Tutorial 8.

1 Binomial coefficients

In lecture, we saw the *binomial coefficients*

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

These represent the number of ways to choose r elements from a set of n elements, where the order does not matter. Binomial coefficients also arise in a famous pattern known as Pascal's triangle.

Pascal's Triangle

n=0	1
n=1	1 1
n=2	1 2 1
n=3	1 3 3 1
n=4	1 4 6 4 1

Definition 1 *$P_{n,r}$ = the r^{th} entry of row n, where $0 \leq r \leq n$.*

New levels of the tree are constructed according to the following rules:

$$\forall n : P_{n,0} = P_{n,n} = 1$$
$$P_{n,r} = P_{n-1,r} + P_{n-1,r-1} \quad \text{for} \quad 1 \leq r \leq n-1$$

For example:

$$P_{4,1} = P_{3,1} + P_{3,0} = 3 + 1 = 4$$

Claim 1 $P_{n,r} = \binom{n}{r}$

Proof. by induction on n
I.H. $P(n)$: For $0 \leq r \leq n$, $P_{n,r} = \binom{n}{r}$
Base case n=0: $P_{0,0} = 1 = \binom{0}{0} = \frac{0!}{0!0!}$
Inductive Step: Assume $P(n-1)$ to prove $P(n)$
We consider three cases for $\binom{n}{r}$:

Case 1: $r = 0$

$$\binom{n}{0} = 1 = P_{n,0}$$

Case 2: $r = n$

$$\binom{n}{n} = 1 = P_{n,n}$$

Case 3: $1 \leq r \leq n - 1$

Here we will use a key fact about binomial coefficients:

Claim 2 *For* $1 \leq r \leq n-1$, $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$.

Proof.

$$\begin{aligned} & \binom{n-1}{r} + \binom{n-1}{r-1} \\ &= \frac{(n-1)!}{(n-r-1)!r!} + \frac{(n-1)!}{(n-r)!(r-1)!} \\ &= \frac{(n-r)(n-1)!}{(n-r)!r!} + \frac{r(n-1)!}{(n-r)!r!} \\ &= \frac{(n-r+r)(n-1)!}{(n-r)!r!} \\ &= \frac{n!}{(n-r)!r!} \\ &= \binom{n}{r} \end{aligned}$$

■

There is also a simple combinatorial proof of claim 2.

Proof. $\binom{n}{r}$ = the number of subsets of size r chosen from a set of size n. Pick some element x in a set of size n. Then there are $\binom{n-1}{r}$ subsets of the n elements which do not contain x and $\binom{n-1}{r-1}$ subsets which do contain x. Therefore, there are $\binom{n-1}{r} + \binom{n-1}{r-1}$ subsets in total. ■

We can now use claim 2 to complete our inductive proof of claim 1 as follows:

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

$$= P_{n-1,r} + P_{n-1,r-1} \quad \text{by the inductive hypothesis}$$
$$= P_{n,r} \quad \text{by the rule for} \quad P_{n,r}$$

∎

By looking at Pascal's triangle, we can derive many facts about binomial coefficents. For example, one obvious fact is that binomial coefficents are symmetric. That is:

Theorem 1
$$\binom{n}{r} = \binom{n}{n-r}$$

Proof.

$$\binom{n}{n-r} = \frac{n!}{(n-n+r)!(n-r)!} = \frac{n!}{r!(n-r)!} = \binom{n}{r}$$

∎

There is also a simple combinatorial proof of this fact. The proof is that the number of ways of selecting a subset of size r from a set of size n is equal to the number of ways of selecting the n-r elements not in the subset.

Another property we can note from Pascal's triangle is that values within each row increase until the middle of the row, then decrease after that. That is, each row is *unimodal.* We can prove this with the next theorem, which gives the ratio between successive binomial coefficients (same n, successive r):

Theorem 2 *Suppose* $1 \leq r \leq n$. *Then*
$$\binom{n}{r} = \frac{(n-r+1)}{r}\binom{n}{r-1}.$$

Proof. Consider,
$$\binom{n}{r} / \binom{n}{r-1}$$
$$= \frac{n!}{r!(n-r)!} \times \frac{(r-1)!(n-(r-1))!}{n!} = (n-r+1)/r.$$

∎

Note that this ratio is > 1, which means the successive coefficients are increasing, as long as $r < \frac{n+1}{2}$. Also, the ratio is < 1, which means the coefficient are decreasing, when $r > \frac{n+1}{2}$. This says that the coefficients increase, reach the maximum, then decrease, i.e. they are unimodal.

2 The Binomial Theorem

The values of $\binom{n}{r}$ are called binomial coefficients because they arise in the expansion of $(x+y)^n$ according to the following theorem:

Theorem 3 (Binomial Theorem)

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

Ex: $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$

We will now see two proofs of the theorem, the first combinatorial and the second algebraic.

Proof

$$(x+y)^n = (x+y)(x+y)\cdots(x+y)$$
$$= x^n + nx^{n-1}y + \binom{n}{2} x^{n-2}y^2 + \cdots + \binom{n}{r} x^{n-r}y^r + \cdots + y^n$$

$x^{n-1}y$ has a coefficient of n because because we have n choices for which factor of $(x+y)$ contributes the y. $x^{n-2}y^2$ has a coeffcient of $\binom{n}{2}$ because there are $\binom{n}{2}$ ways to pick which two factors of $(x+y)$ to contribute a y. Similarly, $x^{n-r}y^r$ has coefficient $\binom{n}{r}$ because we can get a factor $x^{n-r}y^r$ from each possible way of choosing r terms from the original product to contribute factors of y. ∎

This proof may not seem convincing, so we will do a more formal algebraic proof as well. This proof will be by induction on n and will use the fact established earlier in the tutorial, that for $1 \le r \le n-1$, $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$.

Proof. by induction on n

I.H. $P(n)$: $(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r}y^r$

Base case n=0: $(x+y)^0 = 1 = \sum_{r=0}^{0} \binom{0}{r} x^{0-r}y^r$

Inductive Step Assume $P(n-1)$ to prove $P(n)$

$$(x+y)^{n-1} = \sum_{i=0}^{n-1} \binom{n-1}{i} x^{n-1-i}y^i$$
$$(x+y)^n = (x+y)(x+y)^{n-1}$$
$$= (x+y)\sum_{i=0}^{n-1} \binom{n-1}{i} x^{n-1-i}y^i$$
$$= \sum_{i=0}^{n-1} \binom{n-1}{i} x^{n-i}y^i + \sum_{i=0}^{n-1} \binom{n-1}{i} x^{n-1-i}y^{i+1}$$

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

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

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

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

■

We will now use this theorem to prove some identities about binomial coefficients.

Corollary 4

$$\sum_{r=0}^{n} \binom{n}{r} = 2^n$$

Proof. Set x=y=1.

$$(1+1)^n = \sum_{r=0}^{n} \binom{n}{r} 1^{n-r} 1^r$$

■

This is closely related to the result we saw in lecture, that the number of subsets of an n-element set is 2^n. Since $\binom{n}{r}$ is the number of subsets of size r, we can sum over all possible values of r to find the total number of subsets.

Corollary 5

$$\sum_{r=0}^{n} (-1)^r \binom{n}{r} = 0$$

Proof. Set x=1, y=-1.

$$(1+(-1))^n = \sum_{r=0}^{n} 1^{n-r} (-1)^r \binom{n}{r}$$

Here is another identity about binomial coefficients.

Theorem 6 *Suppose* $0 \le r \le m, n$. *Then*

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

Proof. Suppose there are m red balls and n blue balls, all distinct. There are $\binom{m+n}{r}$ ways to choose r balls from the two sets combined. This is the LHS of the identity. Now decompose this collection of choices based on how many of the chosen balls are blue and how many are red. For any k, $0 \leq k \leq r$, there are $\binom{m}{r-k}$ ways to choose $r-k$ red balls, and $\binom{n}{k}$ ways to choose k blue balls. By the product rule, that makes $\binom{m}{r-k}\binom{n}{k}$ ways to choose r balls such that k of them are blue. Adding up these numbers for all k we have that this is $\sum_{k=0}^{r}\binom{m}{r-k}\binom{n}{k}$ which is the RHS. ∎

3 Derangements

A *derangement* is a permutation of $1, 2, \ldots, n$ where i is not in the i^{th} position. E.g. the number of ways of addressing n envelopes to n people so that all the envelopes are mailed to wrong addresses. Let us represent the number of derangements on n elements as $D(n)$.

Theorem 7

$$D(n) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

We can prove the theorem using the inclusion-exclusion principle. Recall that for sets $A_1, A_2, \ldots, A_n$,

$$|A_1 \cup \ldots \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}|$$
$$+ \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|$$

Or more succintly,

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{S \subseteq \{1,\ldots,n\}, |S|=k} |\cap_{i \in S} A_i|.$$

This expresses the size of the union of n sets in terms of intersections of subsets of the n sets. We will use this to find the number of derangements by counting the number of permutations that are not derangements. This allows us to construct the following proof of theorem 7:

Proof. Let A_i be the set of permutations which map element i to position i. Then the set of permutations which are not derangements will be:

$$A_1 \bigcup A_2 \bigcup \cdots \bigcup A_n$$

Applying the inclusion-exclusion formula, this tells us that the number of permutations which are not derangements is:

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{S \subseteq \{1,\ldots,n\}, |S|=k} |\cap_{i \in S} A_i|.$$

We can evaluate this sum by noting that there are $\binom{n}{k}$ ways to choose a subset of size k from $\{A_1, \ldots, A_n\}$, and that each subset will have $(n-k)!$ elements, as it keeps k positions fixed and permutes the remaining $(n-k)$ arbitrarily. Therefore, the sum evaluates to:

$$\binom{n}{1}(n-1)! - \binom{n}{2}(n-2)! + \cdots = \sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k}(n-k)!$$

Since this gives us the number of permutations which are not derangements, we can then find the number of permutations which are derangements by subtracting the sum from the total number of permutations, $n!$. This gives:

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

$$= n! - \sum_{k=1}^{n}(-1)^{k+1}\frac{n!(n-k)!}{k!(n-k)!}$$

$$= n! + \sum_{k=1}^{n}(-1)^{k}\frac{n!}{k!}$$

$$= n!(1 + \sum_{k=1}^{n}(-1)^{k}\frac{1}{k!})$$

$$= n!\sum_{k=0}^{n}(-1)^{k}\frac{1}{k!}$$

■

The taylor expansion of e^x is

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$$

That is,

$$e^x = \sum_{k=0}^{\infty}\frac{x^k}{k!}$$

For $x = -1$, we have

$$e^{-1} = 1/e = \sum_{k=0}^{\infty}\frac{(-1)^k}{k!}$$

This looks very close to our formula for derangements which is $n!$ times the first $n+1$ terms in this expansion. In fact, we can observe that the number of derangements is the nearest integer to $n!/e$. To see this, consider the difference $n!/e - D(n)$.

$$n!/e - D(n) = n!(\sum_{k=n+1}^{\infty}\frac{(-1)^k}{k!})$$

$$= (-1)^{n+1}(\frac{1}{n+1} - \frac{1}{(n+1)(n+2)} + .. + \frac{(-1)^{k+1}}{(n+1)(n+2)\dots(n+k)} + ..)$$

So for $n \geq 1$,

$$|n!/e - D(n)| = \frac{1}{n+1} - \frac{1}{(n+1)(n+2)} + .. + \frac{(-1)^{k+1}}{(n+1)(n+2)\dots(n+k)} + ..$$

$$\leq \frac{1}{2} - \frac{1}{2.3} + .. + \frac{(-1)^{k+1}}{(k+1)!} = 1/e$$

The last inequality can be observed by grouping the terms of the summation into pairs (the first two, next two and so on) and then comparing. The difference between $n!/e$ and $D(n)$ is at most $1/e$, so the number of derangements must be the integer closest to $n!/e$.

4 Team Problem

1. The goal of this problem is to show that most boolean functions can only be computed in exponential time in the number of inputs. We will do this by looking at circuits that compute boolean functions and showing that most boolean functions can only be computed by circuits of size exponential in their numbers of inputs. A ciruit is constructed from a set of AND, OR, and NOT gates. Each AND and OR gate has two inputs and each NOT gate has one input. Any gate can have an arbitrary number of outputs. The output of the circuit is the output of some particular gate within the circuit.

For example, figure 1 shows a circuit computing the function $(x_1 \bigvee x_2) \bigwedge (x_3 \bigvee x_4)$.

We define a boolean function on k inputs to be a function from $\{0,1\}^k \to \{0,1\}$. We are going to prove that circuits of size exponential in k are required to compute most such functions. We will do this in several steps.

(a) Find the number of boolean functions with k inputs.

(b) Show that the number of circuits with s gates and k inputs is at most $(3(s+k)^2)^s$. (Note: this is an upper bound and can be made tighter, but you do not need to prove that.)

(c) Show that more than half of boolean functions on k inputs require circuits of size at least $\frac{2^k}{6k}$, provided $k \geq 9$.

(d) Last tutorial, we showed that not all boolean functions are computable. How can you reconcile that with the result you just proved?

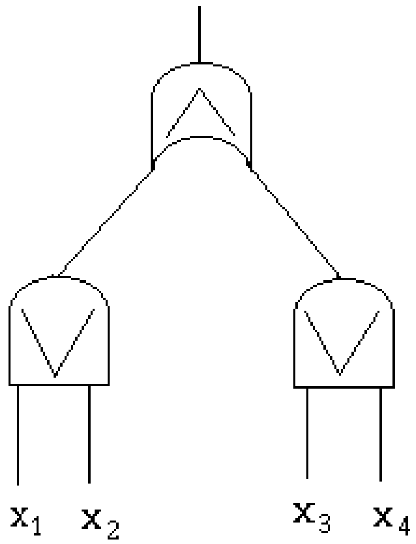

Figure 1: Circuit for $(x_1 \bigvee x_2) \bigwedge (x_3 \bigvee x_4)$