01204211 Discrete Mathematics
Lecture 1: Introduction

Jittat Fakcharoenphol

August 18, 2015

What is this course about?

This is a math class.
But, what is mathematics?
Ah... that's a philosopical question.
IMHO, mathematics is a mean to communicate *precise* ideas.

It's like learning a new language

- Do you remember the time when you start learning English?
- There are a few things you have to learn and get used to.
- They might not make so much sense in the beginning, but over time, you will get comfortable with how the language is used.
- As your knowledge of the language gets better, everything becomes more natural. Learning a new language sometimes expands your view of the world.
- I hope it is also true with this course.

The goals of this course

There are two goals:

- To learn how to make mathematical arguments.
- To learn various fundamental mathematical concepts that are very useful in computer science.

Why should we learn how to prove? (1)

Look at this program.

```
if a > b:
    return a
else:
    return b
```

The author claims that this program takes two variables a and b and returns the larger one.

Do you believe the author of the code? Why?

Finding the maximum value. (1)

Now look at this program.

```
if a > b:
    if a > c:
        return a
    else:
        return c
else:
    if c > b:
        return c
    else:
        return b
```

The author claims that this program takes three variables a, b and c and returns the largest one.

Do you believe the author of the code? Why?

Finding the maximum value. (2)

Finally, look at this program.

```
// Input: array A with n elements: A[0],...,A[n-1]
m = 0
for i = 0, 1, ..., n-1:
  if A[i] > m:
    m = A[i]
return m
```

The author claims that this program takes an array A with n elements and returns the maximum element.

Do you believe the author of the code? Why?

Can we try to test the code with all possible inputs?

Finding the maximum value. (3)

Let's try again.

```
// Input: array A with n elements: A[0],...,A[n-1]
m = A[0]
for i = 1, 2, ..., n-1:
  if A[i] > m:
    m = A[i]
return m
```

Do you believe the author of the code? Why?

Can we try to test the code with all possible inputs?

Another example: testing primes (1)

A *prime* is a natural number greater than 1 that has no positive divisors other 1 and itself. E.g., 2,3,5,7,11 are primes.

```
Algorithm CheckPrime(n):      // Input: an integer n
    if n <= 1:
        return False
    i = 2
    while i <= n-1:
        if n is divisible by i:
            return False
        i = i + 1
    return True
```

The code above checks if n is a prime number. How fast can it run?
Note that if n is a prime number, the for-loop repeats for $n-2$ times. Thus, the running time is approximately proportional to n. Can we do better?

Another example: testing primes (2)

Consider the following code.

```
Algorithm CheckPrime2(n):  // Input: an integer n
    if n <= 1:
        return False
    let s = square root of n
    i = 2
    while i <= s:
        if n is divisible by i:
            return False
        i = i + 1
    return True
```

How fast can it run? Note that $s = \sqrt{n}$; therefore, it takes time approximately proportional to $\sqrt{n}$ to run.

Ok, it should be faster. **But is it correct?**

Informal arguments (1)

- Let's try to argue the Algorithm `CheckPrime2` works correctly.
- Note that if n is a prime number, the algorithm answers correctly. (Why?)
- Therefore, let's consider the case when n is not prime (i.e., n is a composite).
- If that's the case, n has some positive divisor which is not 1 or n. Let's call this number a.
- Now, if $2 \leq a \leq \sqrt{n}$, at some point during the execution of the algorithm, $i = a$ and i should divides n; thus the algorithm correctly returns `False`.
- Are we done?

Informal arguments (2)

- Recall that we are left with the case that (1) n is not prime and (2) its positive divisor a is larger than $\sqrt{n}$.
- Let $b = n/a$. Since n and a are positive integers and a divides n, b is also a positive integer.
- Note that if we can argue that $2 \leq b \leq \sqrt{n}$, we are done. (why?)
- How can we do that?

The goals

- Let's take a break and look back at what we are trying to do.

Original goal: To show that Algorithm `CheckPrime2` is correct.

Current (sub) goal: Consider a positive composite n and its positive divisor a, where $a > \sqrt{n}$. Let $b = n/a$. We want to show that $2 \leq b \leq \sqrt{n}$.

- Before we continue, I'd like to add a bit of formalism to our thinking process.

The main goal

- **Original goal:** To show that Algorithm `CheckPrime2` is correct.
- Let's focus on the statement we want to argue for:

  > **"Algorithm `CheckPrime2` is correct."**

- Note that this statement can either be "true" or "false." If we can demonstrate, using logical/mathematical arguments that this statement is true, we can say that we **prove** the statement.

The (sub) goal

- **Current (sub) goal:** Consider a positive composite n and its positive divisor a, where $a > \sqrt{n}$. Let $b = n/a$. We want to show that $2 \leq b \leq \sqrt{n}$.
- Let's focus only on the statement we want to argue for:

$$2 \leq b \leq \sqrt{n}.$$

- If we only look at this statement, it is unclear if the statement is true or false because there are variables b and n in the statement. It can be true in some case and it can be false in some case depending on the values of n and b.
- Are we doom? Not really. The statement above is not precisely the statement we want to prove.

The (sub) goal (second try)

- **Current (sub) goal:** Consider a positive composite n and its positive divisor a, where $a > \sqrt{n}$. Let $b = n/a$. We want to show that $2 \leq b \leq \sqrt{n}$.
- We can be more specific about what values of n and b that we want to consider.

> **Revised statement**
>
> For all positive composite integer n, and for every divisor a of n such that $\sqrt{n} < a < n$,
>
> $$2 \leq b \leq \sqrt{n},$$
>
> where $b = n/a$.

- Note that this revised statement is now "quantified," that is, every variable in the statement has specific scope. Now the statement is either true or false.

Propositions

- A *proposition* is a statement which is either **true** or **false**.
- It is our basic unit of mathematical "facts".
- Examples:
  - Algorithm `CheckPrime2` is correct.
  - $10^2 = 90$.
  - $\sqrt{2}$ is irrational.
- Examples of statements which are not propositions (why?):
  - $x > 10$.
  - $1 + 2 + \cdots + 10$.
  - This algorithm is fast.
  - Run, run quickly.

Combining propositions

- We usually use a variable to refer to a proposition. For example, we may use P to stand for “it rains” or Q to stand for “the road is wet.”
- The truth value of a variable is the truth value of the proposition it stands for.
- Many propositions can be combined to get a complex statement using logical operators.
- For example, we can join P and Q with “and” (denoted by “$\wedge$”) and get

  $$P \wedge Q,$$

  which stands for “it rains and the road is wet”.
- An expression $P \wedge Q$ is an example of *propositional forms*. The logical value of a propositional form “usually” depends on the truth value of its variables.

Connectives: “and”, “or”, “not”

Given propositions P and Q, we can use connectives to form more complex propositions:

- **Conjunction:** $P \wedge Q$ (“P and Q”),
  (True when both P and Q are true)
- **Disjunction:** $P \vee Q$ (“P or Q”),
  (True when at least one of P and Q is true)
- **Negation:** $\neg P$ (“not P”)
  (True only when P is false)

If P stands for “today is Tuesday” and Q stands for “dogs are animals”, then

- $P \wedge Q$ stands for “today is Tuesday and dogs are animals”,
- $P \vee Q$ stands for “today is Tuesday or dogs are animals”, and
- $\neg P$ stands for “today is not Tuesday”.

Truth tables

To represents values of propositional forms, we usually use truth tables.

And/Or/Not

P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$
T	T	T	T	F
T	F	F	T	
F	T	F	T	T
F	F	F	F	

Quick check 1

For each of these statements, define propositional variables representing each proposition inside the statement and write the proposition form of the statement.

- All prime numbers are larger than 0 and all natural numbers is at least one.
- You are smart or you won't be taking this class.

Quick check 2

Use a truth table to find the values of (1) $P \wedge \neg P$ and (2) $P \vee \neg P$.

And/Or/Not

P	$\neg P$	$P \wedge \neg P$	$P \vee \neg P$
T	F	F	T
F	T	F	T

Note that $P \wedge \neg P$ is always false and $P \vee \neg P$ is always true.
A propositional form which is always true regardless of the truth values of its variables is called a *tautology.* On the other hand, a propositional form which is always false regardless of the truth values of its variables is called a *contradiction.*

Implications

Given P and Q, an implication

$$P \Rightarrow Q$$

stands for "if P, then Q". This is a very important propositional form.

It states that "when P is true, Q must be true". Let's try to fill in its truth table:

Implications

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

What?

- Yes, when P is false, $P \Rightarrow Q$ is **always true** no matter what truth value of Q is.
- We say that in this case, the statement $P \Rightarrow Q$ is *vacuously true.*
- You might feel a bit uncomfortable about this, because in most natural languages, when we say that if P, then Q we sometimes mean something more than that in the logical expression "$P \Rightarrow Q$."

One explanation

- But let's look closely at what it means when we say that:

> if P is true, Q must be true.

- Note that this statement does not say anything about the case when P is false, i.e., it only considers the case when P is true.
- Therefore, having that $P \Rightarrow Q$ is true is OK with the case that (1) Q is false when P is false, and (2) Q is true when P is false.
- This is an example when mathematical language is "stricter" than natural language.

Noticing if-then

We can write "if P, then Q" for $P \Rightarrow Q$, but there are other ways to say this. E.g., we can write (1) Q if P, (2) P only if Q, or (3) when P, then Q.

Quick check 3

For each of these statements, define propositional variables representing each proposition inside the statement and write the proposition form of the statement.

- If you do not have enough sleep, you will feel dizzy during class.
- If you eat a lot and you do not have enough exercise, you will get fat.
- You can get A from this course, only if you work fairly hard.

Only-if

Let P be "you get A from this course."
Let Q be "you work fairly hard."
Let R be "You can get A from this course, only if you work fairly hard."
Let's think about the truth values of R.

Only if you work fairly hard.

P	Q	R
T	T	
T	F	
F	T	
F	F	

Thus, R should be logically equivalent to $P \Rightarrow Q$. (We write $R \equiv P \Rightarrow Q$ in this case.)

If and only if: ($\Leftrightarrow$)

Given P and Q, we denote by

$$P \Leftrightarrow Q$$

the statement "P if and only if Q." It is logically equivalent to

$$(P \Leftarrow Q) \wedge (P \Rightarrow Q),$$

i.e., $P \Leftrightarrow Q \equiv (P \Leftarrow Q) \wedge (P \Rightarrow Q)$.
Let's fill in its truth table.

P	Q	$P \Rightarrow Q$	$P \Leftarrow Q$	$P \Leftrightarrow Q$
T	T			
T	F			
F	T			
F	F			

An implication and its friends

When you have two propositions

- $P =$ "I own a cell phone", and
- $Q =$ "I bring a cell phone to class".

We have

- an implication $P \Rightarrow Q \equiv$
  "If I own a cell phone, I'll bring it to class",
- its **converse** $Q \Rightarrow P \equiv$
  "If I bring a cell phone to class, I own it", and
- its **contrapositive** $\neg Q \Rightarrow \neg P \equiv$
  "If I do not bring a cell phone to class, I do not own one".

Quick check 4

Let's consider the following truth table:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$\neg Q \Rightarrow \neg P$
T	T			
T	F			
F	T			
F	F			

Do you notice any equivalence?

Right, $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$.

How about our subgoal?

- In many cases, the statement we are interested in contains variable.
- For example, "x is even," "p is prime," or "s is a student."
- As we previously did with propositions, we can use variables to represent these statements. E.g.,
  - let $E(x) \equiv$ "x is even",
  - let $P(y) \equiv$ "y is prime, and
  - let $S(w) \equiv$ "w is a student.

  We call $E(x)$, $P(y)$, and $S(w)$ *predicates*. (You can think of predicates as statements that may be true of false depending on the values of its variables.)

Quantifiers (1)

- As we note before, these predicates are not propositions. But if we know the value of the variables, then they becomes propositions. For example, if we let $x = 5$, then $E(5)$ is a proposition which is false. Also, $P(7)$ is true.
- Since the truth values of predicates depend on the assignments of its variables, we can put *quantifiers* to specify the scope of these variables and how to interprete the truth values of the predicates over these values.
- Let $A = \{2, 4, 6, 8\}$.
- Note that $E(2), E(4), E(6)$, and $E(8)$ are true, i.e., $E(x)$ is true for every $x \in A$.
  In this case, we say that the following proposition is true:

$$(\forall x \in A)E(x).$$

Quantifiers (2)

- Again, let $A = \{2, 4, 6, 8\}$.
- Note that $P(2)$ is true. This means that $P(y)$ is true for some $y \in A$.
  In this case, we say that the following proposition is true:
  $$(\exists y \in A) P(y).$$
- "$\forall x$" and "$\exists y$" are quantifiers. They give predicates $E(x)$ and $P(y)$ precise scopes of considerations.
- When the universe A is clear, we can leave it out and just write $\forall x E(x)$ or $\exists y P(y)$.

The main goal

- Let's try to be more specific about our main goal:

  > Algorithm `CheckPrime2` is correct.

- Can we re-write this statement so that the input/output of the algorithm are explicit?
- Note that the set of its input n is an integer. Thus, we are interested in every $n \in \mathbb{Z}$, where $\mathbb{Z}$ denote the set of all integers.
- Let's rewrite the goal as:

  $$\forall n \in \mathbb{Z},\ C(n) \Leftrightarrow P(n),$$

  where $C(n) \equiv$ "`CheckPrime2(n)` returns True", and $P(n) \equiv$ "n is a prime."

Quantified propositions with more than one variables

Let our universe be integers ($\mathbb{Z}$). Which of the following statements is true?

- $\forall x \forall y (x = y)$
- $\forall x \exists y (x = y)$
- $\exists x \forall y (x = y)$
- $\exists x \exists y (x = y)$

When you have many quantifiers, we can interprete the statement by nesting the quantifiers. E.g,

$$\exists x \forall y P(x, y) \equiv \exists x (\forall y (P(x, y))).$$

$$\forall y \exists x P(x, y) \equiv \forall y (\exists x (P(x, y))).$$

Also note that usually, $\exists x \forall y P(x, y) \not\equiv \forall y \exists x P(x, y)$.

Quick check 5

- Let's consider the current subgoal. (Note that in this version, variable b is replaced with n/a.)

  Another revised statement

  For all positive composite integer n, and for every divisor a of n such that $\sqrt{n} < a < n$,

  $$2 \leq n/a \leq \sqrt{n}.$$

- Define all required predicates and describe a quantified proposition equivalent to the revised statement above.

Next lecture...

- We will discuss a few proof techniques and will formally prove the correctness of `CheckPrime2`.
- The next lecture will be availabe as VDO clips. Please watch it before the next section. We will work on homework in class.