Wilson's theorem for block designs
Talks given at LSBU June–August 2014
Tony Forbes

Steiner systems $S(2,k,v)$

For $k \ge 3$, a *Steiner system* $S(2,k,v)$ is usually defined as a pair $(V,\mathcal{B})$, where V is a set of cardinality v of *points* and $\mathcal{B}$ is a set of k-element subsets of V, usually called *blocks*, or *lines* if the system has some geometric significance, with the property that each pair of points is contained in precisely one block. For example, to construct a Steiner system $S(2,3,7)$ we may take $V = \{0,1,2,3,4,5,6\}$ and

$$\mathcal{B} \;=\; \{\{0,1,3\},\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,0\},\{5,6,1\},\{6,0,2\}\}.$$

In this example each line has three points and a point occurs at the intersection of three lines, This is the Fano plane, a finite projective plane of order 2.

We say that a positive integer v is *admissible* if $v(v-1) \equiv 0 \pmod{k(k-1)}$ and $v-1 \equiv 0 \pmod{k-1}$. A necessary condition for the existence of a Steiner system $S(2,k,v)$ is that v is admissible. This guarantees that the cardinality of the block set, $v(v-1)/(k(k-1))$, as well as the number of times a specific point occurs amongst the blocks, $(v-1)/(k-1)$, are both non-negative integers. Numbers of the form $v = k(k-1)x+1$ and $v = k(k-1)x+k$, $x \ge 0$, are always admissible, and if k is a prime power there are no others.

The *existence problem* for given k asks for which admissible v does there exist a Steiner system $S(2,k,v)$. Two *trivial* Steiner systems always exist, namely the $S(2,k,1)$, with empty block set, and the $S(2,k,k)$, where there is a single block of size k. The existence problem is completely solved for $k=3$ (Kirkman, 1847) and for $k=4,5$ (Hanani, 1961); Steiner systems $S(2,k,v)$ exist for $k=3,4,5$ and all admissible v. For $k=6,7,8,9$, the existence problem is solved for all except a small number of admissible v; see [2] for details. For prime power q, there are a few infinite classes of known designs (see [2] and [4] for details):

(i) $S(2,q,q^n)$, affine geometries (affine planes when $n=2$),
(ii) $S(2,q,q^{2n+2}-q^{2n+1}+q)$, $q \ge 3$,
(iii) $S(2,q+1,q^n+\cdots+q+1)$, projective geometries (projective planes if $n=2$),
(iv) $S(2,q+1,q^3+1)$, unital designs,
(v) $S(2,q+1,q^{2n+1}+1)$,
(vi) $S(2,q+1,q^{2n+2}+q^{2n+1}+1)$,
(vii) $S(2,q+1,q^{2n+2}+q+1)$,
(viii) $S(2,2^r,2^{2r+1}-2^r)$, $r \ge 2$, oval designs,
(ix) $S(2,2^r,2^{r+s}+2^r-2^s)$, $s > r \ge 2$, Denniston designs.

The only known Steiner system with $k \ge 10$ and $(v-1)/(k-1) \le 41$ apart from affine and projective planes is the oval/Denniston design $S(2,16,496)$ [4].

Admissibility is not always sufficient. Fisher's inequality asserts that a non-trivial $S(2,k,v)$ must have at least as many blocks as points, implying that $v \ge k(k-1)+1$. Also we have the Bruck-Ryser theorem. *If a Steiner system $S(2,k,k^2)$ (affine plane of order k) exists and $k \equiv 1$ or $2 \pmod 4$, then k is the sum of two integer squares.* Moreover, a Steiner system $S(2,k+1,k^2+k+1)$ (projective plane of order k) exists if and only if an affine plane of order k exists. Hence there is no $S(2,k,k^2)$ and no $S(2,k+1,k^2+k+1)$ for $k=6,14,21,22,30,\ldots$. Finally, there is no $S(2,10,100)$ and no $S(2,11,111)$ (Lam, Thiel & Swiercz, 1989), and there is no $S(2,6,42)$ (Houghten, Thiel, Janssen & Lam, 2001).

Let us look at the case $k=10$. For non-prime-power k further residue classes modulo $k(k-1)$ are admissible, and indeed when $k=10$ the admissible v are $90x+d$, $d=$

$1, 10, 45, 55$, $x \geq 0$. The trivial $S(2, 10, 1)$ and $S(2, 10, 10)$ exist. However $S(2, 10, 45)$ and $S(2, 10, 55)$ do not by Fisher's inequality. The next in the sequence is $S(2, 10, 91)$, the projective plane of order 9, which exists, followed by $S(2, 10, 100)$, the affine plane of order 10, which does not. Ignorance prevents me from saying anything about $S(2, 10, 135)$, $S(2, 10, 145)$ and many others with small v. Some designs appear in [1], and I have managed to produce examples of $S(2, 10, v)$ with v = 1621, 2161, 2251, 2341 (Zoe's design II), 2521, 2791, 2971, 3061, 3331, 3511 and 3691.

The *extremal existence problem* was solved by R. M. Wilson in 1975 [7]. *Given $k \geq 3$, for all sufficiently large admissible v, there exists a Steiner system $S(2, k, v)$.* And more recently the extremal existence problem was solved by Peter Keevash for more general designs. *Given $t \geq 2$ and $k > t$, for all sufficiently large admissible v, there exists a Steiner system $S(t, k, v)$.*

Although Wilson and Keevash appear to have killed the subject, one can nevertheless argue that there is still quite a lot of work to do, especially for $k \geq 10$ in the finite but vast range from $v = 1$ to 'sufficiently large'. So I suggest that the *concrete existence problem* might have some interest: *given suitable k, exhibit a non-trivial Steiner system $S(2, k, v)$*, or more generally, *given suitable t and k, exhibit a non-trivial Steiner system $S(t, k, v)$*. As far as I am aware, even for $S(2, k, v)$ designs this problem has not been solved for large k where neither k nor $k - 1$ is a prime power. I have found Steiner systems $S(2, 15, 243391)$, $S(2, 21, 2031451)$ and $S(2, 22, 4578883)$ but I do not know of a single example of a non-trivial $S(2, 100, v)$, say.

A *cyclic* Steiner system $S(2, k, v)$ is one where the block set is invariant under the mapping $x \mapsto x + 1 \pmod{v}$. The $S(2, 3, 7)$ is cyclic. We may take the single *starter block* $\{0, 1, 3\}$ and generate the entire block set by repeated application of $x \mapsto x + 1 \pmod{7}$. Similarly, the 57 blocks of a cyclic $S(2, 3, 19)$ are obtained from the three starter blocks

$$\{1, 3, 9\}, \quad \{8, 5, 15\}, \quad \{7, 2, 6\}$$

under the action of the mapping $x \mapsto x + 1 \pmod{19}$. A cyclic Steiner system $S(2, k, v)$ exists if the differences generated by the starter blocks cover all non-zero elements of $\mathbb{Z}_v$. You can confirm that the differences generated by the starter blocks of the $S(2, 3, 19)$, namely

$$\{\pm 2, \pm 6, \pm 8\}, \quad \{\pm 3, \pm 9, \pm 7\}, \quad \{\pm 5, \pm 4, \pm 1\},$$

are indeed all distinct and non-zero modulo 19. In general a cyclic Steiner system of the form $S(2, k, k(k-1)t + 1)$ requires t starter blocks.

A simple form of Wilson's theorem

Theorem 1 *Given $k \geq 3$, for all sufficiently large t, there exists a Steiner system $S(2, k, v)$ whenever $v = k(k-1)t + 1$ is prime.*

Proof Suppose $k \geq 3$, $t \geq 1$ and $v = k(k-1)t + 1$ is prime. Let ρ be a primitive root modulo v and for $x \not\equiv 0 \pmod{v}$ define $\log x$ as the unique number ϕ, $0 \leq \phi \leq v - 2$, such that $x = \rho^\phi$. Henceforth let us agree to do arithmetic modulo v on the elements of $\mathbb{Z}_v$ and modulo $v - 1$ on their logarithms.

Write $K = k(k-1)/2$ and let $w = \rho^K$. Then $w^t = -1$ and $w^h \neq \pm 1$ for $0 < h \leq t - 1$. Let

$$B = \{1, a, a^2, \ldots, a^{k-1}\}$$

and we shall attempt to find a such that $\{w^h B : 0 \leq h \leq t - 1\}$ form the t starter blocks of a cyclic Steiner design $S(2, k, v)$. For this to happen the set of differences

$$D = \{(-1)^\epsilon w^h (a^s - a^r) : \epsilon = 0, 1, \ 0 \leq h \leq t - 1, \ 0 \leq r < s \leq k - 1\}$$

must cover the non-zero residues modulo v. Observe that there are $K = k(k-1)/2$ choices for (r, s), t choices for h and two choices for ϵ, making a total of $2Kt = v - 1$. Therefore the elements of D as described must be distinct modulo v. Taking logs gives

$$\Delta = \{\epsilon Kt + Kh + \log(a^s - a^r) : \ \epsilon = 0, 1, \ 0 \le h \le t-1, \ 0 \le r < s \le k-1\}$$

since $-1 = \rho^{Kt}$. We now require Δ to cover all residues modulo $v - 1 = 2Kt$. But

$$\{K(\epsilon t + h) : \ \epsilon = 0, 1, \ 0 \le h \le t-1\}$$

covers all multiples of K and is independent of a. Therefore it suffices to choose a such that the K numbers

$$\Delta_{r,s} = \log(a^s - a^r), \quad 0 \le r < s \le k-1,$$

cover the residue classes modulo K. This construction really does work sometimes for large k and small v. For instance, $a = 16662$ and multiplier $w = 118347$ give the Steiner system $S(2, 15, 243391)$, where $t = 1159$, $\rho = 3$ and $a^k = 1$. Note that any number of the form w^j with $\gcd(j, 2t) = 1$ can be be used as the multiplier, the smallest one for this design being $234 = 118347^{1017}$.

Let $\Phi_n(x)$ denote the n-th cyclotomic polynomial, so that

$$\Phi_1(x) = x - 1, \ \Phi_2(x) = x + 1, \ \Phi_3(x) = x^2 + x + 1, \ \Phi_4(x) = x^2 + 1, \ \ldots .$$

Then, recalling that $x^n - 1 = \prod_{d|n} \Phi_d(x)$,

$$\Delta_{r,s} = \log(a^s - a^r) = r \log a + \sum_{d|s-r} \log \Phi_d(a).$$

By choosing suitable values modulo K for $\log a$ and $\log \Phi_d(a)$ we can ensure that the K values of $\Delta_{r,s}$, $0 \le r < s \le k-1$, cover the residues modulo K. For this purpose we define

$$\gamma_n = (n-1)k - \frac{n(n-1)}{2} - \sum_{d|n, \ 1<d<n} \gamma_d.$$

Observe that if

$$\log a \equiv \alpha, \quad \gcd(\alpha, K) = 1, \quad \text{and} \quad \log \Phi_n(a) \equiv \alpha\gamma_n, \quad n = 2, 3, \ldots, k-1, \quad (\text{mod } K) \quad (1)$$

then

$$\Delta_{r,s} \equiv \log(a-1) + \alpha r + \alpha \sum_{d|s-r, \ d>1} \gamma_d, \quad 0 \le r < s \le k-1 \pmod K$$

will indeed have the desired property. For example, with $k = 6$ we have $\gamma_2 = 5$, $\gamma_3 = 9$, $\gamma_4 = 7$, $\gamma_5 = 14$, and we can compute $\Delta_{r,s}$ as in the following table.

r	s	$\Delta_{r,s} - \log(a-1)$	r	s	$\Delta_{r,s} - \log(a-1)$	r	s	$\Delta_{r,s} - \log(a-1)$
0	1	0	1	2	α	2	4	$\alpha(2+\gamma_2) = 7\alpha$
0	2	$\alpha\gamma_2 = 5\alpha$	1	3	$\alpha(1+\gamma_2) = 6\alpha$	2	5	$\alpha(2+\gamma_3) = 11\alpha$
0	3	$\alpha\gamma_3 = 9\alpha$	1	4	$\alpha(1+\gamma_3) = 10\alpha$	3	4	3α
0	4	$\alpha(\gamma_2+\gamma_4) = 12\alpha$	1	5	$\alpha(1+\gamma_2+\gamma_4) = 13\alpha$	3	5	$\alpha(3+\gamma_2) = 8\alpha$
0	5	$\alpha\gamma_5 = 14\alpha$	2	3	2α	4	5	4α

So it suffices to find a such that (1) holds with $\alpha = 1$, say. Define a multiplicative character of order K modulo v by $\chi(x) = \exp(2\pi i/K \log(x))$. Define $\chi(0) = 0$. Define the polynomials

$$f_1(x) = x\rho^{-1}, \quad f_n(x) \;=\; \Phi_n(x)\rho^{-\gamma_n}, \quad n = 2, 3, \ldots, k-1.$$

We now want to show that there exists a such that

$$\chi(f_n(a)) \;=\; 1 \;\text{ for } 1 \le n \le k-1, \tag{2}$$

for then we will have $\log f_n(a) \equiv 0 \pmod K$, $n = 1, 2, \ldots, k-1$. Let

$$\pi(x) \;=\; \prod_{n=1}^{k-1} \sum_{i_n=0}^{K-1} \chi(f_n(x)^{i_n}) \;=\; \left(\sum_{i_1=0}^{K-1} \chi(f_1(x)^{i_1})\right) \cdots \left(\sum_{i_{k-1}=0}^{K-1} \chi(f_{k-1}(x)^{i_{k-1}})\right).$$

If (2) holds then $\pi(a) = K^{k-1}$. On the other hand, if $\chi(f_n(a)) \neq 1$ for some n, then $\pi(a) = 0$ except possibly for those a corresponding to roots of $f_n(x)$. Here we are using the fact that

$$1 + \chi(z) + \chi(z)^2 + \cdots + \chi(z)^{K-1} \;=\; \begin{cases} 1 & \text{if } \chi(z) = 0, \\ K & \text{if } \chi(z) = 1, \\ 0 & \text{if } \chi(z) \neq 0, 1. \end{cases}$$

So we have reduced our task to showing that there exists a such that $\pi(a) \neq 0$ and a avoids the roots of the polynomials $f_n(x)$. Put

$$\Sigma \;=\; \sum_{x=0}^{v-1} \pi(x)$$

and observe that

$$\pi(x) \;=\; 1 + \underbrace{\sum_{i_1=0}^{K-1} \sum_{i_2=0}^{K-1} \cdots \sum_{i_{k-1}=0}^{K-1}}_{i_1,\, i_2,\, \ldots,\, i_{k-1} \text{ not all zero}} \prod_{n=1}^{k-1} \chi(f_n(x)^{i_n}),$$

as can be seen by multiplying out the expression for $\pi(x)$ and splitting off the term where all the exponents of the $f_n(x)$ are zero. Thus

$$\begin{aligned} \Sigma \;&=\; \sum_{x=0}^{v-1} \left(1 \;+\; \sum_{\substack{i_1=0 \\ i_1,\, i_2,\, \ldots,\, i_{k-1} \text{ not all zero}}}^{K-1} \sum_{i_2=0}^{K-1} \cdots \sum_{i_{k-1}=0}^{K-1} \prod_{n=1}^{k-1} \chi(f_n(x)^{i_n}) \right) \\ &=\; v \;+\; \sum_{\substack{i_1=0 \\ i_1,\, i_2,\, \ldots,\, i_{k-1} \text{ not all zero}}}^{K-1} \sum_{i_2=0}^{K-1} \cdots \sum_{i_{k-1}=0}^{K-1} \; \sum_{x=0}^{v-1} \chi\left(\prod_{n=1}^{k-1} f_n(x)^{i_n} \right). \end{aligned}$$

Now if $m > n \ge 1$ and v divides neither m nor n, then $\gcd(\Phi_m(x), \Phi_n(x)) = 1$ in $\mathbb{Z}_v[x]$ (see, for example [5, Theorem 8.2.2]). Moreover, if v does not divide n, $x^n - 1$ has no repeated roots in $\mathbb{Z}_v[x]$ ([5, Corollary 8.2.1]). Therefore, provided v is not too small, none of the polynomials $\prod_{n=1}^{k-1} f_n(x)^{i_n}$ can be a constant multiple of a K-th power modulo v. So it follows from Weil's theorem [6, Theorem 2C] that

$$\sum_{x=0}^{v-1} \chi\left(\prod_{n=1}^{k-1} f_n(x)^{i_n} \right) \;=\; O(\sqrt{v}).$$

Hence we have $\Sigma > v - O(\sqrt{v})$ and therefore, since the number of roots of the polynomials $f_n(x)$ is bounded as $v \to \infty$, for sufficiently large v there exists a such that $\pi(a) \neq 0$ and $f_n(a) \neq 0$ for $n = 1, 2, \ldots, k-1$. $\square$

Alternatively, if t is odd, we can put $w = \rho^{2K}$. The set of logarithms of differences becomes

$$\Delta' = \{\epsilon K t + 2Kh + \log(a^s - a^r) : \epsilon = 0, 1,\ 0 \leq h \leq t-1,\ 0 \leq r < s \leq k-1\}$$

in which $\{\epsilon t + 2h : \epsilon = 0, 1,\ 0 \leq h \leq t-1\}$ covers the multiples of K modulo $v-1$, and the proof proceeds as before. For instance, multipliers $77314 = 3^{210}$ and $305 = 77314^{313}$ also work with $a = 16662$ to create a Steiner system $S(2, 15, 243391)$.

It would not be surprising if there is no realistic prospect of finding a multiplier system $S(2, k, k(k-1)t+1)$ with large k and base block $\{1, a, \ldots, a^{k-1}\}$ where the somewhat restrictive condition (1) actually holds. The value $a = 16662$ used as above for constructing an $S(2, 15, 243391)$ does not satisfy (1). On the other hand, $a = 107466$ with $\rho = 17$ for $S(2, 7, 173293)$ and $a = 118008$ with $\rho = 5$ for $S(2, 8, 1287553)$ do.

The proof should work also for powers of sufficiently large primes using appropriate Galois fields. Or one can use the product construction: given Steiner systems $S(2, k, v)$ and $S(2, k, w)$ as well as $k-2$ MOLS of side v, there exists a Steiner system $S(2, k, vw)$.

References

[1] R. J. R. Abel, Some New BIBDs with $\lambda = 1$ and $6 \leq k \leq 10$, *J. Combin. Designs* **4** No. 1 (1996), 27–50.

[2] P. Adams, D.E. Bryant and M. Buchanan, A survey on the existence of G-designs, *J. Combin. Des.* **16** (2008), 373–410.

[3] I. Anderson, *Combinatorial Designs and Tournaments*, Oxford, 1997.

[4] C. J. Colbourn & J. Dinitz, *Handbook of Combinatorial Designs*, Boca Raton, 2007.

[5] P. Garrett, *Abstract Algebra*, CRC Press LLC, 2007.

[6] W. M. Schmidt, *Equations over Finite Fields, An Elementary Approach*, Springer–Verlag, Lecture Notes in Mathematics 536, Berlin, 1976. *Proc. British Combinatorial Conf.* 1975, 647–659.

[7] R. M. Wilson, Decompositions of complete graphs into subgraphs isomorphic to a given graph, *Proc. British Combinatorial Conf.* 1975, 647–659.