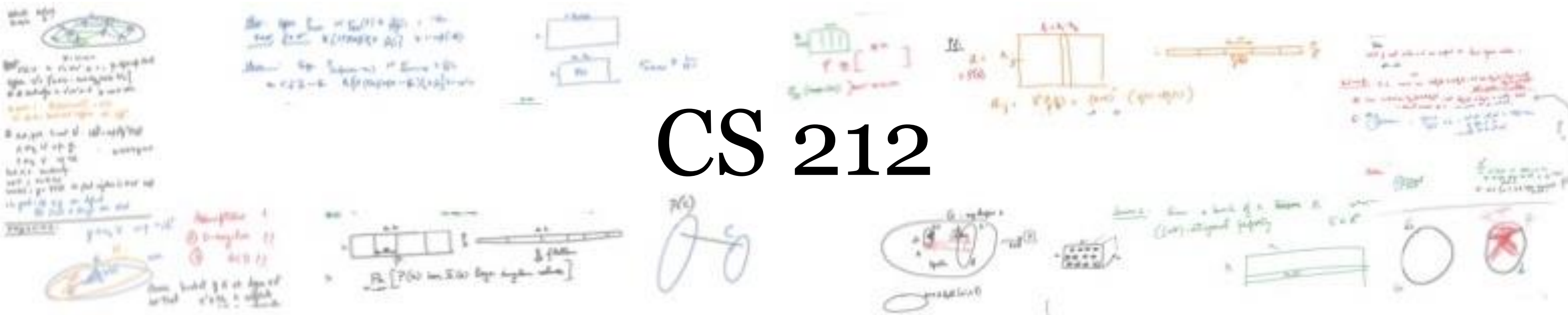


CS 212

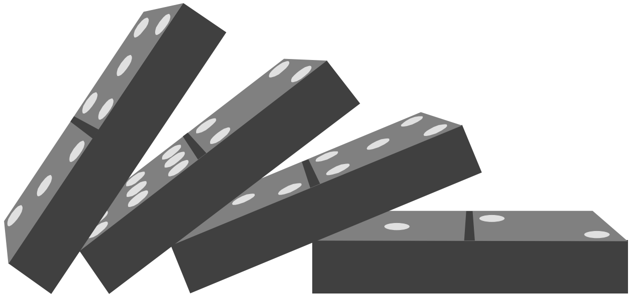
Mathematical Foundations of Computer Science

Lecture 4: Induction

Announcements

- Homework posted on CrowdMark.
  - Due Tuesday Oct 4 at 11:59 P.M.
  - Must be submitted individually
- Discussion sections started today
  - See Canvas syllabus for time/location

Induction

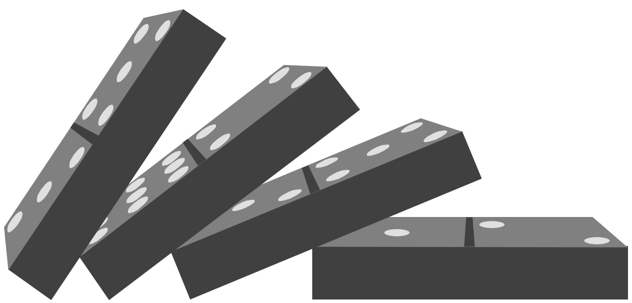


Induction can be used to

- Prove theorems
- Argue about correctness of programs
- Construct and define objects
  - Sequences, e.g., Fibonacci
  - Geometric objects, e.g., Fractals
  - Sets with cool properties, e.g., Cantor set

Dominoes

Domino Principle:
Line up any number of dominoes in a row; knock the first one over and they will all fall



Two requirements:

1. The first domino falls over
2. The dominoes are set up so that for all k, the kth domino knocks over the $k+1$th domino.

*Acknowledgement: This description of Induction based on Prof. Rudich and Prof. Gupta's course in CMU

Idea Behind Induction

Goal: Prove P(k) true for k=0,1,2,3,4,…

Idea: Prove first case , then prove "next" case.

Step 1: Prove $P(0)$ is true.

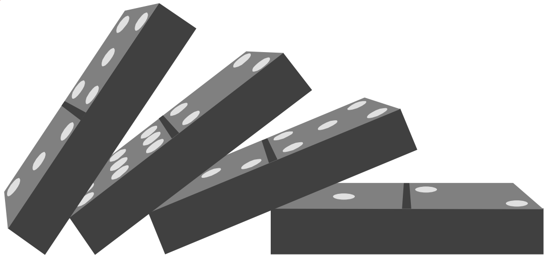
then: Show $P(0) \Rightarrow P(1)$

then: Show $P(1) \Rightarrow P(2)$

Step 2: Show $P(k) \Rightarrow P(k+1)$

Two Steps in Inductive proofs

To prove: For all $k \in \mathbb{N}$, predicate $P(k)$ is true.



Two steps:

1. Base case: *Establish that* $P(0)$ *is true.*
2. For all $k \in \mathbb{N}$: $P(k) \implies P(k+1)$

Assume that P(k) is true. Establish that P(k+1) is true.

Note: The assumption that $P(k)$ is true is called the induction hypothesis

4 year old Gauss knew this!

Theorem. For all $n \geq 1 \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$

Proof. We will prove by induction on k.

Let $P(k)$ be predicate: "$1 + 2 + \cdots + k = k(k+1)/2$"

1. Base case: *P(1) is true since 1 = (1)(1+1)/2=1.*

2. Hypothesis: *Assume $P(k)$ is true i.e.*

$$\underbrace{1 + 2 + \cdots + k}\quad = \quad k(k+1)/2$$

Derive $P(k+1)$: "$\underbrace{1 + 2 + \cdots + k} + (k+1) \quad = \quad (k+1)(k+2)/2$"

inductive hypothesis $\Rightarrow$ //

So p(k) true by induction

$$\frac{k(k+1)}{2} + k+1 = \frac{k^2+k}{2} + \frac{2k+2}{2} = \frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2}$$

Power of Inductive Proofs

+ A powerful tool to prove true statements involving natural numbers.

- Less revealing than direct proofs.

$1+2+\ldots+(n-1)+n$

$+\ n+n-1+\ldots+2+1$

$(n+1)+(n+1)+(n+1)+\ldots+(n+1)$

Warnings

- Base case is very important!
- Base case is not necessarily $k=0$.

$\begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}a&b\\c&d\end{bmatrix}=[$

Multiplying Matrices

Prove that for all integers $k \geq 1$, all the entries of $\begin{bmatrix}1&1\\0&1\end{bmatrix}^k$ are less than or equal to k.

Proof. By induction on k. P(k): "All entries of $\begin{bmatrix}1&1\\0&1\end{bmatrix}^k$ are at most k". *Base case:* $\begin{bmatrix}1&1\\0&1\end{bmatrix}^1 = \begin{bmatrix}1&1\\0&1\end{bmatrix}$. Hence true.

Assume $P(k)$ i.e. $\begin{bmatrix}1&1\\0&1\end{bmatrix}^k = \begin{bmatrix}a&b\\c&d\end{bmatrix}$ where $a,b,c,d \leq k$

$a+c\ ,\ b+d \leq 2k$

$$\begin{bmatrix}1&1\\0&1\end{bmatrix}^{k+1} = \begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix}^k \underset{\text{inductive hypothesis}}{=} \begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}a&b\\c&d\end{bmatrix} = \begin{bmatrix}a+c&b+d\\c&d\end{bmatrix}$$

So, is it false?

Is $P(2)$ true? $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ yes!

$P(3)$: $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$

$P(4)$: $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^4 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}$

$P(k)$: $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \stackrel{?}{=} \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$

Prove a stronger statement!

Inductive Hypothesis: $P(k)$ is "$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}^k = \begin{bmatrix}1 & k\\0 & 1\end{bmatrix}$"

$P(1)$: $\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}^1 = \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$ so true

Assume $P(k)$: $\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}^k = \begin{bmatrix}1 & k\\0 & 1\end{bmatrix}$ and prove $P(k+1)$

$$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}^{k+1} = \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}^k \overset{\text{induction hypo}}{=} \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}\begin{bmatrix}1 & k\\0 & 1\end{bmatrix} = \begin{bmatrix}1 & k+1\\0 & 1\end{bmatrix}$$

So $P(k+1)$ true. Hence all entries of $\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}^k$ are $\leq k$

Prove a stronger statement!

Takeaway:

1. *Often, to prove a statement inductively you may have to prove a stronger statement first!*
2. *Work out examples for small values of k*

Working out examples is a go to problem solving strategy!

What "stronger" means

Say that $P(k)$ is stronger then $Q(k)$

if $P(k)$ being true $\Rightarrow$ $Q(k)$ is true

$$P(k): \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$$

$Q(k)$: Entries of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k$ are $\leq \underline{k}$

Making Induction Stronger

$12 = 2^2 \cdot 3$

Factoring into Primes

Theorem. Every natural number $n \geq 2$ can be written as a product of primes (and powers of primes).

Proof. By induction on k. P(k) : 'k can be factored into primes'.

Base case: P(2) is true, since 2 is itself a prime.

Inductive Hypothesis (I.H): P(k) is true i.e.
k can be written as a product of primes.

Case 1: $k+1$ is prime. $\Rightarrow P(k+1)$ is true

$k + 1 = ?$

Case 2: $k+1$ not prime. $k+1 = ab$ where $2 \leq a, b < k$