**Mathematical Toolkit** **Autumn 2016**

# Lecture 1: September 27, 2016

Lecturer: Madhur Tulsiani

The primary goal of this course is to collect a set of basic mathematical tools which are often useful in various areas of computer science. We will mostly focus on various applications of linear algebra and probability. Please see the course webpage for a more detailed list of topics.

The course will be evaluated on the basis of the following:

- Homeworks: 40% (four homeworks contributing 10% each)
- Quizzes: 10% (two quizzes contributing 5% each)
- Midterm: 20%
- Final: 30%

We will spend 3-4 of lectures reviewing some of the basic concepts of linear algebra before we move on to some of the applications.

Here's a couple of problems to think about if you are already familiar with the contents of this lecture. These are taken from the excellent book "Thirty Three Miniatures" by Jiří Matoušek [Mat10], which I highly recommend for many more fun applications of Linear Algebra.

**Problem 0.1** *Let $x$ be an irrational number. Use linear algebra to show that a rectangle with sides $1$ and $x$ cannot be tiled with a finite number of non-overlapping squares.*

**Problem 0.2** *Let $K_n$ denote the complete graph on the vertex set $[n] = \{1, \ldots, n\}$. Also, for disjoint $S, T \subseteq [n]$, let $K_{S,T}$ denote the complete bipartite graph with the edge set*

$$E_{S,T} = \{\{i, j\} \mid i \in S, j \in T\} .$$

*Show that if $(S_1, T_1), \ldots, (S_m, T_m)$ are such that each edge of $K_n$ is present in exactly one of the graphs $K_{S_i,T_i}$, then $m \geq n - 1$. Is this tight?*

## 1 Fields

A field, often denoted by $\mathbb{F}$, is simply a nonempty set with two associated operations $+$ and $\cdot$ mapping $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$, which satisfy:

- **commutativity**: $a + b = b + a$ and $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{F}$.
- **associativity**: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in \mathbb{F}$.
- **identity**: There exist elements $0_{\mathbb{F}}, 1_{\mathbb{F}} \in \mathbb{F}$ such that $a + 0_{\mathbb{F}} = a$ and $a \cdot 1_{\mathbb{F}} = a$ for all $a \in \mathbb{F}$.
- **inverse**: For every $a \in \mathbb{F}$, there exists an element $(-a) \in \mathbb{F}$ such that $a + (-a) = 0_{\mathbb{F}}$. For every $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, there exists $a^{-1} \in \mathbb{F}$ such that $a \cdot a^{-1} = 1_{\mathbb{F}}$.
- **distributivity of multiplication over addition**: $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbb{F}$.

**Example 1.1** $\mathbb{Q}$, $\mathbb{R}$ *and* $\mathbb{C}$ *with the usual definitions of addition and multiplication over these fields.*

**Example 1.2** *For any prime $p$, we can define addition and multiplication on $\mathbb{Q}^2$ as*

$$(a, b) + (c, d) = (a + c, b + d) \qquad \text{and} \qquad (a, b) \cdot (c, d) = (ac + pbd, ad + bc)\,.$$

*These operations define a field. This is equivalent to taking $\mathbb{F} = \left\{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\right\}$ with the same notion of addition and multiplication as for real numbers.*

**Example 1.3** *For any prime $p$, the set $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ (also denoted as GF(p)) is a field with addition and multiplication defined modulo $p$.*

**Exercise 1.4** *Show that the set $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ is a field.*

## 2 Vector Spaces

A vector space $V$ over a field $\mathbb{F}$ is a nonempty set with two associated operations $+ : V \times V \to V$ (vector addition) and $\cdot : \mathbb{F} \times V \to V$ (scalar multiplication) which satisfy:

- **commutatitivity of addition**: $v + w = w + v$ for all $v, w \in V$.
- **associativity of addition**: $u + (v + w) = (u + v) + w \ \forall u, v, w \in V$.

- **pseudo-associativity of scalar multiplication**: $a \cdot (b \cdot v) = (a \cdot b) \cdot v \; \forall a, b \in \mathbb{F}, v \in V$.
- **identity for vector addition**: There exists $0_V \in V$ such that for all $v \in V$, $v + 0_V = v$.
- **inverse for vector addition**:$\forall v \in V, \; \exists (-v) \in V$ such that $v + (-v) = 0_V$.
- **distributivity**: $a \cdot (v + w) = a \cdot v + a \cdot w$ and $(a + b) \cdot v = a \cdot v + b \cdot v$ for all $a, b \in \mathbb{F}$ and $v, w \in V$.
- **identity for scalar multiplication**: $1_{\mathbb{F}} \cdot v = v$ for all $v \in V$.

**Example 2.1** *Any field* $\mathbb{F}$ *is a vector space over itself.*

**Example 2.2** $\mathbb{R}$ *is a vector space over* $\mathbb{Q}$.

**Example 2.3** $\mathbb{R}[X]$ *is a vector space over* $\mathbb{R}$.

**Example 2.4** $C([0,1], \mathbb{R}) = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$ *is a vector space over* $\mathbb{R}$.

**Example 2.5** $\mathsf{Fib} = \left\{ f \in \mathbb{R}^{\mathbb{N}} \mid f(n) = f(n-1) + f(n-2) \; \forall n \geq 2 \right\}$ *is a vector space over* $\mathbb{R}$.

**Definition 2.6 (Linear Dependence)** *A set* $S \subseteq V$ *is* linearly dependent *if there exist distinct* $v_1, \ldots, v_n \in S$ *and* $a_1, \ldots, a_n \in \mathbb{F}$ *not all zero, such that* $\sum_{i=1}^{n} a_i \cdot v_i = 0_V$. *A set which is not linearly dependent is said to be* linearly independent.

**Example 2.7** *The set* $\left\{1, \sqrt{2}, \sqrt{3}\right\}$ *is linearly independent in the vector space* $\mathbb{R}$ *over the field* $\mathbb{Q}$.

**Exercise 2.8** *Let* $a_1, \ldots, a_n \in \mathbb{R}$ *be distinct and let* $g(x) = \prod_{i=1}^{n} (x - a_i)$. *Define*

$$f_i(x) \;=\; \frac{g(x)}{x - a_i} \;=\; \prod_{j \neq i} (x - a_j) \,,$$

*where we extend the function at point* $a_i$ *by continuity. Prove that* $f_1, \ldots, f_n$ *are linearly independent in the vector space* $\mathbb{R}[x]$ *over the field* $\mathbb{R}$.

**Exercise 2.9** *Prove that the set of functions*

$$S \;=\; \{1\} \cup \{\sin(kx) \mid k \in \mathbb{N}, k \geq 1\} \cup \{\cos(kx) \mid k \in \mathbb{N}, k \geq 1\} \;,$$

*is linearly independent in the vector space of continuous real-valued functions over* $\mathbb{R}$.

# References

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