Mathematical Toolkit **Autumn 2018**

Lecture 3: October 9, 2018

Lecturer: Madhur Tulsiani

1 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 1.1 *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 1.2 (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 1.3 *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 $Y\mathbb{Z}$ 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 linearly 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 $\varphi(v) = \alpha(v)\ \forall v \in B$.*

Definition 2.4 *Let $\varphi : V \to W$ be a linear transformation. We define its* kernel *and* image *as:*

- $\ker(\varphi) := \{v \in V \mid \varphi(v) = 0_W\}$.
- $\mathrm{im}(\varphi) = \{\varphi(v) \mid v \in V\}$.

Proposition 2.5 $\ker(\varphi)$ *is a subspace of V and* $\mathrm{im}(\varphi)$ *is a subspace of W.*

Proposition 2.6 (rank-nullity theorem) *If V is a finite dimensional vector space and $\varphi : V \to W$ is a linear transformation, then*

$$\dim(\ker(\varphi)) + \dim(\mathrm{im}(\varphi)) \;=\; \dim(V)\,.$$

$\dim(\mathrm{im}(\varphi))$ is called the rank and $\dim(\ker(\varphi))$ is called the nullity of φ.

Example 2.7 *Consider the matrix A which defines a linear transformation from $\mathbb{F}_2^7$ to $\mathbb{F}_2^3$:*

$$A \;=\; \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

- $\dim(\mathrm{im}(\varphi)) = 3$.
- $\dim(\ker(\varphi)) = 4$.
- *Check that* $\ker(\varphi)$ *is a* code *which can recover from one bit of error.*
- *Check that this is also true for the $(2^k - 1) \times k$ matrix A_k where the i^{th} column is the number i written in binary (with the most significant bit at the top).*

This code is known as the Hamming Code and the matrix A is called the parity-check matrix of the code.

3 Eigenvalues and eigenvectors

Definition 3.1 *Let V be a vector space over the field $\mathbb{F}$ and let $\varphi : V \to V$ be a linear transformation. $\lambda \in \mathbb{F}$ is said to be an* eigenvalue *of φ if there exists $v \in V \setminus \{0_V\}$ such that $\varphi(v) = \lambda \cdot v$. Such a vector v is called an* eigenvector *corresponding to the eigenvalue λ. The set of eigenvalues of φ is called its* spectrum*:*

$$\mathrm{spec}(\varphi) = \{\lambda \mid \lambda \textit{ is an eigenvalue of } \varphi\}\ .$$

Example 3.2 *Consider the following transformations:*

- *Differentiation is a linear transformation on the class of (say) infinitely differentiable functions and each function of the form $c \cdot \exp(\lambda x)$ is an eigenvector with eigenvalue λ.*
- *Consider the transformation $\varphi_{\mathrm{left}} : \mathbb{R}^{\mathbb{N}} \to \mathbb{R}^{\mathbb{N}}$. Any geometric progression with common ratio r is an eigenvector of φ_{left} with eigenvalue r (and these are the only eigenvectors for this transformation).*