Homework 5

Instructor: Mrinal Kumar | Algebra & Computation-F21

Instructions

- This problem set will not be graded. You are encouraged to think about the problems and talk to me if you have queries.

Problems

1. For natural numbers $n, d \in \mathbb{N}$ where $d \leq n$, the elementary symmetric polynomial of degree d on n variables, denoted by $E_{n,d}$ is defined as

$$E_{n,d}(x_0, x_2, \ldots, x_{n-1}) = \sum_{S \subseteq [n], |S|=d} \prod_{i \in S} x_i \,.$$

   Show that over every field $\mathbb{F}$ of size at least $n+1$, there exist degree 1 polynomials $\{L_{i,j} : i, j \in [n]\}$ such that

$$E_{n,d} = \sum_{i \in [n]} \prod_{j \in [n]} L_{i,j} \,.$$

   Here $[n]$ denotes $\{0, 1, \ldots, n-1\}$.

2. Recall the $\mathsf{Trace} : \mathbb{F}_{p^k} \to \mathbb{F}_p$ function from Homework 2. Show that if $p = 2$, then the polynomial $A(x) = \mathsf{Trace}(x)(\mathsf{Trace}(x) + 1)$ is zero for every $x \in F_{2^k}$.

   Now, recall the Cantor-Zassenhaus algorithm for factoring univariate polynomials over finite fields from the class. In the class, we only discussed the algorithm for fields of odd characteristic. Use the polynomial $A(x)$ above to get a variant of the Cantor-Zassenhaus algorithm for finite fields of characteristic 2.

3. 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.

4. Let B be a deterministic algorithm that takes as input an arithmetic circuit and correctly outputs where B is identically zero or not in time polynomially bounded in the size and degree of the input circuit.

Using the algorithm B above as a subroutine, design a deterministic algorithm that takes as input an arithmetic circuit and correctly outputs a setting of the variables from the underlying field where the circuit evaluates to a non-zero value, if such a setting exists. Moreover, this algorithm should run in time polynomially bounded in the circuit size and degree.

It might be helpful to assume that the underlying field is large enough.

5. Design an algorithm that takes as input two arithmetic circuits C_1 and C_2 and decides if C_1 divides C_2 in time polynomially bounded in the sizes and degrees of the input circuits.

   For simplicity you can assume that you are working over a large enough field and are working in the unit cost model where every field operation can be done in unit time. Ideas from Strassen's division elimination that we saw in the class might be relevant.

6. Let $P(x), Q(x) \in \mathbb{F}[x]$ be relatively prime univariate polynomials over the field $\mathbb{F}$ and let $d = \max(\deg(P), \deg(Q))$.

   Let D be a multiple of d. Show that for every polynomial $G(x) \in \mathbb{F}[x]$ of degree at most $D-1$, there is a unique tuple $(G_0(x), G_1(x), \ldots, G_{d-1}(x))$ of polynomials of degree at most $D/d - 1$ such that

$$G(x) = Q(x)^{D/d-1} \cdot \left(\sum_{i=0}^{d-1} G_i(P/Q) \cdot x^i \right) .$$

   We saw a very special case of this when $Q(x) = 1$ and $P(x) = x^2$ while discussing the Fast Fourier transform in class.