PRPL

Amit Rajaraman

Last updated January 22, 2022

Contents

§1. Introduction

1.1. Projective Planes

Definition 1.1 (Incidence System)**.** An *incidence system* is a pair $(\mathcal{P}, \mathcal{L})$, where $\mathcal{P}$ is a set and $\mathcal{L}$ is a set of subsets of $\mathcal{P}$. Elements of $\mathcal{P}$ are called *points* and elements of $\mathcal{L}$ are called *lines*. A line ℓ is said to be *incident* on a point p if $p \in \ell$.

Definition 1.2 (Partial Linear Space)**.** An incidence system $(\mathcal{P}, \mathcal{L})$ is said to be a *partial linear space* if

1. for each $\ell \in \mathcal{L}$, $|\ell| \geq 2$.
2. for distinct $x, y \in \mathcal{P}$, there is at most one $\ell \in \mathcal{L}$ such that $\{x, y\} \subseteq \mathcal{P}$.

Definition 1.3 (Linear Space)**.** An incidence system $(\mathcal{P}, \mathcal{L})$ is said to be a *linear space* if

1. for each $\ell \in \mathcal{L}$, $|\ell| \geq 2$.
2. for distinct $x, y \in \mathcal{P}$, there is a unique $\ell \in \mathcal{L}$ such that $\{x, y\} \subseteq \mathcal{P}$.

Definition 1.4 (Dual)**.** Given a partial linear space $\mathcal{X} = (\mathcal{P}, \mathcal{L})$, the incidence system $\mathcal{X}^* = (\mathcal{P}^*, \mathcal{L}^*)$ is said to be its *dual* if there exist bijections $f : \mathcal{P} \to \mathcal{L}^*$ and $g : \mathcal{L} \to \mathcal{P}^*$ such that for any $p \in \mathcal{P}, \ell \in \mathcal{L}$, $p \in \ell$ iff $g(\ell) \in f(p)$.

We remark that the dual is unique up to isomorphism.

Definition 1.5 (Projective Plane)**.** An incidence system $\mathcal{X} = (\mathcal{P}, \mathcal{L})$ is said to be a *projective plane* if

1. $\mathcal{X}$ is a linear space.
2. $\mathcal{X}^*$ is a linear space.
3. For any distinct $\ell, \ell' \in \mathcal{L}$, there exists $p \in \mathcal{P}$ such that $p \notin \ell \cup \ell'$. This condition is equivalent to asserting that for distinct $p, p' \in \mathcal{P}$, there exists $\ell \in \mathcal{L}$ such that $\{p, p'\} \cap \ell = \varnothing$.

Given distinct points x_1, x_2, we denote by $x_1 \vee x_2$ the (unique) line passing through x_1 and x_2. Similarly, given distinct lines ℓ_1, ℓ_2, we denote by $\ell_1 \wedge \ell_2$ the (unique) point in their intersection.

Definition 1.6. Given a projective plane $\mathcal{X}$, fix a line ℓ and point x not incident on ℓ. The function defined by $y \mapsto x \cup y$ is one from the set of points in ℓ to the set of lines through x. Further, it has inverse $m \mapsto m \cap \ell$ and is thus a bijection. These two bijections are referred to as *perspectivities* on the projective plane.

Using perspectivities, the following may be shown.

Lemma 1.1. Given a projective plane $\mathcal{X}$, there exists a number $n \geq 0$, known as the *order* of $\mathcal{X}$, such that

1. any point is incident with exactly $n+1$ lines.
2. any line contains exactly $n+1$ lines.
3. the total number of points is n^2+n+1.
4. the total number of lines is n^2+n+1.

One common example of a projective plane is $\mathrm{PG}(2,\mathbb{F})$, the projective plane over field $\mathbb{F}$. This has point set V_1 equal to the set of all 1-dimensional subspaces of $\mathbb{F}^3$ (as a vector space over $\mathbb{F}$), and line set V_2 equal to the set of all 2-dimensional subspaces of $\mathbb{F}^3$, where we identify each such subspace with the set of all 1-dimensional subspaces contained in it.
In particular, $\mathrm{PG}(2,\mathbb{F}_q)$ (where q is a prime power) is of order q.

The second projective plane of interest is the *free projective plane*. We define it using a sequence $(\mathcal{X}_n)$ of incidence systems. Define $\mathcal{X}_\infty = (\mathcal{P}_1, \mathcal{L}_1)$ by $\mathcal{P}_1 = [4]$, $\mathcal{L}_1 = \binom{\mathcal{P}_1}{2}$. Given $\mathcal{X}_n = (\mathcal{P}_n, \mathcal{L}_n)$, the next incidence system is defined by taking $\mathcal{X}_n$ then performing the following operations:

1. for each pair $\{\ell_1, \ell_2\}$ of lines in $\mathcal{X}_n$ which have no common point, introduce a new point $\ell_1 \cap \ell_2$. This new point is incident with ℓ_1, ℓ_2 and no other line.
2. for each pair $\{x_1, x_2\}$ of points in $\mathcal{X}_n$ which have no line in common, introduce a new line $x_1 \cup x_2$. This new line is incident on x_1, x_2 and no other point.

Finally, define the free projective plane $\mathcal{X} = (\bigcup_{n=1}^\infty \mathcal{P}_n, \bigcup_{n=1}^\infty \mathcal{L}_n)$ as the "limiting element" of this sequence.
The free projective plane is denoted $\mathcal{F}$.

Definition 1.7 (Subplane)**.** A projective plane $(\mathcal{P}', \mathcal{L}')$ is said to be a projective *subplane* of projective plane $(\mathcal{P}, \mathcal{L})$ if

$$\mathcal{L}' = \{\ell \cap \mathcal{P}' : \ell \in \mathcal{L}\}.$$

Definition 1.8. A *prime* projective plane is a projective plane that has no proper subplane.

For example, $\mathrm{PG}(2,\mathbb{F})$ is prime if $\mathbb{F}$ is a prime field (such as $\mathbb{Q}$ or $\mathbb{F}_p$ for prime p). The free projective plane is prime as well.

Remark. We are interested in both prime projective planes and projective planes of prime order. Observe which one is being referred to in any sentence!

Conjecture. The only examples of prime projective planes are the free projective plane and the projective planes over prime fields.

It turns out that any prime projective plane is a homomorphic image of $\mathcal{F}$. Consequently, it may be interesting to study the sequence $\mathcal{X}_n$ of projective planes involved in the definition of $\mathcal{F}$.

For $q > 8$ that is a non-prime prime power (so p^r for $r \geq 2$), there are constructions of projective planes of order q which are not the field plane $\mathrm{PG}(2, \mathbb{F}_q)$. However, we have nothing similar for prime q.

Conjecture. Up to isomorphism, $\mathrm{PG}(2, \mathbb{F}_p)$ is the only projective plane of prime order p.

The two conjectures given do have some resemblance, but we have nothing concrete. In fact, it is not even known if a projective plane of prime order is necessarily a prime projective plane, or if a finite prime projective plane must have prime order.
A stronger version of Section 1.1 is the following, conjectured by H. Neumann.

Conjecture. A finite projective plane has no subplane of order two if and only if it is isomorphic to $\mathrm{PG}(2, \mathbb{F}_q)$ for some odd prime power q.

1.2. Coding Theory

Definition 1.9. Given an incidence system $\mathcal{X} = (\mathcal{P}, \mathcal{L})$ and a field $\mathbb{F}$, we define the p-ary linear code $\mathcal{C}_{\mathbb{F}}(\mathcal{X})$ over $\mathbb{F}^{\mathcal{P}}$ as follows. Identify each line ℓ with the codeword in $\mathbb{F}^{\mathcal{P}}$ whose xth coordinate is 1 if $x \in \ell$ and 0 otherwise. $\mathcal{C}_{\mathbb{F}}(\mathcal{X})$ is then the space spanned by the codewords corresponding to the lines in $\mathcal{L}$.
If $\mathbb{F} = \mathbb{F}_q$, we sometimes denote the above as $\mathcal{C}_q(\mathcal{X})$.

We call the code $\mathcal{X} = (\mathcal{P}, \mathcal{L})$ *trivial* at q if $\mathcal{C}_q(\mathcal{X}) = \mathbb{F}^{\mathcal{P}}$.

Theorem 1.2. If π is a projective plane of order n and q is a prime power that does not divide n, then $\mathcal{C}_q(\pi)$ is trivial.

Proof. For each $x \in \mathcal{P}$, consider the word v_x formed by adding all the lines that pass through x. This word has $n+1$ in the xth coordinate and 1 in all remaining coordinates. For distinct $x, y \in \mathcal{C}_p(\pi)$, the word $v_x - v_y$ is thus the vector that has n in the xth coordinate, $-n$ in the yth coordinate, and all remaining coordinates are 0. Since q does not divide n, n and $-n$ are nonzero in $\mathbb{F}_q$, and so $e_x - e_y$ lies in $\mathcal{C}_q(\pi)$. This implies that the dual $\mathbf{1}^\top$ of the all 1s vector is contained in $\mathcal{C}_q(\pi)$. If we manage to show that $\mathbf{1}$ is contained in the code, we are done. ∎

Definition 1.10. Given a code $\mathcal{C}$ over $\mathbb{F}_q^{\mathcal{P}}$, its *dual* is

$$\mathcal{C}^\top = \{v \in \mathbb{F}_q^{\mathcal{P}} : \langle v, w \rangle = 0 \text{ for all } w \in \mathcal{C}\},$$

where

$$\langle v, w \rangle = \sum_{x \in \mathcal{P}} v_x w_x.$$

Observe that perhaps counter to one's intuition, a code and its dual need not be disjoint.

We are interested in the *weight* of the codes $\mathcal{C}_q(\mathcal{X})$ and $\mathcal{C}_q(\mathcal{X})^\top$ for projective planes or partial linear spaces $\mathcal{X}$ (typically of prime order).

1.3.