1 Counting

We want to be able to determine the cardinalities of sets defined by their descriptions. This is an important tool to compute probabilities, to estimate resources needed by algorithms, and has many other applications in combinatorics and in Computer Science.

We present two almost trivial principles that underline many of these computations. Rosen calls them the Sum Rule and the Product Rule for finite sets.

Fact 1 (Sum Rule). Let $A, B$ be disjoint sets. Then $|A \cup B| = |A| + |B|$

In reality, this is a special case of a theorem from Chapter 2 of Rosen:

Theorem 2 (Inclusion-Exclusion). Let $A, B$ be finite sets. Then $|A \cup B| = |A| + |B| - |A \cap B|$

Fact 1 is the case of $A, B$ disjoint.

Fact 3 (Product Rule). Let $A, B$ be finite sets. Then $|A \times B| = |A| \cdot |B|$

Recall that the Cartesian Product of sets $A$ and $B$, $|A \times B|$ is the set of ordered pairs $\{(a, b) : a \in A, b \in B\}$ The definition extends to Cartesian products of $n$ sets.
These simple rules underly many of the techniques for counting. For example, it is clear that the number of binary strings of length $n$ is $2^n$ since they are the $n$-fold Cartesian product of the set $B = \{0, 1\}$ of cardinality 2. (Another proof: they represent the number from 0 to $2^n - 1$ in binary.)

1.1 Applications

What is important is to use these simple tools to count all kinds of things. First, let us consider (modern) auto plates for passenger cars in Illinois.

1.1.1 Counting Plates

A simplified version of the rule for possible plate numbers is the following:

let $a$ denote an (uppercase) letter, and $n$ a decimal digit. Modern formats include

1. $aa\Box nnnn$ ($\Box$ denotes whitespace)
2. $aaa\Box nnn$
3. $ann\Box nnn$
4. $annn\Box nnn$
5. $ann\Box nnnn$
6. $aan\Box nnnn$

The first letter cannot be an M, U, or W. Note that all $n$s must be digits, so for example AA 53 is not a valid instance of scheme 1, while AA 0053, and AA 5300 both are (and are different license plates.)

It seems that it is also the case that the last letter in a grade sequence of two or more letters cannot be an O or an I (because they can be confused with a 0 and a 1 respectively.)

Now let’s count the number of possible plates in each category:

1. $(26 - 3) \cdot (26 - 2) \cdot 10^4$
2. $(26 - 3) \cdot 26 \cdot (26 - 2) \cdot 10^3$
3. $(26 - 3) \cdot 10^5$
4. \((26 - 3) \cdot 10^6\)

5. \((26 - 3) \cdot 10^6\)

6. \((26 - 3) \cdot (26 - 2) \cdot 10^5\)

EXERCISE: compute this. How many more numbers would one get if one added an extra letter at the end?

1.1.2 Permanent Calendars

If January first starts on a Monday in two different years, then January 2nd will be a Tuesday, January 10th a Wednesday in both years. So it seems that one could get away with just 7 different printed calendars (and a PostIt \(\copyright\to\) indicate the year.) This is almost correct: we need to account for leap years, so we need 14 calendars. EXERCISE: If you started in 1938, which calendar was used the most?

1.1.3 Other examples

The number of 1:1 functions \(A \rightarrow B\) where \(|A| = m\) and \(|B| = n\), with \(n \geq m\) is \(n(n - 1) \cdots (n - m + 1)\)

If 3 people, say A, B and K go to a beerfest where 10 brewers offer 4 varieties of beer from each brewery, and they decide that no two of them will try a beer from the same brewery, how many choices do they have for the first round of beer?

Answer:
A will have \(4 \times 10 = 40\) choices
B will have \(40 - 4 = 36\) choices
K will have \(40 - 8 = 32\) choices.
The number of possibilities is \(40 \times 36 \times 32 = 46,080\)

How many passwords are there, if passwords can have 6, 7, or 8 characters, are composed of lower case letters or digits, and must have at least one digit?

Answer: It is clear that what we want to do is to solve the 6-character problem first: the solutions for 7 and 8 characters should be similar, and we can use the Sum Rule to add the cardinalities of the 3 subsets (Why? How do we know the subsets are disjoint?)
A first attempt to count the 6-character passwords is to fix the position of the mandatory digit (there are 6 possible positions, and 10 possible choices for the choice of the digit) and then argue that the other 5 positions can be any of 36 characters (26 letters + 10 digits), which yields $36^5$ strings, and a total of $60 \times 36^5$ passwords.

This is obviously wrong – there are only $36^6$ strings of 6-character words, and passwords of length 6 are a subset.

(What was our mistake?)

A simple correct argument counts the total number of strings ($36^6$) then subtracts the number of invalid strings of length 6. The latter are the strings that do not contain a digit. There are $26^6$ of those.

So the number of passwords is $36^6 - 26^6 + 36^7 - 26^7 + 36^8 - 26^8$

Exercise: compute this value. How many years does it take to break into a system protected by such passwords, if you can try a guessed password every 15 sec? What if you have a parallel machine with 64 processors, each running the algorithm? What if you had the encrypted passwords of a million users?

2 The Pigeonhole Principle

The pigeonhole principle is simply the assertion that if you have $k$ boxes and $k+1$ objects to be put in the boxes, than there will be a box with more than 1 object in it. The ‘pigeonhole’ name comes from applying the definition to the case where the boxes are pigeonholes, and the objects, pigeons.

A more mathematical formulation:

**Theorem 4.** Let $f$ be a function $f : A \rightarrow B$ with $|A| = n + 1$ and $|B| = n$. Then $f$ is not 1-1.

It is easy to prove this by induction on $n$ (Do it!)

It should be clear that this formalization is equivalent to the intuitive description above.

There is an easy generalization:

**Theorem 5.** If we want to put $O$ objects in $B$ boxes, we’ll have a box with $\geq \lceil \frac{O}{B} \rceil$ objects.
For example, if we want to put 7 objects in 3 boxes, we’ll have to put at least 3 in some box, since if we put 2 or less, we can take care of at most 6 objects.

There are some simple applications:

- In a group of 8 people, two will have their birthday on the same day of the week
- Among 27 English words, there are two that start with the same letter
- In a course where grades can be 0, 1, 2, \cdots 10, among 12 students, two will have the same grade
- If you grab 4 single socks from a drawer that has white, black, and red socks, you will have a pair with matching colors
- Consider standard playing cards (4 suits, 13 cards in each suit.) If you draw 9 cards, your are guaranteed to get 3 of the same suit (but if you want 3 of a particular suit, say hearts, you may need to draw 42 cards.)

We can answer some less obvious questions. For example, how many area codes are needed to accommodate 25 million users (in North America)?

Phone numbers obey the following scheme (NANP): a phone number is of the form

\[(a_1a_2a_3)\ o_1o_2o_3\ s_1s_2s_3s_4\]

where the \(a_1a_2a_3\) is the area code, \(o_1o_2o_3\) is the office code (a remainder of the time where neighborhoods had their own exchanges [google PEnnsylvania 6-5000 for a use of the office code in popular culture] – earlier the scheme was 2 letters, each denoting a number – P was 7, E was 3), and the final 4 digits are the station code. There are restrictions on the digits allowed: the first and the fourth digit cannot be a 0 or a 1 in the \(o_1o_2o_3 - s_1s_2s_3s_4\) part. The number of such phone numbers is \(8 \times 10^2 \times 8 \times 10^6 = 6.4 \times 10^9\). We need at least 4 different area codes to come up to 25 million distinct phone numbers. (This is Example 8 in Rosen)

Your parents may remember a time when all Chicago had area code 312. Now you know why there are 773 and 872 area codes! (Some people and companies were upset with the change.) For a short history of Illinois area codes, see

\[https://en.wikipedia.org/wiki/List\ of\ Illinois\ area\ codes\]