Mathematical Toolkit **Autumn 2025**

Lecture 3: October 7, 2025

Lecturer: Madhur Tulsiani

1 Specifying a Linear Transformation

While some times linear transformations are specified as matrices, the following gives a more abstract way of characterizing a linear transformation.

Proposition 1.1 *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 $\varphi(v) = \alpha(v)\ \forall v \in B$.*

The above can also be used to give a linear-algebraic solution to be beautiful problem from [Mat10] (try it without reading the solution).

Problem 1.2 ([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.

2 Kernel and Image of a Linear Transformation

Definition 2.1 *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 2.2 $\ker(\varphi)$ *is a subspace of V and* $\mathrm{im}(\varphi)$ *is a subspace of W.*

Proposition 2.3 (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 2.4 *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 matrix*

$$M = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix},$$

which can be viewed as a linear transformation from $\mathbb{R}^2$ *to* $\mathbb{R}^2$*. Note that*

$$\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 2x_1 \\ 0 \end{bmatrix} = \lambda \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

is only satisfied if $\lambda = 0, x_1 = 0$ *or* $\lambda = 2, x_2 = 0$*. Thus* $\text{spec}(M) = \{0, 2\}$*.*

Example 3.3 *It can also be the case that* $\text{spec}(\varphi) = \emptyset$*, as witnessed by the rotation matrix*

$$M_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},$$

when viewed as a linear transformation from $\mathbb{R}^2$ *to* $\mathbb{R}^2$*.*

Example 3.4 *Consider the following transformations:*

- *Differentiation is a linear transformation on the class of (say) infinitely differentiable real-valued functions over* $[0, 1]$ *(denoted by* $C^\infty([0, 1], \mathbb{R})$*). Each function of the form* $c \cdot \exp(\lambda x)$ *is an eigenvector with eigenvalue* λ*. If we denote the transformation by* φ_0*, then* $\text{spec}(\varphi_0) = \mathbb{R}$*.*

- *We can also consider the transformation* $\varphi_1 : \mathbb{R}[x] \to \mathbb{R}[x]$ *defined by differentiation i.e., for any polynomial* $P \in \mathbb{R}[x]$*,* $\varphi_1(P) = dP/dx$*. Note that now the only eigenvalue is 0, and thus* $\text{spec}(\varphi) = \{0\}$*.*

- *Consider the transformation* $\varphi_{\text{left}} : \mathbb{R}^{\mathbb{N}} \to \mathbb{R}^{\mathbb{N}}$*. 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).*

Proposition 3.5 *Let* $U_\lambda = \{v \in V \mid \varphi(v) = \lambda \cdot v\}$*. Then for each* $\lambda \in \mathbb{F}$*,* U_λ *is a subspace of* V*.*

Note that $U_\lambda = \{0_V\}$ if λ is not an eigenvalue. The dimension of this subspace is called the geometric multiplicity of the eigenvalue λ.

Proposition 3.6 *Let* $\lambda_1, \ldots, \lambda_k$ *be distinct eigenvalues of* φ *with associated eigenvectors* $v_1, \ldots, v_k$*. Then the set* $\{v_1, \ldots, v_k\}$ *is linearly independent.*

Proof: We can prove via induction that for all $r \in [k]$, the subset $\{v_1, \ldots, v_r\}$ is independent. The base case follws from the fact that $v_1 \neq 0_V$, and thus $\{v_1\}$ is a linearly independent set. For the induction step, assume that that the set $\{v_1, \ldots, v_r\}$ is linearly independent.

If the set $\{v_1, \ldots, v_{r+1}\}$ is linearly *dependent*, there exist scalars $c_1, \ldots, c_{r+1} \in \mathbb{F}$ such that

$$c_1 \cdot v_1 + \cdots + c_{r+1} \cdot v_{r+1} \ = \ 0_V \,.$$

Also, note that we must have at least one of $c_1, \ldots, c_r \neq 0$ (since $v_{r+1} \neq 0$). Applying φ on both sides gives

$$\lambda_1 \cdot c_1 \cdot v_1 + \cdots + \lambda_{r+1} \cdot c_{r+1} \cdot v_{r+1} \ = \ 0_V \,.$$

Multiplying the first equality by λ_{r+1} and substracting the two gives

$$(\lambda_1 - \lambda_{r+1}) \cdot c_1 \cdot v_1 + \cdots (\lambda_r - \lambda_{r+1}) c_r \cdot v_r \ = \ 0_V \,.$$

Since all the eigenvalues are distinct, and at least one of $c_1, \ldots, c_r$ is non-zero, the above shows that $\{v_1, \ldots, v_r\}$ is linearly dependent, which contradicts the inductive hypothesis. Thus, the set $v_1, \ldots, v_{r+1}$ must be linearly independent. ■

References

[Mat10] Jiří Matoušek, *Thirty-three miniatures: Mathematical and algorithmic applications of linear algebra*, vol. 53, American Mathematical Soc., 2010. 1