# CSC236 fall 2014

## Theory of computation

Danny Heap
heap@cs.toronto.edu
BA4270 (behind elevators)
http://www.cdf.toronto.edu/~csc236h/fall/
416-978-5899

Using Introduction to the Theory of Computation, Section 1.2

# Outline

Introduction

Chaper 1, Simple induction

Notes

# Why reason about computing?

- It's more than just hacking — computer scientists now
- Testing isn't enough → infinite # of test cases, some-times
- You might get to like it (?!*) → really!

# How to reason about computing

- It's messy... many, many drafts + redrafts.
- It's art... there's golden algorithm for a solution.

# How to do well at this course

- Read the course information sheet as a two-way promise
- Question, answer, record, synthesize
- Collaborate with respect

# What should you already know?

- Chapter 0 material from *Introduction to Theory of Computation*

  sequence, subsequence

- CSC165 material, especially the mathematical prerequisites (Chapter 1.5), proof techniques (Chapter 3), and the introduction to big-Oh (Chapter 4).

# What'll you know by December?

- Understand, and use, several flavours of induction

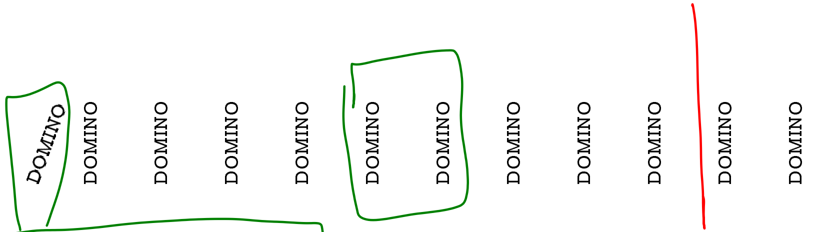
  simple, complete, well-ordering principle, structural induction

- Complexity and correctness of programs — both recursive and iterative → 165 topic

- Formal languages, regular languages, regular expressions

  $(1^* + 0^*)$

# Domino fates foretold




If the initial domino falls, and each domino that falls implies its successor falls, then all dominoes fall.

Falling is preserved.

we know ... believe

# count subsets

How many subsets does $\{1\}$ have? How do you know?

$2 - \{\{1\}, \{\}\}$

How many subsets does $\{1, 2\}$ have? How do you know?

$4 - \{\{\}, \{1,2\}, \{1\}, \{2\}\}$

What about $\{a\}$ and $\{a, b\}$?

$\{\{\}, \{1,2\}, \{1\}, \{2\}\}$

$\{\{\}, \{a,b\}, \{a\}, \{b\}\}$

# counting systematically

Count the subsets of $\{1\}$ by enumerating them, in a **power set**.

$\mathcal{P}(\{1\}) = \{\{1\}, \{\}\}$

How do you get from the set of subsets of $\{1\}$ to the set of subsets for $\{1, 2\}$?

$$\mathcal{P}(\{1,2\}) = \{\{1\}, \{\}, \{2,1\}, \{2\}\}$$

# gathering data systematically

| set | number of subsets |
|---|---|
| $\{\}$ | 1 |
| $\{1\}$ | 2 |
| $\{1, 2\}$ | 4 |
| $\{1, 2, 3\}$ | 8 |
| $\vdots$ | $\vdots$ |
| $\{1, 2, 3, \ldots, n\}$ | $2^n$ |

$2 \times 2 \times \cdots \times 2$ n times

$$2^n = \begin{cases} 1 & \text{if } n = 0 \\ 2 \times 2^{n-1} & \text{if } n > 0 \end{cases}$$

# Every set with $n$ elements has exactly $2^n$ subsets

why? Proof

The only set of size 0 is the empty set, and it has exactly $1 = 2^0$ subsets.

Now assume $n$ is some natural number, and that any set of size $n$ has $2^n$ subsets

Suppose $|S| = n+1 > 0$, so there is some $x \in S$. Split (partition) the subsets of $S$ into those that contain $x$ and those that don't. Since the subsets that do not contain $x$ are the subsets of $S - \{x\}$, which has $n$ elements, hence $2^n$ subsets. There is a matching (add or remove $x$) between subsets with & without $x$, so there are also $2^n$ subsets of $S$ ~~in~~ contain $x$.

So $S$ has $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$ subsets.

Shown that if any set of then a
size $n$ has $2^n$ elements,

# Every set with $n$ elements has exactly $2^n$ subsets

why?

→ Conclude that $\forall n$, set of size $n$ having $2^n$ elements $\Longrightarrow$ set of size $n+1$ has $2^{n+1}$ elements

---

Conclude (by Induction)

Every set of size $n$ elements has $2^n$ subsets, $\forall n \in \mathbb{N}$

# general form

Predicate sentence, open in one variable

$$\left[\, \underbrace{P(0)}_{\text{first domino}} \wedge \left( \forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1) \right) \right] \Longrightarrow \forall n \in \mathbb{N}, P(n)$$

believe,

prove the antecedent, then you know the consequent

# Every set with $n$ elements has exactly $2^n$ subsets...

Use: $[P(0) \wedge (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))] \Longrightarrow \forall n \in \mathbb{N}, P(n)$

$P(n)$: "all sets of size $n$ ~~has~~ have $2^n$ subsets"

Proof (induction)

- Prove $P(0)$
- Prove that $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$

---

# Every set with $n$ elements has exactly $2^n$ subsets...

Use: $[\,P(0) \wedge (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))\,] \Longrightarrow \forall n \in \mathbb{N}, P(n)$

Proof: By induction.

Base case: A set with 0 elements must be the empty set, and $\{\}$ has exactly $1 = 2^0$ subsets (itself). So $P(0)$ is true.

Induction Step: assume $n$ is some typical natural number and that $P(n)$ is true: every set with $n$ elements has $2^n$ subsets (this assumption is called the Induction Hypothesis, IH).

If $S$ is some set with $|S| = n+1 > 0$ elements, we can choose some $x \in S$ and partition the subsets of $S$ into those that include $x$ and those that do not. The subsets that do not include $x$ are the subsets of $S - \{x\}$, a set of $n$ elements, which (by IH) has $2^n$ subsets. There is a natural matching between the subsets of $x$ that include $x$ and those that don't — just remove or add $x$ to a subset $\longrightarrow$

# Every set with $n$ elements has exactly $2^n$ subsets...

Use: $[\,P(0) \wedge (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))\,] \Longrightarrow \forall n \in \mathbb{N}, P(n)$

So there are the same number — $2^n$ — subsets of $S$ with and without $x$. Altogether $S$ has $2^n + 2^n = 2 \times 2^n = 2^{n+1}$ subsets, so $P(n+1)$.

We've shown that $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$

Conclude: $\forall n, P(n)$ — Every set with $n$ elements has exactly $2^n$ subsets — by Induction.

# fill in the table rows

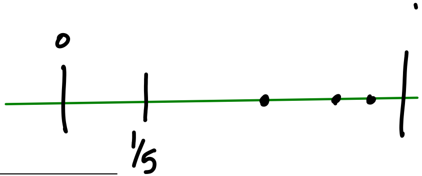
```
def a(n):
    if n > 0:
        return (1 + a(n-1)) / 2
    else:
        return 1/5
```

$a(n)$

$a_n$

$$\frac{a_n+1}{2}$$

$$\frac{a_n+1}{2} < \frac{a_{n+1}+1}{2}$$




| n | a(n) |
|---|---|
| 0 | 1/5 |
| 1 | 3/5 |
| 2 | 4/5 |
| 3 | 9/10 |
| 4 | 19/20 |
| ⋮ | |

# patterns?

Any patterns about **a(n)** that are true no matter which natural number you substitute for **n**?

$a(n) < 1 \quad \forall n \in \mathbb{N}$

Any patterns about consecutive pairs **(a(n), a(n+1))** ?

$a(n) < a(n+1) \quad \forall n \in \mathbb{N}$

Prove that some pattern is true for all **a(n)**, no matter which natural number you substitute for **n**.

- is it true at the beginning?

yes $a(0) = 1/5 < 1$

- is it preserved from one to the next?

yes $a(n) < 1$

$\Rightarrow a(n) + 1 < 2$

$\Rightarrow \frac{a(n)+1}{2} < 2/2 = 1$

$\Rightarrow a(n+1) < 1$

def

# induction steps...

No, NEVER EVER DO THIS

devise a predicate, **P(n)**, in other words a sentence that is **open** in **n**.

[Do not add $\forall n \in \mathbb{N}$ $\forall 236 \in \mathbb{N}$]

$P(n): \quad a(n) < 1$

$P(236) \quad a(236) < 1$

show that your predicate is true at the beginning (where's the beginning)?

show $P(0)$ true, ie $a(0) = 1/5 < 1$

show that your predicate is preserved from one natural number to the next

show $\forall n, P(n) \Rightarrow P(n+1)$, in other words $a(n) < 1 \Rightarrow a(n+1) < 1$.

know (conclude) that your predicate is true (preserved) no matter which natural number is substituted for **n**

$\forall n \in \mathbb{N}, P(n)$.

# general form of induction

$$[\,P(0) \;\wedge\; (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)\,)\,] \Longrightarrow \forall n \in \mathbb{N}, P(n)$$

technique is to prove the antecedent, then conclude the consequent prove: $\forall n \in \mathbb{N}, a(n) < 1$

conventional form

# For every $n \in \mathbb{N}$, $12^n - 1$ is a multiple of 11

| n | $12^n - 1$ | $11 \times ?$ |
|---|---|---|
| 0 | | |
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| $\vdots$ | | |

# For every $n \in \mathbb{N}$, $12^n - 1$ is a multiple of 11

Use: $[\,P(0) \wedge (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))\,] \Longrightarrow \forall n \in \mathbb{N}, P(n)$

# How many odd-sized subsets of a set of size $n$?

Use $[\, P(0) \;\wedge\; (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)\,)\,] \Longrightarrow \forall n \in \mathbb{N}, P(n)$

What's $P(n)$?

# How many odd-sized subsets of a set of size $n$?

Use $[\,P(0) \;\wedge\; (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))\,] \Longrightarrow \forall n \in \mathbb{N}, P(n)$

# How many odd-sized subsets of a set of size $n$?

Use $[\, P(0) \;\wedge\; (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)\,)\,] \Longrightarrow \forall n \in \mathbb{N}, P(n)$

# How many odd-sized subsets of a set of size $n$?

Use $[\, P(0) \;\wedge\; (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)\,)\,] \Longrightarrow \forall n \in \mathbb{N}, P(n)$

# Notes