Topics in Discrete Mathematics

Latin Squares & Projective Planes

Dr Scott Harper

`scott.harper@bristol.ac.uk`

University of Bristol

2021

Description

In this half of the course we focus on two particular combinatorial structures: orthogonal Latin squares and finite projective planes. These objects are motivated by both practical applications and pure mathematical questions. Beginning with Euler's famous 36 Officers Problem, the main thrust of this part of the course is to ask when these structures exist. We will see surprising connections with topics in algebra, combinatorics, geometry, number theory and statistics. This course naturally continues the ideas introduced in the second-year course Combinatorics.

1 The Thirty-Six Officers Problem

In 1782, Leonhard Euler wrote a paper that began as follows

> "A very curious problem, which has exercised for some time the ingenuity of many people, has inspired me to undertake the following research, which seems to open a new field of analysis, in particular the study of combinations. The question revolves around arranging thirty-six officers to be drawn from six different ranks and also from six different regiments in a square such that in each row and each column there are six officers each of a different rank and different regiment. But after spending much effort to resolve this problem, we must acknowledge that such an arrangement is absolutely impossible, though we cannot give a rigorous proof."

Euler presented this paper to the St Petersburg Academy of Sciences in 1779, and folklore has it that this question, now known as the Thirty-Six Officers Problem, was initially posed to Euler by Catherine the Great, who founded the Academy two years before Euler arrived.

Consider the easier "Nine Officers Problem", where we have three regiments A, B, C each containing one officer of each rank 1, 2, 3. Then the arrangement

A1	B2	C3
B3	C1	A2
C2	A3	B1

has the property that every row and every column contains exactly one officer from each regiment and from each rank. Euler thought that the analogous problem for thirty-six officers was impossible. The first section of this course explores the mathematics that arises from this seemingly innocent problem.

2 Latin squares

We begin with the main definition of the course.

Definition 2.1. For a positive integer n, a *Latin square* of order n is an $n \times n$ array with entries taken from a set of n symbols (usually $\{1, 2, \ldots, n\}$) such that every symbol occurs exactly once in each row and each column.

Example 2.2. Below is a Latin square of order 4. A sudoku is a Latin square of order 9 and a slice of Battenberg cake is a Latin square of order 2.

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

Example 2.3. For any positive integer n, the $n \times n$ array $A = (a_{ij})$ whose rows and columns are indexed by $\{0, 1, \ldots, n-1\}$ that is defined as $a_{ij} = i + j \pmod{n}$ is a Latin square of order n with entries in $\{0, 1, \ldots, n-1\}$. The squares obtained for $n \in \{1, 2, 3, 4, 5\}$ are given below. Note that the Latin square obtained for $n = 4$ is the same as the one in Example 2.2 but with the symbols relabelled.

0

0	1
1	0

0	1	2
1	2	0
2	0	1

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

Example 2.4. The Latin square in Example 2.3 is the *Cayley table* (or *multiplication table*) of the group $\mathbb{Z}/n\mathbb{Z}$, the integers under addition modulo n (otherwise known as the cyclic group of order n). Indeed, the Cayley table of any group is a Latin square (see Problem 1* on Sheet 1). For instance, below we give the Cayley table of the dihedral group of order six (where a is an rotation of order 3 and b is a reflection of order 2). Here, and elsewhere, we use $A \longleftrightarrow B$ to informally mean "A and B are the same Latin square but with the symbols relabelled".

$$\begin{array}{|cccccc|}\hline 1 & a & a^2 & b & ab & a^2b \\ a & a^2 & 1 & ab & a^2b & b \\ a^2 & 1 & a & a^2b & b & ab \\ b & a^2b & ab & 1 & a^2 & a \\ ab & b & a^2b & a & 1 & a^2 \\ a^2b & ab & b & a^2 & a & 1 \\ \hline\end{array} \quad \longleftrightarrow \quad \begin{array}{|cccccc|}\hline 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \\ 3 & 1 & 2 & 6 & 4 & 5 \\ 4 & 6 & 5 & 1 & 3 & 2 \\ 5 & 4 & 6 & 2 & 1 & 3 \\ 6 & 5 & 4 & 3 & 2 & 1 \\ \hline\end{array}$$

3 Orthogonal Latin squares I

The Thirty-Six Officers Problem requires that both the arrangement of ranks and the arrangement of regiments be Latin squares of order six. However, this alone is not enough: we also need the two Latin squares to relate to each other in a way that ensures that each regiment contains exactly one officer of each rank. This additional condition is captured by the following definition.

Definition 3.1. Two $n \times n$ arrays $A = (a_{ij})$ and $B = (b_{ij})$ are *orthogonal* if $(a_{ij}, b_{ij}) \neq (a_{kl}, b_{kl})$ for all distinct pairs $(i,j), (k,l) \in \{1, 2, \ldots, n\}^2$.

Example 3.2. Consider these two Latin squares of order 3:

$$A = \begin{array}{|ccc|}\hline 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ \hline\end{array} \qquad B = \begin{array}{|ccc|}\hline 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \\ \hline\end{array}$$

The squares $A = (a_{ij})$ and $B = (b_{ij})$ are orthogonal since the pairs (a_{ij}, b_{ij}) are all distinct:

$$\begin{array}{|ccc|}\hline (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \\ \hline\end{array}$$

Regarding Example 3.2, by using letters rather than numbers for the entries of A, the pair of orthogonal Latin squares (A, B) is the solution to the Nine Officers Problem from Section 1. In this light, solving the Thirty-Six Officers Problem amounts to finding two orthogonal Latin squares of order six. Euler claimed that this was impossible, but it was not until 1900 that Tarry proved the following theorem.

Theorem 3.3. *There do not exist two orthogonal Latin squares of order* 6.

Proof. Omitted. (This is beyond the scope of this course, but if you are interested, see [Stinson].) □

Question 3.4. For which positive integers n, do there exist two orthogonal Latin squares of order n?

Remark 3.5. *Terminology*. Euler represented a pair of orthogonal Latin squares in one square using letters from the Latin alphabet for the first square and letters from the Greek alphabet from the second. For instance, the pair in Example 3.2 would have been written as

$$\begin{array}{|ccc|}\hline a\alpha & b\beta & c\gamma \\ b\gamma & c\alpha & a\beta \\ c\beta & a\gamma & b\alpha \\ \hline\end{array}$$

He called these *Graeco–Latin square*. The Latin letters alone gives a *Latin square*, hence the name.

Question 3.6. For each positive integer n, what is the maximum size of a set of mutually orthogonal Latin squares of order n?

Here, and throughout, Latin squares $A_1, A_2, \ldots, A_r$ are said to be *mutually orthogonal Latin squares*, or *MOLS* for short, if A_i and A_j are orthogonal for all distinct $i, j \in \{1, \ldots, r\}$.

We begin by giving an upper bound.

Proposition 3.7. *Let $A_1, A_2, \ldots, A_r$ be mutually orthogonal Latin squares of order $n \geqslant 2$. Then $r \leqslant n-1$.*

Proof. For $1 \leqslant k \leqslant r$, write $A_k = (a^k_{ij})$. By relabelling the symbols if necessary, we will assume that $a^k_{11} = 1$ for all $1 \leqslant k \leqslant r$. Define the set

$$X = \{(i,j,k) \in \{2,\ldots,n\} \times \{2,\ldots,n\} \times \{1,\ldots,r\} \mid a^k_{ij} = 1\}.$$

We will prove the result by counting the elements of X in two different ways.

First fix $1 \leqslant k \leqslant r$. Since $a^k_{11} = 1$, we know that 1 appears exactly once in each of the $n-1$ rows of the subgrid obtained from A_k by removing the first row and first column. Therefore,

$$|X| = \sum_{k=1}^{r} |\{(i,j) \in \{2,\ldots,n\} \times \{2,\ldots,n\} \mid a^k_{ij} = 1\}| = r(n-1).$$

Second fix $2 \leqslant i,j \leqslant n$. If $1 \leqslant k,l \leqslant r$ are distinct, then since A_k and A_l are orthogonal, we know that

$$(1,1) = (a^k_{11}, a^l_{11}) \neq (a^k_{ij}, a^l_{ij}),$$

so at most one of a^k_{ij} and a^l_{ij} is equal to 1. Therefore,

$$|X| = \sum_{i=2}^{n} \sum_{j=2}^{n} |\{k \in \{1,\ldots,r\} \mid a^k_{ij} = 1\}| \leqslant (n-1)^2.$$

We conclude that $r(n-1) = |X| \leqslant (n-1)^2$, so $r \leqslant n-1$, as claimed. □

Remark 3.8. *Experimental design*. In the 1920s, R. A. Fischer pioneered the use of Latin squares in designing experiments while at Rothamsted Experimental Station. The general idea is roughly the following. Suppose you want to test n varieties of a crop. Arrange an $n \times n$ array of plots in the field. Since there may be some systematic variation as you move across the field (irrigation, fertility etc), we should place each variety of crop exactly once in each row and each column of the array. That is, arrange the crops in a Latin square. If subsequent experiments are to be carried out on the same piece of land, to avoid systematic effects, we should avoid placing one crop next year in exactly the same n plots as one of the crops this year. Ideally, the crops in the second experiment should be arranged in a Latin square orthogonal to the first. Orthogonal Latin squares, and related combinatorial objects, continue to play an important role in the statistical design of experiments today.

4 Finite fields

Recall from *Algebra 2* or *Linear Algebra 2* that a *field* is, roughly speaking, a type of number system that behaves somewhat like the real numbers. Formally, a field is a set F together with two distinct distinguished elements *zero* 0 and *one* 1 and two operations *addition* $+$ and *multiplication* $\cdot$ such that $(F, +)$ is an abelian group with identity 0, $(F \setminus \{0\}, \cdot)$ is an abelian group with identity 1 and multiplication *distributes* over addition (that is, $x \cdot (y+z) = x \cdot y + x \cdot z$ for all $x, y, z \in F$). The sets of rational, real and complex numbers, with the usual addition and multiplication, are all fields.

This is a course on finite mathematics, so we will work with *finite fields*. Here is the key result.

Theorem 4.1. *If F is a finite field, then $|F|$ is a power of a prime. Conversely, for every prime p and positive integer a, there is a unique field F, up to isomorphism, such that $|F| = p^a$ and we denote this field $\mathbb{F}_{p^a}$.*

Proof. Omitted. (This is proved in *Algebra 2*. See also [Cameron, Appendix 9.9].) □

Example 4.2. The fields of prime order are easy to describe. For a prime p, the finite field $\mathbb{F}_p$ is simply $\mathbb{Z}/p\mathbb{Z}$, that is, the integers under addition and multiplication modulo p.

However, in general, a finite field $\mathbb{F}_{p^a}$ is *not* $\mathbb{Z}/p^a\mathbb{Z}$. In the next example we describe $\mathbb{F}_4$ explicitly.

Example 4.3. The field $\mathbb{F}_4$ is the set $\{0, 1, \alpha, \alpha^2\}$ together with the addition and multiplication given by the following two tables

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

and

$\cdot$	1	α	α^2
1	1	α	α^2
α	α	α^2	1
α^2	α^2	1	α

Alternatively, you can apply the usual field axioms together with the additional rules $x + x = 0$ for all $x \in \mathbb{F}_4$ and $\alpha^2 = \alpha + 1$ (which together imply $\alpha^3 = 1$).

Finite fields play an important role in this course, but you do not need to know more than the content of this section. In particular, the only fields you will need to be able to concretely work with in this course (including on problems sheets and in the final exam) will be the fields of prime order and the field with four elements.

5 Orthogonal Latin squares II

By Proposition 3.7, we cannot find more than $n - 1$ mutually orthogonal Latin squares of order n. Using finite fields, we will now show that we can achieve this bound in a special case.

Proposition 5.1. *Let n be a power of a prime. Then there exist $n - 1$ mutually orthogonal Latin squares of order n.*

Proof. Write $\mathbb{F}_n = \{x_1, x_2, \dots, x_{n-1}, x_n = 0\}$. For each $1 \leqslant k \leqslant n - 1$, define $A_k = (a^k_{ij})$ as follows

$$a^k_{ij} = x_k \cdot x_i + x_j.$$

Let $1 \leqslant k \leqslant n - 1$. We will prove that A_k is a Latin square. We first claim that no symbol appears twice in any row. To prove this, we fix a row index $1 \leqslant i \leqslant n$ and two column indices $1 \leqslant j_1, j_2 \leqslant n$. Observe that if $a^k_{ij_1} = a^k_{ij_2}$, then $x_k \cdot x_i + x_{j_1} = x_k \cdot x_i + x_{j_2}$, which implies that $x_{j_1} = x_{j_2}$ and hence $j_1 = j_2$. This proves the claim. Similarly, to see that no symbol appears twice in any column, note that if $a^k_{i_1 j} = a^k_{i_2 j}$ for some $1 \leqslant i_1, i_2, j \leqslant n$, then $x_k \cdot x_{i_1} + x_j = x_k \cdot x_{i_2} + x_j$, which implies that $x_k \cdot x_{i_1} = x_k \cdot x_{i_2}$ and hence $x_{i_1} = x_{i_2}$ (since $x_k \neq 0$ and therefore has an inverse) and hence $i_1 = i_2$. Therefore, A_k is a Latin square.

Now let $1 \leqslant k, l \leqslant n - 1$ be distinct. We claim that A_k and A_l are orthogonal. Let $(i_1, j_1), (i_2, j_2) \in \{1, \dots, n\}^2$ such that $(a^k_{i_1 j_1}, a^l_{i_1 j_1}) = (a^k_{i_2 j_2}, a^l_{i_2 j_2})$. This implies that

$$x_k \cdot x_{i_1} + x_{j_1} = x_k \cdot x_{i_2} + x_{j_2}$$
$$x_l \cdot x_{i_1} + x_{j_1} = x_l \cdot x_{i_2} + x_{j_2}$$

Subtracting the second equation from the first gives

$$(x_k - x_l)x_{i_1} = (x_k - x_l)x_{i_2},$$

which implies that $x_{i_1} = x_{i_2}$ (since $(x_k - x_l)$ has an inverse as $x_k \neq x_l$) and hence $i_1 = i_2$. Substituting $x_{i_1} = x_{i_2}$ into the first equation yields

$$x_k \cdot x_{i_1} + x_{j_1} = x_k \cdot x_{i_1} + x_{j_2},$$

so $x_{j_1} = x_{j_2}$ and hence $j_1 = j_2$. Therefore, A_k and A_l are orthogonal. □

Example 5.2. We apply Proposition 5.1 with $n = 3$. Here $\mathbb{F}_3 = \{x_1 = 1, x_2 = 2, x_3 = 0\}$. We obtain the following two orthogonal Latin squares of order 3:

$$A_1 = (x_i + x_j) = \begin{array}{|ccc|}\hline 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \\ \hline\end{array} \qquad A_2 = (2x_i + x_j) = \begin{array}{|ccc|}\hline 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \\ \hline\end{array}$$

6 Direct products

It is commonplace across mathematics to devise constructions that provide new examples of mathematical structures from existing examples. We will do this now for Latin squares.

Definition 6.1. Let $A = (a_{ij})$ be an $m \times m$ array and let $B = (b_{ij})$ be an $n \times n$ array. The *direct product* of A and B, written $A \times B$, is the $mn \times mn$ array indexed by $\{1, \dots, m\} \times \{1, \dots, n\}$ where the entry in the $((i, j), (k, l))$ position is (a_{ik}, b_{jl}).

Example 6.2.

$$\begin{array}{|cc|}\hline 1 & 2 \\ 2 & 1 \\ \hline\end{array} \times \begin{array}{|ccc|}\hline 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ \hline\end{array} = \begin{array}{|cccccc|}\hline (1,1) & (1,2) & (1,3) & (2,1) & (2,2) & (2,3) \\ (1,2) & (1,3) & (1,1) & (2,2) & (2,3) & (2,1) \\ (1,3) & (1,1) & (1,2) & (2,3) & (2,1) & (2,2) \\ (2,1) & (2,2) & (2,3) & (1,1) & (1,2) & (1,3) \\ (2,2) & (2,3) & (2,1) & (1,2) & (1,3) & (1,1) \\ (2,3) & (2,1) & (2,2) & (1,3) & (1,1) & (1,2) \\ \hline\end{array} \longleftrightarrow \begin{array}{|cccccc|}\hline 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \\ 3 & 1 & 2 & 6 & 4 & 5 \\ 4 & 5 & 6 & 1 & 2 & 3 \\ 5 & 6 & 4 & 2 & 3 & 1 \\ 6 & 4 & 5 & 3 & 1 & 2 \\ \hline\end{array}$$

Lemma 6.3. *Let A be a Latin square of order m and let B be a Latin square of order n. Then $A \times B$ is a Latin square of order mn.*

Proof. Let $A = (a_{ij})$ have order m and $B = (b_{ij})$ have order n. Let $(i_1, j_1), (i_2, j_2), (k, l) \in \{1, \dots, m\} \times \{1, \dots, n\}$. Suppose that the $((i_1, j_1), (k, l))$ and $((i_2, j_2), (k, l))$ positions of $A \times B$ agree. Then $(a_{i_1 k}, b_{j_1 l}) = (a_{i_2 k}, b_{j_2 l})$. Since A is a Latin square, $a_{i_1 k} = a_{i_2 k}$ implies that $i_1 = i_2$, and since B is a Latin square, $b_{j_1 l} = b_{j_2 l}$ implies that $j_1 = j_2$. Therefore, $(i_1, j_1) = (i_2, j_2)$, so no symbol is repeated in a column. A similar argument shows that no symbol is repeated in a row, so $A \times B$ is a Latin square. The rows and columns of $A \times B$ are indexed by $\{1, \dots, m\} \times \{1, \dots, n\}$, so it is a Latin square of order mn. □

Lemma 6.4. *Let A_1 and A_2 be orthogonal Latin squares of order m and let B_1 and B_2 be orthogonal Latin squares of order n. Then $A_1 \times B_1$ and $A_2 \times B_2$ are orthogonal Latin squares of order mn.*

Proof. By Lemma 6.3, $A_1 \times B_1$ and $A_2 \times B_2$ are Latin squares of mn. We need to prove that they are orthogonal. Write $A_1 = (a^1_{ij})$, $A_2 = (a^2_{ij})$, $B_1 = (b^1_{ij})$, $B_2 = (b^2_{ij})$. Let $((i_i, j_1), (k_1, l_1)), ((i_2, j_2), (k_2, l_2)) \in (\{1, \dots, m\} \times \{1, \dots, n\})^2$ such that

$$((a^1_{i_1 k_1}, b^1_{j_1 l_1}), (a^2_{i_1 k_1}, b^2_{j_1 l_1})) = ((a^1_{i_2 k_2}, b^1_{j_2 l_2}), (a^2_{i_2 k_2}, b^2_{j_2 l_2})).$$

Since A_1 and A_2 are orthogonal, $(a^1_{i_1k_1}, a^2_{i_1k_1}) = (a^1_{i_2k_2}, a^2_{i_2k_2})$ implies that $i_1 = i_2$ and $k_1 = k_2$. Similarly, since B_1 and B_2 are orthogonal, $(b^1_{j_1l_1}, b^2_{j_1l_1}) = (b^1_{j_2l_2}, b^2_{j_2l_2})$ implies that $j_1 = j_2$ and $l_1 = l_2$. Therefore, $((i_1, j_1), (k_1, l_1)) = ((i_2, j_2), (k_2, l_2))$. We conclude that $A_1 \times B_1$ and $A_2 \times B_2$ are orthogonal. □

7 Orthogonal Latin squares III

We will now use the direct product construction to obtain sets of mutually orthogonal Latin squares.

Proposition 7.1. *Let $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ for positive integers $a_1, a_2, \ldots, a_s$ and distinct primes $p_1, p_2, \ldots, p_s$. Let m be the minimum of $p_1^{a_1}$, $p_2^{a_2}$, ..., $p_s^{a_s}$. Then there exist $m - 1$ mutually orthogonal Latin squares of order n.*

Proof. By Proposition 5.1, for each $1 \leqslant i \leqslant s$, there exists a set $\{A_{i1}, \ldots, A_{i(m-1)}\}$ of $m-1$ mutually orthogonal Latin squares of order $p_i^{a_i}$. For each $1 \leqslant j \leqslant m-1$, write $B_j = A_{1j} \times A_{2j} \times \cdots \times A_{sj}$, which, by Lemma 6.3 is a Latin square of order $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$. By Lemma 6.4, $\{B_1, B_2, \ldots, B_{m-1}\}$ is a set of $m-1$ mutually orthogonal Latin squares of order n. □

Corollary 7.2. *Let $n \not\equiv 2 \pmod 4$. Then there exist two orthogonal Latin squares of order n.*

Proof. Write $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ for positive integers $a_1, a_2, \ldots, a_s$ and distinct primes $p_1, p_2, \ldots, p_s$ and let m be the minimum of $p_1^{a_1}$, $p_2^{a_2}$, ..., $p_s^{a_s}$. Let $1 \leqslant i \leqslant s$. If p_i is odd, then $p_i^{a_i} \geqslant p_i \geqslant 3$. If $p_i = 2$, then since $n \not\equiv 2 \pmod 4$, we must have $a_i \geqslant 2$, so $p_i^{a_i} \geqslant 4$. Therefore, $m \geqslant 3$, so Proposition 7.1 implies that there exists a set of $m - 1 \geqslant 2$ mutually orthogonal Latin squares of order n, as required. □

Euler knew that there exist two orthogonal Latin squares of order n whenever $n \not\equiv 2 \pmod 4$ but he conjectured that it was impossible when $n \equiv 2 \pmod 4$. As we saw earlier, he was right that it is impossible when $n \in \{2, 6\}$. However, almost two centuries later, Euler was proved wrong! On 26 April 1959, Bose, Parker and Shrikhande appeared on the front page of the New York Times with the headline "Major Mathematical Conjecture Propounded 177 Years Ago Is Disproved". They had proved the following theorem.

Theorem 7.3. *There exist two orthogonal Latin squares of order n if and only if $n \notin \{2, 6\}$.*

Proof. Omitted. (The existence of two orthogonal Latin squares of order $n \geqslant 10$ when $n \equiv 2 \pmod 4$ is given in [van Lint & Wilson, pages 290–294], but the construction is quite technical.) □

Example 7.4. Here is an "Euler spoiler", two orthogonal Latin squares of order 10 (we use letters for the first square and numbers for the second). See also the front cover of [Wilson & Watkins].

A1	B2	C3	D4	E5	F6	G7	H8	I9	J0
B3	C0	A4	E9	I6	D7	J2	F1	G8	H5
C5	J4	E8	G6	A7	H3	B0	I2	D1	F9
H4	E1	D6	J7	F0	B5	C9	G3	A2	I8
E2	A6	H7	I5	B9	C8	F4	D0	J3	G1
J6	F7	G9	B8	C1	I4	E3	A5	H0	D2
I7	D8	B1	C2	G4	E0	H6	J9	F5	A3
F8	H9	J5	A0	D3	G2	I1	B4	C6	E7
D9	G5	I0	F3	H2	J1	A8	E6	B7	C4
G0	I3	F2	H1	J8	A9	D5	C7	E4	B6

8 Transversals of Latin squares

Let n be a positive integer and assume that $n \notin \{2,6\}$. Then there exist two orthogonal Latin squares of order n, but that is not to say that *every* Latin square of order n has an orthogonal mate.

Definition 8.1. An *orthogonal mate* of a Latin square A is any Latin square that is orthogonal to A.

Indeed we have the following general theorem.

Theorem 8.2. *For all integers $n \geqslant 4$, there exists a Latin square of order n that is not orthogonal to any other Latin square.*

Euler knew that Theorem 8.2 was true for even n and the case $n \equiv 1 \pmod 4$ was proved in 1944, but the case $n \equiv 3 \pmod 4$ remained open until 2005! The aim of this section is to prove Theorem 8.2. We will do so by introducing the concept that was actually Euler's main focus: transversals.

Definition 8.3. Let A be a Latin square of order n. A *transversal* of A is a set of n entries such that no two entries share a column, row or symbol.

Example 8.4. The set $\{(1,1),(2,2),(3,3)\}$ is a transversal of A but not a transversal of B.

$$A = \begin{array}{|ccc|} \hline \boldsymbol{1} & 2 & 3 \\ 2 & \boldsymbol{3} & 1 \\ 3 & 1 & \boldsymbol{2} \\ \hline \end{array} \qquad B = \begin{array}{|ccc|} \hline \boldsymbol{1} & 2 & 3 \\ 3 & \boldsymbol{1} & 2 \\ 2 & 3 & \boldsymbol{1} \\ \hline \end{array}$$

The next lemma highlights the significance of transversals.

Lemma 8.5. *Let A be a Latin square. Then there exists a Latin square that is orthogonal to A if and only if A is the union of disjoint transversals.*

Proof. Let $A = (a_{ij})$ be a Latin square of order n. First, assume that $B = (b_{ij})$ is orthogonal to A. We claim that A is the union of disjoint transversals. For $1 \leqslant k \leqslant n$, let $T_k = \{(i,j) \in \{1,\dots,n\}^2 \mid b_{ij} = k\}$. Clearly, $\{1,2,\dots,n\}^2 = \bigcup_{k=1}^{n} T_k$ is a disjoint union. Fix $1 \leqslant k \leqslant n$. We claim that T_k is a transversal. We first observe that no row is repeated in T_k, since if $(i,j_1),(i,j_2) \in T_k$, then $b_{ij_1} = k = b_{ij_2}$, but B is a Latin square, so $j_1 = j_2$. Similarly, no column is repeated, since if $(i_1,j),(i_2,j) \in T_k$, then $b_{i_1 j} = k = b_{i_2 j}$, so $i_1 = i_2$. Finally, no symbol is repeated since if $(i_1,j_1),(i_2,j_2) \in T_k$ with $a_{i_1,j_1} = a_{i_2,j_2}$, then

$$(a_{i_1 j_1}, b_{i_1 j_1}) = (a_{i_1 j_1}, k) = (a_{i_2 j_2}, k) = (a_{i_2 j_2}, b_{i_2 j_2}),$$

but A and B are orthogonal, so $(i_1,j_1) = (i_2,j_2)$. This proves that T_k is a transversal of A.

Conversely, assume that A is the union of disjoint transversals, $T_1, T_2, \dots, T_n$. Define the $n \times n$ array $B = (b_{ij})$ as $b_{ij} = k$ if and only if $(i,j) \in T_k$. An argument very similar to that of the first half of the proof shows that B is orthogonal to A (see Problem 5 on Sheet 2). □

The key lemma for proving Theorem 8.2 is the following.

Lemma 8.6. *Let $A = (a_{ij})$ be a Latin square of order n with entries in $\{0,1,\dots,n-1\}$. Let T be a transversal of A. Then*

$$\sum_{(i,j)\in T} (i + j - a_{ij}) \pmod n = \begin{cases} 0 & \text{if } n \text{ is odd} \\ \frac{n}{2} & \text{if } n \text{ is even.} \end{cases}$$

Proof. Since T is a transversal of A, every element of $\{0,1,\ldots,n-1\}$ appears in each coordinate of exactly one element of $\{(i,j,a_{ij}) \mid (i,j) \in T\}$. Therefore,

$$\begin{aligned}\sum_{(i,j)\in T} (i+j-a_{ij}) \pmod{n} &= \left(\sum_{(i,j)\in T} i + \sum_{(i,j)\in T} j - \sum_{(i,j)\in T} a_{ij}\right) \pmod{n} \\ &= \left(\frac{n(n-1)}{2} + \frac{n(n-1)}{2} - \frac{n(n-1)}{2}\right) \pmod{n} \\ &= \begin{cases} 0 & \text{if } n \text{ is odd} \\ \frac{n}{2} & \text{if } n \text{ is even.} \end{cases} \pmod{n} \qquad \square\end{aligned}$$

Proof of Theorem 8.2. First assume that n is even. Let $A = (a_{ij})$ be the Latin square of order n whose rows and columns are indexed by $\{0,1,\ldots,n-1\}$ that is defined as $a_{ij} = i+j \pmod{n}$. Suppose there exists a Latin square B orthogonal to A. Then Lemma 8.5 implies that A has a transversal T. Now

$$\sum_{(i,j)\in T} (i+j-a_{ij}) \pmod{n} = \sum_{(i,j)\in T} 0 \pmod{n} = 0,$$

which contradicts Lemma 8.6. Therefore, A is not orthogonal to any Latin square.

Now assume that n is odd. We make a more delicate choice of order n Latin square $A = (a_{ij})$. Define

$$a_{ij} = \begin{cases} 1 & \text{if } (i,j) \in \{(0,0),(1,n-1)\} \\ 0 & \text{if } (i,j) \in \{(1,0),(2,n-1)\} \\ j+2 & \text{if } i=0 \text{ and } j \in \{1,3,5,\ldots,n-2\} \\ j & \text{if } i=2 \text{ and } j \in \{1,3,5,\ldots,n-2\} \\ i+j & \text{otherwise.} \end{cases}$$

It is easy to check that A is indeed a Latin square. Suppose there exists a Latin square B orthogonal to A. Then Lemma 8.5 implies that there is a transversal T of A containing $(1,0)$. Let $(i,j) \in T \setminus \{(1,0)\}$. We claim that

$$i+j-a_{ij} = \begin{cases} -2 & \text{if } i=0 \text{ and } j \in \{1,3,5,\ldots,n-2\} \\ 2 & \text{if } i=2 \text{ and } j \in \{1,3,5,\ldots,n-2\} \\ 0 & \text{otherwise.} \end{cases}$$

Certainly, if $j \in \{1,3,5,\ldots,n-2\}$, then $i+j-a_{ij} = 0+j-(j+2) = -2$ if $i=0$ and $i+j-a_{ij} = 2+j-j = 2$ if $i=2$. Otherwise, since $(i,j) \in T$, we know that $i \neq 1$ and $j \neq 0$, and in addition, $a_{ij} \neq 0$ since $a_{10} = 0$, so $a_{ij} = i+j$, which implies that $i+j-a_{ij} = 0$. Therefore, $(i+j-a_{ij}) \pmod{n}$ is 0 for every $(i,j) \in T \setminus \{(1,0)\}$ except for at most one choice of (i,j) where it is 2 and at most one choice of (i,j) where it is -2. Therefore,

$$0 = \sum_{(i,j)\in T} (i+j-a_{ij}) \pmod{n} = (1+0-a_{10}) + \sum_{(i,j)\in T\setminus\{(1,0)\}} (i+j-a_{ij}) \pmod{n} = 1+x \pmod{n},$$

where $x \in \{-2,0,2\}$, which is a contradiction, noting that $n \geqslant 4$. Therefore, there is no Latin square orthogonal to A. This completes the proof. $\square$

Remark 8.7. *The Hall–Paige Conjecture.* The Cayley tables of which finite groups have an orthogonal mate? Problem 4 on Sheet 2 establishes that if G is a cyclic group of order n, then the Cayley table of G does not have an orthogonal mate if and only if n is even. Let G be any finite group. In 1955, Hall and Paige proved that if the Cayley table of G does not have an orthogonal mate, then the Sylow 2-subgroup of G is trivial or noncyclic, and the converse became known as the Hall–Paige Conjecture. This was not proved until 2019 and the proof uses the Classification of Finite Simple Groups.

9 Projective planes

We now turn to a seemingly entirely different sort of mathematical object, one that captures our familiar ideas of perspective (that is, when three-dimensional geometry is presented on a two-dimensional canvas with the consequence that "parallel lines meet").

Definition 9.1. A *projective plane* is a set $\mathcal{P}$ of *points* and a set $\mathcal{L}$ of subsets of $\mathcal{P}$ called *lines* such that

(1) for any two distinct points $p, p' \in \mathcal{P}$ there is a unique line $l \in \mathcal{L}$ containing both p and p'

(2) for any two distinct lines $l, l' \in \mathcal{L}$ there is a unique point $p \in \mathcal{P}$ contained in both l and l'

(3) there exist four points in $\mathcal{P}$, no three of which are contained in a common line of $\mathcal{L}$.

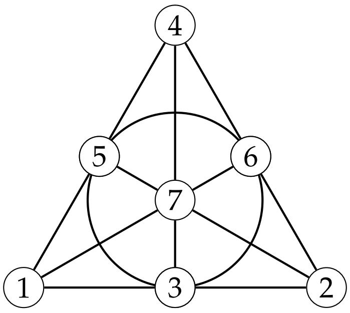
Let us comment on the axioms in Definition 9.1. Axiom (1) is the familiar geometric fact that two points define a unique line. Axiom (2) is where the idea of perspective (and the word "projective") appear: any two lines intersect (in a unique point). Axiom (3) is a *nondegeneracy* condition that is included simply to avoid degenerate examples. These axioms are investigated in Problem 2 on Sheet 2.

The motivating example of projective planes is the *real projective plane* discussed in Example 10.1. However, in this course, we will be mainly concerned with finite objects. Indeed, we say that a projective plane $(\mathcal{P}, \mathcal{L})$ is a *finite projective plane* if $\mathcal{P}$ (and hence $\mathcal{L}$) is finite.

Example 9.2. Let $\mathcal{P} = \{1, 2, 3, 4, 5, 6, 7\}$ and

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

Then $(\mathcal{P}, \mathcal{L})$ is a projective plane, known as *the Fano plane*.



The following result gives important combinatorial information about finite projective planes.

Proposition 9.3. *Let $(\mathcal{P}, \mathcal{L})$ be a finite projective plane. Then there exists a positive integer n such that*

(i) $|\mathcal{P}| = n^2 + n + 1$

(ii) $|\mathcal{L}| = n^2 + n + 1$

(iii) *every point lies is on exactly $n + 1$ lines*

(iv) *every line contains exactly $n + 1$ points.*

Proposition 9.3 motivates the following definition.

Definition 9.4. The *order* of a finite projective plane $(\mathcal{P}, \mathcal{L})$ is the positive integer n such that

$$|\mathcal{P}| = |\mathcal{L}| = n^2 + n + 1.$$

We begin with two lemmas.

Lemma 9.5. *Let $(\mathcal{P}, \mathcal{L})$ be a finite projective plane. Let $p \in \mathcal{P}$ and $l \in \mathcal{L}$ such that $p \notin l$. The number of lines containing p equals the number of points contained in l.*

Proof. Write $l = \{p_1, p_2, \ldots, p_m\}$. Since $p \notin l$, for each $1 \leqslant i \leqslant m$, Axiom (1) implies that there is a unique line l_i that contains p and p_i. Let $1 \leqslant i, j \leqslant m$ and suppose that $l_i = l_j$. Note that $l_i \neq l$ since $p \in l_i$ but $p \notin l$. Therefore, Axiom (2) implies that $|l \cap l_i| = 1$, but $p_i, p_j \in l \cap l_i$, so $p_i = p_j$ and hence $i = j$. Therefore, we deduce that $l_1, l_2, \ldots, l_m$ are distinct. Now let l' be any line containing p. By Axiom (2), $|l \cap l'| = 1$, so fix $1 \leqslant i \leqslant m$ such that $l \cap l' = \{p_i\}$. Now p and p_i are contained on l_i and l', so Axiom (1) forces $l' = l_i$. Therefore, $l_1, l_2, \ldots, l_m$ are the distinct lines through p. □

Lemma 9.6. *Let $(\mathcal{P}, \mathcal{L})$ be a finite projective plane. Then all lines in $\mathcal{L}$ contain the same number of points.*

Proof. Seeking a contradiction, suppose that $l, l' \in \mathcal{L}$ contain different numbers of points. If there exists $p \in \mathcal{P}$ such that $p \notin l$ and $p \notin l'$, then Lemma 9.5 implies that $|l|$ and $|l'|$ both equal the number of lines through p, which is a contradiction, so every point in $\mathcal{P}$ is contained in l or l'. In particular, by Axiom (2), every line in $\mathcal{L}$ other than l and l' has two points (one on l and one on l'). Write $l \cap l' = \{q\}$. If $|l| \geqslant 3$ and $|l'| \geqslant 3$, then we can fix distinct $p_1, p_2 \in l \setminus \{q\}$ and $p'_1, p'_2 \in l' \setminus \{q\}$, but then $\{p_1, p'_1\}$, the unique line containing p_1 and p'_1, is disjoint from $\{p_2, p'_2\}$, the unique line containing p_2 and p'_2, which contradicts Axiom (2). Therefore, without loss of generality, either $|l| = |\mathcal{P}|$ and $|l'| = 1$, or $|l| = |\mathcal{P}| - 1$ and $|l'| = 2$. In particular, given any four points of $\mathcal{P}$, at least three are contained in l, which contradicts Axiom (3). Therefore, any two lines contain the same number of points. □

Proof of Proposition 9.3. By Lemma 9.6, we can fix a positive integer n such that $|l| = n + 1$ for all $l \in \mathcal{L}$. Let $p \in \mathcal{P}$. There exists $l \in \mathcal{L}$ such that $p \notin l$ (see Problem 9 on Sheet 2), so by Lemma 9.5, the number of lines through p equals $|l| = n + 1$. This proves (iii) and (iv).

Now consider (i) and (ii). Define the set

$$X = \{(p, l) \in \mathcal{P} \times \mathcal{L} \mid p \in l\}.$$

We will count the number of elements of X in two different ways. Since each point in $\mathcal{P}$ lies on exactly $n + 1$ lines, we have $|X| = |\mathcal{P}|(n + 1)$. Since each line in $\mathcal{L}$ contains exactly $n + 1$ points, we have $|X| = |\mathcal{L}|(n + 1)$. Therefore,

$$|\mathcal{L}| = |\mathcal{P}|.$$

Next define the set

$$Y = \{(p, q, l) \in \mathcal{P} \times \mathcal{P} \times \mathcal{L} \mid p, q \in l \text{ and } p \neq q\}.$$

We now count the elements of Y in two different ways. For any line $l \in \mathcal{L}$, there are exactly $n(n + 1)$ pairs of distinct points on l, so $|Y| = |\mathcal{L}|n(n + 1)$. For any pair of distinct points $(p, q) \in \mathcal{P}$, by Axiom (1), there is a unique line $l \in \mathcal{L}$ such that $p, q \in l$, so $|Y| = |\mathcal{P}|(|\mathcal{P}| - 1)$. Therefore,

$$|\mathcal{L}| = \frac{|\mathcal{P}|(|\mathcal{P}| - 1)}{n(n + 1)}$$

Equating these two expressions for $|\mathcal{L}|$ gives

$$|\mathcal{P}| = \frac{|\mathcal{P}|(|\mathcal{P}| - 1)}{n(n + 1)},$$

so $n(n + 1) = |\mathcal{P}| - 1$ and hence $|\mathcal{P}| = n^2 + n + 1$ and $|\mathcal{L}| = |\mathcal{P}| = n^2 + n + 1$, as required. □

Example 9.7. The Fano plane from Example 9.2 has order 2 since it has $7 = 2^2 + 2 + 1$ points. Moreover, in agreement with Proposition 9.3, for this plane, each point is contained on $3 = 2 + 1$ lines and each line contains $3 = 2 + 1$ points.

The numerical properties in Proposition 9.3 actually fully characterise finite projective planes.

Proposition 9.8. *Let $\mathcal{P}$ be a finite set and let $\mathcal{L}$ be a set of subsets of $\mathcal{P}$. Let $n \geqslant 2$. Then $(\mathcal{P}, \mathcal{L})$ is a finite projective plane of order n if and only if*

(I) $|\mathcal{P}| = n^2 + n + 1$

(II) $|l| = n + 1$ *for all $l \in \mathcal{L}$*

(III) *for any distinct $p, p' \in \mathcal{P}$ there exists a unique $l \in \mathcal{L}$ such that $p, p' \in l$.*

Proof. One direction is given by Proposition 9.3 and the other is proved in Problem 10 on Sheet 2. □

10 Projective planes and finite fields

Let us present the motivating example of a projective plane.

Example 10.1. Let us introduce the *real projective plane* $\mathrm{P}_2(\mathbb{R})$ (commonly denoted $\mathbb{RP}^2$), which, roughly speaking, is the standard Euclidean plane together with a "line at infinity" that allows parallel lines to meet. More formally, write $l_\infty = \{p_a \mid a \in \mathbb{R} \cup \{\infty\}\}$, and define the set of points $\mathcal{P} = \mathbb{R}^2 \cup l_\infty$ and the set of lines $\mathcal{L} = \{l_\infty\} \cup \bigcup_{a \in \mathbb{R} \cup \{\infty\}} \mathcal{L}_a$, where

$$\mathcal{L}_a = \begin{cases} \{\{(x, ax+b) \mid x \in \mathbb{R}\} \cup \{p_a\}\} \mid b \in \mathbb{R}\} & \text{if } a \in \mathbb{R} \\ \{\{(c, y) \mid y \in \mathbb{R}\} \cup \{p_\infty\}\} \mid c \in \mathbb{R}\} & \text{if } a = \infty. \end{cases}$$

Then $\mathrm{P}_2(\mathbb{R}) = (\mathcal{P}, \mathcal{L})$ is a projective plane.

It is easy to see that if we replaced $\mathbb{R}$ by $\mathbb{Q}$ or $\mathbb{C}$ in Example 10.1, then we would still obtain a projective plane. Indeed, we have the following general result.

Definition 10.2. Let F be a field. Fix a symbol ∞ not in F and a set of symbols $l_\infty = \{p_a \mid a \in F \cup \{\infty\}\}$. The *projective plane over F* is $\mathrm{P}_2(F) = (\mathcal{P}, \mathcal{L})$ where $\mathcal{P} = F^2 \cup l_\infty$ and $\mathcal{L} = \{l_\infty\} \cup \bigcup_{a \in F \cup \{\infty\}} \mathcal{L}_a$, where

$$\mathcal{L}_a = \begin{cases} \{\{(x, ax+b) \mid x \in F\} \cup \{p_a\}\} \mid b \in F\} & \text{if } a \in F \\ \{\{(c, y) \mid y \in F\} \cup \{p_\infty\}\} \mid c \in F\} & \text{if } a = \infty. \end{cases}$$

Proposition 10.3. *Let F be a field. The projective plane $\mathrm{P}_2(F)$ over F is a projective plane.*

Proof. We need to verify the three axioms in Definition 9.1.

Axiom (1) Let $p, p' \in \mathcal{P}$ be distinct. First assume that $p, p' \in l_\infty$. Then l_∞ is the unique line containing p and p' since no other lines in $\mathcal{L}$ contain more than one point in l_∞. Next assume that $p \in l_\infty$ and $p' \notin l_\infty$. Write $p = p_a$ for some $a \in F \cup \{\infty\}$ and $p' = (u, v)$ for $u, v \in F$. If $a = \infty$, then $\{(u, y) \mid y \in F\} \cup \{p_\infty\}\}$ is the unique line in $\mathcal{L}$ containing p and p'. If $a \in F$, then there exists a unique $b \in F$ such that $v = au + b$ and $\{(x, ax+b) \mid x \in F\} \cup \{p_a\}$ is the unique line in $\mathcal{L}$ containing p and p'. Finally assume that $p, p' \notin l_\infty$ and write $p = (u, v)$ and $p' = (u', v')$. If $u = u'$, then $\{(u, y) \mid y \in F\} \cup \{p_\infty\}\}$ is the unique line in $\mathcal{L}$ containing p and p'. If $u \neq u'$, then for $a = (v - v')/(u - u')$, since $v - au = v' - au'$ there exists a unique $b \in F$ such that $v = au + b$ and $v' = au' + b$, so $\{(x, ax+b) \mid x \in F\} \cup \{p_a\}$ is the unique line in $\mathcal{L}$ that contains both p and p'.

Axiom (2) Let $l, l' \in \mathcal{L}$ be distinct. If $l' = l_\infty$, then $l \cap l_\infty = \{p_a\}$ for some $a \in F \cup \{\infty\}$. It now remains to assume that neither l nor l' is l_∞. Fix $a, a' \in F \cup \{\infty\}$ such that $p_a \in l$ and $p_{a'} \in l'$. First assume that $a = a' = \infty$. Then $l = \{(c, y) \mid y \in F\} \cup \{p_\infty\}$ and $l' = \{(c', y) \mid y \in F\} \cup \{p_\infty\}$, so $l \cap l' = \{p_\infty\}$. Next assume that $a \neq a' = \infty$. Then $l = \{(x, ax + b) \mid x \in F\} \cup \{p_a\}$ and $l' = \{(c, y) \mid y \in F\} \cup \{p_\infty\}$, so $l \cap l' = \{(c, ac + b)\}$. Now assume that $a = a' \neq \infty$. Then $l = \{(x, ax + b) \mid x \in F\} \cup \{p_a\}$ and $l' = \{(x, ax + b') \mid x \in F\} \cup \{p_a\}$ with $b \neq b'$, so $l \cap l' = \{p_a\}$ since $ax + b \neq ax + b'$ for all x. Finally assume that $a, a' \neq \infty$ are distinct. Then $l = \{(x, a'x + b) \mid x \in F\} \cup \{p_a\}$ and $l' = \{(x, a'x + b) \mid x \in F\} \cup \{p_{a'}\}$, so $l \cap l' = \{(x, ax + b)\}$ where $x = (b' - b)/(a - a')$.

Axiom (3) It is easy to check that no three of $(0,0), (0,1), (1,0), (1,1)$ are collinear. □

Corollary 10.4. *Let n be a power of a prime. Then there exists a finite projective plane of order n.*

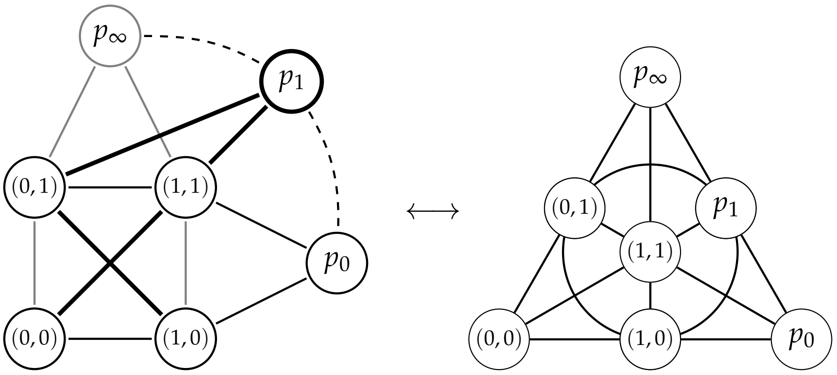
Proof. By Proposition 10.3, $\mathrm{P}_2(\mathbb{F}_n)$ is a finite projective plane of order n. □

Example 10.5. We construct $\mathrm{P}_2(\mathbb{F}_2) = (\mathcal{P}, \mathcal{L})$. Here $\mathcal{P} = \{(0,0), (0,1), (1,0), (1,1), p_0, p_1, p_\infty\}$ and

$$\begin{aligned}
\mathcal{L}_0 &: \{(x,0) \mid x \in \mathbb{F}_2\} \cup \{p_0\} = \{(0,0), (1,0), p_0\}, & \{(x,1) \mid x \in \mathbb{F}_2\} \cup \{p_0\} &= \{(0,1), (1,1), p_0\},\\
\mathcal{L}_1 &: \{(x,x) \mid x \in \mathbb{F}_2\} \cup \{p_1\} = \{(0,0), (1,1), p_1\}, & \{(x,x+1) \mid x \in \mathbb{F}_2\} \cup \{p_1\} &= \{(0,1), (1,0), p_1\},\\
\mathcal{L}_\infty &: \{(0,y) \mid y \in \mathbb{F}_2\} \cup \{p_\infty\} = \{(0,0), (0,1), p_\infty\}, & \{(1,y) \mid y \in \mathbb{F}_2\} \cup \{p_\infty\} &= \{(1,0), (1,1), p_\infty\},
\end{aligned}$$

$$l_\infty = \{p_0, p_1, p_\infty\}.$$

This is the Fano plane from Example 9.2.



11 Projective planes and Latin squares

As with sets of $n-1$ mutually orthogonal Latin squares of order n, we have seen that finite projective planes of order n exist when n is a power of a prime, but we have no examples otherwise. This is not a coincidence.

Theorem 11.1. *Let $n \geqslant 2$. Then there exists a finite projective plane of order n if and only if there exist $n-1$ mutually orthogonal Latin squares of order n.*

Proof. **This proof is nonexaminable.**

Write $I = \{1, 2, \ldots, n\}$.

Step 1: $n-1$ MOLS of order $n \implies$ projective plane of order n

Let $A_1, A_2, \ldots, A_{n-1}$ be mutually orthogonal Latin squares of order n, and for each $1 \leqslant k \leqslant n-1$, write $A_k = (a^k_{ij})$. Fix a set of symbols $l_\infty = \{p_0, p_1, \ldots, p_n\}$. Let $\mathcal{P} = I^2 \cup l_\infty$ and $\mathcal{L} = \{l_\infty\} \cup \bigcup_{k=0}^{n} \mathcal{L}_k$, where

$$\mathcal{L}_k = \begin{cases} \{\{(x,j) \mid x \in I\} \cup \{p_0\}\} \mid j \in I\} & \text{if } k = 0 \\ \{\{(i,j) \mid a^k_{ij} = m\} \cup \{p_k\}\} \mid m \in I\} & \text{if } 1 \leqslant k \leqslant n-1 \\ \{\{(i,y) \mid y \in I\} \cup \{p_n\}\} \mid i \in I\} & \text{if } k = n. \end{cases}$$

We leave it as an exercise to verify that $(\mathcal{P}, \mathcal{L})$ satisfies Axioms (1) to (3).

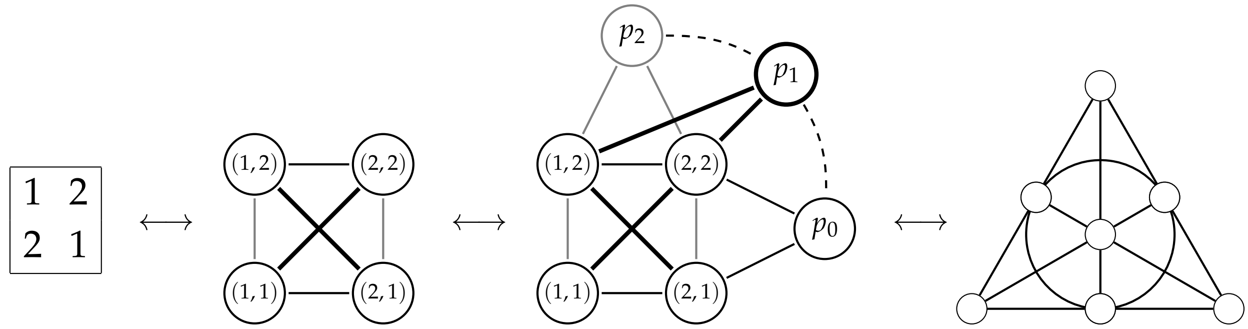
Step 2: projective plane of order $n \implies n-1$ MOLS of order n

Let $(\mathcal{P}, \mathcal{L})$ be a finite projective plane of order n. Fix a line $l_\infty = \{p_0, p_1, \ldots, p_n\} \in \mathcal{L}$. Define $\mathcal{P}' = \mathcal{P} \setminus l_\infty$ and $\mathcal{L}' = \mathcal{L} \setminus \{l_\infty\}$. For each $0 \leqslant k \leqslant n$, define $\mathcal{L}'_k = \{l \setminus \{p_k\} \mid l \in \mathcal{L}' \text{ and } p_k \in l\}$ and write $\mathcal{L}'_k = \{l_{k1}, \ldots, l_{kn}\}$. Define $f \colon I^2 \to \mathcal{P}'$ as $\{f(i,j)\} = l_{0i} \cap l_{nj}$. Axiom (1) ensures that f is a well defined bijection. For each $1 \leqslant k \leqslant n-1$, let $A_k = (a^k_{ij})$ be the $n \times n$ array defined as $a^k_{ij} = m$ if and only if $f(i,j) \in l_{km}$. We claim that $A_1, A_2, \ldots, A_{n-1}$ are mutually orthogonal Latin squares.

Let $1 \leqslant k \leqslant n$. We will prove that A_k is a Latin square. We claim that no symbol appears twice in any row. Fix a $1 \leqslant i, j_1, j_2 \leqslant n$. Observe that if $a^k_{ij_1} = m = a^k_{ij_2}$, then $f(i,j_1), f(i,j_2) \in l_{km}$ but also $f(i,j_1), f(i,j_2) \in l_{0i}$. This implies that $f(i,j_1) = f(i,j_2)$ and hence $j_1 = j_2$. This proves the claim. Similarly, to see that no symbol appears twice in any column, note that if $a^k_{i_1 j} = m = a^k_{i_2 j}$ for some $1 \leqslant i_1, i_2, j \leqslant n$, then $f(i_1,j), f(i_2,j) \in l_{km}$ and $f(i_1,j), f(i_2,j) \in l_{nj}$, which implies that $f(i_1,j) = f(i_2,j)$ and hence $i_1 = i_2$. Hence, A_k is a Latin square.

Now let $1 \leqslant k_1, k_2 \leqslant n$ be distinct. We claim that A_{k_1} and A_{k_2} are orthogonal. For a contradiction, suppose otherwise. Then there exist distinct $(i_1, j_1), (i_2, j_2) \in \{1, \ldots, n\}^2$ such that $(a^{k_1}_{i_1 j_1}, a^{k_2}_{i_1 j_1}) = (a^{k_1}_{i_2 j_2}, a^{k_2}_{i_2 j_2})$. This implies that $a^{k_1}_{i_1 j_1} = m_1 = a^{k_1}_{i_2 j_2}$ and $a^{k_1}_{i_2 j_2} = m_2 = a^{k_2}_{i_2 j_2}$, which in turn implies that $f(i_1, j_1), f(i_2, j_2) \in l_{k_1 m_1}$ and $f(i_1, j_1), f(i_2, j_2) \in l_{k_2 m_2}$, which contradicts Axiom (1). Therefore, A_1, A_2, $\ldots$, A_{n-1} are mutually orthogonal Latin squares of order n. □

Example 11.2. The following indicates the proof of Theorem 11.1 with $n = 2$.



12 The Bruck–Ryser Theorem

A finite projective plane of order n (or equivalently, $n-1$ mutually orthogonal Latin squares of order n) exist if n is a power of a prime. Do they exist for any other values of n? Very little is known. The most significant result is the following.

Theorem 12.1 (Bruck–Ryser Theorem). *Let $n \equiv 1$ or $2 \pmod 4$. If there exists a projective plane of order n, then n is the sum of two squares of integers.*

Consider $n \leqslant 14$. By Corollary 10.4, projective planes of order n exist when $n \in \{2,3,4,5,7,9,11,13\}$, and by the Bruck–Ryser Theorem, they do not exist when $n \in \{6, 14\}$. However, since $10 = 1^2 + 3^2$, the Bruck–Ryser Theorem does not exclude the possibility of a finite projective plane of order 10. In 1989, by way of a huge computation, Lam, Swiercz and Thiel showed that no such plane could exist. It is still unknown whether there exists a finite projective plane of order 12.

The remainder of this section is nonexaminable.

Let us now discuss the proof of the Bruck–Ryser Theorem. Here number theory and linear algebra play important roles. We follow the discussion in [Section 9.8, Cameron], where you can find further details, including proofs of the following three number theoretic lemmas, which we omit here.

Lemma 12.2 (Lagrange's Four Squares Theorem)**.** *Every positive integer is the sum of four integer squares.*

Lemma 12.3 (Four Squares Identity)**.** *Let $a_1, a_2, a_3, a_4, x_1, x_2, x_3, x_4 \in \mathbb{Z}$. Then*

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

where

$$\begin{aligned} y_1 &= a_1x_1 - a_2x_2 - a_3x_3 - a_4x_4 \\ y_2 &= a_1x_2 + a_2x_1 + a_3x_3 - a_4x_3 \\ y_3 &= a_1x_3 + a_3x_1 + a_4x_2 - a_2x_4 \\ y_4 &= a_1x_4 + a_4x_1 + a_2x_3 - a_3x_2. \end{aligned}$$

Lemma 12.4. *Let $n \in \mathbb{Z}$. If there exist $x, y, z \in \mathbb{Z}$ such that $x^2 + y^2 = nz^2$ and $(x, y, z) \neq (0, 0, 0)$, then n is the sum of two integer squares.*

We now prove the Bruck–Ryser Theorem.

Proof of Theorem 12.1. Let $(\mathcal{P}, \mathcal{L})$ be a projective plane of order n. Let $N = n^2 + n + 1$ and note that $N \equiv 3 \pmod 4$. Write $\mathcal{P} = \{p_1, \dots, p_N\}$ and $\mathcal{L} = \{l_1, \dots, l_N\}$.

Let $B = (b_{ij})$ be the $N \times N$ matrix defined as

$$b_{ij} = \begin{cases} 1 & \text{if } p_i \in l_j \\ 0 & \text{otherwise.} \end{cases}$$

The (i, j)th entry of $BB^\top$ is the dot product $b_i.b_j$, which is the number of lines containing p_i and p_j, so

$$(BB^\top)_{ij} = \begin{cases} n+1 & \text{if } i = j \\ 1 & \text{otherwise.} \end{cases}$$

Therefore, if I is the $N \times N$ identity matrix and J is the $N \times N$ all-ones matrix, then $BB^\top = nI + J$.

Let $x_1, \dots, x_{N+1}$ be variables and write $x = (x_1, \dots, x_N)$. Define $z = (z_1, \dots, z_N) = xB$, noting that each z_i is a nonzero integer linear combination of the $x_1, \dots, x_N$. Then

$$zz^\top = (xB).(xB)^\top = xBB^\top x^\top = x(nI + J)x^\top = nxx^\top + xJx^\top. \tag{1}$$

Note that $zz^\top = z_1^2 + \cdots + z_N^2$ and $xx^\top = x_1^2 + \cdots + x_N^2$, and if we define $w = x_1 + \cdots + x_N$, then

$$xJx^\top = (w, \dots, w).(x_1, \dots, x_N) = w^2.$$

Therefore, from (1) we obtain

$$z_1^2 + \cdots + z_N^2 = n(x_1^2 + \cdots + x_N^2) + w^2,$$

which we rewrite as

$$z_1^2 + \cdots + z_N^2 + nx_{N+1}^2 = n(x_1^2 + x_2^2 + x_3^2 + x_4^2) + \cdots + n(x_{N-2}^2 + x_{N-1}^2 + x_N^2 + x_{N+1}^2) + w^2. \tag{2}$$

By Lemma 12.2, there exist $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ such that $n = a_1^2 + a_2^2 + a_3^2 + a_4^2$. By Lemma 12.3, for each $0 \leqslant i < (N+1)/4$, we may write

$$\begin{aligned} n(x_{4i+1}^2 + x_{4i+2}^2 + x_{4i+3}^2 + x_{4i+4}^2) &= (a_1^2 + a_2^2 + a_3^2 + a_4^2)(x_{4i+1}^2 + x_{4i+2}^2 + x_{4i+3}^2 + x_{4i+4}^2) \\ &= y_{4i+1}^2 + y_{4i+2}^2 + y_{4i+3}^2 + y_{4i+4}^2, \end{aligned}$$

where $y_{4i+1}, y_{4i+2}, y_{4i+3}, y_{4i+4}$ are a nonzero integer linear combinations of $x_1, \ldots, x_{N+1}$. Therefore, from (2) we obtain

$$z_1^2 + \cdots + z_N^2 + nx_{N+1}^2 = y_1^2 + \cdots + y_{N+1}^2 + w^2. \tag{3}$$

We are now going to repeatedly take special cases of (3) and in this way eliminate the variables $x_1, \ldots, x_N$ and hence $y_1, \ldots, y_N$ and $z_1, \ldots, z_N$.

We begin by eliminating x_1. The coefficient of x_1 must be nonzero in the expressions for at least one of y_1, y_2, y_3, y_4 and at least one of $z_1, \ldots, z_N$; without loss of generality, assume that the coefficient a_1 is nonzero in the expression

$$y_1 = a_1x_1 - a_2x_2 - a_3x_3 - a_4x_4$$

and the coefficient b_{11} is nonzero in the expression

$$z_1 = b_{11}x_1 + \cdots + b_{N1}x_N.$$

We now divide into two cases: $a_1 \neq b_{11}$ and $a_1 = b_{11}$.

If $a_1 \neq b_{11}$, then we add the constraint that

$$x_1 = (a_1 - b_{11})^{-1}((a_2 + b_{21})x_2 + (a_3 + b_{31})x_3 + (a_4 + b_{41})x_4 + b_{51}x_5 + \cdots + b_{N1}x_{N1}),$$

which implies that $y_1 = z_1$.

If $a_1 = b_{11}$, then we add the constraint that

$$x_1 = (a_1 + b_{11})^{-1}((a_2 - b_{21})x_2 + (a_3 - b_{31})x_3 + (a_4 - b_{41})x_4 - b_{51}x_5 + \cdots - b_{N1}x_{N1}),$$

which implies that $y_1 = -z_1$.

In both cases, $y_1^2 = z_1^2$, and we can also replace the expression $x_1 + \cdots + x_N$ for w by a rational linear combination of $x_2, \ldots, x_N$. Therefore,

$$z_2^2 + \cdots + z_N^2 + nx_{N+1}^2 = y_2^2 + \cdots + y_{N+1}^2 + w^2.$$

We now apply this same procedure a further $N-1$ times. For each $1 \leqslant k \leqslant N$, at the kth stage, we choose x_k as a particular rational linear combination of $x_{k+1}, \ldots, x_{N+1}$ such that $y_k \in \{z_k, -z_k\}$ and we update the expression for w so that it is a rational linear combination of $x_{k+1}, \ldots, x_{N+1}$. In this way, we eventually obtain the equation

$$nx_{N+1}^2 = y_{N+1}^2 + w^2, \tag{4}$$

where $y_{N+1} = \frac{p_1}{q_1}x_{N+1}$ and $w = \frac{p_2}{q_2}x_{N+1}$ for some nonzero $p_1, q_1, p_2, q_2 \in \mathbb{Z}$.

(There is a technicality that has been overlooked in this discussion. Why do we know that x_k will have a nonzero coefficient in one of the (updated) defining rational linear combinations of $x_k, \ldots, x_{N+1}$ for at least one of $y_k, \ldots, y_{N+1}$ and at least one of $z_k, \ldots, z_N$? The answer: this is ensured by the fact that the equation (3) defines a *positive definite* quadratic form. It would be too much of a digression into linear algebra to explain what this means.)

We now choose $x_{N+1} = q_1q_2$, which gives the equation

$$n(q_1q_2)^2 = (p_1q_2)^2 + (p_2q_1)^2.$$

Therefore, Lemma 12.4 implies that n is the sum of two squares. □

13 Desargues' Theorem

This section is nonexaminable.

For any field F, by Proposition 10.3, we can construct the projective plane $\mathrm{P}_2(F)$. In particular, whenever n is a power of a prime, $\mathrm{P}_2(\mathbb{F}_n)$ gives an example of a finite projective plane of order n. At the end of the previous section, we noted that there are no known examples of finite projective planes of any other order. However, there are many other examples of finite projective planes other than $\mathrm{P}_2(\mathbb{F}_n)$.

In this section, we will give the geometric criterion that characterises the projective planes $P_2(F)$, where F is a field, among the more general class of projective planes.

We begin with some terminology.

Definition 13.1. Let $(\mathcal{P}, \mathcal{L})$ be a projective plane.

(i) Points $p_1, p_2, \ldots, p_k \in \mathcal{P}$ are said to be *collinear* if there exists $l \in L$ such that $p_1, p_2, \ldots, p_k \in l$.

(ii) Lines $l_1, l_2, \ldots, l_k \in \mathcal{L}$ are said to be *concurrent* if there exists $p \in \mathcal{P}$ such that $p \in l_1 \cap l_2 \cap \cdots \cap l_k$.

The focus of this section is on *triangles*, which are sets of three points that are not collinear.

Definition 13.2. Let $T_1 = \{a_1, b_1, c_1\}$ and $T_2 = \{a_2, b_2, c_2\}$ be triangles. Let A_i, B_i, C_i be the lines containing $\{b_i, c_i\}$, $\{a_i, c_i\}$, $\{a_i, b_i\}$ respectively.

(i) The triangles T_1 and T_2 are *perspective from a point* if there exists $p \in \mathcal{P}$ such that each of $\{p, a_1, a_2\}$, $\{p, b_1, b_2\}$ and $\{p, c_1, c_2\}$ are sets of collinear points.

(ii) Two triangles T_1 and T_2 are *perspective from a line* if there exists $l \in \mathcal{L}$ such that each of $\{l, A_1, A_2\}$, $\{l, B_1, B_2\}$ and $\{l, C_1, C_2\}$ are sets of concurrent lines.

The following theorem generalises a well known result about $\mathrm{P}_2(\mathbb{R})$, first proved by Desargues.

Theorem 13.3 (Desargues' Theorem). *Let F be a field. In $\mathrm{P}_2(F)$, two triangles are perspective from a point if and only if they are perspective from a line.*

Proof. Omitted. (This is beyond the scope of the course.) □

Desargues' Theorem motivates the next definition.

Definition 13.4. A projective plane is said to *desarguesian* if two triangles are perspective from a point if and only if they are perspective from a line.

Let us make precise what it means for two projective planes to be essentially the same.

Definition 13.5. Projective planes $(\mathcal{P}_1, \mathcal{L}_1)$ and $(\mathcal{P}_2, \mathcal{L}_2)$ are said to be *equivalent* if there exists a bijection $f \colon \mathcal{P}_1 \to \mathcal{P}_2$ such that for $l \subseteq \mathcal{P}_1$ we have that $l \in \mathcal{L}_1$ if and only if $f(l) \in L_2$.

We can now characterise the projective planes that arise from fields.

Theorem 13.6. *A projective plane is desarguesian if and only if it is equivalent to $\mathrm{P}_2(F)$ for a field F.*

Proof. Omitted. (This is beyond the scope of the course.) □

To return to the motivation of this section, let us record that all finite projective planes of order $n < 9$ are desarguesian, but examples of nondesarguesian finite projective planes of order n have been constructed for all $n = p^{2k} \geqslant 9$ where p is prime. The first example, of order 9, was discovered by Veblen and Wedderburn in 1907, and this construction was generalised to all $p^{2k} \geqslant 9$ by Hall in 1943.

14 Cyclic difference sets

Let us now turn to a seemingly number theoretic object. Recall that $\mathbb{Z}/v\mathbb{Z}$ is the set of integers $\{0, 1, \ldots, v-1\}$ under addition and multiplication modulo v.

Definition 14.1. A (v, k, λ) *cyclic difference set* is a subset $S \subseteq \mathbb{Z}/v\mathbb{Z}$ of size k such that computing all differences $x - y$ for distinct $x, y \in S$ gives every nonzero element of $\mathbb{Z}/v\mathbb{Z}$ exactly λ times.

Example 14.2. The nonzero differences between elements of $S = \{1, 2, 4\} \subseteq \mathbb{Z}/7\mathbb{Z}$ are

$$\begin{aligned} 4 - 2 \pmod 7 &= 2, \quad 4 - 1 \pmod 7 = 3, \quad 2 - 1 \pmod 7 = 1, \\ 2 - 4 \pmod 7 &= 5, \quad 1 - 4 \pmod 7 = 4, \quad 1 - 2 \pmod 7 = 6. \end{aligned}$$

Since we obtain each of $1, 2, 3, 4, 5, 6$ exactly once, S is a $(7, 3, 1)$ cyclic difference set.

The three parameters of a cyclic difference set are related in the following way.

Lemma 14.3. *Let $S \subseteq \mathbb{Z}/v\mathbb{Z}$ be a (v, k, λ) cyclic difference set. Then $k(k-1) = \lambda(v-1)$.*

Proof. We count $D = \{(x, y, x - y) \in S^2 \times \mathbb{Z}/v\mathbb{Z} \mid x \neq y\}$ in two different ways. On the one hand, $|D| = k(k-1)$ since there are $k(k-1)$ distinct pairs of elements in S. On the other hand, $|D| = \lambda(v-1)$ since every nonzero element of $\mathbb{Z}/v\mathbb{Z}$ arises as a difference $x - y$ for exactly λ pairs $(x, y) \in S^2$. Therefore, $k(k-1) = \lambda(v-1)$. □

We now ask the usual question: when do (v, k, λ) cyclic difference sets exist? In general, this is a difficult open question. We begin by giving one general family of cyclic difference sets.

Proposition 14.4. *Let $m \geqslant 1$ such that $p = 4m - 1$ is prime. Then $S = \{x^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\} \setminus \{0\}$ is a $(4m-1, 2m-1, m-1)$ cyclic difference set.*

Proof. **This proof is nonexaminable.**

Let $X = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$. Write $-S = \{-s \mid s \in S\}$. We will begin by proving X is the disjoint union $S \cup -S$ where $|S| = |-S| = |X|/2$. To do this, we will use a small amount of group theory from *Introduction to Proofs and Group Theory*.

Recall that X is a group under multiplication modulo p, and note that S is a subgroup of X since $x^2y^2 = (xy)^2 \in S$ and $(x^2)^{-1} = (x^{-1})^2$ for all $x, y \in X$. For all $x, y \in X$, note that $x^2 = y^2$ if and only $y \in \{x, -x\}$ and note that $x \neq -x$ since $2x \neq 0$ as $p > 2$ (we can divide through by x since $x \neq 0$ and $\mathbb{Z}/p\mathbb{Z}$ is a field). Therefore, $|S| = |X|/2$.

Suppose that $-1 \in S$. Then there exists $x \in X$ such that $x^2 = -1$, so $x^4 = 1$, which implies that x has order 4 in the group $X = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ under multiplication modulo p. However, by Lagrange's theorem the order of x must divide the order of $|X| = p - 1 = 4m - 2$, which is a contradiction. Therefore, $-1 \notin S$. This implies that we can write X as a disjoint union of cosets $S \cup -S$, as claimed.

For each $z \in X$, write $D_z = \{(x, y) \in S^2 \mid x - y = z\}$. We will prove that $|D_z| = |D_1|$ for all $z \in X = S \cup -S$. If $z \in S$, then $|D_z| = |D_1|$ since $D_1 \to D_z$ defined as $(x, y) \mapsto (zx, zy)$ is a bijection. If $z \in -S$, then $|D_z| = |D_{-1}|$ since $D_{-1} \to D_z$ defined as $(x, y) \mapsto (-zx, -zy)$ is a bijection. It remains to note that $|D_{-1}| = |D_1|$ since $D_1 \to D_{-1}$ defined as $(x, y) \mapsto (y, x)$ is a bijection.

We have shown that $|\mathbb{Z}/p\mathbb{Z}| = 4m - 1$ and $|S| = |X|/2 = 2m - 1$, and that every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ arises as $x - y$ for the same number, say λ, of pairs $(x, y) \in S^2$. In other words, S is a $(4m-1, 2m-1, \lambda)$ cyclic difference set. By Lemma 14.3, $\lambda(4m-2) = (2m-1)(2m-2)$, so $\lambda = m - 1$. This completes the proof. □

Example 14.5. Let us apply Proposition 14.4 with $m = 2$. Modulo $p = 7$, we have

$$1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9 = 2, \quad 4^2 = 16 = 2, \quad 5^2 = 25 = 4, \quad 6^2 = 36 = 1,$$

so $S = \{1, 2, 4\}$, which is the $(7, 3, 1)$ cyclic difference set from Example 14.2.

We now give two ways of obtaining new cyclic difference sets from an existing one.

Proposition 14.6. *Let $S \subseteq \mathbb{Z}/v\mathbb{Z}$ be a (v, k, λ) cyclic difference set. Then the complement $(\mathbb{Z}/v\mathbb{Z}) \setminus S$ is a $(v, v-k, v-2k+\lambda)$ cyclic difference set.*

Proof. This is proved in Problem 2 on Sheet 3. □

For $S \subseteq \mathbb{Z}/v\mathbb{Z}$ and $a \in \mathbb{Z}/v\mathbb{Z}$, we write $S + a = \{s + a \mid s \in S\}$ for the *translate* of S by a.

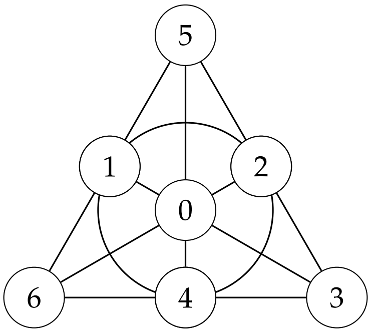
Proposition 14.7. *Let $S \subseteq \mathbb{Z}/v\mathbb{Z}$ be a (v, k, λ) cyclic difference set. Then $S + a$ is a (v, k, λ) cyclic difference set for all $a \in \mathbb{Z}/v\mathbb{Z}$.*

Proof. Let $a \in \mathbb{Z}/v\mathbb{Z}$. For all $x, y \in S$ we have $(x + a) - (y + a) = x - y$. Therefore, the differences $x' - y'$ for all distinct $x', y' \in S + a$ are exactly the differences $x - y$ for all distinct $x, y \in S$, so, in particular, we obtain every nonzero element of $\mathbb{Z}/v\mathbb{Z}$ exactly λ times. □

Example 14.8. Recall from Example 14.2 that $S = \{1, 2, 4\} \subseteq \mathbb{Z}/7\mathbb{Z}$ is a $(7, 3, 1)$ cyclic difference set. Therefore, so are all of the translates

$$S + 0 = \{1, 2, 4\}, \quad S + 1 = \{2, 3, 5\}, \quad S + 2 = \{3, 4, 6\}, \quad S + 3 = \{4, 5, 0\},$$
$$S + 4 = \{5, 6, 1\}, \quad S + 5 = \{6, 0, 2\}, \quad S + 6 = \{0, 1, 3\}.$$

Representing these translates pictorially returns the familiar Fano plane (see Example 9.2).



The following result generalises Example 14.8.

Theorem 14.9. *Let $S \subseteq \mathbb{Z}/v\mathbb{Z}$ be a $(v, k, 1)$ cyclic difference set with $v > 3$.*

(i) *There exists a positive integer n such that $v = n^2 + n + 1$ and $k = n + 1$.*

(ii) *Let $\mathcal{P} = \mathbb{Z}/v\mathbb{Z}$ and $\mathcal{L} = \{S + a \mid a \in \mathbb{Z}/v\mathbb{Z}\}$. Then $(\mathcal{P}, \mathcal{L})$ is a finite projective plane of order n.*

Proof. Let $n = k - 1$. Therefore, $k = n + 1$, and Lemma 14.3 implies that $v - 1 = k(k-1) = (n+1)n$, so $v = n^2 + n + 1$. This proves (i).

We now turn to (ii). We will apply Proposition 9.8. Part (i) tells us that conditions (I) and (II) are satisfied. We now establish condition (III). Let $p_1, p_2 \in \mathcal{P}$ be distinct. We claim that there is a unique element of $\mathcal{L}$ that contains p_1 and p_2. Since S is a $(v, k, 1)$ cyclic difference set, there is a unique pair

$(x, y) \in S^2$ such that $x - y = p_1 - p_2$. Let $a = p_1 - x = p_2 - y$. Then $p_1 = x + a$ and $p_2 = y + a$, so $p_1, p_2 \in S + a$. Now let $b \in \mathbb{Z}/v\mathbb{Z}$ such that $p_1, p_2 \in S + b$. There exist $s, t \in S$ such that $p_1 = s + b$ and $p_2 = t + b$, so $p_1 - p_2 = s - t$, so $(s, t) = (x, y)$ and $b = p_1 - s = p_1 - x = a$. Therefore, $S + a$ is the unique translate of S to contain p_1, p_2. By Proposition 9.8, $(\mathcal{P}, \mathcal{L})$ is a projective plane of order n. □

By Theorem 14.9, if there exists a $(n^2 + n + 1, n + 1, 1)$ cyclic difference set, then there exists a projective plane of order n, but it is not known whether the converse is true. However, there do certainly exist $(n^2 + n + 1, n + 1, 1)$ difference sets whenever n is a prime power. Perhaps unsurprisingly by now, these are constructed from the finite field $\mathbb{F}_n$, but this construction requires particular results about finite fields which are beyond the scope of this course, so we omit this (if you are interested, see [van Lint & Wilson, pages 377–379]).

15 Dobble

This section is nonexaminable.

Dobble is card game with a deck of 55 cards each of which features 8 pictures (of a possible 57). At any time each player has a pile of cards face up in front of them and there is a card face up in the middle, and the players each try to find the one picture that appears on both their card and the card in the middle. Crucially any two cards have exactly one picture in common. However, Dobble is mathematically unsatisfying. For example, some pictures occur on more cards than others: 42 pictures occur 8 times, 14 pictures occur 7 times and the snowman sadly occurs only 6 times.

My recommendation is to add the following two cards to your Dobble set

dog, exclamation mark, eye, hammer, ladybird, lightbulb, skull & crossbones, snowman
cactus, dinosaur, flower, ice cube, leaf, person, question mark, snowman

With this improved version of Dobble, if $\mathcal{P}$ is the set of pictures and $\mathcal{L}$ is the set of cards (which are sets of pictures), then $(\mathcal{P}, \mathcal{L})$ is a projective plane of order 7 (noting that $57 = 7^2 + 7 + 1$ and $8 = 7 + 1$). In particular there are exactly 57 pictures and exactly 57 cards, each card features exactly 8 pictures and each picture is featured on exactly 8 cards, any two cards have a unique picture in common and any two pictures feature together on a unique card.

Further reading

I hope that you have enjoyed this half of the course. If you want to find out more about the topics in this course, then here are some good places to start.

P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, 1994.
– This book is accessible. See Chapters 6 and 9.

J.H van Lint & R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 2001.
– This book is more advanced. See Chapters 17, 19, 22, 23 and 27.

R. Wilson & J. J. Watkins, *Combinatorics: Ancient and Modern*, Oxford University Press, 2013.
– This is a book on the history of combinatorics. See Chapters 10 and 11.

D. R. Stinson, *A Short Proof of the Nonexistence of a Pair of Orthogonal Latin Squares of Order Six*, Journal of Combinatorial Theory, Series A **36**, 373–376 (1984).
– This is a journal article that gives what it says in the title.