CSCI 2200

Foundations of Computer Science

Lecture 4: Proof Techniques

CSCI 2200

Foundations of Computer Science

Lecture 4: Proof Techniques

“Mute City” by Yumiko Kanki (from *F-Zero*)

Announcements & reminders

- Dr. DiTursi's office hours for this week and next week:
  - Tuesday 9:30 – 12:00 and Friday 12:00 – 14:30
- TA Eric's office hours for the rest of the semester:
  - Thursday 12:00 – 14:00
- HW1 due tonight before 9pm. HW2 posted after class today.
- No class on Monday; Monday is also the add/drop deadline.

- Exam 1 is in less than two weeks. (Wed. 1/29)

Plan for today

Proving a quantified statement

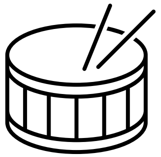
Proving & disproving implications

Proving “if and only if”

Indirect proofs (proofs by contradiction)

Proofs about sets

But first, a word from our ~~sponsor~~ textbook author…

- A proof is a mathematical essay.
- The goal of a proof is to convince a reader of a theorem.
- A proof that leaves a reader with some doubts has failed.
- Therefore, a proof must be well written, so that the reader can follow the chain of reasoning.
  - Among other things, that means you should… *proofread!* 

Which of these are hard/easy to prove?

- $\forall x \, P(x)$
- $\exists x \, P(x)$
- $\neg \forall x \, P(x)$
- $\neg \exists x \, P(x)$

Which of these are hard/easy to prove?

- $\forall x\, P(x)$
  - Hard! Can try "proof by exhaustion" on finite sets.
- $\exists x\, P(x)$
  - Relatively easy – just find an example
- $\neg\forall x\, P(x)$
  - Relatively easy – just find a counterexample
- $\neg\exists x\, P(x)$
  - Hard!

Concrete examples

- Prove: $\forall n > 2$, if n is an even integer, n can be written as the sum of two prime numbers.
    - 4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 3 + 7, …
    - But we can't actually list all of them!

- Prove: $\exists (a, b, c) \in \mathbb{N}^3, a^2 + b^2 = c^2$
    - Select a = 3, b = 4, c = 5. 9 + 16 = 25. Done!

A few number theory facts

Divisibility and remainders

- What does “n is divisible by 3” mean?
  - $n = 3k$, for some integer k (yes, this includes zero)
- “n is odd” means $n = 2k + 1$
  - “n mod 4 = 3” means $n = 4k + 3$
- “n is composite” means $n = pq$, for integers $p,q > 1$
  “n is prime” means $n > 1$ and not composite
- $n \in \mathbb{Q}$ means $n = p / q$, for integers $p,q \neq 0$

Reasoning about implications

Many (most?) of the statements we will want to prove will be universally quantified implications, e.g. "$\forall n \in \mathbb{N}$, if n is even, then n^2 is even."

We know that $p \rightarrow q$ can only be falsified when p is true and q is false. This suggests a few approaches to proving that such a statement is always true:

- Direct proof: <u>Assume</u> p is true. Show q <u>must</u> also now be true.
- Proving the contrapositive: <u>Assume</u> q is false. Show p <u>must</u> also now be false.
- Indirect proof: <u>Assume</u> p is true <u>and</u> q is false. Show that this leads to an impossible situation.

Direct proofs

Direct proof – steps

1. Clearly state your claim. (“If p, then q.”)
2. Assume the antecedent. (“Assume p is true.”)
3. Use known mathematical facts to create a chain of true statements that ends at the consequence. (“Because p, we know …, which then means that …, which in turn implies … q!”)
4. State that you have proven the claim. (“Therefore, we have proven that p implies q.”)
5. Use an end-of-proof marker. (“QED” or ∎)

Direct proof – example #1

Claim: $y, z \in \mathbb{Q} \Rightarrow (y + z) \in \mathbb{Q}$

State the claim you wish to prove. (p ⇒ q)

Proof: Assume $y \in \mathbb{Q}$ and $z \in \mathbb{Q}$

Assume p.

This means $y = \frac{a}{b}$ and $z = \frac{c}{d}$ for some integers a, b, c, d $(b, d \neq 0)$.

Use the definition of rational number.

Thus, $y + z = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad+bc}{bd}$

Often, algebra required.

Direct proof – example #1

$y + z = \frac{ad+bc}{bd}$

We take as an axiom that integers are *closed* under addition and multiplication.

"Axiom" is often code for "this is obvious and I don't want to prove it."

Therefore, ad, bc, bd and $ad + bc \in \mathbb{Z}$.

Moving back towards the definition of rational.

Since $(ad + bc)$ and bd are both integers, this means $y + z$ is rational. ∎

Direct proof – example #2

Claim: $\forall x \in \mathbb{R}$, If $4^x - 1$ is divisible by 3, then $4^{x+1} - 1$ is also divisible by 3.

State the claim you wish to prove. ($p \Rightarrow q$)

Proof: Assume $4^x - 1$ is divisible by 3.

Assume p.

Then $4^x - 1 = 3k$, for some $k \in \mathbb{N}$.

Use the definition of "divisible by 3".

Next, multiply by 4: $4^{x+1} - 4 = 12k$

How do we get to 4^{x+1}?

Now add 3: $4^{x+1} - 1 = 12k + 3$

Continue the process of making it look like q.

Direct proof – example #2

$4^{x+1} - 1 = 12k + 3$

Factor a 3 out of the right side:
$4^{x+1} - 1 = 3(4k + 1)$

Since $4k+1$ is an integer[citation needed], this shows that $4^{x+1} - 1$ is divisible by 3, which is what we were trying to show.

Since we placed no restrictions on x, this proves the claim for any x. ■

Remember, we need to show divisibility by 3.

Use the definition of “divisible by 3” again.

This is a key idea: we said nothing about x as part of proof, so it could have been anything!

Your turn!

Claim: If a and b are even, then $a+b$ is even.

Your turn!

Claim: If a and b are even, then $a+b$ is even.

- **Proof:** Assume a and b are even.
- Then $a = 2j$ and $b = 2k$, where j & k are integers.
- $a + b = 2j + 2k = 2(j + k)$
- Since $(j + k)$ is also an integer, $(a + b)$ also meets the definition of even. ■

Proof by contraposition

Proving the contrapositive – steps

1. Clearly state your claim. ("If p, then q.")
2. Assume the consequence is false. ("Assume $\neg q$.")
3. Use known mathematical facts to create a chain of true statements that ends at the opposite of the antecedent. ("… therefore p must be false.")
4. State that you have proven the claim. ("Since we have shown $\neg q \Rightarrow \neg p$, we have proven that p implies q.")
5. Use an end-of-proof marker. ("QED" or ■)

Contrapositive proof – example

Claim: $\forall n > 2 \in \mathbb{N}$, 2^n – n is prime ⇒ n is odd.

State the claim you wish to prove. (p ⇒ q)

Proof: Assume n is even.

Assume ¬q.

This means n = 2k, for some $k > 1$

Definition of even

Thus, $2^n - n = 2^{2k} - 2k = 2(2^{2k-1} - k)$

Work towards the other side of the implication

Contrapositive proof – example

$2^n - n = 2(2^{2k-1} - k)$

For $k > 1 \in \mathbb{N}$, $2^{2k-1} - k$ is always an integer greater than one.

Move towards the definition of "not prime"

So $2^n - n$ is the product of two integers greater than or equal to two, and thus composite

Definition of composite

Since when n is even then $2^n - n$ must be composite, this proves the original claim. ■

Contrapositive and implication are equivalent

Your turn!

Claim: If n^2 is not divisible by 4, then n is odd.

Your turn!

Claim: If n^2 is not divisible by 4, then n is odd.

- Assume n is even.
- Then $n = 2k$, where $k \in \mathbb{Z}$.
- n^2 is thus $(2k)^2$, or $4k^2$.
- Since k^2 is an integer, this means $4k^2$, and thus n^2, is divisible by 4.
- Since the only times n is <u>not</u> odd are when n^2 <u>is</u> divisible by 4, the claim is proven by contraposition. ■

Disproving an implication

- Since most implications are (at least implicitly) "for all" statements, all you need is a <u>single</u> counterexample to disprove them.
- Claim: $\forall n \in \mathbb{Z}, \frac{n}{n+1} \notin \mathbb{Z}$
  - Try -2! $\frac{-2}{-2+1} = 2 \in \mathbb{Z}$.
  - The claim is disproven.

Logical equivalence – “if and only if”

- Written several different ways:
  - $p \Leftrightarrow q$
  - p if and only if q
  - p iff q
- They all mean the same thing:
  - $p \Rightarrow q \land q \Rightarrow p$
- To prove an “if and only if”, you must prove both implications.

Proof by contradiction (indirect proof)

Indirect proof (“reductio ad absurdum”)

1. Clearly state your claim.
2. Assume the <u>claim</u> is false! (Frequently, this gives you TWO assumptions to work with: p and $\neg q$.)
3. Use known mathematical facts to create a chain of true statements that produces <u>two opposite statements</u> ($s \wedge \neg s$) - a contradiction!
4. State that you have proven the claim. (“Since assuming our claim was false produces a contradiction, it must instead be true.”)
5. Use an end-of-proof marker. (“QED” or ∎)

The infinitude of the primes

- From Euclid’s *Elements*, Book IX, Proposition 20:
  - “Prime numbers are more than any assigned multitude of prime numbers.”
  - This is more commonly stated these days as “There are an infinite number of prime numbers.”

A classic proof by contradiction

- **Claim:** There are an infinite number of prime numbers.
- **Proof:** Assume, for contradiction, that the set of primes is instead finite. Let $n = |P|$, the number of primes.
- Then it is possible to make a list of <u>all</u> of the primes in ascending order: $\{p_1, p_2, \ldots, p_n\}$
  - *Side note:* This is not actually a trivial fact. It depends upon a property of $\mathbb{N}$ called the Well-Ordered Principle. We'll discuss this idea more next class when we talk about induction. For now, we can take it as an axiom.

A classic proof by contradiction

- Now that we have the list $\{p_1, p_2, \dots, p_n\}$, consider the number $q = 1 + p_1 \cdot p_2 \cdot \cdots \cdot p_n$. (That is, multiply all of the primes together and then add 1 to the result.)
  - Most proofs have one critical point where some spark of creativity is required – one crucial insight that makes the rest of the proof work. This is that key idea for this proof.
- The Fundamental Theorem of Arithmetic says that every integer greater than 1 is either prime itself or can be written as the product of primes.
  - "Proof by cases" is often something we try to avoid. It is <u>only OK</u> when the cases cover <u>every</u> possible situation.

A classic proof by contradiction

- Case 1: q is prime. In that case, we observe that $q > p_n$ (why?), and since p_n is the largest prime in our list, then q is a prime that is not in our list.
- Case 2: q is the product of primes. Let p' be one of them. Then $q = p'k$, where p' is prime and $k \in \mathbb{N}$.
- Next, observe that q cannot be divisible by p_i for any p_i in our list of primes, because q is a multiple of p_i plus 1. Therefore p' is a prime that is not in our list.
- But our list contained every prime number…


Objection!

A classic proof by contradiction

- Our list contained every prime number, but then we found one that wasn't in the list! This is a *CONTRADICTION*.
- Unless we have made an error in reasoning (which can be pretty easy to do!), the only way we can arrive at a contradiction is if we have made a bad assumption.
- The only assumption in our reasoning was the initial one: that the number of primes is finite.
- Therefore, that assumption must be false, and we have proven that there are an infinite number of primes. ■

Proofs about sets

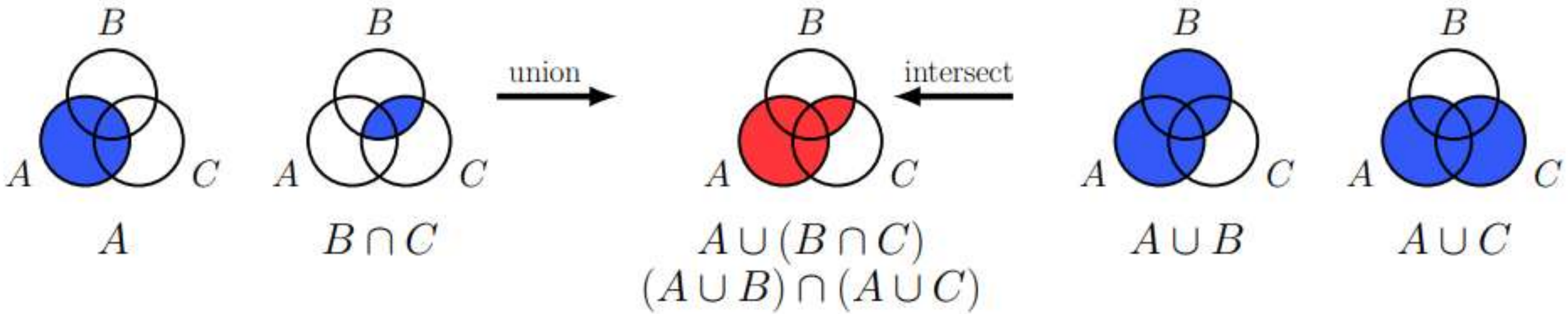
Set relations & formal proofs

- Proofs about sets usually involve one of our set relations: $A \subseteq B, A \subset B, A = B$ or their negations.
- To complete a formal proof relating to these, you'll want to fall back on the definitions.

In order to prove:	You must show:
$A \subseteq B$	$\forall x : x \in A \Rightarrow x \in B$
$A \nsubseteq B$	$\exists x : x \in A \wedge x \notin B$
$A \subset B$	$A \subseteq B \wedge B \nsubseteq A$
$A = B$	$A \subseteq B \wedge B \subseteq A$

“Proof by picture”

- A Venn diagram can be really helpful in conveying what’s going on, especially when more than two sets are involved.
- Prove: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$



- If a formal proof is not required, sometimes such a diagram is sufficient. But if a formal proof is needed, you’ll have to fall back on the previous table.

Wrapping up

- How do you decide what type of proof to use? Here are some suggestions for where to start. (No promises!)

Situation / claim	Suggested proof method
$p \Rightarrow q$; can easily go from p to q	Direct proof
$p \Rightarrow q$; can easily go from $\neg q$ to $\neg p$	Contraposition
$\exists x : P(x)$ - "there exists"	Just find an example!
$\neg\exists x : P(x)$ - "there does not exist"	Indirect proof (contradiction)
$\exists x : \left(P(x) \wedge \nexists y : \left(x \neq y \wedge P(y)\right)\right)$; unique x	Indirect proof (contradiction)
$\forall x : P(x)$ – "for all x"	"Choose" an arbitrary x
$\neg\forall x : P(x)$ – "it is not the case for all x"	Just find a counterexample!

Class survey

- Reminders: HW 1 due tonight
- No office hours this afternoon (moved to Friday afternoon)
- HW 2 posted later today