Асимптотики и оценки комбинаторных величин

В данной лекции речь пойдёт об аналитических оценках различных комбинаторных величин, которые были изучены в курсе основ комбинаторики и теории чисел. Эти знания будут полезны в дальнейшем при решении самых разнообразных задач.

Основной комбинаторной величиной является биномиальный коэффициент $C_n^k = \dfrac{n!}{k!(n-k)!}$. Рассмотрим скорость роста данной величины в зависимости от параметра k при $n \to \infty$.

Теорема 1 (без доказательства)

Для биномиального коэффициента справедливы следующие цепочки неравенств:

$$C_{2n}^0 < C_{2n}^1 < \dots < C_{2n}^n$$

$$C_{2n}^n > C_{2n}^{n+1} > \dots > C_{2n}^{2n}$$

Такая симметризация происходит потому, что $C_n^k = C_n^{n-k}$. Для удобства вместо n было рассмотрено чётное число $2n$, чтобы можно было делить на 2 в коэффициенте C_{2n}^n.

Данная картинка имеет вид в каком-то смысле похожий на нормальное распределение. В рамках ближайших лекций мы поймём, что нормальное распределение возникает на основе конструкции, которая называется биномиальный коэффициент. Поведение биномиальных коэффициентов обобщается на задачу о нормальном распределении и кривая, представленная на рисунке, будет похожа на гауссовскую.

Теорема 2

Изучим устройство самого большого биномиального коэффициента в нашем ряду.

Теорема гласит:

$$C_{2n}^n \leqslant 2^{2n}$$

$$C_{2n}^n \geqslant \frac{2^{2n}}{2n+1}$$

Первая оценка вытекает из того факта, что если просуммировать все биномиальные коэффициенты, среди которых присутствует и C_{2n}^n, то в сумме получится в точности 2^{2n}. Поскольку суммируются положительные слагаемые, то каждый из них (и в частности самое большое из них) не превосходит их суммы.

Вторая оценка вытекает из тех же самых соображений, что и первая. В упомянутой выше сумме $(2n+1)$ слагаемое и C_{2n}^n самое большое из них. Ясно, что самое большее слагаемое не меньше, чем общая сумма, разделённая на количество слагаемых. Несмотря на очевидность полученных результатов, с их помощью можно получить следующие интересные следствия.

Следствие

$$\ln(C_{2n}^n) \sim 2n\ln(2)$$

Доказательство. Если прологарифмировать верхнюю оценку из теоремы 2, то получится в точности $2n\ln(2)$, а если прологарифмировать нижнюю оценку, то получится $2n\ln(2) - \ln(2n+1)$, но $\ln(2n+1) \ll 2n\ln(2)$.

Таким образом, имеет место асимптотика, изложенная в следствии. Данная запись со значком $\sim$ означает асимптотическое равенство. Это не значит, что если вычесть из левой части правую, то в пределе получится ноль. Это означает, что если поделить левую часть на правую, то в пределе получится 1. По-другому это можно записать следующим образом:

$$\ln(C_{2n}^n) = (1 + o(1))2n\ln(2).$$

Асимптотика $\ln(C_{2n}^n)$ теперь известна, но она вовсе ничего не говорит относительно асимптотики исходной величины C_{2n}^n. Можно ли найти эту асимптотику в точности? Да, можно. Рассмотрим следующую теорему.

Теорема 3: Формула Стирлинга (без доказательства)

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

Данную формулу необходимо знать всем, кто занимается комбинаторикой, в которой решаются какие-либо перечислительные, экстремальные задачи (например, если требуется найти найти максимальное или минимальное множество объектов).

Упражнение

Докажите неравенство:

$$n! \geqslant \left(\frac{n}{e}\right)^n.$$

Следствие

Применим формулу Стирлинга для нахождения асимптотики C_{2n}^n:

$$C_{2n}^n = \frac{(2n)!}{(n!)^2} \sim \frac{2^{2n}}{\sqrt{\pi n}} = \frac{4^n}{\sqrt{\pi n}}.$$

В каком-то смысле полученная асимптотическая «истина» лежит посередине между верхней и нижней оценками теоремы 2. Слово "посередине" имеет тот смысл, что в результате получилось среднее геометрическое с точностью до $\sqrt{\pi}$ в знаменателе.

Для удобства введём следующее обозначение. Представим себе, что есть какая-то функция $f(n)$, принимающая, как и биномиальные коэффициенты, положительные значения. Про эту функцию известно, что $\ln(f(n)) \sim n\ln(a)$ при $n \to \infty$, $a > 1$. Будем записывать $f(n)$ в следующем виде:

$$f(n) = (a + o(1))^n. \tag{1}$$

Некоторая функция $f(n)$ равна $(a+o(1))^n$, если удаётся проверить, что её логарифм ведёт себя как $n\ln(a)$ в асимптотике.

Возьмем натуральный логарифм от правой и левой частей последнего равенства. Получим:

$$\ln(f(n)) = n\ln(a + o(1)).$$

Если $a > 1$, то логарифм суммы a и слагаемого, стремящегося к нулю, асимптотически ведёт себя так же, как $\ln(a)$, т.е.

$$\ln(f(n)) = n\ln(a + o(1)) \sim n\ln(a).$$

Смысл полученного выражения следующий: если какая-то функция похожа на экспоненту, но таковой не является, то зачастую её можно записать в виде (1). Она не в точности является экспонентой, т.е. никто не утверждает, что $f(n) = a^n$. Например, может быть следующая ситуация:

$$f(n) = \left(3 + \frac{1}{\sqrt{n}}\right)^n.$$

За $o(1)$ могут скрываться любые функции, стремящие к нулю, по-разному стремящиеся к нулю. Но легко сообразить, что

$$f(n) = \left(3 + \frac{1}{\sqrt{n}}\right)^n = 3^n\left(1 + \frac{1}{3\sqrt{n}}\right)^n = 3^n\left(1 + \frac{1}{3\sqrt{n}}\right)^{3\sqrt{n}\cdot\frac{\sqrt{n}}{3}} = 3^n \cdot e^{\frac{\sqrt{n}}{3}\cdot(1+o(1))}.$$

Таким образом $\left(3+\dfrac{1}{\sqrt{n}}\right)^n$ – это не 3^n, а 3^n умноженное на некую растущую функцию, но растущую гораздо медленнее, чем 3^n. Поэтому (1) — это просто запись, обобщающая экспоненту, это экспонента, умноженная или поделённая на слагаемое, которое растёт или убывает медленнее, чем исходная экспонента. Такая запись удобна для формулировки следующей теоремы.

Теорема 4

$$C_n^{[an]} = \left(\frac{1}{a^a(1-a)^{1-a}} + o(1)\right)^n, a \in (0,1)$$

Приведенная формула — «огрублённая» формула Стирлинга. Не будем искать совершенно точную асимптотику, как это было сделано в следствии к теореме 3. Требуется лишь огрубить эту асимптотику. Кстати, можно продолжить равенство из следствия к теореме 3 и записать:

$$\frac{4^n}{\sqrt{\pi n}} = (4+o(1))^n.$$

Когда пишется знак $''+''$ перед $o(1)$, вовсе не подразумевается, что то, что прибавляется, строго положительно. То есть вместо $o(1)$ вполне может быть функция, которая принимает отрицательные значения, но при этом стремится к нулю при $n \to \infty$. Например $\left(4-\dfrac{1}{\ln(n)}\right)^n$ вполне укладывается в эту форму записи. Принято писать $o(1)$, подразумевая, что $o(1)$ — это некоторая функция, которая по модулю стремится к нулю, но при этом она может иметь значения с различными знаками.

Доказательство. Воспользуемся формулой Стирлинга:

$$C_n^{[an]} = \frac{n!}{[an]!(n-[an])!} \sim \frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n}{\sqrt{2\pi[an]}\left(\frac{[an]}{e}\right)^{[an]}\sqrt{2\pi(n-[an])}\left(\frac{n-[an]}{e}\right)^{n-[an]}}. \tag{2}$$

Сократим асимптотически с точностью до $o(1)$ в основании экспоненты. В дальнейшем будем логарифмировать данное выражение и смотреть, куда стремится логарифм.

Предположим, что в полученном выражении нет целых частей. Также обозначим комбинацию $\sqrt{2\pi n}$, $\sqrt{2\pi[an]}$ и $\sqrt{2\pi(n-[an])}$ как $P(n)$. Таким образом выражение (2) условно (в том смысле, что следующим шагом будут сняты все целые части в остальных выражениях) равно следующему:

$$P(n)\cdot\frac{\left(\frac{n}{e}\right)^n}{\left(\frac{an}{e}\right)^{an}\left(\frac{n-an}{e}\right)^{n-an}} = \frac{P(n)}{a^{an}(1-a)^{n-an}} = P(n)\cdot\left(\frac{1}{a^a(1-a)^{1-a}}\right)^n. \tag{3}$$

Возьмём логарифм от полученного выражения:

$$\ln(P(n)) + n\ln\left(\frac{1}{a^a(1-a)^{1-a}}\right).$$

$\ln(P(n))$ — это что-то, ведущее себя как $\ln(n)$, исходя из определения $P(n)$, а $n\ln\left(\dfrac{1}{a^a(1-a)^{1-a}}\right)$ имеет порядок роста n, то есть гораздо больше, чем $\ln(P(n))$. Таким образом

$$\ln(P(n)) + n\ln\left(\frac{1}{a^a(1-a)^{1-a}}\right) \sim n\ln\left(\frac{1}{a^a(1-a)^{1-a}}\right),$$

и по определению в (3) получаем:

$$P(n)\cdot\left(\frac{1}{a^a(1-a)^{1-a}}\right)^n = \left(\frac{1}{a^a(1-a)^{1-a}} + o(1)\right).$$

Таким образом, теорема 4 почти доказана (в смысле условного равенства между (2) и (3)). Однако в процессе доказательства видно, что умножение на многочлен ($P(n)$ можно сверху оценить многочленом) вносит вклад только в $o(1)$. Это следует из того факта, что функция, похожая на экспоненту, — это в точности экспонента, умноженная на что-нибудь растущее или убывающее медленнее любой экспоненты, например, на многочлен. Получим вместо условного равенства обычное алгебраическое равенство двух выражений.

Вспомним, что an^{an} было записано вместо $[an]^{[an]}$. Целая часть отличается от своего аргумента на некоторое $\varepsilon \in [0, 1]$, зависящее от n, поэтому запишем следующее:

$$[an]^{[an]} = (an - \varepsilon)^{an-\varepsilon} = (an)^{an-\varepsilon}\left(1 - \frac{\varepsilon}{an}\right)^{an-\varepsilon} = (an)^{an} \cdot (an)^{-\varepsilon}\left(1 - \frac{\varepsilon}{an}\right)^{an}\left(1 - \frac{\varepsilon}{an}\right)^{-\varepsilon}.$$

$(an)^{an}$ — та часть, которая была оставлена в (3), и эта часть домножается на $(an)^{-\varepsilon}$, ограниченное многочленом, который, как было показано, «загоняется» в $o(1)$. Так же $(an)^{an}$ домножается на $\left(1 - \frac{\varepsilon}{an}\right)^{an}$. Применяя замечательный предел, в асимптотике получим $e^{-\varepsilon}$, а $\varepsilon \in [0, 1]$, то есть это просто некоторая константа. Ещё $(an)^{an}$ домножается на $\left(1 - \frac{\varepsilon}{an}\right)^{-\varepsilon} \sim 1$. Таким образом, все множители, отличные от $(an)^{an}$, уйдут в $o(1)$. Аналогичные рассуждения можно проделать и для $(n - an)^{n-an}$. Теорема полностью доказана.

$$\frac{1}{a^a(1-a)^{1-a}} = e^{-a\ln(a)-(1-a)\ln(1-a)}.$$

Функция $H(a) = -a\ln(a) - (1-a)\ln(1-a)$, стоящая в показателе экспоненты, называется энтропией. Оценки, проделанные выше, принято называть энтропийными оценками, потому что в них возникает данная функция $H(a)$.

Теорема 5 (без доказательства)

Данная теорема является естественным обобщением утверждения, доказанного в теореме 4.

Формулировка. *Справедлива следующая оценка для полиномиального коэффициента:*

$$P([a_1n], [a_2n], \ldots, [a_kn]) = \left(\frac{1}{a_1^{a_1}a_2^{a_2}\ldots a_k^{a_k}} + o(1)\right)^n, \quad a_1 + \ldots + a_k = 1, \quad a_i > 0 \ \ \forall i = 1, \ldots, k$$

.

В точности такое же утверждение, как доказанное в теореме 4. Если в качестве полиномиального коэффициента взять коэффициент, у которого только 2 аргумента, то получится обычный биномиальный коэффициент. Тогда второй аргумент будет $1 - a_1$ и $P([a_1n], [(1-a_1)n]) = \frac{1}{a_1^{a_1}(1-a_1)^{1-a_1}}$, то есть доказанная только что теорема 4 — частный случай утверждения теоремы 5.

Напомним, что такое полиномиальный коэффициент:

$$P(n_1, \ldots, n_k) = \frac{(n_1 + \ldots + n_k)!}{n_1! \cdot \ldots \cdot n_k!}.$$

То есть это количество способов составить слово длины $(n_1 + \ldots + n_k)$, имея на руках n_1 символов a_1, n_2 символов a_2, … , n_k символов a_k. $P(n_1, \ldots, n_k)$ называется полиномиальным коэффициентом потому, что он участвует в разложении $(x_1 + \ldots + x_k)^n$. Соответственно получается естественное обобщение бинома Ньютона, в котором участвуют обычные биномиальные коэффициенты.

Теорема 6

Формулировка. *Справедливы следующие оценки:*

1) $C_n^k \leqslant \frac{n^k}{k!}$;

2) $C_n^k \sim \frac{n^k}{k!}$, если $k = o(\sqrt{n})$;

3) $C_n^k \leqslant \frac{n^k}{k!} \cdot e^{-\frac{k(k-1)}{2n}}$;

4) $C_n^k \leqslant \dfrac{n^k}{k!} \cdot e^{-\frac{k(k-1)}{2n}} + O\left(\dfrac{k^3}{n^2}\right)$;

5) $C_n^k \sim \dfrac{n^k}{k!} \cdot e^{-\frac{k^2}{2n}}$, если $k^3 = o(n^2)$.

Перед тем, как доказывать теорему, дадим небольшой комментарий. Ситуации 2 и 5, рассмотренные в теореме, совершенно не относятся к случаям, рассмотренным в теореме 4 и теореме 5, потому что в теореме 4 $k = [an]$, а теперь k может быть функцией от n, но если и растущей, то достаточно медленно, например, медленнее, чем $\sqrt{n}$, а в п. 5 медленнее, чем $n^{\frac{2}{3}}$. В этом случае асимптотика устроена совершенно не так, как это было в случае энтропийных оценок.

Доказательство.

1) $C_n^k = \dfrac{n!}{k!(n-k)!} = \dfrac{n(n-1)\dots(n-k+1)}{k!}$.

Понятно, что каждая из скобок в числителе не превосходит n, а если быть точным меньше, чем n. Количество скобок равно k, поэтому окончательно получаем

$$C_n^k \leqslant \frac{n^k}{k!},$$

что и требовалось доказать.

4) $C_n^k = \dfrac{n(n-1)\dots(n-k+1)}{k!} \overset{[1]}{=} \dfrac{n^k}{k!}\left(1-\dfrac{1}{n}\right)\left(1-\dfrac{2}{n}\right)\cdot\ldots\cdot\left(1-\dfrac{k-1}{n}\right) \overset{[2]}{=} \dfrac{n^k}{k!} \cdot e^{\ln\left(1-\frac{1}{n}\right)+\ln\left(1-\frac{2}{n}\right)+\ldots+\ln\left(1-\frac{k-1}{n}\right)} \overset{[3]}{=}$

$\overset{[3]}{=} \dfrac{n^k}{k!} \cdot e^{-\frac{1}{n}+O\left(\frac{1}{n^2}\right)-\frac{2}{n}+O\left(\frac{4}{n^2}\right)+\ldots-\frac{k-1}{n}+O\left(\frac{(k-1)^2}{n^2}\right)} \overset{[4]}{=} \dfrac{n^k}{k!} \cdot e^{-\frac{k(k-1)}{2n}+O\left(\frac{k^3}{n^2}\right)}$

[1] Из каждой скобки выносим n;

[2] Каждую скобку представляем как экспоненту логарифма от этой скобки. Тогда в показателе экспоненты логарифмы суммируются

[3] Раскладываем каждый из логарифмов по формуле Тейлора

[4] Вычисляем сумму слагаемых вида $\dfrac{i}{n}, i = 1, \dots, k-1$, как сумму аримфметической прогрессии. Под знаком O суммируются слагаемые вида $\dfrac{i^2}{n^2}, i = 1, \dots, k-1$. Точная формула данной суммы, в общем, не нужна. В O мы записываем результат с точностью до константы, поэтому нам важно знать лишь порядок роста суммы квадратов. Понятно, что она растёт примерно как k^3. Каждое из слагаемых не больше, чем k^2 и их k штук, значит сумма не превосходит k^3. Оценка снизу: есть много слагаемых порядка $\dfrac{k}{2}$, у которых величина уже порядка k^3.

Таким образом пункт 4 доказан.

5) Доказательство пункта 5 очевидно следует из пункта 4. Если $k^3 = o(n^2)$, то $O\left(\dfrac{k^3}{n^2}\right) \to 0$ при $n \to 0$. Число e в степени, стремящейся к нулю, равно 1. Поэтому запишем:

$$C_n^k \sim \frac{n^k}{k!} \cdot e^{-\frac{k(k-1)}{2n}}.$$

Так как $k^3 = o(n^2)$, то $\dfrac{k}{n} \to 0$, поэтому -1 в показателе экспоненты можно опустить. Окончательно получаем:

$$C_n^k \sim \frac{n^k}{k!} \cdot e^{-\frac{k^2}{2n}}.$$

2) Вернёмся к доказанному в пункте 4

$$C_n^k = \frac{n^k}{k!} \cdot e^{-\frac{k(k-1)}{2n}+O\left(\frac{k^3}{n^2}\right)}.$$

Если $k^2 = o(n)$, то $k^3 = o(n^2)$, поэтому $O\left(\frac{k^3}{n^2}\right) \to 0$. Более того, $\frac{k^2}{n} \to 0$ в предположении пункта 2 о том, что $k = o(\sqrt{n})$. Получается, что весь показатель экспоненты стремится к нулю в данном случае. Это значит, что экспонента стремится к 1. И мы получаем

$$C_n^k \sim \frac{n^k}{k!}.$$

3) Вернёмся к равенству [2] из доказательства пункта 4 и запишем вместо него следующее неравенство, оценивая логарифмы сверху. Хорошо известно, что $\ln(1-x) \leqslant -x$. Получаем следующее:

$$\overset{[2]}{\leqslant} \frac{n^k}{k!} \cdot e^{-\frac{1}{n}-\frac{2}{n}-\ldots-\frac{k-1}{n}} = \frac{n^k}{k!} \cdot e^{-\frac{k(k-1)}{2n}}.$$

Теорема полностью доказана.

В таких ситуациях можно как-то хитро оценивать биномиальные коэффициенты, не прибегая явным образом к формуле Стирлинга, а пользуясь формулой Тейлора. Во многих приложениях в дальнейшем будем пользоваться именно таким ходом рассуждений.

Вернёмся к формулировке теоремы 6. Например, в пункте 5 возникает некая функция $e^{-\frac{k^2}{2}}$. Те, кто когда-либо слышал о вероятности в случае нормального распределения узнают в этом нечто очень знакомое, ведь нормальное распределение — это что-то в духе $e^{-\frac{x^2}{2}}$. Значит рассуждения о том, что биномиальные коэффициенты являются некоторой мотивировка к возникновения нормального распределения, важного для теории вероятностей и статистики.

Теорема 7

$$\frac{C_n^{\frac{n}{2}-x}}{C_n^{\frac{n}{2}}} = e^{\frac{-2x^2}{n} + O\frac{x^3}{n^2}}$$

Доказательство данной теоремы абсолютно аналогично доказательству пункта 4 теоремы 6.

Но каков смысл данной теоремы? Вернёмся к графику, рассмотренному в начале лекции. На него нанесены биномиальные коэффициенты и максимальным из них является C_{2n}^n. В теореме указано, чему равно отношение величины биномиального коэффициента, отступающего от максимального на некоторую величину, и величины самого большого биномиального коэффициента. Именно отсюда и возникает график $e^{-\frac{x^2}{2}}$, изображённый на рисунке. Таким образом и возникает на самом деле нормальная плотность.

На данной лекции были рассмотрены некоторые асимптотики. В дальнейшем будет рассмотрено, каким образом такая асимптотическая деятельность помогает при решении конкретных задач комбинаторики и дискретного анализа.