Math 221 Winter 2023, Lecture 12: Enumeration

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wd`

4. An introduction to enumeration

Enumeration is a fancy word for counting – i.e., answering questions of the form "how many things of a certain type are there?". Here are some examples of counting problems:

- How many ways are there to choose 3 odd integers between 0 and 20, if the order matters (i.e., we count the choice $1, 3, 5$ as different from the choice $3, 1, 5$)? (The answer is 1000.)

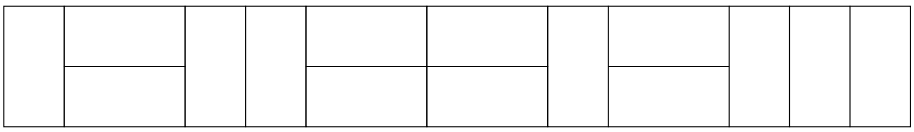
- How many ways are there to choose 3 odd integers between 0 and 20, if the order does not matter? (The answer is 220.)

- How many ways are there to choose 3 distinct odd integers between 0 and 20, if the order matters? (The answer is 720.)

- How many ways are there to choose 3 distinct odd integers between 0 and 20, if the order does not matter? (The answer is 120.)

- How many prime factorizations does 200 have (where we count different orderings as distinct)? (The answer is 10. This is a mix between a number theory problem and a counting problem.)

- How many ways are there to tile a 2×15-rectangle with dominos (i.e., rectangles of size 1×2 or 2×1) ? (The answer is 987. For instance, the tiling

  is one of these 987 ways.)

- How many addends do you get when you expand the product $(a + b)(c + d + e)(f + g)$? (The answer is 12.)

- How many different monomials do you get when you expand the product $(a - b)(a^2 + ab + b^2)$? (This one is more of an algebra problem, but I wanted to list it because it is connected to counting. The answer is 2, because $(a - b)(a^2 + ab + b^2) = a^3 - b^3$.)

- How many positive divisors does 24 have? (We can actually list them: 1, 2, 3, 4, 6, 8, 12, 24. This one is again a mix of a counting problem and a number theory problem.)

We will first solve a few basic counting problems informally, and then make the underlying concepts rigorous.

4.1. A refresher on sets

In prerequisite courses, you have seen basic properties of sets, and basic notations around sets, but let me quickly remind you of them.

Formally, the notion of a set is fundamental and cannot be defined.

Informally, a **set** is a collection of objects (which can be anything: numbers, matrices, functions or other sets) that knows which objects it contains and which objects it doesn't.

That is, if S is a set and p is any object, then S can either contain p (in which case we write $p \in S$) or not contain p (in which case we write $p \notin S$). There is no such thing as "containing p twice".

The objects that a set S contains are called the **elements** of S; they are said to **belong to** S (or **lie in** S, or **be contained in** S).

A set can be finite or infinite (i.e., contain finitely or infinitely many elements). It can be empty (i.e., contain nothing) or nonempty (i.e., contain at least one element).

An example of a set is the set of all odd integers. This is the set that contains each odd integer and no other objects. Generally, "the set of X" means the set that contains X and nothing else.

When a set is finite, it can be written by listing all its elements. For example, the set of all odd integers between 0 and 10 can be written as

$$\{1, 3, 5, 7, 9\}.$$

The braces { and } around the list are there to signal that we mean the set of all the elements, not the single elements themselves. These braces are called "set braces", and are involved in several different notations for sets.

Some more examples of finite sets are

$$\begin{aligned}
&\{1, 2, 3, 4, 5\}, \\
&\{1, 2\}, \\
&\{1\} \qquad \text{(this is the set that only contains 1)}, \\
&\{\} \qquad \text{(the empty set, also denoted } \varnothing), \\
&\{1, 2, \ldots, 1000\} \qquad \text{(you understand what " \ldots " means here)}.
\end{aligned}$$

Some infinite sets can also be written in this form:

$$\{1,2,3,\ldots\} \qquad (\text{this is the set of all positive integers}),$$
$$\{0,1,2,\ldots\} \qquad (\text{this is the set of all nonnegative integers}),$$
$$\{4,5,6,\ldots\} \qquad (\text{this is the set of all integers } \geq 4),$$
$$\{-1,-2,-3,\ldots\} \qquad (\text{this is the set of all negative integers}),$$
$$\{\ldots,-2,-1,0,1,2,\ldots\} \qquad (\text{this is the set of all integers}).$$

Some others cannot. For example, how would you list all the real numbers? Or even all the rational numbers?

Another way to describe a set is just by putting a description of its elements in set braces. For example:

$$\{\text{all integers}\} \qquad (\text{this is the set of all integers}),$$
$$\{\text{all integers between 3 and 9 inclusive}\},$$
$$\{\text{all real numbers}\}.$$

Often, you want to define a set that contains all objects of a certain type that satisfy a certain condition. For example, let's say you want the set of all integers x that satisfy $x^2 < 13$. There is a notation for this:

$$\left\{x \text{ is an integer} \mid x^2 < 13\right\}.$$

The vertical bar $\mid$ here should be read as "such that" (don't mistake it for a divisibility or absolute value bracket). The part before this bar says what type of objects you are considering (in our case, it is the integers x); the part after this bar imposes a condition (or several) on these objects (in our case, the condition is $x^2 < 13$). What you get is the set of all objects of the former type that satisfy the latter condition. For instance,

$$\begin{aligned} &\left\{x \text{ is an integer} \mid x^2 < 13\right\} \\ &= \{\text{all integers whose square is smaller than 13}\} \\ &= \{-3,-2,-1,0,1,2,3\}. \end{aligned}$$

Some authors write a colon (:) instead of the vertical bar $\mid$. Thus, they write $\{x \text{ is an integer} \mid x^2 < 13\}$ as $\{x \text{ is an integer} : x^2 < 13\}$.

Some sets have standard names:

$$\mathbb{Z} = \{\text{all integers}\} = \{\ldots,-2,-1,0,1,2,\ldots\};$$
$$\mathbb{N} = \{\text{all nonnegative integers}\} = \{0,1,2,\ldots\}$$
$$(\text{beware that some authors use } \mathbb{N} \text{ for } \{1,2,3,\ldots\} \text{ instead});$$
$$\mathbb{Q} = \{\text{all rational numbers}\};$$
$$\mathbb{R} = \{\text{all real numbers}\} \qquad (\text{you barely need them in this course});$$
$$\mathbb{C} = \{\text{all complex numbers}\} \qquad (\text{you don't need them in this course});$$
$$\varnothing = \{\} \qquad (\text{this is the empty set}).$$

Using these notations, we can rewrite

$$\left\{x \text{ is an integer} \ \mid \ x^2 < 13\right\} \qquad \text{as} \qquad \left\{x \in \mathbb{Z} \ \mid \ x^2 < 13\right\}.$$

Yet another way of defining sets is when you let a variable range over a given set and collect certain derived quantities. For example,

$$\left\{x^2 + 2 \ \mid \ x \in \{1, 3, 5, 7, 9\}\right\}$$

means the set whose elements are the numbers $x^2 + 2$ for all $x \in \{1, 3, 5, 7, 9\}$. Thus,

$$\begin{aligned} \left\{x^2 + 2 \ \mid \ x \in \{1, 3, 5, 7, 9\}\right\} &= \left\{1^2 + 2,\ 3^2 + 2,\ 5^2 + 2,\ 7^2 + 2,\ 9^2 + 2\right\} \\ &= \{3,\ 11,\ 27,\ 51,\ 83\}. \end{aligned}$$

In general, if S is a given set, then the notation

$$\{\text{an expression} \ \mid \ x \in S\}$$

stands for the set whose elements are the values of the given expression for all $x \in S$.

Some more examples of this:

$$\begin{aligned} \left\{\frac{x+1}{x} \ \mid \ x \in \{1, 2, 3, 4, 5\}\right\} &= \left\{\frac{1+1}{1}, \frac{2+1}{2}, \frac{3+1}{3}, \frac{4+1}{4}, \frac{5+1}{5}\right\} \\ &= \left\{2, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \frac{6}{5}\right\} \end{aligned}$$

and

$$\begin{aligned} \left\{x^2\%5 \ \mid \ x \in \mathbb{N}\right\} &= \left\{0^2\%5,\ 1^2\%5,\ 2^2\%5,\ 3^2\%5,\ 4^2\%5,\ 5^2\%5,\ 6^2\%5,\ \ldots\right\} \\ &= \{0,\ 1,\ 4,\ 4,\ 1,\ 0,\ 1,\ 4,\ 4,\ 1,\ 0,\ 1,\ 4,\ 4,\ 1,\ 0,\ \ldots\}. \end{aligned}$$

Note that the remainders $x^2\%5$ repeat every five steps, because every integer x satisfies $(x+5)^2 \equiv x^2 \bmod 5$ and thus $(x+5)^2\%5 = x^2\%5$ (by Proposition 3.3.15 in Lecture 9).

Let me stress once again that a set cannot contain an element more than once. Also, sets do not come with an ordering of their elements. Thus,

$$\{1, 2\} = \{2, 1\} = \{2, 1, 1\} = \{1, 2, 1, 2, 1\},$$

since each of these four sets contains 1 and 2 and nothing else. If S is a set and p is an object, then S either contains p or does not contain p; it cannot "contain p twice", nor can it contain an element "before" another. So when you write $\{2, 1, 1\}$, you aren't making a set that contains 1 twice; you are just saying twice that it contains 1, and this is equivalent to saying the same thing once. Likewise, the sets $\{1,2\}$ and $\{2,1\}$ do not "contain 1 and 2 in different orders"; you are just saying in different orders that they contain 1 and 2, but the meaning is the same. So

$$\left\{x^2\%5 \mid x \in \mathbb{N}\right\} = \{0,\ 1,\ 4,\ 4,\ 1,\ 0,\ 1,\ 4,\ 4,\ 1,\ 0,\ 1,\ 4,\ 4,\ 1,\ 0,\ \ldots\}$$
$$= \{0,\ 1,\ 4\}.$$

This is a finite set, even though $\mathbb{N}$ is infinite!

Sets can be compared and combined in several ways:

Definition 4.1.1. Let A and B be two sets.

(a) We say that A is a **subset** of B (and we write $A \subseteq B$) if every element of A is an element of B.

(b) We say that A is a **superset** of B (and we write $A \supseteq B$) if every element of B is an element of A. This is tantamount to saying $B \subseteq A$.

(c) We say that $A = B$ if the sets A and B contain the same elements. This is tantamount to saying that both $A \subseteq B$ and $A \supseteq B$ hold.

(d) We define the **union** of A and B to be the set

$$A \cup B := \{\text{all elements that are contained in } A \text{ or } B\}$$
$$= \{x \mid x \in A \text{ or } x \in B\}.$$

(The "or" is non-exclusive, as usual. So this includes the elements that are contained in both A and B.)

(e) We define the **intersection** of A and B to be the set

$$A \cap B := \{\text{all elements that are contained in both } A \text{ and } B\}$$
$$= \{x \mid x \in A \text{ and } x \in B\}.$$

(f) We define the **set difference** of A and B to be the set

$$A \setminus B := \{\text{all elements that are contained in } A \text{ but not in } B\}$$
$$= \{x \mid x \in A \text{ and } x \notin B\}.$$

This is also denoted by $A - B$ by certain authors.

(g) We say that A and B are **disjoint** if $A \cap B = \varnothing$ (that is, A and B have no element in common).

For example,

$$\begin{aligned}
\{1,3,5\} &\subseteq \{1,2,3,4,5\}, \\
\{1,2,3,4,5\} &\supseteq \{1,3,5\}, \\
\text{we } \textbf{don't} \text{ have } \{5,6,7\} &\subseteq \{1,2,3,4,5\}, \\
\{1,2,3\} &= \{3,2,1\}, \\
\{1,3,5\} \cup \{3,6\} &= \{1,3,5,3,6\} = \{1,3,5,6\}, \\
\{1,3,5\} \cap \{3,6\} &= \{3\}, \\
\{1,2,4\} \cap \{3,5\} &= \varnothing \qquad (\text{so that the sets } \{1,2,4\} \text{ and } \{3,5\} \text{ are disjoint}), \\
\{1,3,5\} \setminus \{3,6\} &= \{1,5\}, \\
\mathbb{Z} \setminus \mathbb{N} &= \{-1,-2,-3,\ldots\} = \{\text{all negative integers}\}.
\end{aligned}$$

Definition 4.1.2. Several sets $A_1, A_2, \ldots, A_k$ are said to be **disjoint** if any two of them (not counting a set and itself) are disjoint, i.e., if we have $A_i \cap A_j = \varnothing$ for all $i < j$.

For example, the three sets $\{1,2\}$, $\{5\}$ and $\{0,7\}$ are disjoint.

4.2. Counting, informally

Now, let us see how the elements of a set can be counted. Formally speaking, we will define "counting" later, so we will play around with not-quite-rigorous concepts for now. As long as we are working with finite sets, your intuitive understanding of "counting" should not mislead you.

For example, the set of all odd integers between 0 and 10 has 5 elements (1, 3, 5, 7, 9), and this doesn't change if you write it redundantly as $\{1,3,5,5,5,5,7,9\}$. In other words, there are 5 odd integers between 0 and 10.

More generally, I claim:

Proposition 4.2.1. Let $n \in \mathbb{N}$. Then, there are exactly $(n+1)\,//2 = \left\lfloor \dfrac{n+1}{2} \right\rfloor$ odd integers between 0 and n (inclusive).

Informal proof. The equality $(n+1)\,//2 = \left\lfloor \dfrac{n+1}{2} \right\rfloor$ follows from Proposition 3.3.13 in Lecture 8. It remains to show that there are exactly $\left\lfloor \dfrac{n+1}{2} \right\rfloor$ odd integers between 0 and n. (We shall always understand the word "between" to be inclusive, so that n itself is counted if n is odd.)

We prove this by induction on n:

Base case: For $n = 0$, the claim is true, because there are $0 = \left\lfloor \dfrac{0+1}{2} \right\rfloor$ odd integers between 0 and 0.

Induction step: Let n be a positive integer. Assume (as the induction hypothesis) that the claim is true for $n-1$. That is, assume that there are exactly $\left\lfloor \frac{n}{2} \right\rfloor$ odd integers between 0 and $n-1$. We must show that the claim also holds for n, i.e., that there are exactly $\left\lfloor \frac{n+1}{2} \right\rfloor$ odd integers between 0 and n.

Let me introduce a shorthand: The symbol "#" shall mean "number". Thus, our induction hypothesis says

$$(\text{# of odd integers between 0 and } n-1) = \left\lfloor \frac{n}{2} \right\rfloor, \tag{1}$$

and our goal is to prove that

$$(\text{# of odd integers between 0 and } n) = \left\lfloor \frac{n+1}{2} \right\rfloor.$$

We are in one of the following two cases:

Case 1: The number n is even.

Case 2: The number n is odd.

Let us consider Case 1 first. In this case, n is even. Thus, n is not odd. Therefore, the odd integers between 0 and n are precisely the odd integers between 0 and $n-1$ (since the extra integer n does not qualify as odd). Hence,

$$\begin{aligned}
&(\text{# of odd integers between 0 and } n) \\
&= (\text{# of odd integers between 0 and } n-1) \\
&= \left\lfloor \frac{n}{2} \right\rfloor \qquad (\text{by (1)}).
\end{aligned} \tag{2}$$

However, $n+1$ is odd (since n is even), and thus $2 \nmid n+1$. Therefore, Corollary 3.3.17 **(b)** in Lecture 9 (applied to 2 and $n+1$ instead of d and n) yields $\left\lfloor \frac{n+1}{2} \right\rfloor = \left\lfloor \frac{(n+1)-1}{2} \right\rfloor = \left\lfloor \frac{n}{2} \right\rfloor$. Comparing this with (2), we find

$$(\text{# of odd integers between 0 and } n) = \left\lfloor \frac{n+1}{2} \right\rfloor.$$

Thus, we have achieved our goal in Case 1.

Let us now consider Case 2. In this case, n is odd. Thus, the odd integers between 0 and n are precisely the odd integers between 0 and $n-1$ along with the new odd integer n. Hence,

$$\begin{aligned}
&(\text{# of odd integers between 0 and } n) \\
&= (\text{# of odd integers between 0 and } n-1) + 1 \\
&= \left\lfloor \frac{n}{2} \right\rfloor + 1 \qquad (\text{by (1)}).
\end{aligned} \tag{3}$$

However, $n+1$ is even (since n is odd), and thus $2 \mid n+1$. Therefore, Corollary 3.3.17 **(a)** in Lecture 9 (applied to 2 and $n+1$ instead of d and n) yields $\left\lfloor \dfrac{n+1}{2} \right\rfloor = \left\lfloor \dfrac{(n+1)-1}{2} \right\rfloor + 1 = \left\lfloor \dfrac{n}{2} \right\rfloor + 1$. Comparing this with (3), we find

$$(\text{\# of odd integers between 0 and } n) = \left\lfloor \frac{n+1}{2} \right\rfloor .$$

Thus, we have achieved our goal in Case 2.

So the goal has been achieved in either case, and the induction step is complete. This proves Proposition 4.2.1. □

Note: We called the above proof "informal" because we still don't have a rigorous definition of the size of a set (i.e., of what "the number of" means). But we will soon see such a definition. Once we have learnt this definition and its basic properties, the above proof will become a formal proof with trivial changes.

Incidentally, let me state the formula for the number of integers (not just odd integers) in a given interval:

Proposition 4.2.2. Let $a, b \in \mathbb{Z}$ be such that $a \leq b+1$.

Then, there are exactly $b-a+1$ numbers in the set $\{a,\ a+1,\ a+2,\ \ldots,\ b\}$. In other words, there are exactly $b-a+1$ integers between a and b (inclusive).

Informal proof. This is intuitively obvious and can be rigorously proved by induction on b. □

The hard part about Proposition 4.2.2 is not the proof, but rather remembering the "+1"! If your intuition comes from calculus, you think of the interval $[a,b]$ as having length $b-a$ (if $b \geq a$). But since we are doing discrete mathematics, we are computing not the geometric length of this interval, but rather the number of integers on this interval, including both endpoints; and this number is 1 larger than the length. (For example, if $a = b$, then the geometric interval $[a,b]$ has zero length, but it contains one integer, namely a.)

It is also worth saying that if two integers a and b satisfy $a \leq b-1$, then there are exactly $b-a-1$ integers between a and b exclusive (meaning that we count neither a nor b).

Convention 4.2.3. We agree to use the symbol "#" for "number".

4.3. Counting subsets

4.3.1. Counting them all

Now, let us count something less trivial than numbers.

How many subsets does the set $\{1, 2, 3\}$ have? These subsets are

$$\{\}, \quad \{1\}, \quad \{2\}, \quad \{3\},$$
$$\{1,2\}, \quad \{1,3\}, \quad \{2,3\}, \quad \{1,2,3\}.$$

(Yes, every set A satisfies $A \subseteq A$ and $\{\} \subseteq A$.) Thus, there are 8 subsets of $\{1, 2, 3\}$ in total.

Likewise,

- there are 4 subsets of $\{1, 2\}$, namely $\{\}, \{1\}, \{2\}, \{1,2\}$.
- there are 2 subsets of $\{1\}$, namely $\{\}$ and $\{1\}$.
- there is 1 subset of $\{\}$, namely $\{\}$.
- there are 16 subsets of $\{1, 2, 3, 4\}$.

The pattern here is hard to miss:

Theorem 4.3.1. Let $n \in \mathbb{N}$. Then,

$$(\text{\# of subsets of } \{1, 2, \ldots, n\}) = 2^n.$$

Informal proof. We induct on n.

The *base case* ($n = 0$) is easy: The set $\{1, 2, \ldots, 0\}$ is empty, and thus its only subset is $\{\}$ itself; hence, the # of subsets of $\{1, 2, \ldots, 0\}$ is $1 = 2^0$.

Induction step: We proceed from $n - 1$ to n. Thus, let n be a positive integer. We assume (as the induction hypothesis) that Theorem 4.3.1 holds for $n - 1$ instead of n, and we set out to prove that it holds for n.

So our induction hypothesis says that

$$(\text{\# of subsets of } \{1, 2, \ldots, n-1\}) = 2^{n-1}.$$

Our goal is to prove that

$$(\text{\# of subsets of } \{1, 2, \ldots, n\}) = 2^n.$$

We define

- a **red set** to be a subset of $\{1, 2, \ldots, n\}$ that contains n;
- a **green set** to be a subset of $\{1, 2, \ldots, n\}$ that does not contain n.

For example, if $n = 3$, then the red sets are

$$\{3\}, \qquad \{1,3\}, \qquad \{2,3\}, \qquad \{1,2,3\},$$

whereas the green sets are

$$\{\}, \qquad \{1\}, \qquad \{2\}, \qquad \{1,2\}.$$

Each subset of $\{1,2,\ldots,n\}$ is either red or green, but not both. Hence,

$$(\text{\# of subsets of } \{1,2,\ldots,n\}) = (\text{\# of red sets}) + (\text{\# of green sets}).$$

(This is an instance of a basic counting principle: If some objects are classified into two types, then we can count these objects by counting the objects of each type and adding the results. Later we will state this as a rigorous theorem, called the **sum rule for two sets**.)

Thus it remains to count the red sets and the green sets separately.

The green sets are easy: They are just the subsets of $\{1,2,\ldots,n-1\}$. Hence,

$$(\text{\# of green sets}) = (\text{\# of subsets of } \{1,2,\ldots,n-1\}) = 2^{n-1}$$

(by the induction hypothesis).

Counting the red sets is trickier, but we can reduce the problem to counting the green sets: Indeed, the red sets are just the green sets with the element n inserted into them. To be more precise: Each green set can be turned into a red set by inserting n into it[1]. Conversely, each red set can be turned into a green set by removing the element n from it. These two operations are mutually inverse, and thus set up a one-to-one correspondence between the green sets and the red sets.[2] This reveals that the # of red sets is the # of green sets. Thus,

$$(\text{\# of red sets}) = (\text{\# of green sets}) = 2^{n-1}.$$

Combining what we have shown, we now obtain

$$\begin{aligned}(\text{\# of subsets of } \{1,2,\ldots,n\}) &= \underbrace{(\text{\# of red sets})}_{=2^{n-1}} + \underbrace{(\text{\# of green sets})}_{=2^{n-1}} \\ &= 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n.\end{aligned}$$

This is precisely what we needed to prove. This completes the induction step, and thus Theorem 4.3.1 is proved. □

[1] For example, if $n = 3$, then the green set $\{2\}$ becomes $\{2,3\}$ in this way.

[2] For instance, for $n = 3$, it looks like this:

green set	$\{\}$	$\{1\}$	$\{2\}$	$\{1,2\}$
	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
red set	$\{3\}$	$\{1,3\}$	$\{2,3\}$	$\{1,2,3\}$

.