6 Sept 2018

Review: Notation $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}, \forall, \exists, \in$

Logic & Proofs: $\sim\ = \neg =$ not, $\wedge$ = and, $\vee$ = or

$p \Rightarrow q \Leftrightarrow \sim q \Rightarrow \sim p$ (Contrapositive)

$q \Rightarrow p$ is the converse of $p \Rightarrow q$

Direct, contrapositive, exhaustion, induction

$P(n)$ = statement about the natural numbers

Base case: $P(1)$ is true [$P(k_0)$ is true]

Induction step: $P(k) \Rightarrow P(k+1)$ $k \geq 1$ [$P(k) \Rightarrow P(k+1)$, $k \geq k_0$]

Conclusion: $P(n)$ true $\forall n \geq 1$ [$P(n)$ true $\forall$ $n \geq k_0$]

- **Second Principle of Induction (Strong Induction):** Let $P(n)$ be a statement about the natural numbers with the following properties:

  (a) Base Case: $P(1)$ is true.

  (b) Induction: If $P(j)$ is true for all $1 \leq j \leq k$, then $P(k+1)$ is true.

  Conclusion: $P(n)$ is true for all $n \geq 1$ ($n \geq$ Base Case).

- Equivalent to ordinary induction on

  $\tilde{P}(n) = P(1) \wedge P(2) \wedge \cdots \wedge P(n)$

- You can change the Base Case to k_0 and induction to If $P(j)$ is true for $k_0 \leq j \leq k$, then $P(k+1)$ true.

Def. $n \in \mathbb{N}, n \geq 2$ is composite if $\exists\, a, b \in \mathbb{N}$ such that $n = ab$ and $2 \leq a, b, \leq n-1$. Otherwise n is prime.

Theorem (Fundamental Thm of Arithmetic)

Every natural number $n \geq 2$ can be written as the product of one or more primes.

Proof: $P(n)$: If $n \geq 2$, then n can be expressed as a product of one or more primes.

Base case: $P(2)$ is true because 2 is prime.

Induction: Assume now that $2 \leq j \leq k$, $P(j)$ is true. To show: $P(k+1)$ is true.

Two cases: $k+1$ is either prime or composite.

Case 1: $k+1$ is prime. Then $P(k+1)$ is trivially true.

Case 2: $k+1$ is composite. Hence, $\exists\, a, b \in \mathbb{N}$, such that $k+1 = a \cdot b$ and $2 \leq a, b \leq k$

Hence $\exists$ primes such that

$$a = p_1 p_2 \cdots p_\ell$$

$$b = q_1 q_2 \cdots q_m$$

Therefore, $k+1 = a \cdot b = p_1 \cdots p_\ell q_1 \cdots q_m$

is a product of primes. $\square$

Proof by Contradiction

A contradiction is a logical statement that is both true and false.

Let R be a logical statement.

$R \wedge (\sim R)$ true is a contradiction.

Example R = m and n $\in \mathbb{N}$, and have no common factors.

m and n are even is a contradiction of R.

Euclid's famous proof that $\sqrt{2}$ is irrational!

p: $\sqrt{2}$ is irrational

$\sim p$: $\sqrt{2}$ is rational.

Will show $\sim p$ leads to a contradiction and hence $\sim p$ must be FALSE.

$\therefore$ p is TRUE.

If $\sqrt{2}$ is rational, $\exists\, m, n \in \mathbb{N}$ such that

R1 : m, n have no common factors

R2 : $\sqrt{2} = \frac{m}{n}$

R2 $\Rightarrow$ $2 = \frac{m^2}{n^2}$ $\Rightarrow$ $2n^2 = m^2$

$\Rightarrow$ m^2 even $\Rightarrow$ m is even. (Tuesday)

m even $\Rightarrow$ $\exists\, k \in \mathbb{N}$ such that $m = 2k$.

$\therefore$ $2n^2 = (2k)^2$ $\Rightarrow$ $n^2 = 2k^2$ $\Rightarrow$

n^2 even $\Rightarrow$ n even.

$\therefore$ m, n have a common factor, namely 2.

$\therefore$ $\sim R_1$ is true.

$\therefore$ Contradiction $R_1 \wedge (\sim R_1)$.

$\therefore$ $\sim p$ is false and thus p is true.

Relation to the contrapositive

$p \Rightarrow q \Leftrightarrow \sim q \Rightarrow \sim p$

In another very common method of contradiction we do the following: Assume $p \wedge (\sim q)$ true and seek to derive a contradiction. This gives us $\sim (p \wedge (\sim q))$ is true.

Truth Tables

P	$\sim P$
T	F
F	T

For $\neg$

www.PrintablePaper

For $\wedge$

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Truth Table for $P \Rightarrow Q$

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

P = 100% on Final Exam

Q = Passing Grade

Contradiction

P	Q	$\sim Q$	$P \wedge \sim Q$	$\sim (P \wedge \sim Q)$
T	T	F	F	T
T	F	T	T	F
F	T	F	F	T
F	F	T	F	T

www.PrintablePaper.net

Tools

$$P \Rightarrow Q \iff (\sim Q \Rightarrow \sim P) \iff \Big(\sim(P \wedge \sim Q)\Big)$$

Direct — contrapositive — contradiction

See Handout on Max & Sup and Min & Inf.

Max & min must be an element of the given set, while sup and inf do not have to satisfy this restriction.

Negating a Statement

$p: \ x > 0$

$\sim p: \ x \leq 0$

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

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

$\Updownarrow$

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

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

$\sim p$: $\exists x \in \mathbb{R}$, such that $f(x) \leq 0$.

Pattern $\sim\forall \longleftrightarrow \exists$

Also true $\sim\exists \longleftrightarrow \forall$

Let $y \in \mathbb{R}$

p: $\forall \delta > 0$, $\exists x \in \mathbb{Q}$ such that $|x-y| < \delta$

$\sim p$: not (for all $\delta > 0$, there exists $x \in \mathbb{Q}$ such that $|x-y| < \delta$)

$\sim p$: For some $\delta > 0$, not (there exists $x \in \mathbb{Q}$ such that $|x-y| < \delta$)

$\sim p$: $\exists\, \delta > 0$, $\nexists\, x \in \mathbb{Q}$ such that $|x-y| < \delta$

$\sim p$: $\exists\, \delta > 0$, $\underbrace{\forall x \in \mathbb{Q},\ |x-y| \geq \delta.}_{(\nexists x \in \mathbb{Q} \text{ s.t. } |x-y| < \delta)}$

Remark: Better to avoid $\not\forall$ and $\nexists$, but they are legal!!!

p: $\forall y \in \mathbb{R}$, $\forall \delta > 0$, $\exists\, x \in \mathbb{Q}$ such that $|x-y| < \delta$

$\sim p$: $\exists\, y \in \mathbb{R}$ such that not$(\forall \delta > 0, \exists\, x \in \mathbb{Q}$ such that $|x-y| < \delta)$

$\therefore$ $\sim p$: $\exists\, y \in \mathbb{R}$ such that $\exists\, \delta > 0$ such that $\forall x \in \mathbb{Q}$ $|x-y| \geq \delta$.

Rob 501 Handout: Grizzle

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 $\max\{A\}$.

Max of a set must belong to the set.

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.*

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 *least upper bound* of A if

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

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

Upperbound does not have to belong to the set. The smallest element of all the upperbounds always exists and is called the SUPREMUM

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 $\min\{A\}$.

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.*

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 $b^* \geq b$.

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 ∞?

∞ satisfies, $\forall x \in \mathbb{R}$, $x < \infty$

$-\infty$ satisfies, $\forall x \in \mathbb{R}$, $-\infty < x$.

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

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

Final Remark: MATH 451 constructs 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)!