COSC 290 Discrete Structures

Lecture 10: Proofs by contradiction and cases

Prof. Michael Hay

Wednesday, Feb. 14, 2018

Colgate University

Plan for today

1. Proof by contradiction
2. Examples of proof by contradiction
3. Proof by contradiction vs. proof by contrapositive
4. Proof by cases

Logistics

- First midterm exam: 1 week from this Friday!
- Lab 1: continue to work on it this week

Proof by contradiction

Proof by contradiction

To prove that proposition φ is true,

you can assume φ is false (i.e, $\neg\varphi$ is true) and show that this assumption leads to a contradiction.

Procedure for proof by contradiction

Goal: prove that φ is true.

Process:

1. Negate the proposition, resulting in $\neg\varphi$.
   (*Note: you typically want to* ***simplify*** *this expression, pushing the negation down.*)

Procedure for proof by contradiction

Goal: prove that φ is true.

Process:

1. Negate the proposition, resulting in $\neg\varphi$.
   (*Note: you typically want to* ***simplify*** *this expression, pushing the negation down.*)
2. Assume $\neg\varphi$ is true.

Procedure for proof by contradiction

Goal: prove that φ is true.

Process:

1. Negate the proposition, resulting in $\neg\varphi$.
   (*Note: you typically want to* ***simplify*** *this expression, pushing the negation down.*)
2. Assume $\neg\varphi$ is true.
3. Show that this leads to a contradiction, i.e.,

Procedure for proof by contradiction

Goal: prove that φ is true.

Process:

1. Negate the proposition, resulting in $\neg\varphi$.
   (*Note: you typically want to* ***simplify*** *this expression, pushing the negation down.*)
2. Assume $\neg\varphi$ is true.
3. Show that this leads to a contradiction, i.e., leads to two statements that are opposed to one another.

Why does this work?

A little more formally, proof by contradiction works like this.

- Assume $\neg\varphi$
- Find some proposition ψ such that you can show...
- $\neg\varphi \implies \psi$, and
- $\neg\varphi \implies \neg\psi$.
- But $\psi \wedge \neg\psi \equiv$ *False*!

In other words, we have shown $\neg\varphi \implies$ *False*. So what?

Truth table for contradiction

Claim:

$$(\neg p \implies False) \equiv p$$

Proof:

Truth table for contradiction

Claim:

$$(\neg p \implies \mathit{False}) \equiv p$$

Proof: Recall that $p \implies q \equiv \neg p \vee q$.

Truth table for contradiction

Claim:

$$(\neg p \implies \mathit{False}) \equiv p$$

Proof: Recall that $p \implies q \equiv \neg p \vee q$.

p	q	$p \implies q$	$\neg p \vee q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Thus,

$$(\neg p \implies \mathit{False}) \equiv (\neg\neg p \vee \mathit{False}) \equiv (p \vee \mathit{False}) \equiv p$$

Proof by Contradiction Template

- **Claim**: *Write the theorem/claim to be proved, "φ is true."*
- **Proof by contradiction**: Assume the claim is false. In other words, *[state negated form of φ]*
  It's critical that you (a) explicitly state this is a proof by a contradiction and (b) state the assumption that will lead to the contradiction! Why?

Proof by Contradiction Template

- **Claim**: *Write the theorem/claim to be proved, "φ is true."*
- **Proof by contradiction**: Assume the claim is false. In other words, *[state negated form of φ]*
    - *Write main body of proof...*
    - *... establish some ψ must be true.*
    - *... establish some $\neg\psi$ must also be true.*
    - But *[state ψ and $\neg\psi$]* is a contradiction. Be sure to clearly identify the contradiction!

Proof by Contradiction Template

- **Claim**: *Write the theorem/claim to be proved, "φ is true."*
- **Proof by contradiction**: Assume the claim is false. In other words, *[state negated form of φ]*
    - *Write main body of proof...*
    - *... establish some ψ must be true.*
    - *... establish some $\neg\psi$ must also be true.*
    - But *[state ψ and $\neg\psi$]* is a contradiction. Be sure to clearly identify the contradiction!
    - **Conclusion**: Therefore the original assumption that *[restate $\neg\varphi$]* is false, and we can conclude that *[restate φ]* is true.

Examples of proof by contradiction

Poll: no integer is both even and odd

- **Claim**: There is no integer that is both even and odd.
- **Proof by contradiction**: Assume the claim is false. In other words, ... what goes here?

A) All integers are both odd and even.

B) All integers are not odd or not even.

C) There is an integer n that is both odd and even.

D) There is an integer n that is neither odd nor even.

E) None of above / More than one of above

Exercise: complete the proof

- **Claim**: There is no integer that is both even and odd.
- **Proof by contradiction**: Assume the claim is false. In other words, suppose there exists an integer n that is both even and odd.
- Work in small groups to find a contradiction!
- Useful tools:
  - $\mathbb{Z}$ is the set of all integers
  - $\mathit{Even}(x) :\equiv \exists k \in \mathbb{Z} : x = 2k$
  - $\mathit{Odd}(x) :\equiv \exists \ell \in \mathbb{Z} : x = 2\ell + 1$
  - Sum/Difference of two integers is an integer.
  - Algebra, logic.

Complete proof

- **Claim**: There is no integer that is both even and odd.
- **Proof by contradiction**: Assume the claim is false. In other words, suppose there exists an integer n that is both even and odd.
  Since n is odd, $\exists \ell \in \mathbb{Z} : n = 2\ell + 1$.
  Since n is even, $\exists k \in \mathbb{Z} : n = 2k$.
  Since k and ℓ are integers, $k - \ell$ is an integer.
  However, some algebra shows that,

  $$2\ell + 1 = 2k1 \qquad = 2(k - \ell)\frac{1}{2} = (k - \ell)$$

  and thus $(k - \ell)$ is non-integral. This is a contradiction!
  This means the assumption that n is both even and odd is false and therefore, we can conclude there is no integer that is both even and odd.

Rational numbers

Recall: a rational number is a real number that can be expressed as the ratio of two integers.

$$Rational(y) := \exists n \in \mathbb{Z} : \exists d \in \mathbb{Z}^{\neq 0} : y = n/d$$

Rational numbers

Recall: a rational number is a real number that can be expressed as the ratio of two integers.

$$Rational(y) := \exists n \in \mathbb{Z} : \exists d \in \mathbb{Z}^{\neq 0} : y = n/d$$

We will consider the following claim: if x^2 is irrational, then x is irrational.

Poll: from English to predicate logic

Consider the claim,

"If x^2 is irrational, then x is irrational."

Formulate this claim in predicate logic:

A) $\exists x \in \mathbb{R} : \neg Rational(x^2) \land \neg Rational(x)$

B) $\exists x \in \mathbb{R} : \neg Rational(x^2) \implies \neg Rational(x)$

C) $\forall x \in \mathbb{R} : \neg Rational(x^2) \land \neg Rational(x)$

D) $\forall x \in \mathbb{R} : \neg Rational(x^2) \implies \neg Rational(x)$

E) None of above / More than one of above

Poll: irrational squares

- **Claim**:

$$\forall x \in \mathbb{R} : \neg Rational(x^2) \implies \neg Rational(x)$$

(If x^2 is irrational, then x is irrational.)

- **Proof by contradiction**: Assume the claim is false. In other words, … what goes here? be careful with negation!

A) There exists x where both x and x^2 are rational.

B) There exists x where both x and x^2 are irrational.

C) There exists x where x is rational and x^2 is irrational.

D) There exists x where x is irrational and x^2 is rational.

E) None of above / More than one of above

Exercise: complete the proof

- **Claim**: If x^2 is irrational, then x is irrational.
- **Proof by contradiction**: Assume the claim is false. In other words, suppose there exists an x such that x is rational but x^2 is irrational.
- Work in small groups to find a contradiction!
- Useful tools:
  - $\mathbb{R}$ is the set of all real numbers
  - $\mathbb{Z}$ is the set of all integers
  - $\mathit{Rational}(y) :\equiv \exists n \in \mathbb{Z} : \exists d \in \mathbb{Z}^{\neq 0} : y = n/d$
  - Product of two integers is an integer.
  - Algebra, logic.

Proof by contradiction vs. proof by contrapositive

Contradiction vs. contrapositive

- **Claim**: If x^2 is irrational, then x is irrational.
- **Proof by contradiction**: Assume the claim is false. In other words, suppose there exists an x such that x is rational but x^2 is irrational. We will show this leads to a contradiction...
- **Proof by contrapositive**: Assume that x is rational. We will show that x^2 is rational.

Contradiction vs. contrapositive

- Contradiction can be used for *any* proposition φ. Contrapositive only applies to φ of the form $p \implies q$.

Contradiction vs. contrapositive

- Contradiction can be used for *any* proposition φ. Contrapositive only applies to φ of the form $p \implies q$.
- How do they compare when $\varphi \coloneqq p \implies q$?

Contradiction vs. contrapositive

- Contradiction can be used for *any* proposition φ. Contrapositive only applies to φ of the form $p \implies q$.
- How do they compare when $\varphi := p \implies q$?
- Contrapositive: given $\neg q$, show $\neg p$.
- Contradiction: ??
  Let's look at $\neg(p \implies q)$ on the board.

Contradiction vs. contrapositive

- Contradiction can be used for *any* proposition φ. Contrapositive only applies to φ of the form $p \implies q$.
- How do they compare when $\varphi \coloneqq p \implies q$?
- Contrapositive: given $\neg q$, show $\neg p$.
- Contradiction: given $\neg(p \implies q) \equiv \neg q \wedge p$, show *some* contradiction (any contradiction you can think of!).
  For example, you could assume $\neg q \wedge p$ and show the contrapositive (i.e. $\neg q \implies \neg p$) and then you have a contradiction $p \wedge \neg p$.

When to use proof by contradiction?

There isn't an easy answer.[1]

Try other techniques first.

Situations where I've found it useful...

- proving a "negative": $\sqrt{2}$ is irrational (i.e., *not* rational).
- proving that a particular algorithm always computes the "best" solution

[1] https://gowers.wordpress.com/2010/03/28/when-is-proof-by-contradiction-necessary/

Proof by cases

Example

Claim: among any 6 people, there are 3 who all know each other (a club) or 3 who don't know each other (strangers).

This proof assume any two people either know each other or not (A knows B iff B knows A).

We will use the strategy of proof by cases.

Proof by cases

Claim: among any 6 people, there are 3 who all know each other (a club) or 3 who don't know each other (strangers).

Proof: The proof is by cases. Let x denote one of the 6 people. There are two cases:

1. x knows at least 3 of the other 5 people
2. x knows at most 2 of the other 5 people

Some quick asides:

- Notice it says "there are two cases"
- You'd better be right there are no more cases!
- Cases must completely cover possibilities
- Cases *could* overlap, but generally don't.
- Tip: you don't need to worry about trying to make the cases "equal size" or scope.

Proof continued...

Claim: among any 6 people, there are 3 who all know each other (a club) or 3 who don't know each other (strangers).

Case 1, x knows at least 3 people, can be split into two sub cases.

1.1 Among the the ones that x knows, no pair knows each other. Then we have at least 3 strangers.

1.2 Among the the ones that x knows, there is one pair that knows each other. They both also know x, so a club.

Some quick asides:

- Again, notice it says "there are two subcases"
- Cases must completely cover possibilities *within this case*

Proof continued...

Claim: among any 6 people, there are 3 who all know each other (a club) or 3 who don't know each other (strangers).

Case 2, x knows at most 2 people, can be split into two sub cases.

2.1 Among the the ones that x does *not* know, they all know each other. There are at least 3, so we have a club.

2.2 Among the the ones that x does *not* know, there exists a pair that does not know each other. Then, together with x, we have 3 strangers.