Here, the symbol "$\overset{0}{=}$" means that the left hand side and the right hand side differ only in addends that are 0, and thus are equal. Thus, Thm. 2.18 is proven $x \in \mathbb{N}$. □

2nd proof of Thm. 2.18 for the case when $x \in \mathbb{N}$ and $y \in \mathbb{N}$:

How many ways are there to choose an n-element subset of $\{1, 2, \ldots, x\} \cup \{-1, -2, \ldots, -y\}$?

1st answer: $\binom{x+y}{n}$.

2nd answer: First, decide how many positive elements our subset will have. Let's say it will have k positive elements ($k \in \{0, 1, \ldots, n\}$). Then, choose these k positive elements (this gives $\binom{x}{k}$ choices). Then, choose the remaining $n-k$ elements (this gives $\binom{y}{n-k}$ choices). $\Rightarrow$ The answer is $\sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k}$.

Now, compare the 2 answers. This proves Thm. 2.18 when

$x \in \mathbb{N}$ & $y \in \mathbb{N}$. □

3rd proof for all x & y. See [detnotes, first proof of Thm. 2.29 (or 3.29 in future versions)]. (Induction on n, using $n\binom{y}{n} = y\binom{y-1}{n-1}$ (the "absorption identity").) □

(by Prop. 2.2, applied to $y, n, 1$ instead of $n, g, 6$)

Cor. 2.19. Let $n \in \mathbb{N}$. Then, $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

Proof. Thm. 2.18 (applied to $x=n$ & $y=n$) yields

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k} \underbrace{\binom{n}{n-k}}_{=\binom{n}{k} \text{ (by symmetry)}} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k}^2.$$ □

Rmk. No formula for $\sum_{k=0}^{n} \binom{n}{k}^3$ is known.

However, there are such formulas for $\sum_{k=0}^{n} (-1)^k \binom{n}{k}^i$ with

$i = 1, 2, 3$. We've seen the one for $i = 1$, and will soon see the one for $i = 2$.

Next, I claim that just one trick suffices to make the first two proofs of Thm. 2.18 yield it for ALL $x, y \in \mathbb{R}$.

This is the "polynomial identity trick":

A reminder on polynomials: Polynomials are NOT functions!

Informally, a polynomial (with rational coefficients, in 1 variable X) is a "formal expression" of the form

$$\alpha X^a + \beta X^b + \gamma X^c + \ldots + \omega X^z \quad \text{with } \alpha, \beta, \ldots, \omega \in \mathbb{Q} \text{ and } a, b, \ldots, z \in \mathbb{N}.$$

These expressions obey rules:

$\varphi X^n + \psi X^n = (\varphi + \psi) X^n$ ("combining like terms");

$0 X^a$ can be removed;

terms can be swapped.

X^0 is written as 1; X^1 is written as X.

subtraction is defined by

$$(\alpha X^a + \beta X^b) - (\gamma X^c + \delta X^d) = \alpha X^a + \beta X^b + (-\gamma) X^c + (-\delta) X^d;$$

multiplication is defined by distributivity and $(\alpha X^a)(\beta X^b) = \alpha\beta X^{a+b}$;

the <u>degree</u> of a polynomial is the largest exponent appearing in it with coefficient $\neq 0$.

<u>Substituting</u> a number (or matrix, or another polynomial) x into a polynomial $P = \alpha X^a + \beta X^b + \gamma X^c + \dots$ yields $\alpha x^a + \beta x^b + \gamma x^c + \dots$. This result is called $P(x)$.

A number x ($\in \mathbb{Q}$ or $\in \mathbb{R}$ or $\in \mathbb{C}$) is a <u>root</u> of a polynomial P if & only if $P(x) = 0$.

For a formal definition of polynomials, see [detnotes, §1.5] or [Loehr] (most recommended) or most good algebra texts or one of the later chapters of this class.

Thm. 2.20. (the "polynomial identity trick").

(a) A polynomial (with rational coefficients, in 1 variable X) of degree $\leq n$ (for a given $n \in \mathbb{N}$) has $\leq n$ roots (in $\mathbb{Q}$, in $\mathbb{R}$ or in $\mathbb{C}$), unless it is the 0 polynomial (i.e., its coefficients are all 0).

(b) If a polynomial P has infinitely many roots, then P is the 0 polynomial.

(c) Let P and Q be polynomials. If

$$P(x) = Q(x) \quad \forall x \in \mathbb{N},$$

then $P = Q$.

Proof. E.g., see Goodman, "Algebra: Abstract & Concrete", Cor. 1.8.24. □

Salvaging our 1st proof of Thm. 2.18. Fix $y \in \mathbb{R}$ and $n \in \mathbb{N}$. We've already proven

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

for all $x \in \mathbb{N}$. We want to prove it for all $x \in \mathbb{R}$.

Define two polynomials P, Q by

$$P = \binom{X+y}{n} \quad \text{and} \quad Q = \sum_{k=0}^{n} \binom{X}{k}\binom{y}{n-k}.$$

These are well-defined polynomials, since

$$P = \binom{X+y}{n} = \frac{(X+y)(X+y-1)\cdots(X+y-n+1)}{n!}$$

and $$Q = \sum_{k=0}^{n} \binom{X}{k}\binom{y}{n-k} = \sum_{k=0}^{n} \frac{X(X-1)\cdots(X-k+1)}{k!}\binom{y}{n-k}.$$

Thus, $P(x) = Q(x)$ $\forall x \in \mathbb{N}$ (since we have proven (7) for all $x \in \mathbb{N}$). Hence, Thm. 2.20 (c) yields $P = Q$.

Hence, $P(x) = Q(x)$ $\forall x \in \mathbb{R}$. In other words, (7) holds for all $x \in \mathbb{R}$. This completes the 1st proof of Thm. 2.18. $\square$

Salvaging our 2nd proof of Thm. 2.18.

Same idea, but now we need to do it twice:

Step 1: Fix $y \in \mathbb{N}$, and $n \in \mathbb{N}$. Use the same argument as before to prove that (7) holds for all $x \in \mathbb{R}$.

Step 2: Fix $x \in \mathbb{R}$, and $n \in \mathbb{N}$. Use an analogous argument (using y instead of x) to prove that (7) holds for all $y \in \mathbb{R}$. □

Rmk. Thm. 2.20 (c) can be applied to other identities:

- Prop. 2.2 (trinomial revision) says

$$\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b} \quad \forall n, a, b \in \mathbb{R}.$$

We gave a bijective proof for the case $n, a, b \in \mathbb{N}$.

Using Thm. 2.20 (c), we can extend this to $n \in \mathbb{R}$, but a, b still have to stay in $\mathbb{N}$, since "$\binom{n}{k}$" does not make sense.

- Cor. 2.3 said $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = [n=0] \quad \forall n \in \mathbb{N}$.

This cannot be generalized to $n \in \mathbb{Q}$ or $n \in \mathbb{R}$, since n appears as the upper bound of the sum.

- Thm. 2.15 said $k^m = \sum_{i=0}^{n} \operatorname{sur}(m,i) \binom{k}{i} \quad \forall k \in \mathbb{N} \; \forall m \in \mathbb{N}$.

Thm. 2.20(c) yields that this holds for all $k \in \mathbb{R}$ and $m \in \mathbb{N}$.
But not for $m \in \mathbb{R}$.

- HW 2 Exe 2 said $\sum_{i=0}^{n} \binom{n}{i} \binom{n-i}{k-2i} 2^{k-2i} = \binom{2n}{k} \quad \forall n \in \mathbb{N} \; \forall k \in \mathbb{N}$.

Per se, we cannot generalize this to $n \in \mathbb{R}$ or $k \in \mathbb{R}$.
But we can replace $\sum_{i=0}^{n}$ by $\sum_{i=0}^{\lfloor k/2 \rfloor}$, and then we can let $n \in \mathbb{R}$.

- HW 2 Exe 4 said $\sum_{k=0}^{m} (-1)^k \binom{n}{k} = (-1)^m \binom{n-1}{m} \quad \forall n \in \mathbb{N} \; \forall m \in \mathbb{N}$.

Thm. 2.20(c) lets us extend this to $n \in \mathbb{R}$, but not to $m \in \mathbb{R}$.

Thm. 2.18 is called the (Chu-) Vandermonde identity.

It has several "mutated" versions.

The following two identities can be used to "mutate" it:

- UpNeg (= upper negation = Prop. 1.15):
$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k} \quad \forall n \in \mathbb{R}, \ k \in \mathbb{Z}.$$

- Symm (= symmetry = Thm. 1.17): $\binom{n}{k} = \binom{n}{n-k}$ $\forall n \in \mathbb{N}, k \in \mathbb{Z}$.

Here is one example of "mutated" Vandermonde identity:

Prop. 2.21 ("upside-down Vandermonde"). Let $n, x, y \in \mathbb{N}$.

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

Rmk. This cannot be generalized using Thm. 2.20 (c), since the RHS is not a polynomial function in any of n, x, y. And indeed, the equality is false for $n=6$, $x=-1$, $y=3$.

1st proof of Prop. 2.21. (from [detnotes, §2.3?])

If $n < x+y$, then both sides are 0

(indeed, each addend on the RHS is 0, because if $k \in \{0,1,\ldots,n\}$ is such that $\binom{k}{x}\binom{n-k}{y} \neq 0$, then $\binom{k}{x} \neq 0 \Rightarrow k \geq x$ and $\binom{n-k}{y} \neq 0 \Rightarrow n-k \geq y$

and thus $n = \underbrace{k}_{\geq x} + \underbrace{n-k}_{\geq y} \geq x+y$ ↯).

So we WLOG assume $n \geq x+y$. Thus,

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

$$\overset{\text{Symm}}{=} \binom{k}{k-x} \qquad \overset{\text{Symm}}{=} \binom{n-k}{n-k-y}$$

$$\overset{\text{UpNeg}}{=} (-1)^{k-x}\binom{-k+(k-x)-1}{k-x} \qquad \overset{\text{UpNeg}}{=} (-1)^{n-k-y}\binom{-(n-k)+(n-k-y)-1}{n-k-y}$$

$$= (-1)^{k-x}\binom{-x-1}{k-x} \qquad = (-1)^{n-k-y}\binom{-y-1}{n-k-y}$$

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

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

$$= (-1)^{n-x-y} \underbrace{\sum_{k=x}^{n-y} \binom{-x-1}{k-x} \binom{-y-1}{n-k-y}}$$

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

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

(by Thm. 2.18, applied to $n-x-y$, $-x-1$ and $-y-1$ instead of n, x and y)

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

$$\underline{\underline{\text{UpNeg}}} \quad (-1)^{n-x-y} (-1)^{n-x-y} \binom{-((-x-1)+(-y-1))+(n-x-y)-1}{n-x-y}$$

$$= \binom{n+1}{n-x-y} \underline{\underline{\text{Symm}}} \binom{n+1}{n+1-(n-x-y)} = \binom{n+1}{x+y+1}. \quad \square$$

2nd proof of Prop. 2.21. Double-count the number of $(x+y+1)$-elt. subsets of $[n+1]$:

1st answer: $\binom{n+1}{x+y+1}$.

2nd answer: Construct such a subset as follows:

- Choose the $(x+1)$-th smallest element of this subset. Call it $k+1$. Thus, $k \in \{0,1,\ldots,n\}$.

- Choose the x smallest elements of this subset.
  There are $\binom{k}{x}$ options for this (since they need to be chosen from the k-elt. set $\{1,2,\dots,k\}$).
- Choose the remaining y elements of this subset.
  There are $\binom{n-k}{y}$ options for this (why?).

$\Rightarrow$ The answer is $\sum_{k=0}^{n} \binom{k}{x}\binom{n-k}{y}$.

Compare the 2 answers $\Rightarrow \binom{n+1}{x+y+1} = \sum_{k=0}^{n} \binom{k}{x}\binom{n-k}{y}$. □

2.5 Counting subsets again

Recall Thm. 1.19: If S is an n-elt. set and $k \in \mathbb{Z}$, then

$$\binom{n}{k} = (\#\text{ of } k\text{-elt. subsets of } S).$$

We proved this by induction. We'll now re-prove this by "multijection":

Def. Let S be a set. Let $k \in \mathbb{N}$.

A k-tuple $(s_1, s_2, \ldots, s_k) \in S^k$ is called injective if $s_1, s_2, \ldots, s_k$ are distinct.

Let S^k_{dist} be the set of all injective k-tuples in S^k.

Ex: $(3,2,5)$ is injective, but $(4,2,4)$ is not.

Note that injective k-tuples are also known as "k-samples without replacement".

Prop. 2.22. Let S be a set. Let $k \in \mathbb{N}$. Then, $|S^k_{dist}| = |S|^{\underline{k}}$.

Proof. The injective k-tuples are in 1-to-1 correspondence with the injective maps from $[k]$ to S.

Rigorously: There is a bijection

$$\{\text{injective maps from } [k] \text{ to } S\} \longrightarrow S^k_{dist},$$
$$f \longmapsto (f(1), f(2), \ldots, f(k)).$$

Thus,

$$|S^k_{\text{dist}}| = |\{\text{inj. maps from } [k] \text{ to } S\}|$$
$$= (\#\text{ of inj. maps from } [k] \text{ to } S)$$
$$= |S|^{\underline{k}}$$

(by Thm. 2.5, applied to $A = [k]$, $B = S$, $m = k$, $n = |S|$). $\square$

2nd proof of Thm. 1.19. WLOG assume $k \geq 0$ (else, we just claim $0 = 0$). Then, $|S| = n$, so Prop. 2.22 yields $|S^k_{\text{dist}}| = |S|^{\underline{k}} = n^{\underline{k}}$. But

$$|S^k_{\text{dist}}| = (\#\text{ of injective } k\text{-tuples } \vec{s} \in S^k)$$
$$= \sum_{\substack{W \subseteq S; \\ |W| = k}} \underbrace{(\#\text{ of injective } k\text{-tuples } \vec{s} \in S^k \text{ such that the set of entries of } \vec{s} \text{ is } W)}_{= (\#\text{ of injective } k\text{-tuples } \vec{s} \in W^k)}$$

↑ by Observation 1 (below)