REU 2013: Apprentice Program **Summer 2013**

Lecture 1: June 24, 2013

Madhur Tulsiani Scribe: Young Kun Ko

1 Small Digression to Graph Theory

Exercise 1.1 (Puzzle) *Number of people who have made an odd number of handshakes must be even.*

Definition 1.2 *A graph G is defined by a set of vertices V and a set of edges $E \subseteq V \times V$. G is called an undirected graph if the edge (i, j) is the same as the edge (j, i) (in this case we actually have $E \subseteq \binom{V}{2}$).*

Definition 1.3 (Degree) *A degree of a vertex i is the number of edges including the vertex i.*

Theorem 1.4 (Handshake theorem) *Let d_i denote the degree of vertex i. Then,*

$$\sum_{i \in V} d_i = 2 \cdot |E|$$

2 Linear Algebra

Definition 2.1 (Number Field) *A number field $\mathbb{F}$ is a subset of $\mathbb{C}$ such that*

- $1 \in \mathbb{F}$
- *$\mathbb{F}$ is closed under addition, substraction, multiplication and division (except by 0).*

Exercise 2.2

1. *Rational numbers ($\mathbb{Q}$) form a number field.*
2. *Any number field must contain $\mathbb{Q}$.*
3. *$\mathbb{F} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a number field*
4. *$\mathbb{F} = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b \in \mathbb{Q}\}$ is a number field*

Definition 2.3 (Vector Space) *V is a vector space over a field $\mathbb{F}$ if there exists two operators: $+ : V \times V \to V$ (vector addition) and $\cdot : \mathbb{F} \times V \to V$ (scalar multiplication) such that $+$ is*

1. *commutative, that is $v_1 + v_2 = v_2 + v_1$.*

2. *associative, that is* $v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$.

3. *additive identity exists, that is* $\exists 0 \in V$ *such that* $0 + v = v (\forall v \in V)$.

4. *additive inverse exists, that is* $\forall v \in V,\ \exists v^* \in V$ *such that* $v + v^* = 0$.

and $\cdot$ *is*

1. *distributive, that is* $(\alpha_1 + \alpha_2) \cdot v = \alpha_1 \cdot v + \alpha_2 \cdot v$ *and* $\alpha(v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2$.

2. *(pseudo-)associative, that is* $\alpha(\beta \cdot v) = (\alpha\beta) \cdot v$.

3. *normalization factor exists, that is* $\exists 1 \in \mathbb{F}$ *such that* $1 \cdot v = v\ (\forall v \in V)$.

Exercise 2.4 *Verify that*

1. $0 \cdot v = 0\ (\forall v \in V)$

2. $\alpha \cdot 0 = 0\ (\forall \alpha \in \mathbb{F})$

Example 2.5

1. $\mathbb{R}$ *is a vector space over* $\mathbb{Q}$.

2. $\mathbb{R}[x]$ *is a set of polynomials in* x *with real coefficients. Then* $\mathbb{R}[x]$ *is a vector space over* $\mathbb{R}$.

3. *Space of all functions from* $\mathbb{R}$ *to* $\mathbb{R}$ *is a vector space over* $\mathbb{R}$.

2.1 Linear Independence

Definition 2.6 (Linear Independence) *Vectors* $v_1, \ldots, v_l \in V$ *are said to be linearly independent if*

$$\alpha_1 \cdot v_1 + \cdots + \alpha_l \cdot v_l = 0 \ \Rightarrow\ \alpha_1, \ldots, \alpha_l = 0\,.$$

An infinite set of vectors is said to be linearly independent if every finite subset is linearly independent.

Example 2.7

1. $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *and* $v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ *are linearly independent in* $\mathbb{R}^2$ *over* $\mathbb{R}$.

2. $1, \sqrt{2}, \sqrt{3}$ *are liearly independent in* $\mathbb{R}$ *when considered as a vector space over* $\mathbb{Q}$.

Exercise 2.8 *Let* $a_1, \ldots, a_n \in \mathbb{R}$ *be distinct. Let* $g(x) = (x - a_1) \ldots (x - a_n)$ *and* $f_i(x) = \frac{g(x)}{(x - a_i)}$. *Then show that* $f_1, \ldots, f_n$ *are linearly independent over* $\mathbb{R}$.

Exercise 2.9

1. *Prove that the functions* $\sin x, \cos x$ *are linearly independent over* $\mathbb{R}$.

2. *Prove that* $\{1, \sin x, \cos x, \sin 2x, \cos 2x, \ldots\}$ *are linearly independent over* $\mathbb{R}$.

2.2 First Miracle of Linear Algebra

Definition 2.10 (Span) *We define a span of a set of vectors S as follows*

$$Span(S) = \{\alpha_1 \cdot v_1 + \cdots \alpha_k \cdot v_k \mid k \in \mathbb{N}, v_1, \ldots, v_k \in S, \alpha_1, \ldots, \alpha_k \in \mathbb{F}\}$$

Definition 2.11 (Basis) *A set of vectors S is called a basis for V if S is linearly independent and $Span(S) = V$.*

Example 2.12 $\left\{ e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_k = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\}$ *is a basis for $\mathbb{R}^k$ with $\mathbb{F} = \mathbb{R}$.*

Proposition 2.13 *Any maximal linearly independent set of vectors is a basis.*

Proof: Proof via contradiction. Let S be a maximal linearly independent collection of vectors. Let $Span(S) \neq V$. Then $\exists w \in V$ such that $w \notin Span(S)$. Then $S \cup \{w\}$ must be a linearly independent collection, which contradicts maximality of S. This is because if $S \cup \{w\}$ is not linearly independent, then there exists $v_1, \ldots, v_k \in S$ and $\beta, \alpha_1, \ldots, \alpha_k \in \mathbb{F}$, not all zero, such that

$$\beta \cdot w + \alpha_1 \cdot v_1 + \cdots + \alpha_k \cdot v_k = 0\,.$$

Also, we must have $\beta \neq 0$ since S is linearly independent. But then,

$$w = (-\alpha_1/\beta) \cdot v_1 + \cdots + (-\alpha_k/\beta) \cdot v_k\,,$$

which contradicts the assumption that $w \notin Span(S)$. ■

Theorem 2.14 (First Miracle of Linear Algebra) *Let $v_1, \ldots, v_k \in Span(w_1, \ldots w_l)$. If $v_1, \ldots, v_k$ are linearly independent, then $k \leq l$.*

Lemma 2.15 (Steinitz Exchange Principle) *Under above assumptions, $\forall i \in [k],\ \exists j \in [l]$ such that $\{v_1, \ldots, v_{i-1}, w_j, v_{i+1}, \ldots, v_k\}$ are linearly independent.*

Proof of Lemma: Suppose not. Then $\exists i$ such that $\forall j$, $\{v_1, \ldots, v_{i-1}, w_j, v_{i+1}, \ldots, v_k\}$ is not linearly independent. This implies that we can write $w_j = \alpha_1 v_1 + \cdots + \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \cdots + \alpha_k v_k$ for some $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_k \in \mathbb{F}$. In other words, $\forall j$, $w_j \in Span(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k)$. Then we must have $Span(w_1, \ldots w_l) \subseteq Span(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k)$. But this implies that $v_i \in Span(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k)$, which is a contradiction. ■

Proof of Theorem: Proof via contradiction. Assume $k > l$ and keep applying the lemma exchanging $v_1, v_2, \ldots$ and so on. If $k > l$, we must the w_j twice for some j and then the set obtained cannot be linearly independent. ■

Corollary 2.16 *If V has a finite basis, then all bases have equal size.*

2.3 Lagrange Interpolation

Goal Given $f(a_1) = b_1, \ldots, f(a_n) = b_n$, for some polynomial of degree $\leq n-1$, find f.

Exercise 2.17 *Lagrange Interpolation can be proved via following steps.*

- $\mathbb{R}^{\leq (n-1)}[x]$ *is a vector space and has a basis of size* n.
- *Let* $g(x) = (x - a_1) \ldots (x - a_n)$. *Then* $f_i = g(x)/(x - a_i)$ *are linearly independent. Then* $f_1, \ldots, f_n$ *must form a basis*
- *Thus,* $\exists \alpha_1 \ldots \alpha_n$ *such that* $f = \sum_i \alpha_i f_i$. *Find* $\alpha_1, \ldots, \alpha_n$.