The Bruck–Ryser theorem for projective planes

Talks given at LSBU, October 2014

Tony Forbes

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

For $k \geq 3$, 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 $V = \{1,2,3,4,5,6,7\}$ and

$$\mathcal{B} \;=\; \{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}\}.$$

In this example each line has three points and a point occurs at the intersection of three lines, This is the Fano plane, the 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 $v = k(k-1)x+k$, $x \geq 0$, are always admissible, and if k is a prime power there are no others. When $x = 0$, we get the two *trivial* systems $S(2,k,1)$ and $S(2,k,k)$. Of more interest is the case $x = 1$: an $S(2,n+1,n^2+n+1)$ is called a *projective plane* of order n and an $S(2,n,n^2)$ is called an *affine plane* of order n. A projective plane of order n exists iff an affine plane of order n exists, and both exist whenever n is a prime power. For example, the affine plane of order 3 has 9 points and 12 blocks:

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

Partitioning into four sets of parallel lines, adding 'points at infinity' and a 'line at infinity' gives the projective plane of order 3, with 13 points and 13 blocks:

$$\{1,2,3,10\},\{4,5,6,10\},\{7,8,9,10\},\{1,4,7,11\},\{2,5,8,11\},\{3,6,9,11\},$$
$$\{1,5,9,12\},\{2,6,7,12\},\{3,4,8,12\},\{1,6,8,13\},\{2,4,9,13\},\{3,5,7,13\},$$
$$\{10,11,12,13\}.$$

Admissibility is not sufficient. Fisher's inequality asserts that a non-trivial $S(2,k,v)$ must have at least as many blocks as points, implying that $v \geq k(k-1)+1$. Also we have the Bruck–Ryser theorem, below, as well as the result of Lam, Thiel & Swiercz (1989), *there is no projective plane of order 10.*

The Bruck–Ryser theorem

Theorem 1 *If a projective plane of order n exists and $n \equiv 1$ or $2 \pmod 4$, then n is the sum of two integer squares.*

Proof

This is based on [1, section 9.8]. Suppose $n \equiv 1$ or $2 \pmod 4$ and a projective plane $\mathcal{P}$ of order n exists. Let A be an *incidence matrix* of $\mathcal{P}$, where the rows correspond to points and the columns to blocks. Thus $A_{p,b} = 1$ if point p occurs in block b, $A_{p,b} = 0$ otherwise. Let $v = n^2+n+1$ be the number of points in $\mathcal{P}$. Then $\mathcal{P}$ has v blocks and

so its incidence matrix A is square. Moreover, $|A| = (n+1)n^{n(n+1)/2}$ and hence A is non-singular. Furthermore,

$$AA^{\mathrm{T}} \;=\; A^{\mathrm{T}}A \;=\; nI + J,$$

where J is the $v \times v$ all-ones matrix.
Let $x_1, \ldots, x_v$ denote variables, let $x = [x_1 \;\ldots\; x_v]$ and let $z = [z_1 \;\ldots\; z_v] = xA$. Then

$$zz^{\mathrm{T}} \;=\; xAA^{\mathrm{T}}x^{\mathrm{T}} \;=\; nxx^{\mathrm{T}} + xJx^{\mathrm{T}}.$$

Hence

$$\sum_{i=1}^{v} z_i^2 \;=\; n\sum_{i=1}^{v} x_i^2 + \left(\sum_{i=1}^{v} x_i\right)^2.$$

Let x_{v+1} denote another variable and add nx_{v+1}^2 to both sides:

$$\sum_{i=1}^{v} z_i^2 + nx_{v+1}^2 \;=\; n\sum_{i=1}^{v+1} x_i^2 + \left(\sum_{i=1}^{v} x_i\right)^2 \;=\; n\sum_{i=1}^{v+1} x_i^2 + s^2, \tag{1}$$

say. Observe that $v+1$ is a multiple of 4. (This is where we require the assumption that $n \equiv 1$ or $2 \pmod 4$.) So we can split the x_i^2 sum into $(v+1)/4$ sets of four.

$$n\sum_{i=1}^{v+1} x_i^2 \;=\; \sum_{i=0}^{(v+1)/4-1} n(x_{4i+1}^2 + x_{4i+2}^2 + x_{4i+3}^2 + x_{4i+4}^2).$$

Suppose $n = n_1^2 + n_2^2 + n_3^2 + n_4^2$, let

$$N \;=\; \begin{bmatrix} n_1 & -n_2 & -n_3 & -n_4 \\ n_2 & n_1 & -n_4 & n_3 \\ n_3 & n_4 & n_1 & -n_2 \\ n_4 & -n_3 & n_2 & n_1 \end{bmatrix}$$

and observe that $|N| = n^2$; so N is non-singular. For $i = 0, 1, \ldots, (v+1)/4 - 1$, let

$$\begin{bmatrix} y_{4i+1} \\ y_{4i+2} \\ y_{4i+3} \\ y_{4i+4} \end{bmatrix} \;=\; N \begin{bmatrix} x_{4i+1} \\ x_{4i+2} \\ x_{4i+3} \\ x_{4i+4} \end{bmatrix}.$$

Then

$$y_{4i+1}^2 + y_{4i+2}^2 + y_{4i+3}^2 + y_{4i+4}^2 \;=\; n(x_{4i+1}^2 + x_{4i+2}^2 + x_{4i+3}^2 + x_{4i+4}^2),$$

and plugging these 4-tuples into (1) gives

$$\sum_{i=1}^{v} z_i^2 + nx_{v+1}^2 \;=\; \sum_{i=1}^{v+1} y_i^2 + s^2. \tag{2}$$

The left-hand side of (2) and the sum on the right-hand side of (2) are positive definite quadratic forms. Moreover, matrix A and N are non-singular. Therefore by part (i) of Lemma 1, the left-side and the right-hand sum of (2) are positive definite quadratic forms in terms of all the variables $x_1, x_2, \ldots, x_{v+1}$. So it is possible to find

$$y_i = a_1x_1 + a_2x_2 + \cdots + a_{v+1}x_{v+1} \;\text{ and }\; z_j = b_1x_1 + b_2x_2 + \cdots + b_vx_v,$$

where a_1 and b_1 are not both zero. Now put

$$x_1 \;=\; -\,\frac{(a_2 \pm b_2)x_2 + \cdots + (a_v \pm b_v)x_v + a_{v+1}x_{v+1}}{a_1 \pm b_1},$$

choosing a sign which makes $a_1 \pm b_1$ non-zero. Then $y_i \pm z_j = 0$; so $y_i^2 = z_j^2$, and hence y_i^2 and z_j^2 can be cancelled from both sides of (2). By Lemma 1, part (ii), after the substitution and cancellation, the left-hand side and the right-hand sum are positive definite quadratic forms in all of x_2, x_3, ..., x_{v+1}. So the process may be repeated with x_2. After v such cancellations we are left with

$$nx_{v+1}^2 \;=\; Y^2 + s^2,$$

Where Y represents the last surviving y_i. Then s as well as Y are rational multiples of x_{v+1}, the last remaining variable. Finally we choose x_{v+1} to be an integer that makes both Y^2 and s^2 integers. Hence there exist integers X, Y and s such that

$$nX^2 = Y^2 + s^2.$$

The theorem now follows from Lemma 3. □

A *quadratic form* involving r real variables $x_1, x_2, ..., x_r$ is an expression such as

$$q(x_1, x_2, \ldots, x_r) \;=\; \sum_{1 \le i,j \le r} c_{i,j} x_i x_j. \tag{3}$$

A quadratic form $q(x_1, x_2, \ldots, x_r)$ is *positive definite* if $q(x_1, x_2, \ldots, x_r) > 0$ unless $x_1 = x_2 = \cdots = x_r = 0$. So each variable must actually occur with non-zero coefficient somewhere on the right of (3). If $q(x_1, x_2, \ldots, x_r) = X^{\mathrm{T}}QX$ for some matrix Q, where $X = (x_1, x_2, \ldots, x_r)$, then $q(x_1, x_2, \ldots, x_r)$ is positive definite iff all the eigenvalues of Q are positive. A useful property of these things is that we can make substitutions and non-singular linear transformations without affecting positive definiteness and without unexpected loss of variables. This is expressed more formally in Lemma 1.

Lemma 1 *Let $q(x_1, x_2, \ldots, x_r)$ be a positive definite quadratic form in variables $x_1, x_2, \ldots, x_r$.*
(i) Let $x = (x_1, x_2, \ldots, x_r)$, $u = (u_1, u_2, \ldots, u_r)$ and suppose $x = Pu$ for some non-singular matrix P. Then $q'(u_1, u_2, \ldots, u_r)$, obtained by making the substitutions $x = Pu$ in $q(x_1, x_2, \ldots, x_r)$, is a positive definite quadratic form in all variables $u_1, u_2, \ldots, u_r$.
(ii) Furthermore, $q''(x_2, \ldots, x_r)$, obtained by making the substitution $x_1 = k_2x_2 + \cdots + k_rx_r$ in $q(x_1, x_2, \ldots, x_r)$, is a positive definite quadratic form in all variables $x_2, \ldots, x_r$.

Proof
(i) Suppose $q'(a_1, a_2, \ldots, a_r) \le 0$ with $a_1, a_2, \ldots, a_r$ not all zero. Then $(b_1, b_2, \ldots, b_r) = P(a_1, a_2, \ldots, a_r)$ is non-zero and $q(b_1, b_2, \ldots, b_r) = q'(a_1, a_2, \ldots, a_r) \le 0$, contradicting the positive definiteness of q. Now suppose a variable is missing from q', say u_1 by relabelling if necessary. Then $(c_1, c_2, \ldots, c_r) = P(1, 0, \ldots, 0)$ is non-zero and $q(c_1, c_2, \ldots, c_r) = q'(1, 0, \ldots, 0) = 0$, again contradicting positive definiteness.
(ii) If $q''(a_2, \ldots, a_r) \le 0$ for some $a_2, \ldots, a_r$ not all zero, then $q(k_2a_2 + \cdots + k_ra_r, a_2, \ldots, a_r) \le 0$, contradicting the positive definiteness of q. Now suppose a variable is missing from q'', say x_2 by relabelling if necessary. Then $q(k_2, 1, 0, \ldots, 0) = q''(1, 0, \ldots, 0) = 0$, again contradicting positive definiteness. □

Lemma 2 *Suppose p is prime and there exist integers A and B, not both divisible by p, such that*

$$A^2 + B^2 \equiv 0 \pmod{p}.$$

Then p is the sum of two integer squares.

Proof

The case $p = 2$ is left to the reader. So assume p is odd and suppose $A^2 + B^2 = rp$ with $r > 0$ and with A and B chosen to make r as small as possible.

Now suppose $r \neq 1$. Since $r > 1$ we can find a, b such that

$$a \equiv A \pmod{r}, \quad b \equiv B \pmod{r} \quad \text{and} \quad |a|, |b| \leq r/2.$$

Then

$$a^2 + b^2 \equiv A^2 + B^2 \equiv 0 \pmod{r}, \qquad a^2 + b^2 = rt, \text{ say.}$$

Moreover, $t < r$ since $a^2 + b^2 \leq r^2/2 < r^2$. So

$$r^2 tp = (A^2 + B^2)(a^2 + b^2) = (Aa + Bb)^2 + (Ab - Ba)^2. \tag{4}$$

But

$$Aa + Bb \equiv A^2 + B^2 \equiv 0 \equiv AB - AB \equiv Ab - Ba \pmod{r}.$$

So we can divide (4) by r^2 to obtain

$$\left(\frac{Aa + Bb}{r}\right)^2 + \left(\frac{Ab - Ba}{r}\right)^2 = tp$$

with $t < r$, contradicting the smallestness of r. □

Lemma 3 *For positive integer n, suppose there exist integers A, B and C, not all zero, such that*

$$nC^2 = A^2 + B^2.$$

Then n is the sum of two squares.

Proof

Suppose n is square-free, $n = p_1 \dots p_r$, say, where $p_1, \dots, p_r$ are distinct primes. We may assume that A, B, C have no common factor. So A and B cannot both be divisible by p_i, for otherwise $p_i | C$; hence, by Lemma 2, p_i is the sum of two squares. Therefore, making use of the identity,

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2,$$

we can deduce that n is the sum of two integer squares.

Now suppose $n = mq^2$ with square-free m. Then $A^2 + B^2 = m(qC)^2$. As m is square-free, we can assume by what we have just proved that m is the sum of two squares. Hence so is n. □

Products of sums of squares

We have already seen that

$$(a^2+b^2)(c^2+d^2) \;=\; (ac-bd)^2+(ad+bc)^2 \;=\; (ac+bd)^2+(ad-bc)^2$$

and that the linear transformation

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} n_1 & -n_2 & -n_3 & -n_4 \\ n_2 & n_1 & -n_4 & n_3 \\ n_3 & n_4 & n_1 & -n_2 \\ n_4 & -n_3 & n_2 & n_1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$$

gives

$$(n_1^2+n_2^2+n_3^2+n_4^2)(x_1^2+x_2^2+x_3^2+x_4^2) \;=\; y_1^2+y_2^2+y_3^2+y_4^2.$$

Also, from

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \end{bmatrix} = \begin{bmatrix} n_1 & -n_2 & -n_3 & -n_4 & -n_5 & -n_6 & -n_7 & -n_8 \\ n_2 & n_1 & -n_4 & n_3 & -n_6 & n_5 & n_8 & -n_7 \\ n_3 & n_4 & n_1 & -n_2 & -n_7 & -n_8 & n_5 & n_6 \\ n_4 & -n_3 & n_2 & n_1 & -n_8 & n_7 & -n_6 & n_5 \\ n_5 & n_6 & n_7 & n_8 & n_1 & -n_2 & -n_3 & -n_4 \\ n_6 & -n_5 & n_8 & -n_7 & n_2 & n_1 & n_4 & -n_3 \\ n_7 & -n_8 & -n_5 & n_6 & n_3 & -n_4 & n_1 & n_2 \\ n_8 & n_7 & -n_6 & -n_5 & n_4 & n_3 & -n_2 & n_1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix}$$

we get

$$\begin{aligned}(n_1^2+n_2^2+n_3^2+n_4^2+n_5^2+n_6^2+n_7^2+n_8^2)&(x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2+x_7^2+x_8^2) \\ &= \; y_1^2+y_2^2+y_3^2+y_4^2+y_5^2+y_6^2+y_7^2+y_8^2,\end{aligned}$$

an identity involving the product of sums of eight squares.

One is tempted to ask if there are identities of the form

$$(n_1^2+n_2^2+\cdots+n_k^2)(x_1^2+x_2^2+\cdots+x_k^2) \;=\; y_1^2+y_2^2+\cdots+y_k^2, \tag{5}$$

where the y_i are bilinear combinations of the x_i and n_i, for k other than 1, 2, 4, 8. The answer is actually no, as was proved by Hurwitz in 1898 (see [2] for example).

For k not a multiple of 4, using the proof of the Bruck–Ryser Theorem one can see why. Suppose a k squares identity like (5) exists for some $k \geq 3$, $k \not\equiv 0 \pmod 4$. Find a prime $n \equiv 3 \pmod 8$ such that $n^2+n+2 = 4a+kb$ for some non-negative integers a and b. So n is not the sum two squares, but is the sum of k squares.[1] Then, ignoring the condition $n \equiv 1$ or $2 \pmod 4$, work through the proof of the Bruck–Ryser Theorem using the k squares identity as well as the four squares identity to reduce equality (1) to equality (2). Continue with the proof and eventually conclude that n must be the sum of two squares, a contradiction.

References

[1] P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge, 1994.

[2] D. Shapiro, Products of Sums of Squares, lecture notes, 1999.

[1] Recall that $n = \square+\square+\square$ unless $n = 4^s(8t+7)$ with non-negative s and t.