Apprentice Linear Algebra, 1st day, 6/27/05

REU 2005

Instructor: László Babai
Scribe: Eric Patterson

Definitions 1.1.

- An *abelian group* is a set G with the following properties:

  (i) $(\forall a, b \in G)(\exists! a + b \in G)$

  (ii) the addition in (i) is associative

  (iii) $(\exists 0)(\forall a \in G)(a + 0 = a)$

  (iv) $(\forall a)(\exists b)(a + b = 0)$

  (v) $a + b = b + a$

- A *vector space* is an abelian group $(V, +)$ with a multiplication by scalars:

  – $(\forall \alpha \in \mathbb{R})(\forall \mathbf{a} \in V)(\exists! \alpha\mathbf{a} \in V)$

  – $(\alpha\beta)\mathbf{a} = \alpha(\beta\mathbf{a})$

  – $(\alpha + \beta)\mathbf{a} = \alpha\mathbf{a} + \beta\mathbf{a}$

  – $\alpha(\mathbf{a} + \mathbf{b}) = \alpha\mathbf{a} + \alpha\mathbf{b}$

Theorem 1.2. *$\alpha\mathbf{a} = 0 \Leftrightarrow \alpha = 0$ or $\mathbf{a} = 0$.*

Corollary 1.3. *$(-1)\mathbf{a} = -\mathbf{a}$.*

Examples 1.4. Some examples of vector spaces.

1. $\mathbb{R}^n$
2. geometric vectors in 2 or 3 dimensions
3. $k \times \ell$ matrices
4. $C[0, 1]$, the continuous functions from $[0, 1]$ to $\mathbb{R}$
5. the space of infinite sequences
6. $\mathbb{R}^\Omega$, the functions from Ω to $\mathbb{R}$

- $\Omega = \{1, \dots, n\}$ is example 1 above
- $\Omega = \{1, \dots, k\} \times \{1, \dots, \ell\}$ is example 3
- $\Omega = [0, 1]$ contains example 4
- $\Omega = \mathbb{N}$ is example 5

Definitions 1.5.
- A *linear combination* of $\mathbf{a}_1, \dots, \mathbf{a}_k \in V$ is a sum $\sum_{i=1}^{k} \alpha_i \mathbf{a}_i$ for some $\alpha_1, \dots, \alpha_k \in \mathbb{R}$.

- The *span* of $\mathbf{a}_1, \dots, \mathbf{a}_k$, written $\text{Span}(\mathbf{a}_1, \dots, \mathbf{a}_k)$, is the set of all linear combinations of $\mathbf{a}_1, \dots, \mathbf{a}_k$. More generally, for a possibly infinite subset S of V, $\text{Span}(S)$ is the set of all linear combinations of all finite subsets. By convention, $\text{Span}(\emptyset) = \{\mathbf{0}\}$.

- A *subspace* of V is a subset W which is a vector space under the same operations. This is written $W \leq V$. Equivalently, a subset W is a subspace if it is nonempty and closed under addition and multiplication by scalars:

  1. $W \neq \emptyset$
  2. $(\forall \mathbf{a}, \mathbf{b} \in W)(\mathbf{a} + \mathbf{b} \in W)$
  3. $(\forall \mathbf{a} \in W)(\forall \lambda \in \mathbb{R})(\lambda \mathbf{a} \in W)$.

  Equivalently, a subspace is a nonempty subset closed under linear combinations.

  Corollary 1.6. *$W \leq V$ iff $\text{Span}(W) = W$.*

  Exercise 1.7. If $S \subseteq W$, then $\text{Span}(S) \leq W$.

- The vectors $\mathbf{a}_1, \dots, \mathbf{a}_k$ are *linearly independent* if $(\forall \alpha_1, \dots \alpha_k \in \mathbb{R})(\sum_{i=1}^{k} \alpha_i \mathbf{a}_i = 0 \Rightarrow \alpha_1 = \dots = \alpha_k = 0)$. An infinite set of vectors is linearly independent if all finite subsets are linearly independent. If a set of vectors is not linearly independent, it is *linearly dependent*.

Examples 1.8. Some more examples of vector spaces.

- $\mathbb{R}[x] = \{\text{polynomials with real coefficients}\}$.

- $\mathbb{R}(x) = \{\text{rational functions with real coefficients}\}$. That is, the set of $\frac{p}{q}$ with p, $q \in \mathbb{R}[x]$, $q \neq 0$, and $\frac{p_1}{q_1} = \frac{p_2}{q_2}$ iff $p_1 q_2 = p_2 q_1$.

Claim 1.9. *$\{\frac{1}{x-\alpha} : \alpha \in \mathbb{R}\}$ is linearly independent in $\mathbb{R}(x)$.*

Definitions 1.10.
- Let $S \subseteq V$. The *rank* of S, $\text{rk}(S)$, is the maximum number of linearly independent vectors in S.

- Let $W \leq V$. The *dimension* of W, $\dim(W)$, is the rank of W.

- Let $B \subseteq W \leq V$. B is a *basis* of W if (i) $\text{Span}(B) = W$ and (ii) B is linearly independent.

- A vector $\mathbf{a}$ depends on a set $S \subseteq V$ if $\mathbf{a} \in \mathrm{Span}(S)$.

Corollary 1.11. $\{\mathbf{a}_1, \ldots, \mathbf{a}_k\}$ *is a basis of* W *if* $(\forall w \in W)$ $(\exists! \alpha_1, \cdots, \alpha_k \in \mathbb{R})(\sum \alpha_i \mathbf{a}_i = w)$.

If $\{\mathbf{a}_1, \ldots, \mathbf{a}_k\}$ is a basis for W and $w \in W$, then the *coordinates* of w with respect to the basis $\{\mathbf{a}_1, \ldots, \mathbf{a}_k\}$ is the column vector of the unique α_i given by the corollary; we write

$$[w]_{\{\mathbf{a}_1, \ldots, \mathbf{a}_k\}} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{bmatrix}.$$

The coordinates of w depend on the choice of basis for W. Later we shall see how coordinate vectors change under change of basis.

Observation 1.12. A set of vectors S is linearly dependent iff there is a member which depends on the rest.

Note 1.13. A set containing $\mathbf{0}$ is never linearly independent. Also, a sequence of vectors with repetitions is never linearly independent.

Exercise 1.14. Prove that these functions are linearly independent in $\mathbb{R}^{\mathbb{R}}$: $1, \cos x, \sin x, \cos 2x, \sin 2x, \ldots, \cos nx, \sin nx, \ldots$.

Theorem 1.15 (Magic #1). *If* $\mathbf{u}_1, \ldots, \mathbf{u}_k \in \mathrm{Span}(\mathbf{v}_1, \ldots, \mathbf{v}_\ell)$ *and* $\mathbf{u}_1, \ldots, \mathbf{u}_k$ *are linearly independent, then* $k \leq \ell$.

(Prove later.)

Corollary 1.16. *If* B_1 *and* B_2 *are bases of* W*, then* $|B_1| = |B_2|$.

Exercise 1.17. Every vector space has a basis. In fact, every set of generators contains a basis, and every linearly independent set can be extended to a basis.

Exercise 1.18. Let $L \subseteq G \subseteq W$, and suppose $\mathrm{Span}(G) = W$. If L is linearly independent, then there is a basis B such that $L \subseteq B \subseteq G$.

Lemma 1.19. *If* $\mathbf{a}_1, \ldots, \mathbf{a}_k$ *are linearly independent but* $\mathbf{a}_1, \ldots, \mathbf{a}_{k+1}$ *are linearly dependent then* $\mathbf{a}_{k+1} \in \mathrm{Span}(\mathbf{a}_1, \ldots, \mathbf{a}_k)$.

The polynomials $1, x, x^2, \ldots$ are a basis for $\mathbb{R}[x]$, showing that $\dim \mathbb{R}[x]$ is countable. However, $\dim \mathbb{R}(x)$ is uncountable since $\{\frac{1}{x-\alpha} : \alpha \in \mathbb{R}\}$ is linearly independent and uncountable.

A sequence $(\alpha_0, \alpha_1, \alpha_2, \ldots)$ is a Fibonacci-type sequence if for $n \geq 2$, $\alpha_n = \alpha_{n-1} + \alpha_{n-2}$. Let F be the set of all Fibonacci-type sequences. The Fibonacci-type sequence with $\alpha_0 = 0$ and $\alpha_1 = 1$ is called the Fibonacci sequence, $f = (0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots)$.

Claim 1.20. F *is a 2-dimensional subspace of* $\mathbb{R}^{\mathbb{N}}$.

A geometric sequence is one of the form $(1, q, q^2, \dots)$. Can a geometric sequence be a Fibonacci-type sequence?

Exercise 1.21. The sequence $(1, q, q^2, \dots)$ is Fibonacci-type iff $1 + q = q^2$.

The equation $q^2 = q + 1$ has two solutions: $\frac{1 \pm \sqrt{5}}{2}$. The two geometric sequences $(1, \frac{1+\sqrt{5}}{2}, \dots)$ and $(1, \frac{1-\sqrt{5}}{2}, \dots)$ are linearly independent and, thus, a basis for F.

Corollary 1.22. *The Fibonacci sequence is a linear combination of these two geometric sequences.*

Exercise 1.23. The nth term in the Fibonacci sequence is

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Exercise 1.24.

$$f_n = \left\lfloor \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n \right\rceil$$

where $\lfloor x \rceil$ means round x to the nearest integer.

Definitions 1.25. A $k \times \ell$ matrix can be considered a set of ℓ columns, $[\mathbf{a}_1, \dots, \mathbf{a}_\ell]$, or a set of k rows, $[\mathbf{b}_1, \dots, \mathbf{b}_k]$. The *row space* of the matrix is the span of these rows: $\text{Span}(\mathbf{b}_1, \dots, \mathbf{b}_k) \leq \mathbb{R}^\ell$. Similarly, the *column space* of the matrix is the span of the columns: $\text{Span}(\mathbf{a}_1, \dots, \mathbf{a}_\ell) \leq \mathbb{R}^k$. The *row-rank* of the matrix is the dimension of the row space, and the *column-rank* of the matrix is the dimension of the column space.

Theorem 1.26 (Magic #2). *For any $k \times \ell$ matrix, the column rank and the row rank are equal.*

Exercise 1.27. Prove. (Do not use determinants).

Fisher's Inequality

Let $t \geq 1$. Let $A_1, \dots, A_m$ be subsets of $\{1, \dots, n\}$ such that

$$(\forall i \neq j)(|A_i \cap A_j| = t). \tag{1}$$

How big can m be? If $t = 1$, we can find n such sets.

Examples 1.28.

- Let $A_i = \{i, n\}$ for $i = 1, \dots, n-1$ and $A_n = \{1, \dots, n-1\}$.
- For $n = 7$, the Fano Plane is a remarkable set of 7 subsets of size 3 of $\{1, \dots, 7\}$ with pairwise intersection size $t = 1$.

Theorem 1.29 (Fisher's Inequality). *Condition (1) implies $m \leq n$.*

Definition 1.30. For $A \subseteq \{1, \ldots, n\}$, define the *incidence vector* v_A as $v_A = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$ where $\alpha_i = \begin{cases} 1 & \text{if } i \in A \\ 0 & \text{if } i \notin A \end{cases}$

Fisher's Inequality follows from Magic #1 and the following exercise.

Exercise 1.31. Let $\mathbf{a}_1, \ldots, \mathbf{a}_m$ be incidence vectors for sets $A_1, \ldots, A_m$ such that $(\forall i \neq j)(|A_i \cap A_j| = t)$. Then $\mathbf{a}_1, \ldots, \mathbf{a}_m$ are linearly independent in $\mathbb{R}^n$.