CS711 Assignment 3

Sankalp Gambhir
180260032

October 5, 2021

Question 1.

Proof. Given the set $S_{d,n}$ as defined, suppose if possible that we cannot find an assignment $\mathbf{b}$ in this set for some non-zero polynomial P of degree $\leq d$ in n variables such that the evaluation is non-vanishing, i.e., $P(\mathbf{b}) = 0 \forall \mathbf{b} \in S_{d,n}$.

Write the polynomial P defined by the $\binom{n+d}{d}$ coefficients $\{a_{\alpha_1 \alpha_2 \dots \alpha_n}\}$ as a linear functional acting on a vector of pre-evaluated monomials $\{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}\}$ with $\sum \alpha_i \leq d$,

$$P(x_1, x_2, \dots, x_n) = \begin{pmatrix} a_{00\dots0} & a_{10\dots0} & \dots & a_{00\dots d} \end{pmatrix}_{1 \times \binom{n+d}{d}} \begin{pmatrix} 1 & x_1 & \dots & x_n^d \end{pmatrix}^{\top}_{1 \times \binom{n+d}{d}}$$

Writing the condition for $\mathbf{b}$ in this notation, it resolves to the coefficient vector being acted on the right by the matrix M with columns as the x-vector pre-evaluated over each $\mathbf{b}$. The condition assumed above is equivalent to this matrix having a non-trivial kernel, i.e., there existing a coefficient vector which is non-zero, such that all its evaluations over this set are 0.

Consider any two distinct assignments $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$ and $B = (\beta_1, \beta_2, \dots \beta_n)$. Suppose their pre-evaluated x-vectors (columns of M) are linearly dependent, we have

$$\exists\ \lambda, \delta \in \mathbb{C}\ \lambda \vec{X}(A) + \delta \vec{X}(B) = \vec{0}\ .$$

Cherry-picking dimensions from this vector equation, first the degree 0 condition, and finally all the degree 1 conditions, we find

$$\begin{aligned} \lambda \cdot 1 + \delta \cdot 1 = 0\ , \\ \lambda = -\delta\ , \\ \vec{X}(A) = \vec{X}(B)\ ,\ \text{and} \\ \alpha_i = \beta_i \forall i\ . \end{aligned}$$

However, we stipulated that these assignments were distinct, so this is a contradiction. Thus, columns of M, which represent distinct assignments, cannot be linearly dependent, M is of full-rank, and thus has a trivial kernel. This again, is a contradiction, so contrary to assumption, we must be able to find $\mathbf{b} \in S_{d,n}$ for every non-zero polynomial P of degree $\leq d$ in n variables such that it evaluates to a non-zero quantity over $\mathbf{b}$.

$\square$

Question 2.

Proof. Given the set $T_{d,n}$ as defined, suppose if possible, that we cannot find any vector in the set such that a given non-zero polynomial P of degree d in n variables evaluates to a non-zero value on it. I prove that this leads to a contradiction.

The evaluation condition implies $P(\mathbf{b}) = 0$ for every $\mathbf{b} \in T_{d,n}$. Instead of writing it as a polynomial system, evaluate each possible variable in $P(x_1, x_2, \ldots, x_n)$ and write it as the following linear system

$$\begin{pmatrix} a_{00\ldots0} & a_{10\ldots0} & \ldots & a_{00\ldots0d} \end{pmatrix} \begin{pmatrix} x_1^0 x_2^0 \ldots x_n^0 & x_1^1 x_2^0 \ldots x_n^0 & \ldots & x_1^0 x_2^0 \ldots x_n^d \end{pmatrix}^\top$$

This linear system has dimension $\binom{n+d}{d}$. Given that we have evaluations on $\binom{n+d}{d}$ points as well, we can write this as the linear system

$$\begin{pmatrix} a_{00\ldots0} & a_{10\ldots0} & \ldots & a_{00\ldots0d} \end{pmatrix} \begin{pmatrix} p_1^{0\cdot0} p_2^{0\cdot0} \ldots p_n^{0\cdot0} & p_1^{0\cdot1} p_2^{0\cdot1} \ldots p_n^{0\cdot1} & \ldots & p_1^{0\cdot t} p_2^{0\cdot t} \ldots p_n^{0\cdot t} \\ p_1^{1\cdot0} p_2^{0\cdot0} \ldots p_n^{0\cdot0} & p_1^{1\cdot1} p_2^{0\cdot1} \ldots p_n^{0\cdot1} & \ldots & p_1^{1\cdot t} p_2^{0\cdot t} \ldots p_n^{0\cdot t} \\ \vdots & \ddots & \ddots & \vdots \\ p_1^{0\cdot0} p_2^{0\cdot0} \ldots p_n^{d\cdot0} & p_1^{0\cdot1} p_2^{0\cdot1} \ldots p_n^{d\cdot1} & \ldots & p_1^{0\cdot t} p_2^{0\cdot t} \ldots p_n^{d\cdot t} \end{pmatrix} = \begin{pmatrix} 0 & 0 \ldots & 0 \end{pmatrix},$$

with $t = \binom{n+d}{d}$. This matrix must have a non-trvial kernel, since the coefficients were constrained to be non-zero. However, note that this is the Vandermonde matrix in the $\binom{n+d}{d}$ integers $\{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}\}$, with $\sum \alpha_i \leq d$. Since these are distinct primes, there are no duplicates in this set, and thus the determinant of the Vandermonde matrix must be non-zero. However, this would mean that it is of full rank and has a trivial kernel, this is a contradiction.

Thus, our assumption of being unable to produce a non-zero evaluation over the given set was incorrect, and there exists a vector in $T_{d,n}$ for every polynomial of maximum total degree d and n variables such that it evaluates to a non-zero complex quantity over the given vector provided that it is not identically zero.

$\square$

Question 3.

Proof. Consider a multilinear polynomial $P \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. Since it is multilinear, and thus linear in x_1, we can express it as:

$$P(x_1, x_2, \ldots, x_n) = x_1^0 P_1(x_2, x_3, \ldots, x_n) + x_1^1 P_1'(x_2, x_3, \ldots, x_n) \ .$$

As this decomposes into the $(n-1)$ problem, it is easy to see that if either of the polynomials P_1 or P_1' have non-zero assignments in $\{0,1\}^{n-1}$, then we can generate a non-zero assignment including $x_1 \in \{0,1\}$. The proof proceeds by induction.

Base case: $n = 1$.

P_1, P_1' in this case are constants, with atleast one of them non-zero. If P_1 is 0, choose $x_1 = 1$, else choose $x_1 = 1$. $P \not\equiv 0$ guarantees this assignment leads to a non-vanishing result.

Induction: Given that $\forall m \in \mathbb{N}, m < n$, every non-zero multilinear polynomial in m variables has a non-zero satisfying assignment, the same holds for non-zero multilinear polynomials in n variables.

As before, write

$$P(x_1, x_2, \ldots, x_n) = x_1^0 P_1(x_2, x_3, \ldots, x_n) + x_1^1 P_1'(x_2, x_3, \ldots, x_n) \ ,$$

where P_1, P_1' depend on atmost $n-1$ variables. If $P_1 \not\equiv 0$, by the induction hypothesis, it has an assignment such that it is non-vanishing. Append to such an assignment, $x_1 = 0$. Else, $P_1 \equiv 0$, so we must have $P_1' \not\equiv 0$ since P is given to be non-zero. Append $x_1 = 1$ to a non-vanishing assignment of P_1'.

This produces a satisfying assignment for any non-zero multilinear polynomial of degree n.

□

Question 4.

Given the matrix M as defined and the functions $\{f_i(\mathbf{y})\}$, note that the non-vanishing of the $\det(M)$ implies the linear independence of $\{(f_i(\mathbf{x}_j))\}$ as vectors of functions. I prove instead the converse, that their linear *dependence* correspond to each other.

Forward Implication $\Rightarrow$: Linear dependence of $\{f_i(\mathbf{y})\}$ implies the vanishing of $\det(M)$.

Given that the functions with the y's as variables are linearly dependent, we can find a set of coefficients $\{\alpha_i\}$ such that

$$\sum \alpha_i f_i(\mathbf{y}) = 0 \ .$$

Substituting one-by-one $\mathbf{y}$ by each $\mathbf{x}_i$, we obtain n linear dependence equations, which combined imply

$$\sum \alpha_i \begin{pmatrix} f_1(\mathbf{x}_i) & f_2(\mathbf{x}_i) & \ldots & f_n(\mathbf{x}_i) \end{pmatrix}^\top = 0 \ .$$

This is precisely the condition for linear dependence of the columns of M, and thus its determinant vanishes.

<u>Backward Implication $\Leftarrow$:</u> Vanishing of $\det(M)$ implies the linear dependence of $\{f_i(\mathbf{y})\}$.

Given that the determinant vanishes, we know that the *rows* must be linearly dependent, i.e., we can find a set $\{\alpha_i\}$ such that

$$\sum \alpha_i \begin{pmatrix} f_i(\mathbf{x}_1) & f_i(\mathbf{x}_2) & \ldots & f_i(\mathbf{x}_n) \end{pmatrix}^\top = 0 \ .$$

Pick an arbitrary coordinate and substitute for the $\mathbf{x}_j$ with y, and we recover the dependence criterion for the $f_i(\mathbf{y})$.

This proves that the linear dependence of the $\{f_i(\mathbf{y})\}$ is equivalent to the vanishing of $\det(M)$, and by extension, the linear independence is equivalent to its non-vanishing.