REVIEW OF PROOF TECHNIQUES

DISCRETE MATHEMATICS AND THEORY 2

MARK FLORYAN

GOALS!

1. Why do we need ***proofs*** for theory of computation? Do we HAVE to do it?

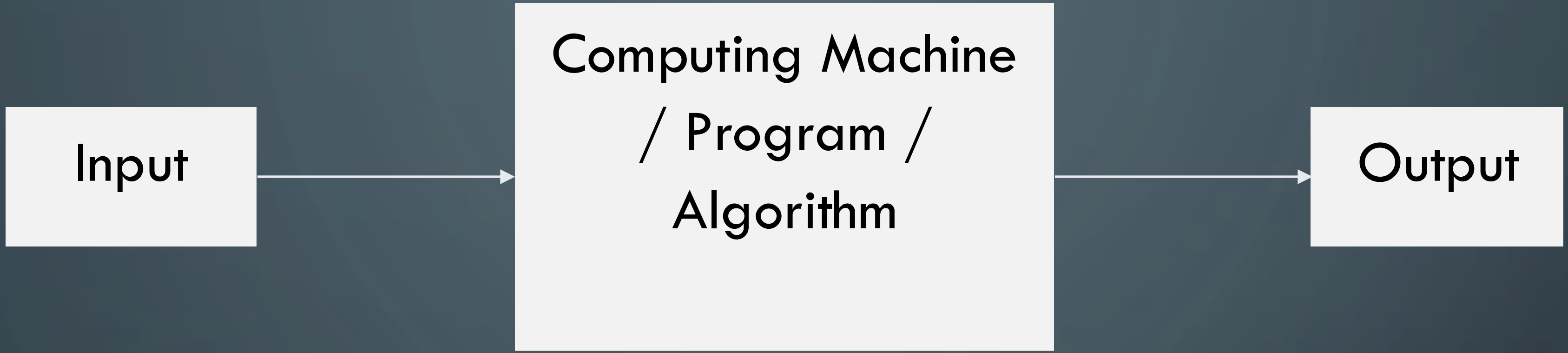
2. What are the main ***proof techniques*** we will be using? Let's review each one!

PART 1: WHY DO WE NEED PROOFS?

DISCUSSION! WHY DO WE NEED PROOFS?

What do you think?

DISCUSSION! WHY DO WE NEED PROOFS?



Imagine we have two computational models A and B (for middle box)

Proofs allow us to answer questions like:

- Is there a some function A can compute but B cannot?
- Can B be compute all the same functions as A?
- Is there a function that neither A nor B can compute?

PART 2: REVIEW OF PROOF TECHNIQUES

PROOF STRATEGIES

- Construction
- Direct Proof
- Contradiction
- Cases
- Induction

Important: Some proofs could employ multiple strategies! Others might not fit any well!

DIRECT PROOF

DIRECT PROOF

Direct Proof: Given starting assumptions, show a set of logical steps that lead to the desired conclusion.

Theorem 1: There is SOME natural number that is divisible by 3 but not divisible by 9

Theorem 2: Every natural number divisible by 9 is divisible by 3

DIRECT PROOF CHECKLIST

- Start only with what the theorem assumes.
- Draw “obvious” conclusions from the assumptions and/or prior conclusions.
- End with the desired statement being true.

DIRECT PROOF

<u>Theorem 1</u>: There is SOME natural number that is divisible by 3 but not divisible by 9

Proof: Find a specific number that fits the description!

DIRECT PROOF

Theorem 1: There is SOME natural number that is divisible by 3 but not divisible by 9

Proof: Find a specific number that fits the description!

Start w/ assumption: 6 is a number divisible 3

Obvious Conclusion: 6 is not divisible by 9

Thus there is some natural number that is divisible by 3 but not 9

DIRECT PROOF

Theorem 2: Every natural number divisible by 9 is divisible by 3

Proof: Start w/ assumption and proceed 1 step at a time

DIRECT PROOF

Theorem 2: Every natural number divisible by 9 is divisible by 3

Proof: Start w/ assumption and proceed 1 step at a time

Start w/ assumption: if a natural number is divisible by 9. So grab an arbitrary one $n = 9k$ for some $k \in N$

Obvious Conclusions:

$n = (3)3k$ for some $k \in N$

n is divisible by 3 ← This is what we wanted to prove

PROOF BY CONSTRUCTION

PROOF BY CONSTRUCTION

Proof By Construction: When a theorem states that a particular type of object exists, we can demonstrate HOW to construct it.

Anatomy of proof by construction:

Purple boxes are NESTED proofs. Often use / require another proof technique.

Theorem: something P exists

Step 1: Describe this algorithm

INPUT: None

<Algorithm>

Output: P

Step 2: Prove algorithm correctly constructs P

Prove proposition S:

S = Algorithm given in step 1 correctly constructs P with desired properties

PROOF BY CONSTRUCTION

Proof By Construction: When a theorem states that a particular type of object exists, we can demonstrate HOW to construct it.

Theorem: For each even number $n > 2$, there exists a 3-regular graph with n nodes.

*Proof idea: Show how to construct the graph for any arbitrary n. Usually this is a **process** for constructing the graph (an algorithm!)*

3-regular means every node has degree 3

PROOF BY CONSTRUCTION CHECKLIST

- Fully define construction
- Describe how we know it satisfies the theorem

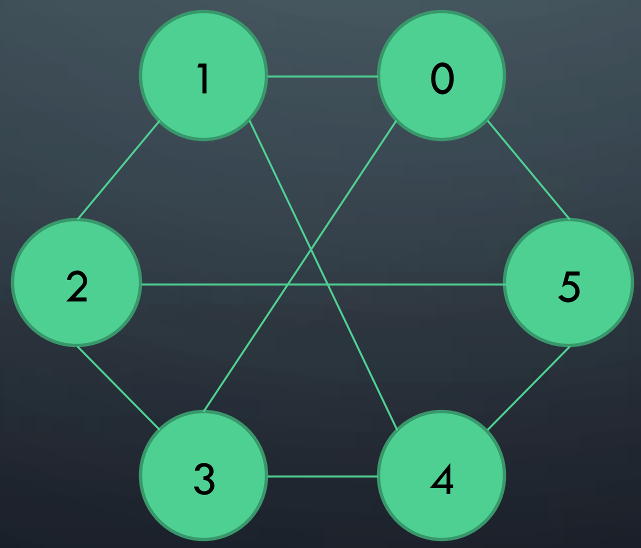
PROOF BY CONSTRUCTION

<u>Theorem</u>: For each even number $n > 2$, there exists a 3-regular graph with n nodes.

PROOF BY CONSTRUCTION

Theorem: For each even number $n > 2$, there exists a 3-regular graph with n nodes.

Overall Idea: Draw nodes in a circle and number them 0 through n-1. Match each node with the one next to it (2 edges per node) and also to the one directly across from it (node that is n/2 away).



PROOF BY CONSTRUCTION

Theorem: For each even number $n > 2$, there exists a 3-regular graph with n nodes.

$$G = (V, E)$$
$$V = \{0, 1, \ldots, n-1\}$$

$$E = \{\{i, i+1\} \mid 0 \le i \le n-2\} \cup \{\{n-1, 0\}\} \cup \left\{\left\{i, i+\frac{n}{2}\right\} \middle| \, 0 \le i \le \frac{n}{2} - 1\right\}$$

How do we know G satisfies the theorem (is 3-regular). Because each node is "drawn in a circle" and paired with its neighbors and the one directly across the circle. Even number n means the pairing is perfect, so every node has 3 edges.

PROOF BY CONSTRUCTION

Proof By Construction: When a theorem states that a particular type of object exists, we can demonstrate HOW to construct it.

Anatomy of proof by construction:

Theorem: $p \rightarrow q$

INPUT: p

<Algorithm>

Output: q

Step 1: Describe this algorithm

Step 2: Prove algorithm correctly constructs P

Prove proposition S:

S = Algorithm given in step 1 correctly constructs q from p with desired properties

Purple boxes are NESTED proofs. Often use / require another proof technique.

PROOF BY CONTRADICTION

PROOF BY CONTRADICTION

Proof by Contradiction: Assume the theorem is FALSE, and show through direct proof that this leads to some impossibility

PROOF BY CONTRADICTION

Anatomy of proof by contradiction:

Theorem: p

Assume: $\neg p$

<Logical Conc. 1>

<logical Conc. 2>

…

<logical conc. n>

2=1 or some contradictory statement

Conclusion: p

Note that each logical step may involve a sub-proof that proves that logical step. Not always

Proof that:

<Log. Conc. 1> → <Log. Conc. 2>

PROOF BY CONTRADICTION

Anatomy of proof by contradiction:

Theorem: $p \rightarrow q$

Assume: $p \wedge \neg q$

<Logical Conc. 1>

<logical Conc. 2>

…

<logical conc. n>

2=1 or some contradictory statement

Conclusion: $p \rightarrow q$

Note that each logical step may involve a sub-proof that proves that logical step. Not always

Proof that:

<Log. Conc. 1> → <Log. Conc. 2>

PROOF BY CONTRADICTION

Proof by Contradiction: Assume the theorem is FALSE, and show through direct proof that this leads to some impossibility

Theorem: $\sqrt{2}$ is irrational

Oftentimes, contradiction proofs are much easier than direct proofs. Sometimes not.

PROOF BY CONTRADICTION CHECKLIST

- Start by assuming the opposite of the statement
  - Usually this means assuming that something satisfied the left-hand-side of an implication but not the right-hand side
- Draw “obvious” conclusions from the assumptions and/or prior conclusions
- Show that the conjunction of 2 assumptions and/or conclusions is obviously false

PROOF BY CONTRADICTION

Theorem: $\sqrt{2}$ is irrational

Prove this by contradiction:

Suppose that $\sqrt{2}$ is NOT irrational. Thus, it is rational

Thus there exist integers $m, n \in Z$ such that $\sqrt{2} = \frac{m}{n}$ (note that m, n cannot be 0)

Simplify m and n by dividing by any common divisors.

After this, one of m and n must be odd.

Multiply to obtain: $n\sqrt{2} = m$

Square both sides: $2n^2 = m^2$

Because m^2 is twice an integer, we know that m^2 is even, thus, m is also even because square of odd number is also odd. Thus we can write $m = 2k$ for some $k \in Z$

Substitute for m: $2n^2 = (2k)^2$

$2n^2 = 4k^2$

$n^2 = 2k^2$ //But n was supposed to be odd! Contradiction!

PROOF BY INDUCTION

PROOF BY INDUCTION CHECKLIST

- Show the theorem holds for some initial value b (i.e. “Base Case”)
- Assume that the theorem holds for some arbitrary value $n \geq b$. (i.e. “Inductive Hypothesis”)
- Show that we can conclude that the theorem holds for $n + 1$ (i.e. “Inductive Step”)

PROOF BY INDUCTION

Anatomy of proof by induction:

Theorem: $\forall_n p(n)$

Base Case

Provide a proof for small n (first n or first few n). Usually trivial.

$p(n_k) \rightarrow p(n_{k+1})$

Inductive Hypothesis

Assume $p(n_k)$ for some arbitrary k (sometime "up through k").

Inductive Step

Prove $p(n_{k+1})$

This usually involves using another proof technique!

Almost always references or leverages the assumed truth of $p(n_k)$

Remember that purple boxes are sub-proofs!!

THERE ARE 2^n BINARY STRINGS OF LENGTH $n | n \geq 1$.

Base Case (n=1): $2^1 = 2$, Strings are "0" and "1"

THERE ARE 2^n BINARY STRINGS OF LENGTH $n|n \geq 1$.

Base Case (n=1):	$2^1 = 2$, Strings are "0" and "1"
Ind. Hypothesis	Suppose 2^k strings exist for length k

THERE ARE 2^n BINARY STRINGS OF LENGTH $n | n \geq 1$.

Base Case (n=1):	$2^1 = 2$, Strings are "0" and "1"
Ind. Hypothesis	Suppose 2^k strings exist for length k
Ind. Step	2^k strings exist for length k Consider length k+1 For each of the 2^k strings of length k, we can add a 0 (2^k total) For each of the 2^k strings of length k, we can add a 1 (2^k total) Grand total number of strings of length k+1 is: $2^k + 2^k = 2(2^k) = 2^{k+1}$

THERE ARE $n!$ PERMUTATIONS OF A LIST OF LENGTH n

FOR A FINITE SET S, $|\mathcal{P}(S)| = 2^{|S|}$

PROOF BY INDUCTION

Anatomy of proof by induction:

Theorem: $\forall_n p(n)$

Base Case

Provide a proof for small n (first n or first few n). Usually trivial.

$p(n_k) \rightarrow p(n_{k+1})$

Inductive Hypothesis

Assume $p(n_k)$ for some arbitrary k (sometime "up through k").

Inductive Step

Prove $p(n_{k+1})$

This usually involves using another proof technique!

Almost always references or leverages the assumed truth of $p(n_k)$

Remember that purple boxes are sub-proofs!!

FLORYAN'S PROOF WRITING TIPS

1. Identify the nature of the claim
   - Is it a "there exists" statement, a "for all" statement?
2. Write out all the important definitions (assumptions, the goal, etc.)
3. Manipulate definitions to see how they relate and develop intuition
4. Organize your discoveries into one or more proof strategies
   - There exists: usually by construction, sometimes by other means
   - For all: rarely by construction, typically by one of the other methods
5. Write your proof to be obvious to the typical CS3102 student last week.
   - Name your proof strategy, briefly mention how you're going to use the strategy, explain what you mentioned in detail
   - If some step would have been confusing to the typical classmate last week, you should break it up into smaller steps