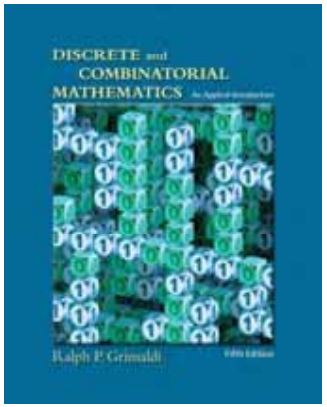
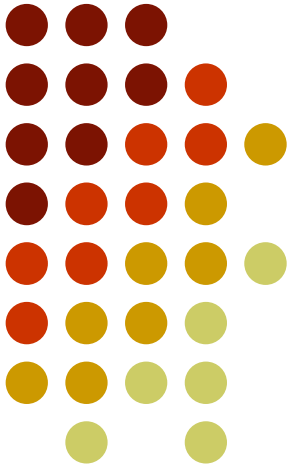
Discrete Mathematics

-- *Chapter 4: Properties of the Integers: Mathematical Induction*





Hung-Yu Kao (高宏宇)

Department of Computer Science and Information Engineering,

National Cheng Kung University

Outline

- 4.1 The Well-Ordering Principle: Mathematical Induction
- 4.2 Recursive Definitions

4.1 The Well-Ordering Principle: Mathematical Induction

- **The Well-Ordering Principle**: Every nonempty subset of $\mathbf{Z}^+$ contains a **smallest** element.
  ($\mathbf{Z}^+ = \{x \in \mathbf{Z} \mid x > 0\} = \{x \in \mathbf{Z} \mid x \geq 1\}$)
  $\mathbf{Z}^+$ is well ordered
- **The Principle of Mathematical Induction**: Let $S(n)$ denote an open mathematical statement that involves one or more occurrences of the variable n, which represents a positive integer.
  a) If $S(1)$ is true; and (basis step)
  b) If whenever $S(k)$ is true, then $S(k+1)$ is true. (inductive step)

  then $S(n)$ is true for all $n \in \mathbf{Z}^+$
- Using quantifiers

$$[S(n_0) \wedge [\forall k \geq n_0 [S(k) \Rightarrow S(k+1)]]] \Rightarrow \forall n \geq n_0 \; S(n)$$

4.1 The Well-Ordering Principle: Mathematical Induction

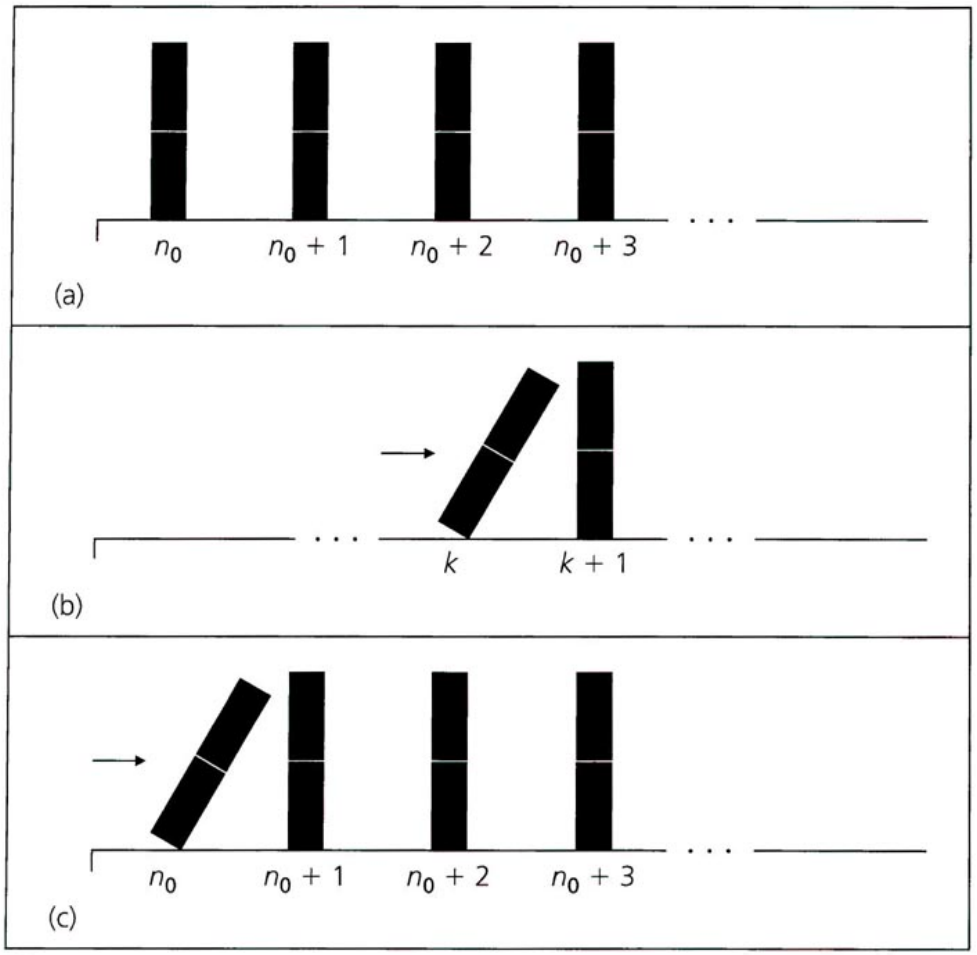


Figure 4.1

$P(n_0)$
$P(n_0+1)$
$P(n_0+2)$
.
.
.

Why Induction Works

- More rigorously, the validity of a proof by mathematical induction relies on the well-ordering of $\mathbf{Z}^+$.
- Let S be a statement for which we have proven that S(1) holds and for all $n \in \mathbf{Z}^+$ we have $S(n) \Rightarrow S(n+1)$. Claim: S(n) holds for all $n \in \mathbf{Z}^+$

- **Proof by contradiction**: Define the set $F \subseteq \mathbf{Z}^+$ of values for which S does not hold: $F = \{ m \mid S(m) \text{ does not hold} \}$.
  - If F is non-empty, then F **must have a smallest element** (well-ordering of $\mathbf{Z}^+$), let this number be z with $\neg S(z)$. Because we know that S(1), it must hold that $z>1$. Because z is the smallest value, it must hold that $S(z-1)$, which contradicts our proof for all $n \in \mathbf{Z}^+$: $S(n) \Rightarrow S(n+1)$.
  - Contradiction: F has to be empty: S holds for all $\mathbf{Z}^+$.

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.1** : For any $n \in \mathbf{Z}^+, \sum_{i=1}^{n} i = 1+2+3+\cdots+n = \frac{n(n+1)}{2}$
  - Proof

Let $S(n): \sum_{i=1}^{n} i = 1+2+3+\cdots+n = \frac{n(n+1)}{2}$

(i) $S(1): \sum_{i=1}^{1} i = 1 = \frac{1\times(1+1)}{2}$

(ii) Assume $S(k)$ is true, i.e., $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

(iii) Then $S(k+1): \sum_{i=1}^{k+1} i = 1+2+3+\cdots+k+(k+1)$

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

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

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.3** : Among the 900 three-digit integers (100 to 999), where the integer is the same whether it is read from left to right or from right to left, are called palindromes. Without actually determining all of these three-digit palindromes, we would like to determine their sum.
  - Solution

The typical palindrome: $aba = 100a + 10b + a = 101a + 10b$

$$\sum_{a=1}^{9}\left(\sum_{b=0}^{9} aba\right) = \sum_{a=1}^{9}\sum_{b=0}^{9}(101a + 10b)$$

$$= \sum_{a=1}^{9}\left[10(101a) + 10\sum_{b=0}^{9} b\right] = \sum_{a=1}^{9}\left[1010a + 10 \cdot 45\right]$$

$$= 1010\sum_{a=1}^{9} a + 9 \cdot 450 = 49{,}500$$

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.5**
  - Consider pseudocode procedures (comparisons)
  - Procedure 1: *n* additions and *n* multiplications (additionally, counter i)
  - Procedure 2: *2* additions, *3* multiplications, and 1 division

```
procedure SumOfSquares1
begin
   sum:= 0
   for i:= 1 to n do
      sum := sum + i^2
end
```

```
procedure SumOfSquares2
begin
   sum:= n*(n+1)*(2*n+1)/6
end
```

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.8**
  - For $n \geq 6,\ 4n < (n^2 - 7)$.
  - Solution

n	$4n$	n^2-7	n	$4n$	n^2-7
1	4	-6	5	20	18
2	8	-3	6	24	29
3	12	2	7	28	42
4	16	9	8	32	57

$$S(k): 4k < (k^2 - 7),\ k \geq 6$$

2*6+1=13 ≥4

$$S(k+1): 4(k+1) = 4k + 4 < (k^2 - 7) + 4 < (k^2 - 7) + (2k + 1)$$

$$\Rightarrow 4(k+1) < (k^2 - 7) + (2k + 1) = (k+1)^2 - 7$$

$\therefore S(n)$ is true.

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.9** : Harmonic numbers $H_1 = 1, H_2 = 1 + \frac{1}{2}, \cdots, H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$

  For all n, $\sum_{j=1}^{n} H_j = (n+1)H_n - n$

  - Proof

    Verify $S(1): \sum_{j=1}^{1} H_j = H_1 = 1 = (1+1)H_1 - 1$

    Assume $S(k)$ true : $\sum_{j=1}^{k} H_j = (k+1)H_k - k$

    Verify $S(k+1): \sum_{j=1}^{k+1} H_j = \sum_{j=1}^{k} H_j + H_{k+1} = [(k+1)H_k - k] + H_{k+1}$

    $$= (\mathrm{k}+1)H_k - k + H_{k+1}$$

    $$= (\mathrm{k}+1)[H_{k+1} - \frac{1}{k+1}] - k + H_{k+1}$$

    $$= (\mathrm{k}+2)H_{k+1} - (k+1)$$

    $\therefore S(n)$ is true.

The Well-Ordering Principle: Mathematical Induction

- Mathematical induction plays a major role in programming verification.
- **Ex 4.11** :
  - The pseudocode program segment is supposed to produce the answer xy^n.
  - Proof

```
while n≠ 0 do
  begin
    x := x * y
    n := n - 1
  end
answer := x
```

Verify $S(0)$: answer $= x = xy^0$

Assume $S(k)$ true: answer $= xy^k$

Verify $S(k+1)$: when $n = k+1$, the program reach the the top of the 'while' loop for the first time, the loop instructionsare executed and return to the top of the 'while' loop again, now we find

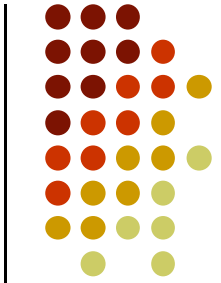
- $x_1 = xy$
- $n = (k+1) - 1 = k$

And the 'while' loop will continue with x_1, y and $n = k$

$\therefore$ The final answer $= x_1 y^k = (xy)y^k = xy^{k+1}$

$\therefore S(n)$ is true.

The Well-Ordering Principle: Mathematical Induction



- **Ex 4.13** :
  - Show that for all $n \geq 14$ we can express n using only 3's and 8's as summands. (e.g., $14 = 3 + 3 + 8$)
  - Proof

Assume $S(k)$ true :

Verify $S(k+1)$:

While $n = k$

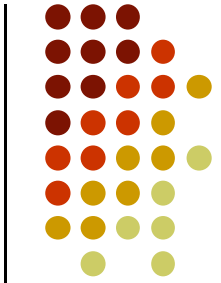
case (i) at least one 8 appears in the sum, replace 8 with three 3's for $n = k+1$

case (ii) no 8 appears in the sum, $\because \geq 14, \therefore$ the sum have at least five 3's ,

replace five 3's with two 8's for $n = k+1$

$\therefore S(k) \Rightarrow S(k+1)$

Fibonacci Sequence



- Consider the sequence 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89,… which is defined by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$
- Clearly this sequence $F_1, F_2, \ldots$ will grow, but how fast?
- **Conjecture**: $F_n \geq (3/2)^n$ for all n>10
- **Proof by induction**:

Base case: Indeed $F_{11} = 89 \geq (3/2)^{11} = 86.49756\ldots$

Other base case: also $F_{12} = 144 \geq (3/2)^{12} = 129.746338\ldots$

- Inductive step for n>10:

Assume $F_n \geq (3/2)^n$ and $F_{n+1} \geq (3/2)^{n+1}$, then indeed

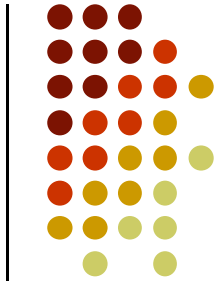
- $F_{n+2} = F_n + F_{n+1} \geq (3/2)^n + (3/2)^{n+1} = (3/2)^n(1 + (3/2))$
- $= (3/2)^n(5/2) \geq (3/2)^n (9/4) = (3/2)^{n+2}$
- By induction on n, the conjecture holds.

Other Induction Proofs

- We just saw a different kind of proof by induction where the inductive step is $\forall n>10$: [P(n), P(n+1) $\Rightarrow$ P(n+2)]
  This time the basis step is proving P(11) *and* P(12).

- There are many variations of proof by induction:
  Strong/ Complete induction: Here the inductive step is:
  Assume all of P(1),…,P(n), then prove P(n+1).
  The basis step is P(1) for this alternative form of induction.

Fibonacci Numbers



- The sequence 1,1,2,3,5,8,13,21,34,… defined by $F_{n+2}= F_n+F_{n+1}$ is the famous **Fibonacci sequence**.

- A closed expression of F_n is

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

- For large n, it grows like $F_n \approx 0.447214 \times 1.61803^n$.
- This $(1+\sqrt{5})/2 \approx 1.61803$ is the **Golden Ratio**.

The Well-Ordering Principle: Mathematical Induction

- Theorem 4.2: The Principle of Mathematical Induction – Alternative Form: (or the **Principle of Strong Mathematical Induction**)
  - Let $S(n)$ denote an open mathematical statement that involves one or more occurrences of the variable n, which represents a positive integer.
    a) If $S(n_0)$, $S(n_0+1)$, …, $S(n_1-1)$, and $S(n_1)$ are true ← *Basic step*
    b) If whenever $S(n_0)$, $S(n_0+1)$, …, $S(k-1)$, and $S(k)$ are true for some $k \in \mathbf{Z}^+$, where $k \geq n_1$, then $S(k+1)$ is also true ← *inductive step*

  then $S(n)$ is true for all $n \geq n_0$.

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.14** :
  - Show that for all $n \geq 14$, n can be written as a sum of only 3's and 8's. (e.g., 14 = 3+3+8, 15 = 3+3+3+3+3, 16 = 8+8)
  - Proof

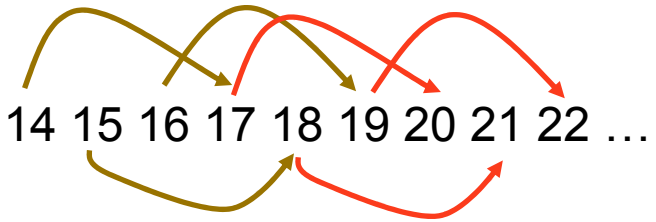
Verify $S(14), S(15)$, and $S(16)$ are true.

Assume $S(14), S(15), \cdots, S(k-2), S(k-1)$ and $S(k)$ are true, where $k \geq 16$

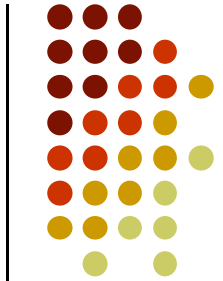
Verify $S(k+1)$:

$\because k+1 = (k-2)+3$, and $14 \leq k-2 \leq k$, $S(k-2)$ is true

$\therefore S(k+1)$ is true



The Well-Ordering Principle: Mathematical Induction



- **Ex 4.15** :
  - Show that $a_n \le 3^n$, where

$$\begin{cases} a_0 = 1, a_1 = 2, a_2 = 3, \text{and} \\ a_n = a_{n-1} + a_{n-2} + a_{n-3}, \text{ for all } n \in \mathbf{Z}^+ \text{ where } n \ge 3 \end{cases}$$

  - Proof

(i) $a_0 = 1 = 3^0 \le 3^0$

$a_1 = 2 \le 3 = 3^1$

$a_2 = 3 \le 9 = 3^2$

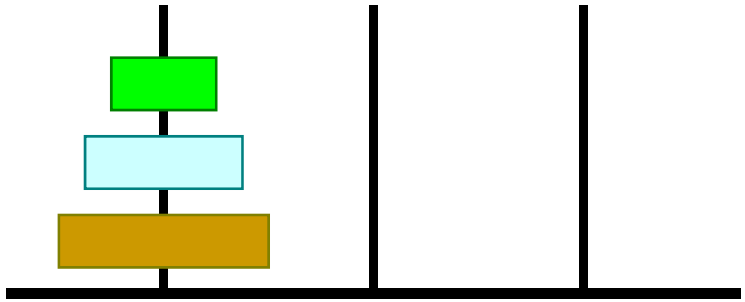
(ii) $a_{k+1} = a_k + a_{k-1} + a_{k-2}$

$\le 3^k + 3^{k-1} + 3^{k-2}$

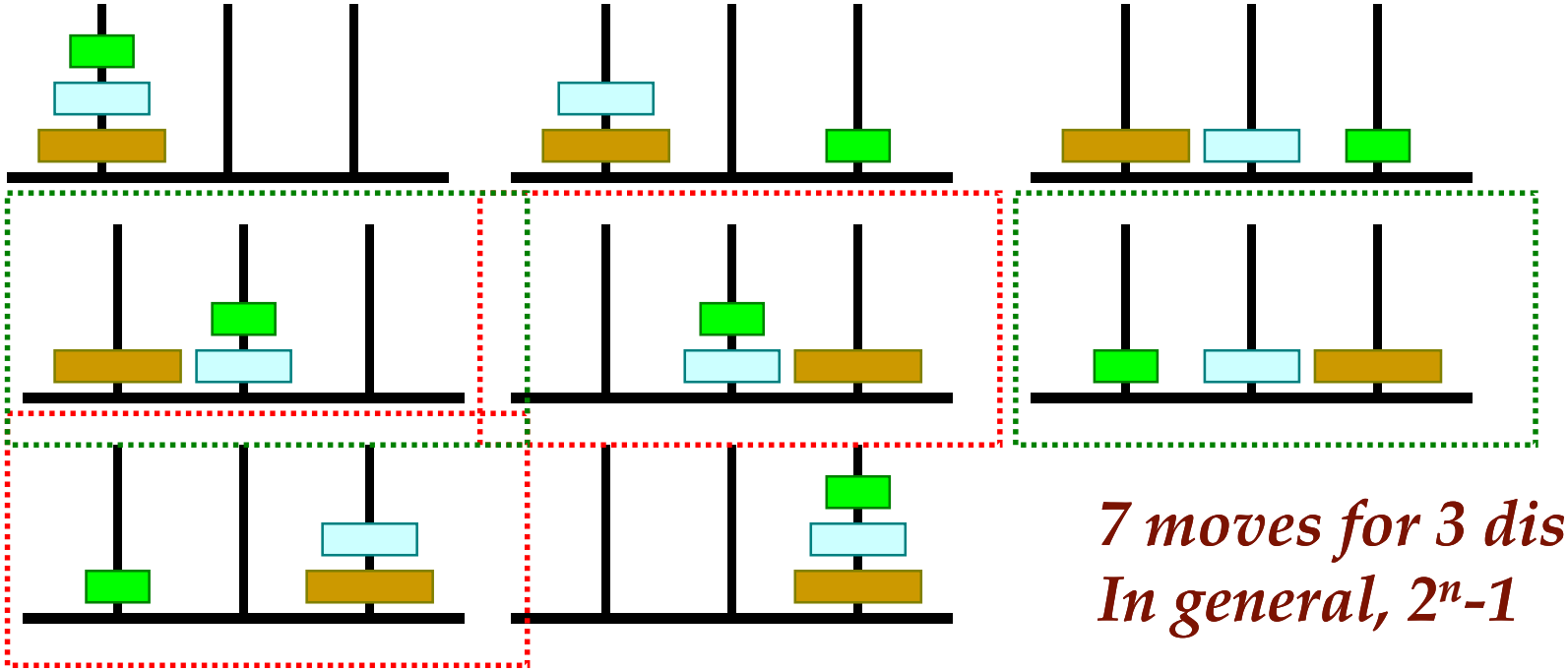
$\le 3^k + 3^k + 3^k = 3(3^k) = 3^{k+1}$

Induction, another example

- **Towers of Hanoi**: (1883)
  We have three poles and n golden disks
  the disks are only allowed in pyramid shape:
  no big disks on top of smaller ones
- How to move the disks from one pole to another?
  How many moves are requires?
- Call this number M(n).
  Note M(1)=1 and M(2)=3
  What about M(3)?



Inductive, Recursive



7 moves for 3 disks
In general, 2^n-1

Making a Conjecture

- To prove something by induction, you need a conjecture about the general case M(n).

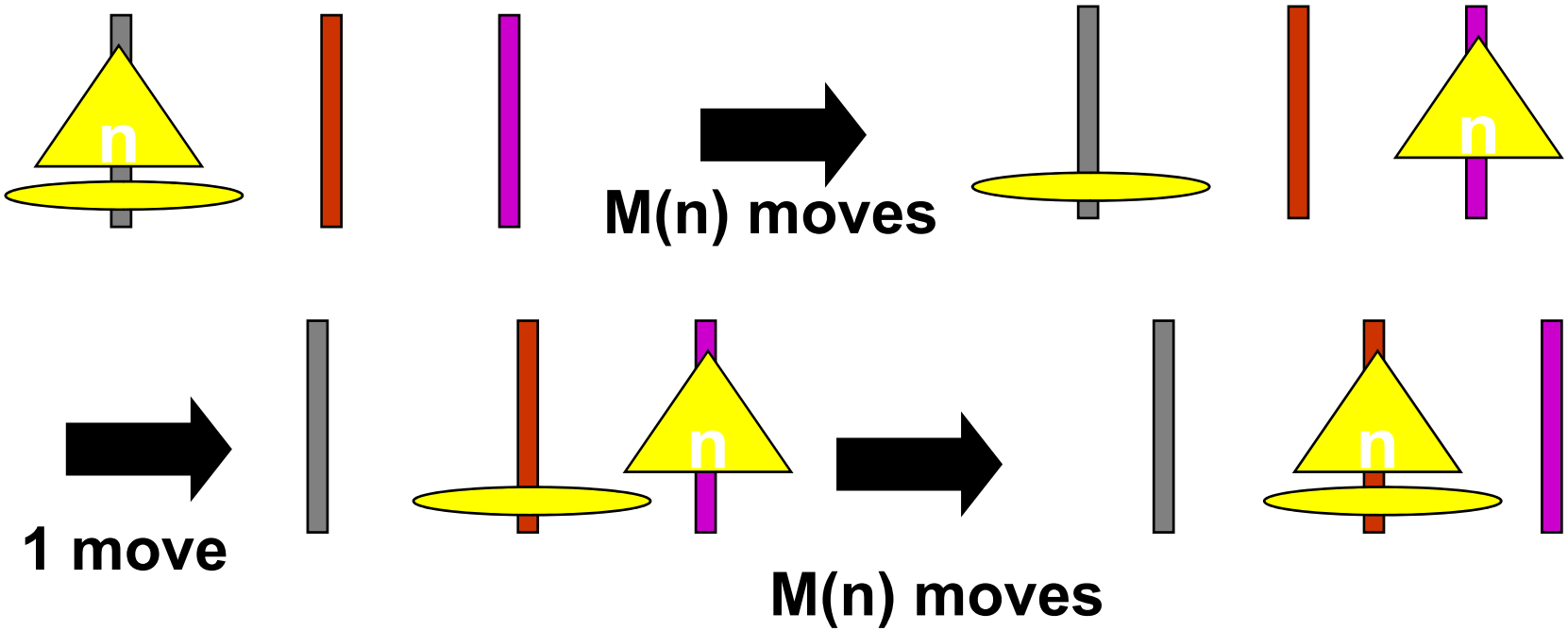
- Here we have: M(1)=1, M(2)=3, M(3)=7,…
- Obvious conjecture… $M(n) = 2^n - 1$ for all $n > 0$

- Clearly, the basis step M(1)=1 holds.

- Feeling for general n case: Each additional disk (almost) doubles the number of moves:
M(n+1) consists of two M(n) cases…

Inductive Step

How to move n+1 disks, using an n-disk 'subroutine'?

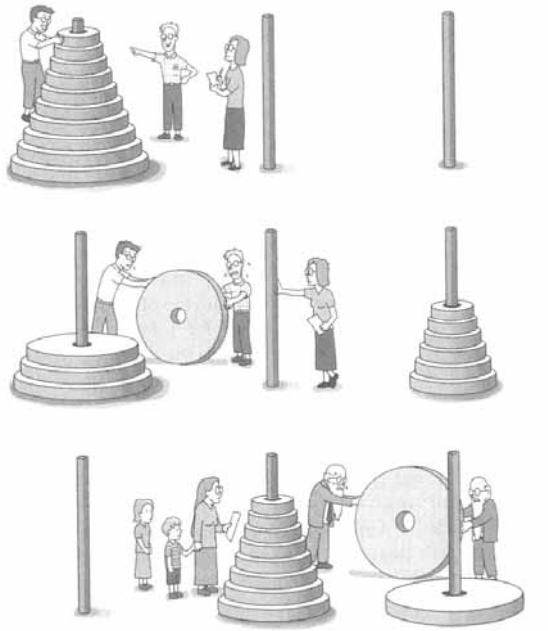


In sum: M(n+1) = 2 M(n)+1

Proof of ToH

- We just saw that for all n, we have $M(n+1) = 2M(n)+1$.
This enables our proof of the conjecture $M(n)=2^n–1$.
- Proof: Basis step: $M(1) = 2^1–1 = 1$ holds.
- Assume that $M(n)=2^n–1$ holds. Then, for next n+1:
- $M(n+1) = 2\ M(n) + 1 = 2(2^n–1) + 1 = 2^{n+1} – 1$.
- Hence it holds for n+1. End of proof by induction on n.

With n=64 golden disks, and one move per second, this amounts to almost 600,000,000,000 years of work.



Induction in CS

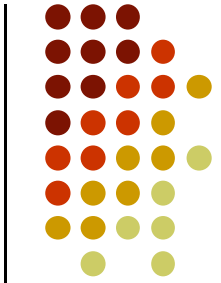
- Inductive proofs play an important role in computer science because of their similarity with **recursive algorithms**.

- Analyzing recursive algorithms often require the use of recurrent equations, which require inductive proofs.

Structural Induction

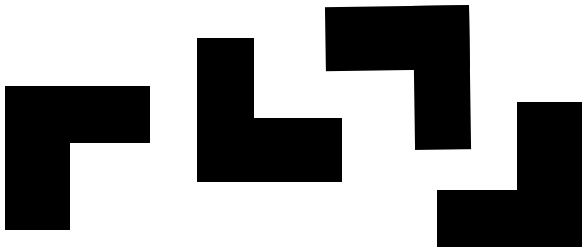
- The method of induction can also be applied to structures other than integers, like graphs, matrices, trees, sequences and so on.
- The crucial property that must hold is the **well-ordered principle**: there has to be a notion of size such that all objects have a finite size, and each set of objects must have a smallest object.
- **Examples**: vertex size of graphs, dimension of matrices, depth of trees, length of sequences and so on.

L-Tiling an $2^n \times 2^n$ Square

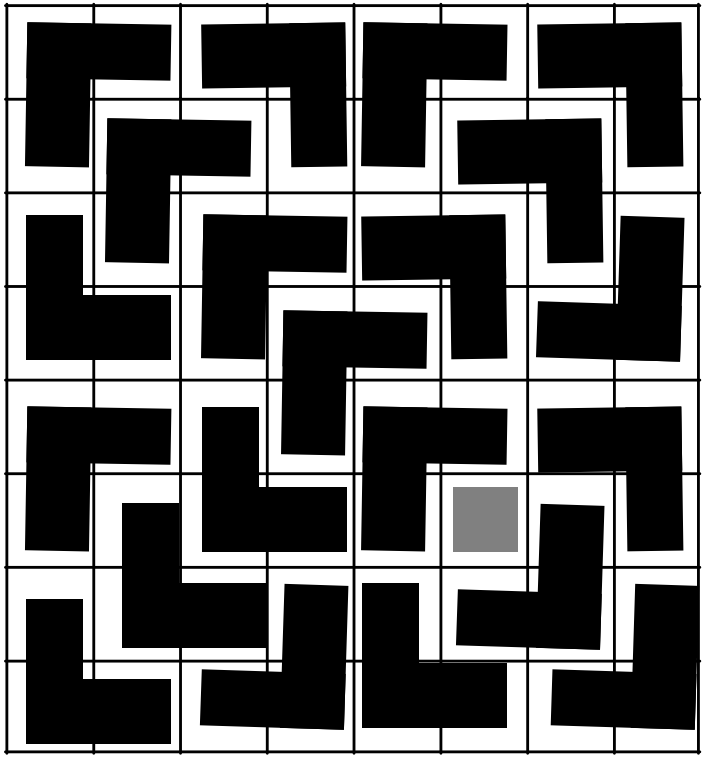


Take a $2^n \times 2^n$ square with one tile missing

Can you tile it with L-shapes?

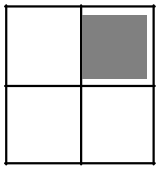


Theorem:
Yes, you can for all n.



Example for 8×8:

Proving L-Tiling



Basis step of 2×2 squares is easy.

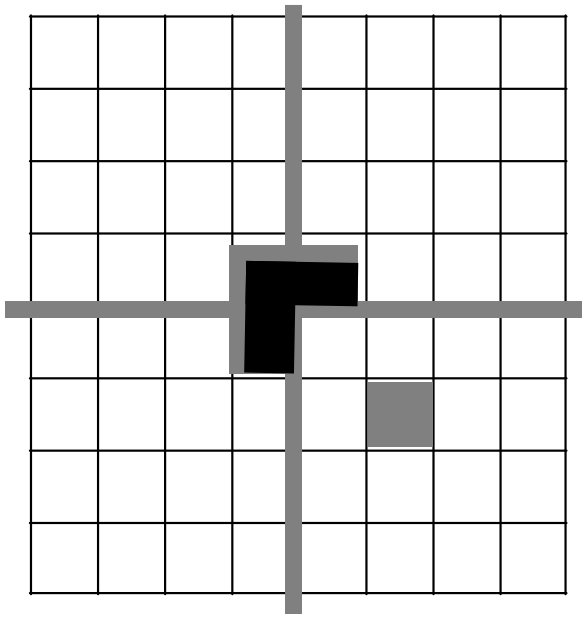
Inductive step: Assuming that $2^n\times2^n$ tiling is possible,
tile a $2^{n+1}\times2^{n+1}$ square by looking at 4 sub-squares:

Put the 3 holes in the middle:

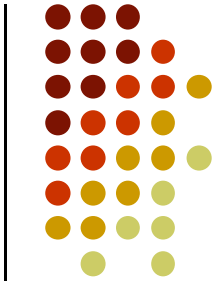
Put an L in the middle,
and tile the sub-squares
using the assumption.

Proof by induction on n.

This is a constructive proof.



4.2 Recursive Definitions



- **Ex 4.19** : Fibonacci numbers

  1) $F_0 = 0; F_1 = 1;$

  2) $F_n = F_{n\text{-}1} + F_{n\text{-}2},$ for all $n \in \mathbf{Z}^+$ where $n \geq 2$

$$\forall n \in \mathbf{Z}^+ \sum_{i=0}^{n} F_i^2 = F_n \times F_{n+1}$$

- Proof

basis step, $F_0^2 + F_1^2 = 1*1$

$$\text{Assume } \sum_{i=0}^{k} F_i^2 = F_k \times F_{k+1}$$

$$\text{Then } \sum_{i=0}^{k+1} F_i^2 = \sum_{i=0}^{k} F_i^2 + F_{k+1}^2$$

$$= F_k \times F_{k+1} + F_{k+1}^2$$

$$= F_{k+1} \times (F_k + F_{k+1})$$

$$= F_{k+1} \times F_{k+2}$$

Recursive Definitions

- **Ex 4.20** : Lucas numbers

1) $L_0 = 2; L_1 = 1;$

2) $L_n = L_{n-1} + L_{n-2},$ for all $n \in \mathbf{Z}^+$ where $n \geq 2$

Table 4.2

n	0	1	2	3	4	5	6	7
L_n	2	1	3	4	7	11	18	29

$$\forall n \in \mathbf{Z}^+ \; L_n = F_{n-1} + F_{n+1}$$

Proof :

basis step, $L_1 = 1 = 0 + 1 = F_0 + F_2$, $L_2 = 3 = 1 + 2 = F_1 + F_3$

Assume $L_n = F_{n-1} + F_{n+1}$ for $n = 1,2,3,\ldots,k-1,k$, where $k \geq 2$

Then $L_{k+1} = L_k + L_{k-1} = (F_{k-1} + F_{k+1}) + (F_{k-2} + F_k)$

$= (F_{k-1} + F_{k-2}) + (F_{k+1} + F_k)$

$= F_k + F_{k+2}$

$= F_{(k+1)-1} + F_{(k+1)+1}$