# Polynomials in Combinatorics Seminar Notes

Aaryan Sukhadia

## 1 Introduction

Suppose we have a combinatorial problem where we have a set $\mathcal{C}$ of combinatorial objects that relate to one another in some way, and we are trying to bound $|\mathcal{C}|$. A slick combinatorial trick we can use is creating an injection:

$$f : \mathcal{C} \to K[\vec{x}]$$

, where $K[\vec{x}]$ is some vector space of polynomials over a field $K$.

From there, we want to show that $f(\mathcal{C})$ is necessarily a linearly independent set. If we can then show that all elements of $f(\mathcal{C})$ must necessarily be of a certain form, we can restrict the dimension of $K[\vec{x}]$, thereby restricting the size of $\mathcal{C}$, using linear independence.

This general method is in the same class as Noga Alon's famous *Combinatorial Nullstellensatz*, and there are a host of similar methods revolving around using polynomials to solve combinatorial problems.
We present a gallery of examples. Though written quite briefly, some of them can take more than an hour to properly understand in detail (or at least, they did for me).

## 2 Point Sets with restricted distances

**Q:.** *How many points can we have in $\mathbb{R}^n$ such that every pairwise distance is in a fixed set $\{a, b\}$?*

**Example 2.0.1.** *In $\mathbb{R}^2$, we can have 5 points with pairwise , arranged in a regular pentagon, as shown in Figure 1:*

To try and generalise to $\mathbb{R}^n$, we might attempt something like the following: denote $x^P$ as the indicator vector of a pair $P \subset [n]$. Note that the entries of each $n$-tuple $x^P$ will all be 0 except

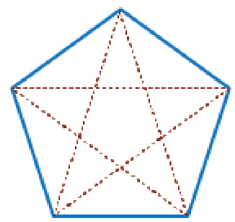

Figure 1: Convince yourself that this Satanic-looking pentagram is the best we can do

for 2 of them. Note that 2 distinct vectors can differ in either 2 or 4 places, and so the distances between them will be either $\sqrt{2}$ or 2.

There are $\binom{n}{2}$ such vectors that can exist, so we know the answer is *at least* quadratic in $n$. We now show that we cannot do much better.

**Theorem 2.0.2.** *We cannot have more than* $\frac{1}{2}(n+1)(n+4)$ *points in* $\mathbb{R}^n$ *with 2 possible pairwise distances.*

Let $S$ be a set of points with 2 possible pairwise distances $a$ or $b$. Then, for any $\vec{s_i}, \vec{s_j} \in S$, we make the following observation:

$$(||\vec{s_i} - \vec{s_j}||^2 - a^2)(||\vec{s_i} - \vec{s_j}||^2 - b^2) = 0$$

For each $\vec{s_i}$, we set up a polynomial as follows:

$$f_i(\vec{x}) = (||\vec{s_i} - \vec{x}||^2 - a^2)(||\vec{s_i} - \vec{x}^2|| - b^2)$$

Note that $f(\vec{x}) = 0 \iff \vec{x}$ is a valid possible point with $\vec{s_i}$. Thus, what we want for $S$ is $\forall i \neq j$, $f_i(\vec{s_j}) = 0$, and observe that $f_i(\vec{s_i}) = (ab)^2$.

Let $|S| = m$. We now show an important result.

**Lemma 2.0.3.** $f_1, f_2 ... f_m$ *are linearly independent in* $K[\vec{x}]$.

*Proof.* Suppose that we had non-trivial linear combination equalling 0: $\sum_{i=0}^{m} \alpha_i f_i = 0$. If we plug in $\vec{s_j}$ into this, we get:

$$\begin{aligned}\sum_{i=0}^{m} \alpha_i f_i(\vec{s_j}) &= \alpha_j f_j(\vec{s_j}) \\ &= \alpha_j a^2 b^2 = 0 \\ \implies \alpha_j = 0\end{aligned}$$

And of course we can do this for any $\vec{s_j}$, and hence we get the polynomials must be linearly independent, proving our lemma. □

We now try and bound the dimension of the subspace in which these polynomials exist.

Let $W := \text{span}(f_1 ... f_m) \subset K[\vec{x}]$. Each $f_i$ is of the form:

$$f_i(\vec{x}) = \big(\sum_{\ell=1}^{n} x_\ell^2 - 2\sum_{\ell=1}^{n} p_i \ell x_\ell + q^2\big)\big(\sum_{k=1}^{n} x_k^2 - 2\sum_{k=1}^{n} p_i k x_k + r^2\big)$$

Letting $X := \sum_{\ell=1}^{n} x_\ell^2$, we get:

$$\big(X - 2\sum_{\ell=1}^{n} p_{i\ell} x_\ell + q^2\big)\big(X - 2\sum_{k=1}^{n} p_{ik} x_k + r^2\big)$$

Thus, $W$ can be generated by the following polynomials:

- $X^2$ - There is 1 such polynomial
- $x_k X, k \in [n]$ - There are $n$ such polynomials
- $x_\ell x_k$, for $k \neq \ell \in [n]$ - There are $\binom{n}{2}$ such polynomials
- $(x_k)^2, k \in [n]$ - There are $n$ such polynomials
- $x_k, k \in [n]$ - There are $n$ such polynomials
- 1 - there is 1 such polynomial

Adding all these generators together, we get that:

$$\begin{aligned}\dim(W) &\leq \binom{n}{2} + 3n + 2 \\ &= \frac{1}{2}(d+1)(d+4)\end{aligned}$$

which was what we wanted to show.

## 3 Medium-Sized Intersections

The field of *extremal set theory* problems asks, given a set and some subset with desired properties, how large can that subset be? We analyse such a problem here.

Let $n = 4p$ for some prime $P$, and let $\mathcal{A} \subset P([n])$ be the set of all subsets of cardinality $2p-1$. We will show that it is somewhat 'hard' to avoid intersections of 'medium' sizes relative to the subsets, that is intersections of size $p-1$.

**Theorem 3.0.1.** *Given a family $\mathcal{F} \subseteq \mathcal{A}$, if $|\mathcal{F}| > \frac{1}{1.1^n}|\mathcal{A}|$, then $\exists A, B \in \mathcal{F}$ such that $|A \cap B| = p-1$*

Suppose we have a family $\mathcal{F}$ without any $A, B$ with intersection size $p-1$. For any $A \in \mathcal{F}$, assign a polynomial $f_A : \mathbb{F}_p^n \to \mathbb{F}_p$ as :

$$f_A(x_1, x_2 ... x_n) = \prod_{s=0}^{p-2} \Big( \sum_{i \in A} x_i - s \Big)$$

Let $\mathbb{1}_A$ be the indicator vector of $A \in \mathcal{F}$. Then we note that $f_A(\mathbb{1}_B) = \prod^{p-2}(|A \cap B| - s)$.
Moreover, note that $f_A(\mathbb{1}_A) = \prod^{p-2}(|A| - s) = \prod^{p-2}(2p-1-s)$. Since every term of this product is non-zero in $\mathbb{F}_p$, the value of $f_A(\mathbb{1}_A) \neq 0$ for all $A \in \mathcal{F}$
Combining those 2 facts, we get:

**Claim.**

$$f_A(\mathbb{1}_B) \neq 0 \iff A = B$$

Thus, using the same logic as in Lemma 2.0.3, we deduce that $\{f_A : A \in \mathcal{F}\}$ are linearly independent polynomials in $\mathbb{F}_P[x]$.

**<u>One more trick:</u>** We make use of the fact that our inputs are all in $\{0,1\}^n$. Given any $f_A$, we create $g_A$ by crossing out the exponents in $f$, i.e replacing any $x_i^k$ by $x_i$. We observe that $g_A(\mathbb{1}_A) = f_A(\mathbb{1}_A) \neq 0$ and for $B \neq A$, $g_A(\mathbb{1}_B) = f_A(\mathbb{1}_B) = 0$. Thus, by the same logic, all the polynomials $\{g_A : A \in \mathcal{F}\}$ are also linearly independent.

Thus, the space $W \subset \mathbb{F}_p[x]$ in which all the polynomials exist is spanned by:

$$W = \text{span}\Big( \{ \prod_{i \in S} x_i : S \subset [n], |S| \leq p-1 \} \Big)$$

We conclude that $\dim(W) = \sum_{k=0}^{p-1} \binom{n}{k}$. Through the power of mathematical behind-the-scenes calculations, we can conclude that $\dim(W) < \left(\frac{2}{3}\right)^{n/4} \binom{4p}{2p-1} < \frac{1}{1.1^n}\mathcal{A}$.

Thus, we conclude that if $\mathcal{F} \geq \frac{1}{1.1^n}|\mathcal{A}|$, no matter the elements of $\mathcal{F}$, there must exist $A, B \in \mathcal{F}$ such that $|A \cap B| = p - 1$.

## 4 Chromatic Number of $\mathbb{R}^n$

**Definition.** A **coloring** of a metric space $X$ is an assignment of a color to each point $x \in X$ such that there are no points with the same color that are distance 1 apart. If we can do this with $k$ colors, we say $X$ is **$k$-colorable**. The **chromatic number** $\chi(X)$ is the minimum $k$ for which $X$ is $k$-colorable

**Q:.** *What is the chromatic number of* $\mathbb{R}^n$*?*

An easy lower bound of $n + 1$ is given by the $n$-simplex, but we can do much better.

**Theorem 4.0.1.** $\chi(\mathbb{R}^n) \geq 1.1^n$

*Proof.* Let $\mathcal{A} = \{A \subset [n] : |A| = 2p - 1\}$.

For every $A \in \mathcal{A}$, let $\vec{x_A} \in \mathbb{R}^n$ be an indicator vector defined as:

$$(\vec{x_A})_i = \begin{cases} \frac{1}{\sqrt{2n}} & \text{if } i \in A \\ -\frac{1}{\sqrt{2n}} & \text{if } i \notin A \end{cases}$$

Note that $\forall A \in \mathcal{A}, ||\vec{x_A}||^2 = \sum_{i=1}^{n} \frac{1}{2n} = \frac{1}{2}$.

For 2 distinct $A, B \in \mathcal{A}$, consider $||\vec{x_A} - \vec{x_B}||^2$. We have the following:

$$||\vec{x_A} - \vec{x_B}||^2 = ||\vec{x_A}||^2 + ||\vec{x_B}||^2 - 2\vec{x_A} \cdot \vec{x_B} = 1 - 2\vec{x_A} \cdot \vec{x_B}$$

Observe that $\vec{x_A} \cdot \vec{x_B}$ would be equal to $\frac{1}{2n}(|A \cap B| + |(A \cup B)'| - |A \Delta B|)$. This arises from the fact that the absolute value of the product of any two coordinates is $\frac{1}{2n}$. If $i$ is in both A and B or in neither $A$ nor $B$, then the product of the $i$th coordinates of the vectors would be positive and if it was in only one of $A$ or $B$ it would be negative.

We know $|A| = |B| = 2p - 1$, and let $s = |A \cap B|$. Then,

$$|A \Delta B| = |A| + |B| - 2|A \cap B| = 4p - 2 - 2s$$

We also see that:

$$|(A \cup B)'| = 4p - (|A \Delta B| + |A \cap B|) = 4p - (4p - 2 - 2s) - s = 2 + s$$

Thus,

$$\begin{aligned} 2\vec{x_A} \cdot \vec{x_B} &= 2(\frac{1}{2n}(s + 2 + s - 4p + 2 + 2s)) \\ &= \frac{1}{n}(4s - 4p + 4) \\ &= \frac{4}{n}(s - (p - 1)) \end{aligned}$$

which is equal to 0 exactly when $s = p - 1$.

Thus, $||\vec{x_A} - \vec{x_B}||^2 = 1 \implies ||\vec{x_A} - \vec{x_B}|| = 1$ when $|A \cap B| = p - 1$.

Going back to our construction, we have a set of points $X$ in $\mathbb{R}^n$ defined by $X = \{\vec{x_A} : A \in \mathcal{A}\}$. Each point in $X$ will have one of $k$ colors. Since $k < 1.1^n$, by the pigeonhole principle there must exist a set $X_F \subset X$ of same-colored points such that $|X_F| > \frac{X}{1.1^n}$. Since there is a bijection between our set of points $X$ and sets in $\mathcal{A}$, the subset $X_F$ corresponds to a subset $\mathcal{F} \subset \mathcal{A}$ such that $|\mathcal{F}| > \frac{|\mathcal{A}|}{1.1^n}$.
Using Theorem 3.0.1, $\exists A, B \in \mathcal{F}$ such that $|A \cap B| = 1$, which implies $||\vec{x_A} - \vec{x_B}|| = 1$, and so there must exist two points of the same color with Euclidean distance 1.

Thus, $\chi(\mathbb{R}^n) \geq 1.1^n$, and so the chromatic number is (at least) exponential in terms of $n$.

□

*Remark.* This remarkably simple technique gives us something pretty close to the forefront of modern combinatorial research, because the best known lower bound is given by $\chi(\mathbb{R}^n) > (1 + o(1))(1.2)^n$, which was shown by Frankl and Wilson in 1981.

## 5 Covering the Hypercube

**Q:.** *How many hyperplanes do we need to cover all but one vertices of the hypercube?*

**Definition.** We define a **canonical hypercube** in $\mathbb{R}^n$ to be the set of points in $\{0,1\}^d$.

We aim to cover every vertex of the canonical hypercube except for the origin. Recall a hyperplane in $\mathbb{R}^n$ is a set of vectors $\vec{x}$ satisfying $\sum_{i=1}^n a_i x_i = b$, for some $b \in \mathbb{R}$, and not-all-zero $a_i \in \mathbb{R}$. Note we can always cover all but one vertices using $n$ hyperplanes:

$$\{H_1 := x_1 = 1, H_2 := x_2 = 1, ...H_n := x_n = 1\}$$

We show that this is the best you can do.

**Theorem 5.0.1.** *You always need at least $n$ hyperplanes to cover all but one vertex of the canonical hypercube in $\mathbb{R}^n$.*

*Proof.* Suppose we have $m$ hyperplanes. Each hyperplane $H_i$ can be expressed by the equation $\sum_{j=1}^n a_i j x_j = b_i$. Note that $b_i \neq 0$, otherwise the hyperplane would cover 0, which is not what we want. Thus, we can scale all of them and assume WLOG that $b_i = 1, \forall i$.

Define a function $f : \{0,1\}^n \to \mathbb{R}$ as:

$$f(\vec{x}) = \prod_{i=1}^m \Big(1 - \sum_{j=1}^n a_i j x_J\Big) - \prod_{j=1}^n (1 - x_j)$$

and let this live in the space of such polynomials $V$.

**Observation.** *For any $\vec{x} \in \{0,1\}^n$, $f(\vec{x}) = 0$. As an exercise, verify this.*

We proceed with proof by contradiction. If $m < n$, then we note that $f$ has degree $n$, and moreover the only term in $f$ with degree $n$ is the monomial $(\pm)x_1 x_2 ... x_n$. We can think of $f$ as a linear combination of monomials, and since $f$ is the zero function in this vector space, it follows that $x_1 x_2 ... x_n$ must be expressible as a linear combination of the other terms in $f$. Specifically, it must be a linear combination of monomials of lower degree.

**One more trick... again:** We use the same idea as in the problem of medium-sized intersections. Since $f$ is a function taking inputs in $\{0,1\}^n$, it holds that $x_i^2 = x_i$ for any term, so we can replace each monomial with its exponent-less counterpart.

Thus, $x_1 x_2 ... x_n$ must be a linear combination of monomials of the form:

$$\prod_{i \in I \subset [n]} x_i, \text{ which we denote by } \kappa_I$$

**Claim.** $\{\kappa_I : I \subseteq n\}$ *is a linearly independent set in* $V$*.*

Suppose we had some linear combination:

$$\sum_{I \subseteq [n]} \alpha_I \kappa_I = 0 \tag{1}$$

Let $I*$ be a minimal subset of $[n]$ such that $\alpha_{I*} \neq 0$. Define the vector $\vec{x} \in \{0,1\}^n$ by $x_i = 1$ if $i \in I*$, and 0 otherwise.

The only non-zero term remaining in 1 is the term $\alpha_{I*} \kappa_{I*} = \alpha_{I*} = 0$, which is a contradiction, and we are done.

□

*Remark.* We can generalize this problem to ask how many hyperplanes do we need to cover all-but-one point of the canonical hypercube at least $k$ times each? This was recently solved by Sauermann and Wigderson (who was a former T.A of mine!), showing a tight lower bound of $n + 2k - 3$. The methods used are essentially the same as those discussed in these notes.