# Solutions to Exercises
# Chapter 8: Steiner triple systems

**1** Kirkman's original (incomplete, but basically correct) proof of the existence of Steiner triple systems went as follows. Kirkman defined two kinds of structure: $S_n$, what we have called a Steiner triple system of order $n$; and $S'_n$, whose exact details don't concern us here. He claimed to show:

(a) $S_1$ exists;

(b) if $S_n$ exists, then $S_{2n+1}$ exists;

(c) if $S_n$ exists and $n > 1$, then $S'_{n-2}$ exists;

(d) if $S'_n$ exists, then $S_{2n-1}$ exists.

Prove that, from (a)–(d), it follows that $S_n$ exists for all positive integers $n \equiv 1$ or 3 (mod 6). For which values of $n$ does $S'_n$ exist?

Suppose that the conclusion is false, and let $n$ be the smallest integer congruent to 1 or 3 mod 6 for which $S_n$ fails to exist.

(i) If $n \equiv 3$ or 7 $\pmod{12}$, then $n = 2m+1$, where $m \equiv 1$ or 3 $\pmod 6$; by (b), $S_m$ does not exist, contradicting the minimality of $n$.

(ii) If $n \equiv 1$ or 9 $\pmod{12}$, and $n > 1$, then $n = 2m-1$. By (d), $S'_m$ does not exist. Then by (c), $S_{m+2}$ does not exist. Again the minimality of $n$ is contradicted, since $m+2 \equiv 3$ or 7 $\pmod 6$, and $m+2 > 1$.

(iii) The case $n = 1$ is excluded by (a).

By (c), $S'_n$ exists for all $n \equiv 1$ or 5 $\pmod 6$.

**2** Construct a Netto system of order 25.

To show that $z^2 - z + 1$ is irreducible over GF(5), it is enough to show that none of the five elements of GF(5) is a root:

$$\begin{aligned} 0^2 - 0 + 1 = 1 &\neq 0, \\ 1^2 - 1 + 1 = 1 &\neq 0, \\ 2^2 - 2 + 1 = 3 &\neq 0, \\ 3^2 - 3 + 1 = 2 &\neq 0, \\ 4^2 - 4 + 1 = 3 &\neq 0. \end{aligned}$$

Alternatively, a root of the quadratic is a primitive 6th root of unity (since $z^2-z+1$ divides $z^6-1$ but doesn't divide $z^3-1$ or $z^2-1$); but the multiplicative group of $\mathrm{GF}(5)$ has order 4 and has no primitive 6th root of unity.

So $\mathrm{GF}(25)$ can be represented as claimed.

The subgroup generated by $z$ is $\{1,z,z-1,-1,-z,-z+1\}$ (see page 118). Now choose a new element, say 2, and form the coset $\{2,2z,2z-2,-2,-2z,-2z+2\}$; another, say $z+1$, and form $\{z+1,2z-1,z-2,-z-1,-2z+1,-z+2\}$; and finally, say $z+2$, which gives the remaining six non-zero elements. (To do these calculations, use the ordinary laws of algebra, remembering that $5=0$ and $z^2+z-1$.)

So the four base triples are $\{0,1,z\}$, $\{0,2,2z\}$, $\{0,z+1,2z-1\}$, and $\{0,z+2,-2z-1\}$. The other triples are obtained by adding the elements of $\mathrm{GF}(25)$ to each of these.

**3** Prove that, given any STS(7), its points can be numbered $1,\ldots,7$ so that its triples are those listed in Fig. 8.1(a). Prove a similar statement for STS(9).

Prove that there are just two non-isomorphic Steiner triple systems of order 13.

More generally, the number of triples of a STS($n$) disjoint from a given triple is $(n-3)(n-7)/6$: for there are $n(n-1)/6$ triples altogether, of which each point of a triple $T$ lies in $(n-1)/2$ triples, $(n-3)/2$ of which meet $T$ in one point, and

$$\frac{n(n-1)}{6}-1-\frac{3(n-3)}{2}=\frac{(n-3)(n-7)}{6}.$$

This expression evaluates to 0 when $n=7$, and 2 when $n=9$.

For $n=7$, let $1,2,4$ be any three points not forming a triple. There are unique triples through any two of them, which we may label $123,145,246$. Then the triples through 16, 25 and 43 must each contain the one remaining point, say 7. Finally, the three pairs 36, 35, 56 must each lie on a triple, and since only one triple remains to be found, it must be 356.

For $n=9$, the two triples disjoint from a given one are disjoint from one another. For if $T$ is a triple and $x\notin T$, then $x$ lies on four triples, three of which meet $T$, so just one is disjoint from $T$. Hence the twelve triples fall into four sets of three mutually disjoint triples, so that triples from different sets intersect. Then two of these sets form a square grid, and we can number the points so that these triples are $123,456,789,147,258,369$. Now the remaining six triples are determined. For example, every point except 9 already lies on a triple with either 1 or 5; so 159 must be a triple.

The statements about isomorphisms follow with care from these proofs. For $n = 7$, if $x_1, x_2, x_4$ are three points of a Steiner triple system not forming a triple, then we can label the remaining points $x_3, x_5, x_6, x_7$ as in the proof. Now, if $y_1, y_2, y_4$ form non-triple in another STS, then we can similarly label its other points $y_3, y_5, y_6, y_7$; then the map taking $x_i$ to $y_i$ for $i = 1, \ldots, 7$ is an isomorphism, and is the unique isomorphism carrying the first non-triple to the second.

The argument is similar for $n = 9$. In fact, given three points $x, y, z$ not forming a triple, the two families of triples in the above proof are determined (those containing the triples through $xy$ and $xz$); and the triples in each family are also specified (since they contain $2, 1, 0$ of the three points). So again it is true that any non-triple can be mapped to any other by a unique isomorphism.

Determining STS of order 13 is a project (so I do not give the solution). Start with the analysis used above for $n = 9$: there are ten triples disjoint from a given one, each of the ten points lying on three triples. Classify the configurations formed by these ten triples.

**4** An *automorphism* of a Steiner triple system is an isomorphism from the system to itself. Prove that a Steiner triple system of order 7 or 9 has 168 or 432 automorphisms respectively.

Use the analysis of Question 3. For $n = 7$, any three points $x, y, z$ not forming a triple can be mapped to any other three such points by a unique isomorphism. If we take the two systems to be the same, then isomorphisms are automorphisms. So the number of automorphisms is equal to the number of choices of $x, y, z$, which is $7 \cdot 6 \cdot 4 = 168$. For $n = 9$, the argument is similar, and yields $9 \cdot 8 \cdot 6 = 432$ as the number of automorphisms.

**5** (a) Prove that, in an affine triple system, each triangle lies in a subsystem of order 9.

(b) Prove that an affine triple system is a Kirkman system.

(a) Given a triangle $x, y, z$, consider the set

$$\{\lambda x + \mu y + \nu z : \lambda + \mu + \nu = 1\}.$$

This set contains nine points. (There are nine choices of $(\lambda, \mu, \nu)$ with sum zero in the integers mod 3. If two choices lead to the same vector, we have $\alpha + \beta y + \gamma z = 0$ for some $\alpha, \beta, \gamma$ with $\alpha + \beta + \gamma = 0$. Up to permutation, there are two cases:

(a) $\alpha = \beta = \gamma \neq 0$: this contradicts $x + y + z \neq 0$.

(b) $\alpha = 1$, $\beta = -1$, $\gamma = 0$: this implies $x = y$, which is false.

Moreover, these nine points form a subsystem. For suppose that

$$a_i = \lambda_i x + \mu_i y + \nu_i z, \qquad \lambda_i + \mu_i + \nu_i = 0$$

for $i = 1, 2$, and let $a_3 = -(a_1 + a_2)$ be the third point of the triple through $a_1$ and $a_2$. Then

$$a_3 = -(\lambda_1 + \lambda_2)x - (\mu_1 + \mu_2)y - (\nu_1 + \nu_2)z,$$

and

$$-(\lambda_1 + \lambda_2) - (\mu_1 + \mu_2) - (\nu_! + \nu_2) = -1 - 1 = 1.$$

(b) For each inverse pair $a, -a$ of non-zero elements of $V$, the family of triples of the form $\{x, x+a, x-a\}$ partitions $V$. Each triple lies in exactly one of these families.

**6** Verify the following values of the packing and covering functions for small $n$.

| $n$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|
| $p(n)$ | 1 | 1 | 2 | 4 | 7 | 8 | 12 |
| $c(n)$ | 1 | 3 | 4 | 6 | 7 | 11 | 12 |

In all cases of the table except $p(5)$, the entry agrees with the bound given by (8.4.2).So we are required just to exhibit packings and coverings attaining the bounds. This is clear for the values $n = 3, 7, 9$ for which STS exist, and also for $p(6)$ and $p(8)$, by (8.4.3). For the other values we have:

- $p(4)$: 123
- $c(4)$: $123, 124, 134$
- $c(5)$: $123, 145, 234, 235$
- $c(6)$: $123, 124, 345, 346, 5651, 562$
- $c(8)$: STS(7) together with $128, 348, 568, 678$.

We see that $p(5) \leq 2$ as follows: two 3-sets can have at most one point in common, so are $123, 145$ without loss of generality. A further 3-set could contain at most one of $1, 2, 3$ and at most one of $4, 5$, so cannot exist. A packing of size 2 is $123, 145$.

**7** If a SQS of order $n$ exists, with $n \geq 2$, then $n \equiv 2$ or 4 (mod 6).

If $(X, \mathcal{B})$ is a SQS and $x \in X$, let $Y = X \setminus \{x\}$ and let $\mathcal{C}$ be the set of triples $T$ such that $T \cup \{x\} \in \mathcal{B}$. Then $(Y, \mathcal{C})$ is a STS. Hence if a SQS of order $n$ exists, then $n-1 \equiv 1$ or 3 mod 6, whence $n \equiv 2$ or 4 mod 6.

**8** If $(X, \mathcal{B})$ is a SQS of order $n$, then $|\mathcal{B}| = n(n-1)(n-2)/24$.

Count pairs $(x, U)$, where $x$ is a point and $U$ a quadruple containing it. We see that $4|\mathcal{B}| = n \cdot (n-1)(n-2)/6$. (By the remarks in the preceding solution, the number of quadruples containing $x$ is equal to the number of triples in a STS of order $n-1$.)

**9** Let $X$ be a vector space over $\mathbf{Z}(2)$, and let $\mathcal{B}$ be the set of 4-subsets $\{x, y, z, w\}$ of $X$ for which $x+y+z+w = 0$. Show that $(X, \mathcal{B})$ is a SQS.

Given three distinct vectors $x, y, z$, let $w = x+y+z$. Since $-1 = 1$, we have $x+y+z+w = 0$. Could $w$ be equal to one of $x, y, z$? If $w = x$, then $y+z = 0$, whence $y = z$, contrary to assumption. The other cases are similar. So $\{w, x, y, z\}$ is a quadruple, clearly the unique quadruple containing $x, y, z$.

**10** Let $(X, \mathcal{B})$ be a SQS of order $n \geq 2$. Take a disjoint copy $(X', \mathcal{B}')$ of this system. Take a tournament schedule on $X$ with rounds $R_1, \ldots, R_{n-1}$, and one on $X'$ with rounds $R'_1, \ldots, R'_{n-1}$. (This is possible since $n$ is even — see Section 8.6.) Now let $Y = X \cup X'$, and $\mathcal{C} = \mathcal{B} \cup \mathcal{B}' \cup \mathcal{R}$, where $\mathcal{R}$ is the set of 4-sets $\{x, y, z', w'\}$ such that

- $x, y \in X$, $z', w' \in X'$;
- for some $i$ ($1 \leq i \leq n-1$), $\{x, y\} \in R_i$ and $\{z', w'\} \in R'_i$.

Show that $(Y, \mathcal{C})$ is a SQS of order $2n$.

Clearly all elements of $\mathcal{C}$ are 4-sets. We have to show that any three points $x, y, z$ lie in exactly one quadruple. There are several cases:

(a) $x, y, z \in X$. Then a unique quadruple in $\mathcal{B}$ contains them.

(b) $x, y \in X$, $z \in X'$. There is a unique $i$ such that $\{x, y\} \in R_i$, and then a unique $w$ such that $\{z, w\} \in R'_i$. Then $\{x, y, z, w\}$ is the unique quadruple containing the three points.

(c) $x \in X$, $y, z \in X'$. Dual to (b).

(d) $x, y, z \in X'$. Dual to (a).

**11** Let $(X, \mathcal{B})$ be a STS of order $n$, and $Y$ a subsystem of order $m$, where $m < n$. Prove that $n \geq 2m+1$. Show further that $n = 2m+1$ if and only if every triple in $\mathcal{B}$ contains either 1 or 3 points of $Y$.

Let $x \in X \setminus Y$. Then $x$ lies in $(n-1)/2$ triples. But the points of $Y$ lie on distinct triples through $x$, since a triple containing two points of $Y$ is contained within $y$. As there are $m$ such triples, we have $m \leq (n-1)/2$, or $n \geq 2m+1$.

Equality holds if and only if every triple containing $x$ meets $Y$. Since this is true for each point outside $Y$, equality holds if and only if no triple is disjoint from $Y$. By the definition of a subsystem, no triple can meet $Y$ in two points. So, finally, equality holds if and only if every triple meets $Y$ in one or three points.

**12** Let $(X, \mathcal{B})$ be a STS of order $n = 2m+1$, and $Y$ a subsystem of order $m$; say $Y = \{y_1, \ldots, y_m\}$. For $i = 1, \ldots, m$, let $R_i$ be the set of all pairs $\{z, z'\} \subseteq X \setminus Y$ for which $\{y_i, z, z'\} \in \mathcal{B}$. Show that $\{R_1, \ldots, R_m\}$ is a tournament schedule on $X \setminus Y$. Show further that this construction can be reversed: a STS($m$) and a tournament schedule of order $m+1$ can be used to build a STS($2m+1$).

Given any $z, z' \in X \setminus Y$, the triple containing $z$ and $z'$ meets $Y$ in a point $y_i$ (see Question 11); so $\{z, z'\} \in R_i$. On the other hand, $y_i$ lies on $m$ triples, of which $(m-1)/2$ are in the subsystem $Y$, so $(m+1)/2$ have the form $\{y_i, z, z'\}$ for some $z, z' \in X \setminus Y$. Since the pairs $\{z, z'\}$ are disjoint, they cover the $m+1$ points of $x \setminus Y$. So we do have a tournament schedule.

The converse follows the argument of Section 8.6 (the case $m = 7$).

**13** Let $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ be STS, of orders $m$ and $n$ respectively. Let $Z = X \times Y$, and let $\mathcal{D}$ consist of all triples of the following types:

- $\{(x,y_1),(x,y_2),(x,y_3)\}$ for $x \in X$, $\{y_1, y_2, y_3\} \in \mathcal{C}$;
- $\{(x_1,y),(x_2,y),(x_3,y)\}$ for $\{x_1, x_2, x_3\} \in \mathcal{B}$, $y \in Y$;
- $\{(x_1,y_1),(x_2,y_2),(x_3,y_3)\}$ for $\{x_1, x_2, x_3\} \in \mathcal{B}$, $\{y_1, y_2, y_3\} \in \mathcal{C}$.

(Note that a triple in $\mathcal{B}$ and one in $\mathcal{C}$ give rise to six triples of the third type, corresponding to the six possible bijections from one to the other.) Show that $(Z, \mathcal{D})$ is a STS of order $mn$. Show further that, if $m > 1$ and $n > 1$, then $(Z, \mathcal{D})$ contains a subsystem of order 9.

Take two points $(x_1,y_1)$ and $(x_2,y_2)$ of $X \times Y$. There are several cases:

(a) If $x_1 = x_2$ and $y_1 \neq y_2$, there is a unique triple $\{y_1,y_2,y_3\} \in \mathcal{C}$: then $(x_1,y_3)$ is the third point of the triple through the two given points.

(b) $x_1 \neq x_2$, $y_1 = y_2$: dual to (a).

(c) $x_1 \neq x_2$ and $y_1 \neq y_2$. There are unique triples $\{x_1,x_2,x_3\} \in \mathcal{B}$ and $\{y_!,y_2,y_3\} \in \mathcal{C}$; then $(x_3,y_3)$ is the third point of the triple.

If $\{x_1,x_2,x_3\} \in \mathcal{B}$ and $\{y_1,y_2,y_3\} \in \mathcal{C}$, then $\{(x_i,y_j) : i,j = 1,2,3\}$ is a subsystem of order 9.

**14** What can you say about the set

$$\{n : \text{ there exists a STS}(n) \text{ with a subsystem of order } 9\}?$$

Two useful observations are:

(a) In the construction of (8.3.1), if either the STS($v$) or the STS($w$) contains an STS(9), then so does the constructed STS($u+w(v-u)$).

(b) The result of Exercise 13.

This allows many constructions; the difficulty is deciding just what we get! Here, for the record, is a result which is close to the best possible:

**Theorem** *For any admissible $n \geq 33$, there is an* STS$(n)$ *containing subsystems of orders* 7 *and* 9.

The proof requires a few preliminaries. The equations $19 = 1+9(3-1)$, $21 = 3.7$, and $25 = 1+3(9-1)$ show that there are STSs of orders $19,21,25$ containing subsystems of orders 7 and 9. The affine STS of order 27 has a subsystem of order 9.

There is a STS(33) containing subsystems of orders 7 and 9. This is more difficult to show, and the proof will be outlined. First, there is a Latin square of order 10 having subsquares of orders 2 and 3. (Take a $10 \times 10$ matrix with submatrices of orders 3 and 2 on the diagonal forming Latin squares with disjoint symbol sets, complete the first five rows, and then use (6.3.1).) Now the construction of (8.3.1) can be generalised: instead of the integers mod $m$, we may use any Latin square of order $m$ in the construction. Now arrange three STS(13)s intersecting in

a triple containing a point $p$, and number the other points in each system so that the indices of the subsquare of order 3 label a triple, while those of the subsquare of order 2 form a triple with $p$. Now check that the constructed STS(33) has the required subsystems.

Finally, there is an STS(37) containing subsystems of orders 7 and 9: this uses a similar construction based on a Latin square of order 12.

Now check that the following equations show the result for orders up to 99. In an expression $n = u \cdot v$, choose a system of order $v$ having a subsystem of order 7.

$$\begin{aligned}
39 &= 1+19(3-1)\\
43 &= 1+21(3-1)\\
45 &= 3\cdot 15\\
49 &= 7\cdot 7\\
51 &= 1+25(3-1)\\
55 &= 1+27(3-1)\\
57 &= 3\cdot 19\\
61 &= 1+3(21-1)\\
63 &= 3\cdot 21\\
67 &= 1+33(3-1)\\
69 &= 3+3(25-3)\\
73 &= 1+3(25-1)\\
75 &= 3\cdot 25\\
79 &= 1+3(27-1)\\
81 &= 3\cdot 27\\
85 &= 7+3(33-7)\\
87 &= 3+21(7-3)\\
91 &= 13\cdot 7\\
93 &= 3\cdot 31\\
97 &= 1+3(33-1)\\
99 &= 3\cdot 33
\end{aligned}$$

For larger values, the constructions in the text can be used, choosing constituent systems containing subsystems of orders 7 and 9.

So far as the original question is concerned, only the case $n = 31$ remains. You

should try this for yourself.

15 and 16 are projects (no solution given).