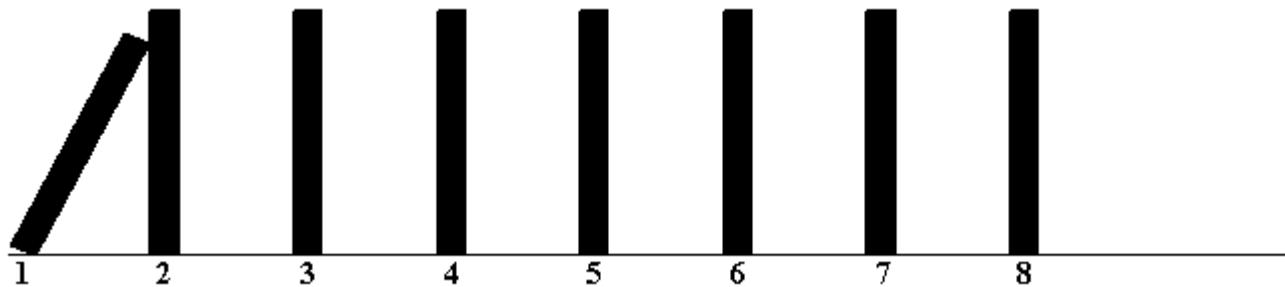
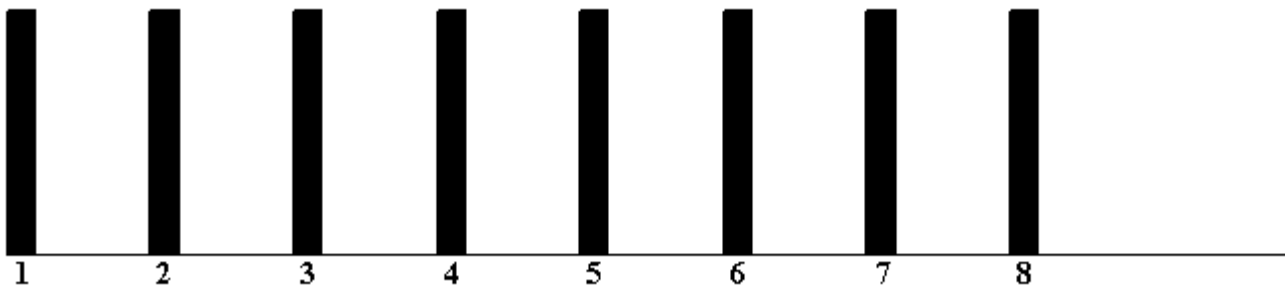


Discrete Mathematics for Computer Science

Lecture 7

Mathematical Induction



Example 1

Prove with mathematical induction that for all

$$n \in \mathbb{N}, n \geq 1: \sum_{i=1}^n (2i-1) = n^2$$

Proof:

1. Basis Step:

The statement is true for $n = 1$, because:

$$\sum_{i=1}^1 (2i-1) = (2 \cdot 1 - 1) = 1 \quad \text{and also} \quad 1^2 = 1$$

Proof (continued)

2. Induction Step:

Let $k \geq 1$ and suppose that:

$$\sum_{i=1}^k (2i - 1) = k^2 \quad \mathbf{IH} \text{ (Induction Hypothesis)}$$

We will (try to) show that IH implies:

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

Proof (continued)

2. Show that for any $k \geq 1$

$$\sum_{i=1}^k (2i-1) = k^2 \quad \text{IH} \quad \text{implies} \quad \sum_{i=1}^{k+1} (2i-1) = (k+1)^2$$

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

IH $\rightarrow = k^2 + (2(k+1)-1)$

$$= k^2 + 2k + 1$$

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

From 1 and 2 we conclude that

for all $n \geq 1$: $\sum_{i=1}^n (2i-1) = n^2$

Example 2

$$0^2 + 0 + 41 = 41 \rightarrow \text{prime!}$$

$$1^2 + 1 + 41 = 43 \rightarrow \text{prime!}$$

$$2^2 + 2 + 41 = 47 \rightarrow \text{prime!}$$

$$3^2 + 3 + 41 = 53 \rightarrow \text{prime!}$$

$$4^2 + 4 + 41 = 61 \rightarrow \text{prime!}$$

Statement:

For all $n \geq 0$: $n^2 + n + 41$ is prime

Proof (?)

For all $n \geq 0$: $n^2 + n + 41$ is prime

1. Basis Step:

The statement is true for $n = 0$, because
 $0^2 + 0 + 41 = 41$ is prime.

2. Induction Step

Let $k \geq 0$, and suppose that

$k^2 + k + 41$ is prime **IH**

We will (try to) show that IH implies:

$(k + 1)^2 + (k + 1) + 41$ is prime

Proof (?) (continued)

2. Show that for any $k \geq 0$

$k^2 + k + 41$ is prime **IH**

implies $(k+1)^2 + (k+1) + 41$ is prime

Well: $(k+1)^2 + (k+1) + 41 = k^2 + 2k + 1 + k + 1 + 41$
 $= (k^2 + k + 41) + 2k + 2$ (*)

The first part is prime by IH.

But does this imply that also (*) is prime ???

No! The statement is not true for all n .

E.g. if we take $n = 41$:

$41^2 + 41 + 41 = 43 \cdot 41$ is not a prime!⁸

Mathematical Induction

Theorem 4.1

Let, for each $n \in \mathbb{Z}^+$, $S(n)$ be an open statement.

(so the truth value of $S(n)$ depends on n)

Then $S(n)$ is true for all $n \in \mathbb{Z}^+$ if:

1. $S(1)$ is true and

2. For all $k \in \mathbb{Z}^+$ the following implication holds:

$$S(k) \rightarrow S(k+1)$$

(1. is the Basis Step, 2. is the Induction Step)

Well-Orderings Principle of \mathbb{Z}^+

Every nonempty subset of \mathbb{Z}^+ contains a smallest element.

Remark:

- This is also true for \mathbb{N} , but not for \mathbb{Q}^+ and \mathbb{R}^+ .
- This principle is used in the Principle of Mathematical Induction

1. $S(1)$ is true and

2. For all $k \in \mathbb{Z}^+$: $S(k) \rightarrow S(k+1)$

Proof:

Let $F = \{t \in \mathbb{Z}^+ \mid S(t) \text{ is false}\}$ We will show that $F = \emptyset$.

We will show this by contradiction: Suppose: $F \neq \emptyset$.

Obviously $F \subseteq \mathbb{Z}^+$.

So, by the Well Orderings Principle of \mathbb{Z}^+ , F has a smallest element. Let $j \in F$ be this smallest element.

Then: $j > 1$, since $S(1)$ is true.

Moreover, $S(j-1)$ is true, because j is the smallest value for which $S(j)$ is false.

But this contradicts 2. (take $k = j - 1$),

since $S(j-1)$ true implies $S(j)$ true. Therefore $F = \emptyset$.

Remarks to Theorem 4.1

1. The Principle of Mathematical Induction not only holds for \mathbf{Z}^+ , but for each set of the form:

$$\{n_0, n_0 + 1, n_0 + 2, n_0 + 3, \dots\} \text{ with } n_0 \in \mathbf{Z}$$

2. We have seen that the Induction Step in a proof by Mathematical Induction is essential. But this is also the case for the Basis Step!

For example, by only verifying the Induction Step, one could “prove” the nonsense statement:

$$\sum_{i=1}^n (2i - 1) = n^2 + 137 \text{ for all } n \in \mathbf{Z}^+$$

Example 3

Prove with mathematical induction that for all $n \in \mathbb{N}$, $3 \mid (n^3 - n)$ (i.e, 3 divides $n^3 - n$)

In other words: there exists a $t \in \mathbb{Z}$ with $n^3 - n = 3t$

Proof:

1. Basis Step for $n = 0$:

$$0^3 - 0 = 0 = 3 \cdot 0 \quad (\text{take } t = 0)$$

Proof (continued)

2. Induction Step:

Let $k \geq 0$ and suppose there exists $t \in \mathbb{Z}$ with

$$k^3 - k = 3t \quad \text{IH}$$

We will show that there exists an $s \in \mathbb{Z}$ with:

$$(k+1)^3 - (k+1) = 3s$$

Well: $(k+1)^3 - (k+1)$

$$= k^3 + 3k^2 + 3k + 1 - (k+1)$$

IH

$$= (k^3 - k) + 3k^2 + 3k = 3t + 3k^2 + 3k$$

$$= 3(t + k^2 + k) \quad (\text{so: take } s = t + k^2 + k)$$

Example 4

Prove with mathematical induction that for all $n \in \mathbb{N}, n \geq 5$: $n^2 < 2^n$

Proof:

1. Basis Step:

The statement is true for $n = 5$, because:

$$5^2 = 25 \text{ and } 2^5 = 32$$

$$\text{So } 5^2 < 2^5$$

Proof (continued)

2. Induction Step:

Let $k \geq 5$ and suppose that $k^2 < 2^k$ **IH**

We will show that: $(k+1)^2 < 2^{k+1}$

Well: $(k+1)^2 = k^2 + 2k + 1 < 2^k + 2k + 1$

So it suffices to show that

$$2^k + 2k + 1 \leq 2^{k+1} \quad (= 2 \cdot 2^k)$$

So it suffices to show that $2k + 1 \leq 2^k$

This is straightforward, since $k \geq 5$:

$$2k + 1 < 2k + k = 3k < 5k \leq k \cdot k = k^2 < 2^k$$

Example 5 (Harmonic numbers)

Let, for $n \geq 1$,

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \sum_{i=1}^n \frac{1}{i}$$

Prove with mathematical induction that for all $n \geq 0$,

$$H_{2^n} \leq n + 1$$

Proof:

1. **Basis Step:**

The statement is true for $n = 0$, because:

$$H_{2^0} = H_1 = \sum_{i=1}^1 \frac{1}{i} = 1 \quad \text{and} \quad 1 \leq 0 + 1$$

Proof (continued)

$$H_n = \sum_{i=1}^n \frac{1}{i}$$

2. Induction Step:

Let $k \geq 0$ and suppose that $H_{2^k} \leq k + 1$ **IH**

We will show that IH implies $H_{2^{k+1}} \leq (k + 1) + 1$ **IH**

Well: $H_{2^{k+1}} = \sum_{i=1}^{2^{k+1}} \frac{1}{i} = \sum_{i=1}^{2^k} \frac{1}{i} + \sum_{i=2^k+1}^{2^{k+1}} \frac{1}{i} \leq k + 1 + \sum_{i=2^k+1}^{2^{k+1}} \frac{1}{i}$

Now it remains to show that

$$\sum_{i=2^k+1}^{2^{k+1}} \frac{1}{i} \leq 1$$

In expanded form: $\frac{1}{2^k+1} + \frac{1}{2^k+2} + \dots + \frac{1}{2^{k+1}} \leq 1$

This inequality holds, since its left hand side consists of 2^k terms which are all $\leq 1/2^k$:

$$\frac{1}{2^k+1} + \frac{1}{2^k+2} + \dots + \frac{1}{2^k+2^k} \leq \frac{1}{2^k} + \dots + \frac{1}{2^k} = \frac{2^k}{2^k} = 1$$