数理解析研究所講究録
第2012巻 2016年 23-30

Self-Orthogonal Designs and Equitable Partitions

東北大学・情報科学研究科
純粋・応用数学研究センター
宗政昭弘
Akihiro Munemasa
Research Center for Pure and Applied Mathematics
Graduate School of Information Sciences
Tohoku University

September 30, 2015

定義 1. t-(v,k,λ) デザインとは、組 $(X,\mathcal{B})$ で

- X は有限集合で $|X|=v$,
- $\mathcal{B}\subset\binom{X}{k}=\{X\text{ の }k\text{ 点部分集合}\}$,
- $\forall T\in\binom{X}{t}$, $\lambda=|\{B\in\mathcal{B}\mid B\supset T\}|$

をみたすものをいう.

集合 X の元は「点」と呼ばれ，集合 $\mathcal{B}$ の元はブロックと呼ばれる.
Teirlinck [5] 以前は，t-デザインで $t\geq 5$ なるものはわずかしか知られていなかった.

定理 2 (Teirlinck). 任意の $t\geq 1$ に対して非自明な t-デザインは存在する．すなわち，

$$\forall t\geq 1,\ \exists v,\exists\lambda \text{ s.t. } \exists t\text{-}(v,t+1,\lambda)\ \text{デザイン}.$$

一方，具体的な t,v,k,λ が与えられたとき，t-(v,k,λ) デザインが存在するかどうかは一般的には難しい問題である．CRC Handbook of Combinatorial Designs [1] によれば，例えば 3-(16,7,5) デザインの存在が未解決になっている．最近 Nakić [2] はこのようなデザインが存在するとしたら位数 3 の自己同型を持たないことを示しているが，存在問題自体は依然未解決のままである.

本講演では，$1\leq\mu\leq 5$ に対して，次のような特別な性質を持つ 3-$(16,8,3\mu)$ デザインの構成を与える.

定義 3. デザイン $(X, \mathcal{B})$ が自己直交的であるとは,

$$|B \cap B'| \equiv 0 \pmod 2 \quad (\forall B, B' \in \mathcal{B})$$

をみたすときをいう.

特に, t-(v, k, λ) デザインが自己直交的ならば, k は偶数である. 自己直交的なデザインは, 符号との関係から [3] で詳しく調べられている.

例 4. Witt [6] は 5-$(24, 8, 1)$ デザインの一意性を示している. このデザインは自己直交的である.

H を位数 $8n$ のアダマール行列, すなわち, 成分が ± 1 の $8n$ 次正方行列で $HH^\top = 8nI$ をみたすもの, とすると, 自己直交的な 3-$(8n, 4n, 2n-1)$ が得られる. 実際, H を正規化, すなわち、第 1 行がすべて 1 のベクトル $\boldsymbol{j}$ となるように列を ± 1 倍すると

$$H = \begin{bmatrix} \boldsymbol{j} \\ H_1 \end{bmatrix},$$

となり, 行列

$$M = \frac{1}{2}\begin{bmatrix} J - H_1 \\ J + H_1 \end{bmatrix}.$$

は 3-$(8n, 4n, 2n-1)$ の結合行列を与える. ただし, J は成分がすべて 1 の行列を表す. このデザインが自己直交的であることは, $MM^\top$ を計算することでわかる. なぜなら, M を, その列が点の集合で添字づけられた結合行列とするとき,

$$\text{デザインが自己直交的} \iff MM^\top = 0 \text{ over } \mathbb{F}_2$$

となるからである. M の行ベクトルの生成する $\mathbb{F}_2$ 上のベクトル空間 C をそのデザインの符号と呼ぶ. デザインが自己直交的であることと $C \subset C^\perp$ は同値である.

例 5. 位数 8 のアダマール行列から作られる自己直交的 3-$(8, 4, 1)$ デザインは次のようなものである. 行列 $\begin{bmatrix} I_4 & J_4 - I_4 \end{bmatrix}$ の行ベクトルの生成する $\mathbb{F}_2$ 上のベクトル空間には 14 個の重さ 4 のベクトルが含まれ, これらが自己直交的 3-$(8, 4, 1)$ デザインを与える.

同様にして, 位数 16 のアダマール行列からは 3-$(16, 8, 3)$ デザインが得られ, これも自己直交的である. では, 3-$(16, 8, 3\mu)$ デザインで $\mu > 1$ なるものは存在するであろうか. Disjoint なものを見つけてしかも直交するようにできれば, このようなデザインが見つかったことになる. いかにも単純な方法ではあるが, magma で実行してみる.

```
HD:=HadamardDatabase();
H:=Matrix(HD,16,2);
H;
D:=HadamardRowDesign(H,1);
D;

x:=Random(Sym(16));
D2:=Design(Sum([D,D^x]),3);
D2;

int:={0,2,4,6};
is_self_orthogonal:=
 func< D | &and{ #(B1 meet B2) in int
  : B1,B2 in Blocks(D) | B1 ne B2 } >;

is_self_orthogonal(D2);

self_orthogonal_union:=
 func< x | is_self_orthogonal(Sum([D,D^x])) >;

tf:=false;
while not tf do
 tf:=self_orthogonal_union(Random(Sym(16)));
end while;
```

なかなか見つからない．そこで，もう少し効率よく探すために，このデザインの符号 C の自己同型 $\sigma \in \mathrm{Aut}(C)$ で $\mathcal{B} \cup \sigma(\mathcal{B}) \subset C$ となるものを探してみる．

```
C:=LinearCode(D,GF(2));
AutC:=AutomorphismGroup(C);
exists(x){ x : x in AutC | self_orthogonal_union(x) };
D2:=Design(Sum([D,D^x]),3);
D2;
```

こんどはすぐに見つかる．違いは

```
#Sym(16) eq 20922789888000;
#AutC eq 5160960;
```

という，探す範囲の大きさの違いによる．このように，自己直交的なデザインを調べるにはその符号を見ることが重要となるが，それには次のような性質がある．一般に，

t-デザインの符号 C の双対符号 $C^{\perp}$ は最小重みが少なくとも $t+1$ である．さらに，次の補題が成り立つ．

補題 6. 自己直交的な 3-(v,k,λ) デザインの符号 C の双対符号が最小重み 4 を持つとすると，$v=2k\equiv 0 \pmod 4$ が成り立つ．

すると，小さい v に対して，自己直交的な 3-(v,k,λ) デザインの可能性がかなり絞られる．3-$(8,4,1)$ デザインはアダマール行列から得られたが，自己直交的な 3-$(12,6,\lambda)$ デザインは存在しない．では，自己直交的な 3-$(16,8,\lambda)$ デザインはどのような λ に対して存在するだろうか．簡単な数え上げにより，$\lambda\equiv 0 \pmod 3$ が必要であることがわかる．自己直交性を仮定しないと，λ の上界は

$$\lambda \le \binom{16}{8}\binom{8}{3}\binom{16}{3}^{-1} = 1287$$

だが，自己直交性を仮定すると λ はかなり小さくならざるを得ない．$\lambda=3\mu$ とおく．$\mu=1$ のときはアダマール行列から得られる．一般には，$|\mathcal{B}|=10\lambda=30\mu$ 個のブロックを

$$\binom{16}{8} = 12870.$$

個から選んでくる必要があるので，やみくもにやるのではうまくいかない．前述の通り，その符号を考えるのだが，C はある自己双対符号に含まれる．長さ 16 の自己双対符号は分類されていて，実は 2 つしかない．それらは $e_8\oplus e_8$ と d_{16} と書かれる．ここでは詳細は省略するが，$e_8\oplus e_8$ の場合はデザインの非存在がすぐわかるので，d_{16} を考える．これは，次の行列の行ベクトルで生成される．

$$\begin{bmatrix}
01 & 01 & 01 & 01 & 01 & 01 & 01 & 01 \\
11 & & & & & & & 11 \\
 & 11 & & & & & & 11 \\
 & & \ddots & & & & & \vdots \\
 & & & & & & 11 & 11
\end{bmatrix}$$

d_{16} は $128+70$ 個の重さ 8 のベクトルを持つ．これらは，$64+35$ 個の，互いに補集合となる 8 点部分集合の組からなる．符号が d_{16} に含まれるような自己直交的な 3-$(16,8,3\mu)$ デザインを見つけるには，これらから 15μ 個の組を選び出して 3-デザインになるようにしなければならない．$\mu=1$ についてはアダマール行列から得られた．$\mu=2$ については 2 番目の magma program で見つかる．$\mu\ge 3$ について探すため，まず $64+35$ 個の組の構造を良く調べる．これら $64+35$ 個の組全体の集合を点集合とするようなグラフを次の隣接関係により定義する．

$$\{B_1, B_1^c\} \sim \{B_2, B_2^c\} \iff |B_1\cap B_2| \in \{2,6\}.$$

すると

$$64 = \text{folded halved 8-cube, 28 正則}$$
$$35 = \text{lines of } P^3(\mathbb{F}_2),\ 16 \text{ 正則}$$

となる．ここで，8-cube とは，頂点の集合が $\{0,1\}^8$ であり，ただ一つの座標で成分が異なるような頂点の組を辺で結んで得られるグラフのことである．また，

$$\text{'halved'} = \text{偶数重みのみ},$$
$$\text{'folded'} = \text{補集合との組を同一視}$$

でちょうど2つの座標で成分が異なるような頂点の組を辺で結ぶことにしたものである（偶数重みのみにしたことで，ちょうど1つの座標で成分が異なるということはあり得ない）という意味である．したがって folded halved 8-cube というグラフ Γ は $2^6 = 64$ 個の頂点を持ち，16 正則であることがわかる．

射影空間 $P^3(\mathbb{F}_2)$ は 35 本の直線を持ち，これらは自然にグラフの構造を持つ．これを Δ で表す．

デザインの存在問題をこれらのグラフの性質で言い換えるため，equitable partition の概念を定義する．

定義 7. グラフの equitable partition とは，その頂点集合 X の分割 $X_1 \cup X_2$ であって，次の条件をみたすものをいう．$i,j \in \{1,2\}$ に対してある定数 a_{ij} が存在して，任意の $x \in X_i$ は X_j のちょうど a_{ij} 個の頂点と隣接している．このとき，このグラフは

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

という形の equitable partition をもつという．

補題 8. 上記の $64+35$ 個の互いに補集合となる8点部分集合2つの組から，15μ 個の組を選ぶとき，次は同値：

(1) これらは 3-$(16,8,3\mu)$ デザインを定義する．

(2) Γ が

$$\begin{bmatrix} 4(\mu-1) & 4(8-\mu) \\ 4\mu & 4(7-\mu) \end{bmatrix}$$

という形の equitable partition をもち，かつ Δ が

$$\begin{bmatrix} 4(\mu-1) & 4(5-\mu) \\ 4\mu & 4(4-\mu) \end{bmatrix}$$

という形の equitable partition をもつ．

ここで，条件 (2) の後半の，Δ が equitable partition をもつことは，射影空間の性質を用いると理論的にも容易にわかることなので，前半をみたす Γ の部分グラフを見つけることを magma を用いて実行する．まず，μ を $8-\mu$ で置き換えても条件は同じなので，$\mu \leq 4$ について考えれば十分であることに注意しておく．

$\mu = 4$ について，

$$\begin{bmatrix} 12 & 16 \\ 16 & 12 \end{bmatrix}$$

という形の Γ の equitable partition を見つけるために，Γ の自己同型群を求めて，その位数 32 の部分群による軌道で条件をみたすものが見つかる．

```
load "foldedHalvedCubeGraph.txt";
G:=foldedHalvedCubeGraph(8);
V:=VertexSet(G);
AutG:=AutomorphismGroup(G);
sub32:=Subgroups( AutG : OrderMultipleOf:=32 );
sub32:=[ H`subgroup : H in sub32 ];
orb32:=[ Orbits(H) : H in sub32 ];
orb32:=[ O : O in orb32 | [ #o : o in O ] eq [32,32] ];
orb32:=[ [ { V|x : x in  o } : o in O ] : O in orb32 ];
exists(O){ O : O in orb32 | [ Valence(sub<G|o>) :o in O ] eq [12,12] };
```

ここで，Γ の定義が書かれた `foldedHalvedCubeGraph.txt` というファイルは [4] からダウンロードできる．

もうひとつの方法は，$(0,1)$ 最適化と呼ばれる方法である．線形計画法と似ていて，線形不等式で表された制約条件の下で，目的関数を最大化する解を求めるのであるが，解を $(0,1)$ ベクトルのみの中から探すということが線形計画法と異なる．magma にはこのような機能が実装されている．この方法については少し解説を補足しておこう．$\mu = 3$ について，

$$\begin{bmatrix} 8 & 20 \\ 12 & 16 \end{bmatrix}$$

という形の equitable partition を探す．簡単な数え上げから，これは Γ の 64 点を $24+40$ に分ける必要があることがわかる．

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}.$$

を Γ の adjacency matrix として、仮にこのような equitable partition によってブロック分けされたものだとしよう．すると

$$A_{11}\boldsymbol{j} = 8\boldsymbol{j}, \qquad A_{21}\boldsymbol{j} = 12\boldsymbol{j},$$

よって

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} \boldsymbol{j} \\ 0 \end{bmatrix} = \begin{bmatrix} 8\boldsymbol{j} \\ 12\boldsymbol{j} \end{bmatrix} = \begin{bmatrix} 12\boldsymbol{j} \\ 12\boldsymbol{j} \end{bmatrix} - \begin{bmatrix} 4\boldsymbol{j} \\ 0 \end{bmatrix}.$$

これはつまり，このような分割が未知だとしてその特性ベクトルを x としたとき

$$Ax = 12\boldsymbol{j} - 4x, \text{ すなわち } (A+4I)x = 12\boldsymbol{j}$$

を意味している．ここで等式 $(A+4I)x = 12\boldsymbol{j}$ を成分ごとの不等式

$$(A+4I)x \leq 12\boldsymbol{j}$$

に変えて，最大化問題を解くのである．

```
Z:=Integers();
A:=AdjacencyMatrix(foldedHalvedCubeGraph(8));
lhs:=A+ScalarMatrix(64,4);
allone:=Matrix(Z,64,1,[1:i in [1..64]]);
rel:=-allone;
rhs:=12*allone;
obj:=Transpose(allone);
s:=MaximalZeroOneSolution(lhs,rel,rhs,obj);
s;
&+Eltseq(s) eq 24;
```

ちなみに，$\mu = 1,2,3,4$ のすべてについてもこの方法で解が一瞬で見つかる．

```
for mu in [1..4] do
rhs:=4*mu*allone;
obj:=Transpose(allone);
s:=MaximalZeroOneSolution(lhs,rel,rhs,obj);
print mu,&+Eltseq(s) eq 8*mu;
end for;
```

まとめると

定理 9. 次は同値：

(1) 自己直交的な 3-$(16,8,3\mu)$ デザインが存在，

(2) $\mu \in \{1,2,3,4,5\}$.

参考文献

[1] J. Dinitz and C. Colbourn, eds., The CRC Handbook of Combinatorial Designs, 2nd ed., Chapman & Hall/CRC Press, 2006.

[2] A. Nakić, Non-existence of a simple 3-$(16, 7, 5)$ design with an automorphism of order 3, Discrete Math. 338 (2015), 555–565.

[3] M. Lalaude-Labayle, On binary linear codes supporting t-designs, IEEE Trans. Inform. Theory 47 (2001), 2249–2255.

[4] A. Munemasa, `http://www.math.is.tohoku.ac.jp/~munemasa/magma.html`

[5] L. Teirlinck, Non-trivial t-designs without repeated blocks exist for all t, Discrete Math. 65 (1987), 301–311.

[6] E. Witt, Über Steinersche systeme, Abh. Math. Sem. Univ. Hamburg. 12 (1938), 265–275.