Lecture 16: Counting Methods

Reading: 7.2, 11.1 - 11.4, 11.10

Goal: Develop tools for counting one set by another

Applications in probability, proofs

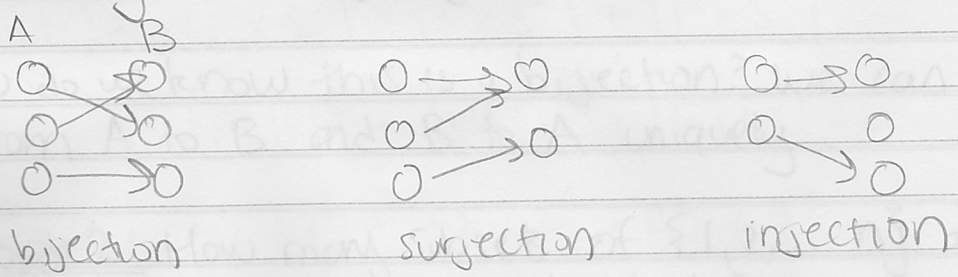
---

def A function $f: A \to B$ is bijection if

surjective (1) for all $b \in B$, there is an $a \in A$ with $f(a) = b$

injective (2) for all $a_1 \neq a_2 \in A$, $f(a_1) \neq f(a_2)$

Pictorially



bijection surjection injection

Bijection Rule: If there is a bijection, $f: A \to B$ then $|A| = |B|$

Recall if $A_1, A_2 \ldots A_n$ are sets then

$$A_1 \times A_2 \times \ldots \times A_n$$

is the set of all sequences $a_1, a_2 \ldots a_n$ where each $a_i \in A_i$

Product Rule: $|A_1 \times A_2 \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$

Example: How many subsets of $\{1, 2, \dots n\}$ are there?

Let's count by bijection

A (subsets)		B (binary strings)
ϕ	→	0 0 .. 0 0
$\{1\}$	→	0 0 .. 0 1
$\{1, 2 \dots n\}$	→	1 1 .. 1 1

$|B| = 2 \cdot 2 \cdot 2 \dots \cdot 2 = 2^n$
(product rule)

Hence $|A| = 2^n$ by bijection rule

How do we know this is a bijection? We can go from A to B and B to A uniquely

Example 2: How many subsets of $\{1, 2, \dots n\}$ are there that either contain both 1 & 2 or neither?

A (subsets) (valid)
ϕ
$\{1, 2\}$
$\{3\}$
$\{1, 2 \dots n\}$

B (binary strings)

1	2	3	...	n
0	0		...	0
1	0		...	0
0	1		...	0
1	1		...	1

$|A| = |B| = 2^{n-1}$

Sum Rule: If $A_1, A_2, \ldots A_n$ are disjoint then

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \ldots + |A_n|$$

Example 3: Passwords are length 6–8
start with a letter (upper or lower case)
rest are letters or digits

How many passwords are there?

Let $F = \{a, b, \ldots z, A, B, \ldots Z\}$
$S = \{a, b, \ldots z, A, B, \ldots Z, 0, 1, \ldots 9\}$

$$P = (F \times \underbrace{S \times S \ldots \times S}_{5}) \cup (F \times \underbrace{S \times S \ldots \times S}_{6}) \cup (F \times \underbrace{S \times S \ldots S}_{7})$$

Thus $|P| = |F \times S^5| + |F \times S^6| + |F \times S^7|$

$$= |F||S|^5 + |F||S|^6 + |F||S|^7$$

$$= 52 \cdot 62^5 + 52 \cdot 62^6 + 52 \cdot 62^7$$

Application: to security (show xkcd comic)

Generalized Product Rule: Let S be length k sequences

- n_1 possible first entries
- n_2 possible second entries for each first entry
- n_3 possible third entries for each first, second entry
- ⋮

then $|S| = n_1 \cdot n_2 \cdot n_3 \ldots \cdot n_k$

Example 4: Permutations of $\{1, 2, 3 \ldots k\}$
(sequence where every i appears once)

$$|S| = k(k-1)(k-2)\ldots 1 \triangleq k!$$

e.g. $(3, 2, k, \ldots 4)$

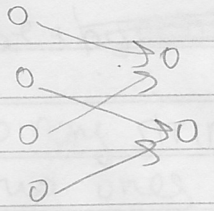
Example 5: Defective dollar bills: 8-digit serial number repeats a digit

What fraction are nondefective?

$$\text{fraction nondefective} = \frac{10 \cdot 9 \cdot 8 \ldots 3}{10^8} \leq 0.019$$

Division Rule: If $f: A \to B$ is d-to-1 then $|A| = d|B|$

e.g.

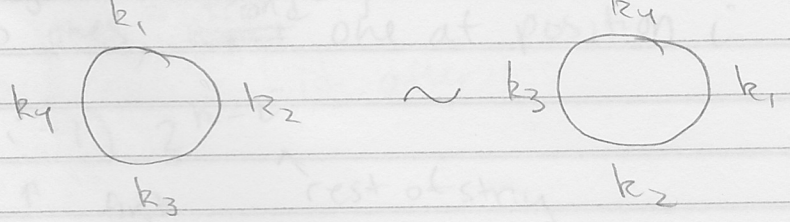


2-to-1

Example 6: Knights of the round table

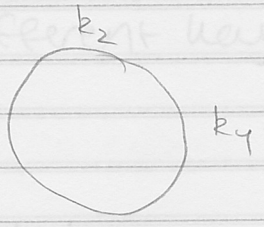
How many ways are there to seat n knights, where we consider seatings that differ by rotation as equivalent?

e.g.



Let A = permutations of knights
B = seating arrangements

Then (k_2, k_4, k_1, k_3) →
(k_4, k_1, k_3, k_2) →
(k_1, k_3, k_2, k_4) →
(k_3, k_2, k_4, k_1) →



Function is 4-to-1 (more generally n-to-1), thus

$$n! = |A| = n\,|B|$$

thus $|B| = (n-1)!$

Challenging Example: Prove $\sum_{i=1}^{k} (i-1)\,2^{k-i} = 2^k - k - 1$

We will use a ~~bijection~~ combinatorial proof:

A = binary strings of length k with at least two ones

From sum rule, $|A| = 2^k - k - 1$

- 2^k: all strings
- k: strings with a single one
- 1: no one

A_i = binary strings of length k with at least two ones, ~~first~~ second one at position i

$|A_i| = (i-1)\,2^{k-i}$

- $(i-1)$: where is first ~~second~~ one?
- 2^{k-i}: rest of string

boolloc c // arbitrary

Again by sum rule, $|A| = |A_1| + |A_2| \dots |A_k|$

Thus l.h.s and r.h.s are two different ways of counting same set

---

Pigeon Hole Principle: If $|A| > |B|$ then for any function $f: A \to B$, there are $a_1 \neq a_2 \in A$ with $f(a_1) = f(a_2)$

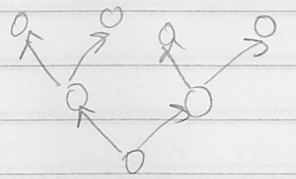
Why is this called the pigeon hole principle?

Simple, but powerful consequences

- There are two (non-bald) people in NYC with the same number of hairs on their head
  ($\leq$ 500k hairs, $\geq$ 8m people)
- Impossible to losslessly compress every length k file to a shorter file

$$f: \{0,1\}^k \to \{0,1\}^\ell \quad \text{for } \ell < k$$

- Your family tree is not a tree



4000 years
$\leq 10^{12}$ people

assume: noone has a child after 100

But $2^{40} > 10^{12}$