Self-Orthogonal Designs

東北大学大学院情報科学研究科
宗政 昭弘 (Akihiro Munemasa)
Graduate School of Information Sciences,
Tohoku University
October 4, 2005

1 Introduction

It is well-known that for any positive integer $t$, a nontrivial $t$-$(v,k,\lambda)$ design exists for some $v,k,\lambda$. However, it seems that there are very few self-orthogonal $t$-designs known for large $t$. Recall that a $t$-$(v,k,\lambda)$ design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is said to be self-orthogonal if the parity of the size of intersection of any two blocks is the same as the parity of $k$.

The purpose of this talk is to formulate a conjecture on the nonexistence of self-orthogonal designs for large $t$ with $t \geq \left\lceil \frac{k}{4} \right\rceil + 1$, where $k$ is even. We show that the conjecture is true for $(t,k) = (6,20)$, for example. The method employed is the same as the one developed in [1], where a self-orthogonal 5-$(72,36,78)$ design is investigated.

2 Saturated designs

Definition 1. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a self-orthogonal $t$-$(v,k,\lambda)$ design. Assume that $k$ is even, so that the binary code $C$ generated by the rows of the block-point incidence matrix of $\mathcal{D}$ is self-orthogonal. We call the design $\mathcal{D}$ saturated, if $C$ is self-dual, $C$ has minimum weight $k$, and every minimum weight codeword of $C$ is the support of a block of $\mathcal{D}$. 
Let \( k = (k_1, \ldots, k_t) \) be a nonzero left null vector of the \( t \times (t + 1) \) matrix
\[
A_t = \begin{pmatrix}
2 & 4 & \cdots & 2(t-1) \\
3 & 5 & \cdots & 2(t-1) \\
\vdots & \vdots & \ddots & \vdots \\
(t) & (t+1) & \cdots & 2(t-1)
\end{pmatrix}
\]
(1)

Since the matrix \( A_t \) has rank \( t-1 \), the vector \( k \) is unique up to a scalar multiple.

**Lemma 1.**
\[
\sum_{i=1}^{t} i(-2)^{t-i-1} \binom{2t-i-1}{i} \binom{2j}{i} = (-1)^{t-1} 2^{t-j} t \binom{j}{t}.
\]
**Proof.** Induction on \( j \). \( \square \)

**Proposition 2.** Let \( \mathcal{D} = (\mathcal{P}, \mathcal{B}) \) be a self-orthogonal \( t-(v, k, \lambda) \) design. Assume that \( k \) is even, so that the binary code \( C \) generated by the rows of the block-point incidence matrix of \( \mathcal{D} \) is self-orthogonal. If \( C \) has minimum weight \( k \) and
\[
t \geq t_0 := \left\lceil \frac{k}{4} \right\rceil + 1,
\]
then
\[
\lambda_s = \frac{(-1)^{t_0-1} 2^{t_0-1} t_0 \binom{k/2}{t_0}}{\sum_{i=1}^{t_0} i(-2)^{t-i-1} \binom{2t-i-1}{i} \prod_{j=i}^{t_0-1} \frac{v-j}{k-j}} \prod_{j=s}^{t_0-1} \frac{v-j}{k-j}
\]
(3)
is an integer for \( s = 0, 1, \ldots, t_0 \).

**Proof.** Fix a block \( B_0 \) of \( \mathcal{D} \). Since \( X \) is a \( t_0 \)-design, we have
\[
\sum_{B \in \mathcal{B}} \binom{|B \cap B_0|}{i} = \lambda_i \binom{k}{i} \quad (i = 1, 2, \ldots, t_0),
\]
(4)
where
\[
\lambda_i = \lambda_{t_0} \prod_{j=1}^{t_0-1} \frac{v-j}{k-j}.
\]
(5)
Put
\[
n_j = |\{ B \in \mathcal{B} \mid 2j = |B \cap B_0| \}| \quad (j = 0, 1, 2, \ldots).
\]
Since $C$ has minimum weight $k$, $|B \cap B_0| \leq k/2$ unless $B = B_0$. Thus 

$$n_j = 0 \text{ for } j > \lfloor \frac{k}{4} \rfloor, \ j \neq \frac{k}{2};$$

and obviously $n_{k/2} = 1$. Now (4) can be written as

$$\sum_{j=0}^{t_0-1} (\begin{array}{l}2j \end{array}) n_j = (\lambda_i - 1) (\begin{array}{l}k \end{array}) \quad (i = 1, 2, \ldots, t_0).$$

Let $k = (k_1, \ldots, k_{t_0})$ be the vector defined by

$$k_i = i (-2)^{i-1} \binom{2t_0 - i - 1}{t_0 - 1}.$$

Then $k$ is a left null vector of $A_{t_0}$ by Lemma 1, and hence we have

$$\sum_{i=1}^{t_0} k_i \lambda_i \binom{k}{i} = \sum_{i=1}^{t_0} k_i \lambda_i \binom{k}{i}.$$

By (6) we have

$$\lambda_{t_0} \sum_{i=1}^{t_0} k_i \lambda_i \prod_{j=i}^{t_0-1} \frac{v-j}{k-j} = \sum_{i=1}^{t_0} k_i \lambda_i \binom{k}{i}.$$

Applying (5) again, we obtain

$$\lambda_{t_0} = \sum_{i=1}^{t_0} k_i \lambda_i \prod_{j=i}^{t_0-1} \frac{v-j}{k-j}.$$ 

The result then follows from (7) and Lemma 1.

As a special case of (3), we have

$$\lambda_{t_0} = \frac{(-1)^{t_0-1} 2^{2t_0-1} t_0 (\begin{array}{l}k/2 \end{array})}{\sum_{i=1}^{t_0} i (-2)^{i-1} \binom{2t_0-i-1}{t_0-1} \prod_{j=i}^{t_0-1} \frac{v-j}{k-j}}.$$

Observe that the denominator is a polynomial in $v$ of degree $t_0 - 1$ with positive leading coefficient. Thus, for a given $t_0$, there are only finitely many $v$ for which $\lambda_{t_0}$ is an integer.
Proposition 3. Let $D = (\mathcal{P}, B)$ be a self-orthogonal $t$-(v, k, \lambda) design, where $k < v$. Assume that $k$ is even, so that the binary code $C$ generated by the rows of the block-point incidence matrix of $D$ is self-orthogonal. If $C$ has minimum weight $k$ and

\[ t \geq t_0 := \left\lfloor \frac{k}{4} \right\rfloor + 1 \text{ and } k \leq 24, \]  

then

\[
(t_0, v, k, \lambda) = (1, v, 2, 1),
(2, 7, 4, 2), (2, 8, 4, 3), (2, 9, 4, 6),
(2, 16, 6, 2), (2, 21, 6, 4), (2, 22, 6, 5), (2, 24, 6, 10), (2, 25, 6, 20),
(3, 16, 8, 3), (3, 22, 8, 12), (3, 23, 8, 16), (3, 24, 8, 21),
(3, 25, 8, 28), (3, 29, 8, 16), (3, 30, 8, 12), (3, 32, 8, 7),
(3, 26, 10, 3), (3, 42, 10, 9), (3, 46, 10, 8), (3, 50, 10, 6),
(4, 47, 12, 15), (4, 48, 12, 36), (4, 51, 12, 2640),
(5, 56, 16, 42), (5, 64, 16, 91), (5, 72, 16, 78),
(7, 120, 24, 231).
\]

Proof. If $k = 2$, then clearly $\lambda = 1$.

If $k = 4$, then

\[ \lambda = \frac{6}{10 - v}, \]

hence $v = 7, 8$ or 9.

If $k = 6$, then

\[ \lambda = \frac{20}{26 - v}, \]

hence $v = 16, 21, 22, 24, 25$.

If $k = 8$, then

\[ 0 \geq 336 \left( \frac{1}{\lambda} - 1 \right) \]
\[ = (v - 8)(v - 44), \]

hence $8 < v \leq 44$. Since $\lambda_3, \ldots, \lambda_0$ are also integers, we have $v = 16, 22, 23, 24, 26, 29, 30$ or 32.
If $k = 10$, then

\[0 \geq 1152\left(\frac{1}{\lambda} - 1\right) - (v - 10)(v - 74),\]

hence $10 < v \leq 74$. Since $\lambda_3, \ldots, \lambda_0$ are also positive integers, we have $v = 10, 26, 42, 46$ or $50$.

If $k = 12$, then

\[\lambda = \frac{31680}{v^3 - 127v^2 + 5456v - 80592},\]

hence

\[0 \geq v^3 - 127v^2 + 5456v - 80592 = v^2(v - 127) + 5456(v - 15) + 1248.\]

This implies $v < 127$. Since $\lambda_4, \ldots, \lambda_0$ are also positive integers, we have $v = 12, 36, 47, 48, 51, 52$ or $57$.

If $k = 14$, then

\[\lambda = -\frac{549120}{5v^3 - 875v^2 + 52952v - 1132668},\]

hence

\[0 \geq 5v^3 - 875v^2 + 52952v - 1132668 = 5v^2(v - 175) + 52950(v - 22) + 32232.\]

This implies $v \leq 174$. Since $\lambda_4, \ldots, \lambda_0$ are also positive integers, we have $v = 14$.

If $k = 16$, then

\[\lambda = \frac{4193280}{v^4 - 235v^3 + 20960v^2 - 848000v + 13292544},\]

hence

\[0 \geq 4193280\left(\frac{1}{\lambda} - 1\right) = (v - 16)(v^2(v - 219) + 17456(v - 33) + 7344).\]
Thus $v < 219$. Since $\lambda_5, \ldots, \lambda_0$ are also positive integers, we have $v = 16, 56, 64$ or 72.

If $k = 18$, then

$$0 \geq 102359040 \frac{1}{\lambda(18)} - 1$$

$$= 7v^3(v - 299) + 240404v(v - 53) + 37200v + 162256464.$$ 

Thus $16 \leq v < 299$. Since $\lambda_5, \ldots, \lambda_0$ are also positive integers, we have $v = 18$.

If $k = 20$, then

$$0 > \frac{5000970240}{\lambda}$$

$$- 7v^4(v - 376) + 399861v^2(v - 78) + 1215608048(v - 17)$$

$$+ 350602v^2 + 887460016,$$

hence $v < 376$. Since $\lambda_5, \ldots, \lambda_0$ are also positive integers, we have $v = 20$.

If $k = 22$, then

$$0 > - \frac{2500485120}{\lambda}$$

$$= v^4(v - 456) + 84659v^2(v - 96) + 394932588(v - 21)$$

$$+ 79328v^2 + 200001388,$$

hence $v < 456$. Since $\lambda_5, \ldots, \lambda_0$ are also positive integers, we have $v = 22$.

If $k = 24$, then

$$0 \geq 148852408320 \frac{1}{\lambda} - 1$$

$$= (v - 24)((v - 526)(v^4 + 114511v^2 + 47117192v + 25600739920)$$

$$+ 13441571438560),$$

hence $v < 526$. Since $\lambda_5, \ldots, \lambda_0$ are also positive integers, we have $v = 24$ or 120.

\[\square\]

3 Unsaturated designs

In this section we let $D = (\mathcal{P}, \mathcal{B})$ be a self-orthogonal $t$-$(v, k, \lambda)$ design with $k$ even, so that the binary code $C$ generated by the rows of the block-point
incidence matrix of $\mathcal{D}$ is self-orthogonal. We assume that the design $\mathcal{D}$ is unsaturated, i.e., either $C$ is not self-dual, or $C$ has a codeword of weight at most $k$ different from the support of a block of $\mathcal{D}$. This implies that there exists a coset $x + C$, possibly equal to $C$, such that it contains a nonzero vector with minimal weight other than the support of any block of $\mathcal{D}$. Let $S$ be the support of such a vector, put $m = |S|$. Then

$$|B \cap S| \leq \frac{k}{2}$$

for any block $B$. Since

$$\sum_{B \in \mathcal{B}} \binom{|B \cap S|}{i} = \lambda_i \binom{m}{i} \quad (i = 1, 2, \ldots, t),$$

putting

$$n_j = |\{B \in \mathcal{B} | 2j = |B \cap B_0|\} | \quad (j = 0, 1, 2, \ldots),$$

we have

$$\sum_{j=0}^{[k/4]} \binom{2j}{i} n_j = \lambda_i \binom{m}{i}.$$  

Assume

$$t \geq t_0 := \left\lfloor \frac{k}{4} \right\rfloor + 1.$$ 

Then, as in the previous section, we have

$$\sum_{i=1}^{t_0} i (-2)^{i-1} \binom{2t_0 - i - 1}{i} \lambda_i \binom{m}{i} = 0$$

By (5), we have

$$\sum_{i=1}^{t_0} i (-2)^{i-1} \binom{2t_0 - i - 1}{i} \binom{m}{i} \prod_{j=1}^{t_0-1} \frac{v - j}{k - j} = 0 \quad (11)$$

If $k$ is given, then this is a Diophantine equation in $m, v$. The only integer solutions of equation (11) in the range $0 < m < v \leq 1000, k = 8, 10, \ldots, 20$
are

\[ k = 8, (v, m) = (16, 4), (16, 6), (22, 6), (22, 7), (23, 7), \]
\[ k = 10, (v, m) = (20, 4), (22, 6), (26, 6), \]
\[ k = 12, (v, m) = (24, 8), (36, 8), (47, 11), (68, 16), (156, 36), (311, 71), \]
\[ k = 14, (v, m) = (80, 16), (159, 31), \]
\[ k = 16, (v, m) = (32, 8), (43, 8), (43, 11), (48, 12), (56, 12), (58, 13), \]
\[ k = 18, (v, m) = (36, 8). \]

Therefore, we obtain the following result.

**Proposition 4.** Let \( D = (\mathcal{P}, \mathcal{B}) \) be a self-orthogonal \( t-(v, k, \lambda) \) design. Assume that \( k \) is even, and \( t \geq \left\lceil \frac{k}{4} \right\rceil + 1 \), and \( 8 \leq k \leq 20, 2k \leq v \leq 1000 \). The binary code \( C \) generated by the rows of the block-point incidence matrix \( M \) of \( D \) is self-dual and the codewords of \( C \) of weight \( k \) are precisely the rows of \( M \), unless \( (k, v) \) is one of the pairs listed above, in which case, either \( C^\perp/C \) contains a coset of weight \( m \) whose values are listed above.

**References**