Direct Proof

Last time:
$\forall a, b, c \in \mathbb{N} \quad [(a|b) \wedge (b|c) \Rightarrow (a|b)]$
$\forall a, b, c \in \mathbb{N} \quad [R(a,b,c) \Rightarrow S(a,b)]$

Why is it proved by assuming $R(a,b,c)$, then proving S?

$R(a,b,c)$	$S(a,b)$	$R \Rightarrow S$
0	0	1
0	1	1
1	0	0
1	1	1

The proof requires us to show that the case $R(a,b,c)$ true, $S(a,c)$ false cannot happen.
To do, assume R, then prove S.

Proof by Contrapositive

Since $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$.
To prove $P \Rightarrow Q$, you can assume $\neg Q$, prove $\neg P$.

ex. $\forall n, a, b \in \mathbb{N} \quad (n = ab \Rightarrow (a \leq \sqrt{b} \vee b \leq \sqrt{n}))$
proof.
Assume $\neg(a \leq \sqrt{b} \vee b \leq \sqrt{n}) \equiv (a > \sqrt{n} \wedge b > \sqrt{n})$. Then,
$ab > \sqrt{n} \cdot \sqrt{n} = n$, so $n \neq ab$ i.e. $\neg(n = ab)$. □

Vacuous Proof

ex. Prove $\forall n \in \mathbb{N} \ (0 = 1 \Rightarrow n \text{ is prime})$.
proof.
Let $n \in \mathbb{N}$. $\neg(0 = 1) \vee (n \text{ is prime})$.
We know $0 \neq 1$ i.e. $\neg(0 = 1)$ is true, so $\neg(0 = 1) \vee (n \text{ prime})$ always true. □

Proof by Contradiction

To prove by contradiction:
(1) Assume $\neg P$.
(2) Derive $Q \wedge \neg Q$ i.e. derive a contradiction.
(3) Conclude P is true.
In fact, we are proving:

$$\begin{aligned} \neg P \Rightarrow (Q \wedge \neg Q) &\equiv \neg P \Rightarrow 0 \\ &\equiv \neg\neg P \vee 0 \\ &\equiv P \vee 0 \\ &\equiv P \end{aligned}$$

ex. Formulate there is no least positive rational number and prove it.

proof.

Want to prove: $\neg\exists n \in \mathbb{Q}\,(n>0 \wedge (\forall m \in \mathbb{Q}\,(m>0 \Rightarrow n \leq m))$.

By contradiction, assume

$\neg(\neg\exists n \in \mathbb{Q}\,(n>0 \wedge (\forall m \in \mathbb{Q}\,(m>0 \Rightarrow n \leq m)))$.

Re-write as:

$\exists n \in \mathbb{Q}\,(n>0 \wedge (\forall m \in \mathbb{Q}\,(m>0 \Rightarrow n \leq m)))$.

Now we can use this n.

Set $m = n/2$.

We know $\forall m \in \mathbb{Q}\,(m>0 \Rightarrow n \leq m)$ by $n \leq m = n/2$

and $m = n/2 \in \mathbb{Q}$ (since $n \in \mathbb{Q}$ and $m>0$ since $n>0$).

So,

$n \leq n/2$, so $1 \leq 1/2$ (possible since $n>0$).

We obtained $1 \leq 1/2$, which is false. So original statement is true.

ex. Prove that $\sqrt{2}$ is irrational. ($\sqrt{2} \notin \mathbb{Q}$).

proof.

Assume for contradiction that $\sqrt{2} \in \mathbb{Q}$.

Then, $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}$ and $q \neq 0$.

If p, q have common factors, cancel them to obtain $\sqrt{2} = \ell/m$ where ℓ, m have no common factors.

Then, square both sides:

$\sqrt{2}^2 = \ell^2/m^2$ so $2m^2 = \ell^2$.

Claim $2 \mid \ell$ i.e. ℓ is even.

Sub-proof: By contradiction, assume ℓ is odd.

So, $\ell = 2n+1$ for some $\ell \in \mathbb{Z}$.

Then,

$\ell^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 2(2n^2+2n)+1$.

let $k = 2(2n^2+2n)$. Then $\ell^2 = 2k+1$, i.e. ℓ^2 is odd.

But $\ell^2 = 2m^2$, so ℓ^2 is even. Contradiction.

The assumption is false.

So, if ℓ^2 is even then ℓ is even. Then, $\ell = 2t$ for some $\ell \in \mathbb{Z}$.

Then,

$2m^2 = \ell^2 = 4t^2$

$m^2 = 2t^2$.

Similarly to before, ℓ^2 even $\Rightarrow \ell$ even;

m^2 even $\Rightarrow m$ even.

Then, m, ℓ have 2 as a common factor. But m and ℓ were defined to not have any common factors. Thus, $\sqrt{2} \in \mathbb{Q}$ false, so $\sqrt{2} \notin \mathbb{Q}$. □

ex. Prove no integer is both even or odd.

proof.

Claim: $\neg(\forall n \in \mathbb{Z}\ (n \text{ is even} \wedge n \text{ is odd}))$.

Assume claim is false: $\exists n \in \mathbb{Z}\ (n \text{ is even} \wedge n \text{ is odd})$.

So, $\exists n, k_1, k_2 \in \mathbb{Z}\ (n = 2k_1 \wedge n = 2k_2 + 1)$.

So, $2k_1 = 2k_2 + 1$.

$2k_1 - 2k_2 = 1$.

$2(k_1 - k_2) = 1$.

$k_1 - k_2 = 1/2$.

Contradiction. $k_1, k_2 \in \mathbb{Z}$ so $k_1 - k_2 \in \mathbb{Z}$.

The initial assumption is false. Therefore there is no integer that is both even and odd. □

Sets

Assume we have a universe U.

def. $A \subseteq B$ means $\forall x \in U\ (x \in A \Rightarrow x \in B)$. A is a subset of B.

def. The empty set has no elements, and is $\emptyset$ or $\{\}$.

Proposition.

For any set A,

(1) $A \subseteq A$

(2) $\emptyset \subseteq A$

proof of (2).

To prove $\forall x \in U\ (x \in \emptyset \Rightarrow x \in A)$.

Let $x \in U$. Then, $x \notin \emptyset$ so $x \in \emptyset \Rightarrow x \in A$ is true (vacuously). □

Set Operations & Logic

Let A, B be sets. Define:

$A \cap B = \{x \in U \mid x \in A \wedge x \in B\}$

$A \cup B = \{x \in U \mid x \in A \vee x \in B\}$

$\bar{A} = \{x \in U \mid x \notin A \quad \neg(x \in A)\} = U \setminus A$

$A \setminus B = \{x \in U \mid x \in A \wedge x \notin B\}$

Set Identities

De Morgan's laws

(i) $\overline{A \cap B} = \bar{A} \cap \bar{B}$

(ii) $\overline{A \cup B} = \bar{A} \cup \bar{B}$

In general, to prove $X = Y$ (sets X, Y), you can prove $X \subseteq Y$ and $Y \subseteq X$.

Alison Li

proof #1 of (i).

Prove $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$. i.e. $\forall x \in U \ (x \in \overline{A \cap B} \Rightarrow x \in \bar{A} \cup \bar{B})$.

let $x \in U$. Assume $x \in \overline{A \cap B}$ so $x \notin A \cap B$. Then, two cases:

(1) If $x \notin A$, then $x \in \bar{A}$ so $x \in \bar{A} \cup \bar{B}$.

(2) If $x \notin B$, then $x \in \bar{B}$ so $x \in \bar{A} \cup \bar{B}$.

Either way, $x \in \bar{A} \cup \bar{B}$.

Prove $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$.

let $x \in \bar{A} \cup \bar{B}$. Then, two cases:

(1) $x \in A$ so $x \notin B$ so $x \notin A \cap B$ so $x \in \overline{A \cap B}$.

(2) $x \in B$ so $x \notin A$ so $x \notin A \cap B$ so $x \in \overline{A \cap B}$.

Conclude $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

proof #2 of (i).

$$\begin{aligned}
\overline{A \cap B} &= \{x \in U \mid x \notin A \cap B\} \\
&= \{x \in U \mid \neg(x \in A \cap B)\} \\
&= \{x \in U \mid \neg(x \in A \wedge x \in B)\} \\
&= \{x \in U \mid x \notin A \vee x \notin B\} \quad \text{by de Morgan on Logic} \\
&= \{x \in U \mid x \in \bar{A} \vee x \in \bar{B}\} \\
&= \bar{A} \cup \bar{B} \quad \text{by definition of union.}
\end{aligned}$$

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\bar{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \bar{A} \cup \bar{B}$ $\overline{A \cup B} = \bar{A} \cap \bar{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \bar{A} = U$ $A \cap \bar{A} = \emptyset$	Complement laws

ex. Simplify $((A \setminus B) \cup A) \cap (\bar{A} \cup B)$.

$$\begin{aligned}
&= ((A \cap \bar{B}) \cup A) \cap (\bar{A} \cup B). \\
&= A \cap (\bar{A} \cup B) \quad \text{by absorption.} \\
&= (A \cap \bar{A}) \cup (A \cap B) \\
&= \emptyset \cup (A \cap B) \\
&= A \cap B.
\end{aligned}$$