8. Mathematical Induction

WN Chin / Aaron Tan

AY2024/25 Semester 1

Mathematical Induction

- A very powerful method for showing a property is true for natural numbers (0, 1, 2, 3, …)
- It characterizes the natural numbers (by Dedekind-Peano axioms).

Importance of Mathematical Induction in Computer Science

- Mathematical induction (MI) plays a central role in discrete mathematics and computer science. It is a defining characteristics of *discrete* mathematics.
- MI and recursion are closely linked. Hence, proof of correctness for recursive algorithms are usually done with MI.
- Natural generalizations of induction characterize recursively defined objects.

8. Mathematical Induction

8.1 Sequences

- Definitions: Sequence, term, explicit formula. Sequence Builders.
- Summation notation; product notation; properties of summations and products.
- Change of variable; some common sequences.

8.2 Mathematical Induction I

- Principle of mathematical induction
- Examples: Sum of first *n* integers, sum of a geometric sequence

8.3 Mathematical Induction II

- Strong mathematical induction
- Example: Any integer > 1 is divisible by a prime number

8.4 Well-Ordering Principle

- Well-ordering principle for the integers

8.5 Recurrence Relations

- Definition
- Recursively defined sets
- Structural induction

Reference: Epp's Chapter 5 Sequences, Mathematical Induction and Recursion

8.1 Sequences

8.1.1. Definitions

Definitions: Sequence and Terms

A **sequence** is an ordered set with members called **terms**. Usually, the terms are numbers. A sequence may have infinite terms.

Examples:

- 1, 2, 4, 8, 16.
- 5, 8, 11, 14, 17, …
- $\frac{1}{2}, \frac{-3}{4}, \frac{5}{8}, \frac{-7}{16}, \frac{9}{32}, \cdots$

General form:

$$a_m, a_{m+1}, a_{m+2}, \cdots, a_n$$

where $m \leq n$.

The k in a_k is called a **subscript** or **index**.

Infinite sequence:

$$a_m, a_{m+1}, a_{m+2}, \cdots$$

An explicit formula for a sequence is a rule that shows how the values of a_k depend on k.

Example #1: Compute the first 5 terms of the sequence:

$$a_k = \frac{k}{k+1} \text{ for all integers } k \geq 1.$$

$$a_1 = \frac{1}{2}; a_2 = \frac{2}{3}; a_3 = \frac{3}{4}; a_4 = \frac{4}{5}; a_5 = \frac{5}{6}.$$

Does the following formula define the same sequence?

$$b_{k-1} = \frac{k-1}{k} \text{ for all integers } k \geq 2.$$

Yes.

Explicit Formula vs Seq Comprehension

Explicit Formula

$$a_k = \frac{k}{k+1} \text{ for all integers } k \geq 1.$$

$a_1 \,.\, a_2 \,.\, a_3 \;\ldots$

seq element separator

Sequence Comprehension

$a \;=\; [\; (k/k+1) \;:\; k \in [1..] \;]$

Type Signature: Seq(Q) = ([1,∞) → Q)

Sequence Equivalence

Explicit Formula

$$a_k = \frac{k}{k+1} \text{ for all integers } k \geq 1.$$

$$b_{k-1} = \frac{k-1}{k} \text{ for all integers } k \geq 2.$$

Sequence Comprehension

b = [*(k-1/k)* : $k \in$ [2..]]

a = [*(k/k+1)* : $k \in$ [1..]]

Are the two sequences a=b equal?

[*(k/k+1)* : $k \in$ [1..]] = [*(k-1/k)* : $k \in$ [2..]]

can add indexes if needed
for higher fidelity to explicit form

Set Comprehension (Zermelo–Fraenkel set theory)

Set Builder

order not important, duplicates discarded

$\{k \in U : R(x)\} : P(U)$ $\qquad$ $R : U \rightarrow \text{Bool}$

predicate

Set Replacement

$\{ f(k) : k \in S\} : P(B)$ $\qquad$ $f : S \rightarrow B$

replacement *generator*

Set Comprehension (an example)

$\{ f(k_1,k_2) : k_1 \in S_1, k_2 \in S_1, R(k_1, k_2)\} : P(S_3)$

$R : S_1 \times S_2 \rightarrow \text{Bool}$ $\qquad$ $f : S_1 \times S_2 \rightarrow S_3$

One replacement, multiple generators and multiple predicates

8.1.2. Summation Notation

Definition: Summation

If m and n are integers, $m \leq n$, the symbol

$$\sum_{k=m}^{n} a_k$$

is the **sum** of all the terms $a_m, a_{m+1}, a_{m+2}, \cdots, a_n$.

We say that $a_m + a_{m+1} + a_{m+2} + \cdots + a_n$ is the **expanded form** of the sum, and we write

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \cdots + a_n.$$

We call k the **index** of the summation, m the **lower limit** of the summation and n the **upper limit** of the summation.

Example #2: Write the following summation in expanded form: $\sum_{i=0}^{n} \frac{(-1)^i}{i+1}$

$$\sum_{i=0}^{n} \frac{(-1)^i}{i+1} = \frac{(-1)^0}{0+1} + \frac{(-1)^1}{1+1} + \frac{(-1)^2}{2+1} + \frac{(-1)^3}{3+1} + \cdots + \frac{(-1)^n}{n+1}$$
$$= \frac{1}{1} + \frac{-1}{2} + \frac{1}{3} + \frac{-1}{4} + \cdots + \frac{(-1)^n}{n+1} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{(-1)^n}{n+1}$$

Example #3: Express the following expanded form using summation notation:

$$\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \cdots + \frac{n+1}{2n}$$

$$\sum_{k=0}^{n} \frac{k+1}{n+k}$$

Summation can be expressed using recursive definition.

If m is any integer, then

$$\sum_{k=m}^{m} a_k = a_m$$

and

$$\sum_{k=m}^{n} a_k = \left(\sum_{k=m}^{n-1} a_k\right) + a_n \quad \text{for all integers } n > m.$$

By convention, an empty sum (eg: $\sum_{k=m}^{n} a_k$ where $m > n$) is equal to the additive identity 0.

Some sums can be transformed into telescoping sums, which then can be rewritten as a simple expression.

Example #4: Observe that

$$\frac{1}{k} - \frac{1}{k+1} = \frac{(k+1)-k}{k(k+1)} = \frac{1}{k(k+1)}.$$

Use the above to find a simple expression for $\sum_{k=1}^{n} \frac{1}{k(k+1)}$

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1}\right)$$

$$= \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots + \left(\frac{1}{n-1} - \frac{1}{n}\right) + \left(\frac{1}{n} - \frac{1}{n+1}\right)$$

$$= 1 - \frac{1}{n+1}$$

8.1.3. Product Notation

Definition: Product

If m and n are integers, $m \leq n$, the symbol

$$\prod_{k=m}^{n} a_k$$

is the **product** of all the terms $a_m, a_{m+1}, a_{m+2}, \cdots, a_n$.

We write

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \cdots \cdot a_n.$$

Sequences: Product Notation

Recursive definition for the product notation:

If m is any integer, then

$$\prod_{k=m}^{m} a_k = a_m$$

and

$$\prod_{k=m}^{n} a_k = \left(\prod_{k=m}^{n-1} a_k\right) \cdot a_n \quad \text{for all integers } n > m.$$

By convention, an empty product (eg: $\prod_{k=m}^{n} a_k$ where $m > n$) is equal to the multiplicative identity 1.

Example #5: Compute the product $\prod_{k=1}^{5}(k+2)$

$$\prod_{k=1}^{5}(k+2) = 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 2520$$

8.1.4. Properties of Summations and Products

Theorem 5.1.1

If $a_m, a_{m+1}, a_{m+2}, \cdots$ and $b_m, b_{m+1}, b_{m+2}, \cdots$ are sequences of real numbers and c is any real number , then the following equations hold for any integer $n \geq m$:

1. $$\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$$

2. $$c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$$ (generalized distributive law)

3. $$\left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right) = \left(\prod_{k=m}^{n} (a_k \cdot b_k)\right)$$

Example #6: Let $a_k = k + 1$ and $b_k = k - 1$ for all integers k. Write the following as a single summation.

(a) $\sum_{k=m}^{n} a_k + 2 \cdot \sum_{k=m}^{n} b_k$

$$= \sum_{k=m}^{n} (k+1) + 2 \cdot \sum_{k=m}^{n} (k-1)$$ (by substitution)

$$= \sum_{k=m}^{n} (k+1) + \sum_{k=m}^{n} 2 \cdot (k-1)$$ (by Theorem 5.1.1 (2))

$$= \sum_{k=m}^{n} \big((k+1) + 2 \cdot (k-1)\big)$$ (by Theorem 5.1.1 (1))

$$= \sum_{k=m}^{n} (3k-1)$$ (by basic algebra)

Example #6: Let $a_k = k+1$ and $b_k = k-1$ for all integers k. Write the following as a single product.

(b) $\left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right)$

$$= \left(\prod_{k=m}^{n} (k+1)\right) \cdot \left(\prod_{k=m}^{n} (k-1)\right)$$ (by substitution)

$$= \prod_{k=m}^{n} (k+1) \cdot (k-1)$$ (by Theorem 5.1.1 (3))

$$= \prod_{k=m}^{n} (k^2-1)$$ (by basic algebra)

8.1.5. Change of Variable

$$\sum_{k=1}^{3} k^2 = \sum_{i=1}^{3} i^2 = \sum_{k=3}^{5} (k-2)^2$$

Dummy variables

Example #7: Transform the following summation by changing the range of k from $[1, n+1]$ to $[0, n]$.

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

8.1.6. Some Common Sequences

Definition: Arithmetic Sequence

A sequence $a_0, a_1, a_2, \cdots$ is called an **arithmetic sequence** (or **arithmetic progression**) iff there is a constant d such that

$$a_k = a_{k-1} + d \qquad \text{for all integers } k \geq 1.$$

It follows that,

$$a_n = a_0 + dn \qquad \text{for all integers } n \geq 0.$$

d is the common difference, a_0 the initial value.

Examples:

- 1, 5, 9, 13, 17, ...
- 12, 7, 2, -3, -8, -13, ...

Summing an arithmetic sequence of n terms:

$$\sum_{k=0}^{n-1} a_k = \frac{n}{2}(2a_0 + (n-1)d)$$

Definition: Geometric Sequence

A sequence $a_0, a_1, a_2, \cdots$ is called a **geometric sequence** (or **geometric progression**) iff there is a constant r such that

$$a_k = r a_{k-1} \qquad \text{for all integers } k \geq 1.$$

It follows that,

$$a_n = a_0 r^n \qquad \text{for all integers } n \geq 0.$$

r is the common ratio, a_0 the initial value.

Examples:

- 1, 3, 9, 27, 81, …
- 8, 4, 2, 1, ½, ¼, …

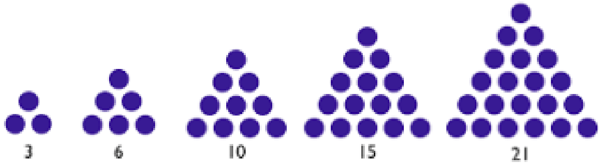
Summing a geometric sequence of n terms ($r \neq 1$),

$$\sum_{k=0}^{n-1} a_k = a_0 \left(\frac{1 - r^n}{1 - r} \right)$$

Sequences: Some Common Sequences

Squares: 1, 4, 9, 16, 25, 36, 49, ...

Triangle numbers: 1, 3, 6, 10, 15, 21, 28, ...



Fibonacci numbers: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

$$F_1 = 1$$
$$F_2 = 1$$
$$F_n = F_{n-1} + F_{n-2} \text{ for } n > 2$$

Lazy Caterer's Sequence: 1, 2, 4, 7, 11, 16, ...

(See AY2018/19 Semester 1 Exam Paper.)

Using Sequence Comprehension

$squares$ = [$k \times k$: $k \in$ [1..]]

$triangle$ = [tri(k) : $k \in$ [1..]]

tri(1) = 1
tri(n) = n+tri(n-1), n>1

$fibs$ = [F(k) : $k \in$ [1..]]

F(1) = 1
F(2) = 1
F(n) = F(n-1)+F(n-2), n>2

$LazyCat$ = [cuts(k) : $k \in$ [0..]]

cuts(k) =$(k^2+k+2)/2$

8.2 Mathematical Induction I

8.2.1. Climbing an Infinite Ladder

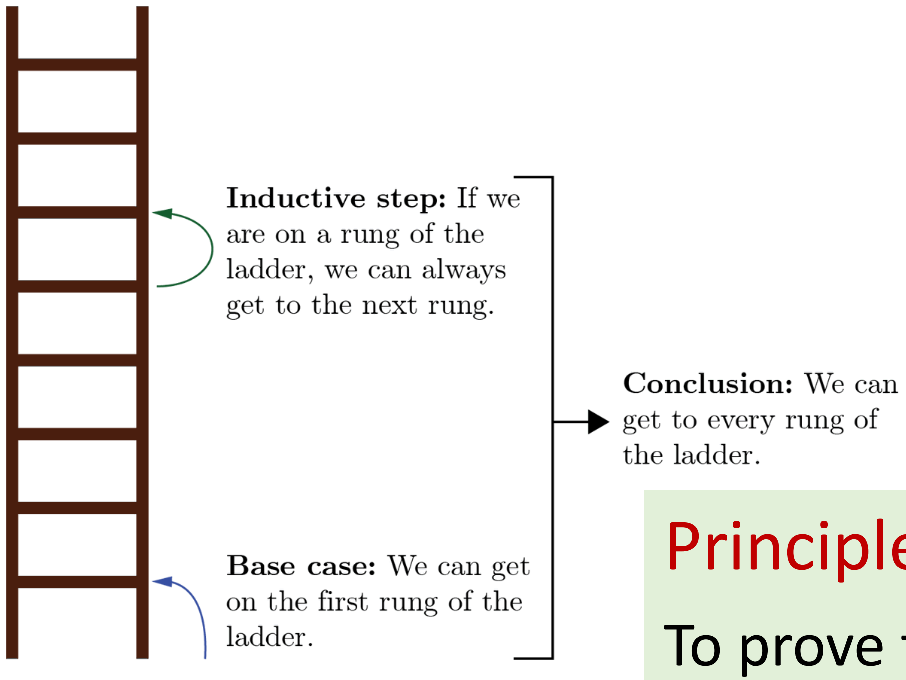
How do you prove that you can climb an infinite ladder, even though you would never reach the top?

Show that

(1) We can reach the first rung of the ladder;

(2) If we can reach a particular rung, we can reach the next higher rung.

Mathematical Induction I



Principle of Mathematical Induction

To prove that $P(n)$ is true for all $n \in \mathbb{Z}^+$:

- Basis step: Show that $P(1)$ is true.
- Inductive step: Show that $P(k) \Rightarrow P(k+1)$ for all $k \in \mathbb{Z}^+$.
- Therefore $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Inductive hypothesis

Note that in general, the basis step needs not be $P(1)$; it can be $P(a)$ where a is a fixed integer.

8.2.2. Principle of Mathematical Induction (PMI)

Principle of Mathematical Induction (PMI)

Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following 2 statements are true:

1. $P(a)$ is true.
2. For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then the statement "for all integers $n \geq a, P(n)$" is true.

The validity of proof by mathematical induction is generally taken as an axiom. That is why it is referred to as the principle of mathematical induction rather than as a theorem. We may use PMI as a short-form for Principle of Mathematical Induction.

Mathematical Induction I

Proving a statement by mathematical induction is a two-step process. The first step is called the *basis step*, and the second step is called the *inductive step*.

Method of Proof by Mathematical Induction

Consider a statement of the form, "For all integers $n \geq a$, a property $P(n)$ is true." To prove such a statement, perform the following two steps:

Step 1 (basis step): Show that $P(a)$ is true.

Step 2 (inductive step): Show that for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true. To perform this step,

suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq a$.

[This supposition is called the **inductive hypothesis.***]*

Then

show that $P(k+1)$ is true.

Induction Principle

base step (proof)

inductive step (proof)

$$\frac{\begin{array}{l} P(a) \\ \forall k \geq a.\ P(k) \Rightarrow P(k+1) \end{array}}{\therefore\ \forall k \geq a.\ P(k)}$$

intended conclusion

This is usually taken as an axiom/principle rather than a theorem? Why is this <u>not</u> a theorem?

$$\frac{\begin{array}{l} P(a) \\ P(a) \Rightarrow P(a+1) \\ P(a+1) \Rightarrow P(a+2) \\ P(a+2) \Rightarrow P(a+3) \\ \quad \vdots \end{array}}{\therefore\ \forall k \geq a.\ P(k)}$$

- Structural Inductive Proof
- Based on data construction

  N ::= 0 | N+1
- Good reason for proof to hold

Proof Rules

base step (proof)

inductive step (proof)

$$\frac{\begin{array}{l} P(a) \\ \forall k \geq a,\ P(k) \Rightarrow P(k{+}1) \end{array}}{\therefore\ \forall k \geq a,\ P(k)}$$

intended conclusion

assume induction hypothesis P(k)

$$\frac{\begin{array}{c} \text{Suppose } k \geq a \quad P(k) \\ \vdots \\ P(k{+}1) \end{array}}{\therefore\ k \geq a \quad P(k) \Rightarrow P(k{+}1)}$$

Prove P(k+1)

Sub-Goal to Prove

Example #8: Use mathematical induction to prove

Theorem 5.2.2 (5th: 5.2.1) Sum of the First n Integers

For all integers $n \geq 1$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Proof (by *mathematical induction*):

1. Let $P(n) \equiv \left(1 + 2 + \cdots + n = \frac{n(n+1)}{2}\right), \forall n \in \mathbb{Z}^+$. (Set up predicate.)
2. Basis step: $1 = \frac{1(1+1)}{2}$, therefore $P(1)$ is true. P(1)
3. Assume $P(k)$ is true for some $k \geq 1$. That is,
$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$
4. Inductive step: (To show $P(k+1)$ is true.) ∀k ≥ 1. P(k) ⇒ P(k+1)

   4.1. $1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{⍰\ 2} + (k+1) = \frac{(k+1)((k+1)+1)}{2}$

   4.2. Therefore $P(k+1)$ is true.
5. (We have proved $P(1)$ and $k \geq 1 \quad P(k) \rightarrow P(k+1)$)
   Therefore, $P(n)$ is true for $n \in \mathbb{Z}^+$.

Text in green are comments that may be omitted in your solution.

How we make use of $P(k)$.

Definition: Closed Form

If a sum with a variable number of terms is shown to be equal to a formula that does not contain either an ellipsis (...) or a summation symbol (Σ), we say that it is written in **closed form**.

Example:

$\frac{n(n+1)}{2}$ is the closed form formula for $1 + 2 + 3 + \cdots + n$.

Example #9: Use mathematical induction to prove

Theorem 5.2.3 (5th: 5.2.2) Sum of a Geometric Sequence

For any real number $r \neq 1$, and any integers $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$

Proof (by *mathematical induction*):

1. Let $P(n) \equiv \left(\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}\right), r \neq 1, n \geq 0$. (Set up predicate.)
2. Basis step: $r^0 = 1 = \frac{r^1-1}{r-1}$, therefore $P(0)$ is true. P(0)
3. Assume $P(k)$ is true for $k \geq 0$. That is, $\sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$
4. Inductive step: (To show $P(k+1)$ is true.)

   4.1. $\sum_{i=0}^{k+1} r^i = \sum_{i=0}^{k} r^i + r^{k+1} = \frac{r^{k+1}-1}{r-1} + r^{k+1} = \frac{r^{k+1}-1+r^{k+1}(r-1)}{r-1}$

   $= \frac{r^{((k+1)+1)}-1}{r-1}$ $\forall k \geq 0.\ P(k) \Rightarrow P(k+1)$

   4.2. Therefore $P(k+1)$ is true.
5. Therefore, $P(n)$ is true for $n \geq 0$.

Example #10: Use mathematical induction to prove

Proposition 5.3.1 (5th: 5.3.2)

For all integers $n \geq 0, 2^{2n} - 1$ is divisible by 3.

Proof (by *mathematical induction*):

1. Let $P(n) \equiv (3 \mid (2^{2n} - 1))$ for all integers $n \geq 0$.
2. Basis step: $2^{2 \cdot 0} - 1 = 0$ is divisible by 3, therefore $P(0)$ is true.

   P(0)
3. Assume $P(k)$ is true for $k \geq 0$. That is, $3 | (2^{2k} - 1)$.

   3.1 This means that $2^{2k} - 1 = 3r$ for some integer r (by defn of divisibility).
4. Inductive step: (To show $P(k+1)$ is true.)

   4.1. $2^{2(k+1)} - 1 = 2^{2k} \cdot 4 - 1 = 2^{2k} \cdot (3+1) - 1 = 2^{2k} \cdot 3 + (2^{2k} - 1)$

   $= 2^{2k} \cdot 3 + 3r = 3(2^{2k} + r)$

   ∀k ≥ 0. *P*(k) ⇒ *P*(k+1)

   4.2. Since $3 | (2^{2(k+1)} - 1)$, therefore $P(k+1)$ is true.
5. Therefore, $P(n)$ is true for all integers $n \geq 0$.

Example #11: Use mathematical induction to prove

Proposition 5.3.2 (5th: 5.3.3)

For all integers $n \geq 3$, $2n + 1 < 2^n$.

Proof (by *mathematical induction*):

1. Let $P(n) \equiv (2n + 1 < 2^n), \forall n \in \mathbb{Z}_{\geq 3}$.

   P(3)

2. Basis step: $2 \cdot 3 + 1 = 7 < 8 = 2^3$, therefore $P(3)$ is true.
3. Assume $P(k)$ is true for $k \geq 3$. That is, $2k + 1 < 2^k$.
4. Inductive step: (To show $P(k + 1)$ is true.)

   4.1. $\mathbf{2(k + 1) + 1} = 2k + 3 = (2k + 1) + 2 < 2^k + 2 < 2^k + 2^k = \mathbf{2^{k+1}}$

   (because $2 < 2^k$ for all integers $k \geq 2$)

   4.2. Therefore $P(k + 1)$ is true.

   $\forall k \geq 3.\ P(k) \Rightarrow P(k+1)$

5. Therefore, $P(n)$ is true for all integers $n \geq 3$.

Example #12: A Negative Example

Claim: All cows have the same colour.

Example #12: A Negative Example

Claim: All cows have the same colour.

What is wrong with this proof?

Proof (by *mathematical induction*):

1. Let $P(n) \equiv$ (Any group of n cows have the same colour), $\forall n \in \mathbb{Z}^+$
2. Basis step: Clearly, a single cow has one colour, so $P(1)$ is true. *P*(1)
3. Assume $P(k)$ is true for $k \geq 1$.
4. Inductive step: (To show $P(k+1)$ is true.)
   - 4.1. In any group of $k+1$ cows, number them from 1 to $k+1$.
   - 4.2. Then cows #1 to #k form a group of k cows, which have the same colour by the Inductive Hypothesis.
   - 4.3. Similarly, cows #2 to #$k+1$ have the same colour.
   - 4.4. Now, cows #2 to #k are common to both groups, and cows don't change colour! $P(\{\#1..\#k\}) \wedge P(\{\#2..\#k+1\}) \wedge k \geq 2 \Rightarrow P(\{\#1..\#k+1\})$
   - 4.5. Thus cow #$k+1$ has the same colour as cow #1, which means all $(k+1)$ cows have the same colour.
   - 4.6. Therefore, $P(k+1)$ is true.
5. Therefore, $P(n)$ is true, i.e., all cows have the same colour!

$$\frac{P(1) \qquad \forall k \geq 1,\ P(k) \Rightarrow P(k+1)}{\therefore\ \forall k \geq 1,\ P(k)}$$

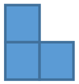
regular induction over Nat

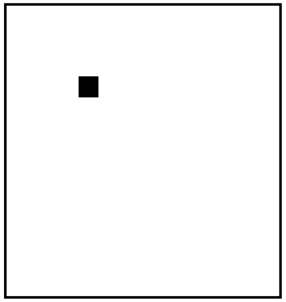
$$\frac{P(1) \qquad \forall k \geq 2,\ P(\{\#1..\#k\}) \wedge P(\{\#2..\#k+1\}) \Rightarrow P(\{\#1..\#k+1\})}{\therefore\ \forall k \geq a,\ P(k)}$$

wrong induction scheme

Mathematical induction is not restricted to proving formulas.

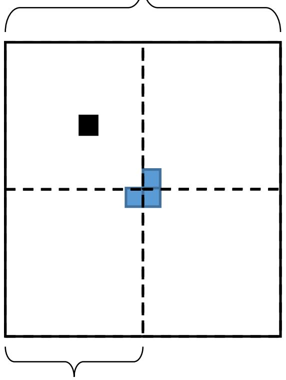
Example #13: For $n \in \mathbb{Z}^+$, any $2^n \times 2^n$ board with one square removed can be tiled by L-trominoes.

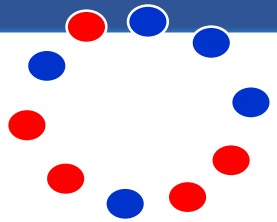
L-tromino 



Proof (by *mathematical induction*):

1. Let $P(n) \equiv$ ($2^n \times 2^n$ board with one square removed can be tiled by L-trominoes), $\forall n \in \mathbb{Z}^+$.
2. Basis step: $P(1)$ is true as such a board is an L-tromino. *P*(1)
3. Assume $P(k)$ is true for $k \geq 1$.
4. Inductive step: (To show $P(k+1)$ is true.)
   4.1. Let B be a $2^{k+1} \times 2^{k+1}$ board with one square removed.
   4.2. Divide B into four $2^k \times 2^k$ quadrants.
   4.3. Let Q be the quadrant containing the removed square.
   4.4. Remove one L-tromino from the centre of B such that each quadrant other than Q has one square removed.
   4.5. We have four $2^k \times 2^k$ quadrants, each with one square removed.
   4.6. By the induction hypotheses, each quadrant can be tiled by L-trominoes.
   4.7. Therefore, $P(k+1)$ is true. $P(n) \wedge P(n) \wedge P(n) \wedge P(n) \wedge k \geq 1 \Rightarrow P(k+1)$
5. Therefore $\forall n \in \mathbb{Z}^+ \; P(n)$ is true.





Exercise: This is a past year's assignment question. Discuss on the Canvas forum or QnA.

n red balls and n blue balls ($n > 0$) are arranged to form a circle. You walk around the circle exactly once in a clockwise direction and count the number of red and blue balls you pass. If at all times during your walk, the number of red balls (that you have passed) is greater than or equal to the number of blue balls (that you have passed), then your trip is said to be successful. (Note that whether successful or not, you will pass exactly $2n$ balls after walking one round.)

Define $P(n) \equiv$ (In any circle formed by n red and n blue balls, there exists a successful trip), $\forall n \in \mathbb{Z}^+$.

Prove by mathematical induction that you can always make a successful trip if you can choose where you start.

8.3 Mathematical Induction II

8.3.1. Strong Mathematical Induction

Principle of Strong Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. $P(a)$, $P(a+1)$, $\ldots$, and $P(b)$ are all true. **(basis step)**
2. For any integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true. **(inductive step)**

Then the statement

$$\text{for all integers } n \geq a,\ P(n)$$

is true. (The supposition that $P(i)$ is true for all integers i from a through k is called the **inductive hypothesis.** Another way to state the inductive hypothesis is to say that $P(a)$, $P(a+1)$, $\ldots$, $P(k)$ are all true.)

Comparison between "weak" and "strong" induction.
Let $P(n)$ denotes the property on all integers $n \geq a$.

Weak (regular) induction (or 1PI)

If
- $P(a)$ holds
- For every $k \geq a, P(k) \Rightarrow P(k+1)$

Then $P(n)$ holds for all $n \geq a$.

We may prove strong induction from weak and weak induction from strong (proofs omitted). This means both types of induction are equal in "power".

Hence, using more neutral terms, we can call the regular/strong versions the First Principle of Mathematical Induction (1PI) and Second Principle of Mathematical Induction (2PI) respectively.

Strong induction (or 2PI)

If
- $P(a)$ holds
- For every $k \geq a, \big(P(a) \wedge P(a+1) \wedge \cdots \wedge P(k)\big) \Rightarrow P(k+1)$

Then $P(n)$ holds for all $n \geq a$.

Strong induction (or 2PI) (variation – other variations possible)

If
- $P(a), P(a+1), \ldots, P(b)$ hold
- For every $k \geq b, P(k) \Rightarrow P(k+b-a+1)$

Then $P(n)$ holds for all $n \geq a$.

$$\frac{P(a) \qquad \forall k \geq a,\ P(k) \Rightarrow P(k+1)}{\therefore\ \forall k \geq a,\ P(k)}$$

regular induction (or 1PI)

$$\frac{P(a) \qquad \forall k \geq a,\ P(a) \wedge P(a+1) \wedge .. \wedge P(k) \Rightarrow P(k+1)}{\therefore\ \forall k \geq a,\ P(k)}$$

strong induction (or 2PI)

$$\frac{P(a) \wedge P(a+1) \wedge .. \wedge P(b) \qquad \forall k \geq b,\ P(k) \Rightarrow P(k+b-a+1)}{\therefore\ \forall k \geq a,\ P(k)}$$

strong induction (or 2PI) variation

Exercise #14: Prove that

Any integer > 1 is divisible by a prime number.

Idea: If a given integer greater than 1 is not itself prime, then it is a product of two smaller positive integers, each of which is greater than 1.

Since you are assuming that each of these smaller integers is divisible by some prime number, by transitivity of divisibility, those prime numbers also divide the integer you started with.

Theorem 4.3.3 (5th: 4.4.3) Transitivity of Divisibility

For all integers a, b and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Prove: Any integer greater than 1 is divisible by a prime number.

Proof (by *2PI*):

1. Let $P(n) \equiv (n$ is divisible by a prime), for $n > 1$.
2. Basis step: $P(2)$ is true since 2 is divisible by 2.
3. Inductive step: To show that for all integers $k \geq 2$, if $P(i)$ is true for all integers i from 2 through k, then $P(k+1)$ is also true.
   - 3.1. Case 1 ($k+1$ is prime): In this case $k+1$ is divisible by a prime number which is itself.
   - 3.2. Case 2 ($k+1$ is not prime): In this case $k+1 = ab$ where a and b are integers with $1 < a < k+1$ and $1 < b < k+1$.
     - 3.2.1. Thus, in particular, $2 \leq a \leq k$ and so by inductive hypothesis, a is divisible by a prime number p.
     - 3.2.2. In addition, because $k+1 = ab$, so $k+1$ is divisible by a.
     - 3.2.3. By transitivity of divisibility, $k+1$ is divisible by a prime p.
4. Therefore any integer greater than 1 is divisible by a prime.

Example #15: Use 1PI to prove that any whole amount of ≥ \$12 can be formed by a combination of \$4 and \$5 coins.

Proof (by *1PI*):

1. Let $P(n) \equiv$ (the amount of \$$n$ can be formed by \$4 and \$5 coins) for $n \geq 12$.
2. Basis step: $12 = 3 \times 4$, so three \$4 can be used. Therefore $P(12)$ is true.
3. Assume $P(k)$ is true for $k \geq 12$.
4. Inductive step: (To show $P(k+1)$ is true.)
   - 4.1. Case 1: If a \$4 coin is used for \$$k$ amount, replace it by a \$5 coin to make \$$(k+1)$.
   - 4.2. Case 2: If no \$4 coin is used for \$$k$ amount, then $k \geq 15$, so there must be at least three \$5 coins. We can then replace three \$5 coins with four \$4 coins to make \$$(k+1)$.
   - 4.3. In both cases, $P(k+1)$ is true.
5. Therefore, $P(n)$ is true for $n \geq 12$.

Example #16: Use 2PI to prove that:

This is the same problem as Example #15.

For all integers $n \geq 12, n = 4a + 5b$ for some $a, b \in \mathbb{N}$.

Proof (by *2PI*):

1. Let $P(n) \equiv (n = 4a + 5b)$, for some $a, b \in \mathbb{N}, n \geq 12$.
2. Basis step: Show that $P(12), P(13), P(14), P(15)$ hold.
   $12 = 4 \cdot 3 + 5 \cdot 0;\ 13 = 4 \cdot 2 + 5 \cdot 1;\ 14 = 4 \cdot 1 + 5 \cdot 2;\ 15 = 4 \cdot 0 + 5 \cdot 3;$
   P(12) ∧ P(13) ∧ P(14) ∧ P(15)
3. Assume $P(i)$ holds for $12 \leq i \leq k$ given some $k \geq 15$.
4. Inductive step: (To show $P(k+1)$ is true.)
   4.1. $P(k-3)$ holds (by induction hypothesis),
   so, $k - 3 = 4a + 5b$ for some $a, b \in \mathbb{N}$
   4.2. $k + 1 = (k-3) + 4 = (4a + 5b) + 4 = 4(a+1) + 5b$
   4.3. Hence, $P(k+1)$ is true.
   $\forall k \geq 15.\ P(k-3) \Rightarrow P(k+1)$
5. Therefore, $P(n)$ is true for $n \geq 12$.

8.4 Well-Ordering Principle

8.4.1. Well-Ordering Principle

Well-Ordering Principle for the Integers

Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.

Note: The above is the generally accepted (and well-known) definition of well-ordering principle. However, Epp's definition extends the set to include possibly negative integers: "Let S be a set of integers containing one or more integers all of which are greater than some fixed integer. Then S has a least element." We will stick with the above more generally accepted definition.

The well-ordering principle for the integers looks very different from both the regular and the strong principles of mathematical induction, but it can be shown that all three principles are equivalent (proof omitted).

(For our purpose, we will focus on using Mathematical Induction.)

Well-Ordering Principle for Non-Negative Integers

Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.

Proof (by contradiction):

1. Suppose not, i.e. let $S \subseteq \mathbb{Z}_{\geq 0}$ be non-empty with no smallest element.
2. For each $n \in \mathbb{Z}_{\geq 0}$, let $P(n)$ be the proposition "$n \notin S$".
3. Inductive step:
   - 3.1. Let $k \in \mathbb{Z}_{\geq 0}$ such that $P(0), P(1), \cdots, P(k-1)$ are true, i.e., $0,1,\cdots,k-1 \notin S$.
   - 3.2. If $k \in S$, then k is the smallest element of S by the induction hypothesis as $S \subseteq \mathbb{Z}_{\geq 0}$, which contradicts our assumption that S has no smallest element
   - 3.3. So $k \notin S$ and thus $P(k)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geq 0}\ P(n)$ is true by 2PI.
5. This implies $S = \emptyset$, contradicting line 1 that S is non-empty.

Example #17: For each of the following, if the set has a least element, state what it is. If not, explain why the well-ordering principle is not violated.

a. The set of all positive real numbers.
b. The set of all nonnegative integers n such that $n^2 < n$.
c. The set of all nonnegative integers of the form $46 - 7k$, where k is an integer.

a. There is no least positive real number. If x is any positive real number, then $x/2$ is a positive real number smaller than x.

The well-ordering principle is not violated because the principle refers **only to sets of integers**.

b. There is no least nonnegative integer n such that $n^2 < n$ because there is no nonnegative integer that satisfies this inequality.

The well-ordering principle is not violated because the principle refers **only to non-empty sets**.

Example #17: For each of the following, if the set has a least element, state what it is. If not, explain why the well-ordering principle is not violated.

a. The set of all positive real numbers.
b. The set of all nonnegative integers n such that $n^2 < n$.
c. The set of all nonnegative integers of the form $46 - 7k$, where k is an integer.

c. Integers of the form $46 - 7k$ are …, -10, -3, 4, 11, 18, 25, 32, 46, …
So, 4 is the least nonnegative integer among them.

8.5 Recurrence Relations

8.5.1. Definition

Definition

A **recurrence relation** for a sequence $a_0, a_1, a_2, \cdots$ is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, \cdots, a_{k-i}$, where i is an integer with $k - i \geq 0$.

If i is a fixed integer , the **initial conditions** for such a recurrent relation specify the values of $a_0, a_1, a_2, \cdots, a_{i-1}$.

If i depends on k, the initial conditions specify the values of $a_0, a_1, a_2, \cdots, a_m$, where m is an integer with $m \geq 0$.

Example #18: Recurrence relation for Fibonacci sequence F_n.

$$F_0 = 0$$
$$F_1 = 1$$
$$F_n = F_{n-1} + F_{n-2}, \text{ for } n > 1$$

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...

Sometimes, we call such a definition a recursive definition.

Examples:

- Recursive definition of *factorial*:

$$0! = 1$$
$$n! = n \cdot (n-1)! \text{ for } n \geq 1$$

- Recursive definition of *power*:

$$a^0 = 1$$
$$a^n = a^{n-1} \cdot a \text{ for } n \geq 1$$

Recall the recursive definitions of summation and product in sections 5.1.2 and 5.1.3 respectively.

$$\sum_{k=m}^{n} a_k = \left(\sum_{k=m}^{n-1} a_k\right) + a_n \quad \text{for all integers } n > m.$$

$$\prod_{k=m}^{n} a_k = \left(\prod_{k=m}^{n-1} a_k\right) \cdot a_n \quad \text{for all integers } n > m.$$

The recursive definitions are used with mathematical induction to establish various properties of general finite sums and products.

8.5.2. Example

Example #19: Prove that for any positive integer n, if $a_1, a_2, \cdots, a_n$ and $b_1, b_2, \cdots, b_n$ are real numbers, then $\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$.

Proof (by *mathematical induction*):

1. Let $P(n) = \left(\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i\right)$, for $n \geq 1$.
2. Basis step: $P(1)$ is true since
$$\sum_{i=1}^{1}(a_i + b_i) = a_1 + b_1 = \sum_{i=1}^{1} a_i + \sum_{i=1}^{1} b_i.$$
3. Inductive hypothesis: for some $k \geq 1$,
$$\sum_{i=1}^{k}(a_i + b_i) = \sum_{i=1}^{k} a_i + \sum_{i=1}^{k} b_i.$$
4. Inductive step:

$$\sum_{i=1}^{k+1}(a_i + b_i) = \left(\sum_{i=1}^{k}(a_i + b_i)\right) + (a_{k+1} + b_{k+1})$$ (by definition of $\sum$)

$$= \sum_{i=1}^{k} a_i + \sum_{i=1}^{k} b_i + (a_{k+1} + b_{k+1})$$ (by inductive hypothesis)

$$= \cdots$$

Example #20: Prove that for any positive integer n, if $a_1, a_2, \cdots, a_n$ and $b_1, b_2, \cdots, b_n$ are real numbers, then $\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$.

4. Inductive step:

$\sum_{i=1}^{k+1}(a_i + b_i) = \left(\sum_{i=1}^{k}(a_i + b_i)\right) + (a_{k+1} + b_{k+1})$ (by definition of $\sum$)

$= \sum_{i=1}^{k} a_i + \sum_{i=1}^{k} b_i + (a_{k+1} + b_{k+1})$ (by inductive hypothesis)

$= \sum_{i=1}^{k} a_i + a_{k+1} + \sum_{i=1}^{k} b_i + b_{k+1}$ (by the associative and commutative laws of algebra)

$= \sum_{i=1}^{k+1} a_i + \sum_{i=1}^{k+1} b_i$ (by definition of $\sum$)

Therefore $P(k+1)$ is true.

5. Therefore $P(n)$ is true for any positive integer n.

8.5.3. Recursively Defined Sets

Definition

Let S be a finite set with at least one element. A **string over** S is a finite sequence of elements from S. The elements of S are called **characters** of the string, and the **length** of a string is the number of characters it contains. The **null string over** S is defined to be the "string" with no characters. It is usually denoted ϵ and is said to have length 0.

$S = \{c_1,.., c_n\}$

$Str(S) ::= \varepsilon \mid c.Str(S)$ st $c \in S$

Example #21: Certain configurations of parentheses in algebraic expressions are legal [such as (())() and ()()()], whereas others are not [such as (()))) and ())()(].

Here is a recursive definition to generate the set P of legal configurations of parentheses.

I. Base: () is in P.

II. Recursion:

a. If E is in P, so is (E).

b. If E and F are in P, so is EF.

III. Restriction: No configurations of parentheses are in P other than those derived from 1 and 2 above.

P ::= () | (P) | P P

Derive the fact that $(())()$ is in P.

Example #21: Derive the fact that $(())()$ is in P.

I. Base: $()$ is in P.

II. Recursion:
   a. If E is in P, so is (E).
   b. If E and F are in P, so is EF.

III. Restriction: No configurations of parentheses are in P other than those derived from 1 and 2 above.

1. By I, $()$ is in P.
2. By (1) and IIa, $(())$ is in P [let $E = ()$].
3. By (2), (1) and IIb, $(())()$ is in P [let $E = (())$ and $F = ()$].

Example #22: Recursive definition of $\mathbb{Z}_{\geq 0}$.

$\mathbb{Z}_{\geq 0}$ is the unique set with the following properties:

(1. what the founders are) $0 \in \mathbb{Z}_{\geq 0}$. (base clause)

(2. what the constructors are) If $x \in \mathbb{Z}_{\geq 0}$, then $x + 1 \in \mathbb{Z}_{\geq 0}$. (recursion clause)

(3. nothing more) Membership for $\mathbb{Z}_{\geq 0}$ can always be demonstrated by (finitely many) successive applications of the clauses above. (minimality clause)

$\mathbb{Z}_{\geq 0}$

$0 \; {}_{+1} \quad 1 \; {}_{+1} \quad 2 \; {}_{+1} \quad 3 \; {}_{+1} \quad 4 \; {}_{+1} \quad \cdots$

Example #23: Recursive definition of $2\mathbb{Z}$ (the set of even integers).

$2\mathbb{Z}$ is the unique set with the following properties:

(1. what the founders are) $0 \in 2\mathbb{Z}$. (base clause)

(2. what the constructors are) If $x \in 2\mathbb{Z}$, then $x - 2, x + 2 \in 2\mathbb{Z}$. (recursion clause)

(3. nothing more) Membership for $2\mathbb{Z}$ can always be demonstrated by (finitely many) successive applications of the clauses above. (minimality clause)

$2\mathbb{Z}$

$$\cdots \quad {}_{-2}\ -4 \quad {}_{-2}\ -2 \quad {}_{-2}\ 0 \quad {}_{+2}\ 2 \quad {}_{+2}\ 4 \quad {}_{+2}\ \cdots$$

8.5.4. Structural Induction

Recursive definition of of a set S.

(base clause) Specify that certain elements, called founders, are in S: if c is a founder, then $c \in S$.

(recursion clause) Specify certain functions, called constructors, under which the set S is closed: if f is a constructor and $x \in S$, then $f(x) \in S$.

(minimality clause) Membership for S can always be demonstrated by (finitely many) successive applications of the clauses above.

Structural induction over S.

To prove that $\forall x \in S\ P(x)$ is true, where each $P(x)$ is a proposition, it suffices to:

(basis step) show that $P(c)$ is true for every founder c; and

(induction step) show that $\forall x \in S\left(P(x) \Rightarrow P\big(f(x)\big)\right)$ is true for every constructor f.

In words, if all the founders satisfy a property P, and P is preserved by all constructors, then all elements of S satisfy P.

This is taken from Dr Wong Tin Lok's notes.

$$\frac{P(0) \qquad \forall k \geq 0,\ P(k) \Rightarrow P(k+1)}{\therefore\ \forall k \geq 0,\ P(k)}$$

1PI structural induction on Nat

Nat ::= 0 | 1+Nat

$$\frac{P(\varepsilon) \qquad \forall a \in A,\ s \in Str(A),\ P(s) \Rightarrow P(a.s)}{\therefore\ \forall\ s \in Str(A),\ P(s)}$$

1PI structural induction on Str(A)

Str(A) ::= ε | A.Str(A)

Example #24b: Define a set H recursively as follows:

(1) $1 \in H$. (base clause)

(2) If $x \in H$, then $2x \in H$ and $3x \in H$ and $5x \in H$. (recursion clause)

(3) Membership of H can always be demonstrated by (finitely many) successive applications of the clauses above. (minimality clause)

Which of the numbers 9,10,11,12,13 are in H? Which are not?

$9, 10, 12 \in H$

$11, 13 \notin H$

$H = \{2^i 3^j 5^k : i, j, k \geq 0\}$

Hamming numbers

Structural induction over H:

To prove $\forall x \in H\ P(n)$ is true, where each $P(n)$ is a proposition, it suffices to:

(basis step): show that P(1) is true; and

(induction step): show that $\forall x \in H\big(P(x) \Rightarrow P(2x) \land P(3x) \land P(5x)\big)$ is true.

$H ::= 1 \mid 2\times H \mid 3\times H \mid 5\times H$

$$\frac{P(1) \qquad \forall n\in H,\ P(n) \Rightarrow P(2\times n) \wedge P(3\times n) \wedge P(5\times n)}{\therefore\ \forall n\in H,\ P(n)}$$

1P1 structural induction on H

END OF FILE