Mathematical Toolkit **Autumn 2018**

Lecture 2: October 4, 2018

Lecturer: Madhur Tulsiani

1 Linear Independence and Bases

Definition 1.1 *Given a set $S \subseteq V$, we define its* span *as*

$$\text{Span}\,(S) \;=\; \left\{ \sum_{i=1}^{n} a_i \cdot v_i \mid a_1, \ldots, a_n \in \mathbb{F}, v_1, \ldots, v_n \in S, n \in \mathbb{N} \right\}.$$

Note that we only include finite *linear combinations.*

Remark 1.2 *Note that the definition above and the previous definitions of linear dependence and independence, all involve only finite linear combinations of the elements. Infinite sums cannot be said to be equal to a given element of the vector space without a notion of convergence or distance, which is not necessarily present in an abstract vector space.*

Definition 1.3 *A set B is said to be a basis for the vector space V if B is linearly independent and* $\text{Span}\,(B) = V$.

It is often useful to use the following alternate characterization of a basis.

Proposition 1.4 *Let V be a vector space and let $B \subseteq V$ be a maximal linearly independent set i.e., B is linearly independent and for all $v \in V \setminus B$, $B \cup \{v\}$ is linearly dependent. Then B is a basis.*

The following proposition and it's proof will be very useful.

Proposition 1.5 (Steinitz exchange principle) *Let $\{v_1, \ldots, v_k\}$ be linearly independent and $\{v_1, \ldots, v_k\} \subseteq \text{Span}\,(\{w_1, \ldots, w_n\})$. Then $\forall i \in [k]$ $\exists j \in [n]$ such that $w_j \notin \{v_1, \ldots, v_k\} \setminus \{v_i\}$ and $\{v_1, \ldots, v_k\} \setminus \{v_i\} \cup \{w_j\}$ is linearly independent.*

Proof: Assume not. Then, there exists $i \in [k]$ such that for all $w_j \notin \{v_1, \ldots, v_k\} \setminus \{v_i\}$, $\{v_1, \ldots, v_k\} \setminus \{v_i\} \cup \{w_j\}$ is linearly dependent. Note that this means we cannot have $v_i \in \{w_1, \ldots, w_n\}$ (why?)

The above gives that for all $j \in [n], w_j \in \text{Span}\left(\{v_1, \ldots, v_k\} \setminus \{v_i\}\right)$. However, this implies

$$\{v_1, \ldots, v_k\} \subseteq \text{Span}\left(\{w_1, \ldots, w_n\}\right) \subseteq \text{Span}\left(\{v_1, \ldots, v_k\} \setminus \{v_i\}\right),$$

which is a contradiction. ■

1.1 Finitely generated spaces

A vector space V is said to be finitely generated if there exists a finite set T such that $\text{Span}(T) = V$. The following is an easy corollary of the Steinitz exchange principle.

Corollary 1.6 *Let $B_1 = \{v_1, \ldots, v_k\}$ and $B_2 = \{w_1, \ldots, w_n\}$ be two bases of a finitely generated vector space V. Then, they must have the same size i.e., $k = n$.*

Proof Sketch: Use the exchange principle to successively replace elements from B_1 by those from B_2. Since we need to replace k elements and no element of B_2 can be used twice (why?) we must have $k \leq n$. By symmetry, we must also have $n \leq k$. □

The above proves that all bases of a finitely generated vector space (if they exist!) have the same size. It is easy to see that a similar argument can also be used to prove that a basis must always exist.

Exercise 1.7 *Prove that a finitely generated vector space with a generating set T has a basis (which is a subset of the generating set T).*

The above argument can also be used to prove a stronger statement.

Exercise 1.8 *Let V be a finitely generated vector space and let $S \subseteq V$ be any linearly independent set. Then S can be "extended" to a basis of V i.e., there exists a basis B such that $S \subseteq B$.*

The size of all bases of a vector space is called the dimension of the vector space, denoted as $\dim(V)$. Using the above arguments, it is also easy to check that *any* linearly independent set of the right size must be a basis.

Exercise 1.9 *Let V be a finitely generated vector space and let S be a linearly independent set with $|S| = \dim(V)$. Prove that S must be a basis of V.*

1.2 Lagrange interpolation

Lagrange interpolation is used to find the unique polynomial of degree at most $n - 1$, taking given values at n distinct points. We can derive the formula for such a polynomial using basic linear algebra.

Let $a_1, \ldots, a_n \in \mathbb{R}$ be distinct. Say we want to find the unique (why?) polynomial p of degree at most $n-1$ satisfying $p(a_i) = b_i \; \forall i \in [n]$. Recall that the space of polynomials of degree at most $n-1$ with real coefficients, denoted by $\mathbb{R}^{\leq n-1}[x]$, is a vector space. Also, recall from the last lecture that if we define $g(x)$ as $\prod_{i=1}^{n}(x - a_i)$, the degree $n-1$ polynomials defined as

$$f_i(x) \;=\; \frac{g(x)}{x - a_i} \;=\; \prod_{j \neq i}^{n}(x - a_j)\,,$$

are n linearly independent polynomials in $\mathbb{R}^{\leq n-1}[x]$. Thus, they must form a basis for $\mathbb{R}^{\leq n-1}[x]$ and we can write the required polynomial, say p as

$$p \;=\; \sum_{i=1}^{n} c_i \cdot f_i\,,$$

for some $c_1, \ldots, c_n \in \mathbb{R}$. Evaluating both sides at a_i gives $p(a_i) = b_i = c_i \cdot f_i(a_i)$. Thus, we get

$$p(x) \;=\; \sum_{i=1}^{n} \frac{b_i}{f_i(a_i)} \cdot f_i(x)\,.$$

1.3 Secret Sharing

Note that the only property of the field $\mathbb{R}$ we used in Lagrange interpolation, was the fact that $\mathbb{R}$ is large enough to contain n distinct points $a_1, \ldots, a_n$. Check that the same argument can be used to find a polynomial of degree at most $n-1$ in the space $\mathbb{F}[x]$ for any field $\mathbb{F}$ such that $|\mathbb{F}| \geq n$. This can then be used to develop another nice application as below.

Consider the problem of sharing a secret with a group of n people, such that if any d of them get together, they are able to learn the secret message. However, if fewer than d of them are together, they do not get any information about the secret. We can then proceed as follows:

- Choose a finite field, say $\mathbb{F}_p$, with $p > n$ and such that secret message can be encoded as an element (say) b_0 of the field.
- Choose distinct points $a_0, \ldots, a_n \in \mathbb{F}_p$.
- Choose a polynomial $Q \in \mathbb{F}_p^{\leq d-1}[x]$ such that $Q(a_0) = b_0$ (why should such a polynomial always exist?)
- Disclose the points $\{a_0, \ldots, a_n\}$ to everyone. Also, disclose the value $b_i = Q(a_i)$ to the i^{th} person for each $i \in [n]$.

Note that if any group of d or more people get together, they can uniquely determine the polynomial Q by Lagrange interpolation. They can then recover the secret by evaluating Q at b_0. However, if fewer than d of them gather, then there is always a polynomial consistent with the values they hold, and any possible value at a_0. To precisely say that they learn nothing about the secret, we will choose $a_0, \ldots, a_n$ as well as Q at random. We will analyze this later when we discuss probability in the second half of the course.