Lecture 11

The relationship between Latin squares and 2-design

Problem Can we use a Latin square to reprencent a Steiner triple system of order $v \equiv 1$ or $3 \pmod 6$?

Answer: Yes, but how?

Example A Latin square of order 7 which represents STS(7)

$*$	0	1	2	3	4	5	6
0	0	3	6	1	5	4	2
1	3	1	4	0	2	6	5
2	6	4	2	5	1	3	0
3	1	0	5	3	6	2	4
4	5	2	1	6	4	0	3
5	4	6	3	2	0	5	1
6	2	5	0	4	3	1	6

013
124
235
346
450
561
602

We can define a Latin square as a quasigroup $(X, *)$ such that $x*y = z = y*x$, $x*z = y = z*y$, $y*z = x = z*y$ if $\{x,y,z\} \in \mathcal{B}$, furthermore $\forall\, x \in X$, $x^2 = x$. In fact, this is an idempotent (commutative) total symmetric Latin square, i.e., $x^2 = x$, $x*(x*y) = y$ and $(x*y)*y = x$. Can you see this?

Example STS(9)

0	1	2
3	4	5
6	7	8

Blocks:

012	036	048	057
345	147	156	138
678	258	237	246

.

	0	1	2	3	4	5	6	7	8
0	0	2	1	6			3		
1	2	1	0						
2	1	0	2						
3	6			3	5	4	0		
4				5	4	3			
5				4	3	5			
6	3			0			6	8	7
7							8	7	6
8							7	6	8

The other entries can be filled by using $x*y=z$ if $\{x,y,z\}$ is a block.

If we don't use the three sub-squares in the diagonal, then we have a 3-GDD of type 3^3.

(*) Notice that the latin square is an idempotent Latin square.

(*) If $k=3$, then the square is indeed a total-symmetric Latin squre. For the case $k\neq 3$, then the representation will not be unique! (In fact, may not exist!)

($\Rightarrow$) only.

Proposition If $(X, \mathbb{B})$ is a $2-(v, K, 1)$ design such that there exists an idempotent Latin square of order $k \in K$, then there exists an idempotent Latin square of order v obtained from this construction.

Proof. It suffices to define a quasigroup $\langle X, * \rangle$ by using the idempotent $LS(k)$ for each $k \in K$. By the way, the idempotent $LS(k)$ is defined on the block B of size k. For example, if $B = \{x_1, x_2, \cdots, x_k\}$, then the Latin square will use x_i's as its entries. Now, we are ready for the Latin square of order v: L. Let $X = \{x_1, x_2, \cdots, x_v\}$. Then, let (1) $x_i^2 = x_i$, $i = 1, 2, \cdots, v$, and $x_i * x_j = x_k$ provided the (i,j)-entry in $B \supseteq \{x_i, x_j\}$ is x_k. It's not difficult to check that L is an idempotent Latin square. (See 3' for an example!) $\blacksquare$

Lemma A If there exist three mutually orthogonal $LS(n)$, then there exist two orthogonal idempotent $LS(n)$.

α-(12, {3,4}, 1) design

3'

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

0	2	1
2	1	0
1	0	2

0 1 2 3
0 0 0 0

4 5 6 7
0 0 0 0

8 9 10 11
0 0 0 0

B

0 4 8   0 1 2 3
1 5 9   4 5 6 7
2 6 10   8 9 10 11
3 7 11
0 5 10
0 6 11
0 7 9
1 4 11
1 6 8
1 7 10
2 4 9
2 5 11
2 7 8
3 4 10
3 5 8
3 6 9

Corresponding LS(12)

0	2	3	1	8				4			
3	1	0	2								
1	3	$\boxed{2}$	0	$\boxed{9}$					$\boxed{4}$		
2	0	1	3	10						4	
8		$\boxed{9}$	10	$\boxed{4}$	6	7	5		$\boxed{2}$	3	
				7	5	4	6				
				5	7	6	4				
				6	4	5	7				
4				0				8	10	11	9
		$\boxed{4}$		$\boxed{2}$				11	$\boxed{9}$	8	10
			4	3				9	11	10	8
								10	8	9	11

$$\begin{array}{|c|c|c|c|}\hline 0&1&2&3\\\hline 2&3&0&1\\\hline 3&2&1&0\\\hline 1&0&3&2\\\hline\end{array}\qquad\begin{array}{|c|c|c|c|}\hline 0&1&2&3\\\hline 1&0&3&2\\\hline 2&3&0&1\\\hline 3&2&1&0\\\hline\end{array}\qquad\begin{array}{|c|c|c|c|}\hline 0&1&2&3\\\hline 3&2&1&0\\\hline 1&0&3&2\\\hline 2&3&0&1\\\hline\end{array}$$

Idempotent (Diagonal) $\Leftarrow$ Unipotent $\Rightarrow$ Idempotent (Diagonal)

$$\begin{pmatrix}0&1&2&3\\0&2&3&1\end{pmatrix}\qquad\qquad\begin{pmatrix}0&1&2&3\\0&3&1&2\end{pmatrix}$$

Proof. We can permute either rows or columns simultaneously to obtain one unipotent Latin square. Then, the other two squares must be diagonal Latin squares. Therefore, by using permutation on entries, we obtain two orthogonal idempotent Latin squares. ∎

(***) Known result

For each $n > 10$, there exist two orthogonal idempotent Latin squares of order n.

Theorem Let $(X, \mathbb{B})$ be a 2-$(v, K, 1)$ design such that for each $k \in K$ there exist three orthogonal $LS(k)$. Then, there exists a pair of orthogonal $LS(v)$.

Proof. By Lemma A, for each $k \in K$, there exist two MOLS(k). Now, let L_1 and L_2 be obtained respectively by using two MOLS(k) in $(X, \mathbb{B})$. Then, it is easy to see that L_1 and L_2 are mutually orthogonal idempotent Latin squares of order v. (Use two fingers' rule!) ∎

Exercise 2.6. (10 points)

Write (in more details) down the proof of the above theorem.

Bonus

Prove that there exist two MOLS(n)'s for each $120 \geq n \geq 100$.