# Math 222 Fall 2022, Lecture 14: Binomial coefficients

**website:** `https://www.cip.ifi.lmu.de/~grinberg/t/22fco`

# 2. Binomial coefficients (cont'd)

## 2.2. Revisiting trinomial revision

In Lecture 8, we have proved the following:

**Proposition 2.2.1** (trinomial revision formula)**.** Let $n, a, b \in \mathbb{R}$. Then,

$$\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}.$$

We proved this proposition algebraically. Let us now try to prove it combinatorially.

### 2.2.1. A partial proof by double counting

We first consider the case when $n \in \mathbb{N}$.

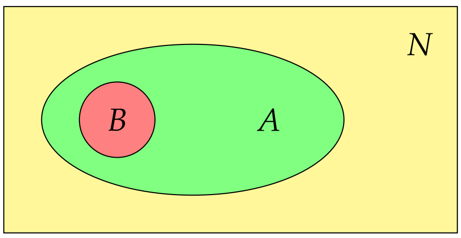
*Partial proof of Proposition 2.2.1 in the case when $n \in \mathbb{N}$.* Let us first argue informally.

Assume that $n \in \mathbb{N}$. Fix a set $N$ of $n$ people.

We consider pairs $(A, B)$, where $A$ is a committee consisting of $a$ people from $N$ (that is, an $a$-element subset of $N$), and where $B$ is a subcommittee consisting of $b$ people from $A$ (that is, a $b$-element subset of $A$). Such pairs will be called **CS pairs** (for "committee-subcommittee pairs"). Formally speaking, a CS pair is a pair $(A, B)$ of sets satisfying

$$B \subseteq A \subseteq N \qquad \text{and} \qquad |A| = a \qquad \text{and} \qquad |B| = b.$$

Here is a symbolic picture of this situation:




.

How many CS pairs are there? Let us count this number in two ways:

- *First way:* We construct a CS pair $(A, B)$ by first choosing $A$ and then choosing $B$. We have $\binom{n}{a}$ many options for $A$ (since $A$ has to be an $a$-element subset of the $n$-element set $N$). Once $A$ is chosen, we then have $\binom{a}{b}$ many options for $B$ (since $B$ has to be a $b$-element subset of the $a$-element set $A$). So, in total, there are $\binom{n}{a}\binom{a}{b}$ many ways to make these choices.
- *Second way:* We construct a CS pair $(A, B)$ by first choosing $B$ and then choosing $A$. We have $\binom{n}{b}$ many options for $B$. Once $B$ is chosen, we then have $\binom{n-b}{a-b}$ many options for $A$ (by Proposition 1.4.15 on Lecture 10, since $A$ has to be a subset of $N$ that contains $B$ as a subset). So, in total, there are $\binom{n}{b}\binom{n-b}{a-b}$ many ways to make these choices.

But these two ways are counting the same number. Thus, by comparing them, we obtain

$$\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}.$$

This proves Proposition 2.2.1 again in the case when $n \in \mathbb{N}$. □

How can the above argument be formalized? On the surface, it looks like we have applied the product rule to get the products $\binom{n}{a}\binom{a}{b}$ and $\binom{n}{b}\binom{n-b}{a-b}$. However, this is not the case. To get a product like $\binom{n}{a}\binom{a}{b}$ from the product rule, we'd have to find two sets $X$ and $Y$ such that $|X| = \binom{n}{a}$ and $|Y| = \binom{a}{b}$, and somehow our CS pairs would have to be in bijection with the elements of $X \times Y$. Finding such an $X$ is easy:

$$X = \mathcal{P}_a(N) = \{a\text{-element subsets of } N\}.$$

However, what would $Y$ be? We are tempted to set

$$Y = \mathcal{P}_b(A) = \{b\text{-element subsets of } A\},$$

which is however not allowed, since there is no "$A$" fixed at this point. In other words, when we are choosing a CS pair $(A, B)$, the options available for $B$ depend on our choice of $A$, but this is not how a Cartesian product would work (a Cartesian product $X \times Y$ contains all pairs $(x, y)$ with $x \in X$ and $y \in Y$; the available options for $y$ do not depend on the $x$).

Fortunately, at least the **number** of possible choices for $B$ does not depend on the choice of $A$; this number is always $\dbinom{a}{b}$. In such a situation, the total # of ways is still a product, but this no longer follows from the product rule; instead, we need the following more flexible rule:

> **"Dependent product rule" for two sets:** Consider a situation in which you have to make two choices (sequentially). Assume that you have $a_1$ options available in choice 1, and then (after making choice 1) you have $a_2$ options available in choice 2 (no matter which option you chose in choice 1). Then, the total # of ways to make both choices is $a_1 a_2$.

This statement is still fairly informal, but it can be formalized. (See Theorem 2.2.2 in the 2019 notes for a formalization.)

This "dependent product rule" can also be extended to $n$ choices:

> **"Dependent product rule" for $n$ sets:** Consider a situation in which you have to make $n$ choices (sequentially). Assume that you have $a_1$ options available in choice 1, and then (after making choice 1) you have $a_2$ options available in choice 2 (no matter which option you chose in choice 1), and then (after making choices 1 and 2) you have $a_3$ options in choice 3, and so on. Then, the total # of ways to make all the choices is $a_1 a_2 \cdots a_n$.

However, there is a different (in my opinion, cleaner) way to formalize the above proof of Proposition 2.2.1. Instead of tweaking the product rule to apply to our situation, we just use the sum rule instead:

*Partial proof of Proposition 2.2.1, formalized using the sum rule.* Again, let $n \in \mathbb{N}$. Pick an $n$-element set $N$. Define a **CS pair** to be a pair $(A, B)$ of sets satisfying

$$B \subseteq A \subseteq N \qquad \text{and} \qquad |A| = a \qquad \text{and} \qquad |B| = b.$$

Then, we shall count the # of CS pairs in two ways.

- *First way:* The first entry of a CS pair is always a subset $A$ of $N$ satisfying

$|A| = a$. Hence, by the sum rule, we have

$$(\text{\# of CS pairs}) = \sum_{\substack{A \subseteq N; \\ |A|=a}} \underbrace{(\text{\# of CS pairs whose first entry is } A)}_{\substack{=(\text{\# of } b\text{-element subsets of } A) \\ \text{(by the bijection principle, because the} \\ \text{map from } \{\text{CS pairs whose first entry is } A\} \\ \text{to } \{b\text{-element subsets of } A\} \\ \text{that sends each CS pair } (A,B) \text{ to } B \text{ is a bijection)}}}$$
$$= \sum_{\substack{A \subseteq N; \\ |A|=a}} \underbrace{(\text{\# of } b\text{-element subsets of } A)}_{=\binom{a}{b}}$$
$$= \sum_{\substack{A \subseteq N; \\ |A|=a}} \binom{a}{b} = \binom{n}{a}\binom{a}{b}$$

(since the sum has $\binom{n}{a}$ many addends).

- *Second way:* The second entry of a CS pair is always a subset $B$ of $N$ satisfying $|B| = b$. Hence, by the sum rule, we have

$$(\text{\# of CS pairs}) = \sum_{\substack{B \subseteq N; \\ |B|=b}} \underbrace{(\text{\# of CS pairs whose second entry is } B)}_{\substack{=(\text{\# of } a\text{-element sets } A \text{ such that } B \subseteq A \subseteq N) \\ \text{(by the bijection principle, because the} \\ \text{map from } \{\text{CS pairs whose second entry is } B\} \\ \text{to } \{a\text{-element sets } A \text{ such that } B \subseteq A \subseteq N\} \\ \text{that sends each CS pair } (A,B) \text{ to } A \text{ is a bijection)}}}$$
$$= \sum_{\substack{B \subseteq N; \\ |B|=b}} \underbrace{(\text{\# of } a\text{-element sets } A \text{ such that } B \subseteq A \subseteq N)}_{\substack{=\binom{n-b}{a-b} \\ \text{(by Proposition 1.4.15 on Lecture 10)}}}$$
$$= \sum_{\substack{B \subseteq N; \\ |B|=b}} \binom{n-b}{a-b} = \binom{n}{b}\binom{n-b}{a-b}$$

(since the sum has $\binom{n}{b}$ many addends).

Comparing these results, we find $\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}$. This again proves Proposition 2.2.1 for $n \in \mathbb{N}$. □

What have we done here? We have used the sum rule instead of the "dependent product rule" in this formalization. It boils down to the same thing because a sum of several equal addends is just one of these addends times the number of the addends (i.e., we have $\sum_{k \in K} \lambda = |K| \cdot \lambda$). However, in general, the sum rule tends to be more versatile than the "dependent product rule", since it also applies to situations where the number of options in choice 2 is not independent of choice 1. (Of course, this results in a sum which you may or may not be able to simplify.)

### 2.2.2. The polynomial identity trick

So we have found a nice combinatorial proof of Proposition 2.2.1, which unfortunately works only for $n \in \mathbb{N}$. This looks like a dead-end; after all, there is no way we can extend our counting argument to $n = \frac{1}{2}$ or $n = -7$ or $n = \sqrt{2}$.

But is it? We will now learn a "simple" trick that will help us extend this proof to the full generality of Proposition 2.2.1. More generally, this trick will guarantee that if a binomial identity of a certain kind (there are some restrictions, which we will soon see, but the trinomial revision formula qualifies) has been proved for all nonnegative integers, then it must automatically hold for all real numbers (or complex numbers, or anything else[1]). Thus, when proving such identities, we will be able to restrict ourselves to nonnegative integers without loss of generality.

This trick is called the **polynomial identity trick** (the simplest form of what is called the **Zariski density argument** in algebraic geometry). The underlying theorem is the following:

**Theorem 2.2.2** (easy half of the Fundamental Theorem of Algebra)**.** Let $n \in \mathbb{N}$. Then, a nonzero polynomial of degree $\leq n$ has $\leq n$ roots.

Here (and in the rest of this section), "polynomial" means "polynomial in 1 indeterminate with real coefficients", and we use the capital letter "$X$" to denote the indeterminate.

**Example 2.2.3. (a)** The polynomial $X^3 - 3X + 1$ has 3 real roots, and its degree is 3.

**(b)** The polynomial $X^2 + 2X + 1 = (X+1)^2$ has only 1 real root (unless you count with multiplicity), and its degree is 2.

**(c)** The polynomial $X^2 + 1$ has 0 real roots, and its degree is 2.

In all these cases, the # of roots is $\leq$ to the degree, just as Theorem 2.2.2 predicts.

[1] An algebraically experienced reader will want to replace the words "anything else" by the less vague "elements of a commutative $\mathbb{Q}$-algebra" (or at least by "elements of a field of characteristic 0"). This level of generality can be useful, but there is nothing substantially new happening at it; every argument we will be making for real numbers can be repeated verbatim for commutative $\mathbb{Q}$-algebras or fields of characteristic 0. We have chosen real numbers just to have something definite to talk about.

*A few words about the proof of Theorem 2.2.2.* The key lemma is that if a polynomial $P$ has a root $a$, then $P$ is divisible by the linear polynomial $X - a$. Thus, if a polynomial $P$ has several distinct roots $a_1, a_2, \ldots, a_k$, then we can divide $P$ by $X - a_1,\ X - a_2,\ \ldots,\ X - a_k$ in turn; this decreases its degree by $k$. Therefore, if $P$ had degree $\leq n$ at the onset, then it will have degree $\leq n - k$ at the end of this division process. But this degree cannot be negative (unless $P = 0$). So we conclude that $n - k \geq 0$, and thus $k \leq n$. (For details, see any textbook on abstract algebra. Some references can be found in §2.6.2 of the 2019 notes.) □

We will mostly use Theorem 2.2.2 via the following two corollaries:

**Corollary 2.2.4.** If a polynomial $P$ has infinitely many roots, then $P$ is the zero polynomial.

*Proof.* Assume the contrary. Thus, $P$ is nonzero. Hence, Theorem 2.2.2 (applied to $n = \deg P$) yields that $P$ has $\leq n$ roots. This contradicts the assumption that $P$ has infinitely many roots. □

**Corollary 2.2.5.** Let $P$ and $Q$ be polynomials. Assume that

$$P(x) = Q(x) \qquad \text{for each } x \in \mathbb{N}.$$

Then, $P = Q$.

*Proof.* For each $x \in \mathbb{N}$, we have

$$(P - Q)(x) = P(x) - Q(x) = 0 \qquad \text{(since we assumed that } P(x) = Q(x)\text{)}.$$

In other words, each $x \in \mathbb{N}$ is a root of the polynomial $P - Q$. So the polynomial $P - Q$ has infinitely many roots, and thus (by Corollary 2.2.4) is the zero polynomial. In other words, $P = Q$. □

Corollary 2.2.5 allows us to prove a polynomial identity $P = Q$ by showing only that $P(x) = Q(x)$ for all $x \in \mathbb{N}$. The latter equality can often be proved combinatorially.

### 2.2.3. Salvaging our proof of trinomial revision

Let us apply this technique to turn our above partial proof of Proposition 2.2.1 into a complete proof – i.e., extending it from the case $n \in \mathbb{N}$ to the case $n \in \mathbb{R}$. First, we explain in which sense our trinomial revision formula

$$\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}$$

is a "polynomial identity". What makes this work is the following:

**Definition 2.2.6.** We have previously defined $\dbinom{n}{k}$ whenever $n$ and $k$ are numbers. We now extend this definition to the case when $n$ is a polynomial (while $k$ is still a number).

Thus, if $P$ is a polynomial[2] and if $k \in \mathbb{N}$, then

$$\dbinom{P}{k} = \frac{P \cdot (P-1) \cdot (P-2) \cdot \cdots \cdot (P-k+1)}{k!}$$

[3]. Note that the right hand side here is clearly a polynomial (since a product of polynomials is a polynomial). For example, for any $k \in \mathbb{N}$, we have

$$\dbinom{X}{k} = \frac{X(X-1)(X-2)\cdots(X-k+1)}{k!}.$$

For instance,

$$\dbinom{X}{2} = \frac{X(X-1)}{2} = \frac{1}{2}X^2 - \frac{1}{2}X.$$

If $P$ is a polynomial and $k \notin \mathbb{N}$, then $\dbinom{P}{k}$ is again a polynomial, although a pretty boring one (it is the zero polynomial, by definition).

Now, we can finish our second proof of Proposition 2.2.1:

*Second proof of Proposition 2.2.1: the last mile.* Fix $a, b \in \mathbb{R}$. Consider the following two polynomials:

$$P := \dbinom{X}{a}\dbinom{a}{b} \qquad \text{and} \qquad Q := \dbinom{X}{b}\dbinom{X-b}{a-b}.$$

Having proved Proposition 2.2.1 for the case $n \in \mathbb{N}$, we thus know that $P(n) = Q(n)$ for all $n \in \mathbb{N}$ (since this equation $P(n) = Q(n)$ is exactly equivalent to $\dbinom{n}{a}\dbinom{a}{b} = \dbinom{n}{b}\dbinom{n-b}{a-b}$). In other words, $P(x) = Q(x)$ for all $x \in \mathbb{N}$. Thus, by Corollary 2.2.5, we conclude that $P = Q$. By substituting $n$ for $X$ on both sides of this equality $P = Q$, we conclude that

$$P(n) = Q(n) \qquad \text{for any } n \in \mathbb{R}.$$

In other words,

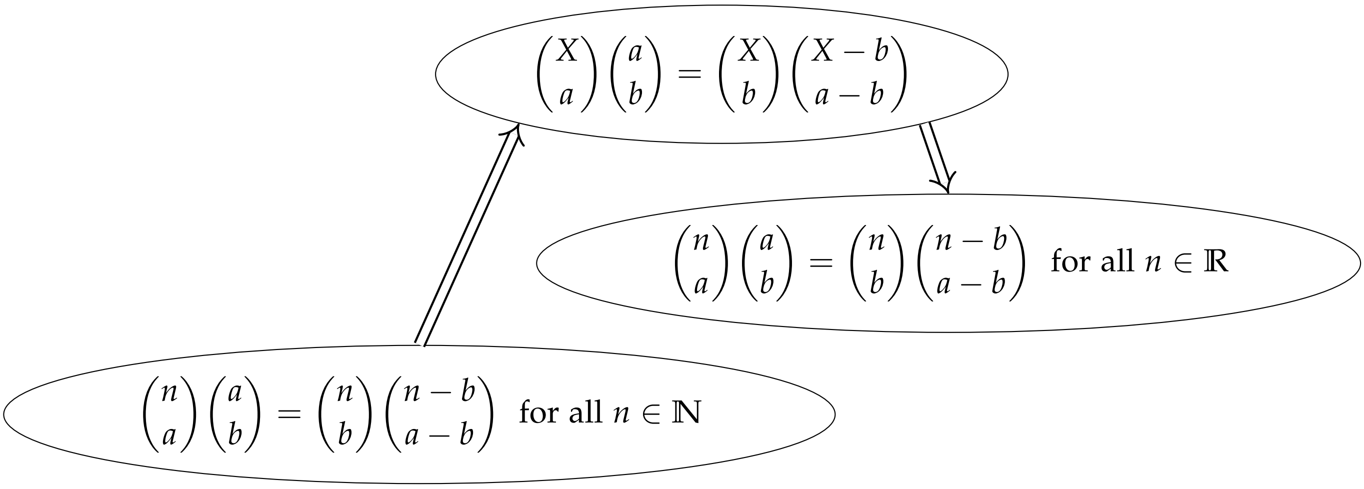
$$\dbinom{n}{a}\dbinom{a}{b} = \dbinom{n}{b}\dbinom{n-b}{a-b} \qquad \text{for any } n \in \mathbb{R}.$$

Thus, Proposition 2.2.1 holds for every $n \in \mathbb{R}$, not just for $n \in \mathbb{N}$. □

[2]You may be more used to writing $P(X)$ instead of $P$ when $P$ is a polynomial. There is nothing wrong about this (it certainly helps one remember that the indeterminate is called $X$), but it isn't strictly required. Writing "$P = 2X^2 + 3X + 7$" is just as good as writing "$P(X) = 2X^2 + 3X + 7$".

[3]I have written out the "$\cdot$" signs so that the first product $P \cdot (P-1)$ is not mistaken for the result of substituting $P-1$ into $P$.

The technique we have just applied to generalize our result from $n \in \mathbb{N}$ to $n \in \mathbb{R}$ is known as the **polynomial identity trick**. The following picture symbolically illustrates the rather peculiar logical endgame that happened when we applied the trick:




We will soon see some more interesting applications of this technique.