

One way of formulating last lecture's theorem

$N(t)$  = number of nodes in binary tree  $t$ .

$L(t)$  = number of leaves in binary tree.

### Theorem 1

A binary tree with  $n$  nodes has at most  $\lceil \frac{n}{2} \rceil$  leaves.



For all  $t \in B$  and all  $N \in \mathbb{N}$ , let  $S(t, n)$  = "that  $n$  nodes" and let  $AL(t, n)$  = " $t$  has at most  $n$  leaves". Denote  $P(n) = \forall t \in B. [S(t, n) \text{ IMPLIES } AL(t, \lceil \frac{n}{2} \rceil)]$

Prove  $\forall n \in \mathbb{N}. p(n)$  using strong induction on  $n$ .



Another way of formulating the theorem

Recursive Definition of  $B$

Base Case: the empty tree is in  $B$

Constructor Case: If  $t_1, t_2 \in B$  and  $r$  is a node, then  $t := t_1 - r - t_2 \in B$  where  $\text{left}(t)=t_1$ ,  $\text{right}(t)=t_2$

Let  $g : B \rightarrow \{T, F\}$  be such that  $g(t) = "L(t) \leq \lceil \frac{N(t)}{2} \rceil"$

$N : B \rightarrow \mathbb{N}$

Base Case

$N(\text{empty tree})=0$

Constructor Case

$N(t)=1+N(\text{left}(t))+N(\text{right}(t))$

$L : B \rightarrow \mathbb{N}$

Base Cases

$L(\text{empty tree}) = 0$

$L(\text{one node tree}) = 1$

Constructor Case:

$L(t)=L(\text{left}(t))+L(\text{right}(t))$

To prove  $\forall t \in B. g(t)$ , we use structural induction.

Let  $t \in B$  be arbitrary

Case 1:  $t$  is the empty tree

$N(t) = 0, L(t) = 0$

so  $L(t) = 0 = \lceil \frac{0}{2} \rceil = \lceil \frac{N(t)}{2} \rceil$

Case 2:  $t := t_1 - r - t_2$ :

Assume  $g(t_1)$  and  $g(t_2)$ , by definition  $L(t_1) \leq \lceil \frac{N(t_1)}{2} \rceil$  and  $L(t_2) \leq \lceil \frac{N(t_2)}{2} \rceil$

Then  $L(t) = L(t_1) + L(t_2)$ ,  $N(t) = N(t_1) + N(t_2) + 1$

So  $L(t) \leq \lceil \frac{N(t_1)}{2} \rceil + \lceil \frac{N(t_2)}{2} \rceil \leq \dots \leq \frac{N(t)+1}{2}$

Since  $N(t)$  is an integer, we have  $L(t) \leq \lceil \frac{N(t)+1}{2} \rceil \leq \lceil \frac{N(t)}{2} \rceil$





structural induction  $\forall t \in S.p(t)$ . can be proved using strong induction.

Let  $E_0$  = set of elements of  $S$  due to base case

$E_1$  = set of elements of  $S$  obtained from elements of  $E_0$  by applying constructor case once.

$\vdots$

$E_i$  = set of elements of  $S$  obtained from elements of  $E_{i-1}$  by applying constructor case  $i$  times.

We can see  $S = \bigcup_{i \geq 0} E_i$

Let  $q(i) = \forall t \in E_i.p(t)$ , then we can prove  $\forall i \in \mathbb{N}.q(i)$  using strong induction on  $i$  instead of structural induction. 

## Theorem 2

Every integer greater than  $n = 1$  can be written as a product of primes

*Proof.* Suppose the claim is false. Let  $n$  be the smallest integer greater than 1 that cannot be written as a product of prime.

If  $n$  is prime, then  $n$  is a product of 1 prime, thus  $n$  is composite.

So there exist integers  $m, k > 1$  such that  $n = m \times k$

But  $m$  and  $k$  are both less than  $n$ , so they can both be written as a product of primes.

Hence  $n = m \times k$  can be written as a product of primes.

This contradicts the definition of  $n$ , hence the claim is true.

Q.U.B.D.  
E.H.A.T.  
D.E.M.



## Definition 1

A set  $S$  is partially ordered if there exist  $R : S \times S \rightarrow \{T, F\}$  such that  $\forall x \in S. \forall y \in S. \forall z \in S.$

$R(x, x) = T$	(reflexive)
$R(x, y) \text{ AND } R(y, x) \text{ IMPLIES } x = y$	(antisymmetry)
$R(x, y) \text{ AND } R(y, z) \text{ IMPLIES } R(x, z)$	(transitivity)

In this case  $R$  is called a partial order.

Examples:  $(\mathbb{Z}, \preceq), (\mathbb{R}, \preceq), (P(\{1, 2, 3\}), \subseteq)$

Not example:

$R(x, y) = \mathbb{C}$  with " $|x| \leq |y|$ "; we can see  $|i| \leq |1|$  and  $|1| \leq |i|$  but  $|i| \neq |1|$  thus not antisymmetry.

$H$ =hockey teams,  $R(t, t')$  if  $t$  has beaten by  $t'$ , we can see it is not transitive.



## Definition 2

A set  $S$  is totally ordered if there exists a partial order  $R : S \times S \rightarrow \{T, F\}$  such that  $\forall x, y \in S, R(x, y) \text{ OR } R(y, x)$  (comparability),  $R$  is a total order.

Examples:  $\mathbb{R}, \mathbb{Z}, \leq$  Not example:

$P(\{1, 2, 3\}), \subseteq$ : since  $\{1, 2\} \not\subseteq \{2, 3\}$  and  $\{2, 3\} \not\subseteq \{1, 2\}$ , thus not totally ordered.





**Definition 3**

A totally ordered set  $S$  is well-ordered if every non-empty subset  $S' \subseteq S$  has a smallest element  $m$ . That is,  $R(m, x) = T$  for all  $x \in S'$

$\leq$  is a well ordering for  $\mathbb{N}$

$\leq$  is NOT a well ordering for  $\mathbb{Z}$  (negatives) or  $\mathbb{Q}^+$  (archimedean)

This is an example for  $\mathbb{Z}$ :  $x \preceq y$  IFF  $[(|x| < |y|) \text{ OR } (|x| = |y| \text{ AND } x \leq y)]$

$0 \preceq -1 \preceq 1 \preceq -2 \preceq 2 \dots$  is a well ordering for  $\mathbb{Z}$

This is an example for  $\mathbb{Q}^+$ :

Consider ordering based on  $\max\{\text{numerator}, \text{denominator}\}$  when written in reduced form i.e.  $\gcd(\text{numerator}, \text{denominator}) = 1$  and then by value

$$\frac{1}{1} \preceq \frac{1}{2} \preceq \frac{2}{1} \preceq \frac{2}{3} \preceq \frac{3}{2} \preceq \frac{3}{1}$$

**Definition 4**

If  $\preceq$  is a well ordering, then  $x \prec y$  means “ $x \preceq y$  and  $x \neq y$ ”.



Suppose  $\preceq$  is a well ordering of the set  $S$ . Then to prove  $\forall e \in S. p(e)$ :

To obtain a contradiction, suppose  $\forall e \in S. P(e)$  is false.

Let  $C = \{e \in S \mid P(e) = F\}$  be the set of counterexamples to  $P$ .

$C \neq \emptyset$ ; by definition of the previous 2 lines

Let  $e$  be the smallest element of  $C$ ; (since  $S$  is well ordered and  $C$  is non-empty)

Let  $e' = \dots$ ;

$\dots$

$e' \in C$ ;

$e' \prec e$ ;

This is a contradiction (contradicting  $e$  is the smallest such element in  $C$ )

Thus using contradiction, we show that  $\forall e \in S. p(e)$  is true.





**Theorem 3**

Every positive rational number  $\frac{m}{n}$  can be expressed in reduced form.

*Proof.*

Suppose there exist  $m, n \in \mathbb{Z}^+$  such that  $\frac{m}{n}$  cannot be expressed in reduced form;

Let  $C = \{m \in \mathbb{Z}^+ \mid \exists n \in \mathbb{Z}^+ \text{ such that } \frac{m}{n} \text{ cannot be expressed in reduced form}\}$ ;

Then  $C \neq \emptyset$ .

Since  $\mathbb{Z}^+$  is well ordered, and  $\emptyset \neq C \subseteq \mathbb{Z}^+$ ,  $C$  has a smallest element  $m_0$ .

By definition of  $C$  there exists  $n_0 \in \mathbb{Z}^+$  such that  $\frac{m_0}{n_0}$  cannot be expressed in reduced form.

In particular,  $\gcd(m_0, n_0) > 1$  (otherwise it is in reduced form).

Let  $p$  be a prime factor of  $\gcd(m_0, n_0)$ ;

Let  $m'_0 = \frac{m_0}{p} \in \mathbb{Z}^+$ ;

Let  $n'_0 = \frac{n_0}{p} \in \mathbb{Z}^+$ ;

Since  $\frac{m'_0}{n'_0} = \frac{m_0}{n_0}$ , it cannot be expressed in reduced form.

Hence  $m'_0 \in C$  such that  $m'_0 < m_0$ ;

The above line is a contradiction.

Therefore, every positive rational number  $\frac{m}{n}$  can be expressed in reduced form.

QUOD  
ERAT  
DEMONSTRATUM

**Theorem 4**

For every positive integer  $i$ , let  $E(i) =$  “The subset of  $[i] = \{j \in \mathbb{Z}^+ \mid j \leq i\}$  that contain an even number of elements”.

Let  $U(i) =$  “subsets of  $[i]$  that contain an odd number of elements”

For all  $i \in \mathbb{Z}^+$ .  $|E(i)| = |U(i)| = 2^{i-1}$

*Proof.*

For every  $i \in \mathbb{Z}^+$ , let  $P(i) = “|E(i)| = |U(i)| = 2^{i-1}.”$

Suppose  $\forall i \in \mathbb{Z}^+ . P(i)$  is false;

Let  $C = \{i \in \mathbb{Z}^+ \mid \text{NOT}(P(i))\}$ ;

Then  $C \neq \emptyset$ ;

Since  $C$  is well ordered, it has a smallest element  $x$ ;

$x \neq 1$  since  $\{1\}$  has  $1 = 2^{x-1}$  subset which contains an even number of elements,  $\emptyset$ ; 1 subset which contains an odd number of elements,  $\{1\}$ .

Let  $E'(x) = \{S \in E(x) \mid x \in S\}$ ;

Then  $E(x) = E'(x) \dot{\cup} E(x-1)$ ;

$|E(x)| = |E'(x)| + |E(x-1)|$ ;

There is a 1 to 1 correspondence between  $E'(x)$  and  $U(x-1)$  (we can add  $x$  from one in  $U(x-1)$  or remove  $x$  from one in  $E'(x)$ );

Hence  $|E'(x)| = |U(x-1)|$ ;

Hence  $|E(x)| = |U(x-1)| + |E(x-1)|$

$x-1 \notin C$  so  $= 2^{x-2} + 2^{x-2} = 2^{x-1}$

$|U(x)| = 2^{x-1}$  by symmetry or  $|U(x)| = 2^x - |E(x)| = 2^{x-1}$  (alternating);

Thus  $x \notin C$ , this is a contradiction.

QUOD  
ERAT  
DEMONSTRATUM





**Definition 5 – Countable + Uncountable Sets**

A function  $f : A \rightarrow B$  is surjective or onto means

$$\forall y \in B. \exists x \in A. (f(x) = y),$$

when  $A$  and  $B$  are finite sets, we can conclude  $|B| \leq |A|$ .

A non-empty set  $C$  is countable if there is a surjective function from  $\mathbb{N}$  to  $C$ .

Every non-empty finite set is countable.

*Proof.* Suppose the elements of  $C$  are  $c_0, c_1, \dots, c_{n-1}$   
 define  $f : \mathbb{N} \rightarrow C$  by  $f(i) = c_i$  for  $i \in \{0, 1, \dots, n-1\}$ ,  $f(i) = c_{n-1}$  for  $i \geq n$ .  
 Then  $f$  is surjective, thus  $C$  is countable.

QVOD  
ERAT  
DEMONSTRATUM



The empty set is also considered to be countable.

Any well ordered set is countable.

Suppose  $A$  and  $B$  are countable, then  $A \cup B$  is countable,  $A \times B = \{(a, b) \mid a \in A \text{ AND } b \in B\}$  is also countable.

For  $\mathbb{Z}$ :  $f(0) = 0$ ,  $f(2i-1) = -i$  for  $i > 0$ ,  $f(2i) = i$  for  $i < 0$ , so  $\mathbb{Z}$  is countable.

For  $\mathbb{N} \times \mathbb{N}$ : we use the diagonal argument, from top left to bottom right, we can list all the elements of  $\mathbb{N} \times \mathbb{N}$  (insert the 2D table here, where the row is  $\mathbb{N}$  and with  $i$ ; column is  $\mathbb{N}$  and with  $j$ , then there is a mapping of  $(i, j)$  to  $(i, j) \in \mathbb{N} \times \mathbb{N}$ ).

If  $A$  is countable and  $B \subseteq A$ , then  $B$  is also countable.

**Lemma 1**

If  $A$  is nonempty and countable, then there exists a surjective function  $f : A \rightarrow B$  then  $B$  is countable.

