Instructor: Girish Varma

IIIT Hyderabad

1 Linear Algebra Basics

1.1 Boolean Function Spaces

Let $\mathbb{F}_2$ be the field of two elements $\{0,1\}$ where addition is $\mod 2$ and multiplication is AND. $\mathbb{F}_2^n$ is the n dimensional vector space over $\mathbb{F}_2$ consisting of n tuples of $\mathbb{F}_2$. Let $\mathcal{F}$ be the set of all functions with domain $\mathbb{F}_2^n$ and codomain $\mathbb{F}_2$. It is easy to verify that $\mathcal{F}$ is a 2^n dimensional vector space over $\mathbb{F}_2$ with the natural scalar multiplication and vector addition ($\mod 2$). Assume $n \geq 2$.

a.) For any subset S of $\{1, \cdots n\}$, let $\text{PARITY}_S : \mathbb{F}_2^n \to \mathbb{F}_2 \in \mathcal{F}$ be defined as:

$$\text{PARITY}_S(x) = \bigoplus_{i \in S} x_i.$$

For $S = \emptyset$, define $\text{PARITY}_S(x) = 1$ (constant 1 function). Show that the following set of 2^n parity functions are linearly dependent:

$$\{\text{PARITY}_S : S \subseteq \{1, \cdots, n\}\}$$

b.) For any subset S of $\{1, \cdots n\}$, let $\text{AND}_S : \mathbb{F}_2^n \to \mathbb{F}_2 \in \mathcal{F}$ be defined as:

$$\text{AND}_S(x) = \bigwedge_{i \in S} x_i.$$

For $S = \emptyset$, define $\text{AND}_S(x) = 1$ (constant 1 function). Show that the following set of 2^n functions forms a basis for $\mathcal{F}$:

$$\{\text{AND}_S : S \subseteq \{1, \cdots, n\}\}$$

1.2 Infinite Dimensional Vector Spaces

a.) Consider the set of all functions with domain $\mathbb{R}$ and codomain $\mathbb{R}$ as a vector space over $\mathbb{R}$. Define a set of basis functions. Are they countable or uncountable? If so why?

b.) Consider $\mathbb{R}$ as a vector space over the field $\mathbb{Q}$ (rational numbers). Is there a basis set for the above vector space that is countable. (Remember countable and uncountable sets from your discrete math course). Explain why?

1.3 Rank over different Fields

Let $\mathbb{K}, \mathbb{F}$ be fields such that $\mathbb{F} \subset \mathbb{K}$ and the addition, multiplication operations in $\mathbb{F}$ is the same as that in $\mathbb{K}$. For example $\mathbb{K}$ can be $\mathbb{R}$ and $\mathbb{F}$ can be $\mathbb{Q}$ (or $\mathbb{C}, \mathbb{R}$ respectively). $\mathbb{F}^{n\times m}$ is the set of $n \times m$ matrices with entries in $\mathbb{F}$. For any matrix $M \in \mathbb{F}^{n\times m}$, we can define rank with respect to $\mathbb{F}$ as well as $\mathbb{K}$. The rank with respect to $\mathbb{K}$ denoted by $\mathrm{rank}_{\mathbb{K}}(M) = \dim(\mathrm{span}_{\mathbb{K}}(\mathrm{columns}(M)))$ where $\mathrm{span}_{\mathbb{K}}(S)$ denotes the vector space spanned by S by taking linear combinations with scalars from $\mathbb{K}$. Similarly we define $\mathrm{rank}_{\mathbb{F}}(M)$.

a.) Show that for $M \in \mathbb{F}^{n\times m}$, $\mathrm{rank}_{\mathbb{F}}(M) = \mathrm{rank}_{\mathbb{K}}(M)$.

b.) Given a binary matrix $M \in \{0,1\}^{m\times n}$, show that $\mathrm{rank}_{\mathbb{R}}(M) \geq \mathrm{rank}_{\mathbb{F}_2}(M)$. Note that addition and multiplication over $\mathbb{F}_2$ is different from $\mathbb{R}$. $\mathrm{rank}_{\mathbb{R}}, \mathrm{rank}_{\mathbb{F}_2}$ are defined as earlier with the respective definition of addition and multiplication in $\mathbb{R}, \mathbb{F}_2$ (ie normal arithmetic and $\mod 2$ arithmetic).

1.4 Help Alice & Bob Communicate

Alice and Bob needs to compute a known function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. They know the function beforehand and can agree upon a plan. Later Bob will go to Mars. Then both of them will be given some $x, y \in \{0,1\}^n$ (not known beforehand) respectively and Alice will be allowed to sent a message to Bob. Alice will have access to only x, Bob will have access to only y and they do not know the other persons input. Every bit of message Alice communicates is expensive. After getting Alice's message Bob should be able to find out $f(x,y)$.

Let $M \in \{0,1\}^{2^n \times 2^n}$ (binary matrix) be defined as $M_{i,j} = f(\mathrm{bin}(i), \mathrm{bin}(j))$, where $\mathrm{bin}(i)$ is the n bit binary representation of i ($0 \leq i, j < 2^n$). Can you design a protocol for them such that Alice only needs to sent $\mathrm{rank}_{\mathbb{F}_2}(M)$ bits of communication?

2.1 Random Walks **submit**

Consider an undirected graph $G = (V, E)$ without any isolated vertices, where V is a set of n nodes and

$$E \subseteq \{\{a, b\} : a \neq b \text{ and } a, b \in V\}$$

is a set of edges. The random walk matrix of G is a matrix M defined by

$$M_{a,b} = \begin{cases} 1/d_b \text{ if } \{a, b\} \in E \\ 0 \text{ otherwise} \end{cases} \quad \text{where } a, b \in V \text{ and } d_b = |\{\{a, b\} \in E : a \in V\}|$$

d_b is called the degree of the vertex b.

a.) Show that if λ is a real eigenvalue ($\in \mathbb{R}$) of M then $-1 \leq \lambda \leq 1$.

> **Hint 1** *Need to use the facts that a.) eigenvalues of M = eigenvalues of M^T b.) columns of M sum upto 1. Consider an eigenvector v of λ of M^T. Let i be the coordinate of v, which has the highest absolute value. This coordinate is going to be crucial for the proof to work.*

b.) Show that the column vector v defined by $v_a = d_a / (\sum_{b \in V} d_b), \forall a \in V$ is an eigenvector of M with eigenvalue 1. That is $Mv = v$, for any graph G.

c.) Show that the maximal number of linearly independent eigenvectors with eigenvalue 1 is equal to the number of connected components in G.

d.) Show that -1 is an eigenvalue of M if and only if G is a bipartite graph.

> **Hint 2** *Try to show that LHS $\Rightarrow$ RHS and RHS $\Rightarrow$ LHS separately for the last two questions.*

2.2 Polynomials **submit**

Let $\mathcal{P}_n$ be the set of polynomials (on one variable) of degree less than n. As you know $p \in \mathcal{P}_n$, can be written as a linear combination of the standard monomial basis as follows $p = \sum_{d=0}^{n-1} p_d x^d$, where p_d's are coordinates with respect to this basis.

a.) For any polynomial $q \in \mathcal{P}_n$ (having coordinates $q_0, \cdots q_{n-1}$ in standard monomial basis), define the function $T_q : \mathcal{P}_n \to \mathcal{P}_{2n-1}$, which maps $p \mapsto q \times p$ (ie. polynomial multiplication). Is T_q a linear transformation? If so what is the matrix of the transformation in the standard monomial basis ie $\{1, x, x^2, x^3, \cdots, x^{n-1}\}$? Give the formula for each entry of the matrix for general n, in the standard monomial basis.

b.) Let $n = 4$. Consider the change of basis, which maps the dth standard basis ($d = 0, 1, 2, 3$) to the column vector $[1, \omega^d, \omega^{2\cdot d}, \omega^{3\cdot d}]$, where $\omega = e^{i\cdot\frac{2\pi}{4}}$ (a complex number; $i = \sqrt{-1}$). What is the matrix of T_q with respect to this basis? What is the change of basis matrix for changing coordinates from this new basis back to the standard monomial basis?

2.3 Invarience of Eigenvalues **submit**

a.) Let $M \in \mathbb{R}^{n\times n}$. We can define eigenvalues from the left and the right as follows. λ is left eigenvalue of M iff there exists a nonzero row vector v, such that $vM = \lambda v$. Similarly λ is a right eigenvalue of M iff there exists a nonzero column vector v, such that $Mv = \lambda v$.

- Show that the set of left eigenvalues and right eigenvalues of any matrix are equal.
- Are the left and right eigenvectors (similarly defined) the same (by taking transpose)?

b.) Let M, M' be matrices corresponding to the same linear operator $T : V \to V$ (V is a n dimensional vector space over some field) with respect to different basis. Also assume that T is a rank n operator and M has n eigenvalues $\lambda_1, \cdots, \lambda_n$.

- Show that set of eigenvalues of M is equal to the set of eigenvalues of M'.
- Show that $\det(M) = \det(M') = \prod_{i=1}^n \lambda_i$.
- Define trace of a matrix, as the sum of diagonal entries. ie $\text{trace}(M) = \sum_{j=1}^n M_{jj}$. Show that $\text{trace}(M) = \text{trace}(M') = \sum_{i=1}^n \lambda_i$.

3.1 An Orthonomal Basis for Boolean Functions

Consider the set of functions with domain $\{+1, -1\}^n$ and range $\mathbb{R}$. Observe that it is a vector space over $\mathbb{R}$ of dimension 2^n. Consider the inner product and norm defined by

$$\langle f, g\rangle = \frac{1}{2^n} \sum_{x \in \{+1,-1\}^n} f(x)g(x) \qquad \text{and} \qquad \|f\| = \sqrt{\langle f, f\rangle}.$$

a.) Define the following set of functions,

$$\{\chi_S\}_{S \subseteq \{1,\cdots,n\}} \qquad \text{where} \qquad \chi_S(x) = \prod_{i \in S} x_i.$$

For $S = \emptyset$, χ_S is the constant 1 function. Show that these functions form an orthonormal basis under the inner product defined.

b.) Let f be any function in this space with range $\{+1, -1\}$ such that

$$f = \sum_{S \subseteq \{1,\cdots,n\}} \widehat{f}_S \chi_S \qquad \text{where} \qquad \forall S \subseteq \{1, \cdots, n\}, \widehat{f}_S \in \mathbb{R}$$

That is $(\widehat{f}_S)_{S \subseteq \{1,\cdots,n\}}$ are the coordinates with respect to the χ_S basis. Show that

$$\sum_{S \subseteq \{1,\cdots,n\}} (\widehat{f}_S)^2 = 1.$$