cs2001
Introduction to the Theory of Computation

Lecture 5

Ruth Urner

January 23, 2023

Logic

Reading: ITC Section 0.2

Propositional logic models the way we reason about the truth value of statements (propositions).

A propositional variable is a variable (that stands for a statement) that can take on one of two values:

- true (we also use T or 1 for true)
- false (we also use F or 0 for false)

A truth assignment is a function from a set P of propositional variables to the set of truth values $\{0, 1\}$ (or $\{T, F\}$).

Given basic propositi ments p and q we can use boolean operations to derive plex statements (and their truth values):

- $\neg$
- $\wedge$
- $\vee$
- $\rightarrow$
- $\leftrightarrow$
- $\oplus$

Truth values of composed statements

We define the truth values of composed propositional statements by the following truth table:

α	β	$(\neg\alpha)$	$(\alpha \vee \beta)$	$(\alpha \wedge \beta)$	$(\alpha \to \beta)$	$(\alpha \leftrightarrow \beta)$	$(\alpha \oplus \beta)$
T	T	F	T	T	T	T	F
T	F	F	T	F	F	F	T
F	T	T	T	F	T	F	T
F	F	T	F	F	T	T	F

Say, we have propositional variables p and q, and a formula $\alpha = ((p \to q) \vee (q \to p))$ and a truth assignment v that sets p to T and q to F.

To figure out the truth value of α under this assignment, we build a truthtable with one column for every element in a construction sequence of α as follows:

	p	q	$(p \to q)$	$(q \to p)$	$((p \to q) \vee (q \to p))$
v	T	F	F	T	T

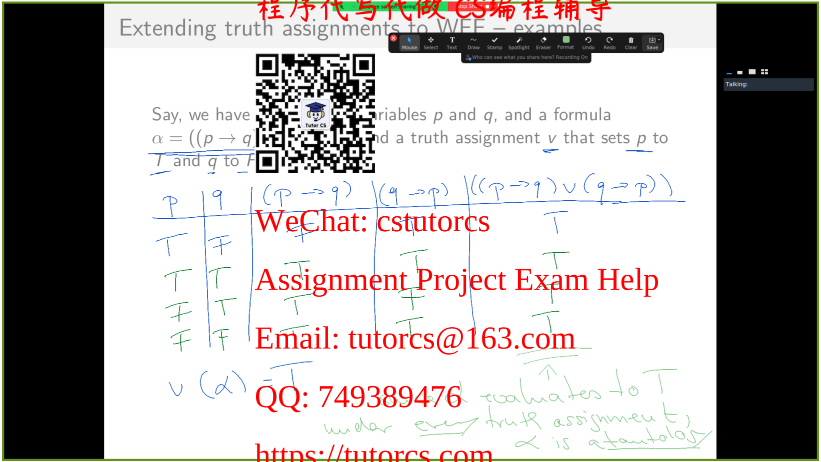
We start with filling the first columns using the truth assignment v and then successively fill the other columns using the truth table for the connectives.

Extending truth assignments to WFF – examples

Say, we have ... riables p and q, and a formula $\alpha = ((p \to q)$ ... nd a truth assignment v that sets p to T and q to F

p	q	$(p \to q)$	$(q \to p)$	$((p \to q) \vee (q \to p))$
T	F	F		T

$v(\alpha) = T$


Extending truth assignments to WFF – examples
Say, we have
riables p and q, and a formula
α = ((p → q)
nd a truth assignment v that sets p to
T and q to F
p q (p → q) (q → p) ((p → q) ∨ (q → p))
T F T
T T T T T
F T T F T
F F T T T
v(α) = T
evaluates to T
under every truth assignment,
α is a tautology

Logical equivalence

Definition: We call two propositional formulas (statements) α and β logically equivalent if they have the same truth table (that is, they evaluate to the same truth value under all truth assignments).

Show that the following pairs of formulas α and β are logically equivalent:

- $\alpha = p$ and $\beta = (\neg(\neg p))$
- $\alpha = (p \to q)$ and $\beta = ((\neg q) \to (\neg p))$
- $\alpha = (\neg(p \land q))$ and $\beta = ((\neg p) \lor (\neg q))$
- $\alpha = (\neg(p \lor q))$ and $\beta = ((\neg p) \land (\neg q))$

Exercises

Show that th[illegible] of formulas α and β are logically equivalent:

If it rains then the street is wet.

- $\alpha = p$ and $\beta = (\neg(\neg p))$

If the street is not wet, I can conclude that it's not raining.

- $\alpha = (p \to q)$ and $\beta = ((\neg q) \to (\neg p))$

p	q	$(p \to q)$	$(\neg p)$	$(\neg q)$	$((\neg q) \to (\neg p))$
T	T	T	[illegible]	[illegible]	[illegible]
T	F	F	F	T	F
F	T	[illegible]	[illegible]	[illegible]	[illegible]
F	F	T	T	T	T

Talking: Ruth Urner

Exercises

Show that th[illegible]s of formulas α and β are logically equivalent:

- $\alpha = p$ and $\beta = (\neg(\neg p))$
- $\alpha = (p \rightarrow q)$ and $\beta = ((\neg q) \rightarrow (\neg p))$ Exercise!
- $\alpha = (\neg(p \wedge q))$ and $\beta = ((\neg p) \vee (\neg q))$ prove these!
- $\alpha = (\neg(p \vee q))$ and $\beta = ((\neg p) \wedge (\neg q))$

Talking: Ruth Urner

More exercises

Show that the following pairs of formulas α and β are logically equivalent:

- $\alpha = (p \vee q)$ and $\beta = (\neg((\neg p) \wedge (\neg q)))$
- $\alpha = (p \rightarrow q)$ and $\beta = ((\neg p) \vee q)$
- $\alpha = (\neg(p \rightarrow q))$ and $\beta = (p \wedge (\neg q))$
- $\alpha = (p \leftrightarrow q)$ and $\beta = ((p \rightarrow q) \wedge (q \rightarrow p))$
- $\alpha = (p \oplus q)$ and $\beta = (\neg(p \leftrightarrow q))$

More exercises

Show that the pairs of formulas α and β are logically equivalent:

- $\alpha = (p \vee q)$ and $\beta = (\neg((\neg p) \wedge (\neg q)))$
- $\alpha = (p \to q)$ and $\beta = ((\neg p) \vee q)$
- $\alpha = (\neg(p \to q))$ and $\beta = (p \wedge (\neg q))$
- $\alpha = (p \leftrightarrow q)$ and $\beta = ((p \to q) \wedge (q \to p))$
- $\alpha = (p \oplus q)$ and $\beta = (\neg(p \leftrightarrow q))$

Exercise: prove these equivalences.

Show that the following pairs of formulas α and β are not logically equivalent:

- $\alpha = (p \vee q)$ and $\beta = (\neg(p \wedge q))$
- $\alpha = (p \rightarrow q)$ and $\beta = ((\neg p) \rightarrow (\neg q))$
- $\alpha = (p \oplus q)$ and $\beta = (p \vee q)$

More exercises

Show that the pairs of formulas α and β are **not logically equivalent**:

- $\alpha = (p \lor q)$ and $\beta = (\neg(p \land q))$

We know β is logically equivalent to $\gamma = (q \to p)$

Thus we now also showed that α and γ are not logically equivalent.

- $\alpha = (p \to q)$ and $\beta = ((\neg p) \to (\neg q))$

p	q	$(p \to q)$	$(\neg p)$	$(\neg q)$	$((\neg p) \to (\neg q))$
T	T	T	F	F	T
T	F	F	F	T	T
F	T	T	T	F	F
F	F	T	T	T	T

there is a truth assignment for which the truth values of the two formulas differ hence they are not logically equivalent!

Talking: Ruth Urner

More exercises: Show the distributive laws

Show that the follow[illegible] of formulas α and β are logically equivalent:

- $\alpha = (p \wedge (q \vee r))$ and $\beta = ((p \wedge q) \vee (p \wedge r))$

- $\alpha = (p \vee (q \wedge r))$ and $\beta = ((p \vee q) \wedge (p \vee r))$

These two logical equivalences are called distributive laws of propositional logic.

More exercises: Show the distributive laws

Show that the pairs of formulas α and β are logically equivalent:

have identical evaluations for all truth assignments

- $\alpha = (p \wedge (q \vee r))$ and $\beta = ((p \wedge q) \vee (p \wedge r))$

p	q	r	$(q \vee r)$	$p \wedge (q \vee r)$	$(p \wedge q)$	$(p \wedge r)$	β
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

$2^3 = 8$ possible truth assignments for 3 variables

Talking:

Tautologies and contradictions

We call a propositional formula a tautology if it evaluates to true under every truth assignment.

We call a propositional formula a contradiction if it evaluates to false under every truth assignment.

Tautologies and contradictions

We call a pro... ...ula a tautology if it evaluates to true under every t... ...

Example: ... $(\neg p))$

We call a propositional formula a contradiction if it evaluates to false under every truth assignment.

Example: $(p \wedge (\neg p))$

Extending truth assignments to WFF – examples

Say, we have [QR code] variables p and q, and a formula $\alpha = ((p \to q)$ [QR code] nd a truth assignment v that sets p to T and q to F

p	q	$(p \to q)$	$(q \to p)$	$((p \to q) \vee (q \to p))$
T	F	F		T
T	T	T	T	T
F	T	T	F	T
F	F	T	T	T

$v(\alpha) = T$

α evaluates to T under every truth assignment, α is a tautology

First order/Predicate logic–motivation

Assumptions:
- All people are mortal
- I am a person

(Sad) **Conclusion:**
- I am mortal

Question: Can propositional logic explain the pattern used in this example of reasoning?

Answer: No. Propositional logic can only relate truths or falsehood of statements as a whole. It does not provide as a means of reasoning about objects and properties that these objects may have.

First order/Predicate logic–motivation

Assumptions:
- All people are mortal
- I am a person

(Sad) **Conclusion:**
- I am mortal

To explain this example of reasoning, we need means to refer to the inner structure of these statements (not just the statements as a whole). First order logic allows us to

- refer to objects (for example people)
- state that objects have certain properties (for example being mortal)
- make statements about relationships between objects
- quantify over objects (for example state that something holds for all (all people are mortal) objects or that there exists an object that has a certain property)

In mathematical reas[illegible] make statements that quantify over objects, for example:

- **Definition:** A g[illegible] (V, E) is connected, if for every pair of vertices $v_1, v_2 \in V$ there exists a path from v_1 to v_2.

- To express that there are infinitely prime numbers, we say: For every prime number p, there exists a prime number p' with $p' > p$.

- If I want to show that some propositional formula is not a tautology, I need to show that there exists truth assignment to its variables, for which α evaluates to false.

In general, I recommend that you **spell out** mathematical statements and proofs in the **English language**.

Sometimes, it is useful to have some shorthand for statements. We use

- the symbol $\forall$ to stand for **for all**, and
- the symbol $\exists$ to stand for **there exists**.

First order/Predicate logic–negating statements with quantifiers

It is important to rea[illegible] when we negate statements in first order logic the two q[illegible] $\forall$ and $\exists$ "change roles":

- $\neg(\forall x\ P(x))$ is equivalent to $\exists x\ (\neg P(x))$
- $\neg(\exists x\ P(x))$ is equivalent to $\forall x\ (\neg P(x))$

First order/Predicate logic–negating statements with quantifiers

It is important [...]t, when we negate statements in first order logic th[...]s $\forall$ and $\exists$ "change roles":

- $\neg(\forall x\ P(x))$ is equivalent to $\exists x\ (\neg P(x))$

Example: [...] having population larger than 1 000 000.

It's not [...] population larger than 1000 000.

There exist a city with less than 1000 000 inhabitants.

First order/Predicate logic–negating statements with quantifiers

It is importan t, when we negate statements in first order logic th s $\forall$ and $\exists$ "change roles":

- $\neg(\forall x\ P(x))$ is equivalent to $\exists x\ (\neg P(x))$

- $\boxed{\neg(\exists x\ P(x))}$ is equivalent to $\boxed{\forall x\ (\neg P(x))}$

There does not exist a student in my class that is confused.

All students in my class are not confused.

Talking: Ruth Urner

First order/Predicate logic–negating statements with quantifiers

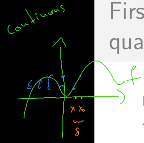
Example: The definition of continuity for a function $f : \mathbb{R} \to \mathbb{R}$ at a point $x_0 \in \mathbb{R}$ can be compactly written as follows:

$$\forall \epsilon > 0 \; \exists \delta > 0 \; \forall x \in \mathbb{R} \; (|x - x_0| < \delta \to |f(x) - f(x_0)| < \epsilon)$$

To prove that function $f : \mathbb{R} \to \mathbb{R}$ is not continuous in x_0, we need to show:

$$\exists \epsilon > 0 \; \forall \delta > 0 \; \exists x \in \mathbb{R} \; (|x - x_0| < \delta \land |f(x) - f(x_0)| \geq \epsilon)$$

First order/Predicate logic–negating statements with quantifiers

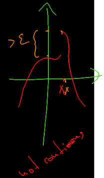


Example: The uity for a function $f : \mathbb{R} \to \mathbb{R}$ at a point $x_0 \in \mathbb{R}$ can be c s follows:

$\forall \epsilon >$ $(|x - x_0| < \delta \to |f(x) - f(x_0)| < \epsilon)$

To prove that function $f : \mathbb{R} \to \mathbb{R}$ is not continuous in x_0, we need to show:

$$\exists \epsilon > 0 \forall \delta > 0 \exists x \in \mathbb{R} \, (|x - x_0| < \delta \wedge |f(x) - f(x_0)| \geq \epsilon)$$



Talking: Ruth Urner

Mathematical statements and proofs

Reading: ITC Section 0.3 andd 0.4

Definition

A statement that cle[illegible]es an object/structure/concept based on previously d[illegible]ms.

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..

Definition
A statement [illegible] nes an object/structure/concept based on prev[illegible] erms.

Theorem
A statement that has been proven to be true.

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

what not to do: "proof by example"

Example: "[illegible] natural numbers are prime"

~~"proof" (by example): 1, 3, 5, 7, ...~~

To refute a statement [illegible], a counter-example is a sufficient proof.

Counter-example to the claim: 9 is odd and $9 = 3 \cdot 3$ is not prime. Thus the claim is false.

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 alway[illegible]ure you understand the statement fully.

- When you attempt [illegible]mething, I recommend to always first develop an intuitio[illegible]tement 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 :)

Types of proofs–constructive proofs

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.

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.

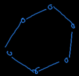
Proof

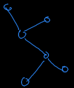
Types of proofs–constructi

Definition

For a natural ... we call a graph $G = (V, E)$ a k-regular gra... x in V has degree k.

a 2-regular graph:





not a k-regular graph for any k

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

Theorem

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

Proof (by construction).

Let $n \geq 4$ ... and ...

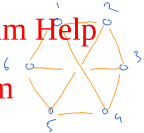
vertex set $V = [n] = \{1, 2, \ldots, n\}$.

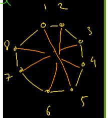
We define the following

$$E = \{\{i, i+1\} \mid i \in \{1, \ldots, n-1\}\} \cup \{\{n, 1\}\}$$

$$\cup \{\{i, \tfrac{n}{2} + i\} \mid i \in \{1, 2, \ldots, \tfrac{n}{2}\}\}$$

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





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.

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

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

This then lets us conclude that $(\neg p)$ must be false, and thus statement p must be true.

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

Theorem

$\sqrt{2}$ is not a rational

Proof

See textbook.

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

Theorem

There are infinitely m[illegible]e numbers.

Proof

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

Theorem

There are infi[illegible]me numbers.

Proof

B.w.o.c. (by way of contradiction), let's assume the [illegible] is false, that is that there are only finitely, say $n \in \mathbb{N}$, many prime numbers [illegible] p_n.

(and let's assume $p_i > 1$ for all i).

Now, let's [illegible]

$$N = (p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n) + 1$$

We have N [illegible] 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.

Talking: Ruth Urner

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

Theorem

The set $\mathbb{R}$ of real nu[illegible]ot countable.

Proof

We’ll proves this in the tutorial on Friday.

Types of proofs–proof by (structural) induction

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 f all (biological) relatives of mine (living and dead ones

- **I can not make**
  (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 forma[illegible]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** $O = \{o_1, o_2, \ldots, o_n\}$ **of operations from** $o_i : U^{r_i} \rightarrow U$ **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 $\mathcal{A}$ have 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

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

Structural induction

- 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 on a table as follows:

$$\cap \quad \cup$$

(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 w[illegible]ne the set of all reachable cup-configurations as [illegible]tively 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 [illegible] define the set of all reachable cup-configura[illegible]ctively 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, $C_c = \{\cup\cap\cup\}$
- 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 $\cup\cup\cup \in \mathcal{I}(U_c, C_c, O_c)$?

→ No!

|| we'll prove that the number of upside cups is always even. ||

Structural induction–example

Conjecture: It is not [illegible]o get all cups upright..

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

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

Structural induction—example

2) if we flip the two up cups, then X/Y/Z must have had two up cups (since even), thus we end up with zero up-cups.

3) If we flip two down-cups X/Y/Z must have had 0 up-cups and end up with 2 up cups

Proof by

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

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

Induction step: for a flip of XYZ, there are three cases: 1) if we flip one up and one down, the number of up cups stays the same.

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

Structural induction–example

Property: The numb[illegible]ght cups is even.

Proof by in induction:

Base case In the initial configuration $\sqcup \cup \cap \cup \sqcup$, 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 (si[illegible] the only even numbers smaller than 3). This observati[illegible] 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.