Infimum/Supremum and Introduction to Abstract Linear Algebra

ROB 501

Course administration

- There are discussion sessions today and tomorrow
- HW#2 is going to be posted today
- GSI office hours **announced**:
  - Andrew Wintenberg: Mon 6-7pm, Tue 5-6pm
  - Ishank Juneja: Mon 12-1pm, Fri (With Zoom Option) 2-3pm
  - Location FRB 3310
- Next week (9/12, 9/14) lectures will be remote over Zoom

Exercise :

p	q	$\neg q$	$p \wedge \neg q$	$\neg(p \wedge \neg q)$
T	T	F	F	T
T	F	T	T	F
F	T	F	F	T
F	F	T	F	T

Quick review

- Proof techniques
  - Direct proof
  - Proof by contrapositive
  - Proof by exhaustion
  - Proof by induction (standard induction and strong induction)
  - Proof by contradiction
- Negating statements (used, e.g., when using proof by contradiction)

Ex: p : $x > 0$

$\neg p$: $x \leq 0$

Ex: p : $\forall x \in \mathbb{R}, f(x) > 0$

$\neg p$: not (for all $x \in \mathbb{R}$, $f(x) > 0$)

$\neg p$: for some $x \in \mathbb{R}$, not $(f(x) > 0)$

$\neg p$: for some $x \in \mathbb{R}$, $f(x) \leq 0$

$\neg p$: $\exists\, x \in \mathbb{R}$ s.t. $f(x) \leq 0$

*Pattern: $\neg \forall (\cdot) \longleftrightarrow \exists$ not $(\cdot)$

$\neg \exists (\cdot) \longleftrightarrow \forall$ not $(\cdot)$

<u>Ex:</u> Let $y \in \mathbb{R}$,

p: $\forall \varepsilon > 0$, $\exists\, x \in \mathbb{Q}$ s.t. $|x-y| < \varepsilon$

$\neg p$: For some $\varepsilon > 0$ not (there exist $x \in \mathbb{Q}$ s.t. $|x-y| < \varepsilon$)

$\neg p$: $\exists\, \varepsilon > 0$ not $\underbrace{(\exists\, x \in \mathbb{Q} \text{ s.t. } |x-y| < \varepsilon)}$

$\neg p$: $\exists\, \varepsilon > 0$ $\forall x \in \mathbb{Q}$ $\neg (\, |x-y| < \varepsilon)$

$\neg p$: $\exists\, \varepsilon > 0$ $\forall x \in \mathbb{Q}$, $|x-y| \geq \varepsilon$

Remark (on notation): $\nexists$, $\not\forall$ (short hand for

$\nexists$: there does not exist

$\not\forall$: not for all)

$\rightarrow$ better to avoid

Rob 501 Handout[1]

Supremum versus Maximum
and
Infimum versus Minimum

Let A be a subset of the reals, $\mathbb{R}$.

Def. An element $b \in A$ is a *maximum* of A if $x \leq b$ for all $x \in A$. We note that in the definition, b must be an element of A. We denote it by max A or max$\{A\}$.

$(0, 1)$
$\shortparallel$

Remark: A *max* of a set may not exist! Indeed, the set $A = \{x \in \mathbb{R} \mid 0 < x < 1\}$ does not have a maximum element. We will see later that it does not have a minimum either. This is what motivates the notions of supremum and infimum.

Def. An element $b \in \mathbb{R}$ is an *upper bound* of A if $x \leq b$ for all $x \in A$. We say that A is *bounded from above.*

Ex: For $A = (0,1)$ 1, 10, 5234 are all upper bounds of A.

Remark: We note that in the definition of upper bound, b does NOT have to be an element of A.

Def. An element $b^* \in \mathbb{R}$ is the $\overbrace{\textit{least upper bound}}^{= \text{supremum}}$ of A if

Ex: $A = (0,1)$
$\sup A = 1$

1. b^* is an upper bound, that is $\forall\, x \in A$, $x \leq b^*$, and
2. if $b \in \mathbb{R}$ satisfies $x \leq b$ for all $x \in A$, then $b^* \leq b$.

Notation and Vocabulary. The least least upper bound of A is also called the **supremum** and is denoted

$$\sup A \quad \text{or} \quad \sup\{A\}$$

[1] Courtesy of Jessy Grizzle

Theorem If $A \subset \mathbb{R}$ is bounded from above, then $\sup\{A\}$ exists.

Examples:

- $A = \{x \in \mathbb{R} \mid 0 < x < 1\}$. Then $\sup A = 1$.
- $A = \{x \in \mathbb{R} \mid x^2 \leq 2\}$. Then $\sup A = \sqrt{2}$.

Remark: The existence of a *supremum* is a special property of the real numbers. If you are working within the rational numbers, a bounded set may not have a rational supremum. Of course, if you view the set as a subset of the reals, it will then have a supremum.

Examples:

- $A = \{x \in \mathbb{Q} \mid 0 < x < 1\}$. Then $\sup A = 1$. Indeed, 1.0 is a rational number, it is an upper bound, and it less than or equal to any other upper bound; hence it is the supremum.
- $A = \{x \in \mathbb{Q} \mid x^2 \leq 2\}$. Then $(1.42)^2 = 2.0164$, and thus $b = 1.42$ is a rational upper bound. Also $(1.415)^2 = 2.002225$, and thus $b = 1.1415$ is a smaller rational upper bound. However, there is no least upper bound within the set of rational numbers. When we view the set A as being a subset of the real numbers, then there is a real number that is a least upper bound and we have $\sup A = \sqrt{2}$. This is what I mean when I say that the existence of a supremum is a special or distinguishing property of the real numbers.

Remark: If the *supremum* is in the set A, then it is equal to the *maximum*.

Consider once again a set A contained in the real numbers, that is $A \subset \mathbb{R}$.

Def. An element $b \in A$ is a *minimum* of A if $b \leq x$ for all $x \in A$. We note that in the definition, b must be an element of A. We denote it by min A or min$\{A\}$.

$A = (0,1)$ does not have a minimum

Remark: A *min* of a set may not exist! Indeed, the set $A = \{x \in \mathbb{R} \mid 0 < x < 1\}$ does not have a minimum element.

Def. An element $b \in \mathbb{R}$ is a *lower bound* of A if $b \leq x$ for all $x \in A$. We say that A is *bounded from below.*

Ex: For $A = (0,1)$ -100, -10, 0 are all lower bounds

Remark: We note that in the definition of lower bound, b does NOT have to be an element of A.

Def. An element $b^* \in \mathbb{R}$ is the *greatest lower bound* of A if

1. b^* is a lower bound, that is $\forall\, x \in A$, $b^* \leq x$, and
2. if $b \in \mathbb{R}$ satisfies $b \leq x$ for all $x \in A$, then $b^* \geq b$.

$\equiv$ infimum

Ex: $A = (0,1)$

inf $A = 0$

Notation and Vocabulary. The greatest lower bound of A is also called the **infimum** and is denoted

$$\inf A \quad \text{or} \quad \inf\{A\}$$

Theorem If the set A is bounded from below, then inf A exists.

Examples:

- $A = \{x \in \mathbb{R} \mid 0 < x < 1\}$. Then $\inf A = 0$.
- $A = \{x \in \mathbb{R} \mid x^2 \leq 2\}$. Then $\inf A = -\sqrt{2}$.

Remark: If the *infimum* is in the set A, then it is equal to the *minimum.*

What is ∞? A symbol! $+\infty$ satisfies $\forall x \in \mathbb{R}$ $x < +\infty$

∞ is not in $\mathbb{R}$ $-\infty$ satisfies $\forall x \in \mathbb{R}$ $x > -\infty$

Additional detail: If $A \subset \mathbb{R}$ is not bounded from above, we define $\sup A = +\infty$. If $A \subset \mathbb{R}$ is not bounded from below, we define $\inf A = -\infty$. Of course $+\infty$ and $-\infty$ are not real numbers. The *extended real numbers* are sometimes defined as

$$\mathbb{R}_e := \underline{\{-\infty\} \cup \mathbb{R} \cup \{+\infty\}}.$$

Final Remark: MATH 451 <u>constructs</u> the real numbers from the rational numbers! This is a very cool process to learn. Unfortunately, we do not have the time to go through this material in ROB 501. The existence of supremums and infimums for bounded subsets of the real numbers is a consequence of how the real numbers are defined (i.e., constructed)!

- Real numbers is a scalar <u>field</u>.

<u>Abstract linear algebra</u>:

What are scalars? What are vectors?

Fields

A field consists of a set $\mathcal{F}$ of scalars and two operators: addition "+", and multiplication "·" such that

Set $\mathcal{F}$, $+$, $\cdot$

$\forall \alpha, \beta \in \mathcal{F}$ $\overbrace{\alpha+\beta}^{\text{sum}} \in \mathcal{F}$

1. $\mathcal{F}$ is closed under addition and multiplication

   $\forall \alpha, \beta \in \mathcal{F}$ $\underbrace{\alpha \cdot \beta}_{\text{product}} \in \mathcal{F}$

2. Addition and multiplication are commutative

   $\forall \alpha, \beta \in \mathcal{F}$ $\alpha + \beta = \beta + \alpha$, $\forall \alpha, \beta \in \mathcal{F}$ $\alpha \cdot \beta = \beta \cdot \alpha$

3. Addition and multiplication are associative

   $\forall \alpha, \beta, \gamma \in \mathcal{F}$ $(\alpha+\beta)+\gamma = \alpha + (\beta+\gamma)$, $\forall \alpha, \beta, \gamma \in \mathcal{F}$ $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

4. Multiplication is distributive over addition

   dition and multi

   $\forall \alpha, \beta, \gamma \in \mathcal{F}$ $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$

5. $\mathcal{F}$ contains additive (0) and multiplicative (1) identity elements such that $\forall \alpha \in \mathcal{F}$ $\alpha + 0 = \alpha$, $1 \cdot \alpha = \alpha$

6. Each element has an additive inverse : $\forall \alpha \in \mathcal{F}$ $\exists \beta \in \mathcal{F}$ (called additive inverse of α) s.t. $\alpha + \beta = 0 \rightarrow$ additive identity

7. Each element (except for 0) has a multiplicative inverse

   $\forall \alpha \in \mathcal{F} \setminus \{0\}$ $\exists \gamma \in \mathcal{F}$ (called the multiplicative inverse of α) s.t. $\alpha \cdot \gamma = 1$

   $\hookrightarrow$ multiplicative identity most relevant to us

$\mathbb{R}$ (with the usual addition and multiplication) is a field

$\mathbb{C}$ (with the usual addition and multiplication) is a field

$\mathbb{Q}$ " is a field

$\mathbb{Z}$ (integers) is not a field (because Axiom 7 fails)

$\{A \mid A$ is a 2×2 real matrix$\}$

: fails axiom 2 (because

matrix multiplication is not commutative)

- fails axiom 7 (not all matrices are invertible)

- Examples

$\mathbb{R}$ set of real numbers
$\mathbb{C}$ set of complex numbers

- Non-examples

$\mathbb{N}$ set of natural numbers
- Fails axioms 6 and 7

$\{A \mid A \in \mathbb{R}^{2\times 2}\}$
- Fails axiom 2 and 7

More examples and non-examples

$\mathbb{R}(s) =$ set of rational functions in s ✓

$= \{\frac{n(s)}{d(s)} \mid n(s), d(s)$ real polynomials$\}$

$\mathbb{P}[s] =$ set of polynomial functions in s ✗

$\{0,1\}$ with operations $+ = XOR$ and $\cdot = AND$ ✓

Q set of rational numbers ✓

Irrational numbers ✗

Purely imaginary numbers ✗

A	B	XOR	AND
0	1	1	0
1	0	1	0
0	0	0	0
1	1	0	1

multiplicative identity = 1

additive identity: 0

Vector spaces

A linear (vector) space over a field $\mathcal{F}$, denoted by $\mathcal{X}, \mathcal{F}$ consists of a set $\mathcal{X}$ of vectors, a field $\mathcal{F}$, and two operations *vector addition* and *scalar multiplication* such that

$\mathcal{X}$ a set, $\mathcal{F}$ a field, $+$, $\cdot$ $(\underline{\mathcal{X}}, \underline{\mathcal{F}})$

properties of vector addition

1. $\mathcal{X}$ is closed under vector addition
   $\forall x_1, x_2 \in \mathcal{X} \quad x_1 + x_2 \in \mathcal{X}$
2. Vector addition is commutative
   $\forall x_1, x_2 \in \mathcal{X} \quad x_1 + x_2 = x_2 + x_1$
3. Vector addition is associative
   $\forall x_1, x_2, x_3 \in \mathcal{X} \quad (x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)$
4. $\mathcal{X}$ contains a zero vector $\underline{\mathbf{0}}$ (origin of the vector space) s.t.
   $\forall x \in \mathcal{X} \quad x + \mathbf{0} = x$
5. Each element of $\mathcal{X}$ has an additive inverse
   $\forall x \in \mathcal{X} \quad \exists \bar{x} \in \mathcal{X}$ s.t. $x + \bar{x} = \mathbf{0}$.

properties of scalar multiplication

6. $\mathcal{X}$ closed under scalar multiplication for any $\alpha \in \mathcal{F}$
   $\forall x \in \mathcal{X} \quad \forall \alpha \in \mathcal{F} \quad \alpha \cdot x \in \mathcal{X}$
7. Scalar multiplication is associative
   $\forall \alpha, \beta \in \mathcal{F} \quad \forall x \in \mathcal{X} \quad (\alpha \cdot \beta) \cdot x = \alpha \cdot (\beta \cdot x)$
8. Scalar multiplication is distributive over vector addition
   $\forall \alpha \in \mathcal{F} \quad \forall x_1, x_2 \in \mathcal{X} \quad \alpha \cdot (x_1 + x_2) = \alpha \cdot x_1 + \alpha \cdot x_2$
9. Scalar multiplication is distributive over scalar addition
   $\forall \alpha, \beta \in \mathcal{F} \quad \forall x \in \mathcal{X} \quad (\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$
10. For any $\mathbf{x} \in \mathcal{X}$, $1\mathbf{x} = \mathbf{x}$ where 1 is the multiplicative identity in $\underline{\mathcal{F}}$

scalar multiplication with $1 \in \mathcal{F}$

Ex: $(\mathbb{R}^n, \mathbb{R})$ is a vector space

Ex: $(\mathbb{R}, \mathbb{R})$ is a vector space

Ex: $(\mathcal{F}, \mathcal{F})$ is a vector space

Ex: $(\mathbb{R}^{2\times 3}, \mathbb{R})$ is a vector space

Ex: $\mathcal{F} = \mathbb{R}$. take $D \subset \mathbb{R}$

(e.g. $D = [a, b]$, $D = [0, \infty)$, $D = \mathbb{R}$, etc.)

Define:

$$X = \{ f : D \to \mathbb{R} \} = \{ \text{set of functions from } D \text{ to } \mathbb{R} \}$$

Define $\forall f, g \in X$

vector addition:

$f+g$: $\forall x \in D \ (f+g)(x) = f(x) + g(x)$

$\forall \alpha \in \mathbb{R}, \ \forall f \in X$

scalar multiplication:

$\alpha \cdot f$: $\forall x \in D$

$(\alpha \cdot f)(x) = \alpha \cdot f(x)$

a vector space!

Some questions: (you can prove)

- For fields, the element 0 & 1 are unique
- For vector spaces, the origin $(\mathbf{0})$ is unique.

OFFICE HOURS

A	B	C	(A XOR B) XOR C

A	B	C	A XOR (B XOR C)