eecs2001

Introduction to the Theory of Computation

Lecture 6

Ruth Urner

January 25, 2023

Mathematical statements and proofs

Reading: ITC Section 0.3 andd 0.4

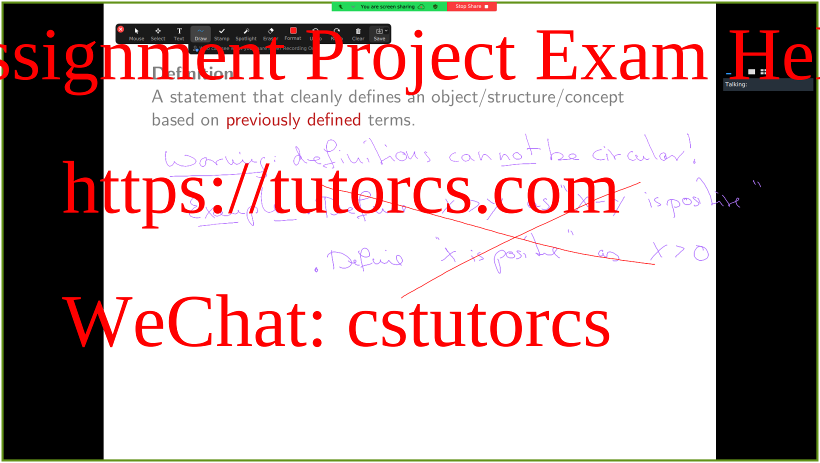
Definition
A statement that clearly defines an object/structure/concept based on previously defined terms.

Theorem
A statement that has been proven to be true.

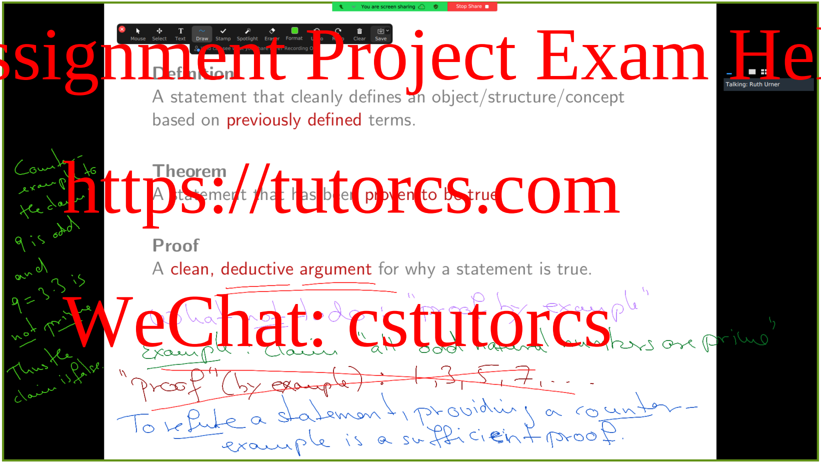
Proof
A clean, deductive argument for why a statement is true.

Lemma
A "helper theorem", typically only stated as a step in a proof of some theorem.

Examples of what not to do..



Examples of what not to do..



Some comments

- Understanding a statement is not the same as understanding why the statement is true (or false). The first step in attempting to prove a statement, is always to make sure you understand the statement fully.

- When you attempt to prove something, I recommend to always first develop an intuition for the statement and what may be the proof. Eg, first come up with some simple examples to illustrate the statement, then develop an intuition for why the statement is true, then develop a proof for it.

- Understanding whether a proof is correct and complete, is an important skill. It's important that you learn to evaluate whether your own proofs are correct.

- If you want to prove a statement, you need to provide a general argument. If you want to disprove a statement, you need to present a counter-example.

- Learning to prove mathematical statements is a skill that develops with practice. Be patient with yourself :)

If the statement that we are aiming to proof is a claim about existence of some object, then often we can prove the statement by constructing such an object.

Types of proofs–constructive proof example

Definition

For a natural number $k \in \mathbb{N}$, we call a graph $G = (V, E)$ a *k-regular graph* if every vertex in V has degree k.

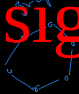
Theorem

For every even natural number $n \geq 4$, there exists a 3-regular graph with n vertices.

Proof

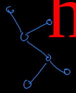
Types of proofs–constructi...

a 2-regular graph:



Definition

For a natural number $k \in \mathbb{N}$, we call a graph $G = (V, E)$ a *k-regular graph* if every vertex in V has degree k.

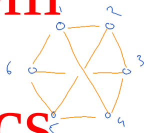


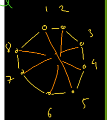
not a k-regular graph for any k

Theorem

For every even natural number $n \geq 4$, there exists a 3-regular graph with n vertices.

for claims of existence often "proof by construction" is a useful technique





Proof (by construction)

Let $n \geq 4$ be even, and define vertex set $V = [n] = \{1, 2, \dots, n\}$.

We define the following edge set:

$E = \{\{i, i+1\} \mid i \in \{1, \dots, n-1\}\} \cup \{\{1, n\}\}$
$\cup \{\{i, \frac{n}{2} + i\} \mid i \in \{1, 2, \dots, \frac{n}{2}\}\}$

This results in a graph, where every vertex has degree 3.

Sometimes, in order to prove that some statement is true, we assume that the statement is false and then show that this assumption leads to a contradiction. This, in turn, implies that the statement is true.

Types of proofs– "by way of contradiction"

Sometimes, in order to prove that some statement is true, we assume that the statement is false and then show that this assumption leads to a contradiction. This, in turn, implies that the statement is true.

To prove statement p, we show that

$((\neg p) \to F)$ is a true statement.

This tells us that $(\neg p)$ must be false, and thus the statement p must be true.

Types of proofs– examples of proofs "by way of contradiction"

Theorem

$\sqrt{2}$ is not a rational number.

Proof

See textbook.

Types of proofs– examples of proofs "by way of contradiction"

Theorem

There are infinitely many prime numbers.

Proof

Types of proofs– examples of proofs "by way of contradiction"

Theorem

There are infinitely many prime numbers.

Proof.

B.w.o.c. (by way of contradiction), let's assume the statement is false, that is that there are only finitely, say, $n \in \mathbb{N}$ many prime numbers. Let's call them $p_1, p_2, p_3, \dots, p_n$. (and let's assume $p_i > 1$ for all i).

Now, let's consider the number

$N = p_1 \cdot p_2 \cdot p_3 \cdots$ [illegible] none of the p_i divides

We have $N > p_i$ for all i, and none of the p_i divides N. Thus N must be a new prime number, a contradiction to the assumption that there are only n primes.

Thus, the assumption was false, and therefore there exist infinitely many prime numbers.

Types of proofs– examples of proofs “by way of contradiction”

Theorem

The set $\mathbb{R}$ of real numbers is not countable.

Proof

We’ll proves this in the tutorial on Friday.

We can use a proof by induction, if we want to prove a statement about elements of a set that is (or can be) defined inductively.

Inductive definition of sets – motivating example

Say, I'd like to define the set of all (biological) relatives of mine (living and dead ones).

- **I can not make a list**
  (I don't know them all, especially not those that lived a thousand years ago..)
- **I can not give a precise characteristic**
  (Maybe I could if I was a biologist, but I am not..)
- **But I know some operations that will allow me to get from me to all of them!**
  The idea is to start with me, and consider everyone that can be reached by successively considering all children and all parents of previously reached people.

Inductive definition of sets – motivating example

Here is a more formal way of defining all my biological relatives:

Consider the following three components:

1. **Universe:** all people
2. **Core set:** me
3. **Operations:** parent-of, child-of

The set of all my relatives: Start with me, and successively apply the operations parent-of and child-of. The set of all my relatives are all people that can be "reached" this way.

Inductive definition of sets – general pattern

An inductive definition of a set consists of

1. **A universe set** U
2. **A core set** $C \subseteq U$
3. **A finite set** $O = \{o_1, o_2, \dots o_n\}$ **of operations from** $o_i : U^{r_i} \to U$ **for some arities** $r_i \in \mathbb{N}$

We define $\mathcal{I}(U, C, O)$ as the set of elements that we obtain by starting with the core set and putting all those elements of U into $\mathcal{I}(U, C, O)$ that one can reach by successively applying the operations in O.

Structural induction–general definition

Consider some inductively defined set $\mathcal{A} = \mathcal{I}(U, C, O)$. To show that all elements of $\mathcal{A}$ satisfy property $\mathcal{P}$ we prove the following:

Base case Show that all elements $c \in C$ of the core set satisfy the property.

Induction hypothesis Assume that some $a_1, a_2, \ldots a_n \in I(U, C, O)$ satisfy the property (where n is the largest arity of the operations in O).

Induction step Show that for all operation $o_i \in O$, if the induction hypothesis holds, then the property also holds for

$$o_i(a_1, a_2, \ldots a_{r_i}).$$

- When proving something by (structural) induction, it is very important that you clearly state the hypothesis and make it clear to yourself where in the induction step you are actually using it. If it is not clear where you use it, there is likely something wrong with your proof..!

Game with cups

We consider three cups placed on a table as follows:

$$\cup \; \cap \; \cup$$

(That is, two upright and the middle one upside down.)

- We can now play with the cups by, at each step, flipping exactly two of them
- Eg, flipping the two left ones results in $\cap \; \cup \; \cup$

Question: Can we, by repeatedly flipping two cups, end up with all cups upright $\cup \; \cup \; \cup$?

Structural induction–example

First, we note that we can define the set of all reachable cup-configurations as an inductively defined set:

- Universe: $U_c =$All ways to place three cups on the table.
  (Question for you: How big is this universe?)

- Coreset: The initial configuration, $C_c = \{\bigcup \bigcap \bigcup\}$
- Operations: $O_c = \{$flip-left-two, flip-outer-two, flip-right-two$\}$

Question: Is $\bigcup \bigcup \bigcup \in \mathcal{I}(U_c, C_c, O_c)$?

Structural induction–example

First, we note that we can define the set of all reachable cup-configurations as an inductively defined set:

- Universe: U_c =All ways to place three cups on the table.
  (Question for you: How big is this universe?) → 8

- Preset: The initial configuration $C_c = \{\cup\cap\cup\}$
- Operations: $O_c = \{$flip-left-two, flip-outer-two, flip-right-two$\}$

→ This defines (inductively) the set of all reachable states in this game.

Question: Is $\cup\cup\cup \in \mathcal{I}(U_c, C_c, O_c)$?

we'll prove by induction, that the number of upside cups is always even.

Conjecture: It is not possible to get all cups upright..

We will prove the following property by induction:
In all reachable states, the number of upright cups is even.

Since $\cup\cup\cup$ has an odd number of upright cups, this will imply that this state is not reachable.

Structural induction–example

Proof by induction

Base case: in the initial configuration ∪∩∪, there are two (i.e. even number of) of up-cups.

Induction hypothesis: Assume XYZ is a configuration with even ~~num~~ number of up-cups.

Induction step: If we flip 2 of XYZ, there are three cases:

1) if we flip one up and one down cups, the number of up cups stays the same.

2) if we flip two up cups, then XYZ must have (even) two up cups (since even), thus, we will end up with zero up cups.

3) If we flip two down-cups, XYZ must have had 0 up cups and end up with 2 up cups

Thus the property is maintained under the operations, and therefore holds for all reachable configurations by induction.

Property: The number of upright cups is even.

Proof by in induction:

Base case In the initial configuration $\bigcup\bigcap\bigcup$, the property holds (2 cups are up, which is even).

Induction hypothesis Assume that for some configuration $XYZ \in \mathcal{I}(U_c, C_c, O_c)$ the number of up-cups is even.

Structural induction–example

Induction step First, note that if the number of up-cups in XYZ is even, it is either 0 or 2 (since these are the only even numbers smaller than 3). This observation yields the following case distinction:

Case 1: It is 0 Then flipping two cups results in 2 up-cups, which is even again.

Case 2: It is 2 Then we either flip the two up-cups in XYZ or we flip one up-cup and one down-cup. In the first case, we end up with 0 up-cups, which is even, in the second case, we maintain 2 up-cups.

Thus in all cases, the number of up-cups in flip-left-two(XYZ), flip-outer-two(XYZ), flip-right-two(XYZ) is even again.

Question for you: Where did we use the induction hypothesis?

Types of proofs–proof by induction

When we use a structural induction proof for the set of natural numbers, we often simply call it "proof by induction".

Example of proof by induction for natural numbers

Theorem

For a natural number $n \geq 1$, we let $S(n)$ denote the sum of the natural numbers up to n. Then the following equality holds:

$$S(n) = \frac{1}{2} \cdot n \cdot (n+1)$$

Proof

This is part of exercise 0.11, and we'll prove it in the Tutorial on Friday.

Example of proof by induction for natural numbers

Theorem

For a natural number $n \geq 1$, we let $S(n)$ denote the sum of the natural number up to n. Then the following equality holds:

$$S(n) = \frac{1}{2} \cdot n \cdot (n+1)$$

Inductive definition of $\mathbb{N}$:

Universe : real numbers $\mathbb{R}$

Core set : $\{0\}$

Operation : $O_{+1} : n \mapsto n+1$

$O_{+1}(n) = n+1$

You are screen sharing · Stop Share

Example of proof by induction for natural numbers

Mouse Select Text Draw Stamp Spotlight Eraser Format Undo Redo Clear Save

Who can see what you share here? Recording On

Talking:

Theorem

For a natural number $n \geq 1$, we let $S(n)$ denote the sum of the natural numbers up to n. Then the following equality holds:

$$S(n) = \frac{1}{2} \cdot n \cdot (n+1)$$

Defining integers $\mathbb{Z}$ inductively:

Universe: $\mathbb{R}$

Core-set: $\{0\}$

Operations:

$o_{+1}: n \mapsto n+1$

$o_{-1}: n \mapsto n-1$

Inductive definition of $\mathbb{N}$:

Universe: real numbers $\mathbb{R}$

Core set: $\{0\}$

Operations: $O_{+1}: n \mapsto n+1$

$O_{+1}(n) = n+1$

Regular Languages

Finite Automata

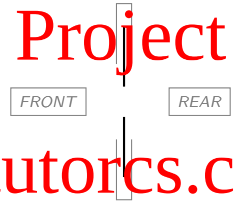
Reading: ITC Section 1.1

A finite automaton or finite state machine is a simple computational model.

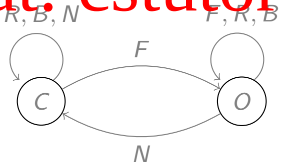
We will work with this model of computation for the next part of this course.

A simple automaton–sliding door example

Consider an automatic sliding door sliding door with two pads that receive signals if someone is standing on them:

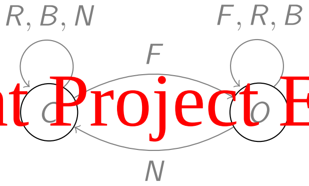


We can model the controller of the sliding door as a simple automaton:



Here we use: $C = CLOSED$, $O = OPEN$, $F = FRONT$, $R = REAR$, $B = BOTH$, $N = NEITHER$

A simple automaton–sliding door example



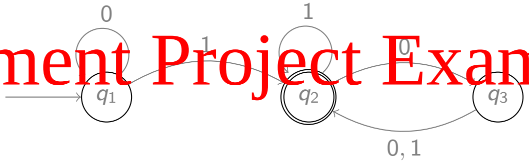
Here we use: $C = CLOSED$, $O = OPEN$, $F = FRONT$, $R = REAR$, $B = BOTH$, $N = NEITHER$

The behavior of the door can be described in terms of the following transition function:

	NEITHER	FRONT	REAR	BOTH
CLOSED	CLOSED	OPEN	CLOSED	CLOSED
OPEN	CLOSED	OPEN	OPEN	OPEN

State diagram of M_1

We can use a state diagram to describe a finite automaton M_1:



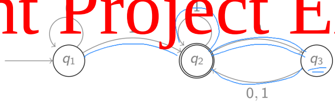
Interpretation of the state diagram: The arrow "coming out of nowhere" going into the leftmost state, signals, that this state is the start state. This automaton can read letters from the alphabet $\Sigma = \{0, 1\}$. Being in some state q, receiving letter σ, the computation finds the outgoing edge from q that has a label σ, and moves along that arrow to a new state.

Examples:

- If we feed the string 10010 to M_1, we move through the states $q_1, q_2, q_3, q_2, q_2, q_3$, and end up in state q_3, which is not an accept state.
- If we feed the string 1101 to M_1, we end up in state q_2, which is an accept state (accept states are the nodes with a double circle).
- If we feed the empty string ϵ to M_1, we end up in state q_1, which is not an accept state.

State diagram of M_1

We can use a state diagram to describe a finite automaton M_1:



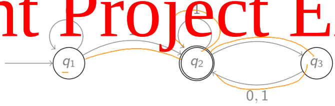
Interpretation of the state diagram: The arrow "coming out of nowhere" going into the leftmost state, signals, that this state is the start state. This automaton can read letters from the alphabet $\Sigma = \{0, 1\}$. Being in some state q, receiving letter σ, the computation finds the outgoing edge from q that has a label σ, and moves along that arrow to a new state.

Examples:

- If we feed the string 10010 to M_1, ~~a~~ results in q_3

State diagram of M_1

We can use a state diagram to describe a finite automaton M_1:



Interpretation of the state diagram: The arrow "coming out of nowhere" going into the leftmost state, signals, that this state is the start state. This automaton can read letters from the alphabet $\Sigma = \{0, 1\}$. Being in some state q, receiving letter σ, the computation finds the outgoing edge from q that has a label σ, and moves along that arrow to a new state.

Examples:

- If we feed the string 10010 to M_1, we move through the states $q_1, q_2, q_3, q_2, q_2, q_3$, and end up in state q_3, which is not an accept state.
- If we feed the string 1101 to M_1 → we end up in q_2 so this string is accepted.

Formal definition of a finite automaton

Definition

A finite automaton is a 5-tuple $(Q, \Sigma, \delta, q_0, F)$, where

1. Q is a finite set called the set of states,
2. Σ is a finite set called the alphabet,
3. $\delta : Q \times \Sigma \to Q$ is the transition function,
4. $q_0 \in Q$ is the start state, and
5. $F \subseteq Q$ is the set of accept states.

Formal definition of a finite

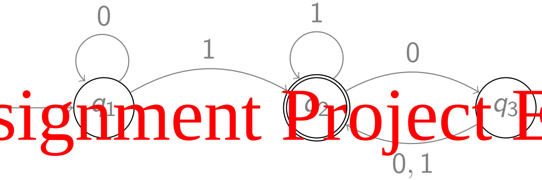
deterministic

Definition

A finite automaton is a 5-tuple $(Q, \Sigma, \delta, q_0, F)$, where

1. Q is a finite set called the set of states,
2. Σ is a finite set called the alphabet,
3. $\delta : Q \times \Sigma \to Q$ is the transition function,
4. $q_0 \in Q$ is the start state, and
5. $F \subseteq Q$ is the set of accept states.

Formal description of M_1



The above state diagram corresponds to the following formal description:
$M_1 = (Q, \Sigma, \delta, q_1, F)$, where

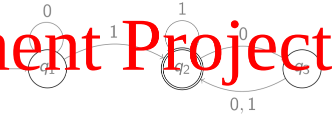
1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0, 1\}$,
3. δ is defined by the following table:

δ	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F \subseteq \{q_2\}$.

Given the description of an automaton, we can ask: which strings will lead to an accept state when fed into the automaton? As we have seen in the example computations with M_1 before, some strings do and others don't. The set of strings that do lead to an accept state form a language over Σ, the language of M_1.

Formal description of M_1



The above state diagram corresponds to the following formal description:
$M_1 = (Q, \Sigma, \delta, q_1, F)$, where

$Q = \{q_1, q_2, q_3\}$

$\Sigma = \{0, 1\}$

q_1 is the starting state

$F = \{q_2\}$

δ	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

Language accepted by an automaton

Let Σ be the alphabet of some automaton M. Then we let

$$L(M) = \{w \in \Sigma^k \mid k \in \mathbb{N} \text{ and } w \text{ is accepted by } M\}$$

denote the language of machine M. The is $L(M)$ is the set of all words over Σ that are accepted by machine M.

For the language $A = L(M)$ we also say machine M recognizes (or accepts) A.

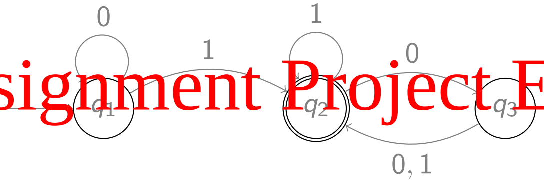
Formal definition of acceptance

Definition

Let $M = (Q, \Sigma, \delta, q_0, F)$ a finite automaton and $\mathbf{w} = w_1 w_2 \dots w_n$ a string over Σ. We say that M **accepts $\mathbf{w}$** if there exists a sequence $s_0 s_1 s_2 \dots s_n$ of states such that

1. $s_0 = q_0$,
2. $\delta(s_i, w_{i+1}) = s_{i+1}$ for $i = 0, 1, \dots, n_1$, and
3. $s_n \in F$

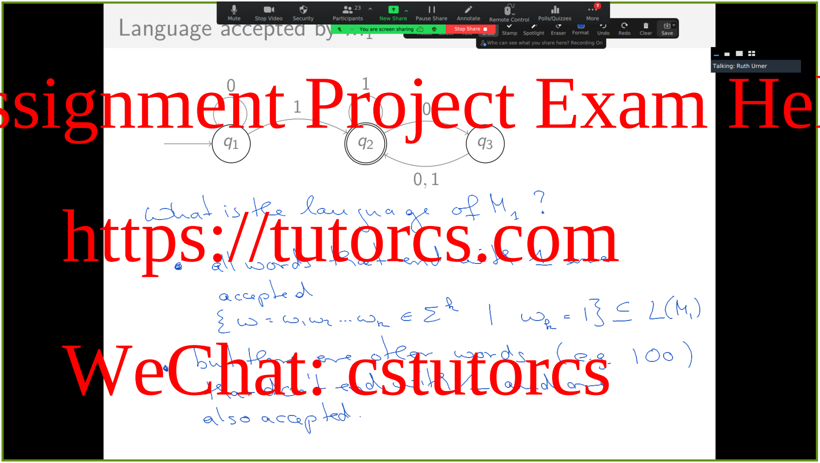
Language accepted by M_1



For the machine M_1 we get

$L(M_1) =$

Task for you: figure out what exactly is the set of words accepted by this automaton.


Language accepted by M_1
0
1
1
0
0, 1
q_1
q_2
q_3
What is the language of M_1?
all words that end with 1 are accepted
$\{ w = w_1 w_2 \dots w_k \in \Sigma^k \mid w_k = 1 \} \subseteq L(M_1)$
but there are other words (e.g. 100)
also accepted.
Talking: Ruth Urner