Where we are

1. Logical reasoning
    - Propositions and Predicates
        - Laws of logic, Rules of Inference
        - Valid arguments
        - How to construct proofs
2. Sets
    - Set Operations: union, intersection, cross-product, difference, complement
    - Set identities
    - Set cardinality: finite, countably infinite, well-ordering principle, uncountable
3. Relations
    - Properties: reflexive, symmetric, transitive, equivalence, closures
4. Functions
    - Properties: injective, surjective, bijective

Where we're headed

Use what we've learned to build stronger proof techniques

- Principle of Induction

Use our proof techniques to solve problems

- Graph theory
  - Exploit structure in real world applications to create efficient solutions
- Number theory
  - Design cryptographic systems that are hard to crack
- Counting
  - How many instructions will my program execute?

Predicates over $\mathbb{N}$

Let $P(x)$ be a predicate over the natural numbers.

$$P(x): \ 0 + 1 + 2 + \cdots + x = x(x+1)/2$$

Propositions: $P(0): \quad 0 = 0 \cdot (0+1)/2$

$P(1): \ 0 + 1 = 1 \cdot (1+1)/2$

$P(2), P(3), P(4), \ldots$ all are true

Is each of these (infinitely many) propositions TRUE?

How do we prove the truth of infinitely many propositions?

Modus Ponens Revisited

Let $P(x)$ be a predicate over the natural numbers.

Suppose we are told that each of the following is true:

$$P(0)$$

$$P(0) \Rightarrow P(1)$$

We can conclude that $P(1)$ is true.

What if we're also told that $P(1) \Rightarrow P(2)$ is true?

We can conclude that $P(2)$ is true.

Modus Ponens Ad Infinitum

Suppose we are told that

$P(0)\ is\ true$

$P(0) \Rightarrow P(1)$

$P(1) \Rightarrow P(2)$

$P(2) \Rightarrow P(3)$

$P(3) \Rightarrow P(4)$

.

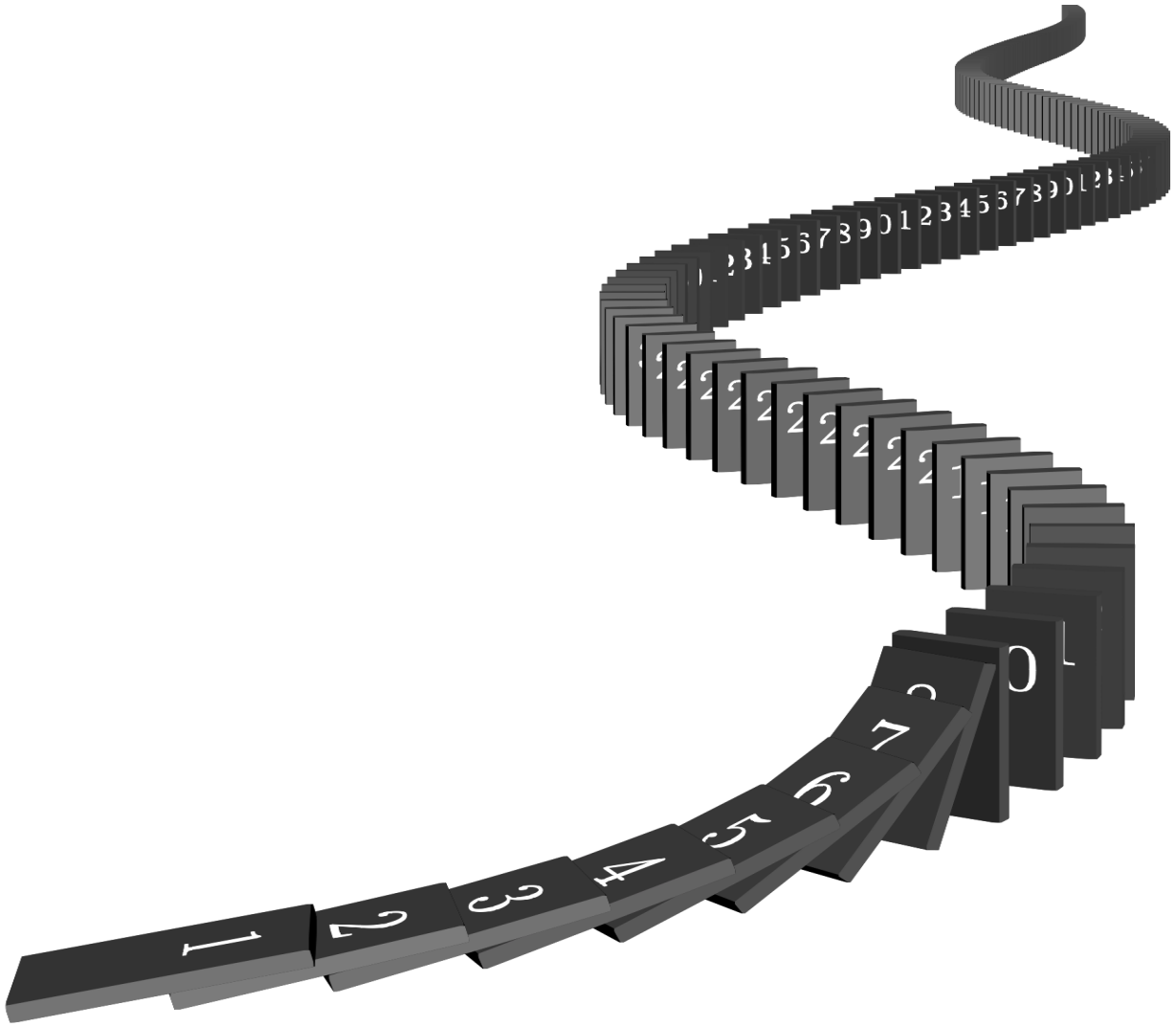
.

$for\ arbitrary\ k\colon\ \ P(k) \Rightarrow P(k+1)$

Can there exist a natural number m such that $P(m)$ is false?

What can we conclude?

Falling Dominoes



Initially all dominoes are standing.

When the first domino falls, will the rest all fall?

The first domino falls
If the first domino falls, the second domino falls
If the second domino falls, the third domino falls

If any domino falls, then so does the next one
Therefore, every domino will fall

$$P(0)$$
$$\underline{\forall k \geq 0:\ P(k) \Rightarrow P(k+1)}$$
$$\forall n \geq 0:\ \ P(n)$$

The Principle of Induction (PI)

$$\frac{\begin{array}{c} P(0) \\ \forall k \geq 0\colon\ P(k) \Rightarrow P(k+1) \end{array}}{\therefore\ \forall n \in \mathbb{N}\colon\ P(n)}$$

To prove that $P(x)$ is TRUE for all natural numbers:

Step 1. **(BASIS)** Show that $P(0)$ is TRUE

Step 2. **(INDUCTIVE HYPOTHESIS)** State $P(k)$, k is an arbitrary number

Step 3. **(INDUCTIVE STEP)** Show that $P(k) \Rightarrow P(k+1)$ is TRUE for all k

PI in Action

Theorem. $\forall n \in \mathbb{N}\ P(n)$, where $P(n)$: $\quad 0 + 1 + 2 + \cdots + n = n(n+1)/2$

PROOF:

Step 1. (Basis) $P(0)$: $\quad 0 = 0 \cdot (0+1)/2$ $\quad$ is TRUE.

Step 2. (Inductive Hypothesis) $P(k)$: $0 + 1 + \cdots + k = k(k+1)/2$

Step 3. (Inductive Step) $0 + 1 + \cdots + k + (k+1)$

$$= (0 + 1 + \cdots + k) + (k+1)$$

$$= k(k+1)/2 \ + \ (k+1) \ \text{(applying the inductive hypothesis } P(k))$$

$$= \ (k+1)(k/2 + 1)$$

$$= (k+1)(k+2)/2$$

In other words, $P(k+1)$ is TRUE.

So, we have shown that, for every $k \geq 0$, $\ P(k) \Rightarrow P(k+1)$, and the theorem follows from PI.

Another Predicate over $\mathbb{N}$

Consider the sequence created by summing the odd numbers

$$1, 1+3, 1+3+5, 1+3+5+7, 1+3+5+7+9, \ldots$$

The sequence is $1,\ 4,\ 9, 16, 25, \ldots$

But this is the same as $1^2, 2^2, 3^2, 4^2, 5^2, \ldots$

The first n odd numbers are $1, 3, \cdots, (2n-1)$

Let $P(n)$: $1 + 3 + \cdots + (2n-1) = n^2$

$P(1)$: $1 = 1^2$

$P(2)$: $1 + (2 \cdot 2 - 1) = 2^2$

Are $P(1), P(2), P(3), P(4), P(5), P(6), \ldots$ *all TRUE?*

PI to the rescue!

Theorem. $\forall n > 0 \;\; P(n)$, where $P(n)$: $\;\; 1 + 3 + \cdots + (2n-1) = n^2$

PROOF:

Step 1. (Basis) $P(1)$: $\;\; 1 = 1^2$ is TRUE.

Step 2. (Inductive Hypothesis) $P(k)$: $1 + \cdots + (2k-1) = k^2$

Step 3. (Inductive Step) $1 + \cdots + (2(k+1)-1)$

$$= (1 + \cdots + (2k-1)) \;\; + \;\; (2k+1)$$

$$= k^2 + (2k+1) \quad \text{(applying the inductive hypothesis } P(k))$$

$$= (k+1)^2$$

In other words, $P(k+1)$ is TRUE.

Since, for every k: $\quad P(k) \Rightarrow P(k+1)$, the theorem follows from PI.

The Principle of Induction (PI)

$$\frac{\begin{array}{c} P(0) \\ \forall k \geq 0\colon\ P(k) \Rightarrow P(k+1) \end{array}}{\therefore\ \forall n \in \mathbb{N}\colon\ P(n)}$$

To prove that $P(x)$ is TRUE for all natural numbers:

Step 1. **(BASIS)** Show that $P(0)$ is TRUE

Step 2. **(INDUCTIVE HYPOTHESIS)** State $P(k)$

Step 3. **(INDUCTIVE STEP)** Show that $P(k) \Rightarrow P(k+1)$ is TRUE for all k

To prove $P(k+1)$ we can assume that $P(k)$ is true.

Recursion: The Flip Side of Induction

Recursive function to compute the sum of natural numbers up to N.

```
(define (sum_upto n)
          (if (= 0 n) 0
                      (+ n sum_upto (- n 1))))
```

If `(sum_upto (- n 1))` is correct, then so is `(sum_upto n)`

In defining `(sum_upto n)` we assume that `(sum_upto (- n 1))` is correct.

The Happy Monastery

Monks do not communicate with each other (in any form).

Starting on Day 1, every morning all the monks gather in one place for morning prayers. Each monk sees every other monk (no monk is blind), but no word or note is exchanged, nor a gesture made.

After prayers, each monk spends the day in isolation.

If a monk had unknowingly sinned before Day 1, there is a mark on his forehead.

When a monk realizes he has a mark on his forehead, he must leave the monastery that same day.

Happy monks are unaware if they have sinned or if they have a mark. There are no mirrors.

No happy monk will leave unless he had proof that he was marked.

Happy monks are master logicians and make deductions instantaneously.

Will any monk ever leave the happy monastery?

Trouble Arrives at the Monastery

A stranger arrives for morning prayers on Day 1 and truthfully announces “I see that at least one of you has a mark on his forehead.”

What ensues?

If there is only one marked monk?

Two marked monks?

Three?

k marked monks?

Trouble Arrives at the Monastery

A stranger arrives for morning prayers on Day 1 and truthfully announces "I see that at least one of you has a mark on his forehead."

What ensues? If there are k marked monks?

Claim: All k marked monks leave on day k.

Proof:

BASIS: $k = 1$. $P(1)$: "The single marked monk leaves on day 1" (when the stranger announces that he sees a mark, the marked monk deduces that he is marked).

INDUCTIVE HYPOTHESIS: $P(k)$: If k monks are marked they all leave on day k.

INDUCTIVE STEP: If $k + 1$ monks are marked, then on day $k + 1$ each marked monk figures as follows:

If there were k marked monks, then (by the inductive hypothesis) they would have all left on day k. Furthermore, since I see k marked monks it must mean that I'm marked.

So, each marked monk leaves on day $k + 1$. In other words, $P(k) \Rightarrow P(k + 1)$.

By the Principle of Induction, it follows that $\forall n\, P(n)$.

WOP ⇒ PI

$$\frac{P(0) \ \wedge \ \forall k \geq 0: (P(k) \rightarrow P(k+1))}{\forall n \in \boldsymbol{N}: P(n)}$$

Proof. (by contradiction):

Let $C = \{n \in \boldsymbol{N}: P(n) = False\}$

Suppose that C is non-empty.

Then, by the well-ordering principle, it has a least element k.

Now, $k \neq 0$, because $P(0)$ is true. Therefore $k > 0$.

Since $k - 1 \notin C, P(k-1) = True$

By the inductive step, $P(k-1) \Rightarrow P(k)$

Therefore, $P(k)$ is true. Contradiction!

Therefore, C is empty and PI is proved.