PROPOSITIONS & CONNECTIVES[1]

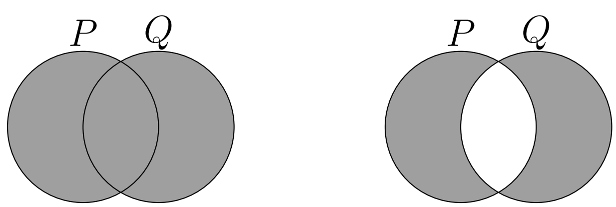
A proposition is a statement that has *exactly one* truth value: true or false.

Example:

1. "$1 + 1 = 2$"
2. "Sarah won a Nobel Prize in economics in 2019"
3. "$x^2 = 36$"

We can use connectives to create compound propositions:

$P, Q, R, \ldots$	How we denote propositions
$\neg P$	"Not P"
$P \wedge Q$	"P and Q" ($\wedge$ looks like the A in AND)
$P \vee Q$	"P or Q or both" (inclusive or)



Inclusive Or
$P \vee Q$

Exclusive Or
$(P \vee Q) \wedge \neg(P \wedge Q)$

Example:

- P: Sarah is on Zoom
- Q: Woongchan is on Zoom
- $\neg P$: Sarah is not on Zoom
- $P \wedge Q$: Sarah and Woongchan are on Zoom
- $P \vee Q$: Sarah or Woongchan (or both) is on Zoom

[1] Prepared by Sarah Robinson

For the different truth values of P and Q, we can determine the truth values of the compound propositions using a truth table:

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$P \vee Q$	$\neg(\neg P)$
T	T					
T	F					
F	T					
F	F					

Two propositions are equivalent if they have the same truth tables.

Conditional

The most important compound proposition is the conditional, $P \Rightarrow Q$ ("if P then Q" or "P implies Q").

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

- If P is true, then in order for $P \Rightarrow Q$ to be true, Q must be true.
  - In order to prove $P \Rightarrow Q$, we are going to start by assuming P is true and showing that Q is true (1^{st} line holds, 2^{nd} line doesn't)
- If P is false, then $P \Rightarrow Q$ is automatically true.
  - This is trivial for any Q, so we don't worry about the 3^{rd} and 4^{th} lines (get them for free)

Notice that $P \Rightarrow Q$ is true exactly when P is false or Q is true ($P \Rightarrow Q$ is equivalent to $\neg P \vee Q$).

If $P \Rightarrow Q$ is true, then P is a sufficient (but not necessary) condition for Q.

Writing Proofs

The basic format for writing proofs if we are asked to show $P \Rightarrow Q$:

- List of definitions, theorems, etc. that you might want to use
- Might be on scratch paper to help yourself with the proof
- Theorem 1: $P \Rightarrow R$
- Theorem 2: $R \Rightarrow Q$

To Show: Q

Proof:

Let P	(by hypothesis)
$\Rightarrow R$	(by Theorem 1)
$\Rightarrow Q$	(by Theorem 2)

$\blacksquare$

Note that every step has a clear justification.

Example:
Let x be an integer. Prove that if x is odd, then $x + 1$ is even.

- $\mathbb{Z}$ is the set of integers
- Def. of even: $y \in \mathbb{Z}$ is even $\iff \exists\, k \in \mathbb{Z} \ni y = 2k$
- Def. of odd: $x \in \mathbb{Z}$ is odd $\iff \exists\, j \in \mathbb{Z} \ni x = 2j + 1$
- Closure property: the sum of two integers is an integer
- Successor property: If $x \in \mathbb{Z}$, x has a unique successor $x + 1$

<u>To Show:</u> $x + 1$ is even

<u>Proof:</u>

Let x be an odd integer	(by hypothesis)
$\implies \exists\, k \in \mathbb{Z} \ni x = 2k + 1$	( )
$\implies x + 1 = (2k + 1) + 1$	( )
$\implies x + 1 = 2k + 2$	( )
$\implies x + 1 = 2(k + 1)$	( )
$\implies (k + 1)$ is an integer	( )
$\implies x + 1$ is even	( )

■

Converse & Contrapositive

For $P \Rightarrow Q$:

- The converse is $Q \Rightarrow P$
- The contrapositive is $\neg Q \Rightarrow \neg P$
- Do not confuse them

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

Moving between equivalent propositional forms (e.g., from a proposition to its contrapositive) can be extremely helpful when writing proofs. Sometimes, the contrapositive is easier to prove.

Clearly state that this is what you are doing (so the grader doesn't miss it).

Example: Proof by Contrapositive
Let m be an integer. Prove that if m^2 is even, then m is even.

- $\mathbb{Z}$ is the set of integers
- Def. of even: $y \in \mathbb{Z}$ is even $\iff \exists\, k \in \mathbb{Z} \ni y = 2k$
- Def. of odd: $x \in \mathbb{Z}$ is odd $\iff \exists\, j \in \mathbb{Z} \ni x = 2j + 1$
- Closure property: the sum of two integers is an integer
- Successor property: If $x \in \mathbb{Z}$, x has a unique successor $x + 1$
- Theorem 1: An integer is odd if and only if it is not even

<u>To Show (by contrapositive):</u>

<u>Proof:</u>

Biconditional

The biconditional is $P \Leftrightarrow Q$ ("P if and only if Q" or "P iff Q").

$P \Leftrightarrow Q$ is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

If $P \Leftrightarrow Q$ is true, then P is a necessary and sufficient condition for Q.

To prove $P \Leftrightarrow Q$, we will usually prove $P \Rightarrow Q$ and then prove $Q \Rightarrow P$.

If all of the steps and justifications are *exactly the same* (every step holds in both directions), you can consolidate this into one proof. Use with caution.

Example: Biconditional Proof
Show that $\neg(P \wedge Q)$ if and only if $Q \Rightarrow \neg P$

- Def. of conditional: $P \Rightarrow Q$ iff $\neg P \vee Q$
- Contrapositive: $P \Rightarrow Q$ iff $\neg Q \Rightarrow \neg P$
- DeMorgan's Laws (pt 1): $\neg(P \wedge Q)$ iff $\neg P \vee \neg Q$
- DeMorgan's Laws (pt 2): $\neg(P \vee Q)$ iff $\neg P \wedge \neg Q$

To Show ($\Rightarrow$): $Q \Rightarrow \neg P$
Proof:

To Show ($\Leftarrow$): $\neg(P \wedge Q)$
Proof:

Tautologies & Contradictions

A tautology is a proposition that always true (no matter the truth values of its components).

A contradiction is a proposition that is always false (no matter the truth values of its components).

P	$\neg P$	$P \vee \neg P$	$P \wedge \neg P$
T	F		
F	T		

You can always state a tautology anywhere in your proof. For example, one line might read "$P \vee \neg P$" (by tautology). We'll look at an example later of how this can be useful.

Proof by contradiction is a powerful tool. Say you want to prove $(P \wedge Q) \Rightarrow R$, and you remember a handy theorem that $(P \wedge \neg R) \Rightarrow \neg Q$

To Show: R
Proof:

Let $P \wedge Q$ (by hypothesis)

Suppose $\neg R$ (towards a contradiction)

$\implies \neg Q$ (with your theorem)

$\implies Q \wedge \neg Q$ (logic)

$\implies R$ (by contradiction)

■

You suppose something you want to reject, and then show that it leads to a contradiction. Then you can reject that supposition.

Example: Proof by Contradiction
Let $x^2 + y = 13$ and $y \neq 4$. Prove that $x \neq 3$.

<u>To Show:</u> $x \neq 3$

<u>Proof:</u>

Let $x^2 + y = 13$	(by hypothesis)
Let $y \neq 4$	(by hypothesis)

This is a silly example, but proof by contradiction is extremely useful.

Make sure to clearly state "towards contradiction" somewhere early on, so the grader knows you know what you're doing. (Notice a trend yet? Don't lose points because the TA or professor couldn't follow.)

Quantifiers

Recall that when defining propositions, we saw that $x^2 = 36$ was not a proposition, because it was true for some x and false for others.

Quantifiers let us say something about how many values of x make such statements true.

$P(x)$	An open sentence (truth value depends on x)
U	The universe of potential x values
$\in$	"In"
$\ni$	"Such that"

$\forall\, x \in U, P(x)$	"For all x in U, $P(x)$"
$\exists\, x \in U \ni P(x)$	"There exists an x in U such that $P(x)$"
$\exists!\, x \in U \ni P(x)$	"There exists a unique x in U such that $P(x)$"

Example: Now these are all propositions ($\mathbb{R}$ is the set of real numbers)

1. $\forall\, x \in \mathbb{R} \ni x^2 = 36$
2. $\exists\, x \in \mathbb{R} \ni x^2 = 36$
3. $\exists!\, x \in \mathbb{R} \ni x^2 = 36$

Say you want to prove $\forall\ x \in U, P(x)$. Start by picking an arbitrary element in x in the universe U, and prove that it satisfies the statement. Because x was arbitrary, then it's true for all x in U.

<u>To Show:</u> $P(x)$
<u>Proof:</u>

Let $x \in U$	(by hypothesis)
$\Rightarrow P(x)$	(with theorems, algebra, etc.)

■

However, you cannot then put any additional restrictions on x by hypothesis. Remember that x needs to stay completely arbitrary.

NOT THIS

<u>To Show:</u> $P(x)$
<u>Proof:</u>

Let $x \in U$	(by hypothesis)
Let $x < 10$	(by hypothesis)
$\Rightarrow P(x)$	(with theorems, algebra, etc.)

■

If you need to prove $\forall\ x \in U \ni x < 10, P(x)$ then you can do it this way (from all the x that are less than 10, choose arbitrarily):

<u>To Show:</u> $P(x)$
<u>Proof:</u>

Let $x \in U \ni x < 10$	(by hypothesis)
$\Rightarrow P(x)$	(with theorems, algebra, etc.)

■

If you want to show that $\exists\ x \in U \ni P(x)$, all you need is one example (don't need to set up a formal proof).

If you want to show that $\exists!\ x \in U \ni P(x)$, first pick an example x and show that it is in U and satisfies $P(x)$. Then pick an arbitrary y that is in U and satisfies $P(x)$, and prove that y must equal x.

If you want to show that a $\forall\ x$ statement is *false*, all you need is one counterexample (don't need to set up a formal proof).

If you want to show that a $\exists\ x$ statement is *false*, how would you do it?

Proof by Mathematical Induction

Example: For every $n \in \{0, 1, 2, 3, \dots\}$, prove that
$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$

<u>To Show:</u> Base case $P(0)$

<u>Proof:</u>

Let $n = 0$ (by hypothesis)
$\implies 2^0 = 1$ (algebra)
$\implies 2^{n+1} - 1 = 1$ (algebra)
$\implies 2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$ (algebra)

<u>To Show:</u> $P(n) \Rightarrow P(n+1)$

<u>Proof:</u>

Assume $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$ (by inductive hypothesis)
$\implies 2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1}$ (adding 2^{n+1} to both sides)
$\implies$ " $= 2(2^{n+1}) - 1$ (algebra)
$\implies$ " $= 2^{n+1+1} - 1$ (algebra)

■

Logical Equivalences

P	$\neg(\neg P)$	(Double Negation)
$P \vee Q$	$Q \vee P$	(Commutative Laws)
$P \wedge Q$	$Q \wedge P$	”
$P \vee (Q \vee R)$	$(P \vee Q) \vee R$	(Associative Laws)
$P \wedge (Q \wedge R)$	$(P \wedge Q) \wedge R$	”
$P \wedge (Q \vee R)$	$(P \wedge Q) \vee (P \wedge R)$	(Distributive Laws)
$P \vee (Q \wedge R)$	$(P \vee Q) \wedge (P \vee R)$	”
$P \wedge P$	P	(Idempotent Laws)
$P \vee P$	P	”
$P \vee (P \wedge Q)$	P	(Absorption Laws)
$P \wedge (P \vee Q)$	P	”
$\neg(P \wedge Q)$	$\neg P \vee \neg Q$	(DeMorgan’s Laws)*
$\neg(P \vee Q)$	$\neg P \wedge \neg Q$	” *
$P \Rightarrow Q$	$\neg P \vee Q$	(Def. of Conditional)
$P \Leftrightarrow Q$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$	(Def. of Biconditional)*
$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$	(Contrapositive)*

$P \Rightarrow (Q \vee R)$	$(P \wedge \neg Q) \Rightarrow R$	(Or in the Hypothesis)
$P \Rightarrow (Q \Rightarrow R)$	$(P \wedge Q) \Rightarrow R$	(Hypothesis in the Conclusion)
$(P \vee Q) \Rightarrow R$	$(P \Rightarrow R) \vee (Q \Rightarrow R)$	(logic)
$P \Rightarrow (Q \wedge R)$	$(P \Rightarrow R) \wedge (Q \Rightarrow R)$	(logic)

$\neg(\forall\, x, P(x))$	$\exists\, x \ni \neg P(x)$	(logic, remember to define universe U)*
$\neg(\exists\, x \ni P(x))$	$\forall\, x, \neg P(x)$	(logic, remember to define universe U)*

If you can't remember the name of any of these, "(logic)" can be an acceptable justification for a step in a proof IF it's obviously equivalent to whoever is grading it (they are sure you aren't making it up). So use your best judgment. If it's not obvious in one step, try breaking it down into smaller steps. The equivalences with an * are my favorites.

Proof Strategies

$P \Rightarrow Q$

- Let P (by hypothesis)
- Show Q

$P \Rightarrow Q$ by contrapositive (sometimes easier)

- Let $\neg Q$ (by hypothesis)
- Show $\neg P$

$P \Leftrightarrow Q$

- Prove $P \Rightarrow Q$ and prove $Q \Rightarrow P$
- (Can do as one proof if *every line is a biconditional*)

Proof by contradiction (e.g, want to show R)

- Suppose $\neg R$ (towards contradiction)
- Show a contradiction (e.g., $Q \wedge \neg Q$)
- Then R (by contradiction)

$\forall\ x \in U, P(x)$

- Let $x \in U$ (by hypothesis)
- Show that x makes $P(x)$ true
- Remember to keep x arbitrary

$\exists\ x \in U \ni P(x)$

- Let $x =$ [example]
- Show that x is in U and satisfies $P(x)$
- For $\exists!\ x$, then also:
  - Pick an arbitrary y that is in U and satisfies $P(x)$
  - Show that y must equal x (contradiction may be helpful)

Proof by Mathematical Induction (e.g, want to show $P(n)\ \forall n \in \mathbb{N}$)

- Let $n = 1$ (by hypothesis)
- Show $P(1)$
- Assume $P(n)$ (by inductive hypothesis)
- Show $P(n+1)$

You can ...

- Separate $\wedge$ into single parts $\quad P \wedge Q \implies P$
- Create $\wedge$ e.g., if you already have $\implies P$ and $\implies Q$, then you can declare $\implies P \wedge Q$
- Declare a tautology at any time $\quad P \vee \neg P$
- Separate $\vee$ into separate cases $\quad$ If $P \ldots$ and If $Q \ldots$
  (sometimes useful to also do: If $P \wedge Q \ldots$)
- Create $\vee$ e.g., if you already have $\implies P$, you can declare $\implies P \vee Q$