Soham Chatterjee
Email: soham.chatterjee@tifr.res.in
Course: Algebra, Number Theory and Computation

Assignment - 2
Dept: STCS, TIFR
Date: March 24, 2025

Problem 1 — 15 Points

Assume that $\mathbb{F}$ is any large enough field.
Earlier in the course, we saw that for every $d \in \mathbb{N}$ and for every set of points $\{(\alpha_i, \gamma_i) : i \in \{1, 2, \ldots, d+1\}\} \subseteq \mathbb{F}^2$ with $\alpha_i \neq \alpha_j$ for all $i \neq j$, there is a unique univariate polynomial P of degree at most d such that for all $i \in \{1, 2, \ldots, d+1\}, P(\alpha_i) = \gamma_i$.
In this question, you will show that this property does not extend to polynomials in a larger number of variables. Show that for every $d \geq 2$, there exists a set of points $\{(\alpha_i, \beta_i, \gamma_i) : i \in \left\{1, 2, \ldots, \binom{d+2}{2}\right\}\} \subseteq \mathbb{F}^3$ with $(\alpha_i, \beta_i) \neq \left(\alpha_j, \beta_j\right)$ for all $i \neq j$, such that for every bivariate polynomial $P(x, y) \in \mathbb{F}[x, y]$ of total degree at most d,

$$\exists i \in \left\{1, 2, \ldots, \binom{d+2}{2}\right\}, \quad P(\alpha_i, \beta_i) \neq \gamma_i.$$

Solution: We will show that even for $d+2$ points $\{(\alpha_i, \beta_i, \gamma_i)\}_{i \in [d+2]}$ such that for every bivariate polynomial $P(x, y) \in \mathbb{F}[x, y]$ of total degree at most d such that $\exists\, i \in [d+2], P(\alpha_i, \beta_i) \neq \gamma_i$. Consider any univariate polynomial $f(x) \in \mathbb{F}[x]$ with degree d. Let $\alpha_i \in \mathbb{F}$, $i \in [d+2]$ where $\alpha_i \neq \alpha_j$ for $i \neq j$ and $i, j \in [d+2]$. So consider the points

$$\{(\alpha_i, \beta, f(\alpha_i))\}_{i \in [d+1]} \cup \{(\alpha_{d+2}, \beta, f(\alpha_{d+2}) + 1)\}$$

for some $\beta \in \mathbb{F}$. Suppose there exists a bivariate polynomial $P(x, y) \in \mathbb{F}[x, y]$ with total degree at most d which passes through all these points. Then $P(\alpha_i, \beta) = f(\alpha_i)$ for all $i \in [d+1]$ and $P(\alpha_{d+2}, \beta) = f(\alpha_{d+2}) + 1$. Therefore consider the univariate polynomial $g(x) = P(x, \beta)$. Since total degree of P is at most d therefore $\deg(g) \leq d$. Therefore $g(\alpha_i) = f(\alpha_i)$ for all $i \in [d+1]$ and $g(\alpha_{d+2}) = f(\alpha_{d+2}) + 1$. Now there exist an unique polynomial of degree at most d which passes through the points $(\alpha_i, f(\alpha_i))$ for all $i \in [d+1]$. Since g and f both passes through them we have $g = f$. But f doesn't passes through $(\alpha_{d+2}, f(\alpha_{d+2}) + 1)$ and g does. Which is not possible. Hence contradiction. No bivariate polynomial of total degree at most d passes through these $d+2$ points. ■

Problem 2 — 25 Points

A set $\{f_1(x), f_2(x), \ldots, f_k(x)\}$ of polynomials over a set $\mathbb{F}$ are said to be linearly independent over $\mathbb{F}$ there are no $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$ that are not all zeros such that $\sum_i \alpha_i f_i$ is the identically zero polynomial. In this problem, we will explore some equivalent ways of characterizing linear independence of univariate polynomials.

(a) **(5 points)** Let d be an upper bound on the degree of f_i s and let M be an $k \times (d+1)$ matrix over $\mathbb{F}$ where $M(i, j)$ equals the coefficient of x^j in the polynomial f_i. In other words, row i of $\mathbb{F}$ is just the coefficient vector of f_i. Show that $\{f_1(x), f_2(x), \cdots, f_k(x)\}$ are linearly independent over $\mathbb{F}$ if and only if the matrix M has rank k.

(b) **(15 points)** Let $\mathbb{F}$ be a field of characteristic zero or larger than d, and let W be a $k \times k$ matrix with its i^{th} column being equal to $\left(f_i, \frac{df_i}{dx}, \ldots, \frac{d^{k-1} f_i}{dx^{k-1}}\right)$. Show that $\{f_1(x), f_2(x), \ldots, f_k(x)\}$ are linearly independent over $\mathbb{F}$ if and only if the determinant of W is a non-zero polynomial.

(c) **(5 points)** Can we relax the requirement on the field in the above problem ? For instance, does linear independence of $\{f_1(x), f_2(x), \ldots, f_k(x)\}$ continue to be characterized by the singularity of W for finite fields of characteristic p with $0 < p < d$?

Solution:

(a) Since the matrix M has k many rows the rank of matrix can be at most k. So we will show that $f_1(x)$, $f_2(x)$, $\cdots$, $f_k(x)$ are not linearly independent i.e. linearly dependent if and only if rank of M is $< k$. Let $f_{i,j}$ denote the coefficient of x^j of f_i. Let M_i denote the i^{th} column of M.

$$
\begin{aligned}
f_1(x), f_2(x), \cdots, f_k(x) \text{ linearly dependent} &\iff \exists\ \alpha_i \in \mathbb{F} \text{ for } i \in [n] \text{ not all zero such that } \sum_{i=1}^{n} \alpha_i f_i(x) = 0 \\
&\iff \sum_{i=1}^{n} \alpha_i f_{i,j} = 0 \text{ for all } j \in [d]. \\
&\iff \sum_{i=1}^{n} \alpha_i M_i = 0 \\
&\iff \text{Columns of } M \text{ are linearly dependent.} \\
&\iff \text{rank}(M) < k.
\end{aligned}
$$

(b) We will show $f_1(x), f_2(x), \ldots, f_k(x)$ are linear dependent if and only if determinant of W is zero. Let $\frac{d^0 f_i}{dx^0}$ denotes $f_i(x)$ for all $i \in [n]$.

$$
\begin{aligned}
f_1(x), f_2(x), \cdots, f_k(x) \text{ linearly dependent} &\iff \exists\ \alpha_i \in \mathbb{F} \text{ for } i \in [n] \text{ not all zero such that } \sum_{i=1}^{n} \alpha_i f_i(x) = 0 \\
&\iff \frac{d^j}{dx^j}\left[\sum_{i=1}^{n} \alpha_i f_i(x)\right] \equiv 0 \text{ for all } j \in \{0, \ldots, k-1\}. \\
&\iff \sum_{i=1}^{n} \alpha_i \frac{d^j f_i}{dx^j} \equiv 0 \text{ for all } j \in \{0, \ldots, k-1\}. \\
&\iff \sum_{i=1}^{n} \alpha_i W_i \equiv 0 \\
&\iff \text{Columns of } M \text{ are linearly dependent.} \\
&\iff \det(W) \equiv 0.
\end{aligned}
$$

(c) Suppose $p = k = 2$. $f_1(x) = x^4$ and $f_2(x) = x^6$. Then

$$
W = \begin{bmatrix} x^4 & x^6 \\ 0 & 0 \end{bmatrix} \implies \det(W) = 0
$$

Here x^4 and x^6 are linearly independent but the determinant of the matrix is 0. Therefore we cannot relax the requirement on the field characteristic being less than the degree of the polynomials. But if we make the characteristic bigger than the degree bound then all the steps of the proof in the above follows concluding that the polynomials are linearly independent if and only if the determinant of the matrix is non-zero polynomial.

■

Problem 3 15 Points

For $i \in \{1, 2, \ldots, k\}$, let $\mathbf{x}_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,n})$ be disjoint n-tuples of variables. For n variate polynomials $f_1(\mathbf{y}), \ldots, f_k(\mathbf{y}) \in \mathbb{C}[y_1, y_2, \ldots, y_n]$, let M be the $k \times k$ matrix such that $M_{i,j} = f_i\left(\mathbf{x}_j\right)$. Show that $f_1(\mathbf{y}), f_2(\mathbf{y}), \ldots, f_k(\mathbf{y})$ are linearly independent over $\mathbb{C}$ if and only if the determinant of M is non-zero.

Solution: We will show that $f_1(\mathbf{y}), f_2(\mathbf{y}), \ldots, f_k(\mathbf{y})$ are linearly dependent over $\mathbb{C}$ if and only if determinant of M is zero. Let M_i denote the i^{th} row of M.

$$
\begin{aligned}
f_1(\mathbf{y}), f_2(\mathbf{y}), \ldots, f_k(\mathbf{y}) \text{ linearly dependent} &\iff \exists\ \alpha_i \in \mathbb{C} \text{ for all } i \in [n] \text{ not all zero such that } \sum_{i \in [n]} \alpha_i f_i(\mathbf{y}) \equiv 0 \\
&\iff \forall\ j \in [n], \sum_{i \in [n]} \alpha_i f_i(\mathbf{x}_j) \equiv 0 \\
&\iff \sum_{i \in [n]} \alpha_i M_i \equiv 0 \\
&\iff \text{Rows of } M \text{ are not linearly independent} \\
&\iff \det(M) = 0
\end{aligned}
$$

Hence we get that $f_1(\mathbf{y}), f_2(\mathbf{y}), \ldots, f_k(\mathbf{y})$ are linearly independent over $\mathbb{C}$ if and only if the determinant of M is non-zero. ■

Problem 4 15 Points

Design an efficient deterministic algorithm that takes as input the description of a finite field $\mathbb{F}$ and a univariate polynomial $f \in \mathbb{F}[x]$ and decides if f is an irreducible polynomial.

Solution: We have the following lemma:

Lemma 1. *Let $f \in \mathbb{F}[x]$ be a polynomial with $\deg(f) = d$ where $\mathbb{F}$ is a finite field.. f is irreducible if and only if*

1. $f \mid x^{q^d} - x$
2. $gcd\left(f, x^{q^{\frac{d}{t}}} - x\right) = 1$ *for all prime divisor t of d.*

Proof: Let f is irreducible. Now we know if g is a irreducible then $g \mid x^{q^d} - x \iff \deg(g) \mid d$. Since $\deg(f) = d$, $f \mid x^{q^d} - x$. And since $d \nmid \frac{d}{t}$ for all prime divisor t of d we have $f \nmid x^{q^{\frac{d}{t}}} - x$. Therefore $gcd\left(f, x^{q^{\frac{d}{t}}} - x\right) = 1$ for all prime divisor t of d.

Now suppose f satisfies both properties. Suppose f is not irreducible. Let g is an irreducible factor of f and $\deg(g) < d$. Then $\deg(g) \mid \frac{d}{t'}$ for some prime divisor t' of d. Therefore $g \mid x^{q^{\frac{d}{t'}}} - x$. Therefore $g \mid gcd\left(f, x^{q^{\frac{d}{t'}}} - x\right)$ which contradicts that $gcd\left(f, x^{q^{\frac{d}{t}}} - x\right) = 1$ for all prime divisor t of d. Hence contradiction $\lightning$ f is irreducible. □

Algorithm 1: Efficient Deterministic Irreducibility Testing

Input: Description of finite field $\mathbb{F}$ and $f \in \mathbb{F}[x]$ with $\deg(f) = d$.
Output: Decide if f is irreducible

```
1  begin
2      if d = 0 then
3          return "Reducible"
4      if d = 1 then
5          return "Irreducible"
6      g ⟵ Compute x^{q^d} (mod f) by repeated squaring
7      if g ≠ x then
8          return "Reducible"
9      h ⟵ x
10     for i = 1, ..., d − 1 do
11         h ⟵ Compute h^q (mod f) by repeated squaring        //Computes x^{q^i} mod f
12         if deg(gcd(h − x, f)) ≥ 1 then
13             return "Reducible"
14     return "Irreducible"
```

The lemma above gives the correctness of the algorithm. We only have to calculate the number of field operations of the algorithm. Now to compute $g = x^{q^d}$ it takes $d \log q$ many multiplications in the repeated squaring. Now in each multiplication two $d-1$ degree polynomial since each time we are multiplying modulo f. Therefore to compute g it take $O(dM(d)\log q)$ many field operations. Now at any iteration of the for loop h is a polynomial with degree at most d. Therefore to compute h^q repeated squaring it takes $O(\log q)$ many multiplications of degree d polynomials which takes at most $O(M(d)\log q)$ field operations. Both $h - x$ and f has degree at most d. So the $gcd(h-x, f)$ can be computed using $O(M(d)\log d)$ field operations. So each iteration takes $O(M(d)(\log d + \log q))$ many field operations. Since there are d iterations of the for loop it takes $O(dM(d)(\log q + \log d))$ field operations to check if f is irreducible. ■