ALGEBRAIC STRUCTURE AND DEGREE REDUCTION

Let $S \subset \mathbb{F}^n$. We define $deg(S)$ to be the minimal degree of a non-zero polynomial that vanishes on S. We have seen that for a finite set S, $deg(S) \leq n|S|^{1/n}$. In fact, we can say something a little sharper. Let $V(d)$ be the vector space of polynomials of degree $\leq d$ in n variables. It has dimension $\binom{d+n}{n}$. If $N < dimV(d)$, then $deg(S) \leq d$. This bound is sharp for generic sets S. (should we prove it?...) If $deg(S)$ is significantly smaller than $|S|^{1/n}$, then it means that S has more algebraic structure than a generic set.

We are going to explore the connection between combinatorial properties of a set S and its algebraic structure. We will see that interesting examples in the kind of incidence geometry questions we have been studying need to have algebraic structure. Once we prove that a set has some algebraic structure, it makes sense to try to use that structure to study the set.

As a warmup, we consider a set of L lines in $\mathbb{F}^3$. It's easy to find a degree L polynomial that vanishes on the L lines, but in fact we can do better.

Proposition 0.1. *For any L lines in $\mathbb{F}^3$, there is a polynomial of degree $\leq 3L^{1/2}$ that vanishes on each line.*

Proof. Let $V(d)$ be the space of polynomials in three variables of degree $\leq d$. The dimension of $V(d)$ is $\binom{d+3}{3} \geq (1/6)d^3$. We will choose the degree d later. We pick $d+1$ points on each of the L lines. If $dimV(d) > (d+1)L$, we can find a non-zero polynomial of degree $\leq d$ that vanishes on all the points. Since it vanishes on $d+1$ points on each line, it will also vanish on all the lines. Therefore, we can find such a polynomial as long as $(1/6)d^3 > (d+1)L$. □

1. Degree reduction

We have seen that the union of any L lines in $\mathbb{F}^3$ has degree $\lesssim L^{1/2}$. Now we consider arrangements of lines with lots of incidences and prove that the the union has much lower degree. This process is called degree reduction.

Proposition 1.1. *Let X be a union of L lines in $\mathbb{F}^3$. Suppose that each line contains $\geq A$ intersection points with other lines. Then the degree of X is $\lesssim L/A$.*

This proposition holds automatically if $A \leq L^{1/2}$, and it becomes interesting when A is significantly larger than $L^{1/2}$. For example, suppose that we have L lines in $\mathbb{R}^3$ with much more than $L^{3/2}$ intersection points. If there are approximately the same number of intersection points on each line, then each line would contain much more

than $L^{1/2}$ intersection points. Then the proposition would imply that the union of the lines has degree much smaller than $L^{1/2}$. The union has some special polynomial structure, and it's reasonable to try to use the polynomial structure to study the lines.

The first proof of the joints theorem used degree reduction. I think of it as one of the main steps/ideas in the polynomial method. This proposition is the first step in the proof of the Elekes-Sharir conjecture on the number of intersection points of a set of lines in $\mathbb{R}^3$. I also think of it as philosophically important in explaining why polynomials are relevant. The combinatorial structure of the problem forces the set of points or lines to have a special algebraic structure - and then it makes sense to use this structure to study the problem. The proof of degree reduction is similar to the proof of finite field Nikodym or other fundamental results. By counting dimensions, we find a low degree polynomial that vanishes on some points of X. Then by using the vanishing lemma, we see that it also has to vanish at other points of X, and eventually we prove that it vanishes on all of X.

We begin with heuristics - with an informal argument that describes the main idea of the proof. Let $\mathfrak{L}$ be our set of lines. Let d be a degree that we will choose later. We randomly choose a subset $\mathfrak{L}_0 \subset \mathfrak{L}$ of size $(1/10)d^2$. By the last proposition, we can find a non-zero degree d polynomial P that vanishes on every line of $\mathfrak{L}_0$.

Now the key point is that there are many incidences between the lines of $\mathfrak{L}_0$ and the other lines of $\mathfrak{L}$. Therefore, our polynomial vanishes at many points on other lines of $\mathfrak{L}$. If we can check that our polynomial vanishes at $d+1$ points on each line of $\mathfrak{L}$, then it vanishes on all the lines of $\mathfrak{L}$. So let's pick a line $l \in \mathfrak{L}$ and try to estimate how many points of l intersect a line of $\mathfrak{L}_0$.

Pick a line $l \in \mathfrak{L}$. It has A intersection points with other lines of $\mathfrak{L}$. Fix one of the intersection points. The probability that this intersection point lies in one of the lines of $\mathfrak{L}_0$ is $\geq (1/10)d^2/L$. Therefore, the expected number of intersection points between l and lines of $\mathfrak{L}_0$ is $E \geq (1/10)Ad^2/L$. We are going to choose d so that $E \geq 100d$. It suffices to choose d so that

$$(1/10)Ad^2/L \geq 100d.$$

Rearranging, it suffices to choose d so that $d \geq 1000LA^{-1}$. We now choose d to be an integer which is $\leq 1001L/A$ and so that $E \geq 100d$. On average, the polynomial P vanishes on $\geq 100d$ points of l. This suggests that it vanishes on $> d$ points of l with high probability. Since l was an arbitrary line of $\mathfrak{L}$, this suggests that P usually vanishes on most of the lines of $\mathfrak{L}$.

To get rigorous estimates, we need a little bit of probability. In particular, we will use the following lemma.

Lemma 1.2. *(Probability lemma) Let S be a set of N elements. Let $X \subset S$ be a random subset where each element of S is included in X independently with probability p. The expected size of X is pN.*

(1) $\mathbb{P}[|X| > 2pN] \leq exp(-\frac{1}{100}pN)$.
(2) $\mathbb{P}[|X| < (1/2)pN] \leq exp(-\frac{1}{100}pN)$.

We will prove the probability lemma at the end. The lemma says that the size of $|X|$ is close to the expected value pN almost all the time. Now we can begin the formal proof of Proposition 1.1. We will use large constants that hopefully make the argument more transparent.

Proof. Let d be a degree which we will choose later. Let p be the number $(1/20)d^2/L$. We form a subset $\mathfrak{L}_0 \subset \mathfrak{L}$ by including each line independently with probability p. With high probability, the size of $\mathfrak{L}_0$ is at most $(1/10)d^2$, and therefore we can find a non-zero polynomial P of degree $\leq d$ that vanishes on the lines of $\mathfrak{L}_0$. (The probability of this step going wrong is at most $exp(-\frac{1}{2000}d^2)$, which we can arrange is always $< 1/100$.)

Fix a line l. It contains $\geq A$ intersection points with other lines of $\mathfrak{L}$. Each of these intersection points has a probability $\geq p$ of lying in a line of $\mathfrak{L}_0 \setminus \{l\}$. These events are independent. The expected number of points of l lying in lines of $\mathfrak{L}_0$ is $E \geq Ap = (1/20)d^2A/L$.

We now choose d in the range $(10^6 - 1)L/A \leq d \leq 10^6 L/A$. An easy calculation shows that $E \geq 10^4 d$.

If l intersects $\mathfrak{L}_0$ in $\geq d+1$ points, then $P = 0$ on l. But by the probability lemma, the probability that l intersects $\mathfrak{L}_0$ in $\leq d$ points is $\leq exp(-\frac{1}{100}E) \leq exp(-100d) \leq exp(-10^7 L/A)$.

If $L/A > 1000 \log L$ then the probaiblity that l contains $\leq d$ intersection points with $\mathfrak{L}_0$ is $< L^{-10}$. In this case, with high probability, $P = 0$ on every line of $\mathfrak{L}$, and we are done. This is the main case.

In the case that L/A is quite small, the proposition is still true but the proof is trickier. We sketch what to do in this minor case. We can arrange that P vanishes on 99% of the lines of $\mathfrak{L}$. Let $\mathfrak{L}' \subset \mathfrak{L}$ be the lines where P doesn't vanish. We have $|\mathfrak{L}'| \leq (1/100)|\mathfrak{L}|$. Each line of $\mathfrak{L}'$ has $\leq d$ intersection points with lines of $\mathfrak{L} \setminus \mathfrak{L}_0$. But it has $\geq A$ intersection points with lines of $\mathfrak{L}$. Now in this case, A is close to L and d is extremely small, so we can assume that each line of $\mathfrak{L}'$ has $\geq (99/100)A$ intersection points with other lines of $\mathfrak{L}'$. Now we can iterate or induct to find a polynomial P' that vanishes on $\mathfrak{L}'$ with degree $d' \leq (1/10)d$, and we're done. □

Here is a related result which is special to finite fields.

Proposition 1.3. *Suppose that $X = \cup_{l \in \mathfrak{L}} l \subset \mathbb{F}_q^3$. If each point of X lies in at least 2 lines of $\mathfrak{L}$, then $degX \lesssim \log q |X| q^{-2}$.*

Before we prove the result, let's discuss the bound. We saw in an early lecture that a non-zero polynomial of degree d vanishes at $\leq dq^2$ points of $\mathbb{F}_q^3$. Therefore, for any set $X \subset \mathbb{F}_q^3$, we have $|X|q^{-2} \leq degX \lesssim |X|^{1/3}$. Sets with degree near the upper bound have no particular algebraic structure. Sets with degree near the lower bound have the most algebraic structure. So this proposition says that unions of lines with ≥ 2 lines through every point are almost as algebraically structured as possible. In fact, we will see that the $\log q$ factor can be removed as long as $|X|q^{-2} \geq \log q$.

As a heuristic, imagine that we also knew that each point of X lies in ≤ 10 lines of $\mathfrak{L}$. Then $|\mathfrak{L}| = L \leq 10|X|/q$. Each line of $\mathfrak{L}$ contains q points of intersection with other lines of $\mathfrak{L}$. In this case, the last proposition implies that $deg(X) \lesssim L/A \sim |X|q^{-2}$. The full proof is a modification of the proof of the last proposition, and the annoying special case at the end seems harder to deal with.

Proof. We form a subset $\mathfrak{L}_1 \subset \mathfrak{L}$ as follows. Suppose that the lines of $\mathfrak{L}$ are put in order, $l_1, l_2, ...$ We go through the list of lines one at a time and decide whether to add each line to $\mathfrak{L}_1$. If a given line contains $\geq q/2$ points which are not in any line already in $\mathfrak{L}_1$, then we add the line to $\mathfrak{L}_1$. Otherwise we don't. Since each line of $\mathfrak{L}_1$ brings $\geq q/2$ new points of X, $|\mathfrak{L}_1| \leq 2|X|q^{-1}$. Every line in $\mathfrak{L} \setminus \mathfrak{L}_1$ intersects lines of $\mathfrak{L}_1$ at $\geq q/2$ distinct points. (Otherwise, we would have added it to $\mathfrak{L}_1$.) We let $L = |\mathfrak{L}_1| \sim |X|/q$.

We let d be a degree to be chosen later, and as above we let $\mathfrak{L}_0 \subset \mathfrak{L}_1$ be a random subset where each line of $\mathfrak{L}_1$ is included independently with probability $p = (1/20)d^2/L$. With high probability, $|\mathfrak{L}_0| \leq (1/10)d^2$, and we can choose a non-zero polynomial P of degree $\leq d$ so that $P = 0$ on each line of $\mathfrak{L}_0$.

Let's assume for now that $|X|q^{-2} \geq \log q$. Let l be a line of $\mathfrak{L}$ that intersects lines of $\mathfrak{L}_1$ at $\geq A = q/2$ points. Note that every line of $\mathfrak{L}\setminus\mathfrak{L}_1$ has this property. The expected number of intersections between l and lines of $\mathfrak{L}_0$ is $\geq E = Ap = (1/20)d^2A/L$. As in the last proof, we choose E so that $E \geq 10^4 d$. We can do this with a degree $d \sim L/A \sim |X|q^{-2}$. More precisely, we can arrange that d is between $10^5|X|q^{-2}$ and $10^6|X|q^{-2}$, and that $E \geq 10^4 d$. Now the probability that l intersects lines of $\mathfrak{L}_0$ in $\leq d$ places is $\leq exp(-\frac{1}{100}E) \leq exp(-10^7|X|q^{-2}) \leq exp(-10^7 \log q) = q^{-10^7}$. The total number of lines in $\mathbb{F}_q^3$ is $\leq 10q^4$, which is much smaller. So we can arrange that P vanishes on every line l with $\geq q/2$ intersections with lines of $\mathfrak{L}_1$. In particular P vanishes on all the lines of $\mathfrak{L} \setminus \mathfrak{L}_1$. Finally, a line of $\mathfrak{L}_1$ either intersects lines of $\mathfrak{L}_1$ in $\geq q/2$ points, or else it intersects lines of $\mathfrak{L} \setminus \mathfrak{L}_1$ in $\geq q/2$ points. Either way, we conclude that P vanishes on l. To summarize, assuming that $|X|q^{-2} \geq \log q$, we have proven that $deg(X) \leq 10^6|X|q^{-2}$.

Next we turn to the small case, $|X|q^{-2} < \log q$. The argument goes basically the same, but now we need to choose E so that $E \geq 10^4 d$ and $E \geq 10^4 \log q$. The second criterion may be harder in the small case. To arrange it, we need to know that

$(1/20)d^2A/L \geq 10^4 \log q$, and so $d^2 \geq CLA^{-1} \log q = |X|q^{-2} \log q \leq C(\log q)^2$. In this case we can arrange that $d \lesssim \log q$. The rest of the argument goes the same. □

Remark: It would be nice to remove this suspicious $\log q$ factor, and it would also be nice to clean up the proof.

Let's try to list examples of such sets. A plane has this property. A regulus (like $z = xy$) has this property. If X_i are sets with this property then the union of X_i has this property. In particular, unions of planes and reguli have this property. Very large sets also have this property - say the complement of a few points. Of course, the complement of a few points is a union of planes, but I wouldn't be surprised to find sets with $\sim q^3$ points with this property which aren't unions of planes and reguli. Later we will meet a strange example: the Heisenberg group. The Heisenberg group has this property, it has $\sim q^{5/2}$ points, and it is not a union of planes and reguli. I conjecture that a set X with this property and $< (1/100)q^{5/2}$ points is a union of planes and reguli.

2. An Application

Proposition 2.1. *Let $\mathfrak{L} = \{l_i\} i \in I$ be a set of lines in $\mathbb{F}_q^3$. Let $S_i \subset l_i$ be a subset of size $\geq q/2$. Let $X = \cup_i S_i \subset \cup_i l_i = Y$.*

Then $|Y| \leq C(\log q)|X|$.

Remark: As above, the $\log q$ factor appears only if $|X| < (\log q)q^2$. Perhaps it can be removed entirely.

We start with a naive application of the polynomial method. We can find a non-zero polynomial P that vanishes on X with degree $d \lesssim |X|^{1/3}$. If $|X|$ is close to q^3, there is nothing to prove, and so we can assume that $d < q/2$. Now P vanishes on $\geq q/2 > d$ points on each line l_i, so P vanishes on Y. However, this does not give such a good bound for $|Y|$. It only implies that $|Y| \leq C|X|^{1/3}q^2$. For example, if $|X| = q^{5/2}$, we get $|Y| \lesssim q^{17/6}$.

We can do better by a degree reduction argument. We sketch the argument here. It is similar to the last proposition. We make a subset $I_1 \subset I$ as follows. We consider the lines l_i one at a time and decide whether to add $ito I_1$. We add i to I_1 if S_i contains $\geq q/4$ points that aren't already in the union of $\{S_i\}_{i \in I_1}$. At the end $|I_1| = L \leq 4|X|q^{-1}$. Also for each $i \in I \setminus I_1$, S_i intersects the sets in I_1 in $\geq A = q/4$ points.

By the same argument as above, we can find a non-zero polynomial P of degree $d \leq 10^6 \log q |X| q^{-2}$ so that that P vanishes on l_i for each $i \in I \setminus I_1$, and vanishes on l_i for $i \in I_1$ as long as S_i intersects other sets $\{S_i\}_{i \in I}$ for $\geq q/4$ points.

Define $I_{meager} \subset I$ to be the set of i so that S_i intersects other S_i's in $\leq q/4$ points. The polynomial P vanishes on l_i for each $i \in I \setminus I_{meager}$. The union of lines l_i with

$i \in I \setminus I_{meager}$ has size $\leq dq^2 \lesssim \log q|X|$. The size of I_{meager} is $\leq 4|X|q^{-1}$. So the union of the lines in I_{meager} has size $\leq 4|X|$.

3. A Probability Lemma

We recall and prove the probability lemma that we used above.

Lemma 3.1. *(Probability lemma) Let S be a set of N elements. Let $X \subset S$ be a random subset where each element of S is included in X independently with probability p. The expected size of X is pN.*

(1) $\mathbb{P}[|X| > 2pN] \leq exp(-\frac{1}{100}pN)$.
(2) $\mathbb{P}[|X| < (1/2)pN] \leq exp(-\frac{1}{100}pN)$.

Proof. We let a_j be 1 if the j^{th} element of S is included in X and 0 otherwise. The functions a_j are independent, and the probability that $a_j = 1$ is p. Also $|X| = \sum_j a_j$.

Using independence we get the following equation, which holds for any number $\beta \in \mathbb{R}$:

$$\mathbb{E}e^{\beta|X|} = \mathbb{E}\prod_j e^{\beta a_j} = \prod_j \mathbb{E}e^{\beta a_j} = (pe^{\beta} + 1 - p)^N.$$

On the other hand, $\mathbb{P}[|X| > 2pN]\, e^{2\beta pN} \leq \mathbb{E}e^{\beta|X|}$. Combining these equations, we get the following upper bound for the probability that $|X|$ is $> 2pN$:

$$\mathbb{P}[|X| > 2pN] \leq \left[\frac{pe^{\beta} + 1 - p}{e^{2\beta p}}\right]^N.$$

This bound holds for any β. If $\beta > 0$, then the fraction in brackets is < 1. Taking $\beta = 1$, the fraction in brackets is $\leq (1+p(e-1))/(1+2p) \leq exp(-p/100)$. Therefore, inequality 1 holds.

To prove inequality 2, we use a similar argument. We observe that $\mathbb{P}[|X| < (1/2)pN]\, e^{(1/2)\beta pN} \leq \mathbb{E}e^{\beta|X|}$. Thus we get the following upper bound for the probability that $|X|$ is $< (1/2)pN$:

$$\mathbb{P}[|X| < (1/2)pN] \leq \left[\frac{pe^{\beta} + 1 - p}{e^{(1/2)\beta p}}\right]^N.$$

This bound again holds for any β. If β is negative and close to zero, then the expression in brackets is < 1. In particular, if $\beta = -1/10$ then the the expression in brackets is at most

$$\frac{1 - (1/10)p + (2/100)p}{1 - (1/20)p} \leq exp(-p/100).$$

Therefore, inequality 2 holds. □

18.S997 The Polynomial Method
Fall 2012