DAY 1 PROBLEMS

A GUIDE TO DOING HOMEWORK

Each homework problem falls into one of these four categories:

1. **required:** These are problems that I expect you to work on. Typically, there will be time in class to work on these.
2. **recommended:** These are problems whose statements you should be familiar with. They are helpful to work on if you need more practice with the material.
3. **optional:** These are problems that are related to the material we will cover, but that you do not need to work on! It's fine if you don't even read them.
4. **bonus:** These are problems that are only tangentially related to the material in class, but I think they are fun to think about. Like optional problems, they are completely optional.

A REFRESHER ON TODAY'S RESULTS

Remember that in this class, a field $\mathbb{F}$ is always $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{F}_p$, where p is a prime.

Lemma 1 (The set vanishing lemma)**.** *If $S \subset \mathbb{F}^n$ has size at most $\binom{d+n}{n}$, there is a polynomial of degree d in $\mathbb{F}[X_1, \ldots, X_n]$ that vanishes on S.*

Lemma 2 (The univariate lemma)**.** *A polynomial of degree D in $\mathbb{F}[X]$ has at most D roots.*

Lemma 3 (Vanishing lemma)**.** *If a polynomial of degree D in $\mathbb{F}[X_1, \ldots, X_n]$ vanishes at $D+1$ points on a line in $\mathbb{F}^n$, then it vanishes at all points on that line.*

APPLICATIONS OF THE LEMMAS IN $\mathbb{R}^n$

1. (required) Show that there is a 2-variable polynomial of degree ≤ 2000 that vanishes on a given set of 1 million points in $\mathbb{R}^2$.
2. (required) Show that for any k points in $\mathbb{R}^n$, there is a polynomial of degree at most $\sim \cdot k^{1/n}$ vanishing at all k points.
3. (optional) Show that for any k *lines* in $\mathbb{R}^3$, there is a polynomial of degree at most $\sim k^{1/2}$ that vanishes on all k lines.

The joints problem in $\mathbb{R}^3$

Let $\mathcal{L}$ be a set of lines in $\mathbb{R}^3$. A point p in $\mathbb{R}^3$ is called a joint if p is the intersection points of 3 lines of L that do not all lie in the same plane. (If you know linear algebra, the three lines that meet at p are linearly independent.) What is the maximum number of joints you can form from N lines?

1. (required) Let $\mathcal{L}$ be a collection of N lines, and let $\mathcal{J}$ be the set of joints. Fix $\delta = \frac{|\mathcal{J}|}{2|\mathcal{L}|}$. If a line in $\mathcal{L}$ has fewer than δ joints on it, throw it away. Repeat this process until we have some set $\mathcal{L}' \subset \mathcal{L}$ so that every line in $\mathcal{L}'$ has at least δ joints on it. Let $\mathcal{J}'$ be the new set of joints. Show that $|J'| \geq \frac{|\mathcal{J}|}{2}$ and that $\mathcal{L}'$ is nonempty, i.e. we could not have thrown away all lines of $\mathcal{L}$.

2. (required) Let $g(X, Y, Z)$ be a nonzero polynomial of *minimal* degree vanishing on $\mathcal{J}'$. Show that the degree of g is at most $\sqrt[3]{6} \cdot |\mathcal{J}'|^{1/3}$.

3. (required) Show that g must vanish on every line in $\mathcal{L}'$.

4. (required) The *gradient* of g is a polynomial defined by taking the derivative of g in each coordinate, i.e.

$$\nabla g = \left(\frac{d}{dx}g, \frac{d}{dy}g, \frac{d}{dz}g\right).$$

   A fact from linear algebra tells us that since g vanishes on three linearly independent lines, ∇g also vanishes on those lines. Use this fact to find a contradiction!

The geometry of finite fields

5. (recommended) Draw all lines through the origin in $\left(\mathbb{F}_2\right)^2$, $\left(F_3\right)^2$, and $\left(\mathbb{F}_4\right)^2$.

6. (optional) Try to visualize or draw $\left(\mathbb{F}_2\right)^3$. Can you draw a plane in this space?

7. (bonus) Can you think of the points of $\left(\mathbb{F}_2\right)^n$ as a shape in $\mathbb{R}^n$?

The finite field Nikodym problem

You will need an extra lemma:

Lemma 4 (The zero lemma for $\mathbb{F}_p$)**.** *Suppose $f \in \mathbb{F}_p[X_1, \ldots, X_n]$ has degree at most $p-1$. If f vanishes at every point in $\left(\mathbb{F}_p\right)^n$, then f is the zero polynomial.*

A set N is a *Nikdoym set* in $\left(\mathbb{F}_p\right)^n$ if for every $x \notin N$, there is a line l through x such that $l \setminus \{x\} \subset N$.

1. (optional) Find a Nikodym set in $\left(\mathbb{F}_2\right)^2$.

2. (recommended) Show that if N is a Nikodym set in $\left(\mathbb{F}_p\right)^n$, then

$$|N| \geq \binom{p-2+n}{n}.$$

Day 2 problems

A guide to doing homework

Each homework problem falls into one of these four categories:

1. **required:** These are problems that I expect you to work on. Typically, there will be time in class to work on these.
2. **recommended:** These are problems whose statements you should be familiar with. They are helpful to work on if you need more practice with the material.
3. **optional:** These are problems that are related to the material we will cover, but that you do not need to work on! It's fine if you don't even read them.
4. **bonus:** These are problems that are only tangentially related to the material in class, but I think they are fun to think about. Like optional problems, they are completely optional.

Lines in $\left(\mathbb{F}_p\right)^n$

1. (required) How many points are in $\left(\mathbb{F}_p\right)^n$?
2. (required) If l is a line in $\left(\mathbb{F}_p\right)^n$, how many points are on l?
3. (required) For a fixed point $v \in \left(\mathbb{F}_p\right)^n$, how many lines pass through p?

We can think of lines and directions in $\left(\mathbb{F}_p\right)^n$ like we think of them in $\mathbb{R}^n$. For a fixed point $b \in \left(\mathbb{F}_p\right)^n$, a line in direction b is a line of the form $\{a + tb : t \in \mathbb{F}_p\}$ for some fixed a. Think of a as a point on the line, and b as the direction of the line from a.

The Kakeya conjecture without polynomials

Remember, a set $K \subset \left(\mathbb{F}_p\right)^n$ is called a *Kakeya set* if K contains a line in every direction.

4. (recommended) Pick any line $l \subset \left(\mathbb{F}_p\right)^n$. Show that $K = \left(\mathbb{F}_p\right)^n \setminus l$ is a Kakeya set. What is the size of K?
5. (optional) Let $s \leq p$. Show that for any s lines $l_1, \ldots, l_s$ in $\left(\mathbb{F}_p\right)^n$, their union contains at least $(1/2)ps$ points.
6. (optional) Use the previous problem to conclude that a Kakeya set always has size at least $(1/2)p^2$.

THE KAKEYA CONJECTURE WITH POLYNOMIALS

All problems in this section are required. We will show that the size of every Kakeya set in $\left(\mathbb{F}_p\right)^n$ must be at least $\sim p^n$. Suppose for contradiction that K is a Kakeya set with

$$|K| < \binom{p-1+n}{n}.$$

7. (required) Argue that there is a nonzero polynomial $f \in \mathbb{F}_p[X_1, \ldots, X_n]$ of degree at most $p-1$ that vanishes on K.

8. (required) There is nothing for you to solve here, just make sure you understand it: Let D be the degree of f. Write $f = f_D + g$, where every term of f_D has degree exactly D, and g is a polynomial of degree strictly less than D. This is just separating the max degree terms of f.

9. (required) If f is nonzero, why does f_D have to be nonzero?

10. (required) For any $b \in \left(\mathbb{F}_p\right)^n$, there is some vector a so that the line $a + tb$ is contained in K. Why is the polynomial f restricted to this line a polynomial in one variable?

11. (required) What is the coefficient of X^D in the restriction of f to this line, in terms of f_D and g?

12. (required) Show that $f_D(b) = 0$.

13. (required) Use this to derive a contradiction!

Day 3 problems

A guide to doing homework

Each homework problem falls into one of these four categories:

1. **required:** These are problems that I expect you to work on. Typically, there will be time in class to work on these.
2. **recommended:** These are problems whose statements you should be familiar with. They are helpful to work on if you need more practice with the material.
3. **optional:** These are problems that are related to the material we will cover, but that you do not need to work on! It's fine if you don't even read them.
4. **bonus:** These are problems that are only tangentially related to the material in class, but I think they are fun to think about. Like optional problems, they are completely optional.

The main tool for today is the *Schwartz–Zippel lemma*.

Lemma 5 (Schwartz–Zippel)**.** *Let S be a nonempty subset of a field $\mathbb{F}$. For any polynomial $f \in \mathbb{F}[X_1, \ldots, X_n]$ of degree at most d, the number of roots of f in the set $S^n \subset \mathbb{F}^n$ is at most $d|S|^{n-1}$.*

This has a natural probabilistic formulation.

Lemma 6 (Schwartz–Zippel again)**.** *Let S be a nonempty subset of a field $\mathbb{F}$, and $f \in \mathbb{F}[X_1, \ldots, X_n]$ a polynomial of degree at most d. If we choose $s_1, \ldots, s_n \in S$ uniformly at random, the probability that $f(s_1, \ldots, s_n) = 0$ is at most $d|S|^{-1}$.*

1. (required) Show that the two forms of the Schwartz–Zippel lemma are equivalent.
2. (recommended) Can you prove the Kakeya conjecture using the Schwartz-Zippel lemma?

Polynomial identity testing

Suppose we have some kind of formula for two polynomials that helps us bound their degree and tells us how to evaluate them as functions, but doesn't actually give us their coefficients. How can we efficiently determine if they are equal?

3. (required) Let $f, g \in \mathbb{F}[X_1, \ldots, X_n]$ be two polynomials of degree at most d. Use the Schwartz–Zippel lemma to develop an algorithm that decides if $f = g$ with error probability $\leq 1/2$.
4. (required) Can you modify this algorithm to decide if $f = g$ with error probability $\leq 1/2^m$, where m is any integer?

Multilinear polynomials

The next few problems will help you prove a better bound on the Schwartz–Zippel lemma for *multilinear polynomials*. A polynomial $f \in \mathbb{F}[X_1, \ldots, X_n]$ is *multilinear* if every *variable* has degree 1 in every term. Somewhat informally, there are no exponents that are greater than 1. For example, $X^2 - 2X$ is not a multilinear polynomial, but $XY - 2X$ is.

We will focus on multilinear polynomials over $\mathbb{F}_2$, so the coefficients can only be 0 or 1. Here is the statement: if $f \in \mathbb{F}_2[X_1, \ldots, X_n]$ is a nonzero multilinear polynomial of degree d, then the probability that f evaluates to zero at a random point in $(\mathbb{F}_2)^n$ is at most $1 - 2^{-d}$.

5. (recommended) Show that the statement is equivalent to saying that the number of roots of f in $(\mathbb{F}_2)^n$ is at most $2^n - 2^d$.

6. (recommended) We will prove this by induction on n. Prove the base case $n = 1$.

7. (recommended) For the inductive step, suppose the statement is true for $n - 1$ variables and let f be a nonzero multilinear polynomial in $\mathbb{F}[X_1, \ldots, X_n]$. Since f is nonzero, some variable, say X_1, has to show up somewhere in f. Write $f = X_1 f_1 + g_1$ by collecting the terms that are divisible by X_1. Argue that f_1 and g_1 are multilinear.

8. (recommended) If g_1 is the zero polynomial, use the inductive hypothesis to show that f has at most $2^n - 2^d$ roots.

9. (recommended) If $f_1 + g_1$ is the zero polynomial, show that $f = (X_1 + 1)f_1$. Again, use the inductive hypothesis to show that f has at most $2^n - 2^d$ roots.

10. (recommended) The final case is if g_1 and $f_1 + g_1$ are both nonzero polynomials. Argue that $\vec{a} = (a_1, \ldots, a_n)$ is a root of f if and only if either $a_1 = 0$ and $g_1(\vec{a}) = 0$ OR $a_1 = 1$ AND $(f_1 + g_1)(\vec{a}) = 0$. Again, use the inductive hypothesis to show that f has at most $2^n - 2^d$ roots.

11. Profit!

An application involving graphs and matrices

If you know some graph theory, these problems are **recommended**. If not, they are **optional**.

A *bipartite graph* is a graph whose vertex set can be partitioned into two sets A and B, so that the only edges in the graph are between A and B. A *perfect matching* in a bipartite graph is a set of edges such that every vertex of the graph is contained in EXACTLY one edge of the matching.

12. Show that if G is a bipartite graph that has a perfect matching, then $|A| = |B|$.

Can we guess whether a bipartite graph has a perfect matching? Let G be a bipartite graph with $|A| = |B| = n$. The *incidence matrix* of G is the $n \times n$ matrix M_G defined by

$$M_G(i, j) = \begin{cases} 1, & a_i b_j \text{ is an edge;} \\ 0, & \text{otherwise.} \end{cases}$$

The rows of M_G are indexed by the vertices in A, the columns by the vertices in B, and an entry is equal to 1 if and only if the corresponding vertices form an edge. We need one last definition. The *determinant* of an $n \times n$ matrix M can be expressed using the formula

$$\det(M) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} (-1)^{\mathrm{sgn}(\sigma)} M_{i,\sigma)i)},$$

where σ runs over all permutations of n elements and the sign $\mathrm{sgn}(\sigma)$ is a technical thing. If you think about the formula for the 3×3 determinant, the + and − signs that show up are the signs of the corresponding permutations.

13. Let G be a bipartite graph with $|A| = |B| = n$. Define the matrix $M[X]$ by setting $M_{i,j} = X_{i,j}$ if $M_G(i, j) = 1$, and to 0 otherwise. This is just replacing all the ones in M_G with a variable. Show that $\det(M[X])$ is a nonzero *polynomial* if and only if G has a perfect matching.

How do we find this perfect matching if $\det(M[X])$ is actually a nonzero polynomial?

14. Fix an edge ab in G. Change the ab entry of $M_G[X]$ to be equal to 1. Show that the determinant of this new matrix is a nonzero polynomial if and only if there is a perfect matching containing the edge ab.

The proof of Schwartz–Zippel, if you're interested

Proof. We will prove the probabilistic formulation by induction on n, the number of variables.

The base case $n = 1$ is equivalent to the Fundamental Theorem of Algebra.

For the inductive case, assume that the theorem is true for $(n-1)$–variate polynomials. Let $f \in F[X_1, X_2, \ldots, X_n]$ be a degree d polynomial. We can view f as a polynomial with coefficients $f_i \in F[X_2, \ldots, X_n]$;

$$f(X_1, X_2, \ldots, X_n) = \sum_{i=0}^{d} f_i(X_2, \ldots, X_n) X_1^i. \tag{1}$$

Then $\deg f_i \leq d - i$.

Let t be the largest value of i such that X_1^i appears; i.e. $f_t \neq 0$. Then $\deg f_t \leq d - t$.

Pick random $s_2, \ldots, s_m \in S$. Since f_t is an $(m-1)$-variate polynomial, we have by the induction hypothesis:

$$\mathbb{P}[f_t(s_2, \ldots, s_m) = 0] \leq \frac{d-t}{|S|}. \tag{2}$$

Let B be the event that $f(s_2, \ldots s_m) = 0$, and $\bar{B}$ the event that $f(s_2, \ldots s_m) \neq 0$.

If $f_t(s_2, \ldots, s_m) \neq 0$, then $f(X_1, s_2, \ldots, s_m)$ has degree t (note the variables; we are viewing f as a univariate polynomial with coefficients $f_i(s_2, \ldots, s_m)$).

So:

$$\mathbb{P}[f(s_1, s_2, \ldots, s_m) = 0 \mid f_t(s_2, \ldots, s_m) \neq 0] \leq \frac{t}{|S|}, \tag{3}$$

where the $\mid$ denotes conditional probability:

$$P[A \mid B] = \frac{P[A \cap B]}{P[B]}. \tag{4}$$

Let A be the event that $f(s_1, s_2, \ldots, s_m) = 0$. For our events A and B,

Then:

$$\begin{aligned} \mathbb{P}[f(s_1, s_2, \ldots, s_m) = 0] &= P[A] \\ &= P[A \cap B] + P[A \cap \bar{B}] \\ &= P[A \mid B]P[B] + P[A \mid \bar{B}]P[\bar{B}] \\ &\leq P[B] + P[A \mid \bar{B}] \\ &\leq \frac{d-t}{|S|} + \frac{t}{|S|} \\ &= \frac{d}{|S|}, \end{aligned} \tag{5}$$

nullity

as desired (where $\bar{B}$ denotes the complement of event B). □

Day 4 problems

A guide to doing homework

Each homework problem falls into one of these four categories:

1. **required:** These are problems that I expect you to work on. Typically, there will be time in class to work on these.
2. **recommended:** These are problems whose statements you should be familiar with. They are helpful to work on if you need more practice with the material.
3. **optional:** These are problems that are related to the material we will cover, but that you do not need to work on! It's fine if you don't even read them.
4. **bonus:** These are problems that are only tangentially related to the material in class, but I think they are fun to think about. Like optional problems, they are completely optional.

Today's tool is really a giant hammer: the *Combinatorial Nullstellensatz*.

Theorem 7 (Combinatorial Nullstellensatz)**.** *Suppose $f \in \mathbb{F}[X_1, \cdots, X_n]$ is a polynomial of degree $t = t_1 + \cdots + t_n$ and the term $X_1^{t_1} \cdots X_n^{t_n}$ has nonzero coefficient in f. If $S_1, \cdots, S_n \subset \mathbb{F}$ are sets of size $|S_i| = t_i + 1$, then there exists $s \in S_1 \times \cdots \times S_n$ such that $f(s) \neq 0$.*

An example application

This theorem is incredibly powerful for additive number theory. If $A, B \subseteq \mathbb{F}_p$, define $A + B = \{a + b : a \in A, b \in B\}$. Additive number theorists *love* questions about the size of $A + B$. Here is an example application of the Nullstellensatz.

Theorem 8 (Cauchy–Davenport)**.** *If $A, B \subseteq \mathbb{F}_p$, then*

$$|A + B| \geq \min\big(|A| + |B| - 1, p\big).$$

Proof. We first consider the case $|A| + |B| \leq p + 1$. Suppose for contradiction that $|A + B| \leq |A| + |B| - 2$. Choose a set S so that $A + B \subseteq S$ and $|S| = |A| + |B| - 2$. Define a polynomial $f(X, Y)$ by

$$f(X, Y) = \prod_{s \in S} (X + Y - s).$$

The degree of f is $|S| = |A| + |B| - 2$. To apply the Nullstellensatz, we want to look at the term $X^{|A|-1}Y^{|B|-1}$. Since it is a max degree term, its coefficient will be the binomial coefficient $\binom{|A|+|B|-2}{|A|-1}$. Since $|A| + |B| - 2 \leq p - 1$ by assumption, this is a nonzero coefficient modulo p.

Unfortunately, now we apply the Combinatorial Nullstellensatz with our polynomial f and the set $A \times B \subseteq \left(\mathbb{F}_p\right)^2$. There must be some $a \in A$ and $b \in B$ so that $f(a, b) = 0$, which is of course not possible :(

The case $|A| + |B| \geq p + 2$ is much less interesting. One way to prove the theorem is to choose a subset $A' \subseteq A$ so that $|A'| + |B| = p + 1$, so we can apply the first case to A' and B. Then, $|A' + B| \geq |A'| + |B| - 1 = p$, so it must be all of $\mathbb{F}_p$. Of course $A' + B \subset A + B$, so $A + B$ is also all of $\mathbb{F}_p$. □

Some fundamental applications

Let's prove a modified version of Cauchy–Davenport. Define $A +^* B = \{a + b : a \in A, b \in B, a \neq b\}$. We will show that if $|A| \neq |B|$, then

$$|A +^* B| \geq \min\big(|A| + |B| - 2, p\big).$$

1. (required) Suppose that $|A|+|B| \leq p-2$ but $|A+^*B| \leq |A|+|B|-3$. By the same trick as Cauchy–Davenport, we have a set S containing $A + B$ with $|S| = |A| + |B| - 3$. Construct a polynomial $f(X, Y)$ of degree $|S| + 1$ such that $f(a, b) = 0$ for all $a \in A$ and $b \in B$. (Even when $a = b$!)

2. (required) Find the coefficient of $X^{|A|-1}Y^{|B|-1}$ and argue that it is nonzero.

3. (required) Profit!!

4. (required) Now prove the statement when $|A| + |B| \geq p - 1$.

5. (optional) When $|A| = |B|$, show that

$$|A +^* B| \geq \min\big(|A| + |B| - 3, p\big).$$

Another classical application is to the Chevalley–Warning theorem.

Theorem 9. *Let $f_1, \ldots, f_k$ be polynomials in $\mathbb{F}_p[X_1, \ldots, X_n]$. Suppose $n > \sum_{i=1}^k \deg(f_i)$. If the polynomials have a common root $(c_1, \ldots, c_n)$ in $\left(\mathbb{F}_p\right)^n$, then they have another.*

6. (recommended) We *want* to consider a polynomial like

$$F(X_1, \ldots, X_n) = \prod_{i=1}^{k} \Big(1 - f_i(X_1, \ldots, X_n)^{p-1}\Big).$$

   Show that $F(a_1, \ldots, a_n) = 0$ if and only if the point $(a_1, \ldots, a_n)$ is a root of each f_i. Why can't we just apply the Combinatorial Nullstellensatz and be done?

7. (recommended) Argue that the *number* (in $\mathbb{F}_p$) given by the formula

$$\prod_{i=1}^{n} \prod_{a \in \mathbb{F}_p, a \neq c_i} (c_i - a)$$

   is nonzero.

8. (recommended) What we really need is to find a polynomial of the form

$$G(X_1, \ldots, X_n) = F(X_1, \ldots, X_n) + g(X_1, \ldots, X_n),$$

   so that if $G(a_1, \ldots, a_n) \neq 0$ then $(a_1, \ldots, a_n)$ is a common root of the f_is BUT $G(c_1, \ldots, c_n) \neq 0$. Can you find a good candidate for the "error polynomial" g by using the previous problem?

9. (recommended) Once you find g, finish the proof by applying the Nullstellensatz.

If you like number theory (OPTIONAL)

Theorem 10 (Erdős–Ginzburg–Ziv)**.** *For any prime p and sequence of integers $(a_1, \ldots, a_{2p-1})$, there is a subsequence $(a_{i_1}, \ldots, a_{i_p})$ of length p such that*

$$\sum_{j=i_1}^{i_p} a_{i_j} \equiv 0 \mod p.$$

10. Define two polynomials in $2p-1$ variables over $\mathbb{F}_p$:

$$f_1(X_1, \ldots, X_{2p-1}) = \sum_{i=1}^{2p-1} X_i^{p-1},$$
$$f_2(X_1, \ldots, X_{2p-1}) = \sum_{i=1}^{2p-1} a_i X_i^{p-1}.$$

    Show that f_1 and f_2 are both equal to zero at the point $(0, \ldots, 0)$.

11. Make sure you can apply the Chevalley–Warning theorem to find another common root.

12. How can you find your subsequence of length p from this other common root? (Hint: use the fact that $a^{p-1} \equiv 1 \mod p$ if $a \neq 0$.

If you like geometry (OPTIONAL)

A *hyperplane* in $\mathbb{R}^n$ is a set of the form

$$\Big\{x \in \mathbb{R}^n : \langle x, h\rangle = r\Big\},$$

where h is a fixed vector in $\mathbb{R}^n$ and r is a fixed real number. Think of planes in $\mathbb{R}^3$, where h represents the normal vector and r represents how far you translate it from the origin. How many hyperplanes do we need to cover most of the vertices of the hypercube, $\{0,1\}^n$? Let $H_1, \ldots, H_k$ be hyperplanes that cover all vertices of the cube EXCEPT for the origin, where each hyperplane is parametrized by

$$H_i = \Big\{x \in \mathbb{R}^n : \langle x, h_i\rangle = r_i\Big\},$$

where each $h_i \in \mathbb{R}^n$ and $r_i \in \mathbb{R}$ is fixed. For this application, we will try something a little different to *discover* the right bound for k.

13. This is going to be similar to our proof of Chevalley–Warning. We *want* a polynomial like

$$F_i(X_1, \ldots, X_n) = \prod_{i=1}^{k} \Big(\langle X, h_i\rangle - r_i\Big),$$

    where X is the vector $(X_1, \ldots, X_n)$. We *want* to apply the Nullstellensatz with this polynomial and the set $\{0,1\}^n$. What goes wrong?

14. Again, we need to find an "error polynomial" $g(X_1, \ldots, X_n)$, so that $F + g$ vanishes on *all* vertices of the hypercube. Find it!

15. Now apply the Nullstellensatz to $F + g$. What should the bound on k be to get a contradiction?

IF YOU LIKE GRAPH THEORY (OPTIONAL)

The *degree* of a vertex in a graph is the number of edges adjacent to it. The *average degree* of a graph G with vertex set $\{v_1, \ldots, v_n\}$ is

$$\frac{1}{n} \sum_{i=1}^{n} \deg(v_i).$$

In an ideal world, every vertex of a graph has the same degree. When this happens, we say the graph is *regular*. Also in an ideal world, the degrees of vertices can't deviate too much from the average degree, so you should be able to find a nice regular subgraph on a subset of the vertices.

For a prime p, suppose G is a graph whose average degree is $> 2p - 2$ and the maximum degree of any vertex is $2p - 1$. (This tells us that many degrees are concentrated around $2p - 2$.) Then, G has a subgraph (some subset of vertices and edges) that is p-regular.

16. This is a counting problem: show that G has at most $n(p - 1)$ edges. (Hint: relate it to the average degree.)

17. For each edge $e \in E$, define a variable X_e. We want to choose some edges for our subgraph so that each vertex has either 0 or p of the chosen edges adjacent to it. Convince yourself that we want this.

18. Define a polynomial

$$F = \prod_{v \in V(G)} \left(1 - \left(\sum_{e \in E : v \in e} X_e\right)^{p-1}\right),$$

where the sum is just summing over all the edges corresponding to v. Suppose we evaluate F at a vector that only takes the values 0 and 1. Think of this vector as an indicator vector for a set of edges (the 1s tell you which edges to choose). What is the relationship between the chosen set of edges and the polynomial F?

19. We run into out usual problem: the zero vector is not a root of F. We want to find a non-root that is NOT the zero vector. Find a polynomial g so that $F + g(\vec{0}) = 0$, AND if $(F + g)(\vec{a}) \neq 0$ for some $\vec{a} \in \{0, 1\}^{|E|}$, then the corresponding set of edges gives you a p-regular subgraph.