Homework 1

Date : Aug 9, 2020 — Algebra & Computation-A20

Instructor: Mrinal Kumar — Due: September 6, 2020

Instructions

- It is slightly preferred that you type your homeworks up in LaTeX. In case you turn in scans of handwritten notes, please make sure that they are legible.
- Discussion on the problems with other members of the class is permitted and to an extent, even encouraged. But, you *must* write the solutions on your own. You *must* also acknowledge any discussions you might have had with others separately for every problem.
- Do not look up solutions on the internet or in other references. In case you use any sources outside the notes for this course, again properly acknowledge them.
- To get the most out of the problem sets, you are encouraged to think about the problems on your own before discussing them with others, consulting the references or looking at the hints (which some of the problems might have).

Problems

1. **(5 points)** Let $\mathbb{F}$ be a field of characteristic equal to p. Then, show that over the polynomial ring $\mathbb{F}[x, y]$, $(x + y)^p = x^p + y^p$.

2. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct elements of some field $\mathbb{F}$. And, let $V(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be the $n \times n$ matrix whose (i, j) entry equals α_i^{j-1}.

   (a) **(5 points)** Show that V has rank equal to n.

   (b) **(10 points)** Show that the determinant of V equals $\prod_{i<j}(\alpha_j - \alpha_i)$.

3. **(5 points)** Let $(\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_n, \beta_n)$ be points in $\mathbb{F} \times \mathbb{F}$ for some field $\mathbb{F}$ with $\alpha_i \neq \alpha_j$ for all $i \neq j$. Then, show that there is a unique polynomial $f \in \mathbb{F}[x]$ of degree at most $n - 1$ such that for every $i \in \{1, 2, \ldots, n\}$, $f(\alpha_i) = \beta_i$.

4. Let $\mathbb{C}$ be the field of complex numbers. $\alpha \in \mathbb{C}$ is said to be a zero (or root) of multiplicity k of a non-zero polynomial $f(x) \in \mathbb{C}[x]$ if $f(\alpha) = \frac{\partial f}{\partial x}(\alpha) = \cdots = \frac{\partial^{k-1} f}{\partial x^{k-1}}(\alpha) = 0$ and $\frac{\partial^k f}{\partial x^k}(\alpha) \neq 0$.[1]

   (a) **(10 points)** Show that α is a zero of multiplicity at least k of f if and only if $(x - \alpha)^k$ divides $f(x)$.

   (b) **(10 points)** If $\alpha_1, \alpha_2, \ldots, \alpha_t$ are distinct elements of $\mathbb{C}$, then show that

$$\sum_{i=1}^{t} (\mathrm{Mult}(f, \alpha_i)) \leq \mathrm{Degree}(f)\,,$$

   where $\mathrm{Mult}(f, \alpha_i)$ denotes the multiplicity of f at α_i.

[1] k is said to be the multiplicity of f at α.

5. Let $\mathbb{F}$ be any field. The elementary symmetric polynomial of degree $d \in \{1, 2, \ldots, n\}$ on variables $x_1, x_2, \ldots, x_n$ is defined as

$$E_d(x_1, x_2, \ldots, x_n) = \sum_{S \subseteq [n], |S| = d} \prod_{j \in S} x_j \,.$$

   (a) **(10 points)** Now, consider the polynomial $f(x_1, \ldots, x_n) = \prod_{i=1}^{n}(x_i + 1)$ and observe that all the elementary symmetric polynomials appear as homogeneous components of f of varying degrees. Use this to argue that over every field with at least $n+1$ elements and for every $d \in \{1, 2, \ldots, n\}$, E_d can be expressed as

$$E_d = \sum_{i=1}^{t} \prod_{j=1}^{n} L_{i,j} \,,$$

   where $t \leq n+1$ and each $L_{i,j}$ is an affine function[2] in $\mathbb{F}[x_1, x_2, \ldots, x_n]$.

   (b) **(10 points)** A much trickier task is to prove that in some sense, this representation is essentially the best possible. As a first step towards this, show that there are values of d (for instance, $d = n/100$) such that for any representation of E_d as

$$E_d = \sum_{i=1}^{t} \prod_{j=1}^{n} L_{i,j} \,,$$

   the number of summands t is at least $\Omega(n)$. Here again, every $L_{i,j}$ is an affine function.

[2] An affine function (or an affine polynomial) in $\mathbb{F}[x_1, x_2, \ldots, x_n]$ is a polynomial of the form $\beta + \sum_{i=1}^{n} \alpha_i x_i$, where $\beta, \alpha_1, \ldots, \alpha_n \in \mathbb{F}$. In particular, $1 + x_i$ is an affine function.