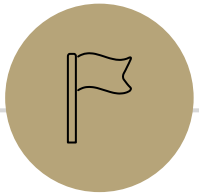
"Proof by contradiction is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game" - G. H. Hardy

Proof by Contradiction

CSE 311: Foundations of Computing I
Lecture 15

Announcements

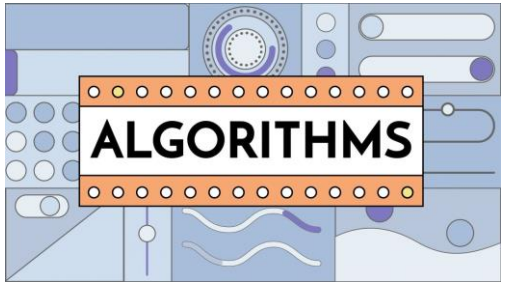
- HW4 solutions at the front, grades posted tonight
- HW5 due Wednesday at 11:59 pm.
  - Feedback before the midterm is only guaranteed if you don't use late days.
- Midterm is on Friday in class.
  - Optional review session tomorrow (Tuesday) from 3:00 – 4:20 in DEM 104. Will be recorded on Panopto.
  - Info about the exam has been published on the course website under the Exams tab. Includes problem categories and a practice exam.
- No new HW released this week.

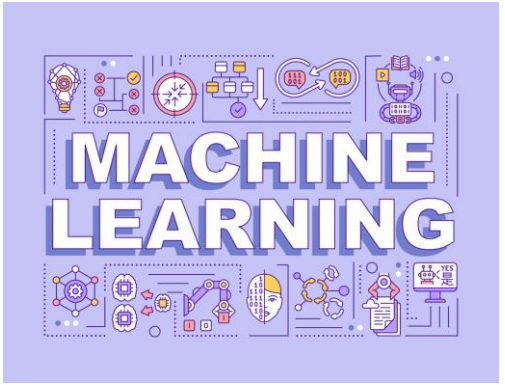


Proof by Contradiction

Proof Strategies

- Direct Proof
- Proof by Contrapositive
- Proof of Biconditional
- Proof by Cases
- Existence Proof
- Induction
  - Weak Induction
  - Strong Induction
  - Structural Induction (coming soon!)
- Proof by Contradiction

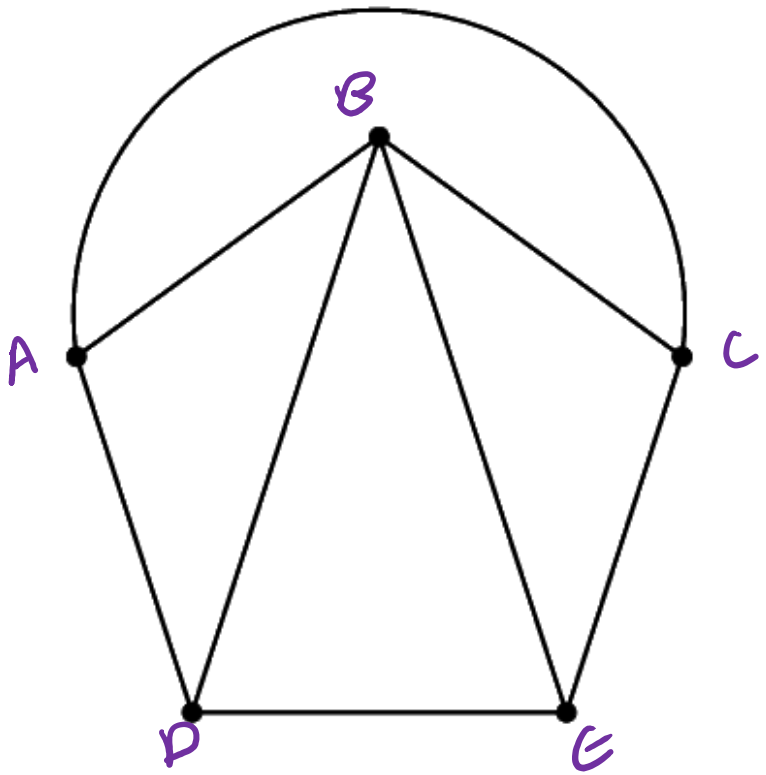




Warm-Up

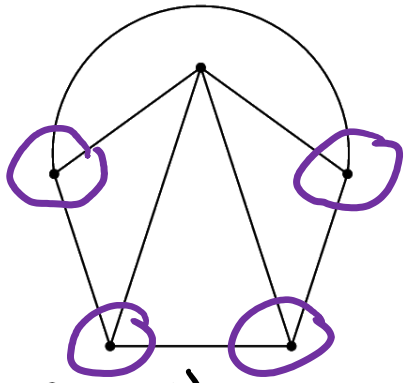
Traverse the following graph by traveling along each edge exactly once.

Any of the vertices may be selected as the starting or ending vertex.



There is no path!
Can we prove it?

Warm-Up



Claim: It is impossible to traverse this graph by traveling along each edge exactly once.

Proof: Suppose that it were possible to traverse this graph by travelling along each edge exactly once. Consider how many times each vertex would be passed through. For every time a vertex is entered, it is exited. Therefore if each edge is traversed exactly once, each vertex should have an even number of edges connected to it. The only exceptions are the starting & ending vertex, of which there are at most 2. However, this graph has 4 vertices with an odd number of edges connected to them. So, no traversal is possible.

What did we just do?

To prove that the claim p holds:

1. We assume p does not hold, i.e. assume $\neg p$

2. From $\neg p$, derive a false statement.

Why does that work?

Observe from our logical equivalences:

$$\neg p \rightarrow F \equiv \neg\neg p \vee F \quad \text{L.O.I}$$

$$\equiv p \vee F \quad \text{Double Negation}$$

$$\equiv p \quad \text{Identity}$$

Proof by Contradiction

Proof by contradiction is a strategy for proving statements of any form.

- The strategy to prove p is to assume $\neg p$, and derive false (i.e. derive a contradiction)
- E.g. the strategy to prove $p \to q$ is to assume $p \wedge \neg q$, and derive False.
- E.g. the strategy to prove $p \vee q$ is to assume $\neg p \wedge \neg q$, and derive False.

$$\neg(p \to q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$$

Proof by Contradiction Skeleton

Suppose for the sake of contradiction $\neg p$.

…

Then some statement s must hold.

…

And some statement $\neg s$ must hold.

But s and $\neg s$ is a contradiction. So p must be true.

2 or less vertices have odd # of edges

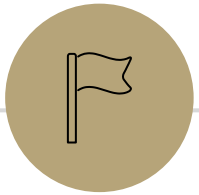
$S \wedge \neg S \equiv F$

4 vertices

Proof by Contradiction: Remarks

- Unlike other proof techniques, we don't know *where* we're going. We're trying to find **any** contradiction. That can make it harder.
- Contradiction is a sledge-hammer.
  It can be used to prove many things. But it makes a mess.
- Use contradiction as a last-resort.

Contradiction is a sledge-hammer



Proof by Contradiction Examples

Claim 1: No integer is even and odd.

Suppose for the sake of contradiction that there exists an integer x that is both even and odd. By definition, $x=2a$ and $x=2b+1$ for some integers a and b. Observe:

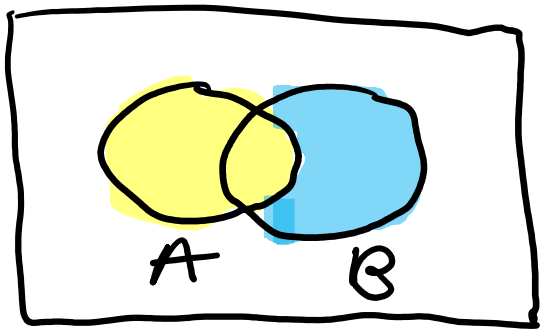
$$2a = 2b+1$$
$$2a-2b = 1$$
$$2(a-b) = 1$$
$$a-b = 1/2$$

Since a, b are integers, $a-b$ is also an integer. But $\frac{1}{2}$ is not an integer. This is a contradiction.

Thus, no integer can be even and odd.

Claim 2: For all sets A, B, we have $A \cap (B \setminus A) = \emptyset$.

Suppose for the sake of contradiction, that there exists some sets A, B such that $A \cap (B \setminus A) \neq \emptyset$. Then, there exists some element of $A \cap (B \setminus A)$, call it x. Since $x \in A \cap (B \setminus A)$, by def of intersect $x \in A$ and $x \in B \setminus A$. By def of set difference, $x \in B$ and $x \notin A$. Since $x \in A$ and $x \notin A$, this is a contradiction.



Thus for all sets A, B, $A \cap (B \setminus A) = \emptyset$.

[Exercise] Claim 3: The sum of any four consecutive integers is not divisible by 4.

Suppose for the sake of contradiction that there exists some 4 consecutive integers whose sum is divisible by 4.

Then there is some integer x such that $4 \mid (x + (x+1) + (x+2) + (x+3))$.

By def of divides, there exists some integer k such that

$$x + (x+1) + (x+2) + (x+3) = 4k$$

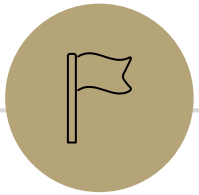
$$4x + 6 = 4k$$

$$6 = 4k - 4x$$

$$6 = 4(k - x)$$

Since k, x are integers, $k - x$ is an integer, so $\underline{4 \mid 6.}$

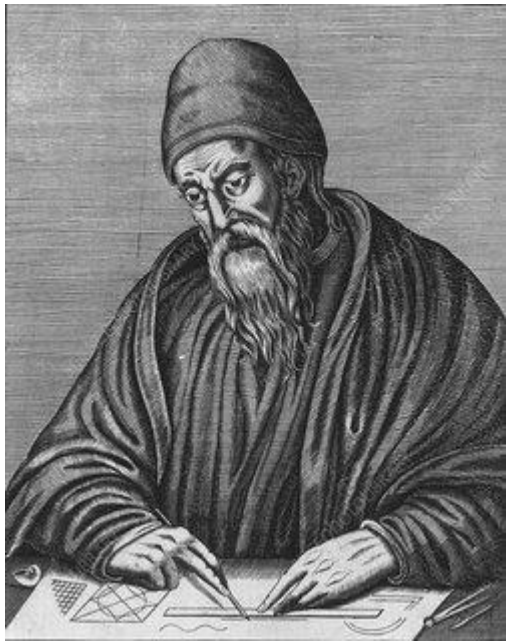
But $\underline{4 \nmid 6.}$ This is a contradiction. So the sum of any four consecutive ints. is not $\nmid 4$.



Euclid’s Theorem

Euclid's Theorem: There are infinitely many prime numbers.

2, 3, 5, 7, 11, 13, …



Euclid ~300 BC

Euclid's Theorem: There are infinitely many prime numbers.

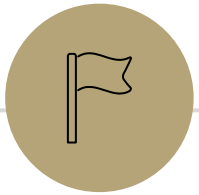
Assume for the sake of contradiction that there are finitely many prime numbers. List them out as $p_1, p_2, p_3, \ldots p_k$. Consider the number $q = p_1 \cdot p_2 \cdot p_3 \cdots p_k + 1$.

Case 1: q is prime. Then q is a prime number larger than p_i for all i from 1 to k. But every prime was supposed to be in the list $p_1, \ldots, p_k$. This is a contradiction.

Case 2: q is composite. Then q must have some prime factor. So there exists some p_i that divides q. I.e.

the remainder $q \% p_i = 0$. But

$q \% p_i = (p_1 \cdot p_2 \cdots p_k + 1) \% p_i = 1$. This is a contradiction.



Discussion

Several strategies to prove $p \rightarrow q$

1) Direct Proof

Assume p is true. Show q is true.

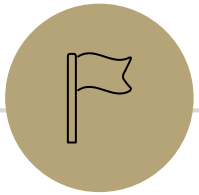
2) Proof by Contrapositive

Assume $\neg q$ is true. Show $\neg p$ is true.

3) Proof by Contradiction $\neg(p \rightarrow q) \equiv p \wedge \neg q$

Assume p is true and $\neg q$ is true. Derive False.

$\neg p$



More Examples

There is no smallest positive rational number.

Recall: $\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$