Bonus Lecture 1: Formal Proof Systems

Because Formalism Improves Everything

Why Formal Proofs?

Proofs so far designed to be human-readable

- Lots of fluff
- Quote simple results without proving
- etc

Why Formal Proofs?

Proofs so far designed to be human-readable

- Lots of fluff
- Quote simple results without proving
- etc

Hard for a computer to understand :(
Hard to prove things about proofs :(

Why Formal Proofs?

Proofs so far designed to be human-readable

- Lots of fluff
- Quote simple results without proving
- etc

Hard for a computer to understand :(
Hard to prove things about proofs :(

Formalizing a proof system addresses these issues
But at the cost of readability, length

Why Formal Proofs?

Proofs so far designed to be human-readable

- Lots of fluff
- Quote simple results without proving
- etc

Hard for a computer to understand :(
Hard to prove things about proofs :(

Formalizing a proof system addresses these issues
But at the cost of readability, length

Today, focus on propositional logic (no quantifiers)

Axioms

Need logical axioms to get anywhere
System for today based on properties of $\Rightarrow$ and $\neg$

Axioms

Need logical axioms to get anywhere
System for today based on properties of $\Rightarrow$ and $\neg$

(1) $\varphi_1 \Rightarrow \varphi_1$

Axioms

Need logical axioms to get anywhere

System for today based on properties of $\Rightarrow$ and $\neg$

(1) $\varphi_1 \Rightarrow \varphi_1$

(2) $\varphi_1 \Rightarrow (\varphi_2 \Rightarrow \varphi_1)$

Axioms

Need logical axioms to get anywhere
System for today based on properties of $\Rightarrow$ and $\neg$

(1) $\varphi_1 \Rightarrow \varphi_1$
(2) $\varphi_1 \Rightarrow (\varphi_2 \Rightarrow \varphi_1)$
(3) $\varphi_1 \Rightarrow [(\neg\varphi_1) \Rightarrow \varphi_2]$

Axioms

Need logical axioms to get anywhere
System for today based on properties of $\Rightarrow$ and $\neg$

(1) $\varphi_1 \Rightarrow \varphi_1$
(2) $\varphi_1 \Rightarrow (\varphi_2 \Rightarrow \varphi_1)$
(3) $\varphi_1 \Rightarrow [(\neg\varphi_1) \Rightarrow \varphi_2]$
(4) $[(\neg\varphi_1) \Rightarrow \varphi_1] \Rightarrow \varphi_1$

Axioms

Need logical axioms to get anywhere
System for today based on properties of $\Rightarrow$ and $\neg$

(1) $\varphi_1 \Rightarrow \varphi_1$
(2) $\varphi_1 \Rightarrow (\varphi_2 \Rightarrow \varphi_1)$
(3) $\varphi_1 \Rightarrow [(\neg\varphi_1) \Rightarrow \varphi_2]$
(4) $[(\neg\varphi_1) \Rightarrow \varphi_1] \Rightarrow \varphi_1$
(5) $(\neg\varphi_1) \Rightarrow (\varphi_1 \Rightarrow \varphi_2)$

Axioms

Need logical axioms to get anywhere
System for today based on properties of $\Rightarrow$ and $\neg$

(1) $\varphi_1 \Rightarrow \varphi_1$

(2) $\varphi_1 \Rightarrow (\varphi_2 \Rightarrow \varphi_1)$

(3) $\varphi_1 \Rightarrow [(\neg\varphi_1) \Rightarrow \varphi_2]$

(4) $[(\neg\varphi_1) \Rightarrow \varphi_1] \Rightarrow \varphi_1$

(5) $(\neg\varphi_1) \Rightarrow (\varphi_1 \Rightarrow \varphi_2)$

(6) $\varphi_1 \Rightarrow \Big([\neg\varphi_2] \Rightarrow [\neg(\varphi_1 \Rightarrow \varphi_2)]\Big)$

Axioms

Need logical axioms to get anywhere
System for today based on properties of $\Rightarrow$ and $\neg$

(1) $\varphi_1 \Rightarrow \varphi_1$
(2) $\varphi_1 \Rightarrow (\varphi_2 \Rightarrow \varphi_1)$
(3) $\varphi_1 \Rightarrow [(\neg\varphi_1) \Rightarrow \varphi_2]$
(4) $[(\neg\varphi_1) \Rightarrow \varphi_1] \Rightarrow \varphi_1$
(5) $(\neg\varphi_1) \Rightarrow (\varphi_1 \Rightarrow \varphi_2)$
(6) $\varphi_1 \Rightarrow \Big([\neg\varphi_2] \Rightarrow [\neg(\varphi_1 \Rightarrow \varphi_2)]\Big)$
(7) $[\varphi_1 \Rightarrow (\varphi_2 \Rightarrow \varphi_3)] \Rightarrow [(\varphi_1 \Rightarrow \varphi_2) \Rightarrow (\varphi_1 \Rightarrow \varphi_3)]$

φs are any propositional formula

Why These Axioms?

Where did these precise axioms come from?

Why These Axioms?

Where did these precise axioms come from?

Turns out, sufficient for *completeness*
"If it's true, we can prove it"

Why These Axioms?

Where did these precise axioms come from?

Turns out, sufficient for *completeness*
"If it's true, we can prove it"

Could include more axioms, but more cumbersome

Formal Proofs, Formally

Start with set of givens Γ.

[1] This is known as *Modus Ponens* because Latin

Formal Proofs, Formally

Start with set of givens Γ.

Proof is sequence of formulae $(\varphi_1, \varphi_2, \ldots, \varphi_n)$

[1] This is known as *Modus Ponens* because Latin

Formal Proofs, Formally

Start with set of givens Γ.

Proof is sequence of formulae $(\varphi_1, \varphi_2, \ldots, \varphi_n)$
$\forall i$, must have one of:

- φ_i is an axiom
- φ_i in Γ
- $\exists j, k < i$ such that φ_k is $\varphi_j \Rightarrow \varphi_i$[1]

[1] This is known as *Modus Ponens* because Latin

Formal Proofs, Formally

Start with set of givens Γ.

Proof is sequence of formulae $(\varphi_1, \varphi_2, \ldots, \varphi_n)$
$\forall i$, must have one of:

- φ_i is an axiom
- φ_i in Γ
- $\exists j, k < i$ such that φ_k is $\varphi_j \Rightarrow \varphi_i$[1]

Say Γ proves φ ($\Gamma \vdash \varphi$) if $\exists$ a proof with $\varphi_n = \varphi$

[1] This is known as *Modus Ponens* because Latin

An Example Proof

Start with $\Gamma = \{\neg(\neg P)\}$, prove P

An Example Proof

Start with $\Gamma = \{\neg(\neg P)\}$, prove P

Proof:

- $[\neg(\neg P)] \Rightarrow [(\neg P) \Rightarrow P]$ *(Axiom 5)*
- $[(\neg P) \Rightarrow P] \Rightarrow P$ *(Axiom 4)*
- $\neg(\neg P)$ *(In Γ)*

An Example Proof

Start with $\Gamma = \{\neg(\neg P)\}$, prove P

Proof:

- $[\neg(\neg P)] \Rightarrow [(\neg P) \Rightarrow P]$ *(Axiom 5)*
- $[(\neg P) \Rightarrow P] \Rightarrow P$ *(Axiom 4)*
- $\neg(\neg P)$ *(In Γ)*
- $(\neg P) \Rightarrow P$ *(Modus Ponens)*

An Example Proof

Start with $\Gamma = \{\neg(\neg P)\}$, prove P

Proof:

- $[\neg(\neg P)] \Rightarrow [(\neg P) \Rightarrow P]$ *(Axiom 5)*
- $[(\neg P) \Rightarrow P] \Rightarrow P$ *(Axiom 4)*
- $\neg(\neg P)$ *(In Γ)*
- $(\neg P) \Rightarrow P$ *(Modus Ponens)*
- P *(Modus Ponens)*

Inconsistent Beginnings...

Start with $\Gamma = \{P, \neg P\}$, prove Q

Inconsistent Beginnings...

Start with $\Gamma = \{P, \neg P\}$, prove Q

Proof:

- $P \Rightarrow [(\neg P) \Rightarrow Q]$ *(Axiom 3)*
- P *(In Γ)*
- $\neg P$ *(In Γ)*

Inconsistent Beginnings...

Start with $\Gamma = \{P, \neg P\}$, prove Q

Proof:

- $P \Rightarrow [(\neg P) \Rightarrow Q]$ *(Axiom 3)*
- P *(In Γ)*
- $\neg P$ *(In Γ)*
- $(\neg P) \Rightarrow Q$ *(Modus Ponens)*
- Q *(Modus Ponens)*

Inconsistent Beginnings...

Start with $\Gamma = \{P, \neg P\}$, prove Q

Proof:

- $P \Rightarrow [(\neg P) \Rightarrow Q]$ *(Axiom 3)*
- P *(In Γ)*
- $\neg P$ *(In Γ)*
- $(\neg P) \Rightarrow Q$ *(Modus Ponens)*
- Q *(Modus Ponens)*

Wait — where did Q come from?

Inconsistent Beginnings...

Start with $\Gamma = \{P, \neg P\}$, prove Q

Proof:

- $P \Rightarrow [(\neg P) \Rightarrow Q]$ *(Axiom 3)*
- P *(In Γ)*
- $\neg P$ *(In Γ)*
- $(\neg P) \Rightarrow Q$ *(Modus Ponens)*
- Q *(Modus Ponens)*

Wait — where did Q come from?

Principle of Explosion: If you start with a false statement, you can prove anything.

...Lead Anywhere

Γ *inconsistent* if proves both φ and $\neg\varphi$ for some φ

Claim: If Γ inconsistent, can prove anything!

…Lead Anywhere

Γ *inconsistent* if proves both φ and $\neg\varphi$ for some φ
Claim: If Γ inconsistent, can prove anything!

Why?
Consider proof of ψ for any ψ:

- *Proof of* φ
- *Proof of* $\neg\varphi$

...Lead Anywhere

Γ *inconsistent* if proves both φ and $\neg\varphi$ for some φ
Claim: If Γ inconsistent, can prove anything!

Why?
Consider proof of ψ for any ψ:

- *Proof of* φ
- *Proof of* $\neg\varphi$
- $\varphi \Rightarrow [(\neg\varphi) \to \psi]$ *(Axiom 3)*

...Lead Anywhere

Γ *inconsistent* if proves both φ and $\neg\varphi$ for some φ
Claim: If Γ inconsistent, can prove anything!

Why?
Consider proof of ψ for any ψ:

- *Proof of* φ
- *Proof of* $\neg\varphi$
- $\varphi \Rightarrow [(\neg\varphi) \to \psi]$ *(Axiom 3)*
- $(\neg\varphi) \to \psi$ *(Modus Ponens)*
- ψ *(Modus Ponens)*

Can't Get No...

How do we determine if proofs make sense?

Can't Get No...

How do we determine if proofs make sense?
What should be provable?

Can't Get No...

How do we determine if proofs make sense?
What should be provable?

Idea: back to formulae as functions

Can't Get No...

How do we determine if proofs make sense?
What should be provable?

Idea: back to formulae as functions
Consider inputs st all formulae in Γ are true
If φ true on these, say Γ satisfies φ ($\Gamma \vDash \varphi$)

Can't Get No...

How do we determine if proofs make sense?
What should be provable?

Idea: back to formulae as functions
Consider inputs st all formulae in Γ are true
If φ true on these, say Γ satisfies φ ($\Gamma \vDash \varphi$)

Ideally, Γ proves φ iff Γ satisfies φ

We're Halfway There

Theorem: If Γ proves φ, Γ satisfies φ

We're Halfway There

Theorem: If Γ proves φ, Γ satisfies φ

Proof:

- Suppose $\exists$ proof $(\varphi_1, \varphi_2, \ldots, \varphi_n = \varphi)$
- Prove Γ satisfies φ_i by induction on i

We're Halfway There

Theorem: If Γ proves φ, Γ satisfies φ

Proof:

- Suppose $\exists$ proof $(\varphi_1, \varphi_2, ..., \varphi_n = \varphi)$
- Prove Γ satisfies φ_i by induction on i
- BC ($i = 1$): Axiom (always true) or in Γ

We're Halfway There

Theorem: If Γ proves φ, Γ satisfies φ

Proof:

- Suppose $\exists$ proof $(\varphi_1, \varphi_2, ..., \varphi_n = \varphi)$
- Prove Γ satisfies φ_i by induction on i
- BC $(i = 1)$: Axiom (always true) or in Γ
- IS: Same as above if axiom or in Γ
- Else have $j, k < i$ st φ_k is $\varphi_j \Rightarrow \varphi_i$

We're Halfway There

Theorem: If Γ proves φ, Γ satisfies φ

Proof:

- Suppose $\exists$ proof $(\varphi_1, \varphi_2, ..., \varphi_n = \varphi)$
- Prove Γ satisfies φ_i by induction on i
- BC $(i = 1)$: Axiom (always true) or in Γ
- IS: Same as above if axiom or in Γ
- Else have $j, k < i$ st φ_k is $\varphi_j \Rightarrow \varphi_i$
- φ_j and φ_k satisfied by IH
- Those both true means φ_i true as well!

We're Halfway There

Theorem: If Γ proves φ, Γ satisfies φ

Proof:

- Suppose $\exists$ proof $(\varphi_1, \varphi_2, ..., \varphi_n = \varphi)$
- Prove Γ satisfies φ_i by induction on i
- BC $(i = 1)$: Axiom (always true) or in Γ
- IS: Same as above if axiom or in Γ
- Else have $j, k < i$ st φ_k is $\varphi_j \Rightarrow \varphi_i$
- φ_j and φ_k satisfied by IH
- Those both true means φ_i true as well!

Other direction also true, but much more difficult

But Wait!

What about inconsistent Γ? Proves everything!

But Wait!

What about inconsistent Γ? Proves everything!

If Γ inconsistent, no input makes all formulae true

- Recall $\Gamma = \{P, \neg P\}$ from before

But Wait!

What about inconsistent Γ? Proves everything!

If Γ inconsistent, no input makes all formulae true

- Recall $\Gamma = \{P, \neg P\}$ from before

So for any φ, Γ satisfies φ vacuously
Not a counterexample after all

Fin

If you found this interesting, consider Math 125A!