Discrete Mathematics for Computer Science

Department of Computer Science

Lecturer: Nazeef Ul Haq

Reference Book: Discrete Mathematics and its applications BY Kenneth H. Rosen – 8th edition

Proof Terminology

- A ***proof*** is a valid argument that establishes the truth of a mathematical statement
- ***Axiom*** (or ***postulate***): a statement that is assumed to be true
- ***Theorem***
  - A statement that has been proven to be true
- ***Hypothesis***, ***premise***
  - An assumption (often unproven) defining the structures about which we are reasoning

More Proof Terminology

- ***Lemma***
  - A minor theorem used as a stepping-stone to proving a major theorem.
- ***Corollary***
  - A minor theorem proved as an easy consequence of a major theorem.
- ***Conjecture***
  - A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, regardless.)

Proof Methods

- For proving implications $p \rightarrow q$, we have:
  - ***Direct* proof:**
  - ***Indirect* proof:**
    - ***Proof by Contraposition*** ($\neg q \rightarrow \neg p$):
      Assume $\neg q$, and prove $\neg p$.
    - ***Proof by Contradiction***:
      Assume $p \wedge \neg q$, and show this leads to a contradiction. (i.e. prove $(p \wedge \neg q) \rightarrow$ **F)**
  - ***Vacuous* proof:** Prove $\neg p$ by itself.

Direct Proof Example

- **Definition:** An integer n is called *odd* iff $n=2k+1$ for some integer k; n is *even* iff $n=2k$ for some k.
- **Theorem:** Every integer is either odd or even, but not both.
  - This can be proven from even simpler axioms.
- **Theorem:**
  (For all integers n) If n is odd, then n^2 is odd.

  Proof:

  If n is odd, then $n = 2k + 1$ for some integer k.

  Thus, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

  Therefore n^2 is of the form $2j + 1$ (with j the integer $2k^2 + 2k$), thus n^2 is odd. ■

Indirect Proof Example: Proof by Contraposition

- **Theorem:** (For all integers n)
  If $3n + 2$ is odd, then n is odd.

- **Proof:** Can we apply direct proof method? NO

  (Contrapositive: If n is even, then $3n + 2$ is even)

  Suppose that the conclusion is false, *i.e.*, that n is even.

  Then $n = 2k$ for some integer k.

  Then $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.

  Thus $3n + 2$ is even, because it equals $2j$ for an integer $j = 3k + 1$. So $3n + 2$ is not odd.

  We have shown that $\neg(n \text{ is odd}) \rightarrow \neg(3n + 2 \text{ is odd})$, thus its contrapositive $(3n + 2 \text{ is odd}) \rightarrow (n \text{ is odd})$ is also true. ■

Proof by Contradiction Example: Implication

- **Theorem:** (For all integers n)
  If $3n + 2$ is odd, then n is odd.

- **Proof:**

  Assume that the conclusion is false, *i.e.*, that n is even, and that $3n + 2$ is odd.

  Then $n = 2k$ for some integer k and $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. Thus $3n + 2$ is even, because it equals $2j$ for an integer $j = 3k + 1$.

  This contradicts the assumption "$3n + 2$ is odd".

  This completes the proof by contradiction, proving that if $3n + 2$ is odd, then n is odd. ■

Trivial and Vacuous Proof

- ***Trivial Proof***: If we know *q* is true, then
  $p \rightarrow q$ is true as well.
  "If it is raining then $1=1$."

- ***Vacuous Proof***: If we know *p* is false then
  $p \rightarrow q$ is true as well.
  "If I am both rich and poor then $2 + 2 = 5$."

Mistakes in Proof

- ***Prove that 1=2***

Step	Reason
1. $a = b$	Premise
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

- The error is that a-b is zero.

Mistakes in Proof

- **Theorem:** If n^2 is positive, then n is positive.

Proof: Suppose that n^2 is positive. Because the conditional statement "If n is positive, then n^2 is positive" is true, we can conclude that n is positive.

- Let $P(n)$ be "n is positive" and $Q(n)$ be "n^2 is positive."

Then our hypothesis is $Q(n)$.

The statement is $\forall n(P(n) \rightarrow Q(n))$. From the hypothesis $Q(n)$ and the statement $\forall n(P(n) \rightarrow Q(n))$ we cannot conclude $P(n)$, because we are not using a valid rule of inference. A counter example is supplied by $n = -1$ for which $n^2 = 1$ is positive, but n is negative.

Exhaustive Proof

- Prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Solution: $(n + 1)^3 \geq 3^n$ when $n = 1, 2, 3,$ and 4.

For $n = 1$, we have $(n + 1)^3 = 2^3 = 8$ and $3^n = 3^1 = 3$;

For $n = 2$, we have $(n + 1)^3 = 3^3 = 27$ and $3n = 3^2 = 9$;

For $n = 3$, we have $(n + 1)^3 = 4^3 = 64$ and $3^n = 3^3 = 27$;

For $n = 4$, we have $(n + 1)^3 = 5^3 = 125$ and $3^n = 3^4 = 81$.

In each of these four cases, we see that $(n + 1)^3 \geq 3n$. We have used the method of exhaustion to prove that $(n + 1)^3 \geq 3n$ if n is a positive integer with $n \leq 4$.

Proof By Cases

- **Prove that if n is an integer, then $n^2 \geq n$.**

Solution: We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$,
when $n \geq 1$, and when $n \leq -1$

Case (i): When $n = 0$, because $0^2 = 0$, and $0^2 \geq 0$. TRUE

Case (ii): When $n \geq 1$, when we multiply both sides of the inequality $n \geq 1$ $n^2 \geq n$ TRUE

Case (iii): When $n \leq -1$. However, $n^2 \geq 0$ and $n^2 \geq n$. TRUE

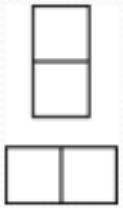
Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$.

Proof and disproof: Tilings

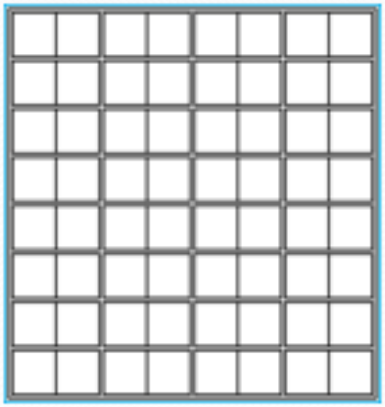
Example 1: Can we tile the standard checkerboard using dominos?

Solution: Yes! One example provides a constructive existence proof.

The Standard Checkerboard



Two Dominoes



One Possible Solution

Proof and disproof: Tilings

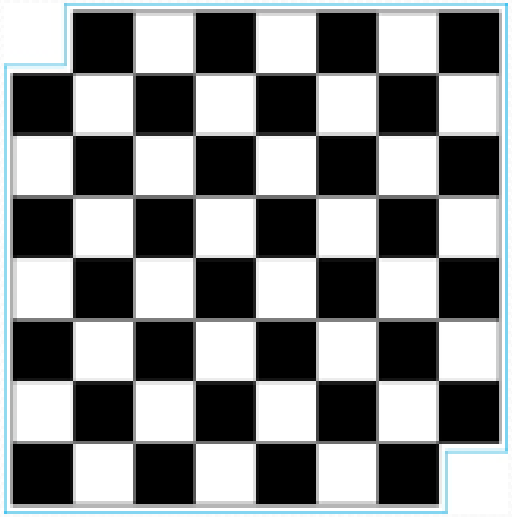
Example 2: Can we tile a checkerboard obtained by removing one of the four corner squares of a standard checkerboard?

Solution:

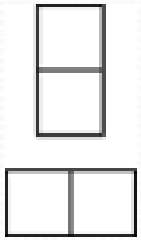
- Our checkerboard has $64 - 1 = 63$ squares.
- Since each domino has two squares, a board with a tiling must have an even number of squares.
- The number 63 is not even.
- We have a contradiction.

Proof and disproof: Tilings

Example 3: Can we tile a board obtained by removing both the upper left and the lower right squares of a standard checkerboard?



Nonstandard Checkerboard



Dominoes

Proof and disproof: Tilings

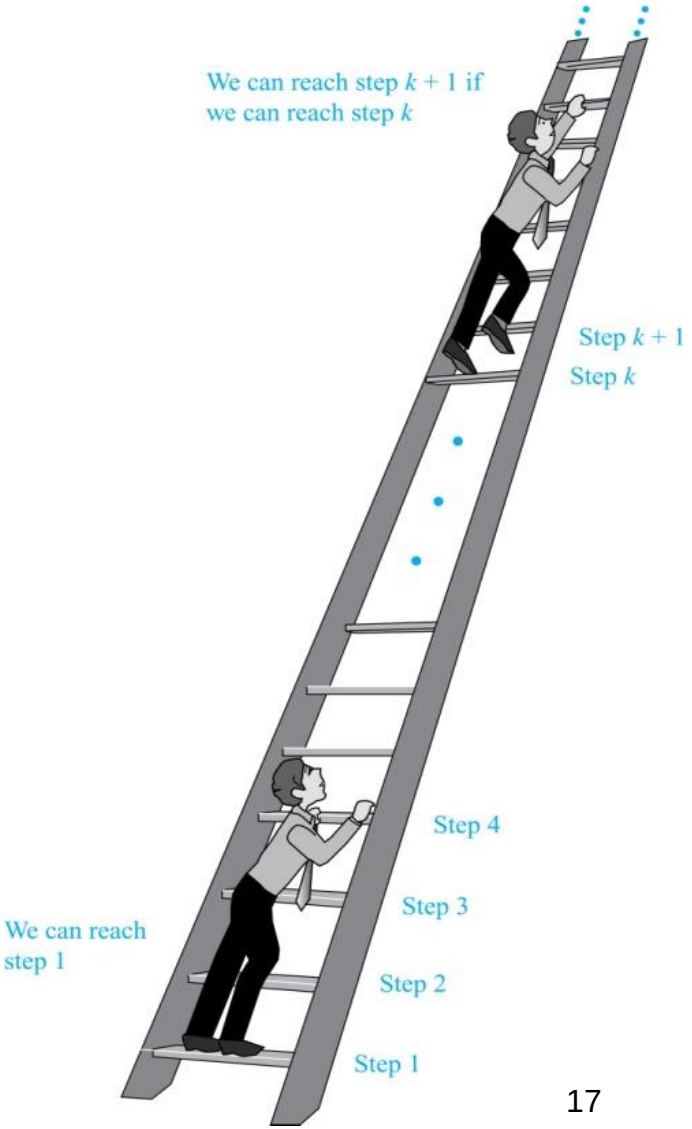
- **Solution**:
- There are 62 squares in this board.
- To tile it we need 31 dominos.
- *Key fact*: Each domino covers one black and one white square.
- Therefore the tiling covers 31 black squares and 31 white squares.
- Our board has either 30 black squares and 32 white squares or 32 black squares and 30 white squares. Contradiction!

Proof By Mathematical Induction

- Suppose we have an infinite ladder:

1. We can reach the first rung of the ladder.
2. If we can reach a particular rung of the ladder, then we can reach the next rung.

From (1), we can reach the first rung. Then by applying (2), we can reach the second rung. Applying (2) again, the third rung. And so on. We can apply (2) any number of times to reach any particular rung, no matter how high up.



Proof By Mathematical Induction

- ***Principle of Mathematical Induction*:** To prove that $P(n)$ is true for all positive integers n, we complete these steps:

***Basis Step*:** Show that $P(1)$ is true.

***Inductive Step*:** Show that $P(k) \rightarrow P(k + 1)$ is true for all positive integers k.

To complete the inductive step, assuming the *inductive hypothesis* that $P(k)$ holds for an arbitrary integer k, show that must $P(k + 1)$ be true.

Proof By Mathematical Induction

- Use Mathematical Induction to prove that

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}$$ for all integers n $\geq$ 1

SOLUTION

Let

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

Basis Step:

P(1) is true.

For n = 1, left hand side of P(1) is the sum of all the successive integers starting at 1 and ending at 1, so LHS = 1 and RHS is

Proof By Mathematical Induction

and RHS is

$$R.H.S = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

so the proposition is true for n = 1.

Inductive Step: Suppose P(k) is true for, some integers $k \geq 1$.

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

To prove P(k + 1) is true. That is,

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

Proof By Mathematical Induction

- Consider L.H.S. of (2)

$$1+2+3+\cdots+(k+1) = 1+2+3+\cdots+k+(k+1)$$

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

$$= (k+1)\left[\frac{k}{2}+1\right]$$

$$= (k+1)\left[\frac{k+2}{2}\right]$$

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

- Hence by principle of Mathematical Induction the given result true for all integers greater or equal to 1.

Proof By Mathematical Induction

- Prove that $n^3 - n$ is divisible by 3, for every positive integer n.

Solution: Let $P(n)$ be the proposition that $n^3 - n$ is divisible by 3.

BASIS STEP: $P(1)$ is true since $1^3 - 1 = 0$, which is divisible by 3.

INDUCTIVE STEP: Assume $P(k)$ holds, i.e., $k^3 - k$ is divisible by 3. To show that $P(k + 1)$ follows:

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

Therefore, $n^3 - n$ is divisible by 3, for every integer positive integer n.

Proof By Mathematical Induction

DO YOURSELF

- Use mathematical induction to prove that
  $1+3+5+\ldots+(2n-1) = n^2$ for all integers $n \geq 1$.
- Use mathematical induction to prove that
  $1+2+2^2+\ldots+2^n = 2^{n+1}-1$ for all integers $n \geq 0$
- Prove by mathematical induction for all integers $n \geq 1$

$$1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$$

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

$$\sum_{i=1}^{n+1} i2^i = n\cdot 2^{n+2}+2, \qquad \text{for all integers } n \geq 0$$

Proof By Strong Induction

- ***STRONG INDUCTION:*** To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

BASIS STEP: We verify that the proposition $P(1)$ is true.

INDUCTIVE STEP: We show that the conditional statement $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ is true for all positive integers k.

- Also called the **second principle of mathematical induction** or **complete induction**.

Proof By Strong Induction

- **Example**: Suppose we can reach the first and second rungs of an infinite ladder, and we know that if we can reach a rung, then we can reach two rungs higher. Prove that we can reach every rung.

(Try this with mathematical induction.)

Solution: Prove the result using strong induction.

BASIS STEP: We can reach the first step.

INDUCTIVE STEP: The inductive hypothesis is that we can reach the first k rungs, for any $k \geq 2$. We can reach $(k + 1)$st rung since we can reach the $(k - 1)$st rung by the inductive hypothesis. Hence, we can reach all rungs of the ladder.

Proof By Strong Induction

Example: Prove that every amount of postage of 12 cents or more can be formed using just 4-cent and 5-cent stamps.

Solution: Let $P(n)$ be the proposition that postage of n cents can be formed using 4-cent and 5-cent stamps.

BASIS STEP: $P(12)$, $P(13)$, $P(14)$, and $P(15)$ hold.

$P(12)$ uses three 4-cent stamps.

$P(13)$ uses two 4-cent stamps and one 5-cent stamp.

$P(14)$ uses one 4-cent stamp and two 5-cent stamps.

$P(15)$ uses three 5-cent stamps.

INDUCTIVE STEP: The inductive hypothesis states that $P(j)$ holds for $12 \leq j \leq k$, where $k \geq 15$. Assuming the inductive hypothesis, it can be shown that $P(k + 1)$ holds.

Using the inductive hypothesis, $P(k - 3)$ holds since $k - 3 \geq 12$. To form postage of $k + 1$ cents, add a 4-cent stamp to the postage for $k - 3$ cents.

Hence, $P(n)$ holds for all $n \geq 12$.

Well Ordering Property

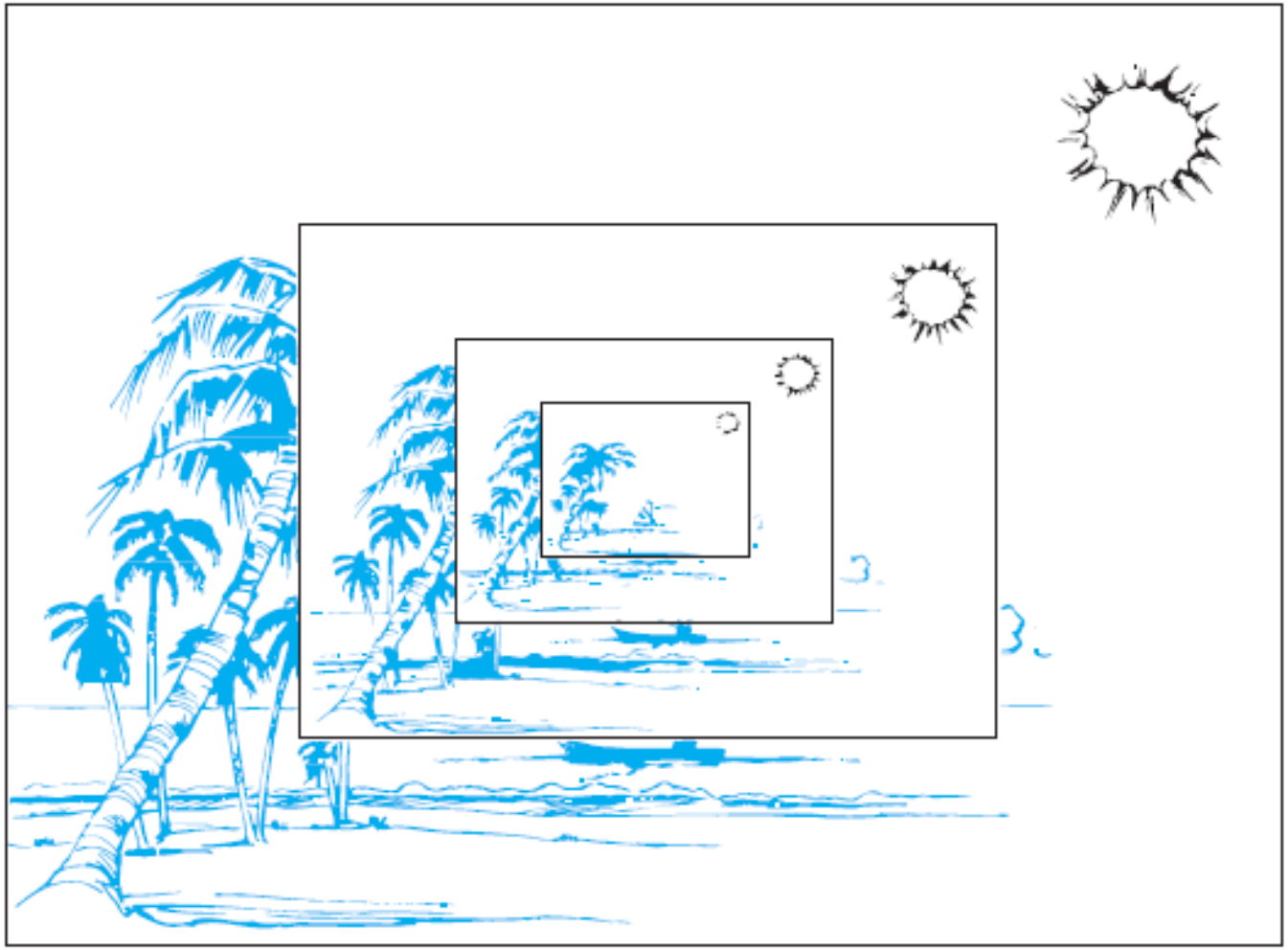
- **Definition:** Every non-empty set of non-negative integers has a least element.

Example: Use the well-ordering property to prove the division algorithm, which states that if a is an integer and d is a positive integer, then there are unique integers q and r with $0 \leq r < d$, such that $a = dq + r$.

Solution: Let S be the set of nonnegative integers of the form $a - dq$, where q is an integer. The set is nonempty since $-dq$ can be made as large as needed.

By the well-ordering property, S has a least element $r = a - dq_0$. The integer r is nonnegative. It also must be the case that $r < d$. If it were not, then there would be a smaller nonnegative element in S, namely, $a - d(q_0 + 1) = a - dq_0 - d = r - d \geq 0$.Therefore, there are integers q and r with $0 \leq r < d$.

Recursively Defined Functions



Recursively Defined Functions

- **Definition**: A *recursive* or *inductive definition* of a function consists of two steps.

BASIS STEP: Specify the value of the function at zero.

RECURSIVE STEP: Give a rule for finding its value at an integer from its values at smaller integers.

Recursively Defined Functions

- **Example**: Suppose f is defined by:

  $f(0) = 3$,

  $f(n + 1) = 2f(n) + 3$

  Find $f(1)$, $f(2)$, $f(3)$, $f(4)$

  Solution:

  $f(1) = 2f(0) + 3 = 2 \cdot 3 + 3 = 9$

  $f(2) = 2f(1) + 3 = 2 \cdot 9 + 3 = 21$

  $f(3) = 2f(2) + 3 = 2 \cdot 21 + 3 = 45$

  $f(4) = 2f(3) + 3 = 2 \cdot 45 + 3 = 93$

Example: Give a recursive definition of the factorial function $n!$:

Solution:

$f(0) = 1$

$f(n + 1) = (n + 1) \cdot f(n)$

Recursively Defined Sets

- *Recursive definitions* of sets have two parts:

Basis step specifies an initial collection of elements.

Recursive step gives the rules for forming new elements in the set from those already known to be in the set.

Sometimes the recursive definition has an *exclusion rule*, which specifies that set contains nothing other than those elements specified in the basis step and generated by applications of the recursive step.

We will always assume that the exclusion rule holds, even if it is not explicitly mentioned.

Structural Induction

- **Definition**: To prove a property of the elements of a recursively defined set, we use *structural induction*.

BASIS STEP: Show that the result holds for all elements specified in the basis step of the recursive definition.

RECURSIVE STEP: Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

Full Binary Tree

- **Definition**: The *height h(T)* of a full binary tree *T* is defined recursively as follows:

BASIS STEP: The height of a full binary tree *T* consisting of only a root *r* is $h(T) = 0$.

RECURSIVE STEP: If T_1 and T_2 are full binary trees, then the full binary tree $T = T_1 \cdot T_2$ has height $h(T) = 1+\max(h(T_1),h(T_2))$.

- The number of vertices $n(T)$ of a full binary tree *T* satisfies the following recursive formula:

BASIS STEP: The number of vertices of a full binary tree *T* consisting of only a root *r* is $n(T) = 1$.

RECURSIVE STEP: If T_1 and T_2 are full binary trees, then the full binary tree $T = T_1 \cdot T_2$ has the number of vertices

$$n(T) = 1 + n(T_1) + n(T_2).$$

Structural Induction Example

- **Theorem**: If T is a full binary tree, then $n(T) \leq 2^{h(T)+1} - 1$.

BASIS STEP: The result holds for a full binary tree consisting only of a root, $n(T) = 1$ and $h(T) = 0$. Hence, $n(T) = 1 \leq 2^{0+1} - 1 = 1$.

RECURSIVE STEP: Assume $n(T_1) \leq 2^{h(T1)+1} - 1$ and also $n(T_2) \leq 2^{h(T2)+1} - 1$ whenever T_1 and T_2 are full binary trees.

$n(T) = 1 + n(T_1) + n(T_2)$ (*by recursive formula of n(T)*)

$\leq 1 + (2^{h(T1)+1} - 1) + (2^{h(T2)+1} - 1)$ (*by inductive hypothesis*)

$\leq 2 \cdot \max(2^{h(T1)+1}, 2^{h(T2)+1}) - 1$

$= 2 \cdot 2^{\max(h(T1),h(T2))+1} - 1$ ($\max(2^x, 2^y) = 2^{\max(x,y)}$)

$= 2 \cdot 2^{h(t)} - 1$ (*by recursive definition of h(T)*)

$= 2^{h(t)+1} - 1$

Generalized Induction

- ***Generalized induction*** is used to prove results about sets other than the integers that have the well-ordering property.
- For example, consider an ordering on **N**× **N**, ordered pairs of nonnegative integers. Specify that (x_1, y_1) is less than or equal to (x_2, y_2) if either $x_1 < x_2$, or $x_1 = x_2$ and $y_1 < y_2$ This is called the *lexicographic ordering*.
- Strings are also commonly ordered by a *lexicographic ordering*.

Generalized Induction

- **Example**: Suppose that $a_{m,n}$ is defined for $(m,n) \in \mathbf{N} \times \mathbf{N}$ by $a_{0,0} = 0$ and

$$a_{m,n} = \begin{cases} a_{m-1,n} + 1 & \text{if } n = 0 \text{ and } m > 0 \\ a_{m,n-1} + n & \text{if } n > 0 \end{cases}.$$

show that $a_{m,n} = m + n(n + 1)/2$ is defined for all $(m,n) \in \mathbf{N} \times \mathbf{N}$.

Solution: Use generalized induction.

BASIS STEP: $a_{0,0} = 0 = 0 + (0 \cdot 1)/2$

INDUCTIVE STEP: Assume that $a_{m',n'} = m' + n'(n' + 1)/2$ whenever (m',n') is less than (m,n) in the lexicographic ordering of $\mathbf{N} \times \mathbf{N}$.

If $n = 0$, by the inductive hypothesis we can conclude

$a_{m,n} = a_{m-1,n} + 1 = m - 1 + n(n + 1)/2 + 1 = m + n(n + 1)/2$.

If $n > 0$, by the inductive hypothesis we can conclude

$a_{m,n} = a_{m-1,n} + 1 = m + n(n - 1)/2 + n = m + n(n + 1)/2$.