Lecture 11

(t- design) May, 2, 4

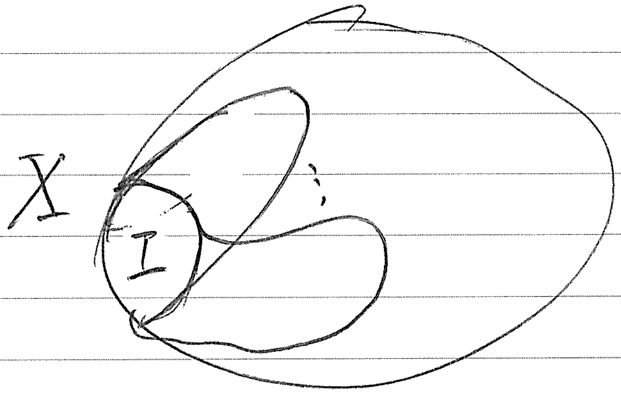
When $t \geq 3$, then finding a good t-design is getting more complicate especially when the block size is also larger. The followings are some basic properties of t-designs.

- If $(X, \mathbb{B})$ is a t-(v,k,λ) design, then

(a) $\lambda \binom{v}{t} / \binom{k}{t}$ is an integer,

(b) for each $0 \leq i \leq t$, the collection of all blocks $\mathbb{B}_i$ containing a given i-subset of X is exactly $\lambda \binom{v-i}{t-i} / \binom{k-i}{t-i}$, and

(c) if I is an i-subset with $i \leq t$, then the collection of blocks $\mathbb{B}_i = \{ B \setminus I \mid B \in \mathbb{B} \}$ is a $(t-i)$-$(v-i, k-i, \lambda)$ design. with $X_i = X - I$



- Let $k \geq t \geq 2$ Then, the collection of all k-subsets of $X = \mathbb{Z}_v$ is in fact a t-design $t-(v,k,\lambda)$ design where $\lambda = \binom{v-t}{k-t}$ if $k > t$ and $\lambda = 1$ if $k = t$.

- If $k=3$ and $t=2$, then $\binom{\mathbb{Z}_v}{3}$ forms a $2-(v,3,\lambda)$ design where $\lambda = v-2$. (If $k=4$ and $t=2$, then $\binom{\mathbb{Z}_v}{4}$ is a $2\text{-}(v,4,\lambda)$ design with $\lambda = \binom{v-2}{2}$.)

- In case of $k=3$, if $\binom{\mathbb{Z}_v}{3}$ can be partitioned into $v-2$ disjoint STS(v)'s, then we have a <u>large set of Steiner triple systems</u>.

(*) You may try the case when $v=7$ and $k=3$.

- <u>Theorem</u> (Lu, Jia-Xi, 陸家羲) <u>1935–1983</u> 高中老师

  A large set of STS(v)'s exists except for some small cases.

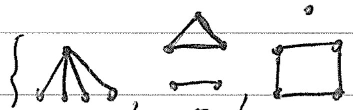
<u>Definition</u> (<u>Steiner systems</u>)

In a t-design $(X,\mathcal{B})$, if $k = t+1$ and $\lambda = 1$, Then we have a Steiner t-design of order $|X|$. A Steiner triple system of order v is a $2-(v,3,1)$ design and a Steiner quadruple system of order v is a $3-(v,4,1)$ design or $S(t,k,v)$ in short where $t = k-1$.

- <u>Small examples</u> $t=3$ and $k=4$

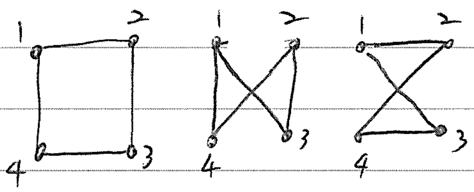
Let $X = \mathbb{Z}_2^4$ and $\mathcal{B} = \left\{ \{\vec{w}, \vec{x}, \vec{y}, \vec{z}\} \;\middle|\; \begin{array}{l} \vec{w}, \vec{x}, \vec{y}, \vec{z} \in \mathbb{Z}_2^4, \\ \vec{w} + \vec{x} + \vec{y} + \vec{z} = \vec{0} \end{array} \right\}$.

Notice that $\vec{x}, \vec{y}, \vec{z}$ and $\vec{w}$ are distinct vectors. Then, $(\mathbb{Z}_2^4, \mathcal{B})$ is an $S(3,4,16)$. <u>It is also true for an $S(3,4,2^m)$ where $m \in \mathbb{N}$.</u>

- Let $X = E(K_5)$ and $\mathcal{B} = \{$  $\mid$ labeled subgraphs of $K_5 \}$.

$\binom{5}{1}$, $\binom{5}{3}$, $3\binom{5}{4}$

Then, $(X, \mathcal{B})$ is an $S(3,4,10)$.



$(1,2,3,4)$, $(1,3,2,4)$, $(1,2,4,3)$

- How about $t=3$ and v in general?

- $v \equiv 2$ or $4 \pmod 6$. (Let $(X, \mathcal{B})$ be an $S(3,4,v)$.)

Let $x_0 \in X$ and $\mathcal{B}' = \{ B \setminus \{x_0\} \mid B \in \mathcal{B} \}$. Then, $(X', \mathcal{B}')$ is an $STS(v-1$
$(X' = X \setminus \{x_0\})$

This implies that $|X'| = v-1 \equiv 1$ or $3 \pmod 6$.

- <u>Theorem</u> (H. Hanani, 1960)

An $S(3,4,v)$ exists if and only if $v \equiv 2$ or $4 \pmod 6$.

<u>Proof.</u> It takes a lot of effort in proving the sufficient part.

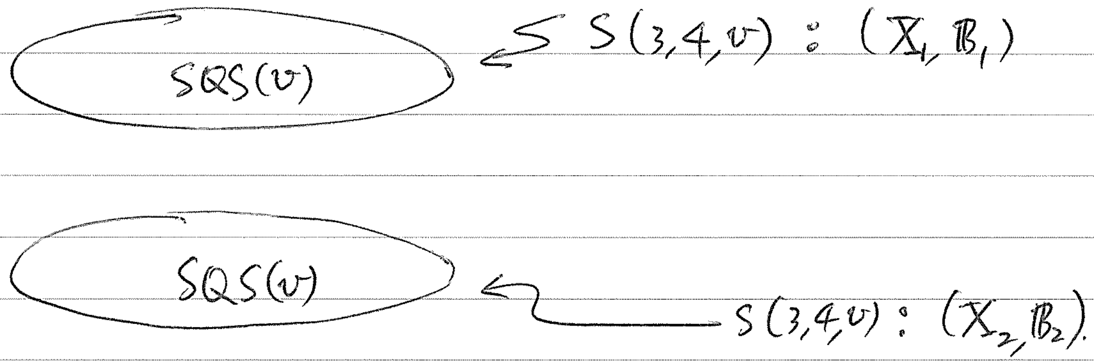
SEASON

Doubling Construction

Construct 1. An $S(3,4,2v)$ exists if an $S(3,4,v)$ exists.

Proof.

(a)



Let K_{X_i} denote the complete graph defined on X_i, $i=1,2$. Since $|X_i|$ is even, K_{X_i} can be decomposed into 1-factors, there are $v-1$ of them, called $F_1, F_2, \cdots, F_{v-1}$ and $G_1, G_2, \cdots, G_{v-1}$ for $i=1,2$ respectively. Now, we use F_j and G_j, $j=1,2,\cdots,v-1$ to defind $\left(\frac{v}{2}\right)^2$ quadruples by the following way:

$$F_j = \left\{ \{a_i, b_i\} \mid i=1,2,\cdots,\tfrac{v}{2} \right\}$$
$$\Rightarrow \{a_i, b_i, c_j, d_j\} \in \mathbb{B}.$$
$$G_j = \left\{ \{c_j, d_j\} \mid j=1,2,\cdots,\tfrac{v}{2} \right\}$$

Combining with $\mathbb{B}_1$ and $\mathbb{B}_2$, we have an $S(3,4,2v)$. (or $SQS(2v)$).

(*). This $SQS(2v)$ contains two disjoint sub-design $SQS(v)$.

SEASON

(b) Let $Y' = \{y' \mid x \in Y\}$ and $X = Y \cup Y'$. Let $(Y, \mathbb{C})$ be an $SQS(v)$.

Define $\mathbb{B}$.

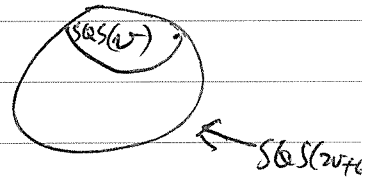
(1) $\forall \{x, y, z, w\} \in \mathbb{C}$, let $\{x, y, z, w'\}, \{x, y, z', w\}, \{x, y', z, w\}$, $\{x', y, z, w\}, \{x', y', z', w\}, \{x', y', z, w'\}, \{x', y, z', w'\}$ and $\{x, y', z', w'\}$ be in $\mathbb{B}$.

(2) For any two elements $\{x, y\} \subseteq Y$, let $\{x, y, x', y'\} \in \mathbb{B}$.

Combining (1), (2), we have an $SQS(2v) = (X, \mathbb{B})$.

It is a routine matter to check $(X, \mathbb{B})$ is indeed an $SQS(2v)$ for both constructions: (a) and (b).

The above doubling construction can only handle the cases $v \equiv 4$ or $8 \pmod{12}$. For the other cases, it takes more effort. (We omit the details here.)



<u>Conjecture</u> $v \to 2v+6$ Construction

For each $SQS(v)$, there exists an $SQS(2v+6)$ which contains $(X_1, \mathbb{B}_1)$ as a subsystem.

(*) If we have $v \to 2v$ and $v \to 2v+6$ constructions, then the theorem about the existence of SQS(v)'s is proved.

Proof. Consider $v \equiv 2$ or 4 or 8 or $10 \pmod{12}$. Clearly, if $v \equiv 4$ or $8 \pmod{12}$, then by $v \to 2v$, we can construct such a system. On the other hand, if $v \equiv 2$ or $10 \pmod{12}$, let $v = 12k+2$ or $12k+10$ respectively. By direct counting, $12k+2 = 2(6k-2)+6$ and $12k+10 = 2(6k+2)+6$. Hence, the construction $v \to 2v+6$ works. ▨

The best known construction besides $v \to 2v$ on SQS(v) is the following

Theorem (Hartman) (Tripling Construction!)

If an SQS(v) contains a subsystem SQS(u), then there exists an SQS($3v-2u$) which contains the above SQS(v).

Note that we can also use this theorem to prove the cases $v \equiv 2$ or $10 \pmod{12}$ except some small cases. (?)

$v \equiv 2$ or $10 \pmod{12}$

$\Longrightarrow v \equiv 2, 10, 14, 22, 26, 34 \pmod{36}$

$$\begin{cases} 36k+2 = 3\cdot(12k+2) - 4 & (u=2) \\ 36k+10 = 3(12k+4) - 2 & u=1 \\ 36k+14 = 3(12k+10) - 16 & u=8 \\ 36k+22 = 3(12k+14) - 20 & u=10 \\ 36k+26 = 3(12k+14) - 16 & u=8 \\ 36k+34 = 3(12k+14) - 8 & u=4 \end{cases}$$

SQS(2) is a trivial system

$u=1$ (one element)

<u>Exercise 2.7.</u> (20 points)

Constructing SQS(v) for as many v as possible.

(*) Turn in your Homework (II) by combining 120 points. (at most)