Lecture 6: Other Proof Methods

CAB203 Discrete Structures

Matthew McKague

Queensland University of Technology

cab203@qut.edu.au

Outline

Direct Proofs

- What does a proof look like?
- What doesn't a proof look like?
- Things you might be asked to prove

Proof by Contradiction

- How it works
- Examples

Proof by Contrapositive

- How it works
- Examples

Other Proof Methods

- By Construction
- Counter Examples
- Other Tips

Readings

This week:

- Lawson: Chapter 2 relates to lectures 4,5,6

Next week: no readings.

Outline

Direct Proofs

- What does a proof look like?
- What doesn't a proof look like?
- Things you might be asked to prove

Proof by Contradiction

- How it works
- Examples

Proof by Contrapositive

- How it works
- Examples

Other Proof Methods

- By Construction
- Counter Examples
- Other Tips

Outline

- Direct Proofs
  - What does a proof look like?
  - What doesn't a proof look like?
  - Things you might be asked to prove
- Proof by Contradiction
  - How it works
  - Examples
- Proof by Contrapositive
  - How it works
  - Examples
- Other Proof Methods
  - By Construction
  - Counter Examples
  - Other Tips

Proof Structure

A proof should have a beginning, a middle, and an end AND (very important) the thing you're trying to prove should be at the end.

BEGINNING	Assume x and y
MIDDLE	Some steps that immediately follow the assumptions at the beginning. Maybe some algebraic manipulations, maybe just some worded statements. Maybe both.
END	Therefore we have proven by (insert proof method) that x and y implies z

Outline

Direct Proofs

- What does a proof look like?
- What doesn't a proof look like?
- Things you might be asked to prove

Proof by Contradiction

- How it works
- Examples

Proof by Contrapositive

- How it works
- Examples

Other Proof Methods

- By Construction
- Counter Examples
- Other Tips

Try to avoid any of these things.

- Beginning at the end and ending at the beginning
- Taking flying leaps
- Handwaving
- Incorrect logic
- Incorrect assumptions
- Incorrect use of definitions
- Too much assumption

Example of Bad Proof

Find what I shouldn't have done in the following proof!

Theorem 1

Suppose A and B are sets. If $P(A) \subseteq P(B)$, then $A \subseteq B$

Proof.

Assume $P(A) \subseteq P(B)$. To show $A \subseteq B$, suppose that $a \in A$.
Then $\{a\} \subseteq A$ so $\{a\} \in P(A)$.
It follows that $\{a\} \in P(B)$ because $P(A)$ and $P(B)$ are the same.
Therefore $\{a\} \subseteq B$ which means $a \in B$. This proves that $A \subseteq B$. □

Correct Version

Theorem 1
Suppose A and B are sets. If $P(A) \subseteq P(B)$, then $A \subseteq B$

Proof.
Assume $P(A) \subseteq P(B)$. Based on this assumption, we must show that $A \subseteq B$.
To show $A \subseteq B$, suppose that $a \in A$.
Then the one element set $\{a\}$ is a subset of A, so $\{a\} \in P(A)$.
But then, since $P(A) \subseteq P(B)$, it follows that $\{a\} \in P(B)$ because $P(A)$ and $P(B)$ are the same.
Therefore $\{a\} \subseteq B$ which means $a \in B$. This proves that $A \subseteq B$.
We've shown that $a \in A$ implies $a \in B$, so therefore $A \subseteq B$. $\square$

Direct Proofs

This previous example was an example of a direct proof. A direct proof starts at the beginning and follows straightforward steps to arrive at the end, without making any further assumptions.

Outline

Direct Proofs

- What does a proof look like?
- What doesn't a proof look like?
- Things you might be asked to prove

Proof by Contradiction

- How it works
- Examples

Proof by Contrapositive

- How it works
- Examples

Other Proof Methods

- By Construction
- Counter Examples
- Other Tips

There are many different types of statements you might be asked to prove. Here are a few *general* examples:

- $\forall x\, P(x)$ is **true**
- $\exists x\, P(x)$ is **true**
- $\exists! x\, P(x)$ is **true** (There exists a **unique** x)
- $\forall x\, P(x) \to Q(x)$
- $\exists x\, P(x) \to Q(x)$

And often these statements should each be approached in a different way.

Outline

Direct Proofs
- What does a proof look like?
- What doesn't a proof look like?
- Things you might be asked to prove

Proof by Contradiction
- How it works
- Examples

Proof by Contrapositive
- How it works
- Examples

Other Proof Methods
- By Construction
- Counter Examples
- Other Tips

Outline

- Direct Proofs
  - What does a proof look like?
  - What doesn't a proof look like?
  - Things you might be asked to prove
- Proof by Contradiction
  - How it works
  - Examples
- Proof by Contrapositive
  - How it works
  - Examples
- Other Proof Methods
  - By Construction
  - Counter Examples
  - Other Tips

How it works

- Given some statement (p)
- Assume the opposite is TRUE ($\neg p$)
- Follow the logic
- Contradiction (e.g $2 + 2 = 3$)
- Therefore, p is TRUE

"When you have eliminated the impossible, whatever remains, however improbable, must be the truth" - Sherlock Holmes, in the novel The Sign of the Four (1890) by Sir Arthur Conan Doyle

If $P \rightarrow Q$

- Assume p and $\neg q$ are BOTH true
- Follow the logic
- Contradiction
- Therefore, $p \rightarrow q$ must be TRUE

Logical underpinnings

We want to prove $A \vDash B$ by contradiction

- First show $A \wedge \neg B \vDash F$, i.e. assuming $\neg B$ gives a contradiction
- $A \wedge \neg B \vDash F$ means that $A \wedge \neg B \rightarrow F$ is a tautology
- By the truth table of $\rightarrow$ we see that $A \wedge \neg B \equiv F$
- Equivalently $\neg(A \wedge \neg B) \equiv T$
- Then $\neg A \vee B \equiv T$ by De Morgan's law and a double negation
- Using $P \rightarrow Q \equiv \neg P \vee Q$ find that $A \rightarrow B \equiv T$
- Thus $A \vDash B$.

Outline

- Direct Proofs
  - What does a proof look like?
  - What doesn't a proof look like?
  - Things you might be asked to prove
- Proof by Contradiction
  - How it works
  - Examples
- Proof by Contrapositive
  - How it works
  - Examples
- Other Proof Methods
  - By Construction
  - Counter Examples
  - Other Tips

Some Propositions

Proposition 1

There are no intergers x, y such that $x^2 = 4y + 2$.

Proposition 2

$\sqrt{2}$ is irrational

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Some Propositions

Proposition 1

There are no intergers x, y such that $x^2 = 4y + 2$.

Proposition 2

$\sqrt{2}$ is irrational

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proposition 1

Proposition 1

There are no intergers x, y such that $x^2 = 4y + 2$.

Proof.

Suppose integers x and y **do** exist such that $x^2 = 4y + 2$.

$$x^2 = 4y + 2 = 2(2y + 1)$$

Therefore x^2 is even. This means there exists a number $k \in \mathbb{Z}$ such that $x = 2k$. Subbing this in we have:

$$\begin{aligned} x^2 &= 2(2y+1) \\ (2k)^2 &= 2(2y+1) \\ 4k^2 &= 2(2y+1) && \text{(cancel the 2)} \\ 2k^2 &= 2y+1 \end{aligned}$$

Proposition 1 Cont.

Proposition 1

There are no intergers x, y such that $x^2 = 4y + 2$.

Proof. (cont.)
$2k^2$ is even, whereas $2y + 1$ is odd. These cannot be equal, therefore we have reach a contradiction and one of our earlier assumptions must be false.

□

Some Propositions

Proposition 1

There are no intergers x, y such that $x^2 = 4y + 2$.

Proposition 2

$\sqrt{2}$ is irrational

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proposition 2

Proposition 2

$\sqrt{2}$ is irrational

left as an exercise to the student (tutorial activity) - Solutions to be released at the end of the week

Some Propositions

Proposition 1

There are no intergers x, y such that $x^2 = 4y + 2$.

Proposition 2

$\sqrt{2}$ is irrational

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proposition 3

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proof (by contradiction)

- This is an IF THEN statement
- Therefore, assume the first premise is true and the seond false
- Try to arrive at a contradiction

Proposition 3

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proof.

Suppose that there exists some even a such that $a^2 - 2a + 7$ is even. If a is even, then there must exist some number, k, such that $a = 2k$. Sub in a.

$$\begin{aligned} a^2 - 2a + 7 &= (2k)^2 - 2(2k) + 7 \\ &= 4k^2 - 4k + 6 + 1 \\ &= 2(2k^2 - 2k + 3) + 1 \end{aligned}$$

$2(2k^2 - 2k + 3) + 1$ is odd. But we were told $a^2 - 2a + 7$ was even. It cannot be both, therefore we have a contradiction. $\square$

Outline

Direct Proofs
- What does a proof look like?
- What doesn't a proof look like?
- Things you might be asked to prove

Proof by Contradiction
- How it works
- Examples

Proof by Contrapositive
- How it works
- Examples

Other Proof Methods
- By Construction
- Counter Examples
- Other Tips

Outline

- Direct Proofs
  - What does a proof look like?
  - What doesn't a proof look like?
  - Things you might be asked to prove
- Proof by Contradiction
  - How it works
  - Examples
- Proof by Contrapositive
  - How it works
  - Examples
- Other Proof Methods
  - By Construction
  - Counter Examples
  - Other Tips

How it works

- Given some statement, $p \rightarrow q$
- Prove the contrapositive, $\neg q \rightarrow \neg p$
- Follow the logic
- Find that $\neg q \rightarrow \neg p$ is TRUE
- Therefore, $p \rightarrow q$ is TRUE

Truth Table

In propositional logic we derived the contraspositive logical equivalence

$$(p \to q) \equiv (\neg q \to \neg p)$$

Proof by truth table

p	q	$p \to q$	$\neg p$	$\neg q$	$\neg q \to \neg p$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

Outline

- Direct Proofs
  - What does a proof look like?
  - What doesn't a proof look like?
  - Things you might be asked to prove
- Proof by Contradiction
  - How it works
  - Examples
- Proof by Contrapositive
  - How it works
  - Examples
- Other Proof Methods
  - By Construction
  - Counter Examples
  - Other Tips

Some Propositions

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proposition 4

For any integers a and b, $a + b \geq 15$ implies that $a \geq 8$ or $b \geq 8$.

Proposition 5

If n is a positive integer such that $n \mod (4)$ is equal to 2 or 3, then n is not a perfect square.

Some Propositions

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proposition 4

For any integers a and b, $a + b \geq 15$ implies that $a \geq 8$ or $b \geq 8$.

Proposition 5

If n is a positive integer such that $n \mod (4)$ is equal to 2 or 3, then n is not a perfect square.

Proposition 3 (again!)

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proof.

The contrapositive statement is "If a is not odd, then $a^2 - 2a + 7$ is not even". This means if we assume a is even, we should be able to show that $a^2 - 2a + 7$ is odd.
If a is even, then there must exist some number $k \in \mathbb{Z}$ such that $a = 2k$.

$$a^2 - 2a + 7 = (2k)^2 + 2(2k) + 7 = 4k^2 + 4k + 6 + 1 = 2(2k^2 + 2k + 3) + 1$$

Which is odd. We have shown that the contrapositive is true, therefore, the original statement must be true.

□

Some Propositions

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proposition 4

For any integers a and b, $a + b \geq 15$ implies that $a \geq 8$ or $b \geq 8$.

Proposition 5

If n is a positive integer such that $n \mod (4)$ is equal to 2 or 3, then n is not a perfect square.

Proposition 4

For any integers a and b, $a + b \geq 15$ implies that $a \geq 8$ or $b \geq 8$.

Left as an exercise to the student (tutorial activity) - Solutions to be released at the end of the week

Some Propositions

Proposition 3

Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proposition 4

For any integers a and b, $a + b \geq 15$ implies that $a \geq 8$ or $b \geq 8$.

Proposition 5

If n is a positive integer such that $n \mod (4)$ is equal to 2 or 3, then n is not a perfect square.

Proposition 5

Proposition 5

If n is a positive integer such that $n \mod (4)$ is equal to 2 or 3, then n is not a perfect square.

Proof.

The contrapositive of this statement is "If n **is** a perfect square, then $n \mod (4)$ must be a 0 or a 1", since 0 and 1 are the only other options $\mod (4)$. Based on this, let's suppose there exists some number $k \in \mathbb{Z}$ such that $n = k^2$. k can be equal to $0, 1, 2, \text{or } 3 \mod (4)$ so we have 4 cases to consider.

1. If $k \mod (4) = 0$, then $k = 4q$ for some $q \in \mathbb{Z}$.
   Then $n = k^2 = (4q)^2 = 16q^2 = 4(4q^2)$ i.e. $n \mod (4) = 0$
2. If $k \mod (4) = 1$, then $k = 4q + 1$ for some $q \in \mathbb{Z}$.
   Then $n = k^2 = (4q + 1)^2 = 16q^2 + 8q + 1 = 4(4q^2 + 2q) + 1$
   i.e. $n \mod (4) = 1$

Proposition 5

Proposition 5

If n is a positive integer such that $n \mod (4)$ is equal to 2 or 3, then n is not a perfect square.

Proof. (cont.)

3. If $k \mod (4) = 2$, then $k = 4q + 2$ for some $q \in \mathbb{Z}$.
   Then $n = k^2 = (4q+2)^2 = 16q^2 + 16q + 4 = 4(4q^2 + 4q + 1)$
   i.e. $n \mod (4) = 0$
4. If $k \mod (4) = 3$, then $k = 4q + 3$ for some $q \in \mathbb{Z}$.
   Then
   $n = k^2 = (4q+3)^2 = 16q^2 + 24q + 9 = 4(4q^2 + 6q + 2) + 1$
   i.e. $n \mod (4) = 1$

All cases show that if n is a perfect square, then $n \mod (4)$ is 0 or 1. The contrapositive is true, therefore the original statement is also true.

□

Outline

Direct Proofs
- What does a proof look like?
- What doesn't a proof look like?
- Things you might be asked to prove

Proof by Contradiction
- How it works
- Examples

Proof by Contrapositive
- How it works
- Examples

Other Proof Methods
- By Construction
- Counter Examples
- Other Tips

Proof Methods

Proof methods you are now familiar with:

- Proof by truth table
- Direct Proof
- Proof by Contradiction
- Proof by Contrapositive

Other proof methods:

- Proof by counterexample
- Proof by construction

Outline

- Direct Proofs
  - What does a proof look like?
  - What doesn't a proof look like?
  - Things you might be asked to prove
- Proof by Contradiction
  - How it works
  - Examples
- Proof by Contrapositive
  - How it works
  - Examples
- Other Proof Methods
  - By Construction
  - Counter Examples
  - Other Tips

Proof by Construction

- Typically used to prove existence statements
- State the claim
- Describe an algorithm that constructs the thing you want
- Prove that the algoithm is correct

Example

Theorem

If a and b are real numbers ($\in \mathbb{R}$) and $a \neq 0$, then there exists a unique r such that $ar + b = 0$.

This proof must be done in two steps. The first step is to show that such a number *exists*, and the second is to show that the number is *unique*.

Proof.

To prove existance we start with the original equation, and try to construct r.

$$\begin{aligned} ar + b &= 0 \\ ar &= -b \\ r &= \frac{-b}{a},\ a \neq 0 \end{aligned}$$

Example

Theorem

If a and b are real numbers ($\in \mathbb{R}$) and $a \neq 0$, then there exists a unique r such that $ar + b = 0$.

Proof. (cont.)

To prove uniqueness, we use proof by contradiction. Suppose that there exists some other value, $s \in \mathbb{R}$ such that $as + b = 0$.

Then

$$ar + b = as + b$$

$$ar = as$$

$$r = s$$

In order for s and r to both exist, they must be the same number, hence r is unique.

□

Outline

- Direct Proofs
  - What does a proof look like?
  - What doesn't a proof look like?
  - Things you might be asked to prove
- Proof by Contradiction
  - How it works
  - Examples
- Proof by Contrapositive
  - How it works
  - Examples
- Other Proof Methods
  - By Construction
  - Counter Examples
  - Other Tips

Counter Examples

- Not a proof method per se. Used to show that a "for all" statement is false.
- Find a single example where the statement is false
- Can use construction and other proof methods
- Eg. Show $\forall x \in \mathbb{Z}^+ y \in \mathbb{Z}\ y^2 = x \rightarrow y \geq 0$. We can use $x = 1, y = -1$ as a counter example because $(-1)^2 = 1$ but $-1 < 0$.

Outline

- Direct Proofs
  - What does a proof look like?
  - What doesn't a proof look like?
  - Things you might be asked to prove
- Proof by Contradiction
  - How it works
  - Examples
- Proof by Contrapositive
  - How it works
  - Examples
- Other Proof Methods
  - By Construction
  - Counter Examples
  - Other Tips

Other Tips

- WRITE STUFF DOWN
- Start by attempting a direct proof
- If you can't figure out where to start, try contradiction
- Some proofs have multiple cases
- Sometimes it's easier to start at the conclusion and work backwards. Make sure that the logic still works backwards, and reverse to get the proof in the correct order when you write it up. Useful for algebraic manipulation.