the vector space $\mathbf{F}_2^r$ and $u, v \in \mathbf{F}_2^r$ are adjacent if and only if the hamming distance $d(u,v) = 1$; i.e., $\#\{i \mid u_i \neq v_i\} = 1$ where $u = (u_1, \ldots, u_r)$ and $v = (v_1, \ldots, v_r)$.

Let us call $H(3)$ a *cubic*, and the graph shown in the next figure a *tulip* with petals p, q, r.



A connected graph G is said to be *locally hamming* if it satisfies:

1. G has no triangle.

2. For $u, v \in V(G)$ satisfying $d(u, v) = 2$, the span of u and v is a quadrilateral; in other words, there exist exactly two vertices adjacent to both u and v.

3. Let T be a subgraph of G isomorphic to a tulip with petals p, q, r. Then there exists a vertex $x \in V(G)$ adjacent to all p, q, and r. (The uniqueness of x follows from the condition 2.)

It can easily be proved that $H(r)$ with $r \geq 3$ is a locally hamming graph, and that a distance regular graph with parameters $a_1 = 0$, $a_2 = 0$, $c_2 = 2$, and $c_3 = 3$ (see [1] for the definition of a distance regular graph and its parameters) is also a locally hamming graph (see [5][7]). Recently, a comprehensive book on this material is also published[4].

A mapping $f : V(G) \to V(H)$ is a *morphism* $f : G \to H$ if $uv \in E(G)$ implies $f(u)f(v) \in E(H)$. A morphism $f : G \to H$ is a *locally injection* (or *locally isomorphism*) if for every $v \in V(G)$, $f|_{N(v)} : N(v) \to N(f(v))$ is injective (resp. bijective), where $N(v)$ denotes the set of vertices adjacent to v. A morphism f is a *covering* if it is locally isomorphic and surjective as a mapping $V(G) \to V(H)$.

Proposition 1. (Existence of a prolongation and its uniqueness.)
Let G be a locally hamming graph, and u be a vertex of G. Let $H(r)$ be the r-dimensional hamming scheme, and v be a vertex of $H(r)$. Given an injection $g : N(v) \to N(u)$, there exists a unique locally injection $f : H(r) \to G$ such that $f(v) = u$ and $f|_{N(v)} = g$.

This proposition and even its generalization were already proved in [3][5][7] somewhat implicitly as for uniqueness. So, this paper provides only a sketch of proof to lessen the readers' effort.

Sketch of proof. Put $H_i := \{x \in V(H(r)) \mid d(x, v) = i\}$ for $i = 0, 1, \cdots, r$. We construct locally injections

$$f_i :< H_0 \cup H_1 \cup \cdots \cup H_i >\to G$$

with $f_i|_{N(v)} = g$ by induction on i. (Here $<>$ denotes the induced subgraph.)
$i = 1$. Clearly $f|_{H_1} = g$ gives the unique solution.

$i = 2$. Let $x \in H_2$. Then there exist $x_1, x_2 \in H_1$ such that x_1x, x_2x are edges. Condition 2 in the definition of locally hamming graphs assures that there exists a unique $y \in V(G)$ such that both $f_1(x_1)y$ and $f_1(x_2)y$ are edges in G. Clearly $f_2(x)$ must coincide with y, and this provides the unique f_2. Locally injectiveness follows by a straightforward argument using Conditions 1 and 2.
$i \geq 3$. Let $x \in H_i$, then there exist exactly i vertices in H_{i-1} adjacent to x. We denote these vertices by $x_1, \ldots, x_i$. There is an $x' \in H_{i-2}$ adjacent to both x_1 and x_2. Then Condition 2 assures the existence of a unique $y \in V(G)$, $y \neq x'$, which is adjacent to both $f_{i-1}(x_1)$ and $f_{i-1}(x_2)$. The vertex $f_i(x)$ must coincide with y, and the uniqueness follows. For existence, well-definedness and locally injectiveness of f_i must be proved. For well-definedness, it is enough to prove that even if we choose x_2 and x_3 in place of x_1 and x_2, we obtain the same y above. Clearly a tulip with petals x_1, x_2, and x_3 is contained in $< H_{i-3} \cup H_{i-2} \cup H_{i-1} >$. By locally injectiveness of f_{i-1}, this tulip is isomorphically mapped into G, and Condition 3 asserts that the existence of unique z which is adjacent to all of $f_{i-1}(x_1)$, $f_{i-1}(x_2)$, and $f_{i-1}(x_3)$. It follows from Condition 2 that the above defined y coincides with this z independently of the choice of two of x_1, x_2, and x_3. Locally injectiveness straightforwardly follows from Condition 2. ■

Corollary 1. If G is a locally hamming graph, G is regular.

Proof. Let r be the maximum degree of G and take $u \in G$ with $\deg(u) = r$. Take the locally injection f of the proposition. The image of f in G is an r-regular subgraph of G, and the connectedness of G implies that the image equals G. ■

We call this r the *dimension* of G. It is clear that f in this proof is a covering. From now on, r is fixed; i.e., we consider only r-dimensional locally hamming graphs. Accordingly, locally injectiveness implies locally isomorphism and surjectiveness; that is, coveringness.

Corollary 2. (Universality of $f : H(r) \to G$)
Let $f : H(r) \to G$ be the above covering, H be an r-dimensional locally hamming graph, and $h : H \to G$ be a covering. Let w be a vertex of G, and take $v \in f^{-1}(w) \subset V(H(r))$ and $u \in h^{-1}(w) \subset V(H)$, arbitrarily. Then, there exists a unique covering $k : H(r) \to H$ such that $f = hk$ and $k(v) = u$.

Proof. Set $G' := H$ and $g' := (h|_{N(v)})^{-1} \circ (f|_{N(v)})$ and apply the proposition for $(G', u, H(r), v, g')$. Then we get $f' : H(r) \to G' = H$ such that $f'(v) = u$ and $f'|N(v) = g'$. Let k be f'. Then, $(h \circ k)|_{N(v)} = h|_{N(u)} \circ k|_{N(v)} = h|_{N(u)} \circ g' = f|_{N(v)}$ implies $h \circ k = f$ by uniqueness. The uniqueness of such k follows from the fact that $k|_{N(v)}$ must be g'. ∎

Corollary 3. (Uniqueness Theorem)
Let $g, h : H \to G$ be two coverings of locally hamming graphs. If $g|_{N(u)\cup\{u\}} = h|_{N(u)\cup\{u\}}$ for some $u \in H$, then $g = h$.

Proof. Take a covering $f : H(r) \to H$, and take a $v \in f^{-1}(u)$. Then $gf|_{N(v)\cup\{v\}} = hf|_{N(v)\cup\{v\}}$, and consequently, we have $gf = hf$ by Proposition 1, and since f is a surjection, we have $g = h$. ∎

Let $h : H \to G$ be a covering. For $u \in G$, the set $h^{-1}(u)$ is called the *fiber* on u. The *Galois group* $\mathrm{Gal}(H/G)$ of the covering $h : H \to G$ is defined to be $\{\gamma \in \mathrm{Aut}(H) \mid h \circ \gamma = h\}$. It is obvious that if $v \in V(H)$ is a vertex in the fiber on u, then γv is again in the same fiber for any $\gamma \in \mathrm{Gal}(H/G)$; i.e., $\mathrm{Gal}(H/G)$ acts on every fiber. This action is easily proved to be faithful as follows. Suppose that $\gamma \in \mathrm{Gal}(H/G)$ satisfies $\gamma(v) = v$ for some $v \in V(H)$. If $\gamma|_{N(v)} \neq \mathrm{id}$, then there exists $s \in N(v)$ such that $\gamma(s) \neq s$, and since $h\gamma(s) = h(s)$, h is not locally injective. Thus, $\gamma|_{N(v)} = \mathrm{id}$ holds, and $\gamma = \mathrm{id}$ follows from Corollary 3.

A covering $h : H \to G$ is said to be *Galois* if $\mathrm{Gal}(H/G)$ transitively acts on every fiber. This is an analogue of the Galois covering in the algebraic geometry[6].

Corollary 4. The universal covering $f : H(r) \to G$ is Galois.

Proof. This is a special case of Corollary 2 where $H = H(r)$. Note that a covering $h : H \to K$ is an isomorphism if $\#(V(H)) = \#(V(K))$.

2 Galois Groups

Let H be a locally hamming graph, and let Γ be a subgroup of $\mathrm{Aut}(H)$. We define a graph H/Γ, which contains no multi-edges but may contain loops, and obtain a canonical projection $f : H \to H/\Gamma$. The vertex set of H/Γ is

$\{\Gamma u \mid u \in H\}$, where $\Gamma u = \{\gamma u \mid \gamma \in \Gamma\}$, and Γu is adjacent to Γv in H/Γ if and only if there exists a $\gamma \in \Gamma$ such that γu is adjacent to v in H. The canonical projection f is defined by $f : u \mapsto \Gamma u$. We define the *discreteness* d_Γ of Γ by

$$\min\{d(u, \gamma u) \mid \gamma \in \Gamma, \gamma \neq \mathrm{id}, u \in V(H)\},$$

where d denotes the usual distance in the graph H. As usual, $d_{\{\mathrm{id}\}}$ is defined to be ∞.

Proposition 2. For a locally hamming graph H and a subgroup Γ of $\mathrm{Aut}(H)$, H/Γ is a locally hamming graph if and only if $d_\Gamma \geq 5$. In this case, the canonical projection is a covering.

Proof. First, we prove the sufficiency. H/Γ contains a loop if and only if there exist two adjacent vertices $s, t \in \Gamma u$ for some $u \in V(H)$. This implies $\gamma s = t$ for some $\gamma \in \Gamma$; that is, $d_\Gamma \leq 1$. For the check of Conditions 1, 2, and 3, we use the next lemma.

Lemma 1. Let $\Gamma x_1, \Gamma x_2, \ldots, \Gamma x_i$ be a walk in H/Γ; i.e., Γx_j is adjacent to Γx_{j+1} for $j = 1, 2, \ldots, i-1$. Then, there exist $x'_2, \ldots, x'_i$ such that $\Gamma x'_j = \Gamma x_j$ for $j = 2, \ldots, i$ and that $x_1, x'_2, \ldots, x'_i$ is a walk in H. Moreover, if $\Gamma x_i = \Gamma x_1$, d_Γ, and $i \geq 5$, then $x'_i = x_1$.

Proof. Since Γx_1 is adjacent to Γx_2, there exists an $x'_2 \in \Gamma x_2$ adjacent to x_1. Thus, the existence of x'_js is obvious. Suppose that $\Gamma x_i = \Gamma x_1$, that $i \leq 5$, and that $x'_i \neq x_1$. Then, since $x_1, x'_2, \ldots, x'_i$ is a path, $d(x_1, x'_i) \leq i - 1 \leq 4$. Since x'_i is in $\Gamma x_i = \Gamma x_1$, $x'_i = \gamma x_1$ for some $\gamma \in \Gamma$, and consequently $d(x_1, \gamma x_1) \leq 4$, which is a contradiction. ■

Check of Condition 1. Suppose that H/Γ contains a triangle; in other words, that $i = 3$ holds in the latter half of Lemma 1. Then, Lemma 1 asserts that the triangle can be lifted up into H, a contradiction.

Check of Condition 2. Suppose that $\Gamma u, \Gamma w, \Gamma v$ is a path of length 2. Then, by Lemma 1, we may assume that uwv is also a path, by retaking w and v. Then, there exists an x such that $< u, w, v, x >$ is a quadrilateral. It is easy to see that $< \Gamma u, \Gamma w, \Gamma v, \Gamma x >$ is a quadrilateral. Suppose that all distinct $\Gamma u, \Gamma v, \Gamma w, \Gamma x, \Gamma y$ satisfy the condition that both $< \Gamma u, \Gamma w, \Gamma v, \Gamma x >$

and $< \Gamma u, \Gamma w, \Gamma v, \Gamma y >$ are quadrilaterals in H/Γ. Apply Lemma 1 on the $< \Gamma u, \Gamma w, \Gamma v, \Gamma x >$, we get w', v', and x' so that $< u, w', v', x' >$ is a quadrilateral in H. Similarly we have y' so that $< u, w', v', y' >$ is a quadrilateral in H, and since H is a locally hamming graph, $x' = y'$ holds; that is, $\Gamma x = \Gamma x' = \Gamma y' = \Gamma y$. This completes the check of Condition 2.

Check of Condition 3. Let T be a tulip in H/Γ. Using Lemma 1 on the three quadrilaterals in T, we can lift T up into H. Then, the existence of a vertex adjacent to all petals of T in H assures the existence of the one in H/Γ. This completes the proof of sufficiency.

For the necessity, it is enough to check the following easy statements. If $d_\Gamma = 0$, then there exists a $\gamma \neq \mathrm{id}$ such that $\gamma(u) = u$. It follows from the r-regularity of H/Γ that $\gamma|_{N(u)}$ must be the identity function, and $\gamma = \mathrm{id}$ follows from the uniqueness theorem. If $d_\Gamma = 1$, then H/Γ contains a loop. If $d_\Gamma = 2$, then H/Γ is not r-regular. If $d_\Gamma = 3$, then H/Γ contains a triangle. If $d_\Gamma = 4$, then H/Γ does not satisfy the uniqueness in Condition 2. ∎

If $d_\Gamma \geq 5$, we call Γ a *discrete subgroup* of $\mathrm{Aut}(H)$.

Lemma 2. Let Γ be a discrete subgroup of $\mathrm{Aut}(H)$. Then the canonical projection $f : H \to H/\Gamma$ is Galois with $\mathrm{Gal}(H/(H/\Gamma)) = \Gamma$.

Proof. Straightforward.

Lemma 3. Let G and H be locally hamming graphs and let $f : H \to G$ be a covering. Then there exists a unique covering $h : H/\mathrm{Gal}(H/G) \to G$ such that $H \to H/\mathrm{Gal}(H/G) \to G$ coincides with f. This covering h is an isomorphism if and only if $f : H \to G$ is Galois.

Proof. The covering h is defined by $h : \mathrm{Gal}(H/G)u \mapsto fu$. The uniqueness follows from the surjectiveness of $H \to H/\mathrm{Gal}(H/G)$. It is an isomorphism if and only if it is injective on the vertex sets; i.e., $f(u) = f(v)$ implies $\mathrm{Gal}(H/G)u = \mathrm{Gal}(H/G)v$. This is equivalent to saying that $\mathrm{Gal}(H/G)$ transitively acts on every fibers; i.e., that $f : H \to G$ is Galois. ∎

The Galois correspondence between coverings and discrete subgroups is as usual best described in terms of categorical framework. Let $f : H \to G$ be a Galois covering between two locally hamming graphs. We define a category $\mathcal{S}ub(H/G)$ as follows. Its object set is the set of intermediate covering between H and G; that is, $\{< k, K, g > \mid k : H \to K, g : K \to G :$ coverings such that $f = gk\}$. Its arrow $l :< k, K, g > \to < k', K', g' >$ is a covering $l : K \to K'$ satisfying $k' = lk$ (and consequently $g = g'l$). Another category $\mathcal{G}al(H/G)$ is defined as follows. Its object set is the set of subgroups of $\mathrm{Gal}(H/G)$. For $\Gamma, \Gamma' \in \mathcal{G}al(H/G)$, there exists at most one arrow $\Gamma \to \Gamma'$, and it exists if and only if $\Gamma \subset \sigma\Gamma'\sigma^{-1}$ for some $\sigma \in \mathrm{Gal}(H/G)$. Obviously Γ and Γ' are isomorphic in $\mathcal{G}al(H/G)$ if and only if they are conjugate.

Theorem 1. For a Galois covering $f : H \to G$, $\mathcal{S}ub(H/G)$ is categorically equivalent to $\mathcal{G}al(H/G)$ by

$$\begin{array}{ccc} \mathcal{S}ub(H/G) & \cong & \mathcal{G}al(H/G) \\ < h, K, k > & \mapsto & \mathrm{Gal}(H/K) \\ H/\Gamma & \leftarrow\!\shortmid & \Gamma. \end{array}$$

Moreover, the covering $k : H \to G$ is Galois if and only if $\mathrm{Gal}(H/K)$ is a normal subgroup of $\mathrm{Gal}(H/G)$, and in this case we have a canonical isomorphism $\mathrm{Gal}(K/G) \cong \mathrm{Gal}(H/G)/\mathrm{Gal}(H/K)$.

We have another similar correspondence. For a locally hamming graph H, the category $\mathcal{S}ub(H)$ is defined by: (i) the object set is $\{< g, G > \mid g : H \to G :$ a Galois covering$\}$, (ii) an arrow $h :< g, G > \to < g', G' >$ is a covering $h : G \to G'$ with $g' = gh$. Also, the category $\mathcal{D}aut(H)$ is defined by (i) the objects are the discrete subgroups of $\mathrm{Aut}(H)$, (ii) there exists exactly one arrow $\Gamma \to \Gamma'$ if Γ is contained in some conjugate of Γ' in $\mathrm{Aut}(H)$, and none exists otherwise.

Theorem 2. Let H be a locally hamming graph. Then, the categories $\mathcal{S}ub(H)$ and $\mathcal{D}aut(H)$ are categorically equivalent by

$$\begin{array}{ccc} \mathcal{S}ub(H) & \cong & \mathcal{D}aut(H) \\ < g, G > & \mapsto & \mathrm{Gal}(H/G) \\ H/\Gamma & \leftarrow\!\shortmid & \Gamma. \end{array}$$

We can prove the above two theorems in exactly the same way with the case of Galois coverings in algebraic geometry (see [6]). The proofs are straightforward in the presence of Corollaries 1–4 of Proposition 1, Proposition 2, and Lemmas 2 and 3, and left to the readers as easy exercises. One may need an easy fact that if gh is a Galois covering then h is also. By setting $H := H(r)$ in Theorem 2, we have the next corollary.

Corollary 1. The isomorphic classes of r-dimensional hamming graphs are in 1-to-1 correspondence with the conjugate classes of discrete subgroups of $\mathrm{Aut}(H(r))$.

Thus, the classification problem of locally hamming graphs is reduced to the one of discrete subgroups of $\mathrm{Aut}(H(r))$. For an r-dimensional locally hamming graph G, the *fundamental group* $\pi_1(G)$ of G is defined to be $\mathrm{Gal}(H(r)/G)$ by taking a covering $H(r) \to G$. In the next section, the structure of $\mathrm{Aut}(H(r))$ is analyzed and examples of discrete subgroups are stated.

Remark. Any r-dimensional locally hamming graph G has a Galois covering $f : H(r) \to G$. For any $u \in V(G)$, $\pi_1(G) \cong \mathrm{Gal}(H(r)/G)$ transitively and faithfully acts on every fiber $f^{-1}(u)$, and consequently $\#(f^{-1}(u)) = \#(\pi_1(G))$. Since $2^r = \#(V(H(r))) = \sum_{u \in V(G)} \#(f^{-1}(u)) = \#(V(G)) \times \#(\pi_1(G))$, we have that both $\#(V(G))$ and $\#(\pi_1(G))$ are power of 2. It follows that every group appeared so far is a 2-group.

3 Examples

Proposition 2. (The structure of $\mathrm{Aut}(H(r))$)
The group $\mathrm{Aut}(H(r))$ is isomorphic to the wreath product $\mathbf{F}_2 \mathrm{wr} \mathcal{S}_r$.

Proof. The wreath product $\mathbf{F}_2 \mathrm{wr} \mathcal{S}_r$ is by definition (i) as a set, it is $\mathcal{S}_r \times \mathbf{F}_2^r$, where $\mathcal{S}_r$ is considered as the group of permutation matrices of size r over $\mathbf{F}_2$, (ii) the operation $\cdot$ is defined by $< \sigma, d > \cdot < \sigma', d' > = < \sigma\sigma', \sigma d' + d >$ for $\sigma, \sigma' \in \mathcal{S}_r$ and $d, d' \in \mathbf{F}_2^r$.

We construct a homomorphism $\Phi : \mathbf{F}_2 \mathrm{wr} \mathcal{S}_r \to \mathrm{Aut}(H(r))$ by $< \sigma, d > \mapsto \phi : \phi(z) = \sigma z + d$ for any $z \in \mathbf{F}_2^r$. It is easy to show that ϕ is in fact in $\mathrm{Aut}(H(r))$. The kernel of Φ is easily proved to be $\{\mathrm{id}\}$. To prove the surjectiveness, take an arbitrary $\gamma \in \mathrm{Aut}(H(r))$. Put $d := \gamma(0)$ and define

$\sigma \in \mathcal{S}_r$ so that $\sigma(e_i) = \gamma(e_i) - \gamma(0)$ holds, where e_i denotes the i-th unit vector whose components are all zero except for the i-th. We can easily check that $\Phi(<\sigma, d>)|_{N(0)\cup\{0\}} = \gamma|_{N(0)\cup\{0\}}$, and $\Phi(<\sigma, d>) = \gamma$ follows from Uniqueness Theorem. ∎

From now on, we identify Aut($H(r)$) with $\mathbf{F}_2 \mathrm{wr} \mathcal{S}_r$, and denote any element in Aut($H(r)$) in the form of $\sigma z + d$. In case that $\sigma = \mathrm{id}$, it is denoted by d. In the rest of this section, we enumerate some examples of discrete subgraph $\Gamma \subset \mathrm{Aut}(H(r))$.

Example 1. Distance-regular case.
$\Gamma = <\mathbf{1}>$, where $\mathbf{1}$ is the vector whose entries are all 1, and $<>$ denotes the generated group. Γ is discrete if and only if $r \geq 5$. It is known that $H(r)/\Gamma$ is a distance-regular graph. The next conjecture is a paraphrase of a well-known conjecture.

Conjecture. If $H(r)/\Gamma$ is a locally hamming distance-regular graph, then $\Gamma = <\mathbf{1}>$ and $r \geq 5$, or $\Gamma = \{\mathrm{id}\}$.

Rifa[5] and Nomura[7] settled some special cases of this conjecture using code theory. For the relation between completely regular codes and distance-regular graphs, see [3].

Example 2. Linear codes. Suppose that $\Gamma = <d_1, d_2, \ldots, d_i>$. In this case, we can identify Γ with a subspace in $\mathbf{F}_2^r$. A vector space $V \subset \mathbf{F}_2^r$ is said to be *k-error correcting linear code* if $\min\{d(u,v) \mid u, v \in V, u \neq v\} = 2k+1$. Thus, Γ is discrete if and only if Γ is a 2-error correcting linear code. (There are many kinds of such codes. See [2].)

Example 3. The case $\pi_1(G)$ is non-abelian. Suppose that $\Gamma \subset \mathrm{Aut}(H(r))$, and let s be a positive integer. Then, it is clear that the s-ary cartesian products of Γ, $\Gamma \times \Gamma \times \cdots \times \Gamma$, acts on $H(r \times s)$, for a positive integer s. Take the diagonal subgroup Δ of $\Gamma \times \cdots \times \Gamma$. It is isomorphic to Γ, and clearly $d_\Delta = s \cdot d_\Gamma$ holds. Thus, if one has a Γ with $d_\Gamma > 0$; in other words, a $\Gamma \subset \mathrm{Aut}(H(r))$ which has no fixed point, then there is a $\Delta \subset \mathrm{Aut}(H(5r))$ such that $\Gamma \cong \Delta$ and that $H(5r)/\Delta$ is a locally hamming graph. Let D_8 be the group generated by a, b satisfying the equation $ba = a^3 b$; i.e., the fourth dihedral group. This is the smallest non-abelian 2-group. It is clear that D_8 is isomorphic to Aut($H(2)$) and acts on $H(2)$ or $\mathbf{F}_2^2$. Let D_8 act on $H(3)$ or $\mathbf{F}_2^3 = \mathbf{F}_2^2 \oplus \mathbf{F}_2$ by setting $\sigma \cdot < d, s > := < \sigma \cdot d, s + \text{sign}(\sigma) >$ for $\sigma \in D_8$, $d \in \mathbf{F}_2^2$, and $s \in \mathbf{F}_2$, where sign(σ) is defined to be 0 if $\sigma = \text{id}$, a, a^2, or a^3, and to be 1 otherwise. With no difficulty we can check that D_8 is in fact a subgroup of Aut($H(3)$) without fixed point. Thus, there is a $\Delta \subset$ Aut($H(15)$) isomorphic to D_8 such that $H(15)/\Delta$ is a locally hamming graph.

References

[1] Bannai, E. and Ito, T. *Algebraic Combinatorics* I, Benjamin 1984.

[2] Berlekamp, E. R. *Algebraic coding theory*, McGraw-Hill, New York 1968.

[3] Brouwer, A. E. On the uniqueness of a regular thin near octagon (or partial 2-geometry, or parallelism) derived from the binary Golay code. *IEEE Trans. Inf. Theory* IT-29(1983) 370–371.

[4] Brouwer, A.E. et. al. *Distance-Regular Digraphs*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3.Folge·Band 18, Springer, 1989.

[5] Rifa, J. and Huguet, Ll. Classification of a class of distance-regular graphs via completely regular codes. *Acts. CO87.* Southampton 1987.

[6] Grothendieck, A. *Séminaire de géometrie algébrique* 1, LNM 224, Springer, 1971.

[7] Nomura, K. Distance-regular graphs of hamming type, *J. Combin. Theory Ser.* B, To appear.

[8] Nomura, K. On local structure of a distance-regular graph of hamming type. *J. Combin. Theory Ser.* B **47** (1989).

Nearly triply regular symmetric designs

伊藤昇（甲南大理），Blessilda Raposa
（Ateneo de Manila大；De la Salle大）

1．$D=(P,B)$を2-(v,k,λ)対称デザインとする．ここでP，BはそれぞれDの点およびブロックの集合を示す．任意の相異なる$\alpha,\beta,\gamma\in B$に対し$|\alpha\cap\beta\cap\gamma|$がきっかり2つの値$\mu,\nu$（$0\leq\nu<\mu\leq\lambda$）を取るなら，$D$はnearly triply regular（NTR）であるという．次の事実はすぐに確められる。

（1）上で$|\alpha\cap\beta\cap\gamma|$がconstantとすると，$D$は自明なデザイン，即ち$k=v-1$となる．逆もよい，それで以下$D$は自明でないとする．

（2）$\lambda=1,2$なら何時でもNTRである．それで以下$\lambda\geq3$とする．

（3）DがNTRならDのcomplementもNTRである．逆もよい。それで以下

$v \geq 2k+1$ とする。

2. NTRという概念は最初Herzog-Reid [1]によって、Dが特殊なアダマールデザイン、即ちアダマールトーナメントのとき、有向グラフの言葉を使って導入された様に思はれる。彼等の主要な結果は $\nu=0$ なら $\lambda=1,2$ になるということであった。然しNTRは対称デザインについての概念である。著者の1人はそこでまずアダマールデザインの時を考察した。$\mu=\lambda$ のときは $GF(2)$ 上の射影幾何型のアダマールデザインとして特徴付けられる。~~一般には~~以下 $\lambda>\mu$ とする。

(1) $\lambda\{(k-2)(\mu+\nu-1)-(\lambda-1)(\lambda-2)\}=\mu\nu(v-2)$

という容易に得られる関係式から出発する。

$\nu=0$ なら

(2) $(k-2)(\mu-1)=(\lambda-1)(\lambda-2)$

が得られる。アダマールデザインの時 $k=2\lambda+1$ であるから、$\nu=0$ なら $\lambda=1,2$ は自明で、それがHerzog-Reidの主要な結果の簡単な証明となる。そこで $\nu>0$ とする。(1)から、$v=4\lambda+3$ なので、$\mu\nu=a\lambda$、aは正整数、とおける。

$\lambda > \mu > \nu > a$ なので $12a \leq 12\lambda - 33$

である。(1) から

(3) $12a + 3 = (2\lambda - 1)(4\mu + 4\nu + 1 - 8a - 2\lambda)$

それで $4\mu + 4\nu + 1 - 8a - 2\lambda = 1, 3$ または 5

が得られる。$= 5$ のときは $6a = 5\lambda - 4$、したがって

$6\mu\nu = (5\lambda - 4)\lambda$, $6\mu + 6\nu = 13\lambda - 2$

となるが、これから $\mu > \lambda$ が出てしまう。$= 3$ の

ときは、$2a = \lambda - 1$, $2\mu\nu = (\lambda - 1)\lambda$, $2\mu + 2\nu$

$= 3\lambda - 1$ となるが、これらから $\mu = \lambda$ が出てしまう

それで、$= 1$ となる。このとき $6a = \lambda - 2$, $6\mu\nu =$

$(\lambda - 2)\lambda$, $6\mu + 6\nu = 5\lambda - 4$ である。これから

$\mu = \frac{\lambda}{2}$, $\nu = \frac{\lambda - 2}{3}$ が得られる。α, β を固定した

とき、$|\alpha \cap \beta \cap \gamma| = \nu$ となる γ の個数を d とすると、

このとき $d = 9 - \frac{36}{\lambda + 4}$ が得られる。それで

$\lambda = 8, 14, 32$。然し $|\alpha \cap \beta \cap \gamma| = \nu$ となるトリオ

$\{\alpha, \beta, \gamma\}$ 全部の個数 $t = \dfrac{\binom{4\lambda+3}{2} d}{3}$ である。

$\lambda = 14, 32$ のとき t 整数とならないので、$\lambda = 8$

を得る。この時は $d = 6$, $t = 1190$ となり、数論

的な矛盾を得るのは困難である。然し実際に

構成しようとしてみると、存在しないことは比較的

簡単にわかる（[5] 参照）

3．一般の対称デザインについて考察したとき，もう1人の著者は，$\mu=\lambda$ という仮定の下ではNTRはDembowski-Wagnerのsmoothという概念のdualということに気付いた．それで $\mu=\lambda$ のときはGF(q)上の射影幾何型のデザインとして特徴付けられた．

4．それでまた以下 $\lambda>\mu$ とする．著者達はNTRの全体像を未だ推測出来ていない。例えば $\nu=0$ なら (2) があるのであるが，はっきりわからない．それでアダマールデザインの次のデザイン類として $v=4(k-\lambda)$（アダマールは $v=4(k-\lambda)-1$ の時である）のとき，即ち正則アダマール行列型（RH）のときを考察してみた．このとき $v=4m^2$, $k=2m^2-m$, $\lambda=m^2-m$ とパラメタライズされる．もしNTRであるとすると $\mu=\frac{m^2-m}{2}$, $\nu=\frac{m^2-2m}{2}$ となることが，2でアダマールデザインの時に述べた様な仕方でわかる．とくに m は偶数となる．それで無限列を構成することを考えた．もっとも

普通の RH型デザインは $A_0 = \begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$,

$B_0 = -A_0$, $A_{i+1} = \begin{pmatrix} A_i & B_i & B_i & B_i \\ B_i & A_i & B_i & B_i \\ B_i & B_i & A_i & B_i \\ B_i & B_i & B_i & A_i \end{pmatrix}$, $B_{i+1} = -A_{i+1}$

$(i=0, 1, 2, \cdots)$ とするとき $C_{2l-1} = B_{2l-1}$ で $-1 \to 0$ としたもの、$C_{2l} = A_{2l}$ で $-1 \to 0$ として得られる $C_1, C_2, C_3, \ldots$ というシリーズである。このとき $m = 2^n$ $(n = 1, 2, 3, \ldots)$。そうするとこれが NTR であることが induction で示される。

然し、RH型デザインで NTR でないものがあることは、$m=4$ のみで（RH型デザインは m をきめるとき、mとともに非常に沢山になることが知られている）示される。

さらに $v = 4(k-\lambda)+1$ という形のときは NTR にならないことも示される。

5. NTR の dual は NTR か？ という様な問にも答が得られていない。著者達もはじめたばかりで、文献なども充分に check されていない。ご教示を待つ次第です。

[1] Herzog - Reid, Regularity in tournaments, Lecture Note in Math. 642, 442-453 (1978) Springer Verlag.

[2] Ito, Nearly triply regular Hadamard designs and tournaments; Submitted to Math. J. Okayama Univ.

[3] Raposa, On nearly triply regular symmetric designs; Submitted to Math. J. Okayama Univ.

[4] Ito - Raposa, Nearly triply regular symmetric designs of RH type; Submitted to Graphs and Combinatorics.

[5] Ito, On the non-existence of a nearly triply regular Hadamard 2-(35, 17, 8) design; to appear in Mem. Konan Univ. (1989)

Products of Hadamard Matrices, Williamson Matrices and Other Orthogonal Matrices using M-Structures

Jennifer Seberry* and Mieko Yamada†

Abstract

The new concept of M-structures is used to unify and generalize a number of concepts in Hadamard matrices including Williamson matrices, Goethals-Seidel matrices, Wallis-Whiteman matrices and generalized quaternion matrices. The concept is used to find many new symmetric Williamson-type matrices, both in sets of four and eight, and many new Hadamard matrices. We give as corollaries "that the existence of Hadamard matrices of orders $4g$ and $4h$ implies the existence of an Hadamard matrix of order $8gh$" and "the existence of Williamson type matrices of orders u and v implies the existence of Williamson type matrices of order $2uv$". This work generalizes and utilizes the work of Masahiko Miyamoto and Mieko Yamada. Lists of odd orders < 1000 for which Hadamard and Williamson type matrices are known are given.

1 Definitions and Introduction

For the definitions used in this paper, and for detailed proofs, we refer the reader to [47].

2 M-structures

An orthogonal matrix of order $4t$ can be divided into sixteen (16) $t \times t$ blocks M_{ij}. This partitioned matrix is said to be an M-structure. If the orthogonal matrix can be partitioned into sixty-four (64) $s \times s$ blocks M_{ij} it will be called a 64 block M-structure.

An Hadamard matrix made from (symmetric) Williamson matrices W_1, W_2, W_3, W_4 is an M-structure with

$$\begin{aligned} W_1 = M_{11} = M_{22} = M_{33} = M_{44}, \\ W_2 = M_{12} = -M_{21} = M_{34} = -M_{43}, \\ W_3 = M_{13} = -M_{31} = -M_{24} = M_{42}, \quad \text{and} \\ W_4 = M_{14} = -M_{41} = M_{23} = -M_{32}. \end{aligned}$$

An Hadamard matrix made from four (4) circulant (or type 1) matrices A_1, A_2, A_3, A_4 of order n, where R is the matrix which makes all the A_iR back-circulant (or type 2), is an M-structure with

$$\begin{aligned} A_1 = M_{11} = M_{22} = M_{33} = M_{44}, \\ A_2 = M_{12}R = -M_{21}R = RM_{34}^T = -RM_{43}^T, \\ A_3 = M_{13}R = -M_{31}R = -RM_{24}^T = RM_{42}^T, \quad \text{and} \\ A_4 = M_{14}R = -M_{41}R = RM_{23}^T = -RM_{32}^T. \end{aligned}$$

The next theorem and corollary are easy to prove using M-structures.

Theorem 1 *Suppose there are T-matrices of order t. Further suppose there is an $OD(4s; u_1, \ldots, u_n)$ constructed of sixteen circulant (or type 1) $s \times s$ blocks on the variables $x_1, \ldots, x_n$. Then there is an $OD(4st; tu_1, \ldots, tu_n)$. In particular if there is an $OD(4s; s, s, s, s)$ constructed of sixteen circulant (or type 1) $s \times s$ blocks then there is an $OD(4st; st, st, st, st)$.*

Corollary 2 *Suppose the T-matrices are of order t. Then there are orthogonal designs $OD(20t; 5t, 5t, 5t, 5t)$ and $OD(36t; 9t, 9t, 9t, 9t)$.*

Conjecture 3 *There exists an $OD(4t; t, t, t, t)$ for every positive integer t.*

We also conjecture

Conjecture 4 *There exists an M-structure $OD(4t; t, t, t, t)$ for every $t \equiv 1 \pmod 4$ comprising sixteen circulant or type 1 blocks.*

3 Some properties of certain amicable orthogonal matrices

We use the following three lemmas proved in [47].

Lemma 5 *Suppose there exist two amicable* $(0,+1,-1)$ *matrices* U, V *of order* u *satisfying* $UU^T + VV^T = (2u-1)I$. *Then there exist matrices* A, B, D *of order* u *satisfying*

$$AA^T + BB^T = B^TB + D^TD = (2u-1)I$$
$$A^T = (-1)^{\frac{1}{2}(u-1)}A, D^T = (-1)^{\frac{1}{2}(u-1)}D,$$

where A *and* D *have zero diagonal.*

Lemma 6 *Let* $q+1$ *be the order of a conference matrix. Then there exist four matrices* C_1, C_2, C_3, C_4, *of order* $\frac{1}{2}(q-1)$ *satisfying*

$$C_1C_1^T + C_2C_2^T = C_3C_3^T + C_4C_4^T = qI - 2J,$$
$$eC_1^T = eC_4^T = e, \quad eC_2^T = eC_3^T = 0,$$
$$C_1C_3^T - C_2C_4^T = 0, \quad C_1^T = C_1, \quad C_4^T = C_4, \quad C_3^T = C_2,$$

where e *is the* $1 \times \frac{1}{2}(q-1)$ *matrix of ones,* C_1 *and* C_4 *have zero diagonal elements* ± 1, C_2 *and* C_4 *have elements* ± 1.

Lemma 7 *Suppose there exist two amicable* $(0,+1,-1)$ *matrices* U, V *of order* u *satisfying* $UU^T + VV^T = (2u-1)I$. *Further suppose* U *has zero diagonal and* U, V *have other elements* $+1$ *or* -1. *Then there exist matrices* A, B *of order* $u-1$ *satisfying*

$$AA^T + BB^T = (2u-1)I_{u-1} - 2J_{u-1},$$
$$eA^T = e, \quad eB^T = 0, \quad AB^T = BA^T,$$

where A *has one zero element per row and column and the other entries of* A *and* B *are* ± 1. *Further if* U *and* V *are symmetric (or skew-type respectively) then* A *and* B *are symmetric (or skew-type respectively).*

Furthermore if U *and* V *satisfy* $UU^T + VV^T = 2uI$ (U, V *are* $(1,-1)$ *matrices),* u *even, then there exist matrices* A, B *of order* $u-1$, *with entries* ± 1, *satisfying*

$$AA^T + BB^T = 2uI_{u-1} - 2J_{u-1},$$
$$eA^T = e, \quad eB^T = e, \quad AB^T = BA^T,$$

and if U *and* V *are symmetric (or skew-type respectively) then* A *and* B *are symmetric (or skew-type respectively).*

4 A multiplication Theorem using M-structures

Theorem 8 *Let* $N = (N_{ij})$, $i,j = 1,2,3,4$ *be an Hadamard matrix of order* $4n$ *of M-structure. Further let* T_{ij}, $i,j = 1,2,3,4$ *be 16* $(0,+1,-1)$ *type 1 or circulant matrices of order* t *which satisfy* *(i)* $T_{ij} * T_{ik} = 0$, $T_{ji} * T_{ki} = 0$, $j \neq k$, *(* the Hadamard product)*

(ii) $\sum_{k=1}^{4} T_{ik}$ *is a* $(1, -1)$ *matrix,* (1)

(iii) $\sum_{k=1}^{4} T_{ik}T_{ik}^T = tI_t = \sum_{k=1}^{4} T_{ki}T_{ki}^T$,

(iv) $\sum_{k=1}^{4} T_{ik}T_{jk}^T = 0 = \sum_{k=1}^{4} T_{ki}T_{kj}^T$, $i \neq j$.

Then there is an M-structure Hadamard matrix of order $4nt$.

Corollary 9 *If there exists an Hadamard matrix of order* $4h$ *and an orthogonal design* $OD(4u; u_1, u_2, u_3, u_4)$, *then an* $OD(8hu; 2hu_1, 2hu_2, 2hu_3, 2hu_4)$ *exists.*

Corollary 10 *If there exists an Hadamard matrix of order* $4h$ *and an orthogonal design* $OD(4u; u, u, u, u)$, *then there exists an* $OD(8hu; 2hu, 2hu, 2hu, 2hu)$.

This gives the theorem of Agayan and Sarukhanyan [2] as a corollary by setting all variables equal to one:

Corollary 11 *If there exists Hadamard matrices of orders* $4h$ *and* $4u$ *then there exists an Hadamard matrix of order* $8hu$.

We now give as a corollary a result, motivated by, and a little stronger than that of Agayan and Sarukhanyan [2]:

Corollary 12 *Suppose there are Williamson or Williamson type matrices of orders* u *and* v. *Then there are Williamson type matrices of order* $2uv$.

If the matrices of orders u *and* v *are symmetric the matrices of order* $2uv$ *are also symmetric.*

If the matrices of orders u *and* v *are circulant and/or type 1 the matrices of order* $2uv$ *are type 1.*

5 Miyamoto's Theorem and Corollaries via M-structures

We reformulate Miyamoto's results so that symmetric Williamson-type matrices can be obtained.

Lemma 13 (Miyamoto's Lemma Reformulated) *Let* U_i, V_j, $i, j = 1, 2, 3, 4$ *be* $(0, +1, -1)$ *matrices of order* n *which satisfy*

(i) U_i, U_j, $i \neq j$ *are pairwise amicable,*

(ii) V_i, V_j, $i \neq j$ *are pairwise amicable,*

(iii) $U_i \pm V_i$, *$(+1,-1)$ matrices,* $i = 1,2,3,4$,

(iv) the row sum of U_1 *is 1, and the row sum of* U_j, $i = 2,3,4$ *is zero,*

(v) $\sum_{i=1}^{4} U_i U_i^T = (2n+1)I - 2J$, $\sum_{i=1}^{4} V_i V_i^T = (2n+1)I$.

Then there are 4 Williamson type matrices of order $2n+1$. *If* U_i *and* V_i *are symmetric,* $i = 1,2,3,4$ *then the Williamson-type matrices are symmetric. Hence there is a Williamson type Hadamard matrix of order* $4(2n+1)$.

Corollary 14 *Let* $q \equiv 1 \pmod 4$ *be a prime power then there are symmetric Williamson type matrices of order* $q+2$ *whenever* $\frac{1}{2}(q+1)$ *is a prime power or* $\frac{1}{2}(q+3)$ *is the order of a symmetric conference matrix. Also there exists an Hadamard matrix of Williamson type of order* $4(q+2)$.

Remark 15 Some of the results in Corollary 14 are also due to A.L. Whiteman [35]. This gives symmetric Williamson-type matrices of orders

7	11	15	19	27	39	51	55	63	75
83	91	99	123	159	195	243	279	315	339
363	399	423	451	459	543	579	615	627	663
675	735	759	843	879	883	999	1095	1155	1203
1215	1239	1251	1323	1383	1455	1623	1659	1683	1755
1875	1935	1995							

(since Mathon found conference matrices of orders 46 and 442). Almost all these, with symmetry, are new though Miyamoto [12] has found Williamson-type matrices for these orders and hence Hadamard matrices for four times these orders.

Koukouvinos and Kounias [10] have shown there are no circulant symmetric Williamson matrices of order 39 but here a symmetric but not circulant Williamson matrix of order 39 is given.

Corollary 16 *Let* $q \equiv 1 \pmod 4$ *be a prime power. Then*

(i) if there are Williamson type matrices of order $(q-1)/4$ *or an Hadamard matrix of order* $\frac{1}{2}(q-1)$ *there exist Williamson type matrices of order* q;

(ii) if there exist symmetric conference matrices of order $\frac{1}{2}(q-1)$ *or a symmetric Hadamard matrix of order* $\frac{1}{2}(q-1)$ *then there exist symmetric Williamson type matrices of order* q.

Hence there exists an Hadamard matrix of Williamson type of order $4q$.

Remark 17 Part (i) of Corollary 16 for Williamson matrices of order $(q-1)/4$ was found by Miyamoto [12]. Part (i) with Hadamard matrices of order $\frac{1}{2}(q-1)$ is new. Part (ii) with symmetry is new.

Corollary 16 (ii) gives symmetric Williamson-type matrices of order q when $q \equiv 1 \pmod 4$ is a prime power and $\frac{1}{2}(q-1)$ is the order of a symmetric conference matrix. This gives symmetric Williamson-type matrices for the following orders:

13	29	37	53	61	101	109	125	149	181
197	229	277	317	349	389	397	461	541	557
677	701	709	797	821	1021	1061	1117	1229	1237
1549	1597	1621	1709	1861	1877	1997			

Corollary 16 part (ii) gives symmetric Williamson-type matrices of order q when $q \equiv 1 \pmod 4$ is a prime power and $\frac{1}{2}(q-1)$ is the order of a symmetric Hadamard matrix. Rembering that symmetric Hadamard matrices exist for orders $p+1$ when $p \equiv 3 \pmod 4$ is a prime power we have symmetric Williamson-type matrices for the following orders:

5	9	17	25	41	49	73	81	89	97
113	121	169	193	241	257	281	289	337	353
361	401	409	433	449	457	529	569	577	593
601	617	625	641	673	729	761	769	841	881
929	937	961	977	1009	1033	1049	1097	1129	1153
1201	1217	1249	1289	1297	1321	1361	1369	1409	1481
1489	1553	1601	1609	1657	1681	1697	1721	1777	1801
1849	1873								

Corollary 16 part (i) gives Williamson-type matrices of order q when $q \equiv 1 \pmod 4$ is a prime power and $\frac{1}{2}(q-1)$ is the order of an Hadamard matrix. This gives Williamson-type matrices for the following orders not given above:

137	233	313	521	809	953	1193	1753	1889	1993

Corollary 16 part (i) gives Williamson-type matrices of order q when $q \equiv 1 \pmod 4$ is a prime power and $(q-1)/4$ is the order of Williamson-type matrices. This result is also due to Miyamoto [12]. This gives Williamson-type matrices for the following orders:

157	173	293	373	613	757	757	773	1109	1301
1453	1493	1637	1693	1733	1741				

Corollary 18 *Let $q \equiv 1 \pmod 4$ be a prime power or $q+1$ the order of a symmetric conference matrix. Let $2q-1$ be a prime power. Then there exist*

symmetric Williamson type matrices of order $2q+1$ and an Hadamard matrix of Williamson type of order $4(2q+1)$.

Remark 19 Corollary 18 is satisfied for the appropriate primes or conference matrix orders to give symmetric Williamson-type matrices for the following orders:

11	19	27	51	75	83	91	99	123	195
243	315	339	363	451	459	579	627	675	843
883	1155	1203	1251	1323	1659	1683	1755	1875	1995
2019	2139	2403	2475	2595	2859	3043	3219	3315	3363
3483	3699	3723							

Note this last corollary is a modified version of Miyamoto's Corollary 5 (original manuscript). A new proof of Miyamoto's result, preserving symmetry, gives:

Corollary 20 *Let $q \equiv 5 \pmod 8$ be a prime power. Further let $\frac{1}{2}(q-3)$ be a prime power or $\frac{1}{2}(q-1)$ be the order of a symmetric conference matrix then there exist symmetric Williamson type matrices of order q and an Hadamard matrix of Williamson type of order $4q$.*

Theorem 21 (Miyamoto's Theorem Reformulated) *Let U_{ij}, V_{ij}, $i,j = 1,2,3,4$ be $(0,+1,-1)$ matrices of order n which satisfy*

(i) U_{ki}, U_{kj}, $i \neq j$ *are pairwise amicable,* $k = 1,2,3,4$,

(ii) V_{ki}, V_{kj}, $i \neq j$ *are pairwise amicable,* $k = 1,2,3,4$,

(iii) $U_{ki} \pm V_{ki}$, $(+1,-1)$ *matrices,* $i,k = 1,2,3,4$,

(iv) the row sum of U_{ii} is 1, and the row sum of U_ij is zero, $i \neq j$, $i,j = 1,2,3,4$,

(v) $\sum_{i=1}^{4} U_{ji}U_{ji}^T = (2n+1)I - 2J$, $\sum_{i=1}^{4} V_{ji}V_{ji}^T = (2n+1)I$, $j = 1,2,3,4$,

(vi) $\sum_{i=1}^{4} U_{ji}U_{ki}^T = 0$, $\sum_{i=1}^{4} V_{ji}V_{ki}^T = 0$, $j \neq k$, $j,k = 1,2,3,4$.

If conditions (i) to (v) hold, there are four Williamson matrices type of order $2n+1$ and thus a Williamson type Hadamard matrix of order $4(2n+1)$. Furthermore if the matrices U_{ki} and V_{ki} are symmetric for all $i,j = 1,2,3,4$ the Williamson matrices obtained of order $2n+1$ are also symmetric.

If conditons (iii) to (vi) hold, there is an M-structure Hadamard matrix of order $4(2n+1)$.

Proof: Use

$$X_{11}=\begin{bmatrix} -1 & -e \\ -e^T & S_{11} \end{bmatrix} \quad X_{12}=\begin{bmatrix} 1 & e \\ e^T & S_{12} \end{bmatrix} \quad X_{13}=\begin{bmatrix} 1 & e \\ e^T & S_{13} \end{bmatrix} \quad X_{14}=\begin{bmatrix} -1 & e \\ e^T & S_{14} \end{bmatrix}$$

$$X_{21}=\begin{bmatrix} 1 & e \\ e^T & S_{21} \end{bmatrix} \quad X_{22}=\begin{bmatrix} -1 & -e \\ -e^T & S_{22} \end{bmatrix} \quad X_{23}=\begin{bmatrix} 1 & e \\ e^T & S_{23} \end{bmatrix} \quad X_{24}=\begin{bmatrix} -1 & e \\ e^T & S_{24} \end{bmatrix}$$

$$X_{31}=\begin{bmatrix} 1 & e \\ e^T & S_{31} \end{bmatrix} \quad X_{32}=\begin{bmatrix} 1 & e \\ e^T & S_{32} \end{bmatrix} \quad X_{33}=\begin{bmatrix} -1 & -e \\ -e^T & S_{33} \end{bmatrix} \quad X_{34}=\begin{bmatrix} -1 & e \\ e^T & S_{34} \end{bmatrix}$$

$$X_{41}=\begin{bmatrix} -1 & e \\ e^T & -S_{41} \end{bmatrix} \quad X_{42}=\begin{bmatrix} 1 & e \\ e^T & -S_{42} \end{bmatrix} \quad X_{43}=\begin{bmatrix} -1 & e \\ e^T & -S_{43} \end{bmatrix} \quad X_{44}=\begin{bmatrix} -1 & -e \\ -e^T & -S_{44} \end{bmatrix}$$

We note that the following always holds as it is just a case of Miyamoto's Lemma Reformulated:

$$\sum_{i=1}^{4} S_{ji}S_{ji}^T = 4(2n+1)I_{2n} - 4J_{2n}. \tag{2}$$

In all cases though assumption (vi) assures us that

$$\sum_{i=1}^{4} S_{ki}S_{ji}^T = 0, \quad j \neq k. \tag{3}$$

Note that if we write our M-structure from the theorem as

-1	1	1	-1	-e	e	e	e
1	-1	1	-1	e	-e	e	e
1	1	-1	-1	e	e	-e	e
1	1	1	1	-e	-e	-e	e
$-e^T$	e^T	e^T	e^T	S_{11}	S_{12}	S_{13}	S_{14}
e^T	$-e^T$	e^T	e^T	S_{21}	S_{22}	S_{23}	S_{24}
e^T	e^T	$-e^T$	e^T	S_{31}	S_{32}	S_{33}	S_{34}
$-e^T$	$-e^T$	$-e^T$	e^T	S_{41}	S_{42}	S_{43}	S_{44}

and we can see Yamada's matrix with trimming [46] or the J. Wallis-Whiteman [30] matrix with a border embodied in the construction.

Corollary 22 *Suppose there exists a symmetric conference matrix of order $q+1 = 4t+2$ and an Hadamard matrix of order $4t = q-1$. Then there is an Hadamard matrix with M-structure of order $4(4t+1) = 4q$. Further if the Hadamard matrix is symmetric the Hadamard matrix of order $4q$ is of the form*

$$\begin{bmatrix} X & Y \\ -Y & X \end{bmatrix},$$

where X, Y are amicable and symmetric.

We note that complex Hadamard matrices of order $n \equiv 2 \pmod 4$ do exist when symmetric conference matrices cannot exist (see [22, Chapter VI]). These complex Hadamard matrices may be written as $K = X + iY$ where $KK* = kI_k$ ($*$ the Hermitian conjugate).

Hence we have

Corollary 23 *Let $q \equiv 4f + 1$ be a prime power. Suppose there is a complex Hadamard matrix of order $2f$. Then there is an Hadamard matrix of order $4(4f + 1)$.*

Note complex Hadamard matrices exist for orders 22, 34, 58, 86, 306, 650, 870, 1046, 2450, 3782, ..., for which either a symmetric conference matrix cannot exist or is not known. None of these orders give new Hadamard matrices.

6 Using 64 Block M-structures

In a similar fashion, we consider the following lemma so symmetric 8-Williamson-type matrices can be obtained.

Lemma 24 *Let U_i, V_j, $i, j = 1, \ldots, 8$ be $(0, +1, -1)$ matrices of order n which satisfy*

(i) U_i, U_j, $i \neq j$ *are pairwise amicable,*

(ii) V_i, V_j, $i \neq j$ *are pairwise amicable,*

(iii) $U_i \pm V_i$, $(+1, -1)$ *matrices,* $i = 1, \ldots, 8$,

(iv) the row(column) sums of U_1 *and* U_2 *are both 1, and the row sum of* U_j, $i = 3, \ldots, 8$ *is zero,*

(v) $\sum_{i=1}^{8} U_i U_i^T = 2(2n + 1)I - 4J$, $\sum_{i=1}^{8} V_i V_i^T = 2(2n + 1)I$.

Then there are 8-Williamson type matrices of order $2n + 1$. Furthermore, if the U_i and V_i are symmetric, $i = 1, \ldots, 8$, then the 8-Williamson type matrices are symmetric. Hence there is a block type Hadamard matrix of order $8(2n + 1)$.

Corollary 25 *Let $q + 1$ be the order of amicable Hadamard matrices $I + S$ and P. Suppose there exist 4 Williamson type matrices of order q. Then there exist Williamson type matrices of order $2q + 1$. Furthermore there exists an Hadamard matrix of block type of order $8(2q + 1)$.*

Using the amicable Hadamard matrices given in [22] and [16, Table 1] we get 8 Williamson type matrices for the following orders for which 4 Williamson matrices are not known:

47, 111, 127, 167, 319, 487, 655, 831, ...

This gives new constructions for Hadamard matrices of orders 8.167 and 8.487.

Corollary 26 *Let q be a prime power and $(q-1)/2$ be the order of four (symmetric) Williamson type matrices. Then there exist (symmetric) 8-Williamson type matrices of order q and an Hadamard matrix of block structure of order $8q$.*

In particular we have 8-Williamson matrices for the following orders for which no Williamson type matrices are known:
59, 67, 103, 107, 151, 163, 179, 227, 251, 283, 347, 463, 467, 523, 563, 571, 587, 631, 643, 823, 859, 919, 947, ...

This gives new Hadamard matrices or new constructions for Hadamard matrices of orders 8.107, 8.163, 8.179, 8.251, 8.283, 8.347, 8.463, 8.523, 8.571, 8.631, 8.643, 8.823, 8.859, 8.919, 8.947, ...

Corollary 27 *Let $q \equiv 1 \pmod 4$ be a prime power or $q+1$ the order of a symmetric conference matrix. Suppose there exist four (symmetric) Williamson type matrices of order q. Then there exist (symmetric) 8-Williamson type matrices of order $2q+1$ and an Hadamard matrix of block structure of order $8(2q+1)$.*

This corollary gives 8 Williamson type matrices for the following new orders:
219, 275, 299, 395, 483, 515, 579, 635, 699, 707, 723, 779, 795, 803, 899, 915, 923, ...

It does not give new Hadamard matrices for these orders.

Corollary 28 *Let $q = 9^t$, $t > 0$. Now there exist four (symmetric) Williamson type matrices of order 9^t, $t > 0$. Hence there exist (symmetric) 8-Williamson type matrices of order $2\cdot 9^t + 1$, $t > 0$, and an Hadamard matrix of block structure of order $8(2\cdot 9^t + 1)$.*

This gives symmetric 8-Williamson type matrices for the new order 163, 13123, ...

Also we have the following theorem:

Theorem 29 *Let U_{ij}, V_{ij}, $i,j = 1,\dots,8$ be $(0,+1,-1)$ matrices of order n which satisfy*

(i) U_{ki}, U_{kj}, $i \neq j$ are pairwise amicable, $k = 1,\dots,8$,

(ii) V_{ki}, V_{kj}, $i \neq j$ are pairwise amicable, $k = 1,\dots,8$, *(iii)* $U_{ki} \pm V_{ki}$, $(+1,-1)$ *matrices*, $i,k = 1,\ldots,8$,

(iv) the row(column) sum of U_{ab} *is 1 for* $(a,b)\epsilon\{(i,i),(i,i+1),(i+1,i)\}$, $i = 1,3,5,7$, *the row(column) sum of* U_{aa} *is -1 for* $(a,a) = 2,4,6,8$ *and otherwise, and the row(column) sum of* U_{ij}, $i \neq j$ *is zero,*

(v) $\sum_{i=1}^{8} U_{ji}U_{ji}^T = 2(2n+1)I - 4J$, $\sum_{i=1}^{8} V_{ji}V_{ji}^T = 2(2n+1)I$, $j = 1,\ldots,8$,

(vi) $\sum_{i=1}^{8} U_{ji}U_{ki}^T = 0$, $\sum_{i=1}^{8} V_{ji}V_{ki}^T = 0$, $j \neq k$, $j,k = 1,\ldots,8$.

If (iii) to (vi) hold, there is a 64 block M-structure Hadamard matrix of order $8(2n+1)$.

Proof: Use

$$X_{11}=\begin{bmatrix} -1 & -e \\ -e^T & S_{11} \end{bmatrix},\ X_{12}=\begin{bmatrix} -1 & -e \\ -e^T & S_{12} \end{bmatrix},\ X_{13}=\begin{bmatrix} 1 & e \\ e^T & S_{13} \end{bmatrix},\ X_{14}=\begin{bmatrix} 1 & e \\ e^T & S_{14} \end{bmatrix},$$

$$X_{15}=\begin{bmatrix} 1 & e \\ e^T & S_{15} \end{bmatrix},\ X_{16}=\begin{bmatrix} 1 & e \\ e^T & S_{16} \end{bmatrix},\ X_{17}=\begin{bmatrix} -1 & e \\ e^T & S_{17} \end{bmatrix},\ X_{18}=\begin{bmatrix} -1 & e \\ e^T & S_{18} \end{bmatrix},$$

$$X_{21}=\begin{bmatrix} -1 & -e \\ -e^T & S_{21} \end{bmatrix},\ X_{22}=\begin{bmatrix} 1 & e \\ e^T & S_{22} \end{bmatrix},\ X_{23}=\begin{bmatrix} 1 & e \\ e^T & S_{23} \end{bmatrix},\ X_{24}=\begin{bmatrix} -1 & -e \\ -e^T & S_{24} \end{bmatrix},$$

$$X_{25}=\begin{bmatrix} 1 & e \\ e^T & S_{25} \end{bmatrix},\ X_{26}=\begin{bmatrix} -1 & -e \\ -e^T & S_{26} \end{bmatrix},\ X_{27}=\begin{bmatrix} -1 & e \\ e^T & S_{27} \end{bmatrix},\ X_{28}=\begin{bmatrix} 1 & -e \\ -e^T & S_{28} \end{bmatrix},$$

$$X_{31}=\begin{bmatrix} 1 & e \\ e^T & S_{31} \end{bmatrix},\ X_{32}=\begin{bmatrix} 1 & e \\ e^T & S_{32} \end{bmatrix},\ X_{33}=\begin{bmatrix} -1 & -e \\ -e^T & S_{33} \end{bmatrix},\ X_{34}=\begin{bmatrix} -1 & -e \\ -e^T & S_{34} \end{bmatrix},$$

$$X_{35}=\begin{bmatrix} 1 & e \\ e^T & S_{35} \end{bmatrix},\ X_{36}=\begin{bmatrix} 1 & e \\ e^T & S_{36} \end{bmatrix},\ X_{37}=\begin{bmatrix} -1 & e \\ e^T & S_{37} \end{bmatrix},\ X_{38}=\begin{bmatrix} -1 & e \\ e^T & S_{38} \end{bmatrix},$$

$$X_{41}=\begin{bmatrix} 1 & e \\ e^T & S_{41} \end{bmatrix},\ X_{42}=\begin{bmatrix} -1 & -e \\ -e^T & S_{42} \end{bmatrix},\ X_{43}=\begin{bmatrix} -1 & -e \\ -e^T & S_{43} \end{bmatrix},\ X_{44}=\begin{bmatrix} 1 & e \\ e^T & S_{44} \end{bmatrix},$$

$$X_{45}=\begin{bmatrix} 1 & e \\ e^T & S_{45} \end{bmatrix},\ X_{46}=\begin{bmatrix} -1 & -e \\ -e^T & S_{46} \end{bmatrix},\ X_{47}=\begin{bmatrix} -1 & e \\ e^T & S_{47} \end{bmatrix},\ X_{48}=\begin{bmatrix} 1 & -e \\ -e^T & S_{48} \end{bmatrix},$$

$$X_{51}=\begin{bmatrix} 1 & e \\ e^T & S_{51} \end{bmatrix},\ X_{52}=\begin{bmatrix} 1 & e \\ e^T & S_{52} \end{bmatrix},\ X_{53}=\begin{bmatrix} 1 & e \\ e^T & S_{53} \end{bmatrix},\ X_{54}=\begin{bmatrix} 1 & e \\ e^T & S_{54} \end{bmatrix},$$

$$X_{55}=\begin{bmatrix} -1 & -e \\ -e^T & S_{55} \end{bmatrix},\ X_{56}=\begin{bmatrix} -1 & -e \\ -e^T & S_{56} \end{bmatrix},\ X_{57}=\begin{bmatrix} -1 & e \\ e^T & S_{57} \end{bmatrix},\ X_{58}=\begin{bmatrix} -1 & e \\ e^T & S_{58} \end{bmatrix},$$

$$X_{61}=\begin{bmatrix} 1 & e \\ e^T & S_{61} \end{bmatrix},\ X_{62}=\begin{bmatrix} -1 & -e \\ -e^T & S_{62} \end{bmatrix},\ X_{63}=\begin{bmatrix} 1 & e \\ e^T & S_{63} \end{bmatrix},\ X_{64}=\begin{bmatrix} -1 & -e \\ -e^T & S_{64} \end{bmatrix},$$

$$X_{65}=\begin{bmatrix} -1 & -e \\ -e^T & S_{65} \end{bmatrix},\ X_{66}=\begin{bmatrix} 1 & e \\ e^T & S_{66} \end{bmatrix},\ X_{67}=\begin{bmatrix} -1 & e \\ e^T & S_{67} \end{bmatrix},\ X_{68}=\begin{bmatrix} 1 & -e \\ -e^T & S_{68} \end{bmatrix},$$

$$X_{71}=\begin{bmatrix} 1 & -e \\ -e^T & S_{71} \end{bmatrix},\ X_{72}=\begin{bmatrix} 1 & -e \\ -e^T & S_{72} \end{bmatrix},\ X_{73}=\begin{bmatrix} 1 & -e \\ -e^T & S_{73} \end{bmatrix},\ X_{74}=\begin{bmatrix} -1 & -e \\ -e^T & S_{74} \end{bmatrix},$$

$$X_{75}=\begin{bmatrix} 1 & -e \\ -e^T & S_{75} \end{bmatrix},\ X_{76}=\begin{bmatrix} 1 & -e \\ -e^T & S_{76} \end{bmatrix},\ X_{77}=\begin{bmatrix} 1 & e \\ e^T & S_{77} \end{bmatrix},\ X_{78}=\begin{bmatrix} 1 & e \\ e^T & S_{78} \end{bmatrix},$$

$$X_{81}=\begin{bmatrix} 1 & -e \\ -e^T & S_{81} \end{bmatrix},\ X_{82}=\begin{bmatrix} -1 & e \\ e^T & S_{82} \end{bmatrix},\ X_{83}=\begin{bmatrix} 1 & -e \\ -e^T & S_{83} \end{bmatrix},\ X_{84}=\begin{bmatrix} -1 & e \\ e^T & S_{84} \end{bmatrix},$$

$$X_{85}=\begin{bmatrix} 1 & -e \\ -e^T & S_{85} \end{bmatrix},\ X_{86}=\begin{bmatrix} -1 & e \\ e^T & S_{86} \end{bmatrix},\ X_{87}=\begin{bmatrix} 1 & e \\ e^T & S_{87} \end{bmatrix},\ X_{88}=\begin{bmatrix} -1 & -e \\ -e^T & S_{88} \end{bmatrix},$$

Then provided conditions (i) to (v) hold and $S_{7i}^T = S_{7i}$, $i = 1, \ldots, 8$ are symmetric, X_{7i}, $i = 1, \ldots, 8$ are symmetric 8-Williamson type matrices. Otherwise X_{7i}, $i = 1, \ldots, 8$ are 8-Williamson type matrices. This can be verified by straightforward checking. Hence there is an Hadamard matrix of block structure of order $8(2n+1)$.

If conditions (iii) to (vi) hold then straightforward verification shows the 64 block M-structure X_{ij} is an Hadamard matrix of order $8(2n+1)$. □

Corollary 30 *Let q be an odd prime power and suppose there exist Williamson-type matrices of order $\frac{1}{2}(q-1)$. Then there exists an M-structure Hadamard matrix of order $8q$.*

Remark 31 This corollary gives new Hadamard matrices of order $8q$ for $q =$ 179, 1087, 1283, 1327, 1619, 1907, 2099, 2459, 2579, 2647, ...

Corollary 32 *Let $q = 2m+1 \equiv 9 \pmod{16}$ be a prime power. Suppose there are Williamson-type matrices of order q. Then there is a M-structure Hadamard matrix of order $8(2q+1)$.*

The analogous Yamada-J. Wallis-Whiteman structure to Theorem 29 is:

$$\begin{array}{cccccccccccccccc}
-1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -e & -e & e & e & e & e & e & e \\
-1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -e & e & e & -e & e & -e & e & -e \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & e & e & -e & -e & e & e & e & e \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & e & -e & -e & e & e & -e & e & -e \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & e & e & e & e & -e & -e & e & e \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & e & -e & e & -e & -e & e & e & -e \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -e & -e & -e & -e & -e & -e & e & e \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -e & e & -e & -e & e & e & -e & e \\
-e^T & -e^T & e^T & e^T & e^T & e^T & e^T & e^T & S_{11} & S_{12} & S_{13} & S_{14} & S_{15} & S_{16} & S_{17} & S_{18} \\
-e^T & e^T & e^T & -e^T & e^T & -e^T & e^T & -e^T & S_{21} & S_{22} & S_{23} & S_{24} & S_{25} & S_{26} & S_{27} & S_{28} \\
e^T & e^T & -e^T & -e^T & e^T & e^T & e^T & e^T & S_{31} & S_{32} & S_{33} & S_{34} & S_{35} & S_{36} & S_{37} & S_{38} \\
e^T & -e^T & -e^T & e^T & e^T & -e^T & e^T & -e^T & S_{41} & S_{42} & S_{43} & S_{44} & S_{45} & S_{46} & S_{47} & S_{48} \\
e^T & e^T & e^T & e^T & -e^T & -e^T & e^T & e^T & S_{51} & S_{52} & S_{53} & S_{54} & S_{55} & S_{56} & S_{57} & S_{58} \\
e^T & -e^T & e^T & -e^T & -e^T & e^T & e^T & -e^T & S_{61} & S_{62} & S_{63} & S_{64} & S_{65} & S_{66} & S_{67} & S_{68} \\
-e^T & -e^T & -e^T & -e^T & -e^T & -e^T & e^T & e^T & S_{71} & S_{72} & S_{73} & S_{74} & S_{75} & S_{76} & S_{77} & S_{78} \\
-e^T & e^T & -e^T & e^T & -e^T & e^T & e^T & -e^T & S_{81} & S_{82} & S_{83} & S_{84} & S_{85} & S_{86} & S_{87} & S_{88}
\end{array}$$

We can see Yamada's matrix with trimming [46] or the J. Wallis-Whiteman [30] matrix with a border embodied in the construction.

References

[1] S.S. Agaian, *Hadamard Matrices and their Applications*, Lecture Notes in Mathematics, Vol 1168, Springer-Verlag, Berlin-Heidelberg-New York-Tokyo, 1985.

[2] S.S. Agayan and A.G. Sarukhanyan, Recurrence formulas for the construction of Williamson-type matrices, translated from *Matemacheskie Zametki*, **30**, (1981), 603–617 = *Math Notes*, **30**, (1982), 796–804.

[3] L.D. Baumert and M. Hall, Jr., Hadamard matrices of Williamson type, *Math. Comp.* **19**, (1965), 442–447.

[4] L.D. Baumert and M. Hall, Jr., A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.*, **71**, (1965), 169–170.

[5] Joan Cooper and Jennifer Wallis, A construction for Hadamard arrays, *Bull. Austral. Math. Soc.*, **7**, (1972), 269–278.

[6] Gavin Cohen, David Rubie, Christos Koukouvinos, Stratis Kounias, Jennifer Seberry and Mieko Yamada, A survey of base sequences, disjoint complementary sequences and OD($4t; t, t, t, t$), *JCMCC*, **5**, (1989), 69–104.

[7] P. Delsarte, J-M. Goethals and J.J. Seidel, Orthogonal matrices with zero diagonal, II, *Canad. J. Math.*, **23**, (1971), 816–832.

[8] A.V. Geramita and Jennifer Seberry, *Orthogonal Designs: Quadratic forms and Hadamard matrices*, Marcel Dekker, New York-Basel, 1979, viii, 460 pages.

[9] C. Koukouvinos and S. Kounias, Hadamard matrices of the Williamson type of order $4m$, $m = pq$. An exhaustive search for $m = 33$, *Discrete Math.*, **68**, (1988), 45–57.

[10] C. Koukouvinos and S. Kounias, There are no circulant symmetric Williamson matrices of order 39, (to appear).

[11] C. Koukouvinos, S. Kounias and Jennifer Seberry, Further results on base sequences, disjoint complementary sequences, OD($4t; t, t, t, t$) and the excess of Hadamard matrices, *Ars Combinatoria*, (to appear).

[12] Masahiko Miyamoto, A construction for Hadamard matrices, *J. Combinatorial Th.*, Ser. A, (to appear).

[13] Tamio Ono and Kazue Sawade, The Baumert-Hall-Welch array of order 36, in Japanese (translation by Mieko Yamada).

[14] R.E.A.C. Paley, On orthononal matrices, *J. Math. Phys.*, **12**, (1933), 311–320.

[15] Kazue Sawade, Hadamard matrices of order 100 and 108, *Bull. Nagoya Inst. Technol.*, **29**, (1977), 147–152.

[16] Jennifer Seberry, On skew Hadamard matrices, *Ars Combinatoria*, **6**, (1978), 255–276.

[17] Jennifer Seberry, A new construction for Williamson-type matrices, *Graphs and Combinatorics*, **2**, (1986), 81–87.

[18] Jennifer Seberry, Hadamard matrices of order $2^t \cdot pq$: *I*, *Ars Combinatoria*, **23B**, (1987), 195–213.

[19] Jennifer Seberry Wallis, Some matrices of Williamson-type, *Utilitas Math.*, **4**, (1973), 147–154.

[20] Jennifer Seberry Wallis, Williamson matrices of even order, *Combinatorial Mathematics, Proceedings of the Second Australian Conference*, editor D.A. Holton, Lecture Notes in Mathematics, Vol 403, Springer-Verlag, Berlin-Heidelberg-New York-Tokyo 1974, 132–142.

[21] Jennifer Seberry Wallis, Construction of Williamson type matrices, *Linear and Multilinear Algebra*, **3**, (1975), 197–207.

[22] Jennifer Seberry Wallis, Hadamard matrices, in W.D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, *Combinatorics: Room Squares, Sum-free Sets, Hadamard matrices*, Lecture Notes in Mathematics, Vol 292, Springer-Verlag, Berlin-Heidelberg-New York, 1972, 508 pages.

[23] E. Spence, An infinite family of Williamson matrices, *J. Austral. Math. Soc. Ser A*, **24**, (1977), 252–256.

[24] G. Szekeres, Tournaments and Hadamard matrices, *Enseignment Math.*, **15**, (1969), 269–278.

[25] G. Szekeres, Cyclotomy and complementary difference sets, *Acta. Arith.*, **18**, (1971), 349–353.

[26] Jennifer (Seberry) Wallis, A skew-Hadamard matrix of order 92, *Bull. Austral. Math. Soc.*, **5**, (1971), 203–204.

[27] Jennifer (Seberry) Wallis, Amicable Hadamard matrices, *J. Combinatorial Th., Ser. A.*, **11**, (1971), 296–298.

[28] Jennifer (Seberry) Wallis, A note on amicable Hadamard matrices, *Utilitas Math.*, **3**, (1973), 119–125.

[29] Jennifer (Seberry) Wallis, Some remarks on supplementary difference sets, *Colloq. Math. Soc. Janos Bolyai*, **10**, (1973), 1503–1526.

[30] Jennifer Wallis and Albert Leon Whiteman, Some classes of Hadamard matrices with constant diagonal, *Bull. Austral. Math. Soc.*, **7**, (1972), 233–249.

[31] Albert Leon Whiteman, An infinite family of skew-Hadamard matrices, *Pacific J. Math.*, **38**, (1971), 817–822.

[32] Albert Leon Whiteman, Skew-Hadamard matrices of Goethals-Seidel type, *Discrete Math.*, **2**, (1972), 397–405.

[33] Albert Leon Whiteman, An infinite family of Hadamard matrices of Williamson type, *J. Combinatorial Th., Ser. A.*, **14**, (1973), 334–340.

[34] Albert Leon Whiteman, Hadamard matrices of Williamson type, *J. Austral. Math. Soc.*, **21**, (1976), 481–486.

[35] Albert Leon Whiteman, Hadamard matrices of order $4(2p+1)$, *J. Number Theory*, **8**, (1976), 1–11.

[36] John Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.*, **11**, (1944), 65–81.

[37] K. Yamamoto, Hadamard matrices of Williamson type and the maximal-length shift register sequences, Abstract, *Symp. Combinatorics at Osaka City University*, December 1978 (in Japanese).

[38] K. Yamamoto, On a generalized Williamson equation, *Colloq. Math. Janos Bolyai*, **37**, (1981), 839–850.

[39] K. Yamamoto and Mieko Yamada, Williamson matrices of Turyn's type and Gauss sums, *J. Math. Soc. Japan*, **37**, (1985), 703–717.

[40] Mieko Yamada, On the Williamson type j matrices of orders 4.29, 4.41 and 4.37, *J. Combinatorial Th., Ser. A.*, **27**, (1979), 378–381.

[41] Mieko Yamada, On the Williamson matrices of Turyn's type and of type j, *Comment. Math. Univ. San Pauli*, **31**, (1982), 71–73.

[42] Mieko Yamada, Hadamard matrices generated by an adaption of the generalized quaternion type array, *Graphs and Combinatorics*, **2**, (1986), 179–187.

[43] Mieko Yamada, Supplementary relative difference sets and their application to Hadamard matrices, *Ars Combinatoria*, **26A**, (1989), 223–238.

[44] Mieko Yamada, Some new series of Hadamard matrices, *J. Austral. Math. Soc., Ser. A*, **46**, (1989), 371–383.

[45] Mieko Yamada, Supplementary difference sets and Jacobi sums, *Discrete Math.*, (to appear).

[46] Mieko Yamada, Hadamard matrices of generalized quaternion type, *Discrete Math.*, (to appear).

[47] Jennifer Seberry and Mieko Yamada, On the Products of Hadamard Matrices, Williamson Matrices and Other Orthogonal Matrices using M-Structures, *JCMCC*, (to appear).

[48] L.D. Baumert, Hadamard matrices of orders 116 and 232, *Bull. Amer. Math. Soc.*, **72**, (1966), 237.

[49] L.D. Baumert, S.W. Golomb, M. Hall, Jr., Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.*, **68**, (1962), pp. 237–238.

[50] Jennifer Seberry Wallis, On Hadamard matrices, *J. Combinatorial Theory, Ser. A*, **18**, (1975), pp. 149–164.

[51] R.J. Turyn, An infinite class of Williamson matrices, *J. Combinatorial Theory, Ser. A*, **12**, (1972), pp. 319–321.

[52] R.J. Turyn, A special class of Williamson matrices and difference sets, *J. Combinatorial Th(A)*, **36**, (1984), pp. 111–115.

* Department of Computer Science
University College
University of New South Wales
ADFA
Canberra, 2600
AUSTRALIA

† Department of Mathematics
Tokyo Woman's Christian University
Zempukuji
Suginami-Ku
Tokyo, 167
JAPAN

Index of Williamson Matrices

This table contains odd integers $q < 40000$ for which Williamson matrices exist. The following legend gives the method of construction used

Key	Method	Explanation
w1	$\{1, \ldots, 33, 37, 41, 43\}$	
w2	$\frac{p+1}{2}$	$p \equiv 1 (mod 4)$ a prime power
w3	9^d	d a natural number
w4	$\frac{p(p+1)}{2}$	$p \equiv 1 (mod 4)$ a prime power
w5	$s(4s+3), s(4s-1)$	$s \in \{1, 3, 5, \ldots, 31\}$
w6	93	
w7	$\frac{(f-1)(4f+1)}{4}$	$p = 4f+1, f$ odd, is a prime power of the form $1+4t^2$, $\frac{f-1}{8}$ is the order of a good matrix
w8	$\frac{(f+1)(4f+1)}{4}$	$p = 4f+1, f$ odd, is a prime power of the form $25+4t^2$, $\frac{f+1}{8}$ is the order of a good matrix
w9	$\frac{p(p-1)}{2}$	$p = 4f+1$ is a prime power and $\frac{p-1}{4}$ is the order of a good matrix
w0	$(p+2)(p+1)$	$p \equiv 1 (mod 4)$ a prime power, $p+3$ is the order of a symmetric Hadamard matrix
wa	$\frac{(f+1)(4f+1)}{2}$	$p = 4f+1, f$ odd, is a prime power of the form $9+4t^2$, $\frac{f-1}{2} \equiv 1 (mod 4)$ a prime power
wb	$\frac{(f-1)(4f+1)}{2}$	$p = 4f+1, f$ odd, is a prime power of the form $49+4t^2$, $\frac{f-3}{2} \equiv 1 (mod 4)$ a prime power
wc	$2p+1$	$q = 2p-1$ is a prime power p is a prime
wd	7.3^i	$i \geq 0$
w#e	$7^{i+1}, 11.7^i$	$i \geq 0$ (Gives 8-Williamson matrices)
wf	$\frac{q^d(q+1)}{2}$	$q \equiv 1 (mod 4)$ is a prime $d \geq 2$
wg	$\frac{p^2(p+1)}{2}$	$p \equiv 1 (mod 4)$ is a prime power
wh	$\frac{p^2(p+1)}{4}$	$p \equiv 3 (mod 4)$ is a prime power and $\frac{p+1}{4}$ is the order of a Williamson type matrix
wi	$q+2$	$q \equiv 1 (mod 4)$, is a prime power and $\frac{q+1}{2}$ is a prime power
wj	$q+2$	$q \equiv 1 (mod 4)$, is a prime power and $\frac{q+3}{2}$ is the order of a symmetric conference matrix

Key	Method	Explanation
wk	q	$q \equiv 1(mod4)$ is a prime power and $\frac{q-1}{2}$ is the order of a symmetric conference matrix or the order of a symmetric hadamard matrix
wl	q	$q \equiv 1(mod4)$, is a prime power and $\frac{q-1}{4}$ is the order of a williamson type matrix
wm	q	$q \equiv 1(mod4)$, is a prime power and $\frac{q-1}{2}$ is the order of a hadamard matrix
wn	wn	w is the order of a williamson type matrix n is the order of a symmetric conference matrix
wo	$2wu$	w and u are the orders of williamson type matrices
w#p	$2q+1$	$q+1$ is the order of an amicable hadamard matrix and q is the order of a willliamson type matrix
w#q	q	q is a prime power and $\frac{q-1}{2} isthe$ order of a williamson type matrix
w#r	$2q+1$	$q \equiv 1(mod4)$ is a prime power or $q+1$ is the order of a symmetric conference matrix and q is the order of a williamson type matrix
w#s	2.9^t+1	$t > 0$

$S = \{1, \ldots, 31\}$ is the set of good matrices.

$q-1$ is a Hadamard matrix of SC-form if one of the following is true
(i) $\frac{q-1}{4}$ is a Williamson matrix.
(ii) $\frac{q-1}{2}$ is a Conference matrix.
(iii) $\frac{q-1}{4}$ is a Hadamard matrix. Note: The fact that if there is a

Williamson matrix of order n then there is a Williamson matrix of order $2n$, is used in the calculation of wg.

[The references for these papers are w1 [48], [4], [49], [40], [22], w2 [51], [33], w3 [52], w4 [19], w5, w6 [21], w7, w8, w9, w0, we, wl [20], wf, wg [17], wh, wi, wj, wk [12]]

q	t	Method	q	t	Method	q	t	Method	q	t	Method	q	t	Method
1	0	w1	101	0	wk	201	0	w2	301	0	w2	401	0	wk
3	0	w1	103	0	w#q	203	1	w9	303	1	w7	403	1	wn
5	0	w1	105	1	wn	205	0	w2	305	1	wn	405	0	w2
7	0	w1	107	0	w#q	207	1	wn	307	0	w2	407	1	wn
9	0	w1	109	0	wk	209	1	wn	309	0	w2	409	0	wk
11	0	w1	111	1	wn	211	0	w2	311			411	0	w2
13	0	w1	113	0	wk	213			313	0	w2	413		
15	0	w1	115	0	w2	215	1	wn	315	0	w5	415	0	w2
17	0	w1	117	0	w2	217	0	w2	317	0	wk	417	1	wn
19	0	w1	119	1	wn	219	1	wn	319	1	wo	419		
21	0	w1	121	0	w2	221	1	wn	321	0	w2	421	0	w2
23	0	w1	123	0	wi	223			323	1	wn	423	0	wi
25	0	w1	125	0	wk	225	0	w2	325	0	w4	425	1	wn
27	0	w1	127	0	w#p	227	0	w#q	327	0	w2	427	0	w2
29	0	w1	129	0	w2	229	0	w2	329			429	0	w2
31	0	w1	131			231	0	w2	331	0	w2	431		
33	0	w1	133	1	wn	233	0	wl	333	1	w9	433	0	wk
35	1	wn	135	0	w2	235			335			435	0	w4
37	0	w1	137	0	wl	237	1	wn	337	0	w2	437	1	wn
39	0	wi	139	0	w2	239			339	0	w2	439	0	w2
41	0	w1	141	0	w2	241	0	wk	341	1	wn	441	0	w2
43	0	w1	143	1	wn	243	0	wj	343	1	wn	443		
45	0	w2	145	0	w2	245	1	wn	345	1	wn	445	1	wn
47	0	w#p	147	0	w2	247	1	wn	347	0	w#q	447	1	wn
49	0	w2	149	0	wk	249	1	wn	349	0	wk	449	0	wk
51	0	w2	151	0	w#q	251	0	w#q	351	0	w2	451	0	wj
53	0	wk	153	0	w4	253	1	wn	353	0	wl	453		
55	0	w2	155	1	wn	255	0	w2	355	0	w2	455	1	wn
57	0	w2	157	0	w2	257	0	wl	357	1	wn	457	0	wk
59	0	w#q	159	0	w2	259	1	wn	359			459	0	wi
61	0	w1	161	1	wn	261	0	w2	361	0	wk	461	0	wk
63	0	w2	163	0	w#q	263			363	0	wi	463	0	w#q
65	1	wn	165	1	wn	265	0	w2	365	0	w2	465	0	w2
67	0	w#q	167	0	w#p	267	1	wn	367	0	w2	467	0	w#q
69	0	w2	169	0	w2	269			369	1	wn	469	0	w2
71			171	1	wn	271	0	w2	371	1	wn	471	0	w2
73	0	wk	173	0	wl	273	1	wn	373	0	wl	473	0	w5
75	0	w2	175	0	w2	275	1	wn	375	0	wf	475	1	wn
77	1	wn	177	0	w2	277	0	wk	377	1	wn	477	0	w2
79	0	w2	179	0	w#q	279	0	w2	379	0	w2	479		
81	0	w3	181	0	w2	281	0	wl	381	0	w2	481	0	w2
83	0	wi	183	1	wn	283	0	w#q	383			483	1	wn
85	0	w2	185	1	wn	285	0	w2	385	0	w2	485	1	wn
87	0	w2	187	0	w2	287	1	wn	387	0	w2	487	0	w#p
89	0	wl	189	0	w5	289	0	w2	389	0	wk	489	0	w2
91	0	w2	191	0	w#p	291	1	wn	391	1	wn	491		
93	0	w6	193	0	wk	293	0	wl	393			493	1	wo
95	0	w5	195	0	w2	295			395	1	wn	495	1	wn
97	0	w2	197	0	wk	297	0	w2	397	0	wk	497		
99	0	w2	199	0	w2	299	1	wn	399	0	w2	499	0	w2

Existence of Williamson Matrices

q	t	Method	q	t	Method	q	t	Method	q	t	Method	q	t	Method
501			601	0	w2	701	0	wk	801	0	w2	901	0	w2
503			603	1	wn	703	0	w4	803	1	wo	903	1	wn
505	0	w2	605	1	wn	705	0	w2	805	0	w2	905	1	wn
507	0	w2	607	0	w2	707	1	wn	807	0	w2	907		
509			609	0	w2	709	0	wk	809	0	wl	909	1	wn
511	0	w2	611			711	1	wn	811	0	w2	911		
513	1	wn	613	0	wl	713	1	wn	813	1	wn	913	1	wo
515	0	w#r	615	0	w2	715	0	w2	815			915	1	w9
517	0	w2	617	0	wl	717	0	w2	817	1	wn	917		
519	1	wn	619	0	w2	719			819	0	w2	919	0	w#q
521	0	wl	621	1	wn	721			821	0	wk	921	1	wn
523	0	w#q	623	1	wn	723	1	wn	823	0	w#q	923	0	w#r
525	0	w2	625	0	w2	725	1	wn	825	1	wn	925	0	w2
527	1	wn	627	0	wi	727	0	w2	827			927	1	wn
529	0	wl	629	1	wn	729	0	w3	829	0	w2	929	0	wl
531	0	w2	631	0	w#q	731	1	wo	831	1	wn	931	0	w2
533	1	wn	633	1	wn	733	0	w#q	833	1	wn	933		
535	0	w2	635	0	w#r	735	0	wi	835	0	w2	935	1	wn
537			637	1	wn	737			837	1	wn	937	0	w2
539	1	wn	639	0	w2	739			839			939	0	w2
541	0	wk	641	0	wk	741	0	w2	841	0	w2	941		
543	0	wi	643	0	w#q	743			843	0	wi	943	1	wn
545	1	wn	645	0	w2	745	0	w2	845	1	wn	945	0	w2
547	0	w2	647			747	0	w2	847	0	w2	947	0	w#q
549	0	w2	649	0	w2	749			849	0	w2	949	1	wn
551	1	wn	651	0	w2	751	0	w#q	851	1	wn	951	0	w2
553	1	wn	653			753			853			953	0	wl
555	0	w2	655	0	w#p	755			855	0	w2	955		
557	0	wk	657	1	wn	757	0	wl	857			957	0	w2
559	0	w2	659			759	0	wi	859	0	w#q	959	1	wn
561	1	wn	661	0	w2	761	0	wl	861	0	w2	961	0	wk
563	0	w#q	663	0	w5	763	1	wa	863			963	1	wn
565	0	w2	665	1	wn	765	1	wn	865	1	wn	965	1	wn
567	1	wn	667	1	wn	767			867	0	w2	967	0	w2
569	0	wm	669			769	0	wk	869	1	wn	969	1	wn
571	0	w#q	671	1	wn	771	1	wn	871	0	w2	971		
573			673	0	wk	773	0	wl	873	1	wn	973	1	wn
575	1	wn	675	0	wi	775	0	w2	875	1	wn	975	0	w2
577	0	w2	677	0	wk	777	0	w2	877	0	w2	977	0	wk
579	0	wj	679	1	wn	779	1	wn	879	0	wi	979	1	wo
581	1	wn	681	0	w2	781			881	0	wk	981	1	wn
583	1	wo	683			783	1	wn	883	0	w#q	983		
585	1	wn	685	0	w2	785	1	wn	885	0	w5	985	1	wn
587	0	w#q	687	0	w2	787			887			987	0	w2
589	1	wn	689	1	w9	789			889	0	w2	989	1	wn
591	0	w2	691	0	w2	791	1	wn	891	1	wn	991		
593	0	wk	693	1	wn	793	1	wn	893			993	1	wn
595	1	wn	695	1	wn	795	1	wn	895	0	w2	995	1	wn
597	0	w2	697	1	wn	797	0	wk	897	1	wn	997	0	w2
599			699	1	wn	799	0	w2	899	1	wn	999	0	w2

Existence of Williamson Matrices

q	t	Method	q	t	Method	q	t	Method	q	t	Method	q	t	Method
1001	1	wn	1101	1	wn	1201	0	w2	1301	0	wl	1401	0	w2
1003			1103			1203	0	wi	1303	0	w#q	1403	1	wn
1005	1	wn	1105	0	w2	1205	1	wn	1305	0	w2	1405	0	w2
1007	1	wn	1107	0	w2	1207	0	w5	1307	0	w#r	1407	1	wn
1009	0	w2	1109	0	wl	1209	0	w2	1309	0	w2	1409	0	wl
1011	1	wn	1111	0	w2	1211	1	wn	1311	0	w2	1411	1	wo
1013	1	wn	1113	1	wn	1213	0	w#q	1313	1	wn	1413	1	wn
1015	0	w2	1115	0	w#r	1215	0	wi	1315			1415		
1017	1	wn	1117	0	wk	1217	0	wk	1317	0	w2	1417	0	w2
1019	0	w#r	1119	0	w2	1219	0	w2	1319			1419	0	w2
1021	0	wk	1121			1221	0	w2	1321	0	wl	1421	1	wn
1023	1	wn	1123			1223			1323	0	wi	1423		
1025	1	wn	1125	1	wn	1225	0	w4	1325	1	wn	1425	0	w5
1027	0	w2	1127	1	wn	1227	1	wn	1327	0	w#p	1427		
1029	1	wn	1129	0	wk	1229	0	wk	1329	0	w2	1429	0	w2
1031			1131	1	wn	1231	0	w#p	1331	1	wn	1431	0	w2
1033	0	wk	1133			1233	1	wn	1333	1	wn	1433		
1035	0	w2	1135	0	w2	1235	1	wn	1335	1	wn	1435	1	wn
1037	1	wn	1137	0	w2	1237	0	w2	1337			1437		
1039			1139	0	w5	1239	0	w2	1339	0	w2	1439		
1041	0	w2	1141	0	w2	1241	1	wo	1341	1	wb	1441		
1043	1	wn	1143	1	wn	1243	1	wn	1343	1	wn	1443	1	wn
1045	0	w2	1145	1	wn	1245	1	wn	1345	0	w2	1445	1	wn
1047	1	wn	1147	0	w2	1247	1	wo	1347	0	w2	1447		
1049	0	wm	1149	0	w2	1249	0	wl	1349			1449	0	w2
1051	0	w#q	1151			1251	0	wi	1351	1	wn	1451		
1053	1	wn	1153	0	wk	1253			1353	1	wn	1453	0	wl
1055	1	wn	1155	0	w2	1255			1355	1	wn	1455	0	w2
1057	0	w2	1157	1	wn	1257			1357	0	w2	1457		
1059	1	wn	1159	1	wn	1259			1359			1459	0	w2
1061	0	wk	1161	1	wn	1261	0	w2	1361	0	wk	1461		
1063	0	w#q	1163			1263	1	wn	1363			1463	2	wn
1065	0	w2	1165	1	wn	1265	1	wn	1365	0	w2	1465	1	wn
1067	1	wn	1167	0	w2	1267	1	wn	1367			1467	1	wn
1069	0	w2	1169			1269	1	wn	1369	0	wl	1469	1	wn
1071	0	w2	1171	0	w2	1271	1	wn	1371	0	w2	1471	0	w#p
1073	1	wn	1173	1	wn	1273			1373	0	w#q	1473		
1075	1	wn	1175			1275	0	w2	1375	0	w2	1475		
1077	0	w2	1177			1277	0	w#q	1377	0	w2	1477	0	w2
1079	1	wn	1179	0	w2	1279	0	w2	1379	1	wn	1479	0	w2
1081	0	w2	1181			1281	1	wn	1381	0	w#q	1481	0	wl
1083	1	wn	1183	0	wf	1283	0	w#q	1383	0	wi	1483	0	w#q
1085	1	wn	1185	1	wn	1285	1	wn	1385	1	wn	1485	0	w2
1087	0	w#p	1187	0	w#q	1287	1	wn	1387	1	wn	1487		
1089	1	wn	1189	0	w2	1289	0	wl	1389	0	w2	1489	0	wl
1091			1191	0	w2	1291	0	w#q	1391			1491		
1093	0	w#q	1193	0	wl	1293			1393	1	wn	1493	0	wl
1095	0	wi	1195	0	w2	1295	2	wn	1395	0	w2	1495	1	wn
1097	0	wl	1197	0	w2	1297	0	w2	1397			1497	1	wn
1099	0	w2	1199	1	wo	1299	1	wn	1399	0	w2	1499		

Existence of Williamson Matrices

q	t	Method	q	t	Method	q	t	Method	q	t	Method	q	t	Method
1501	0	w2	1601	0	wk	1701	1	wn	1801	0	wk	1901	0	w#q
1503			1603	1	wn	1703			1803	1	wn	1903	1	wo
1505	1	wn	1605	0	w2	1705	1	wn	1805	0	wh	1905	1	wn
1507	1	wo	1607			1707	0	w2	1807	0	w2	1907	0	w#q
1509			1609	0	w2	1709	0	wk	1809	0	w2	1909	1	wn
1511			1611	0	w2	1711			1811			1911	0	w2
1513	1	wn	1613	0	w#q	1713			1813	1	wn	1913		
1515	1	wn	1615	0	w2	1715	0	w#r	1815	1	wn	1915		
1517	1	wn	1617	1	wn	1717	0	w2	1817	1	wn	1917	0	w2
1519	0	w2	1619	0	w#q	1719			1819	0	w2	1919	1	wn
1521	0	w2	1621	0	wk	1721	0	wl	1821	1	wn	1921	1	wn
1523	0	w#q	1623	0	wi	1723	0	w#q	1823	1	wn	1923	1	wn
1525	0	w2	1625	1	wn	1725	0	w2	1825	1	wn	1925	1	wn
1527			1627	0	w2	1727	1	wn	1827	0	w5	1927	0	w2
1529	1	wn	1629	0	w2	1729	0	w2	1829			1929		
1531	0	w2	1631	1	wn	1731	0	w2	1831			1931		
1533	1	wn	1633			1733	0	wl	1833	1	wn	1933	0	w#q
1535	1	wn	1635	1	wn	1735	0	w2	1835	1	wn	1935	0	wi
1537	1	wo	1637	0	wl	1737	1	wn	1837	0	w2	1937	1	wn
1539	1	wn	1639	1	wo	1739			1839	0	w2	1939	0	w2
1541			1641	1	wn	1741	0	w2	1841			1941	0	w2
1543			1643	1	wn	1743	0	w5	1843	1	wn	1943		
1545	0	w2	1645			1745	1	wn	1845	1	wn	1945	0	w2
1547	1	wn	1647	1	wn	1747			1847			1947	1	wn
1549	0	wk	1649	1	wn	1749	1	wn	1849	0	w2	1949		
1551	1	wn	1651	0	w2	1751			1851	0	w2	1951	0	w#p
1553	0	wk	1653	1	wn	1753	0	wl	1853	1	wo	1953	1	wn
1555	0	w2	1655	1	wn	1755	0	wi	1855	0	w2	1955	1	wn
1557	1	wn	1657	0	w2	1757			1857	1	wn	1957		
1559			1659	0	wi	1759	0	w2	1859	1	wn	1959	0	w2
1561	0	w2	1661			1761			1861	0	w2	1961	1	wn
1563	0	w2	1663			1763	1	wn	1863	1	wn	1963		
1565	1	wn	1665	0	w2	1765	0	w2	1865	1	wn	1965	0	w2
1567			1667			1767	0	w2	1867	0	w2	1967	1	wn
1569	0	w2	1669	0	w#q	1769	1	wn	1869	1	wn	1969		
1571			1671	1	wn	1771	0	w2	1871			1971	1	wn
1573	1	wn	1673			1773	1	wn	1873	0	wk	1973	0	w#q
1575	1	wn	1675			1775	1	wn	1875	0	wf	1975	1	wn
1577	1	wn	1677	1	wn	1777	0	wl	1877	0	wk	1977		
1579			1679	1	wn	1779	0	w2	1879	0	w#q	1979		
1581	1	wn	1681	0	w2	1781	1	wn	1881	0	w2	1981		
1583			1683	0	wj	1783			1883	0	w#r	1983	1	wn
1585	0	w2	1685	1	wn	1785	1	wn	1885	0	w2	1985	1	wn
1587	1	wh	1687	0	w2	1787			1887	1	wn	1987		
1589			1689			1789	0	w#q	1889	0	wm	1989	1	wn
1591	0	w2	1691	1	wn	1791	0	w2	1891	0	w4	1991	1	wn
1593	1	wn	1693	0	wl	1793			1893			1993	0	wl
1595	1	wn	1695	0	w2	1795			1895	1	wn	1995	0	w2
1597	0	wk	1697	0	wl	1797	0	w2	1897	0	w2	1997	0	wk
1599	1	wn	1699	0	w#q	1799	1	wn	1899	0	w2	1999	0	w#p

Existence of Williamson Matrices

Index of Hadamard Matrices

This table contains odd integers $q < 40000$ for which Hadamard matrices of the form $2^t q$ exist. The key for the methods of construction follows.

Amicable Hadamard Matrices.

Key	Method	Explanation
a1	$p^r + 1$	$p^r \equiv 3(mod4)$, is a prime power
a2	$2(q+1)$	$2q+1$ is a prime power, $q \equiv 1(mod4)$, is a prime
a5	nh	n, h, are amicable hadamard matrices

Skew Hadamard Matrices.

Key	Method	Explanation
s1	$2^t \prod k_i$	t all positive integers, $k_i - 1 \equiv 3(mod4)$ a prime power
s2	$(p-1)^u + 1$	p is a skew Hadamard matrix, $u > 0$ is an odd integer
s3	$2(q+1)$	$q \equiv 5(mod8)$ is a prime power
s4	$2(q+1)$	$q = p^t$ is a prime power where $p \equiv 5(mod8)$ and $t \equiv 2(mod4)\cdot$
s5	$4m$	$3 \leq m \leq 25$
s6	$4(q+1)$	$q \equiv 9(mod16)$ is a prime power
s7	$(\lvert t \rvert + 1)(q+1)$	$q = s^2 + 4t^2 \equiv 5(mod8)$ is a prime power and $\lvert t \rvert + 1$ is a skew Hadamard matrix
s8	$4(q^2+q+1)$	q is a prime power, $q^2+q+1 \equiv 3,5,7(mod8)$ a prime or $2(q^2+q+1)+1$ is a prime power
s0	hm	h is a skew hadamard matrix and m is an amicable hadamard matrix

Spence Hadamard Matrices.

Key	Method	Explanation
p1	$4(q^2+q+1)$	$q^2+q+1 \equiv 1(mod8)$ is a prime
p2	$4n$ or $8n$	$n, n-2$ are prime powers, if $n \equiv 1(mod4)$ there exists a Hadamard matrix of order $4n$, if $n \equiv 3(mod4)$ there exists a Hadamard matrix of order $8n$
p3	$4m$	m is an odd prime power for which an integer $s \geq 0$ such that $\frac{(m-(2^{s+1}+1))}{2^{s+1}}$ is an odd prime power, exists

Symmetric Hadamard Matrices.

If there exists a Conference matrix of order n then there is symmetric Hadamard matrix of order $2n$, for this reason symmetric hadamard matrices indexed according to the method used to derive the order of a conference matrix with the exception of c6 wich produces a symmetric Hadamard matrix.

Key	Method	Explanation
c1	p^r+1	$p^r \equiv 1(mod4)$ is a prime power
c2	$(h-1)^2+1$	h is a skew Hadamard matrix
c3	$q^2(q-2)+1$	$q \equiv 3(mod4)$ is a prime power
		$q-2$ is a prime power
c4	$5.9^{2t+1}+1$	$t \geq 0$
c5	$(n-1)^s+1$	n is a conference matrix
		$s \geq 2$
c6	nh	n is a conference matrix
		h is a Hadamard matrix

Note: a conference matrix of order n exists only if $n-1$ is the sum of two squares.

Hadamard Matrices Obtained From Williamson Matrices.

If a Williamson matrix of order 2^tq exists then there is a Hadamard matrix of order $2^{t+2}q$, the same key as in the Index of Williamson Matrices is used to index the Hadamard matrices produced from them.

OD Hadamard Matrices.

Key	Method	Explanation
o1		If a T-matrix of order 2^tq exists then there is a hadamard matrix of order $2^{t+2}q$
o2	ow	o is an OD-hadamard matrix and w is a Williamson matrix

Yamada Hadamard Matrices.

Key	Method	Explanation
y1	$4q$	$q \equiv 1(mod8)$ is a prime power
		$\frac{q-1}{2}$ is a Hadamard matrix
y2	$4(q+2)$	$q \equiv 5(mod8)$ is a prime power
		$\frac{q+3}{2}$ is a skew Hadamard matrix
y3	$4(q+2)$	$q \equiv 1(mod8)$ is a prime power
		$\frac{q+3}{2}$ is a conference matrix

Miyamoto Hadamard Matrices.

Key	Method	Explanation
m1	$4q$	$q \equiv 1(mod4)$ is a prime power
		$q-1$ is a Hadamard matrix
m2	$8q$	$q \equiv 3(mod4)$ is a prime power
		$2q-3$ is a prime power

Seberry.

Key	Method	Explanation
se	$2^t q$	where t is the smallest integer such that
		for given odd q, $a(q+1)+b(q-3)=2^t$
		has a solution for a, b non-negative integers

q	t	Method	q	t	Method	q	t	Method	q	t	Method	q	t	Method
1		a2	101		wk	201		o2	301		o2	401		wk
3		a2	103		y2	203		a2	303		o2	403		o2
5		a2	105		a2	205		o2	305		o2	405		a2
7		a2	107	3	w#q	207		a2	307		s3	407		a2
9		o2	109		wk	209		o2	309		c1	409		wk
11		a2	111		a2	211		s3	311	3	m2	411		o2
13		s4	113		c2	213	3	c6	313		c1	413		o2
15		a2	115		o2	215		a2	315		a2	415		o2
17		a2	117		a2	217		o2	317		wk	417		a2
19		s3	119		o2	219		o2	319		o2	419	4	a2
21		a2	121		o2	221		a2	321		a2	421		s4
23		s5	123		a2	223	3	a2	323		a2	423		o2
25		o2	125		a2	225		o2	325		o2	425		a2
27		a2	127		y2	227		a2	327		a2	427		o2
29		wl	129		o2	229		c1	329		o2	429		o2
31		s3	131		a2	231		o2	331		s3	431		a2
33		a2	133		o2	233		wl	333		a2	433		wk
35		a2	135		o2	235		o2	335		o2	435		o2
37		c1	137		a2	237		a2	337		c1	437		a2
39		o2	139		s3	239	4	a2	339		o2	439		s3
41		a2	141		a2	241		wk	341		o2	441		o2
43		wl	143		a2	243		a2	343		o2	443	3	m2
45		a2	145		o2	245		o2	345		o2	445		o2
47		o1	147		a2	247		o2	347	3	w#q	447		a2
49		o2	149		wk	249		o2	349		wk	449		wk
51		o2	151		y2	251	3	w#q	351		o2	451		o2
53		a2	153		o2	253		o2	353		wl	453		a2
55		o2	155		a2	255		a2	355		s3	455		o2
57		a2	157		c1	257		wl	357		a2	457		wk
59		o1	159		o2	259		o2	359	4	a2	459		o2
61		a2	161		a2	261		o2	361		o2	461		wk
63		a2	163	3	a2	263		a2	363		a2	463	3	w#q
65		o2	165		a2	265		o2	365		a2	465		o2
67		o1	167	3	w#p	267		o2	367		s3	467		a2
69		o2	169		o2	269		m1	369		o2	469		o2
71		a2	171		a2	271		s3	371		a2	471		o2
73		wk	173		a2	273		a2	373		wl	473		o2
75		o2	175		o2	275		o2	375		a2	475		o2
77		a2	177		o2	277		wk	377		o2	477		a2
79		s3	179	3	w#q	279		o2	379		s3	479	16	se
81		o2	181		c1	281		a2	381		a2	481		o2
83		a2	183		o2	283	3	w#q	383		a2	483		a2
85		o2	185		a2	285		o2	385		o2	485		o2
87		a2	187		o2	287		o2	387		o2	487	3	w#p
89		wl	189		o2	289		o2	389		wk	489		c1
91		o2	191	3	w#p	291		a2	391		o2	491	15	se
93		o2	193		wk	293		a2	393		a2	493		o2
95		a2	195		o2	295		o2	395		a2	495		a2
97		c1	197		a2	297		a2	397		wk	497		a2
99		o2	199		s3	299		o2	399		o2	499		s3

Existence of Hadamard Matrices

q	t	Method	q	t	Method	q	t	Method	q	t	Method	q	t	Method
501		a2	601		c1	701		a2	801		a2	901		o2
503		a2	603		a2	703		o2	803		o2	903		o2
505		o2	605		o2	705		a2	805		o2	905		o2
507		a2	607		s3	707		o2	807		s3	907	3	m2
509		m1	609		o2	709		wk	809		wl	909		o2
511		o2	611		o2	711		a2	811		s3	911		a2
513		o2	613		c2	713		a2	813		a2	913		o2
515	3	w#r	615		a2	715		o2	815		a2	915		a2
517		o2	617		a2	717		c1	817		o2	917	4	a5
519		o2	619		s3	719	4	a2	819		o2	919	3	a2
521		a2	621		o2	721	4	o2	821		wk	921		o2
523	3	w#q	623		o2	723		o2	823	3	s7	923		a2
525		a2	625		o2	725		o2	825		a2	925		o2
527		o2	627		o2	727		s3	827		a2	927		o2
529		o2	629		o2	729		o2	829		c1	929		wl
531		o2	631	3	w#q	731		o2	831		a2	931		o2
533		a2	633		a2	733		m1	833		a2	933	4	c6
535		s3	635		a2	735		a2	835		s3	935		a2
537	4	c6	637		o2	737		o2	837		a2	937		c1
539		o2	639		s3	739	16	se	839	18	se	939		o2
541		wk	641		wk	741		a2	841		o2	941		m1
543		o2	643	3	w#q	743		a2	843		a2	943		o2
545		a2	645		a2	745		o2	845		o2	945		a2
547		a2	647	3	m2	747		o2	847		o2	947	3	w#q
549		o2	649		o2	749	5	o2	849		c1	949		o2
551		a2	651		o2	751	3	a2	851		o2	951		a2
553		o2	653	4	o1	753		a2	853	3	a2	953		wl
555		o2	655		y2	755		a2	855		o2	955	3	a2
557		wk	657		o2	757		s8	857		m1	957		o2
559		o2	659	17	se	759		o2	859	3	a2	959		o2
561		a2	661		c1	761		c2	861		o2	961		o2
563		a2	663		o2	763		o2	863	3	m2	963		a2
565		o2	665		a2	765		o2	865		o2	965		o2
567		a2	667		o2	767		a2	867		a2	967		s3
569		p3	669	3	a2	769		wk	869		o2	969		o2
571	3	a2	671		a2	771		a2	871		o2	971	6	a2
573	3	a2	673		wk	773		wl	873		a2	973		o2
575		o2	675		a2	775		o2	875		a2	975		o2
577		c1	677		a2	777		o2	877		c1	977		a2
579		o2	679		o2	779		o2	879		o2	979		o2
581		o2	681		c1	781	3	a2	881		wk	981		a2
583		o2	683		a2	783		o2	883	3	w#q	983		a2
585		a2	685		o2	785		o2	885		a2	985		o2
587		a2	687		o2	787	3	m2	887		a2	987		a2
589		o2	689		o2	789	3	a2	889		c1	989		o2
591		o2	691		s3	791		a2	891		o2	991	3	a2
593		a2	693		o2	793		o2	893		a2	993		o2
595		o2	695		o2	795		o2	895		s3	995		o2
597		o2	697		o2	797		a2	897		o2	997		c1
599	17	se	699		o2	799		o2	899		o2	999		o2

Existence of Hadamard Matrices

q	t	Method	q	t	Method	q	t	Method	q	t	Method	q	t	Method
1001		a2	1101		o2	1201		c1	1301		c2	1401		c1
1003		o2	1103	3	m2	1203		o2	1303	3	w#q	1403		o2
1005		a2	1105		o2	1205		o2	1305		o2	1405		o2
1007		a2	1107		o2	1207		w5	1307		a2	1407		o2
1009		c1	1109		wl	1209		o2	1309		o2	1409		wl
1011		o2	1111		o2	1211		o2	1311		o2	1411		o2
1013		a2	1113		a2	1213		m1	1313		o2	1413		a2
1015		o2	1115	3	w#r	1215		o2	1315	4	a5	1415		a2
1017		o2	1117		wk	1217		wk	1317		o2	1417		o2
1019	3	w#r	1119		o2	1219		o2	1319	18	se	1419		o2
1021		wk	1121		a2	1221		o2	1321		wl	1421		a2
1023		a2	1123	3	m2	1223	19	se	1323		o2	1423	3	a2
1025		a2	1125		o2	1225		o2	1325		o2	1425		o2
1027		o2	1127		a2	1227		o2	1327	3	w#p	1427	3	m2
1029		o2	1129		wk	1229		wk	1329		c1	1429		c1
1031	6	a2	1131		a2	1231		y2	1331		a2	1431		o2
1033		wk	1133	4	a2	1233		a2	1333		o2	1433		m1
1035		a2	1135		s3	1235		o2	1335		o2	1435		o2
1037		o2	1137		a2	1237		c1	1337		a2	1437	4	o1
1039	3	a2	1139		o2	1239		o2	1339		s3	1439	19	se
1041		c1	1141		c1	1241		o2	1341		o2	1441	3	a2
1043		o2	1143		o2	1243		o2	1343		o2	1443		o2
1045		o2	1145		o2	1245		o2	1345		c1	1445		a2
1047		o2	1147		o2	1247		a2	1347		a2	1447	19	se
1049		p3	1149		c1	1249		wl	1349	4	o2	1449		o2
1051	3	w#q	1151		a2	1251		a2	1351		o2	1451	6	a2
1053		a2	1153		wk	1253		a2	1353		o2	1453		wl
1055		a2	1155		o2	1255	3	a2	1355		a2	1455		o2
1057		c1	1157		o2	1257	5	c6	1357		o2	1457		a2
1059		o2	1159		o2	1259	4	a2	1359	3	c6	1459		s3
1061		a2	1161		a2	1261		o2	1361		a2	1461		a2
1063	3	w#q	1163		a2	1263		a2	1363		o2	1463		a2
1065		a2	1165		o2	1265		a2	1365		o2	1465		o2
1067		o2	1167		o2	1267		o2	1367	3	m2	1467		a2
1069		c1	1169	5	o2	1269		o2	1369		o2	1469		o2
1071		a2	1171		s3	1271		o2	1371		a2	1471	3	w#p
1073		o2	1173		a2	1273		o2	1373		m1	1473	3	a2
1075		o2	1175		o2	1275		a2	1375		o2	1475		o2
1077		c1	1177	5	a2	1277		a2	1377		a2	1477		o2
1079		o2	1179		s3	1279		s3	1379		o2	1479		o2
1081		o2	1181		a2	1281		o2	1381		m1	1481		a2
1083		o2	1183		o2	1283	3	w#q	1383		a2	1483	3	a2
1085		a2	1185		o2	1285		o2	1385		o2	1485		a2
1087	3	w#p	1187	3	w#q	1287		a2	1387		o2	1487	3	m2
1089		o2	1189		o2	1289		wl	1389		c1	1489		wl
1091		a2	1191		o2	1291	3	w#q	1391		a2	1491	3	a2
1093		p2	1193		wl	1293		a2	1393		o2	1493		wl
1095		o2	1195		s3	1295		a2	1395		o2	1495		o2
1097		wl	1197		a2	1297		c1	1397	4	o2	1497		a2
1099		o2	1199		o2	1299		o2	1399		s3	1499	18	se

Existence of Hadamard Matrices

q	t	Method	q	t	Method	q	t	Method	q	t	Method	q	t	Method
1501		o2	1601		wk	1701		a2	1801		wk	1901		a2
1503		a2	1603		o2	1703	4	o2	1803		a2	1903		o2
1505		o2	1605		o2	1705		o2	1805		a2	1905		o2
1507		o2	1607		a2	1707		a2	1807		o2	1907	3	w#q
1509	3	a2	1609		c1	1709		wk	1809		o2	1909		o2
1511		a2	1611		s3	1711		o2	1811		a2	1911		a2
1513		o2	1613		a2	1713	4	a2	1813		o2	1913	4	o1
1515		o2	1615		o2	1715		a2	1815		o2	1915	3	a2
1517		a2	1617		o2	1717		o2	1817		o2	1917		o2
1519		o2	1619	3	w#q	1719	3	a2	1819		s3	1919		o2
1521		o2	1621		wk	1721		a2	1821		a2	1921		o2
1523		a2	1623		a2	1723		s8	1823		c4	1923		a2
1525		o2	1625		o2	1725		a2	1825		o2	1925		a2
1527	3	c6	1627		s3	1727		a2	1827		a2	1927		o2
1529		o2	1629		o2	1729		o2	1829		o2	1929	4	c6
1531		s3	1631		o2	1731		o2	1831	3	m2	1931		a2
1533		a2	1633	3	a2	1733		wl	1833		a2	1933		p2
1535		o2	1635		o2	1735		s3	1835		o2	1935		o2
1537		o2	1637		a2	1737		a2	1837		c1	1937		o2
1539		o2	1639		o2	1739		o2	1839		o2	1939		o2
1541		a2	1641		a2	1741		c1	1841	4	a5	1941		c1
1543	3	a2	1643		a2	1743		a2	1843		o2	1943		o2
1545		o2	1645		o2	1745		o2	1845		o2	1945		o2
1547		o2	1647		o2	1747	3	m2	1847	3	m2	1947		o2
1549		wk	1649		o2	1749		o2	1849		o2	1949	4	a2
1551		a2	1651		s3	1751	4	o2	1851		o2	1951		y2
1553		a2	1653		o2	1753		wl	1853		a2	1953		o2
1555		s3	1655		a2	1755		a2	1855		o2	1955		o2
1557		o2	1657		c1	1757		a2	1857		o2	1957	4	o2
1559	4	a2	1659		o2	1759		s3	1859		o2	1959		s3
1561		c1	1661	4	o2	1761		a2	1861		s4	1961		o2
1563		o2	1663	3	m2	1763		o2	1863		a2	1963		s7
1565		o2	1665		a2	1765		o2	1865		a2	1965		c1
1567	19	se	1667	3	m2	1767		o2	1867		s3	1967		a2
1569		c1	1669		p2	1769		o2	1869		o2	1969	10	a5
1571	18	se	1671		o2	1771		o2	1871	3	m2	1971		a2
1573		o2	1673		a2	1773		o2	1873		wk	1973		m1
1575		a2	1675		o2	1775		o2	1875		a2	1975		o2
1577		o2	1677		o2	1777		wl	1877		a2	1977		a2
1579	5	a2	1679		o2	1779		o2	1879	3	a2	1979	4	a2
1581		a2	1681		o2	1781		o2	1881		a2	1981	5	a2
1583	3	m2	1683		o2	1783	18	se	1883	3	w#r	1983		o2
1585		o2	1685		o2	1785		o2	1885		o2	1985		o2
1587		o2	1687		o2	1787	3	m2	1887		a2	1987	16	se
1589	4	a2	1689	3	c6	1789		p2	1889		m1	1989		o2
1591		o2	1691		a2	1791		o2	1891		o2	1991		a2
1593		o2	1693		wl	1793	4	a2	1893	4	c6	1993		wl
1595		a2	1695		a2	1795	6	a5	1895		o2	1995		o2
1597		wk	1697		wl	1797		a2	1897		o2	1997		wk
1599		o2	1699	3	a2	1799		o2	1899		o2	1999		y2

Existence of Hadamard Matrices

Toward the classification of distance-transitive graphs of affine type

富士通国際研 横山 和弘

1. はじめに

近年、重要視されてきている問題に distance regular graph の完全分類問題がある。その分類問題の一つの部分問題として distance transitive graph の分類がある。distance regular graph の部分クラスである distance transitive graph は、本来 distance regular graph が持つ組合せ論的な性質の上に群論的な性質を持っており、この二つの重要な性質により、distance transitive graph の分類は distance regular graph の分類と比較して容易であると考えられる。しかも、distance transitive graph の分類は distance regular graph の分類に大きく貢献することにもなる（一つのステップとも考えられる）。すなわち、まず解き易い問題として distance transitive graph の分類を捉えることができる。現在 distance transitive graph の分類は一歩一歩進展しており、ここでは、distance transitive graph の分類プログラムの概要とその途中経過について報告する。

2. distance transitive graph の分類プログラム

distance transitive graph の分類問題は大きく次の部分問題（ステップ）に分けることができる。

(1) primitive distance transitive graph の分類

(2) primitive の場合の分類を用いて imprimitive の場合を分類する。

imprimitive な場合には、derived graph もしくは halved graph (bipartite half) を考えることにより primitive なグラフが現れるので、(1)⇒(2) という問題の 2 ステップ分割が考えられる。（この状況は distance regular graph でも同様であるが、現在の distance regular graph の分類においてはこの戦略はとっていないようである。）

(2) の問題は distance regular graph の場合と比べて、自己同形群の立場を使えるので、(2) の解決はかなり容易であると思われる。というのは、imprimitive なグラフ Γ より作られる primitive なグラフ Γ' が derived graph である場合には、$\mathrm{Aut}(\Gamma) = K\cdot\mathrm{Aut}(\Gamma')$, K はある正規部分群, となり、halved graph である場合には $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma')2$ となる。この事実は群論的にかなり強い制約であることから、『問題が解ける』ことが予想される。

さて、上により問題はまず(1)を解くことに帰着された。そこで、以下 primitive distance transitive graph の分類を考える。diameter が2以下の場合には、2重可移群の分類、ランク3の置換群の分類により完全に解決せれている。そこで、diameter は3以上であるとしてよいことになる。primitive distance transitive graph の分類は次の定理により更に細分化される。

定理 (Praeger & Saxl & Yokoyama (1987))

Γ を diameter が2以上の primitive distance transitive graph とし、その自己同形群を G とおく。この時、次のいずれかが成り立つ。

(i) Γ は Hamming graph であるか、もしくは diameter が2である Hamming graph の complement graph である。

(ii) G は almost simple である。(すなわち、ある単純群 X が存在して $X \leq G \leq$Aut(X))

(iii) G は Γ の頂点全体に正則に作用する elementary abelian 正規部分群を持つ。

((ii) の場合を almost simple の場合と呼び、(iii) の場合を affine の場合と呼ぶ。)

上の定理により分類問題は二つの部分問題へと分割されることになる。一つは (ii) almost simple の場合の分類であり、他方は (iii) affine の場合の分類である。almost simple の場合の分類は Van Bon, Cohen, Cuypers, Inglis, Ivanov, Liebeck, Praeger, Saxl 等により、有限単純群の分類定理を利用しての『蟲潰し』的な方法で研究されており、置換指標の既約分解における各既約指標の重複度が1である事実を利用して解いたものと、それにグラフ的性質を利用して解いたものとがある。分類リストを挙げると、

交代群(対称群) – Saxl, Ivanov, Liebeck & Praeger & Saxl

PSL(n, q) – Inglis, Liebeck & Saxl, Van Bon & Cohen

13次元以下の古典群 – Inglis

Held の群 – Van Bon & Cohen & Cuypers

almost simple の場合はほぼ終結したと言えるが、現時点では、まだ完全分類の結果は論文として出版されてはいない。

ここまでの話は、Brouer & Cohen & Neumaier (1989) または、Bannai & Ito (1986) を参照されたい。

3. affine の場合の分類

『affine の場合の分類をどのように解くか』については方針が固まっているわけではない。現在 affine の場合に現れるグラフは diameter に関する無限系列として 3 種類のみが知られている。

Hermitian forms graph – 隣接する 2 点を含む極大閥は唯一つ

Bilinear forms graph – 隣接する 2 点を含む極大閥は 2 個

Alternating forms graph – 隣接する 2 点を含む極大閥は 3 個以上

(diameter が 3 の無限系列には Affine $E_6(q)$ graph がある。Quadratic forms graph は distance regular ではあるが、distnce transitive ではない。)

上の状況より、隣接する 2 点を含む極大閥の個数を指定してグラフを分類するアプローチが考えられる。そして、現時点では diameter が充分大きい場合に、『隣接する 2 点を含む極大閥の個数を指定すればグラフは上記のものが抽出される』ことが目標になる。

このアプローチ上のひとつの結果として、隣接する 2 点を含む極大閥が 2 個の場合について次がある。

定理 (Yokoyama (1989)) Γ が affine の場合でしかも正則部分群は 2- 群ではないとし、更に次の 2 条件を満たすとする。

(1) 隣接する 2 点を含む極大閥は 2 個、

(2) Γ の自己同形群 G は三角形にはならない長さ 2 のパス全体の上に可移に作用する。

この時、Γ は Bilinear forms graph である。

残念ながら、その後の進展はまだない。現在私が挑戦している問題は

(1) 隣接する 2 点を含む極大閥が唯一の場合を分類する。(Hermitian forms graph を特徴付け、抽出する。)

(2) 上の定理を条件 (2) を取って証明する。

の 2 点である。

最後に分類を試みる上での重要と思われる点について述ておく。上記の 3 種の無限系列において、特徴的であることは、無限系列における diameter が n のグラフを $\Gamma(n)$ とおけば、次が成り立つことである。

$\Gamma(n)$ の距離 i ($2 \leq i \leq n$) の2頂点を x, y とする。この時、 x, y を含む部分グラフ Γ' で、 $\Gamma(i)$ に同形であるものが唯一存在する。

この性質により、与えられたグラフが $\Gamma(n)$ であることを示すためには、局所的な部分グラフとして $\Gamma(i)$ に同形なものを（帰納的に）構成していく方法が考えられるのである。（実際、隣接する2点を含む極大閥が2個の場合に Bilinear forms graph を抽出するのにはこの手法を用いた。）

今回の報告の終わりにあたり、分類プログラムの概要の説明に留まり、新しい結果の発表に至らなかったことをおわびします。

参考文献

E. Bannai & T. Ito (1986), Current researches on algebraic combinatorics, Graphs Combin. **2**, 287-308.

A. E. Brouwer & A. M. Cohen & A. Neumaier, Distance-regular graphs, Springer-Verlag.

C. E. Praeger & J. Saxl & K. Yokoyama (1987), Distance transitive graphs and finite simple groups, Proc. London Math. Soc. (3) **55**, 1-21.

K. Yokoyama (1989), On distance transitive graphs whose automorphism groups are affine, preprint. (submitted to J. Combin. Th. (B).)

INTERSECTION DIAGRAMS OF DISTANCE-REGULAR GRAPHS

Tokyo Ikashika University

Kazumasa NOMURA

1. INTRODUCTION

Let G be a connected graph and let ∂ denote the usual metric on the vertex set $V = V(G)$ of G. For vertices u, v in G and non-negative integers r, s, we define

$$\Gamma_r(u) = \{ x \in V \mid \partial(x, u) = r \},$$
$$D^r_s(u, v) = \Gamma_r(u) \cap \Gamma_s(v).$$

G is said to be *distance-regular* if the size of D^r_s depends only on the distance between u and v, rather than the individual vertices. In this case, we write $p^t_{r\,s} = | D^r_s(u, v) |$, where $t = \partial(u, v)$. Let $d = d(G)$ be the diameter of G and k be the valency of G, and let

$$\left\{ \begin{matrix} 0 & c_1 & \cdots\cdots & c_r & \cdots\cdots & c_{d-1} & c_d \\ 0 & a_1 & \cdots\cdots & a_r & \cdots\cdots & a_{d-1} & a_d \\ k & b_1 & \cdots\cdots & b_r & \cdots\cdots & b_{d-1} & 0 \end{matrix} \right\}$$

be the *intersection array* of G, where $c_r = p^r_{1\,r-1}$, $a_r = p^r_{1\,r}$, $b_r = p^r_{1\,r+1}$. More precise description about distance-regular graphs will be found in [1], [2].

In this note we shall prove the following result.

THEOREM 1. *Let G be a distance-regular graph with odd diameter $d = 2r+1 \geqq 3$. If G has the following intersection array*

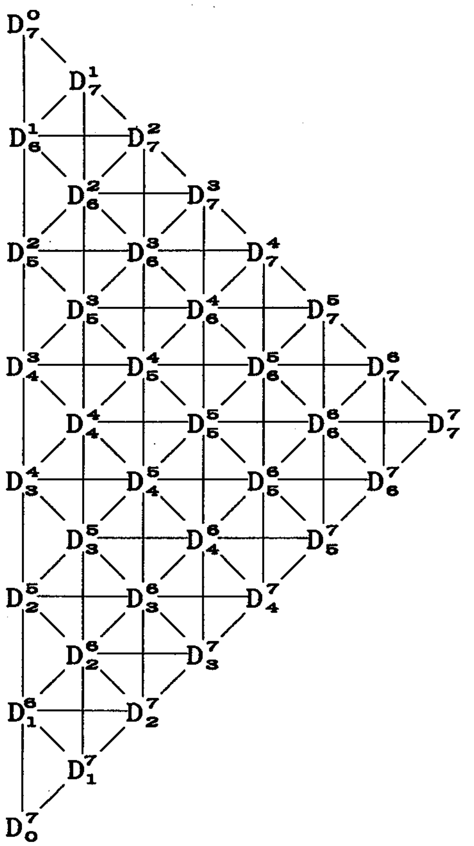
$$\left\{\begin{matrix} 0 & 1 & c_2 & \cdots\cdots & c_r & c_{r+1} & c_{r+2} & \cdots\cdots & c_{d-1} & k \\ 0 & 0 & 0 & \cdots\cdots & 0 & a_{r+1} & 0 & \cdots\cdots & 0 & 0 \\ k & b_1 & b_2 & \cdots\cdots & b_r & b_{r+1} & b_{r+2} & \cdots\cdots & b_{d-1} & 0 \end{matrix}\right\}$$

and $p^d_{j\,d} = 0$ for $j \geqq 3$, then G is bipartite (i.e. $a_{r+1} = 0$).

Theorem 1 gives a partial answer to a question of E. Bannai and T. Ito about multiple P-polynomial structure of association schemes (see [1], III.4, pp.259). The notion of the intersection diagrams plays a very important role in the proof of the above theorem. We have already obtained several applications of the intersection diagram with respect to adjacent vertices. In this note we shall use the intersection diagram with respect to non-adjacent vertices.

2. THE INTERSECTION DIAGRAM

Let G be a distance-regular graph which satisfies the assumptions of Theroem 1. Fix two vertices u, v in G with $\partial(u, v) = d = d(G)$, and put $D^i_j = D^i_j(u, v)$. We draw the family $\{D^i_j\}_{ij}$ as follows. Throughout this paper we shall give figures for the case $d = 7 = 2r + 1$, $r = 3$.



In the above diagram, a line between two entries indicates possibility of existence of edges between them. We call the above diagram the *intersection diagram* of G with respect to u, v.

LEMMA 2. $D^d_j = D^j_d = \emptyset$ *for* $3 \leqq j \leqq d$.

Proof. Since $\partial(u, v) = d$, $D^i_s = p^d_{i\,s}$ holds for every i, s. By the assumption of Theorem 1 we have $p^d_{j\,d} = 0$, therefore $D^j_d = \emptyset$ for $j \geqq 3$. By similar arguments we have also $D^d_j = \emptyset$ since $p^d_{d\,j} = p^d_{j\,d} = 0$ for $j \geqq 3$. ■

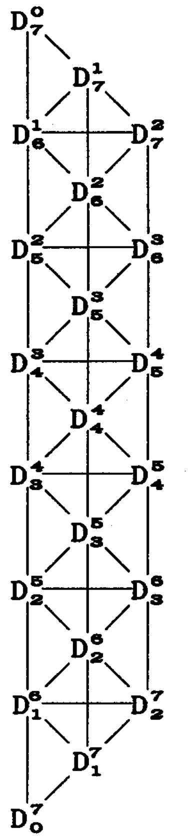
LEMMA 3. $D^i_j = \emptyset$ *for all* i, j *with* $i + j \geqq d + 3$.

Proof. Assume $D^i_j \neq \emptyset$ for some i, j with $i + j \geqq d + 3$, where we take i to be maximal. Then $i < d$ by Lemma 2. Let x be a vertex in D^i_j. Since $x \in \Gamma_i(u)$, there are b_i edges from x to $\Gamma_{i+1}(u)$, where $b_i > 0$ by $i < d$. This implies

$$D^{i+1}_{j-1} \cup D^{i+1}_j \cup D^{i+1}_{j+1} \neq \emptyset.$$

This contradicts to the maximality of i. ■

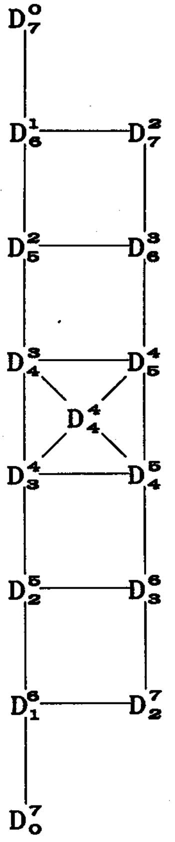
By Lemma 3, the intersection diagram becomes as follows.



LEMMA 4. $D^i_{d+1-i} = \emptyset$ *for* $i \neq r+1$.

Proof. Assume $D^i_{d+1-i} \neq \emptyset$ for some i, where we take i to be minimal. It is clear $i > 0$, and we may assume $i \leqq r$. Put $j = d+1-i$, and take a vertex x in D^i_j. We have $D^{i-1}_{j+1} = \emptyset$ by the minimality of i. Since $x \in \Gamma_i(u)$, there are c_i edges from x to $\Gamma_{i-1}(u)$. So we get $e(x, D^{i-1}_j) = c_i > 0$. Therefore there is an edge xy with $y \in D^{i-1}_j$. Thus xy is an edge in $\Gamma_j(v)$. But we have $a_j = 0$ since $r + 2 \leqq j \leqq d$. a contradiction. ■

By Lemma 4, the diagram becomes as the following.



3. EDGE PATTERNS

We consider the intersection diagram given in the previous section. For a vertex x in a entry D^i_j of the diagram, we shall determine the number of edges from x to another entry $D^{i'}_{j'}$. For a subset A in G, the number of edges from a vertex x to A will be denoted by $e(x, A)$.

LEMMA 5. *If* $i + j = d$ *and* $x \in D^i_j$. *Then* $e(x, D^{i-1}_{j+1}) = c_i$ *and* $e(x, D^{i+1}_{j-1}) = c_j$ *hold.*

Proof. Since $x \in \Gamma_i(u)$, there are c_i edges from x to $\Gamma_{i-1}(u)$. Then we get $e(x, D^{i-1}_{j+1}) = c_i$. We get also $e(x, D^{i+1}_{j-1}) = e(x, \Gamma_{j-1}(v)) = c_j$.
■

LEMMA 6. *If* $i + j = d + 2$ *and* $x \in D^i_j$. *Then* $e(x, D^{i-1}_{j+1}) = b_j$ *and* $e(x, D^{i+1}_{j-1}) = b_i$ *hold.*

LEMMA 7. *If* $i + j = d$, $1 \leqq i \leqq r$ *and* $x \in D^i_j$, *then* $e(x, D^{i+1}_{j+1}) = b_j - c_i$.

Proof. Since $x \in \Gamma_j(v)$ and D^i_{j+1} is empty, we have

$$b_j = e(x, \Gamma_{j+1}(v)) = e(x, D^{i-1}_{j+1}) + e(x, D^{i+1}_{j+1}).$$

We have also, by Lemma 5, $e(x, D^{i-1}_{j+1}) = c_i$. Thus we get $e(x, D^{i+1}_{j+1}) = b_j - c_i$. ■

LEMMA 8. *If* $i + j = d$, $1 \leqq i \leqq r$ *and* $x \in D^{i+1}_{j+1}$, *then* $e(x, D^{i}_{j}) = c_{i+1} - b_{j+1}$.

LEMMA 9. *If* $x \in D^{r+1}_{r+1}$ *then* $e(x, D^{r}_{r+1}) = c_{r+1}$ *and* $e(x, D^{r+1}_{r}) = b_{r+1}$

LEMMA 10. *If* $x \in D^{r}_{r+1}$ *then* $e(x, D^{r+1}_{r+1}) = a_{r+1}$.

Proof. Since $x \in \Gamma_{r+1}(v)$, there are a_{r+1} edges from x to $\Gamma_{r+1}(v)$. Here, there is no edge from x to D^{r}_{r+1} since $D^{r}_{r+1} \subset \Gamma_{r}(u)$ and $a_r = 0$. This implies $e(x, D^{r+1}_{r+1}) = a_{r+1}$. ■

LEMMA 11. *If* $x \in D^{r+1}_{r+2}$ *then* $e(x, D^{r+1}_{r+1}) = a_{r+1}$.

4. PROOF OF THEOREM 1

Let G be a distance-regular graph which satisfies the assumption of Theorem 1. We assume $a_{r+1} > 0$. Let m denote the size of D^{r+1}_{r+1}. Remark $m > 0$ by Lemma 10. By counting the number of edges between D^{r+1}_{r+1} and D^{r}_{r+1} using Lemma 9 and Lemma 10, we get $|D^{r}_{r+1}| = \dfrac{mc_{r+1}}{a_{r+1}}$. Similarly we get $|D^{r+1}_{r+2}| = \dfrac{mb_{r+1}}{a_{r+1}}$ by Lemma 9, 11. Then by counting the number of edges between D^{r}_{r+1} and D^{r+1}_{r+2} using Lemma 7, 8, we get,

$$\frac{mc_{r+1}}{a_{r+1}}(b_{r+1} - c_r) = \frac{mb_{r+1}}{a_{r+1}}(c_{r+1} - b_{r+2})$$

This implies the following relation by $m > 0$.

$$c_r c_{r+1} = b_{r+1} b_{r+2}. \tag{1}$$

By counting the number of edges between D^{r-1}_{r+2} and D^{r}_{r+3}, we get

$$\frac{mc_{r+1}c_r}{a_{r+1}c_{r+2}}(b_{r+2} - c_{r-1}) = \frac{mb_{r+1}b_{r+2}}{a_{r+1}b_r}(c_r - b_{r+3}).$$

Here we have $b_{r+2} - c_{r-1} = b_{r-1} - c_{r+2}$, $c_r - b_{r+3} = c_{r+3} - b_r$. So the above equality implies, by using (1),

$$b_{r-1} b_r = c_{r+2} c_{r+3} \tag{2}$$

By counting the number of edges between D^{r-2}_{r+3} and D^{r-1}_{r+4}, we get

$$\frac{mc_{r+1}c_r c_{r-1}}{a_{r+1}c_{r+2}c_{r+3}}(b_{r+3} - c_{r-2}) = \frac{mb_{r+1}b_{r+2}b_{r+3}}{a_{r+1}b_r b_{r-1}}(c_{r-1} - b_{r+4}).$$

This implies, by (1) and (2),

$$c_{r-2} c_{r-1} = b_{r+3} b_{r+4} \tag{3}$$

We repeat the above arguments. In the case r is odd, we get

$$c_1c_2 = b_{2r}b_{2r+1}.$$

This is impossible since $b_{2r+1} = b_d = 0$. In the case r is even, we get

$$b_1b_2 = c_{2r}c_{2r+1}.$$

Here we have $b_1 = k - 1$ and $c_{2r+1} = k$. Thus we get

$$(k-1)b_2 = c_{2r}k.$$

Then k divides b_2 and hence $k \leqq b_2$, a contradiction. ■

REFERENCES

[1] Bannai - Ito : "Algebraic Combinatorics I," Benjamin (1984).

[2] Brouwer - Cohen - Neumaier : "Distance-Regular-Graphs," Springer (1989).

Factor sets associated with regular collineation groups

大阪大学教養部　平峰　豊

(Yutaka Hiramine)

§1. Introduction

正則な自己同型群 A をもつ対称デザイン $\mathbb{D}$ は A が含む差集合を用いて記述できることが知られているが、点上正則な自己同型群をもつアフィン平面について類似の方法でとらえることを考えてみたい。以下ではこれが群の特殊な拡大の問題と関連していることを示し、それをもとに得られるいくつかの結果を紹介する。

§2 位数 n^2 のアーベル群と位数 n のアフィン平面.

A を位数 n^2 のアーベル群とし H を位数 n の部分群, $G = A/H = \{1, \sigma, \cdots\}$, $\{c(\sigma,\tau)\}$ を拡大 $A > H$ の正規化された因子団の一つとする。すなわち, $\{c(\sigma,\tau)\}$ は A/H の適当な代表系 $D = \{t(\sigma) \mid \sigma \in G = A/H\} \ni 1$ (ただし各 $t(\sigma) \in A$ で $\sigma = t(\sigma)H$) をとれば次をみたす。

$$t(\sigma)t(\tau) = t(\sigma\tau)\,c(\sigma,\tau)\ ,\quad c(\sigma,\tau)\in H$$

$$c(\sigma,\tau)\,c(\sigma\tau,\rho) = c(\sigma,\tau\rho)\,c(\tau,\rho)$$

$$c(1,\sigma) = c(\sigma,1) = 1 \qquad {}^\forall\sigma,\tau,\rho\in G$$

この因子団 $\{c(\sigma,\tau)\}$ に対して次のような結合構造

$\mathbb{D} = \underline{\mathbb{D}(c)}$ を考える：

$\mathbb{D}$の点集合 $\mathbb{P}$ = Aの元の全体

$\mathbb{D}$のブロックの集合 $\mathbb{B} = \{Dx \mid x\in A\} \cup A/H$

$\mathbb{D}$の結合関係 = "$\in$"により自然に定まるもの.

この時. 次の(*)が成りたっている.

(*) $|\mathbb{P}| = n^2\ ,\quad |\mathbb{B}| = n^2+n\ ,\quad |B| = n\ ,\ {}^\forall B\in\mathbb{B}$

このことから $\mathbb{D}(c)$ は位数 n のアフィン平面

(2-$(n^2,n,1)$ デザイン) に近い形をしていることが

分かるが. これが実際にアフィン平面であるための

条件が因子団の言葉を用いて次のように言える.

<u>定理1</u>. $\mathbb{D}(c)$：アフィン平面

$\iff \{c(\sigma,\tau)\}$: *bijective* ${}^\forall\tau\in G^* = G-\{1\}$.

(ここでは $c(\sigma,\tau)$ を $\sigma\longmapsto c(\sigma,\tau)$ により G から H

への写像とみている.)

(証明) 上の(*)より $\mathbb{D}(c)$：アフィン平面 $\iff |B_1\cap B_2|\leqq 1$

$Dx\ ({}^\forall x\in A)$ も A/H の代表系であるから, $({}^\forall B_1 \underset{(\neq)}{,} {}^\forall B_2\in\mathbb{B})$

$B_1 \overset{(\#)}{,} B_2 \in \{Dx \mid x \in A\}$ の時以外は常に $|B_1 \cap B_2| \leqq 1$.

$\therefore$ $\mathbb{D}(C)$: アフィン平面 $\Leftrightarrow |Dx \cap Dy| \leqq 1 \quad {}^\forall x \overset{(\#)}{,} y \in A$

$\Leftrightarrow |D \cap Dz| \leqq 1 \qquad {}^\forall z \in A - \{1\}$

$\Leftrightarrow |\{(\sigma, \rho) \mid t(\sigma)t(\tau)h = t(\rho) \quad {}^\exists\sigma, {}^\exists\rho \in G\}| \leqq 1$

$({}^\forall z = t(\tau)h \quad \tau \in G,\ h \in H \quad z \neq 1)$

$\Leftrightarrow |\{(\sigma, \sigma\tau) \mid c(\sigma, \tau) = h^{-1} \quad {}^\exists\sigma \in G\}| \leqq 1$

$\Leftrightarrow \{c(\sigma, \tau)\}$: bijective

<u>bijective な因子団の例</u>

(1) G, H を位数 n の群とし f を G から H の中への planar function ([1] §5.1 参照) とするとき $c(\sigma, \tau) = f(\sigma\tau)f(\tau)^{-1}f(\sigma)^{-1}$ は bijective な因子団となる.

(2) $F = F(+, \circ)$ を可換な semifield (i.e. "$+$" に関して群, "$\circ$" に関して loop, 左右の分配律をみたす代数系) とし, $H = G = F^+$ とみる. $c(\sigma, \tau) = \sigma \circ \tau$ $(G \times G \to H)$ とおくと, bijective な因子団 $\{c(\sigma, \tau)\}$ が得られる. これが定める拡大は, $F \times F$ に次のように積を定めたものに同型である: (**)

$$(\sigma_1, \tau_1)(\sigma_2, \tau_2) = (\sigma_1 + \sigma_2,\ \tau_1 + \tau_2 + \sigma_1 \circ \sigma_2)$$

このとき H は $\{(0, \tau) \mid \tau \in F\}$ と同一視される. また

有限な semifield の加法群 F^+ はある素数 p に対して基本可換 p 群であることが知られている。([2])

$(\sigma_1, \tau_1)(\sigma_2, \tau_2) = (\sigma_2, \tau_2)(\sigma_1, \tau_1)$ が (※※) より確かめられる。従って A は、アーベル群であるが、

$(\sigma, \tau)^m = (m\sigma,\ m\tau + (1+2+\cdots+m-1)\sigma\circ\sigma)$ であるから F の性質 $p\sigma = 0$ $(\forall\sigma \in F)$ を用いて

$$A \cong \begin{cases} \text{基本可換 } p \text{ 群} & (p > 2) \\ \text{exponent 4 の homocyclic 2-群} & (p = 2) \end{cases}$$

結合構造 $\mathbb{D}(C)$ では群 A が点集合 $\mathbb{P}$ 上に可移に作用するように定義されていたが、アフィン平面の場合にこの逆について考える。

$\mathbb{D} = (\mathbb{P}, \mathbb{B})$ を位数 n のアフィン平面とし Aut $\mathbb{D}$ が位数 n^2 の可換部分群 A をもつと仮定する。

$\mathbb{D}$ が定める射影平面 $\widetilde{\mathbb{D}}$ に Orbit Theorem ([2] §13) を用いることにより A は $\mathbb{P}$ 又は $\mathbb{B}$ 上に長さ n^2 の orbit をもつ。このことから、必要ならば $\widetilde{\mathbb{D}}$ の中の部分アフィン平面と取り換えることにより次のいずれかが起るとしてよい。

(1) $^{\exists}B_1, \cdots, {}^{\exists}B_{n+1} \in \mathbb{B}$, $\mathbb{B} = B_1^A \cup \cdots \cup B_{n+1}^A$

ここで各 $B_i^A = \{B_i x \mid x \in A\}$ は平行類

(2) $^{\exists}B_1, {}^{\exists}B_2 \in \mathbb{B}$, $\mathbb{B} = B_1^A \cup B_2^A$, B_1^A は平行類

(1)が起きる時はよく知られているようにAはtranslation groupとなるのである素数pに対して基本可換p群となりこれはすべてのp^{2m}に対して多くの例が存在する．

従って以下では(2)を仮定しこの場合について考える．

$B_1 \cap B_2 \ni Q$をとる．Aは$\mathbb{P}$上に正則に作用するから$\mathbb{P}$の任意の点Qx $(x \in A)$とAの元xを同一視して$\mathbb{B}$の各元はAの部分集合とみる．とくに$1 \in B_1 \cap B_2$

$\forall x \in B_1 \rightarrow B_1 \cap B_1 x \ni x$　　$\therefore$ B_1^Aが平行類であることより$B_1 x = B_1$　　　$\therefore$ B_1はAの部分群。

B_1^Aは剰余類A/B_1に一致。故にB_1^Aのどの元もB_2と一点で交わるということはB_2がA/B_1の代表系であることを意味する．$\therefore H = B_1$, $D = B_2$とおくと

$A > H$ (部分群), $A \supset D$ (部分集合)

$|A| = n^2$, $|H| = |D| = n$,　　$A = HD$

さらに次が成りたつ

<u>定理2</u>　Dを拡大$A>H$の代表系として選ぶとき対応する因子団はbijectiveである．

(証明) $G = A/H = \{1, \sigma, \cdots\}$, $D = \{t(\sigma) \mid \sigma \in G\}$とおく．ここで$t(\sigma) \in A$　, $t(\sigma)H = \sigma$とする．

$B \in B_2^A$とするとBを含む平行類はB^Hであるから

$G \ni \tau \neq 1$ を fix すると $|D \cap Dt(\tau)h| = 1 \quad {}^\forall h \in H.$

$\therefore |\{(\sigma, \rho) \mid t(\sigma) = t(\rho)t(\tau)h\}| = 1 \quad {}^\forall h \in H.$

因子団 $\{c\}$ は $t(\rho)t(\tau) = c(\rho, \tau)t(\rho\tau)$ により定義されるから

$$|\{(\rho\tau, \rho) \mid c(\rho, \tau) = h^{-1},\ \rho \in G\}| = 1 \quad {}^\forall h \in H$$

$\therefore$ $\{c\}$ は bijective.

以上のことにより次の対応が示された。

{アーベル群から得られる bijective な因子団の全体}

↓↑

{点上可移な可換自己同型群(除 translation gps)をもつアフィン平面の全体}

§3 bijective な因子団の性質といくつかの応用.

定理3. Aを群Hの群Gによる中心拡大とし、$\{t(\sigma)\}$ を A/H の代表系 ($t(1)=1$), $\{c(\sigma, \tau)\}$ を対応する因子団とする. Gのある元 ρ が次の条件を満たせば $\langle H, t(\rho)\rangle$ はH上の分裂拡大である:

$$\prod_{m=0}^{o(\rho)-1} c(\rho, \rho^m) = 1 \qquad (o(\rho) = \rho\text{の位数})$$

(証明) $\psi(j) = c(\rho, \rho^j)$ $j = 0, \pm 1, \cdots$ とおく.

$c(\rho^i, \rho^j)c(\rho^i\rho^j, \rho^k) = c(\rho^i, \rho^j\rho^k)c(\rho^j, \rho^k) \quad {}^\forall i, j, k$

$\therefore$ 帰納法により $C(\rho^p,\rho^q)=\left(\prod_{s=0}^{p-1}\psi(q+s)\right)\left(\prod_{t=0}^{p-1}\psi(t)\right)^{-1}$

$=\left(\prod_{s=0}^{p+q-1}\psi(s)\right)\left(\prod_{s=0}^{q-1}\psi(s)\right)^{-1}\left(\prod_{t=0}^{p-1}\psi(t)\right)^{-1}$ が成りたつ.

$\therefore C(\rho^p,\rho^q)=\Gamma(p+q)\Gamma(p)^{-1}\Gamma(q)^{-1}$

ここで $\Gamma(m)=\prod_{s=0}^{m-1}\psi(s)$

$\langle\rho\rangle$ から H への写像を $\Delta(\rho^m)=\Gamma(m)^{-1}$ で

定義するとこれは well-defined. なぜなら

$r=o(\rho)$ とおくと $\Gamma(\rho^{m+r})=\prod_{s=0}^{m-1}\psi(s)\prod_{s=m}^{m+r-1}\psi(s)$

$=\Gamma(m)\prod_{t=0}^{r-1}C(\rho,\rho^t)=\Gamma(m)$

$\therefore C(\rho^p,\rho^q)=\Delta(\rho^p\rho^q)^{-1}\Delta(\rho^p)\Delta(\rho^q)$

つまり $C(*,*)$ は coboundary, よって $\langle H,t(\rho)\rangle$

は H 上 split する.

<u>定義</u> A, H, G を定理3と同じ条件にとる. 因子団

$C(\sigma,\tau)$ が $\prod_{\tau\in G}C(\sigma,\tau)=1\ (\forall\sigma\in G)$ をみたすとき

$C(\sigma,\tau)$ を <u>homogeneous</u> な因子団という.

<u>補題4</u> $\{C(\sigma,\tau)\}$ が bijective な因子団ならば

$\{C(\sigma,\tau)\}$ は homogeneous か又は $n=2\ (A\cong\mathbb{Z}_4)$

が成りたつ.

(証明) A は中心拡大であるから H はアーベル群であるが

アーベル群の元すべての積が H の 2-Sylow 群 S が唯一つの

位数2の元を含む場合を除き単位元であるという事を

用いて示すことができる。$S \neq 1$, かつ S が cyclic の時は定理1を用いてアフィン平面を考えて、アフィン平面の中で考えて $n=2$ を示す。

<u>定理5</u> $\{c(\sigma,\tau)\}$ を homogeneous, p を奇素数, P を A の p-Sylow 群とする。もし $P/P\cap H$ が cyclic ならば P は $P\cap H$ 上分裂する。とくに A の各 p-Sylow 群 $(p\neq 2)$ は cyclic でない。

<u>定理6</u> $\{c(\sigma,\tau)\}$ を bijective, P を A の 2-Sylow 群とする。このとき次が成りたつ

(1) A の位数2の元はすべて P に含まれる。

(2) $P\cap H$ が cyclic $(\neq 1)$ ならば $n=2$ $(A\cong \mathbb{Z}_4)$.

(定理5, 6 は Hoffman の定理 ([1] p210) の一般化になっている。)

以上の結果は A がアーベル群でなくても成りたつものが多い (定理1, 2 など)。また、$2\nmid |A|$ の時は $\{c(\sigma,\tau)\}$ は分裂因子団であることが予想される。$2\,|\,|A|$ の時は A が2群になると予想されるがこの場合は前者よりやさしいような気がする。一般にアフィン平面(射影平面)の位数は素数巾に等しいと予想されているが、その根拠は

は分かりにくいように思う．可移な自己同型群をもつアフィン平面の場合は納得させるに足る理由があるように思われる。（[3]に詳しい）Aがアーベル群の場合は証明できてもよいような気がする。

文　献

[1] P. Dembowski, "Finite Geometries", Berlin-Heidelberg-New York, Springer, 1968.

[2] D.R. Hughes and F.C. Piper: "Projective Planes", Berlin-Heideberg-New York, Springer, 1973.

[3] M.J. Kallaher, "Affine Planes with transitive collineation groups" North Holland, New York-Amsterdam-Oxford, 1982.

Splitting Fields of Association Schemes

大阪教育大学
宗政昭弘

定義 d-class association scheme $(X, \{R_i\}_{i=0}^d)$ とは、有限集合 X と $X\times X$ の分割 $\{R_i\}_{i=0}^d$ で、

(i) $R_0=\{(x,x) \mid x\in X\}$

(ii) $\forall i, \exists i'$ s.t. $\{(x,y) \mid (y,x)\in R_i\} = R_{i'}$

(iii) $\forall i,j,k$ $\forall (x,y)\in R_k$,
$p_{ij}^k = \#\{z\in X \mid (x,z)\in R_i, (z,y)\in R_j\}$ は (x,y) によらず一定

(iv) $p_{ij}^k = p_{ji}^k$ $\quad \forall i,j,k$.

adjacency matrix A_i を次のように定義する

$$(A_i)_{xy} = \begin{cases} 1 & (x,y)\in R_i \\ 0 & (x,y)\notin R_i \end{cases}$$

$\mathfrak{A}$ を $A_0, A_1, \cdots, A_d$ で $\mathbb{C}$ 上生成される線形空間と

すると、$\mathfrak{A}$は可換な$\mathbb{C}$代数になる。$\mathfrak{A}$を adjacency algebra と呼ぶ。$\mathfrak{A}$は$M_n(\mathbb{C})$ $(n=|X|)$ の subalgebra と考えると自然に$\mathbb{C}^n$に作用する。$\mathfrak{A}$の極大共通固有空間は丁度 $d+1$個あることがわかり、そのうちのひとつは$(1,1,\cdots,1)$で生成される1次元空間である：$\mathbb{C}^n=V_0\oplus V_1\oplus\cdots\oplus V_d$, $V_0=(1,1,\cdots,1)$. $\mathbb{C}^n$からV_iへの射影をE_iとおく。特に$E_0=\frac{1}{n}J$, Jは all 1 matrix である。すると

$$A_j=\sum_{i=0}^{d}P_j(i)E_i \qquad (1)$$

と書ける。ただし$P_j(i)$はA_jのV_i上での固有値である。$P=(P_j(i))$を character table と呼び $K=\mathbb{Q}(P_j(i),\ 0\leq i,j\leq d)\subset\mathbb{C}$ を splitting field を呼ぶ。

問題　Kは円分体に含まれるか。

つまり、association scheme の character table が 1 の巾根で書けるかということだが、この問題は未解決である。association scheme の代表的な例として、有限群の等質空間があるが、この場合には、その置換表現に現れる指標の値を使って$P_j(i)$を表せるので、確かに円分体に含まれている。

さて、(1)式は $\{E_i\}_{i=0}^{d}$ について解くことができて、

$$\mathfrak{A} = \langle A_0, A_1, \cdots, A_d \rangle = \langle E_0, E_1, \cdots, E_d \rangle$$

となる。従って、$\mathfrak{A}$ は行列の乗法だけでなく、行列の成分ごとの乗法（Hadamard積）についても閉じていることがわかる。

$$E_i \circ E_j = \frac{1}{n} \sum_{k=0}^{d} q_{ij}^{k} E_k$$

と書いたとき（$\circ$ は Hadamard積）q_{ij}^{k} をKrein parameterと呼ぶ。$L = \mathbb{Q}(q_{ij}^{k},\ 0 \leq i, j, k \leq d)$ とおくと $L \subset K$ である。さらに次のことがわかる。

定理　$Gal(K/L) \subset Z(Gal(K/\mathbb{Q}))$

証明の概略を述べよう。$\sigma \in Gal(K/\mathbb{Q})$ とすると、σ は $\mathfrak{A}$ の自己同型を引き起こし、primitive idempotents $\{E_i\}_{i=0}^{d}$ を置換する。$\tau \in Gal(K/L)$ とすると τ は Krein parameter を fix するので、Hadamard積に関する primitive idempotents $\{A_j\}_{j=0}^{d}$ を置換する。これより、

$$P_j(i)^{\sigma\tau} = P_j(i^{\varphi(\sigma)})^{\tau} = P_{j^{\psi(\tau)}}(i^{\varphi(\sigma)})$$
$$= P_{j^{\psi(\tau)}}(i)^{\sigma} = P_j(i)^{\tau\sigma}$$

（ただし $\varphi(\sigma)$, $\psi(\tau)$ は $\{0, 1, \cdots, d\}$ の置換）となり、$\sigma\tau = \tau\sigma$

が成り立つ。すなわち $\tau \in Z(Gal(K/\mathbb{Q}))$.

系 Krein parameter が有理数ならば、Kは円分体に含まれる。

実際、定理から、$L=\mathbb{Q}$ なら $Gal(K/\mathbb{Q})$ が abelian であることがわかり、Kronecker-Weber の定理により、Kが円分体に入ることがわかる。

$L=\mathbb{Q}$ でない association scheme は、等質空間の場合にもあり得るが、筆者の知る限り、Lは2次体か4次体である。Krein parameter は、character table の成分から計算する公式があるので、character table が与えられれば Krein parameter が有理数かどうか判定できる。定理の証明に使われている議論を応用すると、この判定が容易にできる。この方法を示す例をあげよう。$PGL(3,2)$ は、$X=\{(x, \ell) \mid x$ は射影空間 $PG(2,2)$ の点, ℓ は直線, $x \notin \ell\}$ の上に可移に作用し、Coxeter graph と呼ばれる distance-transitive graph (従って association scheme) ができる。その character table は

$$P=\begin{pmatrix} 1 & 3 & 6 & 12 & 6 \\ 1 & -1+\sqrt{2} & -2\sqrt{2} & -2 & 2+\sqrt{2} \\ 1 & -1-\sqrt{2} & 2\sqrt{2} & -2 & 2-\sqrt{2} \\ 1 & 2 & 1 & -2 & -2 \\ 1 & -1 & -2 & 4 & -2 \end{pmatrix}$$

従って $K=\mathbb{Q}(\sqrt{2})$ である。$\sigma:\sqrt{2}\mapsto-\sqrt{2}\in Gal(K/\mathbb{Q})$ は、Pの行の置換を引き起こす（$\{E_i\}_{i=0}^{d}$の置換）が、列の置換は引き起こさない。つまり Hadamard 積を保存しない、Krein parameter を fix しない、ということがわかる。このようにして、Pの形を見ただけで Krein parameter が有理数かどうかが判定できるのである。

一方、もしKが円分体に含まれないような association scheme があったとすれば、どのような形をしているであろうか。$Gal(K/\mathbb{Q})$は非可換でなければならない。手初めとして、$Gal(K/\mathbb{Q})=S_3$ となる例はあるだろうか。A_j の最小多項式は $\prod_{i=0}^{d}(X-P_j(i))$ で $P_j(0)$は整数だから、3次の既約成分を持つためには $d\geqq3$ でなくてはならない。$d=3$ の時を考えると $\dim V_1=\dim V_2=\dim V_3$

となり p_{ij}^k は次の形になる

$$B_1=\begin{pmatrix}0&1&0&0\\a+b+c&a-1&b&c\\0&b&c&a\\0&c&a&b\end{pmatrix}\quad B_2=\begin{pmatrix}0&0&1&0\\0&b&c&a\\a+b+c&c&a-1&b\\0&a&b&c\end{pmatrix}$$

$$B_3=\begin{pmatrix}0&0&0&1\\0&c&a&b\\0&a&b&c\\a+b+c&b&c&a-1\end{pmatrix}$$

ただし $p_{ij}^k=(B_i)_{jk}$, a,b,c は $a^2+b^2+c^2-ab-bc-ca=a$ をみたす整数。character table P は

$$P=\begin{pmatrix}1&m&m&m\\1&\theta_1&\theta_2&\theta_3\\1&\theta_2&\theta_3&\theta_1\\1&\theta_3&\theta_1&\theta_2\end{pmatrix}$$

ただし $m=a+b+c$, $\{\theta_1,\theta_2,\theta_3\}$ は3次方程式 $x^3+x^2-mx+bc-a^2=0$ の3根である。(cf. Brouwer-Cohen-Neumaier, "Distance-regular graphs", Lemma 12.7.4 on P.389)。実は上の3次方程式の判別式は平方であることがわかって、Galois群は S_3 でないことがわかる。

ところで、上にあげた本には、この3次方程式が可約

となる必要十分条件は $b=c$ である、と書かれているが、これは間違いである。実際、

$$a=343t^2+464t+157$$
$$b=343t^2+463t+156$$
$$c=343t^2+445t+144$$

とおくと

$$(x+7t+5)(x+28t+19)(x-35t-23)$$

と因数分解される。$t=-1$ のとき association scheme は実在し、それは $GF(7^3)$ の3乗剰余からつくられる cyclotomic scheme と呼ばれるものである。

一般に $GF(q)$ 上の e-class cyclotomic scheme とは association scheme $(X, \{R_i\}_{i=0}^{e})$ で、$X=GF(q)$, $GF(q)^*=\langle\theta\rangle$, $C_i=\langle\theta^e\rangle\theta_i$ (e乗剰余), $R_i=\{(x,y)\mid x-y\in C_i\}$ $(i=1,2,\cdots,e)$ で定義される。cyclotomic scheme の splitting field が $\mathbb{Q}$ になるのはどのような時かという質問を提示したところ、味村良雄氏(神戸大)、山本幸一氏(東京女子大)、から回答があり、それらを一般化して次の結果が得られた。

定理 $GF(p^r)$上の e-class cyclotomic scheme (pは素数, $p^r-1=ef$, $e>1$, $f>1$) の splitting field は $\mathbb{Q}(\zeta_p)/\mathbb{Q}$の次数 $(p-1)/(p-1,f)$ の中間体である。

特に $GF(7^3)$上 3-class のときは $7^3-1=3\cdot 114$で $(p-1)/(p-1,f)=6/(6,114)=1$より splitting field は$\mathbb{Q}$である。一般に cyclotomic scheme の character table は次のように書ける

$$\underline{P}=\begin{pmatrix} 1 & f & f & & f \\ 1 & \chi(\underline{C_1}) & \chi(\underline{C_2}) & \cdots & \chi(\underline{C_e}) \\ 1 & \chi(\underline{C_e}) & \chi(\underline{C_1}) & \cdots & \chi(\underline{C_{e-1}}) \\ \vdots & \vdots & & & \vdots \\ 1 & \chi(\underline{C_2}) & \chi(\underline{C_3}) & \cdots & \chi(\underline{C_1}) \end{pmatrix}$$

ここで、χは nontrivial な $GF(q)$ の加法的指標、

$$\chi(\underline{C_i})=\sum_{a\in C_i}\chi(a)$$

で、これは Gauss の周期と呼ばれるものである。

On spherical t-designs (a survey)

坂内 英一 (九大・理)

§1. Introduction

この講演では spherical t-design に関する最近の仕事についての survey を与える。この方面の研究は日本ではあまりなじみがないと思われるので、証明などの技術的なことの解説よりも、どのような問題が考えられてきたか、またどのような文献があるかということを主に解説する。(この報告集では講演で述べられなかったことも少し補足してある。) この方面に興味を持ち、研究を始められる方の役に立てば幸いである。

$$S^d = \{(x_1, \cdots, x_{d+1}) \in \mathbb{R}^{d+1} \mid x_1^2 + \cdots + x_{d+1}^2 = 1\} \subset \mathbb{R}^{d+1}$$

を単位球とする。S^d の有限部分集合 X についての "combinatorics" を研究したいわけである。S^d の有限部分集合 X の研究には色々な方向があるであろう。コーディング理論の立場からは (大雑把に言えば) X の2点間の距離 $d(x,y)$ 達に注目し、例えば $d(x,y)$ が

特別な値を取り（あるいは $\mathrm{Min}\, d(x,y)$ が出来るだけ大きく）かつ $|X|$ が出来るだけ大きくなるものに興味があろう。デザイン理論の立場からは，単位球 S^d を有限個の点で"良く近似するもの"に興味があろう。次の S^d における t-design の概念は Delsarte-Goethals-Seidel (1977) により導入された非常に自然なかつ非常に役立つ概念である。

<u>定義</u>（Delsarte-Goethals-Seidel (1977)）単位球 S^d の有限部分集合 X が spherical t-design（または t-design in S^d）であるとは，

$$\frac{1}{|S^d|}\int_{S^d} f(x)\,dx = \frac{1}{|X|}\sum_{x\in X} f(x)$$

for $^\forall f(x) = f(x_1,\cdots,x_{d+1})$: polynomials of degree $\leq t$

が成り立つことと定義する。

（この条件は次の条件

$$\sum_{x\in X} f(x) = 0 \quad \text{for } ^\forall f \in \mathrm{Harm}(i)\ ,\ 1\leq i\leq t,$$

と同値である。ここで $\mathrm{Harm}(i)$ は $x_1,\cdots,x_{d+1}$ の i 次の homogeneous harmonic polynomials の作るベクトル空間を表わす。$L^2(S^d) = \bigoplus_{i\geq 0} \mathrm{Harm}(i)$ であり，

$\dim \mathrm{Harm}(i) = \binom{d+i}{i} - \binom{d+i-2}{i-2}$ となる。

従ってXが spherical t-design であるか否かは有限個の多項式 $f(x)$ に関してcheckすればよい条件である。)

Spherical t-design の基本的な性質についてのもっと詳しいことは、Delsarte-Goethals-Seidel (1977)、あるいは、survey paper : Bannai (1988) を参照されたい。

S^d の有限部分集合の "combinatorics" についての重要な結果を要約する。

<u>定理</u> (Delsarte-Goethals-Seidel (1977)) X が S^d の t-design なら、

$$|X| \geq \begin{cases} \binom{d+[\frac{t}{2}]}{[\frac{t}{2}]} + \binom{d+[\frac{t}{2}]-1}{[\frac{t}{2}]-1} & \text{for } t=\text{even} \\ 2\cdot\binom{d+[\frac{t}{2}]}{[\frac{t}{2}]} & \text{for } t=\text{odd}. \end{cases}$$

(Fisher 型不等式)

(上で等号の成り立つXを <u>tight t-design</u> と呼ぶ。)

<u>定理</u> (Bannai-Damerell (1979, 80)) Tight t-design in S^d $(d\geq 2)$ が存在するならば、$t=2, 3, 4, 5, 7$ or 11 である。

<u>注意</u> $t=4, 5, 7$ に対する tight t-design in S^d の分類は依然未解決である。

S^d における t-design X の色々な例は $O(d+1)$ の有限部分群 G の orbits : $X=x^G$ with $x\in S^d$ と

なるものを中心に色々と調べられた。一方，$d \geq 2$ の時，大きい t に対して t-design in S^d が存在するか否かは，次の Seymour-Zaslavsky の定理が得られるまで未解決であった。

<u>定理</u>（Seymour-Zaslavsky (1984)）$\forall t$, $\forall d$ に対して t-design X in S^d が存在する。

このSeymour-Zaslavsky の結果は非常に一般的な結果であり，上の定理はその極く特別な場合である。この論文で3種類の証明が与えられている（例えば一番易しい証明は implicit function theorem（陰函数定理）を用いる）が，いずれも完全に <u>non-constructive</u> な証明である。例えば t と d を与えたとき，X の存在はわかるが，$|X|$ がどの位の大きさに出来るか（小さい程良い）は一般的には全く計算不可能であった。

従って，残された問題として，与えられた t と d に対して，どの位小さな $|X|$ を持った t-design X in S^d が存在するかが決められるか，またそのような X をどのように explicit に構成することが出来るか，ということが重要な問題となる。次の § でこの問題に関しての最近の進展を述べる。

§2. Spherical t-design に関する最近の結果

この節では survey paper : Bannai (1988) 以後の spherical t-design についての極く最近の研究について述べる。

S^1 = unit circle ($\subset \mathbb{R}^2$) に内接する正 $(t+1)$-角形の頂点は t-design in S^1 である。Fisher 型不等式は $|X| \geqq t+1$ なので、正 m 角形 ($m \geqq t+1$) を考えることにより、$|X| \geqq t+1$ となる任意の $|X|$ に対して t-design in S^1 が explicit に構成出来る。また $t=1$ の時は問題は trivial となるので、以下 $t \geqq 2$ かつ $d \geqq 2$ の場合のみを考える。

$t=2$ の時、Fisher 型不等式は $|X| \geqq d+2$ となる。(S^d に内接する regular simplex の頂点が $|X| = d+2$ (tight) の例を与える。) $t=2$ に対する完全な結果は、1987/8 に Ohio に滞在していた味村良雄氏(神戸大)により得られた。

<u>定理</u> (Mimura (to appear))

(i) d=even, $|X| = d+3$ の 2-design X in S^d は存在しない。

(ii) 上の例外を除き、任意の $|X| \geqq d+2$ に対して、

2-design X in S^d が存在する（かつ explicit に構成される）。

<u>注意</u>　$t \geq 3$ の時はこの種の完全な結果は未解決である。他の小さな t の値に対しての味村氏の仕事の拡張の試みは，Bela Bajnok により成された。

<u>定理</u>（Bajnok (1989, to appear)）（結果の要約）
$|X| \geq (d+1)2^{d+2}$ となる任意の $|X|$ に対して，5-design X in S^d が存在する（かつ explicit に構成される。）
（注意：Fisher 型 bound は $|X| \geq 2\binom{d+2}{2} \approx d^2$.）

<u>定理</u>（Bajnok (1989)）　上と同様な結果が $t=7$ に対して得られる。［ただし $|X|$ は大きく，$|X|$ がある合同条件をみたさなければならず，また X が multi-set を許す（i.e. X が同じ点を2個以上含む可能性 —— ブロックデザインの理論における repeated blocks の概念に対応する）可能性が完全には除かれていないので $t=5$ の時とくらべるとまだ少し弱い結果である。］

<u>注意</u>　この方向を更に進めて，一般の t に対して同様な結果が得られることが望まれる（がまだ未解決である。）

Spherical t-design と似た（ある意味で易しく，また群の表現論が使えないという意味では難かしくなるが）概念である次の interval design の概念は興味深い。

<u>定義</u>（実区間 $[-1,1]$ で考える —— 他の区間でもよいが）有限集合 $X \subset [-1,1]$ が t-design in $[-1,1]$（interval t-design）であるとは，

$$\frac{1}{|X|}\sum_{x \in X} f(x) = \frac{1}{2}\int_{-1}^{1} f(x)\,dx$$

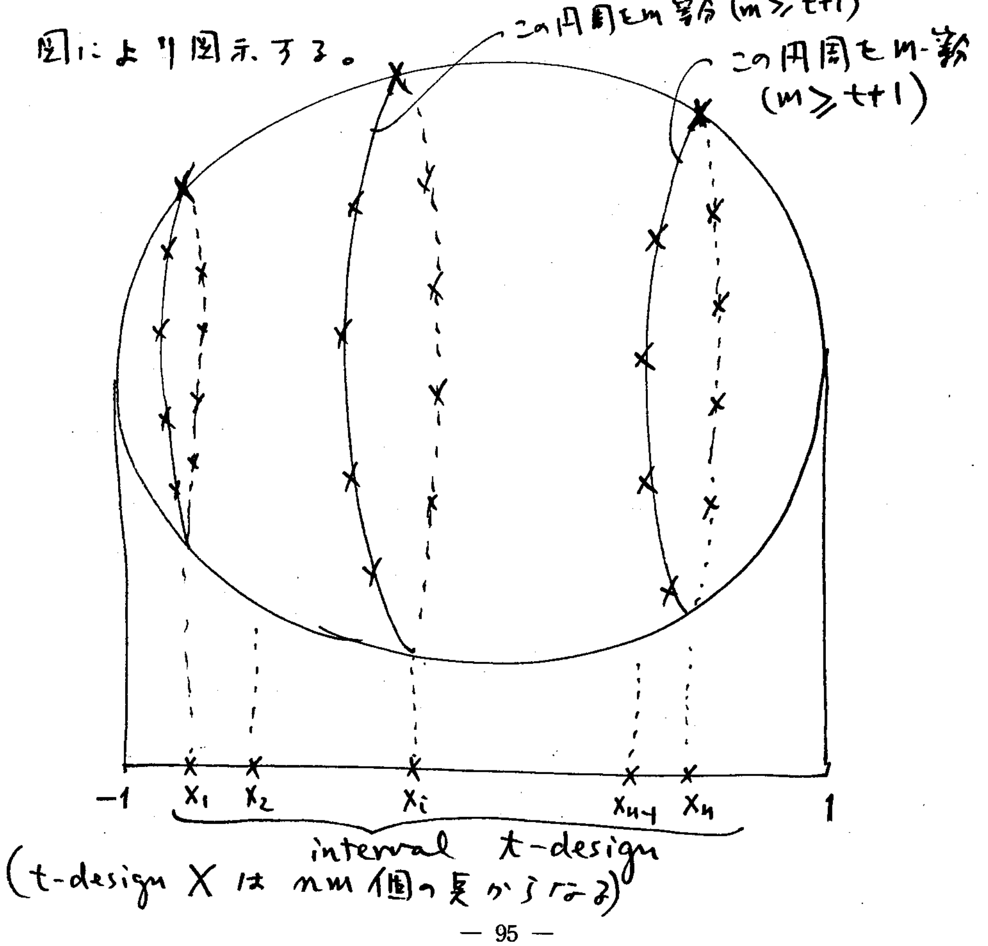
for $^\forall$ polynomial $f(x)$ of degree $\leq t$ と定義する。

<u>注意</u> この概念は "quadrature formula with equal weight" の存在と同値であり，解析（主に approximation theory）で古くから研究されて来た。X が interval t-design の時 $|X| \geqq t+1$ が成り立ち，tight (i.e. $|X| = t+1$) となるのは $t \leqq 7$ および $t=9$ の時に限ることが S. Bernstein により 1940年代に証明されている。（Krylov (1962), Natanson (1965) 参照。）
また Bernstein は，ある absolute constant c で X が interval t-design $\Rightarrow |X| \geqq c \cdot t^2$ となるものが存在することも示した。（Krylov (1962), Natanson (1965) 参照。）従って $t \to \infty$ の時 $|X|$ は

tight の bound よりはるかに大きくなる。

<u>注意</u>　Seymour-Zaslavsky の存在定理は、一番初めに（私が Ohio の seminar で提出した）interval t-design の存在問題を解いたのが始まりであり、それが spherical t-design を含む一般の存在定理に直ちに拡張されたわけである。

Bajnok (1989) は S^2 の spherical t-design を S^1 の spherical t-design と interval t-design を組み合わせて得られることを示した。この構成を次の図により図示する。



注意 (何らかの形で)類似なことが S^d ($d \geqq 3$) の場合に言えると望ましいが未解決である。

de Reyna (1988) は interval t-design の存在 (Seymour-Zaslavsky の定理の特別な場合) の別証を与えた。これは 3ページの短い論文であり、トポロジー (ホモトピー論) の極く基本的なことのみを用いる。私はこの証明を使って $|X|$ を具体的に計算出来る可能性に気付き、Bajnok はそれを実行して、(ある具体的な定数 c_i $(i=1,2)$ が存在して) 任意の $n \geqq c_1 \cdot t^{9/2}$ に対して $|X|=n$ となる interval t-design X が常に存在することを証明した。従って Bajnok の前に述べた結果から、任意の $n \geqq c_2 \cdot t^{11/2}$ に対して、$|X|=n$ となる t-design X in S^2 が常に存在することがわかったわけである (Bajnok (in preparation))。

極く最近 (1989年7月) Wagner (to appear) の preprint をもらった。そこでは interval t-design の explicit な存在についての別証明を与えた。(この結果は de Reyna - Bajnok の bound よりも悪いと思われ

る。）その論文の中で、任意の $n \geq C_d \cdot t^{12d^4}$ に対して、$|X|=n$ となる t-design X in S^d が常に存在することが announce されている（ただし詳細は今の所不明である。）いずれにせよ、存在がわかっているsize $|X|$ は tight の bound よりずっと大きい。この間をどれ位埋めていけるか、また explicit な t-design がどのように構成されていくかが、今後の興味ある問題であろう。

§3. 補足

1. spherical t-design はいくらでも存在するわけであるが、では特別に興味深いのはどのようなものであろうか。私自身は rigid t-design の概念がおもしろく、その分類問題は非常に重要になると考える。（詳しくは、Bannai (1988, 1988 bis) 等を参照。）

2. sphere の中の t-design の概念は compact rank 1 symmetric space の t-design に拡張され、色々な類似の結果がそこでも証明されている。（Bannai (1988), Bannai-Hoggar (1989) 等参照。）

3. $\mathbb{R}^d$（または non-compact rank 1 symmetric

space）の有限部分集合 X の "combinatorics" は S^d の場合に比べ難かしくなる。$\mathbb{R}^d$ における t-design X をどう定義するかは、Neumaier-Seidel (1988), Delsarte-Seidel (1989) に一つの試みがある。これらはおもしろい論文であるが、まだ最終的な結果ではないと思える。ちなみに、彼らの定義は、X が "t-design in $\mathbb{R}^d$" であるとは、

$$\sum_{x\in X}(x,x)^{l}\cdot h_i(x)=0 \qquad \text{for } \forall h_i(x)\in \mathrm{Harm}(i)$$

with $2l+i\leq t$ $(i\geq 1)$ となることである。（ただし、$(x,x)=x_1^2+\cdots+x_d^2$.）

X が $\mathbb{R}^d$ の s-distance set の時、$|X|\leq\binom{d+s}{s}$ が知られている (Blokhuis (1984), Bannai-Bannai-Stanton (1983))。t-design in $\mathbb{R}^d$ の最上の定義としては、$|X|=\binom{d+s}{s}$ をみたす s-distance set X in $\mathbb{R}^d$ が $2s$-design になれば一番望ましいが、先の定義ではそれは多分喜びけないであろう。野田隆三郎氏は最近、$X\subset\mathbb{R}^d$ が $|X|=\binom{d+2}{2}$ なる 2-distance set ならば

$$\sum_{x\in X}(x,x)^{l}h_i(x)=0 \qquad \text{for } \forall h_i(x)\in \mathrm{Harm}(i)$$

with $l+i \leq 2$ $(i \geq 1)$ を示された。(これが何を意味するか、またこの結果が $\mathbb{R}^d$ における t-design の最終的な定義を見つけるのに役立つか否かは今の所不明であるが、何かの役に立つ可能性はあると思う。

文献

- B. Bajnok (1989): Construction of spherical t-designs, Ph.D. thesis, Ohio State Univ. 1989.
- ——— (to appear): Construction of spherical 4- and 5-designs, submitted to Graphs and Combinatorics.
- ——— (in preparation).
- E. Bannai (1988): On extremal finite sets in the sphere and other metric spaces, London Math. Soc. Lecture Note Series No. 131, pp 13–38.
- ——— (1988 bis): Rigid spherical t-designs and a theorem of Y. Hong, J. Fac. Sci. Univ. Tokyo 34, 485-489.
- E. Bannai - E. Bannai - D. Stanton: An upper bound for the cardinality of an s-distance set in real Euclidean space, II. Combinatorica 3 (1983), 147–152.
- E. Bannai - R.M. Damerell (1979): Tight spherical designs I,

J. Math. Soc. Japan, 31, 199-207.

- ―――――――― (1980): Tight spherical designs II. J. London Math. Soc. 21, 13-30.
- E. Bannai - S.G. Hoggar (1989): Tight t-designs and square-free integers, Europ. J. Comb. 10, 113-135.
- A. Blokhuis (1984): Few distance sets, CWI Tract 7, Math. Centrum.
- P. Delsarte - J.M. Goethals - J.J. Seidel (1977): Spherical codes and designs. Geom. Dedicata, 6, 363-388.
- P. Delsarte - J.J. Seidel (1989): Fisher type Inequalities for Euclidean t-designs, Lin Alg. and its Appl. 114/115, 213-230.
- J. A. de Reyna (1988): A generalized Mean-Value Theorem, Monatsch. Math. 106, 95-97.
- V. I. Krylov (1962): Approximate calculation of integrals, Macmillan Co.
- Y. Mimura (to appear): A construction of spherical 2-designs, to appear in Graphs and Combinatorics.
- I. P. Natanson (1965): Constructive Function Theory, Frederick Unger Publ. Company, N.Y.

- A. Neumaier - J. J. Seidel (1988): Discrete measures for spherical designs, eutactic stars and lattices, Indag. Math. 91, 321-334.
- P. Seymour - T. Zaslavsky (1984): Averaging sets: a generalization of mean values and spherical designs, Advs. in Math. 52, 213-240.
- G. Wagner (to appear): Quadrature formulas with equal weights. (preprint).

TRIANGULATIONS WITH WEIGHTED VERTICES

J.A. Hoskins, W.D. Hoskins, R.G. Stanton
Department of Computer Science
University of Manitoba
Winnipeg, Canada
R3T 2N2

Abstract. If three points A, B, C, are given in the plane, then the right bisectors of the sides of triangle ABC divide the plane up into regions that "belong" to the three vertices. If weights are attached to the vertices, then the regions obtained are bounded by circular arcs, and the conditions for intersection can be found by an application of the Heron formula for the area of a triangle. A series of diagrams illustrate various configurations obtained in some practical applications in the field of forestry.

1. Introduction. In the biological sciences, the occurrence of competition models is frequent (cf. Daniels, Burkhart, and Clason **[1]**); for a description of various different competition designs, we refer to Street and Street **[2]**). As one instance, we may take three points A, B, C, in the plane and imagine them to represent three trees that are competing for nutrients and water from the soil. If the trees are of equal size, we can reasonably postulate that they have equal attractive strengths, and it is natural to use the right bisectors of AB, AC, and BC to divide the plane up into three regions that "belong" to the three trees A, B, C; the circumcentre of triangle ABC then becomes the point at which the attractive forces of the three trees are equal. We shall look at the case when the trees are of different sizes, and consequently their attractive strengths are different; we model this situation by attaching positive weights u, v, and w, to points A, B, and C. There is no loss in generality in assuming that the points are labelled in such a way that u, v, and w are in decreasing magnitude, that is, $u \geq v \geq w > 0$.

2. Discussion of the Model. In Figure 1, the triangle ABC is arbitrary (the three vertices can be considered as representing the positions of three trees). Weights u, v, and w, are attached to the vertices A, B, and C, respectively. It is assumed that all the weights are positive and that $u \geq v \geq w$. If the co-ordinates of A, B, and C are represented by (x_1,y_1), (x_2,y_2), and (x_3,y_3), respectively, then the locus of points P_1 such that $AP_1/BP_1 = u/v$ is given by

$$v^2 [(x - x_1)^2 + (y - y_1)^2] = u^2 [(x - x_2)^2 + (y - y_2)^2].$$

This locus has the general form

$$K_1(x^2 + y^2) + K_2x + K_3y + K_4 = 0,$$

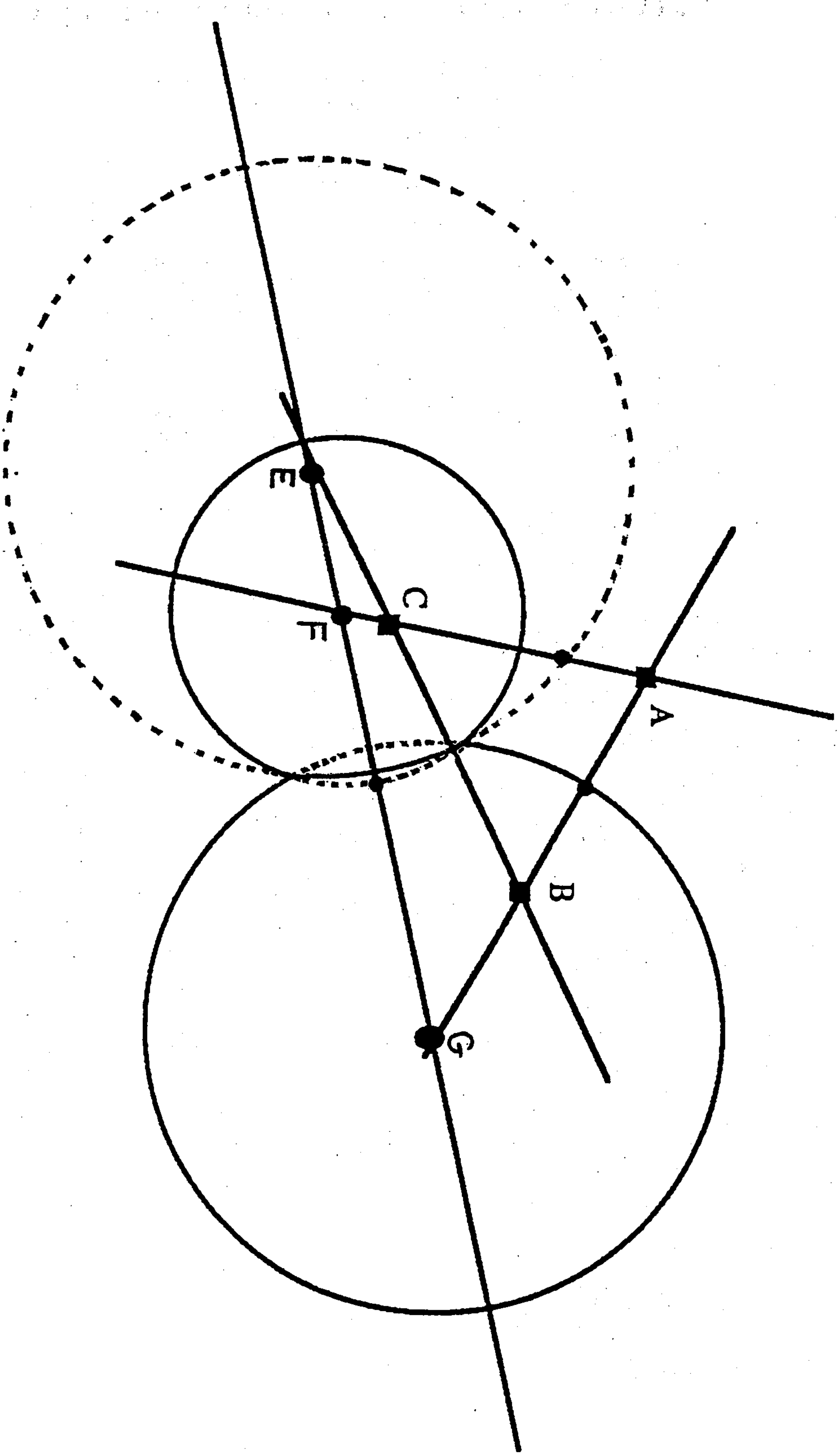


Figure 1

and hence is a circle whose centre lies on the line AB. Similarly, we find that the locus of points P_2 such that $BP_2/CP_2 = v/w$ is a circle whose centre is on the line BC and whose equation is

$$w^2 [(x - x_2)^2 + (y - y_2)^2] = v^2 [(x - x_3)^2 + (y - y_3)^2].$$

Finally, the locus of points P_3 such that $CP_3/AP_3 = w/u$ is a circle whose centre is on the line AC and whose equation is

$$u^2 [(x - x_3)^2 + (y - y_3)^2] = w^2 [(x - x_1)^2 + (y - y_1)^2].$$

These three circles are just the circles of Apollonius associated with each of the pairs of points. So we may state our first result as

Lemma 1. The loci partitioning the plane into areas belonging to A, B, and C (in the sense that the attractive forces from A, B, and C are dominant in the areas) are simply arcs of circles.

Figure 1 illustrates such a situation; the partitioning arcs are shown as solid lines, whereas the remainder of each circle is shown as a dotted arc. In this diagram, the circles intersect in two real points, that is, there are two points K such that AK : BK : CK = u : v : w (zero points of intersection and one point of contact are also possibilities)

We next note that the equations of any two of the three circle can be combined to give the other equation; this means that any points common to two of the circles also lie on the third circle. Consequently, the three circles all possess the same common chord. Since the centres of the three circles lie on the common chord, we have

Lemma 2. The centres of the three circles are all collinear.

It is interesting to note that this result can be derived in another way. If we denote the centres of the three circles by G, E, and F, respectively, then it is easy to calculate that

$$AG/GB = u^2/v^2, \quad BE/EC = v^2/w^2, \quad CF/FA = w^2/u^2.$$

It thus follows that the points G, E, and F divide the sides of the triangle in such a way that the product of AG/GB, BE/EC, and CF/FA is unity. Consequently, the Theorem of Menelaus guarantees that G, E, and F all lie upon a straight line.

It is clear that, as the ratio u : v : w approaches the ratio 1 : 1 : 1, then the circles approach circles of infinite radius (straight lines). One of the points of intersection recedes to infinity, as does the line GEF. The other point of intersection becomes the intersection of the right bisectors of the three sides, that is, the circumcentre of triangle ABC.

3. Condition for Real Intersections. Figure 1 illustrates the situation when the circles have two real points of intersection. These two points may coincide or they may be non-real. The case when the two points coincide is clearly the dividing line between the real and non-real situations. We shall now investigate the algebraic conditions for real intersections; the conditions take a particularly symmetric form if we employ the Heron formula for the area of a triangle.

First, it is useful to obtain a somewhat different form for the Heron formula; normally, this formula states that the area Δ is given by

$$\Delta^2 = s(s - a)(s - b)(s - c),$$

where a, b, c, are the lengths of the sides opposite A, B, C, respectively, and where $2s = a + b + c$. If we substitute for s, we have

$$16\Delta^2 = (a+b+c)(a+b-c)(a-b+c)(b+c-a);$$

from this form of the equation, we note that failure of the triangle inequality (that is, a negative value for one term such as a+b-c) shows up as a negative value for Δ^2 (or, equivalently, as a non-real value for Δ). Further algebra produces the alternative formula

$$16\Delta^2 = 2(a^2b^2 + a^2c^2 + b^2c^2) - a^4 - b^4 - c^4.$$

It will also be useful to introduce an auxiliary triangle whose sides are au, bv, and cw. The area of this auxilary triangle is a quantity T where

$$16T^2 = 2[(au)^2(bv)^2+(au)^2(cw)^2+(bv)^2(cw)^2] - (au)^4 - (bv)^4 - (cw)^4.$$

We now consider Figure 2, where K represents a point of intersection of the circles; then the distances AK, BK, and CK are given by ku, kv, and kw, repectively, where k is a constant of proportionality that remains to be determined. The cosine formula immediately gives us the results that

$$\cos AKB = [k^2(u^2 + v^2) - c^2]/2k^2uv,$$

$$\cos BKC = [k^2(v^2 + w^2) - a^2]/2k^2vw,$$

$$\cos CKA = [k^2(u^2 + w^2) - b^2]/2k^2uw.$$

However, the angles AKB, BKC, and CKA add to 360°, and it is well known that, for any angles P, Q, and R that add to 360°, we have the identity

$$\cos^2P + \cos^2Q + \cos^2R - 2\cos P \cos Q \cos R = 1.$$

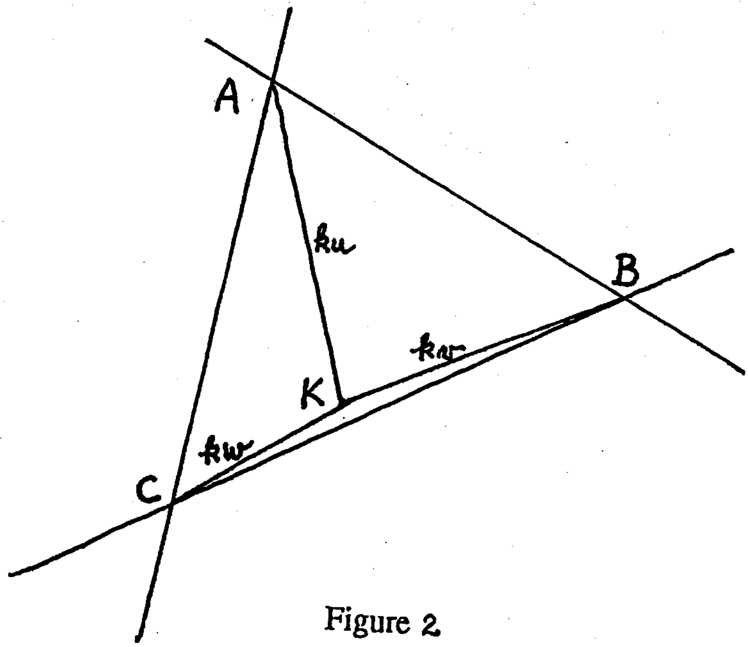


Figure 2

Substitution in this identity yields the following equation for k (all terms in k^6 cancel out):

$$k^4[a^2(u^2-v^2)(u^2-w^2)+ b^2(v^2-u^2)(v^2-w^2)+ c^2(w^2-v^2)(w^2-u^2)] +$$

$$k^2[(au)^2(a^2-b^2-c^2)+ (bv)^2(b^2-a^2-c^2)+ (cw)^2(c^2-b^2-c^2)] + (abc)^2 = 0.$$

We note that, if $u = v = w = 1$, then k simply becomes R, the circumradius of triangle ABC. The equation then reduces to

$$R^2(-16\Delta^2) + (abc)^2 = 0,$$

and this gives the familiar formula for the circumradius of the triangle, namely,

$$R = abc/4\Delta.$$

We further note that the equation is quadratic in k^2; consequently, the condition for k^2 to be real can immediately be written down as

$$[(au)^2(a^2-b^2-c^2)+ (bv)^2(b^2-a^2-c^2)+ (cw)^2(c^2-b^2-c^2)]^2 -$$

$$4(abc)^2 [a^2(u^2-v^2)(u^2-w^2)+ b^2(v^2-u^2)(v^2-w^2)+ c^2(w^2-v^2)(w^2-u^2)] \geq 0.$$

This condition simplifies to the requirement that the product of

$$\{2(a^2b^2 + a^2c^2 + b^2c^2) - a^4 - b^4 - c^4]\}$$

$$\text{and } \{2[(au)^2(bv)^2+(au)^2(cw)^2+(bv)^2(cw)^2] - (au)^4 - (bv)^4 - (cw)^4\}$$

be non-negative; thus

$$(16\Delta^2)(16T^2) \geq 0.$$

Since ABC is a given triangle, we certainly have $\Delta^2 > 0$. However, the auxiliary triangle may not be real. If the auxiliary triangle is real, then $T^2 > 0$, and the two values for k^2 correspond to the two points of intersection of the circles. If $T^2 = 0$, then there is only one point of intersection of the circles (the common chord becomes a common tangent). Finally, if $T^2 < 0$, then the auxiliary triangle ceases to be real, and the circles do not possess real points of intersection.

We thus have

Lemma 4. There are two real points of intersection of the circles if and only if the conditions

$$au + bv > cw, \quad bv + cw > au, \quad cw + au > bv,$$

are satisfied. If one of these equalities becomes an equality, then $T = 0$, and there is a single point of intersection. If any inequality is reversed, then the circles do not have real points of intersection.

We note that, if $u = v = w = 1$, then the conditions just become the ordinary triangle inequalities for the triangle ABC; these conditions are automatically satisfied and so we have the comforting result that the right bisectors of the sides of the triangle do meet in a real point.

It is also possible to deduce the result of Lemma 4 in a somewhat less symmetrical fashion. Let R_1 and R_2 be the radii of the circles with centres G and F, respectively. Then there will be real points of intersection if and only if we have the two conditions

$$(R_1 + R_2)^2 \geq (FG)^2,$$

$$(R_1 - R_2)^2 \leq (FG)^2.$$

It is easy to calculate that

$$R_1 = uvc/(u^2-v^2), \quad R_2 = uwb/(u^2-w^2).$$

Also, FG can be calculated from the cosine law for triangle AFG. After considerable algebra, these two inequalities reduce to the result already given in Lemma 4.

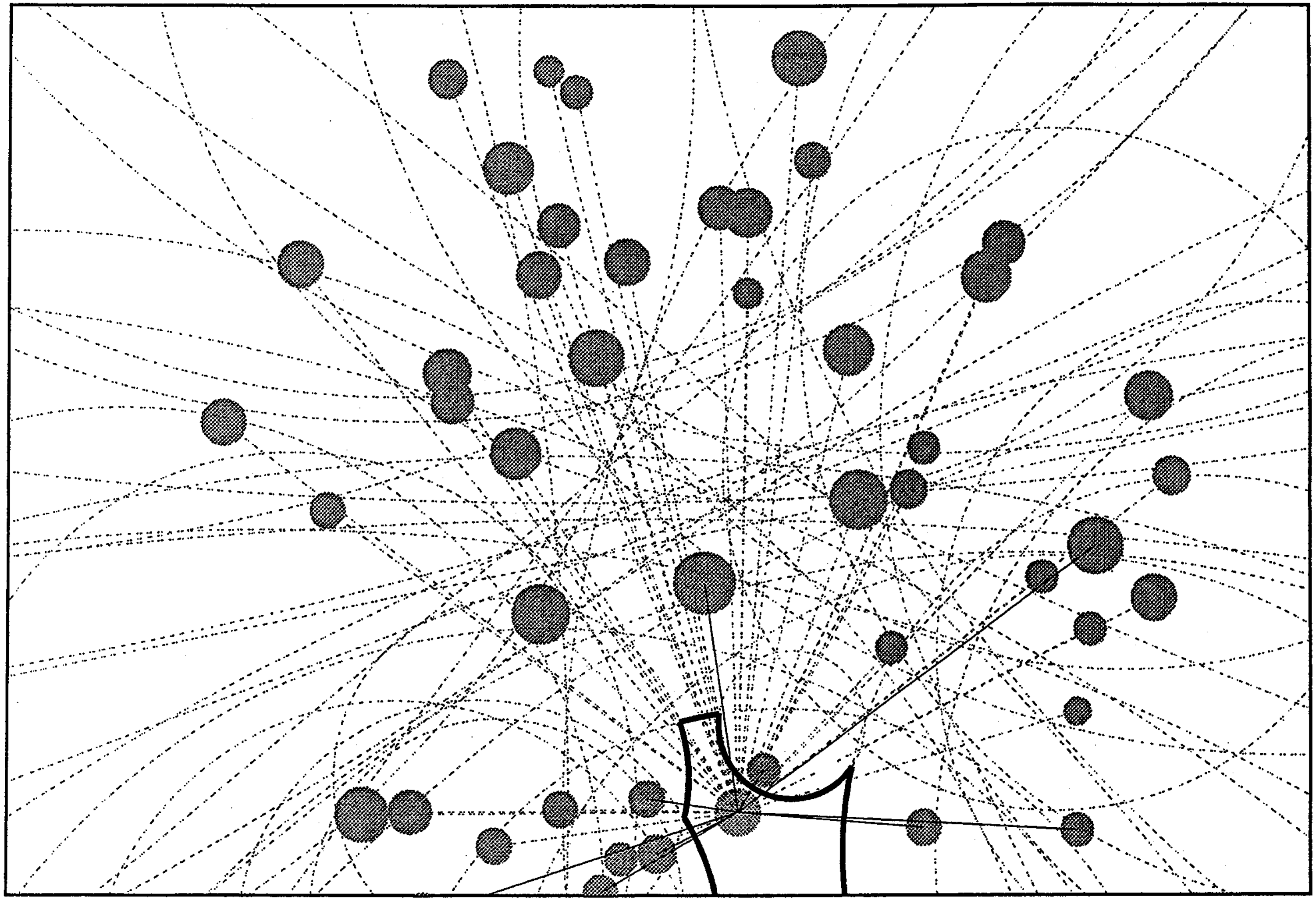
4. Conclusion. The results described in this paper have been implemented in algorithmic form, and Figures 3 to 10 show some actual results of the algorithm as applied to forest data. The values of u, v, w, are proportional to the attractive powers of the trees (these attractive powers are indicated by the size of the representing points). Figure 3 shows all the construction lines for various combinations of points, and the resulting region dominated by a single point. Figure 4 is identical with Figure 3, except that the construction lines have been eliminated and the regions associated with each point have been drawn in. Figures 5 through 10 indicate some of the different possibilities can arise when there are trees of vastly differing attractive powers (in practice, this involves trees of different sizes or ages).

5. Acknowledgment. We take this opportunity to express our gratitude to Mr Robert Chan who implemented the computer algorithm that produced Figures 3 to 10.

REFERENCES

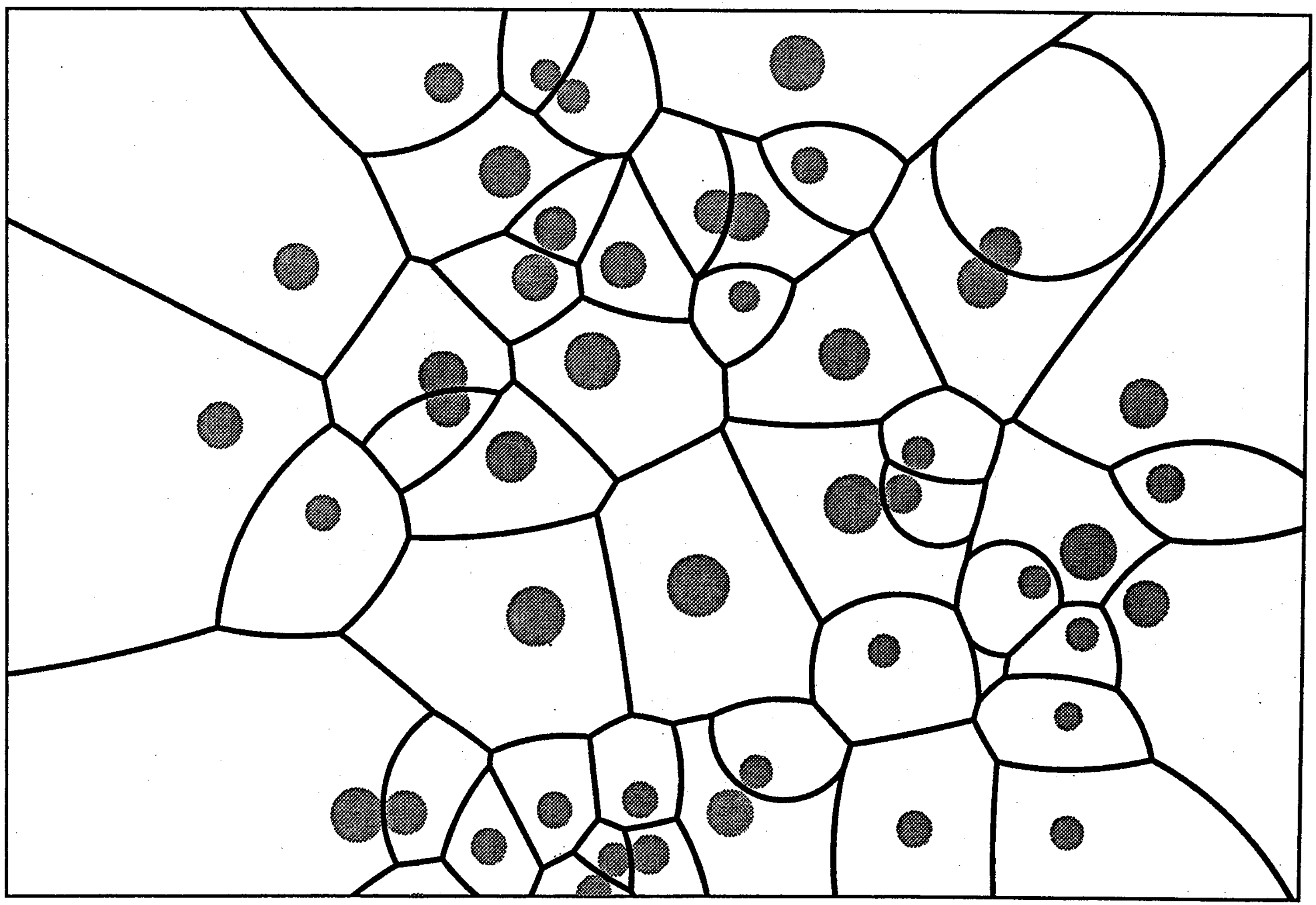
[1] R.F. Daniels, H.E. Burkhart, and T.R. Clason, *A comparison of Competition Measures for Predicting Growth of Loblolly Pine Trees*, Canadian J. of Forest Research **16** (1986), 1230-1237.

[2] A.P. Street and D.J. Street, *Combinatorics of Experimental Design*, Oxford University Press, Oxford (1986).



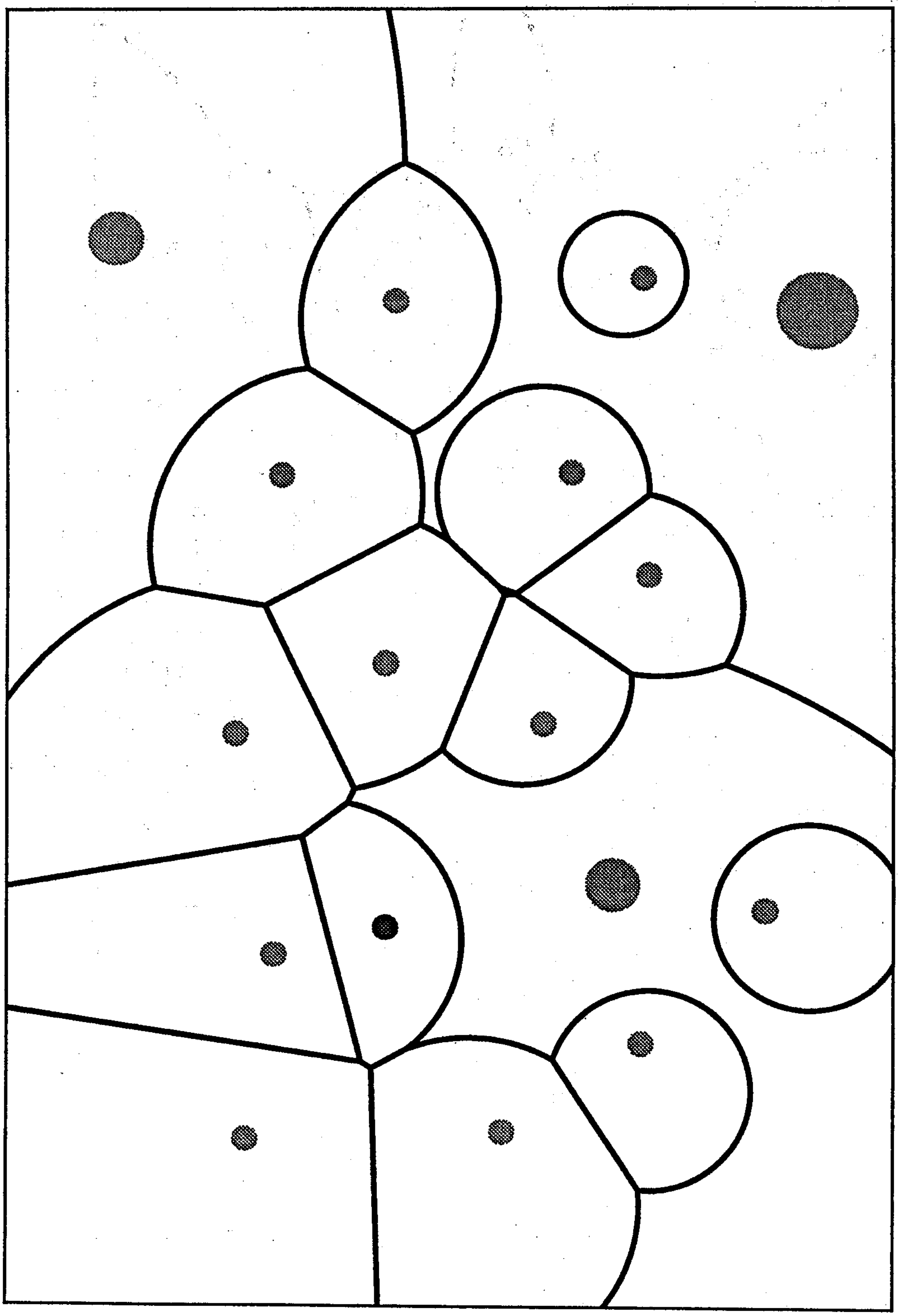
Internal:RChan:WDT Folder:Vertices Folder:a.a.78.ps.one.tile

Figure 3



Internal:RChan:WDT Folder:Vertices Folder:a.a.Vertices.78.v18.ps

Figure 4



80meg:1

Figure 5

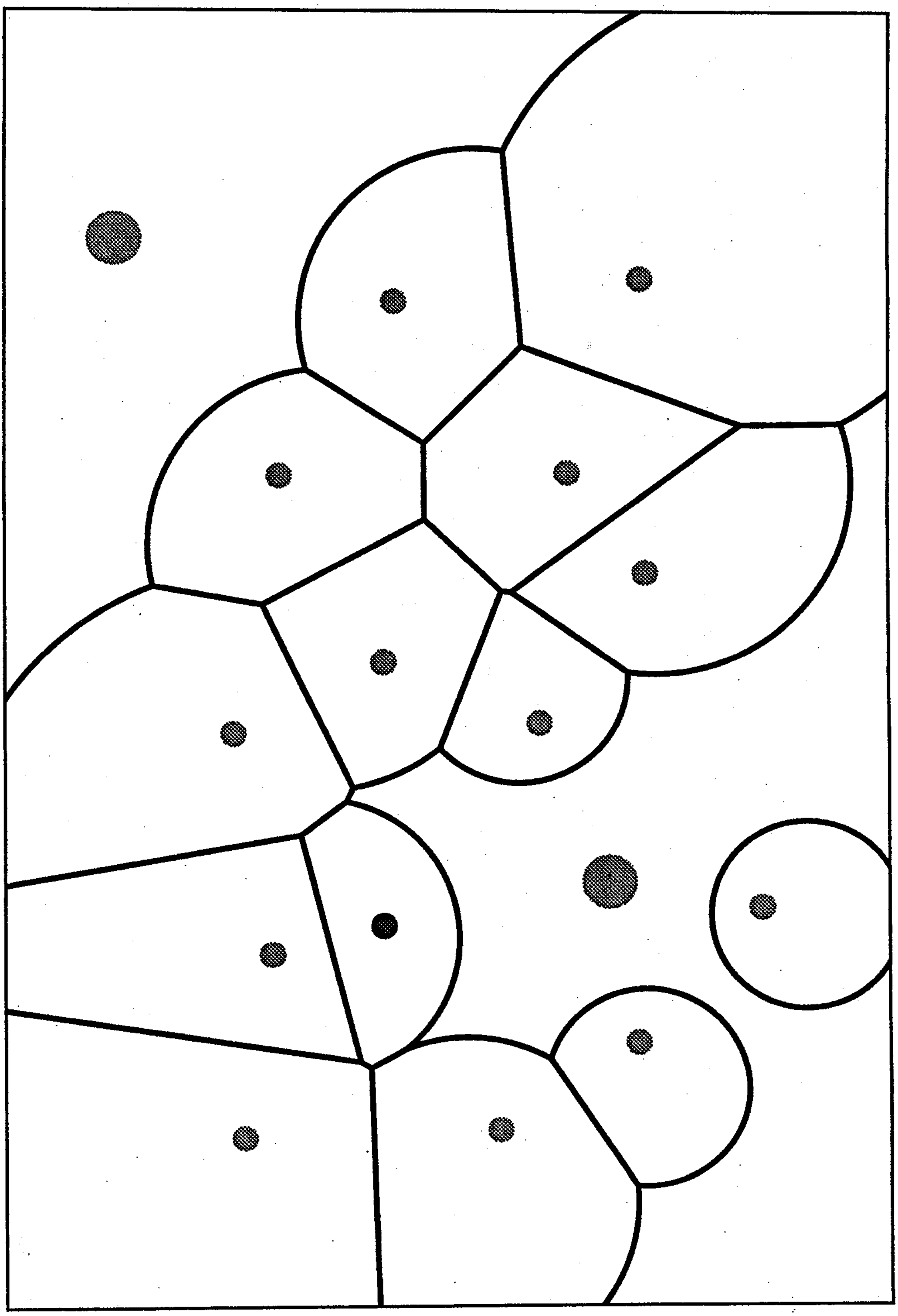


Figure 6

80meg:2

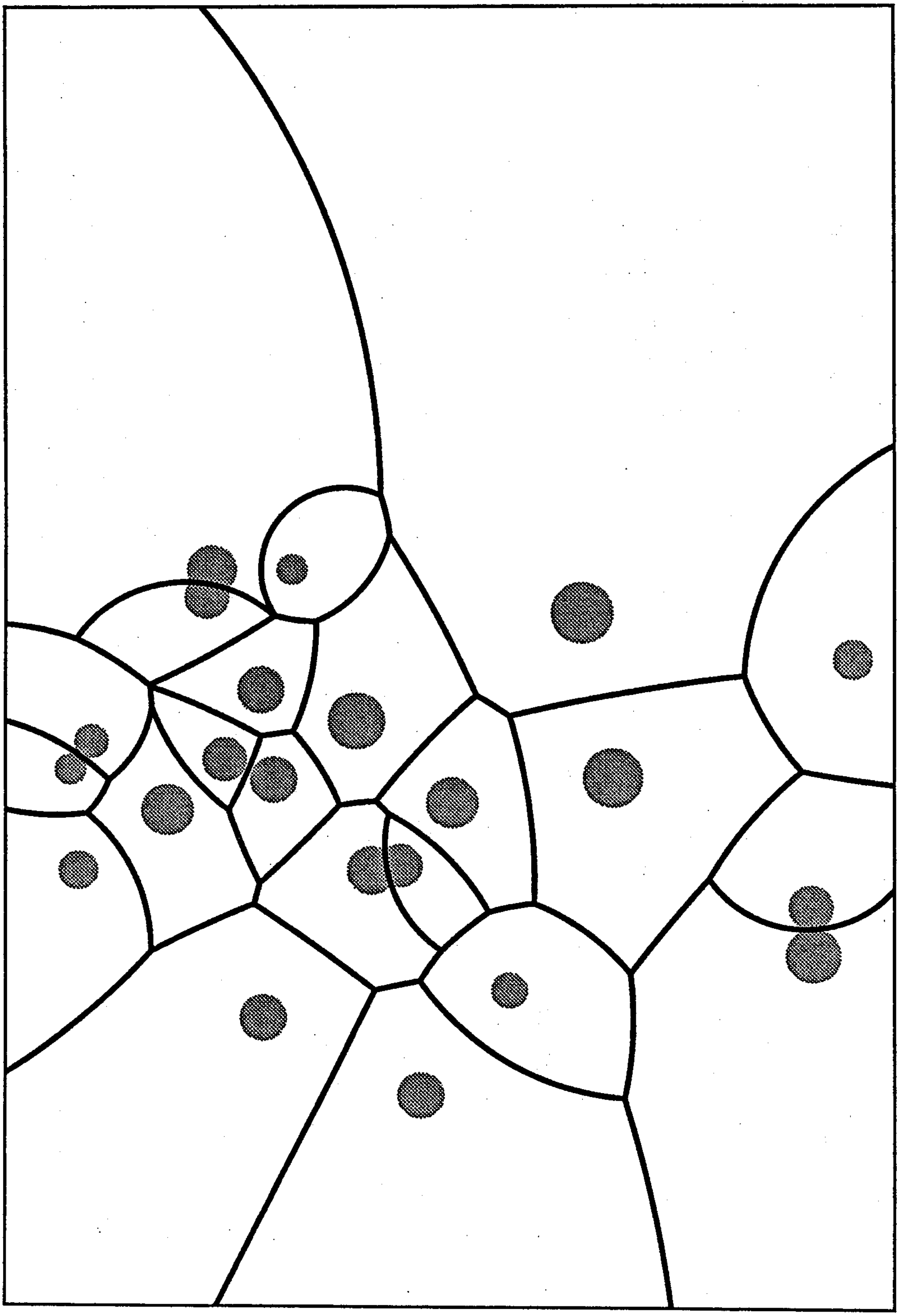
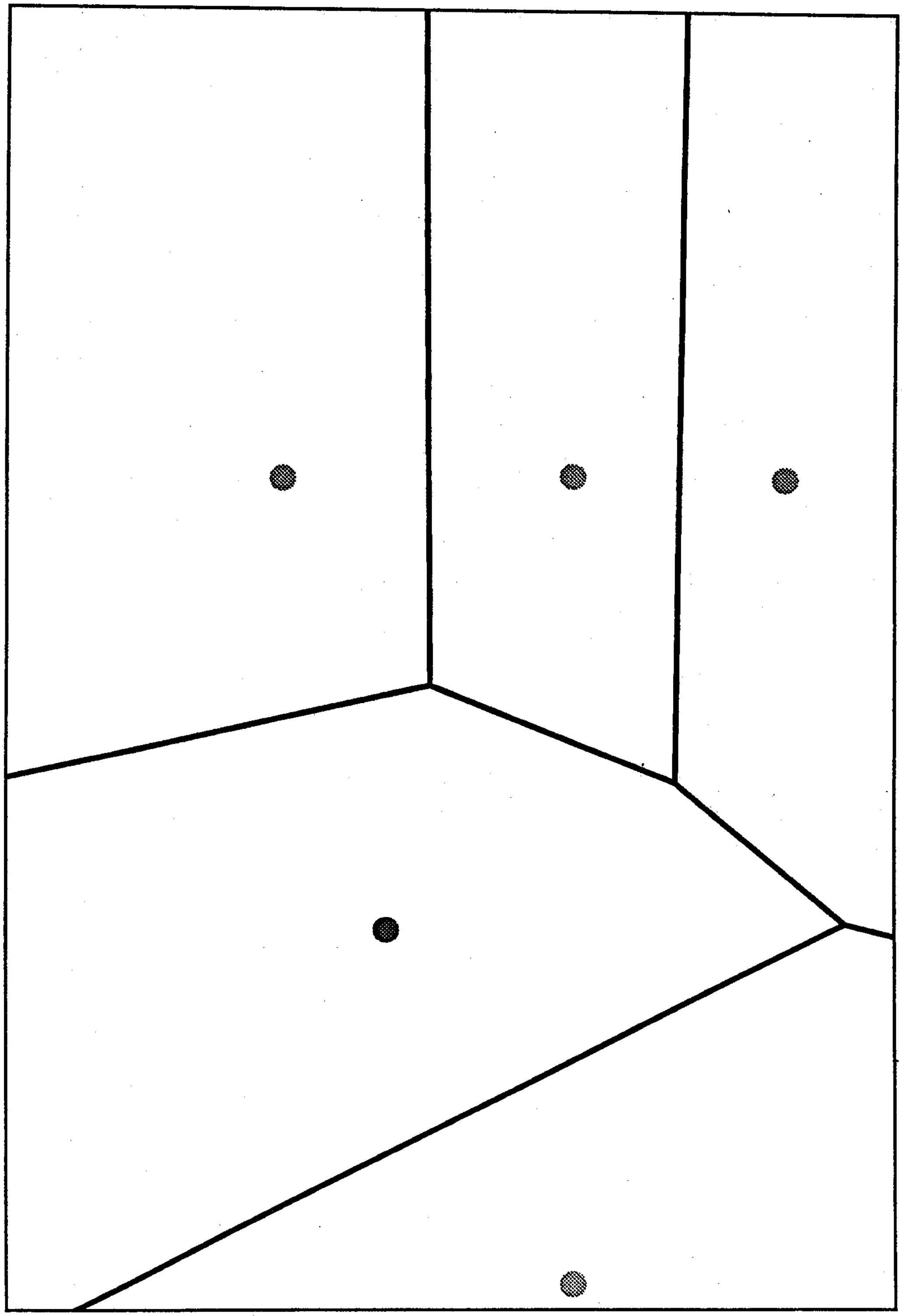


Figure 7

80meg:3



80meg:4

Figure 8

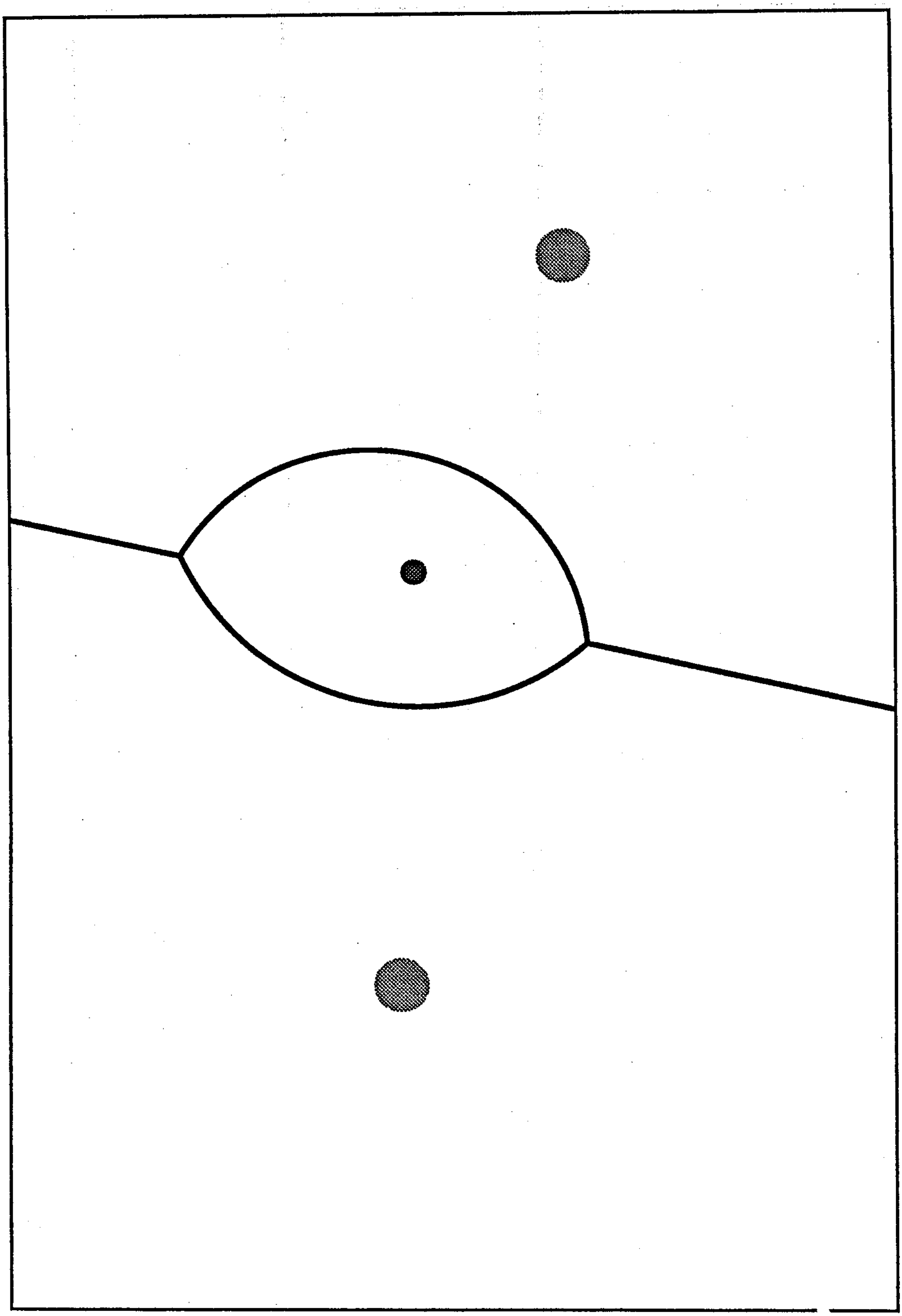
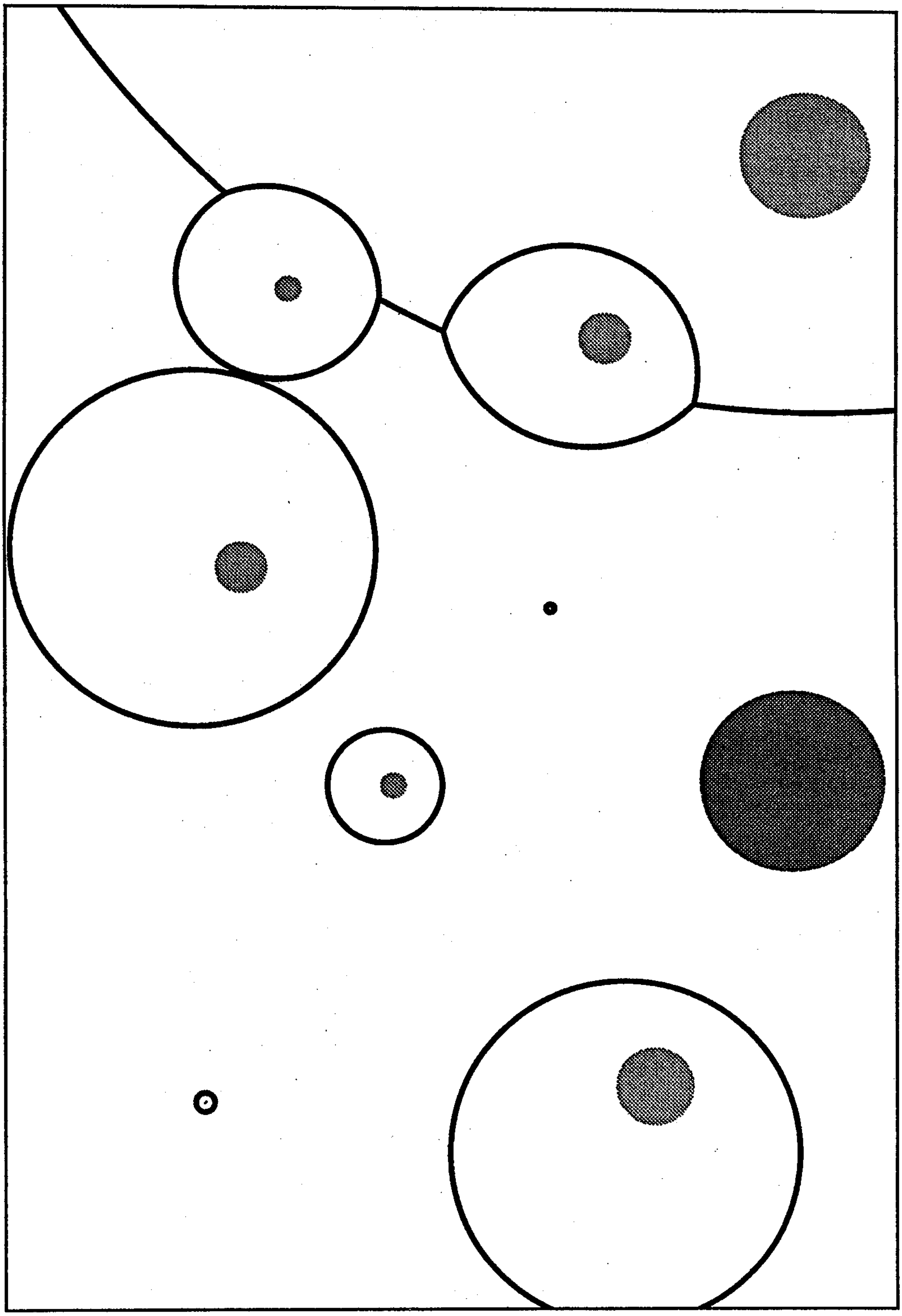


Figure 9

80meg:5



80meg: 6

Figure 10

Algebraic-geometric code on a curve

水野 弘文　電気通信大学 - 情報工学

安藤 清　日本医科大学 - 基礎科学

1. 緒言

V. D. Goppa は代数曲線論と符号理論の間の重要な関係を見い出して代数幾何符号を導入し、それ以前のすべての線形符号は射影直線を基底とする代数幾何符号とみなせることを示した[2),3)]。M. Tsfasman, S. G. Vladut, Th. Zink は Y. Ihara の結果[1)] を用いて、従来の線形符号では到達できなかった極めて性能の良い代数幾何符号の無限列を構成した[10)]。また、J. H. van Lint and T. A. Spriner[6)]、J. P. Hansen[5)]、J. Yustesen et al..[12)] 等は、具体的な平面代数曲線の上に代数幾何符号を構成し、復号法に関しても考察した。HansenはGF(2^3)上定義された Klein の4次曲線

$$X: x^3y + y^3z + z^3x = 0$$

を基底とする符号長21の代数幾何符号を構成し、その性能がBCH符号とほぼ同等であることを調べた。

ここでは、$l \equiv 3 \pmod 6$、$s = 2^l + 1$ とするとき、GF(2^{3l})上で定義された平面代数曲線

$$X_S: x^sy + y^sz + z^sx = 0$$

を基底とする代数幾何符号について報告する。この符号の構成に用いるX_sのF有理点全体に正則に作用する非可換群Gが存在し、構成された符号は群環$F[G]$のイデアルとみなせる。R. M. Tannar は同じ非可換群が作用する符号（ただし代数幾何符号ではない）を構成している。このTannarの結果やJ. Yustesen et al..

の結果についても一部紹介する。

2. 代数幾何符号

代数幾何符号について、以下で必要となる事柄を復習しておく。代数幾何符号一般についてはGoppaの文献[4]を見られたい。また水野[6]、山西[11]にその概要が紹介されている。

$F=\mathrm{GF}(q)$を位数qの有限体とし、n次元ベクトル空間F^nの部分ベクトル空間Cを符号長nの線形符号と呼ぶ。

$$x=(x_1,x_2,\ldots,x_n),\quad y=(y_1,y_2,\ldots,y_n)\in F^n$$

に対し、

$$d(x,y)=\#\{\, i \mid x_i\neq y_i \,\}$$

とおいて、F におけるHamming 距離 $d(x,y)$ を定義する。

$$d(C)=min\{d(x,y) \mid x,y\in C, x\neq y\}$$

とおいて $d(C)$ を符号 C の最小距離と呼ぶ。

$$k=\dim_F C$$

を符号Cの次元と呼ぶ。符号は雑音のある通信路における誤りを検出し、訂正することを目標とするので、与えられた符号長および次元に対して大きな最小距離を有する符号を構成することが重要である。

Xを有限体 $F=\mathrm{GF}(q)$上定義された特異点を持たないm次代数曲線とする。XはFの代数的閉包$\bar{F}$上で既約、すなわち絶対既約であるとする。Xの種数を$g(X)$であらわす。このとき

$$g(X)=\frac{(m-1)(m-2)}{2}$$

体F上定義されるX上の有理的関数全体を$F(X)$であらわす。

F上有理的な因子

$$E = m_1Q_1 + m_2Q_2 + \ldots + m_jQ_j$$

に対して

$$L(E) = \{ f \in F(X) \mid (f) \geqq -E \}$$

とおく。すなわち$L(E)$はQ_iで高々m_i位の極をもち他では正則なX上の有理的関数全体である。このとき代数曲線論で次の定理が知られている。

定理 (Riemann-Roch)　$L(E)$はF上有限次元ベクトル空間となり、その次元は

$$\dim_F L(E) = \deg E - g(X) + 1$$

で与えられる。もし$\deg(E) > 2g(X) - 2$ ならば $i(E) = 0$である。

$$E = \sum_{i=1}^{j} m_iQ_i, \qquad D = \sum_{i=1}^{n} P_i$$

をともに体F上有理的な因子とし、EとDのどの成分も互いに異なるものとする。またDの各成分P_i はX上のF-有理点でさらに

$$\deg E < \deg D = n$$

とする。ベクトル空間 $L(E)$からベクトル空間 F^nへの写像 ψを

$$\psi(f) = (f(P_1), f(P_2), \ldots, f(P_n))$$

で定義する。このとき写像 ψの像を曲線Xを底曲線とする代数幾何符号と呼び、$C(D, E; X)$とあらわす。符号$C(D, E; X)$の次元をk、最小距離をdとするとReimann - Roch の定理より

(i) $k = \dim_F L(E)$

(ii) $k \geqq \deg E - g(X) + 1$

(iii) $d \geqq n - \deg E$

が成り立つ。したがって、良いパラメータをもつ符号を構成するためにはその種数に比較して有理点の数の多い曲線を見い出す必要がある。

3. Xs上のF-有理点

lを$l\equiv 3\pmod 6$を満たす整数、$s=2^l+1$、$F=\mathrm{GF}(2^{3l})$とおく。体F上で

$$X_s : x^s y + y^s z + z^s x = 0$$

定義される平面代数曲線

$$g(X_s) = \frac{s(s-1)}{2} = 2^{l-1}(2^l+1)$$

を考えよう。X_sは種数

をもち、 絶対既約で特異点をもたない曲線である。

$$Q_0=[1:0:0],\quad Q_1=[0:1:0],\quad Q_2=[0:0:1]$$

は任意のsについてX_sのF-有理点になるので、これらを自明な有理点と呼ぶ。X_sの自明でないF-有理点全体を$R(X_s, F)$であらわす。

2次射影線形群をPGL(2;F)であらわす。βを$\beta^3+\beta+1=0$を満たすGF(2^3)の原始元とし

$$t=\frac{2^{3l}-1}{2^3-1}$$

とおく。さらに$\alpha^t=\beta$を満たすFの原始元αを1つとり固定する。 $u=2^{2l}$, $v=2^l$とおき, PGL(2;F)の2元a, bを

$$a=\begin{pmatrix}\alpha & 0 & 0\\ 0 & \alpha^u & 0\\ 0 & 0 & \alpha^v\end{pmatrix},\qquad b=\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}$$

と定義する。このとき

$$K=\langle a,\ b\rangle\subset PGL(2,F)$$

とおけばKはX_sに作用し、その位数は$3(2^{2l}+2^l+1)$である。

$r=(2^{2l}+2^l+1)$とおく。Kは基本関係式$a^r=1, b^3=1, ab=b^v a$をもつ有限非可換群である。Fの0以外の元のつくる乗法群の位数rの部分群をUとする。このとき、次の定理が成り立つ。すなわち

定理 $x^s+x+1=0$がUの生成元をその根にもてば、

$$\#R(Xs, F) \geqq r(l+2).$$

定理の証明には先に構成した群Kを用いる。その詳細は水野,安藤[8]を見られたい。

4. X_S上の代数幾何符号

前節の定理により得られるXsのF有理点を

$$\{P_i \mid i=0, 1, \ldots, 3(l+2)(2^{2l}+2^l+1)\}$$

とおく。

mを $\dfrac{2^{l-1}(2^l-1)}{3} < m < \dfrac{n}{3}$ を満たす整数とする。

Xsの正因子として

$$D=\sum_{i=1}^{3(l+2)(2^{2l}+2^l+1)} P_i, \qquad E=m(Q_0+Q_1+Q_2)$$

をとり、X_s上の代数幾何符号$C=C(D, E; Xs)$を考える。Cの符号長は

$$\deg D=n$$

である。Cの次元をk、最小距離をdとおくと、

(i) $n=3(l+2)(2^{2l}+2^l+1)$,

(ii) $k \geqq 3m-2^{l-1}(2^l+1)+1$,

(iii) $d \geqq n-3m$

が成立する。

例 $l=3$ の場合。

このとき、$s=9$、$F=GF(2^9)$、$g(X_s)=36$、$r=73$、$|K|=219$ となる。α を $\alpha^9+\alpha^4+1=0$ を満たすGF(2^9)の原始元とする。このとき、$\xi=\alpha^{119}$ は $\xi^9+\xi+1=0$ を満たすUの生成元である。定理よりX_9上には1095点のF-有理点が存在する。

これらの有理点を用いて $36 \leqq m \leqq 394$ なる整数mについて、

(i) $n = 1095$,

(ii) $k \geqq 3m - 35$,

(iii) $d \geqq n - 3m$

なる GF(2^9)上の符号が構成される。

5. Yustesen達の代数幾何符号とTannerの符号

この節ではYustesen達の代数幾何符号とTannerの符号について簡単に紹介する。

まず、Yustesen達の代数幾何符号の定義を述べよう。

$F=GF(q)$を有限体、Xをm次代数曲線、$\{P_1,...,P_n\}$をX上のF-有理点の集合とする。jを$j<q$なる整数とするとき、j 次同次多項式全体と$\{0\}$からなるF上のベクトル空間をV_jであらわす。曲線Xを基底とする符号長n の2つの線形符号GおよびHを

$$G_X(j)=\{f(P_1), f(P_2), ..., f(P_n) \mid f \in V_j\},$$

$$H_X(j)=G_X(j)^{\perp}$$

で定義する。これらがYustesen達の代数幾何符号である。

$G_X(j)$ の次元を$k(G)$、最小距離を$d(G)$とおくと、代数曲線論のBezoutの定理より、$n>mj$ なるm について

$$k(G)=\begin{cases} \binom{j+2}{2} & j<m \\ \binom{j+2}{2}-\binom{j-m+2}{2} & j\geq m \end{cases}$$

$$d(G) \geqq n - mj,$$

が成り立つ。

その定義より$H_X(j)$の次元$k(H)$は$k(H) = n - k(G)$。よってXが非特異でかつ$j \geqq m$ ならば

$$k(H) = mj - g(X) + 1$$

$H_X(j)$の最小距離$d(H)$については、Xが非特異、$n > mj$、$j \geqq m - 2$の条件もとにRiemann-Rochの定理から

$$d(H) \geqq mj - 2g(X) + 1$$

が成り立つ。

また彼等は1変数多項式から出発する方法で素数pと正整数rにたいして、$(p^{3r} - 1)(p^{2r} - 1)$点のGF(p^{6r})-有理点をもつ曲線の族

$$x^{p^r - 1} z^{p^{2r} - 1} - z^{p^r - 1} y^{p^{2r} - 1} + x^{p^{2r} - 1} y^{p^r - 1} = 0$$

を得ることに成功した。

一方Tannerは群の作用する線形符号について研究し、新しい線形符号を構成した(代数曲線上の符号ではない)。nを正整数、j、qをnと互いに素な数とする。Z_nの置換$i \rightarrow i+j$、$i \rightarrow qi$をそれぞれA、Mであらわし、A、Mで生成される群

$$\langle A, M \rangle$$

を考える。Tanner はこの群の作用する符号長nのGF(q)上の符号を調べ、多くの線形符号を構成した。彼の符号の中には、例えば、符号長315、次元271、最小距離 11なるパラメータを有するものもある。

Yustesen達やTannerはともに復号に関しても考察している。詳細については文献9), 12)を参照されたい。

参　考　文　献

1) Ihara, Y. : "Some remarks on the number of rational points of algebraic curves

over finite fields", *J. Fac. Sci. Tokyo*, 28, 721 - 729 (1982).

2) Goppa, V. D. : "Codes on Algebraic Curves", *Soviet Math. Dokl.*, 24, 170 - 172 (1981).

3) Goppa, V. D. : "Algebraico-Geometric Codes", *Math. USSR Isvestia*, 21, 75 - 90 (1981).

4) Goppa, V. D. : *Geometry and Codes*, Kluwer Academic Publishers, 1988.

5) Hansen, J. P. : "Codes on the Klein quatric, Ideals and Decoding", *IEEE Trans. Inf. Theory.* IT - 33, 923 - 925 (December 1984).

6) van Lint, J. H. and Springer, T. A. : "Generalized Reed-Solomon codes from algebraic geometry", IEEE Trans. Inf. Theory. IT - 33, no. 3, 305 - 310, (1987).

7) 水野 弘文 : " 符号理論と代数", 数理科学, No. 273, (1986).

8) 水野 弘文, 安藤 清 : " 曲線 $X_S : x^Sy + y^Sz + z^Sx = 0$ 上の代数幾何符号" 電気通信大学紀要 2 巻 2 号 (1989) 掲載予定.

9) Tanner, R. M., : "A Transform Theory for a Class of Group-Invariant Codes", *IEEE, Trans. Inf. Theory*, Vol. 34, No. 4, (July 1988).

10) Tsfasman, M., Vladut, S. G. and Zink, Th. : "Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound", *Math. Nachr*, 109, 21 - 28, (1982).

11) 山西 健司 : "代数幾何符号理論", 数理科学, No. 303, (1988).

12) Yustesen, J., Larsen, K. J., Jensen, H. E., Havemose, A. and Hoholdt, T. : "Construction and Decoding of a class of Algebraic Geometry Codes", *IEEE, Trans. Inf. Theory*, Vol. 35, No. 4, (July 1989).

Construction of Even Unimodular Lattices from Self-Dual Codes over Finite Fields

弘前大理 小関 道夫 Michio Ozeki

Dec.1,1989

1 Self-dual Code over a Finite Field

Let p be a prime and $\mathbf{F}_p = GF(p)$ the field of p elements. Let $V = \mathbf{F}_p^n$ be the vector space of dimension n over $\mathbf{F}_p$. A linear $[n, k]$ code $\mathbf{C}$ is a vector subspace V of dimension k. In V, the inner product, which is denoted by $(\mathbf{x}, \mathbf{y})$ for $\mathbf{x}$, $\mathbf{y}$ in V, is defined as usual. The dual code $\mathbf{C}^{\perp}$ of $\mathbf{C}$ is defined by

$$\mathbf{C}^{\perp} = \{\mathbf{u} \in V \mid (\mathbf{u}, \mathbf{v}) = 0 \, \forall \mathbf{v} \in \mathbf{C}\}.$$

The code $\mathbf{C}$ is called self-orthogonal $\Longleftrightarrow$ $\mathbf{C} \subseteq \mathbf{C}^{\perp}$.
The code $\mathbf{C}$ is called self-dual $\Longleftrightarrow$ $\mathbf{C} = \mathbf{C}^{\perp}$.

2 Complete Weight Enumerator

Let $X_0, X_1, \cdots, X_{p-1}$ be independent variables, then the complete weight enumerator $W_{\mathbf{C}}(X_0, X_1, \cdots, X_{p-1})$ of $\mathbf{C}$ is defined by

$$\begin{aligned} &W_{\mathbf{C}}(X_0, X_1, \cdots, X_{p-1}) \\ &\quad = \sum_{\mathbf{v} \in \mathbf{C}} X_0^{n_0(\mathbf{v})} X_1^{n_1(\mathbf{v})} \cdots X_{p-1}^{n_{p-1}(\mathbf{v})}, \end{aligned}$$

where $n_i(\mathbf{v})$ is the number of the coordinates v_j of the codeword $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ such that $v_j \equiv i \pmod{p}$. Obviously we have

$$n_0(\mathbf{v}) + n_1(\mathbf{v}) + \cdots + n_{p-1}(\mathbf{v}) = n$$

and

$$n_0(\mathbf{v}) + 2^2 n_1(\mathbf{v}) + \cdots + (p-1)^2 n_{p-1}(\mathbf{v}) \equiv 0 \pmod{p}.$$

The last congruence comes from the fact $(\mathbf{v},\mathbf{v}) = 0$ for $\mathbf{v} \in \mathbf{C} = \mathbf{C}^{\perp}$. The polynomial $W_{\mathbf{C}}(X_0, X_1, \cdots, X_{p-1})$ can be rewritten as

$$\begin{aligned} &W_{\mathbf{C}}(X_0, X_1, \cdots, X_{p-1}) \\ &= \sum_{n_0+n_1+\cdots+n_{p-1}=n} A(n_0, n_1, \cdots, n_{p-1}) X_0^{n_0} X_1^{n_1} \cdots X_{p-1}^{n_{p-1}}, \end{aligned}$$

where $A(n_0, n_1, \cdots, n_{p-1})$ is the number of codewords $\mathbf{v}$ in $\mathbf{C}$ such that

$$n_0(\mathbf{v}) = n_0, n_1(\mathbf{v}) = n_1, \cdots, n_{p-1}(\mathbf{v}) = n_{p-1}.$$

The cases where we have clear description of $W_{\mathbf{C}}(X_0, X_1, \cdots, X_{p-1})$, are $p = 2$ and $p = 3$ (Conf.[4],[5], and [6]). A rather unsatisfactory description of the complete weight enumerator for $p = 5$ is given in [7].

3 Construction of Even Unimodular Lattices from Codes over $GF(p)$

Let $\mathbf{C}$ be a self-dual $[2m, m]$ code over $\mathbf{F}_p$. We take vectors $\omega_1, \omega_2, \cdots, \omega_{2m} \in \mathbf{R}^{2m}$ so that

$$(\omega_i, \omega_j) = p\delta_{ij}.$$

holds.
We form a lattice M by

$$M = [\pm\omega_i \pm \omega_j]_{\mathbf{Z}}$$

Note that M is even integral and $d(M) = 2^2 p^{2m}$. Put $M^{\sharp} = \{\mathbf{z} \in \mathbf{R}^{2m} \mid (\mathbf{x},\mathbf{z}) \in \mathbf{Z} \ \ \forall \mathbf{x} \in M\}$. $M^{\sharp}$ is the dual lattice of M and it satisfies

$$index[M^{\sharp} : M] = 2^2 p^{2m}.$$

Let $\mathbf{v}_i = (v_{i1}, v_{i2}, \cdots, v_{i2m})$ $(1 \le i \le m)$ be a basis of $\mathbf{C}$. From $\mathbf{v}_i$ we define vectors $\mathbf{y}_i$ in a following manner :

$$\mathbf{y}_i = \frac{1}{p}\sum_{j=1}^{2m} b_{ij}\omega_j \qquad (1 \le i \le m),$$

where b_{ij} are integers satisfying

$$b_{ij} \bmod p = v_{ij}.$$

We put

$$J = M + \mathbf{Z}\mathbf{y}_1 + \mathbf{Z}\mathbf{y}_2 + \cdots + \mathbf{Z}\mathbf{y}_m.$$

It can be verified that J is an integral lattice. By taking b_{ij}'s suitably, we can make J to be even (by adjusting $(\mathbf{y}_i, \mathbf{y}_i) \equiv 0 \bmod 2$). A general element $\mathbf{y}$ of J is expressed as

$$\mathbf{y} = \mathbf{u} + \sum_{i=1}^{m} a_i \mathbf{y}_i \qquad a_i \in \mathbf{Z}, \mathbf{u} \in M.$$

$supp(\mathbf{y})$ is a vector in $\mathbf{F}_p^{2m}$ defined by

$$supp(\mathbf{y}) = \sum_{i=1}^{m} \bar{a}_i \mathbf{v}_i \quad ,$$

where

$$\bar{a}_i = a_i \bmod p.$$

We can prove that the mapping

$$\varphi : \mathbf{y} \mapsto supp(\mathbf{y})$$

defines a linear mapping from J to $\mathbf{C}$ and the kernel of φ is M. Therefore

$$J/M \simeq \mathbf{C}.$$

In particular, we have

$$[J : M] = \mid \mathbf{C} \mid = p^m.$$

At this stage we know that

$$M^{\prime} \supset J^{\prime} \supset J \supset M$$

and

$$[M^{\prime} : M] = [M^{\prime} : J^{\prime}][J^{\prime} : J][J : M] = 2^2 p^{2m}.$$

Since $[M^{\prime} : J^{\prime}] = [J : M] = p^m$, we have

$$[J^{\prime} : J] = 2^2.$$

If we choose $\mathbf{y}_0 \in J^{\prime} - J$ with $(\mathbf{y}_0, \mathbf{y}_0) \equiv 0 \bmod 2$ and form a lattice L:

$$L = J + \mathbf{Z}\mathbf{y}_0 \quad ,$$

then L is an even unimodular lattice.

4 Special Topics

The Gosset lattice E_8 has many representations. It is a well-known fact that E_8 is constructed from the Hamming binary $[8,4,4]$ code. Here we give several constructions of E_8 from other codes over $GF(p)$ $(p \geq 3)$.

$\star(T)$ Ternary code construction of E_8.

$$\mathbf{C} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \end{pmatrix}.$$

$\mathbf{C}$ is a generator matrix of a self-dual $[8,4]$ code over $GF(3)$. Let ω_i $(1 \leq i \leq 8)$ be vectors in $\mathbf{R}^8$ s.t. $(\omega_i, \omega_j) = 3\delta_{ij}$ and $M = [\pm\omega_i \pm \omega_j]_{\mathbf{Z}}$. Representatives $\mathbf{y}_1$, $\mathbf{y}_2$, $\mathbf{y}_3$ and $\mathbf{y}_4$ of J/M are

$$\mathbf{y}_1 = \frac{1}{3}(\omega_1 + \omega_2 - 2\omega_3), \mathbf{y}_2 = \frac{1}{3}(\omega_2 - \omega_3 - 2\omega_4)$$
$$\mathbf{y}_3 = \frac{1}{3}(\omega_5 + \omega_6 - 2\omega_7), \mathbf{y}_4 = \frac{1}{3}(\omega_6 - \omega_7 - 2\omega_8)$$
$$\mathbf{y}_0 = \frac{1}{6}(\omega_1 + \omega_2 + \omega_3 - 3\omega_4 + \omega_5 + \omega_6 + \omega_7 - 3\omega_8)$$
$$E_8 = J + \mathbf{Z}\mathbf{y}_0, 2\mathbf{y}_0 \in J, \mathbf{y}_0 \notin J.$$

$\star(Q)$ Quinary code construction of E_8.

$$\mathbf{C} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 4 & 4 \\ 0 & 0 & 1 & 0 & 1 & 4 & 1 & 4 \\ 0 & 0 & 0 & 1 & 1 & 4 & 4 & 1 \end{pmatrix}.$$

$\mathbf{C}$ is a generator matrix of a self-dual $[8,4]$ code over $GF(5)$. Let ω_i $(1 \leq i \leq 8)$ be vectors in $\mathbf{R}^8$ s.t. $(\omega_i, \omega_j) = 5\delta_{ij}$ and $M = [\pm\omega_i \pm \omega_j]_{\mathbf{Z}}$. Representatives $\mathbf{y}_1$, $\mathbf{y}_2$, $\mathbf{y}_3$ and $\mathbf{y}_4$ of J/M are

$$\mathbf{y}_1 = \frac{1}{5}(\omega_1 + \omega_5 + \omega_6 + \omega_7 - 4\omega_8), \mathbf{y}_2 = \frac{1}{5}(\omega_2 + \omega_5 + \omega_6 + 4\omega_7 - \omega_8)$$
$$\mathbf{y}_3 = \frac{1}{5}(\omega_3 + \omega_5 + 4\omega_6 + \omega_7 - \omega_8), \mathbf{y}_4 = \frac{1}{5}(\omega_4 - 4\omega_5 - \omega_6 - \omega_7 + \omega_8)$$

$$\mathbf{y}_0 = \frac{1}{10}(\omega_1 + \omega_2 - \omega_3 + \omega_4 - 3\omega_5 - 3\omega_6 + 3\omega_7 - 3\omega_8)$$

$$E_8 = J + \mathbf{Z}\mathbf{y}_0, 2\mathbf{y}_0 \in J, \mathbf{y}_0 \notin J$$

$\star(S)$ Septenary code construction of E_8.

$$\mathbf{C} = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 2 & 3 \\ 1 & 0 & 1 & 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 1 & 6 & 3 & 0 & 1 & 6 \end{pmatrix}.$$

$\mathbf{C}$ is a generator matrix of a self-dual $[8,4]$ code over $GF(7)$. Let ω_i $(1 \le i \le 8)$ be vectors in $\mathbf{R}^8$ s.t. $(\omega_i, \omega_j) = 7\delta_{ij}$ and $M = [\pm\omega_i \pm \omega_j]_{\mathbf{Z}}$. Representatives $\mathbf{y}_1$, $\mathbf{y}_2$, $\mathbf{y}_3$ and $\mathbf{y}_4$ of J/M are

$$\mathbf{y}_1 = \frac{1}{7}(\omega_1 + 2\omega_5 + 3\omega_6), \mathbf{y}_2 = \frac{1}{7}(\omega_2 + 2\omega_7 + 3\omega_8)$$

$$\mathbf{y}_3 = \frac{1}{7}(\omega_1 + \omega_3 + \omega_4 - 5\omega_6), \mathbf{y}_4 = \frac{1}{7}(\omega_1 + \omega_2 - \omega_4 + 3\omega_5 + \omega_7 - \omega_8)$$

$$\mathbf{y}_0 = \frac{1}{14}(-2\omega_1 + 2\omega_2 - 4\omega_3 + 2\omega_4 - 2\omega_5 + 2\omega_6 - 4\omega_7 + 2\omega_8)$$

$$E_8 = J + \mathbf{Z}\mathbf{y}_0, 2\mathbf{y}_0 \in J, \mathbf{y}_0 \notin J$$

$\star(11)$ $GF(11)$ code construction of E_8.

$$\mathbf{C} = \begin{pmatrix} 1 & 1 & 3 & 0 & 0 & 0 & 0 & 0 \\ 3 & 8 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 & 8 & 0 & 2 \end{pmatrix}.$$

$\mathbf{C}$ is a generator matrix of a self-dual $[8,4]$ code over $GF(11)$. Let ω_i $(1 \le i \le 8)$ be vectors in $\mathbf{R}^8$ s.t. $(\omega_i, \omega_j) = 7\delta_{ij}$ and $M = [\pm\omega_i \pm \omega_j]_{\mathbf{Z}}$. Representatives $\mathbf{y}_1$, $\mathbf{y}_2$, $\mathbf{y}_3$ and $\mathbf{y}_4$ of J/M are

$$\mathbf{y}_1 = \frac{1}{11}(\omega_1 + \omega_2 - 8\omega_3), \mathbf{y}_2 = \frac{1}{11}(3\omega_1 - 3\omega_2 + 2\omega_4)$$

$$\mathbf{y}_3 = \frac{1}{11}(\omega_5 + \omega_3 + \omega_6 - 8\omega_7), \mathbf{y}_4 = \frac{1}{11}(3\omega_5 - 3\omega_6 + 2\omega_8)$$

$$\mathbf{y}_0 = \frac{1}{11}(2\omega_1 - \omega_2 - 4\omega_3 + \omega_4 + 2\omega_5 - \omega_6 - 4\omega_7 + \omega_8)$$

$$E_8 = J + \mathbf{Z}\mathbf{y}_0, 2\mathbf{y}_0 \in J, \mathbf{y}_0 \notin J$$

It may be possible that E_8 can be constructed from a self-dual $[8,4]$ code over arbitrary finite field.

$\star(T)$ Ternary code construction of the Leech lattice

Let $\mathbf{C} = [I_{12}H_{12}]$ be a generator matrix of the Pless code P_{24}, where $H_{12} = (h_{ij})$ $(1 \leq i,j \leq 12)$ is a Paley type matrix of order 12 viewed as the matrix over $GH(3)$. Let ω_i $(1 \leq i \leq 24)$ be vectors in $\mathbf{R}^{24}$ s.t. $(\omega_i, \omega_j) = 3\delta_{ij}$ and $M = [\pm\omega_i \pm \omega_j]_{\mathbf{Z}}$. Representatives $\mathbf{x}_i$ $(1 \leq i \leq 24)$ of J/M are given by

$$\mathbf{x}_i = \frac{1}{3}(\omega_i + \sum_{j=1}^{12} a_{ij}\omega_{j+12}),$$

where a_{ij} are 0,1,-1 according as h_{ij} are 0,1,2 respectively. Put

$$\mathbf{x}_0 = \frac{1}{6}(\sum_{j=1}^{23} \omega_j - 5\omega_{24}),$$

$$Leech = J + \mathbf{Z}\mathbf{x}_0, \ 2\mathbf{x}_0 \in J, \ \mathbf{x}_0 \notin J$$

There also is a quinary code construction of the Leech lattice (c.f.[10]).

The code construction on the general finite fields in our sense may play an important role in the theory of quadratic forms. To glimpse this we show some illustrating examples.

(I) An even unimodular lattice of rank n is called extremal if the minimal vectors of L is a 2k-vector (i.e. a vector $\mathbf{x}$ satisfying $(\mathbf{x},\mathbf{x}) = 2k$) with $2k = 2[\frac{n}{24}] + 2$. Here we give a small table of results.

rank n extremal lattice	8	16	24	32	40	48	56	64
	B	B	B	B	B			
	T	T	T*	T†	T†	T*	T†	T†
	Q	Q	Q	?	?	?	?	
	S	S	?	?	?	?	?	

B: it admits binary code construction
T: it admits ternary code construction
Q: it admits quinary code construction
S: it admits septenary code construction
* : it is found by Leech-Sloane ([2]).
† : it is found by Ozeki ([9]).

Remark : The places which are marked "?" are not examined.

(II)24-dimensional Niemeier lattices

D_{24}	B T	$A_{15}D_9$	T	E_8^3	B T	$A_9^2D_6$	T
E_8D_{16}	B T	$A_7^2D_5^2$	T	D_{12}^2	B T	$A_5^4D_4$	T
D_8^3	B T	A_4^6	T?	A_8^3	T?	A_1^{24}	B T
D_4^6	B T	A_6^4	T?	A_2^{12}	T	A_3^8	T
D_6^4	B T	$A_{11}D_7E_6$	T	E_6^4	T?	$A_{17}E_7$	T
A_{12}^2	T?	$D_{10}E_7^2$	T	A_{24}	T?	Leech	B T

B: it admits binary code construction
T: it admits ternary code construction

Remark : The places marked by "T?" are not yet determined whether it admits a ternary code construction. The reason for this is that the classification of self-dual ternary codes of length 24 is not complete (c.f. [3]).

References

[1] J.H. Conway, V. Pless and N.J.A. Sloane. Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16, IEEE Trans. Inform. Th., IT-25(1979),312-322

[2] J. Leech, and N.J.A. Sloane. Sphere packing and error-correcting Codes, Can. J. Math. Vol.23(1971),718-745

[3] J.S. Leon, V. Pless and N.J.A. Sloane. On ternary self-dual codes of length 24, IEEE Trans. Inform. Th., IT-27(1981),176-180

[4] F.J. MacWilliams, and N.J.A. Sloane. The Theory of Error-Correcting Codes, North-Holland, Amsterdam (1977)

[5] C.L. Mallows, V. Pless and N.J.A. Sloane. Self-dual Codes over $GF(3)$, SIAM. J. Appl. Math. Vol.31(1976),649-666

[6] C.L. Mallows, and N.J.A. Sloane. Weight enumerators of self-orthogonal codes over $GF(3)$, SIAM. J. Alg. Disc. Math. Vol.2(1981),452-460

[7] J.S. Leon, V. Pless and N.J.A. Sloane. Self-dual Codes over $GF(5)$, J. Comb. Th. Ser.A Vol.32(1982),178-194

[8] M. Ozeki, On the Structure of even unimodular extremal lattices of rank 40, Rocky Mountain J. Math. Vol.19(1989)

[9] M. Ozeki, Ternary Code construction of even unimodular lattices, Proceedings of the International Number Theory Conference held at Université Laval, July 5-18, 1987 (1989),772-784

[10] M. Ozeki, Quinary code construction of the Leech lattice, preprint