CDM

Combinatorial Principles

Klaus Sutner

Carnegie Mellon University

Counting is arguably one of the most fundamental activities in mathematics.

By counting we mean determining the cardinality of some set S of objects.

As long as S is finite, this means to find the right number n and to enumerate the set as

$$S = \{a_1, \dots, a_n\}.$$

In other words, we have to establish a bijection $f : [n] \to S$ as in

$$\begin{array}{cccccc} 1 & 2 & 3 & \dots & n-1 & n \\ \updownarrow & \updownarrow & \updownarrow & \dots & \updownarrow & \updownarrow \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n \end{array}$$

In algorithmic applications one sometimes needs to find an actual bijection

$$f : [n] \to S$$

rather than just the cardinality n.

There are lots of possible bijections ($n!$ to be precise), but for algorithmic purposes one would like to find one that is easy to compute and that places the elements of S into some natural order. Furthermore, we also want $f^{-1} : S \to [n]$ to be easily computable.

These special bijections are called ranking (f^{-1}) and unranking functions (f).

We know the cardinality of $S = \mathfrak{P}([n])$ is 2^n.

To get a bijection $f : [2^n] \to \mathfrak{P}([n])$ we can use binary expansions.

$$r = \left(\sum_{i<n} r_i \cdot 2^i \right) + 1$$

$$f(r) = \{ \, i + 1 \mid r_i = 1 \, \}$$

We could avoid the pesky $+1$ offsets by using $\{0, \ldots, 2^n - 1\}$ rather then $[2^n]$.

As in the last example, we are often confronted with with a whole family of sets S_k where $k \geq 0$ is an integral parameter.

In this case we want an answer of the form

$$|S_k| = \dots k \dots$$

where the right hand side is some expression involving k.

Similarly we may have to contend with 2 or more parameters.

One would like a simple answer, using only basic arithmetic: sums, products, exponentials, factorials, binomials, logarithms, etc.

Ideally we want a closed form solution, not some recurrence (though finding a recurrence may be an important step).

As it turns out, we often need additional special functions such Fibonacci numbers, harmonic numbers, Stirling numbers, ...

Needless to say, to find nice solutions it is helpful to have a library of combinatorial identities: equations that reduce once counting problem to another.

Here is one interesting combinatorial principle for finite sets that is rather obvious, but still surprisingly useful in certain proofs.

Lemma (Pigeon Hole Principle (PHP))

For $m > n$, m pigeons will not fit into n pigeon holes.

Less informally:

There are no injections $[m] \to [n]$ when $m > n$.

Expressed this way, we can prove the PHP by induction.

It suffices to show the result for $m = n + 1$ (why?).
We use Induction on n.

Base case $n = 0$ is clear: $[0] = \emptyset$ but $[1] = \{1\}$.

Step $n > 0$: For the sake of a contradiction, suppose $f : [n+1] \to [n]$ is an injection.

Let $a = f(n+1)$, define a function $g : [n] \to [n-1]$ by

$$g(i) = \begin{cases} f(i) & \text{if } f(i) < a, \\ f(i) - 1 & \text{otherwise.} \end{cases}$$

It is easy to check that g is an injection.

But this contradicts the IH, done. □

Lemma

If m pigeons are placed into n pigeonholes, then at least one hole must contain more than $\lfloor \frac{m-1}{n} \rfloor$ pigeons.

If there were at most that many pigeons in all the holes their total number would be bounded by

$$n \cdot \lfloor \frac{m-1}{n} \rfloor \leq m - 1 < m,$$

contradiction.

For example, a group of 100 people must contain a subgroup of at least 9 people with the same birth month.

Application

Proposition

Let $A \subseteq [2n]$ *of size* $n+1$.
Then there exists $a, b \in A$ *such that* a *divides* b.

Proof.

Here is a trick: consider the odd part of a number: $a = 2^k \cdot a_0$.

For $a \in A$, the odd parts range over $1, 3, 5, \ldots, 2n-1$.

By PHP, there must be two elements in A with the same odd part:

$a = 2^k \cdot a_0$ and $b = 2^l \cdot a_0$.

Done. □

Try to do this without PHP. Let me know if you come up with some elegant argument.

Proposition

Choose n positive integers $a_1, \ldots, a_n$, not necessarily distinct.
Then there are $1 \leq r \leq s \leq n$ such that n divides $\sum_{i=r}^{s} a_i$.

Proof.

Consider the set of all partial sums

$$S = \left\{ \sum_{i=1}^{k} a_i \,\middle|\, k = 0, \ldots, n \right\}$$

Then S has size $n + 1$.

By the PHP, two partial sums must have the same remainder upon division by n.

But then their difference does the job.

□

Proposition (Erdős, Szekeres 1935)

Any sequence of $n^2 + 1$ distinct integers must contain an increasing subsequence of $n + 1$ terms, or a decreasing subsequence of $n + 1$ terms.

Proof.

Let $m = n^2 + 1$ and consider a sequence $x_1, x_2, \ldots, x_m$. Define

$$t_i = \text{length the longest inc. subsequence starting at } x_i$$

Assume $t_i \leq n$ for all i.

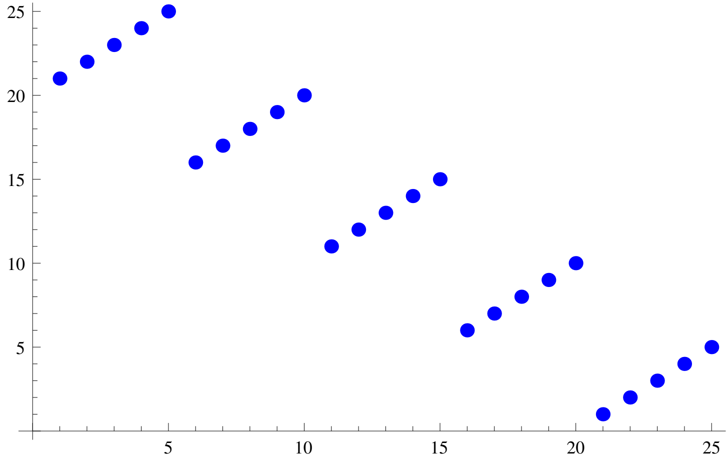
We have $m = n^2 + 1$ pigeons and n holes, so one hole must have at least $n+1$ pigeons: at least $n+1$ of the t_i's have the same value. Say, $I \subseteq [m]$, $|I| = n+1$ where $i \in I \implies t_i = t$.

But then the sequence $(x_i)_{i \in I}$ must be decreasing.

For otherwise $x_i < x_j$ for some $i < j \in I$ and we can prepend x_i to the increasing sequence starting at x_j.

But then $t < t_i$, contradiction.

$\square$


25
20
15
10
5
5
10
15
20
25

Note that PHP fails miserably when we have an infinite sequence of pigeon holes

$$h_0, h_1, h_2, \ldots, h_n, \ldots$$

We can fit $\mathbb{N} + 1$ pigeons in there:

holes	h_0	h_1	h_2	h_3	$\ldots$	h_n	$\ldots$
pigeons	q	p_0	p_1	p_2	$\ldots$	p_{n-1}	$\ldots$

Everybody just moves over by one hole.

Since there is no last hole (whose occupant would be kicked out) there is no problem. This device is also known as Hilbert's hotel.

How many ways can one rearrange the letters in "wedigmath" so that neither "we" nor "dig" nor "math" appears?

All letters are distinct, so there are $9!$ permutations of the letters. Let U be the collection of all these permutations.

Let A_1 be all words in U containing "we", A_2 all words containing "dig", and A_3 all words containing "math".

We want

$$|U| - |A_1 \cup A_2 \cup A_3|$$

But

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| \\ - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ + |A_1 \cap A_2 \cap A_3| \end{aligned}$$

$$
\begin{aligned}
|U| &= 9! \\
|A_1| &= 8! \\
|A_2| &= 7! \\
|A_3| &= 6! \\
|A_1 \cap A_2| &= 6! \\
|A_1 \cap A_3| &= 5! \\
|A_2 \cap A_3| &= 4! \\
|A_1 \cap A_2 \cap A_3| &= 3!
\end{aligned}
$$

Hence we get

$$9! - 8! - 7! - 6! + 6! + 5! + 4! - 3! = 317658$$

A key fact in the last example is that we can compute the cardinality of a union of 3 sets like so:

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| = {} & |A_1| + |A_2| + |A_3| \\ & - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ & + |A_1 \cap A_2 \cap A_3| \end{aligned}$$

Question: How does this generalize to $|A_1 \cup A_2 \cup \ldots \cup A_n|$?

It is more convenient to write all terms on one side, so we should expect a large, alternating sum involving intersections of k sets, for all $k = 0, \ldots, n$.

Lemma

Let $A = \{A_1, A_2, \ldots, A_n\}$ *and* $U = \bigcup A = A_1 \cup A_2 \cup \ldots \cup A_n$. *Then*

$$\sum_{B \subseteq A} (-1)^{|B|} \left| \bigcap B \right| = 0$$

Note that B here is a family of subsets of U, so $\bigcap B$ is a subset of U.

In particular $\bigcap \emptyset = U$.

In some texts you will find this written as

$$|U| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leq \ell_1 < \ell_2 < \ldots < \ell_k \leq n} |A_{\ell_1} \cap A_{\ell_2} \cap \ldots \cap A_{\ell_k}|$$

This is rank insanity.

First, the second sum is over all strictly increasing sequences $\ell_1 < \ell_2 < \ldots < \ell_k$ of length k in the range 1 to n.

This is a bit complicated and wholly unnecessary: in the sum term order does not matter. So, we might as well use a set instead of a sequence.

$$|U| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\beta \subseteq [n], |\beta| = k} |\bigcap_{i \in \beta} A_i|$$

Better.

But we can simplify further by collapsing the first two sums.

$$|U| = \sum_{\emptyset \neq \beta \subseteq [n]} (-1)^{|\beta|+1} \, |\bigcap_{i \in \beta} A_i|$$

This is already quite readable.

But we can do even better than this.

There is no need to sum over index sets, we can just sum over subsets of A directly.

$$|U| = \sum_{\emptyset \neq B \subseteq A} (-1)^{|B|+1} \, |\bigcap B|$$

Now one can actually understand the sum and a computer could read this, too.

End Rant

Define the characteristic function of $C \subseteq U$ to be

$$K_C(x) = \begin{cases} 1 & \text{if } x \in C, \\ 0 & \text{otherwise.} \end{cases}$$

Then $|C| = \sum_{x \in U} K_C(x)$ and we can rewrite the claim as

$$\sum_{B \subseteq A} (-1)^{|B|} \sum_{x \in U} K_{\bigcap B}(x) = 0.$$

We claim that the equation actually holds point-wise, for each $x \in U$.

Fix $x \in U$. We may safely assume that $x \in A_i$ for all i and we have

$$
\begin{aligned}
&\sum_{B \subseteq A} (-1)^{|B|} K_{\bigcap B}(x) \\
&= \sum_{k \leq n} (-1)^k \sum_{B \subseteq A, |B| = k} K_{\bigcap B}(x) \\
&= \sum_{k \leq n} (-1)^k \binom{n}{k} \\
&= 0
\end{aligned}
$$

by the binomial theorem.

As already indicated in the **Rant**, it is often convenient in applications to rewrite this identity as

$$|U| = \sum_{\emptyset \neq B \subseteq A} (-1)^{|B|+1} \left| \bigcap B \right|$$

A derangement is a permutation that leaves no element fixed.

Write D_n for the number of derangements of $[n]$.

For $i = 1, \ldots, n$ let

$$A_i = \text{permutations of } [n] \text{ that fix } i$$

and $A = \{A_1, \ldots, A_n\}$, $U = \bigcup A$.

Then $D_n = n! - |U|$, so we only need to use Inc/Exc to determine the last term.

$$
\begin{aligned}
|U| &= \sum_{\emptyset \neq B \subseteq A} (-1)^{|B|+1} \Big| \bigcap B \Big| \\
&= \sum_{k=1}^{n} (-1)^{k+1} \sum_{B \subseteq A, |B|=k} \Big| \bigcap B \Big| \\
&= \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)! \\
&= n! \sum_{k=1}^{n} (-1)^{k+1} / k!
\end{aligned}
$$

So $D_n = n! - n! \sum_{k=1}^{n} (-1)^{k+1}/k! = n! \sum_{k=0}^{n} (-1)^k / k!$

For large n, the fraction of derangements is about $1/e$.

How many integer solutions are there for

$$x_1 + x_2 + x_3 + x_4 = 40$$
$$0 \le x_i \le 15$$

First line of attack: determine the number of unconstrained solutions to the equation.

This can be interpreted as an occupancy problem: we have to place 40 (indistinguishable) balls into four (distinguishable) boxes. This sounds like a new problem, but isn't really.

For simplicity use 8 balls and 4 boxes:

$$\bullet\bullet|\bullet\bullet\bullet|\bullet|\bullet\bullet \qquad \to 2,3,1,2$$
$$\bullet\bullet|\bullet\bullet\bullet||\bullet\bullet\bullet \qquad \to 2,3,0,3$$
$$\bullet\bullet\bullet\bullet\bullet\bullet\bullet\bullet||| \qquad \to 8,0,0,0$$

Thus we are looking for all words over the alphabet $\{\bullet, |\}$ containing 40 $\bullet$'s and 3 $|$'s.

Writing $C(n, k)$ for the binomial coefficient we see that the unconstrained equation has

$$C(40 + 4 - 1, 4 - 1) = C(43, 3) = 12341$$

solutions $x = (x_1, x_2, x_3, x_4)$.

So far, so good. But we still must subtract "bad" solutions: that's where Inc/Exc comes in.

Define

$$A_i = \text{ solutions with } x_i \geq 16$$
$$A = \{A_1, A_2, A_3, A_4\}$$
$$U = A_1 \cup A_2 \cup A_3 \cup A_4$$

So U is the set of all bad solutions.

By Inc/Exc, we need to compute

$$|U| = \sum_{\emptyset \neq B \subseteq A} (-1)^{|B|+1} \Big| \bigcap B \Big|$$

But we can only have at most 2 bad x_i's in any bad solution x: otherwise we get a sum of at least 48.

Hence $\bigcap B = \emptyset$ for $|B| > 2$.

So, we only need to deal with $B = \{A_i\}$ and $B = \{A_i, A_j\}$.

By symmetry we get $4 \cdot C(27, 3)$ in the first case: there are four choices for i, but the value of i does not matter. Let's assume $i = 1$.

Think of placing 16 balls into x_1, and then distributing the remaining $24 = 40 - 16$ balls into the four boxes. There are $C(24 + 4 - 1, 4 - 1) = C(27, 3)$ ways of doing this.

In the second case we similarly obtain $6 \cdot C(11, 3) = 10710.$

So, the number of solutions is

$$12341 - (11700 - 990) = 1631.$$

Make sure you understand the details, this is a bit tricky.