CSC236 fall 2012

Theory of computation

Danny Heap
heap@cs.toronto.edu
BA4270 (behind elevators)
Course web page 416-978-5899

Using Introduction to the Theory of Computation, Section 1.2

Outline

Why reason about computing?

- It's more than just hacking
- Testing isn't enough
- You might get to like it (?!*)

How to reason about computing

- It's messy...
- It's art...

How to do well at this course

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

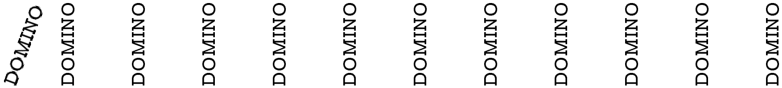
What should you already know?

- Chapter 0 material from *Introduction to Theory of Computation*
- CSC165 material, especially the mathematical prerequisites (Chapter 1.5), proof techniques (Chapter 3), and the introduction to big-Oh (Chapter 4).
- But you can *relax* the structure

What'll you know by December?

- Understand, and use, several flavours of induction
- Complexity and correctness of programs — both recursive and iterative
- Formal languages, regular languages, regular expressions

Domino fates foretold



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

If the initial case works,
and each case that works implies its successor works,
then all cases work

$P(n)$:

Every set with n elements has exactly 2^n subsets

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

$P(0)$: $\{\} \longrightarrow \{\{\}\}$ $\quad 2^0 = 1$ ✓

$P(1)$: $\{y\} \longrightarrow \{\{\}, \{y\}\}$ $\quad 2^1 = 2$ ✓

Scratch work:

$P(2)$: $\{y, x\} \longrightarrow \{\{\}, \{y\}, \{x\}, \{y, x\}\}$ $\quad 2^2 = 4$ ✓

Partition to count: $S^- = \{\{\}, \{y\}\}$, $S^+ = \{\{x\}, \{y,x\}\}$

$f: S^- \to S^+$; $f(s) \to s \cup \{x\}$ is a bijection

$f^{-1}: S^+ \to S^-$; $f(t) \to s - \{x\}$

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

P(n):

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

Proof $\forall n \in \mathbb{N}, P(n)$, by MI (aka SI)

Base case If $n = 0$, the only set of size 0 is $\{\}$ with set of subset $|\{\{\}\}| = 1 = 2^0$, so $P(0)$ is true.

Induction Step [show that $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$]

Assume $n \in \mathbb{N}$ (generic) and that $P(n)$ is true. IH

If S is a generic set with $|S| = n+1$. Now there is some $x \in S$, since $n+1 > 0$, and we partition the subsets of S in two sets:

$\mathcal{S}$ is the set of subsets of S that don't contain x, and $\mathcal{S}^+$ is the set of subsets of S that do contain x.

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

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

Since $f : \mathcal{S}^{-1} \to \mathcal{S}^{+}$, $f(s) = s \cup \{x\}$ is a bijection we know $|\mathcal{S}^{-1}| = |\mathcal{S}^{+}|$. By IH, $|\mathcal{S}^{-1}| = 2^n$, because $\mathcal{S}^{-}$ is the set of subsets of $S - \{x\}$, and $|S - \{x\}| = n+1-1 = n$. So S has $|\mathcal{S}^{-1}| + |\mathcal{S}^{+}| = 2^n + 2^n = 2^{n+1}$ subsets. Since S was arbitrary, this means every set of size $n+1$ has 2^{n+1} subsets, ie $P(n+1)$.

Since, for generic n, $P(n) \Rightarrow P(n+1)$, this shows $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$.

Conclude, $\forall n \in \mathbb{N}, P(n)$, by MI

Computer Science
UNIVERSITY OF TORONTO

$P(n)$:

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

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

$P(0)$: $12^0 - 1 = 0 = 11 \times 0$

$P(1)$: $12^1 - 1 = 11 = 11 \times 1$

$P(2)$: $12^2 - 1 = 143 = 11 \times 13$

Scratch work: How to connect n to $n+1$?

assume there is some $z \in \mathbb{Z}$ st

$12^n - 1 = 11z$

$12(12^n - 1) = 12 \cdot 11 \cdot z$

$12^{n+1} - 12 = 12^{n+1} - 1 - 11 = 11 \cdot 12 \cdot z$

rewrite. $12^{n+1} - 1 = 11 \cdot 12z + 11 = 11(12z + 1)$

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

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

Proof that $\forall n \in \mathbb{N}$, $P(n)$ using MI.

Base case: you do it.

Induction step [show that $\forall n \in \mathbb{N}$, $P(n) \Rightarrow P(n+1)$]

Assume $n \in \mathbb{N}$ and that $P(n)$ is true (IH).

Then there is some $z \in \mathbb{Z}$ s.t.

$12^n - 1 = 11z$ — by IH.

So $12(12^n - 1) = 11 \cdot 12z$

rewritten, this means $12^{n+1} - 1 = 11(12z + 1)$

So, there is some $z' \in \mathbb{Z}$ s.t. $12^{n+1} - 1 = 11z'$,

just pick $z' = 12z + 1 \in \mathbb{Z}$ # by closure of × +

That is, $P(n+1)$ is true.

So, $\forall n \in \mathbb{N}$, $P(n) \Longrightarrow P(n+1)$, since n arbitrary

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

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

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

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

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

$3^0 = 1$
$3^1 = 3$
$3^2 = 9$
$3^3 = 27$
$3^4 = 81$

How many base cases do we need?

1 base case!

(formal proof written after lecture) →

$P(n)$:

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

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

Proof that $\forall n \in \mathbb{N}, P(n)$, by mathematical induction

Base case: If $n = 0$, then $3^0 = 1 \in \{1, 3, 7, 9\}$, so $P(0)$ is true.

Induction step [show that $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$]

Assume $n \in \mathbb{N}$ and $P(n)$ is true. ← (Induction hypothesis) IH

Then there is some $k \in \mathbb{N}$ and $t \in \{1, 3, 7, 9\}$ such that $3^n = 10k + t$, by IH. This means that $3^{n+1} = 3 \cdot 3^n = 3(10k + t) = 30k + 3t$. There are 4 possible cases for t:

Case 1, $t = 1$: Then $3^{n+1} = 30k + 3 = 10(3k) + 3$, so the units digit $3 \in \{1, 3, 7, 9\}$.

Case 2, $t = 3$: Then $3^{n+1} = 30k + 9$, so its units digit $9 \in \{1, 3, 7, 9\}$.

→

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

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

<u>Case 3, $t = 7$</u> Then $3^{n+1} = 30k + 21 = 10(3k+2) + 1$, so the units digit is $1 \in \{1, 3, 7, 9\}$

<u>Case 4, $t = 9$</u> Then $3^{n+1} = 30k + 27 = 10(3k+2) + 7$, So the units digit is $7 \in \{1, 3, 7, 9\}$.

In all 4 possible cases, $t \in \{1, 3, 7, 9\}$, so it follows that 3^{n+1} has its unit digit in $\{1, 3, 7, 9\}$, that is $P(n+1)$

So, $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$, since by assuming $P(n)$ for an arbitrary n we derive $P(n+1)$.

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

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