Basic Combinatorics

Readings: 4-1, 4-3, 5-4, 5-5
Next: 4-3, 5-4
After: 4-6, 4-7

Change of plan. No homework due next tuesday. This week's material will be lightly covered on exam. pset out thursday, due week after quiz.

1 Introduction

The next lectures will present methods for *counting* the number of elements in various sets. Counting is one of the most important concepts of discrete math. The subject called *combinatorics*.

Counting arises in many different ways:

Examples: Counting addresses, keys
How many phone numbers are available for use in the U.S.? Internet addresses? 200-digit primes for RSA cryptography?

Example: Measurement for programs
Counting amount of time, memory, disk space, etc., used by programs.

Example: Programs that enumerate and test
Some programs solve problems by enumerating all candidate solutions and trying them all. To see which is best (optimization problem), or just to try to find some solution.

Operations research optimization problems: travelling salesman problem, etc.
Dynamic programming – a clever method for cutting down the search space.
Circuit testing, by trying all inputs.
Finite-state program verification, by testing all reachable states.

It's nice to know how many candidates there are, so we know how long to expect the program to run. Also, counting methods often yield ways of explicitly *enumerating* the elements, so that you can use the enumeration in the program.

Example: Probability
We want to know the probability that some event happens when some system or program

operates. The probability of an event is closely related to the number of ways that event might happen. Calculating probabilities is based on counting number of ways.

You all understand counting informally. Recall that it's actually a very formal notion, based on *bijections*:
A set A has size (cardinality) n if and only if there is a bijection from A to the set $\{1, \ldots, n\}$. To prove this, we don't always exhibit a bijection directly to $\{1, \ldots, n\}$; or sometimes, show a bijection to another set B, which we already know is of size n. This uses the fact that two sets have the same cardinality if and only if there is a bijection between them.

Often counting arguments look quite informal, but we can always formalize them in terms of bijections.

Combinatorics contains a very large number of formulas to help in counting, and it's impossible to learn them all. The key is to learn the basics, then look up or derive the other formulas when you need them.

The complicated formulas can all be proven formally using algebra. Many of them can also be understood informally, using what we will call a *thought experiment*. This involves giving an intuitive meaning to the expressions on the left-hand side (LHS) and right-hand side (RHS) of an equation, then verifying that these two meanings are the same.

2 Basic Counting Principles

Start with the basic counting principles:
Sum rule, inclusion-exclusion principle, product rule, case analysis, division rule.

2.1 Sum

Theorem 2.1 If A and B are disjoint, then $|A \cup B| = |A| + |B|$.

This expresses the idea as an equation, which we will prove formally in terms of bijections.

We can also understand it by a "thought experiment":
The LHS denotes the number of ways of choosing an element of $A \cup B$,
The RHS denotes the number of ways of choosing an element of A plus the number of ways of choosing an element of B.
Since the sets are disjoint, the LHS is the sum...(informal)

Proof. Let $n_A = |A|$, $n_B = |B|$.
This means that there are bijections f_A and f_B, f_A from A to $\{1, \ldots, n_A\}$, f_B from B to $\{1, \ldots, n_B\}$.
We want a bijection from $A \cup B$ to $\{1, \ldots, n_A + n_B\}$.

So define a function g on $A \cup B$ by:

$$g(a) = \begin{cases} f_A(a) & \text{if } a \in A \\ n_A + f_B(a) & \text{if } a \in B \end{cases}$$

The function g is well-defined since A and B are disjoint.
We must show that g is a bijection, so we must prove it's one-to-one and onto.

One-to-one:
Suppose that $g(a) = g(b)$.
If $a, b \in A$ then $g(a) = f_A(a) = f_A(b) = g(b)$; since f_A is one-to-one, we have $a = b$.
If $a, b \in B$ then $g(a) = n_A + f_B(a) = n_A + f_B(a) = g(b)$; so $f_B(a) = f_B(b)$; since f_B is one-to-one, we again have $a = b$.
If $a \in A$, $b \in B$ (wlog), then $g(a) \leq n_A$ and $g(b) > n_A$; contradiction.

Onto:
Let $n \in \{1, \ldots, n_A + n_B\}$.
If $n \leq n_A$ then $n = f_A(a)$ for some $a \in A$, since f_A is onto; so $n = g(a)$.
If $n > n_A$, then $n = n_A + m$ for some $m \in \{1, \ldots, n_B\}$; then $m = f_B(b)$ for some $b \in B$, since f_B is onto; so $g(b) = n_A + f_B(b) = n_A + m = n$.
Therefore, g is a bijection, as needed. ■

Recall that any bijection has an inverse function.
Inverse here is a function from $\{1, \ldots, n_A + n_B\}$ to $A \cup B$:

$$g^{-1}(n) = \begin{cases} f_A^{-1}(n) & \text{if } n \leq n_A \\ f_B^{-1}(n - n_A) & \text{if } n > n_A \end{cases}$$

In fact, note that a function has an inverse if and only if it is a bijection. Therefore, showing that a function has an inverse is another way of showing that it is a bijection. Here, define the inverse function, show it's defined everywhere, and well-defined.

Example 1 99 math majors, 179 CS majors,
How many majors in math or CS (assume no double majors)?
99 + 179 = 278

Extend sum rule to any number of sets:

Theorem 2.2 If $A_1, \ldots, A_n$ are pairwise disjoint, then $|A_1 \cup \ldots \cup A_n| = |A_1| + |A_2| + \ldots + |A_n|$.

Proof by induction on n.

Example 2 99 math, 179 CS, 24 philosophy
Total in math or CS or philosophy = 302

2.2 Inclusion-Exclusion

What if the sets aren't disjoint? E.g., math and CS majors, where some people are majoring in both?

Consider two sets first:

Theorem 2.3 If A and B are any sets (not necessarily disjoint), then $|A \cup B| = |A| + |B| - |A \cap B|$.

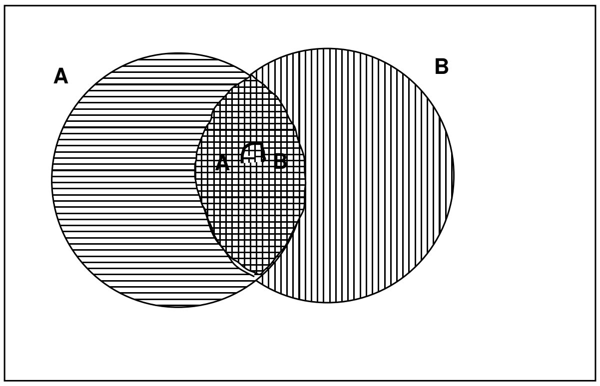

Figure 1: Venn diagram.

Proof. Use Theorem 2.1, for disjoint sets.
Note that

$$\begin{aligned} A \cup B &= (A - B) \cup (A \cap B) \cup (B - A) \\ A &= (A - B) \cup (A \cap B) \\ B &= (B - A) \cup (A \cap B) \end{aligned}$$

and that all these are expressed as disjoint unions (can prove by set theory, obvious by venn diagram). Thus, by disjoint sum rule,

$$\begin{aligned} |A \cup B| &= |A - B| + |A \cap B| + |B - A| \\ |A| &= |A - B| + |A \cap B| \\ |B| &= |B - A| + |A \cap B| \end{aligned}$$

subtracting second and third equation from first gives result. ∎

Example 3 99 math majors, 179 CS majors, 7 majoring in both.
How many majors in math or CS?
99 + 179 - 7 = 271

Example 4 How many numbers in $\{1, \ldots, 100\}$ are divisible by 2 or 5?

- 50 divisible by 2
- 20 divisible by 5
- 10 divisible by both 2 and 5
- total: $50 + 20 - 10 = 60$.

What about more than two sets?
What is $|A \cup B \cup C|$, in general?

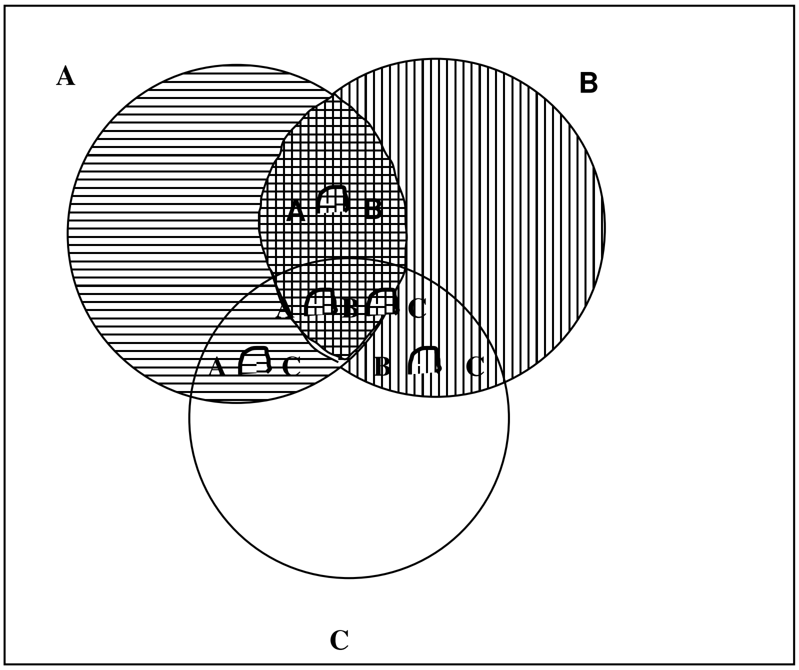

Figure 2: Venn diagram.

Well, $|A \cup B \cup C| = |A| + |B| + |C|$ minus something for the overlapping part. What should we remove for the overlapping part? We counted each 2-overlapped part twice, and the 3-overlapped part 3 times. Suppose we subtract $|A \cap B| + |B \cap C| + |A \cap C|$. Now we're counting the 2-overlapped parts only once, as we want, but the 3-overlapped part isn't counted at all! So need to correct again, this time by *adding* in $|A \cap B \cap C|$, The full expression:

Theorem 2.4 $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |B \cap C| + |A \cap C|) + |A \cap B \cap C|$.

Example 5 99 math, 179 CS, 24 philosophy
math and CS: 7 (includes someone in all 3 also)

math and philo: 12
CS and philo: 2
all 3: 1
Total in math or CS or philosophy = $(99 + 179 + 24) - (7 + 12 + 2) + 1 = 282$.

In general, for m sets, alternate plus and minus terms:

Theorem 2.5 $|\cup_i A_i| = \Sigma_i |A_i| - \Sigma_{i,j \text{ distinct}} |A_i \cup A_j| + \Sigma_{i,j,k \text{ distinct}} |A_i \cup A_j \cup A_k| - \ldots + (-1)^{m+1} |\cap A_i|$

Can be proved by induction on the number of sets (we'll see this later). We'll come back to this Thursday, with a "thought experiment" proof.

Example 6 How many primes less than 100?
99 minus numbers divisible by $2, 3, 5$ or 7 (since non-prime means divisible by some prime $< \sqrt{100}$) plus these 4 numbers. Let

$$P_i = \text{numbers divisible by } i$$

note $|P_i| = \lfloor 100/i \rfloor$.

Then quantity is:

$$\begin{aligned}
99 \;\; - \;\; & \lfloor \frac{100}{2} \rfloor - \lfloor \frac{100}{3} \rfloor - \lfloor \frac{100}{5} \rfloor - \lfloor \frac{100}{7} \rfloor \\
+ \;\; & \lfloor \frac{100}{2 \cdot 3} \rfloor + \lfloor \frac{100}{2 \cdot 5} \rfloor + \lfloor \frac{100}{2 \cdot 7} \rfloor + \lfloor \frac{100}{3 \cdot 5} \rfloor + \lfloor \frac{100}{3 \cdot 7} \rfloor + \lfloor \frac{100}{5 \cdot 7} \rfloor \\
- \;\; & \lfloor \frac{100}{2 \cdot 3 \cdot 5} \rfloor - \lfloor \frac{100}{2 \cdot 3 \cdot 7} \rfloor - \lfloor \frac{100}{2 \cdot 5 \cdot 7} \rfloor - \lfloor \frac{100}{3 \cdot 5 \cdot 7} \rfloor \\
+ \;\; & \lfloor \frac{100}{2 \cdot 3 \cdot 5 \cdot 7} \rfloor
\end{aligned}$$

which is

$$99 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 - 3 - 2 - 1 - 0 + 0 = 21$$

so there are 25 primes.

2.3 Product

Theorem 2.6 If A and B are any sets, then $|A \times B| = |A| \cdot |B|$.

Thought experiment:
LHS represents the number of ways of choosing a pair consisting of an element of A and an element of B.
RHS represents number of ways to choose an element of A, multiplied by number of ways to choose an element of B.
If there are n_A ways to choose an element of A, and n_B ways to choose an element of B, then there are $n_A \cdot n_B$ ways to choose a pair.

Proof. Let $n_A = |A|$, $n_B = |B|$.
Let f_A be a bijection from A to $\{0, \ldots, n_A - 1\}$, f_B from B to $\{0, \ldots, n_B - 1\}$.
These exist since these sets are the same size as the corresponding sets starting at 1.
We want a bijection from $A \times B$ to $\{0, \ldots, n_A \cdot n_B - 1\}$.
Define by:

$$g(a, b) = n_B(f_A(a)) + f_B(b)$$

We can show that g is a bijection with inverse:

$$g^{-1}(n) = (f_A^{-1}(\lfloor \frac{n}{n_B} \rfloor), f_B^{-1}(n \bmod n_B)).$$

In other words, for any $n \in \{0, \ldots, n_A \cdot n_B - 1\}$, write $n = qn_B + r$,
where $0 \leq r < n_B$, by division theorem.
Then

$$g^{-1}(n) = (f_A^{-1}(q), f_B^{-1}(r)).$$

■

Example 7 How many ways can you choose 2 courses in different subjects from among 5 Math, 7 CS, and 10 EE courses?

- 1 Math and 1 CS: $5 \times 7 = 35$ ways (product rule)
- 1 Math and 1 EE: $5 \times 10 = 50$ ways
- 1 CS and 1 EE: $7 \times 10 = 70$ ways.

By sum rule, total of 155 ways.

Extend to m sets:

Theorem 2.7 $|A_1 \times A_2 \times \ldots \times A_m| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_m|$

This says that m successive choices, with exactly n_k choices possible at the k^{th} step, can produce a total of exactly $n_1 n_2 \cdots n_m$ different results.

Example 8 How many binary numbers of length n?
By product rule, $2 \times \ldots \times 2$ (n terms). So 2^n.

Example 9 Number of subsets of n-element set?
We already know this is 2^n. Each subset corresponds to a bit string of length n, with a 1 in position k meaning that the kth element is in the subset. That is, set of subsets has bijection to set of bit strings of length n, which has 2^n elements.

Example 10 License plates – 3 letters followed by 3 digits: $26 \times 26 \times 26 \times 10 \times 10 \times 10$.

Example 11 Number of passwords – length 8, letters and digits, at least one letter.
First calculate number of length 8 strings of letters and digits, counting those with no letters: 36^8.
Then subtract those with no letters: 10^8.
The difference is what's needed: $36^8 - 10^8$.

Example 12 How many functions from set A with m elements to set B with n elements?
Function corresponds to m choices from B, one for each element of A.
That is, set of functions has bijection to set $B \times \ldots \times B$ (m terms).
This set has size n^m, by the product rule.

Example 13 How many length-n palindromes over $\{0, 1\}$?
Turns out exactly $2^{\lceil n/2 \rceil}$.

Proof. We consider the cases n even and odd separately.

- If n is even we define a bijection from the set $\{0, 1\}^{n/2}$ to the set of palindromes of length n. This will imply that there are $|\{0, 1\}^{n/2}| = 2^{n/2}$ palindromes. For a sequence $a = (a_1, \cdots, a_{n/2})$ define $f(a) = (a_1, \cdots, a_{n/2}, a_{n/2}, \cdots, a_1)$. Clearly, $f(a)$ is a palindrome and f is bijective.
- if n is odd, we define a bijection from the set $\{0, 1\}^{\lceil n/2 \rceil}$ to the set of palindromes of length n. This will imply that there are $|\{0, 1\}^{\lceil n/2 \rceil}| = 2^{\lceil n/2 \rceil}$ palindromes. For a sequence $a = (a_1, \cdots, a_{\lceil n/2 \rceil})$ define $g(a) = (a_1, \cdots, a_{\lceil n/2 \rceil}, \cdots, a_1)$. Clearly, $g(a)$ is a palindrome and g is bijective.

Hence, in either case there are $2^{\lceil n/2 \rceil}$ palindromes. ∎

2.4 Case Analysis and its Tree Representation

If we interpret product rule in terms of number of successive choices, and can represent the successive choices by tree, then the total number of choices is the number of leaves.

Example 14 Bit strings of length 3: Draw tree

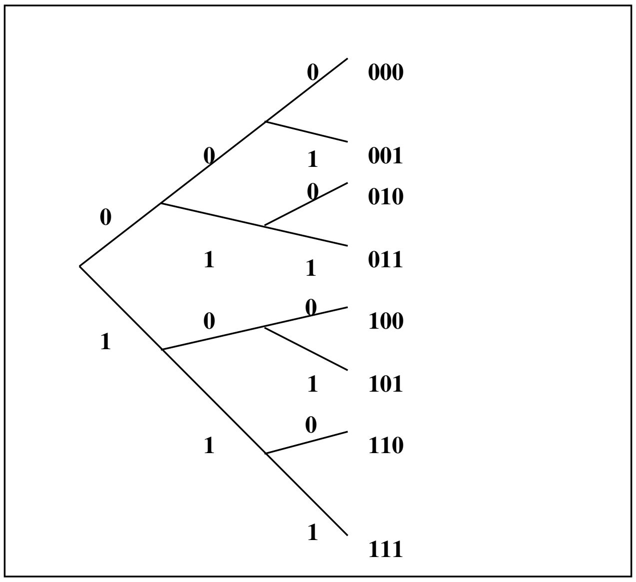

Figure 3: Tree of choices

Note that the tree is a kind of recursive sum rule: the top level is summing over possible first bits, etc.

This tree representation can also be used to count the numbers of successive choices. In the more general case, the choices come from different sets, depending on the results of the earlier choices. In this case the answer isn't a product, but it can still be calculated from the number of leaves of the tree.

Example 15 3 blue shirts, 2 red shirts, 1 green shirt, 2 grey pants and 3 brown pants. How many outfits if grey matches red/blue and brown matches red/green?

- 6 blue-grey, 4 red-grey, 6 red-brown and 3 green-brown makes 19.
- Alternatively, the tree of outcomes may be represented as below (See Fig. 1):

Example 16 Number of strings of letters of length 5, with no repeated letters:
$26 \times 25 \times 24 \times 23 \times 22$.
Show as tree, with later sets depending on earlier choices.

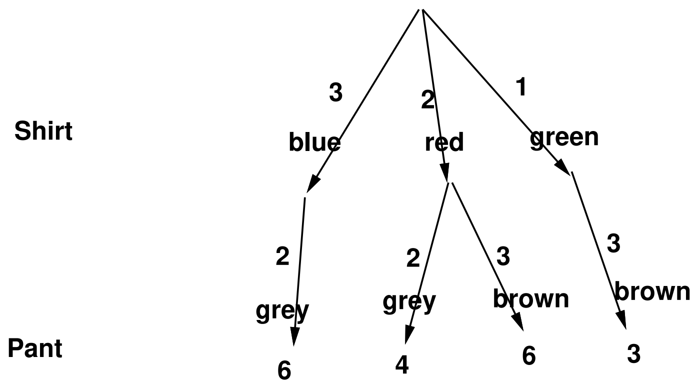

Figure 4: Tree of outcomes.

2.5 Division Rule

One last basic rule: division rule:

Theorem 2.8 If there is a k to 1 mapping from A to B, and $|A| = n$, then $|B| = n/k$.

Example 17 How many subsets of size 2 are there, of a 5-element set A?
Let S be this set of subsets.

First, consider the set P of ordered pairs without repeats. We have $|P| = 5 \times 4$ (since elements can't repeat – consider a tree).

There's a 2 to 1 mapping from P to S – just ignore the order.
So S has $20/2 = 10$ elements.

2.6 A Remark on "Distinct Ways"

Counting problems are often formulated as "how many distinct ways can you..." and this is a somewhat tricky notion. "Distinct" means whatever the poser of the problem wants it to mean. In the clothing example above, I assumed that the 2 red shirts were

distinct. I could have formulated a question asking only about distinct color combinations of clothes—then the answer would be 4, even though the experiment (picking clothes) would be the same.

3 Permutations and Combinations

Some of the examples we have seen (like the last one) deal with the number of ways of choosing some particular number of elements from a set. As you can see in this last example, there are two different ways to select them: in a particular order, or just in an (unordered) set. Selections are called *permutations* when we care about the order, and *combinations* when we don't.

3.1 Permutations

Definition 3.1 An r-*permutation* of a set of n elements is an ordered arrangement of r of the n elements (all distinct).

Example 18 $S = \{A, B, C\}$. The 2-permutations are $(A, B), (B, A), (A, C), (C, A), (B, C), (C, B)$.

There are 6 2-permutations

How many r-permutations of a set of n elements?

- n ways to choose the first element
- given first choice, $n - 1$ ways to choose the second element
- $n - 2$ to choose the third element
- overall:

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

Denote this by $P(n, r)$.

Definition 3.2 A *permutation* of n elements is an n-permutation of them.

$P(n, n) = n!$

Example 19 How many ways can n people stand in a circle?

- Map each permutation to a ring.
- There are n permutations mapped to each ring.
- By the division rule, the number of rings is $n!/n = (n - 1)!$.

3.2 Combinations

Definition 3.3 An r*-combination* of a set of n elements is an (unordered) subset of the n elements.

Example 20 $S = \{A, B, C\}$. The 2-combinations are $\{A, B\}, \{A, C\}, \{B, C\}$. There are 3 of them.

How many r-combinations of a set of n elements?

- Map each r-permutation to an r-combination by ignoring the order.
- How many r-permutations mapped to each r-combination? $r!$ - because there are $P(r, r) = r!$ permutations of a given r-combination.
- By division rule, $P(n, r)/r!$

We denote this by $C(n, r)$, or more commonly as $\binom{n}{r}$.

Theorem 3.4 The number of r-combinations of an n-set is:

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

$\binom{n}{r}$ is called a *binomial coefficient* for reasons that will become clear later.

Example 21 How many ways can 3 distinct numbers be chosen from $1, \ldots, 10$?

This is $\binom{10}{3} = \frac{10!}{3!7!} = 120$.

Example 22 How many ways can 3 distinct numbers be chosen from $1, \ldots, 10$ so that their sum is divisible by 3?

- $A = \{3, 6, 9\}$ $(= 0 \bmod 3)$
- $B = \{1, 4, 7, 10\}$ $(= 1 \bmod 3)$
- $C = \{2, 5, 8\}$ $(= 2 \bmod 3)$

Need sum to be zero mod 3. If any two are equal mod3, then the third must also be equal. So they are all same or all different. Thus the possibilities are:

- 3 from A: $\binom{3}{3} = 1$.

- 3 from B: $\binom{4}{3} = 4$.
- 3 from C: $\binom{3}{3} = 1$.
- One from each: $3 \cdot 4 \cdot 3 = 36$ (product rule).

Total: 42.