REU 2013: Apprentice Program **Summer 2013**

Lecture 2: June 25, 2013

Madhur Tulsiani Scribe: Young Kun Ko

1 Lagrange Interpolation continued

Last class Lagrange interpolation was left as a homework exercise. In fact you can explicitly calculate the coefficients for the polynomial. $\alpha_j = b_j/f_j(a_j)$ where $b_j = f(a_j)$. Set $f(x) = \sum \alpha_j f_j(x)$. The following exercise is a simple application of Lagrange interpolation.

Exercise 1.1 (Secret Sharing) *Say you are given five generals. You want to ensure that at least three generals are needed to get a code to launch a nuclear weapon. How do you ensure this ?*

Proof: Consider the following scheme.

- Pick a degree-2 polynomial f, such that $f(0) = code$.
- Pick $a_1, a_2, \ldots, a_5 \neq 0$. Let $f(a_i) = b_i$.
- Give (a_i, b_i) to ith general

■

2 Return to Linear Algebra

Theorem 2.1 *Every vector space V has a basis*

Proof Sketch:

1. Pick any $v \in V$. Set $\mathcal{B} = \{v\}$
2. While $\mathcal{B}$ is not a maxima linearly independent set of vectors, that is $\exists w \in V$ such that $\mathcal{B} \cup \{w\}$ is linearly independent, $\mathcal{B} \leftarrow \mathcal{B} \cup \{w\}$.

This process gives a basis if we have abn upper boound on the size of a linearly independent set in V. In fact, then the above proof also shows that any linearly independent set of vectors in V can be extended to a basis.

If no such bound is available, one needs to Zorn's lemma from set theory which shows that a linearly independent set of vectors can be extended to a maximal one. □

Definition 2.2 (Subspace) *U is a subspace of V denoted $U \leqslant V$ if $U \subseteq V$ and U is a vector space closed under $(+, \cdot)$ as defined for V.*

Definition 2.3 (rank, dimension) *For $U \subseteq V$,*

$$rank(U) = \text{maximum number of linearly independent vectors in } U$$

If U is a subspace of V, then $rank(U)$ is also called dimension of U, denoted $dim(U)$.

Example 2.4 *Let $V = \{(a_0, a_1, a_2, \ldots) : a_i \in \mathbb{R}\}$ be the space of sequences of real numbers. Then the set $\{e_1 = (1, 0, 0, \ldots), e_2 = (0, 1, 0, \ldots), \ldots\}$ is* not *a basis of V. We require that every element of the vector space can be written as a* finite *linear combination of the basis elements and (for example) the sequence $(1, 1, 1, \ldots)$ can be written as a finite combination of $e_1, e_2, \ldots$.*

Zorn's lemma shows that such a basis (known as a Hamel basis) does exists for this space. However, Zorn's lemma is equivalent to the axiom of choice and it does not give any explicit description of this basis.

Exercise 2.5 *Consider $U = \{(a_0, a_1, a_2, \ldots) : a_i \in \mathbb{R}\}$ where $a_{n+2} = a_{n+1} + a_n,\ \forall n \in \{0\} \cup \mathbb{N}$ which is a subspace of V as defined above. This is called Fibonacci Space.*

1. *What is $dim(U)$?*
2. *Find $v_r = (1, r, r^2, \ldots), v_s = (1, s, s^2, \ldots) \in U$ such that are linearly independent. Then write fibonacci sequence $F = (1, 1, 2, 3, 5, \ldots)$ as $F = \alpha_r v_r + \alpha_s v_s$.*

Exercise 2.6 (Graph Coloring) *Consider $G = (V, E)$. Recall that $deg(v) = \#$ of edges which include v. Define $deg(G) = \max_{v \in V}\{deg(v)\}$. A graph is "properly colored" with k colors if each v is assigned a color, and for any $(u, v) \in E$ u and v have different colors.*

1. *Prove that if $deg(G) \leq d$, it can be colored with $(d + 1)$ colors.*
2. *When can a graph G be 2-colored? Can you find a necessary and sufficient condition? How long does it take to test this condition?*

Exercise 2.7 (Polynomial Puzzle) *Take a circle of radius 1. Inscribe a n-sided regular polyhedron, with vertices labeled $P_0, P_1, \ldots, P_{n-1}$. Then prove that*

$$\prod_{i=1}^{n-1} \overline{P_0 P_i} \;=\; n\,.$$

(Hint: Complex numbers, polynomials)

2.1 Matrices

Definition 2.8 *A $m \times n$ matrix is of the form* $\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$ *where each $a_{ij} \in \mathbb{F}$.*

We can then view row A_i as being in $\mathbb{F}^n$ and column $A^{(j)}$ as being in $\mathbb{F}^m$.

Definition 2.9

$$\begin{aligned} \textit{row-rank}(A) &= \textit{rank}\{A_1, \ldots, A_m\} \\ \textit{column-rank}(A) &= \textit{rank}\{A^{(1)}, \ldots, A^{(n)}\} \end{aligned}$$

Theorem 2.10 (Second Miracle of Linear Algebra) *row-rank*$(A) =$ *column-rank*(A).

Definition 2.11 *column-space*$(A) = \textit{span}\{A^{(1)}, \ldots, A^{(n)}\}$

Exercise 2.12

1. *dim*(*column-space*(A)) = *column-rank*(A)
2. *Columns are linearly independent iff rows span* $\mathbb{F}^n$
3. *Rows are linearly independent iff columns span* $\mathbb{F}^m$

Definition 2.13 (Elementary row/column operations) *The following operations are called elementary row/column operations*

$$\begin{aligned} A_i &\leftarrow A_i - \lambda A_j \\ A^{(i)} &\leftarrow A^{(i)} - \lambda A^{(j)} \quad \lambda \in \mathbb{F}, j \neq i \end{aligned}$$

Exercise 2.14 *Elementary operations maintains row/column rank.*

Proof (2nd miracle): Let the term "leading entry" denote the leftmost non-zero entry in a row. Use elementary row operations (and row exchanges) to convert the matrix into a form (known as the row-reduced form) such that

1. All zero rows are below all the non-zero rows.
2. The leading entry in the i^{th} is to the right of the leading entries in rows $1, \ldots, i-1$.

In the above form, the the columns with the leading entries of the non-zero rows will be linearly independent, showing that *column-rank*$(A) \geq$ *row-rank*(A). Similarly, one can apply elementary column operations to A to show that *row-rank*$(A) \geq$ *column-rank*(A). ■

Definition 2.15 (Matrix multiplication) *Let A be a $m \times n$ matrix and B a $n \times p$ matrix. Then $A \cdot B$ is a $m \times p$ matrix defined as*

$$(A \cdot B)_{ij} = \sum_{l=1}^{n} A_{il} B_{lj}$$

Exercise 2.16 *Find 2×2 matrices A, B such that*

1. $A \cdot B \neq B \cdot A$
2. $A \neq 0$ *but* $A^2 = 0$

Exercise 2.17 *Given* $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, *find* A^k.