Lecture 1: Introduction, subsets and binomial coefficients

Introduction

- course Introduction
- intro to Discrete Math
- course outline

Theorem 1. *The number of subsets of* $[n] = \{1, 2, \ldots, n\}$ *of size* k *is* $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Proof. Sketch:
(1) The number of ordered subsets of size k: $n(n-1)\cdots(n-k+1) = n!/(n-k)!$,
(2) each subset of size k appears $k!$ many times in above.
Hence,

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

□

Corollary 2. $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

Next, let us consider some application of this.

Corollary 3. $\binom{n}{k} = \frac{n!}{(n-k)!k!}$ *is an integer.*

Proof. Because it represents the number of subsets of size k, hence it must be an integer. □

We use the notation $a \mid b$ to denote that a divides b. For example, $3 \mid 12$, but $5 \not\mid 12$.

Lemma 4. *If* p *is a prime number, then* $p \mid \binom{p}{k}$, *for* $k = 1, 2, ..., p-1$.

Proof. Write it down we see that

$$\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!} = p \cdot \frac{(p-1)\ldots(p-k+1)}{k!}$$

It suffices to show that $\frac{(p-1)\ldots(p-k+1)}{k!}$ is an integer.

By Corollary 3, we know $\binom{p}{k}$ must be an integer. This means that $k! \mid p(p-1)\ldots(p-k+1)$. But, since p is a prime and $k < p$, we know that none of $2, 3, ..., k$ is a factor of p. Hence, $k! \mid (p-1)\ldots(p-k+1)$ is an integer. □

Theorem 5. *Fermat Little Theorem: If* p *is a prime, then, for every natural number* x, *the following holds:* $p \mid (x^p - x)$.

Proof. Sketch: Apply Lemma 4 and Induction. Try it yourself. □

Lecture 2: more on binomial coefficients

1 Estimation of binomial coefficients

1.1 basic estimates

- $\binom{n}{k}$ as k changes, depending on whether $k < n/2$
- $\frac{2^n}{n+1} < \binom{n}{n/2} < 2^n$.
- Stirling formula: $n! \sim \sqrt{2\pi n}(n/e)^n$

$$\binom{n}{n/2} = \frac{n!}{(n/2)! \cdot (n/2)!} \sim \sqrt{\frac{2}{\pi}} \cdot \frac{2^n}{\sqrt{n}}$$

1.2 nontrivial estimates

Now, let us try to answer the following
Question: How small is k when $\binom{n}{k} < \binom{n}{n/2}/2$?

Theorem 1.

$$e^{-t^2/(m-t+1)} \le \binom{2m}{m-t} \Big/ \binom{2m}{m} \le e^{-t^2/(m+t)} \tag{1}$$

Proof. sketch: (1) expand $\binom{2m}{m}\Big/\binom{2m}{m-t}$, (2) apply $\ln(1+x) \le x$.
See the detailed proof in reading material. □

Corollary 2. *If $t \ge \sqrt{m \ln C} + \ln C$, then $\binom{2m}{m}\Big/\binom{2m}{m-t} \ge C$.*
If $t \le \sqrt{m \ln C} - \ln C$, then $\binom{2m}{m}\Big/\binom{2m}{m-t} \le C$.

Proof. Homework. □

So, now we can answer the question that approximately: we should have $k = \Theta(\sqrt{n})$.

Theorem 3. *Let $0 \le k \le m$, let $c = \binom{2m}{k}/\binom{2m}{m}$. Then,*

$$\sum_{i=0}^{k-1} \binom{2m}{i} < \frac{c}{2} \cdot 2^{2m}.$$

Proof. sketch: (1) Let A be the quantity we are interested. We want to relate the quantity to 2^{2m}, the simplest relation we can use is $C = \sum_{i=0}^{m-1} \binom{2m}{i} < 2^{2m}/2$. Let $B = C - A$. What can we say about B and A?
(2) use the monotonicity (with respect to k) of $\frac{\binom{n}{k-1}}{\binom{n}{k}}$, to relate A and B.
See the detailed proof in reading material. □

Let us pause for a moment, and ask: why do we prove this strange complicated inequality? Since, obviously, we have a much simpler estimation as follows:

$$\sum_{i=0}^{k-1} \binom{2m}{i} \le k \binom{2m}{k-1} \le k \left(\frac{2m}{k-1}\right)^{k-1}. \tag{2}$$

The point is that, for application purpose, suppose for some reason we need to estimate the k for which the above sum is at most, say 2% of the total (i.e., 2^{2m}), how are you going to calculate k from the inequality (2) ? You will have to solve equations involving product of polynomials (i.e., k) and exponential functions (i.e, $\left(\frac{2m}{k-1}\right)^{k-1}$). Are you happy to do that?

2 Ubiquitous binomial coefficient in counting problems

We know that $\binom{n}{k}$ denotes the following:

- the number of subsets of size k in $\{1, 2, \ldots, n\}$;
- the coefficient of $x^k y^{n-k}$ in $(x + y)^n$;
- the number of ways of partitioning $\{1, 2, \ldots, n\}$ into two subsets: one subset has size k, the other subset has size $n - k$.

Let us now see some natural generalizations and variants for each of them. A useful method is the method of stars and bars.

2.1 multisubset of size k

A multiset is similar to a set, except that it allows repeated elements. So, for example, $\{1, 2\}$ is a subset of size 2 of $\{1, 2, 3\}$, it is also a multisubset of size 2 of $\{1, 2, 3\}$, while $\{2, 2\}$ is a subset of size 2 of $\{1, 2, 3\}$, but not a susbet. We can write down all multisubset of size 2 of $\{1, 2, 3\}$ (for simplicity, we change the notation and use ab to denote the multiset $\{a, b\}$):

$$11, \quad 22, \quad 33, \quad 12, \quad 13, \quad 23.$$

So, there are 6 multisubsets of size 2, while we know that there are only $\binom{3}{2} = 3$ subsets of size 2.

Question: How many multisubsets of size k of $\{1, 2, \ldots, n\}$?

A: $\binom{n+k-1}{k}$.
Why is this?

Proof. sketch: Use the stars and bars method. stars: the k elements, bars: the $n-1$ bars, marking the positions for $1, 2, \ldots, n$. □

Example: let us see a conceret example:

$$11 = **||, \quad 22 = |**|, \quad 33 = ||**, \quad 12 = *|*|, \quad 13 = *||*, \quad 23 = |*|*.$$

2.2 expand $(x + y + z)^n$?

consider a general term in the expansion, $x^p y^q z^r$ (of couse, we must have $p + q + r = n$), what would be its coefficient?
A: $\binom{n}{p} \cdot \binom{n-p}{q} = \frac{n!}{p!q!r!}$.

Exercise: prove $\binom{n}{p} \cdot \binom{n-p}{q} = \binom{n}{p+q} \cdot \binom{p+q}{p}$, without doing any calculation. (pause for a second, and appreciate the beauty of this proof, the point is that: you are not making yourself a calculator.)

2.3 distributing different presents to children

You should be able to answer the following:
Question: If we distribute n different presents to k children, so that the i-th children gets k_i presents. Of course, $\sum_i k_i = n$. How many different ways of doing this?
A: $\frac{n!}{\prod_i k_i!}$. Make sure you understand why.

2.4 distributing identical pennies to children

We can again use the stars and bars method!

Suppose we have n identical stars $(* * * * \cdots * *)$, the only thing to do is to divide them into k groups. Observe that this is equivalent to put $k - 1$ bars among the stars. However, there are two cases:

- each children should gets at least one penny. This means that the bars cannot be put outside of the stars. Hence, there are only $n - 1$ positions for placing the bars, giving $\binom{n-1}{k-1}$.
- any distribution is allowed (i.e., some children could be given no penny at all). This is equivalent to that bars could be put outside of the stars, not necessarily among them, as we see in previous example in Section 2.1. Hence, there are in total $n + k - 1$ places, and we need to choose k places to put the bars, this gives $\binom{n+k-1}{k-1}$.