CS 70 Su23: Lecture 2

Proofs

Berkeley
UNIVERSITY OF CALIFORNIA

Clarifications

- element of: $\in$
  - read: “in (the set)”
  - can denote membership of any set (A, B, S, whatever)
    - the fancy letters denote “common” sets:
      - $\mathbb{N}$ is the natural numbers (for this class, this includes 0!)
      - $\mathbb{Z}$ is the integers
  - (example) $\forall x \in \mathbb{N}$: “for all x in $\mathbb{N}$”, “for all natural numbers
- clarification on grade distribution
  - refer to the ed post

Refresher: implication

Implication

- **P ⇒ Q** ("P implies Q", "if P, then Q")
- What does it mean for an implication to be true (or false)?
  - if **P** is true, **Q** is definitely true
  - if **P** is false, **P ⇒ Q** is (vacuously) true
    - this is different from **Q** being true!
  - if you can find an example where **P** is true and **Q** is false, you know that **P ⇒ Q** is false
- **transitive:** if **P ⇒ Q** and **Q ⇒ R**, then **P ⇒ R**
  - why?

P	**Q**	**P ⇒ Q**
T	T	**T**
T	F	F
F	T	**T**
F	F	**T**

Claim: implication is transitive

Let **P**, **Q**, and **R** be propositions. *Suppose* **P ⇒ Q** and **Q ⇒ R**. We *want to show* **P ⇒ R**.

Suppose **P**.

- note this shorthand for “P is true”
  - this is analogous to shortening `if my_boolean == True:` to `if my_boolean:`

Because **P ⇒ Q**, we know **Q** is true.

Because **Q ⇒ R** (and **Q**), we know **R** is true.

Because **P** is true and **R** is true, **P ⇒ R** is true.

Therefore, (P ⇒ Q) ∧ (Q ⇒ R) ⇒ (P ⇒ R). *QED*

Berkeley
UNIVERSITY OF CALIFORNIA

What just happened?

This is an example of a **proof**:

- a series of statements, each *implied* by the previous statement
- an incredibly powerful application of implication
- can give you logical certainty about statements (without having to fully enumerate a truth table)

Some terminology

Like with programs, proofs have syntax and structure:

- Start by "defining your variables" (list what you know)
  - "Let", "Suppose", "Pick", "Assume", "Consider"
- Declare your "return type" (what you want to show)
  - "Want to show", "Claim", "Theorem"
- Iterate line by line to "execute" (series of logical implications)
- Conclude
  - "Therefore", "∴"
  - "QED", "//", "✓", "□"

For today, these "keywords" will be *italicized*

We have to start from somewhere

It turns out that we can't prove everything

- If we show **P ⇒ Q**, we don't actually know anything about **P**
  - for example, if someone later discovers $1 + 1 \neq 2$, a lot of math will break as a result
- Things we assume (with no proof) are called **definitions** or **axioms**
- You can think of these as import statements: they just work
  - just like in 61A, we will let you know when you can "import" what

Proof types

Direct proof

- Structured as follows:
  - *Want to show* **P ⇒ Q**
  - *Suppose* **P**
  - ???
  - ~~Profit~~ *Therefore,* **Q**
  - *Q.E.D.*
- You'll "modus ponens" in some textbooks
  - not exactly the same as "direct proof", but close enough

We just did one of these, but let's do another with numbers

Berkeley
UNIVERSITY OF CALIFORNIA

Direct proof

Theorem: $\forall x \in \mathbb{N}, \exists y \in \mathbb{N}$ *st* $y > x$.

Without loss of generality, let **n** be a natural number.

- because we make no assumptions about **n**, our argument will hold for *any* $n \in \mathbb{N}$

Because addition is closed under $\mathbb{N}$, we know $\mathbf{n + 1 \in \mathbb{N}}$.

Therefore, there exists a natural number larger than **n**, and we are done. ✓

Proof by cases

Like a direct proof, but exhaustively enumerates all possible inputs

- like a switch statement or a giant if/elif/else block, there are times where this is correct, but it should not be your default instinct

Let’s revisit our transitivity claim from earlier, but with the truth table:

Berkeley
UNIVERSITY OF CALIFORNIA

P	Q	R	P ⇒ Q	Q ⇒ R	(P ⇒ Q) ∧ (Q ⇒ R)	P ⇒ R	[(P ⇒ Q) ∧ (Q ⇒ R)] ⇒ (P ⇒ R)
T	T	T	T	T	T	T	**T**
T	T	F	T	F	F	F	**T**
T	F	T	F	T	F	T	**T**
T	F	F	F	T	F	F	**T**
F	T	T	T	T	T	T	**T**
F	T	F	T	F	F	T	**T**
F	F	T	T	T	T	T	**T**
F	F	F	T	T	T	T	**T**

Proof by cases

Theorem: there exist irrational numbers x and y such that x^y is rational.

Let $x = \sqrt{2}$ and $y = \sqrt{2}$.

Consider $x^y = \sqrt{2}^{\sqrt{2}}$.

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational.

- Crushed it. ✓

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$
- $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$, which is rational. ✓

- We don't actually know (or care!) what x and y end up being
  - similarly, we don't know (or care) if $\sqrt{2}^{\sqrt{2}}$ is rational or irrational
- This is a **non-constructive** proof

Berkeley
UNIVERSITY OF CALIFORNIA

Proof by contraposition

Still a direct proof, but on the **contrapositive** of the original claim

- Structured as follows:
  - *Want to show* **P ⇒ Q**
  - *Suppose* ¬**Q**
  - ???
  - ~~Profit~~ *Therefore,* **¬P**
  - *Q.E.D.*
- You'll "modus tollens" in some textbooks
  - not exactly the same as "proof by contraposition", but close enough

Berkeley
UNIVERSITY OF CALIFORNIA

Proof by contraposition

Theorem: $\forall\ a, b \in \mathbb{Z},\ a + b \geq 15 \Rightarrow a \geq 8 \lor b \geq 8$.

Consider the contrapositive: $\forall\ a, b \in \mathbb{Z},\ (a < 8 \land b < 8) \Rightarrow (a + b < 15)$. We will prove the theorem with a proof by contraposition.

- Like any good anime, you must announce your move before performing it

Let $a, b \in \mathbb{Z}$. *Suppose* $a < 8$ and $b < 8$.

Because *a* and *b* are both integers, we know $a \leq 7$ and $b \leq 7$.

Thus, $a + b \leq 14$.

Therefore, $a + b < 15$. //

Berkeley
UNIVERSITY OF CALIFORNIA

Proof by contradiction

The weirdest one, but (personally) the most satisfying one

- Structured as follows:
  - *Want to show* **P**
  - *Assume* **¬P**
  - ???
  - **R ⇒ ¬R** (for some proposition **R**)
  - →←
  - ~~Profit~~ *Therefore,* **P**
  - *Q.E.D.*

Proof by contradiction

Why does this work?

- We end up showing **¬P ⇒ false** (the contradiction)
- This implication is true, so what does that say about **P**?
  - **¬P** cannot be true (else the implication would be false)
- Alternatively, look at the contrapositive: **true ⇒ P**
  - **P** cannot be false (else the implication would be false)

Thus, **P** must be true

Berkeley
UNIVERSITY OF CALIFORNIA

Proof by contradiction

Theorem: there are an infinite number of prime numbers.

Proof by contradiction. Assume there are a finite number of primes.

- Denote them as $p_1, p_2, \ldots, p_n$, where n is the total number of primes

Let $q = p_1 \times p_2 \times \ldots \times p_n + 1$ ($q \in \mathbb{N}$). Because q is not in our set of prime numbers, q is not prime.

However, q has no prime divisors (by construction, its remainder when divided by any prime is 1).

Thus, q is prime. →←

Therefore, there are an infinite number of primes. □

Proof by contradiction: a warning

Be careful about takeaways from contradiction proofs!

- Does this mean that the product of the first n primes + 1 is prime?
  - 2 + 1 = 3, 2 x 3 + 1 = 7, 2 x 3 x 5 + 1 = 31… maybe we're onto something!
  - but 2 x 3 x 5 x 7 x 11 x 13 + 1 = 30031, which is divisible by 59
- That construction only holds if our original assumption is true
  - But that assumption (there are a finite number of primes) isn't true

Proof?

Theorem: -2 = 2.

Suppose -2 = 2. Squaring both sides, we see that 4 = 4, and we are done.

What did we actually show?

- **P ⇒ true** (a valid claim, but not what we wanted to show)

Proof?

Theorem: 1 = 2.

We will prove a stronger claim. *Let* $x = y$, for some $x, y \in \mathbb{Z}$. *Claim:* $x = x + y$.

With some algebra, we see that $x^2 - xy = x^2 - y^2$.

Factoring, we have $x(x - y) = (x + y)(x - y)$.

Dividing both sides by $(x - y)$ yields $x = x + y$. //

- Dividing by 0 is an invalid step

Common mistakes

- Assuming what you want to show
    - $P \Rightarrow P$ is always true
- Making a false assumption
    - This breaks the chain of implications
    - You may still arrive at the correct conclusion, but the steps will not necessarily be correct
- Trying proof by cases when there are too many cases
    - You want this when there are a small number of cases (even/odd, rational/irrational, etc)
    - It’s tempting to try proof by cases with true/false as the cases
        - This usually winds up going in circles

When to use which proof

It depends

- One is not more “valid” than the others, but may be easier to use
- The problems you’ll see in class often have an “intended” proof method
  - but that doesn’t mean a different method is worse
- If you find yourself having a hard time with one method, try a different one to see if that gives you a flash of insight

Aside: to **disprove** something, it is often sufficient to provide a **counter-example** (that is, an example where **P** is true, but **Q** is false)

- Other times, a disproof is just a proof of the negation

Berkeley
UNIVERSITY OF CALIFORNIA

Alternate proof technique: pigeonhole principle

Claim: Let **n** and **k** be positive integers. Place **n** objects into **k** boxes. If **n** > **k**, then at least one box must contain multiple objects.

Proof by contradiction.

Assume we place **n** objects into **k** boxes (and **n** > **k**) such that no box contains multiple objects.

This means the total number of objects, **n**, must be ≤ **k** (each box has at most one object).

However, there are **n** > **k** objects. →←

Therefore, if **n** > **k**, then at least one box must contain multiple objects.

Advice for writing proofs

- Constantly ask yourself, “why is this true?”
  - be your own annoying 4-year-old cousin/sibling
- Think of writing a proof like writing code
  - Your proof needs to “compile”
    - No undefined variables
    - Statements must connect from one to another (no skipping steps)
    - Return statement must match return type declaration
  - Proofs can have good and bad style/organization
    - The better your proofs are organized/styled, the easier they will be to read/understand (and grade)
- Iterate through multiple drafts
  - The whiteboard is your friend
- If you’re stuck, your TA will always ask some variation of:
  - What are you trying to show?
  - What do you know?

Next class: induction

A proof technique that gets its own lecture