CSE 311

Foundations of Computing I

* All slides are a combined effort between previous instructors of the course

Administrivia Read me!!

If you want to use a token on HW1-HW3, you need to sign up for it by 11:30pm tonight.

Midterm practice materials are up on the website.

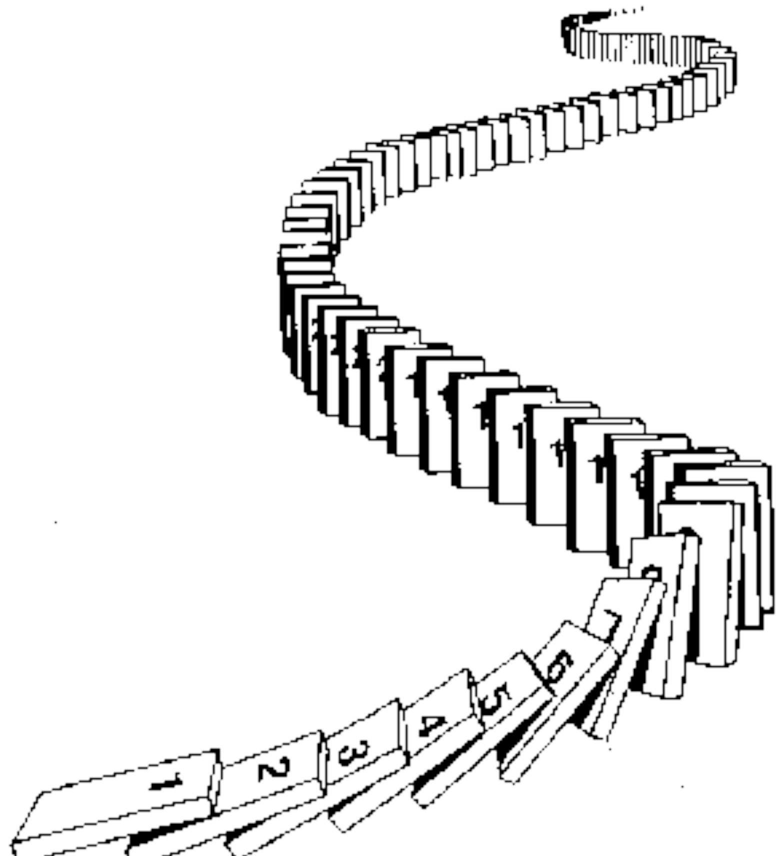
The midterm will be on Wed, May 4 from 4:30pm – 6:00pm in JHN 102

If you cannot make this time, I need to know by **Friday** to schedule a make-up exam.

~~There will be two review sessions time/location TBD.~~

CSE 311: Foundations of Computing

Lecture 14: Induction



Mathematical Induction $\forall (n \in \mathbb{N})\ P(n)$

Method for proving statements about all natural numbers

– **A new logical inference rule!**
  - It only applies over the natural numbers
  - The idea is to **use** the special structure of the naturals to prove things more easily

– **Particularly useful for reasoning about programs!**

```
for(int i=0; i < n; n++) { … }
```

  - Show P(i) holds after i times through the loop

```
public int f(int x) {
    if (x == 0) { return 0; }
    else { return f(x – 1); }
}
```

  - f(x) = x for all values of x ≥ 0 naturally shown by induction.

Prove $\forall(a, b \in \mathbb{Z})\ \forall(i \in \mathbb{N})\ (a \equiv b \pmod{n} \rightarrow a^i \equiv b^i \pmod{n})$

Let $a, b \in \mathbb{Z}$ be arbitrary. Let $i \in \mathbb{N}$ be arbitrary.

Suppose $a \equiv b \pmod{n}$.

We know $\big(a \equiv b \pmod{n} \land a \equiv b \pmod{n}\big) \rightarrow a^2 \equiv b^2 \pmod{n}$ by multiplying congruences. So, applying this repeatedly, we have:

$$\big(a \equiv b \pmod{n} \land a \equiv b \pmod{n}\big) \rightarrow a^2 \equiv b^2 \pmod{n}$$
$$\big(a^2 \equiv b^2 \pmod{n} \land a \equiv b \pmod{n}\big) \rightarrow a^3 \equiv b^3 \pmod{n}$$
$$\ldots$$
$$\big(a^{i-1} \equiv b^{i-1} \pmod{n} \land a \equiv b \pmod{n}\big) \rightarrow a^i \equiv b^i \pmod{n}$$

The "…"s is a problem! We don't have a proof rule that allows us to say "do this over and over".

So, make one!

Domain: Natural Numbers

$$P(0)$$

$$\forall\, k\, (P(k) \rightarrow P(k+1))$$

$$\therefore \forall\, n\, P(n)$$

$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad \ldots$

$P(4)$

Induction Is A Rule of Inference

Domain: Natural Numbers

$$
\begin{array}{l}
P(0) \\
\forall\, k\, (P(k) \;\rightarrow\; P(k+1)) \\
\hline
\therefore\; \forall\, n\, P(n)
\end{array}
$$

How does this technique prove ~~P(5)~~ P(4)?

$P(0) \rightarrow P(1)$

$P(0) \xrightarrow{\text{MP}} P(1) \qquad P(2) \qquad P(3) \qquad P(4)$

Induction Is A Rule of Inference

Domain: Natural Numbers

$$\begin{array}{l} P(0) \\ \forall\, k\, (P(k) \rightarrow P(k+1)) \\ \hline \therefore \forall\, n\, P(n) \end{array}$$

How does this technique prove P(5)?

	✓	✓	✓	✓	✓	✓
By Induction:	$P(0)$	$P(0) \rightarrow P(1)$	$P(1) \rightarrow P(2)$	$P(2) \rightarrow P(3)$	$P(3) \rightarrow P(4)$	$P(4) \rightarrow P(5)$
To Prove:	$P(0)$	$P(1)$	$P(2)$	$P(3)$	$P(4)$	$P(5)$
	✓	✓	✓	✓	✓	✓

First, we prove P(0).

Since P(n) → P(n+1) for all n, we have P(0) → P(1).

Since P(0) is true and P(0) → P(1), by Modus Ponens, P(1) is true.

Since P(n) → P(n+1) for all n, we have P(1) → P(2).

Since P(1) is true and P(1) → P(2), by Modus Ponens, P(2) is true.

Translating to an English Proof

$$P(0)$$
$$\forall\, k\, (P(k) \rightarrow P(k+1))$$
$$\therefore\ \forall\, n\, P(n)$$

1. Prove P(0)		**Base Case**
2. Let k be an arbitrary integer ≥ 0		**Inductive Hypothesis**
3.1. Assume that P(k) is true		
3.2. ...		**Inductive Step**
3.3. Prove P(k+1) is true		
3. $P(k) \rightarrow P(k+1)$	Direct Proof Rule	**Conclusion**
4. $\forall k\, (P(k) \rightarrow P(k+1))$	Intro $\forall$: 2, 3	
5. $\forall n\, P(n)$	Induction: 1, 4	

$\forall$

Translating To An English Proof

1. Prove P(0)		**Base Case**
2. Let k be an arbitrary integer ≥ 0		**Inductive Hypothesis**
3.1. Assume that P(k) is true		
3.2. ...		**Inductive Step**
3.3. Prove P(k+1) is true		
3. $P(k) \rightarrow P(k+1)$	Direct Proof Rule	
4. $\forall k\,(P(k) \rightarrow P(k+1))$	Intro ∀: 2, 3	
5. $\forall n\, P(n)$	Induction: 1, 4	**Conclusion**

Let P(n) be "[truth value]"

We will show that P(n) is true for every $n \in \mathbb{N}$ by Induction.

Base case:
Prove P(0)

IH: Suppose P(k) is true for some $k \in \mathbb{N}$

IS: using IH, Prove P(k+1)

Conclusion

Translating To An English Proof

1. Prove P(0) **Base Case**
2. Let k be an arbitrary integer ≥ 0 **Inductive Hypothesis**
   3.1. Assume that P(k) is true
   3.2. ... **Inductive Step**
   3.3. Prove P(k+1) is true
3. P(k) → P(k+1) Direct Proof Rule
4. ∀k (P(k) → P(k+1)) Intro ∀: 2, 3
5. ∀n P(n) Induction: 1, 4 **Conclusion**

Induction Proof Template

[...Define P(n)...]

We will show that P(n) is true for every $n \in \mathbb{N}$ by Induction.

Base Case: *[...proof of P(0) here...]*

Induction Hypothesis:

Suppose P(k) is true for some $\mathrm{k} \in \mathbb{N}$.

Induction Step:

We want to prove that P(k+1) is true.

[...proof of P(k+1) here...]

The proof of P(k+1) ***must*** *invoke the IH somewhere.*

So, the claim is true by induction.

5 Steps To Inductive Proofs In English

Proof:

1. "We will show that P(n) is true for every $n \geq 0$ by Induction."
2. "Base Case:" Prove P(0)
3. "Inductive Hypothesis:"

   Assume P(k) is true for some arbitrary integer $k \geq 0$"
4. "Inductive Step:" Want to prove that P(k+1) is true:

   Use the goal to figure out what you need.

   Make sure you are using I.H. and point out where you are using it. (Don't assume P(k+1) !!)
5. "Conclusion: Result follows by induction"

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

- We could try proving it with properties of summations?
- We could use calculus?
- Could this be induction?

Let $P(n) ::=$ " $\sum_{i=0}^{n} 2^i = \boxed{2^{n+1} - 1}$ "

We go by induction on n.

Base case ($n=0$): $\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1$

So $P(0)$ is true.

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

- We could try proving it with properties of summations?
- We could use calculus?
- Could this be induction?

Let $P(n)$ be "$\sum_{i=0}^{n} 2^i = 2^{n+1}$". We go by induction on n.

<u>Base Case (n=0):</u>

Note that $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$, which is exactly $P(0)$.

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

Let $P(n)$ be "$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$". We go by induction on n.

Base Case (n=0):

Note that $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$, which is exactly $P(0)$.

Induction Hypothesis:

Suppose $P(k)$ is true for some $k \in \mathbb{N}$.

Induction Step:

We want to show $P(k+1)$. That is, we want to show:

$$\sum_{i=0}^{k+1} 2^i = 2^{(k+1)+1} - 1$$

One of these steps

$$\sum_{i=0}^{k+1} 2^i = \ldots = \ldots = \ldots = 2^{n+1} - 1.$$

must use the IH.

So, the claim is true for all natural numbers by induction.

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

Let $P(n)$ be "$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$". We go by induction on n.

Base Case (n=0): Note that $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$, which is exactly $P(0)$.

Induction Hypothesis: Suppose $P(k)$ is true for some $k \in \mathbb{N}$.

Induction Step: We want to show $P(k+1)$. That is, we want to show: $\sum_{i=0}^{k+1} 2^i = 2^{(k+1)+1} - 1$

Note that $\sum_{i=0}^{k+1} 2^i = \left(\sum_{i=0}^{k} 2^i\right) + 2^{k+1}$ [by sums]

$= 2^{k+1} - 1 + 2^{k+1}$ [by IH]

$= 2^{k+1} + 2^{k+1} - 1$ (algebra)

$= 2(2^{k+1}) - 1$

$= 2^{k+2} - 1$

This is exactly $P(k+1)$. So, $P(k) \rightarrow P(k+1)$.

So, the claim is true for all natural numbers by induction.

We know (by IH)...

$\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$

We're trying to get...

$\sum_{i=0}^{k+1} 2^i = 2^{(k+1)+1} - 1$

Our goal is to find a sub-expression of the left that looks like the left side of the IH.

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

Let $P(n)$ be "$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$". We go by induction on n.

Base Case (n=0): Note that $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$, which is exactly $P(0)$.

Induction Hypothesis: Suppose $P(k)$ is true for some $k \in \mathbb{N}$.

Induction Step: We want to show $P(k+1)$. That is, we want to show: $\sum_{i=0}^{k+1} 2^i = 2^{(k+1)+1} - 1$

$$\text{Note that } \sum_{i=0}^{k+1} 2^i = \left(\sum_{i=0}^{k} 2^i\right) + 2^{k+1} \quad \textbf{[Splitting the summation]}$$

$$= \left(2^{k+1} - 1\right) + 2^{k+1} \quad \textbf{[By IH]}$$

$$= \left(2^{k+1} + 2^{k+1}\right) - 1 \quad \textbf{[Assoc. of +]}$$

$$= \left(2(2^{k+1})\right) - 1 \quad \textbf{[Factoring]}$$

$$= 2^{k+2} - 1 \quad \textbf{[Simplifying]}$$

Don't bother justifying the "obvious" steps. But make sure you say "by IH" somewhere.

This is exactly $P(k+1)$. So, $P(k) \rightarrow P(k+1)$.

So, the claim is true for all natural numbers by induction.

We know (by IH)...

$$\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$$

We're trying to get...

$$\sum_{i=0}^{k+1} 2^i = 2^{(k+1)+1} - 1$$

Our goal is to find a sub-expression of the left that looks like the left side of the IH.

Prove 1 + 2 + 3 + ... + n = n(n+1)/2

Let $P(n)$ be "$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$". We go by induction on n.

Base Case (n=0): $\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$ So, $P(0)$ is true.

Induction Hypothesis: Suppose $P(k)$ is true for some $k \in \mathbb{N}$.

Induction Step: We prove $P(k+1)$

$$\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^{k} i\right) + (k+1)$$

$$= \frac{k(k+1)}{2} + (k+1) \quad \text{by IH}$$

$$= \frac{(k+1)(k+2)}{2}$$

This is exactly $P(k+1)$. So, $P(k) \to P(k+1)$.

So, the claim is true for all natural numbers by induction.

We know (by IH)...

$$\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$$

We're trying to get...

Our goal is to find a sub-expression of the left that looks like the left side of the IH.

Prove 1 + 2 + 3 + … + n = n(n+1)/2

Let $P(n)$ be "$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$". We go by induction on n.

Base Case (n=0): Note that $\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$, which is exactly $P(0)$.

Induction Hypothesis: Suppose $P(k)$ is true for some $k \in \mathbb{N}$.

Induction Step: We want to show $P(k+1)$. That is, we want to show: $\sum_{i=0}^{k+1} i = \frac{(k+1)(k+2)}{2}$

Note that $\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^{k} i\right) + (k+1)$ **[Splitting the summation]**

$= \left(\frac{k(k+1)}{2}\right) + (k+1)$ **[By IH]**

$= (k+1)\left(\frac{k}{2} + 1\right) = (k+1)\left(\frac{k+2}{2}\right)$ **[Algebra]**

$= \frac{(k+1)(k+2)}{2}$ **[Algebra]**

This is exactly $P(k+1)$. So, $P(k) \rightarrow P(k+1)$.

So, the claim is true for all natural numbers by induction.

We know (by IH)…

$$\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$$

We're trying to get…

$$\sum_{i=0}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

Our goal is to find a sub-expression of the left that looks like the left side of the IH.

Prove $3 \mid 2^{2n} - 1$ for all $n \geq 0$.

Let $P(n)$ be "$3 \mid 2^{2n} - 1$." We go by induction on n.

<u>Base Case (n=0):</u>

<u>Induction Hypothesis:</u>

<u>Induction Step:</u>

We know (by IH)…

…which means…

We're trying to get…

…which is true if…