An introduction to Steiner systems*

Mike Grannell and Terry Griggs,
University of Central Lancashire, Preston

The authors are both graduates of the University of London, and have been working together in combinatorial design theory for 15 years. Construction of the Steiner system $S(5, 6, 108)$ described in this article was one of the first problems they tackled (unsuccessfully) many years ago. but a return to it in 1991 proved successful.

1 Introduction

Begin with a base set of nine elements, say the positive integers from 1 to 9 inclusive. Next consider the following subsets: 123, 456, 789, 147, 258, 369, 159, 267, 348, 168, 249 and 357. (Here, and elsewhere in this article, we will, when convenient, use the simpler notation *abc* for the set $\{a, b, c\}$.) Collectively the above subsets, which are more usually called blocks, have the property that every pair of elements of the base set is contained in precisely one of the blocks. Before proceeding further, readers should verify this fact for themselves. Such a collection of blocks is an example of a Steiner system and this particular configuration is usually denoted by $S(2, 3, 9)$. It is quite easy to see what the three integers 2, 3 and 9 describe. Considering them in reverse order, the 9 gives the number of elements in the base set, and these can be any nine elements; we named them as the positive integers 1 to 9 inclusive only for convenience. The 3 gives the number of elements in each block and the 2 tells us that every pair of elements of the base set, i.e. every subset consisting of two elements, is contained in precisely one block. More succinctly we have a covering of pairs of the base set, each precisely once, by a collection of triples. In this short article our aim will be to introduce some of the elementary theory of Steiner systems, which is a branch of combinatorial mathematics, and to try to give the flavour of what we feel is an intrinsically very interesting topic with many fascinating open problems to be solved. In formal terms, a Steiner system $S(t, k, v)$ comprises a base set having v elements and a family of k-element subsets of this base set. These k-element subsets are called blocks. The blocks have the property that each t-element subset of the base set appears in precisely one block. The reason that these structures have the name of Steiner associated with them is that, in

*This article appeared in *Mathematical Spectrum* **26** *no.3* (1994), 74–80.

1853, the Swiss geometer Jakob Steiner (1796-1863) proposed the problem of how to construct them. Six years later M. Reiss published a solution for the case $t = 2$ and $k = 3$. However, as we describe later, both Steiner and Reiss had been anticipated.

Steiner systems and other related structures have applications in statistics through the design of experiments and in coding theory. For example, consider the problem of comparing nine different breakfast cereals. A single person could not rank all nine with confidence; by the time he or she was on the ninth they would have forgotten the taste of the first. To be reasonable, we can only ask people to rank at most three each. If we asked people to rank two each then to get all $\frac{1}{2} \times 9 \times 8 = 36$ comparisons we would need 36 people. However, if we use the $S(2, 3, 9)$ described above then we can reduce this to 12 people each testing three brands and be sure that every pair is compared precisely once. As an example in coding theory, look at the 12 blocks of $S(2, 3, 9)$ above. Each block has built-in redundancy in the sense that if any two of its digits are correctly received then the block is uniquely defined. This property forms the basis for the construction of codes which can both detect and correct errors. Such codes are particularly important in telecommunications. Similar codes have been used in space missions. Further details can be found in the book by Ian Anderson (reference 1). To conclude this introduction it is perhaps instructive to give a second example. Let the base set be $\{A, B, C, D, E, F, G, H\}$ and let the blocks be $ABCH, ADEH, AFGH, BDFH, BEGH, CDGH, CEFH, DEFG, BCFG,$ $BCDE, ACEG, ACDF, ABEF$ and $ABDG$. These form a Steiner system $S(3, 4, 8)$; there are eight elements in the base set, each block contains four elements and it is easily verified that every triple, i.e. every subset consisting of three elements, is contained in precisely one block.

2 Basic theory

Firstly we develop some elementary but important ideas. Suppose t, k and v are integers satisfying $0 < t < k < v$. Now it is impossible for a system $S(t, k, v)$ to be constructed for all values of t, k and v satisfying the inequality as will be quickly realized if the reader attempts to construct an $S(2, 3, 8)$. So we need to ascertain which values of t, k and v may allow us to construct Steiner systems. Simple necessary conditions on these parameters can be deduced from the following two easy theorems.

Theorem 1. If there exists an $S(t, k, v)$ then there exists an $S(t-1, k-1, v-1)$.

Proof. Choose any element, say x, of the system. Remove all the blocks which do not contain x. Those which remain contain precisely once every t-element subset which also contains x. Thus if we remove the element x from these blocks, what is left is a base set of $v - 1$ elements and blocks containing $k-1$ elements which collectively cover every $(t-1)$-element subset precisely once.

As an illustration of this theorem the reader may obtain a Steiner system $S(2,3,7)$ from the $S(3,4,8)$ given above. Simply choose x as any letter from A to H and apply the procedure described in the proof.

Theorem 2. If there exists an $S(t,k,v)$ then ${}^kC_t$ divides ${}^vC_t$.

Proof. ${}^kC_t$ is the number of t-element subsets in a block. If b is the total number of blocks in the system then the number of t-element subsets covered is $b \times {}^kC_t$. But every t-element subset appears precisely once and there are ${}^vC_t$ t-element subsets, so $b \times {}^kC_t = {}^vC_t$. Hence ${}^vC_t/{}^kC_t$ is an integer (b in fact).

Although the two theorems above are elementary, if we combine them we obtain a condition on the parameter set, the so-called admissibility condition, for the possible existence of a Steiner system $S(t,k,v)$.

Admissibility condition. If there exists an $S(t,k,v)$ then ${}^{k-i}C_{t-i}$ divides ${}^{v-i}C_{t-i}$ for each $i = 0,1,2,...,t-1$.

Proof. By continued application of theorem 1, there exists an $S(t-i,k-i,v-i)$ for $i = 0,1,2,...,t-1$. Then apply theorem 2.

At this point it is perhaps worth noting that, in general, each of the admissibility criteria ${}^kC_t$ divides ${}^vC_t$, ${}^{k-1}C_{t-1}$ divides ${}^{v-1}C_{t-1}$, etc., forces different conditions on the parameter set (t,k,v). They are independent constraints and one does not necessarily imply another. A parameter set which satisfies the admissibility criteria is called an admissible set.

3 Steiner triple systems

We are now in a position to deduce, for given values of t and k, which integers v form an admissible parameter set $\{t,k,v\}$. When $t = 1$, the admissibility condition reduces to the statement that k must divide v, which is elementary anyway and it is equally elementary how to construct such systems. As an example, to construct an $S(1,5,15)$ let the base set be $\{a,b,c,d,e,f,g,h,i,j,k,l,m,n,o\}$; the blocks can then be chosen to be $abcde, fghij$ and $klmno$. The first non-trivial case is when $t = 2$ and $k = 3$, the covering of pairs of elements by triples, and these systems are more often called Steiner triple systems. We begin by working out the admissibility condition on v. By theorem 1, if there exists $S(2,3,v)$ then there exists $S(1,2,v-1)$. Hence 2 divides $v-1$, i.e. v is odd and can be written in the form $v = 2s+1$, where s is a positive integer. Now applying theorem 2 to $S(2,3,v)$, we see that ${}^3C_2$ divides ${}^vC_2$, i.e. 3 divides $\frac{1}{2}v(v-1) = s(2s+1)$. Since 3 is prime then either 3 divides s or 3 divides $2s+1$, i.e. either s must be of the form $3r$ or of the form $3r+1$, where r is a positive integer. Hence $v = 6r+1$ or $6r+3$. Note here what we have done and,

more importantly, what still remains to be done. We have not shown that there actually exist Steiner triple systems $S(2,3,v)$ when $v = 6r+1$ or $6r+3$. We have merely shown that these are the only possible values of v for which such systems can exist. The work of showing whether the necessary admissibility condition is also sufficient is still to come and is more difficult. What is required is a general construction or a number of constructions to produce Steiner triple systems. The first person to solve this problem was an Anglican clergyman living in the nineteenth century. The Reverend T. P. Kirkman (1806-1895) was Rector of Croft, near Warrington in what was then Lancashire. In 1847 (reference 4) he published a paper giving the complete solution to the problem of constructing Steiner triple systems. In the sense that he did not earn his living from mathematics, Kirkman belonged to the line of great amateurs whose contributions have so enriched and advanced the subject. By right the systems should be called Kirkman triple systems, but Kirkman's work was overlooked for many years. However. Kirkman's contributions to the development of combinatorial mathematics were eventually recognized and the name Kirkman triple system is now given to a special type of Steiner triple system with additional properties. Since Kirkman's time many other different constructions of Steiner triple systems have been discovered and we give below our favourite which occurs in the work of the American mathematician, R. M. Wilson (reference 8).

List all triples a, b, c (with a, b and c not necessarily distinct) such that $a + b + c = 0 \pmod{v-2}$. It can be proved that the number of triples so obtained is precisely the required number of blocks for an $S(2,3,v)$. Because some triples contain repeated elements and there are only $v-2$ elements rather than v, we do not as yet have a Steiner triple system. But, as will be seen from the example which follows, such a system can easily be constructed with a little modification. We illustrate the method when $v = 15$. There are three types of triples which sum to zero in arithmetic modulo 13.

Type A (all elements different)

$0,1,12$	$0,2,11$	$0,3,10$	$0,4,9$	$0,5,8$	$0,6,7$
$1,2,10$	$1,3,9$	$1,4,8$	$1,5,7$	$2,3,8$	$2,4,7$
$2,5,6$	$3,4,6$	$3,11,12$	$4,10,12$	$5,9,12$	$5,10,11$
$6,8,12$	$6,9,11$	$7,8,11$	$7,9,10$		

Type B (two elements equal)

$1,1,11$	$11,11,4$	$4,4,5$	$5,5,3$	$3,3,7$	$7,7,12$
$12,12,2$	$2,2,9$	$9,9,8$	$8,8,10$	$10,10,6$	$6,6,1$

Type C (all elements equal)

$0,0,0$

For all $v = 6r+1$ or $6r+3$, then $v-2 = 6r-1$ or $6r+1$ is not divisible by 3. Therefore $0,0,0$ will be the only type C triple. Repeated elements in the type B and type C triples must now be replaced by two further elements

which we call X and Y. Firstly $0, 0, 0$ becomes $0, X, Y$. Next, considering type B triples, observe that these are listed to form a cycle with the non-repeated element of each triple being the repeated element of the next. The first triple $1, 1, 11$ becomes $X, 1, 11$; the second $11, 11, 4$ becomes $Y, 11, 4$, the next $4, 4, 5$ becomes $X, 4, 5$. Continuing in this way, replacing one of the repeated elements in the triples alternately with X and Y, we reach $Y, 6, 1$. It is easily verified that we have constructed an $S(2, 3, 15)$ on the base set $\{0, 1, 2, \ldots, 12, X, Y\}$.

The only problem with this method can occur when the type B triples do not form a single cycle as in the example used. This does not matter if all such cycles contain an even number of triples as the replacement by X and Y in each cycle can be handled independently. However, in certain cases, odd cycles occur. For example when $v = 13$ the type B triples are $1, 1, 9$; $9, 9, 4$; $4, 4, 3$; $3, 3, 5$; $5, 5, 1$; and $10, 10, 2$; $2, 2, 7$; $7, 7, 8$; $8, 8, 6$; $6, 6, 10$. However, observe that these two cycles form a pair, each the negative of the other in arithmetic modulo 11. We replace these triples as follows. The first one becomes $X, 1, 9$; $Y, 9, 4$; $X, 4, 3$; $Y, 3, 5$; and $0, 5, 1$, since the latter cannot be either $X, 5, 1$ or $Y, 5, 1$. Similarly the second one becomes $X, 10, 2$; $Y, 2, 7$; $X, 7, 8$; $Y, 8, 6$; and $0, 6, 10$. Finally two of the type A triples $0, 1, 10$ and $0, 5, 6$ are amended to become $Y, 1, 10$ and $X, 5, 6$ respectively. If this procedure seems complicated then it is suggested that the reader tries out the cases $v = 19, 21, 25, 27$, etc., when it will be realized that this is an extremely simple method of constructing Steiner triple systems. In fact this method works for all $v = 6r+1$ or $6r+3$, thus showing that the necessary admissibility condition for a Steiner triple system is indeed sufficient.

4 Large Steiner systems

It is perhaps a surprise that after Kirkman's paper over a century passed until another case was completely solved. In 1960 H. Hanani proved that the necessary admissibility condition $v = 6r + 2$ or $6r + 4$ is also sufficient for Steiner systems $S(3, 4, v)$ (reference 3). Since then Hanani has also proved that the necessary admissibility condition $v = 12r + 1$ or $12r + 4$ and $v = 20r + 1$ or $20r + 5$ are also sufficient for Steiner systems $S(2, 4, v)$ and $S(2, 5, v)$, respectively. Today these are the only four pairs of values of t and k, i.e. $t = 2, k = 3, 4, 5$ and $t = 3, k = 4$ for which the problem of constructing Steiner systems $S(t, k, v)$ for all possible values of v is completely solved. However, some very recent work has resulted in the problem being almost completely solved when $t = 2$ and $k = 6, 7, 8, 9$. At this point it might also be worth noting that, unlike the cases which have been completely solved, in general it is known that the necessary admissibility condition is not always sufficient. For example $v = 36$ is an admissible value for $t = 2$ and $k = 6$, but there is no Steiner system $S(2, 6, 36)$. This problem, which is also known as the problem of the 36 officers and is related to ideas in finite geometry, goes back to Euler and was shown to be impossible by G. Tarry (reference 7).

However, if the state of knowledge concerning the existence of Steiner sys-

tems with $t = 2$ and $t = 3$ is patchy, results dealing with $t = 4$ and $t = 5$ are very scarce indeed and when $t \geq 6$ they are completely non-existent! Until 1975 the only known systems of these types were $S(5, 6, 12)$ and $S(5, 8, 24)$ together with the systems $S(4, 5, 11)$ and $S(4, 7, 23)$ obtained from them using theorem 1. The existence of all these systems is related to some deep results in group theory. In 1975, R. H. F. Denniston (reference 2) constructed further systems $S(5, 6, v)$ for $v = 24, 48$ and 84, and $S(5, 7, 28)$. Two years later W. H. Mills (reference 5) added $S(5, 6, 72)$. There was then no further progress for over 10 years. Denniston's systems were constructed using hand calculations. Recently, using a computer, we have constructed $S(5, 6, 108)$. The reason for using a computer can be seen if the number of blocks in a Steiner system $S(5, 6, 108)$ is calculated: there are precisely 18 578 196 of them. Using sophisticated computer equipment at the University of Toronto and working with Professor Rudi Mathon of that university, we subsequently constructed $S(5, 6, 132)$, consisting of 51 553 216 blocks. Truly enormous systems! Our next target is $(5, 6, 168)$, with no fewer than 175 036 708 blocks, though we appear to be on the limit both of mathematical reasoning concerning what the structure of such a system might be and of computer technology to effect the calculations involved.

To conclude, we give a simple construction of the Steiner system $S(5, 6, 12)$. The construction, which is purely combinatorial in nature. was first given by R. G. Stanton (reference 6). We start by constructing $S(4, 5, 11)$, which contains 66 blocks. Let the base set be $V = \{A, B, C, D, E, 1, 2, 3, 4, 5, 6\}$ and suppose that $ABCDE$ is the first block. It is then easy to calculate the numbers of other blocks which contain specified numbers of letters and numbers. Specifically there are 30 blocks of the form LLLNN, 20 blocks of the form LLNNN and 15 blocks of the form LNNNN, where L is a letter and N a number.

Begin with the LNNNN blocks. Consider the following scheme:

A	12	34	56
B	13	25	46
C	14	26	35
D	15	24	36
E	16	23	45

Note that each pair of digits occurs in the scheme precisely once and further that each digit occurs precisely once in each row. From each row form three blocks of the system by the letter and two of the three pairs of digits. Thus the first row generates blocks $A1234$, $A1256$ and $A3456$. This gives 15 blocks of the form LNNNN.

Considering next the blocks of the form LLNNN, observe that there are six numbers of which we require three in each block and that ${}^6C_3 = 20$, exactly the number required. Each triple of digits is contained in precisely one block and it is determined which the two letters must be. For example, consider 123. Blocks $A1234$, $B1325$ and $E1623$ already occur, so we must have $123CD$.

Finally, when the 30 blocks of the form LLLNN are considered, everything is forced, as the reader will find if the construction is followed through. Obtaining

the larger system $S(5,6,12)$ is easy. First a twelfth element, say ∞, is adjoined to all the blocks of the $S(4,5,11)$. Then 66 further blocks are created as the complements of the existing 66 blocks; the 132 blocks so formed are a Steiner system $S(5,6,12)$.

References

1. I. Anderson, *A First Course in Combinatorial Mathematics*, 2nd edn. (Clarendon Press. Oxford, 1989).
2. R. H. F. Denniston. Some new 5-designs, *Bull. London Math. Soc.* **8** (1976). 263–267.
3. H. Hanani, On quadruple systems, *Canad. J. Math.* **12** (1960), 145–157.
4. T. P. Kirkman, On a problem in combinations. *Cambridge and Dublin Math. J.* **2** (1847), 191–204.
5. W. H. Mills, A new 5-design, *Ars Combinatoria* **6** (1978), 193–195.
6. R. G. Stanton, A conjecture on quintuple systems. *Ars Combinatoria* **10** (1980), 187–192.
7. G. Tarry, Le problème de 36 officiers. *C.R. Assoc. France Avanc. Sci. Nat.* **1** (1900), 122–123.
8. R. M. Wilson, Some partitions of all triples into Steiner triple systems. *Springer Lecture Notes in Mathematics* **411** (1974), 267–277.