Homework 2

Date: Sep 7, 2020 — Algebra & Computation-F20
Instructor: Mrinal Kumar — Due: Oct 7, 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.
- Please 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. Let q be a prime power and let $k > 0$ be a natural number. The polynomial $\mathsf{Trace}(x)$ is defined as
$$\mathsf{Trace}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{k-1}}.$$
   (a) **(5 points)** Show that for every $\alpha \in \mathbb{F}_{q^k}$, $\mathsf{Trace}(\alpha) \in \mathbb{F}_q$.
   (b) **(5 points)** Show that when viewed as a map from the vector space $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$, Trace is $\mathbb{F}_q$ linear. [1]
   (c) **(10 points)** Using the properties of Trace, conclude that for *every* $\mathbb{F}_q$ linear map L from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$, there is an $\alpha_L \in \mathbb{F}_{q^k}$ such that for all $\beta \in \mathbb{F}_{q^k}$, $L(\beta) = \mathsf{Trace}(\alpha_L \cdot \beta)$.[2]

2. **(10 points)** Let q be a prime power, $k > 0$ be a natural number and let $S \subset \mathbb{F}_{q^k}$ be a subspace of $\mathbb{F}_{q^k}$ of dimension s, when we view $\mathbb{F}_{q^k}$ as a k dimensional linear space over $\mathbb{F}_q$. Consider the polynomial $P_S(x)$ defined as
$$P_S(x) = \prod_{\alpha \in S} (x - \alpha).$$
   Show that there exist $\beta_1, \beta_2, \ldots, \beta_s \in \mathbb{F}_{q^k}$ such that
$$P_S(x) = x^{q^s} + \beta_1 x^{q^{s-1}} + \beta_2 x^{q^{s-2}} + \cdots + \beta_s x.$$
   Note the two features of P_S: it is very sparse, but has a lot of roots in $\mathbb{F}_{q^k}$. If you recall, Descarte's rule of signs from high school algebra tells us that a sparse non-zero real polynomial does not have a lot of real roots. These properties make P_S a very useful polynomial to have in many contexts.

[1] Recall that sometimes we view the field $\mathbb{F}_{q^k}$ as the k dimensional vector space over $\mathbb{F}_q$.
[2] The multiplication in $\alpha_L \cdot \beta$ is being done over the field $\mathbb{F}_{q^k}$.

3. **(10 points)** This question is similar to Question 5B in the first homework. Show that for any representation of the polynomial $\sum_{i=1}^{n} x_i y_i$ as a sum of product of affine polynomials, the number of summands is at least $\Omega(n)$.

4. **(10 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 $\{(\alpha_i, \beta_i, \gamma_i) : i \in \{1, 2, \ldots, \binom{d+2}{2}\}\} \subseteq \mathbb{F}^3$ with $(\alpha_i, \beta_i) \neq (\alpha_j, \beta_j)$ 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,

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

5. In this question, we will see a higher dimensional generalization of the algorithm for univariate multipoint evaluation that we saw in class. Let $\mathbb{F}$ be any field.

   (a) **(10 points)** Design a (fast) algorithm which takes as input the coefficient vector of an n variate polynomial f of degree at most $d-1$ in each variable, and a set $S \subset \mathbb{F}$ of size d, and outputs the evaluation of f on every point in the grid $S^n = \{(a_1, \ldots, a_n) : a_i \in S\}$. Note that input is given by $N = O(nd^n)$ field elements, so in the spirit of generalizing the univariate multipoint evaluation algorithm, we would like to have an algorithm which runs in time $N^{1+o(1)}$.

   (b) **(Bonus)** In the above question, we assumed a very strong strong structure on the set of inputs points, namely, that they are all on a grid. Generalize this to design an algorithm which evaluates an n variate polynomial of degree at most $d-1$ in each variable on an arbitrary set of d^n points in nearly linear time. You can work over your favorite field for this problem.