Lecture 26

Lecturer: Madhu Sudan *Scribe: Prahladh Harsha*

In this lecture, we shall give a summary of the topics covered as part of this course, look at why we studied them and also mention some of the topics we did not cover in the course.

1 Factorisation

The first 11 lectures of the course were devoted to factorisation. We looked at factorisation of univariate polynomials over finite fields, integers; multivariate polynomial factorisation using Hensel's lifting, black-box factorisation etc.

The explicit motivation for studying factorisation was that it was a non-trivial algorithm achievement. Another motivation for studying factorisation is in the attempt to answer the question:

When is a function $f : F \to F$ (or more generally $f : F^n \to F$) , where F is a field, a degree d polynomial.

In the case of the univariate version of the above question, for the YES instances, the proof that f is a polynomial is the polynomial $p \in F[x]$ itself such that $p(x) = f(x) \forall x \in F$. For the NO instances of the problem, a simple observation tells us that there exist points $x_1, \ldots x_{d+2} \in F$ such that f when restricted to these points is also not a degree d polynomial. The obvious question that then arises in this case is how can one find such a set of $d + 2$ points. There seems to be no "better" way than examining f on all of F. However, we can do better if the function f were to disagree with every degree d polynomial in $F[x]$ in atleast $\epsilon-$fraction of the points in F (and not atleast one point as before). In that case, a set of $d+2$ points can be found easily. In fact, a random set of $d+2$ points will suffice as a counterexample with probability ϵ.

In the multivariate version of the question (ie., $f : F^n \to F$) for the NO instances as before we have that if f does not agree with any polynomial of degree d and $|F| \geq 2(d+2)$, then there exist points $x_1, \ldots x_{d+2} \in F$ such that f when restricted to these points is also not a degree d polynomial. Here again, if we relax our NO instances to functions which disagree on a $\epsilon-$fraction of points with very degree d polynomial instead of disagreement on atleast one point, we can obtain a conterexample set easily by considering f restricted to a random line as follows: Pick $\hat{x}, \hat{y} \in F^n$ at random and look at $f|_{\hat{x}+t\hat{y}}$ and check whether this is a polynomial of degree d in the single variable t. As mentioned in the univariate case, if $f|_{\hat{x}+t\hat{y}}$ were not a polynomial, we can easily find a random set of points $t_1, \ldots t_{d+2}$ such that they serve as a counterexample. Thus the $d+2$ points $\hat{x} + t_1\hat{y} \ldots \hat{x} + t_{d+2}\hat{y}$ in F^n are proof that f is not a degree d polynomial.

Factorisation of bivariate polynomials can be used to find $\epsilon-$close polynomials to a given (univariate) function f in the following manner: Given a function $f : F \to F$ (where F is a finite field of size $|F|$), we can easily find a $Q \in F[x, y]$ of degree less than $\sqrt{|F|}$ such that $Q(x, f(x)) = 0 \forall x \in F$ and Q not identically 0. Suppose Q is of the form $Q(x, y) = \sum q_{ij}x^iy^j$, then we have $(\sqrt{|F|} + 1)^2$ unknown coefficients and $|F|$ constraints of the form $Q(x, f(x)) = 0$. This linear system can be solved to obtain the q_{ij}'s.

Claim 1 *If there exists a degree d polynomial $p \in F[x]$ such that $p(x) = f(x)$ for atleast $2d\sqrt{|F|}$ of the x's in F, then $y - p(x)$ is a factor of $Q(x, y)$. (where $Q(x, y)$ is the polynomial mentioned earlier)*

Proof Let $g(x) = Q(x, p(x))$. g has degree less then $2d\sqrt{|F|}$. But $g(x) = 0$ whenever $p(x) = f(x)$. Hence g has atleast $2d\sqrt{|F|}$ distinct roots. Therefore, $g \equiv 0$. Thus, $y - p(x)$ divides $Q(x, y)$ ■

Thus with the above claim and having obtained Q, we can factorise Q and search for factors of Q of the form $y - p(x)$. Comparing each such p against f, we can find whether f has any close polynomial and find it if there exists one,

A similar procedure can be adopted when we are given a bivariate function $f : F^2 \to F$. In such a case, we find a $Q \in F[x, y, z]$ of degree $|F|^{\frac{2}{3}}$ such that $Q(x, y, f(x, y)) = 0 \forall x, y \in F$, factorise Q and search for factors of the form $z - p(x, y)$.

Some of the topics we did not cover in this area are

- factorisation over $\mathbb{R}$
- factorisation over $\mathbb{C}$ [Neffs]
- factorisation over function fields and number fields [Cohen], [Shokrollahi, Wasserman]
- factorisation of sparse polynomials [Zippel] and interpolation[Borodin, Tiwari], [Ben-Or, Tiwari]

2 Quantifier Elimination

The second main topic covered in the course was Quantifier Elimination (lectures 12-18). Here we looked at the computational complexity of determining the truth value of statements like

$$Q_1 x_1 \dots Q_n x_n (f_1(x_1 \dots x_n) = \dots f_s(x_1 \dots x_n) = 0)$$

where $Q_i \in \{\exists, \forall\}$ and $f_i \in F[x_1, \dots x_n]$. We then looked at functions of the form $Q_1 x_1 \dots Q_n x_n \Phi(x_1, \dots x_n, y_1, \dots y_m)$ (Q_i's being quantifiers) versus functions of the form $\Phi(y_1, \dots y_m)$ (ie., definable functions vs computable functions) and showed how the former could be reduced to the latter under certain settings. A few of the topics we missed out in this part are

- Quantifier Elimination methods over $\mathbb{R}$
- Effective Hilbert's Nullstellensatz
- Bezout's Theorem.

3 Complexity Classes

In the third part of the course (lectures 19-25), we studied the complexity classes over different algebraic domains and looked at various models of algebraic computation .One of the interesting results not covered is:

$$\mathbf{P}^0_{\mathbb{R},+,-,\geq 0} = \mathbf{PAR}^{\mathbf{0}}_{\mathbb{R},+,-,\geq \mathbf{0}} \iff \mathbf{P} = \mathbf{PAR}$$

where **PAR** stands for class of languages recognised by parallel polynomial time algorithms. This result is different in nature from the results presented in class like

$$\mathbf{P} = \mathbf{PSPACE} \Longrightarrow 0/1\mathbf{P}_{\mathbb{C}} = 0/1\mathbf{NP}_{\mathbb{C}}$$

in the sense that it does not restrict the inputs to be boolean for $\mathbf{P}^{\mathbf{0}}_{\mathbb{R},+,-,\geq \mathbf{0}}$ and $\mathbf{PAR}^{\mathbf{0}}_{\mathbb{R},+,-,\geq \mathbf{0}}$.

We also did not study the notion of p-computable and p-definable functions [Valiant] and find in what cases are p-definable functions also p-computable. A function f is a p-computable function if it is a polynomial (possibly multivariate) of degree $n^{O(1)}$ and computable in polynomial time. A function g is p-definable if $g(y_1, \dots y_n) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_m \in \{0,1\}} f(x_1, \dots x_m, y_1, \dots y_n)$ for some p-computable function f.