Adam Blank — Spring 2016

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?

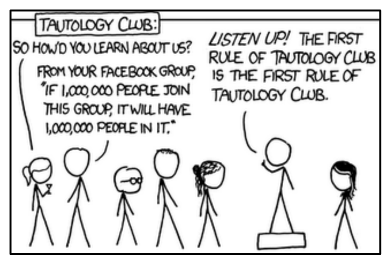
Proof From Last Time

Show that r follows from p, p → q, and q → r

1.	p	Given
2.	p → q	Given
3.	q → 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 ¬p follows from p → q and ¬q

1.	p → q	Given
2.	¬q	Given
3.	¬q → ¬p	Contrapositive: 1
4.	¬p	MP: 2, 3

Inference Rules

If I have a proof of A and I have a proof of B....

Requirements: A B

Conclusions: ∴ C D

Then, I have also proven C

Then, I have also proven D

Example (Modus Ponens):

A A → B

∴ 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: ∴ C D

Then, I have also proven C

Then, I have also proven D

Example (Excluded Middle):

∴ $A \vee \neg A$

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 $A \wedge B$ 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 $A \wedge B$ is true is when A and B are both true.

∧ Introduction

$A \quad B$

$\therefore A \wedge B$

So, we can only prove $A \wedge B$ 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

$A \wedge B$

$\therefore A \quad B$

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

$A \quad A \rightarrow B$

$\therefore B$

∧ Introduction

$A \quad B$

$\therefore A \wedge B$

∧ Elimination

$A \wedge B$

$\therefore A \quad B$

Proofs

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

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!

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

$$\dfrac{\dfrac{p \qquad \dfrac{p \quad p \rightarrow q}{q}\,\text{MP}}{p \wedge q}\,\text{Intro}\wedge \qquad p \wedge q \rightarrow r}{r}\,\text{MP}$$

Simple Propositional Inference Rules

Elimination / Introduction

∧

∧ Elimination

$A \wedge B$

$\therefore A \quad B$

∧ Introduction

$A \quad B$

$\therefore A \wedge B$

∨

∨ Elimination

$A \vee B \quad \neg A$

$\therefore B$

∨ Introduction

A

$\therefore A \vee B \quad B \vee A$

→

Modus Ponens

$A \quad A \rightarrow B$

$\therefore B$

$p \Rightarrow q$

$\therefore p \rightarrow q$

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. $p \to q$ Given

~~2. $(p \lor r) \to q$ Intro $\lor$: 1~~

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

Proofs

Prove that $\neg r$ follows from $p \land s$, $q \to \neg r$, and $\neg s \lor q$.

45. $\neg r$

Idea: Work backwards!

Proofs

Prove that $\neg r$ follows from $p \land s$, $q \to \neg r$, and $\neg s \lor q$.

Idea: Work backwards!

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

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

45. $\neg r$

Proofs

Prove that $\neg r$ follows from $p \land s$, $q \to \neg r$, and $\neg s \lor q$.

Idea: Work backwards!

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

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

44. $q \to \neg r$ Given

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

- So, we can justify line 45 now!

Proofs

Prove that $\neg r$ follows from $p \land s$, Used! and $\neg s \lor q$.

Idea: Work backwards!

We want to eventually get $\neg r$. 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. $q \to \neg r$ Given

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

Proofs

Prove that $\neg r$ follows from $p \land s$, Used! and $\neg s \lor q$.

Idea: Work backwards!

We want to eventually get q. How?

- Find a relevant given!

42. $\neg s \lor q$ Given

43. q ?

This looks like or-elimination.

44. $q \to \neg r$ Given

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

Proofs

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

41.	$\neg\neg s$	It's more likely that $\neg\neg s$ shows up as s...
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 $p \wedge s$, (Used!) and (Used!)

39.	$p \wedge s$	Given
40.	s	Use our last given!
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

Remember, we're allowed to use equivalences!

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

Well, almost, let's renumber the steps:

1.	$p \wedge s$	Given
2.	s	$\wedge$ Elim: 1
3.	$\neg\neg s$	Double Negation: 2
4.	$\neg s \vee q$	Given
5.	q	$\vee$ Elim: 4, 3
6.	$q \rightarrow \neg r$	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 $(p \wedge q) \rightarrow r$

1.	q	Given
2.	$(p \wedge q) \rightarrow r$	Given
3.1.	p	Assumption
3.2.	$p \wedge q$	Intro $\wedge$: 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: $(p \wedge q) \to (p \vee q)$

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

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

Example

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

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

Example

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

(1.1)	$(p \to q) \wedge (q \to r)$	Assumption
(1.2)	$p \to q$	$\wedge$ Elim: 1.1
(1.3)	$q \to r$	$\wedge$ 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)	$(p \to r)$	Direct Proof Rule
(1)	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Direct Proof Rule