Combinatorics Theorems

Jason Sass

May 27, 2023

Combinatorics

Proposition 1. *Let* $n \in \mathbb{Z}^+$.
Then $n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot (n-1) \cdot n$.

Proof. Let $S = \{n \in \mathbb{Z}^+ : n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot (n-1) \cdot n\}$.
We prove $S = \mathbb{Z}^+$ by induction on n.
Basis:
Since $1! = 1$, then $1 \in S$.
Induction:
Let $k \in S$.
Then $k \in \mathbb{Z}^+$ and $k! = 1 \cdot 2 \cdot ... \cdot (k-1)k$.
Observe that

$$\begin{array}{rcl} (k+1)! & = & (k+1) \cdot k! \\ & = & (k+1) \cdot [1 \cdot 2 \cdot ...(k-1) \cdot k] \\ & = & (k+1) \cdot [k \cdot (k-1) \cdot ... \cdot 2 \cdot 1] \\ & = & (k+1) \cdot k \cdot (k-1) \cdot ... \cdot 2 \cdot 1 \\ & = & 1 \cdot 2 \cdot ... \cdot (k-1) \cdot k \cdot (k+1). \end{array}$$

Since $k+1 \in \mathbb{Z}^+$ and $(k+1)! = 1 \cdot 2 \cdot ... \cdot (k-1) \cdot k \cdot (k+1)$, then $k+1 \in S$.
Thus, $k \in S$ implies $k+1 \in S$ for any $k \in S$.
Since $1 \in S$ and $k \in S$ implies $k+1 \in S$ for any $k \in S$, then by PMI, $n! = 1 \cdot 2 \cdot ... \cdot (n-1) \cdot n$ for any positive integer n. $\square$

Proposition 2. ***properties of binomial coefficients***
Let $n \in \mathbb{Z}^+$.
1. $\binom{0}{0} = 1$.
2. $\binom{n}{1} = n$.
3. $\binom{n}{0} = 1$.
4. $\binom{n}{n} = 1$.

5. Let $k \in \mathbb{Z}^+$.
If $k \leq n$, then $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ (Pascal's Recursion Rule)
6. Let $k \in \mathbb{Z}$.
If $0 \leq k \leq n$, then $\binom{n}{k} = \binom{n}{n-k}$. (Symmetry)

Proof. We prove 1.
Since $0 \leq 0$, then $\binom{0}{0} = \frac{0!}{(0-0)!0!} = \frac{0!}{0!0!} = \frac{1}{1 \cdot 1} = 1$. $\square$

Proof. We prove 2.
Since $n \in \mathbb{Z}^+$, then $n \geq 1$, so $1 \leq n$.
Since $0 < 1 \leq n$, then $\binom{n}{1} = \frac{n!}{(n-1)!1!} = \frac{n(n-1)!}{(n-1)!1!} = \frac{n}{1!} = \frac{n}{1} = n$. $\square$

Proof. We prove 3.
Since $n \in \mathbb{Z}^+$, then $n > 0$, so $0 < n$.
Observe that $\binom{n}{0} = \frac{n!}{(n-0)!0!} = \frac{n!}{n!0!} = \frac{1}{0!} = \frac{1}{1} = 1$. $\square$

Proof. We prove 4.
Since $n = n$, then $n \leq n$, so $\binom{n}{n} = \frac{n!}{(n-n)!n!} = \frac{n!}{n!0!} = \frac{1}{0!} = \frac{1}{1} = 1$. $\square$

Proof. We prove 5.
Suppose $k \leq n$.
Then either $k < n$ or $k = n$.
We consider these cases separately.
Case 1: Suppose $k = n$.
Then $\binom{n}{k} = \binom{n}{n} = 1 = 1+0 = \binom{n-1}{n-1} + \binom{n-1}{n} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
Case 2: Suppose $k < n$.
Then $0 < n-k$, so $n-k > 0$.
Since $k \in \mathbb{Z}^+$, then $k > 0$.
Since $n \in \mathbb{Z}^+$, then $n > 0$.
Since $0 < k$ and $k < n$, then $0 < k < n$.
Observe that

$$
\begin{aligned}
\binom{n}{k} &= \frac{n!}{(n-k)!k!} \\
&= \frac{n(n-1)!}{(n-k)!k!} \\
&= \frac{[k+(n-k)](n-1)!}{(n-k)!k!} \\
&= \frac{k(n-1)!+(n-k)(n-1)!}{(n-k)!k!} \\
&= \frac{k(n-1)!}{(n-k)!k!} + \frac{(n-k)(n-1)!}{(n-k)!k!} \\
&= \frac{k(n-1)!}{(n-k)!k(k-1)!} + \frac{(n-k)(n-1)!}{(n-k)(n-k-1)!k!} \\
&= \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-k-1)!k!} \\
&= \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-1-k)!k!} \\
&= \frac{(n-1)!}{[(n-1)-(k-1)]!(k-1)!} + \frac{(n-1)!}{[(n-1)-k]!k!} \\
&= \binom{n-1}{k-1} + \binom{n-1}{k}.
\end{aligned}
$$

□

Proof. We prove 6.

Suppose $0 \leq k \leq n$.

Then

$$
\begin{aligned}
\binom{n}{k} &= \frac{n!}{(n-k)!k!} \\
&= \frac{n!}{k!(n-k)!} \\
&= \frac{n!}{(n-n+k)!(n-k)!} \\
&= \frac{n!}{[n-(n-k)]!(n-k)!} \\
&= \binom{n}{n-k}.
\end{aligned}
$$

□

Theorem 3. ***Binomial Theorem***

Let $a, b \in \mathbb{R}$.

Then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$ for all $n \in \mathbb{Z}^+$.

Proof. We prove by induction on n.

Let $S = \{n \in \mathbb{Z}^+ : (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k\}$.

Basis:

Observe that

$$\begin{aligned} \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k &= \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 \\ &= a + b \\ &= (a+b)^1. \end{aligned}$$

Since $1 \in \mathbb{Z}^+$ and $(a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k$, then $1 \in S$.

Induction:

Suppose $m \in S$.

Then $m \in \mathbb{Z}^+$ and $(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k$.

Since $m \in \mathbb{Z}^+$, then $m+1 \in \mathbb{Z}^+$.

Observe that

$$\begin{aligned} a(a+b)^m &= a \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k \\ &= \sum_{k=0}^{m} \binom{m}{k} a^{m-k+1} b^k \\ &= \binom{m}{0} a^{m-0+1} b^0 + \sum_{k=1}^{m} \binom{m}{k} a^{m-k+1} b^k \\ &= a^{m+1} + \sum_{k=1}^{m} \binom{m}{k} a^{m-k+1} b^k. \end{aligned}$$

Observe that

$$\begin{aligned} b(a+b)^m &= b \sum_{j=0}^{m} \binom{m}{j} a^{m-j} b^j \\ &= \sum_{j=0}^{m} \binom{m}{j} a^{m-j} b^{j+1} \\ &= \binom{m}{0} a^m b + \binom{m}{1} a^{m-1} b^2 + ... + \binom{m}{m-1} a b^m + \binom{m}{m} b^{m+1} \\ &= \sum_{k=1}^{m} \binom{m}{k-1} a^{m-k+1} b^k + \binom{m}{m} b^{m+1} \\ &= \sum_{k=1}^{m} \binom{m}{k-1} a^{m-k+1} b^k + b^{m+1}. \end{aligned}$$

Observe that

$$\begin{aligned}
\sum_{k=1}^{m}\binom{m}{k}a^{m-k+1}b^k+\sum_{k=1}^{m}\binom{m}{k-1}a^{m-k+1}b^k &= [\binom{m}{1}a^mb+\binom{m}{2}a^{m-1}b^2+...+\binom{m}{m}ab^m]+[\binom{m}{0}a^mb+ \\
&= [\binom{m}{0}+\binom{m}{1}]a^mb+[\binom{m}{1}+\binom{m}{2}]a^{m-1}b^2+...+[\binom{m}{m-1} \\
&= \binom{m+1}{1}a^mb+\binom{m+1}{2}a^{m-1}b^2+...+\binom{m+1}{m}ab^m \\
&= \sum_{k=1}^{m}\binom{m+1}{k}a^{m-k+1}b^k.
\end{aligned}$$

Observe that

$$\begin{aligned}
(a+b)^{m+1} &= (a+b)^m(a+b) \\
&= (a+b)(a+b)^m \\
&= a(a+b)^m+b(a+b)^m \\
&= [a^{m+1}+\sum_{k=1}^{m}\binom{m}{k}a^{m-k+1}b^k]+[\sum_{k=1}^{m}\binom{m}{k-1}a^{m-k+1}b^k+b^{m+1}] \\
&= a^{m+1}+[\sum_{k=1}^{m}\binom{m}{k}a^{m-k+1}b^k+\sum_{k=1}^{m}\binom{m}{k-1}a^{m-k+1}b^k]+b^{m+1} \\
&= a^{m+1}+[\sum_{k=1}^{m}\binom{m+1}{k}a^{m-k+1}b^k]+b^{m+1} \\
&= \sum_{k=0}^{m+1}\binom{m+1}{k}a^{m-k+1}b^k \\
&= \sum_{k=0}^{m+1}\binom{m+1}{k}a^{m+1-k}b^k.
\end{aligned}$$

Since $m+1 \in \mathbb{Z}^+$ and $(a+b)^{m+1} = \sum_{k=0}^{m+1}\binom{m+1}{k}a^{m+1-k}b^k$, then $m+1 \in S$.
Hence, $m \in S$ implies $m+1 \in S$.
It follows by induction that $(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$ for all $n \in \mathbb{Z}^+$. $\square$

Theorem 4. *The number of ordered selections of k distinct objects from a set of n distinct objects is $P(n,k) = \frac{n!}{(n-k)!} = n*(n-1)...(n-k+1), 0 < k \leq n$.*

Proof. Let $n \in Z, n \geq 0$.
Let S be a finite set of n distinct objects.
Then $|S| = n =$ the number of distinct objects in $S =$ size of S.
Let S_k be a k-permutation of the n-set $S, 0 < k \leq n$.
Then S_k is an ordered arrangement of k distinct objects from a set of n distinct objects.
How many different S_k exist?

Let $x =$ the number of different S_k.

Let $T = \{t : t \text{ is a } k\text{-permutation}\} = \{t : t = S_k\} = \{S_k : S_k \text{ is a } k\text{-permutation of } n\text{-set}\}$.

Then $x = |T|$.

The number of different S_k is the number of different ways to create a single S_k.

Let $t =$ create a single S_k.

Let $|t| =$ the number of different ways to create a single S_k.

Then $|T| = |t|$.

What does it mean to 'create a single S_k'?

To create a single k-permutation means to choose an object for each of the k positions.

Thus, task t can be decomposed into a sequence of subtasks t_i as follows:

$t =$ create a single $S_k =$

choose a distinct object from S for the first position,

then choose a remaining distinct object from S for the second position,

then choose a remaining distinct object from S for the third position,

then choose a remaining distinct object from S for the fourth position,

...

AND

...

finally, choose a remaining distinct object from S for the k^{th} position.

Let $t_i =$ choose a remaining distinct object from S for placement into the i^{th} position with $i = 1..k$.

Let $|t_i|$

$=$ the number of different ways to choose a remaining distinct object from set S for placement into the i^{th} position with $i = 1..k$

$=$ the number of choices to select a remaining distinct object from S.

Then we can use the multiplication principle to count.

Thus, $|t| = \prod_{i=1}^{k} |t_i|$.

We must compute each $|t_i|, i = 1..k$.

$|t_1| =$ the number of choices to select a remaining distinct object from set $S =$ the number of distinct remaining objects that can be chosen from set $S =$ the count of distinct remaining objects in $S = n$.

$|t_2| =$ the number of choices to select a remaining distinct object from set $S =$ the number of distinct remaining objects that can be chosen from set $S =$ the count of distinct remaining objects in $S = n - 1$.

$|t_3| =$ the number of choices to select a remaining distinct object from set $S =$ the number of distinct remaining objects that can be chosen from set $S =$ the count of distinct remaining objects in $S = n - 2$. ...

$|t_i| =$ the number of choices to select a remaining distinct object from set $S =$ the number of distinct remaining objects that can be chosen from set $S =$ the count of distinct remaining objects in $S = n - (i - 1) = n - i + 1$. ...

$|t_k|$ = the number of choices to select a remaining distinct object from set S = the number of distinct remaining objects that can be chosen from set S = the count of distinct remaining objects in $S = n - k + 1$.

Therefore, $|t| = \prod_{i=1}^{k}(n-i+1) = n*(n-1)*(n-2)*(n-3)*...*(n-k+1)$.

Since $|t|$ is a function of n, k we

let $P(n,k) = \prod_{i=1}^{k}(n-i+1) = n*(n-1)*(n-2)*(n-3)*...*(n-k+1)$.

Thus, $P(n,k) = \frac{n*(n-1)*(n-2)*(n-3)*...*(n-k+1)*(n-k)!}{(n-k)!} = \frac{n!}{(n-k)!}$. ☐

Theorem 5. *There are $(n-1)!$ circular permutations of n distinct elements.*

Proof. Let S be a set of n distinct elements.

Each n-permutation of n distinct elements gives rise to n identical cyclic rotations.

There are $n!$ such n-permutations.

Thus, the number of circular permutations $= \frac{n!}{n} = (n-1)!$. ☐

Theorem 6. $\forall 0 \leq k \leq n. \binom{n}{k} = \frac{n!}{(n-k)!k!}$.

Proof. Let S be a set of n distinct elements.

Let k-subset (k-combination) be an unordered selection of k distinct elements from a set of n distinct elements.

Let $\binom{n}{k}$ = the number of different k combinations.

The number of different ways to arrange the k distinct elements in the k-subset is $P(k,k) = k!$.

Thus, the total number of k-permutations $= \binom{n}{k} * P(k,k) = P(n,k) = \frac{n!}{(n-k)!}$

Hence, $\binom{n}{k} = \frac{n!}{(n-k)!k!}$. ☐

Theorem 7. $\binom{n}{k} = \binom{n}{n-k}$.

Proof. Let S be a set of n distinct elements.

Then $\binom{n}{k}$ represents the number of different k-subsets selected from an n-set.

Selecting a k-subset from an n-set is the same as selecting a $(n-k)$ subset to leave out of the selection. ☐

Theorem 8. ***Pascal's Identity***

Let $n, k \in \mathbb{Z}^+$ with $1 \leq k < n$.

Then $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

Proof. Let S be a set of n distinct elements.

Then $|S| = n$.

Let $T = \{X : X \text{ is a } k\text{-subset of } S\}$.

Then $|T| = \binom{n}{k}$.

Let $e \in S$ be fixed and partition T into $T = T_1 \cup T_2$ and $T_1 \cap T_2 = \emptyset$ where

$T_1 = \{X \in T : e \in X\}$ and

$T_2 = \{X \in T : e \notin X\}$.

T_2 = the set of k-subsets of S that don't contain e = the set of k-subsets of $S - \{e\}$.

Hence, $|T_2| = \binom{n-1}{k}$.

T_1 = the set of k-subsets of S that contain e = the set of $k-1$-subsets of $S - \{e\}$ in which e is added to each.

Hence, $|T_1| = \binom{n-1}{k-1}$.

Since $\{T_1, T_2\}$ is a partition of T, then

$|T| = |T_1 \cup T_2| = |T_1| + |T_2|$.

Thus, $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$. □

Proof. An alternate proof exists.

Let $n, k \in \mathbb{Z}^+$ with $k \leq n$.

Then $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Let n be an arbitrary natural number.

Let k be an arbitrary integer, $k \geq 0$.

Then

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{(n-k)!k!} + \frac{n!}{(n-k+1)!(k-1)!} \\
&= \frac{n!}{(n-k)!k(k-1)!} + \frac{n!}{(n-k+1)(n-k)!(k-1)!} \\
&= \frac{n!}{(n-k)!(k-1)!}[\frac{1}{k} + \frac{1}{n-k+1}] \\
&= \frac{n!}{(n-k)!(k-1)!} \cdot \frac{n+1}{k(n-k+1)} \\
&= \frac{(n+1)!}{(n+1-k)!k!} \\
& \quad \binom{n+1}{k}
\end{aligned}$$

□

Theorem 9. *How many functions exist from an m-set to n-set?*

Proof. Let $B^A = \{f : A \mapsto B : f \text{ is a function}\}$ where $|A| = m$ and $|B| = n$.

Then $|B^A|$ = the number of different functions from m-set to n-set.

An example of a function from A to B is the identity function $I(x) = x$.

Thus, $I \in B^A$, so $B^A \neq \emptyset$.

Hence, $|B^A| > 0$.

How many functions exist in B^A?

We know the number of different functions = the number of different ways to create a single function.

In order to create a single function we must assign each of the elements in the domain.

Let $f : A \mapsto B$ be a function in B^A.

To create f, we can label the domain as follows.

Let $A = \{a_1, a_2, a_3, ..., a_m\}$.

In order to assign each of the elements in the domain,

we assign a_1, then assign a_2, then assign a_3, then ... then assign a_m.

Each of these subtasks are independent, so we can use the multiplication principle.

Thus, the number of ways to create a single function $= \prod_{k=1}^{m} |a_k|$

where $|a_k|$ = the number of different ways to assign a_k in B = the number of different ways to choose $f(a_k)$ in B.

We must now determine each $|a_k|$ for $k = 1..m$.

$|a_1| = |B| = n$.

$|a_2| = n$.

$|a_3| = n$.

$|a_m| = n$.

Thus, $|B^A| = n * n * n * ... * n = n^m$.

Therefore, there are n^m different functions from an m set to n set. □

Theorem 10. *How many injective functions exist from an m-set to n-set?*

Proof. Let $B^A = \{f : A \mapsto B : f \text{ is injective}\}$ where $|A| = m$ and $|B| = n$.

Then $|B^A|$ = the number of different injective functions from m-set to n-set.

An injective function is 1-1, so by the Pigeonhole principle, $m \leq n$.

An example of a 1-1 function from A to B is the identity function $I(x) = x$.

We know I is bijective, so it is also 1-1.

Thus, $I \in B^A$, so $S \neq \emptyset$.

Hence, $|B^A| > 0$.

How many injective functions exist in B^A?

We know the number of different 1-1 functions = the number of different ways to create a single 1-1 function.

In order to create a single 1-1 function we must assign each of the elements in the domain.

Let $f : A \mapsto B$ be a 1-1 function in B^A.

To create f, we can label the domain as follows.

Let $A = \{a_1, a_2, a_3, ..., a_m\}$.

In order to assign each of the elements in the domain,

we assign a_1, then assign a_2, then assign a_3, then ... then assign a_m.

Each of these subtasks are independent, so we can use the multiplication principle.

Thus, the number of ways to create a single 1-1 function $= \prod_{k=1}^{m} |a_k|$

where $|a_k|$ = the number of different ways to assign a_k in B = the number of different ways to choose $f(a_k)$ in B.

We must now determine each $|a_k|$ for $k = 1..m$.

$|a_1| = |B| = n$.

$|a_2| = n - 1$.

$|a_3| = n - 2$.

$|a_m| = n - (m - 1) = n - m + 1$.

Thus, $|B^A| = n * (n - 1) * (n - 2) * ... * (n - m + 1) = P(n, m) = \frac{n!}{(n-m)!}$.

Therefore, there are $\frac{n!}{(n-m)!}$ different injective functions from an m set to n set. $\square$

Theorem 11. *Let S be a finite set containing n elements, $n \geq 0$.*
Then there are 2^n different subsets of S.

Proof. How many subsets of S exist?
Let $n \in \mathbb{Z}, n \geq 0$.
Let S be a finite set of n elements. Then $|S| = n$.
Let $t =$ the number of different subsets of S.
Let $\mathscr{P}(S) = \{X : X \subseteq S\}$ where $\mathscr{P}(S)$ is the powerset of S.
Then $t = |\mathscr{P}(S)|$.
Since $\emptyset \subseteq S$, then $\emptyset \in \mathscr{P}(S)$.
Thus, $\mathscr{P}(S) \neq \emptyset$, so $|\mathscr{P}(S)| > 0$.
How many different subsets of S exist in $\mathscr{P}(S)$?
We can partition $\mathscr{P}(S)$ such that each cell contains all subsets of S that have the same cardinality.
We partition because we'd like to count the number of different subsets of S using the addition principle.
We realize that each subset of S can have from 0 to $|S| = n$ elements.
Thus, a subset of S may have 0 or 1 or 2 or ... or n elements.
Hence, there exist $n + 1$ cells in the partition.
Let $\{A_0, A_1, A_2, ..., A_n\}$ be a partition of $\mathscr{P}(S)$
where each cell (equivalence class) $A_i =$ the set of all subsets of S that have the same cardinality i.
Thus, $\mathscr{P}(S) = \cup_{i=0}^{n} A_i$ and any two distinct cells $A_i \neq A_j$ are disjoint.
For example, equivalence class $A_3 =$ the set of all subsets of S that have the same size of 3.
Since we have a partition we can use the addition principle to count the number of different subsets of S.
Thus, $|\mathscr{P}(S)| = \sum_{k=0}^{n} |A_k|$ where $|A_k| =$ the number of different subsets of size k from a set S of size n.
Define k-set to be a set of size k.
Then $|A_k| =$
the number of different k-sets that can be created from an n-set
$=$ the number of different ways to create a single k-set from an n-set
$=$ the number of ways to select k distinct elements from a set of n distinct elements.
We must determine each $|A_k|$.
How do we create a single k-set from an n-set?
We must select k distinct objects from the n-set.
Since order does not matter, this is a combination.
Let T_k be the task to create a set of size k.
Thus, $|A_k|$ is the number of different ways to create a set of size k from a set of size n

= the number of ways to choose k distinct objects from a set of n distinct objects

We know the number of subsets of size k from a set of size n is a combination of n things taken k at a time.

Thus, $|A_k| = \binom{n}{k}$.

Hence, $t = \sum_{k=0}^{n} \binom{n}{k}$.

We must prove $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Our statement S_n is $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

We prove using mathematical induction.

Basis:

If $n = 0$, the statement S_0 is $\sum_{i=0}^{0} \binom{0}{i} = 2^0$.

The left hand side is $\binom{0}{0} = 1$ and the right hand side is $2^0 = 1$. Thus S_0 is true.

If $n = 1$, the statement S_1 is $\sum_{i=0}^{1} \binom{1}{i} = 2^1$.

The left hand side is $\binom{1}{0} + \binom{1}{1} = 1 + 1 = 2$ and the right hand side is $2^1 = 2$. Thus S_1 is true.

Induction: Suppose $\sum_{i=0}^{k} \binom{k}{i} = 2^k$ for $k \geq 0$.

Observe the following equalities:

$$\begin{aligned}
\sum_{i=0}^{k+1} \binom{k+1}{i} &= \sum_{i=0}^{k+1} [\binom{k}{i-1} + \binom{k}{i}] \\
&= \sum_{i=0}^{k+1} \binom{k}{i-1} + \sum_{i=0}^{k+1} \binom{k}{i} \\
&= \binom{k}{-1} + \binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \ldots + \binom{k}{k} + \sum_{i=0}^{k} \binom{k}{i} + \binom{k}{k+1} \\
&= 0 + \sum_{i=0}^{k} \binom{k}{i} + \sum_{i=0}^{k} \binom{k}{i} + 0 \\
&= 2 * \sum_{i=0}^{k} \binom{k}{i} \\
&= 2 * 2^k \\
&= 2^{k+1}
\end{aligned}$$

Thus $\sum_{i=0}^{k} \binom{k}{i} = 2^k$ implies $\sum_{i=0}^{k+1} \binom{k+1}{i} = 2^{k+1}$ for $k \geq 0$.

By induction it follows that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ for $n \geq 0$. □

Theorem 12. *A finite set of n elements has 2^n subsets.*

Solution. How do we even know to come up with an answer for the number of subsets of S?

The number of different subsets of S is the same as the number of different ways to create a single subset T of S.

So how many ways exist to create a subset of S.

What is the procedure to create a subset T?

Well to create a subset we must decide whether an element is to go into T.

We must decide whether an element of S is to be in the subset T.

Let $t =$decide whether an element of S is to be an element of T.

Then $|t| =$ the number of ways to decide whether an element of S is to go in T.

There are two outcomes: either an element goes in T or it does not.

Thus $|t| = 2$.

To create subset T we have to make this decision for all of the elements of S.

Thus we choose the first element, then choose 2nd,then 3rd, and so on until choose n^{th}.

Each choice has 2 outcomes so by multiplication principle we have $2 * 2 * ... * 2 = 2^n$ different ways to create a subset T.

Thus there are 2^n different subsets of S.

We must prove:

$(\forall n \in \mathbb{N})$, a set S of n elements has 2^n subsets.

Define predicate $p(n)$: a set S of n elements has 2^n subsets.

The statement has the form $(\forall n \in \mathbb{N})(p(n))$, so we use proof by induction.

Let S be the truth set of $p(n)$.

To prove $S = \mathbb{N}$, we must prove:

1. $1 \in S$.
2. $(\forall m \in \mathbb{N})(m \in S \to m + 1 \in S)$.

To prove 1:

we must prove a set S of 1 element has exactly 2^1 subsets.

To prove 2:

Assume $m \in S$ is arbitrary.

Then we assume a set S of m elements has 2^m subsets.

We must prove:

a set of $m + 1$ elements has 2^{m+1} subsets.

We must somehow relate a set S of $m+1$ elements to a set T of m elements.

The trick here is to partition S into two sets: a singleton set containing some element, say c that is in S but not in T, and another set $S - \{c\}$. $\square$

Proof. We prove for every $n \in \mathbb{N}$, a set of n elements has 2^n subsets.

Let S be the truth set of $p(n)$: a set of n elements has 2^n subsets.

To prove $S = \mathbb{N}$ by induction, we must prove:

1. $1 \in S$.
2. $(\forall m \in \mathbb{N})(m \in S \to m + 1 \in S)$.

Basis:

To prove $1 \in S$, we must prove a set of 1 element has 2^1 subsets.

Suppose T is a set containing exactly 1 element.

Then the only subsets of T are $\emptyset$ and T itself.

Hence, there are $2 = 2^1$ subsets of T, as desired.

Induction:

Suppose $m \in S$.

To prove $m+1 \in S$, we must prove a set of $m+1$ elements has 2^{m+1} subsets.

Since $m \in S$, then we assume a set of m elements has 2^m subsets.

Let T be a set of m elements.

Let T' be a set of $m+1$ elements.

Then T' contains one additional element that is not in T.

Thus, let c be an element of T' that is not in T.

Then $T' = T \cup \{c\}$ and $c \notin T$.

We must prove there exist 2^{m+1} subsets of T'.

Let X be a subset of T'.

Then either $c \in X$ or $c \notin X$.

Suppose $c \notin X$.

Then X is a subset of T.

Since T contains m elements, then by assumption, T has 2^m subsets.

Thus, X is one of the 2^m subsets of T.

Hence, there are 2^m subsets of T' that do not contain c.

Let Y be a subset of T' that contains c.

Then $Y = X \cup \{c\}$ for some subset X of T that does not contain c.

Thus, a subset of T' that contains c can be formed from a subset of T' that does not contain c by adding c.

Hence, we create a subset of T' that contains c by adding c to each of the 2^m subsets of T' that do not contain c.

Thus, we can create a total of 2^m subsets of T' that contain c.

Therefore, there are 2^m subsets of T' that do not contain c and there are 2^m subsets of T' that do contain c.

Hence, there are a total of $2^m + 2^m = 2 * 2^m = 2^{m+1}$ subsets of T', as desired. $\square$