Math 222 Fall 2022, Lecture 6: Introduction

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

1. Introduction (cont'd)

1.3. Factorials and binomial coefficients (cont'd)

1.3.3. Fundamental properties of the binomial coefficients (cont'd)

Last time, we proved a first observation about BCs (= binomial coefficients):

Proposition 1.3.5. If $n \in \mathbb{N}$ and $k \in \mathbb{R}$ satisfy $k > n$, then $\dbinom{n}{k} = 0$.

Here are some others:[1]

Proposition 1.3.6 (Upper negation formula)**.** Let $n \in \mathbb{R}$ and $k \in \mathbb{Z}$. Then,

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}.$$

Proof. If $k \notin \mathbb{N}$, then this boils down to $0 = (-1)^k \cdot 0$, which is clear.

So WLOG assume that $k \in \mathbb{N}$. Then, the definition of binomial coefficients yields

$$\binom{-n}{k} = \frac{(-n)(-n-1)(-n-2)\cdots(-n-k+1)}{k!} \qquad \text{and}$$
$$\binom{n+k-1}{k} = \frac{(n+k-1)(n+k-2)(n+k-3)\cdots n}{k!}.$$

These two fractions are equal up to a $(-1)^k$ factor, because

- their denominators are the same, and
- their numerators are the same product, except with its factors reversed and with each factor negated (which is how we get the $(-1)^k$).

Thus, the upper negation formula (Proposition 1.3.6) is proved. $\square$

[1] In the following, I will only sketch the proofs. Detailed proofs can always be found in the 2019 notes (§1.3 to be specific).

The upper negation formula can be used to reduce questions about binomial coefficients $\binom{n}{k}$ with $n \in \{-1, -2, -3, \ldots\}$ to questions about those with $n \in \mathbb{N}$. Thus, most tables of binomial coefficients that appear in the literature omit the part with $n < 0$ and focus on the part with $n \geq 0$. This latter part is known as **Pascal's triangle**. The zeroes to the right of the $k = n$ line (these are the zeroes guaranteed by Proposition 1.3.5) are also omitted. Here is a table of Pascal's triangle with a few more rows than we saw last time:

$$
\begin{array}{r|ccccccccccccccccc}
 & & & & & & & & & & \overset{k=0}{\swarrow} & & & & & & & \\
n=0 \to & & & & & & & & & 1 & & \overset{k=1}{\swarrow} & & & & & & \\
n=1 \to & & & & & & & & 1 & & 1 & & \overset{k=2}{\swarrow} & & & & & \\
n=2 \to & & & & & & & 1 & & 2 & & 1 & & \overset{k=3}{\swarrow} & & & & \\
n=3 \to & & & & & & 1 & & 3 & & 3 & & 1 & & \overset{k=4}{\swarrow} & & & \\
n=4 \to & & & & & 1 & & 4 & & 6 & & 4 & & 1 & & \overset{k=5}{\swarrow} & & \\
n=5 \to & & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \overset{k=6}{\swarrow} & \\
n=6 \to & & & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & \overset{k=7}{\swarrow} \\
n=7 \to & & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 & \\
n=8 \to & 1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1
\end{array}
$$

Now here are some more properties of Pascal's triangle. The following theorem (known as **Pascal's recurrence**, or as the **recurrence of the binomial coefficients**) shows that each entry of this triangle is the sum of its two neighbor entries above it:

Theorem 1.3.7 (Pascal's recurrence)**.** For any $n \in \mathbb{R}$ and $k \in \mathbb{R}$, we have

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

Proof. Three cases are possible:

Case 1: We have $k \notin \mathbb{N}$.

Case 2: We have $k = 0$.

Case 3: We have $k \in \{1, 2, 3, \ldots\}$.

In Case 1, the claim boils down to $0 = 0 + 0$.

In Case 2, the claim boils down to $1 = 0 + 1$.

In Case 3, both k and $k-1$ belong to $\mathbb{N}$. Thus, the definition of BCs (= binomial coefficients) yields

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!};$$
$$\binom{n-1}{k-1} = \frac{(n-1)(n-2)(n-3)\cdots(n-k+1)}{(k-1)!};$$
$$\binom{n-1}{k} = \frac{(n-1)(n-2)(n-3)\cdots(n-k)}{k!}.$$

Bringing these fractions to a common denominator, we obtain

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!};$$
$$\binom{n-1}{k-1} = \frac{k\cdot(n-1)(n-2)(n-3)\cdots(n-k+1)}{k!};$$
$$\binom{n-1}{k} = \frac{(n-1)(n-2)(n-3)\cdots(n-k)}{k!}$$

(since $k! = (k-1)!\cdot k$, as we saw last time). So it remains to prove that

$$n(n-1)(n-2)\cdots(n-k+1)$$
$$= k\cdot(n-1)(n-2)(n-3)\cdots(n-k+1) + (n-1)(n-2)(n-3)\cdots(n-k).$$

After cancelling common factors, this boils down to

$$n = k + (n-k),$$

which is true. So the recurrence formula (Theorem 1.3.7) is proved. □

Next comes a very short formula for binomial coefficients, which however works only under specific conditions:

Theorem 1.3.8 (factorial formula for BCs)**.** Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$ be such that $k \leq n$. Then,

$$\binom{n}{k} = \frac{n!}{k!\cdot(n-k)!}.$$

Proof. The definition of BCs yields

$$\begin{aligned}
&k!\cdot(n-k)!\cdot\binom{n}{k}\\
&= k!\cdot(n-k)!\cdot\frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}\\
&= ((n-k)!)\cdot(n(n-1)(n-2)\cdots(n-k+1))\\
&= (1\cdot 2\cdot\cdots\cdot(n-k))\cdot(n(n-1)(n-2)\cdots(n-k+1))\\
&= 1\cdot 2\cdot\cdots\cdot n \qquad \text{(by reordering the factors of the product)}\\
&= n!,
\end{aligned}$$

qed. $\square$

Warning: The factorial formula $\binom{n}{k} = \dfrac{n!}{k! \cdot (n-k)!}$ only works when $n \in \mathbb{N}$ and $k \in \mathbb{N}$ and $k \leq n$. It does not help you compute $\binom{-1}{1}$ or $\binom{\sqrt{2}}{2}$ or $\binom{2}{3}$. It is nice when it works, but it has its limits!

Here is another property of BCs, which manifests itself on Pascal's triangle as a vertical symmetry (across the vertical axis in the middle of the triangle):

Theorem 1.3.9 (symmetry of binomial coefficients)**.** For any $n \in \mathbb{N}$ and $k \in \mathbb{R}$, we have

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

Proof. Let $n \in \mathbb{N}$ and $k \in \mathbb{R}$. We are in one of the following cases:
Case 1: We have $k \notin \mathbb{N}$.
Case 2: We have $k \in \mathbb{N}$ but $k > n$.
Case 3: We have $k \in \mathbb{N}$ and $k \leq n$.
In Case 1, the claim boils down to $0 = 0$ (why?).
In Case 2, the claim boils down to $0 = 0$ (why?).
In Case 3, we can apply the factorial formula and obtain

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \qquad \text{and}$$
$$\binom{n}{n-k} = \frac{n!}{(n-k)! \cdot (n-(n-k))!} = \frac{n!}{(n-k)! \cdot k!} = \frac{n!}{k! \cdot (n-k)!},$$

which is of course the same number. $\square$

Again, a **warning:** The symmetry $\binom{n}{k} = \binom{n}{n-k}$ does not hold for negative n or for non-integer n. For example, check that it fails for $n = -1$ and $k = 0$.

1.3.4. Binomial coefficients count subsets

The combinatorial meaning of BCs (binomial coefficients) is provided by the following theorem:

Theorem 1.3.10 (combinatorial interpretation of BCs)**.** Let $n \in \mathbb{N}$ and $k \in \mathbb{R}$. Let S be an n-element set. Then,

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

Example 1.3.11. **(a)** Let $n = 4$ and $k = 2$ and $S = \{1, 2, 3, 4\}$. Then, Theorem 1.3.10 says that

$$\binom{4}{2} = (\text{\# of 2-element subsets of } S).$$

Let's check this: We have $\binom{4}{2} = 6$, and the 2-element subsets of S are

$$\{1,2\}, \quad \{3,4\}, \quad \{1,4\}, \quad \{1,3\}, \quad \{2,3\}, \quad \{2,4\}.$$

(b) Let n and S be as before, and let $k = 5$. Then, Theorem 1.3.10 says that

$$\binom{4}{5} = (\text{\# of 5-element subsets of } S).$$

Let's check this: We have $\binom{4}{5} = 0$, and S has no 5-element subsets.

Warning: Theorem 1.3.10 could be used as an alternative definition of BCs, if we only cared about the case of $\binom{n}{k}$ for $n \in \mathbb{N}$ exclusively. But it says nothing about $\binom{-1}{1}$ or $\binom{\sqrt{2}}{2}$.

We shall prove Theorem 1.3.10 by induction on n. The base case ($n = 0$) relies on computing $\binom{0}{k}$:

Lemma 1.3.12. Let $k \in \mathbb{R}$. Then, $\binom{0}{k} = [k = 0]$.

Here we are using the so-called **Iverson bracket notation**:

Definition 1.3.13. If $\mathcal{A}$ is any logical statement, then the integer $[\mathcal{A}]$ is defined to be

$$\begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false.} \end{cases}$$

This integer $[\mathcal{A}]$ is called the **truth value** of $\mathcal{A}$. For example, $[1 + 1 = 2] = 1$ but $[1 + 1 = 1] = 0$.

Proof of Lemma 1.3.12. Straightforward and LTTR (see Lemma 1.3.14 in the 2019 notes). $\square$

Proof of Theorem 1.3.10. Induct on n:

Base case: We need to prove Theorem 1.3.10 for $n = 0$. So let $n = 0$, and let S be a 0-element set (i.e., the empty set). Then, we must show that

$$\binom{0}{k} = (\text{\# of } k\text{-element subsets of } S).$$

But this is clear by computing both sides: The LHS (= left-hand side) is $[k = 0]$ (by Lemma 1.3.12); the RHS (= right-hand side) is also $[k = 0]$, since the empty set S has only one subset, namely itself (which is a 0-element subset). So Theorem 1.3.10 is proved for $n = 0$.

Step: Let $m \in \mathbb{N}$. Assume as the IH (= induction hypothesis) that Theorem 1.3.10 holds for $n = m$. We must prove it for $n = m + 1$.

So let $k \in \mathbb{R}$, and let S be an $(m + 1)$-element set. We must prove that

$$\binom{m+1}{k} \overset{?}{=} (\text{\# of } k\text{-element subsets of } S) .$$

(The question mark above the equality sign here just signals that this equality has not been proved yet.)

Since S is nonempty (because $|S| = m + 1 > m \geq 0$), we can pick an element $t \in S$ and consider the m-element set $S \setminus \{t\}$. Let us do this. The IH can then be applied to $S \setminus \{t\}$ instead of S, and we obtain

$$\binom{m}{k} = (\text{\# of } k\text{-element subsets of } S \setminus \{t\}) \qquad \text{and}$$
$$\binom{m}{k-1} = (\text{\# of } (k-1)\text{-element subsets of } S \setminus \{t\}) .$$

(Note that the IH is a "for all $k \in \mathbb{R}$" statement, so we can indeed apply it to $k - 1$ instead of k, which is precisely what we have done here to get the second of these two equalities.)

By Pascal's recurrence (Theorem 1.3.7), we have

$$\begin{aligned} \binom{m+1}{k} &= \binom{m}{k-1} + \binom{m}{k} \\ &= (\text{\# of } (k-1)\text{-element subsets of } S \setminus \{t\}) \\ &\qquad + (\text{\# of } k\text{-element subsets of } S \setminus \{t\}) . \end{aligned} \tag{1}$$

So we only need to show that this sum equals (# of k-element subsets of S). At last, we're getting to do some combinatorics!

Here is how to show this: We call a subset of S

- **red** if it contains t, and
- **green** if it does not contain t.

Thus, each subset of S is either red or green, but not both. So by the sum rule, we have

$$\begin{aligned} &(\text{\# of } k\text{-element subsets of } S) \\ &= (\text{\# of red } k\text{-element subsets of } S) + (\text{\# of green } k\text{-element subsets of } S) . \end{aligned}$$

Now we need to compute the two addends on the RHS.

The green subsets of S are precisely the subsets of $S \setminus \{t\}$. So

$$\begin{aligned} & (\text{\# of green } k\text{-element subsets of } S) \\ & = (\text{\# of } k\text{-element subsets of } S \setminus \{t\}) . \end{aligned}$$

What about the red ones? They are not subsets of $S \setminus \{t\}$, since they do contain t. However, they are "essentially" $(k-1)$-element subsets of $S \setminus \{t\}$, because if you remove the element t from them, you're left with $(k-1)$-element subsets of $S \setminus \{t\}$. Let us make this rigorous: There is a bijection (= one-to-one-correspondence)

$$\begin{aligned} \{\text{red } k\text{-element subsets of } S\} &\to \{(k-1)\text{-element subsets of } S \setminus \{t\}\} , \\ R &\mapsto R \setminus \{t\} \end{aligned}$$

(its inverse map sends each Q to $Q \cup \{t\}$). Informally, this is just saying that picking a red k-element subset of S is the same as picking a $(k-1)$-element subset of $S \setminus \{t\}$ and inserting t into it. By the bijection principle, this bijection entails that

$$\begin{aligned} & (\text{\# of red } k\text{-element subsets of } S) \\ & = (\text{\# of } (k-1)\text{-element subsets of } S \setminus \{t\}) . \end{aligned}$$

Combining what we have proved, we get

$$\begin{aligned} & (\text{\# of } k\text{-element subsets of } S) \\ & = (\text{\# of red } k\text{-element subsets of } S) + (\text{\# of green } k\text{-element subsets of } S) \\ & = (\text{\# of } (k-1)\text{-element subsets of } S \setminus \{t\}) + (\text{\# of } k\text{-element subsets of } S \setminus \{t\}) \\ & = \binom{m+1}{k} \qquad \text{(by (1))} . \end{aligned}$$

This is precisely what we wanted to show in order to complete the induction step. Thus, Theorem 1.3.10 is proved by induction. □

We take a moment to mention some terminology that we will not use: When S is a set and k is an integer, the k-element subsets of S are sometimes called the **k-combinations of S** (or, more precisely, the **k-combinations of S without repetition**[2]). This notation was widespread until the 1950s, when it fell out of use because "k-element subsets" (or "k-subsets" for short) is clearer and more consistent with other parts of mathematics. Nevertheless, be prepared to occasionally see the old "k-combinations" terminology in the literature.

[2]The "k-combinations with repetition" are the size-k multisubsets of S, which we will define and study in §2.9.

1.3.5. Integrality and arithmetic properties

Here is something that looks completely natural when you look at Pascal's triangle, but actually is not obvious:

> **Theorem 1.3.14** (integrality of binomial coefficients)**.** For any $n \in \mathbb{Z}$ and $k \in \mathbb{R}$, the number $\dbinom{n}{k}$ is an integer.

Proof. If $n \geq 0$, then this number $\dbinom{n}{k}$ counts the k-element subsets of $[n]$ (by Theorem 1.3.10), and thus is obviously an integer. The case $n < 0$ can easily be reduced to the case $n \geq 0$ using upper negation. (See the 2019 notes for details, as well as for an alternative proof.) $\square$

> **Proposition 1.3.15.** Let p be a prime number, and let $k \in \{1, 2, \ldots, p-1\}$. Then, $p \mid \dbinom{p}{k}$.

Proof. We need to know one basic fact about prime numbers: If the prime number p divides a product $a_1 a_2 \cdots a_m$ of m integers $a_1, a_2, \ldots, a_m$, then it must divide (at least) one of these m integers $a_1, a_2, \ldots, a_m$. We shall call this fact "**Euclid's lemma**", although this name is more commonly used for the particular case $m = 2$ (but that doesn't make a big difference, since the general case can easily be derived by induction from the $m = 2$ case).

Now, p divides none of the k integers $1, 2, \ldots, k$ (since all these k integers are > 0 but $< p$). Hence, p cannot divide their product $1 \cdot 2 \cdot \cdots \cdot k$ either (as otherwise, Euclid's lemma would yield that p divides one of these k integers). In other words, p cannot divide $k!$.

However, the definition of BCs yields

$$\binom{p}{k} = \frac{p\,(p-1)\,(p-2)\cdots(p-k+1)}{k!},$$

so that $k! \cdot \dbinom{p}{k} = p\,(p-1)\,(p-2)\cdots(p-k+1)$. This entails that p divides the product $k! \cdot \dbinom{p}{k}$ (since there is a p factor on the RHS of this equality). Hence, by Euclid's lemma, p must divide at least one of the two factors $k!$ and $\dbinom{p}{k}$. Since we already know that p cannot divide $k!$, we thus conclude that p divides $\dbinom{p}{k}$. This proves Proposition 1.3.15. $\square$