群論と対称性

2015 年度 花木章秀

March 19, 2015

一回のゲームを 3 人で行うものとし、7 人の参加者から優勝者を決定したい。どの 2 人も少なくとも一度は対戦するように対戦表を作るとしたら、最低何回の対戦が必要になるだろうか？

他の 6 人すべてと対戦するためには 1 人あたり、最低でも 3 回の対戦がなければならないので、少なくとも 7 回の対戦が必要なことが すぐに分かる。では 7 回の対戦で、これを実現することはできるであろうか？ これは実際に作ってみれば分かる。7 人の参加者を 1 から 7 の数字で表すと

$$123,\ 134,\ 156,\ 246,\ 257,\ 346,\ 357$$

で実現できていることが分かる。したがって、上記の問題の答は 7 である。

この問題には「ゲームを 3 人で行う」、「7 人の参加者」、「どの 2 人も」、「少なくとも 1 度」と多くの数が入っている。これを一般化して、別の数に置き換えた問題ではどうであろうか？

- 「ゲームを k 人で行う」
- 「v 人の参加者」
- 「どの t 人も」
- 「ちょうど λ 度」

としたものが t-(v,k,λ) **デザイン**と呼ばれるものである。どのような t-(v,k,λ) に対して、デザインが存在するかということが、デザイン理論における一つの大きな問題である。

1 結合構造

$\mathfrak{P},\mathfrak{B}$ を (有限) 集合とし、I を直積集合 $\mathfrak{P}\times\mathfrak{B}$ の部分集合とする。このとき $S=(\mathfrak{P},\mathfrak{B},I)$ を**結合構造** (incidence structure) という。$\mathfrak{P}$ の元を**点**、$\mathfrak{B}$ の元を**ブロック**、I の元を**旗**

(flag) という。$p \in \mathfrak{P}$, $B \in \mathfrak{B}$ に対して $(p, B) \in I$ であるとき pIB と書いて、p と B は**結合関係にある**という。p は B 上にある、B は p を通る、などということもある。

以後、断らない限り $\mathfrak{P}$ も $\mathfrak{B}$ も有限集合であるとする。

$p \in \mathfrak{P}$, $B \in \mathfrak{B}$ に対して

$$\begin{aligned}(p) &= \{B \in \mathfrak{B} \mid pIB\},\\ (B) &= \{p \in \mathfrak{P} \mid pIB\}\end{aligned}$$

と定める。

定理 1.1. 次の式が成り立つ。

$$\sum_{B \in \mathfrak{B}} \sharp(B) = \sum_{p \in \mathfrak{P}} \sharp(p)$$

証明. 両辺ともに I の要素の数である。 □

二つの結合構造 $S = (\mathfrak{P}, \mathfrak{B}, I)$ と $S' = (\mathfrak{P}', \mathfrak{B}', I')$ が**同型**であるとは、全単射 $\phi : \mathfrak{P} \to \mathfrak{P}'$ と $\psi : \mathfrak{B} \to \mathfrak{B}'$ が存在して $pIB \Leftrightarrow \phi(p) I' \psi(B)$ となることである。

結合構造は行列を用いて考えると扱いやすい。適当に番号を付けて $\mathfrak{P} = \{p_1, \cdots, p_v\}$, $\mathfrak{B} = \{B_1, \cdots, B_b\}$ とする。$v \times b$ 行列 A を、その (i, j) 成分を $p_i I B_j$ であるとき 1、そうでないとき 0 で定める。この行列を結合構造 $(\mathfrak{P}, \mathfrak{B}, I)$ の**結合行列**という。

例 1.2. 先の 2-$(7, 3, 1)$ デザインの結合行列は以下の通りである。

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

結合行列を作るとき、$\mathfrak{P}$ や $\mathfrak{B}$ の要素に順番を付ける必要があるが、その順番を付け替えると、その結合行列は行や列に置換を施したものになる。二つの結合構造が同型であるということは、このように結合行列で見た場合には、行や列の置換でしか違わないということであり、本質的には同じものであると思うことが出来る。

例 1.3 (双対構造)**.** 結合構造 $S = (\mathfrak{P}, \mathfrak{B}, I)$ において、点をブロック、ブロックを点と読み替えて得られる結合構造を S の**双対構造**という。すなわち $\overline{S} = (\overline{\mathfrak{P}}, \overline{\mathfrak{B}}, \overline{I})$ が $S = (\mathfrak{P}, \mathfrak{B}, I)$ の双対構造であるとは、

$$\overline{\mathfrak{P}} = \mathfrak{B}, \quad \overline{\mathfrak{B}} = \mathfrak{P}, \quad B \overline{I} p \Longleftrightarrow pIB$$

となることである。(結合行列で考えれば、双対構造の結合行列はもとの結合構造の結合行列の転置行列となる。)

2 t-デザイン

$S = (\mathfrak{P}, \mathfrak{B}, I)$ を結合構造とする。次の条件をみたすとき S を t-(v, k, λ) **デザイン**という。

(1) $|\mathfrak{P}| = v$ である。

(2) 任意の $B \in \mathfrak{B}$ に対して $\sharp(B) = k$ である。

(3) $\mathfrak{P}$ の任意の t 個の異なる要素に対して、そのすべてと結合関係にあるブロックの個数は λ である。

このとき、パラメータを省略して、単に t-**デザイン**ともいう。

例 2.1 (戦術的配置)**.** 1-デザインを**戦術的配置**という。このとき、各ブロックの上にある点の数は一定で、また各点を通るブロックの数も一定である。(結合行列で考えれば、各行、各列にある 1 の数がそれぞれ一定であるということである。)

単にデザインという場合には、通常は $t \geq 2$ の場合を考える。

定理 2.2. $S = (\mathfrak{P}, \mathfrak{B}, I)$ を結合構造とする。S が t-デザインであるならば S は任意の $1 \leq i \leq t$ に対して i-デザインである。特に S が t-(v, k, λ) デザインであるならば S は i-(v, k, λ_i) デザインである。ここで

$$\lambda_i = \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} = \lambda \frac{(v-i)(v-i-1)\cdots(v-t+1)}{(k-i)(k-i-1)\cdots(k-t+1)}$$

である。

証明. $\{p_1, \cdots, p_i\}$ を異なる点の集合とする。$\{p_1, \cdots, p_i\}$ をすべて通るブロックの個数 λ_i が最後の式で与えられることを示せばよい。$\mathcal{A}$ を $\{p_1, \cdots, p_i\}$ と共通部分をもたない $t-i$ 個の異なる点の集合 $\{q_1, \cdots, q_{t-i}\}$ と、$\{p_1, \cdots, p_i\}$ と $\{q_1, \cdots, q_{t-i}\}$ をすべて含むブロック B の組 $(\{q_1, \cdots, q_{t-i}\}, B)$ からなる集合とし、$\mathcal{A}$ の要素の個数を数える。とおいて、$\mathcal{A}$ の要素の数を二通りに数える。

まず、条件をみたす $\{q_1, \cdots, q_{t-i}\}$ は $\binom{v-i}{t-i}$ 個ある。$\{q_1, \cdots, q_{t-i}\}$ に対して、条件をみたす B は λ 個ある。よって $|\mathcal{A}| = \lambda\binom{v-i}{t-i}$ である。つぎに、条件をみたす B の個数は λ_i 個である。B に対して、条件をみたす $\{q_1, \cdots, q_{t-i}\}$ は $\binom{k-i}{t-i}$ 個ある。したがって $|\mathcal{A}| = \lambda_i\binom{k-i}{t-i}$ である。二つの式を合せて、求める式が得られる。 □

この定理から $t \geq 2$ に対する t-デザインはすべて 2-デザインである。2-デザインを単に**デザイン**ということもある。1-デザインは通常はデザインであるとは言わない。

戦術的配置 (1-デザイン) $S = (\mathfrak{P}, \mathfrak{B}, I)$ に対し、

$$\begin{aligned} v &= |\mathfrak{P}| = (\text{点の数}) \\ b &= |\mathfrak{B}| = (\text{ブロックの数}) \\ r &= |(p)| = (1 \text{ 点を通るブロックの数}) \\ k &= |(B)| = (\text{一つのブロックに含まれる点の数}) \end{aligned}$$

とおいて、これらを S の**パラメータ**という。t-デザインに対しては

$$\lambda = (\text{与えられた } t \text{ 個の点をすべて含むブロックの数})$$

も含めて S のパラメータという。

定理 2.3. (1) 戦術的配置 $S = (\mathfrak{P}, \mathfrak{B}, I)$ のパラメータについて

$$vr = bk$$

が成り立つ。

(2) $t \geq 2$ ならば t-デザイン $S = (\mathfrak{P}, \mathfrak{B}, I)$ のパラメータについて

$$r(k-1)(k-2)\cdots(k-t+1) = \lambda(v-1)(v-2)\cdots(v-t+1)$$

$$\lambda\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}} \quad (i = 0, 1, \cdots, t)$$

が成り立つ。

証明. (1) は I の要素の数を数えれば分かる。定理 2.2 で $i = 1$ とすれば $\lambda_1 = r$ なので (2) の一つ目の式が成り立つ。次の式は λ_i が整数であることによる。 □

デザインの理論において基本的な問題は次の二つである。

存在の問題

どのような t, v, k, λ に対して t-(v, k, λ) デザインは存在するか？

一意性の問題

t-(v, k, λ) デザインが存在するとき、それはパラメータによって一意的に決まるか？

定理 2.3 のはじめの二つの式から t, v, k, λ によって他のパラメータ b, r は求められる。三つ目の式が成り立つようなパラメータを**認容なパラメータ**という。デザインが存在すればそのパラメータは認容であるが、逆は正しくない。

3 2-デザイン

2-$(v, k\lambda)$ デザインは応用上特に重要で、**釣合い型不完備配置** (Balenced incomplete block design, BIBD) とも呼ばれる。一般に t-$(v, k\lambda)$ デザインは $v = k$ のとき**完備**であるという。これは全ての点がすべてのブロックと結合関係にあるということで、結合行列で考えれば、すべての成分が 1 である自明な場合となる。以後、断らない限り t-デザインは完備でないもののみを考える。

定理 2.3 を $t = 2$ に適用して次の定理が成り立つ。

定理 3.1. 2-デザインのパラメータについて、次が成り立つ。

$$vr = bk, \quad r(k-1) = \lambda(v-1)$$

3.1 Fisher の不等式

D を 2-デザインとし A をその結合行列とする。**D** は 2-デザインであるから、任意の異なる 2 行について、成分に共通して 1 をもつ箇所は λ 個ある。また各行には 1 が r 個ある。これは

$$A^tA = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ & \cdots & \cdots & \\ \lambda & \lambda & \cdots & r \end{pmatrix} = (r-\lambda)I + \lambda J$$

を意味する。ただしここで I は単位行列、J はすべての成分が 1 である行列を表すものとする。J は固有値に v を 1 個、0 を $v-1$ 個もつので、線形代数における Frobenius の定理より A^tA は固有値に $(r-\lambda+\lambda v)$ を 1 個、$(r-\lambda)$ を $v-1$ 個もつことが分かる。

定理 3.2. **D** を 2-デザインとし A をその結合行列とする。このとき

$$AA^t = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ & \cdots & \cdots & \\ \lambda & \lambda & \cdots & r \end{pmatrix}$$

であり、特に $\det AA^t = (n+\lambda v)n^{v-1}$ が成り立つ。ただし $n = r-\lambda$ である。

$n = r-\lambda$ をデザイン **D** の**位数**という。デザインが完備ではないことから $n > 0$ となり、AA^t は正則行列となる。したがって $v \leq \mathrm{rank}A \geq \mathrm{rank}AA^t = v$ となり $\mathrm{rank}A = v$ である。$\mathrm{rank}A \leq b$ より $v \leq b$ が得られ、$vr = bk$ より $r \geq k$ となる。

定理 3.3 (Fisher の不等式)**.** 2-デザインのパラメータについて、次が成り立つ。

$$v \leq b, \qquad r \geq k$$

結合行列からデザインであるかどうかを判定することも出来る。次の定理はデザインの定義から明らかであろう。

定理 3.4. $S = (\mathfrak{P}, \mathfrak{B}, I)$ を結合構造とし A をその結合行列とする。

$$AA^t = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ & \cdots & \cdots & \\ \lambda & \lambda & \cdots & r \end{pmatrix}, \qquad r > \lambda$$

となるならば A は 2-デザインである。

3.2 対称的 2-デザイン

$v = b$ である 2-デザインを**対称的 2-デザイン**という。このとき $vr = bk$ より $r = k$ も成り立つ。対称的 2-デザインの結合行列は正方行列で、各行、各列にちょうど k 個の 1 を含む。また

$$k(k-1) = \lambda(v-1)$$

が成り立つ。

定理 3.5. A を対称的 2-(v,k,λ) デザインの結合行列とすれば次の式が成り立つ。

$$\begin{aligned} AA^t &= A^tA = nI + \lambda J \\ AJ &= JA = kJ \\ \det(AA^t) &= (\det A)^2 = k^2 n^{v-1} \end{aligned}$$

ここで $n = k - \lambda$ はデザインの位数である。

証明. $A^tA = nI + \lambda J$ 以外はこれまでのことからすぐに分かる。($n + \lambda v = k - \lambda + \lambda v = k + \lambda(v-1) = k + k(k-1) = k^2$ にも注意。) A が正則であることから

$$A^tA = A^{-1}AA^tA = A^{-1}(nI + \lambda J)A = nI + \lambda J$$

も分かる。 □

この定理から次が得られる。

定理 3.6. 結合構造 S が対称的 2-デザインであることと、その双対構造 $\overline{S}$ が 2-デザインであることは同値である。

3.3 Bruck-Ryser の定理

認容なパラメータはデザインが存在するための弱い必要条件である。ここでは対称的 2-デザインの存在に関して知られる次の定理を示す。

定理 3.7 (Bruck-Ryser)**.** 対称的 2-(v,k,λ) デザインが存在すれば次のことが成り立つ。

(1) v が偶数ならば、$n = k - \lambda$ は平方数である。

(2) v が奇数ならば、不定方程式

$$x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2$$

は自明でない ($x = y = z = 0$ でない) 整数解をもつ。

証明のために二つの補題を用意する。

補題 3.8 (Euler)**.**

$$(b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

ただし、ここで

$$\begin{aligned} y_1 &= b_1x_1 - b_2x_2 - b_3x_3 - b_4x_4 \\ y_2 &= b_2x_1 + b_1x_2 - b_4x_3 + b_3x_4 \\ y_3 &= b_3x_1 + b_4x_2 + b_1x_3 - b_2x_4 \\ y_4 &= b_4x_1 - b_3x_2 + b_2x_3 + b_1x_4 \end{aligned}$$

この補題は計算によって確認することができるが、四元数体のノルムに関する議論からも得られる。また係数行列

$$A = \begin{pmatrix} b_1 & -b_2 & -b_3 & -b_4 \\ b_2 & b_1 & -b_4 & b_3 \\ b_3 & b_4 & b_1 & -b_2 \\ b_4 & -b_3 & b_2 & b_1 \end{pmatrix}$$

について $AA^t = (b_1^2 + b_2^2 + b_3^2 + b_4^2)I$ が確認でき、したがって b_1, b_2, b_3, b_4 がすべて実数で $(b_1, b_2, b_3, b_4) \neq (0, 0, 0, 0)$ のとき A は正則行列である。このとき x_i $(i = 1, 2, 3, 4)$ を y_i $(i = 1, 2, 3, 4)$ の一次結合で書くことが出来ることに注意しておく。また b_1, b_2, b_3, b_4 がすべて有理数ならば、一次結合の係数は有理数にとることができる。

次の補題の証明は [2] による。証明のために少しだけ準備をする。p を素数とする。p と互いに素な整数 a に対して、a が p の**平方剰余**であるとは、合同式 $x^2 \equiv a \pmod{p}$ が解をもつこととし、そうでないとき**平方非剰余**であるという。平方非剰余と平方非剰余の積は平方剰余となることが基本的な代数学から分かる。

補題 3.9 (Lagrange)**.** 任意の自然数は 4 つの平方数の和として表される。

証明. 補題 3.8 を用いれば、それぞれの素因数を 4 つの平方数の和に書けば十分である。したがって素数 p を考えればよい。$p = 2$ のときは明らかであるから p を奇素数とする。

-1 が p を平方剰余ならば $x^2 + 1 = ph$ なる x と正の数 h が存在する。-1 が平方非剰余とする。1 は平方剰余であり $p - 1$ は平方非剰余なので、ある k があって k は平方剰余、$k + 1$ は平方非剰余となる。したがって $-k - 1$ は平方非剰余二つの積であり、平方剰余である。よって $x_1^2 \equiv k \pmod{p}$, $x_2^2 \equiv -k - 1 \pmod{p}$ なる x_1, x_2 が存在し $x_1^2 + x_2^2 + 1 = ph$ なる正の数 h が存在する。よって、4 つの平方数の和で p の倍数となるものは存在する。

$$\sum_{i=1}^{4} x_i^2 = ph, \qquad h \geq 1$$

ここで $h = 1$ にとれれば定理の証明は終わるので $h > 1$ と仮定する。このとき $0 < h' < h$ なる h' で同様の式が成り立つようにできれば、これを繰り返して証明は終わる。これを示す。

x_i $(i = 1, 2, 3, 4)$ を h で割って

$$x_i \equiv y_1 \pmod{h}, \qquad |y_i| \leq \frac{h}{2} \qquad (i = 1, 2, 3, 4)$$

とする。すると

$$\sum_{i=1}^{4} y_i^2 \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \pmod{h}$$

となるから $\sum_{i=1}^{4} y_i^2 = hh'$ とおく。$ph^2h' = (\sum_{i=1}^{4} x_i^2)(\sum_{i=1}^{4} y_i^2)$ に y_2, y_3, y_4 の符号を変

えて補題 3.9 を適用して、

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_2y_1 - x_1y_2 + x_4y_3 - x_3y_4 \\ z_3 &= x_3y_1 - x_4y_2 - x_1y_3 + x_2y_4 \\ z_4 &= x_4y_1 + x_3y_2 - x_2y_3 - x_1y_4 \end{aligned}$$

とおけば

$$ph^2h' = \sum_{i=1}^{4} z_i^2$$

となる。このとき

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \pmod{h} \\ z_2 &= x_2y_1 - x_1y_2 + x_4y_3 - x_3y_4 \equiv 0 \pmod{h} \end{aligned}$$

$z_3 \equiv z_4 \equiv 0 \pmod{h}$ も同様である。よって $z_i = ht_i$ $(i = 1, 2, 3, 4)$ とおけば

$$\sum_{i=1}^{4} t_i^2 = ph'$$

である。また

$$hh' = \sum_{i=1}^{4} y_i^2 \leq 4\left(\frac{h}{2}\right)^2 = h^2$$

より $h' \leq h$ である。$h = h'$ とすると $y_i = h/2$ $(i = 1, 2, 3, 4)$ で、これは整数である。このとき y_i のとり方から x_i は $h/2$ の奇数倍であり $x_i = (2m_i + 1)h/2$ とおくと

$$\sum_{i=1}^{4}(2m_i + 1)^2 \cdot \frac{h}{4} = p$$

となるが、左辺は偶数となり、p が奇素数であることに反する。よって $h' < h$ となり、証明は終わりである。 □

定理 3.7 の証明. $A = (a_{ij})$ を結合行列とする。

v を偶数とする。定理 3.5 より $(\det A)^2 = \det AA^t = k^2n^{v-1}$ なので n^{v-1} は平方数である。しかし $v - 1$ は奇数なので n 自身が平方数である。

v を奇数とする。$\boldsymbol{x} = (x_1, \cdots, x_v)$ とする。$AA^t = nI + \lambda J$ より $\boldsymbol{x}AA^t\boldsymbol{x}^t = \boldsymbol{x}(nI + \lambda J)\boldsymbol{x}^t$ である。$(L_1, \cdots, L_v) = \boldsymbol{x}A$ とすれば $L_j = \sum_{i=1}^{v} x_i a_{ij}$ であって

$$\boldsymbol{x}AA^t\boldsymbol{x}^t = \sum_{j=1}^{v} L_j^2$$

である。また

$$\boldsymbol{x}(nI+\lambda J)\boldsymbol{x}^t = n\sum_{i=1}^{v} x_i^2 + \lambda\left(\sum_{i=1}^{v} x_i\right)^2$$

である。よって、x_i に関する恒等式

$$\sum_{j=1}^{v} L_j^2 = n\sum_{i=1}^{v} x_i^2 + \lambda\left(\sum_{i=1}^{v} x_i\right)^2$$

が得られる。

$v \equiv 1 \pmod 4$ とする。補題 3.9 より

$$n = b_1^2 + b_2^2 + b_3^2 + b_4^2$$

なる整数 b_i があり $(b_1, b_2, b_3, b_4) \neq (0,0,0,0)$ である。1 から v までの自然数を 4 つずつに切って考える。v だけが余る。$4i+1, 4i+2, 4i+3, 4i+4$ について、補題 3.8 より

$$n(x_{4i+1}^2 + x_{4i+2}^2 + x_{4i+3}^2 + x_{4i+4}^2) = y_{4i+1}^2 + y_{4i+2}^2 + y_{4i+3}^2 + y_{4i+4}^2$$

なる x_{4i+j} の有理数係数一次結合 y_{4i+j} がとれる。また x_{4i+j} も y_{4i+j} の有理数係数一次結合で書ける。更に $y_v = x_v$ とする。これを代入することによって、y_i に関する恒等式

$$\sum_{j=1}^{v} L_j^2 = \sum_{i=1}^{v-1} y_i^2 + ny_v^2 + \lambda\omega^2$$

を得る。ここで L_j, ω は y_i の有理数係数一次結合である。

$L_1 = c_1y_1 + \cdots + c_vy_v$ と書くことができる。$c_1 \neq 1$ ならば $L_1 = y_1$、$c_1 = 1$ ならば $L_1 = -y_1$ に特殊化する。すなわち、この式で定まる超平面に制限して考える。このとき $y_1 = M(y_2, \cdots, y_v)$ と一次式 M を用いて表すことができるので、これを代入すれば y_1 が消去され

$$\sum_{j=2}^{v} L_j^2 = \sum_{i=2}^{v-1} y_i^2 + ny_v^2 + \lambda\omega^2$$

を得る。ここで L_j, ω は y_1 が消去されたものを表している。これは $y_2, \cdots, y_v$ に u 関する恒等式である。

上記の操作を繰り返して、y_v に関する恒等式

$$L_v^2 = ny_v^2 + \lambda\omega$$

を得る。ここで L_v, ω は y_v の有理数倍である。$L_v = (a/c)y_v$, $\omega = (b/c)y_v$ $(a, b, c \in \mathbb{Z}, c \neq 0)$ とおき、$y_v = 1$ を代入すれば

$$a^2 = nc^2 + \lambda b^2$$

となる。$v \equiv 1 \pmod 4$ であるから、$c \neq 0$ に注意して、$(x, y, z) = (a, c, b)$ が求める自明でない整数解である。

$v \equiv 3 \pmod 4$ とする。新しい変数 x_{v+1} を加えて

$$\sum_{j=1}^{v} L_j^2 + nx_{v+1} = n\sum_{i=1}^{v+1} x_i^2 + \lambda\left(\sum_{i=1}^{v} x_i\right)^2$$

を考える。1 から $v+1$ を 4 つずつに切って、前と同じような操作をすれば

$$\sum_{j=1}^{v} L_j^2 + nx_{v+1}^2 = \sum_{i=1}^{v+1} y_i^2 + \lambda\omega^2$$

となる。特殊化を繰り返して

$$nx_{v+1}^2 = y_{v+1}^2 + \lambda\omega^2$$

を得る。$x_{v+1} = (a/c)y_{v+1}$, $\omega = (b/c)y_{v+1}$ $(a, b, c \in \mathbb{Z},\ c \neq 0)$ とおき、$y_v = 1$ を代入すれば $na^2 = c^2 + \lambda b^2$ となり、$(x, y, z) = (c, a, b)$ が自明でない解となる。 □

例 3.10. (1) $(v, k, \lambda) = (22, 7, 2), (46, 10, 2)$ は認容な 2-デザインのパラメータである。しかし $n = k - \lambda = 5, 8$ は平方数ではないので、このパラメータをもつデザインは存在しない。

(2) $(v, k, \lambda) = (29, 8, 2)$ は認容な 2-デザインのパラメータである。このパラメータをもつデザインが存在すれば Bruck-Ryser の定理から不定方程式 $x^2 = 6y^2 + 2z^2$ が自明でない整数解をもつが、これには自明でない整数解がないことが分かるので、そのようなデザインは存在しない。

注意. $x^2 = 6y^2 + 2z^2$ が自明でない整数解をもたないことを示しておく。(x, y, z) を互いに素な整数の組としてよい。まず x が偶数であることはすぐに分かるので $x = 2u$ とおく。代入して整理すれば

$$2u^2 = 3y^2 + z^2$$

である。両辺が偶数になるので、y, z は共に偶数であるか、共に奇数である。共に偶数であるとすれば (x, y, z) が互いに素であることに反するので、y, z は共に奇数である。このとき $y^2 \equiv 1 \pmod 8$, $z^2 \equiv 1 \pmod 8$ となるので、上の式を 8 を法として考えれば

$$2u^2 \equiv 4 \pmod 8$$

となる。しかしこのような u は存在しないので、条件をみたす整数解は存在しない。

3.4 射影平面

$n \geq 2$ に対して 2-$(n^2 + n + 1, n + 1, 1)$ デザインを**射影平面**という。射影平面は対称的となる。$n = p^a$ が素数べきであるときには p^a 個の元をもつ有限体を用いて幾何学的に射影平面が構成され、したがって位数 p^a の射影平面が存在する。

未解決問題

位数 n の射影平面が存在すれば n は素数べきか？

素数べきでない最小の自然数は $n = 6$ である。このとき 2-$(43, 7, 1)$ デザインとなるが、これに Bruck-Ryser の定理を適用すると $x^2 = 6y^2 - z^2$ が自明でない整数解をもつかどうかが問題となる。(x, y, z) を互いに素であるとして、この式を 8 を法として考えれば、そのような整数解はないことが分かる。したがって位数 6 の射影平面は存在しない。

位数 10 の射影平面が存在するかどうかは Bruck-Ryser の定理からは分からない。これは比較的近年、計算機を用いた計算によって非存在が確認されたらしい。現在の未解決な最小の n は 12 である。

References

[1] 永尾汎, 群とデザイン, 岩波書店, 1974.

[2] 高木貞治, 初等整数論講義 (第 2 版), 共立出版, 1971 (初版 1931)