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 $\left\lceil \frac{n}{2} \right\rceil$ 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 $P(n) = \forall t \in B.[S(t,n)$ IMPLIES $AL(t, \left\lceil \frac{n}{2} \right\rceil)]$"

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 left(t)=t_1, right(t)=t_2

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

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

Base Case

N(empty tree)=0

Constructor Case

N(t)=1+N(left(t))+N(right(t))

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

Base Cases

L(empty tree) $= 0$

L(one node tree) $= 1$

Constructor Case:

L(t)=L(left(t))+L(right(t))

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

Let $t \in B$ be arbitrary

Case 1: t is the empty tree

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

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

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

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

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

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

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

☺

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 elelments of S obtained from elemnets 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 br written as a product of primes.

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

quod erat dem■

Definition 1

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

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

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 $R : S \times S \to \{T, F\}$ such that $\forall x, y \in S$, $R(x, y)$ 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 <u>well-ordered</u> 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 $[(|x|< |y|)$ OR $(|x|= |y|$ AND $x \leq y)]$

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

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

Consider ordering based on max{numerator, denominator} when written in reduced form i.e. gcd(numerator, 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.

$C \neq \varnothing$; 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 $e' = \ldots$;

$\ldots$

$e' \in C$;

$e' \prec e$;

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

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

Then $C \neq \varnothing$.

Since Z^+ is well ordered, and $\varnothing \neq C \subseteq \mathbb{Z}^+$, 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 dem ■

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 $C \neq \varnothing$;

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 elmeents, $\varnothing$; 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 etween $E'(x)$ 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 dem ■

Definition 5 – Countable + Uncountable Sets

A function $f : A \to B$ is suejective 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 conutable.

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

quod erat dem ■

☺

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 $\mathbb{N} \times \mathbb{N}$ (insdert 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 conutable, then there exists a surjective function $f : A \to B$ then B is countable.