Plan for today

Formal Proofs

- What is a formal proof?
- How do we write a formal proof?
- Soundness and Completeness
- Examples

What is a proof?

Every theorem you will ever find has the form
"If A and B and C then D".

Example:
"If $x \in \mathbb{N}$ and $x > 1$ then x has a unique prime factorization."

Sometimes this is implicit in the theorem.
"Every planer graph is 4-colorable."
But, this is really
"If G is a graph, and G is planer, then G is 4-colorable."

An implication like this is a **theorem** if it is a tautology.

Notation

All of our theorems have the form
$\mathit{Premise} \wedge \mathit{Premise} \wedge \ldots \rightarrow \mathit{Conclusion}$.

We will write this as
$\mathit{Premise}, \mathit{Premise}, \ldots \vdash \mathit{Conclusion}$.

$\vdash$ is called a turnstile.

Inference Rules

We write formal proofs using Inference Rules.
These are the axioms of proofs.
They have the form

$$\frac{\textit{Premise}}{\textit{Conclustion}}$$

They can be read as "If the Premise is true, then the Conclusion is true."

Proof rules

$$\frac{A \wedge B}{A}\ \wedge E1 \qquad \frac{A \wedge B}{B}\ \wedge E2 \qquad \frac{A \quad B}{A \wedge B}\ \wedge I$$

$$\frac{A}{A \vee B}\ \vee I1 \qquad \frac{B}{A \vee B}\ \vee I2 \qquad \frac{A \vee B \quad A \to C \quad B \to C}{C}\ \vee E$$

$$\frac{\begin{array}{c}[A] \\ \vdots \\ B\end{array}}{A \to B}\ \to I \qquad \frac{A \quad A \to B}{B}\ \to E$$

$$\frac{A \to \bot}{\neg A}\ \neg I \qquad \frac{A \quad \neg A}{\bot}\ \neg E$$

$$\frac{}{\top}\ \top I \qquad \frac{\bot}{A}\ \bot E \qquad \frac{}{A \vee \neg A}\ LEM$$

Two Styles of Proof

There are two styles of proof

- 3 column proofs
- tree proofs

They both have their pros and cons.
3 column proofs are easier to typeset.
tree proofs are easier to read and think about.

I'll be using tree proofs in this class.
If you're using LaTeX I've got some tips on doing tree proofs.

Example: 3-column proofs

Prove: $A \wedge B \vdash B \wedge A$.

1	$A \wedge B$	Premise
2	A	$\wedge E_1$, 1
3	B	$\wedge E_2$, 1
4	$B \wedge A$	$\wedge I$, 3, 2

Things to remember

- Every line has a line number on the left, and justification on the right.
- Every justification must reference the lines it used.
- The order of both lines, and references, is VERY important.

Example: tree proofs

Prove: $A \wedge B \vdash B \wedge A$.

$$\dfrac{\dfrac{A \wedge B}{B}\wedge E2 \qquad \dfrac{A \wedge B}{A}\wedge E1}{B \wedge A}\wedge I$$

Things to remember

- Each leaf of the tree must be a premise.
- You have to match the order and form of the inference rules.

Pattern Matching

Each inference rule is like a pattern. We give it something that "looks like" the premise, and it give us something that looks like the conclusion.

While we have to match the rule, we don't have to be exact.
For example:
$A \wedge B$, $B \wedge A$, and $(C \to D) \wedge (D \to C)$] all *match* the pattern $A \wedge B$.
Formally: a statement S **matches** a pattern P if you can replace the variables in the P so that it is identical to S.

Equality proofs

How do we prove $A \equiv B$?
We could use the equivalences from last time.
But, what if we wanted to do it with inference rules?

We'll use one equivalence
$A \equiv B = A \leftrightarrow B$.
We can prove this by proving $A \vdash B$ and $B \vdash A$.
Example:
Prove: $A \wedge B \leftrightarrow B \wedge A$
$A \wedge B \vdash B \wedge A$

$$\dfrac{\dfrac{A \wedge B}{B}\wedge E2 \quad \dfrac{A \wedge B}{A}\wedge E1}{B \wedge A}\wedge I$$

$B \wedge A \vdash A \wedge B$

$$\dfrac{\dfrac{B \wedge A}{A}\wedge E2 \quad \dfrac{B \wedge A}{B}\wedge E1}{A \wedge B}\wedge I$$

Equality proofs

Prove: $A \wedge B \leftrightarrow B \wedge A$

$A \wedge B \vdash B \wedge A$

1	$A \wedge B$	Premise
2	A	$\wedge E_1$, 1
3	B	$\wedge E_2$, 1
4	$B \wedge A$	$\wedge I$, 3, 2

$B \wedge A \vdash A \wedge B$

1	$B \wedge A$	Premise
2	A	$\wedge E_2$, 1
3	B	$\wedge E_1$, 1
4	$A \wedge B$	$\wedge I$, 2, 3

Examples

Prove: $A \to B, B \to C \vdash A \to C$

$$\dfrac{\dfrac{\dfrac{[A] \qquad A \to B}{B} \to E \qquad B \to C}{C} \to E}{A \to C} \to I$$

Examples 3-column

Prove: $A \to B, B \to C \vdash A \to C$

1	$A \to B$	Premise
2	$B \to C$	Premise
3	A	Assumption
4	B	$\to E$, 1, 3
5	C	$\to E$, 2, 4
6	$A \to C$	$\to I$, 3-5

Examples

Prove: $A \to B, \vdash \neg B \to \neg A$

$$\dfrac{\dfrac{\dfrac{[\neg B] \qquad \dfrac{[A] \qquad A \to B}{B} \to E}{\bot} \neg E}{A \to \bot} \to I}{\neg B \to \neg A} \neg I \to I$$

Examples

Prove: $A \to B, \vdash \neg B \to \neg A$

1	$A \to B$	Premise
2	$\neg B$	Assumption
3	A	Assumption
4	B	$\to E$, 3, 1
5	$\bot$	$\neg E$, 4, 2
6	$A \to \bot$	$\to I$, 3-5
7	$\neg A$	$\neg I$, 6
8	$\neg B \to \neg A$	$\to I$, 2-7

Examples

Prove: $\neg\neg A \vdash A$

$$\dfrac{\dfrac{}{A \vee \neg A}\, LEM \qquad \dfrac{\dfrac{[A] \qquad [A]}{A \to A} \to I \qquad \dfrac{[\neg A] \qquad \dfrac{\dfrac{[\neg A] \qquad \neg\neg A}{\bot} \neg E}{A} \bot E}{\neg A \to A} \to I}{A} \vee E$$

Examples 3-column

Prove: $\neg\neg A \vdash A$

1	$\neg\neg A$	Premise
2	$A \vee \neg A$	LEM
3	$\quad A$	Assumption
4	$A \rightarrow A$	$\rightarrow I$, 3-3
5	$\quad \neg A$	Assumption
6	$\quad \bot$	$\neg E$, 5, 1
7	$\quad A$	$\bot E$, 6
8	$\neg A \rightarrow A$	$\rightarrow I$, 5-7
9	A	$\vee E$, 2,4,8

Examples

Prove: $\vdash (A \to B) \vee (B \to A)$

To save on space, let $C = (A \to B) \vee (B \to A)$

$$\dfrac{\dfrac{}{A \vee \neg A}\,LEM \qquad \dfrac{\dfrac{[A]}{A \to C} \to I \qquad \dfrac{\dfrac{\dfrac{[B] \qquad [A]}{B \to A} \to I}{C} \vee I2 \qquad \dfrac{\dfrac{\dfrac{[A] \qquad [\neg A]}{\bot} \neg E}{B} \bot E}{A \to B} \to I}{C} \vee I1}{\neg A \to C} \to I}{C} \vee E$$

Examples

1	$A \vee \neg A$	LEM
2	$\quad A$	Assumption
3	$\quad\quad B$	Assumption
4	$\quad\quad A$	Assumption
5	$\quad B \to A$	$\to I$, 3-4
6	$\quad A \to B \vee B \to A$	$\vee I$, 5
7	$A \to (A \to B \vee B \to A)$	$\to I$, 2-6
8	$\quad \neg A$	Assumption
9	$\quad\quad A$	Assumption
10	$\quad\quad \bot$	$\neg E$, 8, 9
11	$\quad\quad B$	$\bot E$, 10
12	$\quad A \to B$	$\to I$, 9-11
13	$\quad A \to B \vee B \to A$	$\vee I$, 12
14	$\neg A \to (A \to B \vee B \to A)$	$\to I$, 8-13
15	$(A \to B \vee B \to A)$	$\vee E$, 1,7,14

Soundness and Completeness

This is not the only set of inference rules we can use.
We can derive one set of inference rule from Another.
Just like how we derived every operation from NAND.
We're interested in two properties.

- **sound** if it is impossible to derive $\bot$.
- **complete** if every tautology can be derived.

Examples

If we add the rule

$$\frac{A}{\neg A}$$

Then our system is no longer sound.

If we remove the rule the rule

$$\frac{}{A \vee \neg A}\ LEM$$

Then our system is no longer complete.

If you're ever designing a proof system, this is very easy to screw up.

Recap

- All math theorems have the form if A and B and C then D.
- We can prove something of this form using inference rules.
- A proof is just a tree of inference rules, where the leaves are premises.
- Soundness and completeness are important properties for a proof system.