Lecture 8

Recursive Constructions

April 11, 13

We may also use the idea of recursion to construct all STS(v). There are two constructions.

1. $v \to 2v+1$ (If an STS(v) exists, then an STS($2v+1$) exists.)

Since $v \equiv 1$ or $3 \pmod 6$, K_{v+1} is a complete graph of even order, and thus K_{v+1} can be decomposed into v 1-factors by way of $\chi'(K_{v+1}) = v$. Let $F_1, F_2, \cdots, F_v$ be the set of 1-factors mentioned above. Now, we are ready to construct an STS($2v+1$) $= (\mathbb{Z}_{2v+1}, \mathbb{B})$. Let the given STS($v$) be defined on $\{0, 1, 2, \cdots, v-1\}$ and $V(K_{v+1}) = \{v, v+1, \cdots, 2v\}$. Moreover, let $F_i = \{\{a_1^{(i)}, b_1^{(i)}\}, \cdots, \{a_{\frac{v+1}{2}}^{(i)}, b_{\frac{v+1}{2}}^{(i)}\}\}$ be the ith 1-factor, $i = 1, 2, \cdots, v$. So, $\mathbb{B}$ can be obtained by the following:

(a) If B is a triple (block) in STS(v), then $B \in \mathbb{B}$; and

(b) for each $i \in \{0, 1, 2, \cdots, v-1\}$, $\{i, a_j^{(i+1)}, b_j^{(i+1)}\} \in \mathbb{B}$ where $\{a_j^{(i+1)}, b_j^{(i+1)}\} \in F_{i+1}$. (Use $\langle i, F_{i+1} \rangle$ for convenience.)

It is a routine matter to check that $(X, \mathbb{B}) = (\mathbb{Z}_{2v+1}, \mathbb{B})$ is an STS($2v+1$).

2. $v \longrightarrow 2v+7$

This construction is more complicate comparing to the first one. The main idea comes from the graph $K_{v+7} \approx G(v+7; D)$ where $D = \{1, 2, \cdots, \frac{v+7}{2}\}$. That is, we can view K_{v+7} as a circulant graph with difference set D. By Stern and Lenz's Lemma, $G =_{def} K_{v+7} \setminus G(v+7, \{1,2,3\})$ can be v-edge-colored for each $v \geq 3$. This implies that G can be decomposed into v 1-factors $F_1, F_2, \cdots, F_v$. Now, we are ready to construct an $STS(2v+7)$ by way of an $STS(v)$ defined on $X = \{0, 1, 2, \cdots, v-1\}$. Let $(X, \mathbb{B}_1)$ be an $STS(v)$, and $STS(2v+7) = (\mathbb{Z}_{2v+7}, \mathbb{B})$.

It suffices to find $\mathbb{B}$. The triples of $\mathbb{B}$ are obtained as follows:

(a) $\forall\ B \in \mathbb{B}_1,\ B \in \mathbb{B}$;

(b) Decompose $G(v+7; \{1,2,3\})$ into K_3's defined on $\{v, v+1, \cdots, 2v+6\}$ and let each of them be a triple of $\mathbb{B}$; and

(c) $\langle i, F_{i+1} \rangle \subseteq \mathbb{B}$ for each $i = 0, 1, \cdots, v-1$. ($\langle i, F_{i+1} \rangle$ is similar to (b) in Case 1.)

Again, it is not difficult to check $(\mathbb{Z}_{2v+7}, \mathcal{B})$ is indeed an $STS(2v+7)$.

Based on the above two constructions, we conclude the proof by showing each $STS(u)$ can be obtained by recursive constructions $v \to 2v+1$ or $v \to 2v+7$. First, if $u = 6t+1$, then $u = 12s+1$ or $12s+7$. Since $12s+1 = \underset{\underset{3 \pmod 6}{\equiv}}{(6s-3)} \cdot 2 + 7$ and $12s+7 = (6s+1) \cdot 2 + 1$, an $STS(u)$ can be constructed recursively. On the other hand, if $u = 6t+3$, then $u = 12s+3$ or $12s+9$. Since $12s+3 = (6s+1) \cdot 2 + 1$ and $12s+9 = (6s+1) \cdot 2 + 7$, an $STS(u)$ can be constructed by the same reason. This concludes the proof. ■

Exercise 2.4. (30 points)

Prove that for each $v \equiv 1$ or $3 \pmod 6$, an $STS(v)$ exists by using three distinct constructions. (Not limited to the three ways provided in this note.)

補充說明

<u>Theorem</u> (Stern and Lenz)

Let $G(n;D)$ be a circulant graph with difference set D. If $\frac{n}{2}$ is an integer and $\frac{n}{2} \in D$, then $G(n;D)$ is of Class 1.

This theorem can be applied to prove the well-known Doyen-Wilson theorem on Steiner triple systems.

<u>Theorem</u> (Doyen and Wilson, 1973)

An $STS(v)$ can be embedded in an $STS(u)$ if and only if $u \geq 2v+1$.

<u>Proof.</u> ($\Rightarrow$) Let $(X_1, \mathbb{B}_1)$ be an $STS(v)$ and $(X, \mathbb{B})$ be an $STS(u)$ such that $X_1 \subseteq X$ and $\mathbb{B}_1 \subseteq \mathbb{B}$. Now, consider a fixed element in $X \setminus X_1$, say x_0. Then, for each element $x_i \in X_1$, the triple contain x_0 and x_i should be $\{x_0, x_i, y_i\}$ where $y_i \in X \setminus X_1$. Since there are v elements in X_1, $X \setminus X_1$ contains x_0, y_i, $i = 1, 2, \cdots, v$. Hence, $u \geq 2v+1$.

($\Leftarrow$) It takes some effort to finish the proof. (Omitted.)

Constructing Designs Using Latin Squares

To start, we use a well-known construction to construct an STS(v) where $v \equiv 3 \pmod 6$. Let $v = 6k+3$ and $L = [l_{ij}]$ be an idempotent commutative Latin square of order $2k+1$. Now, we are ready to construct the Steiner triple system of order $6k+3$.

(1) Let $X = \mathbb{Z}_3 \times \mathbb{Z}_{2k+1}$.

(2) $\forall\ i \in \mathbb{Z}_{2k+1}$, let $\{(0,i),(1,i),(2,i)\} \in \mathbb{B}$.

(3) $\forall\ i < j \in \mathbb{Z}_{2k+1}$, let $\{(0,i),(0,j),(1,l_{ij})\}$, $\{(1,i),(1,j),(2,l_{ij})\}$ and $\{(2,i),(2,j),(0,l_{ij})\}$ be triples in $\mathbb{B}$.

Then, $(X,\mathbb{B})$ is an STS($6k+3$).

It is easy to check any two elements of X will occur in a triple and we have in total $(2k+1) + 3 \cdot \frac{(2k+1)^2-(2k+1)}{2} = 2k+1+6k^2+3k$ $= 6k^2+5k+1 = \frac{(6k+3)(6k+2)}{6}$.

(*) If $(X,\mathbb{B})$ is an STS(v), then $|\mathbb{B}| = \frac{v(v-1)}{6}$.

(**) In difference method, the part $v \equiv 3 \pmod 6$ is comparatively more complicate, we can replace it with this construction if we only try to prove the "sufficient" direction.

We can use MOLS(n) to construct designs with larger blocks.

(***) The existence of an Affine plane of order n where n is a prime power.

Step 1. Construct $n-1$ MOLS(n), let them be $L^{(1)}, L^{(2)}, \cdots, L^{(n-1)}$.
(For convenience, we use $1, 2, \cdots, n$ for $\mathbb{Z}_n$.)

Step 2. Let $L^{(r)}$ and $L^{(c)}$ be the row-indices and column-indices squares respectively.

$$L^{(r)} = \begin{array}{|c|c|c|c|} \hline 1 & 1 & \cdots & 1 \\ \hline 2 & 2 & \cdots & 2 \\ \hline & & \vdots & \\ \hline n & n & \cdots & n \\ \hline \end{array} \qquad L^{(c)} = \begin{array}{|c|c|c|c|} \hline 1 & 2 & & n \\ \hline 1 & 2 & & n \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline 1 & 2 & & n \\ \hline \end{array}$$

Step 3. Let $\overline{X} = (\mathbb{Z}_n \cup \{\infty\}) \times \mathbb{Z}_n = X \cup (\{\infty\} \times \mathbb{Z}_n)$.

Step 4. $\forall\ i \neq j \in \mathbb{Z}_n$, let $\overline{B_{i,j}} = \{(0,i),(1,j),(2,L^{(1)}(i,j)),(3,L^{(2)}(i,j)),\cdots,(\infty,L^{(n-1)}(i,j))\}$ be a block in $\overline{\mathbb{B}}$. (There are n^2 blocks.)

Step 5. Let $\mathbb{B}' = \{ \overline{B_{i,j}} - (\infty, L^{(n-1)}(i,j)) \mid \overline{B_{i,j}} \in \overline{\mathbb{B}} \}$.

Step 6. Let $\mathbb{B} = \mathbb{B}' \cup \{ \{i\} \times \mathbb{Z}_n \mid i \in \mathbb{Z}_n \}$.

Then, we conclude the $(X, \mathbb{B})$ is an Affine plane of order n.

(***) Let $\overline{\overline{X}} = \{(\infty,\infty)\} \cup \overline{X}$ and $\overline{\overline{\mathbb{B}}} = \overline{\mathbb{B}} \cup \{ \{(\infty,\infty), \{i\} \times \mathbb{Z}_n\} \mid i \in \mathbb{Z}_n \}$.

Then $(\overline{\overline{X}}, \overline{\overline{\mathbb{B}}})$ is a projective plane of order n.

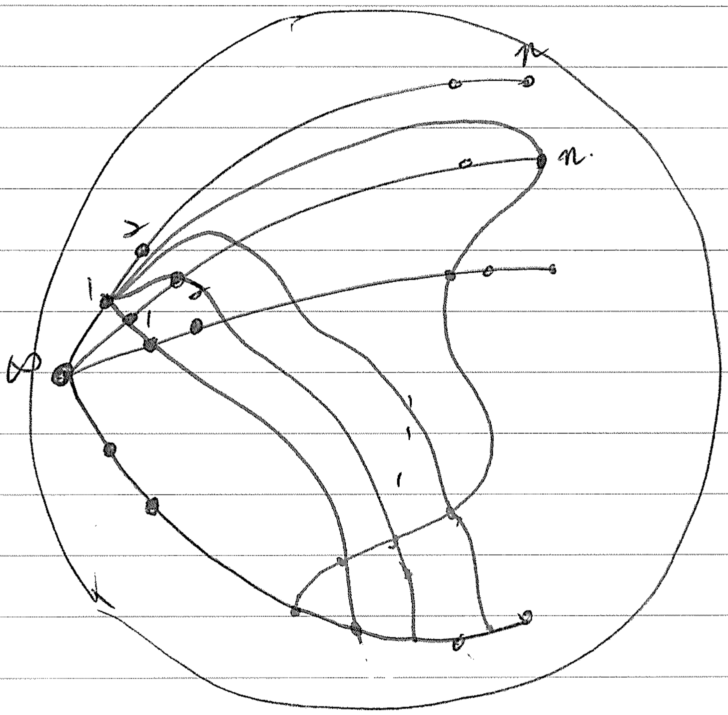
A complete family of MOLS(n)

$\approx \Downarrow$

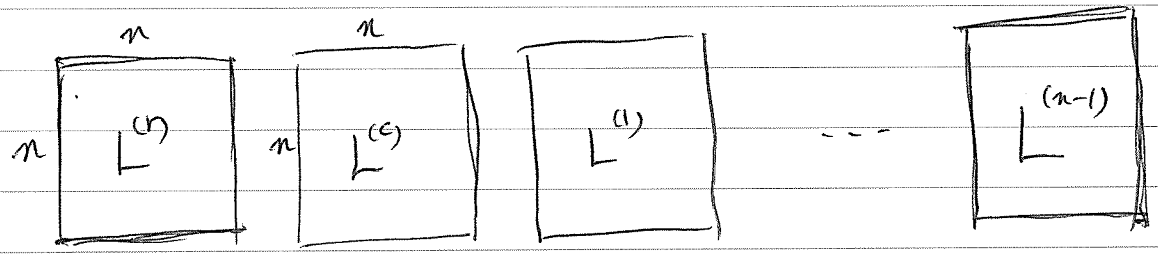
Affine plane of order n $\approx \Rightarrow$ Projective plane of order n

$\overset{?}{\Leftarrow} \approx$

$\overset{?}{\Rightarrow}$



projective plane

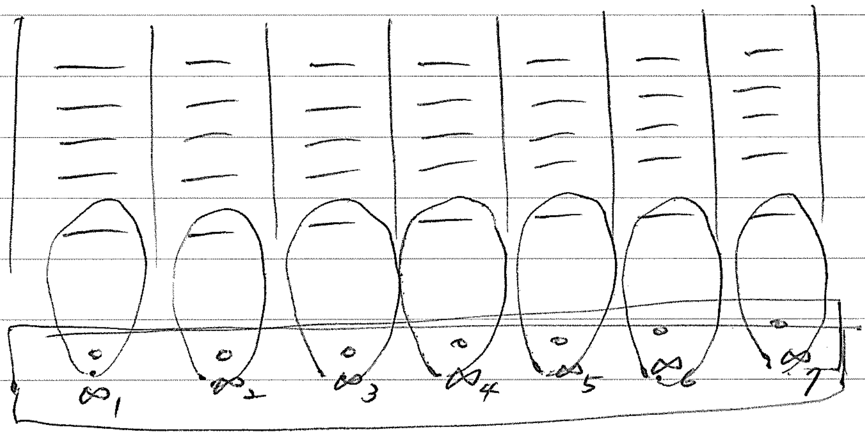


Here, we mention some PBD's.

<u>Theorem 1</u> For each $v \equiv 1 \pmod{3}$, there exists a 2-$(v, K, 1)$-design where $K = \{4, 7\}$ except $v = 10, 19$.

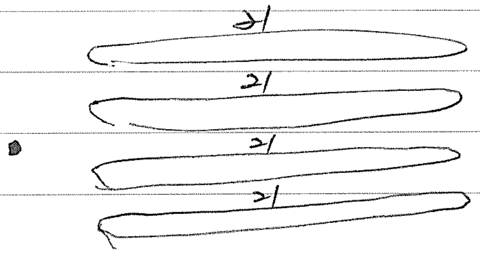
We omit the proof, but we present some examples here.

$v = 22$



By using a Kirkman triple system of order 15, we can attach 7 points in the "infinity" and obtain the desired PBD.

$v = 85$



First, we have a 2-$(85, \{4, 22\}, 1)$-design by using two MOLS(21). Then, a 2-$(85, \{4, 7\}, 1)$-design will be obtained from $v = 22$ case.