

Lecture 8

BIBD with small block sizes

DATE

- A $2-(v, 2, \lambda)$ design exists for all $v \geq 2$.

This is a direct consequence of using $\lambda \cdot K_v$.

- A $2-(v, 3, 1)$ design exists if and only if $v \equiv 1 \text{ or } 3 \pmod{6}$.

This theorem was first proved by T.P. Kirkman in 1847.

Later, there are many different proofs for this seemingly easy but quite complicate "fact".

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

Proof.

N.C. ($\Rightarrow$) As mentioned earlier, if a $2-(v, 3, 1)$ design exists,

then $r = \frac{v-1}{3-1} = (v-1)/2$ and $b = \frac{v(v-1)}{6}$ are both integers. This implies that $v \equiv 1 \text{ or } 3 \pmod{6}$.

S.C. ($\Leftarrow$) We prove this sufficient condition by constructing

a $2-(v, 3, 1)$ design for each $v \equiv 1 \text{ or } 3 \pmod{6}$.

Kirkman's 15 School Girls Problem

000	000					000
000	000					000
000	000					000
000	000					000
000	000					000

Problem 安排 15 個女學生排成 5 列 每列 3 人 走路上學;

可否在七天內完成任兩位同學都有機會在同一起點?

Answer: 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} exist if and only if

$v \equiv 3 \pmod{6}$.

Note. $AG(2,3)$ 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

First, we need to construct Steiner triple systems of small orders, $v = 7, 9, 13$ and 15 . (Defined on $\mathbb{Z}_v$).

$$v = 7 \quad 013, 124, 235, 346, 450, 561, 602. \quad (\text{PG}(2))$$

$$v = 9 \quad 012, 345, 678, 036, 147, 258, \quad (\text{AG}(3)) \\ 048, 156, 237, 057, 138, 246.$$

$$v = 13 \quad \mathcal{B} = \{(0, 3, 4) + i, (0, 2, 7) + i \pmod{13} \mid i \in \mathbb{Z}_{13}\}. \quad (\text{PG}(3))$$

$$v = 15 \quad \mathcal{B} = \{(0, 3, 4) + i, (0, 2, 8) + i, (0, 5, 10) + i \pmod{15} \mid i \in \mathbb{Z}_{15}\}.$$

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

Case 1. $v \equiv 1 \pmod{6}$, $v \geq 19$.

Let $v = 6k+1$, $k \geq 3$. Let $L^{(i)}$ be a ^{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.

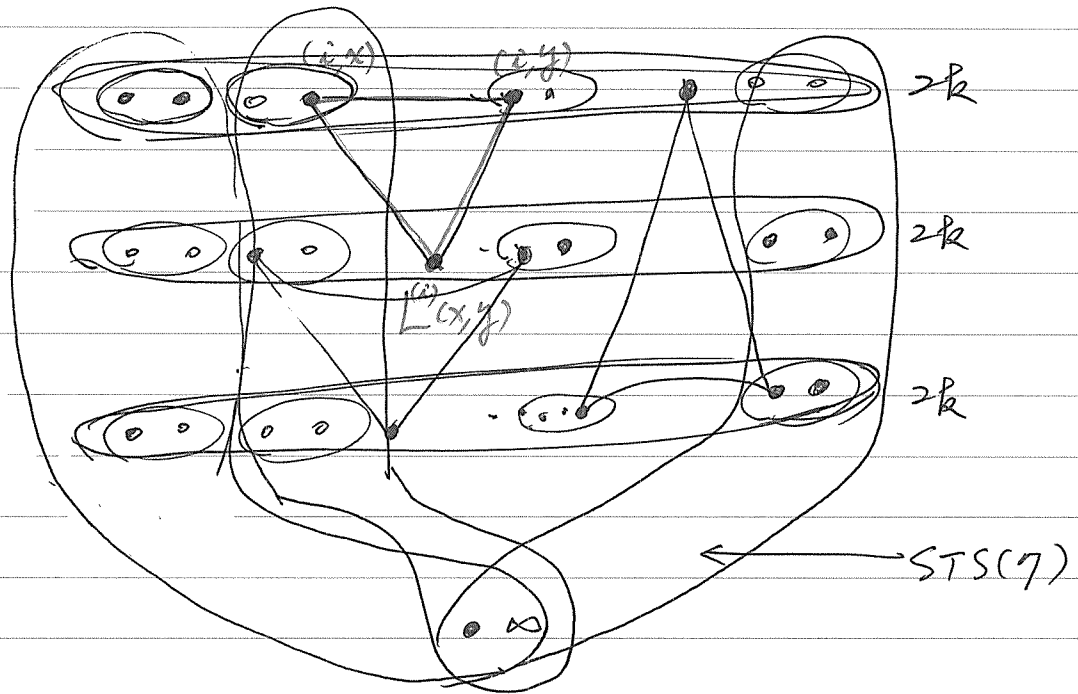
Now, let $(X, \mathcal{B})$ be a design with $X = \{\infty\} \cup (\mathbb{Z}_3 \times \mathbb{Z}_{2k})$, and $\mathcal{B}$ be defined as follows:

(a) $B \in \mathcal{B}$ if B is a block in an $\text{STS}(7)$ defined on

$$\{\infty, (i, 2h), (i, 2h+1) \mid i \in \mathbb{Z}_3\} \text{ for each } 0 \leq h \leq k-1; \text{ and}$$

(b) $\{(i, x), (i, y), (i+1, L^{(i)}(x, y))\} \in \mathcal{B}$ for all $i \in \mathbb{Z}_3$ and $x, y \in \mathbb{Z}_{2k}$ such that (i, x) and (i, y) are not in a 2×2 hole (The first component is taking modulo.)

and the component is taking modulo $2k$.)



It's left to check that $(X, \mathcal{B})$ is an $STS(v)$. First, we

count $|\mathcal{B}|$. Since each entry outside the hole $L^{(i)}$ gives a triple (block), and in the upper part of

we have $3 \cdot \frac{(2k)^2 - (2k) \cdot 2}{2} + 7 \cdot k$ which is equal

to $\frac{12k^2 - 12k + 14k}{2} = 6k^2 + k = \frac{1}{6} (6k+1) \cdot 6k = \frac{v(v-1)}{6}$. Hence,

if each pair of two elements in X occurs, then the pair occurs

at most once. So, we have to verify each pair of elements of X .

does occur in a block of $\mathcal{B}$ defined above, (a) or (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 blocks of (a). On the other hand, if they are not in the holes of $L^{(i)}$, then we have two cases to consider:

(i) $i_1 = i_2 = i$

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

(ii) $i_1 \neq i_2$

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, x) and (i_2, y) will occur in $\{(i, x), (i, z), (i_2, y)\}$ of (b).

This concludes of proof. All STS(v)'s have been constructed, of order $v \equiv 1 \pmod{6}$.

Next, let $v \equiv 3 \pmod{6}$ and $X = \{\infty_1, \infty_2, \infty_3\} \cup (\mathbb{Z}_3 \times \mathbb{Z}_{2k})$.

The construction can be obtained similarly. The blocks in B can be 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.

$$\begin{aligned} \text{Hence } |B| &= 1 + 11 \cdot k + 3 \cdot [(2k)^2 - 4k] / 2 = (2k^2 + 10k + 2) / 2 = k^2 + 5k + 1 \\ &= (2k+1)(3k+1) = \frac{(6k+3)(6k+2)}{6} = \frac{v(v-1)}{6}. \end{aligned}$$

And the existence of every pair of distinct elements in X is similar. ■

Note that the above construction was obtained not long time ago. There are quite a few methods in constructing Steiner triple systems. One of the most "popular" one is called "cyclically constructing" method or in general, difference method. $5', 5''$

Definition (Difference)

Let $X = \mathbb{Z}_n$. Then the difference of two ^{distinct} elements x and y in

X is $\pm(x-y) \stackrel{\text{def}}{=} \pm\|x-y\|$ such that $1 \leq \|x-y\| \leq \lfloor \frac{n}{2} \rfloor$. The differences obtained

Example $S = \{0, 1, 3\} \subseteq \mathbb{Z}_7$

$$\begin{aligned} \text{diff.}(S) &= \{\pm 1, \pm 2, \pm 3\} \pmod{7} \\ &= \{1, 2, 3, 4, 5, 6\}. \end{aligned}$$

in a set S is the set of all difference of two distinct elements in S .

Difference Sets

Given a subset S of $\mathbb{Z}_n$. The set of differences in S , denoted by $D(S)$, is $\{a-b \pmod{n} \mid a, b \in S\}$. For example, if $n=7$ and $S = \{1, 2, 4\}$, then $D(S) = \{1, 2, 3, 4, 5, 6\}$. Moreover, if $n=13$, $S = \{1, 5, 6, 8\}$ then $D(S) = \{1, 2, \dots, 12\}$.

- Observe that if $a, b \in S \subseteq \mathbb{Z}_n$, then $a-b \pmod{n} \in \mathbb{Z}_n^*$ provided $a \neq b$.
- If $|S| = s$, then $|D(S)| \leq 2\binom{s}{2}$ (provided $s \leq n$).
- A set S is called an equi-difference set if the elements of S form an arithmetic progression, i.e., $S = \{a, a+d, \dots, a+(t-1)d\}$ where $a+(t-1)d \leq n$ and $d > 0$.
- For example, $S = \{1, 2, 3, 4\}$ is an equi-difference set in $\mathbb{Z}_8$. ($D(S) = \{1, 2, 3, 5, 6, 7\}$)
- Note that an equi-difference set ^{could} create the minimum number of distinct differences among all other sets of the same cardinality.

- If the difference of a and b is defined as $\min. \{ |a-b|, n-|a-b| \}$, then it is known as the circular difference of a and b or half-difference in short.
- $\{1, 2, 4\}$ in $\mathbb{Z}_7$ will provide three half-differences 1, 2, and 3. Clearly, in $\mathbb{Z}_n$, the set of half-differences will be $\{1, 2, \dots, \lfloor \frac{n}{2} \rfloor\}$.
- So, the set of ^{half-}differences in S is defined as $D_2(S)$.
Moreover, $|D_2(S)| \leq \binom{|S|}{2}$.
- Again, an equi-difference set S is the set whose $D_2(S)$ is of "smaller" cardinality. For example, in $\mathbb{Z}_8$, $D(\{1, 2, 3, 4\}) = \{1, 2, 3\}$ and $D(\{0, 2, 4, 6\}) = \{2, 4\}$.

Definition (Difference set)

A set of k elements $D = \{a_1, a_2, \dots, a_k\}$ in $\mathbb{Z}_v$ is called a (v, k, λ) -difference set if $\forall d \in \mathbb{Z}_v^*$ 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 (Base blocks)

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

- (1) Each set of $\mathcal{C}$ is of size k ; and
- (2) $\bigcup_{S \in \mathcal{C}} \text{diff}(S)$ contains each difference in $\pm\{1, 2, \dots, \lfloor \frac{v}{2} \rfloor\}$ exactly λ times.

• Constructing design cyclically

Theorem 2 If $\mathcal{C}$ is a set of λ base blocks of a $2-(v, k, \lambda)$ design, then $(X, \mathcal{B}) = (\mathbb{Z}_v, \mathcal{B})$

$\mathcal{B} = \{i + S \mid S \in \mathcal{C} \text{ and } i \in \mathbb{Z}_v\}$. (Note that if $S = \{x_1, x_2, \dots, x_k\}$, then $i + S = \{x_1 + i, x_2 + i, \dots, x_k + i\} \pmod{v}$.)

Example $X = \mathbb{Z}_7$, $\mathcal{C} = \{\{0, 1, 3\}\}$ is a set of base block of λ STS(7) on.

Example $X = \mathbb{Z}_{15}$, $\mathcal{C} = \{\{0, 3, 4\}, \{0, 2, 8\}, \{0, 5, 10\}\}$ is a set of base blocks of an STS(15). Note that $\{0, 3, 4\}$ and $\{0, 2, 8\}$ generate 15 blocks resp. and $\{0, 5, 10\}$ generates 5 blocks.

Definition (Full orbit and short orbit)

A base block is of full orbit (short orbit) if the block generates v blocks in $(\mathbb{Z}_v, \mathcal{B})$ resp. (less than v blocks)

Definition (Cyclic design)

A design is called a cyclic design if the design can be obtained by using a set of base blocks.

(*) The above STS(7) and STS(15) are cyclic Steiner Triple systems.

(**) No cyclic STS(9) exists!

Theorem 3 A cyclic Steiner Triple system of order $v \neq 9$ exists.

In order to prove the above theorem, we need to find a set of base blocks for each order $v \equiv 1 \text{ or } 3 \pmod{6}$. Therefore, ~~we~~ a systematic construction should be obtained.

Definition (Skolem sequences)

A Skolem sequence of order n is a sequence of length $2n$ $(a_1, a_2, \dots, a_{2n})$ such that each of ^{the} elements in $\{1, 2, \dots, n\}$ occurs exactly twice, moreover, the indices of "i" occurred exactly "i" apart, i.e., $\widehat{i \in \{1, 2, \dots, n\}}$, if $a_x = i$, then either $a_{x+i} = i$ or $a_{x-i} = i$ (not both).

Example. $n=4$, $\langle 1, 1, 3, 4, 2, 3, 2, 4 \rangle$.
 $a_1 \ a_2 \ a_3 \ a_4 \ a_5 \ a_6 \ a_7 \ a_8$

$$n=5, \quad \langle 1, 1, 3, 4, 5, 3, 2, 4, 2, 5 \rangle.$$

Theorem 4. A Skolem sequence of order n exists if and only if $n \equiv 0, 1 \pmod{4}$. (Type A)

Exercise 2.3. (20 points) Find a proof of Theorem 4 and 5 resp.

For $n \equiv 2 \text{ or } 3 \pmod{4}$, we can obtain an extended Skolem seq.

by using one extra bit. For example, $n=2$, $\langle 1, 1, 2, -2 \rangle$,

$n=3$, $\langle 1, 1, 2, 3, 2, -3 \rangle$. (Use $\langle a_1, a_2, \dots, a_{2n-1}, \overset{\leftarrow}{a_{2n}}, a_{2n+1} \rangle$.)

Theorem 5 An extended Skolem sequence of order n exists if and only if $n \equiv 2 \text{ or } 3 \pmod{4}$. (Type B)

For convenience, we can also use their indices of a Skolem sequence or an extended Skolem sequence to represent the sequences.

For example, $\langle 1, 1, 3, 4, 5, 3, 2, 4, 2, 5 \rangle =_{\text{def}} \{ \{1, 2\}, \{7, 9\}, \{3, 6\}, \{4, 8\}, \{5, 10\} \}$,

and $\langle 1, 1, 2, 3, 2, -3 \rangle =_{\text{def}} \{ \{1, 2\}, \{3, 5\}, \{4, 7\} \}$. Therefore, they are

partitions of $[1, 10]$ and $[1, 7] \setminus \{6\}$ into ^{five} 2-subsets and ^{three} 2-subsets

respectively.

For convenience, we shall use set-notation for Skolem sequence.

So, we have a revised definition for Skolem seq.

Definition

A Skolem sequence of order n is a partition of $[1, 2n]$ into 2-subsets $\{\{a_i, b_i\} \mid i=1, 2, \dots, n\}$ such that $|a_i - b_i| = i, 1 \leq i \leq n$.

An extended Skolem sequence of order n is a partition of

$[1, 2n+1] \setminus \{2n\}$ into 2-subsets $\{\{a_i, b_i\} \mid i=1, 2, \dots, n\}$ such that

$$|a_i - b_i| = i \text{ for } i=1, 2, \dots, n.$$

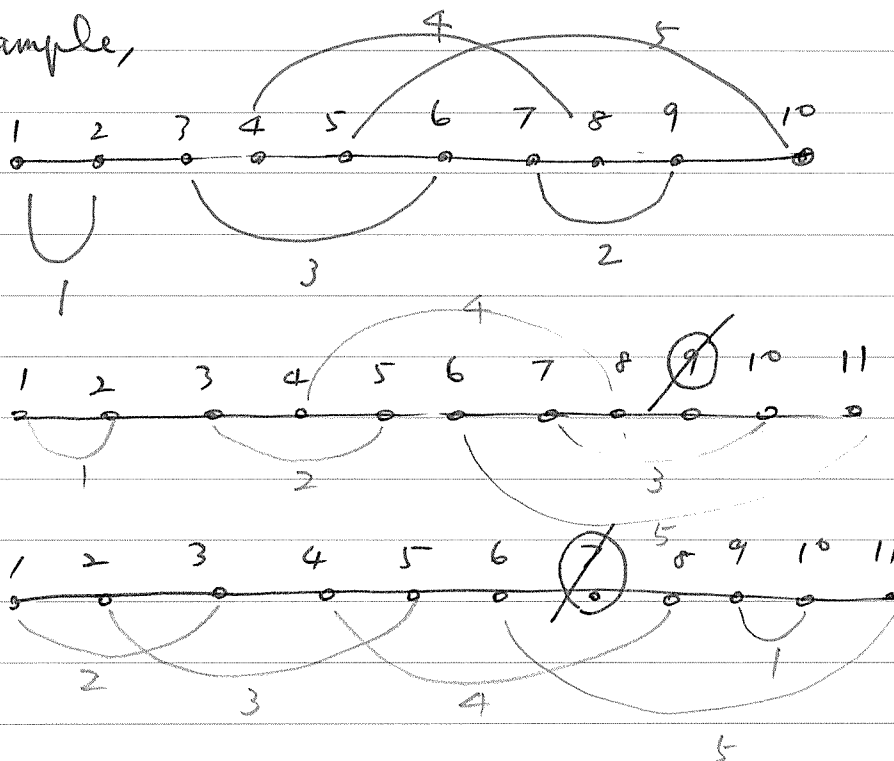
Fact A Skolem sequence of order n exists if $n \equiv 0 \text{ or } 1 \pmod{4}$.

An extended Skolem sequence exists if $n \equiv 2 \text{ or } 3 \pmod{4}$.

Fact For each $d \in \mathbb{N}$, $[1+d, 2n+d]$, a Skolem sequence of order n exists if $n \equiv 0 \text{ or } 1 \pmod{4}$. This is also true for extended Skolem sequence.

In fact, there are quite a few modified sequences by using the above two sequences.

For example,

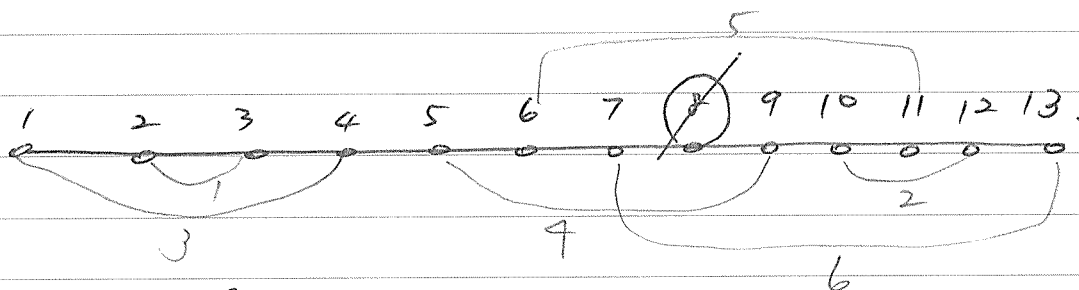


(*) Fact $[1, 2n+1] \setminus \{k\}$ can be partitioned into 2-subsets

$\{\{a_i, b_i\} \mid i=1, 2, \dots, n\}$ such that $|a_i - b_i| = i$ for each $1 \leq i \leq n$ provided

(a) $n \equiv 0 \text{ or } 1 \pmod{4}$ and $k \equiv 1 \pmod{2}$; and

(b) $n \equiv 2 \text{ or } 3 \pmod{4}$ and $k \equiv 0 \pmod{2}$.



(2,2')

Bonus (20 points)

prove the above fact.

Theorem 6 A cyclic STS(v) exists if and only if $v \neq 9$ and $v \equiv 1 \text{ or } 3 \pmod{6}$.

Proof.

Case 1 $v \equiv 1 \pmod{6}$

For convenience, let $v = 6k + 1$ and we consider the "half" difference. Then, the set of differences is $\{1, 2, \dots, 3k\}$. Note that the difference $3k$ is the same as the difference $3k + 1$. Hence, by using Skolem sequences of type A or type B, $\{k+1, k+2, \dots, 3k\}$ or $\{k+1, k+2, \dots, 3k-1, 3k+1\}$ can be partitioned into 2-subsets $\{a_i, b_i\}$ (respectively) $i = 1, 2, \dots, k$, such that $|a_i - b_i| = i$, $i = 1, 2, \dots, k$. Now, we have k difference-triples $\{i, a_i, b_i\}$, $i = 1, 2, \dots, k$. This implies that we can find k base blocks $\{0, i, i + \underset{b_i}{a_i}\}$ ($a_i \leq b_i$) for $i = 1, 2, \dots, k$. And, thus we have a cyclic STS(v).

For your ref. Example, $v = 19$, differences are $1, 2, 3, \dots, 9$.

$4, 5, 6, 7, 8, 10 \Rightarrow$ Difference triples are $\{1, 4, 5\}, \{2, 6, 8\}, \{3, 7, 10\}$.

Base blocks: $\{0, 1, 5\}, \{0, 2, 8\}, \{0, 3, 10\}$.

Case 2 $v \equiv 3 \pmod{6}$

Let $v = 6k+3$ and the set of half differences is $\{1, 2, \dots, 3k+1\}$

First, we delete $2k+1$ from the above set. Hence, the set of

differences is $\{1, 2, \dots, k, k+1, k+2, \dots, 2k, 2k+2, \dots, 3k+1\}$. It remains

to show that $\{k+1, k+2, \dots, 2k, 2k+2, \dots, 3k+1\}$ can be partitioned
(or $3k+2$)

into 2-subsets $\{a_i, b_i\}$ such that $|a_i - b_i| = b_i - a_i = i$ ($b_i > a_i$)

for $i = 1, 2, \dots, k$. Again, it can be done by using either $3k+1$

or $3k+2$ in respective cases. In fact, it is up to the relationship

between k and v . If $k \equiv 1$ or $2 \pmod{4}$, then we partition

$\{k+1, k+2, \dots, 3k+1\} \setminus \{2k+1\}$. On the other hand, if $k \equiv 3$ or $4 \pmod{4}$,
into suitable 2-sets provided $k \equiv 0$ or $1 \pmod{4}$

then we partition $\{k+1, k+2, \dots, 3k+1\} \setminus \{2k+1\}$ into 2-subsets

satisfying $|a_i - b_i| = b_i - a_i = i$ ($b_i > a_i$).

For your ref. Example, $v = 15$, $\{k+1, \dots, 3k+1\} \setminus \{2k+1\} = \{3, 4, 6, 7\}$
(or 8)
Difference triples are $\{1, 3, 4\}, \{2, 6, 8\}, \{5\}$.
Base blocks are: $\{0, 5, 10\}, \{0, 1, 4\}, \{0, 2, 8\}$.
($\uparrow$ $2k+1$)

$$v = 21, \quad D = \{4, 5, 6, 8, 9, 10\}$$

$\underbrace{4, 5, 6}_1 \quad \underbrace{8, 9, 10}_2$

Triples are $\{1, 4, 5\}, \{2, 8, 10\}, \{3, 6, 9\}, \{7\}$.

Base blocks are $\{0, 7, 14\}, \{0, 1, 5\}, \{0, 2, 10\}, \{0, 3, 9\}$.

$$v = 27, \quad 6k+3, \quad k=4$$

$$1, 2, 3, 4, \underbrace{5, 6, 7, 8, 10, 11, 12, 13}$$

$$v = 33, \quad 6k+3, \quad k=5$$

$$1, 2, 3, 4, 5, \underbrace{6, 7, 8, 9, 10, 12, 13, 14, 15, 17}$$

$$v = 39, \quad 6k+3, \quad k=6$$

$$1, 2, 3, 4, 5, 6, \underbrace{7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20}$$

$$v = 45, \quad 6k+3, \quad k=7$$

$$1, 2, 3, 4, 5, 6, 7, \underbrace{8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22}$$

$$v = 51, \quad 6k+3, \quad k=8$$

$$1, 2, 3, 4, 5, 6, 7, 8, \underbrace{9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25}$$