Counting

李昂生

Discrete Mathematics
U CAS
8, May, 2018

Outline

1. Basic principles
2. The Pigeonhole principle
3. Permutation and combinations
4. Combinatorial inequalities
5. With repetition
6. Solving recurrence
7. Exercises

General view

- Understanding the principles
- Applications of the principles

Product rule

Definition 1

(Product rule) Suppose that a **procedure** consists of two tasks. If there are n_1 ways to do the first task and for each of the ways of doing the first task, there are n_2 ways to do the second task. Then there are $n_1 n_2$ possible ways of the procedure.

Understand A *procedure* can be understood as the execution of an algorithm.

Ordered Pairs

Let A, B be two finite sets of n_1, n_2 elements, respectively. Define

$$A \times B$$

to be the set of the ordered pairs (a, b) of $a \in A$ and $b \in B$. Then there are $n_1 n_2$ elements in $A \times B$.
Generally, if $A = A_1 \times A_2 \times \cdots \times A_n$, and for each i, A_i contains k_i elements, then the size of A is

$$|A| = \prod_{i=1}^{n} k_i. \tag{1}$$

Trees

For a rooted tree T, if:
1) The root node $\lambda \in T$ has n_1 immediate successors.
2) For every node $\alpha \in T$, if α is at the i-th level, then there are n_{i+1} immediate successors associated with α.
Assume T has level k, then the number of leaves in T is

$$N = \prod_{i=1}^{k} n_i. \tag{2}$$

Question How many non-leaf nodes are there in T?

Remarks

- The mathematical essence of the product rule is simply the cardinality of product of sets and leaves of trees. However, the applications are usually non-trivial.
- The key to applying the rule is to clearly understand the mathematical essence of the objects.

Power sets

Given a finite set A of n elements, there are 2^n subsets of A.

$$2^A = \{X \mid X \subset A\}, \tag{3}$$

2^A is called the power set of A.
Then

$$|2^A| = 2^{|A|}.$$

Functions

Given finite sets A and B, if A and B have sizes m and n, respectively, then there are n^m many functions from A to B. Let

$$B^A = \{f \mid f : A \to B\}, \tag{4}$$

where f is a function from A to B.
A function f from A to B is usually written as:

$$\begin{aligned} f: \quad & A \to B \\ & a \mapsto b, \end{aligned}$$

where $a \in A$ and $b \in B$. Then

$$|B^A| = |B|^{|A|}.$$

Number of Truth Tables

Show that there are 2^{2^n} different truth table of n propositional variables.

Proof.

A truth table T defines a $0/1$ value for every assignment $\sigma = a_1 a_2 \cdots a_n$ of the n variables.
Therefore,
1) for every assignment σ of length n, there are two choices of the values, 0 or 1,
2) There are 2^n many assignments for the n variables.
The number of the truth tables are hence

$$2^{2^n}.$$

□

The sum rule

If a task can be done either in one of n_1 ways or in one of n_2 ways that are disjoint with the n_1 ways, then there are $n_1 + n_2$ ways to do the task.
This is essentially the disjoint union rule:
Given two finite sets A and B, if $A \cap B = \emptyset$, then

$$|A \cup B| = |A| + |B|. \tag{5}$$

Generally, given finite sets $A_1, A_2, \cdots, A_n$, if for any $i \neq j$, $A_i \cap A_j = \emptyset$, and $A = \cup_{i=1}^{n} A_i$, then

$$|A| = \sum_{i=1}^{n} |A_i|. \tag{6}$$

The subtraction rule

For finite sets A_1 and A_2, if $A = A_1 \cup A_2$, then

$$|A| = |A_1| + |A_2| - |A_1 \cap A_2|. \tag{7}$$

The division rule

If A is a finite set of size n, and A is partitioned into k subsets of equal size, then the size of the subset is

$$\frac{n}{k}.$$

The principle

Theorem 2

(The pigeonhole principle) Let A, B be finite sets of size m and n, respectively. Let $m > n$. Then for any function f from A to B, there are distinct elements $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$.

The principle - continued

Let A, B be sets, $|A| = m$, $|B| = n$, $m > n$. For every function

$$f: \; A \to B.$$

For each $b \in B$, define

$$f^{-1}(b) = \{a \mid a \in A, \& \; f(a) = b\}. \tag{8}$$

Theorem 3

There is an element $b \in B$ such that

$$|f^{-1}(b)| \geq \lceil \frac{m}{n} \rceil. \tag{9}$$

Proof

Proof.

Suppose to the contrary that for each $b \in B$, $|f^{-1}(b)| < \lceil \frac{m}{n} \rceil$, giving $|f^{-1}(b)| \leq \lceil \frac{m}{n} \rceil - 1$.
Hence

$$m = |A| \leq n(\lceil \frac{m}{n} \rceil - 1).$$

Let $m = qn + r$ for $0 \leq r < n$.
If $n|m$, then $m \leq n(q-1)$, impossible.
If $n \not| m$, then $r > 0$, but

$$m = |A| \leq n(q + 1 - 1) = qn, \tag{10}$$

absurd. □

Applications - I

Suppose that $a_1, a_2, \cdots, a_{n+1}$ are natural numbers in $[2n] = \{1, 2, \cdots, 2n\}$. Then there are $i \neq j$ such that $a_i | a_j$.

Proof.

For each i, let $a_i = 2^{k_i} q_i$ be such that $2 \not| q_i$, i.e., q_i is odd. Since there are at most n odd numbers in $[2n]$, there are $i \neq j$, $q_i = q_j = q$, with which either $a_i | a_j$ or $a_j | a_i$. $\square$

Ramsey Theory - Sequence

Theorem 4

Every sequence of $n^2 + 1$ distinct real numbers contains a subsequence of length $n + 1$ that is either increasing or decreasing.

Proof.

Suppose that $a_1, a_2, \cdots, a_{n^2+1}$ is the sequence of distinct real numbers. For each k, let I_k be the length of the longest increasing sequence starting from a_k, and D_k be the length of the longest decreasing sequence starting from a_k.

Suppose to the contrary that the theorem fails to hold. Then for each k, both $I_k \leq n$ and $D_k \leq n$ hold. Therefore, there are at most n^2 pairs (I_k, D_k) for all k from 1 to $n^2 + 1$.

By the Pigeonhole Principle, there are $k_1 < k_2$ such that $I_{k_1} = I_{k_2}$ and $D_{k_1} = D_{k_2}$ both hold. A contradiction. □

Ramsey Number

Definition 5

Let l, r be natural numbers. Define $R(l, r)$ to be the least number n satisfying:
For every simple graph G of n nodes, either there is an l-clique in G, or there is an independent set of size r in G.

Question Characterisation of $R(l, r)$.
There are interesting results and open questions of the form of Ramsey numbers in a wide range of disciplines.

Permutation

A *permutation* of a finite set A is an **ordered** list of A.
If $|A| = n$, an *r-permutation of A* is an ordered subset of r elements of A.
We use

$$P(n, r) \tag{11}$$

to denote the number of r-permutations of a size n set.

Theorem 6

$$P(n, r) = n(n-1)\cdots(n-r+1). \tag{12}$$

Proof.

By counting. $\square$

Note

$$P(n, r) = \frac{n!}{(n-r)!}.$$

Combinations

For a natural number n, let $[n] = \{1, 2, \cdots, n\}$. An *r-combination* of $[n]$ is a subset $X \subset [n]$ of size r.
We use

$$\binom{n}{r} \text{ or } C(n, r), \tag{13}$$

to denote the number of r-combinations of $[n]$, referred to as *binormial coefficient*.

Theorem 7

For $n \geq r \geq 0$,

$$\binom{n}{r} = \frac{n!}{(n-r)!r!} \tag{14}$$

Proof.

Every r-combination of $[n]$ corresponds to $r!$ many r-permutations of $[n]$, so, $\binom{n}{r} = \frac{P(n,r)}{r!}$.

The Binomial Theorem

Theorem 8

Let x and y be variables and n be natural number. Then:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j}. \tag{15}$$

Proof.

Look at

$$(x+y)^n = (x+y)(x+y)\cdot\dots\cdot(x+y) \; (n \,\text{times}).$$

□

Corollaries

1)

$$(1+1)^n = \sum_{j=0}^{n} \binom{n}{j} = 2^n.$$

2)

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

3)

$$(1+2)^n = \sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n.$$

Pascal's Identity

Theorem 9

For natural numbers $n \geq k$,

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}. \tag{16}$$

Proof.

The set of size k subsets of $[n+1]$ is divided into two classes:
A: the subsets of $[n+1]$ that contain 1, with number $\binom{n}{k-1}$,
B: the subsets of $[n+1]$ that fail to contain 1, with number $\binom{n}{k}$.
By the sum rule. □

Vandermonde's Identity

Theorem 10

For natural numbers m, n and r,

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k} \binom{n}{r-k}. \tag{17}$$

Corollary 11

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2. \tag{18}$$

Vandermonde's Identity - Proof

Proof.

Let $A = \{a_1, a_2, \cdots, a_m\}$ and $A = \{b_1, b_2, \cdots, b_n\}$ be two disjoint sets. Let $C = A \cup B$.

$\binom{m+n}{r}$ is the number of subsets of C of size r.

The subsets of C of size r are divided into $r+1$ classes: For k, $0 \le k \le r$,

I_k is the set of size r subsets of C that contain k elements in A and $r-k$ elements in B, by the product rule,

$$|I_k| = \binom{m}{k} \cdot \binom{n}{r-k}$$

By the sum rule,

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

More properties - I

Theorem 12

Let n, r be natural numbers with $r \leq n$. Then,

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}. \tag{19}$$

Proof

Proof.

Repeatedly using the Pascal's identity,

$$\begin{aligned}\binom{n+1}{r+1} &= \binom{n}{r} + \binom{n}{r+1} \\ &= \binom{n}{r} + \binom{n-1}{r} + \binom{n-1}{r+1} \\ &= \binom{n}{r} + \binom{n-1}{r} + \cdots + \binom{r}{r} + \binom{r}{r+1} \\ &= \sum_{j=r}^{n} \binom{j}{r}, \text{ noting that } \binom{r}{r+1} = 0. \qquad (20)\end{aligned}$$

$\square$

A number theory result

Lemma 13

For prime p, and for k with $1 \leq k \leq p-1$, $p \mid \binom{p}{k}$.

Proof.

By definition,

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

This gives

$$k!\binom{p}{k} = p(p-1)\cdots(p-k+1). \tag{21}$$

Since p divides the right hand side and then the left hand side, and since $p \not| k!$, $p \mid \binom{p}{k}$ follows. $\square$

For any $k \geq 1$, $k!$ divides the product of any k consecutive natural numbers.

Proof.

Let n be the largest number of the k consecutive numbers.

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

Therefore,

$$k! \mid n(n-1)\cdots(n-k+1).$$

□

Stirling's Formula

$$n! = \sqrt{2\pi n}(\frac{n}{e})^n(1 + \frac{1}{12n} + O(\frac{1}{n^2})). \tag{22}$$

Furthermore,

Lemma 14

For every n,

$$\sqrt{2\pi n}(\frac{n}{e})^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}(\frac{n}{e})^n e^{\frac{1}{12n}}. \tag{23}$$

Proof of Stirling's formula - 1

Proof.

$$\ln n! = \sum_{i=1}^{n} \ln i \approx \int_{1}^{n} \ln x dx \tag{24}$$

$$= n \ln n - n + 1. \tag{25}$$

Therefore,

$$n! \approx e \cdot (\frac{n}{e})^n. \tag{26}$$

□

Proof of Stirling's formula - 2

Proof.

$$\ln n! = \ln(1 \cdot 2 \cdots n) = \sum_{i=1}^{n} \ln i$$

$$\ln n! - \frac{1}{2} \approx \int_{1}^{n} \ln x dx = n \ln n - n + 1.$$

The error in the approximation is given by the Euler-Maclaurin formula:

$$\ln n! - \frac{1}{2} \ln n = n \ln n - n + 1 + \sum_{k=2}^{m} \frac{(-1)^k B_k}{k(k-1)} \left(\frac{1}{n^{k-1}} - 1\right) + R_{m,n},$$

where B_k is a Bernoulli number and $R_{m,n}$ is the remainder term in the Euler-Maclaurin formula.

Proof of Stirling's formula - 3

Take limits to find that

$$\lim_{n\to\infty}(\ln n! - n\ln n + n - \frac{1}{2}\ln n) = 1 - \sum_{k=2}^{m}\frac{(-1)^k B_k}{k(k-1)} + \lim_{n\to\infty} R_{m,n}.$$

Denoting the limit as y, then

$$R_{m,n} = \lim_{n\to\infty} R_{m,n} + O(\frac{1}{n^m}).$$

Combining the two equations,

$$\ln n! = n\ln(\frac{n}{e}) + \frac{1}{2}\ln n + y + \sum_{k=2}^{m}\frac{(-1)^k B_k}{k(k-1)n^{k-1}} + O(\frac{1}{n^m}).$$

Proof of Stirling's formula - 4

Taking the exponential of both sides, and set $m = 1$,

$$n! = e^y \sqrt{n}(\frac{n}{e})^n(1 + O(\frac{1}{n}))$$

Taking the limit, we get

$$e^y = \sqrt{2\pi}.$$

So

$$n! = \sqrt{2\pi n}(\frac{n}{e})^n(1 + O(\frac{1}{n})).$$

Proof of Stirling's formula - 5

Using the Γ function,

$$n! = \int_0^\infty x^n e^{-x} dx.$$

Setting $x = ny$, we get

$$n! = \int_0^\infty e^{n \ln x - x} dx = e^{n \ln n} n \int_0^\infty e^{n(\ln y - y)} dy.$$

Applying Laplaces's method, we have

$$\int_0^\infty e^{n(\ln y - y)} dy \approx \sqrt{\frac{2\pi}{n}} e^{-n}$$

Proof of Stirling's formula - 6

which gives

$$n! \approx e^{n \ln n} n \sqrt{\frac{2\pi}{n}} e^{-n} = \sqrt{2\pi n} (\frac{n}{e})^n.$$

Further corrections can be obtained by using Laplaces's method.
Computing two-order expansion using Laplace's method gives

$$\int_0^\infty e^{n(\ln y - y)} dy \approx \sqrt{\frac{2\pi}{n}} e^{-n} (1 + \frac{1}{12n})$$

This gives

$$n! \approx e^{n \ln n} n \sqrt{\frac{2\pi}{n}} e^{-n} (1 + \frac{1}{12n}) = \sqrt{2\pi n} (\frac{n}{e})^n (1 + \frac{1}{12n}).$$

Proof of Stirling's formula - 7

Therefore,

$$n! = \sqrt{2\pi n}(\frac{n}{e})^n(1 + \frac{1}{12n} + O(\frac{1}{n^2})).$$

Corollary of Stirling's formula

Lemma 15

For every $n \in \mathbb{N}$ and $\alpha \in (0, 1)$,

$$\binom{n}{\alpha n} = (1 \pm O(n^{-1})) \frac{1}{\sqrt{2\pi n\alpha(1-\alpha)}} 2^{H(\alpha)n}, \qquad (27)$$

where $H(\alpha) = -\alpha \log \alpha - (1-\alpha)\log(1-\alpha)$, the Shannon information of α.

Inequality - I

For $n \geq k \geq 0$,

$$\binom{n}{k} \leq \frac{n^k}{k!}. \tag{28}$$

Inequality - II

For large n,

$$\binom{n}{k} \approx \frac{n^k}{k!}. \tag{29}$$

Inequality - III

$$\binom{n}{k} \leq (\frac{n \cdot e}{k})^k. \tag{30}$$

Inequality - IV

$$\binom{n}{k} \geq (\frac{n}{k})^k. \tag{31}$$

Permutation with repetition

Theorem 16

The number of r-permutations of a set of size n with repetition is

$$n^r.$$

Combinations with repetition

Theorem 17

Given a set A of size n, the number of r-combinations of A with repetition is

$$\binom{n+r-1}{n-1} = \binom{n+r-1}{r}. \tag{32}$$

Proof

Let $A = \{a_1, a_2, \cdots, a_n\}$, for each i, let x_i be the number of times that a_i is chosen.
Then $0 \leq x_i \leq r$ and

$$x_1 + x_2 + \cdots + x_n = r$$

Let $y_i = x_i + 1$,

$$y_1 + y_2 + \cdots + y_n = n + r$$

The number of solutions of the equation is

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

Theorem 18

The number of ways to distribute n distinguishable objects into k distinguishable boxes so that n_i objects are placed in box i, $i = 1, 2, \cdots, k$, is

$$\frac{n!}{\prod_{i=1}^{k} n_i!}.$$

Proof.

Suppose that the n objects are $1, 2, \cdots, n$. Distribute all the objects into k boxes, $B_1, \cdots, B_k$ say. The number of ways are:

$$\begin{aligned} & \binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-\cdots-n_j}{n_{j+1}}\cdots\binom{n_k}{n_k} \\ = & \quad \frac{n!}{\prod_{i=1}^{k} n_i!}. \end{aligned}$$

Simple case

Theorem 19

Let f be an increasing function satisfying

$$f(n) = a \cdot f(\frac{n}{b}) + c, \tag{33}$$

where $a \geq 1$, b is a natural number and $b > 1$, $c > 0$.
Then,

$$f(n) = \begin{cases} O(n^{\log_b a}), & \text{if } a > 1, \\ O(\log n), & \text{if } a = 1. \end{cases} \tag{34}$$

Furthermore, if $n = b^k$ and $a > 1$, then

$$f(n) = C_1 n^{\log_b a} + C_2, \tag{35}$$

where $C_1 = f(1) + \frac{c}{a-1}$, and $C_2 = -\frac{c}{a-1}$.

Proof

Let $n = b^k$ for some natural number k.

$$\begin{aligned} f(n) &= a \cdot f(\frac{n}{b}) + c \\ &= a\left(a \cdot f(\frac{n}{b^2}) + c\right) + c \\ &= a^2 \cdot f(\frac{n}{b^2}) + c(a+1) \\ &= a^k f(1) + c(a^{k-1} + \cdots + a + 1), \text{ by induction.} \end{aligned}$$

If $a > 1$, then

$$\begin{aligned} f(n) &= a^k \cdot f(1) + c\frac{a^k - 1}{a-1} \\ &= O(a^k) = O(n^{\log_b a}). \end{aligned}$$

If $a = 1$, then $f(n) = O(k) = O(\log n)$.

Proof - continued

Generally, let k be such that $b^{k-1} < n \leq b^k$.
Since $f(n) \leq f(b^k)$. The result follows from the proof for $n = b^k$.

Master Theorem

Theorem 20

Let f be an increasing function satisfying

$$f(n) = a \cdot f(\frac{n}{b}) + cn^d. \tag{36}$$

Then,

$$f(n) = \begin{cases} O(n^d), & \text{if } a < b^d, \\ O(n^d \log n), & \text{if } a = b^d, \\ O(n^{\log_b a}), & \text{if } a > b^d. \end{cases} \tag{37}$$

Proof

Let $n = b^k$.

$$\begin{aligned} f(n) &= a \cdot f(\frac{n}{b}) + cn^d \\ &= a\left(a \cdot f(\frac{n}{b^2}) + c(\frac{n}{b})^d\right) + cn^d \\ &= a^2 \cdot f(\frac{n}{b^2} + cn^d(\frac{a}{b^d} + 1)) \\ &= a^k \cdot f(1) + cn^d(1 + \frac{a}{b^d} + \cdots + (\frac{a}{b^d})^{k-1}), \text{ by induction on } k. \end{aligned}$$

$a < b^d$

Let $\alpha = \frac{a}{b^d}$. Then $\alpha < 1$.

$$\begin{aligned}
f(n) &= a^k \cdot f(1) + cn^d(1 + \alpha + \cdots + \alpha^{k-1}) \\
&= a^k \cdot f(1) + cn^d \frac{1 - \alpha^k}{1 - \alpha} \\
&= O(n^{\log_b a}) + O(n^d) \\
&= O(n^d).
\end{aligned}$$

$a = b^d$

$$\begin{aligned} f(n) &= a^k \cdot f(1) + cn^d k \\ &= O(n^d \log n). \end{aligned}$$

$a > b^d$

Let $\beta = \frac{a}{b^d}$. Then $\beta > 1$.

$$
\begin{aligned}
f(n) &= a^k \cdot f(1) + cn^d(1 + \beta + \cdots + \beta^{k-1}) \\
&= a^k \cdot f(1) + cn^d \frac{\beta^k - 1}{\beta - 1} \\
&= O(n^{\log_b a}) + O(n^d \beta^k) \\
&= O(n^{\log_b a}), \text{ the former is the main term.}
\end{aligned}
$$

General n

Let k be such that

$$b^k < n \le b^{k+1}.$$

Since $f(n) \le f(b^{k+1})$.
The theorem follows from the proof for $n = b^{k+1}$.

The Closest-Pair Problem

Given n points

$$(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n),$$

in a plane, find the closest pair of points, where the distance is the Euclidean distance.
Michael Samos, 1985

The Algorithm

1. Sort the points by x_i's
2. Sort the points by y_j's
3. Find a line l, orthogonal to the x-axis that divides the points into two equal sizes, the left and the right part, respectively.
   – let d_L, d_R be the solutions for the left and the right parts, respectively.
   – let $d = \min\{d_L, d_R\}$.
4. For each point on the lower boundary of a rectangle of $2d \times d$ with l as the middle line, which contains at most 8 points of the instance. Find the least distance of the point from at most the 7 other points.

The Time Complexity

The recurrence of the algorithm is:

$$f(n) \leq 2 \cdot f(\frac{n}{2}) + 7n.$$

By the Master Theorem,

$$f(n) = O(n \log n).$$

Exercises - 1

(1) Let n be a natural number. Show that in any set of n consecutive integers, there is exactly one element that is divided by n.

(2) Let n, k be natural numbers. Show that

(2.1)

$$\sum_{j=0}^{k} \binom{n+j}{j} = \binom{n+k+1}{k}$$

(2.2)

$$\sum_{i=1}^{n} i \binom{n}{i} = n2^{n-1}$$

(2.3)

$$\sum_{i=1}^{n} i \binom{n}{i}^2 = n \binom{2n-1}{n-1}$$

Exercises - 2

(3) Show that

$$(x_1+x_2+\cdots+x_k)^n = \sum_{n_1+n_2+\cdots+n_k=n} C(n; n_1, \cdots, n_k) x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$$

where

$$C(n; n_1, n_2, \cdots, n_k) = \frac{n!}{n_1! \cdots n_k!}.$$

(4) Suppose that S is a set of n elements. How many ordered pairs (A, B) are there such that A and B are subsets of S with $A \subseteq B$?

谢谢！