REU 2005 - LINEAR ALGEBRA - LECTURE 2

Instructor: László Babai
Scribe: Justin Noel
June 29, 2005.

2. Lecture 2

2.1. Rank, Magic #1.

V is a vector space, that is, $(V,+)$ is an abelian group and we have a map $\mathbb{R} \times V \to V$, $(\lambda, \mathbf{a}) \mapsto \lambda \mathbf{a}$.

Definition 2.1. A set $\mathbf{a_1}, \dots, \mathbf{a_k} \in V$ are **linearly independent** if $(\forall \alpha_i \in \mathbb{R})(\sum_{i=1}^{k} \alpha_i \mathbf{a_i} = 0 \Longrightarrow \alpha_1 = \dots = \alpha_k = 0)$. In other words, only the trivial linear combination gives zero.

Definition 2.2. A set $\mathbf{b_1}, \dots, \mathbf{b_s} \in V$ **span** (or generate) V iff $(\forall \mathbf{a} \in V)(\exists \beta_1, \dots, \beta_s \in \mathbb{R})(\sum_{i=1}^{s} \beta_i \mathbf{b_i} = \mathbf{a})$.

Definition 2.3. $\mathrm{Span}(\mathbf{b_1}, \dots, \mathbf{b_s}) = \{\sum_{i=1}^{s} \beta_i \mathbf{b_i} \mid \beta_i \in \mathbb{R}\}$.

We say that $\mathbf{v}$ **depends** on $\mathbf{b_1}, \dots, \mathbf{b_s}$ if $\mathbf{v} \in \mathrm{Span}(\mathbf{b_1}, \dots, \mathbf{b_s})$.

Proposition 2.4. *Transitivity of linear dependence: If* $\mathbf{a_1}, \dots, \mathbf{a_k}$ *each depends on* $\mathbf{b_1}, \dots, \mathbf{b_\ell}$ *and* $\mathbf{b_1}, \dots, \mathbf{b_\ell}$ *each depends on* $\mathbf{c_1}, \dots, \mathbf{c_m}$ *then* $\mathbf{a_1}, \dots, \mathbf{a_k}$ *each depends on* $\mathbf{c_1}, \dots, \mathbf{c_m}$. *In other words, if* $A, B, C \subseteq V$, $A \subseteq \mathrm{Span} B$ *and* $B \subseteq \mathrm{Span} C$ *then* $A \subseteq \mathrm{Span} C$.

Exercise 2.5. $\mathrm{Span}(\mathrm{Span}(C)) = \mathrm{Span} C$.

Definition 2.6. $W \leqslant V$ is a subspace if $W \subseteq V$ and W is a vector space under the same operations. Equivalently $W \leqslant V$ iff $W \neq \emptyset$ and W is closed under addition and multiplication by scalars (i.e. it is closed under linear combinations).

Corollary 2.7. $W \leqslant V \Longleftrightarrow W = \mathrm{Span}(W)$.

Corollary 2.8. *For any set* A *of vectors in* V, $\mathrm{Span}(A) \leqslant V$. *Moreover,* $\mathrm{Span}(A)$ *is the* ***smallest*** *subspace containing* A : *If* $W \leqslant V$ *and* $A \subseteq W \Longrightarrow \mathrm{Span} A \subseteq W$.

Corollary 2.9. $\mathrm{Span} A = \bigcap_{A \subseteq W \leqslant V} W$.

Proposition 2.10. *If* $\mathbf{v_1}, \dots, \mathbf{v_k}$ *are linearly independent and* $\mathbf{v_1}, \dots, \mathbf{v_k}, \mathbf{v_{k+1}}$ *are linearly dependent then* $\mathbf{v_{k+1}}$ *depends on* $\mathbf{v_1}, \dots, \mathbf{v_k}$. *In other words* $\mathbf{v_{k+1}} \in \mathrm{Span}(\mathbf{v_1}, \dots, \mathbf{v_k})$, *i.e.* $(\exists \alpha_1, .., \alpha_k \in \mathbb{R})(\mathbf{v_{k+1}} = \sum_{i=1}^{k} \alpha_{ik} \mathbf{v_i})$.

Theorem 2.11 (Magic #1)**.** *If* $\mathbf{v_1}, \dots, \mathbf{v_k}$ *are linearly independent and each depends on* $\mathbf{w_1}, \dots, \mathbf{w_\ell}$ *then* $k \leq \ell$.

The proof is based on the

Theorem 2.12 (Steinitz Exchange Principle)**.** *If* $\mathbf{a_1}, \dots, \mathbf{a_k}$ *are linearly independent and each depends on* $\mathbf{b_1}, \dots, \mathbf{b_\ell}$ *then* $\exists j$ *such that* $\mathbf{b_j}, \mathbf{a_2}, \dots, \mathbf{a_k}$ *are linearly independent.*

Proof. We proceed by contradiction. Suppose $\forall j$ we have $\mathbf{b_j}, \mathbf{a_2}, \ldots, \mathbf{a_k}$ are linearly dependent, i.e. $(\forall j)(\mathbf{b_j} \in \text{Span}\{\mathbf{a_2}, \ldots, \mathbf{a_k}\}$. Since $\mathbf{a_1} \in \text{Span}\{\mathbf{b_1}, \ldots, \mathbf{b_\ell}\} \subseteq \text{Span}\{\mathbf{a_1}, \ldots, \mathbf{a_k}\}$ we have $\mathbf{a_1} \in \text{Span}\{\mathbf{a_2}, \ldots, \mathbf{a_k}\}$. But this is a contradiction since $\mathbf{a_1}, \ldots, \mathbf{a_k}$ are linearly independent. $\square$

Corollary 2.13. *If* $\mathbf{a_1}, \ldots, \mathbf{a_k}$ *are linearly independent and* $(\forall i)(\mathbf{a_i} \in \text{Span}\{\mathbf{b_1}, \ldots, \mathbf{b_\ell}\})$ *then* $(\forall i)(\exists j)(\mathbf{a_1}, \ldots, \mathbf{a_{i-1}}, \mathbf{b_j}, \mathbf{a}_{i+1}, \ldots, \mathbf{a_k})$ *are linearly independent).*

Proof. (Of Magic #1) By repeatedly applying 2.13 we can replace $\mathbf{v_1}$ with some $\mathbf{w_{j_1}}$ and then $\mathbf{v_2}$ with some $\mathbf{w_{j_2}}$ and so on. At each stage $\mathbf{w_{j_1}}, \ldots, \mathbf{w_{j_i}}, \mathbf{v}_{i+1} \ldots, \mathbf{v_k}$ are linearly independent. And we have that $\mathbf{w_{j_1}}, \ldots, \mathbf{w_{j_k}}$ are linearly independent and therefore distinct. So among the $\mathbf{w_1}, \ldots, \mathbf{w_\ell}$ there are k distinct vectors and therefore $k \leq \ell$. $\square$

Definition 2.14. If $\mathbf{v_1}, \ldots, \mathbf{v_m} \in V$ we say that $\mathbf{v_{i_1}}, \ldots, \mathbf{v_{i_k}}$ is a **basis** of $\mathbf{v_1}, \ldots, \mathbf{v_k}$if

(1) $\mathbf{v_{i_1}}, \ldots, \mathbf{v_{i_k}}$ are linearly independent .
(2) $(\forall j)\mathbf{v_j} \in \text{Span}\left\{\mathbf{v_{i_1}}, \ldots, \mathbf{v_{i_k}}\right\}$.

Exercise 2.15. If $\mathbf{v_{i_1}}, \ldots, \mathbf{v_{i_t}}$ are linearly independent then they can be extended to a basis of $\mathbf{v_1}, \ldots, \mathbf{v_m}$.

Exercise 2.16. Every *maximal* linearly independent set of $\mathbf{v_i}$ is a basis of $\mathbf{v_1}, \ldots, \mathbf{v_m}$.

Theorem 2.17. *All bases of* $\mathbf{v_1}, \ldots, \mathbf{v_m}$ *have the same size.*

Definition 2.18. This size is called the **rank** of $\mathbf{v_1}, \ldots, \mathbf{v_m}$.

Definition 2.19. The **row-rank** (resp. the **col-rank**) of a matrix (α_{ij}) is defined to be the rank of the row vectors, $\mathbf{v_1} = (\alpha_{11}, \ldots, \alpha_{1n}), \ldots, \mathbf{v_n} = (\alpha_{n1}, \ldots, \alpha_{nn})$ (resp. the column vectors, $\mathbf{w_1} = (\alpha_{11}, \ldots, \alpha_{n1}), \ldots, \mathbf{w_n} = (\alpha_{1n}, \ldots, \alpha_{nn})$.

2.2. Column-rank and Row-rank of matrices.

Theorem 2.20 (Magic #2)**.** *For a matrix row-rank=col-rank.*

Example 2.21. Diagonal matrices: $A = (\alpha_{ij})$ such that if $i \neq j$ then $\alpha_{ij} = 0$.

$$\begin{pmatrix} \alpha_{11} & 0 & 0 & 0 \\ 0 & \alpha_{22} & 0 & 0 \\ 0 & 0 & \alpha_{33} & 0 \end{pmatrix}.$$

We have that the rank of $A = \text{diag}(\alpha_{11}, \ldots, \alpha_{kk})$ is the number of nonzero diagonal entries.

Definition 2.22. The **transpose,** A^T, of a matrix $A = (\alpha_{ij})$ is defined as $A^T = (\alpha_{ji})$.

Since the transpose of a diagonal matrix is diagonal we see that Magic #2 is true for diagonal matrices.

Definition 2.23. There are two **elementary row operations**:

(1) $\begin{pmatrix} \mathbf{a_1} \\ \vdots \\ \mathbf{a_k} \end{pmatrix}$ $\mathbf{a_i} := \mathbf{a_i} + \lambda\mathbf{a_j}$, $\lambda \in \mathbb{R}$ and $j \neq i$.
(2) Permutation of rows.

Theorem 2.24 (Row-rank invariance)**.** *Elementary row operations do not change the row-rank or the column-rank.*

Proof. (Hints) After applying an elementary operation every row vector remains in the span of the row vectors before the operation. So by Magic #1 the row-rank can only get smaller. Since the inverse of an elementary operation is another elementary operation, we have that the row-rank must not change under elementary operations

For column rank invariance we check that if the column vectors $b_1,..,b_s$ are linearly dependent before applying a row operation they remain linearly dependent after and satisfy the same nontrivial linear relation. $\square$

2.3. **Linear algebra methods in combinatorics.**

2.3.1. *Fisher's Inequality.*

Theorem 2.25 (Fisher's Inequality)**.** *If* $A_1,..,A_m \subseteq \{1,\ldots,n\}$, $t \geq 1$ *and* $(\forall i \neq j)(\left|A_i \cap A_j\right| = t)$ *then* $m \leq n$.

Proof. (Hint) Under these conditions the *incidence vectors* of the A_i are linearly independent (see proof below). So we have m linearly independent vectors in $\mathbb{R}^n \implies m \leq n$ by Magic #1. $\square$

Definition 2.26. $A \subseteq \{1,\ldots,n\}$. The **incidence vector** of A, $\gamma_{\mathbf{A}} = (\gamma_1,\ldots,\gamma_n) \in \mathbb{R}^n$, is defined by $\gamma_i = \begin{cases} 1 & i \in A \\ 0 & i \notin A \end{cases}$.

Definition 2.27 (Inner Product in $\mathbb{R}^n$)**.** If $\mathbf{a} = (\alpha_1,\ldots,\alpha_n)$ and $\mathbf{b} = (\beta_1,\ldots,\beta_n)$ then $\mathbf{a}\cdot\mathbf{b} = \sum_{i=1}^n \alpha_i\beta_i$.

This inner product satisfies the following formulae:

(1) $\mathbf{a}\cdot(\mathbf{b}+\mathbf{c}) = \mathbf{a}\cdot\mathbf{b}+\mathbf{a}\cdot\mathbf{c}$
(2) $\mathbf{a}\cdot(\sum_{i=1}^k \gamma_i\mathbf{c_i}) = \sum_{i=1}^k \gamma_i\mathbf{a}\cdot\mathbf{c_i}$.
(3) $\mathbf{a}\cdot\mathbf{b} = \mathbf{b}\cdot\mathbf{a}$

Proposition 2.28. *If* $A,B \subseteq \{1,\ldots,n\}$ *and* $\mathbf{v}_A,\mathbf{v}_B$ *are their respective incidence vectors then* $\mathbf{v}_A\cdot\mathbf{v}_B = |A\cap B|$.

Example 2.29. Let $A = \{1,2,5\}, B = \{2,3,5\}$ then $\mathbf{v}_A = (1,1,0,0,1)$, $\mathbf{v}_B = (0,1,1,0,1)$ and $\mathbf{v}_A\cdot\mathbf{v}_B = 1\cdot0+1\cdot1+0\cdot1+0\cdot0+1\cdot1 = 2 = |A\cap B|$.

Notation 2.30. Under Fisher's conditions with incidence vectors $\mathbf{v_1} = \mathbf{v}_{A_1},\ldots,\mathbf{v_m} = \mathbf{v}_{A_m} \in \mathbb{R}^n$ for $i \neq j$, $\mathbf{v_i}\cdot\mathbf{v_j} = t$ and $\mathbf{v_i}\cdot\mathbf{v_i} = |A_i| = k_i$.

Definition 2.31. $A_1,\ldots,A_m$ is a **sunflower** if $(\exists C)(\forall i \neq j)(A_i \cap A_j = C)$. C is called the **kernel** of the sunflower.

Proof. (Of 2.25 continued) $\square$

Case 1. $(\exists i_0)(k_{i_0} = t) \implies (\forall j)(A_j \supseteq A_{i_0})$. In this case, we have a sunflower and it is easy to very that the $\mathbf{v_i}$ are linearly independent.

Case 2. $(\forall i)(k_i > t)$ $\mathbf{v_1},..,\mathbf{v_m} \in \mathbb{R}^n$, $i \neq j$, $\mathbf{v_i}\cdot\mathbf{v_j} = t$ and $\mathbf{v_i}\cdot\mathbf{v_i} = k_i > t$.

Lemma 2.32. *If* $\mathbf{v_1},\ldots,\mathbf{v_m} \in \mathbb{R}^n$, $t \in \mathbb{R}$, $(\forall i \neq j)(\mathbf{v_i}\cdot\mathbf{v_j} = t)$ *and* $(\forall i)(\mathbf{v_i}\cdot\mathbf{v_i} > t)$ *then* $\mathbf{v_1},\ldots,\mathbf{v_m}$ *are linearly independent.*

Note. We no longer assume that the $\mathbf{v_i}$ are incidence vectors or that t and $k_i = \mathbf{v_i}\cdot\mathbf{v_i}$ are integers.

Proof. Suppose $\sum_{i=1}^m \alpha_i \mathbf{v_i} = 0$. We want to show that $\alpha_1 = \cdots = \alpha_m = 0$.

We have

$$\begin{aligned} 0 &= \mathbf{v_1} \cdot \left(\sum_{i=1}^m \alpha_i \mathbf{v_i} \right) = \sum_{i=1}^m \alpha_i \left(\mathbf{v_1} \cdot \mathbf{v_i} \right) = t \sum_{i=1}^m \alpha_i - t\alpha_1 + \alpha_1 k_1 \\ &= t \left(\sum_{i=1}^m \alpha_i \right) + \alpha_1 (k_1 - t) \end{aligned}$$

so $t \left(\sum_{i=1}^m \alpha_i \right) = -\alpha_1 (k_1 - t)$. So $\forall j$ we have

$$\alpha_j = -\frac{t \left(\sum_{i=1}^m \alpha_i \right)}{k_j - t}. \tag{2.1}$$

If $\sum_{i=1}^m \alpha_i = 0$ then $(\forall j)(\alpha_j = 0)$. Assume now $\sum_{i=1}^m \alpha_i \neq 0$. Let us add 2.1 for $j = 1$ to m :

$$\sum_{j=1}^m \alpha_j = -t \sum_{j=1}^m \frac{1}{k_j - t} \cdot \sum_{i=1}^m \alpha_i.$$

Dividing both sides by $\sum_{j=1}^m \alpha_j$ we obtain $1 = -t \sum_{j=1}^m \frac{1}{k_j - t} < 0$ which is absurd.

□

This is an example of proving a combinatorial inequality using Linear Algebra. The method was initiated by R.C. Bose in 1949 who proved a special case of 2.25 (he assumed $|A_i| = \cdots = |A_m|$). To learn about other appilications of the method see Babai-Frankl's book *Linear Algebra Methods in Combinatorics.*

2.3.2. *Eventown and Oddtown.* There are n citizens in Eventown. They are forming a collection of clubs. No two clubs are permitted to have identical membership. So we have 2^n possible clubs if we allow the empty club. But in Eventown there are additional rules on the formation of clubs. Namely, the number of people in a given club A_i must be even and the number of people belonging to any two clubs is even. (i.e. $(\forall i, j)(|A_i|$ and $\left|A_i \cap A_j\right|$ are even)).

Exercise 2.33. Show that the number of even subsets of a given set is equal to the number of odd subsets. Give a "combinatorial proof" (explicit matching) and an "algebra proof" (use the binomial theorem).

Exercise 2.34. For what n is it the case that the number of subsets of size divisible by 4 is 2^{n-2}.

Hint: Use complex numbers and the binomial theorem.

Exercise 2.35. Generalize this.

One way to saitsfy the Eventown rules is to pair up the citizens and insist that each pair join exactly the same clubs. This "married couples" solution yields $2^{\lfloor \frac{n}{2} \rfloor}$ clubs.

Exercise 2.36. * Show that $2^{\lfloor \frac{n}{2} \rfloor}$ is the maximum number of possible clubs under Eventown rules.

Exercise 2.37. * Show that there exists $2^{\lfloor \frac{n}{2} \rfloor}$ possible clubs under Eventown rules that isn't given by a "married couples" solution.

Oddtown is also forming a collection of clubs $\{A_i\}$. In Oddtown the rules dictate that for all i, j $|A_i|$ is odd and $\left|A_i \cap A_j\right|$ is even.

Exercise 2.38. There are at least $2^{\frac{n^2}{8}}$ ways to form n clubs in Oddtown.

Exercise 2.39. (Oddtown Theorem) Under Oddtown rules, $m \leq n$, (where m is the number of clubs and n is the number of citizens).

Definition 2.40. Informally a **field** is a set with the usual notions of addition, subtraction, multiplication and division.

Example 2.41. The following are fields $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ and $\mathbb{F}_p$ for p a prime.

Exercise 2.42. A, B are $k \times \ell$ matrices over a field $\mathbb{F}$ show that $\operatorname{rank}(A+B) \leq \operatorname{rank} A + \operatorname{rank} B$.

Exercise 2.43. A is a $k \times \ell$ matrix and B is an $\ell \times m$ matrix then $\operatorname{rank}(AB) \leq \min(\operatorname{rank} A, \operatorname{rank} B)$. And therefore

$$\operatorname{rank}(AA^T) \leq \operatorname{rank} A.$$

Exercise 2.44. Over $\mathbb{R}$: $\operatorname{rank}(AA^T) = \operatorname{rank} A$.

Exercise 2.45. Show that this is false $\mathbb{F} = \mathbb{C}$ or $\mathbb{F} = \mathbb{F}_p$ for all primes p. In fact, over each of these fields, there exist matrices A of large rank such that $AA^T = 0$.