Counting

(Section 1.9)

Combinatorics - the field of mathematics that counts things, often in very clever ways!

Proposition: (subsets of a finite set)

Let S be a set, $|S| = n < \infty$. Then S has 2^n distinct subsets.

proof: Let T be an arbitrary subset of S and suppose $S = \{x_1, x_2, x_3, \dots, x_n\}$.

Then either $x_1 \in T$ or $x_1 \notin T$

(2 choices)

Either $x_2 \in T$ or $x_2 \notin T$

(2 choices)

Similarly, $\forall$ k, $1 \le k \le n$,

either $x_k \in T$ or $x_k \notin T$.

This gives 2 choices for each element of S, for a total of 2^n choices of subsets.

$\square$

Proposition: (k-element subsets of a finite set) Let S be a finite set, $|S| = n < \infty$.

Then if $0 \le k \le n$, the number of k-element subsets of S is

"n choose k" → $\binom{n}{k} = \dfrac{n!}{(n-k)!\,k!}$.

proof: Some convention: $0! = 1$.

So for $k = 0$, we get

$$\frac{n!}{n! \cdot 0!} = 1 \quad ✓$$

In general, if you want to choose k elements of S, we can do this in the following way:

$S = \{x_1, x_2, \dots, x_n\}$, to make a k-element subset of S, you have

- n choices for the first element
- $(n-1)$ choices for the second element
- $(n-2)$ choices for the third element

$\vdots$

- $(n-(k-1))$ choices for the k^{th} element

So you have

$$n(n-1)\cdot(n-2)\cdot\ldots\cdot(n-(k-1))$$

choices, which we can rewrite

as $\dfrac{n!}{(n-k)!}$.

Why do we divide by the additional factorial of k?

For example, if we were choosing 3-element subsets, we could choose in the order

$\{x_1, x_5, x_7\}$, but also

$\{x_5, x_7, x_1\}$. These

are the same sets, just written in a different order.

For a fixed k-element subset of S, there are $k!$ ways to rearrange the order, and all of these count as the same set.

So to exclude repetitions, we divide out by $k!$, which gives us

$$\frac{n!}{(n-k)!\,k!}$$ different k-element subsets.

$\square$

Lemma: (properties of $\binom{n}{k}$)

With the convention that

$k \in \mathbb{Z}$ and if $n \in \mathbb{N}$,

$\binom{n}{k} = 0$ if $k < 0$,

we have

1) $\binom{n}{k} \in \mathbb{Z}$, $\binom{n}{k} \geq 0$

2) $\binom{n}{k} = \binom{n}{n-k}$

3) $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

Theorem: (binomial) Let x and y be commuting indeterminates. If $n \in \mathbb{Z}$, $n \geq 0$,

$$\boxed{(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}}$$

proof: By "commuting indeterminates", we mean that you can add and multiply x and y, with the usual associative and distributive laws applying. The "commuting" part means $xy = yx$, but it is also taken for granted that $x+y=y+x$. Via induction, one can show that

$$(xy)^m = x^m y^m \quad \forall\, m \in \mathbb{N}.$$

Aside: the Binomial Theorem is false for matrices for $n \geq 2$.

$$x = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad y = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$(x+y)^2 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

$$x^2 + 2xy + y^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + 2\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

We'll prove the binomial theorem by induction:

Base case $n=1$ is trivial.

$$(x+y)^1 \stackrel{?}{=} \sum_{k=0}^{1} \binom{1}{k} x^k y^{1-k}$$

$$x+y \stackrel{?}{=} \underbrace{\binom{1}{0}}_{=1} x^0 y^1 + \underbrace{\binom{1}{1}}_{=1} x^1 y^0$$

$$x+y = y+x \checkmark$$

Now assume that

$$\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = (x+y)^n$$

for some $n \in \mathbb{N}$.

$$(x+y)^{n+1} = (x+y)^n (x+y)$$

$$= \Bigg(\underbrace{\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}}_{A}\Bigg)(x+y)$$

$$= A \cdot x + A \cdot y$$

$$= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \cdot x$$

$$+ \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \cdot y$$

By commutativity, this is

$$\sum_{k=0}^{n} \binom{n}{k} \underbrace{x^k \cdot x}_{x^{k+1}} y^{n-k}$$

$$+ \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k+1}$$

Reindex

For the first sum, let $m = k+1$. Then $k = m-1$, so we get

$$\sum_{m=1}^{n+1} \binom{n}{m-1} x^m y^{n-(m-1)}$$

$$= \sum_{m=1}^{n+1} \binom{n}{m-1} x^m y^{n-m+1}.$$

In the second sum, change the index of summation to m to get that

$$(x+y)^{n+1} = \sum_{m=1}^{n+1} \binom{n}{m-1} x^m y^{n-m+1}$$

$$+ \sum_{m=0}^{n} \binom{n}{m} x^m y^{n-m+1}$$

$$= \sum_{m=1}^{n} \left(\binom{n}{m} + \binom{n}{m-1} \right) x^m y^{n-m+1}$$

$$+ \underbrace{\binom{n}{n}}_{1} x^{n+1}$$

$$+ \underbrace{\binom{n}{0}}_{1} y^{n+1}$$

$$= x^{n+1} + y^{n+1} + \sum_{m=1}^{n} \left(\binom{n}{m} + \binom{n}{m-1} \right) x^m y^{n-m+1}$$

By the previous lemma,

$$\binom{n}{m} + \binom{n}{m-1} = \binom{n+1}{m},$$

so we get

$$(x+y)^{n+1} = x^{n+1} + y^{n+1} + \sum_{m=1}^{n} \binom{n+1}{m} x^{m} y^{n+1-m}$$

By induction, the proof is complete.

$\square$