CSC236 Lecture 01: Theory of Computation

Hisbaan Noorani

September 10, 2021

Contents

1 Why reason about computing

- You're not just hackers anymore
  Sometimes you need to analyze code before it runs. Sometimes it should never be run!
- Can you test everything?
  Infinitely many inputs: integers, strings, lists.
- Careful, you might get to like it... (?!*)

2 How to reason about computing

- It's messy...
  interesting problems fight back.

You need to draft, re-draft, and re-re-draft.

You need to follow blind alleys until you find a solution.

You can also find a solution that isn't wrong, but could be better.

- It's art...

  Strive for correctness, clarity, surprise, humor, pathos, and others.

3 How to do well in this course

- read the syllabus as a two-way promise
- question, answer, record, synthesize

  try annotating blank slides.
- collabourate with respect

  You need computerscience friends who are respectful and constructively critical.

4 Assume that you already know

- Chapter 0 material from *Introduction to THeory of Computation.*
- CSC110/111 material, especially proofs and big-$\mathcal{O}$.

5 By December you'll know

- undersatnd and use several flavours of induction.

  some of these flavours will taste new
- Formal languages, regular languages,regular expressions

  Sets of strings
- complexity and correctness of programs — both recursive and iterative

6 domino fates foretold

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

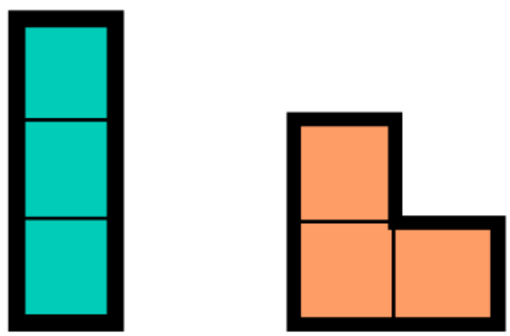
If the inital case works, and each case that works implies its successor works, then all cases work

7 Simple induction outline

- inductive step: introduce n and inductive hypothesis $H(n)$
  - derive conclusion $C(n)$: show that $C(n)$ follows from $H(n)$, indicating **where** you use $H(n)$ and why that is valid.
- Verify base case(s): verify that the claim is true for any cases not covered in the inductie step
- In simple induction $C(n)$ is just $H(n+1)$

8 Trominoes

See `https://en.wikipedia.org/wiki/Tromino`



Can an $n \times n$ square grid, with one subsquare removed, be tiled (covered withotu overlapping) by "chair" trominoes?

- 1×1: Yes.
- 2×2: Yes.
- 3×3: No. The remaining number of squares is not divisible by 3.
- 4×4: Yes.

$P(n)$: a $2^n \times 2^n$ square grid, with one subsquare removed, can be tiled (covered without overlapping) by "chair" trominoes.

<u>*Pf*</u>:

i. Induction on n

Let n be an arbitary, fixed, natural number. (Let $n \in \mathbb{N}$).

Assume $P(n)$, that is a $2^n \times 2^n$ grid, with one square removed can be tiled with "chairs."

I will prove $P(n+1)$, that is a $2^{n+1} \times 2^{n+1}$ grid, with one square removed can be tiled by chairs.

Let G be a $2^{n+1} \times 2^{n+1}$ grid with one square removed. Notice that G can be decomposed into four $2^n \times 2^n$ disjoint quadrant grids. We may assyme, WLOG (wihout loss of generality) that the missing square is in the upper-right quadrant, since otherwise just rotate it there, and rotate back when done. By $P(n)$ I can tile the upper-right quadrant, minus the missing square. By $P(n)$ 3 more times, I can tile the remaining 3 quadrants, omitting for a moment the 3 tiles nearest the centre of G, with chairs. The briefly omitted squares form a chair! So I complete the tiling by adding one more chair. Thus $P(n+1)$.

ii. Base Case

A $2^0 \times 2^0$ grid, with one square removed, is just empty space! This can be tiled with 0 charis. So $P(0)$ is true.

CSC236 Lecture 02: Basic Induction

Hisbaan Noorani

September 13, 2021

Contents

1 $3^n \geq n^3$?

1.1 Scratch Work

scratch work: check for a few values of n:

$3^0 = 1 \geq 0 = 0^3$ ✓

$3^1 = 1 \geq 1 = 1^3$ ✓

$3^2 = 9 \geq 8 = 2^3$ ✓

$3^3 = 27 \geq 27 = 3^3$ ✓

$3^4 = 81 \geq 64 = 4^3$ ✓

$3^{-1} = \frac{1}{3} \geq -1 = -1^3$ ✓

$3^{2.5} =< 2.5^3 = 4^3$ $\times$

1.2 Simple Induction

i. Induction on n

Let $n \in \mathbb{N}$. Assume $H(n)\ :\ 3^n \geq n^3$. I will prove $H(n+1)$ follows, that is $3^{n+1} \geq (n+1)^3$.

$$
\begin{aligned}
& 3^{n+1} \\
&= 3 \cdot 3^n \\
&\geq 3 \cdot n^3 \\
&= n^3 + n^3 + n^3 \\
&\geq n^3 + 3n^2 + 9n && \text{(since } n \geq 3\text{)} \\
&\geq n^3 + 3n^2 + 3n + 6n \\
&= n^3 + 3n^2 + 3n + 1 && \text{(since } 6n \geq 1\text{)} \\
&= (n+1)^3
\end{aligned}
$$

And thus we have shown that, starting at $n = 3$, $H(n) \implies H(n+1)$.

ii. Base Case

$3^3 \geq 3^3$ so $P(3)$ holds.
$3^2 \geq 2^3$ so $P(2)$ holds.
$3^1 \geq 1^3$ so $P(1)$ holds.
$3^0 \geq 0^3$ so $P(0)$ holds.

And thus, we have shown $\forall n \in \mathbb{N}, 3^n \geq n^3$, as needed.

CSC236 Lecture 03: Complete Induction

Hisbaan Noorani

September 17, 2021

Contents

1 Complete Induction

- Every natural number greater than 1 has a prime factorization

$$\begin{aligned}
2 &= 2 \\
3 &= 3 \\
4 &= 2 \times 2 \\
5 &= 5 \\
6 &= 2 \times 3 \\
7 &= 7 \\
8 &= 2 \times 2 \times 2 \\
9 &= 3 \times 3 \\
10 &= 2 \times 5
\end{aligned}$$

- How does the factorization of 8 help with the factorization of 9?

  The fact that 8 can be expressed as a product of primes has nothing to do with 9 being a product of primes.

2 Notational Convenience

Sometimes you will see the following:

$$\bigwedge_{k=0}^{k=n-1} P(k)$$

... as equivalent to

$$\forall k \in \mathbb{N}, k < n \implies P(k)$$

3 More dominos

$$\left(\forall n \in \mathbb{N}, \left[\bigwedge_{k=0}^{k=n-1} P(k)\right] \implies P(n)\right) \implies \forall n \in \mathbb{N}, P(n)$$

If all the previous cases always imply the current case then all cases are true.

4 Complete induction outline

- **Inductive step**: introduce n and state inductive hypothesis $H(n)$
  - **Derive conclusion** $C(n)$: show that $C(n)$ follows from $H(n)$, indicating hwere you use $H(n)$ and why that is valid.
- **Verify base case(s)**: verify that the claim is true for any cases not covered in the inductie step

This is the same outline as simple induction but we modify the inductive hypothesis, $H(n)$ so that it assuems the main claim for every natural number from the starting point up to $n-1$, and the conclusion, $C(n)$ is now the main claim for n.

5 Watch the base cases, part 1

$$f(n) = \begin{cases} 1 & n \leq 1 \\ \left[f(\lfloor\sqrt{n}\rfloor)\right]^2 + 2f(\lfloor\sqrt{n}\rfloor) & n > 1 \end{cases}$$

Check a few cases, and makea conjecture:

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 1 \\ f(2) &= 3 \\ f(3) &= 3 \\ f(4) &= 15 \\ f(5\ldots15) &= 15 \\ f(16) &= 255 \end{aligned}$$

All of these things are divisible by 3. The square of something that is divisible by 3 is still divisible by 3 and the double of something that is divisibly by 3 is still divisibly by 3.

6 For all natural numebrs $n > 1, f(n)$ is a multiple of 3?

For natual numbers n define $P(n) : f(n)$ is a multiple of 3.

I will prove, using complete induction, that $\forall n > 1, P(n)$.

i. Induction on n

Let $n \in N$. Assume $n > 1$. Also assume that $P(k)$ is true for all natural numbers k less than n, and greater than 1.

Notice that the floor of the square root of n is greater than 1. Also, the square root of n is less than n (since $n > 1 \implies n^2 > n \implies n > \sqrt{n}$).

Thus by the induction hypothesis, I have $P(\left\lfloor \sqrt{(n)} \right\rfloor)$, this number is a multiple of 3.

Let $k \in \mathbb{N}$ s.t. $\lfloor \sqrt{n} \rfloor = 3k$, so $f(n) = (3k)^2 + 2\,(3k) = 3\left(3k^2 + 2k\right)$, a multiple of 3.

So $P(n)$ follows in both possible cases.

ii. Base Cases

$P(2)$ claims that $f(2) = 3$ is a multiple of 3, which is true.

$P(3)$ claims that $f(3) = 3$ is a multiple of 3, which is true.

7 Zero pair free binary strings, zpfbs...

Deonte by $zpfbs\,(n)$ the number of binary strings of length n That contain no paris of adjacent zeros. What is $zpfbs\,(n)$ for the first few natural numbers n?

$$
\begin{aligned}
zpfbs\,(0) &= 1\\
zpfbs\,(1) &= 2\\
zpfbs\,(2) &= 3\\
zpfbs\,(3) &= 5\\
zpfbs\,(4) &= 8\\
zpfbs\,(5) &= 13\\
&\cdots\\
zpfbs\,(n) &= zpfbs\,(n-1) + zpfbs\,(n-2)
\end{aligned}
$$

CSC236 Lecture 04: Complete Induction 2

Hisbaan Noorani

September 20, 2021

Contents

1 Zero Pair-Free Binary Strings

Deonte by $zpfbs\,(n)$ the number of binary strings of length n That contain no paris of adjacent zeros. What is $zpfbs\,(n)$ for the first few natural numbers n?

$$\begin{aligned}
zpfbs\,(0) &= 1\\
zpfbs\,(1) &= 2\\
zpfbs\,(2) &= 3\\
zpfbs\,(3) &= 5\\
zpfbs\,(4) &= 8\\
zpfbs\,(5) &= 13\\
&\cdots\\
zpfbs\,(n) &= zpfbs\,(n-1) + zpfbs\,(n-2)
\end{aligned}$$

$$f(n) = \begin{cases} 1, & n = 0 \\ 2, & n = 1 \\ f(n-1) + f(n+2), & n > 1 \end{cases}$$

$\forall n \in \mathbb{N}$, defined predicate $P(n)$ as: $f(n) = zpfbs\,(n)$

Prove by complete induction that for all natural numbers n, $P(n)$.

Let $n \in \mathbb{N}$. Assume that P is true for $0, \ldots, n-1$. I will show that $P(n)$ follows.

For the case $n \geq 2$: Partition the zero-pair-free binary strings of length n into those that end in 1 and those that end in 0. Those that end in 1 are simply those of length $n-1$. with a 1 appended, and by $P(n-1)$ (since $n-1 < n$ and $n-1 \geq 0$, $n \geq 1$), there are $f(n-1)$ of these. Those that end in 0 must actually end in 10 (otherwise they are a zero-pair), and by $P(n-2)$ (since $n-2 \leq n$ and $n-2 \geq 0$, $n \geq 2$), there are $f(n-2)$ of these. Altogether there are $f(n-1)+f(n-2)$ zero-pair-free binary strings of length n when $n \geq 2$, which is $P(n)$.

For the base case $n = 0$: There is one binary string (the empty one) of length 0, and it is zero-pair-free, and $f(0) = 1$ and $P(0)$ is true.

For the base case $n = 1$: There are two binary strings of length 1, and neither have pairs of zeros, and $f(1) = 2$ so $P(1)$ is true.

Thus in all possible cases, $P(n)$ follows.

2 Every natural number greater than 1 has a prime factorization

Each natural number n, let predicate $P(n)$ be: n can be expressed as a product of primes.

Prime factorization: represent as product of 1 or more primes.

Prove by complete induction that for all natural numbers n, $P(n)$.

Let $n \in \mathbb{N}$ s.t. $n > 1$. Assume P is true for $2, \ldots, n-1$. I will show that $P(n)$ follows.

Case n is composite: By definition, n has a natural number factor f_1 such that $1 < f_1 < n$. By $P(f_1)$ (since $1 < f_1 < n$) we know f_1 can be expressed as a product of primes. Let $f_2 = \frac{n}{f_1}$, since $f_1 > 1$, we know that $\frac{n}{f_1} < n$, and also since $f_1 < n$, we know that $\frac{n}{f_1} > \frac{f_1}{f_1} = 1$. Since $f_1 > 1$, then $f_1 = \frac{n}{f_2} > 1$, so $n > f_2$. So, by $P(f_2)$, we know that f_2 can be expressed as a product of primes. Therefore since f_1 and f_2 are both products of primes, $n = f_1 \times f_2$ is a product of primes and $P(n)$ follows.

Case n is prime: Then n is its own primes factorization, and $P(n)$ follows.

In all possible cases, $P(n)$ follows.

CSC236 Lecture 05: Recurrences, Structural Induction

Hisbaan Noorani

September 24, 2021

Contents

1 Recursively defined function

Recall:

$$f(n) = \begin{cases} 1 & n = 0 \\ 2 & n = 1 \\ f(n-1) + f(n-2) & n > 1 \end{cases}$$

For comparison, let

$$r_1 = \frac{1+\sqrt{5}}{2},\ r_2 = \frac{1-\sqrt{5}}{2},\ a = \frac{\sqrt{5}+3}{2\sqrt{5}},\ b = \frac{\sqrt{5}-3}{2\sqrt{5}}$$

... and define

$$f'(n) = ar_1^n + br_2^n$$

Compare the first few values of $f(n)$ to the first few values of $f'(n)$

$$\begin{aligned} f(0) &= 1, \quad f'(0) = 1 \\ f(1) &= 2, \quad f'(1) = 2 \\ f(2) &= 5, \quad f'(2) = 5 \\ f(3) &= 8, \quad f'(3) = 8 \\ f(4) &= 13, \quad f'(4) = 13 \end{aligned}$$

2 Prove that $\forall n \in \mathbb{N}, f(n) = f'(n)$

$\forall n \in \mathbb{N}$, define $P(n)$ by $f(n) = f'(n)$.

Prove by complete induction that $\forall n \in \mathbb{N}, P(n)$. It helps to verify $1 + r_1 = r_1^2$ and $1 + r_2 = r_2^2$.

Let $n \in \mathbb{N}$. Assume the induction hypothesis, $\forall k \in \mathbb{N}$ s.t. $k < n$ has $f(k) = f'(k)$.

- Case $n > 1$:

$$
\begin{aligned}
f(n) &= f(n-1) + f(n-2) && \text{(by definition)} \\
&= ar_1^{n-1} + br_2^{n-1} + ar_1^{n-2} + ar_2^{n-2} && \text{(by IH, since } 0 \leq n-2, n-1 < n\text{)} \\
&= a\left(r_1^{n-2} + r_1^{n-1}\right) + b\left(r_2^{n-2} + r_2^{n-1}\right) \\
&= a\left(r_1^{n-2}\right)(1 + r_1) + b\left(r_2^{n-2}\right)(1 + r_2) \\
&= a\left(r_1^{n-2}\right)\left(r_1^2\right) + b\left(r_2^{n-2}\right)\left(r_2^2\right) \\
&= ar_1^n + br_2^n \\
&= f'(n)
\end{aligned}
$$

  And thus $\forall n > 1, P(n)$ holds.

- Case $n = 0$: $f(0) = 1 = f'(0)$, by evaluating $f'(0)$ so $P(0)$ holds.
- Case $n = 1$: $f(1) = 2 = f'(1)$, by evaluating $f'(1)$ so $P(1)$ holds.

Thus, in all possible cases, $P(n)$ holds. ■

3 Define sets inductively

One way to define the natural numbers:

- $\mathbb{N}$: The smallest set such that
  1. $0 \in \mathbb{N}$
  2. $n \in \mathbb{N} \implies n + 1 \in \mathbb{N}$

By **smallest** we mean $\mathbb{N}$ has no proper subsets that satisfy these two conditions. If we leave out **smallest**, what other sets satisfy the definition? $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z},$ etc.

4 What can you do with it?

The definition on the previous page defined the simplest natural number (0) and the rule to produce new natural numbers from old (add 1). Proof using Mathematical Induction work by showing that 0 has some property, and then that the rule to produce natural numbers preserves the property, that is

1. show that $P(0)$ is true for basis, 0.
2. Prove that $\forall n \in \mathbb{N}, P(n) \implies P(n+1)$.

5 Other structurally-defined sets

Define $\mathcal{E}$: The smallest set such that

1. $x, y, z \in \mathcal{E}$
2. $e_1, e_2 \in \mathcal{E} \implies (e_1 + e_2), (e_1 - e_2), (e_1 \times e_2), (e_1 \div e_2) \in \mathcal{E}$

Form some expressions in $\mathcal{E}$. Count the number of variables (sumbols from $\{x, y, z\}$) and the number of operators symbols from $\{+, -, \times, \div\}$. Make a conjecture

$(x + y), (x \times y) \in \mathcal{E}$

$((x + y) \times (x \times y)) \in \mathcal{E}$

Let $\mathrm{vr}(e)$ count the number of variables in e and let $\mathrm{op}(e)$ count the number of operators in e.

$$\forall e \in \mathcal{E}, \mathrm{vr}(e) = \mathrm{op}(e) + 1$$

6 Structural induction

To prove that a property is true for all $e \in \mathcal{E}$, parallel the recursive set definition:

- **Verify the base case(s)**: Show that the property is true for the simplest members, $\{x, y, z\}$, that is show $P(x), P(y), P(z)$.
- **Inductive step**: Let e_1 and e_2 be arbitrary elements of $\mathcal{E}$. Assume $H(\{e_1, e_2)\}$: $P(e_1)$ and $P(e_2)$, that is e_1 and e_2 have the property.
  - **Show that $C(\{e_1, e_2\})$ follows:**
    All possible combinations of e_1 and e_2 have the property, that is $P((e_1 + e_2)), P((e$