proof techniques

- direct proof
- vacuous proof
- trivial proof
- proof by contraposition
- proof by contradiction
- exhaustive proof
- proof by cases → proof broken into seperate cases where these cases cover all possibilities.
- constructive existence proof (CRT) → a proof that an element with a specified property exists - finds explicitly such an element.
- non-constructive existence proof → does not explicitly find such an element
- uniqueness proof (FTA) / (Division algm) → a proof that there is exactly one element satisfying a specific property.
- mathematical induction
- Structural induction (used to prove results about recursively defined sets)
- Cantor - diagonalization method. (used to prove results about the size of infinite sets)
- Combinatorial proofs. (used to prove results by counting algms).

establishes a result by checking a list of all cases.

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}$$

$p = p_1 p_2 \cdots p_n$,

$\rightarrow N = n_1 n_2 \cdots n_k$, $N_i = \frac{N}{n_i}$, $M_i = N_i^{-1} \bmod n_i$

Soln: $x \equiv \sum_{i=1}^{k} a_i M_i N_i \bmod N$

$M_i = N_i^{-1} \bmod n_i$

$x = a_1 M_1 N_1 + a_2 M_2 N_2 + \cdots + a_k M_k N_k \bmod n_i$

$= a_i M_i N_i \bmod n_i$

$= a_i \bmod n_i$

Example: (The 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 non-negative integer, then S has 2^n subsets.

Soln.

~~Basis~~ Let $P(n)$ be the proposition that a set with n elements has 2^n subsets.

Basis step: $P(0)$ is true, because a set with 0 elements, the empty set, has exactly $2^0 = 1$ subset, namely, itself.

Inductive step:

Let $P(k)$ be true.

i.e. every set with k elements has 2^k subsets.

Claim: $P(k+1)$ is true

i.e. every set with $k+1$ elements has 2^{k+1} subsets.

proof of the claim

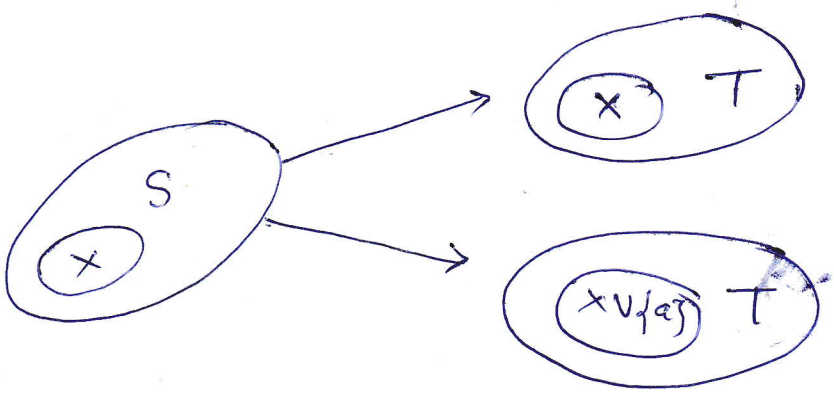
Let T be any set with $k+1$ elements. Then $T = S \cup \{a\}$, where a is one of the elements of T & $S = T - \{a\}$.

Hence $|S| = k$.

- $\phi \rightarrow$ empty set
- ϕ, $\{\phi\}$ not same
- $|\phi| = 0$
- Power set of ϕ $= P(\phi) = \{\phi\}$.
- Power set of $P(\phi)$ $= P(P(\phi)) = \{\phi, \{\phi\}\}$ as $P(\phi) = \{\phi\}$ has exactly two subsets, ϕ & the set $\{\phi\}$.

- Any non-empty set S has at least two subsets, namely, $\phi \subseteq S$ & $S \subseteq S$.
- empty set has exactly one subset, namely, ϕ.

The subsets of T can be obtained from S as follows:



for each subset x of S, there are exactly two subsets of T, namely x & $x \cup \{a\}$.

By induction hypothesis, S has exactly 2^k subsets as S has k elements.

Hence there are $2 \cdot 2^k = 2^{k+1}$ subsets of T.

i.e. P(k+1) is true.

Since P(0) is true

and P(k) true $\Rightarrow$ P(k+1) is true.

By mathematical induction, P(n) is true for all non-negative integers n.

Hence a set with n elements has 2^n subsets whenever n is a non-negative integer.

Example: (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.

(This result is false when there are even number of people).

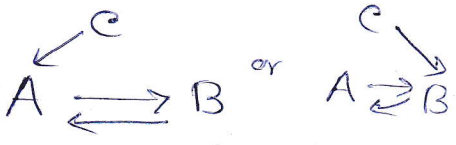
Soln:

Let $P(n)$ be the statement that

there is a survivor wherever $2n+1$ people stand in a yard at distinct mutual distances and each person throws a pie at ~~either~~ their nearest neighbor.

- To prove that $P(n)$ is true for all +ve integers n
  As n runs through all +ve integers, $2n+1$ runs through all odd integers greater than or equal to 3.
- Note that one person cannot engage in a pie fight because there is no one else to throw the pie at.

Base Step: When $n = 1$, there are 3 people in the pie fight A, B, C and let A, B are closest pair.



C is not hit by a pie.

Inductive Step

For the inductive step, assume that P(k) is true. i.e. there is at least one survivor whenever $2n+1$ people stand in a yard at distinct distances & each throws a pie at their nearest neighbor.

To prove that P(k+1) is true.
i.e. there is at least one survivor whenever $2(k+1)+1 = 2k+3$ people stand in a yard at distinct distances & each throws a pie at their nearest neighbor, is also true.

Suppose we have $2k+3$ people in a yard at distinct distances between each pair of people.

Let A, B closest pair of people in the gr. of $2k+3$ people.

Case 1 Someone else throws a pie at either A or B.

A ⇄ B or A ⇄

$2k+3-3 = 2k$ pies remain which should be thrown at the remaining $2k+1$ people (excludes A, B)

at least one survivor

O.W. $2k+1$ pies needed.

Case 2 No one else throws a pie at either A or B.

Besides A & B, there are $2k+1$ people.

We can use induction hypothesis on these $2k+1$ people as the distance between pairs of these people are all different.

So we can conclude that there is at least one survivor S when these $2k+1$ people each throw pies at their nearest neighbor.

Also, S is not hit by either the pie thrown by A or the pie thrown by B because A and B throw their pies at each other.

So S is the survivor because S is not hit by any of the pies thrown by these $2k+3$ people.

This completes the inductive step & proves that $P(n)$ is true for all +ve integers n.

- Division algm
- Fundamental Theorem of Arithmetic (FTA)
- Postage-stamp problem.
- Catalan no., counting binary trees, # of ordering in matrix multiplication. (Generation fn.) fibonacci nos.

X Example: - Suppose we have a group of proposed talks with preset time.

- We would like to schedule as many of these lectures as possib in the main lecture hall.
- How can we schedule the lectures.

talks : $t_1, t_2, \ldots, t_m$

begins : $b_1, b_2, \ldots, b_m$

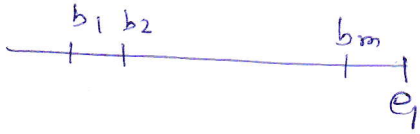
ends : $e_1, e_2, \ldots, e_m$.

- No two lectures can proceed at the same time, but a lectu can begin at the same time another one ends.
- $e_1 \leq e_2 \leq \ldots \leq e_m$.
- We use greedy algorithm.
  - Select at each stage a talk with earliest ending time among all those talks that begin after all talks already scheduled end
  - a lecture with an earliest end time is always selected first by the algm.
- We will show that this greedy algm. is optimal in the sense that it always schedules the most talk possible in the main lecture hall.
- We use mathematical induction on the variable n, the no. of talks scheduled by the algm.

Let P(n) be the proposition that if the greedy algm. schedules n talks, then it is not possible to schedule more than n talks.

Basis step: Suppose the greedy algm. managed to schedule just one ~~talk~~ talk t_1, in the main lecture hall.

This means every other talk cannot start after e_1



Hence, at time e_1 each of the remaining talks needs to use the lecture hall because they start at or before e_1 and end after e_1.

So no two talks can be scheduled because both need to use the hall at time e_1.

$\Rightarrow$ P(1) is true & this completes the basis step.

Inductive step: Let P(k) be true, when k is a +ve integer.

i.e. the greedy algm. always schedules the most possible talks when it selects k talks, when k is a +ve integer, given any set of talks, no matter how large.

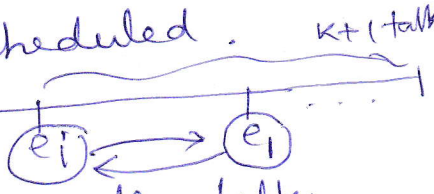
We must show that P(k+1) follows from the assumption that P(k) is true.

i.e. to show that under the assumption of P(k), the greedy algm. always schedules the most possible talks when it selects k+1 talks.

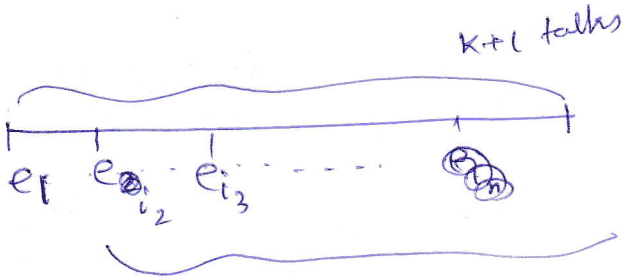
• Suppose the algm. selects $k+1$ talks.

Claim There is a schedule including the most possible talks that contains talk t_1, a talk with the earliest end time.

proof of the claim if there is a schedule that begins with talk t_i, $i > 1$, then we can change talk t_i to talk t_1 as $e_1 \leq e_i$ and all talks that were scheduled to follow talk t_i can still be scheduled.



• Once talk t_1 is scheduled, scheduling the talks so that as many as possible are scheduled is reduced to scheduling as many as possible that begin at or after e_1.



⇒ the greedy algm. has scheduled the most possible talks, $k+1$, when it produces a schedule with $k+1$ talks.

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

by induction hypothesis, of the optimal schedule of the original talks that begin once talk t_1 has ended by greedy algm.

This completes the inductive step.

Principle of mathematical induction (incomplete induction).

To prove that $P(n)$ is true for all positive integer n, where $P(n)$ is a propositional fun., we complete two steps:

Basis Step: We verify that $P(1)$ is true.

Inductive Step: We show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integer k.

- To complete the inductive step of a proof using the principle of mathematical induction, we assume that $P(k)$ is true for an arbitrary +ve integer k & show that under this assumption, $P(k+1)$ must also be true.
- The assumption that $P(k)$ is true is called the inductive hypothesis.

Strong induction (Second principle of mathematical induction / complete induction).

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 integer k.

Note: Some results can be readily proved using either the principle of mathematical induction or Strong induction.

Note: Some results are difficult to prove using the principle of mathematical induction, instead of Strong induction.

(Strong induction)

Example: Consider a game in which two players take turns removing any positive no. of matches they want from one of the two piles of matches. The player who removes the last match wins the game. Show that if the two piles contain the same no. of matches initially, the 2nd player can always guarantee a win.

Soln.

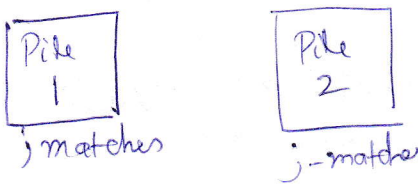
Let $P(n)$ be the proposition that the 2nd player can win when there are initially n matches in each pile.

Base step: $n = 1$

1st player has only one choice, removing one match from one of the piles, leaving a single pile with a single match, which the 2nd player can remove & win the game.

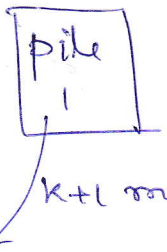
$\therefore P(1)$ is true.

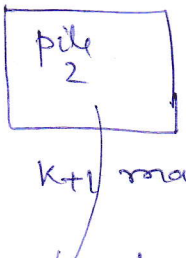
Inductive Step: The inductive hypothesis is the statement that $P(j)$ is true for all j with $j = 1, 2, \cdots, k$.



i.e. Second player can always win whenever there are j matches in each of the two piles at the start of the game, $1 \leq j \leq k$

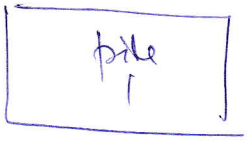
To prove $P(k+1)$ is true.

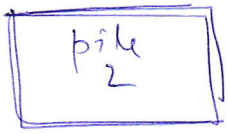




- k+1 matches in each pile initially.

Case 1 :- Let player 1 removes r matches from one of the piles, $1 \le r \le k$, leaving $k+1-r$ matches in that pile.





- Then 2nd player creates a situation where each pile has $k-r+1$ matches.

As $1 \le k-r+1 \le k$, by induction hypotheses, the 2nd player can always win.

Case 2 :- Let player 1 removes $k+1$ matches from one of the pile.
Then the 2nd player can win by removing all the remaining matches.

Note- Using the principle of mathematical induction, instead of strong induction, it is difficult to prove the above result.

Note: Sometimes we need to show that $P(n)$ is true for $n = b, b+1, b+2, \ldots$, where b is an integer other than 1.
We can use mathematical induction to accomplish this as long as we change the basis step.

(FTA, uniqueness not shown)

Example: Show that if n is an integer greater than 1, then n can be written as the product of primes.

Soln: Let $P(n)$ be the proposition that n can be written as the product of primes.

Base step: $P(2)$ is true, because 2 can be written as product of one prime, itself ($P(2)$ is the first case we need to establish)

Inductive Step: The inductive hypothesis is the assumption that $P(j)$ is true for all +ve integers j with $j \leq k$.

i.e. j can be written as the product of two primes where j is a +ve integer at least 2 and not exceeding k.

To complete the inductive step, it must be shown that $P(k+1)$ is true under this assumption.

i.e. $k+1$ is a product of primes.

Case 1 $k+1$ is prime.

Then $P(k+1)$ immediately follows.

Case 2 $k+1$ is composite.

Then $k+1 = ab$, a, b are two +ve integers $2 \leq a \leq b < k+1$.

By the inductive hypothesis, both a & b can be written as product of primes.

Thus, $k+1$ can be written as product of primes, namely, those primes in the factorization of a and those in the factorization of b.

[FTA: Every non-negative integer can be written uniquely as the product of primes in nondecreasing order]

Note: Strong induction is required to prove the above result, instead of the principle of mathematical induction.

Note: The proof can be started with $P(1)$ as the base step as 1 can be thought of as the empty product of no primes.

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

Soln:
(Using mathematic induction)

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

Base step $n = 12$ $P(12)$ is true as Postage of 12 cents can be formed using three 4-cent stamps

Linear Diaphantite Equation.

$4x + 5y = n$ (a, b)

has Soln. in x, y if $n \geq ab - a - b + 1$

- n is feasible if $n \geq ab-a-b+1$ $\forall n \geq 12$.

$ab - a - b = 4 \times 5 - 4 - 5$
$= 20 - 9$
$= 11$

- $n = ab - a - b$ is not feasible.

- Bezout's identity
$au + bv = d = \gcd(a, b)$

Inductive step: Let $P(k)$ be true, $k \geq 12$

i.e. k cents can be formed using 4-cent & 5 cent stamps.

Now consider postage of $k+1$ cents.

Case 1 at least one 4-cent stamp used to form postage of k cents.

Then replacing one such 4-cent stamp by a 5-cent stamp, we get a postage of $k+1$ cents.

Case 2 No 4-cent stamps were used to form postage of k cents. i.e. we have used only 5-cent stamps to form a postage of k cents.

As $k \geq 12$, we must have at least three 5-cent stamps to form a postage of k cents.

Replace any three 5-cent stamps by four 4-cent stamps, we can get a postage of $k+1$ cents

This completes the inductive step.

Because, we have completed both the basis step and the inductive step, we know that $P(n)$ is true for all $n \geq 12$.

i.e. we can form postage of n-cents, when $n \geq 12$, using just 4-cent & 5-cent stamps.

(Using strong induction)

Basis Step : ~~P(12) 3 4's 4 cent~~

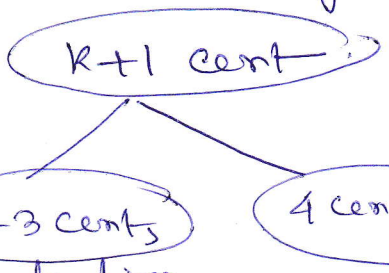
$12 = 4 \times 4$ cent — P(12) true

$13 = 2 \times 4$ cent $+ 1 \times 5$ cent — P(13) true

$14 = 2 \times 5$ cent $+ 1 \times 4$ cent — P(14) true

$15 = 3 \times 5$ cent — P(15) true.

Inductive step : Let P(j) be true for $12 \leq j \leq k$, where k is an integer ≥ 15.



by induction hypothesis

one 4-cent stamp needed additionally.

Postage of k-3 cents can be formed using 4-cent & 3-cent stamps as $k-3 \geq 12$.

Thus if the induction hypothesis is true, then P(k+1) is also true.

This completes the inductive steps.

Because we have completed the basis step and the inductive step of a strong induction proof, we conclude by strong induction that P(n) is true for all integers n with $n \geq 12$.

i.e. every postage of n cents, $n \geq 12$, can be formed using 4-cent & 5-cent stamps.

Example (well-ordering property)

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 ten players $p_1, p_2, \ldots, p_m$ form a cycle if p_1 beats p_2, p_2 beats p_3, $\ldots$, p_{m-1} beats p_m and p_m beats p_1.

Use well-ordering principle to show that if there is a cycle of length m $(m \geq 3)$ among ten players in a round-robin tournament, there must be a cycle of three of these players.

Soln (proof by contradiction)

We assume that there is no cycle of three players.

Let $S = \{n \in \mathbb{N} \mid$ there is a cycle of length $n\}$

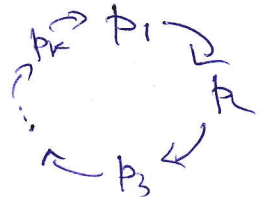
Then $S \neq \emptyset$ as $m \in S$.

Thus S is a non-empty set of +ve integers.

By the well-ordering principle, S must have a least element, say k, which is by assumption > 3.

Let the cycle by $p_1, p_2, \ldots, p_k, p_1$

$k > 3$, no shorter cycle exists.



Consider the 1st. three players p_1, p_2, p_3.

Two possible outcomes of the match between p_1 & p_3

- if p_3 beats p_1, then p_1, p_2, p_3 forms a cycle of length 3, contradicting our assumption that there is no cycle of 3 players.

- if p_1 beats p_3, then we can omit p_2 ~~and~~ from the cycle $p_1, p_2, p_3, \ldots, p_k$ and obtain a cycle $p_1, p_3, \ldots, p_k$ of length $k-1$, contradicting the assumption that the smallest cycle has length k.

Therefore, there must be a cycle of length three.

Example: (Division algm.)

Use the well-ordering property to prove the division algm: if a is an integer and d is a positive integer, then there are unique integers q and r with $0 \le r < d$ and $a = dq + r$.

Soln.

Let $S = \{$ ~~$a - dq > 0$~~ the set of all non-negative integers of the form $a - dq$, where q is an integer $\}$.

Claim: $S \neq \emptyset$

Take $a - (|q|d)$.

$|q| = \begin{cases} q & \text{if } q > 0 \\ -q & \text{if } q < 0 \end{cases}$

~~$a - (|q|d) \in$~~

Then $a - (-|q|d) = \begin{cases} a - (-q)d \\ a - qd \end{cases}$

Recursive Definitions & Structural Induction

or inductive definition.

Functions

Example 1 (factorial) $F(n) = n!$

$$\begin{cases} F(0) = 1 \\ F(n+1) = (n+1)F(n) \end{cases}$$

Example 2 (Fibonacci nos.)

$$\begin{cases} f_0 = 0, f_1 = 1 & \text{(Basis step)} \\ f_n = f_{n-1} + f_{n-2} & \text{(Recursive step)} \end{cases}$$

Sets

Σ^* → the set of strings over the alphabet Σ

Example 3 recursively defined as

$$\begin{cases} \cdot\ \varepsilon \in \Sigma^* & (\varepsilon \text{ is the empty string containing no symbol}) \\ \cdot\ \text{if } \omega \in \Sigma^* \text{ and } \alpha \in \Sigma, \text{ then } \omega\alpha \in \Sigma^* \end{cases}$$

Example 4 Well-formed formulae for Compound Statement Forms

The set of well formed formulae for compound statement forms involving T, F, propositional variables, and operators from the set $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ is recursively defined as;

- T, F, s are well-formed formulae when s is a propositional variable
- if E & F are well-formed formulae, then $\neg E$, $E \wedge F$, $E \vee F$, $E \rightarrow F$, $E \leftrightarrow F$ are well-formed formulae.

e.g. $p \vee \wedge$, $\neg \wedge pq$ are not well-formed formulae.

Example: (Boolean expressions in variables $x_1, x_2, \ldots, x_n$)

- $0, 1, x_1, x_2, \ldots, x_n$ are Boolean expressions
- if E_1 and E_2 are Boolean expressions, then $\overline{E_1}$, E_1E_2, E_1+E_2 are Boolean expressions.

Example:
(well formed formulae of operators and operands)

The set of well-formed formulae consisting of variables, numerals, and operators from the set

$\{+, -, *, /, \uparrow\}$ ($*$ denotes multiplication, $\uparrow$ denotes exponentiation)

is recursively defined as:

- x is a well-formed formula if x is a numeral or variable
- if F and G are well-formed formulae, then $F+G$, $F-G$, $F*G$, F/G and $F\uparrow G$ are well formed formulae.

e.g. x^3+, $y*+x$, $*x/y$ not well-formed formulae

Structures

Example: (full Binary trees)

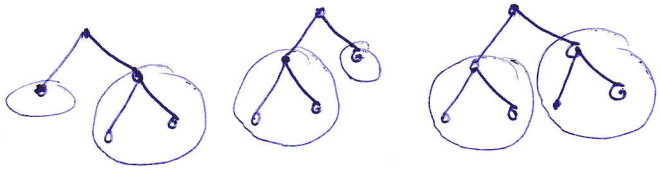
- (Basis step) There is a full binary tree consisting of a single vertex r.
- (Recursive step) If T_1 and T_2 are disjoint full binary trees, there is a full binary tree, denoted by $T_1 \cdot T_2$ consisting of a root r together with edges connecting the root to each of the root of the left subtree T_1 and the right subtree T_2.

Building full Binary trees.

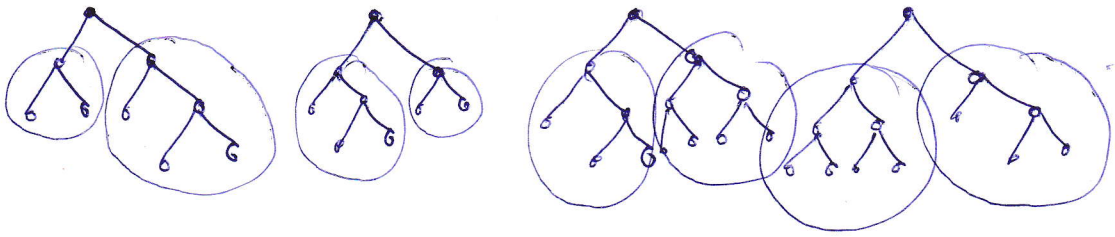
Basis Step

Step 1

Step 3



Step 4.



Example: (Height of a full binary tree)

- The height of the full binary tree T consisting of only a root is $h(T) = 0$
- If T_1 and T_2 are full binary trees, then the full binary tree $T = T_1 \cdot T_2$ has height $h(T) = 1 + \max(h(T_1), h(T_2))$

Theorem.

~~Example~~: (Structural induction)

Use Structural induction to prove the following.

If T is a full binary tree T, then the no. of vertices $n(T) \leq 2^{h(T)+1} - 1$.

proof (proof by Structural induction)

- $n(T) = 1$ when T is a single vertex
- $n(T) = 1 + n(T_1) + n(T_2)$ when $T = T_1 \cdot T_2$.

Structural induction

- **Basis Step:** Show that the ~~statement~~ result holds for all elements specified in the basis step of the recursive def^n. to be in the set.
- **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 def^n., then the result holds for these new elements.

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

proof.

Basis Step

for full binary tree consisting of just the root r, the result is true because $n(T)=1$ and $h(T)=0$ so $n(T)=1 \leq 2^{0+1}-1=1$.

Inductive Step

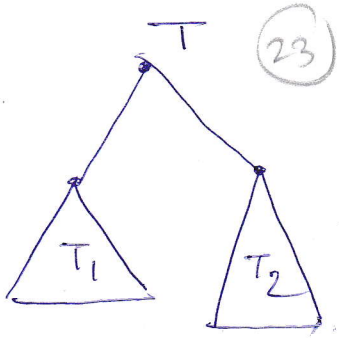
for inductive hypothesis, we assume that

$$n(T_1) \leq 2^{h(T_1)+1} - 1 \quad \text{and} \quad n(T_2) \leq 2^{h(T_2)+1} - 1$$

Whenever T_1 and T_2 are two full binary trees.

By the recursive formulae for $n(T)$ and $h(T)$, we have $n(T) = 1 + n(T_1) + n(T_2)$

and $h(T) = 1 + \max\left(h(T_1), h(T_2)\right)$



We find that—

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

$$\leq 1 + 2^{h(T_1)+1} - 1 + 2^{h(T_2)+1} - 1$$

$$\leq 2 \max\left(2^{h(T_1)+1}, 2^{h(T_2)+1}\right) - 1$$

$$= 2 \cdot 2^{\max\left(h(T_1)+1,\, h(T_2)+1\right)} - 1$$

$$= 2 \cdot 2^{\max\left(h(T_1), h(T_2)\right)+1} - 1$$

$$= 2 \cdot 2^{h(T)} - 1$$

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

$a + b \leq 2\max(a, b)$

$\max(2^a, 2^b) = 2^{\max(a,b)}$

$\max$

$15 \mid x$
$x = 15k$
$= 3 \times 5k$
$3 \mid x, 5 \mid x$

This completes the inductive step.

Generalized induction

Extending mathematical induction about other sets besides the set of integers having the well-ordering property.

e.g. $N \times N$

- **lexicographic ordering**

(x_1, y_1) less of equal to (x_2, y_2)

if either $x_1 < x_2$ or $x_1 = x_2$ and $y_1 < y_2$.

- This ordering has the property that every subset of $N \times N$ has a least element.

Example: (A variant of mathematical induction) Use of

Suppose that $a_{m,n}$ is defined recursively for $(m,n) \in N \times N$ by $a_{0,0} = 0$

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

Show that $a_{m,n} = m + \frac{n(n+1)}{2}$ $\forall (m,n) \in N \times N$.

Proof.

Basis step: $(m,n) = (0,0)$

$$a_{0,0} = 0$$

$$m + \frac{n(n+1)}{2} = 0 + \frac{0 \cdot 1}{2} = 0 = a_{0,0}$$

This completes the basis step.

Inductive step:

let $a_{m',n'} = m' + \frac{n'(n'+1)}{2}$

whenever (m',n') is less than (m,n) in lexicographic ordering of $N \times N$.

- $n = 0$. Then $a_{m,n} = a_{m-1,n} + 1$

as $(m-1, n)$ is less than (m,n), by induction hypothesis, $a_{m-1,n} = (m-1) + \frac{n(n+1)}{2}$.

yielding $a_{m,n} = (m-1) + \frac{n(n+1)}{2} + 1$

$= m + \frac{n(n+1)}{2}$, giving the desired result.

- $n > 0$. Then $a_{m,n} = a_{m,n-1} + n$

as $(m, n-1)$ is less than (m,n), by induction hypothesis, $a_{m,n-1} = m + \frac{(n-1)(n)}{2}$,

yielding $a_{m,n} = m + \frac{(n-1)n}{2} + n = m + \frac{n(n+1)}{2}$, giving the desired result.

Example: Show that whenever $n \geq 3$, $f_n > \alpha^{n-2}$, where $\alpha = \frac{1+\sqrt{5}}{2}$ (golden ratio) [α is a soln of $x^2 = x+1$]

Soln: We can use strong induction to prove the inequality.

Let $P(n)$ be the statement $f_n > \alpha^{n-2}$.

Claim: $P(n)$ is true whenever n is an integer ≥ 3.

Basis Step First, note that—

- $\alpha < 2 = f_3$ i.e. $f_3 > \alpha^{3-2} = \alpha$
- $\alpha^2 = \frac{3+\sqrt{5}}{2} < \frac{3+\sqrt{9}}{2} = 3 = f_4$

  i.e. $f_4 > \alpha^{4-2} = \alpha^2$

$\alpha^2 = \frac{1+5+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2}$

$\alpha = \frac{1+\sqrt{5}}{2} < \frac{1+\sqrt{9}}{2} = 2$

$f_0 = 0, f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, \ldots$

So $P(3)$ & $P(4)$ are true.

Exercise: $f_n \leq \alpha^{n-1}$.

Inductive Step

Assume that $P(j)$ true for all integers j, $3 \leq j \leq k$ when $k \geq 4$.

i.e. $f_j > \alpha^{j-2}$, $3 \leq j \leq k$, $k \geq 4$.

$P(5), P(6), \ldots$ does not include $P(4)$

Claim $P(k+1)$ is true i.e. to prove $f_{k+1} > \alpha^{k+1-2} = \alpha^{k-1}$

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

By induction hypothesis, if $k \geq 4$, we have

$f_k > \alpha^{k-2}$ & $f_{k-1} > \alpha^{k-3}$.

Therefore, we have $f_{k+1} = f_k + f_{k-1} > \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-1}$

It follows that $P(k+1)$ is true. This completes the proof.

Theorem (Lame's Theorem)
Let a and b be positive integers with $a \geq b$.
Then the number of divisions used by the Euclidean algm. to find $\gcd(a,b)$ is $\leq 5 \times (\log_{10} b + 1)$.

↙ the # of decimal digits in b.

Proof: Applying Euclidean algm. to find $\gcd(a,b)$ with $a \geq b$, we find the following sequence of equations

$\gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) = r_n$.

let $a = r_0$, $b = r_1$

$r_2 \mid r_0 \mid q_1$

$r_0 = r_1 q_1 + r_2, \quad 0 \leq r_2 < r_1$

$r_2 \mid r_1 \mid q_2$

$r_1 = r_2 q_2 + r_3, \quad 0 \leq r_3 < r_2$

$r_3 \mid r_2 \mid \cdots$

$\vdots$

$r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1}$

$r_n \mid r_{n-1} \mid q_n$

$r_{n-1} = r_n q_n$

$\gcd \quad 0$

- n divisions are used to find $r_n = \gcd(a,b)$.
- the quotients $q_1, q_2, \cdots, q_n$ are all at least 1

Also $q_n \geq 2$ o.w. if $q_n = 1$, then $r_{n-1} = r_n$ ($\rightarrow\leftarrow$)

Thus we have, $r_n \geq 1 = f_2$ | $f_0 = 0, f_1 = 1, f_2 = 1$, $f_3 = 2, f_4 = 3, \cdots$

$r_{n-1} = r_n q_n \geq 2 r_n \geq 2 f_2 = f_3$

$r_{n-2} \geq r_{n-1} + r_n \geq f_3 + f_2 = f_4$

$\vdots$

$r_2 \geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n$

$$b = r_1 \geq r_2 + r_3 \geq f_n + f_{n+1} = f_{n+1}.$$

As $f_{n+1} > \alpha^{n-1}$, we get $b > \alpha^{n-1}$.
(by the previous example)

$$\Rightarrow \log_{10} b > (n-1)\log_{10}\alpha$$

$$> \frac{(n-1)}{5}.$$

$\log_{10}\alpha \sim 0.208 > \frac{1}{5} = 0.2$

$$\Rightarrow n-1 < 5\log_{10} b < 5k.$$

$$\text{or } n < 5k+1$$

$$\Rightarrow n \leq 5k = 5(\log_{10} b + 1).$$

b has k digits

$\Rightarrow b < 10^k$.

$\log_{10} b < k$

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

$\leq (\log_{10} b + 1)$

Example: (Fundamental Theorem of arithmetic)
(uniqueness skipped)

Show that if n is an integer > 1, then n can be written as the product of primes.

Soln. Basis Step $P(2)$ is true.
2 can be written as product of 1 prime, itself.

Inductive Step Assume that $P(j)$ true for all j, $1 \leq j \leq k$.

Claim $P(k+1)$ is true i.e. to prove $k+1$ can be written as product of primes.

Case 1 $k+1$ is prime $\rightarrow$ $P(k+1)$ true (immediately follow)

Case 2 $k+1$ is composite i.e. $k+1 = ab$, $2 \le a \le b < k+1$

By induction hypothesis, a, b both can be written as the product of primes.

$\Rightarrow$ $k+1$ can be written as product of primes. Namely those primes in the factorization of a & those primes in the factorization of b.

Uniqueness: $\alpha_i, \beta_i \geq 0$ integers

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_r^{\beta_r}$$

distinct lists.

$p_1 < p_2 < \cdots < p_l$ $\qquad$ $q_1 < q_2 < \cdots < q_r$

$p_i \mid (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}) = q_1^{\beta_1} q_2^{\beta_2} \cdots q_r^{\beta_r}$

$\Rightarrow p_i = q_j$, $\exists\ 1 \le j \le r$.