PRPL

Amit Rajaraman

Last updated January 27, 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. Coding Theory

Definition 1.10. 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 $\mathcal{C}_q(\mathcal{X}) = \mathbb{F}^{\mathcal{P}}$. We often denote this code as $\mathcal{C}_{\mathcal{X}}$ or $\mathcal{C}_{\mathcal{L}}$ if q is clear from context.

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 1.11 (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 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. Rigidity Theorems on Partial Linear Spaces

Definition 1.12 (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 1.13 (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 1.3. 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 $|\mathcal{P}| \leq 2n+2-2n/p$. We shall show that $|\mathcal{P}| = 2n + 2 - 2n/p$. Denote $\mathcal{C} = \mathcal{C}_p(\mathcal{X})$. Let w be a word of minimum weight in $\mathcal{C}^\top$, and $\mathcal{P}_w$ be the support of w (the set of coordinates where w is nonzero). Let $(\mathcal{P}_w, \mathcal{L}_0)$ be a partial linear space such that $\mathcal{C}_{\mathcal{L}_0}^\top$ is generated by the restriction of w to $\mathcal{P}_w$. Obviously, $\mathcal{C}_{\mathcal{L}_0}$ is non-trivial at p, and a subset ℓ of $\mathcal{P}_w$ 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 $\mathcal{P}_w$ 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). $(\mathcal{P}_w, \mathcal{L}')$ 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 $\mathcal{P}_w$ is the support of its generator w.

For almost all of the remaining part of the proof, we work with this PLS.
For each $P \in \mathcal{P}_w$, let x_P, y_P, z_P be number of lines through P of cardinalities $2, 3, 4$ respectively. Fix $Q \in \mathcal{P}_w$ of minimal x_Q. Now, colour $\mathcal{P}_w$ 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) and $\mathcal{P}_\alpha \subseteq \mathcal{P}_w$ be the set of all points of colour α. Note that $0 \notin \mathcal{S}$ (Why?). Then, letting S_P be the set of all points that are on a line passing through P,

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

so

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

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

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

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

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

and so,

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

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 $-\alpha$. Since $x_Q > 0$, this implies that $\alpha \in \mathcal{S}$ iff $-\alpha \in \mathcal{S}$. Since $0 \notin \mathcal{S}$, this means that $|\mathcal{S}|$ is even, say it is equal to $2r$ for some $0 < r \le (p-1)/2$. Since there are at least x_Q points of any colour $\alpha \in \mathcal{S}$,

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

This together with the previous equation yields that

$$r \le \frac{n+1-n/p}{1+2n/p} < (p-1)/2,$$

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

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.
First, let us consider the case where $r = 1$. Then, $\mathcal{S} = \{-1, 1\}$ 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,

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

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 $(\mathcal{P}_w, \mathcal{L}')$ is isomorphic to the join of two Steiner 2-designs of the prescribed form.

Note that $(\mathcal{P}_w, \mathcal{L}')$ is then a linear space. If we had replaced a line with its partition in $(\mathcal{P}_w, \mathcal{L}_0)$, this would not have been possible. Further, since $2n + 2 - 2n/p \leq |\mathcal{P}_w| \leq |\mathcal{P}| \leq 2n + 2 - 2n/p$, $\mathcal{P}_w = \mathcal{P}$. Therefore, $(\mathcal{P}_w, \mathcal{L}')$ is our original PLS $(\mathcal{P}, \mathcal{L})$. □

Now, consider the case where $r \geq 2$. We must 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 if there is a 3-line L through Q and $\alpha \in \mathcal{S}$ of degree 1, then $L \cap X_\alpha$ is either empty or equal to $\{Q\}$ (in then 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.

The only possible loop (edge from a vertex to itself) occurs at $(p+1)/2$ if it belongs to $\mathcal{S}$. 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 $(p+1)/2$.

Claim. G_Q is not connected.

Suppose instead that G_Q is connected. It is then just a path. If 1 is the only vertex of degree one, then this path is equal to $1(-1)2(-2)\cdots(\frac{p-1}{2})(\frac{p+1}{2})(\frac{p+1}{2})$ 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 $1 < r < (p-1)$.

Let $T = \mathcal{P}_w \setminus (\{Q\} \cup X_{-r})$. 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. Note that any size 2 line through Q is such a line. Counting points in T that lie on lines through Q,

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

Therefore,

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

Let ℓ be such a line. We now use the fact that the sum of colours on a line is 0.

If ℓ does not contain any point from T, 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 this is greater than p (as a number), then $|\ell| \geq 2 + (p-1)/r \geq (p+r-1)/r$. If this is less than p, then 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). □

Thus, suppose that G_Q is disconnected. Let $\mathcal{S}' \subseteq \mathcal{S}$ be the set of all degree one colours. Since G_Q is disconnected, $|\mathcal{S}'| \geq 3$.
Consider the set of points in $\mathcal{P}_w \setminus \{Q\}$ that are on size 3 lines through Q. This set is of size $2y_Q$. Note that this set 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

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

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 $\mathcal{P}_w \setminus \{Q\}$ that are on size i lines through Q. We have that

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

If any size 4 line intersects $\mathcal{P}_w \setminus T$,

$$|\mathcal{P}_w| \geq z_Q + |T| \geq z_Q + 2y_Q + 3x_Q,$$

which contradicts Equation (1.1). Therefore, there is a size 4 line ℓ contained in T. By property (c) from earlier, $\ell \subseteq \{Q\} \cup X_{-t} \cup X_\alpha$.
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. ■

1.4. Combinatorial Nullstellensatz

The reader is likely familiar with the following famous theorem.

Theorem 1.4 (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 1.5. Let $P = P(x_1, \ldots, x_n)$ be a polynomial over a(n arbitrary) field $\mathbb{F}$. Suppose that for each i, $S_i \subseteq F$ 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

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

where each P_i is a polynomial with $\deg_j$ bounded above by t_j. Observe that for any fixed tuple $(x_1, \dots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$, the polynomial obtained from P by substituting the values of $x_1, \dots, x_{n-1}$ 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 1.7, we give a much stronger version of this

Theorem 1.6 (Combinatorial Nullstellensatz)**.** Let $\mathbb{F}$ be an algebraically closed field and $S_1, \dots, S_n \subseteq \mathbb{F}$. Define

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

for each i. Let $f \in \mathbb{F}[x_1, \dots, x_n]$ vanish on all common zeroes of the (g_i), that is, $f(s_1, \dots, s_n) = 0$ if $s_i \in S_i$ for each i. Then, there are polynomials $h_1, \dots, h_n$ in $\mathbb{F}[x_1, \dots, x_n]$ 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 $f, g_1, \dots, g_n \in R[x_1, \dots, x_n]$ for some subring R of $\mathbb{F}$, then there are polynomials $h_i \in R[x_1, \dots, x_n]$ 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 1.5 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 1.7. Let $P = P(x_1, \dots, x_n)$ 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, $S_i \subseteq F$ with $|S_i| > t_i$. If $P(s_1, \dots, s_n) = 0$ 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. ■