Lecture 1

Methods of Proof (Ref. 1.2.c)

Suppose that you want to show that a statement P implies a statement Q. How can you do this? What this implication means?

		Q	
		true	false
P	true	?	~~impossible~~
	false	?	?

Table 1.

A statement can either be true or false.
If P implies Q, then it cannot be that both P is true and Q is false.

There are several conventional methods of showing $P \underset{\text{(implies)}}{\Rightarrow} Q$:

• deduction • contradiction • contraposition • induction

• **Deduction** (or direct proof) Start by assuming that a statement P holds and use this info to verify that a stat. Q is also true.

Example: The sum of two consecutive odd numbers is divided by 4.
(What is P in this case? $\leadsto$ P is an empty statement, i.e. nothing is assumed)

Proof: (i) Any odd number can be written as $2p+1$, where p is an integer (integers: $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$).

(ii) Two consecutive odd numbers differ by 2. Thus;

(iii) The sum of two consecutive odd numbers is

$$2p+1+(2p+1+2) = 4p+4 = 4(p+1).$$

$\leadsto$ We have shown that the sum of 2 cons. odd numbers is divisible by 4. ∎

• **Contradiction**: Show that if P is true, then Q being false ($\neg Q$) yields a contradiction. I.e. in the Table 1 we, again, can exclude the cell (P=true, Q=false).

(notation: $\forall$ = for all, $\exists$ = exists)

Example: Given two arbitrary real numbers a, b, if for any $\varepsilon > 0$ $a \le b + \varepsilon$, then $a \le b$.

Proof: $P = \{\forall \varepsilon > 0 \ \ a \le b + \varepsilon\}$, $Q = \{a \le b\}$, $\neg Q = \{a > b\}$ (i.e. Q is false when $a > b$.)

Suppose that P and $\neg Q$ hold, and let us find a contradiction.

Choose $\varepsilon = \frac{a-b}{2} > 0$ (as Q is false and $a>b$).
Then $b+\varepsilon = b + \frac{a-b}{2} = \frac{a+b}{2} < a$ (again, as $a>b$).

Thus, we have a contradiction, as P says: $\forall \varepsilon>0 \; b+\varepsilon \geq a$.
$\Rightarrow$ Given P, Q must also be true
$\Rightarrow \{\forall \varepsilon > 0 \;\; a \leq b+\varepsilon \;\Rightarrow a \leq b\}$. ∎

- **Contraposition**: Instead of showing that P implies Q, we show that $\neg Q$ (not Q, i.e. Q is false) implies $\neg P$ (not P, i.e. P is false).
  This is very similar to contrad.: in both we start from $\neg Q$. Yet in contrap. we directly show that $\neg P$ is true, while in contrad. we show that $\neg Q$ & P cannot both be true.
  Why $\neg Q \Rightarrow \neg P$ is the same as $P \Rightarrow Q$? In Table 1 $\neg Q$ is the second column (Q=false), $\neg P$ is the second row (P=false), so, again, $\neg Q \Rightarrow \neg P$ means we exclude the top-right cell. (Q-false, P-true).

Formally, we can justify working with $\neg Q$ and $\neg P$ by the following:

Th. P implies Q if and only if $\neg Q$ implies $\neg P$.

Proof:
- Suppose $P \Rightarrow Q$ and, by contradiction, suppose $\neg Q$ does not imply $\neg P$. Then $\neg Q$ and P can both hold. If P holds, then by $(P \Rightarrow Q)$, we must have that Q is true. However, we also have ($\neg Q$ holds), i.e. Q is false $\Rightarrow$ contradiction, $\neg Q \Rightarrow \neg P$.
- Suppose $\neg Q \Rightarrow \neg P$ and, by contrad., suppose P does not imply Q. Then P and $\neg Q$ can both hold. If $\neg Q$ holds, then by $(\neg Q \Rightarrow \neg P)$, we must have $\neg P$, i.e. P is false. However, we also have P, i.e. P is true $\Rightarrow$ contrad., $P \Rightarrow Q$. ∎

In the previous example (if $\forall \varepsilon>0\ a \le b+\varepsilon$, then $a \le b$):
$\neg Q = \{a>b\}$, $\neg P = \{\exists \varepsilon>0$ s.t. $a>b+\varepsilon\}$. Let us prove $\neg Q \Rightarrow \neg P$:
Suppose $a>b$. Choose $\varepsilon = \frac{a-b}{2}>0$. Then $b+\varepsilon = b+\frac{a-b}{2} = \frac{a+b}{2} < a$,
and we have shown $\neg P$. ■

• Induction: Way to prove that a statement P holds for all natural numbers ($\mathbb{N} = \{1, 2, 3, \dots\}$).

The approach is based on the following axiom:

The principle of induction: $\begin{cases} \text{(i) } P(1) \text{ holds; (base step)} \\ \text{(ii) If for any } n\in\mathbb{N}\ P(n) \text{ implies } P(n+1) \text{ (induction step),} \end{cases}$

then P holds for all natural numbers $n \in \mathbb{N}$.

Example: For every $n\in\mathbb{N}$, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, i.e. $1+2+\dots+n = \frac{n(n+1)}{2}$.

Proof: • Base step: $P(1)$ is $\sum_{k=1}^{1} k = 1 = \frac{1\cdot(1+1)}{2} = \frac{2}{2} = 1$, so $P(1)$ holds.

• Induction step: Suppose $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for some $n\in\mathbb{N}$. We must show that $\sum_{k=1}^{n+1} k = \frac{(n+1)((n+1)+1)}{2} = \frac{(n+1)(n+2)}{2}$

$$\sum_{k=1}^{n+1} k = n+1 + \sum_{k=1}^{n} k \overset{\text{By } P(n)}{=} n+1 + \frac{n(n+1)}{2} = (n+1)\left(1+\frac{n}{2}\right) = \frac{(n+1)(n+2)}{2}.$$

Thus, by the principle of induction our claim is true. ■

The following modification of the induction principle is sometimes useful.

Complete induction: $\begin{cases} \text{(i) } P(1) \text{ holds; (base step)} \\ \text{(ii) If } P \text{ holds for all integers } k=1,\dots,n, \text{ then it also} \\ \quad \text{holds for } k=n+1 \text{ (inductive step),} \end{cases}$

then P holds for all natural numbers.

Example (Fundamental th. of Arithmetic) Every natural number $n>1$ can be written as the product of prime numbers.

Proof: • Base step: 2 = prime number, so the claim holds.

• Induction step: $\forall k=2,\dots,n$ we can write k = product of primes.

If $n+1$ is a prime, we are done.

If $n+1$ is not a prime, then $n+1=p_1\cdot p_2$, $1<p_1<n+1$, $1<p_2<n+1$.

Thus, p_1 = product of primes and p_2 = product of primes.

So $n+1$ is also a product of primes. ■

Sets (Ref 1.1)

Def: A **set** is a collection of objects (**elements**). We will denote sets by capital letters and elements by lowercase letters.
We write $x\in X$ if x is an element of X and $x\notin X$ if x is not an element of X.

A set A is a **subset** of X if all elements of A belong to X.
This is written as $A\subset X$. Formally, $A\subset X \underset{\text{equivalence}}{\Leftrightarrow} (x\in A \overset{\text{implies}}{\Rightarrow} x\in X)$.

If $A\subset B$ and $B\subset A$, then $A=B$.

$\emptyset$ = empty set (set with no elements)

$\emptyset\subset X$ for any X.

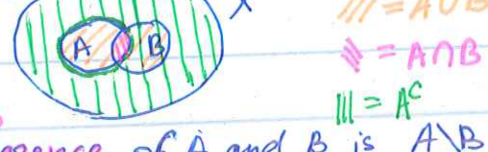
s.t. = such that

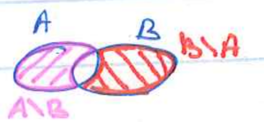
Def. If $A\subset X$, the **complement** of A in X is defined as

$A^c := \{x\in X \text{ s.t. } x\notin A\}$ (also written as $\{x\in X \underset{=\text{s.t.}}{|} x\notin A\}$)

Def. A **union** of A and B is $A\cup B=\{x\in X \mid x\in A \text{ or } x\in B\}$

An **intersection** of A and B is $A\cap B=\{x\in X \mid x\in A \text{ and } x\in B\}$.



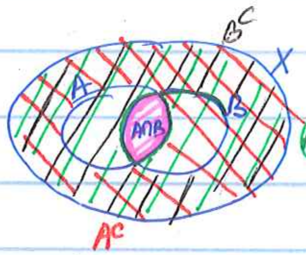


A **difference** of A and B is $A\setminus B=\{x\in A \mid x\notin B\}$.

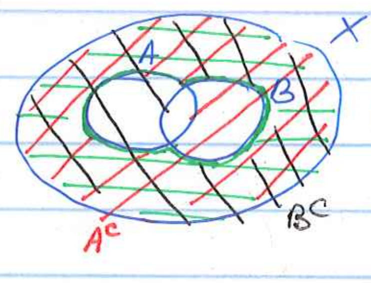
Th. (De Morgan's laws) 1). $(A \cap B)^c = A^c \cup B^c$

2). $(A \cup B)^c = A^c \cap B^c$

Illustration:



$(A \cap B)^c = A^c \cup B^c$



$(A \cup B)^c = A^c \cap B^c$

(can be proved formally)

E.g. for 1). : We prove $(A \cap B)^c \subset A^c \cup B^c$ and $A^c \cup B^c \subset (A \cap B)^c$.

$(A \cap B)^c \subset A^c \cup B^c$ • $x \in (A \cap B)^c \Rightarrow x \notin A \cap B \Rightarrow x \notin A$ or $x \notin B \Rightarrow x \in A^c$ or $x \in B^c \Rightarrow x \in A^c \cup B^c$.

$A^c \cup B^c \subset (A \cap B^c)$ • $x \in A^c \cup B^c \Rightarrow x \in A^c$ or $x \in B^c \Rightarrow x \notin A$ or $x \notin B \Rightarrow x \notin A \cap B \Rightarrow x \in (A \cap B)^c$. ■

Def. A power set of X, 2^X, is the set consisting of all subsets of X,
$2^X = \{A \mid A \subset X\}$.

E.g. $\emptyset, X \in 2^X$.

Cardinality (Ref. 1.4.) How to compare sets? Which set is larger
$\{5, 10\}$ or $\{1, 2, 3\}$?

⤳ Cardinality = size of a set.

Def. Two sets, A, B, are numerically equivalent (have the same cardinality) if their elements can be uniquely matched up and paired off. That is, we can create pairs (a, b), $a \in A, b \in B$ s.t. $\forall a \in A$ belongs to some pair; $\forall b \in B$ belongs to some pair; if $a \neq a'$, then for their pairs: $b \neq b'$; if $b \neq b'$, then for their pairs $a \neq a'$.

(Formally, this means there is a bijection $f: A \to B$. We will define that notion later)

Def. A set is finite if it is numerically equivalent to $\{1, 2, \dots, n\}$ for some n. Then its cardinality $= n$.
A set that is not finite is infinite.

Example: • Set $\{1,2,3\}$ is numerically eqiv. to $\{5,10,11\}$, but not to $\{5,10\}$. Card. of $\{5,10,11\}=3$, of $\{5,10\}=2$.

• Set $\{2,4,\dots,50\}$ is numer. equiv. to $\{1,2,\dots,25\}$:

$$\overset{A}{2}\leftrightarrow\overset{B}{1},\ \overset{A}{4}\leftrightarrow\overset{B}{2},\ \dots,\ \overset{A}{50}\leftrightarrow\overset{B}{25}$$

• Set of natural numbers is infinite.

An infinite set is either countable or uncountable.

Def. An infinite set is **countable** if it is numerically equiv. to $N=\{1,2,\dots\}$

An infinite set that is not countable is called **uncountable**

(That is, for a countable set we can rename its elements as $1,2,3,\dots$)

Example: The set of integers $Z=\{0,1,-1,2,-2,\dots\}$ is countable.

$$\overset{Z}{0}\leftrightarrow\overset{N}{1},\ \overset{Z}{1}\leftrightarrow\overset{N}{2},\ \overset{Z}{-1}\leftrightarrow\overset{N}{3},\ \overset{Z}{2}\leftrightarrow\overset{N}{4},\ \text{etc.}$$

That is, any number $z\in Z$ is paired with $n=\begin{cases}2|z|+1, & z\le 0\\ 2|z|, & z>0\end{cases}$

(Or equivalently $\forall n\in N$ is paired with $z=(-1)^n\lfloor n/2\rfloor$, $\lfloor x\rfloor$ = floor f-n, largest integer $\le x$)

Remark: $N\subset Z$, but $N\neq Z$. Moreover, $Z\setminus N$ is infinite

Other examples?

Th. The set of rational numbers Q is countable.

Proof: $Q=\{\frac{m}{n}\mid m\in Z, n\in N\}$ (if $m<0$, then $\frac{m}{n}<0$, if $m=0$, then $m/n=0$, if $m>0$, then $m/n>0$)

We show a picture, which "renumbers" elements in Q.

$n \backslash m$	0	1	-1	2	-2	3
1	0	1	-1	2	-2	3
2	0	$\frac{1}{2}$	$-\frac{1}{2}$	1	-1	$\frac{3}{2}$
3	0	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{2}{3}$	$-\frac{2}{3}$	
4	0	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{2}$	$-\frac{1}{2}$	

(Any $q=\frac{m}{n}\in Q$ can be found by taking row n, column m)

Go back and forth by pink diagram to number all $q\in Q$, omitting the repeats

That is: $\overset{\mathbb{Q}}{0} \leftrightarrow \overset{\mathbb{N}}{1},\ \overset{\mathbb{Q}}{1} \leftrightarrow \overset{\mathbb{N}}{2},\ \overset{\mathbb{Q}}{\tfrac{1}{2}} \leftrightarrow \overset{\mathbb{N}}{3},\ \overset{\mathbb{Q}}{-1} \leftrightarrow \overset{\mathbb{N}}{4},\ \overset{\mathbb{Q}}{2} \leftrightarrow \overset{\mathbb{N}}{5},\ \overset{\mathbb{Q}}{-\tfrac{1}{2}} \leftrightarrow \overset{\mathbb{N}}{6}, \dots$

Thus, althoug $\mathbb{Q}$ appears to be much larger than $\mathbb{N}$, in fact they are of the same size!

<u>Th.</u> $2^{\mathbb{N}}$, the set of all subsets of $\mathbb{N}$, is uncountable.

(proof by contradiction) <u>Proof:</u> Suppose $2^{\mathbb{N}}$ is countable. That is, we can match $A \longleftrightarrow n$, $A \subset 2^{\mathbb{N}}$, $n \in \mathbb{N}$.
Any set A has its own number n, any number n is matched with a differen set. Denote by A_n the set in $2^{\mathbb{N}}$ which is matched with n.

Now consider the following set $A^* \subset 2^{\mathbb{N}}$:

$$A^* = \{ n \in \mathbb{N} \mid n \notin A_n \}.$$

That is, for each set $A_n \in 2^{\mathbb{N}}$ we check whether $n \in A_n$, and if $n \notin A_n$, then we add $\{n\}$ to A^*.

Because $A^* \subset 2^{\mathbb{N}}$ and we assumed that $2^{\mathbb{N}}$ is countable, A^* was matched with some $m \in \mathbb{N}$, i.e. $A^* \equiv A_m$. However, then

- If $m \notin A_m$, then by definition: $m \in A^* = A_m$ as $m \notin A_m$, and we get a contradiction
- If $m \in A_m$, then by definition: $m \in A^* \Leftrightarrow m \notin A_m = A^*$, and we get a contradiction

$\Rightarrow 2^{\mathbb{N}}$ is uncountable. ■