PRPL

Amit Rajaraman

Last updated April 14, 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 (Steiner 2-design)**.** A *Steiner 2-design* $(\mathcal{P}, \mathcal{L})$ is a linear space wherein the cardinality of any line is the same and the same number of lines pass through any point.

If a Steiner 2-design has P points on each line and L lines through every point, it has a total of $LP - (L-1)$ points and $L(LP - L + 1)/P$ lines.

Definition 1.5 (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 1.6 (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 1.7. Given a projective plane $\mathcal{X}$, fix a line ℓ and point x not incident on ℓ. The function defined by $y \mapsto x \vee y$ is one from the set of points in ℓ to the set of lines through x. Further, it has inverse $m \mapsto m \wedge \ell$ 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 $n+1$ points.
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 $\ell_1 \wedge \ell_2$. 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 $x_1 \vee x_2$. 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 1.8 (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 1.9. 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. The coding theoretic aspect

Definition 1.10. Given an incidence system $\mathcal{X} = (\mathcal{P}, \mathcal{L})$ and a field $\mathbb{F}$, we define the 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 $\mathcal{C}_q(\mathcal{X}) = \mathbb{F}^{\mathcal{P}}$. We often denote this code as $\mathcal{C}_{\mathcal{X}}$ or $\mathcal{C}_{\mathcal{L}}$ if q is clear from context.

Definition 1.11 (Dual)**.** 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.
If the dual of a code over $\mathbb{F}_q$ contains a non-zero vector, then the code is non-trivial at q.
We are often 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).

Definition 1.12 (Complete Weight Enumerator)**.** Given a code $\mathcal{C}$ over $\mathbb{F}_p^{\mathcal{P}}$, the *complete weight enumerator* G of $\mathcal{C}$ is given by

$$G(\underset{\sim}{Z}) = \sum_{f \in \mathcal{C}} \underset{\sim}{Z}^{\text{type}(f)},$$

where for $X, Y \in \mathbb{F}_p^{\mathcal{P}}$,

$$\underset{\sim}{X}^{\underset{\sim}{Y}} = \prod_{P \in \mathcal{P}} X_P^{Y_P} \text{ and}$$
$$\text{type}(f) = (|\{P \in \mathcal{P} : f(P) = \alpha\}| : \alpha \in \mathbb{F}_p).$$

Here, $\underset{\sim}{Z} = (Z_\alpha : \alpha \in \mathbb{F}_p)$ is any p-tuple of commuting variables.

Lemma 1.2. Let $\pi = (\mathcal{P}, \mathcal{L})$ be a projective plane of prime order p. For a $w \in \mathbb{F}_p^{\mathcal{P}}$, $w \in \mathcal{C}_p(\pi)$ iff $\langle w, \ell \rangle = \langle w, \mathbf{1} \rangle$ for all lines ℓ of π.

Proof. Observe that $\{\mathbf{1} - \ell : \ell \in \mathcal{L}\}$ spans $\mathcal{C}_p(\pi)^\top$. Indeed, for any lines $\ell_1 \neq \ell_2$, $\langle \ell_1, \mathbf{1} - \ell_1 \rangle = 0$ trivially, and $\langle \ell_1, \mathbf{1} - \ell_2 \rangle = 2p = 0$. The required immediately follows. ∎

Lemma 1.3. Let $\mathcal{X}$ be a finite PLS and p a prime. Then $\dim(\mathcal{C}_p(\mathcal{X}^*)) = \dim(\mathcal{C}_p(\mathcal{X}))$.

Proof. Consider the "incidence" matrix M of $\mathcal{X}$ indexed by $\mathcal{L}$ and $\mathcal{P}$, where the (ℓ, p)th entry of M is 1 iff $p \in \ell$. $\mathcal{C}_p(\mathcal{X})$ is then just $\{Mv : v \in \mathbb{F}_p^{p \times 1}\}$, so $\dim(\mathcal{C}_p(\mathcal{X}))$ is the column rank of M. Now note that the incidence matrix of $\mathcal{X}^*$ is just $M^\top$ (reindexed appropriately), so $\dim(\mathcal{C}_p(\mathcal{X}^*))$ is the row rank of M. Since the row and column ranks are equal, we are done. ∎

1.3. Projective Planes

Lemma 1.4. Let π_1, π_2 be two projective planes of prime order p that share $p^2 + 1$ lines. Then $\pi_1 = \pi_2$.

Proof. Let $\mathcal{L}_0$ be a common set of lines of size $p^2 + 1$. Since each point P of π_i is contained in $p + 1$ lines and there are $p^2 + p + 1$ lines in all, $P \in \ell$ for some $\ell \in \mathcal{L}\prime$, so the π_i share the same point set.
Let $\mathcal{X} = (\mathcal{P}, \mathcal{L}_0)$. Since the lines of π_i are precisely the supports of the minimum weight words of $\mathcal{C}_p(\pi_i)$, it suffices to show that $\mathcal{C}_p(\pi_i) = \mathcal{C}_p(\pi_2)$. To do this, we shall show that $\mathcal{C}_p(\pi_1) = \mathcal{C}_p(\mathcal{X})$. For the sake of succinctness, denote π_1 as $\pi = (\mathcal{P}, \mathcal{L})$. Since $\mathcal{X}$ is a subsystem of π, this is equivalent to $\dim(\mathcal{C}_p(\pi)) = \dim(\mathcal{C}_p(\mathcal{X}))$, which in turn is equivalent to $\dim(\mathcal{C}_p(\pi^*)) = \dim(\mathcal{C}_p(\mathcal{X}^*))$. Consider the restriction map from $\mathbb{F}_p^{\mathcal{L}}$ to $\mathbb{F}_p^{\mathcal{L}_0}$. This restricts to a linear map from $\mathcal{C}_p(\pi^*)$ to $\mathcal{C}_p(\mathcal{X}*^)$. Observe that the kernel of this map is precisely those words in $\mathcal{C}_p(\pi^*)$ that have support in $\mathcal{L} \setminus \mathcal{L}_0$. Further, since $|\mathcal{L} \setminus \mathcal{L}_0| = p$, and there is no non-zero word in $\mathcal{C}_p(\pi^*)$ with Hamming weight $\leq p$ (any line in π is incident on $p+1$ points). Therefore, the kernel of this map is trivial! This implies that $\dim(\mathcal{C}_p(\pi^*)) = \dim(\mathcal{C}_p(\mathcal{X}^*))$, completing the proof. ∎

Definition 1.13. An incidence system $\mathcal{Y} = (\mathcal{P}, \mathcal{L})$ is said to be *p-admissible* if

1. there are exactly $p^2 + p + 1$ points,
2. any line is incident on exactly $p + 1$ points, and
3. any two distinct lines are incident at a single point.

Observe that if $\pi = (\mathcal{P}, \mathcal{L})$ is a projective plane, then $(\mathcal{P}, \mathcal{L}')$ is p-admissible for any $\mathcal{L}' \subseteq \mathcal{L}$.

Lemma 1.5. Let $\sigma = (\mathcal{P}, \mathcal{L})$ be p-admissible. Then σ has at most $p^2 + p + 1$ lines, with equality iff σ is a projective plane of order p.

Proof. For the first part, we are done if we manage to show that there are at most $p + 1$ lines through any point. This is easily done using perspectivities – letting $\{\ell_i\}_{i=1}^n$ to be the set of all lines through a point P, the sets $\ell_i \setminus \{x\}$ are disjoint, so

$$|\mathcal{P} \setminus \{P\}| = p^2 + p \geq np = \left| \bigcup_{i=1}^{n} \ell_i \setminus \{P\} \right|.$$

Because there are precisely $p + 1$ points through any line in the equality case, the second part is not too difficult to prove either. ■

Lemma 1.6. Let S be the union of $k \geq 1$ lines of a p-admissible incidence system. The $k(p+1) - \binom{k}{2} \leq |S| \leq kp+1$.

Proof. Let $\{\ell_i\}_{i=1}^k$ be a set of k lines in the system.
If $\mathcal{P}'$ is the set of all $\ell_i \wedge \ell_j$, then

$$|S| \geq \sum |\ell_i| - |\mathcal{P}'| \geq k(p + 1) - \binom{k}{2}.$$

For the upper bound on the other hand, we have using the union bound that

$$|S| \leq \left| \bigcup (\ell_i \setminus \mathcal{P}') \right| + |\mathcal{P}'|.$$

Since any ℓ_i must intersect $\mathcal{P}'$ somewhere (and $\mathcal{P}'$ is non-empty), we can use the union bound once more to get that

$$|S| \leq k(p + 1 - 1) + |\mathcal{P}'| \leq kp + 1.$$

■

Lemma 1.7. Let $\mathcal{Y}, \mathcal{Y}'$ be p-admissible incidence systems. Suppose that the union of m lines of $\mathcal{Y}$ is equal to the union of k lines of $\mathcal{Y}'$. If $\binom{k}{2} < p$, $m = k$.

Lemma 1.8. Let k be a positive integer and x_i for $0 \leq i < k$ be non-negative such that $2^k - 1 = \sum_i 2^i x_i$. Then, $\sum_i x_i \geq k$ with equality iff all the x_i are 1.

We omit the proof of the above as it follows by a doable inductive argument.

Lemma 1.9. Let p be a prime and $\mathcal{Y}$ a p-admissible incidence system with exactly k lines $(\ell_i)_{i=0}^{k-1}$. Consider the word $w \in \mathcal{C}_p(\mathcal{Y})$ defined by $w = \sum_{0 \leq i < k} 2^i \ell_i$. Let π be a projective plane of order p, and suppose $w' \in \mathcal{C}_p(\pi)$ with $\text{type}(w) = \text{type}(w')$.
If $p \geq 2^k$, there are lines $(\ell'_i)_{i=0}^{k-1}$ of π such that $w' = \sum_{0 \leq i < k} 2^i \ell'_i$. Further, there is a monomorphism f from $\mathcal{Y}$ into π such that $\ell'_i = f(\ell_i)$ for each i.

Proof. Let $\mathcal{P}, \mathcal{Q}$ be the point sets of $\pi, \mathcal{Y}$. For integers $i \geq 0$ and $x \geq 0$, let $\delta_i(x)$ be the ith digit from the right in the binary representation of x (0-indexed). Note that

$$\ell_i = \{Q \in \mathcal{Q} : \delta_i(w_Q) = 1\}.$$

Inspired by this, define

$$\ell'_i = \{P \in \mathcal{P} : \delta_i(w'_P) = 1\}.$$

We have $w' = \sum_{0 \leq i < k} 2^i \ell'_i$. Since $\text{type}(w) = \text{type}(w')$, there exists a bijection $f : \mathcal{Q} \to \mathcal{P}$ such that $w' = w \circ f$. Thus, for $Q \in \mathcal{Q}$ and any i,

$$Q \in \ell_i \iff \delta_i(w_Q) = 1 \iff \delta_i(w_{f(Q)}) = 1 \iff f(Q) \in \ell'_i.$$

So, $f(\ell_i) = \ell'_i$ for each i. If we manage to show that the ℓ'_i are actually lines in π, then f is a monomorphism from $\mathcal{Y}$ to π and we are done.
Let $S' = \bigcup_i \ell'_i$. Observe that because $p \geq 2^k$, $\operatorname{supp} w' = S'$.
The proof strategy is as follows: we show that S' contains precisely k lines of π, then show that replacing these k lines with the k lines of the isomorphic image of $\mathcal{Y}$ in π yields another projective plane, then use Lemma 1.4 to conclude that the two projective planes are the same since the number of common lines is at least $p^2 + p + 1 - k \geq p^2 + 1$.
Let us first show that replacing the lines yields a projective plane once more.

Claim. For any $\ell \subsetneq S'$ of π, $|\ell \cap \ell'_i| = 1$.
First, note that

$$\begin{aligned}\sum_{0 \leq i < k} 2^i |\ell \cap \ell'_i| &= \sum_{x \in \ell} \sum_{0 \leq i < k} 2^i \ell_i(x) \\ &= \sum_{x \in \ell} w'_x.\end{aligned}$$

Let us now compute the value of this in $\mathbb{N}$. Using In $\mathbb{F}_p$,

$$\sum_{x \in \mathcal{P}} w'(x) = \langle w', \mathbf{1} \rangle = \sum_{0 \leq i < k} 2^i |\ell_i| = \sum_{0 \leq i < k} 2^i = 2^k - 1.$$

Using Lemma 1.2, $\langle w', \ell \rangle = 2^k - 1$ in $\mathbb{F}_p$. Since $p \geq 2^k$, we have for any $y \notin S'$,

$$\begin{aligned}(p+1)(2^k - 1) &\leq \sum_{\ell \ni y} \sum_{x \in \ell} w'_x \\ &= \sum_{x \in \mathcal{P}} w'_x \\ &= \sum_{x \in \mathcal{P}} \sum_{0 \leq i < k} 2^i \ell'_i(x) \\ &= \sum_{0 \leq i < k} 2^i \sum_{x \in \mathcal{P}} \ell'_i(x) \\ &= \sum_{0 \leq i < k} 2^i (p+1) = (p+1)(2^k - 1).\end{aligned}$$

Therefore, for any line $\ell \subsetneq S'$ (which means such a y exists), $\sum_{x \in \ell} w'_x = 2^k - 1$.
Going back to what we were working with,

$$\sum_{0 \leq i < k} 2^i |\ell \cap \ell'_i| = 2^k - 1.$$

By Lemma 1.8, $\sum_i |\ell \cap \ell'_i| \geq k$. Now, for any $y \notin S'$,

$$\begin{aligned}(p+1)k &\leq \sum_{\ell \ni y} \sum_{0 \leq i < k} |\ell \cap \ell'_i| \\ &= \sum_{0 \leq i < k} \sum_{\ell \ni y} |\ell \cap \ell'_i| \\ &= \sum_{0 \leq i < k} |\ell'_i| = (p+1)k.\end{aligned}$$

Therefore, $\sum_i |\ell \cap \ell'_i| = k$, and it follows using Lemma 1.8 that $|\ell \cap \ell'_i| = 1$ for all i. □
Next, let us show that S' contains exactly k lines of π.
If for some $x \neq y$ in ℓ'_i, ℓ is the line of π incident on the two, then we must have by the claim that $\ell \subseteq S'$. It follows that S' is the union of some m lines of π as well as k lines of $\mathcal{Y}'$. However, $p > \binom{k}{2}$, so Lemma 1.7 implies that $m = k$.

Using the procedure described earlier to replace these k lines of π constituting S' with those corresponding to $\mathcal{Y}$, we get that both sets of lines are in fact the same, and therefore, all the ℓ'_i are lines of π, completing the proof. ■

Let us now move to the meat of this particular section.

Definition 1.14. Given incidence systems $\mathcal{X}, \mathcal{Y}$, define

1. $I(\mathcal{Y}, \mathcal{X})$ to be the number of monomorphisms from $\mathcal{Y}$ into $\mathcal{X}$,
2. $i(\mathcal{Y}, \mathcal{X})$ to be the number of isomorphic copies of $\mathcal{Y}$ that are subsystems of $\mathcal{X}$, and
3. $\mathrm{Aut}(\mathcal{X})$ to be the automorphism group of $\mathcal{X}$ (under composition).

Lemma 1.10. For any incidence systems $\mathcal{X}, \mathcal{Y}$,

$$I(\mathcal{Y}, \mathcal{X}) = |\mathrm{Aut}(\mathcal{Y})| \cdot i(\mathcal{Y}, \mathcal{X}).$$

We omit the proof of the above as it is straightforward.

Denote by $\mathcal{J}_p$ the set of all p-tuples $\underset{\sim}{j} = (j_\alpha : \alpha \in \mathbb{F}_p)$ such that $|\underset{\sim}{j}| = \sum j_\alpha = p^2 + p + 1$. Note that $\mathrm{type}(w) \in \mathcal{J}_p$ for any $w \in \mathcal{C}_p(\mathcal{X})$ if $\mathcal{X}$ has $p^2 + p + 1$ points.

Theorem 1.11. Let π be a projective plane of prime order p, and let $f(\underset{\sim}{X}) = \sum_{\underset{\sim}{j} \in \mathcal{J}_p} a_{\underset{\sim}{j}} \underset{\sim}{X}^{\underset{\sim}{j}}$ be the complete weight enumerator of $\mathcal{C}_p(\pi)$. That is, $a_{\underset{\sim}{j}}$ is the number of words of type $\underset{\sim}{j}$ in $\mathcal{C}_p(\pi)$. Then, for any PLS $\mathcal{X}$ with at most $\log_2 p$ lines, there are rationals $\alpha_{\underset{\sim}{j}}$ for $\underset{\sim}{j} \in \mathcal{J}_P$ depending only on $\mathcal{X}$ and p such that

$$i(\mathcal{X}, \pi) = \sum_{\underset{\sim}{j} \in \mathcal{J}_p} \alpha_{\underset{\sim}{j}} a_{\underset{\sim}{j}}.$$

Proof. Observe that up to isomorphism, there exist a finite number of p-admissible systems $\mathcal{Y}_j$ $(1 \leq j \leq m)$ with exactly k lines such that $\mathcal{X}$ is a subsystem of $\mathcal{Y}_j$.
For any isomorphic image $\mathcal{X}'$ of $\mathcal{X}$ in π, there exists a unique isomorphic image $\mathcal{Y}_j'$ of some $\mathcal{Y}_j$ in π such that $\mathcal{X}'$ is a subsystem of $\mathcal{Y}_j$. Indeed, $\mathcal{Y}_j'$ is the unique subsystem of π whose lines are merely the lines ℓ' of π as ℓ varies over the lines of $\mathcal{X}'$, where ℓ' is the unique line in π that contains ℓ. Therefore,

$$i(\mathcal{X}, \pi) = \sum_{j=1}^{m} i(\mathcal{X}, \mathcal{Y}_j) i(\mathcal{Y}_j, \pi).$$

So, it suffices to show that letting $\mathcal{Y} = \mathcal{Y}_j$, there exist some rational $\beta_{\underset{\sim}{j}}$ depending only on $\mathcal{Y}$ such that

$$I(\mathcal{Y}, \pi) = \sum_{j} a_{\underset{\sim}{j}} \beta_{\underset{\sim}{j}}.$$

We use Lemma 1.10 to consider I instead of i.
Now, let us number the k lines of $\mathcal{Y}$ as $(\ell_i)_{i=1}^{k}$, where $p \geq 2^k$. Fix $w = \sum_{i=1}^{k} 2^i \ell_i \in \mathcal{C}_p(\mathcal{Y})$ and $\underset{\sim}{j} = \mathrm{type}(w) \in \mathcal{J}_p$.
For any monomorphism $f : \mathcal{Y} \to \pi$, consider the word $w \circ f^{-1}$. This word is one of the $a_{\underset{\sim}{j}}$ words of type $\underset{\sim}{j}$.
Conversely, let $w' \in \mathcal{C}_p(\pi)$ be of type $\underset{\sim}{j}$ and let f be one of the $\underset{\sim}{j}!$ bijection from the point set of $\mathcal{Y}$ to the point set of π satisfying $w' = w \circ f^{-1}$. By Lemma 1.9, f is a monomorphism! Therefore,

$$I(\mathcal{Y}, \pi) = \underset{\sim}{j}! a_{\underset{\sim}{j}},$$

completing the proof. ■

Corollary 1.12. Let π, σ be two projective planes of prime order p such that their codes $\mathcal{C}_p(\pi)$ and $\mathcal{C}_p(\sigma)$ have the same complete weight enumerator. Then, for any PLS $\mathcal{X}$ with at most $\log_2 p$ lines, $i(\mathcal{X}, \pi) = i(\mathcal{X}, \sigma)$.

Define the partial linear space $\mathbb{P}$, known as the *Pappian configuration*, defined as follows. Fix a point-line incident pair (x, ℓ) in $\mathrm{PG}(2, \mathbb{F}_3)$. The points of $\mathbb{P}$ are the points of $\mathrm{PG}(2, \mathbb{F}_3)$ not incident on ℓ, and lines are the intersections of lines non-incident on x with this point set.
To visualize it slightly better, suppose we have two non-intersecting lines $x_1x_2x_3$ and $y_1y_2y_3$. Add new points

$$\begin{aligned} z_1 &= (x_2 \vee y_3) \wedge (x_3 \vee y_2) \\ z_2 &= (x_3 \vee y_1) \wedge (x_1 \vee y_3) \\ z_3 &= (x_1 \vee y_2) \wedge (x_2 \vee y_1). \end{aligned}$$

Then, the point set of $\mathbb{P}$ is all the x_i, y_i, z_i, and the lines are

$$x_1x_2x_3, y_1y_2y_3, z_1z_2z_3, x_iz_{i+1}y_{i+2}, x_iz_{i-1}y_{i-2}$$

for $1 \leq i \leq 3$, where the additions/subtractions are done modulo 3.

Definition 1.15 (Pappian Projective Plane)**.** Let us call a pair of sets α, β of points in a projective plane π to be admissible if α and β are collinear triples and no four points of $\alpha \sqcup \beta$ are collinear (so the intersection point of the two lines is in neither α nor β). π is said to be *Pappian* if for every pair (α, β) of admissible triples and bijection $f : \alpha \to \beta$, there is a unique isomorphic copy of $\mathbb{P}$ in π such that α and β are lines in $\mathbb{P}$ and for each $x \in \alpha$, x and $f(x)$ are non-collinear in $\mathbb{P}$.

We give the following famous result from projective geometry without proof.

Theorem 1.13. A projective plane is Pappian iff it is the projective plane over a division ring.
In particular, by Wedderburn's Theorem, a finite projective plane is Pappian iff it is a field plane.

Theorem 1.14. Let π be a projective plane of order n. Then

$$i(\mathbb{P}, \pi) \leq \frac{2}{3}\binom{n^2+n+1}{2}\binom{n}{3}^2.$$

Equality holds iff π is a field plane.

Proof. To determine an isomorphic copy of $\mathbb{P}$ in π, we require

1. two lines ℓ_1, ℓ_2. There are $2\binom{n^2+n+1}{2}$ ways of doing this.
2. three points from each of the two lines, none of which are equal to $\ell_1 \wedge \ell_2$. There are $\binom{n}{3}^2$ ways of doing this.
3. a bijection f between the two triplets of points. There are 6 of these.

Further, there are 18 repeats of each copy of $\mathbb{P}$, so

$$i(\mathbb{P}, \pi) \leq \frac{12}{18}\binom{n^2+n+1}{2}\binom{n}{3}^2,$$

with equality iff π is Pappian. ∎

Combining Theorem 1.14 and corollary 1.12, we get the following.

Theorem 1.15. Let π be a projective plane of prime order p that has the same complete weight enumerator as $\mathrm{PG}(2, \mathbb{F}_p)$. If $p > 2^9$, π is isomorphic to $\mathrm{PG}(2, \mathbb{F}_p)$.

1.4. Rigidity Theorems on Partial Linear Spaces

Definition 1.16 (Induced structure)**.** Given a partial linear space $(\mathcal{P}, \mathcal{L})$ and a $\mathcal{P}' \subseteq \mathcal{P}$ such that no line in $\mathcal{L}$ intersects $\mathcal{P}'$ in exactly one point, one can easily come up with a partial linear space $(\mathcal{P}', \mathcal{L}')$ by restricting to those lines in $\mathcal{L}$ which intersect $\mathcal{P}'$. This is known as the *induced structure* on $\mathcal{P}'$.

Definition 1.17 (Join)**.** Given two partial linear spaces $(\mathcal{P}_1, \mathcal{L}_1)$ and $(\mathcal{P}_2, \mathcal{L}_2)$ with $\mathcal{P}_1 \cap \mathcal{P}_2 = \varnothing$, one can define the *join* of the two partial linear spaces by $(\mathcal{P}_1 \cup \mathcal{P}_2, \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3)$, where

$$\mathcal{L}_3 = \{\{x, y\} : x \in \mathcal{P}_1, y \in \mathcal{P}_2\}.$$

Theorem 1.16. If a PLS $\mathcal{X} = (\mathcal{P}, \mathcal{L})$ is non-trivial at p and has at least $n + 1$ lines through every point, then $|\mathcal{P}| \geq 2n + 2 - 2n/p$. Moreover, equality holds iff $\mathcal{X}$ is the join of two Steiner 2-designs with n/p lines through each point and p points on each line.

Proof. The backward direction of the iff statement is direct since each of the Steiner designs has $n - (n/p - 1)$ points and their join thus has $2n + 2 - 2n/p$ points. Similarly, there are $n/p + (n - n/p + 1) = n + 1$ lines through each point in the join.

The converse is trivial for $p = 2$, so assume $p > 2$.
Let $(\mathcal{P}', \mathcal{L}')$ be a PLS which is non-trivial at p, has at least $n{+}1$ lines through every point, and with $|\mathcal{P}'| \leq 2n{+}2{-}2n/p$. Denote $\mathcal{C} = \mathcal{C}_p(\mathcal{X})$. Let w be a word of minimum weight in $\mathcal{C}^\top$, and $\mathcal{P}$ be the support of w (the set of coordinates where w is nonzero). Let $(\mathcal{P}, \mathcal{L}_0)$ be the induced structure on $\mathcal{P}$ – it is a partial linear space such that $\mathcal{C}_{\mathcal{L}_0}^\top$ is generated by the restriction of w to $\mathcal{P}$. Obviously, $(\mathcal{P}, \mathcal{L})$ is non-trivial at p, and a subset ℓ of $\mathcal{P}$ is in $\mathcal{L}_0$ iff its characteristic function is in the dual of $\langle w \rangle$.
Now, repeatedly perform the following sequence of operations on $\mathcal{L}_0$ until it is no longer possible to do so:

1. Choose $\ell \in \mathcal{L}_0$ that can be written as $\ell = \ell' \cup \ell''$, where ℓ' (and so ℓ'') is in $\mathcal{C}_{\mathcal{L}_0}$.
2. Replace ℓ with ℓ' and ℓ''.

Finally, we have a set of lines in $\mathcal{P}$ such that no proper subset of a line is in $\mathcal{C}_{\mathcal{L}_0}$. Let this new set of lines be $\mathcal{L}$ (this is not uniquely defined). $(\mathcal{P}, \mathcal{L})$ satisfies the following properties.

(a) There are at least $n + 1$ lines through every point.

(b) $\mathcal{C}_\mathcal{L} = \mathcal{C}_{\mathcal{L}_0}$.

(c) $\mathcal{C}_\mathcal{L}$ does not contain the characteristic function of a proper non-empty subset of any line in $\mathcal{L}$.

(d) $\mathcal{C}_\mathcal{L}$ is one-dimensional and $\mathcal{P}$ is the support of its generator w.

Claim. Denote by $\mathcal{X} = (\mathcal{P}'', \mathcal{L}'')$ the join of two Steiner designs of the given form. $(\mathcal{P}', \mathcal{L}')$ is isomorphic to $\mathcal{X}$ if and only if $(\mathcal{P}, \mathcal{L})$ is isomorphic to $\mathcal{X}$.
The forward direction of the above is obvious. For the converse, let us show that $(\mathcal{P}, \mathcal{L}) = (\mathcal{P}', \mathcal{L}')$. Since

$$2n + 2 - \frac{2n}{p} = |\mathcal{P}| \leq |\mathcal{P}'| \leq 2n + 2 - \frac{2n}{p},$$

$\mathcal{P} = \mathcal{P}'$.
Note that $(\mathcal{P}, \mathcal{L})$ is a linear space. If we had replaced any line with its partition when going from $\mathcal{L}_0$ to $\mathcal{L}$, then this

would not have been possible. Indeed, if there was a line $\ell \ni x, y$ replaced with ℓ, ℓ' such that $x \in \ell$, $y \in \ell'$, then there would be no line incident on both x and y, contradicting the fact that $(\mathcal{P}, \mathcal{L})$ is a linear space. More generally, this implies that if we apply the partitioning process described above, then the second PLS being a linear space implies that both PLSes are equal.
Therefore, $(\mathcal{P}, \mathcal{L})$ is isomorphic to $(\mathcal{P}', \mathcal{L}')$. $\square$

For the rest of the proof, we work with this PLS.
For each $P \in \mathcal{P}$, let x_P, y_P, z_P be number of lines through P of cardinalities $2, 3, 4$ respectively. Fix $Q \in \mathcal{P}$ of minimal x_Q. Now, colour $\mathcal{P}$ with $\mathbb{F}_p$, by colouring each point P as w_P (the Pth coordinate). Assume that Q is coloured -1. Since any line is in the dual of $\langle w \rangle$, the sum of colours on any line is 0 modulo p.
By property (c), the colours of any non-empty proper subset of a line do not add to 0 modulo p.
Therefore, the lines of size 2 are precisely those that have colours α and $-\alpha$ (for some $\alpha \in \mathbb{F}_p^\times$) and any monochromatic line has length p.
Let $\mathcal{S}$ be the set of all used colours (all the values in $\mathbb{F}_p$ that are equal to some w_P). Further, $0 \notin \mathcal{S}$ since $w_P \neq 0$ for any $P \in \mathcal{P}$. Then, letting S_P be the set of all points that are on a line passing through P, we can use the fact that there is at most one line passing through a pair of distinct points to conclude that

$$1 + x_P + 2y_P + 3z_P + 4(n + 1 - x_P - y_P - z_P) \leq |S_P| \leq 2n + 2 - \frac{2n}{p},$$

so

$$2n + 3 + \frac{2n}{p} \leq 3x_P + 2y_P + z_P. \tag{1.1}$$

Similarly, applying this to only x_P and y_P, we get

$$n + 2 + \frac{2n}{p} \leq 2x_P + y_P. \tag{1.2}$$

Let $\ell_1, \ell_2, \ldots, \ell_m$ be all the lines through P of cardinality at least 4. Then,

$$|S_A| \geq 1 + x_P + 2(n + 1 - x_P - m) + \sum_{i=1}^{m} (|\ell_i| - 1)$$

and so,

$$x_P \geq 1 + \frac{2n}{p} + \sum_{i=1}^{m} (|\ell_i| - 3) \geq 1 + \frac{2n}{p}. \tag{1.3}$$

Since the number of size 2 lines through any point is at least x_Q, for any $\alpha \in \mathcal{S}$, there are at least x_Q points of colour $-\alpha$. Because $x_Q > 0$ by Equation (1.3), this implies that $\alpha \in \mathcal{S}$ iff $-\alpha \in \mathcal{S}$, and this together with $0 \notin \mathcal{S}$ implies that $|\mathcal{S}|$ is even, say $2r$ for some $0 < r \leq (p-1)/2$. As there are at least x_Q points of any colour $\alpha \in \mathcal{S}$,

$$r x_Q \leq n + 1 - \frac{n}{p}. \tag{1.4}$$

This together with the previous equation yields that

$$r \leq \frac{n + 1 - n/p}{1 + 2n/p} < \frac{p-1}{2},$$

where the second inequality uses the fact that $p \geq 3$. Therefore, $|\mathcal{S}| < p - 1$.

Claim. If $r = 1$, then $|\mathcal{P}| = 2n + 2 - 2n/p$ and $(\mathcal{P}, \mathcal{L})$ is isomorphic to the join of two Steiner 2-designs of the described form.
As $r = 1$, $\mathcal{S} = \{-1, 1\}$ and any line is of size either 2 or p. Let X_i be the number of points of colour i for $i \in \mathcal{S}$. Since the number of size 2 lines through any P of colour i is at most $|X_{-i}|$, $|x_Q| \leq n + 1 - n/p$. Consequently, letting S_Q be all the points that are on a line through Q,

$$2n + 2 - \frac{2n}{p} \geq |S_Q| \geq 1 + \underbrace{(p-1)\frac{n}{p}}_{p\text{-lines through } Q} + \underbrace{\left(n + 1 - \frac{n}{p}\right)}_{2\text{-lines through } Q} = 2n + 2 - \frac{2n}{p},$$

so $x_Q = n + 1 - n/p$, there are precisely n/p lines through Q, and $|S_Q| = 2n + 2 - 2n/p$. This implies that $|X_1| = |X_{-1}| = n + 1 - n/p$, and so that the number of size 2 lines (resp. size p lines) through any A is exactly $n + 1 - n/p$ (resp. n/p).
Each of the two X_is is isomorphic to a Steiner 2-design with n/p lines through each point and p points on each line, so $(\mathcal{P}, \mathcal{L})$ is isomorphic to the join of two Steiner 2-designs of the prescribed form. $\square$

Now, consider the case where $r \geq 2$. We shall show that this situation cannot occur at all.
Consider the graph G_Q with vertex set $\mathcal{S}$ where α, β are adjacent iff $\alpha + \beta$ is equal to 0 or 1 (in $\mathbb{F}_p$). Note that for any $\alpha \in \mathcal{S}$ of degree 1 and 3-line L through Q, $L \cap X_\alpha$ is either empty or equal to $\{Q\}$ (in the case where $\alpha = -1$). In particular, the degree of 1 in G_Q is one so no 3-line passes through a point of colour 1.

Claim. G_Q is acyclic.
The only possible loop (edge from a vertex to itself) is at $(p+1)/2$. Consider a cycle $\alpha_1\alpha_2 \cdots \alpha_m\alpha_1$. m must be even since the two types of edges alternate. This pattern of edges also implies that m is a multiple of $2p$ (consider the sum of all α_i). However, this is not possible since $m \leq |\mathcal{S}| < p - 1$, so G_Q contains no cycles. Any connected component of G_Q is a path, with possibly a loop at one end due to $(p+1)/2$. $\square$

Claim. G_Q is not connected.
Suppose instead that G_Q is connected. By the previous claim, it is then just a path. If 1 is the only vertex of degree one, then this path is equal to $1(-1)2(-2)\cdots(\frac{p-1}{2})(\frac{p+1}{2})$ since there must be a loop at the other end. In this case however, $|\mathcal{S}| = p - 1$, which is not possible. So, there is another $-r \in \mathcal{S}$ of degree one, and the path is of the form $1(-1)2(-2)\cdots r(-r)$ for $1 < r < (p-1)/2$.
Let $T = \mathcal{P} \setminus (\{Q\} \cup X_{-r})$. Since $r > 1$,

$$|T| \leq 2n + 2 - \frac{2n}{p} - (1 + x_Q).$$

Let l be the number of lines through Q of size > 2 that contain at most one point from T. Observe that any size 2 line through Q has exactly one point from T. Counting points in T that lie on lines through Q,

$$|T| \geq 2(n + 1 - x_Q - l) + x_Q.$$

Combining the above two equations,

$$l \geq \frac{n}{p} + \frac{1}{2} > \frac{n}{p}.$$

Let ℓ be such a line. We now use the fact that the sum of colours on a line is 0.
If $\ell \cap T = \varnothing$, then it contains at least $(p-1)/r$ points from X_{-r} and thus at least $(p+r-1)/r$ points in all.
If ℓ does contain one point from T, then the colour of this point is $1 + (|\ell| - 2)r$ modulo p.
If $1 + (|\ell| - 2)r$ is greater than p (as a number), then $|\ell| \geq 2 + (p-1)/r \geq (p+r-1)/r$. Otherwise, we must have that this number is itself in $\mathcal{S}$. Since $|\ell| > 2$, this number is greater than r so must be in $\{p - r, \ldots, p - 1\}$. That is, $1 + (\ell - 2)r \geq p - r$. This yields once more that $|\ell| \geq (p + r - 1)/r$.
Since $r < (p-1)/2$, $|\ell| > 3$. Thus, we can use Equation (1.3) to get that

$$x_Q > 1 + \frac{2n}{p} + \frac{n}{p}\left(\frac{p+r-1}{r} - 3\right) = 1 + \frac{n}{r} - \frac{n}{pr},$$

which contradicts Equation (1.4). $\square$

Thus, suppose that G_Q is disconnected. Let $\mathcal{S}' \subseteq \mathcal{S}$ be the set of all degree one colours. As G_Q is disconnected, $|\mathcal{S}'| \geq 3$.
Consider the set of points in $\mathcal{P} \setminus \{Q\}$ that are on size 3 lines through Q. This set is of size $2y_Q$, and does not intersect any X_α for $\alpha \in \mathcal{S}'$. Therefore,

$$2n + 2 - \frac{2n}{p} \geq 2y_Q + |\mathcal{S}'| x_Q. \tag{1.5}$$

We may then use Equation (1.2) to conclude that $|\mathcal{S}'| < 4$, and is so exactly 3.
Combining Equations (1.2) and (1.5), $x_Q \geq 2 + 6n/p$, and $r = |\mathcal{S}|/2$ is $< p/6$.
G_Q has two connected components of the form

$$1(-1)2(-2)\cdots t(-t)$$

for some $1 \leq t < r$ and

$$\left(\frac{p+1}{2}\right)\left(\frac{p-1}{2}\right)\left(\frac{p+3}{2}\right)\left(\frac{p-3}{2}\right)\cdots\left(\frac{p+1}{2}-(r-t)\right),$$

with the vertices of degree 1 being 1, $-t$ and $\alpha = (p+1)/2 - (r-t)$. Consider

$$T = \{Q\} \cup X_{-t} \cup X_{\alpha} \cup \mathcal{P}_2 \cup \mathcal{P}_3,$$

where $\mathcal{P}_i$ is the set of points in $\mathcal{P} \setminus \{Q\}$ that are on size i lines through Q. We have that

$$|T| \geq 3x_Q + 2y_Q.$$

If every size 4 line through Q intersects $\mathcal{P} \setminus T$,

$$2n + 2 - \frac{2n}{p} \geq z_Q + |T| \geq z_Q + 2y_Q + 3x_Q,$$

which contradicts Equation (1.1). Therefore, there exists a size 4 line ℓ through Q contained in T. Further, since there is at most one line incident on a pair of points, $\ell \subseteq \{Q\} \cup X_{-t} \cup X_{\alpha}$.
If ℓ contains $0 \leq i \leq 3$ points from X_{α}, then the sum of colours of ℓ is $-1 + (-t)(3-i) + \alpha i$. This must be a multiple of p. Substituting each of the values of i, this is one of

$$3t + 1, \quad 2(r+t) + 1, \quad 2r - t, \quad 6(r-t) - 1,$$

none of which can be a multiple of p since $1 \leq t < r < p/6$, completing the proof. ∎

§2. Combinatorial Methods

2.1. Combinatorial Nullstellensatz

The reader is likely familiar with the following famous theorem.

Theorem 2.1 (Hilbert's Nullstellensatz)**.** Let $\mathbb{F}$ be an algebraically closed field and $f, g_1, \ldots, g_m$ be elements of the ring $\mathbb{F}[x_1, \ldots, x_n]$ of polynomials such that f vanishes on all common zeroes of the (g_i). Then, there is an integer k and polynomials $h_1, \ldots, h_m$ in $\mathbb{F}[x_1, \ldots, x_n]$ such that

$$f^k = \sum_{i=1}^{m} g_i h_i.$$

Before we get to the main result of this section which is essentially an interesting form of the above when the g_i take a specific form, we give a lemma related to the size of a 'cube' required to evaluate a polynomial at to determine if it is the 0 polynomial.

Lemma 2.2. Let $P = P(x_1, \ldots, x_n)$ be a polynomial over a field $\mathbb{F}$. Suppose that for each i, $S_i \subseteq \mathbb{F}$ with $|S_i| > \deg_i(P)$. If $P(s_1, \ldots, s_n) = 0$ for all choices of $s_i \in S_i$ for each i, then P is identically 0.

Proof. We prove this by induction on n. When $n = 1$, this is direct as it merely states that a polynomial of degree at most t has at most t zeroes. Suppose that the statement is true for $n - 1$. Let $t_i = \deg_i(P)$ for each i. Write P as a sum

$$P = \sum_{i=0}^{t_i} x_n^i P_i(x_1, \ldots, x_{n-1}),$$

where each P_i is a polynomial with $\deg_j$ bounded above by t_j. Observe that for any fixed tuple $(x_1, \ldots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$, the polynomial obtained from P by substituting the values of $x_1, \ldots, x_{n-1}$ vanishes on S_n, and thus by the $n = 1$ case, is identically zero. Therefore, each P_i vanishes on $S_1 \times \cdots \times S_{n-1}$. Applying the inductive hypothesis, each P_i is thus identically 0, yielding that P is identically 0 and completing the proof. ■

Later in Corollary 2.4, we give a much stronger version of this.

Theorem 2.3 (Combinatorial Nullstellensatz)**.** Let $\mathbb{F}$ be an algebraically closed field and $S_1, \ldots, S_n \subseteq \mathbb{F}$. Define

$$g_i(x_i) = \prod_{s_i \in S_i} (x_i - s_i)$$

for each i. Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ vanish on all common zeroes of the (g_i), that is, $f(s_1, \ldots, s_n) = 0$ if $s_i \in S_i$ for each i. Then, there are polynomials $h_1, \ldots, h_n$ in $\mathbb{F}[x_1, \ldots, x_n]$ such that

$$f = \sum_{i=1}^{m} g_i h_i.$$

and $\deg(h_i) \leq \deg(f) - \deg(g_i)$ for each i.
Moreover, if $f, g_1, \ldots, g_n \in R[x_1, \ldots, x_n]$ for some subring R of $\mathbb{F}$, then there are polynomials $h_i \in R[x_1, \ldots, x_n]$ satisfying the above.

Proof. Let $t_i = |S_i| - 1$ for each i. For each i, write $g(x_i) = x_i^{t_i+1} - g_0(x_i)$ – note that g_0 is a polynomial of degree at most t_i. For each $x_i \in S_i$, we then have

$$x_i^{t_i+1} = g_0(x_i).$$

Now, take the polynomial f and subtract polynomials of the form $h_i g_i$, each of which replaces the higher degree terms of x_i (terms with x_i^r for $r > t_i$) with a lower degree one using the above equation, to get a polynomial f_0. Observe that this polynomial f_0 vanishes on $S_1 \times \cdots \times S_n$, and $\deg_i(f_0) \leq t_i$ for each i. We can then use Lemma 2.2 to conclude that f_0 is identically zero, and thus that f is equal to $\sum_i h_i g_i$, completing the proof. ■

The simple proof above betrays the surprising usefulness of this result.

Corollary 2.4. Let $P = P(x_1, \ldots, x_n)$ be a polynomial over a(n arbitrary) field $\mathbb{F}$. Let $\deg(f) = \sum_i t_i$, and let there exist a $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$ term in the polynomial with non-zero coefficient. Suppose that for each i, $S_i \subseteq \mathbb{F}$ with $|S_i| > t_i$. If $P(s_1, \ldots, s_n) = 0$ for all choices of $s_i \in S_i$ for each i, then P is identically 0.

Proof. Let us assume that $|S_i| = t_i + 1$ for each i.
Suppose that the claim does not hold and let $g_i(x_i) = \prod_{s_i \in S_i}(x_i - s_i)$ for each i. Combinatorial Nullstellensatz then implies that

$$P = \sum_i h_i g_i$$

for polynomials h_i of degree at most $\deg(f) - \deg(g_i)$. Now, any monomial of degree $\deg(f)$ must come from one of the $h_i g_i$. However, any term in these polynomials are divisible by $x_i^{|S_i|} = x_i^{t_i+1}$, which implies that there is no $x_i^{t_i}$ term in P, yielding a contradiction and completing the proof. ■

Now, let us give some examples of the use of combinatorial nullstellensatz.

Proposition 2.5. Let $A = (a_{ij})$ be a $n \times n$ matrix over a field F that has non-zero permanent. Then, for any $b = (b_1, \ldots, b_n) \in F^n$ and family $S_1, \ldots, S_n \subseteq F$ of size at least 2, there exists some $x \in S_1 \times \cdots \times S_n$ such that Ax differs from b at every coordinate.

Proof. The polynomial

$$\prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} x_j - b_j \right)$$

is of degree n and the coefficient of $\prod x_i$ in it is the permanent of A, which is non-zero. The desideratum follows on using Corollary 2.4. ■

Given an undirected graph $G = ([n], E)$, define the graph polynomial

$$f_G(x_1, \ldots, x_n) = \prod_{\substack{ij \in E \\ i<j}} (x_i - x_j).$$

Proposition 2.6. A graph $G = ([n], E)$ is not k-colorable if and only if its graph polynomial lies in the ideal generated by $P_i(x) = x_i^k - 1$ (for $1 \leq i \leq n$).

Proof. Number the kth roots of unity as $z_1, \ldots, z_k$.
If f_G is in the mentioned ideal but G is k-colorable, then it does not vanish at some point where each x_i is a kth root of unity. However, this is a common zero of all the P_i, which contradicts the fact that it is in the given ideal.
On the other hand, if G is not k-colorable, then it vanishes at all common zeros of the P_i. Theorem 2.3 then implies the required. ■

Proposition 2.7. Consider the vertices $\{0, 1\}^n$ of the hypercube in $\mathbb{R}^n$. Let $\{H_i\}_{i=1}^m$ be a set of hyperplanes that cover every vertex except one. Then, $m \geq n$.

Proof. Assume that the uncovered vertex is $\mathbf{0}$. Let the m hyperplanes be given be $\langle a_i, x\rangle + b_i = 0$. Observe that $b_i \neq 0$ for all i. Suppose instead that $m < n$. Consider the polynomial

$$P(x_1, \ldots, x_n) = \prod_{i=1}^{m} b_i \prod_{i=1}^{n}(1 - x_i) - \prod_{i=1}^{m}(\langle a_i, x\rangle + b_i)$$

over $\mathbb{F}_2$.
Because $m < n$, the term in P of maximal degree is $(-1)^n \prod_{i=1}^{n} x_i$ and has non-zero coefficient. By Corollary 2.4, there exist some $\underset{\sim}{z} = z_1, \ldots, z_n \in \mathbb{F}_2^n$ such that $P(\underset{\sim}{z}) \neq 0$. However, if $\underset{\sim}{z} = 0$, the first term cancels out with the second term. If $\underset{\sim}{z} \neq 0$, some $\langle a_i, x\rangle + b_i$ vanishes at $\underset{\sim}{z}$, and $z_i = 1$ for some i so the first term vanishes as well. This is a contradiction, and therefore $m \geq n$. ■

Proposition 2.8. Let p be a prime and $P_i(x_1, \ldots, x_n)$ (for $1 \leq i \leq m$) be polynomials in the ring $\mathbb{F}_p[x_1, \ldots, x_n]$. If $n > \sum_i \deg(P_i)$ and the P_i have a common zero, they have another common zero.

Proof. Let $(c_1, \ldots, c_n)$ be a common zero of the P_i, and suppose that no other common zero exists. Consider the polynomial

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{m}\left(1 - P_i(x_1, \ldots, x_m)^{p-1}\right) - \prod_{i=1}^{n}\left(1 - (x_i - c_i)^{p-1}\right).$$

Observe that f vanishes everywhere! However, the term of maximal degree is $\prod_{i=1}^{n} x_i^{p-1}$ and has non-zero coefficient. This leads to a contradiction on using Corollary 2.4, proving the required. ■

2.2. The Polynomial Method

The issue with combinatorial nullstellensatz is that we need to carefully craft a polynomial of low degree that satisfies the constraints we desire. As a result, it often also gives extremely tight bounds.
However, this crafting is not always easy. Enter the polynomial method. Instead of choosing a specific polynomial, we choose a polynomial of lowest degree that vanishes at the desired points. While this may not give as tight a bound as combinatorial nullstellensatz, it often gives good asymptotic bounds.
The primary premise of the polynomial method is the following.

Lemma 2.9. Suppose $S \subseteq \mathbb{F}^n$ is a finite set and $|S| \leq \binom{n+d}{n}$. Then, there exists a non-trivial polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree at most d such that $S \subseteq Z(f)$. In particular, given a finite set S, there is a polynomial of degree at most $n|S|^{1/n}$ such that $S \subseteq Z(f)$.

Lemma 2.10. Suppose $f \in \mathbb{F}[X_1, \ldots, X_n]$ is a polynomial of degree at most d. Then, for any line ℓ, $|\ell \cap Z(f)| \leq d$ or $\ell \subseteq Z(f)$.

Both the above are reasonably easy to prove.
Further observe that neither of the two above lemmas assert that $\mathbb{F}$ is finite.

2.2.1 The finite Kakeya problem

Let q be a prime power. A set $K \subseteq \mathbb{F}_q^n$ is said to be a *Kakeya set* if for every direction v, there is a line ℓ_v parallel to v that is contained in K. Does there exist some constant c_n (independent of q) such that $|K| \geq c_n q^n$?

Proposition 2.11. Given q, n, any Kakeya set $K \subseteq \mathbb{F}_q^n$ is of size at least $(q/2n)^n$.

Proof. Let K be a Kakeya set of size cq^n. Let f be a polynomial of minimal degree that vanishes over K. By Lemma 2.9, $\deg(f) \leq nqc^{1/n}$. Let us show that $nc^{1/n} \leq 1/2$.
Suppose otherwise. Fix some non-zero $v \in \mathbb{F}_q^n$. By the definition of a Kakeya set, there exists $a \in \mathbb{F}_q^n$ such that $g(t) = f(a_1 + tv_1, \ldots, a_n + tv_n) = 0$ for all $t \in \mathbb{F}_q$. g is a polynomial of degree at most $q/2$ that vanishes at q points of the line. Therefore, g is identically zero. Letting f_H be the homogeneous part of highest degree terms of f, we have that the coefficient $f_H(v)$ of t^k obtained from f_H is zero. Since v is arbitrary, f_H must vanish at all v, so f_H is identically zero. However, this is a contradiction, completing the proof. ■

Interestingly, before this, the best known bound was just around $q^{(n+2)/2}$ with very minor improvements over time. A slightly more sophisticated argument may be performed (with the same basic template), taking into account the multiplicities of zeros, to get a bound of $q^n/2^n$ on the Kakeya set. The smallest known Kakeya set is of size $q^n/2^{n-1} + O(q^{n-1})$, so the problem is basically resolved.

2.2.2 The joints problem

Let $\mathcal{L}$ be a collection of lines in $\mathbb{R}^3$. A *joint* j is a point such that three non-coplanar lines of $\mathcal{L}$ pass through j. Given $|\mathcal{L}| = L$, what is the maximum number of joints the lines can determine?

Refer to this maximum quantity as $j(L)$.
Let $\mathcal{L}$ be a set of lines that attains the $j(L)$ bound, and let f be a non-trivial polynomial of minimal degree that vanishes on the set J of joints. Then, $\deg(f) \leq 3j(L)^{1/3}$.

For every line ℓ, either $|\ell \cap Z(f)| \leq 3j(L)^{1/3}$ or $\ell \cap Z(f)$.
If every line ℓ contains more than $3j(L)^{1/3}$, then every ℓ is contained in $Z(f)$. Therefore, f is identically zero when restricted to any of the lines. Since a joint has three non-coplanar lines through it, we have $\nabla f(p) = 0$ at any joint p. However, in this case,

$$\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = \frac{\partial f}{\partial z}(p) = 0.$$

So, each of the partial derivatives of f is a polynomial that vanishes at every joint. Unless all the partial derivatives are identically zero, this contradicts the minimality of f! But in this case, f is identically zero as well, once again leading to a contradiction.

Therefore, there always exists a line ℓ with at most $3j(L)^{1/3}$ lines. In this case,

$$j(L) \leq 3j(L)^{1/3} + j(L-1) \leq \sum_{k=1}^{L} 3j(k)^{1/3} \leq 3Lj(L)^{1/3}.$$

Therefore,

$$j(L) \leq 3^{3/2} L^{3/2}.$$