Writing Convincing Arguments

I have a number $x \in \mathbb{R}$. For any positive $y > 0$, it holds that $x \leq y$. Is it true that $x \leq 0$?

Can you convince a classmate? *Can you prove it?*

A *proof* is a finite list of logical deductions which establishes the truth of a statement.

Today: We will learn strategies for writing valid proofs.

Counterintuitive Mathematics

Why are proofs necessary?

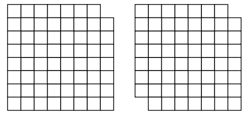
These are known as the *Borwein integrals*:

$$\int_0^\infty \frac{\sin x}{x}\,\mathrm{d}x = \frac{\pi}{2},$$
$$\int_0^\infty \frac{\sin x}{x}\frac{\sin(x/3)}{x/3}\,\mathrm{d}x = \frac{\pi}{2},$$
$$\vdots$$
$$\int_0^\infty \frac{\sin x}{x}\frac{\sin(x/3)}{x/3}\cdots\frac{\sin(x/13)}{x/13}\,\mathrm{d}x = \frac{\pi}{2}.$$

The pattern is clear, right? Actually, **NO!**

$$\int_0^\infty \frac{\sin x}{x}\frac{\sin(x/3)}{x/3}\cdots\frac{\sin(x/15)}{x/15}\,\mathrm{d}x = \frac{\pi}{2} - \frac{6879714958723010531\pi}{935615849440640907310521750000}.$$

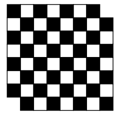
Chessboard Tilings



Can you tile the first grid using 1×2 tiles?

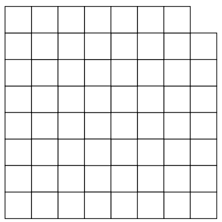
- No. There are an odd number of squares, each tile covers an even number of squares.

Can you tile the second grid using 1×2 tiles? Color it.

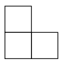


- No. The board has more black squares than white squares.

Preview



Can you tile the grid (with a square missing) with L-shaped tiles?



Next lecture!

Dealing with Quantifiers

How do we prove statements like $\exists x\ P(x)$ and $\forall x\ P(x)$?

Existential statements: $\exists x\ P(x)$.

- Constructive proof: Find an *explicit* example of an x which satisfies $P(x)$.
- Non-constructive proof: Somehow prove the statement *without* finding a specific x. We will see this later today!

Universal statements: $\forall x\ P(x)$.

- Let x be an *arbitrary* element of your universe.
- Then, prove $P(x)$ holds for this generic x.
- Key idea: Since your proof does not use anything special about x, your proof works equally well for *any* x.
  Thus, you proved $\forall x\ P(x)$.

Direct Proofs

Suppose you want to prove an implication $P \implies Q$.

Direct proof: Assume P, prove Q.

Why is this valid?

- If P is False, then the implication $P \implies Q$ is automatically True (called *vacuously* True).
- So, we only have to worry about showing that Q is True whenever P is True.

Remark: If the hypothesis P is never satisfied, then the theorem is vacuously True. "If unicorns exist, then I am bald."

Direct Proof: Example

Background: Given $a, b \in \mathbb{Z}$, we say that a **divides** b, written $a \mid b$, if there exists an integer $d \in \mathbb{Z}$ such that $ad = b$.[1]

- Example: Every integer divides 0 because for any $a \in \mathbb{Z}$, we have $a \cdot 0 = 0$.
- Mathematical definitions require time to parse. Read carefully!
- In symbols: $\forall a, b \in \mathbb{Z}\, (a \mid b \iff \exists d \in \mathbb{Z}\, (ad = b))$.

Fact: For any $a, b, c \in \mathbb{Z}$, if $a \mid b$, then $ac \mid bc$.

- Formally: $\forall a, b, c \in \mathbb{Z}\, (a \mid b \implies ac \mid bc)$.
- Assume P, which is $a \mid b$.
- By definition, there exists $d \in \mathbb{Z}$ such that $ad = b$.
- Multiply by c, so $(ac)d = bc$.
- By definition, $ac \mid bc$, which is Q. $\square$

[1] Remember, if a divides b, then a is supposed to be the smaller one.

Direct Proof: Example II

For any $a, b, c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then $c \mid a + b$.

- Assume $c \mid a$ and $c \mid b$.
- By definition of divisibility, there exist integers $k, \ell \in \mathbb{Z}$ such that $ck = a$ and $c\ell = b$.
- Add them: $ck + c\ell = c(k + \ell) = a + b$.
- By definition of divisibility, $c \mid a + b$. $\square$

Similarly, $c \mid a - b$. In fact, for any $x, y \in \mathbb{Z}$, we have $c \mid xa + yb$.

Proof by Contraposition

Suppose you want to prove an implication $P \implies Q$.

Proof by contraposition: Prove the contrapositive $\neg Q \implies \neg P$.

- Recall that the contrapositive is *equivalent* to the original implication.

When is the contrapositive easier to prove than the original implication?

- When $\neg Q$ gives you more information than P!
- Or... when $\neg P$ is easier to prove than Q.
- Think about how you prove $\neg Q \implies \neg P$.
  - Assume $\neg Q$.
  - Prove $\neg P$.

Proof by Contraposition: Example

For $n \in \mathbb{N}$, if n^2 is even, then n is even.

Try a direct approach: n^2 is even $\implies$ n is even.

- n^2 is even, so $n^2 = 2k$ for some $k \in \mathbb{N}$.
- So $n = \sqrt{2k} \ldots$ which is even... because ...

Try contrapositive: n is odd $\implies$ n^2 is odd.

- n is odd, so $n = 2k + 1$ for some $k \in \mathbb{N}$.
- Square it: $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
- Therefore, n^2 is odd. $\square$

Proof by Contraposition: Example

I have a number $x \in \mathbb{R}$. For any positive $y > 0$, it holds that $x \leq y$. Is it true that $x \leq 0$?

$P \implies Q$:

- $(\forall y > 0\, (x \leq y)) \implies (x \leq 0)$.

$\neg Q \implies \neg P$:

- $(x > 0) \implies \neg(\forall y > 0\, (x \leq y))$
- De Morgan: $(x > 0) \implies (\exists y > 0\, (x > y))$
  - Note: When using De Morgan's Law for Quantifiers, only the quantifier flips; the universe does **NOT** change.
- Assume $\neg Q$, which is $x > 0$.
- Can we find a $y > 0$ such that $x > y$?
- Take $y = x/2$ (for example). Thus, $\exists y > 0\, (x > y)$. This is $\neg P$. $\square$

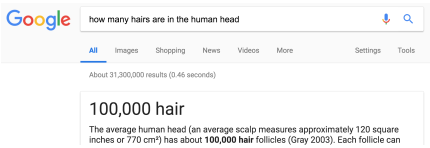
Pigeonhole Principle

Pigeonhole Principle: If you try to place pigeons into holes, when there are more pigeons than holes, then at least one hole must have more than one pigeon.

Sound obvious?

- Statement to prove: If there are more pigeons than holes, then at least one hole has more than one pigeon.
- Contrapositive: If no hole has more than one pigeon, the number of pigeons is at most the number of holes.
- *Proof.* Every hole has zero or one pigeons, so the number of holes is at least as big as the number of pigeons. $\square$

Application of Pigeonhole Principle



Probably no one has more than 500000 head hairs.

How many people are in San Francisco?

Pigeonhole Principle:

- The people of SF are pigeons.
- The number of head hairs that a person has is a "box".
- Conclusion: There are two people in SF who have the same number of hairs on their heads.

Proof by Contradiction

Suppose we want to prove a statement P.

Proof by contradiction: Assume $\neg P$. Show that R (any statement) and its negation $\neg R$ are both True.

- This is called a **contradiction**: $R \wedge \neg R \equiv F$.

Why is this valid?

- We have proved $\neg P \implies R \wedge \neg R$, i.e., $\neg P \implies F$.
- The contrapositive is $T \implies P$.
- Conclude that P is True.
- Intuition: We assumed $\neg P$ but arrived at an absurd conclusion, so our assumption must have been wrong.

Notice the use of the contrapositive. In fact, proof by contraposition and proof by contradiction are not very different.

Proof by Contradiction: Example

I have a number $x \in \mathbb{R}$. For any positive $y > 0$, it holds that $x \le y$. Is it true that $x \le 0$?

How does the proof look like when we use proof by contradiction?

- Assume, for the sake of contradiction, that $x > 0$.
- Then, $x/2$ is a positive number with $x/2 < x$ ($\neg R$).
- This contradicts the statement "for any positive $y > 0$, it holds that $x \le y$" (R).
- We have proven $R \wedge \neg R$.
- Thus, $x \le 0$. $\square$

Remark: In higher mathematics, proofs are usually phrased via contradiction rather than contraposition.

Proof by Contradiction: Irrationality of $\sqrt{2}$

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

Background: x is **rational** if there exist $p, q \in \mathbb{Z}$, with $q \neq 0$, such that $x = p/q$.

- The integers p and q can be chosen to be in *lowest form*, i.e., sharing no common factors.

Proof.

- Assume, for the sake of contradiction, that $\sqrt{2}$ is rational.
- Then, let $p, q \in \mathbb{Z}$ be such that $\sqrt{2} = p/q$. Let p and q be in lowest terms.
- Square it! $2 = p^2/q^2$.
- If p and q share no common factors, then neither do p^2 and q^2... but $p^2 = 2q^2$, so q^2 divides p^2. Contradiction. $\square$

Proof by Contradiction: Infinitude of Primes

Background: A **prime number** is a natural number, larger than 1, whose only positive divisors are 1 and itself.

There are infinitely many prime numbers.[2]

- Assume, for the sake of contradiction, that there are *finitely* many primes $p_1, \dots, p_n$.
- We will construct a prime number outside of this list.
- Consider $q := p_1 \cdots p_n + 1$.
- Fact: Any natural number greater than 1 has a prime divisor. Thus, there is a prime p which divides q.
- Since $p \mid q$ and $p \mid p_1 \cdots p_n$ (since p is in the list of primes), then $p \mid q - p_1 \cdots p_n$, i.e., $p \mid 1$. Contradiction. $\square$

Is $p_1 \cdots p_n + 1$ prime? *Not necessarily.*
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 19 \cdot 97 \cdot 277$.

[2] The proof goes back to Euclid.

Proof by Cases

Suppose we want to prove a statement P.

Divide up the statement into *exhaustive* cases. Show that in each case, the statement holds.

Why is this valid?

- Say that we divide into two cases, C_1 and C_2.
- If the cases are *exhaustive*, then $C_1 \vee C_2 \equiv T$.
- We prove $C_1 \implies P$ and $C_2 \implies P$.
- This gives $(C_1 \vee C_2) \implies P$, i.e., $T \implies P$.
- Conclude P.

Proof by Cases: Triangle Inequality

Triangle Inequality: If $x, y \in \mathbb{R}$, then $|x+y| \leq |x|+|y|$.

- Case $x \geq 0$, $y \geq 0$: $x+y \leq x+y$? True
- Case $x \leq 0$, $y \geq 0$: $|x+y| \leq -x+y$? Need more information.
  - Case $|x| \leq |y|$: $|x+y| = x+y \leq -x+y$? True, since $x \leq 0$.
  - Case $|x| > |y|$: $|x+y| = -x-y \leq -x+y$? True, since $y \geq 0$.
- Case $x \geq 0$, $y \leq 0$: Same as the previous case, with x and y switched around!
- Case $x \leq 0$, $y \leq 0$: Can be deduced from the first case. Replace x with $-x$ and y with $-y$.

When using proof by cases, save work by eliminating unnecessary cases.

Without Loss of Generality

"Without loss of generality", abbreviated WLOG, is often used in proofs. What does it mean?

Example: Suppose $p \in (0,1)$ and let $a > 0$; prove that $(1-p)\cdot(ap)^2 + p\cdot(a-ap)^2 \leq a^2/4$. WLOG $a = 1$. Why?

- If we assume $a = 1$, then we prove $(1-p)\cdot p^2 + p\cdot(1-p)^2 \leq 1/4$.
- Multiplying both sides by a^2 recovers the result we want.
- Now we only have to prove a simpler inequality!

WLOG means we are considering a special case, but *from this special case we can recover the general case easily*.

Proof by Cases: Non-Constructive Proof

Do there exist irrational x and irrational y such that x^y is rational?

Here is a *non-constructive* proof.

- We know that $\sqrt{2}$ is irrational.
- Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational.
  - We are done! Let $x = y = \sqrt{2}$.
- Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.
  - Then, $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$. This is rational! Set $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.
- The cases are exhaustive. $\square$

Proof by Cases: Non-Constructive Proof

In the previous proof, we split into two cases:

- $\sqrt{2}^{\sqrt{2}}$ is rational.
- $\sqrt{2}^{\sqrt{2}}$ is irrational.

Well. . . which case is true?!

We showed the *existence* of irrational x, y such that x^y is rational, *without* explicitly saying what values of x and y work.

Unsatisfying? Here is a constructive proof.

- $e^{\ln 2} = 2$, which is rational.
- e and $\ln 2$ are both known to be irrational. $\square$

(But how do we know e and $\ln 2$ are irrational?)

Incorrect Proof Method

"**Proposition**": $1 = -1$.

- Assume $1 = -1$.
- Square both sides, $1 = 1$. True. ♠

What did we just do?

To prove P, we proved $P \implies T$.

- This is not surprising; $P \implies T$ is always True no matter what P is.
  - Recall: $P \implies Q$ is only False if P is True and Q is False.
  - If Q is True, then $P \implies Q$ is always True.
- From $P \implies T$, we *cannot* deduce that P is True.

Moral: Do not assume what you are trying to prove!

Tips for Writing Proofs

1. Use English. Proofs are meant to be read by humans!
2. If your proof is long and complicated, break it up into smaller results called Lemmas.
   Lemmas are like subroutines in programming.
3. How do I learn to write proofs? Learn by practicing. . . and by reading proofs that others have written.
4. How rigorous should my proof be? Rule of thumb: good enough to convince your skeptical classmate.

Summary

- Direct proof
- Proof by contraposition, proof by contradiction
- Proof by cases
- Pigeonhole principle: More pigeons than holes implies that at least one hole has multiple pigeons.
- Proofs can be non-constructive.
- You learned classical proofs: irrationality of $\sqrt{2}$, infinitude of primes...