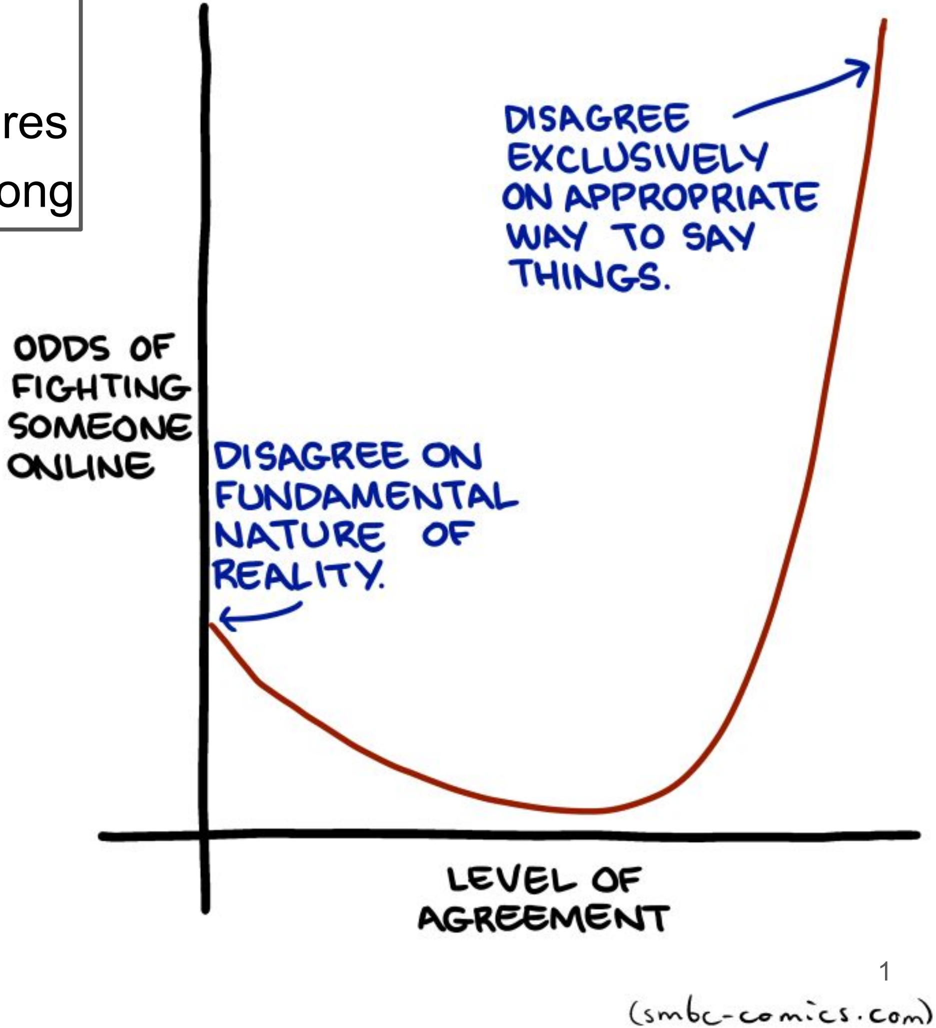
University of Colorado **Boulder**

CSCI 2824: Discrete Structures

Fall 2018 Tony Wong

Lecture 10: Introduction to Proofs



Announcements and reminders

- **Flu shots** -- GET THEM.
  - You owe it to the people around you not to give us the flu.
  - https://www.colorado.edu/healthcenter/flu

- **Voting** --DO IT.
  - You owe it to yourself.
  - https://www.colorado.edu/registrar/students/registration/mycuinfo/register-vote

- HW 3 (Moodle) due Friday at 12 PM Noon

What did we do last time?

- Rules of inference, and using them to construct
- **valid** arguments. (good arguments)
- **sound** arguments (great arguments)
- Recognizing **fallacious** arguments (awful arguments)

Today:

We will start to learn about:

1. Proofs and arguing!
2. Lots and lots of proof examples and strategies.

Intro to proofs

Most of the things we want to prove in math and computational science is of the form $p \rightarrow q$

Example: The Goldbach conjecture:

Every even number greater than 2 can be written as the sum of two prime numbers.

We can rewrite this in the propositional form we have been using:

Intro to proofs

Most of the things we want to prove in math and computational science is of the form $p \rightarrow q$

Example: The Goldbach conjecture:

Every even number greater than 2 can be written as the sum of two prime numbers.

We can rewrite this in the propositional form we have been using:

⇒ $\forall x\,(E(x) \rightarrow P(x))$ where the domain of discourse is the positive integers > 2,
$E(x)$ = x is even, and
$P(x)$ = x can be written as the sum of two primes

⇒ Even though most mathematical propositions aren't stated using this universal quantifier lingo, they have this flavor.

Intro to proofs

So how do we prove a statement of the form $\forall x\,(P(x) \rightarrow Q(x))$?

1. Prove $P(c) \rightarrow Q(c)$ for any **arbitrary** c.
2. Conclude $\forall x\,(P(x) \rightarrow Q(x))$ by **universal generalization**.

We usually do this, but we often do not verbalize Step 2.

There are three main ways that we prove $P(c) \rightarrow Q(c)$

1) Direct proof
2) Contrapositive proof
3) Proof by contradiction

Direct proofs

Direct proof: We want to prove $p \rightarrow q$ is true.

- We only need to show that when p is true, q must be true as well.

Direct proof strategy:

- Assume p is true,
- proceed through a series of rules of inference and mathematical facts (like the stuff we did last time),
- and eventually end up with q being true as well.

Outline for Direct Proof

Proposition If P, then Q.

Proof. Suppose P.

$\vdots$

Therefore Q. ■

Direct proofs

Direct proof: We want to prove $p \to q$ is true.

- We only need to show that when p is true, q must be true as well.

Direct proof strategy:

- Assume p is true,
- proceed through a series of rules of inference and mathematical facts (like the stuff we did last time),
- and eventually end up with q being true as well.

Outline for Direct Proof

Proposition If P, then Q.

Proof. Suppose P.

$\vdots$

Therefore Q. $\blacksquare$

Definition: An integer n is **even** if it can be written as $n = 2k$ for some integer k. And integer n is **odd** if it can be written as $n = 2k + 1$ for some integer k. We call the evenness/oddness of n its **parity**.

Direct proofs

Example: If n is an odd integer, then n^2 is also odd.

Direct proofs

Example: If n is an odd integer, then n^2 is also odd.

Proof:

1. Assume an integer n is odd.
   - n can be written as $n = 2a + 1$ for some integer a
2. Then $n^2 = (2a + 1)^2$
   $= 4a^2 + 4a + 1$
   $= 2(2a^2 + 2a) + 1$
   $= 2m + 1$, where $m = 2a^2 + 2a$ is some integer as well
3. Since $n^2 = 2m + 1$ for some integer m, we know n^2 must be odd.

This concludes the proof. We typically announce this by writing "*QED*" or a little box: $\square$

Direct proofs

Example: If a divides b, and b divides c, then a divides c.

Concept check: "a divides b" means that we can write b as $b = ak$ for some integer k (so b is a multiple of a)

Direct proofs

Example: If a divides b, and b divides c, then a divides c.

Concept check: "a divides b" means that we can write b as $b = ak$ for some integer k (so b is a multiple of a)

Proof:

1. Assume a divides b and b divides c.
2. Then $b = ak$ and $c = bm$ for some integers k and m.
3. Plug $b = ak$ into the c equation:

$$c = (ak)m = a(km)$$

4. (km) is an integer, so a divides c

□

Direct proofs

More examples:

FYOG: If n is an odd integer then n can be written as the difference of two perfect squares.

FYOG: If n is a four-digit palindrome, then n is divisible by 11.

FYOG: Let n be a three digit number where all three digits are the same digit chosen from 1-9, then if you divide n by the sum of the three digits, you get 37.

Contrapositive proof

Contrapositive proof: Say we want to prove $p \rightarrow q$

- Doing this directly might be hard!
- So take the contrapositive: $\neg q \rightarrow \neg p$
- … and then try to do a direct proof on the contrapositive instead!

Contrapositive proof strategy: Assume $\neg q$ is true, then show that this leads us to $\neg p$ being true as well.

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

$\vdots$

Therefore $\sim P$. $\blacksquare$

Contrapositive proof

Example: If n^2 is an even integer, then n is even.

Contrapositive proof

Example: If n^2 is an even integer, then n is even.

Equivalent contrapositive: If n is odd, then n^2 is odd.

Contrapositive proof

Example: If n^2 is an even integer, then n is even.

Equivalent contrapositive: If n is odd, then n^2 is odd.

Proof:

1. Assume an integer n is odd.
   a. n can be written as $n = 2a + 1$ for some integer a
2. Then $n^2 = (2a + 1)^2$
   $= 4a^2 + 4a + 1$
   $= 2(2a^2 + 2a) + 1$
   $= 2m + 1$, where $m = 2a^2 + 2a$ is some integer as well
3. Since $n^2 = 2m + 1$ for some integer m, we know n^2 must be odd.

$\square$ we've proven the contrapositive, thus we've proven the original

Contrapositive proof

Example: If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Contrapositive proof

Example: If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Equivalent contrapositive: If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $n \neq ab$.

Contrapositive proof

Example: If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Equivalent contrapositive: If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $n \neq ab$.

Proof:

1. Assume that $a > \sqrt{n}$ and $b > \sqrt{n}$
2. Then $ab > \sqrt{n}\ \sqrt{n} = n$
3. Since $ab > n$ it must be the case that $ab \neq n$

Thus, we've proven the contrapositive statement.

Therefore, the original statement is proven as well.

□

Contrapositive proof

Use a contrapositive proof to show…

FYOG: If $x^2(y + 3)$ is even, then x is even or y is odd.

FYOG: If $x + y$ is even, then x and y have the same parity.

Proof by contradiction

Proof by contradiction: Say we want to prove that $p \rightarrow q$

- We assume p is true and $\neg q$ is also true.
- Then show that this leads to a **logical contradiction**

$\rightarrow$ i.e., that r and $\neg r$ must both be true for some proposition r

Outline for Proof by Contradiction

Proposition P.

Proof. Suppose $\sim P$.

$\vdots$

Therefore $C \wedge \sim C$. ■

An example is probably the simplest way to get a feel for how this works.

Proof by contradiction

Example: Prove that if $3n + 2$ is odd, then n is odd.

Proof by contradiction

Example: Prove that if $3n + 2$ is odd, then n is odd.

Proof: (by contradiction)

1. Assume (for the sake of contradiction) that $3n + 2$ is odd, but n is even.
2. n even means that $n = 2a$ for some integer a
3. Then $3n + 2 = 3(2a) + 2 = 2(3a + 1)$, which must be even
4. But $3n + 2$ being even contradicts our initial assumption that n is even
5. Thus if $3n + 2$ is odd, then n is odd

$\square$

Question: What is the argument form for proof by contradiction, as a compound proposition?

Proof by contradiction

So why does this work?

- We wanted to prove $p \to q$
- The argument form that we just used looked like this: $((p \land \neg q) \to \mathbf{F}) \to (p \to q)$
- Let's have a look at whether this is valid using a truth table:

p	q				
T	T				
T	F				
F	T				
F	F				

Proof by contradiction

So why does this work?

- We wanted to prove $p \to q$
- The argument form that we just used looked like this: $((p \land \neg q) \to \mathbf{F}) \to (p \to q)$
- Let's have a look at whether this is valid using a truth table:

p	q	$\neg q$	$p \land \neg q$	$(p \land \neg q) \to \mathbf{F}$	$p \to q$	$((p \land \neg q) \to \mathbf{F}) \to (p \to q)$
T	T	F	F	T	T	T
T	F	T	T	F	F	T
F	T	F	F	T	T	T
F	F	T	F	T	T	T

The argument is a **tautology**, so it is **valid**.

Proof by contradiction

Example: Prove that $\sqrt{2}$ is irrational.

By the way: A rational number *n* is a number that can be written as a fraction of two integers, *n* = *a/b*, where *b* ≠ 0 and *a* and *b* have no common factors. A number that is not rational is irrational. (π and *e* are other examples of irrational numbers)

Proof by contradiction

Example: Prove that $\sqrt{2}$ is irrational.

Proof (by contradiction):

Proof by contradiction

Example: Prove that $\sqrt{2}$ is irrational.

Proof (by contradiction):

1. Assume (FSOC) that $\sqrt{2}$ is rational.
2. $\Rightarrow$ $\sqrt{2}$ = a/b, where a and b are integers, $b \neq 0$, and they have no common factors
3. $\Rightarrow$ square both sides to find $2 = a^2/b^2$
4. $\Rightarrow$ $2b^2 = a^2$, which means a^2 is even, so a is also even
5. $\Rightarrow$ $\exists c$ such that (s.t.) $a = 2c$
6. $\Rightarrow$ $2b^2 = a^2 = 4c^2$
7. $\Rightarrow$ $b^2 = 2c^2$, which means b^2 and b must both be even
8. $\Rightarrow$ Oh no! a and b are both even, which means they share a common factor: 2
9. $\rightarrow\leftarrow$ (we often use colliding arrows to denote a contradiction)
10. Thus, our initial assumption was false, and $\sqrt{2}$ must be irrational

$\square$

Proof by contradiction

Use proof by contradiction to show…

FYOG: There are no positive integer solution to $x^2 - y^2 = 10$.

FYOG: There are an infinite number of prime numbers. (This one is tricky so look in the book if you need to. But it is an important problem.)

Proving biconditional statements

Remember that $p \Leftrightarrow q$ (p if and only if q) is logically equivalent to $(p \rightarrow q) \land (q \rightarrow p)$

So to successfully prove the biconditional, we must prove the conditional in **both directions**.

Strategy:

1. Prove $p \rightarrow q$ using any of your handy dandy proof techniques
2. Prove $q \rightarrow p$ as well
3. Conclude that $p \Leftrightarrow q$

Proving biconditional statements

Example: Prove that an integer n is even if and only if $3n + 5$ is odd.

Proving biconditional statements

Example: Prove that an integer n is even if and only if $3n + 5$ is odd.

Solution:

We need to prove both directions:

- ($\Rightarrow$) If n is even then $3n + 5$ is odd
- ($\Leftarrow$) If $3n + 5$ is odd then n is even

Proof:

($\Rightarrow$) Direct proof

Proving biconditional statements

Example: Prove that an integer n is even if and only if $3n + 5$ is odd.

Solution:

We need to prove both directions:

- (⇒) If n is even then $3n + 5$ is odd
- (⇐) If $3n + 5$ is odd then n is even

Proof:

(⇒) Direct proof

1. S'pose n is even. Then $n = 2a$, where a is some integer
2. Then $3n + 5 = 3(2a) + 5 = 6a + 5 = 6a + 4 + 1 = 2(3a + 2) + 1$, which is odd.
3. Thus, if n is even, then $3n + 5$ is odd. ✔

Proving biconditional statements

Example: Prove that an integer n is even if and only if $3n + 5$ is odd.

Solution:

We need to prove both directions:

- ($\Rightarrow$) If n is even then $3n + 5$ is odd
- ($\Leftarrow$) If $3n + 5$ is odd then n is even

Proof:

($\Leftarrow$) by contraposition ("If n is odd, then $3n + 5$ is even")

Proving biconditional statements

Example: Prove that an integer n is even if and only if $3n + 5$ is odd.

Solution:

We need to prove both directions:

- ($\Rightarrow$) If n is even then $3n + 5$ is odd
- ($\Leftarrow$) If $3n + 5$ is odd then n is even

Proof:

($\Leftarrow$) by contraposition ("If n is odd, then $3n + 5$ is even")

1. S'pose n is odd. Then $n = 2a + 1$, where a is some integer
2. Then $3n + 5 = 3(2a + 1) + 5 = 6a + 3 + 5 = 6a + 8 = 2(3a + 4)$, which is even.
3. Thus, if n is odd, then $3n + 5$ is even…
4. Which prove the contrapositive statement, that if $3n + 5$ is odd, then n is even. ✔

We've proved both directions, therefore we have proved the biconditional $\square$

Proving biconditional statements

FYOG: Prove this biconditional statement by proving both directions (using the techniques we learned today):

An integer n is even if and only if $3n + 6$ is even.

Intro to proofs

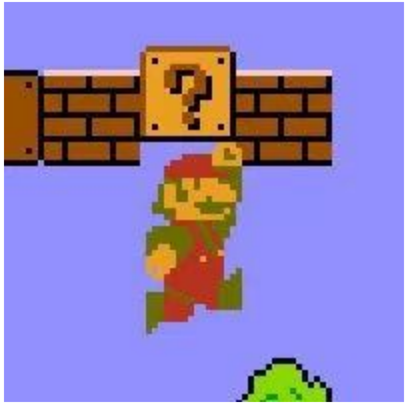
Recap:

- Today, we learned about and saw some examples using:
    - Direct proof
    - Contrapositive proof
    - Proof by contradiction

Next time:

- How do we prove that something exists? (or does not exist?)
- How do we prove that something that does exist is **unique**?
- How can we **exhaustively** prove something?
- What are common mistakes/missteps/blunders in proving stuff?

Bonus material!



Warm-up problem

Example: Translate and show the argument is valid. (Domain = all creatures)

All monsters are not nice

There is a monster who has a pet cat

Consequently, some mean creatures have cats

Warm-up problem

Example: Translate and show the argument is valid. (Domain = all creatures)

All monsters are not nice

There is a monster who has a pet cat

Consequently, some mean creatures have cats

Solution:

- Let $M(x)$ mean "x is a monster", $N(x)$ mean "x is nice" and $C(x)$ mean "x has a pet cat".

$$\forall x\, (M(x) \rightarrow \neg N(x))$$

$$\exists x\, (M(x) \land C(x))$$

$$\therefore\ \exists x\, (\neg N(x) \land C(x))$$

Warm-up problem

	Step	Justification
1.	$\forall x\,(M(x) \rightarrow \neg N(x))$	premise
2.	$\exists x\,(M(x) \land C(x))$	premise
	$\therefore\ \exists x\,(\neg N(x) \land C(x))$	

Warm-up problem

	Step	Justification
1.	$\forall x\,(M(x) \to \neg N(x))$	premise
2.	$\exists x\,(M(x) \land C(x))$	premise
3.	$M(a) \land C(a)$	existential instantiation (2) (for *some a*)
4.	$M(a)$	simplification (3)
5.	$M(a) \to \neg N(a)$	universal instantiation (1)
6.	$\neg N(a)$	modus ponens (4), (5)
7.	$C(a)$	simplification (3)
8.	$\neg N(a) \land C(a)$	conjunction (6), (7)
9.	$\therefore\ \exists x\,(\neg N(x) \land C(x))$	existential generalization (8)