数理解析研究所講究録 1394 巻 2004 年 79-85

Non self-orthogonal designs の構成

中空 大幸 (Hiroyuki Nakasora)

岡山大学, 千葉大学
(Okayama University, Chiba University)

1 Introduction

デザイン理論、コード理論、有限幾何、これらは各々独立した理論または分野として成り立っているが、互いに密接な関係あり、そのため研究対象として興味深いものが数多くあると思える。今回の報告では、デザインとコードの関係から出てきた概念である self-orthogonal designs について考え、結果として 2-$(21,6,4)$ design の構成法を与える。また、この構成法を一般化することにより、古典的な問題であった位数 10 の射影平面の非存在定理との関連についても紹介する。

まず、準備としてデザインの定義から始める。

Definition 1.1. X を v 個の点集合とし、$\mathcal{B}$ は X の k 点の部分集合の族で (ブロックの集合)、性質として任意の t 個の点はちょうど λ 個のブロックに含まれる。

このとき、$D=(X,\mathcal{B})$ は t-(v,k,λ) design と呼ぶ。

デザインとコードの関係において、Assmus-Mattson の定理[1]がある。ここでは詳しく述べないがコードからデザインを作り出す方法として有効な手法である。さて、コードから生成されるデザインについて次のような概念 (self-orthogonal) が考えられている。

Definition 1.2. D を t-(v,k,λ) design とし、$S_1,S_2,\cdots,S_m$ を block intersection numbers とする。このとき、$k\equiv S_1\equiv S_2\equiv\cdots\equiv S_m \pmod 2$ をみたすならば、D を self-orthogonal design と呼ぶ。

self-orthogonal design の最も簡単な例として位数 2 の射影平面 (2-$(7,3,1)$ design) が挙げられる。この場合 block intersection number は 1 だけであり上記の定義をみたしていることが容易に解る。そして、ひじょうに良い性質をもつデザインと言わ

[1]参考文献として [1] を挙げる。また今回はデザインに対する結果が主であるため、コードの定義等を割愛させて頂く。

れている 24 点の Witt system W_{24} (5-(24,8,1) design) [2]がある。この W_{24} から得られる derived design と point-residual design 達を表 1 に挙げる。

表 1: Designs obtained from a 5-(24,8,1) design

No.	t-(v,k,λ) design	
1	5-(24,8,1) design	W_{24}
2	4-(23,7,1) design	W_{23}
3	4-(23,8,4) design	
4	3-(22,6,1) design	W_{22}
5	3-(22,7,4) design	
6	3-(22,8,12) design	
7	2-(21,5,1) design	$PG(2,4)$
8	2-(21,6,4) design	
9	2-(21,7,12) design	
10	2-(21,8,28) design	

$W_{24}, W_{23}, W_{22}, PG(2,4)$ (位数 4 の射影平面) はそれぞれのパラメータに対して一意に存在することはよく知られている。

No. 3, 5, 6, 8, 9, 10 のデザインに対しては、self-orthogonal の仮定を付け加えるとそれぞれのデザインは一意に存在することが Tonchev [10] によって示されている。しかし、self-orthogonal の仮定を外すと決してこれらのデザインは一意的ではない。例えば CRC Handbook [2] のデータによると No. 9 の 2-(21,7,12) design は同型を除いて 10^{18} 個以上存在することが知られている。しかし、No. 8 の 2-(21,6,4) design については CRC Handbook のデータには少なくとも 1 個 (これは self-orthogonal design に対応している) 存在と載っている。よって、今回 Non self-orthogonal 2-(21,6,4) design の構成を試みた次第である[3]。

2 2-(21,6,4) design の構成

この章では、2-(21,6,4) design の構成法[4]について述べる。準備として resolvable 2-design の定義と記号の説明から始める。

Definition 2.1. デザイン D のブロックの集合の分割の類を $\{H_1, \cdots, H_r\}$ とする。

[2]良い性質としてこのパラメータに対してデザインが一意に定まるという他にも、extended Golay code $\mathcal{G}_{24}$ 、24 次 Mathieu 群 M_{24} との関連が挙げられる。

[3]講演の際にも紹介したが、山形大学の原田昌晃先生から頂いた問題である。

[4]この構成法はデザインの点集合を $16+5$ と考えて、2-(16,6,2) design を subdesign として含む場合について考える事によって思い付いた。

D の任意の点が各類の唯一つのブロックに含まれるという性質をもつ時、$\{H_1, \cdots, H_r\}$ を D の平行類という。

デザイン D が平行類をもつ時、D を resolvable 2-design と呼ぶ。

記号として、$\binom{R}{2}$ を R の 2 点部分集合全体を表し、$\binom{R}{2} \times n$ を $\binom{R}{2}$ の各元を n 回繰り返した集合を表すものとする。

Proposition 2.2. まず、次の 3 つを仮定する。

- (P, Q) : 2-(16, 6, 2) *design*
- (P, S) : *resolvable* 2-(16, 4, 2) *design*
  $H_1, \cdots, H_{10}$: 平行類
- (R, S) : $\binom{5}{2} \times 4$

そして、全単射 $\phi : \binom{5}{2} \to \{H_1, \cdots, H_{10}\} = \{\phi(x,y) | \{x,y\} \in \binom{5}{2}\}$ に対して、$S' = \{A \cup \{x,y\} | A \in \phi(x,y), \{x,y\} \in \binom{5}{2}\}$ とする。ここで、$X = P \cup R$, $\mathcal{B} = Q \cup S'$ と置く。すると、$(X, \mathcal{B})$ は 2-(21, 6, 4) *design* である。

Proof. この構成より、$|X| = 21$、任意の $B \in \mathcal{B}$ に対して $|B| = 6$ であることが容易に解る。(P, Q) が 2-(16, 6, 2) design また、(P, S) が 2-(16, 4, 2) design より P の任意の 2 点はちょうど 4 個の $\mathcal{B}$ のブロックに含まれる。同様に、(R, S) が $\binom{5}{2} \times 4$ より R の任意の 2 点はちょうど 4 個の $\mathcal{B}$ のブロックに含まれる。次に (P, S) (resolvable 2-(16, 4, 2) design) の各平行類に対して、R の 2-subsets の 1 つが対応しているから、P と R からそれぞれ 1 点ずつ取ってきた任意の 2 点はちょうど 4 個の S' すなわち $\mathcal{B}$ のブロックに含まれる。よって X の任意の 2 点はちょうど 4 個のブロックに含まれるので $(X, \mathcal{B})$ は 2-(21, 6, 4) design である。 □

	P	R
Q	2-(16, 6, 2) design	0
S	resolvable 2-(16, 4, 2) design	$\binom{5}{2} \times 4$

ここで、この構成法に現れたデザインのデータについて述べる。まず、2-(16, 6, 2) design は昔から同型を除いて 3 個存在することが知られている。一方、resolvable 2-(16, 4, 2) design は最近 Kaski と Östergård [4] によって分類がされている。その結果によると、resolvable 2-(16, 4, 2) design の同型を除いた個数は 325,062 個存在するそうである。講演の際、この構成法から得られるデザインは少なくとも $3 \times 325,062 = 975,186$ 個あると発表したが、重複した数え上げをしている可能性がある事に気が付いたため、ここで訂正をさせて頂き存在証明だけを報告する。実際にこの構成法から得られるデザインの総数を計算するのはかなり困難と思える。もう一つ重要なデータとして、resolvable 2-(16, 4, 2) design 全体の中で位数 4 のアフィン平面 (2-(16, 4, 1) design 一意的に存在) を subdesign として含まないデザインは 5,001 個存在することを挙げる。

Corollary 2.3. (P,S) が 2-$(16,4,1)$ *design* を *subdesign* として含むならば、$(X,\mathcal{B})$ は *Non self-orthogonal* 2-$(21,6,4)$ *design* である。

Proof. $S = A_1 \cup A_2$ (disjoint) と置き、(P, A_1) を 2-$(16,4,1)$ design そして、$H_1, \cdots, H_5$ をそのデザインの平行類とする。すると、$B \in H_i, B' \in H_j$ $(i \neq j)$ に対して、$|B \cap B'| = 1$ である。ここで、D が self-orthogonal design であると仮定する。すると、D の任意の 2 つのブロックは 0 または 2 点で交わるから、1 点で交わる R の 2-subsets が 5 個存在しなければならない。しかし $|R| = 5$ より、1 点で交わる R の 2-subsets は高々 4 個である。よって矛盾より、D は Non self-orthogonal design である。 □

resolvable 2-$(16,4,2)$ design において位数 4 のアフィン平面 を subdesign として含まないデザインは全体の 1.5% 程度であるが、このデザインから self-orthogonal 2-$(21,6,4)$ design の一意性の別証明[5]、また特徴付けを考えている。

3 2-$(n^2+n+1, n+2, n)$ designs

この章では、Proposition 2.2 のデザインの構成の一般化を試みる。ここでは、デザインの点集合を n^2 と $n+1$ に分割した場合を考えて、整数的条件をみたすデザインのパラメータとして 2-$(n^2+n+1, n+2, n)$ design を挙げる。このデザインの構成法は次の通りである。

構成法 (*)

- (P, Q) : 2-$(n^2, n+2, \frac{n}{2})$ design
- (P, S) : resolvable 2-$(n^2, n, \frac{n}{2})$ design
  $H_1, \cdots, H_{\frac{n(n+1)}{2}}$: 平行類
- (R, S) : $\binom{n+1}{2} \times n$

そして、全単射 $\phi : \binom{n+1}{2} \to \{H_1, \cdots, H_{\frac{n(n+1)}{2}}\} = \{\phi(x,y) | \{x,y\} \in \binom{n+1}{2}\}$ に対して、$S' = \{A \cup \{x,y\} | A \in \phi(x,y), \{x,y\} \in \binom{n+1}{2}\}$ とする。ここで、$X = P \cup R$, $\mathcal{B} = Q \cup S'$ と置く。すると、$(X, \mathcal{B})$ は 2-$(n^2+n+1, n+2, n)$ design である。

	P	R
Q	2-$(n^2, n+2, \frac{n}{2})$ design	0
S	resolvable 2-$(n^2, n, \frac{n}{2})$ design	$\binom{n+1}{2} \times n$

[5] 証明として、古典的には位数 4 の射影平面の hyper ovals の集合を扱ったもの、Goethals, Seidel [3] の Witt system W_{24} の一意性を利用した構成によるもの、Tonchev [10] によるコード理論との関係を用いたものが挙げられる。

次に、 2-$(n^2+n+1, n+2, n)$ design の存在性について述べる。

Proposition 3.1. 2-$(n^2+n+1, n+2, n)$ *design* が存在するならば、$n=2,4,10$ である。

Proof. 2-$(n^2+n+1, n+2, n)$ design のブロックの総数を b とする。すると、$b=\frac{n^2(n^2+n+1)}{n+2}$ は正の整数より、

$$\begin{aligned} b &= \frac{n^2(n^2+n+1)}{n+2} \\ &= \frac{(n+2)^4-7(n+2)^3+19(n+2)^2-24(n+2)+12}{n+2} \end{aligned}$$

よって、$\frac{12}{n+2}$ は正の整数である。ゆえに、$n=2,4,10$ である。 □

D を 2-$(n^2+n+1, n+2, n)$ design とする。 $n=2$ ならば、D は symmetric 2-$(7,4,2)$ design である。(位数 2 の射影平面の complementary design)

symmetric 2-design の条件を少し弱めたデザインとして次のような概念がある。

Definition 3.2. 2-design の block intersection numbers が 2 つの値だけをもつ時、そのデザインを quasi-symmetric design と呼ぶ。

Proposition 3.3. $n \neq 2$ とする。2-$(n^2+n+1, n+2, n)$ *design* D が *self-orthogonal* ならば、D は *block intersection numbers* が 0 と 2 である *quasi-symmetric design* である。

Proof. D の 1 つのブロック B に対して、 $m_i(B)$ (m_i と略記する) を B と i 点で交わるブロックの個数とする。ここで、Proposition 3.1 と D は self-orthogonal より i は偶数 $(i=0,2,4,\cdots,n)$ である。すると、

$$\sum_{i=0}^{n} m_i = b-1 \tag{1}$$

$$\sum_{i=0}^{n} i m_i = (r-1)(n+2) = (n^2-1)(n+2) \tag{2}$$

$$\sum_{i=0}^{n} \binom{i}{2} m_i = (n-1)(n+2)(n+1) = (n^2-1)(n+2). \tag{3}$$

(2) と (3) より、$i \geq 4$ に対して $m_i=0$ を得る。よって、(1) より $m_0=\frac{n(n^2-1)(n-2)}{2(n+2)}$, $m_2=\frac{(n^2-1)(n+2)}{2}$ となり、D は block intersection numbers が 0 と 2 である quasi-symmetric design である。 □

表 2: The list of 2-$(n^2+n+1, n+2, n)$ design

2-$(n^2+n+1, n+2, n)$ design	self-orthogonal	non self-orthogonal
2-$(7,4,2)$ design	existence (unique)	non-existence
2-$(21,6,4)$ design	existence (unique)	existence (proposition 2.2)
2-$(111,12,10)$ design	non-existence (Sane)	?

ここで、 2-$(n^2+n+1, n+2, n)$ design の self-orthogonal の条件に対する存在性についてまとめたリストを表 2 に挙げる。2-$(7,4,2)$ design と 2-$(21,6,4)$ design については 1 章 および 2 章で述べた。2-$(111,12,10)$ design について self-orthogonal を仮定すると Proposition 3.3 より quasi-symmetric design となるが、このデザインの存在性について次のような Sane [8] による結果がある。

Theorem 3.4. (*Sane*)
位数 10 の射影平面の拡大デザインが存在することと、*quasi-symmetric* 2-$(111,12,10)$ *design* の存在は同値である。

位数 10 の射影平面に関する結果として、Lam, Mckay, Swiercz and Thiel [5] と Lam, Swiercz and Thiel [6] による次のような 2 つの定理がある。

Theorem 3.5. *(Lam, Mckay, Swiercz and Thiel)*
位数 10 の射影平面は拡大をもたない。

Theorem 3.6. *(Lam, Swiercz and Thiel)*
位数 10 の射影平面は存在しない。

Theorem 3.4 と Theorem 3.5 より、quasi-symmetric 2-$(111,12,10)$ design の非存在が証明される[6]。この quasi-symmetric 2-$(111,12,10)$ design の非存在を Theorem 3.5 および Theorem 3.6 を使わずに独立に証明することができるかどうかという課題が考えられるが当然のように難しい問題と思える。

今回は、Theorem 3.6 および射影平面の存在とアフィン平面の存在の同値性を利用した証明[7]ができることを報告する。ここでは、証明は詳しく述べないが次の補題が大きな役割を果たしている。

Lemma 3.7. $D=(X,\mathcal{B})$ を 2-$(111,12,10)$ *design* とする。D が *self-orthogonal* ならば、任意の $B\in\mathcal{B}$ に対して、$|B\cap Y|=0$ または 2 となる X の 11 点の部分集合 Y が存在する。

[6]参考文献 として Mavron, Shrikhande [7] も挙げる。Sane [8] の論文の中では、quasi-symmetric 2-$(111,12,10)$ design の非存在は書かれていない。

[7]筆者は当初 Sane の結果を全く知らずに研究していたため少々ニュアンスの異なる証明ができたと思っている。

概要としては、この補題よりブロックの部分集合に位数 10 のアフィン平面の dual が存在しなければならないことが示されて、Theorem 3.6 に矛盾するというものである。

Non self-orthogonal 2-(111, 12, 10) design について、2-(100, 12, 5) design と resolvable 2-(100, 10, 5) design が両方とも存在すれば、構成法 (∗) により Non self-orthogonal 2-(111, 12, 10) design の存在が示せるが、2-(100, 12, 5) design と resolvable 2-(100, 10, 5) design のどちらも存在または非存在は知られていないようである。

参考文献

[1] P.C.Cameron and J.H.Van Lint, *Designs, Graphs, Codes and their Links,* London Mathematical Society Student Texts 22, Cambridge University Press, Cambridge (1991).

[2] C.J.Colbourn and J.H.Dinitz, *The CRC Handbook of Combinatorial Designs,* CRC Press, Boca Raton, (1996).

[3] J.M.Goethals and J.J.Seidel, Strongly regular graphs derived from combinatorial designs, *Canadian J. Math.* 22 (1970), 597-614.

[4] P.Kaski and P.R.J.Östergård, Miscellaneous classification results for 2-designs, *Discrete Math.* (in print)

[5] C.W.Lam, J.Mckay, S.Swiercz and L.Thiel, The nonexistence of ovals in a projective planes of order 10, *Discrete Math.* 45 (1983), 319-321.

[6] C.W.Lam, S.Swiercz and L.Thiel, The nonexistence of finite projective planes of order 10, *Canadian J. Math.* 41 (1989), 1117-1123.

[7] V.C.Mavron and M.S.Shrikhande, On designs with intersection numbers 0 and 2, *Arch. Math.* 52 (1989), 407-412.

[8] S.S.Sane, On extendable planes of order 10, *J. Combinatorial Theory (A).* 38 (1985), 91-93.

[9] S.S.Sane and M.S.Shrikhande, Quasi-symmetric designs and biplanes of characteristic three, *J. Combinatorial Theory (A).* 60 (1992), 104-116.

[10] V.D.Tonchev, Quasi-symmetric designs and self-dual codes, *European J. Combin.* 7 (1986), 67-73.