Proof

CS 130

Alex Vondrak

ajvondrak@csupomona.edu

Winter 2012

Proof

Definitions

A proof is a sequence of WFFs **with justifications**. Each line in a proof must be one of:

- An axiom
- The result of an inference rule
- A hypothesis
- A lemma

The particular axioms and inference rules we choose comprise a proof system.

Axioms and Inference Rules

Definition

An axiom is a WFF that we assume to be true by virtue of being of a particular form.

Definition

An inference rule is an argument that allows us to write a new line in the proof based on the assumption that previous lines are true.
We write

$$P_1, \quad P_2, \quad P_3, \quad \ldots, \quad P_n \qquad \vdash \qquad Q$$

if we can prove (or infer) Q given that $P_1, P_2, P_3, \ldots, P_n$ are all true.

Propositional Logic Proof System

Definition (Axioms of Propositional Logic)

The following axioms, due to Jan Łukasiewicz, form the basis for what we hold true in propositional logic. They are true no matter what WFFs we substitute for A, B, and C.

Axiom 1: $\vdash \quad (A \implies (B \implies A))$

Axiom 2: $\vdash \quad ((A \implies (B \implies C)) \implies ((A \implies B) \implies (A \implies C)))$

Axiom 3: $\vdash \quad ((\neg B \implies \neg A) \implies (A \implies B))$

Definition (Inference Rule of Propositional Logic)

Propositional logic has a single inference rule called Modus Ponendo Ponens (or just Modus Ponens for short)

$$(A \implies B), \quad A \quad \vdash \quad B$$

Multiple Choice Question

$$\textbf{Axiom 1: } \vdash \quad (A \implies (B \implies A))$$

Which of the following is an instance of Axiom 1?

(A) $(q \implies (p \implies q))$

(B) $(A \implies (A \implies A))$

(C) $((B \implies C) \implies (\neg Q \implies (B \implies C)))$

(D) All of the above

Multiple Choice Question

Axiom 2: $\vdash \quad ((A \implies (B \implies C)) \implies ((A \implies B) \implies (A \implies C)))$

Which of the following is an instance of Axiom 2?

(A) $((q \implies (p \implies r)) \implies ((q \implies p) \implies (q \implies (p \implies r))))$

(B) $((\neg B \implies \neg(A \implies B)) \implies ((A \implies B) \implies B))$

(C) $((\neg q \implies (\neg p \implies \neg r)) \implies ((\neg q \implies \neg p) \implies (\neg q \implies \neg r)))$

(D) All of the above

Multiple Choice Question

$$\textbf{Axiom 3:} \vdash \quad ((\neg B \implies \neg A) \implies (A \implies B))$$

Which of the following is an instance of Axiom 3?

(A) $((\neg q \implies \neg p) \implies (p \implies (\neg q \implies \neg p)))$

(B) $((\neg(B \implies A) \implies \neg(A \implies B)) \implies ((A \implies B) \implies (B \implies A)))$

(C) $((\neg Q \implies (\neg P \implies \neg Q)) \implies ((\neg Q \implies \neg P) \implies (\neg Q \implies \neg Q)))$

(D) All of the above

Multiple Choice Question

$$\textbf{Modus Ponens: } (A \implies B), \quad A \quad \vdash \quad B$$

Suppose we know the following is true:

- $((A \implies B) \implies ((B \implies A) \implies (A \implies B)))$

What can we conclude by Modus Ponens?

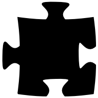
(A) $((B \implies A) \implies (A \implies B))$

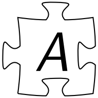
(B) $(B \implies ((B \implies A) \implies (A \implies B)))$

(C) B

(D) None of the above

Thinking About Modus Ponens

$($  $\implies B)$



$$B$$

Multiple Choice Question

$$\textbf{Modus Ponens: } (A \implies B), \quad A \qquad \vdash \qquad B$$

Suppose we know the following are true:

- $((A \implies B) \implies ((B \implies A) \implies (A \implies B)))$
- A

What can we conclude by Modus Ponens?

(A) $((B \implies A) \implies (A \implies B))$

(B) $(B \implies ((B \implies A) \implies (A \implies B)))$

(C) B

(D) None of the above

Multiple Choice Question

$$\textbf{Modus Ponens:}\ (A \implies B),\quad A \qquad \vdash \qquad B$$

Suppose we know the following are true:

- $((A \implies B) \implies ((B \implies A) \implies (A \implies B)))$
- $(A \implies B)$

What can we conclude by Modus Ponens?

(A) $((B \implies A) \implies (A \implies B))$

(B) $(B \implies ((B \implies A) \implies (A \implies B)))$

(C) B

(D) None of the above

Proof Sequence

To prove something of the form

$$P_1, \quad P_2, \quad P_3, \quad \ldots, \quad P_n \qquad \vdash \qquad Q$$

- Write P_1 on a line, justify it as a **hypothesis**
- Write P_2 on a line, justify it as a **hypothesis**
- Write P_3 on a line, justify it as a **hypothesis**
- ...
- Write P_n on a line, justify it as a **hypothesis**
- Through a series of other lines and justifications, the proof is finished when the last line is Q

Justification

- To justify an instance of an axiom, write
  - which axiom it is (Axiom 1, 2, or 3)
  - what the variables are being substituted for—$A :=?$, $B :=?$, $C :=?$
- To justify a line via Modus Ponens, write
  - that you're using Modus Ponens
  - the conclusion you can infer from Modus Ponens
  - the line numbers of the **two** premises you can use to infer said conclusion

Our First Proof

We prove that the following is true (regardless of what WFF A is) by using propositional logic.

$$\vdash \quad (A \implies A)$$

What do we assume as our hypotheses?

(A) A

(B) $(A \implies A)$

(C) Both of the above

(D) None of the above

Our First Proof

$$\vdash \quad (A \implies A)$$

	Well-Formed Formula	Justification
1.	???	???

We don't have any assumptions to make.
What else do we know must be true?

(A) $(A \implies A)$

(B) Inference Rules

(C) Axioms

(D) Nothing

Our First Proof

$$\vdash \quad (A \implies A)$$

	Well-Formed Formula	Justification
1.	$(A \implies ((A \implies A) \implies A))$	???

How do we justify Line 1?

(A) Axiom 1

(B) Axiom 1: $A := A$, $B := A$

(C) Axiom 1: $A := A$, $B := (A \implies A)$

(D) Axiom 1: $A := (A \implies A)$, $B := A$

Our First Proof

$$\vdash \quad (A \implies A)$$

	Well-Formed Formula	Justification
1.	$(A \implies ((A \implies A) \implies A))$	Axiom 1: $A := A$, $B := (A \implies A)$
2.	$((A \implies ((A \implies A) \implies A)) \implies$ $((A \implies (A \implies A)) \implies (A \implies A)))$	???

How do we justify Line 2?

(A) Modus Ponens: Line 1

(B) Axiom 1: $A := A$, $B := (A \implies A)$

(C) Axiom 2: $A := A$, $B := (A \implies A)$, $C := A$

(D) Axiom 3: $A := (A \implies A)$, $B := A$

Our First Proof

$$\vdash \quad (A \implies A)$$

Well-Formed Formula	Justification
1. $(A \implies ((A \implies A) \implies A))$	Axiom 1: $A := A$, $B := (A \implies A)$
2. $((A \implies ((A \implies A) \implies A)) \implies ((A \implies (A \implies A)) \implies (A \implies A)))$	Axiom 2: $A := A$, $B := (A \implies A)$, $C := A$
3. ???	Modus Ponens: Lines 1 and 2

What is the result on Line 3?

(A) $((A \implies (A \implies A)) \implies (A \implies A))$

(B) $(A \implies A)$

(C) $(A \implies (A \implies A))$

(D) $((A \implies (A \implies A)) \implies ((A \implies A) \implies (A \implies A)))$

Our First Proof

$$\vdash \quad (A \implies A)$$

	Well-Formed Formula	Justification
1.	$(A \implies ((A \implies A) \implies A))$	Axiom 1: $A := A$, $B := (A \implies A)$
2.	$((A \implies ((A \implies A) \implies A)) \implies$ $((A \implies (A \implies A)) \implies (A \implies A)))$	Axiom 2: $A := A$, $B := (A \implies A)$, $C := A$
3.	$((A \implies (A \implies A)) \implies (A \implies A))$	Modus Ponens: Lines 1 and 2
4.	???	???

What piece of information do we need in order to “get at” $(A \implies A)$?

(A) $(A \implies A)$

(B) A

(C) $((A \implies (A \implies A)) \implies (A \implies A))$

(D) $(A \implies (A \implies A))$

Our First Proof

$$\vdash \quad (A \implies A)$$

	Well-Formed Formula	Justification
1.	$(A \implies ((A \implies A) \implies A))$	Axiom 1: $A := A$, $B := (A \implies A)$
2.	$((A \implies ((A \implies A) \implies A)) \implies ((A \implies (A \implies A)) \implies (A \implies A)))$	Axiom 2: $A := A$, $B := (A \implies A)$, $C := A$
3.	$((A \implies (A \implies A)) \implies (A \implies A))$	Modus Ponens: Lines 1 and 2
4.	$(A \implies (A \implies A))$	???

Can we actually **justify** Line 4?

(A) No: it's not true in general

(B) Yes: argue by truth table

(C) Yes: it's an instance of Axiom 1

(D) We don't need to justify Line 4

Our First Proof

$$\vdash \quad (A \implies A)$$

	Well-Formed Formula	Justification
1.	$(A \implies ((A \implies A) \implies A))$	Axiom 1: $A := A$, $B := (A \implies A)$
2.	$((A \implies ((A \implies A) \implies A)) \implies ((A \implies (A \implies A)) \implies (A \implies A)))$	Axiom 2: $A := A$, $B := (A \implies A)$, $C := A$
3.	$((A \implies (A \implies A)) \implies (A \implies A))$	Modus Ponens: Lines 1 and 2
4.	$(A \implies (A \implies A))$	Axiom 1: $A := A$, $B := A$
5.	???	???

What should be the next step?

(A) None; we're done

(B) Apply Modus Ponens: Lines 3 and 4

(C) Apply Modus Ponens: Lines 1 and 4

(D) Infer A so we can use Modus Ponens with it and Line 4

The Principle of Identity

Theorem

For any WFF A,

$$\vdash \quad (A \implies A)$$

Proof.

Well-Formed Formula	Justification
1. $(A \implies ((A \implies A) \implies A))$	Axiom 1: $A := A$, $B := (A \implies A)$
2. $((A \implies ((A \implies A) \implies A)) \implies ((A \implies (A \implies A)) \implies (A \implies A)))$	Axiom 2: $A := A$, $B := (A \implies A)$, $C := A$
3. $((A \implies (A \implies A)) \implies (A \implies A))$	Modus Ponens: Lines 1 and 2
4. $(A \implies (A \implies A))$	Axiom 1: $A := A$, $B := A$
5. $(A \implies A)$	Modus Ponens: Lines 3 and 4

□

The Principle of Identity

Theorem

For any WFF A,

$$\vdash \quad (A \implies A)$$

Proof.

A	$(A \implies A)$
F	T
T	T

□

Lemmas

We may use instances of previously proven theorems as lemmas in a proof.

Justification

If the lemma has the form

$$P_1, P_2, P_3, \ldots, P_n \qquad \vdash \qquad Q$$

- write the name of the lemma
- write the line numbers corresponding to the premises

Lemmas

We may use instances of previously proven theorems as lemmas in a proof.

Justification

If the lemma has the form

$$\vdash \quad Q$$

- write the name of the lemma
- write what the variables are being substituted for in the WFF Q
  - $A :=?$
  - $B :=?$
  - $C :=?$
  - etc.

Multiple Choice Question

$$\vdash \quad (P \implies (Q \implies Q))$$

	Well-Formed Formula	Justification
1.	$(Q \implies Q)$	???
2.	$((Q \implies Q) \implies (P \implies (Q \implies Q)))$	Axiom 1 $A := (Q \implies Q)$, $B := P$
3.	$(P \implies (Q \implies Q))$	Modus Ponens Lines 1 and 2

How do we justify Line 1?

(A) Principle of Identity

(B) Principle of Identity: Line 1

(C) Principle of Identity: $A := Q$

(D) Principle of Identity: $Q := A$

Using Hypotheses

$$(Q \implies Q) \quad \vdash \quad (P \implies (Q \implies Q))$$

	Well-Formed Formula	Justification
1.	$(Q \implies Q)$	???
2.	$((Q \implies Q) \implies (P \implies (Q \implies Q)))$	Axiom 1 $A := (Q \implies Q)$, $B := P$
3.	$(P \implies (Q \implies Q))$	Modus Ponens Lines 1 and 2

Unlike lemmas or axioms, hypotheses must be used exactly as stated.

How should we justify Line 1?

(A) Principle of Identity: $A := Q$

(B) Hypothesis

(C) Principle of Identity: Hypothesis

(D) Doesn't matter, since this proof is redundant

The Deduction Theorem

Theorem (Herbrand, 1930)

If: $G_1, \quad G_2, \quad \ldots, \quad G_n, \quad A \quad \vdash \quad B$

Then: $G_1, \quad G_2, \quad \ldots, \quad G_n \quad \vdash \quad (A \implies B)$

Example

On Homework 2, you prove **Modus Ponens Deduction**:

$$(A \implies B), \quad (A \implies (B \implies C)) \quad \vdash \quad (A \implies C)$$

By the Deduction Theorem, it is possible to prove

$$(A \implies B) \quad \vdash \quad ((A \implies (B \implies C)) \implies (A \implies C))$$

Applying the Deduction Theorem again, this is means that

$$\vdash \quad ((A \implies B) \implies ((A \implies (B \implies C)) \implies (A \implies C)))$$

Conversely

Theorem

If: $G_1, \quad G_2, \quad \ldots, \quad G_n \qquad \vdash \qquad (A \implies B)$

Then: $G_1, \quad G_2, \quad \ldots, \quad G_n, \quad A \qquad \vdash \qquad B$

Proof.

1.	G_1	Hypothesis
2.	G_2	Hypothesis
	$\ldots$	
n.	G_n	Hypothesis
$n+1$.	A	Hypothesis
$n+2$.	$(A \implies B)$	Lines 1–n
$n+3$.	B	Modus Ponens: lines $n+1$ and $n+2$

□

Why Have A Proof System?

Definition (Formalism)

The theory that math/logic is a "meaningless game" of "meaningless symbols".

- Descends from David Hilbert's school of thought
- Close connection with computer science (e.g., theorem provers)
- Often associated with mathematical rigor (cf. *Principia Mathematica*)

Note

Due to Gödel's Incompleteness Theorem, we know that strict formalism cannot consistently be used for all mathematical proofs. We can still prove a lot of interesting things, though.

Why This Proof System?

Theorem (Soundness)

If: $\vdash A$

Then: *A is a tautology*

Theorem (Completeness)

If: *A is a tautology*

Then: $\vdash A$

Theorem (Consistency)

There is no formula A in propositional logic such that

$$\vdash A \quad \text{and} \quad \vdash \neg A$$

Why This Proof System?

Axiom 1: $\vdash \quad (A \implies (B \implies A))$

Axiom 2: $\vdash \quad ((A \implies (B \implies C)) \implies ((A \implies B) \implies (A \implies C)))$

Axiom 3: $\vdash \quad ((\neg B \implies \neg A) \implies (A \implies B))$

Modus Ponens: $(A \implies B), \quad A \quad \vdash \quad B$

What about the other Boolean operators ($\wedge$, $\vee$, $\iff$)?

(A) We'd need more axioms about how $\wedge$, $\vee$, and $\iff$ work

(B) We'd need more inference rules about how $\wedge$, $\vee$, and $\iff$ work

(C) Those operators don't matter; they're pretty much useless

(D) This system alone is enough to specify the behaviors of $\wedge$, $\vee$, and $\iff$, since we can define them in terms of $\implies$ and $\neg$

Why This Proof System?

Is it possible to add a new axiom, Axiom X, that proves something new?

Nope!

Let X^* be an instance of Axiom X.
Suppose some formula A can be proven from X^*:

$$X^* \vdash A$$

By the Deduction Theorem, $\vdash (X^* \implies A)$.
By the Completeness Theorem,

$$\vdash X^*$$

without using Axiom X, since instances of axioms are tautologies.
Thus, we can form a proof of A without using Axiom X:

1. X^* — Lemma: $\vdash X^*$
2. $(X^* \implies A)$ — Lemma: $\vdash (X^* \implies A)$
3. A — Modus Ponens: Lines 1 and 2

Why This Proof System?

Is it possible to remove one of the Axioms and still be able to prove the same things?

(A) Yes

(B) No

Why This Proof System?

Is it possible to remove one of the Axioms and still be able to prove the same things?

(A) Yes

(B) No—can't prove any one of the Axioms from the others

Why This Proof System?

It is possible to start completely from scratch!

Definition (Hilbert's Axiom System)

Axiom 1: $(A \implies (B \implies A))$

Axiom 2: $((A \implies (B \implies C)) \implies (B \implies (A \implies C)))$

Axiom 3: $((B \implies C) \implies ((A \implies B) \implies (A \implies C)))$

Axiom 4: $(A \implies (\neg A \implies B))$

Axiom 5: $((A \implies B) \implies ((\neg A \implies B) \implies B))$

Inference Rule: Modus Ponens

Definition (Meredith's Axiom System)

Axiom: $$(((((A \implies B) \implies (\neg C \implies \neg D)) \implies C) \implies E) \implies ((E \implies A) \implies (D \implies A)))$$

Inference Rule: Modus Ponens

Multiple Choice Question

Does the following argument make sense intuitively?

All men are mortal.
Socrates is a man.

$\therefore$ Socrates is mortal.

(A) Seems valid

(B) Seems invalid

Multiple Choice Question

Is the argument valid in propositional logic?

All men are mortal.	a
Socrates is a man.	b
$\therefore$ Socrates is mortal.	$\therefore c$

I.e., is it possible to prove $a, \quad b \quad \vdash \quad c$?

(A) Yes: look at the right line of a truth table

(B) Yes: true in all cases

(C) No: always false

(D) No: not always true

Multiple Choice Question

What if we rephrase the argument?

$$\begin{array}{c} \text{Something is a man} \implies \text{It is mortal} \\ \text{Something is Socrates} \implies \text{It is a man} \\ \hline \therefore \text{Something is Socrates} \implies \text{It is mortal} \end{array}$$

Can we translate this into valid propositional logic?

(A) Yes: this is just Syllogism

(B) Yes: we can see it's a tautology if we build a truth table

(C) No: anaphora makes "It" and "Something" distinct ideas ("It" is a reference to a specific "Something")

(D) No: we don't specify what "Something" might be