Sequences and Mathematical Induction

CSE 215: Foundations of Computer Science

Stony Brook University

http://www.cs.stonybrook.edu/~liu/cse215

Sequences

- A *sequence* is a function whose domain is
  - all the integers between two given integers m and n

    $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$
  - all the integers greater than or equal to a given integer m

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

  a_k is a *term* in the sequence

  k is the *subscript* or *index*

  m is the *subscript of the initial term*

  n is the *subscript of the last term* ($m \leq n$)
- An *explicit formula* or *general formula* for a sequence is a rule that shows how the values of a_k depend on k

Sequences: examples

$a_k = 2^k$ is the sequence 2, 4, 8, 16, 32, 64, 128,…

Index	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Term	2	4	8	16	32	64	128	256

$a_k = k/k + 1$, for all integers $k \geq 1$:

$$a_1 = \frac{1}{1+1} = \frac{1}{2}$$

$$a_2 = \frac{2}{2+1} = \frac{2}{3}$$

$$a_3 = \frac{3}{3+1} = \frac{3}{4}$$

$b_i = i\text{-}1/i$, for all integers $i \geq 2$:

$$b_2 = \frac{2-1}{2} = \frac{1}{2}$$

$$b_3 = \frac{3-1}{3} = \frac{2}{3}$$

$$b_4 = \frac{4-1}{4} = \frac{3}{4}$$

- a_k for $k \geq 1$ is the same sequence as b_i for $i \geq 2$

Sequences: one more example

An *alternating sequence*:

$c_j = (-1)^j$ for all integers $j \geq 0$:

$$c_0 = (-1)^0 = 1$$
$$c_1 = (-1)^1 = -1$$
$$c_2 = (-1)^2 = 1$$
$$c_3 = (-1)^3 = -1$$
$$c_4 = (-1)^4 = 1$$
$$c_5 = (-1)^5 = -1$$
$$\ldots$$

Find an explicit formula for a sequence

- The initial terms of a sequence are:

$$1, \quad -\frac{1}{4}, \quad \frac{1}{9}, \quad -\frac{1}{16}, \quad \frac{1}{25}, \quad -\frac{1}{36}$$

  - a_k is the general term of the sequence, a_1 is the first element
  - observe that the denominator of each term is a perfect square

$$\begin{array}{cccccc} \frac{1}{1^2}, & \frac{(-1)}{2^2}, & \frac{1}{3^2}, & \frac{(-1)}{4^2}, & \frac{1}{5^2}, & \frac{(-1)}{6^2} \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{array}$$

  - observe that the numerator equals ± 1: $\quad a_k = \frac{\pm 1}{k^2}$
  - alternating sequence with -1 when k is even:

$$a_k = \frac{(-1)^{k+1}}{k^2} \quad \text{for all integers } k \geq 1$$

Find an explicit formula for a sequence

- Continuing from previous slide
  - Result sequence:

$$a_k = \frac{(-1)^{k+1}}{k^2} \quad \text{for all integers } k \geq 1$$

  - Alternative sequence:

$$a_k = \frac{(-1)^{k}}{(k+1)^2} \quad \text{for all integers } k \geq 0$$

Summation notation

- If m and n are integers and m ≤ n, the summation from k equals m to n of a_k, $\sum_{k=m}^{n} a_k$, is the sum of all the terms a_m, a_{m+1}, $a_{m+2}, \ldots, a_n$

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

k is the index of the summation

m is the lower limit of the summation

n is the upper limit of the summation

Summation notation: examples

$$a_1 = -2, \quad a_2 = -1, \quad a_3 = 0, \quad a_4 = 1, \quad a_5 = 2$$

$$\sum_{k=1}^{5} a_k = a_1 + a_2 + a_3 + a_4 + a_5 = (-2) + (-1) + 0 + 1 + 2 = 0$$

$$\sum_{k=2}^{2} a_k = a_2 = -1$$

$$\sum_{k=1}^{2} a_{2k} = a_{2\cdot 1} + a_{2\cdot 2} = a_2 + a_4 = -1 + 1 = 0$$

Summation notation: more forms

- Summation notation with formulas:

$$\sum_{k=1}^{5} k^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55$$

- Changing from Summation Notation to Expanded Form:

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

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

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

Summation notation: from expanded

- Changing from Expanded Form to Summation Notation:

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

The general term of this summation can be expressed as $\frac{k+1}{n+k}$ for integers k from 0 to n

$$\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \cdots + \frac{n+1}{2n} = \sum_{k=0}^{n} \frac{k+1}{n+k}$$

Summation: evaluation for small n

- Evaluating expression for given limits:

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n\cdot(n+1)}$$

$$n=1 \qquad \frac{1}{1\cdot 2}=\frac{1}{2}$$

$$n=2 \qquad \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}=\frac{1}{2}+\frac{1}{6}=\frac{2}{3}$$

$$n=3 \qquad \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}=\frac{1}{2}+\frac{1}{6}+\frac{1}{12}=\frac{3}{4}$$

Summation: recursive definition

- Recursive definition:

$$\sum_{k=m}^{m} a_k = a_m \qquad \text{and} \qquad \sum_{k=m}^{n} a_k = \sum_{k=m}^{n-1} a_k + a_n \quad \text{for all integers } n > m$$

- Examples:
  - Separating off final term $$\sum_{i=1}^{n+1} \frac{1}{i^2} = \sum_{i=1}^{n} \frac{1}{i^2} + \frac{1}{(n+1)^2}$$
  - Writing summation $$\sum_{k=0}^{n} 2^k + 2^{n+1} = \sum_{k=0}^{n+1} 2^k$$

Summation: successive cancellation

- Transform sum into *telescoping sums*, then into a simple expression
- Example: $\sum_{k=1}^{n} \frac{1}{k(k+1)}$
  - Use $\frac{1}{k} - \frac{1}{k+1} = \frac{(k+1)-k}{k(k+1)} = \frac{1}{k(k+1)}$

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

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

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

Product notation

- The product from k equals m to n of a_k, $\prod_{k=m}^{n} a_k$, for integers m and n with $m \leq n$, is the product of all the terms

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

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

- Examples:

$$\prod_{k=1}^{5} a_k = a_1 a_2 a_3 a_4 a_5$$

$$\prod_{k=1}^{5} k = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$$

Product notation: recursive definition

- Recursive definition:

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

Summation and product properties

- If $a_m, a_{m+1}, a_{m+2},\ldots$ and $b_m, b_{m+1}, b_{m+2},\ldots$ are sequences of real numbers:

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

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

- Generalized distributive law: if c is any real number:

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

Summation and product properties

- Example: using properties of summation and product

$a_k = k + 1$ $b_k = k - 1$

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

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

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

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

Summation and product properties

- Another example: using properties of summation and product

$a_k = k + 1$ $b_k = k - 1$

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

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

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

Sequences: change of variables

- Examples:

$$\sum_{j=2}^{4}(j-1)^2 = (2-1)^2 + (3-1)^2 + (4-1)^2$$

$$= 1^2 + 2^2 + 3^2$$

$$= \sum_{k=1}^{3} k^2.$$

change of variable

k=j-1

$$\sum_{k=0}^{6}\frac{1}{k+1}$$

change of variable: $j = k+1$

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

$$k=0, \quad j = k+1 = 0+1 = 1$$

$$k=6, \quad j = k+1 = 6+1 = 7$$

$$\sum_{k=0}^{6}\frac{1}{k+1} = \sum_{j=1}^{7}\frac{1}{j}$$

Factorial notation

- The quantity n factorial, n!, is defined to be the product of all the integers from 1 to n:

$$n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$$

0! is defined to be 1: $0! = 1$

$0! = 1$ $\quad$ $1! = 1$

$2! = 2 \cdot 1 = 2$ $\quad$ $3! = 3 \cdot 2 \cdot 1 = 6$

$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ $\quad$ $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$

$6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$

$7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5{,}040$

$8! = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 40{,}320$

$9! = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 362{,}880$

Factorial notation: recursive definition

- Recursive definition for factorial:

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n \cdot (n-1)! & \text{if } n \geq 1. \end{cases}$$

- Examples: computing with factorials

$$\frac{8!}{7!} = \frac{8 \cdot \cancel{7!}}{\cancel{7!}} = 8$$

$$\frac{5!}{2! \cdot 3!} = \frac{5 \cdot 4 \cdot \cancel{3!}}{2! \cdot \cancel{3!}} = \frac{5 \cdot 4}{2 \cdot 1} = 10$$

$$\frac{(n+1)!}{n!} = \frac{(n+1) \cdot \cancel{n!}}{\cancel{n!}} = n + 1$$

$$\frac{n!}{(n-3)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \cancel{(n-3)!}}{\cancel{(n-3)!}} = n \cdot (n-1) \cdot (n-2)$$

$$= n^3 - 3n^2 + 2n$$

n choose r

- n choose r, $\binom{n}{r}$, represents the number of subsets of size r that can be chosen from a set with n elements, for integers n and r with $0 \leq r \leq n$

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

Combination: number of r-combinations from a set of n elements

- Examples:

$$\binom{8}{5} = \frac{8!}{5!(8-5)!} = \frac{8 \cdot 7 \cdot \cancel{6} \cdot \cancel{5} \cdot \cancel{4} \cdot \cancel{3 \cdot 2 \cdot 1}}{(\cancel{5} \cdot \cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot 1) \cdot (\cancel{3 \cdot 2 \cdot 1})} = 56$$

$$\binom{n+1}{n} = \frac{(n+1)!}{n!((n+1)-n)!} = \frac{(n+1)!}{n!1!} = \frac{(n+1) \cdot \cancel{n!}}{\cancel{n!}} = n+1$$

n choose r

- Example: 4 choose 2 = 4! /(2!2!) = 6

- Let S = {1,2,3,4}
  - The 6 subsets of S with 2 elements are:

    {1,2}

    {1,3}

    {1,4}

    {2,3}

    {2,4}

    {3,4}

Sequences in computer programming

- Array: a[1], a[2], . . . , A[50]

a = [7,4,25,9] list in py/da

- **for** $i := 1$ **to** n
    print $a[i]$
  next i

```
for i in range(1,n+1):        ints(1,n)  da
        print (a[i])
```

- Summation

$s := a[1]$
for $k := 2$ **to** n
  $s := s + a[k]$
next k

```
s = a[1]
for k in …
```

```
s = sum(a[k] for k in range(1,n+1))
s = sumof(a[k], k in ints(1,n))  da
```

Example algorithm with arrays

- Convert from base 10 to base 2:

$$38 = 19 \cdot 2 + 0$$

$$= (9 \cdot 2 + 1) \cdot 2 + 0 \qquad = 9 \cdot 2 \cdot 2 + 1 \cdot 2 + 0$$

$$= (4 \cdot 2 + 1) \cdot 2^2 + 1 \cdot 2 + 0 = 4 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0$$

$$= (2 \cdot 2 + 0) \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0$$

$$= 2 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0$$

$$= (1 \cdot 2 + 0) \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0$$

$$= 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0$$

$$a = 2^k \cdot r[k] + 2^{k-1} \cdot r[k-1] + \cdots + 2^2 \cdot r[2] + 2^1 \cdot r[1] + 2^0 \cdot r[0]$$

$$a_{10} = (r[k]r[k-1] \cdots r[2]r[1]r[0])_2$$

Convert from base 10 to base 2

Input: n [a nonnegative integer]

Algorithm Body:

q := n, i := 0

while (i = 0 or q = 0)

  r[i] := q mod 2

  q := q div 2

  i := i + 1

end while

Output: r[0], r[1], r[2], . . . , r[i − 1] [a sequence of integers]

Mathematical induction

Principle of mathematical induction:

Let P(n) be a property that is defined for integers n, and let a be a fixed integer. Suppose the following two 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.

That is:

P(a) is true.

$P(k) \Rightarrow P(k + 1), \forall\, k \geq a$

$\therefore$ P(n) is true, $\forall\, n \geq a$

Mathematical induction: proof method

Method of proof by mathematical induction:

To prove a statement of the form:

"For all integers $n \geq a$, a property $P(n)$ is true."

Step 1. Base 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**:

- Inductive hypothesis: suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq a$.
- Then show that $P(k + 1)$ is true.

Mathematical induction: example 1

For all integers n ≥ 8, n¢ can be obtained using 3¢ and 5¢ coins

Base step: P(8) is true because 8¢ = one 3¢ coin and one 5¢ coin

Inductive step: for all integers k ≥ 8, if P(k) is true then P(k+1) is true

Inductive hypothesis: suppose k is any integer with k ≥ 8:

P(k): k¢ can be obtained using 3¢ and 5¢ coins

We must show P(k+1): (k+1)¢ can be obtained using 3¢ and 5¢ coins

Case 1. There is a 5¢ coin among those used to make up the k¢:

Replace the 5¢ coin by two 3¢ coins; the result will be (k + 1)¢.

Case 2. There is not a 5¢ coin among those used to make up the k¢:

Because k ≥ 8, at least three 3¢ coins must have been used.

Remove three 3¢ coins (9¢) and replace them by two 5¢ coins(10¢);

the result will be (k + 1)¢

Mathematical induction: example 2

Sum of the first n integers:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \quad \text{for all integers } n \geq 1$$

Base step: P(1): $1 = \frac{1(1+1)}{2}$

Inductive step:

Inductive hypo: P(k) is true, for a particular but arbitrarily chosen integer k ≥ 1: $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$

Prove P(k+1): $1 + 2 + \cdots + (k+1) = \frac{(k+1)(k+2)}{2}$

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

Sum of the first n integers

- A formula in *closed form* represents a sum with a variable number of terms without an ellipsis or a summation symbol.

- Examples: apply the formula for the sum of the first n Integers:

$$\begin{aligned} 2 + 4 + 6 + \cdots + 500 &= 2 \cdot (1 + 2 + 3 + \cdots + 250) \\ &= 2 \cdot \left(\frac{250 \cdot 251}{2} \right) \\ &= 62{,}750. \end{aligned}$$

$$5 + 6 + 7 + 8 + \cdots + 50 = (1 + 2 + 3 + \cdots + 50) - (1 + 2 + 3 + 4)$$

Mathematical induction: example 3

Sum of geometric sequence: each term is obtained from the preceding one by multiplying by a constant: if the first term is 1 and the constant is r: $1, r, r^2, r^3, \ldots, r^n, \ldots$

$$1 + r + r^2 + \cdots + r^n = \sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$

Base step: Prove P(0): $\sum_{i=0}^{0} r^i = \frac{r^{0+1} - 1}{r - 1} \Leftrightarrow 1 = 1$ (Proved)

Inductive step:

Inductive hypothesis:

suppose P(k) is true for $k \geq 0$: $\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1}$

Prove P(k + 1): $\sum_{i=0}^{k+1} r^i = \frac{r^{k+2} - 1}{r - 1}$

Sum of geometric sequence

Continued:

Prove P(k +1): $\sum_{i=0}^{k+1} r^i = \frac{r^{k+2}-1}{r-1}$

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

$$= \frac{r^{k+1}-1}{r-1} + r^{k+1}$$

$$= \frac{r^{k+2}-1}{r-1}$$

Sum of geometric sequence: examples

$$1 + 3 + 3^2 + \cdots + 3^{m-2} = \frac{3^{(m-2)+1} - 1}{3 - 1} = \frac{3^{m-1} - 1}{2}.$$

$$3^2 + 3^3 + 3^4 + \cdots + 3^m = 3^2 \cdot (1 + 3 + 3^2 + \cdots + 3^{m-2}) \quad \text{by factoring out } 3^2$$

$$= 9 \cdot \left(\frac{3^{m-1} - 1}{2}\right)$$

Mathematical induction: example 4

Proving a divisibility property:

P(n): for all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3

Basic step: P(0): $2^{2 \cdot 0} - 1 = 0$ is divisible by 3

Inductive step:

Induction hypothesis:

suppose P(k) is true: $2^{2k} - 1$ is divisible by 3

Prove P(k+1): $2^{2(k+1)} - 1$ is divisible by 3

Proving a divisibility property

Continued:

Prove P(k+1): $2^{2(k+1)} - 1$ is divisible by 3

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

$$= 2^{2k} \cdot 2^2 - 1 \quad \text{by the laws of exponents}$$

$$= 2^{2k} \cdot 4 - 1$$

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

$$= 2^{2k} \cdot 3 + (2^{2k} - 1) \quad \text{by the laws of algebra}$$

$$= 2^{2k} \cdot 3 + 3r \quad \text{by inductive hypothesis}$$

$$= 3(2^{2k} + r) \quad \text{by factoring out the 3.}$$

$2^{2k} + r$ is an integer because integers are closed under multiplication and summation

so, $2^{2(k+1)} - 1$ is divisible by 3 ■

Mathematical induction: example 5

Proving an inequality:

P(n): for all integers $n \geq 3$, $2n + 1 < 2^n$

Base step: Prove P(3): $2 \cdot 3 + 1 < 2^3$

$7 < 8$ (true)

Inductive step:

Inductive hypo: suppose for $k \geq 3$, P(k) is true: $2k + 1 < 2^k$

Show P(k+1): $2(k+1) + 1 < 2^{k+1}$

That is: $2k + 3 < 2^{k+1}$

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

because $2k + 1 < 2^k$ by the inductive hypothesis

and because $2 < 2^k$ for all integers $k \geq 3$

Mathematical induction: example 6

A sequence: $a_1 = 2$ and $a_k = 5a_{k-1}$ for all integers $k \geq 2$

Prove: $a_n = 2 \cdot 5^{n-1}$ for all integers $n \geq 1$

Proof by induction: P(n): $a_n = 2 \cdot 5^{n-1}$ for all integers $n \geq 1$

Base step: P(1): $a_1 = 2 \cdot 5^{1-1}$. $2 \cdot 5^{1-1} = 2 \cdot 5^0 = 2 \cdot 1 = 2 = a_1$

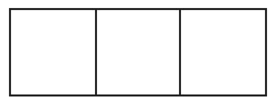
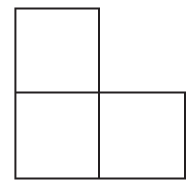
Inductive step: Inductive hypo: suppose P(k) is true: $a_k = 2 \cdot 5^{k-1}$

Show P(k+1): $a_{k+1} = 2 \cdot 5^{(k+1)-1} = 2 \cdot 5^k$

$a_{k+1} = 5a_{(k+1)-1}$	by definition of $a_1, a_2, a_3, \ldots$
$= 5 \cdot a_k$	since $(k + 1) - 1 = k$
$= 5 \cdot 2 \cdot 5^{k-1}$	by inductive hypothesis
$= 2 \cdot (5 \cdot 5^{k-1})$	by regrouping
$= 2 \cdot 5^k$	by the laws of exponents

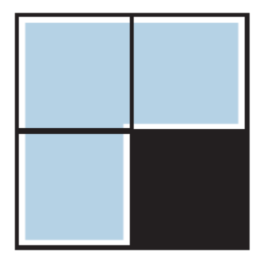
Mathematical induction: example 7

A problem with trominoes (Tetris):

straight  and L-shaped 

For any integer n ≥ 1, if one square is removed from a $2^n \times 2^n$ checkerboard, the remaining squares can be completely covered by L-shaped trominoes

Base step: a 2×2 checkerboard can be covered by 1 L-shaped tromino



A problem with trominoes

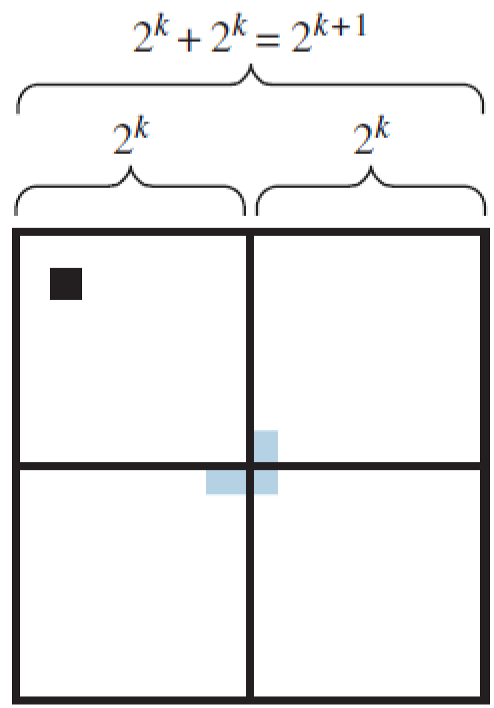
Continued: Inductive step:

Inductive hypothesis: for $k \geq 1$: $P(k)$:

if one square is removed from a $2^k \times 2^k$ checkerboard, the remaining squares can be completely covered by L-shaped trominoes

Proof $P(k+1)$:

if one square is removed from a $2^{k+1} \times 2^{k+1}$ checkerboard, the remaining squares can be completely covered by L-shaped trominoes



Strong mathematical induction

Principle of strong mathematical induction:

P(n) is a property that is defined for integers n, and a and b are fixed integers with $a \leq b$.

Base step: P(a), P(a + 1), . . . , and P(b) are all true

Inductive step:

Inductive hypothesis: 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

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

That is: P(a), P(a+1),…, P(b-1), P(b) are true.

$\forall k \geq b, (\forall a \leq i \leq k, P(i)) \rightarrow P(k + 1)$

$\therefore$ P(n) is true, $\forall n \geq a$

Strong mathematical induction

Any statement that can be proved with ordinary mathematical induction can be proved with strong mathematical induction (and vice versa).

Strong induction: example 1

Divisibility by a prime:

Any integer greater than 1 is divisible by a prime number

P(n): n is divisible by a prime number

Base step: P(2): 2 is divisible by a prime number

2 is divisible by 2 and 2 is a prime number

Inductive step:

Inductive hypothesis: Let k be any integer with $k \geq 2$

suppose P(i) is true for all integers i from 2 through k,

that is, i is divisible by a prime number for int i from 2 to k

Show P(k + 1): k + 1 is divisible by a prime number

Strong induction: example 1 (cont'd)

Show P(k + 1): k + 1 is divisible by a prime number

Case 1 (k + 1 is prime): In this case k + 1 is divisible by itself (a prime number): k+1 = 1*(k+1)

Case 2 (k + 1 is not prime): k + 1 = a*b

where a and b are integers with 1<a<k+1 and 1<b<k+1.

From k + 1 = a*b,   k + 1 is divisible by a.

By inductive hypothesis, a is divisible by a prime number p.

By transitivity of divisibility, k + 1 is divisible by p.

Therefore, k+1 is divisible by a prime number p. ■

Strong induction: example 2

A sequence $s_0, s_1, s_2, \ldots$

$s_0=0$, $s_1=4$, $s_k=6s_{k-1}-5s_{k-2}$ for all integers $k \geq 2$

$s_2 = 6s_1 - 5s_0 = 6 \cdot 4 - 5 \cdot 0 = 24$,

$s_3 = 6s_2 - 5s_1 = 6 \cdot 24 - 5 \cdot 4 = 144 - 20 = 124$

Prove: $\mathbf{s_n = 5^n - 1}$

Base step: P(0) and P(1) are true:

P(0): $s_0=5^0-1 = 1 - 1 = 0$

P(1): $s_1= 5^1-1 = 5 - 1 = 4$

Inductive step: Inductive hypo: Let k be any integer with $k \geq 1$,

$s_i=5^i-1$ for all integers i with $0 \leq i \leq k$

Strong induction: example 2 (cont'd)

Show P(k + 1) is true: $s_{k+1} = 5^{k+1} - 1$

$s_{k+1} = 6s_k - 5s_{k-1}$	by definition of $s_0, s_1, s_2, \ldots$
$= 6(5^k - 1) - 5(5^{k-1} - 1)$	by induction hypothesis
$= 6 \cdot 5^k - 6 - 5^k + 5$	by multiplying out and applying a law of exponents
$= (6 - 1)5^k - 1$	by factoring out 6 and arithmetic
$= 5 \cdot 5^k - 1$	by arithmetic
$= 5^{k+1} - 1$	by applying a law of exponents ■

Strong induction: example 3

The number of multiplications needed to multiply n numbers is (n-1).

P(n): If $x_1, x_2, \ldots, x_n$ are n numbers, then no matter how parentheses are inserted into their product, the number of multiplications used to compute the product is $n - 1$.

Base case: P(1): The number of multiplications needed to compute the product of x_1 is $1 - 1 = 0$

Inductive case:

Inductive hypothesis: Let k by any integer with $k \geq 1$ and for all integers i from 1 through k, if $x_1, x_2, \ldots, x_i$ are numbers, then no matter how parentheses are inserted into their product, the number of multiplications used to compute the product is $i - 1$.

Strong induction: example 3 (cont'd)

We must show $P(k + 1)$: If $x_1, x_2, \ldots, x_{k+1}$ are $k + 1$ numbers, then no matter how parentheses are inserted into their product, the number of multiplications used to compute the product is $(k + 1) - 1 = k$.

When parentheses are inserted in order to compute the product $x_1 x_2 \ldots x_{k+1}$, some multiplication is the final one:

let L be the product of the left-hand l factors (numbers) and

R be the product of the right-hand r factors: $l + r = k + 1$

By inductive hypothesis, evaluating L takes $l - 1$ multiplications and evaluating R takes $r - 1$ multiplications

$(l - 1) + (r - 1) + 1 = (l + r) - 1 = (k + 1) - 1 = k$ ■

Strong induction: example 4

Existence and uniqueness of binary integer representations:

any positive integer n has a unique representation in the form

$$n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0 \qquad P(n)$$

where r is a nonnegative integer, $c_r = 1$, and

$c_j = 0$ or 1 for $j = 0, \ldots, r-1$

Proof of existence:

Base step: $P(1)$: $1 = c_0 \cdot 2^0$ where $c_0 = 1$, $r = 0$.

Inductive hypothesis: $k \geq 1$ is an integer and for all integers i from 1 through k: $P(i)$: $i = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0$

We must show that $k + 1$ can be written in the required form.

Strong induction: example 4 (cont'd)

Case 1. k + 1 is even: (k + 1)/2 is an integer

By inductive hypothesis:

$$(k+1)/2 = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0$$

$$k+1 = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2$$

$$= c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2^1 + 0 \cdot 2^0$$

Case 2. k + 1 is odd: k is even, so k/2 is an integer

By inductive hypothesis:

$$k/2 = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0$$

$$k = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2$$

$$k+1 = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2 + 1$$

$$= c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2^1 + 1 \cdot 2^0$$

Strong induction: example 4 (cont'd)

Proof of uniqueness:

Proof by contradiction: suppose there is an integer n with two different representations as a sum of nonnegative integer powers of 2:

$$2^r + c_{r-1}\cdot 2^{r-1} + \cdots + c_1\cdot 2 + c_0 = 2^s + d_{s-1}\cdot 2^{s-1} + \cdots + d_1\cdot 2 + d_0$$

r and s are nonnegative integers, and each c_i and d_i equal 0 or 1.

Assume: $r < s$

By geometric sequence:

$$2^r + c_{r-1}\cdot 2^{r-1} + \cdots + c_1\cdot 2 + c_0 \leq 2^r + 2^{r-1} + \cdots + 2 + 1 = 2^{r+1} - 1 < 2^s$$

$$2^r + c_{r-1}\cdot 2^{r-1} + \cdots + c_1\cdot 2 + c_0 < 2^s + d_{s-1}\cdot 2^{s-1} + \cdots + d_1\cdot 2 + d_0$$

Contradiction

Well-ordering principle for 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.

- The well-ordering principle is equivalent to both ordinary and strong mathematical induction.

Well-ordering principle: examples

Why is the well-ordering principle not violated in these sets?

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

Solution:

- Not a set of integers
- Empty set
- $\{4, 11, 18, 25, \ldots\}$ where 4 is the least element

Defining sequences recursively

- A sequence can be defined in 3 ways:
  - enumeration: -2,3,-4,5,...
  - general pattern: $a_n=(-1)^n(n+1)$, for all integers $n \geq 1$
  - recursion: $a_1=-2$ and $a_n=(-1)^{n-1}\, a_{n-1} + (-1)^n$
    - **define one or more initial values for the sequence AND**
    - **define each later term in the sequence by reference to earlier terms**
- A **recurrence relation** for a sequence $a_0, a_1, a_2, \ldots$ is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, \ldots, a_{k-i}$, where i is an integer with $k-i \geq 0$
- The **initial conditions** for a recurrence relation specify the values of $a_0, a_1, a_2, \ldots, a_{i-1}$, if i is a fixed integer, OR

  $a_0, a_1, \ldots, a_m$, where m is an integer with $m \geq 0$, if i depends on k.

Recursion: example 1

- **Computing terms of a recursively defined sequence**
- Example:

Initial conditions: $c_0 = 1$ and $c_1 = 2$

Recurrence relation: $c_k = c_{k-1} + k * c_{k-2} + 1$, for all integers $k \geq 2$

$c_2 = c_1 + 2\,c_0 + 1$ by substituting $k = 2$ into the recurrence relation

$= 2 + 2 \cdot 1 + 1$ since $c_1 = 2$ and $c_0 = 1$ by the initial conditions

$= 5$

$c_3 = c_2 + 3\,c_1 + 1$ by substituting $k = 3$ into the recurrence relation

$= 5 + 3 \cdot 2 + 1$ since $c_2 = 5$ and $c_1 = 2$

$= 12$

$c_4 = c_3 + 4\,c_2 + 1$ by substituting $k = 4$ into the recurrence relation

$= 12 + 4 \cdot 5 + 1$ since $c_3 = 12$ and $c_2 = 5$

$= 33$

Recursion: example 2

- **Writing a recurrence relation in more than one way**

- Example:

  Initial condition: $s_0 = 1$

  Recurrence relation 1: $s_k = 3s_{k-1} - 1$, for all integers $k \geq 1$

  Recurrence relation 2: $s_{k+1} = 3s_k - 1$, for all integers $k \geq 0$

Recursion: example 3

- **Sequences that satisfy the same recurrence relation**

- Example:

  Initial conditions: $a_1 = 2$ and $b_1 = 1$

  Recurrence relations: $a_k = 3a_{k-1}$ and $b_k = 3b_{k-1}$ for all integers $k \geq 2$

$a_2 = 3a_1 = 3 \cdot 2 = 6$ $\quad$ $b_2 = 3b_1 = 3 \cdot 1 = 3$

$a_3 = 3a_2 = 3 \cdot 6 = 18$ $\quad$ $b_3 = 3b_2 = 3 \cdot 3 = 9$

$a_4 = 3a_3 = 3 \cdot 18 = 54$ $\quad$ $b_4 = 3b_3 = 3 \cdot 9 = 27$

Recursion: example 4

- **Fibonacci numbers**

1. We have one pair of rabbits (male and female) at the beginning of a year.
2. Rabbit pairs are not fertile during their first month of life but thereafter give birth to one new male & female pair at the end of every month.

$$\begin{bmatrix}\text{the number}\\ \text{of rabbit}\\ \text{pairs alive}\\ \text{at the end}\\ \text{of month } k\end{bmatrix} = \begin{bmatrix}\text{the number}\\ \text{of rabbit}\\ \text{pairs alive}\\ \text{at the end}\\ \text{of month } k-1\end{bmatrix} + \begin{bmatrix}\text{the number}\\ \text{of rabbit}\\ \text{pairs born}\\ \text{at the end}\\ \text{of month } k\end{bmatrix}$$

$$= \begin{bmatrix}\text{the number}\\ \text{of rabbit}\\ \text{pairs alive}\\ \text{at the end}\\ \text{of month } k-1\end{bmatrix} + \begin{bmatrix}\text{the number}\\ \text{of rabbit}\\ \text{pairs alive}\\ \text{at the end}\\ \text{of month } k-2\end{bmatrix}$$

Recursion: example 4 (continued)

- **Fibonacci numbers**

  The initial number of rabbit pairs: $F_0 = 1$

  F_n : the number of rabbit pairs at the end of month n, for each integer $n \geq 1$

  $F_n = F_{n-1} + F_{n-2}$, for all integers $n \geq 2$

  $F_1 = 1$, because the first pair of rabbits is not fertile until the second month

  How many rabbit pairs are at the end of one year?

  January 1st: $F_0 = 1$

  February 1st: $F_1 = 1$

  March 1st : $F_2 = F_1 + F_0 = 1+1= 2$

  April 1st : $F_3 = F_2 + F_1 = 2+1= 3$

  May 1st : $F_4 = F_3 + F_2 = 3+2= 5$

  June 1st : $F_5 = F_4 + F_3 = 5+3= 8$

  July 1st : $F_6 = F_5 + F_4 = 8+5= 13$

  August 1st : $F_7 = F_6 + F_5 = 13+8= 21$

  September 1st : $F_8=F_7+F_6=21+13=34$

  October 1st : $F_9=F_8+F_7=34+21=55$

  November 1st : $F_{10}=F_9+F_8=55+34=89$

  December 1st :
  $F_{11}=F_{10}+F_9=89+55=144$

  January 1st : $F_{12}=F_{11}+F_{10}=144+89=$**233**

Recursion: example 5

- **Compound interest**
- A deposit of \$100,000 in a bank account earning 4% interest compounded annually:

the amount in the account at the end of any particular year

= the amount in the account at the end of the previous year + the interest earned on the account during the year

= the amount in the account at the end of the previous year + 0.04 · the amount in the account at the end of the previous year

$A_0 = \$100,000$

$A_k = A_{k-1} + (0.04) \cdot A_{k-1} = 1.04 \cdot A_{k-1}$, for each integer $k \geq 1$

$$A_1 = 1.04 \cdot A_0 = \$104,000$$

$$A_2 = 1.04 \cdot A_1 = 1.04 \cdot \$104,000 = \$108,160$$

…

Recursion: example 6

- **Compound interest with compounding several times a year**
- An annual interest rate of i is compounded m times per year:

  the interest rate paid per each period is i/m

  P_k is sum of amount at the end of the (k−1)-th period

  and interest earned during k-th period

  $P_k = P_{k-1} + P_{k-1} \cdot i/m = P_{k-1} \cdot (1 + i/m)$

- If 3% annual interest is compounded quarterly, then the interest rate paid per quarter is 0.03/4 = 0.0075

Compound interest: examples

Example: deposit of \$10,000 at 3% compounded quarterly

For each integer $n \geq 1$,

P_n = the amount on deposit after n consecutive quarters.

$P_k = 1.0075 \cdot P_{k-1}$

$P_0 = \$10,000$

$P_1 = 1.0075 \cdot P_0 = 1.0075 \cdot \$10,000 = \$10,075.00$

$P_2 = 1.0075 \cdot P_1 = (1.0075) \cdot \$10,075.00 = \$10,150.56$

$P_3 = 1.0075 \cdot P_2 \approx (1.0075) \cdot \$10,150.56 = \$10,226.69$

$P_4 = 1.0075 \cdot P_3 \approx (1.0075) \cdot \$10,226.69 = \$10,303.39$

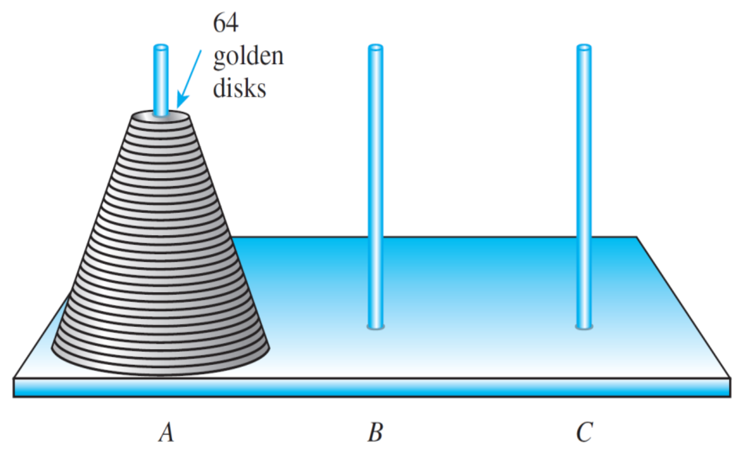
The annual percentage rate (APR) is the percentage increase in the value of the account over a one-year period:

$APR = (10303.39 - 10000)/\ 10000 = 0.03034 = 3.034\%$

Recursion: example 7

- **Towers of Hanoi:** *n* disks piled in order of decreasing size on one pole in a row of three

- Want to move all the disks one by one from one pole to another, never placing a larger disk on top of a smaller one
- How many moves are required to move the disks from pole A to C?

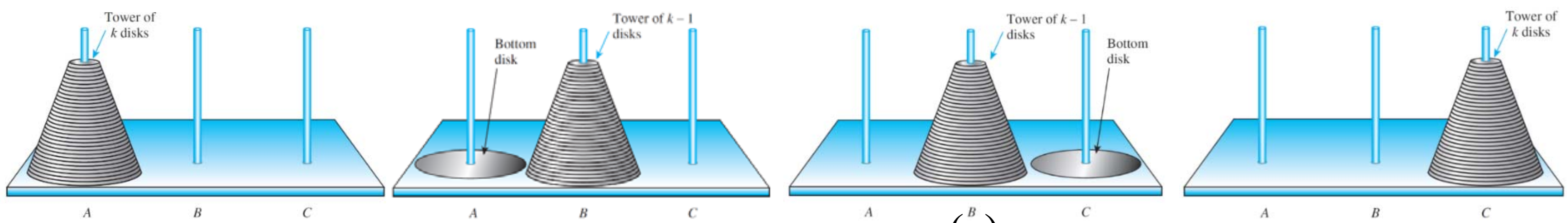


HW 4 extra-credit programming: even generate all moves in 2 lines

- A best way to solve this problem is to think recursively!

Recursion: example 7 (continued)

- Moves must include going from initial position (a) to (b) to (c) to (d).



(a) (b) (c) (d)

- For $k \geq 1$, let m_k benumber of moves to move a tower of k disks from one pole to another.
- (a) to (b) needs m_{k-1} moves, (b) to (c) 1 move, (c) to (d) m_{k-1}

$$m_k \;=\; m_{k-1} + 1 + m_{k-1} \;=\; 2m_{k-1} + 1$$

- Simplest case: 1 disk, so move from pole A to C in one move

$$m_1 = 1$$

- $m_2 = 2m_1 + 1 = 2 \cdot 1 + 1 = 3,$
  $m_3 = 2m_2 + 1 = 2 \cdot 3 + 1 = 7,$
  $m_4 = 2m_3 + 1 = 2 \cdot 7 + 1 = 15,$

Recursive definitions of sum and product

- The summation from i=1 to n of a sequence is defined using recursion:

$$\sum_{i=1}^{1} a_i = a_1 \quad \text{and} \quad \sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n, \quad \text{if } n > 1.$$

$f(1) = a_1 \qquad f(n) = f(n-1) + a_n$

- The product from i=1 to n of a sequence is defined using recursion:

$$\prod_{i=1}^{1} a_i = a_1 \quad \text{and} \quad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) \cdot a_n, \quad \text{if } n > 1.$$

$\Sum \longrightarrow \prod \qquad + \longrightarrow \cdot$

Sum of sums: recursion and induction

- For any positive integer n, if $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ 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 induction** (**using recursive definition of sum**):

$$\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i. \quad \leftarrow P(n)$$

Base step:

$$\sum_{i=1}^{1}(a_i + b_i) = a_1 + b_1 = \sum_{i=1}^{1} a_i + \sum_{i=1}^{1} b_i$$

Inductive hypothesis:

$$\sum_{i=1}^{k}(a_i + b_i) = \sum_{i=1}^{k} a_i + \sum_{i=1}^{k} b_i. \quad \leftarrow P(k)$$

Sum of sums continued

We must show that:

$$\sum_{i=1}^{k+1}(a_i + b_i) = \sum_{i=1}^{k+1} a_i + \sum_{i=1}^{k+1} b_i . \qquad \leftarrow P(k+1)$$

$$\begin{aligned}
\sum_{i=1}^{k+1}(a_i + b_i) &= \sum_{i=1}^{k}(a_i + b_i) + (a_{k+1} + b_{k+1}) && \text{by definition of } \Sigma \\
&= \left(\sum_{i=1}^{k} a_i + \sum_{i=1}^{k} b_i\right) + (a_{k+1} + b_{k+1}) && \text{by inductive hypothesis} \\
&= \left(\sum_{i=1}^{k} a_i + a_{k+1}\right) + \left(\sum_{i=1}^{k} b_i + b_{k+1}\right) && \text{by the associative and cummutative laws of algebra} \\
&= \sum_{i=1}^{k+1} a_i + \sum_{i=1}^{k+1} b_i && \text{by definition of } \Sigma
\end{aligned}$$

Q.E.D.

Solving recurrence relations

- **Arithmetic sequence**: there is a constant d such that

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

  It follows that, $a_n = a_0 + d \cdot n$ for all integers $n \geq 0$.

- **Geometric sequence**: there is a constant r such that

  $a_k = r \cdot a_{k-1}$ for all integers $k \geq 1$

  It follows that, $a_n = a_0 \cdot r^n$ for all integers $n \geq 0$.

A general form of recurrence relation

- A **second-order linear homogeneous recurrence relation** with constant coefficients is a recurrence relation of the form:

  $a_k = A \cdot a_{k-1} + B \cdot a_{k-2}$ for all integers $k \geq$ some fixed integer

  where A and B are fixed real numbers with $B \neq 0$.

- In general: given a sequence, or a recurrence relation, guess a closed-form formula, and prove by induction.

Applications: correctness of algorithms

- A program is correct if it produces the output specified in its documentation for each set of inputs
  - initial state (inputs): pre-condition for the algorithm
  - final state (outputs): post-condition for the algorithm

- Example:

  Algorithm to compute a product of two nonnegative integers

  pre-condition: input variables m and n are nonnegative integers

  post-condition: output variable p equals m*n

Correctness of algorithms

- The steps of an algorithm are divided into sections with assertions about the current state of algorithm

[Assertion 1: pre-condition for the algorithm]

{Algorithm statements}

[Assertion 2]

{Algorithm statements}

…

[Assertion $k - 1$]

{Algorithm statements}

[Assertion k: post-condition for the algorithm]

Correctness of algorithms

- **Loop invariants** are used to prove correctness of a loop with respect to pre- and post-conditions

[pre-condition for the loop]

while (G)

{Statements in the body of the loop}

end while

[post-condition for the loop]

A loop is correct with respect to its pre- and post-conditions if, and only if,

whenever the algorithm variables satisfy the pre-condition for the loop, and the loop terminates after a finite number of steps, the algorithm variables satisfy the post-condition for the loop.

Loop invariant

- A **loop invariant** is a predicate with domain a set of integers, satisfying: for each iteration of the loop, **(induction)** if the predicate is true before the iteration, then it is true after the iteration.

- Furthermore, if the following two conditions hold
  - before the first iteration of the loop,
    the predicate is implied by the pre-condition for the loop,
  - if the loop terminates after a finite number of iterations,
    the predicate ensures the post-condition for the loop,

  then the loop is with respect to its pre- and post-conditions.

Loop invariant: example

- **Correctness of a loop to compute a product**

A loop to compute the product m*x for a nonnegative integer m and a real number x, without using multiplication

[pre-condition: m is a nonnegative integer, x is a real number, $i = 0$, and product = 0]

while $(i \neq m)$

product := product + x

i := i + 1

end while

[post-condition: product = m*x]

Loop invariant I(n): [$i = n \land$ product = n*x]

Guard G: $i \neq m$

Loop invariant I(n): [$i = n \wedge$ product $= n*x$]   Guard G: $i \neq m$

Base property:

[I(0): $i = 0$ and product $= 0 \cdot x = 0$ is true before first iteration]

Inductive property:

[If $G \wedge I(k)$ is true before an iteration (where $k \geq 0$), then I $(k+1)$ is true after the iteration]

Let k is a nonnegative integer such that $G \wedge I(k)$ is true, i.e.,

$$i \neq m \quad \wedge \quad i = k \quad \wedge \quad \text{product} = k*x$$

Since $i \neq m$, the guard is passed and

$$\text{product} = \text{product} + x \qquad = k*x + x \quad = (k + 1)*x$$
$$i = i + 1 \qquad\qquad = k + 1$$

So $I(k + 1)$: $i = k + 1 \wedge \text{product} = (k + 1)*x$ is true after the iteration

Eventual falsity of guard:

[After a finite number of iterations, G becomes false]

After m iterations of the loop: $i = m$ and G becomes false

Loop invariant I(n): $[i = n \wedge product = n*x]$ Guard G: $i \neq m$

Correctness of the post-condition:

[If N is the least number of iterations after which G is false and I (N) is true, then the value of the algorithm variables will be as specified in the post-condition of the loop]

I(N) is true at the end of the loop: $i = N \wedge product = N*x$

G becomes false after N iterations: $i = m$

So $N = i = m$

Post-condition $product = m*x$ after execution of the loop is true.