BIBD with $k = 3$

Facts.

1. A $2-(v, 2, \lambda)$ design exists for all $v \geq 2$.
   This is a direct consequence of using $\lambda \cdot K_v$.
2. A $2-(v, 3, 1)$ design exists if and only if $v \equiv 1$ or $3 \pmod 6$.
   This theorem was first proved by T. P. Kirkman in 1847. Later, there are many different proofs for this seeming easy but quite complicate 'fact'. (More details will be given later.)

Kirkman's 15 school girls problem.
Arrange 15 girls to line up in five rows with each row has three girls to walk to school. Can we complete that any two of girls stay in a row for some day in seven days?

We need at least 7 days since each day we use up 15 pairs and in total there are $\binom{15}{2} = 105$ pairs. So, the extra requirement is that every day, the arrangement is in fact a parallel class. Such designs are also known as Kirkman triple systems. Such systems of order v exists if and only if $v \equiv 3 \pmod 6$. Note that $AG(2, 3)$ is a Kirkman triple system of order 9. Here is an answer of 15 girls problem.

0	1	2	0	3	4	0	5	6	0	7	8	0	9	10	0	11	12	0	13	14
3	7	11	1	7	9	1	8	10	1	11	14	1	12	13	1	3	5	1	4	6
4	9	13	2	12	14	2	11	13	2	4	5	2	3	6	2	8	9	2	7	10
5	10	12	5	8	13	3	9	14	3	10	13	4	8	11	4	10	14	3	8	12
6	8	14	6	10	11	4	7	12	6	9	12	5	7	14	6	7	13	5	9	11

Figure 11.1

Theorem 11.1. *A* $2-(v,3,1)$ *design, known as a Steiner triple system of order* v*, exists if and only if* $v \equiv 1$ *or* $3 \pmod 6$.

Proof.
($\Rightarrow$) As mentioned earlier, if a $2-(v,3,1)$ design exists, then $r = \dfrac{v-1}{3-1} = \dfrac{v-1}{2}$ and $b = \dfrac{v(v-1)}{6}$ are both integers. This implies that $v \equiv 1$ or $3 \pmod 6$.
($\Leftarrow$) We prove this sufficient condition by constructing a $2-(v,3,1)$ design for each $v \equiv 1$ or $3 \pmod 6$.
First, we need to construct Steiner triple systems of small orders: $v = 7, 9, 13$ and 15 (defined on $\mathbb{Z}_v$).

$$v = 7,\ \mathbb{B} = \{013, 124, 235, 346, 561, 602\} \qquad (PG(2))$$
$$v = 9,\ \mathbb{B} = \{012, 345, 678, 036, 147, 258, 048, 156, 237, 057, 138, 246\} \qquad (AG(3))$$
$$v = 13,\ \mathbb{B} = \{(0,3,4)+i,\ (0,2,7)+i \pmod{13} \mid i \in \mathbb{Z}_{13}\} \qquad (PG(3))$$
$$v = 15,\ \mathbb{B} = \{(0,3,4)+i,\ (0,2,8)+i,\ (0,5,10)+i \pmod{15} \mid i \in \mathbb{Z}_{15}\}$$

Now, we shall use the following two constructions to construct all the other Steiner triple system of order v, $STS(v)$ in short.

Case 1. $v \equiv 1 \pmod 6,\ v \geq 19$.
Let $v = 6k+1,\ k \geq 3$. Let $L^{(i)}$ be the commutative Latin square of order $2k$ defined on $\{(i,j) \mid i \in \mathbb{Z}_3 \text{ and } j \in \mathbb{Z}_{2k}\}$ with holes of size 2, see Figure 11.2.

1	2	5	6	3	4
2	1	6	5	4	3
5	6	3	4	1	2
6	5	4	3	2	1
3	4	1	2	5	6
4	3	2	1	6	5

2m×2m

(a)

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

8×8

(b)

Figure 11.2: Commutative Latin square with 2×2 holes. (a) $m = 3$. (b) $m = 4$.
(If m is odd, then L can be constructed by using direct product. But, for even m, it takes some effort!)

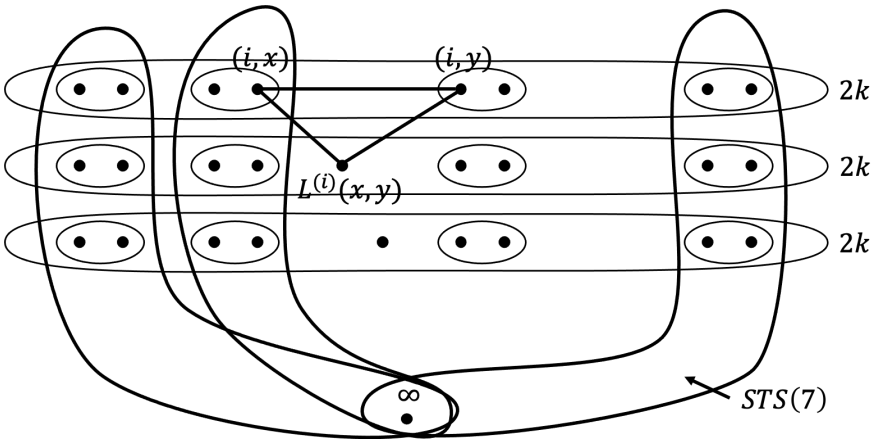

Figure 11.3

Let $(\mathbb{X}, \mathbb{B})$ be a design with $\mathbb{X} = \{\infty\} \cup (\mathbb{Z}_3 \times \mathbb{Z}_{2k})$, and $\mathbb{B}$ defined as follows:

(a) $B \in \mathbb{B}$ if B is a block in an $STS(7)$ defined on $\{\infty, (i, 2h), (i, 2h+1) \mid i \in \mathbb{Z}_3\}$ for each $0 \leq h \leq k-1$; and

(b) $\{(i, x), (i, y), (i+1, L^{(i)}(x, y))\} \in \mathbb{B}$ for all $i \in \mathbb{Z}_3$ and $x, y \in \mathbb{Z}_{2k}$ such that (i, x) and (i, y) are met in a 2×2 hole. (The first component is taking modulo 3 and the second component is taking modulo $2k$.)

It's left to check that $(\mathbb{X}, \mathbb{B})$ is an $STS(v)$. First, we count $|\mathbb{B}|$. Since each entry outside the hole and in the upper part of $L^{(i)}$ gives a triple (block), we have $3 \cdot \dfrac{(2k)^2 - 2(2k)}{2} + 7k = \dfrac{12k^2 - 12k + 14k}{2} = 6k^2 + k = \dfrac{1}{6}(6k+1)6k = \dfrac{v(v-1)}{6}$. Hence, if each pair of two elements in $\mathbb{X}$ occurs, then the pair occurs at most once. So, we have to verify each pair of the elements of $\mathbb{X}$ does occur in a block of $\mathbb{B}$ defined above in (a) and (b). Clearly, if one of the elements is ∞, then $\{\infty, x\}$ occurs in the blocks defined in (a). On the other hand, consider (i_1, x) and (i_2, y) where $i_1, i_2 \in \mathbb{Z}_3$ and $x, y \in \mathbb{Z}_{2k}$. First, if they are in the holes of either $L^{(i_1)}$ or $L^{(i_2)}$ $(= L^{(i)})$, then they occur together in the block of (a). Ob the other hand, if they are not in the holes of $L^{(i)}$, then we have two cases to consider:

(1) $i_1 = i_2 = i$.
Clearly, they occur together in $\{(i, x), (i, y), (i+1, L^{(i)}(x, y))\}$ in (b).

(2) $i_1 \neq i_2$.
Without loss of generality, let $i_2 \equiv i_1 + 1 \pmod 3$ and $i_1 = i$. Since there exists a $z \in \mathbb{Z}_{2k}$ such that $L^{(i)}(x, z) = y$, (i_1, x) and (i_2, y) will occur in $\{(i_1, x), (i_1, z), (i_2, y)\}$ in (b).

This concludes the proof. All $STS(v)$ of order $v \equiv 1 \pmod 6$ have been constructed.

Case 2. $v \equiv 3 \pmod 6,\ v \geq 21$.
The construction can be obtained similarly. Let $\mathbb{X} = \{\infty_1, \infty_2, \infty_3\} \cup (\mathbb{Z}_3 \times \mathbb{Z}_{2k})$, and $\mathbb{B}$ defined as follows:

(a) Use $STS(9)$ instead of $STS(7)$ when $\{\infty\}$ is replaced by $\{\infty_1, \infty_2, \infty_3\}$. Moreover, fix $\{\infty_1, \infty_2, \infty_3\}$ as a block for each $STS(9)$.

(b) Use the same construction.

Hence, $|\mathbb{B}| = 1+11k+\dfrac{3((2k)^2-4k)}{2} = 6k^2+5k+1 = (2k+1)(3k+1) = \dfrac{(6k+3)(6k+2)}{6} = \dfrac{v(v-1)}{6}$. And the existence of every pair of distinct elements in $\mathbb{X}$ can be checked similarly. □

Remark. The above construction was obtained not long time ago. There are quite a few methods in construction of Steiner triple systems. One of the most 'popular' one is called 'cyclic construction' method, or, in general, difference method.

Definition 11.1 (Difference)**.** Let $\mathbb{X} = \mathbb{Z}_n$. Then the difference of two distinct element x and y in $\mathbb{X}$ is $\pm(x-y) := \pm|x-y|$ such that $1 \leq |x-y| \leq \lfloor \frac{n}{2} \rfloor$. The difference obtained in a set S is the set of all difference of two distinct elements in S, denoted by $D(S) = \{x - y \pmod n \mid x, y \in S\}$.

Example.

1. $n = 7,\ S = \{0,1,3\}, D(S) = \{\pm1, \pm2, \pm3\} \pmod 7 = \{1,2,3,4,5,6\}$.
2. $n = 7,\ S = \{1,2,4\},\ D(S) = \{1,2,3,4,5,6\}$.
3. $n = 13,\ S = \{1,2,4,9\}, D(S) = \{1,2,3,...,12\}$.

Remark.

- If $a, b \in S \subseteq \mathbb{Z}_n$, then $a - b \pmod n \in \mathbb{Z}_n^\times$ provided $a \neq 6$.
- If $|S| = s$, then $|D(S)| \leq 2\binom{s}{2}$ (provided $s \leq n$).

Definition 11.2 (Equi-difference set)**.** A set S is called an equi-difference set if the elements of S form an arithmetic progression, i.e., $S = \{a, a+d, ..., a+(k-1)d\}$ where $a + (t-1)d \leq n$ and $d > 0$.

Remark. An equi-difference set could produce the minimum number of distinct differences among all the sets of the same cardinality.

Definition 11.3 (Circular difference)**.** If the difference of a and b is defined as $\min\{|a-b|, n-|a-n|\}$, then it is known as the circular difference of a and b or half difference in short, denoted as $D_2(S)$.

Remark.

- $\{1, 2, 4\}$ in $\mathbb{Z}_7$ provides three half-difference: 1, 2 and 3. Clearly, in $\mathbb{Z}_n$, the set of half-difference will be $\{1, 2, ..., \lfloor \frac{n}{2} \rfloor\}$.
- $|D_2(S)| \leq \binom{|S|}{2}$.
- Again, an equi-difference set S is the set whose $D_2(S)$ is of 'smaller' cardinality. For example, $D(\{1, 2, 3, 4\}) = \{1, 2, 3\}$ and $D(\{0, 2, 4, 6\}) = \{2, 4\}$ in $\mathbb{Z}_8$.

Definition 11.4 (Difference set)**.** A set of k elements $D = \{a_1, a_2, ..., a_k\}$ in $\mathbb{Z}_v$ is called a (v, k, λ)-difference set if $\forall d \in \mathbb{Z}_v^{\times}$, there are exactly λ ordered pairs $(a_i, a_j),\ a_i, a_j \in D$ such that $a_i - a_j \equiv d \pmod{v}$.

Definition 11.5 (Base blocks)**.** A collection of subsets of $\mathbb{X} = \mathbb{Z}_v$ is called a set of base blocks $\mathbb{C}$ of a $2-(v, k, \lambda)$ design if the following conditions satisfied:

1. Each set of $\mathbb{C}$ is of size k; and
2. $\cup_{S \in \mathbb{C}}$ D(S) contains each difference in $\pm\{1, 2, ..., \lfloor \frac{n}{2} \rfloor\}$ exactly λ times.

Constructing design cyclically.

Theorem 11.2. *If $\mathbb{C}$ is a set of base blocks of a $2-(v,k,\lambda)$ design $(\mathbb{X},\mathbb{B})=(\mathbb{Z}_v,\mathbb{B})$, then $\mathbb{B}=\{i+S \mid S\in\mathbb{C} \text{ and } i\in\mathbb{Z}_v\}$. (Note that if $S=\{x_1,x_2,...,x_k\}$, then $i+S=\{x_1+i,x_2+i,...,x_k+i\} \pmod v$.)*

Example.

1. $\mathbb{X}=\mathbb{Z}_7,\ \mathbb{C}=\{\{0,1,3\}\}$ is a set of base block of an $STS(7)$.
2. $\mathbb{X}=\mathbb{Z}_{15},\ \mathbb{C}=\{\{0,3,4\},\{0,2,8\},\{0,5,10\}\}$ is a set of base block of an $STS(15)$. Note that $\{0,3,4\}$ and $\{0,2,8\}$ generate 15 blocks respectively, and $\{0,5,10\}$ generates 5 blocks.
3. For complete proof, refer to Handbook of Combinatorial Designs.