5.1 Mathematical Induction
5.2 Strong Induction

Wenjing Li

wjli@bupt.edu.cn

School of Computer Science

Beijing University of Posts & Telecommunications

Mathematical Induction

- A powerful, rigorous technique for proving that a predicate $P(n)$ is true for all positive integers.
- Essentially a "domino effect" principle.
  - **Premise #1:** Domino #1 falls.
  - **Premise #2:** For every $k \in \mathbf{N}$,
    if domino #k falls, then so does domino #$k+1$.
  - **Conclusion:** All of the dominoes fall down!

Note:
this works
even if there
are infinitely
many dominoes!

Mathematical Induction

- **Based on a predicate-logic inference rule:**

$$\begin{array}{l} P(1) \\ \forall k{\geq}1\ (P(k){\rightarrow}P(k{+}1)) \\ \hline \therefore \forall n{\geq}1\ P(n) \end{array}$$

"The First Principle of Mathematical Induction"

Validity of Induction(1)

- **Proof** that $\forall n \geq 1\ P(n)$ is a valid consequent:
  - Given any $k \geq 1$, the 2nd antecedent $\forall k \geq 1\ (P(k) \rightarrow P(k+1))$ trivially implies that $\forall k \geq 1\ (k<n) \rightarrow (P(k) \rightarrow P(k+1))$, *i.e.*, that

    $$(P(1) \rightarrow P(2)) \wedge (P(2) \rightarrow P(3)) \wedge \ldots \wedge (P(n-1) \rightarrow P(n)).$$

  - Repeatedly applying the **hypothetical syllogism** rule to adjacent implications in this list $n-1$ times, then gives us $P(1) \rightarrow P(n)$
  - Together with $\boldsymbol{P(1)}$ (antecedent #1) and **modus ponens** gives us $P(n)$.
  - Thus $\boldsymbol{\forall n \geq 1\ P(n)}$.

The Well-Ordering Property

- Another way to prove the validity of the inductive inference rule is by using the ***well-ordering property (良序性)***, which says that:
  - Every non-empty set of non-negative integers has a minimum (smallest) element.

$$\forall \varnothing \subset S \subseteq \mathbf{N} : \exists m \in S : \forall n \in S : m \leq n$$

The well-ordering property can be used directly in proofs.

  - This implies that $\{n | \neg P(n)\}$ (if non-empty) has a min element m, but then the assumption that $P(m-1) \rightarrow P((m-1)+1)$ would be contradicted.

Validity of Induction(2)

- **Proof (contradiction):**
  - Suppose that $P(1)$ holds and $P(k) \rightarrow P(k+1)$ is true for all positive integers k.
  - Assume there is at least one positive integer n for which P(n) is false. Then the set ***S*** of positive integers for which P(n) is false is nonempty.
  - By the well-ordering property, S has a least element, say m.
  - We know that m can not be 1 since $P(1)$ holds.
  - Since m is positive and greater than 1, $m-1$ must be a positive integer. Since $m-1 < m$, it is not in S, so $P(m-1)$ must be true.
  - But then, since the conditional $P(k) \rightarrow P(k+1)$ for every positive integer k holds, $P(m)$ must also be true.
  - This contradicts $P(m)$ being false.
  - Hence, $P(n)$ must be true for every positive integer n.

Outline of an Inductive Proof

- **Method:**
  - Let us say we want to prove $\forall n P(n)$.
  - Do the ***base case* (or *basis step*)**: Prove $P(1)$.
  - Do the ***inductive step***: Prove $\forall k(P(k) \rightarrow P(k+1))$.
    - *E.g.* you could use a direct proof, as follows:
      - Let $k \in \mathbf{N}$, assume $P(k)$. (*inductive hypothesis*)
      - Now, under this assumption, prove $P(k+1)$.
  - By mathematical induction, $\forall n P(n)$ is true.

Generalizing Induction

- **Generalizing 1:**
  - Rule can also be used to prove $\forall n \geq c\ P(n)$ for a given constant $c \in \mathbf{Z}$, where maybe $c \neq 1$.
  - In this circumstance, the ***basis step*** is to prove $P(c)$ rather than $P(1)$, and the ***inductive step*** is to prove

    $$\forall k \geq c\ (P(k) \rightarrow P(k+1))$$

  - Can reduce these to the form already shown.
- **Generalizing 2:**
  - Induction can also be used to prove $\forall n \geq c\ P(a_n)$ for any arbitrary series $\{a_n\}$.

Second Principle of Induction

- Characterized by another inference rule:

$$\frac{\begin{array}{l} P(1) \\ \forall k \geq 1\text{: } \overbrace{(\forall 1 \leq j \leq k\ P(j))}^{P \text{ is true in } all \text{ previous cases}} \rightarrow P(k+1) \end{array}}{\therefore \forall n \geq 1\text{: } P(n)}$$

$$\boldsymbol{(P(1) \wedge P(2) \wedge \cdots \wedge P(k)) \rightarrow P(k+1)}$$

- The only difference between this and the 1st principle is that:
  - the inductive step here makes use of the stronger hypothesis that $P(k+1)$ is true for *all* smaller numbers $j<k+1$, not just for $j=k$.

A.k.a. “Strong Induction”

Induction Example (1st princ.)

- **Example 2:**
  - Prove that the sum of the first n odd positive integers is n^2. That is, prove:

$$\underbrace{\forall n \geq 1: \sum_{i=1}^{n}(2i-1) = n^2}_{P(n)}$$

- **Proof by induction:**
  - **Basis step**: Let n=1. The sum of the first 1 odd positive integer is 1 which equals 1^2.
  - **Inductive step**: Prove $\forall n \geq 1: P(n) \rightarrow P(n+1)$.

$$\sum_{i=1}^{n+1}(2i-1) = \left(\sum_{i=1}^{n}(2i-1)\right) + (2(n+1)-1)$$

$$= n^2 + 2n + 1 \quad \textit{By inductive hypothesis } P(n)$$

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

  - By mathematical induction, $\forall n \geq 1\ P(n)$ is true.

Induction Example (1st princ.)

- **Example 5 (Proving Inequalities):**
  - Prove that $\forall n>0, n<2^n$.
- **Proof:**
  - Let $P(n)$: $(\forall n>0 \;\; n<2^n)$
  - **Basis step**: $P(1)$: $(1<2^1)=(1<2)=\mathbf{T}$.
  - **Inductive step**: For $k>0$, prove $P(k) \rightarrow P(k+1)$.
    - Assuming $k<2^k$, prove $k+1 < 2^{k+1}$.
    - Note $k + 1 < 2^k + 1$ (by inductive hypothesis)

      $< 2^k + 2^k$ (because $1<2=2\cdot 2^0 \leq 2\cdot 2^{n-1}= 2^n$)

      $= 2^{k+1}$
  - So $k+1 < 2^{k+1}$, and by mathematical induction, $n<2^n$ is true.

Induction Example (1^{st} princ.)

- **Example 6 (Proving Inequalities)**:
  - Use mathematical induction to prove that $2^n < n!$, $\forall n \geq 4$.
- **Solution**:
  - Let $P(n)$: $\forall n \geq 4$, $2^n < n!$.
  - **Basis Step**: $P(4)$ is true since $2^4 = 16 < 4! = 24$.
  - **Inductive Step**: Assume $P(k)$ holds, i.e., $2^k < k!$ for an arbitrary integer $k \geq 4$. To show that $P(k+1)$ holds:

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &< 2 \cdot k! \qquad \textit{(by the inductive hypothesis)} \\ &< (k+1)k! = (k+1)! \end{aligned}$$

  - Therefore, $2^n < n!$ Holds for every integer $n \geq 4$ by mathematical induction.

Note that here the basis step is $P(4)$,
since $P(0)$, $P(1)$, $P(2)$ and $P(3)$ are all false.

Induction Example (1st princ.)

- **Example 8: Proving divisibility results**
  - Use mathematical induction to prove that n^3 -n is divisible by 3 whenever n is a positive integer.
- **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, for an arbitrary positive integer k. To show that $P(k + 1)$ follows:

$$\begin{aligned}(k + 1)^3 - (k + 1) &= (k^3 + 3k^2 + 3k + 1) - (k + 1)\\ &= (k^3 - k) + 3(k^2 + k)\end{aligned}$$

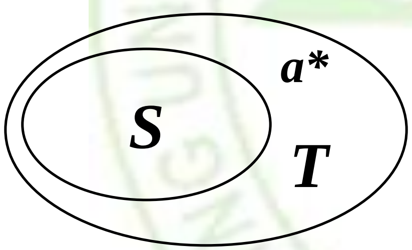
    By the inductive hypothesis, the first term $(k^3 - k)$ is divisible by 3 and the second term is divisible by 3. So by part (i) of Theorem 1 in Section 4.1 , $(k + 1)^3 - (k + 1)$ is divisible by 3.
  - By mathematical induction, $n^3 - n$ is divisible by 3, for every integer positive integer n.

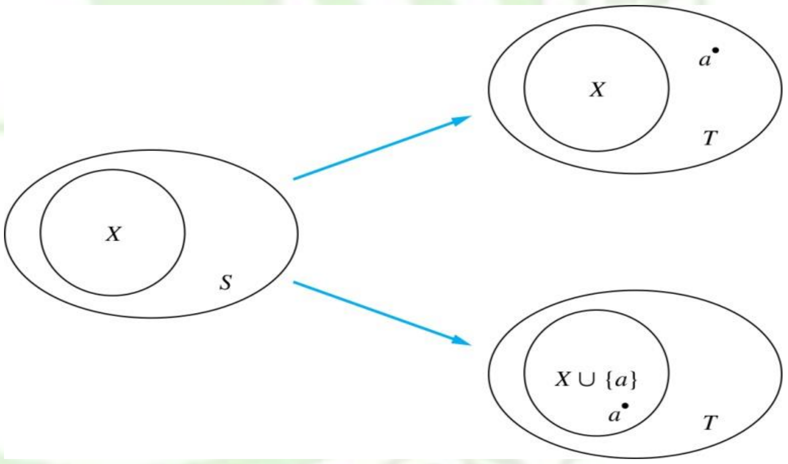
Induction Example (1 st princ.)

- **Example 10: Number of Subsets of a Finite Set**
  - Use mathematical induction to show that if S is a finite set with n elements, where n is a **nonnegative integer**, then S has 2^n subsets. (*Chapter* 6 *uses combinatorial methods to prove this result*.)
- **Solution:**
  - Let $P(n)$ be the proposition that a set with n elements has 2^n subsets.
  - **Basis Step**: $P(0)$ is true, because the empty set has only itself as a subset and $2^0 = 1$.
  - **Inductive Step**: Assume $P(k)$ is true for an arbitrary nonnegative integer k which has 2^k subsets.

Induction Example (1st princ.)

- **Solution(Cont):**
  - **Inductive Hypothesis**: For an arbitrary nonnegative integer k, every set with k elements has 2^k subsets.
  - Let T be a set with $k+1$ elements. Then $T = S \cup \{a\}$, where $a \in T$ and $S = T - \{a\}$. Hence $|S| = k$, $|T| = k+1$.
  - For each subset X of S, there are exactly two subsets of T, i.e., X and $X \cup \{a\}$.





  - By the inductive hypothesis S has 2^k subsets. Since there are two subsets of T for each subset of S, the number of subsets of T is $2 \cdot 2^k = 2^{k+1}$. By mathematical induction, $\forall n P(n)$ is true.

Induction Example (1 st princ.)

- **Example 13: Odd pie fights**
  - An odd number of people stand in a yard at mutually distinct distances.
  - At the same time each person throws a pie at their nearest neighbor, hitting this person.
  - Use mathematical induction to show that there is at least one survivor, that is, at least one person who is not hit by a pie.

Induction Example (1 st princ.)

- **Proof:**
  - Let $P(n)$ be the statement that there is a survivor whenever $2n + 1$ people stand in a yard at mutually distinct distances and each person throws a pie at their nearest neighbor.
  - **Basis Step**: When n = 1, there are 2n + 1 = 3 people in the pie fight. It's true.
  - **Inductive Step**: assume that $P(k)$ is true for an arbitrary integer k with $k \geq 1$ $(2k+1)$. To show $2k+3$ is true.
    - Let A and B be the closest pair of people in this group of $2k + 3$ people.
    - when no one else throws a pie at either A or B.
    - when someone else throws a pie at either A or B
  - By mathematical induction, $\forall n \geq 1$ $P(n)$ is true.

Induction Example (2nd princ.)

- **Example 2: Fundamental Theorem of Arithmetic**
  - Show that if n is an integer greater than 1, then n can be written as the product of primes (*uniqueness is proved in Section* 4.3).
- **Solution:**
  - Let $P(n)$ be the proposition that n can be written as a product of primes.
  - **Basis Step**: $P(2)$ is true since 2 itself is prime.
  - **Inductive Step**: The inductive hypothesis is $P(j)$ is true for all integers j with $2 \leq j \leq k$. To show that $P(k + 1)$ must be true under this assumption, two cases need to be considered:
    - If $k + 1$ is prime, then $P(k + 1)$ is true.
    - Otherwise, $k + 1$ is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k + 1$.
    - By the inductive hypothesis a and b can be written as the product of primes and therefore $k + 1$ can also be written as the product of those primes.
    - Hence, by mathematical induction, it has been shown that every integer greater than 1 can be written as the product of primes.

Induction Example (2nd princ.)

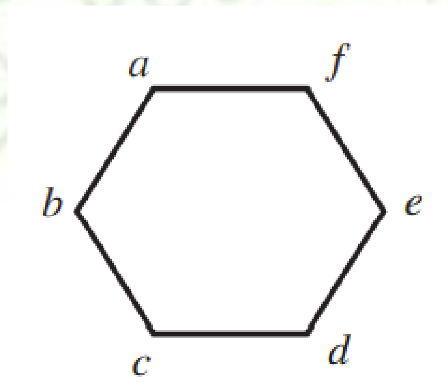
- **Example 4**:
  - Prove that every amount of postage of 12 cents or more can be formed using just 4-cent and 5-cent stamps.
- **Proof 1:**
  - $P(n)$: "n can be…"
  - **Basis step:** 12=3(4), 13=2(4)+1(5), 14=1(4)+2(5), 15=3(5), so $\forall 12 \le k \le 15, P(k)$.
  - **Inductive step:** Let $k \ge 15$, assume $\forall 12 \le j \le k\ P(j)$, to show $P(k+1)$ is true. Note $k-3 \ge 12$, so $P(k-3)$ is true.
  - Add a 4-cent stamp to get postage for $k+1$, thus $P(k+1)$.
  - By mathematical induction, $\forall n \ge 12\ P(n)$ is true.

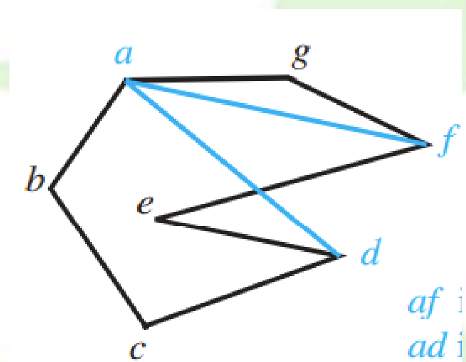
Induction Example (2nd princ.)

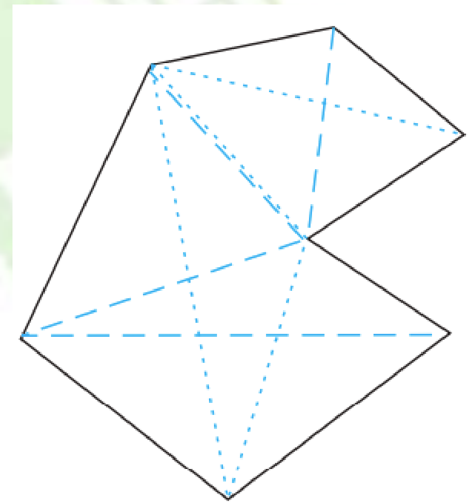
- **Proof 2**:
  - **Basis Step**: Postage of 12 cents can be formed using three 4-cent stamps.
  - **Inductive Step**: The inductive hypothesis $P(k)$ for any positive integer $k \geq 12$ is that postage of k cents can be formed using 4-cent and 5-cent stamps. To show $P(k + 1)$ hold where $k \geq 12$, we consider two cases:
    - If at least one 4-cent stamp has been used, then a 4-cent stamp can be replaced with a 5-cent stamp to yield a total of $k+1$ cents.
    - Otherwise, no 4-cent stamp have been used and at least three 5-cent stamps were used. Three 5-cent stamps can be replaced by four 4-cent stamps to yield a total of $k+1$ cents.
  - Hence, $P(n)$ holds for all $n \geq 12$.

Induction Example (2nd princ.)

- **Strong induction in computational geometry**
  - Polygon
  - Vertex
  - Simple
  - Interior
  - Exterior
  - Diagonal
  - Convex
  - Triangulation







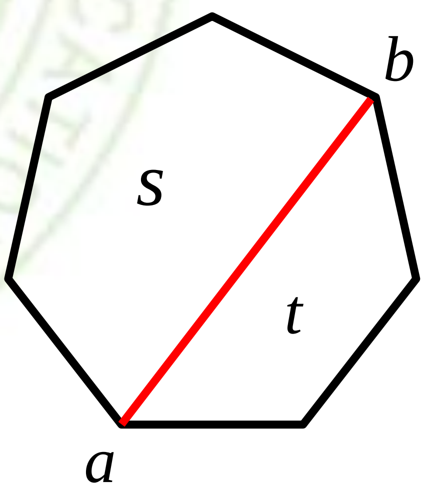
Computational geometry is widely used in computer graphics, computer games, robotics, scientific calculations ……

Induction Example (2nd princ.)

- **Theorem 1: Computational geometry**
  - A simple polygon with n sides, where n is an integer with $n \geq 3$, can be triangulated into $n-2$ triangles.
  - **Lemma:** Every simple polygon with at least four sides has an interior diagonal. ***(which is difficult to prove.)***
- **Proof:**
  - Let $T(n)$ is the statement.
  - **Basis Step**: $T(3)$ is true.
  - **Inductive Step**: Assume all $T(j)$ is true when $3 \leq j \leq k$, that is a simple polygon with j sides can be triangulated into $j-2$ triangles. To show $T(k+1)$ is also true, a simple polygon P with $k+1$ sides can be triangulated into $k-1$ triangles.

INDUCTION EXAMPLE (2^{ND} PRINC.)

- **Proof (cont):**
  - An interior diagonal *ab* splits *P (with k+1 sides)* into two simple polygons with *s* and *t* sides respectively (according to lemma).
  - ***Sides: s+t-2=k+1***
  - We now use the inductive hypothesis. Because both $3 \le s \le k$ and $3 \le t \le k$, by the inductive hypothesis we can triangulate the two polygons into $s-2$ and $t-2$ triangles, respectively. Thus the total triangles are $s+t-4$.
  - ***Triangles: s+t-4= s+t-2-2= k+1-2=k-1***
  - Hence, for all $n \ge 3$ *T(n)* is true.



- **Example 6: Round-robin tournament**
  - In a round-robin tournament every player **plays every other** player exactly once and each match has a winner and a loser. We say that the players $p_1, p_2, \ldots, p_m$ form a **cycle** if p_1 beats p_2, p_2 beats p_3, . . . , p_{m-1} beats p_m, and p_m beats p_1.
  - Use the well-ordering principle to show that if there is a cycle of length m $(m \geq 3)$ among the players in a round-robin tournament, there must be a cycle of three of these players.

Uses of the Well-Ordering Property

- **Solution (contradiction):**
  - We assume that there is no cycle of three players.
  - Because there is at least one cycle in the round-robin tournament, the set of all positive integers n for which there is a cycle of length n is nonempty. By the well-ordering property, this set of positive integers has a least element k, which must be greater than three. Consequently, there exists a cycle of players $p_1, p_2, p_3, \ldots, p_k$ and no shorter cycle exists.
  - Because there is no cycle of three players, we know that $k > 3$.
  - Consider the first three elements of this cycle, p_1, p_2, and p_3. There are two possible outcomes of the match between p_1 and p_3.
    - If p_3 beats p_1, it follows that p_1, p_2, p_3 is a cycle of length three, contradicting our assumption that there is no cycle of three players. Consequently, it must be the case that p_1 beats p_3.
    - This means that we can omit p_2 from the cycle $p_1, p_2, p_3, \ldots, p_k$ to obtain the cycle $p_1, p_3, p_4, \ldots, p_k$ of length $k - 1$, contradicting the assumption that the smallest cycle has length k.
  - We conclude that there must be a cycle of length three.

The Method of Infinite Descent

- **Method of Infinite Descent (无限递降法/费马递降法)**
  - A way to prove that $P(n)$ is false for all $n \in \mathbf{N}$. Sort of a **converse** to the principle of induction.
  - We use method of contradiction, assume $P(n)$ is true.
  - Firstly, by the well-ordering property of **N**, we know that $\exists P(m): \forall P(n): m \le n$
    - Basically, "If there is a P, there is a smallest P."
  - Then prove that $\forall P(n): \exists k < n: P(k)$.
    - Basically, "For every P there is a smaller P."
  - Note that these are contradictory
    - that is, ***P*(*n*) is false.**

思路：
假设一个最小值，又找到比它还小的

The Method of Infinite Descent

- **Example:**
  - **Theorem:** $2^{1/2}$ is irrational.
- **Proof:**
  - Suppose $2^{1/2}$ is rational, then $\exists m,n \in \mathbf{Z}^+$: $2^{1/2}=m/n$.
  - Let M,N be the m,n with the least n.

$$\sqrt{2}=\frac{M}{N}\therefore 2=\frac{M^2}{N^2}\therefore 2N^2=M^2.$$

$$\frac{M}{N}=\frac{M(M-N)}{N(M-N)}=\frac{M^2-MN}{N(M-N)}=\frac{2N^2-MN}{N(M-N)}=\frac{N(2N-M)}{N(M-N)}=\frac{2N-M}{M-N}$$

$$1<\sqrt{2}<2\therefore 1<\frac{M}{N}<2\therefore N<M<2N\therefore 0<M-N<N$$

  - So $\exists k<N$, $\exists j$: $2^{1/2} = j/k$ (let $j=2N-M$, $k=M-N$). Contradiction.

Which Induction Should Be Used?

- We can always use strong induction instead of mathematical induction. But there is no reason to use it if it is simpler to use mathematical induction.
- In fact, the principles of mathematical induction, strong induction, and the well-ordering property are all ***equivalent***. (*Exercises* 41-43)
- Sometimes it is clear how to proceed using one of the three methods, but not the other two.

Homework

- § 5.1
  - 32, 44, 54
- § 5.2
  - 4, 26

5.3 Recursive Definitions and Structural Induction

Wenjing Li

wjli@bupt.edu.cn

School of Computer Science

Beijing University of Posts & Telecommunications

Definitions

- In ***induction (归纳)***, we ***prove*** all members of an infinite set satisfy some predicate *P* by:
  - proving the truth of the predicate for larger members in terms of that of smaller members.
- In ***recursive definitions (递归定义)***, we similarly ***define*** a function, a predicate, a set, or a more complex structure over an infinite domain (universe of discourse) by:
  - defining the function, predicate value, set membership, or structure of larger elements **in terms of those of smaller ones**.
- In ***structural induction (结构归纳)***, we inductively ***prove*** properties of recursively-defined objects in a way that parallels the objects' own recursive definitions. (用对象自己的递归定义来归纳地证明递归定义对象的属性)

Recursion

- **Definition:**
  - ***Recursion*** is the general term for the practice of defining an object in terms of *itself* or of *part of itself*. (This may seem circular, but it isn't necessarily.)
  - An ***inductive proof*** establishes the truth of $P(n+1)$ *recursively* in terms of $P(n)$.
  - There are also recursive *algorithms*, *functions*, *sequences*, *sets*, and other structures.

Recursively Defined Functions

- **Simplest case:**
  - One way to define a function f:**N**$\rightarrow S$ (for any set S) or series $a_n = f(n)$ is to:
    - Define $f(0)$.
    - For $n>0$, define $f(n)$ in terms of $f(0),\ldots,f(n-1)$.
- **Example:**
  - Define the series $a_n :\equiv 2^n$ recursively:
    - Let $a_0 :\equiv 1$.
    - For $n>0$, let $a_n :\equiv 2a_{n-1}$.

Recursively Defined Functions

- **Another Example:**
  - Suppose we define $f(n)$ for all $n \in \mathbf{N}$ recursively by:
    - Let $f(0)=3$
    - For all $n \in \mathbf{N}$, let $f(n+1)=2f(n)+3$
  - What are the values of the following?

$f(1)=$

$f(2)=$

$f(3)=$

$f(4)=$

Recursive definition of Factorial

- Give an inductive (recursive) definition of the factorial function,

  $$F(n) :\equiv n! :\equiv \prod_{1\le i\le n} i = 1\cdot 2\cdot \ldots \cdot n.$$

  - Base case: $F(0) :\equiv 1$
  - Recursive part: $F(n) :\equiv n \cdot F(n-1)$.
    - $F(1)=$
    - $F(2)=$
    - $F(3)=$

Other Recursive definitions

- Write down recursive definitions for:
  - $a \cdot n$ (a real, n natural) using only addition
  - a^n (a real, n natural) using only multiplication
  - $\sum_{0 \le i \le n} a_i$ (for an arbitrary series of numbers $\{a_i\}$)
  - $\prod_{0 \le i \le n} a_i$ (for an arbitrary series of numbers $\{a_i\}$)
  - $\bigcap_{0 \le i \le n} S_i$ (for an arbitrary series of sets $\{S_i\}$)

The Fibonacci Series

- The ***Fibonacci series*** $f_{n\geq 0}$ is a famous series defined by:

$$f_0 :\equiv 0, \quad f_1 :\equiv 1, \quad f_{n\geq 2} :\equiv f_{n-1} + f_{n-2}$$

Leonardo Fibonacci
1170-1250

Inductive Proof about Fib. series

- **Theorem:** $f_n < 2^n$.
- **Proof:** By induction.
  - **Basis step** : $f_0 = 0 < 2^0 = 1$
    $f_1 = 1 < 2^1 = 2$
  - **Inductive step**: Use 2nd principle of induction (strong induction).
  - Assume $\forall k<n,\ f_k < 2^k$.
  - Then $f_n = f_{n-1} + f_{n-2}$ is

$$< 2^{n-1} + 2^{n-2} < 2^{n-1} + 2^{n-1} = 2^n.$$

Inductive Proof about Fib. series

- **Theorem**
  - For all integers $n \geq 3$, $f_n > \alpha^{n-2}$, where $\alpha = (1+5^{1/2})/2 \approx 1.61803$.
- **Proof.** (Using strong induction.)
  - Let $P(n) : (f_n > \alpha^{n-2})$.
  - **Basis step:** For n=3, note that $f_3 = 2 > \alpha$.

    For n=4, $f_4 = 3 > \alpha^2 = (1+2\cdot 5^{1/2}+5)/4 = (3+5^{1/2})/2 \approx 2.61803$
  - **Inductive step:**
    - For $k \geq 4$, assume $P(j)$ is true for $3 \leq j \leq k$, prove $P(k+1)$.
    - By strong inductive hypothesis, $f_k > \alpha^{k-2}$ and $f_{k-1} > \alpha^{k-3}$.
    - **Note $\alpha^2 = \alpha+1$**. Thus, $\alpha^{k-1} = (\alpha+1)\alpha^{k-3} = \alpha^{k-2} + \alpha^{k-3}$.
    - So, $f_{k+1} = f_k + f_{k-1} > \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-1}$. Thus $P(k+1)$.

Lamé's Theorem (拉梅定理)

- **Theorem:**
  - $\forall a,b\in\mathbf{N}$, $a\geq b>0$, the number of steps in Euclid's algorithm to find gcd(a,b) is $\leq 5k$, where $k = \lfloor \log_{10} b \rfloor + 1$ is the number of decimal digits in b.
  - Thus, Euclid's algorithm is linear-time in the number of digits in b.
- **Proof:**
  - Uses the Fibonacci sequence!

Gabriel Lamé (1795-1870)
French

Lamé's Theorem (拉梅定理)

- **Proof (Cont):**
  - Consider the sequence of division-algorithm equations used in Euclid's alg.:

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 && \text{with } 0 \le r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3 && \text{with } 0 \le r_3 < r_2 \\
&\dots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && \text{with } 0 \le r_n < r_{n-1} \\
r_{n-1} &= r_n q_n + r_{n+1} && \text{with } r_{n+1} = 0 \text{ (terminate)}
\end{aligned}
$$

Where
$a = r_0$,
$b = r_1$, and
$\gcd(a,b)=r_n$.

  - The number of divisions (iterations) is $\boldsymbol{n}$.

下一步证明$n \le 5k$，其中$k = \lfloor \log_{10} b \rfloor + 1$

Lamé's Theorem (拉梅定理)

- **Proof (Cont):**
  - Since $r_0 \geq r_1 > r_2 > \ldots > r_n$, each quotient $q_i \equiv \lfloor r_{i-1}/r_i \rfloor \geq 1$.
  - Since $r_{n-1} = r_n q_n$ and $r_{n-1} > r_n$, $q_n \geq 2$.
  - So we have the following relations between r_n and f_n:

$$
\begin{aligned}
&r_n \geq 1 = f_2 \\
&r_{n-1} \geq 2r_n \geq f_2 + f_2 = 2 = f_3 \\
&r_{n-2} \geq r_{n-1} + r_n \geq f_2 + f_3 = f_4 \\
&\ldots \\
&r_2 \geq r_3 + r_4 \geq f_{n-2} + f_{n-1} = f_n \\
&b = r_1 \geq r_2 + r_3 \geq f_{n-1} + f_n = f_{n+1}.
\end{aligned}
$$

$\mathbf{k = \lfloor \log_{10} b \rfloor + 1}$

  - Thus, if $n>2$ divisions are used, then $b \geq f_{n+1} > \alpha^{n-1}$. **(why?)**
  - Thus, $\log_{10} b > \log_{10}(\alpha^{n-1}) = (n-1)\log_{10}\alpha \approx (n-1)0.208 > (n-1)/5$.
  - If b has k decimal digits, then $\log_{10} b < k$, $(n-1)/5 < k$, so $\boldsymbol{n \leq 5k}$.

$\boldsymbol{\Theta(\log(\min(a,b)))}$

Recursively Defined Sets

- **Definition:**
  - An ***infinite set S*** may be defined recursively, by giving:
    - A small finite set of *base* elements of *S*.
    - A rule for constructing new elements of *S* from previously-established elements.
    - Implicitly, *S* has no other elements but these.

- **Example 5:**
  - Let $3 \in S$, if $x,y \in S$, then $x+y \in S$. What is S?

Recursively Defined Sets

- **Definition: (the set of all strings)**
  - Given an alphabet Σ, the set Σ^* of all strings over Σ can be recursively defined by:

$$\varepsilon \in \Sigma^* \text{ } (\varepsilon :\equiv \text{“”, the empty string})$$

$$w \in \Sigma^* \wedge x \in \Sigma \rightarrow wx \in \Sigma^*$$

- **Exercise:**
  - Prove that this definition is equivalent to our old one:

$$\Sigma^* :\equiv \bigcup_{n \in \mathbf{N}} \Sigma^n$$

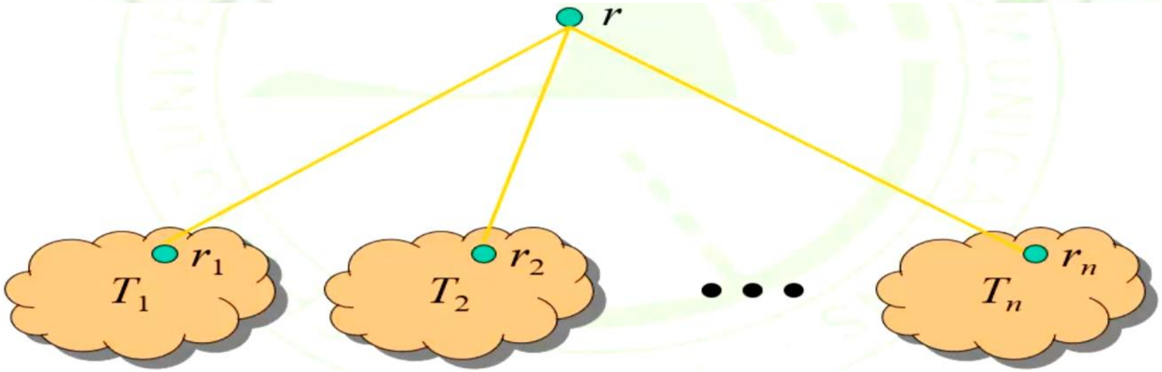
Other String Examples

- Give ***recursive definitions*** for:
  - The concatenation of strings $w_1 \cdot w_2$. (see Definition 2)
  - The length $\ell(w)$ of a string w. (see Example 7)
  - Well-formed formulae of propositional logic involving **T**, **F**, propositional variables, and operators in $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$. (see Example 8)
  - Well-formed arithmetic formulae involving variables, numerals, and ops in $\{+, -, *, \uparrow\}$. (see Example 9)

Recursively Defined Rooted Trees

- **Trees** will be covered in more depth in chapter 11.
  - Briefly, a tree is a graph in which there is exactly one undirected path between each pair of nodes.

- **Definition** of the set of rooted trees:
  - Any single node r is a rooted tree.
  - If $T_1, \ldots, T_n$ are disjoint rooted trees with respective roots $r_1, \ldots, r_n$, and r is a node not in any of the T_i's, then another rooted tree is $\{\{r,r_1\},\ldots,\{r,r_n\}\}\cup T_1\cup\ldots\cup T_n$.



Extended Binary Trees

- A special case of **rooted trees**.
- Recursive definition of EBTs:
  - ***Basis Step***: The empty set $\varnothing$ is an extended binary tree.
  - ***Recursive Step***: If T_1, T_2 are disjoint EBTs, there is an extended binary tree, denoted by $T_1 \cdot T_2$, consisting of a root r together with edges connecting the root to each of the roots of the left subtree T_1 and the right subtree T_2 when these trees are nonempty.

Extended Binary Trees

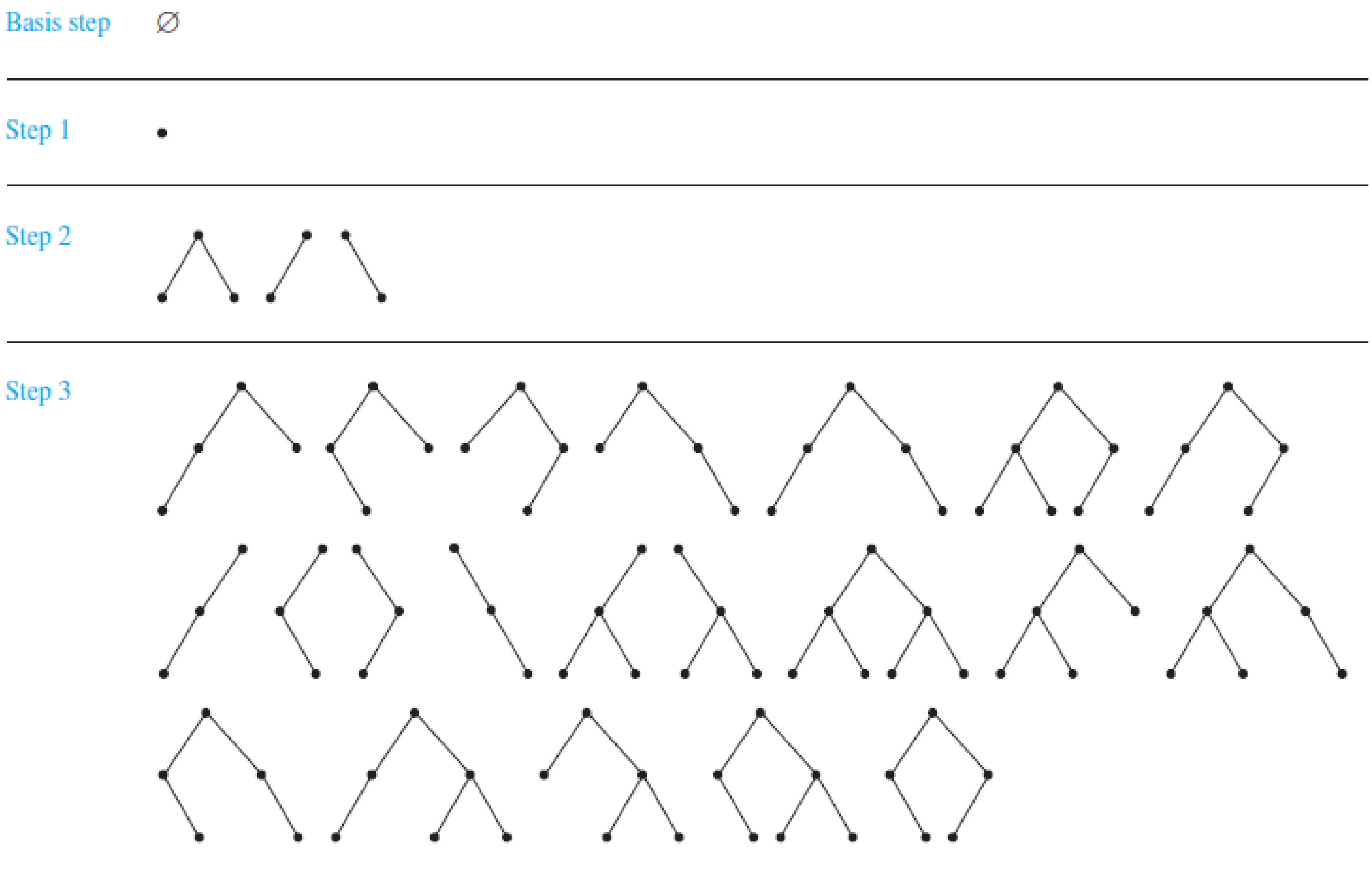


FIGURE 3 Building Up Extended Binary Trees.

Full Binary Trees

- A special case of extended binary trees.
- **Recursive definition** of FBTs:
  - ***Basis Step***: A single node r is a full binary tree.
    - Note this is different from the EBT base case.
  - ***Recursive Step***: If T_1, T_2 are disjoint FBTs, there is a full binary tree, denoted by $T_1 \cdot T_2$, consisting of a root r together with edges connecting the root to each of the roots of the left subtree T_1 and the right subtree T_2.
    - Note this is the same as the EBT recursive case!

Full Binary Trees

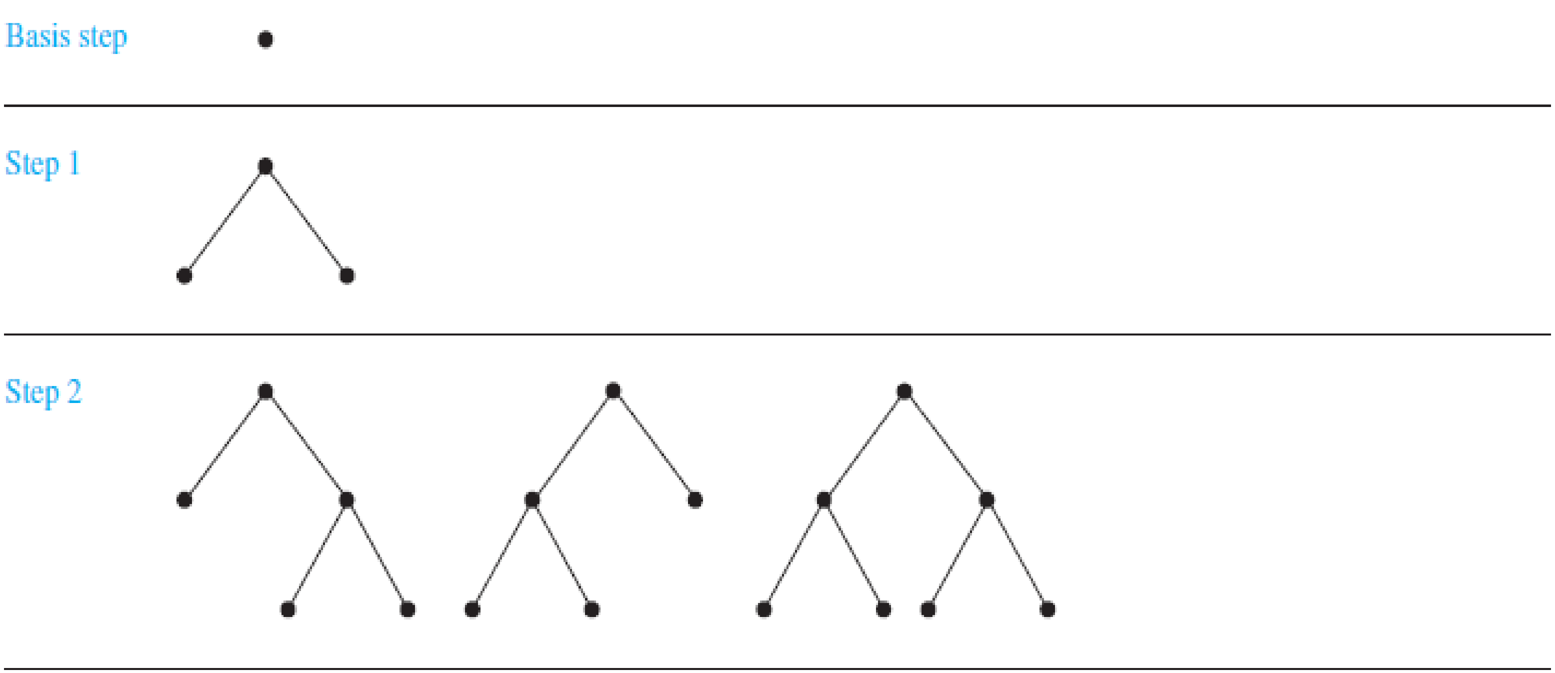


FIGURE 4 Building Up Full Binary Trees.

Structural Induction

- **Definition:**
  - Proving something about a recursively defined object using an inductive proof whose structure mirrors the object's definition. (利用对象的递归定义来归纳地证明该对象的属性)
- **Example problem:**
  - Let $3\in S$, and if $x, y\in S$ then $x+y\in S$.
  - Show S is the set of positive multiples of 3.
  - Let $A = \{n\in \mathbf{Z}^+ | (3|n)\}$.
- **Theorem:** A=S.

Structural Induction

- **Proof:** Let $3 \in S$, if $x,y \in S$ then $x+y \in S$ $A = \{n \in \mathbf{Z}^+ \mid (3|n)\}$.
  - We show that $A \subseteq S$ and $S \subseteq A$.
  - To show $A \subseteq S$, show $(n \in \mathbf{Z}^+ \wedge (3|n)) \rightarrow n \in S$.
    - **Inductive proof.** Let $P(m) :\equiv 3m \in S$.
    - **Basis step:** $m=1$, thus $3*1 \in S$ by def'n. of S.
    - **Inductive step:** Assume $P(k)$ holds ($3k \in S$), prove $P(k+1)$.

    By inductive hyp., $3k \in S$, $3 \in S$, so by def'n of S, $3k+3=3(k+1) \in S$.
  - To show $S \subseteq A$: let $n \in S$, show $n \in A$.
    - **Structural inductive proof.** Let $P(n) :\equiv n \in A$.
    - **Basis step:** *by recursive definition of S*, $n=3$, which is in A.
    - **Recursive step:** *by the second part of recursive definition of S*, $x, y<n$, $x, y \in S$, *then* $n=x+y \in S$. By strong inductive hypothesis, assume the element of S x and y are also in A $(3 \leq x, y<n)$, it follows that $3|x$ and $3|y$. We have $3|(x+y)$, thus $x+y \in A$.

- **Example 13**
  - Suppose that $a_{m,n}$ is defined recursively for $(m,n) \in N*N$ 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 $a_{m,n}=m+n(n+1)/2$ for all $(m,n) \in N*N$, that is for all pairs of nonnegative integers.
- **Solution:**
  - We can prove that $a_{m,n} = m + n(n+1)/2$ using a generalized version of mathematical induction. If the formula holds for all pairs smaller than (m, n) in the lexicographic ordering of N×N, then it also holds for (m, n).

Generalized Induction

- **Proof:**
  - **Basis step:** Let $(m, n) = (0, 0)$. Then by the basis case of the recursive definition of $a_{m,n}$ we have $a_{0,0} = 0$. Furthermore, when $m=n=0$, $m+n(n+1)/2 = 0+(0\cdot 1)/2=0$.
  - **Induction step:** Suppose that $a_{m',n'} = m'+n'(n'+1)/2$ whenever (m', n') is less than (m, n) in the lexicographic ordering of $\mathbf{N}\times\mathbf{N}$.
  - By the recursive definition, if **n=0**, then $a_{m,n} = a_{m-1,n}+1$. Because $(m-1, n)$ is smaller than (m, n), the inductive hypothesis tells us that $a_{m-1,n} =m-1+n(n+1)/2$, so that $a_{m,n}=m-1+ n(n + 1)/2+1 = m+n(n+1)/2$, giving us the desired equality.
  - Now suppose that **n>0**, so $a_{m,n}=a_{m,n-1}+n$. Because $(m, n-1)$ is smaller than (m, n), the inductive hypothesis tells us that $a_{m,n-1} =m+(n-1)n/2$, so $a_{m,n} =m+(n-1)n/2+n = m+n(n+1)/2$.
  - This finishes the inductive step.

Homework

- § 5.3
  - 20，48