# 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 September 30, 2020

# Lecture 1 – Introduction to Proofs

## Outline

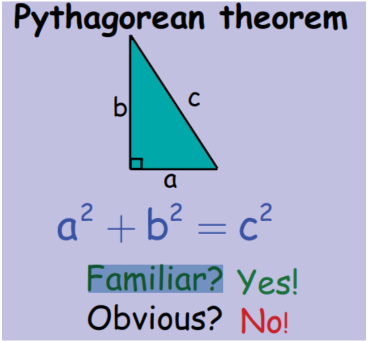
Textbook chapters 1, 2 and 3.

# Part I – Proofs

## Class Contents

1. Intro to Proofs
2. Proof Methods
3. Well Ordering Principle
4. Logical Formulas

# What is a proof?




- Proofs are used to show how you know something
- Proofs are not obvious (more than 100 proofs for pythagoras)

# Why are proofs important for Computer Sciences?

The techniques and ides of proofs can be used for debugging.

**This program outputs the type of triangle**

```
int triangle_type(int a, int b, int c)
  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";
```

- Is this program correct or incorrect?
- How can you show it with confidence?

# What is a Proof?

- A proposition is a statement that can be True or False.
  - This room has 40 chairs.
  - Every intelligent being feels pain.
  - Please say your name.
  - $513 \times 435 = 223165$
  - Every even integer greater than 2 is the sum of two primes.
  - It is raining now.

- A proof is a method of proving the truth or falsehood of a proposition.
  - mathematical proofs normally use logical steps to show the truth of a mathematical proposition.

# Proof Examples

- Pitagoras by pictures
- Getting rich with triangles
- 1 == -1

# Morals of Proofs

- Make sure that you are applying the rules properly.
- Mindless calculation does not replace understanding.

# Common Terms used in Proofs

- Proposition:
- Predicate:
- Axiom:
- Proof:
- Theorem:
- Lemma:
- Corollary:

# Common Terms used in Proofs

- Proposition:
  A statement that is either true or false
- Predicate:
  A preposition that depends on variables
- Axiom:
  A preposition that is accepted to be true
- Proof:
  A sequence of axioms and proved statements that conclude with the proposition of interest
- Theorem:
  An important true proposition
- Lemma:
  A simpler proposition that is useful to prove later propositions
- Corollary:
  A proposition that follows from a theorem in a few logical steps

# Our first proof method: Modus Ponens

$$\frac{P, P \text{ implies } Q}{Q} \text{ or } \frac{P, P \rightarrow Q}{Q}$$

What does "Modus Ponens" mean?

- If P is true.
- and if P being true requires that Q is true too.
- then Q is true.

# How can we use Modus Ponens to prove something?

- We want to prove Q.
- Prove that when P is true, Q must be true
- Prove that P is true
- therefore, Q must be true.

# Proof By Contradiction

A trivial proof:

$$\sqrt[3]{1332} \leq 11$$

# Proof By Contradiction

If an assertion implies something false

Then the assertion must be false!

# Better Example: $\sqrt{2}$ is irrational

Think a little bit by yourselves first.

# Better Example: $\sqrt{2}$ is irrational

Let's prove by contradiction:

1. Assume that $\sqrt{2}$ is rational
2. Therefore $\sqrt{2} = \frac{m}{n}$, and $m$ and $n$ are integers with no common prime factors ($n \neq 0$).
3. Therefore $n\sqrt{2} = m$, $2n^2 = m^2$, and $m^2$ is even.
4. If $m^2$ is even, then $m$ is even too. $m = 2k$ for some integer $k$.
5. Therefore $2n^2 = (2k)^2$, $2n^2 = 4k^2$, $n^2 = 2k^2$, and $n^2$ is even.
6. If $n^2$ is even, then $n$ is even too. $n$ and $m$ are both even (contradiction).

# Proof By Cases

Prove that these two code samples are the same:

### Code 1

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

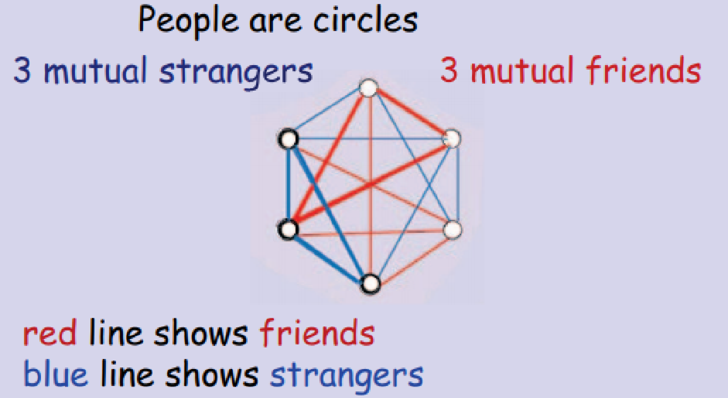
### Code 2

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

# Proof By Cases

- "Proof by Cases" breaks a complicated problem into easier, smaller sub-problems.
- It is important to make sure that the cases cover all possibilities, or the proof is not complete.

# Proof By Cases: Friends and Strangers




- Six people, every two are either friends or strangers.
- **Claim:** There is always a set of 3 mutual friends or 3 mutual strangers.

# Friends and Strangers, and Ramsey's Theorem

For any $k$, every large enough group of people will contain $k$ mutual friends OR $k$ mutual strangers.

- $R(3) = 6$
- $R(4) = 18$
- $R(5) =$ unknown!

# A bogus proof by cases: Prove $2a^2 > a$

1. This proof is by case analysis.
2. There are two cases:
   - Case 1: $a$ is positive
   - Case 2: $a$ is negative
3. One of these cases must always hold, because an integer is either positive or negative.
4. Case 1: Suppose $a$ is positive.
5. Since $a$ is an integer, we must have that $a \geq 1$.
6. Hence, $2a^2 = 2a \times a \geq 2a \times 1 > a$.
7. This implies the claim holds in Case 1.
8. Case 2: Suppose $a$ is negative.
9. Since $a$ is an integer, we must have that $a \leq -1$.
10. Hence, $2a^2 \geq 2 \times (-1 \times -1) = 2 > -1 \geq a$.
11. This implies the claim holds in Case 2.
12. The claim therefore holds in both cases.

# The Well Ordering Principle

- It is a very obvious (but very useful) principle in Mathematics;
- It is so obvious that you have already used it without knowing;

# The Well Ordering Principle

Every non-empty set of
Non-negative Integer Numbers
has one smallest element

# The Well Ordering Principle

Obvious? yes Trivial? no

- Every non-empty set of non-negative rational numbers has one smallest element?
- Every non-empty set of integers numbers has one smallest element?

# Well Ordering Examples

- What is the smallest age of the U.Tsukuba students?
- What is the smallest number of cells in any animal?
- What is the smallest number of coins = 876 yens?

# Proof $\sqrt{2}$ is irrational using well ordering

- if $\sqrt{2}$ is rational, then exist $m, n$ so that $\sqrt{2} = \frac{m}{n}$
- We can always find $m, n > 0$ such as they have no common factors.
- Why always?

# Proof $\sqrt{2}$ is irrational using well ordering

- Suppose that we choose the smallest $m, n$.
- Using the same idea as the previous proof, we show that both numbers must be divisible by two. $(m' = m/2, n' = n/2)$
- Now we found a number smaller than the smallest! (contradiction!)

# More Proofs Using the Well Ordering Principle

- (Easy) Every integer $i > 1$ is a product of primes.
- (Medium) Every number is Postal.
  - A number $n$ is postal if $n + 8$ can be composed of a sum of "threes" and "fives"
- (Difficult) $1 + r + r^2 + \ldots + r^n = \frac{r^n - 1}{r - 1}$

# General form for a Well Ordering proof

You want to prove that $\forall n \in \mathbb{N}, P(n)$ using WOP.

1. Define a set of counter examples $C$, $C ::= \{n \in \mathbb{N} |$ not $P(n)\}$
2. Assume the minimum element of $C$ exists, $m$, by WOP
3. Find a contradiction, for example:
    - Find a contradiction $c \in C, c < m$;
    - Show that $P(m)$ is actually True;

# 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 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