Homework exercises for
Polynomial Method in Combinatorics

1. Consider the map $\gamma\colon \mathbb{R} \to \mathbb{R}^2$ given by
$$\gamma(t) = (t^{17} + t^5 + 3, t^{14} + t^9 - 7t^2 - 1).$$
Prove that there is some non-zero polynomial $P(x, y)$ so that image of γ is contained in the zero-set of P. Can you give some estimate for the degree of P?

2. Show that for any N lines in $\mathbb{R}^3$, there is some non-zero polynomial of degree $O(N^{1/2})$ that vanishes on all lines.

   State and prove a similar result for k-planes in $\mathbb{R}^n$ for any dimensions $k \leq n$.

3. (Schwarz–Zippel lemma) Let $A_i \subset \mathbb{F}$ be finite subsets with $|A_i| = N$ for each $i = 1, \ldots, n$. Let P be a non-zero polynomial over $\mathbb{F}$ on n variables and total degree at most D. Show that the number of zeros of P in $A_1 \times \cdots \times A_n$ is at most DN^{n-1}.

   In particular, a nonzero polynomial of degree D vanishes on at most $D/|\mathbb{F}|$ fraction of points of $\mathbb{F}^n$.

4. (Joints problem in higher dimensions) Let $\mathcal{L}$ be a set of L lines in $\mathbb{R}^n$. A *joint* of $\mathcal{L}$ is defined to be a point that lies in n lines of $\mathcal{L}$ pointing in linearly-independent directons.

   By extending the argument shown in class, prove that a set of L lines in $\mathbb{R}^n$ determines at most $C_n L^{n/(n-1)}$ joints.

5. (Joints of axis parallel lines/Loomis-Whitney theorem) Let $\mathcal{L}_i$ be a set of L_i lines parallel to the x_i-axis in $\mathbb{R}^n$. Let $\mathcal{L} = \bigcup_i \mathcal{L}_i$. Show that the number of joints in $\mathcal{L}$ is at most $\prod_{i=1}^n L_i^{1/(n-1)}$ (note that there is no extra constant).

   It is a good idea to start with the $n = 3$ case.

6. Let $A, B, C \subset \mathbb{R}$ with $|A| < |B| < |C|$. Let $P(x, y, z) = \prod_{a \in A}(x - a)$. Prove that P is a minimum degree polynomial that vanishes on the grid $A \times B \times C$, and furthermore every minimum degree polynoial vanishing on the grid is a multiple of P.

   This example illustrates how the minimum degree polynomial picks up the most important lines in the proof of the joints problem.

   What happens when $|A| = |B| = |C|$?

7. Complete the proof of Wolff's hairbrush method bound: if $\ell_1, \ldots, \ell_M$ are lines in $\mathbb{F}_q$, and suppose that at most $q + 1$ of the lines lie in any plane, then their union has cardinality $\gtrsim q^{3/2} M^{1/2}$ (in particular this implies that if $K \subset \mathbb{F}_q^n$ is a Kakeya set, then $|K| \geq (1/2)|q|^{(n+2)/2}$).

The proof uses the *hairbrush method*. A *hairbrush* is a set of lines ℓ_j meeting a fixed ℓ_i (but not including ℓ_i itself). Show there exists a hairbrush containing $(1/2)q^2M/|X|$ lines.

8. Verify the following properties of the Hermitian variety $H : x^{p+1}+y^{p+1}+z^{p+1}=1$ in $\mathbb{F}_q^3$ with $q=p^2$:

   (a) H contains $\Theta(q^{5/2})$ points

   (b) H contains $\Theta(q^2)$ lines, with at most $O(q^{1/2})$ lines in every 2-plane.

   Also, show that the following analogue of the unitary group on $\mathbb{F}_q^n$ acts transitively on H:

   $$U(\mathbb{F}_q^n) := \{g \in \mathrm{GL}(\mathbb{F}_q^n) : \langle v, w\rangle = \langle gv, g\rangle \text{ for all } v, w \in \mathbb{F}_q^n\},$$

   where the inner product is defined by

   $$\langle v, w\rangle := v_1\overline{w_1} + v_2\overline{w_2} + v_3\overline{w_3}$$

   where $\overline{x} := x^p$ is conjugation in $\mathbb{F}_q$.

9. (Heisenberg surface [Mockenhaupt–Tao]) Let p be a prime. Let $X \subset \mathbb{F}_{p^2}^3$ be the surface defined by the equation $x - x^p + yz^p - zy^p = 0$. Show that X is a set of $\Theta(p^5)$ points, and contains p^4 lines, with no more than p lying on any plane.

10. Let $Q \subset \mathbb{F}_q^4$ be the degree 2 hypersurface defined by the equation $x_1^2 + x_2^2 - x_3^2 - x_4^2 = 1$. Prove that each point $x \in Q$ lies in $\Theta(q)$ lines in Q, and all of these lines lie in a 3-plane. Furthermore, check that Q contains $\Theta(q^3)$ points and $\Theta(q^3)$ lines.

11. Let W be a subspace of functions $\mathbb{F}^n \to \mathbb{F}$ that satisfies the degree D vanishing lemma, i.e., whenever $f \in W$ vanishes at $D+1$ points on a line, then f vanishes at every point on the line.

    Show that if $|\mathbb{F}| \geq D+1$, then $\dim W \leq (D+1)^n$.

    (Open) What is the maximum possible $\dim W$ (as a function of n and D)?

12. Prove the divisibility lemma: if $P(x,y)$ and $Q(x)$ are polynomials such that $P(x,Q(x))$ is the zero polynomial, then $P(x,y) = (y-Q(x))S(x,y)$ for some polynomial $S(x,y)$.

13. Let $D < q$. Show that for any function $g\colon \{0,\dots,D\}^n \to \mathbb{F}_q$, there is a unique polynomial $P\colon \mathbb{F}_q^n \to \mathbb{F}_q$ so that $P = g$ on $\{0,\dots,D\}^n$ and P has degree at most D in every single variable.

14. Let $N \subset \mathbb{F}_q^n$ be a Nikodym set, i.e., for every $x \in \mathbb{F}_q^n$, there is a line $\ell \ni x$ with $\ell \setminus \{x\} \subset N$. Let $P\colon \mathbb{F}_q^n \to \mathbb{F}_q$ be a polynomial of degree at most $D < (q-1)/n$ in each variable. Show that if we know P on a Nikodym set N, then we can recover P everywhere. Combine this observation with the previous exercise to show that $|N| \geq c_n q^n$.

15. Show that the following two versions of Szemerdi–Trotter theorem are equivalent:

    - The number of incidences between any S points and L lines in the plane is $O(S^{2/3}L^{2/3} + S + L)$
    - The number of r-rich points among any L lines in the plane is $O(L^2/r^3 + L/r)$

16. Show that the $O(L^2/r^3+L/r)$ bound on the number of r-rich points cannot be improved by verifying the construction suggested in lecture: the $N \times N$ square grid of points and r different slopes with rational coordinates of small numerators and denominators.

17. (Harnack inequality) Show that if $P(x, y)$ is a nonzero polynomial of degree D in two variables, then $\mathbb{R}^2 \setminus Z(P)$ contains $O(D^2)$ connected components.

    Hint: Use Bezout's theorem to bound the number of "unbounded regions" by considering intersections with a large circle. For bounded regions, note that P must contain a critical point (either a maximum or a minimum) in each bounded region. Analyze the number of critical points of $P(x, y)$ (where both partial derivatives vanish) using Bezout's theorem. (Be careful if the two partial derivatives share a common factor, in which case you can perturb P slightly to remove this issue.)

18. Prove the ham sandwich theorem using the Borsuk–Ulam theorem, stated below.

    Borsuk–Ulam theorem: If $\phi\colon S^N \to \mathbb{R}^N$ is continuous and antipodal (i.e., $\phi(-x) = -\phi(x)$ for all x), then the image of ϕ contains the origin.

19. (Unit distance problem)

    (a) Prove that the number of incidences between N unit circles and S points in the plane is $O(N^{2/3}S^{2/3} + N + S)$. (Hint: use polynomial partitioning)

    (b) As a corollary, show that a set of N points in the plane determines $O(N^{4/3})$ unit distances. (This is currently the best known bound on the unit distance problem. The truth is conjectured to be $N^{1+o(1)}$.)

    (c) Construct a set of N parabolas of the form $y = (x - a)^2 + b$ and N points in the plane so that the number of incidences is $\Theta(N^{4/3})$. This example shows that it is hard to improve the bound on the unit distance problem as it is difficult to distinguish between unit circles and unit parabolas.

20. (a) Prove that the number of incidences between N circles and S points in the plane is $O(S^3 + N)$ (this is an "easy bound").

    (b) Use polynomial partitioning to improve the bound estimate to $O(S^{3/5}N^{4/5} + N + S))$

(c) As a corollary, show that the number of r-rich points is $O(N^2 r^{-5/2})$ (points that are contained in $\geq r$ circles).

21. Let P be a set of N points in the plane with ϵN distinct distances. Show that P has an r-rich partial symmetry with $r \geq e^{c\epsilon^{-1}}$ for some $c > 0$.

22. (The square grid example)

    (a) Let G_0 denote the set of points in $\mathbb{R}^3$ of the form $(a, b, 0)$ with a, b positive integers up to $L^{1/4}$, and G_1 the set of points $(a, b, 1)$ with a, b in the same range. Let $\mathcal{L}$ be the set of lines containing one point of G_0 and one point of G_1. Show that the number of r-rich points in $\mathcal{L}$ is $\gtrsim L^{3/2} r^{-2}$ for all $2 \leq r \leq (1/400) L^{1/2}$.

    (b) Let P be a square grid of N points in the plane. Show that the number of r-rich partial symmetries of P is $\Theta(N^3 r^{-2})$ for all $2 \leq r \leq N/400$.

23. Let $\mathbb{F}$ be an infinite field. Let $N \geq \binom{n+d}{d}$. Prove that there exists a set of N points in $\mathbb{F}^n$ with degree greater than D.