Linear Algebra in Combinatorics – Live Notes

Krit Boonsiriseth

April 19, 2022

Check-in 1. Can you see the lecture notes (i.e. this file)?

Answer. Hopefully yes!

1 Vector spaces

- A **vector space** V **over a field** $\mathbb{F}$ is a set of **vectors** in which we can (i) add vectors together, and (ii) multiply vectors by **scalars**, which are elements of the field $\mathbb{F}$.

  We often denote vectors by writing an arrow above them $\vec{v}$, or with bold text $\mathbf{v}$. Vector addition is usually denoted by the usual plus sign $+$, and scalar multiplication is written as concatenation: $a\vec{v}$ denotes the vector $\vec{v}$ multiplied (or *scaled*) by the scalar a.

- Usually, the *field* $\mathbb{F}$ we will consider will either be the reals $\mathbb{R}$, the complex numbers $\mathbb{C}$, or a prime finite field $\mathbb{F}_p$ (basically addition and multiplication in mod p).

- Formally, the operations of a vector space V need to satisfy some axioms:

  i. $(V, +)$ is an *abelian group*, i.e. V has an associative and commutative addition $(+)$ with identity element $\vec{0}$ and additive inverses.

  ii. For the identity $1 \in \mathbb{F}$, for any $\alpha, \beta \in \mathbb{F}$, and for any $\vec{v}, \vec{w} \in V$ the following properties must hold:

     - $1\vec{v} = \vec{v}$
     - $(\alpha\beta)\vec{v} = \alpha(\beta\vec{v})$
     - $(\alpha + \beta)\vec{v} = \alpha\vec{v} + \beta\vec{v}$
     - $\alpha(\vec{v} + \vec{w}) = \alpha\vec{v} + \alpha\vec{w}$.

- Usually, the *field* $\mathbb{F}$ we will consider will either be the reals $\mathbb{R}$, the complex numbers $\mathbb{C}$, or a prime finite field $\mathbb{F}_p$ (basically addition and multiplication in mod p).

- A prototypical example of a vector space is $\mathbb{R}^n$, in which we often denote vectors by a tuple of n real numbers like this (this example is in $\mathbb{R}^3$), and addition and scalar multiplication works as expected.

$$\begin{bmatrix}1\\2\\3\end{bmatrix} + \begin{bmatrix}10\\-10\\0\end{bmatrix} = \begin{bmatrix}11\\-8\\3\end{bmatrix}, \qquad 5\begin{bmatrix}1\\2\\3\end{bmatrix} = \begin{bmatrix}5\\10\\15\end{bmatrix}$$

  You have probably seen this way of writing vectors in high school math! Using *column* vectors like this is the preferred way of writing vectors, but it can take up a lot of space, so I'll also write vectors like this: $[1, 2, 3]$.

  Check-in 2. Is $\mathbb{R}$ a vector space over $\mathbb{R}$?

Answer. Yes! We can add real numbers ('vectors') together, and we can multiply a real number ('vector') by another real number ('scalar').

Another example of a vector space is the set of complex numbers $\mathbb{C}$ over the field $\mathbb{R}$. In fact, this is the same vector space as $\mathbb{R}^2$, where $a + bi$ is the vector $[a, b]$

Yet another example of a vector space is the set of functions $f : \mathbb{R} \to \mathbb{R}$, with pointwise addition and scalar multiplication.

- A vector $\vec{w}$ is said to be a **linear combination** of vectors $v_1, \dots, v_k$ if there are scalars $a_1, \dots, a_k$ such that

$$a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_k\vec{v}_k = \vec{w}.$$

- The **span** of a set S of vectors is the set of all vectors that can be written as a linear combination of the vectors in S. A set S of vectors is said to be a **spanning set** of V if it spans the entire vector space V.

Check-in 3. Is the set $\left\{ \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix} \right\} \subset \mathbb{R}^3$ a spanning set?

Answer. No. The vector $\begin{bmatrix}0\\0\\1\end{bmatrix}$ cannot be written as a linear combination of the two given vectors.

- A set $S = \{\vec{v}_1, \dots, \vec{v}_k\}$ is said to be **linearly independent** if, for scalars $a_1, \dots, a_k$,

$$a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_k\vec{v}_k = \vec{0}$$

implies $a_1 = a_2 = \cdots = a_k = 0$. Otherwise, S is said to be **linearly dependent**.

Check-in 4. Is the set $\left\{ \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix} \right\} \subset \mathbb{R}^3$ linearly independent?

Answer. Yes.

- A set S of vectors is said to be a **basis** of V if it is linearly independent and also a spanning set of V.

If $S = \{\vec{v}_1, \dots, \vec{v}_k\}$ is a basis of V, then for all $\vec{w} \in V$, there is a *unique* choice of scalars $a_1, \dots, a_k$ such that

$$a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_k\vec{v}_k = \vec{w}.$$

For example, the set

$$\left\{ \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix} \right\}$$

is a basis of $\mathbb{R}^3$. This is called the **standard basis** of $\mathbb{R}^3$. This is far from the only basis of $\mathbb{R}^3$ though.

Check-in 5. Is the set $\left\{ \begin{bmatrix}2\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}0\\1\\-1\end{bmatrix} \right\}$ a basis of $\mathbb{R}^3$?

Answer. Yes!

Check-in 6. Must all bases of $\mathbb{R}^3$ have exactly 3 elements?

Answer. Yes!

- In fact, all bases of a vector space V must have the same size, and this is called the **dimension** of V. This dimension can also be infinite (such as in the vector space of functions $f : \mathbb{R} \to \mathbb{R}$), but we will mostly concern ourselves with finite-dimensional vector spaces.

  A related fact that will be very useful is: if we have an n-dimensional vector space V then

  i. any set of $> n$ vectors must be linearly dependent, and

  ii. any set of $< n$ vectors cannot be a spanning set.

- A **subspace** of a vector space V is a subset of V that also forms a vector space. For example, the plane $\{[x, y, z] : z = 0\}$ is a subspace of $\mathbb{R}^3$.

2 Linear transformations

- In high school, we learned that a **matrix** is something that looks like this

$$M = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}.$$

  However, I'd like you all to think of matrices as **linear transformations**, which are maps between vector spaces that preserves the vector-space-ness, and a matrix M here corresponds to the map $\vec{v} \mapsto M\vec{v}$.

- Formally, a **linear transformation** $T : V \to W$ (where V and W are vector spaces over the same field $\mathbb{F}$) is a map that respects addition and scalar multiplication, i.e.

$$T(\vec{v} + \vec{w}) = T(\vec{v}) + T(\vec{w}) \quad \text{and } T(a\vec{v}) = aT(\vec{v}).$$

- An $m \times n$ matrix (with m rows, n columns) with real entries is a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$.

- For a linear transformation T, the set $\{T(\vec{v})\}$ is called the **image** of T, and the set $\{v \in V : T(\vec{v}) = 0\}$ is called the **kernel** of V.

- Going back to the 2×3 matrix M defined above, we see that the vector $\begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$ lies in the kernel of (the transformation given by M), because

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Check-in 7. Is $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ in the image of the transformation given by the matrix M above?

Answer. Yes, and in fact the image *and* the kernel of any transformation always contain the zero vector.

Check-in 8. Are the vectors $\begin{bmatrix}1\\0\end{bmatrix}$ and $\begin{bmatrix}0\\1\end{bmatrix}$ both in the image of the transformation given by the matrix M above?

Answer. Yes. It's a bit trickier to see here, but $M\begin{bmatrix}2/3\\-1/3\\0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$, and $M\begin{bmatrix}-1\\0\\2/3\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$.

Check-in 9. Are there any vectors in the kernel of M that is *not* of the form $\begin{bmatrix}a\\-2a\\a\end{bmatrix}$ for some $a \in \mathbb{R}$?

Answer. No, but you might need to convince yourself for a bit.

Let's try to find some takeaways from all this. First, we note that both the kernel and the image of M are also vector spaces. In fact, they are subspaces of $V = \mathbb{R}^3$ and $W = \mathbb{R}^2$ respectively.

Also note that here, the kernel, which is spanned by $\left\{\begin{bmatrix}1\\-2\\1\end{bmatrix}\right\} \subset \mathbb{R}^3$, is a subspace of $\mathbb{R}^3$. In general, the span of any set $S \subset V$ is a subspace of V.

- We might also notice that $\dim\ker M = 1$, and $\dim\operatorname{im} M = 2$. It turns out that $1+2 = 3 = \dim\mathbb{R}^3$. This is not a coincidence! In general, we have the following very useful formula:

  Theorem (Dimension formula)**.** *For any linear transformation $T : V \to W$,*

  $$\dim\ker T + \dim\operatorname{im} T = \dim V.$$

  This is also called the **rank-nullity theorem** because $\dim\operatorname{im} T$ is also known as the **rank** of T, and $\dim\ker T$ is also known as the **nullity** of T.

- As you would expect, the **rank** of a matrix is defined to be the rank of the linear transformation corresponding to that matrix. The rank of a matrix is also equal to the dimension of its *column space* (i.e. the space spanned by its column vectors) as well as its *row space* (i.e. the space spanned by its row vectors).

  For example, the rank of

  $$\begin{bmatrix}1 & 2 & 3\\4 & 5 & 6\end{bmatrix}$$

  is 2.

- Some useful facts about ranks of matrices:

  i. For an $m \times n$ matrix A, $\operatorname{rank}(A) \le \min\{m, n\}$.
  ii. For matrices A and B, $\operatorname{rank}(AB) \le \min\{\operatorname{rank}(A), \operatorname{rank}(B)\}$.
  iii. For matrices $A + B$, $\operatorname{rank}(A + B) \le \operatorname{rank}(A) + \operatorname{rank}(B)$.

  Another important fact is that the rank of the $n \times n$ identity matrix I_n is equal to n.

- In general, a square $n \times n$ matrix is said to be **full rank** if its rank is exactly n.

- A matrix A has full rank if and only if it is **invertible**.

3 Finally, a problem!

- **Oddtown problem.** In a certain town with n citizens, a number of clubs are set up. No two clubs have exactly the same set of members. The size of every club is odd, and every pair of (distinct) clubs share an even number of members. What is the maximum number of clubs in this town?

- Let's first try to find a good construction. First, if every citizen form their own lonely club, then we get n clubs. Can we do better? In fact, we can't!

- Let's prove an upper bound of n on the number of clubs. Suppose that there are m clubs. Number the citizens of the town from 1 to n, and for each club, form a vector in $\{0,1\}^n$, such that the c-th entry of the vector is 1 if citizen c is a member of the club (this is known as the **incidence vector** of the club). If we have m clubs, then we get m vectors $\vec{v}_1, \ldots, \vec{v}_m$ in $\{0,1\}^n$, and we wish to show that $m \leq n$.

- Since each club has an odd number of members, each $\vec{v}_i$ has an odd number of ones, therefore $\vec{v}_i \cdot \vec{v}_i$ is odd for all i.

- Since every pair of (distinct) clubs share an even number of members, for all distinct i, j, the vector $\vec{v}_i \cdot \vec{v}_j$ is even! (This is because the dot product counts the number of indices where v_i and v_j are both 1.)

- Now consider the $n \times m$ matrix

$$M = \begin{bmatrix} | & | & & | \\ \vec{v}_1 & \vec{v}_2 & \cdots & \vec{v}_m \\ | & | & & | \end{bmatrix}.$$

It follows that

$$M^T M = \begin{bmatrix} \vec{v}_1 \cdot \vec{v}_1 & \vec{v}_1 \cdot \vec{v}_2 & \cdots & \vec{v}_1 \cdot \vec{v}_m \\ \vec{v}_2 \cdot \vec{v}_1 & \vec{v}_2 \cdot \vec{v}_2 & \cdots & \vec{v}_2 \cdot \vec{v}_m \\ \vdots & \vdots & \ddots & \vdots \\ \vec{v}_m \cdot \vec{v}_1 & \vec{v}_m \cdot \vec{v}_2 & \cdots & \vec{v}_m \cdot \vec{v}_m \end{bmatrix} = \begin{bmatrix} \text{odd} & & \text{even} \\ & \text{odd} & \\ & & \ddots & \\ \text{even} & & & \text{odd} \end{bmatrix}$$

- Let's actually consider this over the field $\mathbb{F}_2$ instead of over $\mathbb{R}$. (This is basically taking integers modulo 2; we can do this for any prime and all the linear algebra will still work out.) Then, it follows that $M^T M = I_m$.

- Taking ranks, we therefore have

$$m = \text{rank}(I_m) = \text{rank}(M^T M) \leq \text{rank}(M) \leq \min\{m, n\},$$

therefore $m \leq n$.