ANKARA UNIVERSITY COM364 AUTOMATA THEORY

Week 2

About Proofs

Kurtuluş KÜLLÜ

REMINDER

- This course will be very mathematical and we will work with proofs
- A good proof should be correct and clear (easy to understand)
- When writing (or describing) a proof, it is helpful to give three levels of detail
  - 1st level: A short phrase/sentence providing a "hint" of the proof
    - E.g. "proof by contradiction", "proof by induction", "follows from the pigeonhole principle"
  - 2nd level: A short, one paragraph description of the main ideas
  - 3rd level: The full proof

LEVELS OF DETAIL EXAMPLE

Suppose $A \subseteq \{1,2,\dots,2n\}$ with $|A| = n + 1$.

True or False?

There are always two numbers in A such that one number divides the other number.

LEVELS OF DETAIL EXAMPLE

Suppose $A \subseteq \{1,2,\dots,2n\}$ with $|A| = n+1$.

True or False?

There are always two numbers in *A* such that one number divides the other number.

Example: If $n = 2$, $A \subseteq \{1,2,3,4\}$ and $|A| = 3$.

- Case 1: If 1 is in A, because 1 divides all other numbers, statement will be true.

- Case 2: If 1 is not in A, A has to be $\{2,3,4\}$. And now, 2 divides 4.

How about $n = 3$?

LEVELS OF DETAIL EXAMPLE

Suppose $A \subseteq \{1,2,\ldots,2n\}$ **with** $|A| = n + 1$.

True or False?

There are always two numbers in *A* such that one number divides the other number.

TRUE

Example: If $n = 2$, $A \subseteq \{1,2,3,4\}$ **and** $|A| = 3$.

- Case 1: If 1 is in A, because 1 divides all other numbers, statement will be true.

- Case 2: If 1 is not in A, A has to be $\{2,3,4\}$. **And now, 2 divides 4.**

How about $n = 3$?

LEVELS OF DETAIL EXAMPLE

LEVEL 1

HINT 1

The Pigeonhole Principle

If you have 10 pigeons and 9 pigeonholes, then at least one pigeonhole will have more than 1 pigeon.

LEVELS OF DETAIL EXAMPLE

LEVEL 1

HINT 1

The Pigeonhole Principle

If you have n+1 pigeons and n pigeonholes, then at least one pigeonhole will have more than 1 pigeon.

HINT 2

Every integer a can be written as $a = 2^k m$, where m is an odd number and k is an integer.

Call m the "odd part" of a.

LEVELS OF DETAIL EXAMPLE

LEVEL 2

Proof Idea:

Given $A \subseteq \{1, 2, \ldots, 2n\}$ with $|A| = n + 1$.

Using the pigeonhole principle, we'll show that there are elements $a_1 \neq a_2$ in A such that

$$a_1 = 2^i m \text{ and } a_2 = 2^j m$$

for some odd m and integers i and k.

LEVELS OF DETAIL EXAMPLE

LEVEL 3

Proof:

Suppose $A \subseteq \{1,2, \dots, 2n\}$ with $|A| = n + 1$.

Write each element of A in the form $a = 2^i m$ where m is an odd number in $\{1,2, \dots, 2n\}$.

Note that there are n odd numbers in $\{1,2, \dots, 2n\}$.

Since $|A| = n + 1$, according to the pigeonhole principle, there must be two different numbers in A with the same odd part.

Let a_1 and a_2 have the same off part m.
Then, $a_1 = 2^i m$ and $a_2 = 2^j m$, so one must divide the other
(If j $> i$, a_1 divides a_2 and vice versa).

REMINDER

- When writing (or describing) a proof, it is helpful to give three levels of detail
  - 1st level: A short phrase/sentence providing a “hint” of the proof
    - E.g. “proof by contradiction”, “proof by induction”, “follows from the pigeonhole principle”
  - 2nd level: A short, one paragraph description of the main ideas
  - 3rd level: The full proof
- The book by Sipser is written in this way and I suggest you do the same when needed
- In the classroom, we will generally talk about the proofs using the first two levels (the details will mostly be excluded)
  - When studying, you should think (and look at the books) about how to complete these details because you might be asked to give complete proofs in exams.
- We will go over some standard proof methods (Both textbooks have parts on these)

TERMINOLOGY

- A ***theorem*** is a mathematical statement that is proved to be true.
  - We generally only use this word for statements of special interest
- Sometimes we prove statements only to use them in other (more important) proofs.
  - These (less important) proven statements are often called ***lemmas***.
  - So, a *lemma* is like a *theorem* but it is often not the main thing we are interested in.
- Most theorems allow us to conclude easily that other, related statements are also true. These are called ***corollaries*** of the theorem.

FINDING PROOFS (1)

- Unfortunately, not always easy and there is no simple set of rules for doing this.
- But, there are some helpful strategies:
  - First and perhaps most important thing is to read and understand the statement to prove
    - Do you understand the notation?
    - Can you rewrite the statement in your own words?
    - Can you break the statement down and consider each part separately?
      - Example1: a statement such as “P if and only if Q” or “P iff Q” is most of the time split into forward direction (“if P then Q”) and backward/reverse direction (“P only if Q” or “if Q then P”)
      - Example2: Proving sets A and B are equal can be split into two parts. 1) Prove A is a subset of B (every element of A is also in B). 2) Prove B is a subset of A (every element of B is also in A).
  - Next, for the statement or a part of it, try to think about whether you think it is true and why.
    - Experimenting with some examples can be very useful.
    - Can you find a *counterexample* (an example that makes the statement false)? If you can, you just proved that the statement is false. If you can’t, the difficulty in finding a counterexample can give you an idea.

FINDING PROOFS (2)

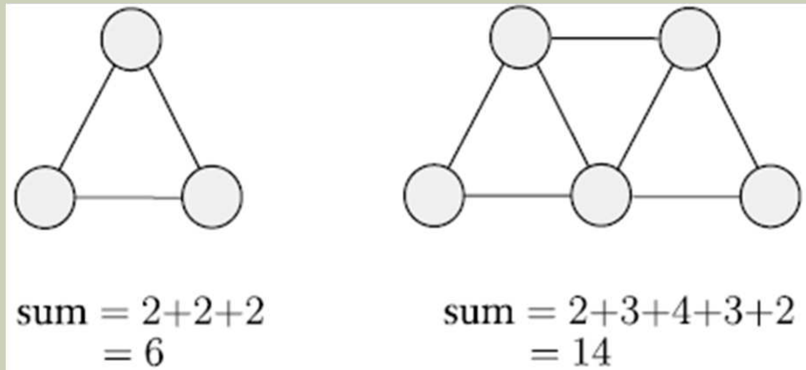
- But, there are some helpful strategies:
  - … (previous page)
  - If you still cannot see a way, try to simplify the statement.
    - For example, if statement has a condition like $k>0$, you can try to prove for $k=1$. If successful, you can try for $k=2$, and so on until you can see a way for the general case (for $k>0$).
    - If even the simpler version is difficult, try simplifying even further.
  - Finally, when you think that you know how to prove, you must write it properly.
    - A well-written proof is a sequence of statements where each statement follows in a simple way from previous statements.
    - Carefully writing a proof is important for 2 main reasons:
      - To make sure that there are no mistakes, and
      - To enable a reader to understand it.

EXAMPLE 1

Prove that, *for every graph G, the sum of the degrees of all the nodes in G is an even number*.

First, make sure you understand what the statement is saying.

Then, you can draw some graphs and observe if this is true.



Next, you can try to find a counterexample. Try to draw a graph in which the sum is an odd number. Can you now see an idea?

EXAMPLE 2

Prove that, *for any two sets* A *and* B, $\overline{A \cup B} = \bar{A} \cap \bar{B}$.

Try on your own…

EXAMPLE 2

Prove that, *for any two sets* A *and* B, $\overline{A \cup B} = \bar{A} \cap \bar{B}$.

Again, first make sure that you understand the statement.

We can show this in two steps,
first show that every element of $\overline{A \cup B}$
has to be an element of $\bar{A} \cap \bar{B}$,
and then show the opposite.

TYPES OF PROOF

- Proof by Construction
  - Many theorems state that a particular type of object exists.
  - *Proof by construction* proves such a theorem by showing how to construct the object.
- Proof by Contradiction
  - Assume that the theorem is false.
  - Then show that this assumption leads to a contradiction (an obviously false result)
- Proof by Induction
  - Generally used to show that all elements of an infinite set have a property
  - E.g., If the set of possible values is $\mathbb{N} = \{1,2,3, \dots\}$ and the property is P, to prove that $P(n)$ is true, we show that both $P(1)$ and $P(k) \rightarrow P(k+1)$ are true. These are called the ***basis*** step and ***induction*** step respectively.

PROOF BY CONSTRUCTION EXAMPLE

Statement

- For each even number $n > 2$, there exists a 3-regular graph with n-nodes. (Note: a graph is *k*-regular if all nodes have degree *k*)

Proof

- Let $n > 2$ be even, construct graph $G = (V, E)$ with n nodes as follows.

$$V = \{0, 1, \dots, n-1\}$$
$$E = \{\{i, i+1\} | \text{for } 0 \leq i \leq n-2\} \cup \{\{n-1, 0\}\}$$
$$\cup \left\{\left\{i, i+\frac{n}{2}\right\} \middle| \text{for } 0 \leq i \leq \frac{n}{2} - 1\right\}$$

- Picture the nodes around a circle. First row of E forms the circular connections. The second row nodes at opposite ends of the circle. You can see why each node in *G* has degree 3.

PROOF BY CONTRADICTION EXAMPLE(1)

Statement

- $\sqrt{2}$ is irrational

Proof

- Assume that $\sqrt{2}$ is rational.
- This means that there are two integers, m and n, such that

$$\sqrt{2} = \frac{m}{n}$$

- If both m and n are divisible by the same integer greater than 1, divide both by the largest such integer
  - This doesn't change the value $\frac{m}{n}$
  - Now, at least one of m and n must be odd
- Next, multiple both sides of the equation by n and obtain

$$n\sqrt{2} = m$$

PROOF BY CONTRADICTION EXAMPLE(2)

Proof (continued)

$$n\sqrt{2} = m$$

- Square both sides

$$2n^2 = m^2$$

- So, m^2 and therefore m must be even. In other words, we can write $m = 2k$ for some integer k. Substitute this into the equation

$$2n^2 = (2k)^2 = 4k^2$$
$$n^2 = 2k^2$$

- But, this shows that n^2 and therefore n are both even.
- We saw that both m and n are even. But we initially reduced them so that they were both <u>not</u> even.
- This is a contradiction, so our assumption that $\sqrt{2}$ is rational must be wrong. $\sqrt{2}$ is irrational.

PROOF BY INDUCTION EXAMPLE (1)

Statement (The formula for monthly loan payments)

- For each $t \geq 0$,

$$P_t = PM^t - Y\frac{M^t - 1}{M - 1}$$

P: principal/amount of loan

Y: monthly payment

M: monthly multiplier calculated with $M = 1 + I/12$
where $I > 0$: yearly interest rate,

e.g., $I = 0.06$ means 6%

P_t: the remaining amount after month *t*

2 things happen each month

1: the amount of the loan increases because of the monthly multiplier

2: the amount decreases because of the payment.

So, $P_0 = P$, $P_1 = MP_0 - Y$, $P_2 = MP_1 - Y$, …

PROOF BY INDUCTION EXAMPLE (2)

Statement (The formula for monthly loan payments)

- For each $t \geq 0$,

$$P_t = PM^t - Y\frac{M^t - 1}{M - 1}$$

Proof

- *Basis:* Prove that the formula is true for $t = 0$.

$$P_0 = PM^0 - Y\frac{M^0 - 1}{M - 1} = P - Y\frac{1 - 1}{M - 1} = P \ \surd$$

- *Induction step:* Show that for each $k \geq 0$, if the formula is true for $t = k$, it is also true for $t = k + 1$.

PROOF BY INDUCTION EXAMPLE (3)

Induction step: In other words, assume that

$$P_k = PM^k - Y\frac{M^k - 1}{M - 1}$$

is true and try to reach

$$P_{k+1} = PM^{k+1} - Y\frac{M^{k+1} - 1}{M - 1}$$

from this assumption.

PROOF BY INDUCTION EXAMPLE (4)

We know that $P_{k+1} = P_k M - Y$. Insert the assumption for P_k into this to get

$$P_{k+1} = \left[PM^k - Y\frac{M^k - 1}{M - 1}\right]M - Y$$

Distribute M inside

$$P_{k+1} = PM^{k+1} - YM\frac{M^k - 1}{M - 1} - Y$$

Group terms with Y with paranthesis

$$P_{k+1} = PM^{k+1} - Y\left[M\frac{M^k - 1}{M - 1} + 1\right]$$

$$= PM^{k+1} - Y\frac{M^{k+1} - M + M - 1}{M - 1}$$

$$= PM^{k+1} - Y\frac{M^{k+1} - 1}{M - 1} \blacksquare$$

MORE ON PROOFS

There are some variations (similar but slightly different versions) of induction

Deductive Proofs

- Start with some initial statement (hyphothesis) and reach a conclusion with a sequence of steps.
- Each step must follow (by some accepted logical principle) from either
  - the given facts, or
  - some of the previous steps, or
  - a combination of the two above.

MORE ON PROOFS

Reduction to Definitions

- If you are not sure how to start, convert all terms in the hypothesis to their definitions.

The Contrapositive

- Every if-then statement has an equivalent form that is sometimes easier to prove.
- The *contrapositive* of the statement “if H, then C” is “if not C, then not H”.