The Vandermonde Convolution and Generalized Binomial Coefficients

Andrew Paul

12/27/2017

Theorem (Vandermonde Convolution):

$$\boxed{\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}}$$

We present two proofs – an algebraic proof and a combinatorial proof (via bijection).

Proof 1: Consider the binomial expansion of $(x+1)^{m+n}$:

$$(x+1)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^{m+n-k} = \binom{m+n}{0} x^{m+n} + \binom{m+n}{1} x^{m+n-1} + ... + \binom{m+n}{m+n}$$

However, we can also evaluate the expansion as the product of two different binomial expansions:

$$(x+1)^{m+n} = (x+1)^m (x+1)^n = \left(\sum_{i=0}^{m} \binom{m}{i} x^{m-i} \right) \left(\sum_{j=0}^{n} \binom{n}{j} x^{n-j} \right)$$

Writing out the latter term by term:

$$(x+1)^{m+n} = \left(\binom{m}{0} x^m + \binom{m}{1} x^{m-1} + \binom{m}{2} x^{m-2} + ... + \binom{m}{m} \right) \left(\binom{n}{0} x^n + \binom{n}{1} x^{n-1} + \binom{n}{2} x^{n-2} + ... + \binom{n}{n} \right)$$

Now we distribute:

$$(x+1)^{m+n} = \binom{m}{0}\binom{n}{0} x^{m+n} + \left[\binom{m}{0}\binom{n}{1} + \binom{m}{1}\binom{n}{0} \right] x^{m+n-1} + ... + \binom{m}{m}\binom{n}{n}$$

Comparing the coefficients of this expansion with our first expansion yields:

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$$

As desired. $\square$

The bijective proof is far prettier (as is the case for virtually all combinatorial identities).

Proof 2: Consider a committee of r people that is to be formed from a group of $m+n$ candidates consisting of m men and n women. The number of ways such a committee could be formed is clearly $\binom{m+n}{r}$. Call the set of these committees formed A (so that $|A| = \binom{m+n}{r}$).

Alternatively, consider the committees formed by choosing k men from the group of $m+n$ candidates and $r-k$ women. For a given k, this is $\binom{m}{k}\binom{n}{r-k}$. We may sum this over all possible k to obtain a set of committees B such that $|B| = \sum_{k=0}^{r}\binom{m}{k}\binom{n}{r-k}$. Since $f : A \to B$ is a bijection, we must have:

$$|A| = |B|$$

or:

$$\binom{m+n}{r} = \sum_{k=0}^{r}\binom{m}{k}\binom{n}{r-k}$$

As desired. $\square$

Interestingly, Pascal's Identity and the Hockey-Stick Identity can be derived from the Vandermonde Convolution. However, to do so, we must first introduce the *generalized binomial coefficient*:

$$\boxed{\binom{\lambda}{k} = \prod_{r=0}^{k-1}\frac{\lambda - r}{k-r}}$$

Here we have $k \in \mathbb{N}$ but not only can we have $\lambda \in \mathbb{C}$ but λ can be an element of *any* commutative ring where all positive integers are invertible (thanks Wikipedia for this cool fact!)[1] We first prove Pascal's Identity:

Proof 3: We simply expand $\binom{n+1}{j+1}$ using the Vandermonde Convolution, letting $n = 1$ and $r = j+1$, and notice that the first j terms are 0 when we use generalized binomial coefficients:

$$\binom{n+1}{j+1} = \underbrace{\binom{n}{0}\binom{1}{j+1} + \binom{n}{1}\binom{1}{j} + \dots}_{0} + \binom{n}{j}\binom{1}{1} + \binom{n}{j+1}\binom{1}{0}$$

Hence:

$$\binom{n+1}{r+1} = \binom{n}{r} + \binom{n}{r+1}$$

[1] I think they are just referring to commutative rings where $\forall n \in \mathbb{N}, \exists! x : x+n = 0$, though rings are super abstract so I wouldn't be surprised if $\exists$ is sufficiently strong.

As desired. □

The Hockey-Stick Identity follows. This goes to show that combinatorial identities – and identities in general – don't underlie other more "complicated" identities. Instead, all identities are simultaneously true by virtue of mutual existence.