Lecture 14 Bounds by Counting Dimensions

Lecturer: Anup Rao

1 Multivariate Polynomials

The following lemma generalizes the fact that there is a bijection between univariate polynomials of degree d and their evaluations on $d+1$ points, the case of multivariate polynomials.

Lemma 1. *If $S_1, S_2, \ldots S_n \subset \mathbb{F}$ are all sets of size $d+1$, and P_d is the set of polynomials whose degree in any variable is at most d, then there is a bijection between polynomials $p \in P_d$, their evaluations $\mathbb{F}^{(d+1)^n}$, where the coordinates of the evaluations are indexed by elements of $S_1 \times \cdots \times S_n$, and the coordinate that corresponds to x is $p(x)$.*

Proof We shall show that the map from polynomials to evaluations is a full rank linear transformation. Given any point $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in S_1 \times \cdots \times S_n$, we define the polys $f_i(X_i) = \prod_{\alpha \in S_i, \alpha \neq \alpha_i} \frac{X_i - \alpha}{\alpha_i - \alpha}$. And define $f_\alpha = \prod_i f_i(X_i)$. This is a polynomial whose degree in each variable is at most d, and for $\beta \in S_1 \times \cdots \times S_n$,

$$f_\alpha(\beta) = \begin{cases} 1 & \text{if } \alpha = \beta, \\ 0 & \text{else.} \end{cases}$$

Thus the rank of the evaluation map is full. ■

Last time, we used polynomials to prove the following theorem:

Theorem 2. *If $\mathcal{F}$ is a family of sets such that for all $A \neq B \in \mathcal{F}$, $|A \cap B| \in L$, then $|\mathcal{F}| \leq \sum_{i=0}^{|L|} \binom{n}{i}$.*

Without much additional work, you will prove the following in homework:

Theorem 3. *If $\mathcal{F}$ is a family of sets and p is a prime such that for all $A \neq B \in \mathcal{F}$, $|A \cap B| \in L \mod p$ and $|A| \notin L \mod p$, then $|\mathcal{F}| \leq \sum_{i=0}^{|L|} \binom{n}{i}$.*

2 Ramsey Graphs

An undirected graph on n vertices is called *k-Ramsey* if it does not have an independent set or clique of size k. Note that if a graph is k-Ramsey, then it is also $(k+1)$-Ramsey. How small can k be as a function of the number of vertices n?

In one of the first illustrations of the probabilistic method, Erdős showed the following theorem:

Theorem 4. *A random graph on n vertices is $2\log n$-Ramsey with high probability.*

Proof The probability that any fixed set of size k is a clique or independent set is exactly $2^{-\binom{k}{2}+1}$. Thus, by the union bound, the probability that there is any clique or independent set of size k is at most

$$2^{-\binom{k}{2}+1}\binom{n}{k} \le 2^{-k^2/2+k/2+1}(en/k)^k = 2^{-k^2/2+k/2+1+k\log n-k\log k+k\log e}.$$

When $k = 2\log n$, this is $2^{-2\log n\log\log n+\log n+1+2\log(en)}$, which tends to 0 as n tends to infinity. ■

Can we construct such a graph deterministically with a fast algorithm? Frankl and Wilson gave the following construction based on Fisher's inequalities: For a prime $p > 2$, the vertices of the graph are $\binom{[p^3]}{p^2-1}$ (namely subsets of $[p^3]$) of size p^2-1. There is an edge between A, B if and only if $|A\cap B| = -1 \mod p$.

Theorem 5. *The graph constructed above is k-Ramsey for $k = \sum_{i=0}^{p-1}\binom{p^3}{i}$.*

Proof If there is an independent set S, for $A \ne B \in S$, $|A\cap B| \in \{0,1,2,\dots,p-2\} \mod p$, and further, $|A| = -1 \mod p$. Thus, by Theorem 3, $|S| \le k$.

On the other hand, if S is a clique, then for $A \ne B \in S$, $|A\cap B| \in \{p-1, 2p-1, \dots, p^2-p-1\}$, which is a set of size $p-1$. So by Theorem 2, $|S| \le k$. ■

In the above theorem, $k \le p^{O(p)} = 2^{O(p\log p)}$ and $n = p^{\Omega(p^2)} = 2^{\Omega(p^2\log p)}$. Thus we obtain a k-Ramsey graph with $k \approx 2^{\sqrt{\log n}}$, which is much larger than the $k \approx 2^{\log\log n}$ promised by the probabilistic method. A few years ago, Barak, Rao, Shaltiel and Wigderson improved this to give an algorithm with better performance.

Theorem 6 (BRSW)**.** *There is a polynomial time algorithm that computes the adjacency matrix of a size n graph that is $2^{(\log n)^{o(1)}}$-Ramsey.*

Unfortunately, this algorithm is much more complicated than the construction of Frankl and Wilson.

3 Bounds on Besicovitch Sets

Let $\mathbb{F}$ be a finite field of size q. A set $S \subset \mathbb{F}^n$ is called a Besicovitch set if it contains a line in every direction, i.e. for every $x \in \mathbb{F}^n$, there exists a $y \in \mathbb{F}^n$ such that the line $\{tx + y : t \in \mathbb{F}\} \subseteq S$. How small can such a set be? We give a proof by Dvir.

Theorem 7. $|S| \ge \binom{q-1+n}{n}$.

Proof Fix any such set S with $|S| < \binom{q-1+n}{n}$. Then consider the space of degree $q-1$ polynomials. This is a space of dimension $\binom{q-1+n}{n}$. We claim that there must be a non-zero polynomial g in this space such that g maps every point of S to 0. Indeed, the constraint that $g(x) = 0$ is a linear constraint on the coefficients of g. Since the number of coefficients is more than the number of constraints, there must be some non-zero setting of coefficients that satisfies all constraints[1].

[1] If this argument is not clear, consider the matrix M whose rows correspond to points of S, columns corresponds to coefficients of a polynomial from the space, and the $M_{i,j}$ is the evaluation of the j'th monomial on the i'th element of S. Thus, for a column vector A, the product MA denotes the evaluation of the polynomial that corresponds to the coefficients A at the points of S. Since the number of rows of M is less than the number of columns, the columns are not linearly independent, and so there must be a non-zero A such that $MA = 0$.

Thus, there is a non-zero polynomial g of total degree $d \leq q-1$ such that for fixed x there exists y for which $L = \{t \cdot x + y : t \in \mathbb{F}\}$, $g(L) = 0$. Since $g(t \cdot x + y)$ is a univariate polynomial of degree at most d, and this polynomial has q roots, it must be the 0 polynomial.

Now consider the degree d coefficient of $g(t \cdot x + y)$ (as a univariate polynomial in t). Let g_d be the degree d homogenous part of g. Then the degree d coefficient of $g(t \cdot x + y)$ is exactly $g_d(x)$. Thus $g_d(x) = 0$ for *every* $x \in \mathbb{F}^n$, so by Lemma 1, g_d must be the 0 polynomial, which is a contradiction.

■