GB13604 - Maths for Computer Science

Lecture 1 – Introduction to Proofs

Claus Aranha
caranha@cs.tsukuba.ac.jp

College of Information Science

2020-10-07

Last updated October 3, 2020

Lecture 1 – Outline

In this lecture, we introduce the concept of **mathematical proofs**:

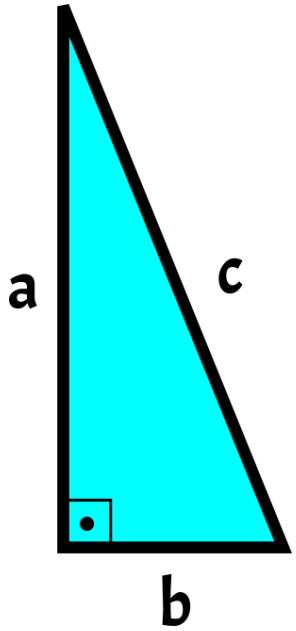
- **Section 1:** What are proofs, and why we need them;
- **Section 2:** Some proof methods;
- **Section 3:** Logical formulas and satisfiability;

This lecture covers the textbook's chapters 1, 2 and 3.

Part 1: Introduction to Proofs.

What is a proof?

Some concepts are easy to understand, but not easy to show that they are true.



- Pythagoras Theorem:

$$a^2 + b^2 = c^2$$

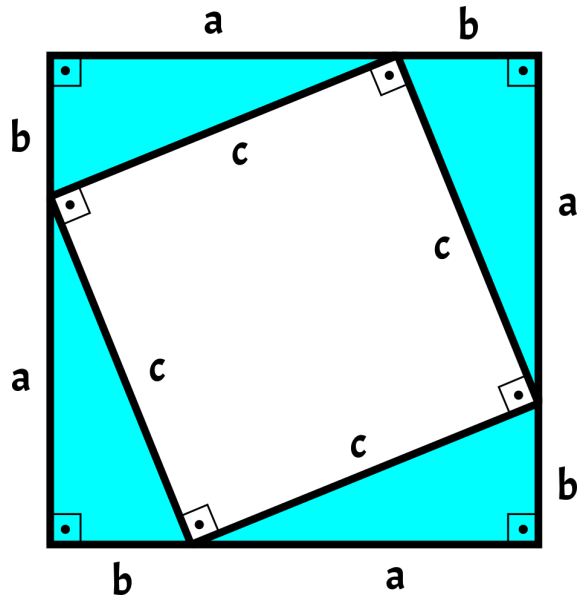
- It is easy to show this is true for **any one triangle**.
- But how do you show it is is true for **all** triangles?

The proof of the Pythagoras theorem is not obvious: there are more than 100 different proofs!

What is a proof?

One Pythagoras Proof

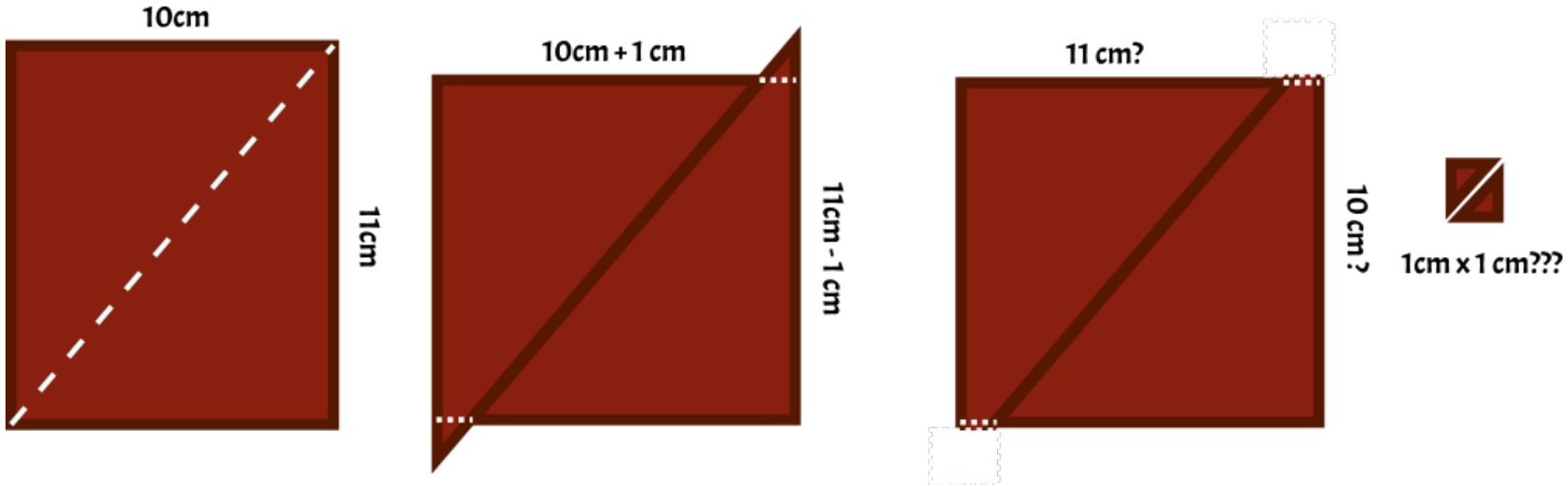
- **Proof**: by geometric construction
- Arrange four identical triangles;
- Show that internal angles are right;
- Internal square area: c^2
- External square area: $(a+b)^2$
- $(a+b)^2 = c^2 + 4(\text{area triangle})$
- $(a+b)^2 = c^2 + 4(\frac{ab}{2})$
- $a^2 + 2ab + b^2 = c^2 + 2ab$
- $a^2 + b^2 = c^2$ ■



Remember: There are many other possible proofs.
(Beautiful proofs, short proofs, wrong proofs, etc.)

False Proofs

Infinite Chocolate!



- What is wrong with the proof above?
- Be careful! A false proof can have many correct steps, and **only one** impossible step.

We can use proofs to show that something is **incorrect** as well!

Proofs and Computer Science

Why are proofs important for Computer Science?

- We don't use proofs only for mathematical equations.
- We can use proofs to **show that a program is correct**. (or incorrect)

- Example cases:
  - Use proofs to show that the result of a program is correct for any input;
  - Use proofs to show that one type of input will cause a bug in the program;
  - Use proofs to show that a program finishes in N steps;

Proofs and Computer Science

Example:

- Is the program below correct or incorrect?
- Can you show by using a proof?

```
int triangle_type(int a, int b, int c)
  // a, b, c are the length of the sides of a triangle
  if (a == b)
    if (b == c)
      return "all sides are equal";
    else
      return "two sides are equal";
  else if (b == c)
    return "two sides are equal";
  else
    return "all sides are different";
```

Proof Concepts

Propositions

A proposition is a statement that is either True or False, and nothing else.

Proposition

- $2 + 3 = 5$
- $1 + 1 = 3$
- $513 \times 435 = 223165$
- There is no human taller than 3 meters.
- It rained on October, 3rd, 2020, 10:00 in Tokyo.
- Emacs is better than Vim.

Not proposition

- What is 2×8?
- Please give me cake.
- It is raining now.

Proof Concepts

Predicates

A predicate is a kind of proposition where the truth value depends on one or more variables:

- $P(n)$: n is a prime number;
- $L(N)$: The name N has five letters;
- $M(x, y)$: x and y are members of the same group;

Do not confuse predicates and number expressions!

Numeric expressions have numeric values, predicates have True or False values.

- $p(x) = x^2 + 3x + 1$. This is a numeric expression;
- $P(X)$: $p(x + 1) = p(x) + x + 1$. This is a predicate;
- $P(X)$ is True for any $x \geq 0$. This is a proposition;

Proof Concepts

Implication (IF)

An implication is a particular type of predicate that we use a lot, so it is important to know it well:

$$P \implies Q$$

There are many ways to describe the implication:

- $I(P, Q)$: If P is true, Q is true;
- $I(P, Q)$: When P is true, Q is true;

We usually don't write the $I(P, Q)$ part, but it is important to remember that the implication itself is a predicate.

- Be Careful! When P is false, Q could be anything.
- A related predicate is **If and only If (iff)**:
  - IFF(P,Q): $P \implies Q$ AND $Q \implies P$.
  - also written as $P \iff Q$

Proof Concepts

Proof Methods

How do we prove something?

Proposition

For every nonnegative integer n, the value of $p(n) = n^2 + n + 41$ is prime.

We could try to test values of n one by one:

$$p(0) = 41, \text{ prime; } p(1) = 43, \text{ prime; } p(2) = 47, \text{ prime; } \ldots,$$
$$p(20) = 461, \text{ prime...}$$

- When do we stop?
- ($p(40) = 41 \times 41$, is not prime...)

We need better ways to prove propositions!

Part 2: Proof Methods

Inference Rules

Inference (or logic deductions) are used to prove new propositions by using propositions that have been proposed before.

We normally write an inference as follows:

$$\frac{P, Q, R}{X}$$

This means "propositions P, Q, R are true, meaning that proposition X is true".

Inference Rules are inferences that are particularly useful to build proofs. Let's see a few:

Inference Rules

Modus Ponens

The *Modus Ponens* inference rule is:

$$\frac{P, P \implies Q}{Q}$$

If P is true, and P implies Q is true, then Q is true.

A few other related inference rules:

$$\frac{P \implies Q, Q \implies R}{P \implies R}, \frac{not(P) \implies not(Q)}{Q \implies P}$$

So one way to prove a proposition is to **start with propositions that you know are true** and **use inference rules to reach the proposition you want to prove**.

Proving an Implication

Direct Proof

The *Modus Ponens* rule says that:

$$\frac{P, P \implies Q}{Q}$$

To prove Q, we have to prove that P, and that P **implies** Q.

We can prove an implication directly, by assuming P is true, and showing that Q must be true, step by step.

Proving an Implication

Direct Proof

Theorem: If $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$

Proof.

- Let's assume $0 \leq x \leq 2$
- We can rewrite $-x^3 + 4x$ as $x(2 - x)(2 + x)$
- If $0 \leq x \leq 2$, then x, $(2 - x)$, $(2 + x)$ are all positive.
- $x(2 - x)(2 + x) \geq 0$
- $x(2 - x)(2 + x) + 1 > 0$
- $-x^3 + 4x + 1 > 0$

□

Proving an Implication

Contrapositive

Another way to prove an implication is to "prove the contrapositive". This means using the following inference rule:

$$\frac{\text{NOT}(Q) \implies \text{NOT}(P)}{P \implies Q}$$

So if we show that when Q is false, then P is always false, it is equivalent to show that when P is true, then Q is always true.

Proving an Implication

Contrapositive

Theorem: if r is irrational, then $\sqrt{r}$ is also irrational.

Proof.

We prove the contrapositive: If $\sqrt{r}$ is rational, then r is also rational.

- If $\sqrt{r}$ is rational, then $\sqrt{r} = \frac{m}{n}$.
- m and n are integers (definition of rational numbers)
- Square both sides: $r = \frac{m^2}{n^2}$.
- m^2 and n^2 are also integers, so r is rational.

□

Proving "If and only If"

Remember that "If and only If" can be defined as:

$$\frac{P \implies Q, Q \implies P}{P \iff Q}$$

So to prove $P \iff Q$, we can first prove the implication from P to Q, and then prove the implication from Q to P.

This is useful to show equivalence between two mathematical statements.

Proof By Cases

Example

Let's say you are refactoring code, and you want to profe that the two code samples below are equivalent. How would you do it?

Code 1

```
If (X > 0 OR (X <= 0 AND Y > 100))
  print("Hello!")
```

Code 2

```
If (X > 0 OR Y > 100)
  print("Hello!")
```

Proof By Cases

Definition

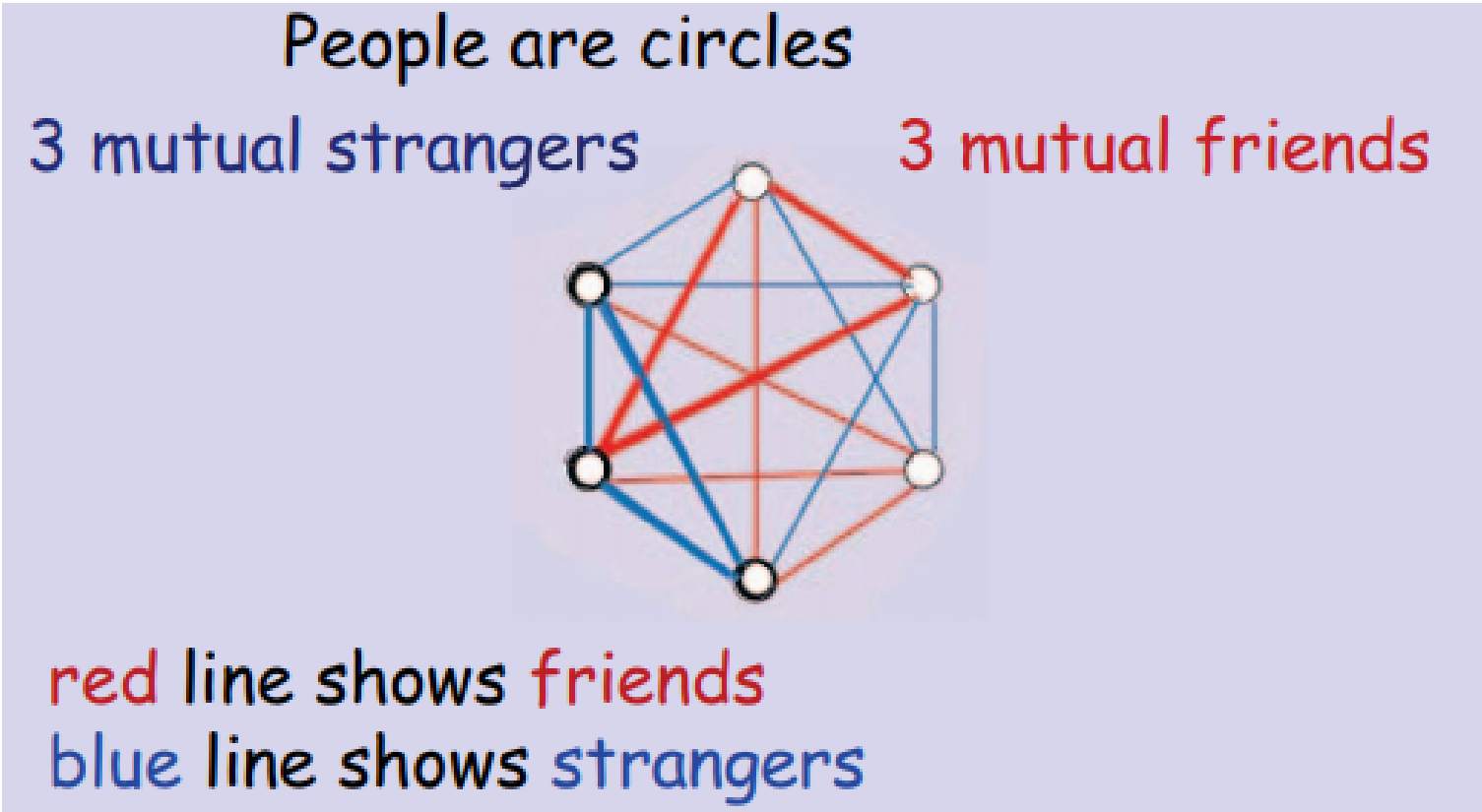
Proof By Cases, is a proof technique that uses the idea of "divide and conquer".

You break one complicated problem into easier, smaller sub-problems.

Important! When you create the cases, make sure that all possible cases are covered!

Example: Friends and Strangers

Theorem: In a group of 6 people, where **every pair** is either a friend or a stranger, then we **always** have at least a set of 3 mutual friends or a set of 3 mutual strangers.



Example: Friends and Strangers

Proof.

The proof is by case analysis. Let "A" be one of the six people. There are two cases:

1. Among the 5 other people, at least 3 are friends with A;
2. Among the 5 other people, at least 3 are strangers with A;

Let's assume case (1). Let's call the three friends B, C, D. There are two subcases:

A. B-C, C-D, or B-D are friends. We have now 3 mutual friends with A and the pair here.

B. B-C, C-D and B-D are strangers. This makes a 3 mutual strangers set with the three pairs.

This means that in case 1, the theorem holds. It is easy to see that case 2 is symmetrical to case 1. □

A WRONG Proof By Cases

Theorem: $2a^2 > a$, for all $a \in \mathbb{Z}$.

Proof.

The proof is by case analysis.

1. Case 1: $a > 0$;
   - $2a^2$ is equal to $2a \times a$
   - Since $a > 0$ and $a \in \mathbb{Z}$, then $a \geq 1$
   - $2 \times 1 \times 1 > 1$
2. Case 2: $a < 0$
   - Since $a < 0$ and $a \in \mathbb{Z}$, then $a \leq 1$
   - For any negative a, a^2 is positive, so $a^2 > a$.

Because the theorem holds for case (1) and case (2), it holds for all possible cases. □

What is wrong with this proof?

Proof By Contradiction

Definition

"Proof by Contradiction" is a technique where you show that **the negative of the theorem implies a false fact to be true**.

For a simple example: "If gravity did not exist, then we would all be flying. Since we are not flying, then gravity must exist."

Sometimes, it can be easy to create a proof by contradiction by finding a good counter-example. Other times, we have to find an absurd consequence of the negative.

Use "Proof by Contradiction" to prove the following theorem:
Theorem: $\sqrt{2}$ is an irrational number.

Proof by Contradiction

Example

Proof.

We use proof by contradiction, and assume $\sqrt{2}$ is rational.

1. $\sqrt{2} = \frac{m}{n}$; $m, n \in \mathbb{Z}$; $n \neq 0$, and m, n have no common factors.
2. $n\sqrt{2} = m$ and squaring both sides give $2n^2 = m^2$.
3. m^2 is even (because $n^2 = \frac{m^2}{2}$)
4. If m^2 is even, then m is even too. So $m = 2k$ for some integer k.
5. So, $2n^2 = (2k)^2$, which leads to $n^2 = 2k^2$.
6. Following the logic of (3) and (4), n^2 is even, and n is even too.
7. However, if m and n are even, it is a contradiction with (1).

□

Well Ordering Principle

Definition

The Well Ordering Principle (WOP) is a very useful principle in mathematics, that can also look a little bit "obvious":

Every non-empty set of
Non-negative Integer Numbers ($\mathbb{Z}^+$)
has one smallest element

Well Ordering Examples

- What is the smallest age among students in Tsukuba?
- What is the smallest number of coins that adds to 876 yens?
- What are the smallest integers m and n so that $x = \frac{m}{n}$?

Well Ordering Principle Proof Example

We can re-write the proof that $\sqrt{2}$ is irrational using WOP.

Proof.

1. $\sqrt{2} = \frac{m}{n}$; $m, n \in \mathbb{Z}$; $n \neq 0$;
2. By WOP, there is a **smallest** m and n so that $\sqrt{2} = \frac{m}{n}$
3. $n\sqrt{2} = m$ and squaring both sides give $2n^2 = m^2$.
4. m^2 is even (because $n^2 = \frac{m^2}{2}$)
5. If m^2 is even, then m is even too. So $m = 2k$ for some integer k.
6. So, $2n^2 = (2k)^2$, which leads to $n^2 = 2k^2$.
7. Following the logic of (4) and (5), n^2 is even, and n is even too.
8. If m and n are even, then $\sqrt{2} = \frac{m/2}{n/2}$, and $m/2$, $n/2$ are smaller than m, n, contradicting the WOP.

□

Why is the WOP useful?

General form for a WOP proof

The WOP gives us a general framework to produce proofs by contradiction:

- Structure your theorem around predicate $P(n)$, where $n \in \mathbb{N}$.
- Define a set C of counter examples, so that $C ::= \{n \in \mathbb{N} | P(n) \text{ is false}\}$.
- By WOP, consider the minimum element $m \in C$.
- Find a contradiction, for example:
  - if m exists, then it implies in the existence of a smaller element $m' < m, m' \in C$.
  - if m exists, then actually $P(m)$ is true, and m is not actually in C.
- Therefore, the minimum element m does not exist, the counter example set C does not exist, and $P(n)$ is true for all n.

WOP Proof examples:

Let's see two quick examples of proofs using WOP. Try doing these two proofs by yourself first:

- **Theorem:** Every $n > 1, n \in \mathbb{N}$ is a product of prime numbers.
- **Theorem:** For every $n \in \mathbb{N}$, $P(n) : n + 8 = 5a + 3b; a, b \in \mathbb{N}$. (for every n, $n + 8$ is composed of a sum of 3s and 5s)

WOP Proof example I: Prime factors

Theorem: Every integers bigger than 1 is a product of prime numbers.

Proof.

Proof by contradiction using the WOP.

- Assume, by WOP, that m is the smallest $\mathbb{N}$ that is not a product of prime numbers.
- Obviously m is not a prime, so $m = a_1 a_2 \ldots a_n$, where a_i is not prime.
- Is a_i a product of prime numbers?
  - If a_i is a product of prime numbers, then $a_i = p_1 p_2 \ldots p_n$, and m is now a product of prime numbers (contradiction)
  - If a_i is not a product of prime numbers, then m is not the **smallest** product of prime numbers. (contradiction)

□

WOP Proof example II: Postal Numbers

Theorem:

For every n, $n + 8$ is composed of 3s and 5s.

Proof.

Proof by contradiction using the WOP

- First, we quickly verify that $P(n)$ is true for 0..8
- By WOP, we assume that there is some minimum $m > 8$ where $P(m)$ is false.
- If $P(m)$ is false, then $m + 8$ cannot be composed of 3s and 5s.
- If m is minimum, then $P(m - 8)$ is true, and m is composed of 3s and 5s.
- If m is composed of 3s and 5s, then $m + 8$ is $m + 3 + 5$, and $P(m)$ is true! (Contradiction)

□

Propositions and Logic

Why Mathematical Language?

- Greeks carry swords or javelins.
- Greeks carry bronze or copper swords.

Mathematical Language

- Mathematical Language helps create non-ambiguous statements.
- We will not through all Logic operators here.
- However, it is important to understand that they are based on binary or boolean logic.

Mathematical Language / Binary Logic

Example: X XOR Y

X	Y	X XOR Y
TRUE	TRUE	FALSE
TRUE	FALSE	TRUE
FALSE	TRUE	TRUE
FALSE	FALSE	FALSE

- A Truth Table is a way to understand a logic operator.
- We can use logic operators to transform ambiguous natural language sentences into clear logical propositions.
  - Greeks carry bronze or copper swords.
  - Greek carry bronze sword XOR greek carry copper sword.

Binary Logic and Truth Tables

The truth table allows us to analyze a logical formula:

- Is it always true? Is it always false?
- Is it equivalent to another logical formula?

To analyze a formula using the truth table, I need to analyse the value of each variable.

Evaluation of a Formula

Given the following variables:
P = True, Q = True, R = False

How do we evaluate the following formula?

NOT(NOT(P) OR Q) AND (R OR (P XOR Q))

Comparison of Two Formulas

We can decide whether two logical formulas are equivalent if the final column of their truth table is identical.

For example, let's prove DeMorgan's Law:

NOT(P OR Q) equiv to NOT(P) AND NOT(Q)

Satisfiability and Validity

- A logic formula is satisfiable if it is true for at least one assignment.
- A logic formula is valid if it is true for all assignments.

- Satisfiable: NOT(B)
- Not Satisfiable: B AND NOT(B)
- Valid: B OR NOT(B)

Checking for Validity and Satisfiability

Checking if a logic formula is satisfiable or not is a very importan problem in CS.

But how to do it?

Alert! If you try to use a truth table, the size of the table grows with the number of variables:

- 1 variable - 2 lines
- 2 variables - 4 lines
- 10 variables - 1024 lines
- n variables - 2^n lines...

Checking for Validity and Satisfiability

- Is there an efficient way to test for satisfiability? (SAT)
- The Efficient SAT problem is equivalent to the P=NP problem
- The validity problem is also related to the SAT problem.

Logic Quantifiers

- For all: $\forall$
- Exists: $\exists$

What is a Predicate?

A predicate is a proposition with variables in it:

$$P(X, Y) ::= [X + 2 = Y]$$

The truth value of a predicate depends on the values of the variables:

- $X = 1$, $Y = 3$, P(X,Y) is True
- $X = 2$, $Y = 2$, P(X,Y) is False

Quantifiers

- $\forall x$ – For ALL X
- $\exists y$ – There exists SOME Y

$\forall x$ works like AND. For example:

$$\forall x, x \in \{1, 2, 3\} | P(X) \text{ equiv } P(1) \text{ AND } P(2) \text{ AND } P(3)$$

$\exists y$ works like OR. For example:

$$\forall x, x \in \{1, 2, 3\} | P(X) \text{ equiv } P(1) \text{ OR } P(2) \text{ OR } P(3)$$

Quantifiers Example

For $x, y \in \mathbb{N}$ (x and y range over the integers).

$$Q(Y) ::= \exists x.x < y.$$

- Q(3) is True. ($[x < 3]$ is T for $x = 1$)
- Q(1) is True. ($[x < 1]$ is T for $x = 0$)
- Q(0) is False. ($[x < 0]$ is not T for any $x \in \mathbb{N}$)

What about a simple example for $\forall$?

Ordering Quantifiers

What is the difference when we order $\exists$ and $\forall$?

Example 1: Medicines

$\forall d \in$ diseases. $\exists m \in$ medicine.
m cures d

Example 2: Panacea

$\exists m \in$ medicine. $\forall d \in$ diseases.
m cures d

We need to be careful when writing mathematical notation!

Validity and Predicates

- Propositional Validity: A proposition is true for all truth assignments of variables.
  - Example: (P implies Q) OR (Q implies P)
- Predicate Calculus Validity: A predicate is valid when it is true for all domains.
  - Example: $\forall z.[P(z) \wedge Q(z)] \rightarrow [\forall x.P(x) \wedge \forall y.Q(y)]$

Conclusion

Important Ideas from this lecture

- Proofs are sequences propositions that establish the truth or falsehood of an statement.
- Proof Techniques are organized ways to construct a proof;
  - Proof By Cases;
  - Contradiction;
  - Well Ordering Principle, etc;
- Predicate Logic use logical operators to show the truth or falsehood of a predicate;
  - Concepts of Validity and Satisfiability;
- There is a close relationship between proving an statement, and proving the correctness of a computer program

Reminder: Exercise sheet at manaba

- The homework for this lecture is on manaba;
- You have to submit your homework before the next lecture;
- The lecturer will be available for questions at the lecture time, so start the exercise during the lecture time;
- You can discuss the exercise with other students, but your homework is **individual**

Slide Credits

These slides were made by Claus Aranha, 2020. You are welcome to copy, re-use and modify this material, following the CC-SA-NC license.

These slides are based on "Mathematics For Computer Science (Spring 2015)", by Albert Meyer and Adam Chlipala, MIT OpenCourseWare. `https://ocw.mit.edu`.

Individual images in some slides might have been made by other authors. Please see the following slides for information about these cases.

Image Credits I