Welcome to CSC236!

Introduction to the Theory of Computation

Amir H. Chinaei, Fall 2016

ahchinaei@cs.toronto.edu
http://www.cs.toronto.edu/~ahchinaei/

Office hours: W 2-4 BA4222

today

- Course outline (bird's-eye view)
  - what this course is about
- Logistics
  - Course organization, information sheet
  - Assignments, grading scheme, *etc.*
- Introduction to
  - proofs

what is this course about?

- some analytical skills
  - reasoning to argue a claim is right or wrong
    - a statement is true or false
    - a math property holds or not
    - a computer program is correct or not
  - the reasoning should follow certain structures
    - otherwise the argument may be messy if valid at all
    - it's an art
    - ==> formal (systematic) reasoning
  - …

anonymous quiz

- true or false?

…

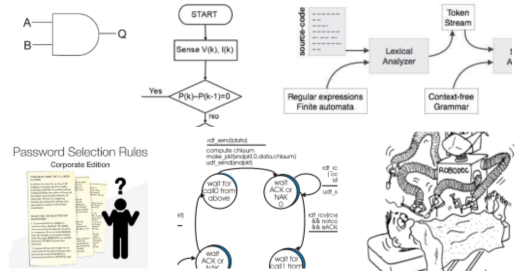
what is this course about?

- some analytical skills
  - …
  - systematic counting
    - e.g. how many different passwords can exist when certain rules exist?
  - intro to formal languages
    - e.g. how natural language sentences can be represented such that computer can reason about them?

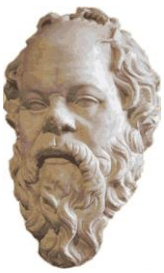
why learning this course?

- these topics can assist us in
  - **computer Science**:
    - designing computer hardware (architecture) and software (algorithms, programming languages, security protocols, network protocols, artificial intelligence, …
  - as well as in other disciplines:
    - such as philosophy, linguistics, law, …
    - actually in our daily life!

computer science



as well as in other disciplines



Socrates (c. 469 BC – 399 BCE) was one of the founders of Western philosophy.

logistics

prerequisite

- need to have solid background from CSC165
  - otherwise,
    - review CSC165 material, especially
      - mathematical prerequisites (Chapter 1.5)
      - proof techniques (Chapter 3)
      - big Oh notation (Chapter 4)
    - read Chapter 0 of Vassos's notes
    - contact me
    - start a discussion in the forum
    - go to the Help Centre

course components

- lectures: concepts
- labs: practice, more details, problem solving, & quizzes
- exercises and assignments: mastering your skills
- peer Instructions: learn from your fellow students
- readings: preparing you for above

course web page

- for important information on
  - lecture and lab time/location/material
  - contact information of course staff
  - office hours and location
  - exercises/Assignments/Readings specification/solution
  - deadlines and evaluation
  - communication and announcements
  - …
- follow the course web page, regularly
  http://www.cdf.toronto.edu/~csc236h/fall/

let's start with a simple question

count subsets 1

- How many subsets does set {} have?
- How many subsets does set {a} have?
- How many subsets does set {a, b} have? **How?**
- How many subsets does set {a, b, c} have? **How?**

messy approach

count subsets 2

- How many subsets does set {} have?
- How many subsets does set {a} have?
- How many subsets does set {a, b} have? **How?**
- How many subsets does set {a, b, c} have? **How?**

a better approach (systematic)

count subsets 3

- How many subsets does set {} have?
- How many subsets does {a} have?
- How many subsets does {a, b} have? **How?**
- How many subsets does {a, b, c} have? **How?**

a **more systematic** approach

observation

an empty set has …. subset, and adding one member to a set will ……..… the number of its subsets.

|set|	| power set |

conjecture: a set with cardinality of *n* has … subsets.

won't sell yet ...

- This is just an observation, or a conjecture at best
  - and begging

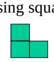
|set|	|power set|
…	…
4	16
5	32
6	64
7	128
…	…

  - does not work
- To sell it, we need to **prove** it first.

proof methods

- Exhaustive proof
- Proof by cases
- Direct proof
- Proof by contraposition
- (Dis)Proof, by contradiction
- **Proof by**
  - **Simple Induction**
  - **Complete Induction**
  - **Structural Induction**
- …

proof by simple induction

- Many (mathematical) statements can be expressed by propositional functions, denoted by ***P*(*n*)**
  - Example 1:
    - ***P*(*n*)**: n^3-n is divisible by 3; for every natural number *n*.
  - Example 2:
    - ***P*(*n*)**: $\sum_1^n i = \frac{n(n+1)}{2}$
  - Example 3:
    - ***P*(*n*)**: every 2^nx2^n checkerboard with one missing square can be tiled with (3-piece) L-shape tiles, i.e. 

proof by simple induction

- **recipe:**
  - To prove that *P*(*n*) is true for all natural numbers *n*, we should demonstrate these steps:
    - ***Proof method:*** "simple induction"
    - ***Basis step***: show that *P*(n) is true for some starting point(s), usually 0 or 1 but not always
    - ***Inductive step***: show that *P*(*k*) → *P*(*k*+1) is true for all natural numbers *k greater than the starting point.*
      - to complete the inductive step, assume *H* holds for an arbitrary natural number *k*, show that C must be true.

Notes

- Proofs by induction do not always start at 1 or 0. They could start at any natural number *b*, and there could be more than one *b*.
- Induction can be expressed as a rule of inference:
  $(P(b) \wedge \forall k\, (P(k) \rightarrow P(k+1))) \rightarrow \forall n\, P(n)$,
  where *b*, *k*, and *n* $\in \mathbb{N}$.
- In the inductive step, we do **NOT** assume that *P*(*k*) is true for all numbers! We should show that if we assume that *P*(*k*) is true for an arbitrary *k*, then *P*(*k*+1) must also be true.

Simple induction as a rule of inference

$$(P(b) \wedge \forall k\, (P(k) \rightarrow P(k+1))) \rightarrow \forall n\, P(n)$$

our first proof

- **Recall our conjecture:**
  - a set with n members has 2^n subsets.
- **Solution:**
  - Proof method: simple induction
    P(n): a set with n members has 2^n subsets.
  - Basis step: $P(0)$ is true, because a set with 0 members (*i.e.* {}) has 2^0 subset (*i.e.* just itself, {}).
  - Inductive step: (c.f. Slide 22) we assume $P(k)$ is true for an arbitrary k, and—by using this assumption—we show that P(k+1) must be true. In other words, we show that $P(k) \rightarrow P(k+1)$ holds. (see next …)

P(n): a set with n members has 2^n subsets.

our first proof (continued)

- Inductive step: we want to show that $P(k) \rightarrow P(k+1)$ holds.
  - Inductive hypothesis: we assume for an arbitrary fixed k, every set S with k members has 2^k subsets.
  - Now let set $T = S \cup \{new\}$, where $new \in T$ and $new \notin S$. Hence $|T| = k+1$.

P(n): a set with n members has 2^n subsets.

our first proof (continued)

- For each subset U of S, there are exactly two subsets of T: *one is U without the new member, the other is U with the new member. (cf. Slide 14). By the inductive hypothesis, S has 2^K* subsets. Since there are two subsets of T for each subset of S, the number of subsets of T is $2 \cdot 2^k = 2^{k+1}$. This concludes that it must be true that every set with k+1 members has 2^{K+1} subsets.
- The inductive step is now complete.

- Therefore, P(n): a set with n members has 2^n subsets is true for all $n \in \mathbb{N}$.

$\square$

Example 2:

n^3-n is divisible by 3; for every natural number n. *i.e.* $\forall n \in \mathbb{N}$, $3 \mid n^3 - n$

scratch work

Example 2: (proof)

Prove $\forall n \in \mathbb{N}$, $3 \mid n^3 - n$

Example 2: (continued)

Prove $\forall n \in \mathbb{N}$, $3 \mid n^3 - n$

Example 3:

The units digit of 3^n is either 1, 3, 7, or 9.

i.e. $\forall n \in \mathbb{N}$, $3^n \equiv 1$ or 3 or 7 or 9 (mod 10)

scratch work

Example 3: (proof)

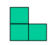
Prove $3^n \equiv 1$ or 3 or 7 or 9 (mod 10); $\forall n \in \mathbb{N}$.

Example 3: (continued)

Prove $3^n \equiv 1$ or 3 or 7 or 9 (mod 10); $\forall n \in \mathbb{N}$.

Example 4:

every 2^nx2^n checkerboard missing a square can be tiled with L-shape tiles.



scratch work

Example 4:

every 2^nx2^n checkerboard missing a square can be tiled with L-shape tiles.

scratch work

Example 4: (proof)

Prove $\forall n \geq 1 \in \mathbb{N}$, 2^nx2^n checkerboards missing a square can be tiled with L-shape tiles.

Example 4: (continued)

Prove $\forall n \geq 1 \in \mathbb{N}$, 2^nx2^n checkerboard missing a square can be tiled with L-shape tiles.

Simple induction recipe (revisited)

0. write out the claim as: "**Let *P*(*n*) denote the claim in terms of *n***" follow next steps to show that *P*(*n*) holds $\forall n \geq b \in \mathbb{N}$, where *b* is staring point(s)
1. write out "***Proof method:* simple induction**"
2. write out "***Basis step:***" followed by reasoning that *P*(*b*) is true
3. write out "***Inductive step:***"
   - 3.1. write out "**Inductive hypothesis:** we assume *P*(*k*) is true for an **arbitrary fixed** $k \geq b$" where *P*(*k*) is the claim in terms of *k*
   - 3.2. reason that *P*(*k*+1) is true
     - **note 1:** in your reasoning here, you must use the inductive hypothesis
     - **note 2:** be sure your reasoning is true for any $k \geq b$, including $k=b$
     - **note 3:** verify if you need to adjust your starting point, *b*
   - 3.3. write out "**This completes the inductive step**"
4. write out "***This proves P(n) is true for $\forall n \geq b \in \mathbb{N}$***" where *P*(*n*) is the claim in terms of *n*
5. Indicate end of proof by "□".

Wrong proofs by induction

Example 5: P(*n*): $\forall n \geq 2 \in \mathbb{N}$, every *n* lines, no two of them are parallel, meet in a common point.

Proof method: simple induction

Basis step: *P*(2) is true because any two lines that are not parallel meet in a common point.

Inductive step:

Inductive hypothesis: we assume P(*k*) is true, i.e. for any $k \geq 2$, that is true that every *k* lines, no two of them parallel, meet in a common point.

Then, we show that *P*(*k*+1) is true too.

Wrong proofs by induction

Consider *k*+1 lines, no two of them parallel. By our I.H., the first *k* of these lines must meet in a common point p_1. Also, by our I. H, the last *k* of these lines meet in a common point p_2.

p_1 and p_2 cannot be different points; otherwise, all lines are the same line.

so, p_1 and p_2 are the same point and this completes our inductive step that *k*+1 lines, no two of them parallel, meet in a common point.

This proves that $\forall n \geq 2 \in \mathbb{N}$, every set of *n* lines, no two of them are parallel, meet in a common point.

□

What's wrong in this proof?