Mathematical Toolkit **Autumn 2023**

Lecture 2: September 28, 2023

Lecturer: Madhur Tulsiani

1 Span and Bases

Recall the definition of the span of a set, discussed in the previous lecture.

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. Also, since linear combinations of vectors are still in V, we have* $\text{Span}(S) \subseteq V$. *In fact, you can check that* $\text{Span}(S)$ *is also a vector space. Such a subset of V, which is also a vector space, is called a* subspace *of V.*

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* $\text{Span}(B) = V$.

We will say that a set $B \subseteq V$ is a maximal linearly independent set if B is linearly independent and for all $v \in V \setminus B$, $B \cup \{v\}$ is linearly dependent. It is often useful to use the following alternate characterization of a basis.

Proposition 1.4 *A set $B \subseteq V$ is a basis for V if and only if B is a maximal linearly independent set.*

Proof: We will prove the "if" part and leave the other part as an exercise. If B is a maximal linearly independent set, then we already know that it is linearly independent, and only need to show that $\text{Span}(B) = V$. By the maximality property, we have that

for all $v \in V \setminus B$, the set $B \cup \{v\}$ is linearly dependent. Thus, for some $n \in \mathbb{N}$, there exist $v_1, \ldots, v_n \in B \cup \{v\}$ and $c_1, \ldots, c_n \in \mathbb{F}$ such that $\sum_{i=1}^{n} c_i \cdot v_i = 0_V$. Also, v must be one of the vectors $v_!, \ldots, v_n$ with a non-zero coefficient (otherwise we have a linear dependency in B itself). Thus, v can be written as a linear combination of the other v_is and we have $v \in \text{Span}(B)$ for all $v \in V \setminus B$. Since it is also true that $B \subseteq \text{Span}(B)$, we get that $V = \text{Span}(B)$. ■

We will now discuss a tool that'll be very helpful in arguing about bases of vector spaces.

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 $j \in [n], w_j \in \text{Span}(\{v_1, \ldots, v_k\} \setminus \{v_i\})$. However, this implies

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

which is a contradiction. ■

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 vector space V. Then, they must have the same size i.e., $k = n$.*

Note that we are already assuming in the above statement that the bases are finite, which may not necessarily be the case for all vector spaces. The above is just saying that *if* there happen to be two finite bases, then they must be of equal sizes.

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 $n \leq k$.

Note that the above argument just needs that we can remove elements from B_1 and replace them by new elements from B_2. While it is true that the intermediate sets we will construct will also be bases, we don't need this to argue $k \leq n$. □

1.1 Finitely generated spaces

A vector space V is said to be finitely generated if there exists a finite set T such that $\text{Span}(T) = V$. Note that Corollary 1.6 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 What if V is not finitely generated?

Of course, it need not always be the case that the vector space we are dealing with is finitely generated. For example, the vector space $\mathbb{R}[x]$ of polynomials has no finite generating set (since the maximum degree in any finite set T generating set will be an upper bound on the degree of polynomials in Span (T).) However, it is still the case that every vector space has a (possibly infinite) basis, such that all elements can be expressed as *finite* linear combinations of the basis elements. Such a basis is known as a Hamel basis. We will present the argument for existence of a Hamel basis below, in case you are interested. However, this will not be incuded in tests or homeworks for the class.

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 1.10 *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 $Z \subseteq X$ is called totally ordered *if for every $x, y \in Z$ we have $x \preceq y$ or $y \preceq x$. A set $Z \subseteq X$ is called* bounded *if there exists $x_0 \in X$ such that $z \preceq x_0$ for all $z \in Z$. An element $x_0 \in X$ is maximal if there does not exist any other $y \in X \in \{x_0\}$ such that $x_0 \preceq x$.*

Proposition 1.11 (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 (which we already saw for finitely generated vector spaces).

Proposition 1.12 *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 $T_1, T_2 \in X$, we say that $T_1 \preceq T_2$ if $T_1 \subseteq T_2$. Let Z be a totally ordered subset of X. Define T^* as

$$T^* := \bigcup_{T \in Z} T = \{v \in V \mid \exists T \in Z \text{ such that } v \in T\} .$$

Then we claim that T^* is linearly independent and is hence in X. It is clear that $T \preceq T^*$ for all $T \in Z$ and this will prove that Z 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 T^* is linearly independent, note that we only need to show that no *finite* subset of T^* is linearly dependent. Indeed, let $\{v_1, \ldots, v_n\}$ be a finite subset of T^*. By the definition of T^*, there exists a $T \in X$ such that $\{v_1, \ldots, v_n\} \subseteq T$. Thus, $\{v_1, \ldots, v_n\}$ must be linearly independent. This proves the claim. ∎

2 Linear Transformations

Definition 2.1 *Let V and W be vector spaces over the same field $\mathbb{F}$. A map $\varphi : V \to W$ is called a* linear transformation *if*

- $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) \quad \forall v_1, v_2 \in V.$
- $\varphi(c \cdot v) = c \cdot \varphi(v) \quad \forall v \in V.$

Example 2.2 *The following are all linear transformations:*

- *A matrix $A \in \mathbb{R}^{m \times n}$ defines a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$.*

- $\varphi : C([0,1],\mathbb{R}) \to C([0,2],\mathbb{R})$ *defined by* $\varphi(f)(x) = f(x/2)$.
- $\varphi : C([0,1],\mathbb{R}) \to C([0,1],\mathbb{R})$ *defined by* $\varphi(f)(x) = f(x^2)$.
- $\varphi : C([0,1],\mathbb{R}) \to C([0,1],\mathbb{R})$ *defined by* $\varphi(f)(x) = f(1-x)$.
- $\varphi_{\text{left}} : \mathbb{R}^{\mathbb{N}} \to \mathbb{R}^{\mathbb{N}}$ *defined by* $\varphi_{\text{left}}(f)(n) = f(n+1)$.
- *The derivative operator acting on* $\mathbb{R}[x]$.

Proposition 2.3 *Let V, W be vector spaces over $\mathbb{F}$ and let B be a basis for V. Let $\alpha : B \to W$ be an arbitrary map. Then there exists a unique linear transformation $\varphi : V \to W$ satisfying $\varphi(v) = \alpha(v)\ \forall v \in B$.*

3 Answer to the puzzle problem

In the previous lecture, we asked the following question:

Problem 3.1 ([Mat10]) *Let x be an irrational number. Use linear algebra to show that a rectangle with sides 1 and $\sqrt{2}$ cannot be tiled with a finite number of non-overlapping squares.*

We can now solve it given our current knowledge of linear algebra. Recall that $\mathbb{R}$ is a vector space over $\mathbb{Q}$ and 1 and $\sqrt{2}$ are linearly independent elements of this vector space. Let us assume that $S_1, \ldots, S_n$ are squares with side lengths $\ell_1, \ldots, \ell_n$, which tile the rectangle R. Let $S = \text{Span}\left(\left\{1, \sqrt{2}, \ell_1, \ldots, \ell_n\right\}\right)$.

Since there exists a basis for S containing 1 and $\sqrt{2}$, and since any map from this basis to $\mathbb{R}$ defines a unique linear transformation, there exists a linear transformation $\varphi : S \to \mathbb{R}$ satisfying $\varphi(1) = 1$ and $\varphi(\sqrt{2}) = -1$. Define the (area like) function $\mu : S \times S \to \mathbb{R}$ as $\mu(a,b) = \varphi(a) \cdot \varphi(b)$. For a rectangle R_0 with sides $a, b \in S$, we use $\mu(R_0)$ to denote $\mu(a,b)$.

One can show that if we extend all line segments bounding the squares to the sides of R then the sides of all new rectangles generated this way, lie in S and hence μ is defined for all these rectangles. Also, it is easy to check that μ adds like area i.e., if a rectangle R_3 is split in to R_1 and R_2, then $\mu(R_3) = \mu(R_1) + \mu(R_2)$. This gives

$$\varphi(1) \cdot \varphi(\sqrt{2}) \;=\; \mu(R) \;=\; \sum_{i=1}^{n} \mu(S_i) \;=\; \sum_{i=1}^{n} \left(\varphi(\ell_i)\right)^2 ,$$

which is a contradiction since the LHS is -1 while the RHS is non-negative.

References

[Mat10] Jiří Matoušek, *Thirty-three miniatures: Mathematical and algorithmic applications of linear algebra*, vol. 53, American Mathematical Soc., 2010. 5