The Polynomial Method, Fall 2012, Problem Set 2

1. Go back to the summaries you made for the proofs of the main examples of the polynomial method we saw in the first chunk of the class: the Berlekamp-Welch algorithm, finite field Nikodym and Kakeya, and the joints problem. Just using the summary, try to reconstruct the proof. (If you think you can do it without looking at your summary, that's great too.) You don't have to turn anything in. If you find a tricky point that you hadn't noticed the first time you learned the proof, you can mention it.

2. Give a short summary of the proof of the crossing number theorem and the Szemerédi-Trotter theorem. The summary should be shorter than the whole proof. Since these proofs are already pretty short, probably 1-3 sentences is a good length for each summary. But you should try to include whatever seems to you to be the most essential points and/or the points that you would be most likely to forget. You might imagine that in a few weeks, you would try to reconstruct the proofs just based on these outlines. What is the key information that you should record for yourself?

3. Incidence theory for circles in the plane. Suppose we have L circles in the plane. We let P_k be the set of points that lie in $\geq k$ circles, and we let $N = |P_k|$. How big can N be in terms of L and k?

a. First, just use the fact that two circles intersect in ≤ 2 points. Using this, prove that $N \lesssim L^2 k^{-2}$. Also, if $k > 10L^{2/3}$, prove that $N \lesssim Lk^{-1}$. If $k > 10L^{2/3}$ show that this upper bound is sharp up to a constant factor.

b. Consider the set of all circles in $\mathbb{F}_q^2$. In this context, a circle is defined to be the set of solutions (x, y) of an equation of the form $(x-a)^2+(y-b)^2 = c$ with $c \neq 0$. Prove that any two circles intersect in ≤ 2 points. You can assume that the polynomial $(x-a)^2+(y-b)^2-c$ is irreducible. Check that the set of all circles has $L \sim q^3$ circles, and that each point of $\mathbb{F}_q^2$ lies in $\gtrsim q^2$ of the circles. In this case, we have $k \sim L^{2/3}$ and $N \sim L^{2/3} \sim L^2 k^{-2}$. You don't have to write details.

c. Now introduce the crossing number theorem and try to prove a better estimate. Initially, let's assume that the centers of the L circles are all distinct. We may as well also assume that $k \leq 10L^{2/3}$, because

of part a. Under these assumptions, prove that $N \lesssim L^2 k^{-2-\epsilon}$ for some $\epsilon > 0$. What's the best ϵ you can prove?

d. (extra credit) Remove the assumption that the centers of the circles are distinct.

4. Let $\mathfrak{L}$ be a set of L lines in $\mathbb{R}^3$ with $\leq B$ lines in any plane or degree 2 surface. Prove that the number of intersection points of $\mathfrak{L}$ is $\lesssim L^{2-\epsilon} + LB$ for some $\epsilon > 0$. I have in mind to do this using reguli. What value of ϵ do you get? If it's helpful, you can assume that each point lies in ≤ 2 lines of $\mathfrak{L}$.

5. The Zarankiewicz problem. Consider an $M \times N$ 0-1 matrix with no $V \times W$ minor of all 1's. By the Kővári-Sós-Turán theorem, the number of 1's in the matrix is at most $C_V W^{1/V} M N^{1-(1/V)}$. In this problem we investigate examples. The two main sources of examples are algebraic and random.

a. Polynomials over finite fields. Let $s \geq 1$. Using graphs of polynomials over $\mathbb{F}_q$ instead of lines, give an example of a 0-1 matrix with dimensions $N^{s/2} \times N$, with no $2 \times s$ minor of all 1's, and with $N^{(s+1)/2}$ 1's in it. (You should give examples for an infinite sequence of $N \to \infty$.)

b. Random construction. Start wih a random $N \times N$ matrix where each entry is 1 with probability p. Determine/estimate the expected number of $V \times V$ minors of all 1's. By editing a random matrix, prove that there exist $N \times N$ matrices with no $V \times V$ minor of all 1's and with $\sim N^{2-\frac{2}{V+1}}$ 1's.

c. (for your reference) Brown's example. W. G. Brown gave an example of $N \times N$ 0-1 matrices with no 3×3 minor of all 1's and with $\gtrsim N^{5/3}$ 1's. I was originally planning to have you find the example with some hints, but it's more complicated than I realized so I decided it wasn't a good problem. The trickiest/cleverest part is in a different direction from the issues we're studying in the course. You can read about it in Brown's paper "On graphs that do not contain a Thomsen graph" (Canad. Math. Bull. 9 1966 281-285). Here is an outline for anyone who's curious.

We let p be a prime, and consider "spheres" in $\mathbb{F}_p^3$. If $a \in \mathbb{F}_p^3$ and $r \in \mathbb{F}_p$, we let $S_r(a)$ be the set of solutions to the equation $(x_1 - a_1)^2 + (x_2 - a_2)^2 + (x_3 - a_3)^2 = r$. We fix r, and consider the incidence matrix of all the spheres $S_r(a)$ with all the points $x \in \mathbb{F}_p^3$. This gives an $N \times N$ 0-1 matrix with $N = p^3$.

i.) For any r, $|S_r(a)| \gtrsim p^2$. In fact it's always $\geq p^2 - p$. Therefore, the number of 1's in the incidence matrix is $\gtrsim N^{5/3}$. If the intersection of any three distinct spheres $S_r(a) \cap S_r(b) \cap S_r(c)$ is at most two points, then the incidence matrix contains no 3×3 minor. Notice that this is true for spheres in $\mathbb{R}^3$ with any radius $r > 0$.

ii.) The intersection of any two spheres $S_r(a) \cap S_r(b)$ lies in a plane - their "perpendicular bisector". The intersection of any three distinct spheres $S_r(a) \cap S_r(b) \cap S_r(c)$ lies in a line. The intersection of this line with $S_r(a)$ is ≤ 2 points, *unless the whole line lies in* $S_r(a)$.

iii.) If p is congruent to 1 mod 4, then S_r contains a line if and only if r is a quadratic residue in $\mathbb{F}_p$. This last part is fiendishly clever. In conclusion, if $p = 1$ mod 4, and r is a quadratic non-residue, then the incidence matrix has no 3×3 minor of all 1's.

6. Degree reduction in four dimensions. Suppose that γ_i are lines in $\mathbb{F}_q^4$. Let $X = \cup_i \gamma_i$. Suppose that each point of X lies in ≥ 2 lines γ_i. We suppose that X is only a small fraction of $\mathbb{F}_q^4$, and try to understand the possible structure of X.

a. With just a counting argument, prove that $|X| \gtrsim q^2$.

In the rest of the problem, you can assume that $|X| > q^{2.01}$ and also that q is sufficiently large.

b. Consider the minimal degree (non-zero) polynomial P that vanishes on X. By pure dimension-counting, note that $degP \lesssim |X|^{1/4}$. Using degree reduction, prove that $degP \lesssim |X|^{1/2} q^{-1}$. For example, if $|X| = q^3$, the simple argument gives $degP \lesssim q^{3/4}$, and the more complicated argument proves that $degP \lesssim q^{1/2}$.

c. Suppose that the polynomial P factors in a non-trivial way as $P = \prod_j P_j$, with P_j irreducible. What does this imply about the structure of X?

d. Assume now that P is irreducible. Let $d := degP$. Prove that there is a polynomial Q with the following properties: Q is not a multiple of P, Q vanishes on X, and $degQ \lesssim |X| q^{-2} d^{-1}$. This is the trickiest part. Hint: compare with our proof of Bezout's theorem.

e. Let $Z = Z(P, Q)$ be the subset of $\mathbb{F}_q^4$ where P and Q vanish. By varying the proof of Bezout's theorem, prove that $|Z| \leq (degP)(degQ) q^2 \lesssim |X|$.

18.S997 The Polynomial Method
Fall 2012