CSE 311

Foundations of Computing I

Pre-Lecture Problem

Suppose that p, and $p \rightarrow (q \wedge r)$ are true. Is q true? Can you prove it with equivalences?

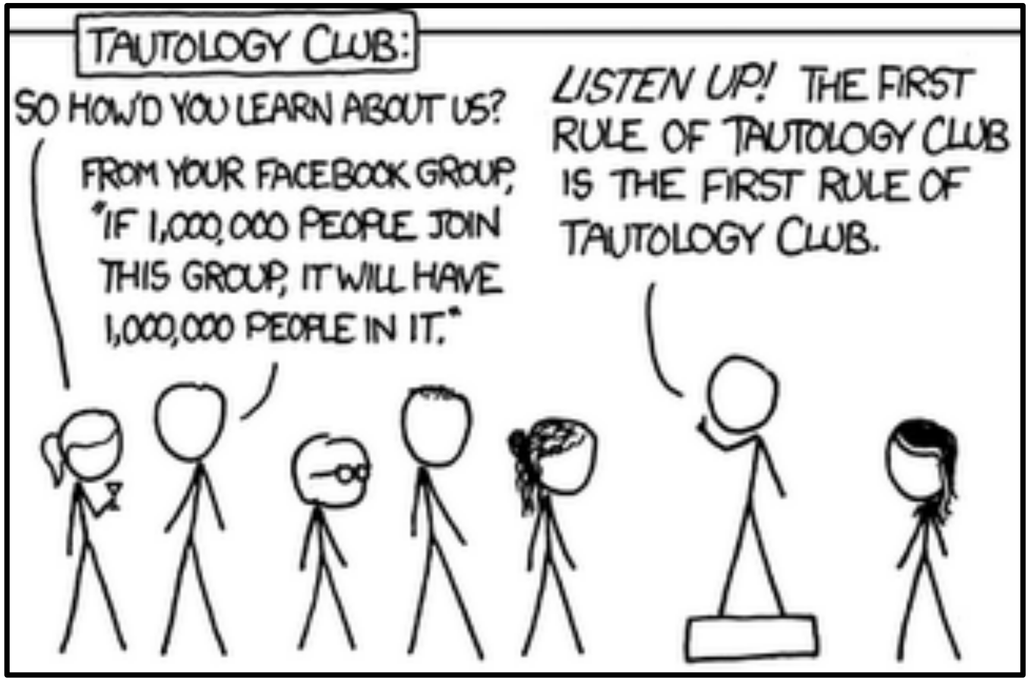
Proof From Last Time

Show that r follows from p, $p \rightarrow q$, and $q \rightarrow r$

1.	p	Given
2.	$p \rightarrow q$	Given
3.	$q \rightarrow r$	Given
4.	q	MP: 1, 2
5.	r	MP: 3, 4

CSE 311: Foundations of Computing

Lecture 7: Proofs

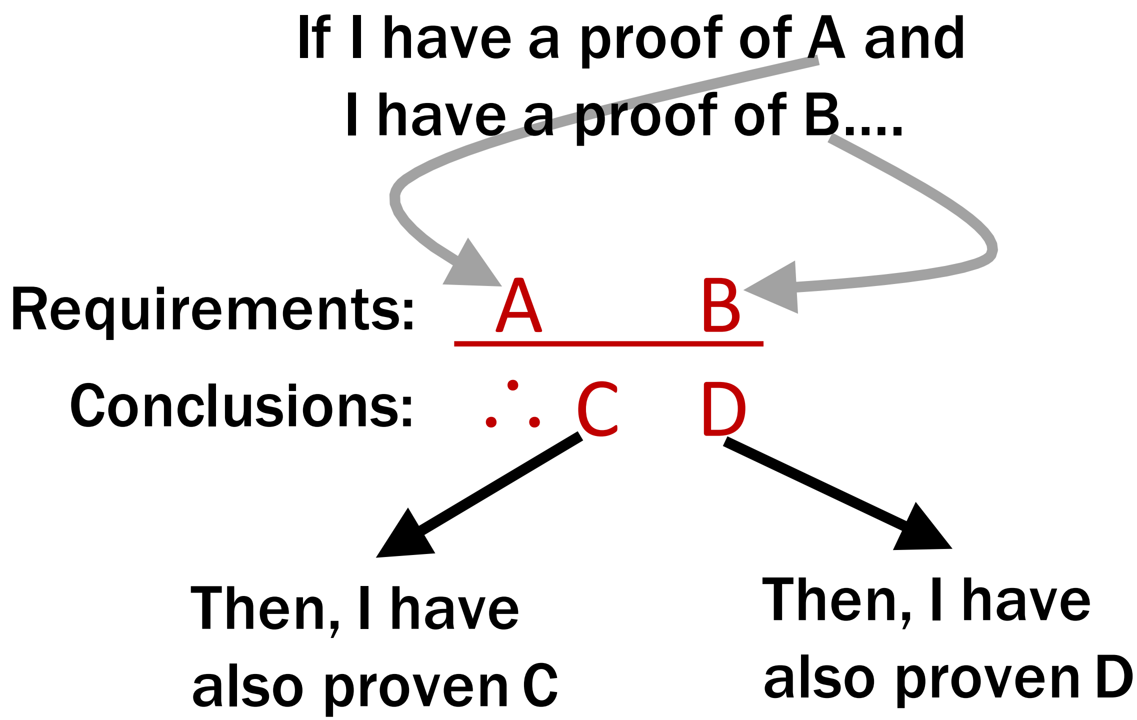


Proofs can use equivalences too

Show that $\neg p$ follows from $p \rightarrow q$ and $\neg q$

1.	$p \rightarrow q$	Given
2.	$\neg q$	Given
3.	$\neg q \rightarrow \neg p$	Contrapositive: 1
4.	$\neg p$	MP: 2, 3

Inference Rules



Example (Modus Ponens):

$$\frac{A \qquad A \rightarrow B}{\therefore \qquad B}$$

If I have a proof of A and A → B,
Then I have a proof of B.

Axioms

If I have nothing...

Requirements:

Conclusions: $\therefore$ C D

Then, I have also proven C

Then, I have also proven D

Example (Excluded Middle):

$\therefore A \vee \neg A$

I have a proof of A $\vee \neg$A.

More Inference Rules

Each connective has an "introduction rule" and an "elimination rule"

Consider "and". To know A ∧ B is true, what do we need to know…?

A	B	A ∧ B
T	**T**	**T**
T	F	F
T	T	F
T	F	F

The only case A ∧ B is true is when A and B are both true.

∧ Introduction

A   B

∴ A ∧ B

So, we can only prove A ∧ B if we already have a proof for A and we already have a proof for B.

More Inference Rules

Each connective has an "introduction rule" and an "elimination rule"

"Elimination" rules go the other way. If we know $A \wedge B$**, then what do we know about A and B individually?**

A	B	A ∧ B
T	**T**	**T**
T	F	F
T	T	F
T	F	F

When $A \wedge B$ **is true, then A is true and B is true.**

∧ Elimination

$$\frac{A \wedge B}{\therefore A \qquad B}$$

So, we if we can prove $A \wedge B$**, then we can also prove A and we can also prove B.**

Proofs

Show that r follows from $p, p \rightarrow q$, and $p \wedge q \rightarrow r$

How To Start:

We have givens, find the ones that go together and use them. Now, treat new things as givens, and repeat.

Modus Ponens

$$\frac{A \qquad A \rightarrow B}{\therefore \quad B}$$

∧ Introduction

$$\frac{A \qquad B}{\therefore \quad A \wedge B}$$

∧ Elimination

$$\frac{A \wedge B}{\therefore \quad A \qquad B}$$

Proofs

Show that r follows from $p, p \to q,$ and $p \land q \to r$

1.	p	Given
2.	$p \to q$	Given
3.	q	MP: 1, 2
4.	$p \land q$	Intro ∧: 1, 3
5.	$p \land q \to r$	Given
6.	r	MP: 4, 5

Two visuals of the same proof. We will focus on the top one, but if the bottom one helps you think about it, that’s great!

$$\dfrac{\dfrac{p \qquad \dfrac{p \qquad p \to q}{q}\,\text{MP}}{p \land q}\,\text{Intro } \land \qquad p \land q \to r}{r}\,\text{MP}$$

Simple Propositional Inference Rules

	Elimination	Introduction
$\wedge$	**$\wedge$ Elimination** $\dfrac{A \wedge B}{\therefore A \quad B}$	**$\wedge$ Introduction** $\dfrac{A \quad B}{\therefore A \wedge B}$
$\vee$	**$\vee$ Elimination** $\dfrac{A \vee B \quad \neg A}{\therefore B}$	**$\vee$ Introduction** $\dfrac{A}{\therefore A \vee B \quad B \vee A}$
$\rightarrow$	**Modus Ponens** $\dfrac{A \quad A \rightarrow B}{\therefore B}$	$\dfrac{p \Rightarrow q}{\therefore p \rightarrow q}$ Direct Proof Rule Not like other rules

Important: Application of Inference Rules

- You can use equivalences to make substitutions of any sub-formula.
- Inference rules only can be applied to whole formulas (not correct otherwise).

e.g. 1. $p \rightarrow q$ Given

~~2. $(p \vee r) \rightarrow q$ Intro $\vee$: 1~~

Does not follow! e.g . p=**F**, q=**F**, r=**T**

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

45. $\neg r$

Idea: Work backwards!

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

<u>Idea: Work backwards!</u>

We want to eventually get $\neg r$. How?

- We can use $q \rightarrow \neg r$ to get there.

45. $\neg r$

Proofs

Prove that ¬ r follows from p ∧ s, q → ¬ r, and ¬ s ∨ q.

Idea: Work backwards!

We want to eventually get ¬ r. How?

- We can use $q \rightarrow \neg r$ to get there.
- The justification between 44 and 45 looks like "implication elim" which is MP.

44.	$q \rightarrow \neg r$	Given
45.	$\neg r$	MP: 44, ?

- So, we can justify line 45 now!

Proofs

Prove that ¬r follows from p ∧ s, Used! and ¬s ∨ q.

Idea: Work backwards!

We want to eventually get ¬r. How?

- Now, we have a new "hole"
- We need to prove q…
  - Notice that at this point, if we prove q, we've proven $\neg r$…

43. q ?

44. $q \rightarrow \neg r$ Given

45. $\neg r$ MP: 44, 43

Proofs

Prove that ¬r follows from p ∧ s, Used! and ¬s ∨ q.

Idea: Work backwards!

We want to eventually get q. How?

- Find a relevant given!

42.	$\neg s \lor q$	**Given**
43.	q	?
44.	$q \rightarrow \neg r$	**Given**
45.	$\neg r$	**MP: 44, 43**

This looks like or-elimination.

Proofs

Prove that ¬r follows from p ∧ s, Used! and Used!

41. $\neg\neg s$ — It's more likely that $\neg\neg s$ shows up as s...
42. $\neg s \lor q$ — Given
43. q — $\lor$ Elim: 42, 41
44. $q \rightarrow \neg r$ — Given
45. $\neg r$ — MP: 44, 43

Proofs

Prove that $\neg r$ follows from $p \wedge s$, Used! and Used!

39. $p \wedge s$ Given

40. s Use our last given!

41. $\neg\neg s$ Double Negation: 40

Remember, we're allowed to use equivalences!

42. $\neg s \vee q$ Given

43. q $\vee$ Elim: 42, 41

44. $q \rightarrow \neg r$ Given

45. $\neg r$ MP: 44, 43

Proofs

Prove that $\neg r$ follows from Used! Used! and Used!

We don't have any holes in the proof left! We're done!

39.	$p \wedge s$	Given
40.	s	$\wedge$ Elim: 39
41.	$\neg\neg s$	Double Negation: 40
42.	$\neg s \vee q$	Given
43.	q	$\vee$ Elim: 42, 41
44.	$q \rightarrow \neg r$	Given
45.	$\neg r$	MP: 44, 43

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

Well, almost, let's renumber the steps:

1.	$p \land s$	Given
2.	s	∧ Elim: 1
3.	$\neg\neg s$	Double Negation: 2
4.	$\neg s \lor q$	Given
5.	q	∨ Elim: 4, 3
6.	$q \to \neg r$	Given
7.	$\neg r$	MP: 6, 5

To Prove An Implication: $A \rightarrow B$

- We use the direct proof rule
- The "pre-requisite" for using the direct proof rule is that we **write a proof** that **Given** A, we can prove B.
- The direct proof rule:

  If you have such a proof then you can conclude that $p \rightarrow q$ is true

Example: Prove $p \rightarrow (p \vee q)$.

proof subroutine

1.	p	Assumption
2.	$p \vee q$	Intro $\vee$: 1
3.	$p \rightarrow (p \vee q)$	Direct Proof Rule

Proofs using the direct proof rule

Show that $p \rightarrow r$ follows from q and $(p \land q) \rightarrow r$

1.	q	Given
2.	$(p \land q) \rightarrow r$	Given
3.1.	p	Assumption
3.2.	$p \land q$	Intro $\land$: 1, 3.1
3.3.	r	MP: 2, 3.2
3.	$p \rightarrow r$	Direct Proof Rule

This is a proof of $p \rightarrow r$

If we know p is true…
Then, we've shown r is true

Example

Prove: $(p \wedge q) \rightarrow (p \vee q)$

There MUST be an application of the Direct Proof Rule to prove this implication.

Where do we start? We have no givens...

Example

Prove: $(p \wedge q) \rightarrow (p \vee q)$

1.1.	$p \wedge q$	Assumption
1.2.	p	Elim $\wedge$: 1.1
1.3.	$p \vee q$	Intro $\vee$: 1.2
1.	$(p \wedge q) \rightarrow (p \vee q)$	Direct Proof Rule

Example

Prove: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

(1.1) $(p \rightarrow q) \wedge (q \rightarrow r)$ **Assumption**

(1.2) $p \rightarrow q$ **∧ Elim: 1.1**

(1.3) $q \rightarrow r$ **∧ Elim: 1.1**

(1.4.1) p **Assumption**

(1.4.2) q **MP: 1.2, 1.4.1**

(1.4.3) r **MP: 1.3, 1.4.2**

(1.4) $(p \rightarrow r)$ **Direct Proof Rule**

(1) $\big((p \rightarrow q) \wedge (q \rightarrow r)\big) \rightarrow (p \rightarrow r)$ **Direct Proof Rule**