NDMI011: Combinatorics and Graph Theory 1

Lecture #5
Finite projective planes (part II)

Irena Penev

1 Reminder from the previous lecture

A *projective plane* is a set system $(X, \mathcal{P})$[1] that satisfies the following three properties:

(P0) there exists a 4-element subset $Q \subseteq X$ such that every $P \in \mathcal{P}$ satisfies $|P \cap Q| \leq 2$;

(P1) all distinct $P_1, P_2 \in \mathcal{P}$ satisfy $|P_1 \cap P_2| = 1$;

(P2) for all distinct $x_1, x_2 \in X$, there exists a unique $P \in \mathcal{P}$ such that $x_1, x_2 \in P$.

Elements of X are called *points*, and elements of $\mathcal{P}$ are called *lines* of the projective plane $(X, \mathcal{P})$.

A projective plane $(X, \mathcal{P})$ is *finite* if X is finite.

In the previous lecture, we proved several results about finite projective planes, which we state below for reference.

Proposition 1.2 from Lecture Notes 4. *Let $(X, \mathcal{P})$ be a finite projective plane. Then all lines in $\mathcal{P}$ have the same number of points.*

The *order* of a finite projective plane $(X, \mathcal{P})$ is the number $|P| - 1$, where P is any line in $\mathcal{P}$.[2] By Proposition 1.2 from Lecture Notes 4, this is well-defined.

Proposition 1.3 from Lecture Notes 4. *The order of any finite projective plane is at least two.*

[1]This means that X is a set and $\mathcal{P} \subseteq \mathscr{P}(X)$, where $\mathscr{P}(X)$ is the power set (i.e. the set of all subsets) of X.

[2]So, if $(X, \mathcal{P})$ is a finite projective plane of order n, then each line in $\mathcal{P}$ contains exactly $n + 1$ points.

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

Figure 2.1: Two 3×3 Latin squares.

$(1, 1)$	$(2, 2)$	$(3, 3)$
$(2, 3)$	$(3, 1)$	$(1, 2)$
$(3, 2)$	$(1, 3)$	$(2, 1)$

Figure 2.2: The matrix obtained by superimposing the left (red) 3×3 Latin square from Figure 2.1 onto the right (blue) one.

Theorem 1.4 from Lecture Notes 4. *Let $(X, \mathcal{P})$ be a finite projective plane of order n. Then all the following hold:*

(a) for each point $x \in X$, exactly $n + 1$ lines in $\mathcal{P}$ pass through x;

(b) $|X| = n^2 + n + 1$;

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

In the previous lecture, we also showed that the "dual" of a finite projective plane is again a projective plane (see Theorem 2.2 from Lecture Notes 4), but we will not need that result in this lecture.

2 Finite projective planes and Latin squares

For a positive integer n, an $n \times n$ *Latin square* is an $n \times n$ array (or matrix) whose entries are numbers $1, \dots, n$, and in which each number $1, \dots, n$ occurs exactly once in each row and in each column. Two 3×3 Latin squares are represented in Figure 2.1. When we write that $[a_{i,j}]_{n \times n}$ is a Latin square, we mean that this Latin square is of size $n \times n$, and that for all $i, j \in \{1, \dots, n\}$, the (i, j)-th entry (i.e. the entry in the i-th row and j-th column) of the Latin square is $a_{i,j}$. Now, two $n \times n$ Latin squares, say $[a_{i,j}]_{n \times n}$ and $[b_{i,j}]_{n \times n}$, are *orthogonal* if each entry of the matrix matrix obtained by superimposing A on B, i.e. of the matrix $[(a_{i,j}, b_{i,j})]_{n \times n}$, is different. Since an $n \times n$ matrix has n^2 entries, and the Cartesian product $\{1, \dots, n\} \times \{1, \dots, n\}$ has exactly

n^2 elements, we see that two $n \times n$ Latin squares are orthogonal if and only if each element of $\{1, \dots, n\} \times \{1, \dots, n\}$ appears exactly once in the matrix obtained by superimposing the two $n \times n$ Latin squares. For instance, the Latin squares from Figure 2.1 are orthogonal, as we can see from Figure 2.2.

For a positive integer n, a Latin square $A = [a_{i,j}]_{n \times n}$ and a permutation π of the set $\{1, \dots, n\}$, we set $\pi(A) = [\pi(a_{i,j})]_{n \times n}$; obviously, $\pi(A)$ is a Latin square. For example, if

$A =$

1	3	2
3	2	1
2	1	3

and if $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, then

$\pi(A) =$

1	2	3
2	3	1
3	1	2

.

Proposition 2.1. *Let $A = [a_{i,j}]_{n \times n}$ and $B = [b_{i,j}]_{n \times n}$ be orthogonal $n \times n$ Latin squares, and let π_A, π_B be permutations of the set $\{1, \dots, n\}$. Then $\pi_A(A)$ and $\pi_B(B)$ are orthogonal Latin squares.*

Proof. Obvious.[3] □

Theorem 2.2. *Let $n \geq 2$ be an integer, and let M be a set of pairwise orthogonal $n \times n$ Latin squares. Then $|M| \leq n - 1$.*

Proof. We may assume that $M \neq \emptyset$, for otherwise, the result is immediate. Set $t = |M|$ and $M = \{A_1, \dots, A_t\}$; we must show that $t \leq n - 1$. First, for each $i \in \{1, \dots, t\}$, we let π_i be the permutation of $\{1, \dots, n\}$ that transforms the first row of A_i into $1, \dots, n$, and let $A'_i = \pi_i(A_i)$. By Proposition 2.1, Latin squares $A'_1, \dots, A'_t$ are pairwise orthogonal. Now, since 1 is $(1,1)$-th entry (i.e. the entry in the first row and first column) of all the matrices $A'_1, \dots, A'_t$, we see that 1 is not the $(2,1)$-th entry (i.e. the entry in the second row and first column) of any of the Latin squares $A'_1, \dots, A'_t$. Further, no two of $A'_1, \dots, A'_t$ can have the same number in the $(2,1)$-th entry; indeed, if for some distinct $i, j \in \{1, \dots, t\}$, we had that the $(2,1)$-th entry of A'_i and A'_j was the same, say k, then (k,k) would be both the $(1,k)$-th and the $(2,1)$-th entry of the matrix obtained by superimposing A'_i and A'_j, contrary to the

[3] Can you see why?

fact that A'_i and A'_j are orthogonal. So, each of $A'_1, \dots, A'_t$ has a number from $2, \dots, n$ in the $(2,1)$-th entry, and no two of $A'_1, \dots, A'_t$ have the same $(2,1)$-th entry; thus, $t \leq n-1$. □

Theorem 2.3. *Let $n \geq 2$ be an integer. Then the following are equivalent:*

(a) there exists a finite projective plane of order n;

(b) there exists a collection of $n-1$ pairwise orthogonal $n \times n$ Latin squares.

Proof of "(b) $\implies$ (a)" (outline). Assume that (b) is true, and let $L_1, \dots, L_{n-1}$ be pairwise orthogonal $n \times n$ Latin squares. We will give a construction of the corresponding finite projective plane of order n.[4]

Our finite projective plane has $n^2 + n + 1$ points, and we call them $r, s, \ell_1, \dots, \ell_{n-1}, x_{1,1}, \dots, x_{1,n}, x_{2,1}, \dots, x_{2,n}, \dots, x_{n,1}, \dots, x_{n,n}$.[5]

Our finite projective plane has n^2+n+1 lines, and we construct them as follows. One line is $B = \{r, s, \ell_1, \dots, \ell_{n-1}\}$. Further, for each $i \in \{1, \dots, n\}$, we have the line $R_i = \{r, x_{i,1}, \dots, x_{i,n}\}$; and for each $j \in \{1, \dots, n\}$, we have the line $S_j = \{s, x_{1,j}, \dots, x_{n,j}\}$.[6] The points and lines constructed thus far are represented in Figure 2.3. Now, for each $i \in \{1, \dots, n-1\}$, the point ℓ_i belongs to the (already constructed) line B, and to n other lines, call them $L_i^1, \dots, L_i^n$, which we construct as follows. For all $i \in \{1, \dots, n-1\}$ and $j \in \{1, \dots, n\}$, we set $L_i^j = \{\ell_i\} \cup \{x_{p,q} \mid 1 \leq p, q \leq n, \text{and the } (p,q)\text{-th entry of } L_i \text{ is } j\}$.

The proof of correctness (i.e. of the fact that we have indeed constructed a finite projective plane) is left for HW.[7] □

We remark that the proof of the "(a) $\implies$ (b)" part of Theorem 2.3 is similar to the "(b) $\implies$ (a)" direction, only it goes the other way (from a finite projective plne to a collection of pairwise orthogonal Latin squares). To check your understanding, you can try to give the construction by yourself.

Example 2.4. *Let L_1 and L_2 be, respectively, the left (red) and right (blue) Latin Square from Figure 2.1. The finite projective plane of order 3 that corresponds to $\{L_1, L_2\}$ is as follows. Its vertices are*

$$r, s, \ell_1, \ell_2, x_{1,1}, x_{1,2}, x_{1,3}, x_{2,1}, x_{2,2}, x_{2,3}, x_{3,1}, x_{3,2}, x_{3,3}.$$

Its lines are as follows:

---

[4]For HW, you will prove that this construction is correct.

[5]So, we have the points r and s; we have $n-1$ points ℓ_i; and we have n^2 points $x_{i,j}$. In total, we have $2 + (n-1) + n^2 = n^2 + n + 1$ points.

[6]We remark that for all $i, j \in \{1, \dots, n\}$, we have that $R_i \cap S_j = \{x_{i,j}\}$. We also remark that, so far, we have constructed $2n+1$ lines, and we need to construct $(n^2+n+1)-(2n+1) = n^2 - n = (n-1)n$ more.

[7]We remark, however, that once we have shown that we have indeed constructed a finite projective plane, Theorem 1.4 from Lecture Notes 4 immediately implies that the order of our finite projective plane is n (e.g. because we have n^2+n+1 points).

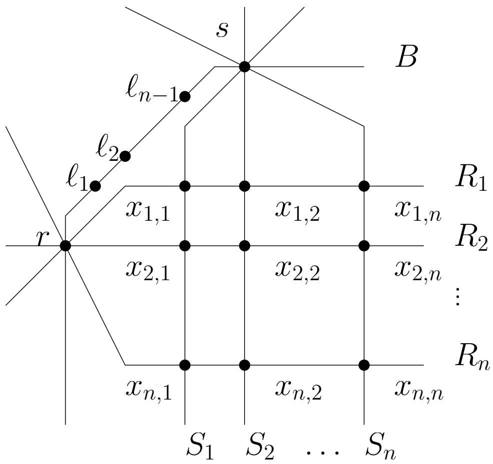

Figure 2.3: Points and lines (except the L_i^j's) of the projective plane from the proof of Theorem 2.3.

- $B = \{r, s, \ell_1, \ell_2\}$;
- $R_1 = \{r, x_{1,1}, x_{1,2}, x_{1,3}\}$;
- $R_2 = \{r, x_{2,1}, x_{2,2}, x_{2,3}\}$;
- $R_3 = \{r, x_{3,1}, x_{3,2}, x_{3,3}\}$;
- $S_1 = \{s, x_{1,1}, x_{2,1}, x_{3,1}\}$;
- $S_2 = \{s, x_{1,2}, x_{2,2}, x_{3,2}\}$;
- $S_3 = \{s, x_{1,3}, x_{2,3}, x_{3,3}\}$;
- $L_1^1 = \{\ell_1, x_{1,1}, x_{2,3}, x_{3,2}\}$;
- $L_1^2 = \{\ell_1, x_{1,2}, x_{2,1}, x_{3,3}\}$;
- $L_1^3 = \{\ell_1, x_{1,3}, x_{2,2}, x_{3,1}\}$;
- $L_2^1 = \{\ell_2, x_{1,1}, x_{2,2}, x_{3,3}\}$;
- $L_2^2 = \{\ell_2, x_{1,2}, x_{2,3}, x_{3,1}\}$;
- $L_2^3 = \{\ell_2, x_{1,3}, x_{2,1}, x_{3,2}\}$.

3 An algebraic construction of projective planes

Let $\mathbb{F}$ be any field. As usual, $+$ and $\cdot$ are, respectively, addition and multiplication in $\mathbb{F}$, and 0 and 1 are, respectively, the additive and multiplicative identity in $\mathbb{F}$. We construct the projective plane $\mathbb{F}P^2$ as follows. We begin with the set $T := \mathbb{F}^3 \setminus \{(0,0,0)\}$, i.e. the set of all ordered triples of elements of $\mathbb{F}$, except for the triple whose entries are all zero. We then form a binary relation $\sim$ on T as follows: for $(x_1, y_1, z_1), (x_2, y_2, z_2) \in T$, we have $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ if and only if there exists a scalar $\lambda \in \mathbb{F} \setminus \{0\}$ such that $(x_2, y_2, z_2) = \lambda(x_1, y_1, z_1)$.[8] It is easy to see that $\sim$ is an equivalence relation on T.[9] The set of points of $\mathbb{F}P^2$ is $T/_{\sim}$; in other words, points of $\mathbb{F}P^2$ are the equivalence classes of the equivalence relation $\sim$ on

[8]This means that $x_2 = \lambda x_1$, $y_2 = \lambda y_1$, and $z_2 = \lambda z_1$.
[9]Check this!

T. We will denote the equivalence class of $(x, y, z) \in T$ by $\overline{(x, y, z)}$, so that $\overline{(x, y, z)} = \{(\lambda x, \lambda y, \lambda z) \mid \lambda \in \mathbb{F} \setminus \{0\}\}$. Thus, the set of points of $\mathbb{F}P^2$ is precisely the set $\{\overline{(x, y, z)} \mid (x, y, z) \in T\}$. Next, for each $(a, b, c) \in T$, we define $P(a, b, c)$ to be the set of all points $\overline{(x, y, z)}$ such that $ax + by + cz = 0$;[10] the lines of $\mathbb{F}P^2$ are precisely the sets $P(a, b, c)$ with $(a, b, c) \in T$. We remark that for all $(a_1, b_1, c_1), (a_2, b_2, c_2) \in T$, we have that $P(a_1, b_1, c_1) = P(a_2, b_2, c_2)$ if and only if $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$.[11]

Theorem 3.1. *For each field $\mathbb{F}$, $\mathbb{F}P^2$ is a projective plane.*

Proof. We use notation from the construction of $\mathbb{F}P^2$. We must verify that the points and lines of $\mathbb{F}P^2$ satisfy (P0), (P1), and (P2) from the definition of a projective plane.

First, we check that (P0) is satisfied for

$$Q = \{\overline{(1, 0, 0)}, \overline{(0, 1, 0)}, \overline{(0, 0, 1)}, \overline{(1, 1, 1)}\}.$$

We note that each of the following four matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

has rank three. So, if A is any one of the four matrices above, then $A\mathbf{x} = \mathbf{0}$ has only the trivial solution, and consequently, no line of $\mathbb{F}P^2$ contains three (or more) points of Q. So, (P0) is satisfied.

Next, we check that (P1) is satisfied. We fix distinct lines P_1, P_2 of $\mathbb{F}P^2$, and we show that $|P_1 \cap P_2| = 1$. By construction, there exist $(a_1, b_1, c_1), (a_2, b_2, c_2) \in T$ such that $P_1 = P(a_1, b_1, c_1)$ and $P_2 = P(a_2, b_2, c_2)$. Since $P_1 \neq P_2$, we have that $(a_1, b_1, c_1) \not\sim (a_2, b_2, c_2)$, that is, neither one of $(a_1, b_1, c_1), (a_2, b_2, c_2)$ is a scalar multiple of the other. We now use Linear Algebra. We consider the 2×3 matrix

$$A = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix}.$$

Since neither row of A is a scalar multiple of the other, we see that $\text{rank}(A) = 2$. On the other hand, by the Rank-Nullity Theorem, we have that $\text{rank}(A) + \dim \ker(A) = 3$. So, $\dim \ker(A) = 1$. Let $\left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \right\}$ be a basis for $\ker(A)$;[12]

[10] Note that for all $\lambda \in \mathbb{F} \setminus \{0\}$, we have that $ax + by + cz = 0$ if and only if $a(\lambda x) + b(\lambda y) + c(\lambda z) = 0$, and so this is well-defined.

[11] Check this!

[12] So, $(x, y, z) \neq (0, 0, 0)$, and we see that $(x, y, z) \in T$. Furthermore, we have that $\ker(A) = \left\{ \begin{bmatrix} \lambda x \\ \lambda y \\ \lambda z \end{bmatrix} \mid \lambda \in \mathbb{F} \right\}$.

then $P_1 \cap P_2 = \left\{\overline{(x, y, z)}\right\}$, and we deduce $|P_1 \cap P_2| = 1$. Thus, (P1) is satisfied.

The proof of the fact that (P2) is satisfied is analogous to the proof that (P1) is satisfied.[13] □

Theorem 3.2. *If $\mathbb{F}$ is a finite field, with $|\mathbb{F}| = n$, then $\mathbb{F}P^2$ is a finite projective plane of order n.*

Proof. By Theorem 3.1, $\mathbb{F}P^2$ is a projective plane. Furthermore, since $\mathbb{F}$ is finite, it is obvious that the projective plane $\mathbb{F}P^2$ is finite. We must show that the order of $\mathbb{F}P^2$ is n. In view of Theorem 1.4 from Lecture Notes 4, it suffices to show that $\mathbb{F}P^2$ has precisely $n^2 + n + 1$ points. Now, note that for all $(x, y, z) \in T$, there exists a unique triple $(x', y', z') \in T$ such that the last non-zero coordinate of (x', y', z') is 1 and $(x, y, z) \sim (x', y', z')$.[14] Now, there are n^2 triples of the form $(x, y, 1)$ in T; there are n triples of the form $(x, 1, 0)$ in T; and there is one triple $(1, 0, 0)$ in T. So, there are $n^2 + n + 1$ equivalence classes of $\sim$, that is, $\mathbb{F}P^2$ has $n^2 + n + 1$ points. As we already pointed out, Theorem 1.4 from Lecture Notes 4 now implies that the finite projective plane $\mathbb{F}P^2$ is of order n. □

It is well-known that for all integers $n \geq 2$, there exists a field of size n if and only if n is a power of a prime (that is, if and only if there exist a prime number p and a positive integer k such that $n = p^k$). This, together with Theorem 3.2, implies that if $n \geq 2$ is a power of a prime, then there is a finite projective plane of order n. However, it is not known whether there exists a finite projective plane whose order is not a power of a prime. It is, however, known that there are no finite projective planes of order 6 or 10. It is not known whether there are finite projective planes of order 12. (Note that every $n \in \{2, \dots, 13\} \setminus \{6, 10, 12\}$ is a power of a prime, and so a finite projective plane of order n does exist.)

[13] Check this!

[14] For existence, we observe that for all $(x, y, z) \in T$, we have the following:

- if $z \neq 0$, then $(x, y, z) \sim (z^{-1}x, z^{-1}y, 1)$;
- if $z = 0$ and $y \neq 0$, then $(x, y, z) \sim (y^{-1}x, 1, 0)$;
- if $y = z = 0$, then $x \neq 0$ (since x, y, z cannot all be zero) and $(x, y, z) \sim (1, 0, 0)$.

Can you check uniqueness?