

On the construction of $2-(v, 4, 1)$ designs

Small cases

$2-(13, 4, 1)$ design $\approx$ projective plane of order 3.

$2-(16, 4, 1)$ design $\approx$ Affine plane of order 4.

Lemma 1 For each $n \geq 17, n \neq 28$, $n \equiv 0 \text{ or } 1 \pmod{4}$, there exists a pairwise balanced GDD with five (or four) groups G_1, G_2, G_3, G_4, G_5 such that $|G_1| = |G_2| = |G_3| = |G_4| = r, |G_5| = r, r \equiv 0 \text{ or } 1 \pmod{4}$, and all blocks are of size 4 or 5. Moreover, a $T(r, 5, 1)$ exists.

Proof. We use $\langle r, r, r, r, r \rangle$ to denote the sizes of groups.
 $17, 20, 21, \dots$

$$24 \rightarrow \langle 5, 5, 5, 5, 4 \rangle$$

$$36 \rightarrow \langle 8, 8, 8, 8, 4 \rangle$$

$$48 \rightarrow \langle 11, 11, 11, 11, 4 \rangle$$

$$25 \rightarrow \langle 5, 5, 5, 5, 5 \rangle$$

$$37 \rightarrow \langle 9, 9, 9, 9, 1 \rangle$$

$$49 \rightarrow \langle 11, 11, 11, 11, 5 \rangle$$

$$29 \rightarrow \langle 7, 7, 7, 7, 1 \rangle$$

$$40 \rightarrow \langle 9, 9, 9, 9, 4 \rangle$$

$$32 \rightarrow \langle 7, 7, 7, 7, 5 \rangle$$

$$41 \rightarrow \langle 9, 9, 9, 9, 5 \rangle$$

$$\begin{aligned} & \text{40 to 41} \\ & n \equiv 0 \text{ or } 1 \\ & \pmod{4} \end{aligned}$$

$$33 \rightarrow \langle 8, 8, 8, 8, 1 \rangle$$

$$44 \rightarrow \langle 9, 9, 9, 9, 8 \rangle$$

$$45 \rightarrow \langle 9, 9, 9, 9, 9 \rangle$$

For $n \geq 52$, $n = 4r + r_1$ where $0 \leq r_1 \leq r$ and $r_1 \equiv 0 \text{ or } 1 \pmod{4}$
 such a pairwise balanced GDD does exist since there are
 at least three MOLS(r)'s for each order $r > 10$. ■

Lemma 2 If a $2-(v, 4, 1)$ exists, then $v \equiv 1 \text{ or } 4 \pmod{12}$.

Proof. It follows by $3 \mid v-1$ and $6 \mid \binom{v}{2}$. ■

Definition (Pairwise balanced GDD, PGDD)

A PGDD (X, B) ^{of order v} denoted by $GD(R, m; S, \lambda)$ is a ^{of order v} GDD _(general)
 whose group sizes are in R and block sizes are in S .

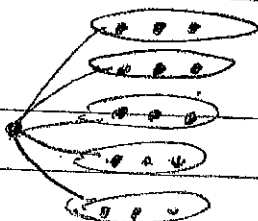
e.g. The truncated $T(r, 5, 1)$ is a $GD(\{r, r\}, 5; \{4, 5\}, 1)$ of order $4r + r_1$.

Lemma 3

✓ Use to for $\{k\}$.

There exists a $GD(3, 5; \underline{4}, 1)$.

Proof. Since a $2-(16, 4, 1)$ design exists, a $GD(3, 5; 4, 1)$ can
 (Affine plane of order 4)
 be obtained by deleting one element from the design.



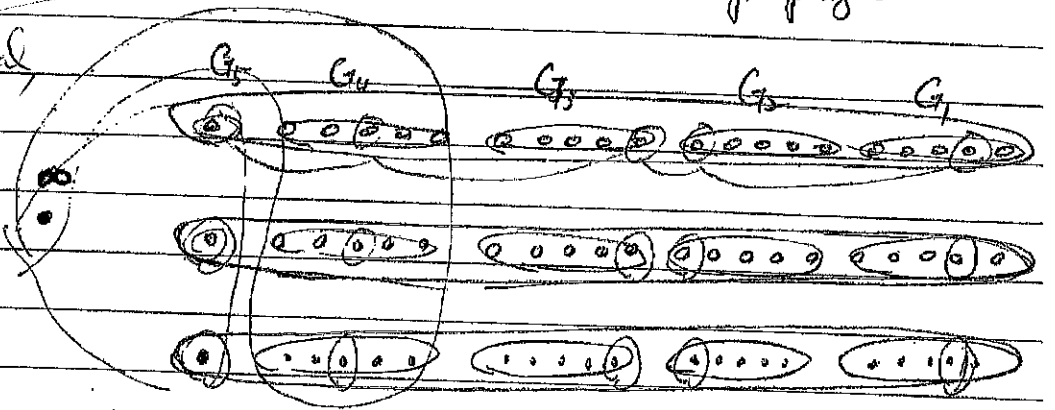
為了容易理解以下就用特殊的例子作說明。

Example A $2-(64, 4, 1)$ design exists.

Proof $64 = 3 \times 21 + 1$

First, we use $r=5$ and $r_1=1$ to obtain a $GD(\{1, 5\}, 5; \{4, 5\}, 1)$

25 blocks in total,
20 of them are
of size 4 and
the other blocks
are of size 5.



Construction (X, B)

Step 1. Use $\{\infty\} \cup (G_i \times \{1, 2, 3\})$ for $i=1, 2, 3, 4, 5$,
to construct a $2-(4, 4, 1)$ and
 $2-(16, 4, 1)$ respectively.

Step 2. For each block $B \in GD(\{1, 5\}, 5; \{4, 5\}, 1)$, construct a
defined on $B \times \{1, 2, 3\}$
 $GD(3, 4; 4, 1)$ or $GD(3, 5; 4, 1)$, depends on the size
of B , $|B|=4$ or 5 . (See the figure above.)

Step 3. Let $X = \{\infty\} \cup ((\bigcup_{i=1}^5 G_i) \times \{1, 2, 3\})$, and $B = B_1 \cup B_2$.

$$|B_1| = 1 + 4 \times 20 = 81.$$

$$\Rightarrow |B| = 336 = \frac{64 \times 63}{4 \times 3} = 16 \times 21$$

$$|B_2| = 5 \times 15 + 20 \times 9 = 255$$

(*) Any two elements occur together in a block. (Check)

(**) Small orders v s.t. a $2-(v, 4, 1)$ design exists can be obtained by direct construction, "25" is the hardest one (?)

Theorem 4 A $2-(v, 4, 1)$ design exists if and only if

$$v \equiv 1 \text{ or } 4 \pmod{12}.$$

Proof. ($\Rightarrow$) By Lemma 1.

($\Leftarrow$) We can construct all $2-(v, 4, 1)$ designs recursively.

Assume that small orders are constructed. Let

$v = 3n+1$ where $n \equiv 0 \text{ or } 1 \pmod{4}$. By the above

construction (of example), it suffices to write $n = 4r + r_1$,
($r > 10$)

where $r_1 \equiv 0 \text{ or } 1 \pmod{4}$ and $3r+1, 3r_1+1 \equiv 1 \text{ or } 4 \pmod{12}$.

(For example, if $n = 301$, then we can write $n = 4 \times 72 + 13$

where $r = 72$ and $r_1 = 13$. Since $3 \times 72 + 1 \equiv 1 \pmod{12}$ and $3 \times 13 + 1$

$\equiv 4 \pmod{12}$, we have a $2-(1904, 4, 1)$ design.)

So, we have two cases to consider.

Case 1. $n \equiv 0 \pmod{4}$

$$n = 12k, k \geq 2, r = 12(k-1) \text{ and } r_1 = 12.$$

$$n = 12k+4, r = 12k, r_1 = 4.$$

$$n = 12k+8, r = 12k, r_1 = 8.$$

Case 2. $n \equiv 1 \pmod{4}$

$$n = 12k+1, k \geq 2, r = 12(k-1)+1 \text{ and } r_1 = 12.$$

$$n = 12k+5, r = 12k, r_1 = 5.$$

$$n = 12k+9, r = 12k, r_1 = 9.$$

This concludes the proof. ■

Bonus Give a complete proof of Theorem 4.

How about $2-(v, k, 1)$ design where $k \geq 4$?

Observations

1. We need a $GD(R, m; k, 1)$ of certain order n first. ($m \geq k$)

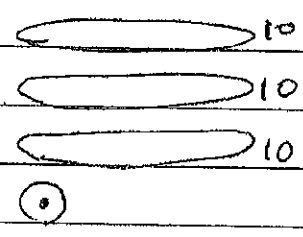
2. $\forall r \in R$, a $2-(m'r+1, k, 1)$ design exists for each $r \in R$.
 3. A $GD(m', k; k, 1)$ and a $GD(m', k+1; k, 1)$ exists.
 ($m' = 3$ for $k = 4$) $\Rightarrow v = 3n+1$.

Review $k=3$ (4th construction!)

Consider $n \equiv 0 \text{ or } 1 \pmod{3}$.

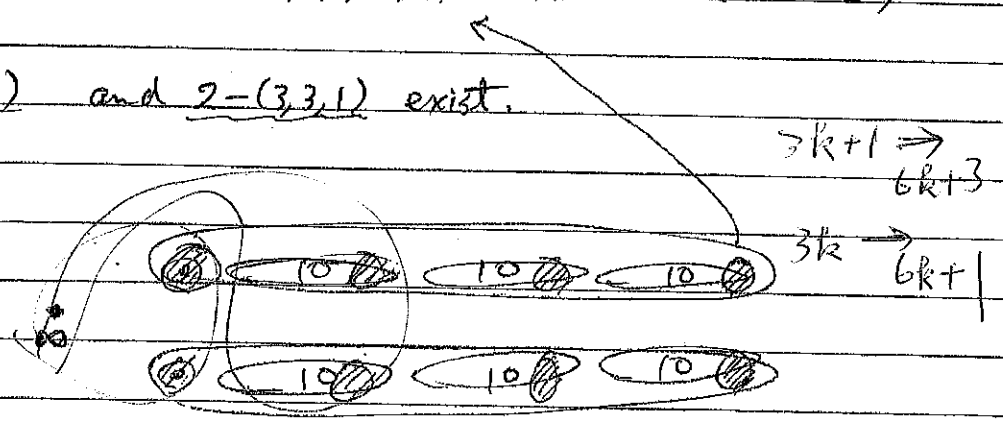
$R = \{3, 4\}$, $n = 3r + r_1$, $r_1 \equiv 0 \text{ or } 1 \pmod{3}$.

Example $n=31$



$GD(2, 3; 3, 1)$ and $GD(2, 4; 3, 1)$ exist. ($m'=2$)

$2-(2, 3, 1)$ and $2-(3, 3, 1)$ exist.

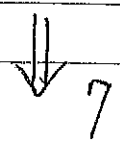


Note R 中的元素不要選 $x \equiv 2 \text{ or } 5 \pmod{6}$ 即可。

(*) 當 $\lambda > 1$ 時, 建構 $2-(v, k, \lambda)$ 設計也是很重要的課題。

In this case, the set of admissible v is larger than for $\lambda=1$ in general. For example, if $\lambda=2$, $k=3$, then

we have: $v \equiv 0 \text{ or } 1 \pmod{3}$.



以上的建構概念提供參考

7

補充說明

① $K_3 \mid \lambda K_v$ 的必要條件分別為

λ	1	2	3	4	5	6	(mod 6)
v	1, 3	1, 3, 4, 0	1, 3, 5	1, 3, 4, 0	1, 3	0, 1, 2, 3, 4, 5	

② $\left(\begin{smallmatrix} \mathbb{Z}_v \\ 3 \end{smallmatrix} \right) \rightarrow v-2 \begin{smallmatrix} \text{STS}(v)'s \\ \text{mutually disjoint} \end{smallmatrix} \quad (v \equiv 1 \text{ or } 3 \pmod{6}).$



A large set of triple systems.

(*) An interesting problem to study. Let G be the intersection graph defined on $\mathcal{B}$ where $(X, \mathcal{B})$ is a PBD with index 1 ($\lambda=1$).

Prove that $\chi(G) \leq |X|$. (Especially consider $(X, \mathcal{B})$ is an $\text{STS}(v)$ for odd v .)

t-design

NO.

8

DATE

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

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

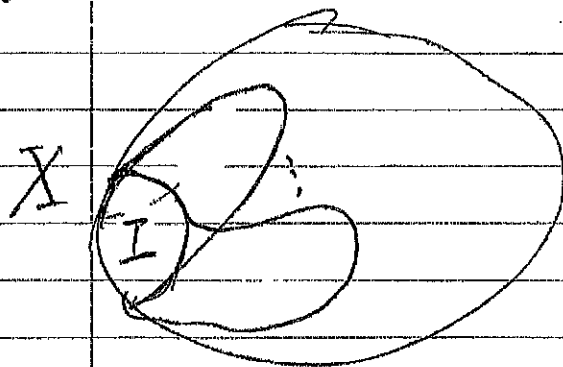
(a) $\lambda \binom{v}{t} / \binom{k}{t}$ is an integer,

(b) for each $0 \leq i \leq t$, the collection of all blocks 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 $\mathcal{B}_i = \{B \setminus I \mid B \in \mathcal{B}\}$ 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, λ) design where

$$\lambda = \binom{v-t}{k-t} \text{ if } k > t \text{ and } \lambda = 1 \text{ if } k = t.$$

- 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 -($v, 4, \lambda$) 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 large set of Steiner triple systems.

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

- Theorem (Lu, Jia-Xi, 陸嘉熹) 1935-1983 高中老師

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

Definition (Steiner systems)

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 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 $t = k-1$.

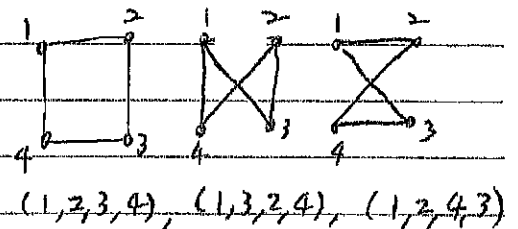
- Small examples $t=3$ and $k=4$

Let $X = \mathbb{Z}_2^4$ and $B = \{\vec{w}, \vec{x}, \vec{y}, \vec{z}\} \mid \vec{w}, \vec{x}, \vec{y}, \vec{z} \in \mathbb{Z}_2^4, \vec{w} + \vec{x} + \vec{y} + \vec{z} = \vec{0}\}$.

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

- Let $X = E(K_5)$ and $B = \left\{ \begin{array}{c} \triangle \\ (5) \\ (1) \end{array}, \begin{array}{c} \triangle \\ (5) \\ (3) \end{array}, \begin{array}{c} \square \\ (5) \\ (3) \end{array} \right\}$ Labeled subgraphs of K_5

Then, (X, B) is an $S(3, 4, 10)$.



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

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

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

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

- Theorem (H. Hanani, 1960)

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

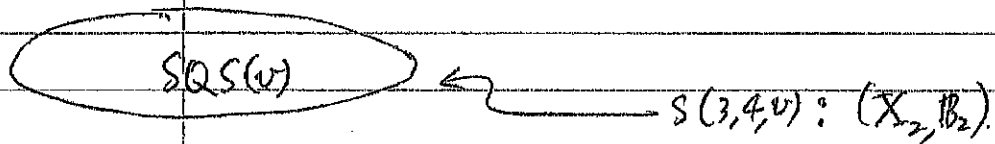
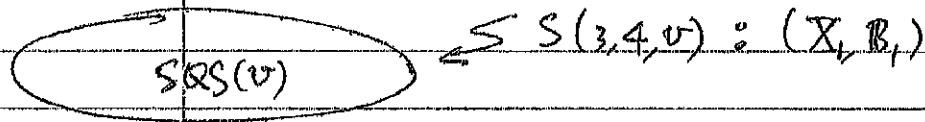
Proof. It takes a lot of effort in proving the sufficient part.

Doubling Construction

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

Proof.

(a)
(Method 1)



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 $F_1, F_2, \dots, F_{v-1}$ and $G_1, G_2, \dots, G_{v-1}$

for $i=1,2$ respectively. Now, we use F_j and G_j , $j=1,2,\dots,v-1$

to define $\binom{\frac{v}{2}}{2}$ quadruples by the following way:

$$F_j = \{ \{a_i, b_i\} \mid i=1,2,\dots,\frac{v}{2} \} \Rightarrow \{a_i, b_i, c_j, d_j\} \in \mathcal{B}$$

$$G_j = \{ \{c_j, d_j\} \mid j=1,2,\dots,\frac{v}{2} \}$$

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

(or $SQS(2v)$).

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

(Method 2)

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

Define $\mathcal{B}$.

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

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

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

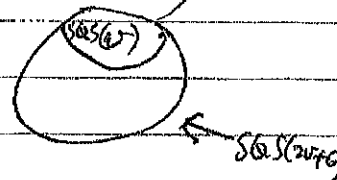
It is a routine matter to check $(X, \mathcal{B})$ is indeed an SQS($2v$) for both constructions: (a) and (b).

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.) ($v \rightarrow 3v-2$ construction)
(Example)

13/ Conjecture $v \rightarrow 2v+6$ Construction
 $(X_1, \mathcal{B}_1)$



For each SQS(v), there exists an SQS($2v+6$) which

contains $(X_1, \mathcal{B}_1)$ as a subsystem.

Let $q(v) = \frac{v(v-1)(v-2)}{24}$, $p(v) = \frac{v(v-1)}{6}$ and

$$q'(v) = q(v) - p(v-1).$$

(*) If $v \equiv 2$ or $4 \pmod{6}$, then $p(v-1) = \frac{(v-1)(v-2)}{6}$.

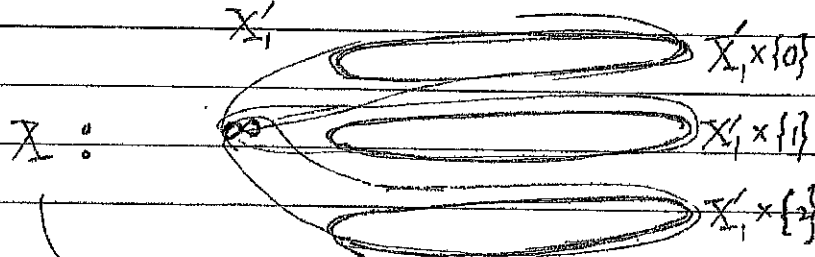
Consider $u \equiv 4$ or $10 \pmod{18}$.

$u = 3v - 2$ where $v \equiv 2$ or $4 \pmod{6}$. (Example: if $v = 8$, then $u = 22$.)

Construction of SQS(u)

Let (X_1, B_1) be an SQS(v) such that $\infty \in X_1$.

Let $X = \{\infty\} \cup \underbrace{(X_1 \setminus \{\infty\})}_{X'_1} \times \mathbb{Z}_3$. So,



Quadruples (B)

1. $\forall \{x, y, z, w\} \subseteq X'_1$ and $\{x, y, z, w\} \in B_1$, let

$\{(x, a_1), (y, a_2), (z, a_3), (w, a_4)\} \in B$ where $a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod{3}$.

$((a_1, a_2, a_3, a_4) \in \{(0, 0, 0, 0), (0, 1, 1, 1), (1, 0, 1, 1), (1, 1, 0, 1), (1, 1, 1, 0),$

$(0, 2, 2, 2), (2, 0, 2, 2), (2, 2, 0, 2), (2, 2, 2, 0),$ and 18 others}).

(*) Type 1 quadruples : $27 \times q'(v)$ quadruples. $\left(27 \cdot \left(\frac{v(v-1)(v-2)}{24} - \frac{(v-1)(v-2)}{6} \right) \right)$

For

2. $\{\infty, u, v, w\} \in B_1$, define the following quadruples and let them in B :

$$\{\infty, (u, b_1), (v, b_2), (w, b_3)\} \in B \text{ where } b_1 + b_2 + b_3 \equiv 0 \pmod{3}.$$

$$(b_1, b_2, b_3) \in \{(0, 0, 0), (1, 1, 1), (2, 2, 2), (0, 1, 2), (0, 2, 1), (1, 0, 2), (1, 2, 0), (2, 0, 1), (2, 1, 0)\}.$$

We have $9 \cdot p(v-1)$ such quadruples. $\left(\frac{9(v-1)(v-2)}{6} \right)$.

3. Continue from 2,

$$\{(u, i), (v, i), (w, i+1), (w, i+2)\}, \quad i \in \mathbb{Z}_3.$$

$$\binom{3}{2} \cdot 3$$

$9 \cdot p(v-1)$ quadruples.

4. $\forall$ pair (α, β) in X'_1 , let

$$\{(\alpha, i), (\beta, i), (\alpha, i+1), (\beta, i+1)\} \in B. \quad \left(3 \cdot \binom{v-1}{2} \text{ quadruples} \right)$$

5. $\forall r \in X'_1$, let

$$\{\infty, (r, 0), (r, 1), (r, 2)\} \in B. \quad (v-1 \text{ quadruples})$$

In total, we have $27 \cdot \left(\frac{v(v-1)(v-2)}{24} - \frac{(v-1)(v-2)}{6} \right) + 9 \cdot \frac{(v-1)(v-2)}{6} +$

$$9 \cdot \frac{v(v-1)(v-2)}{6} + 9 \cdot \frac{(v-1)(v-2)}{6} + (v-1) = \frac{27}{24} v(v-1)(v-2) + (v-1) = \frac{(3v-2)(3v-3)(3v-4)}{24}.$$

(*) If we have $v \rightarrow 2v$ and $v \rightarrow 2v+6$ 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 $v \rightarrow 2v$, 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 $v \rightarrow 2v+6$ works. ■

The best known construction besides $v \rightarrow 2v$ 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.

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

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

$$36k+2 = 3(12k+2) - 4 \quad (u=2) \quad \text{SQS}(2) \text{ is a trivial system}$$

$$36k+10 = 3(12k+4) - 2 \quad u=1 \text{ (one element)}$$

$$36k+14 = 3(12k+10) - 16 \quad u=8$$

$$36k+22 = 3(12k+14) - 20 \quad u=10$$

$$36k+26 = 3(12k+14) - 16 \quad u=8$$

$$36k+34 = 3(12k+14) - 8 \quad u=4$$

Exercise 5-5, 3 points)

Apply Hartman's triple construction to find as many $\text{SQS}(v)$ as possible.