Lecture 2: Proofs

No, not the alcohol kind

Introduction to Proofs

What are proofs?

- Sequence of logical deductions
- Deduce new claims from already known
- Mix of English and mathematical notation

Why proofs?

- Formal way to determine if something is true (or false by proving the negation)
  - Informal methods can be misleading!
- Collect thoughts into a crisp, clear argument
- Convince others that something is true

Today: general proof techniques + examples

Direct Proof

Many theorems take the form $P \implies Q$

- eg, "n is even $\implies n^2$ is even"

Direct proofs do exactly what you would expect: suppose P is true[1] and deduce that Q is also true.

[1] if P is not true, the implication holds vacuously!

Direct Proof Example

Theorem: If $a|b$ ("a divides b") and $a|c$, $a|(b+c)$

Proof:

- Suppose $a|b$ and $a|c$
- $b = aq_1$ and $c = aq_2$ for some $q_1, q_2 \in \mathbb{Z}$
- Hence $b + c = aq_1 + aq_2 = a(q_1 + q_2)$
- Since $q_1 + q_2 \in \mathbb{Z}$, $a|(b+c)$

Proof does not specify what values a, b, and c take on — proves the statement for all a, b, and c!

Similar method to show $a|(b-c)$[2]

[2] In fact, $a|(xb + yc)$ for all integers x and y!

Direct Proof Example 2

Theorem: Let n be a 3-digit natural number. n is divisible by 9 if and only if the sum of its digits is.

Let $n = 100a + 10b + c$

Proof(if):

- Suppose $9|(a+b+c)$, so $a + b + c = 9k$
- Then $n = 100a + 10b + c = 9k + 99a + 9b$
- Hence $n = 9(k + 11a + b)$, so $9|n$

Proof(only if):

- Suppose $9|n$, so $n = 100a + 10b + c = 9j$
- Then $a + b + c = 9j - 99a - 9b$
- Hence $a + b + c = 9(j - 11a - b)$ so $9|(a+b+c)$

Proof by Contraposition

Recall: $P \implies Q \equiv (\neg Q) \implies (\neg P)$

Proving the contrapositive may be easier!

- $\neg Q$ might give more information than P
- $\neg P$ might be easier to get to than Q

Proof by contraposition is just a direct proof of the contrapositive.

Proof by Contraposition Example

Theorem: Let $n \in \mathbb{N}$. If n^2 is even, n is even.

Try proving it directly:

- Since n^2 is even, $n^2 = 2k$ for some integer k
- Then $n = \sqrt{2k}$, so ...

Issue: not enough information to get anywhere :(

Try contrapositive instead: if n is odd, n^2 is odd

- Suppose n is odd, so $n = 2k + 1$
- Then $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
- Thus n^2 is odd

Proof by Contraposition Example 2

Theorem: Let $x \in \mathbb{R}$. If $x \leq y$ for all $y > 0$, $x \leq 0$.

Direct proof? O no...

Contrapositive: if $x > 0$, $\exists y > 0$ such that $x > y$

- Take $y = \frac{x}{2}$
- Since $x > 0$, $x > \frac{x}{2} > 0$

Sometimes called a "proof by example" (or a "proof by counterexample" for disproving a "for all")

Proof by Contraposition Example 3

Theorem: Suppose we place n items into k boxes. If $n > k$, at least one box has more than one item.[3]

Direct proof possible, but messy.

Contrapositive: If all boxes have ≤ 1 item, $n \leq k$.

- Let n_i be the number of items in box i
- Suppose that $n_i \leq 1$ for all i
- Then $n = n_1 + ... + n_k \leq 1 + ... + 1 = k$

[3] This is called the pigeonhole principle

Proof by Contradiction

Idea: show that P being false is nonsensical

Formally: show that $\neg P$ implies something false[4]

Why does this work?

Contrapositive of $(\neg P) \implies$ False is True $\implies P$

Intuition: $(\neg P) \implies$ False, so $\neg P$ can't be true.
But if $\neg P$ is false, P is true by definition!

[4] This is known as "reductio ad absurdum" if you want to sound fancy.

Contradiction Example

Theorem: There are infinitely many primes.

How to construct infinitely many primes? idk...
No implication for contraposition either

Contradiction proof:

- Suppose only finitely many: $p_1, p_2, ..., p_k$
- Consider $q := (p_1 \cdot p_2 \cdot ... \cdot p_k) + 1$
- q can't be a multiple of p_1, or p_2, or ..., or p_k
- So q has no prime factors
- Next time: every number has a prime factor
- Contradiction! Must be infinitely many primes

Contradiction Example 2

Theorem: $\sqrt{2}$ is irrational.

Generally difficult to prove negative results directly
Again, no implication to use in contraposition

Contradiction proof:

- Suppose $\sqrt{2}$ is rational
- Write it in lowest terms as $\frac{a}{b}$
- Since $\frac{a}{b} = \sqrt{2}$, $a^2 = 2b^2$
- a^2 even, so $a = 2k$
- Hence $b^2 = 2k^2$, so b^2 and b even
- a and b both even, so $\frac{a}{b}$ not in lowest terms!
- Contradiction! $\sqrt{2}$ must be irrational

Break Time!

Whew, time for a 4 minute break.

Today's discussion question:
Which is the one true kind of peanut butter: chunky or smooth?

Proof by Cases

Idea: one of these cases happens, but which one? Prove the claim in each case.

Why does this work?
Consider two cases C_1 and C_2. If $C_1 \implies P$ and $C_2 \implies P$, then $(C_1 \vee C_2) \implies P$!

Proof by Cases Example

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

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

- Immediately done: take $x = y = \sqrt{2}$

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

- Take $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$
- Then $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$

But which case?
Doesn't matter, but is case 2.

Proof by Cases Example 2

Theorem: Let $x, y \in \mathbb{R}$. Then $|x + y| \leq |x| + |y|$.[5]

Case 1: $x \geq 0$, $y \geq 0$

- $x + y > 0$, so $|x + y| = x + y = |x| + |y|$

Case 2: $x \geq 0$, $y < 0$

- If $|x| \geq |y|$, $|x + y| = |x| - |y| \leq |x| + |y|$
- Else $|x + y| = |y| - |x| \leq |y| + |x| = |x| + |y|$

Case 3: $x < 0$, $y \geq 0$

- Switch x and y to get case 2!

Case 4: $x < 0$, $y < 0$

- Negate x and y to get case 1!

[5] This is known as the *triangle inequality*.

Error 404: Proof Not Found

Be careful when writing proofs! Very easy to miss small errors that break everything :(

Consider the following "proof":
Claim: $-2 = 2$
"Proof":

- Suppose $-2 = 2$
- Square both sides to get $4 = 4$
- This is true, so we must have that $-2 = 2$

Tried to use $P \implies$ True to conclude P.
But this implication holds even if P is false![6]

[6] In fact, if you start with a false assumption, you can prove anything. This is known as the *Principle of Explosion*.

Other Common Errors

Claim: $1 = 2$
"Proof":

- Let x and y be integers such that $x = y$
- Then $x^2 - xy = x^2 - y^2$
- Divide by $x - y$ to get $x = x + y$
- Take $x = y = 1$ to get $1 = 2$

Issue: $x = y$, so $x - y = 0$. Divided by zero!

Claim: $4 \leq 1$
"Proof":

- We know that $-2 \leq 1$
- Square both sides to get $4 \leq 1$

Issue: squaring multiplied by -2 — flips inequality!

Tips for Proofs

Proof-writing is a skill, and can be difficult. Here are some tips on how to write your own:

- Use full English sentences for clarity.
  - Proofs should be clear enough to convince a skeptical classmate
- Use lemmas to break up a long proof.
- Develop your style through practice.
- Read other's proofs to see their style.

Fin

Next time: induction!