

## Lecture 2: September 29, 2016

Lecturer: Madhur Tulsiani

## 1 Linear Independence and Bases

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

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

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 its proof will be very useful.

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

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

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

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

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  $S$  such that  $\text{Span}(S) = V$ . It is easy to see that a finitely generated vector space has a basis (which is a subset of the generating set  $S$ ). Also, the following is an easy corollary of the Steinitz exchange principle.

**Corollary 1.6** *All bases of a finitely generated vector space have equal size.*

The size of all bases of a vector space is called the dimension of the vector space.

## 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  $a_1, \dots, a_n \in \mathbb{R}$  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

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

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  $c_1, \dots, c_n \in \mathbb{R}$ . 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 Existence of bases in general vector spaces

To prove the existence of a basis for every vector space, we will need Zorn's Lemma (which is equivalent to the axiom of choice). We first define the concepts needed to state and apply the lemma.

**Definition 1.7** Let  $X$  be a non-empty set. A relation  $\preceq$  between elements of  $X$  is called a partial order

- $x \preceq x$  for all  $x \in X$ .
- $x \preceq y, y \preceq x \Rightarrow x = y$ .
- $x \preceq y, y \preceq z \Rightarrow x \preceq z$ .

The relation is called a partial order since not all the elements of  $X$  may be related. A subset  $S \subseteq X$  is called totally ordered if for every  $x, y \in S$  we have  $x \preceq y$  or  $y \preceq x$ . A set  $S \subseteq X$  is called bounded if there exists  $x_0 \in X$  such that  $x \preceq x_0$  for all  $x \in S$ . An element  $x_0 \in X$  is maximal if there does not exist any other  $x \in X$  such that  $x_0 \preceq x$ .

**Proposition 1.8 (Zorn's Lemma)** Let  $X$  be a partially ordered set such that every totally ordered subset of  $X$  is bounded. Then  $X$  contains a maximal element.

We can use Zorn's Lemma to in fact prove a stronger statement than the existence of a basis.

**Proposition 1.9** Let  $V$  be a vector space over a field  $\mathbb{F}$  and let  $S$  be a linearly independent subset. Then there exists a basis  $B$  of  $V$  containing the set  $S$ .

**Proof:** Let  $X$  be the set of all linearly independent subsets of  $V$  that contain  $S$ . For  $S_1, S_2 \in X$ , we say that  $S_1 \preceq S_2$  if  $S_1 \subseteq S_2$ . Let  $Y$  be a totally ordered subset of  $X$ . Define  $S_0$  as

$$S_0 := \bigcup_{T \in Y} T = \{v \in V \mid \exists T \in Y \text{ such that } v \in T\}.$$

Then we claim that  $S_0$  is linearly independent and is hence in  $X$ . It is clear that  $T \preceq S_0$  for all  $T \in Y$  and this will prove that  $Y$  is bounded by  $T$ . By Zorn's Lemma this shows that  $X$  contains a maximal element (say)  $B$ , which must be a basis containing  $S$ .

To show that  $S_0$  is linearly independent, note that we only need to show that no finite subset of  $S_0$  is linearly dependent. Indeed, let  $\{v_1, \dots, v_k\}$  be a finite linearly subset of  $S_0$ . By the definition of  $S_0$ , there exists a  $T \in X$  such that  $\{v_1, \dots, v_k\} \subseteq T$ . Thus,  $\{v_1, \dots, v_k\}$  must be linearly independent. This proves the claim. ■