Massachusetts Institute of Technology | Handout 36
6.042J/18.062J: Mathematics for Computer Science | October 24, 1995
Professors David Karger and Tom Leighton

Notes 13

1 Counting

1.1 Motivation

How many phone numbers are available for use in the U.S.? How about IP addresses? Why does this matter?

How many different 200-digit primes are available for RSA cryptography?

Counting is probably the most important concept of discrete mathematics. It arises in many ways:

Measurement, We need to count the amount of time, memory, or disk space used by a computer program

Resource allocation. How many people/machines are needed to handle all the different possibilities...

Enumeration Many programs are essentially solving a problem in a pretty dumb way: enumerate all candidate solutions, and see which one is best (cleverness comes in figuring out how to restrict the space of candidate solutions). We'd like to know how many candidates there are, so we know how long to spend (also, a counting technique often gives an enumeration technique). e.g. circuit testing: how many inputs do we have to try?

Probability is just another kind of counting using a "normalizing factor." The probability of an event is tied up with the number of ways for that event to happen.

Counting is a very formal process but can often be disguised to look quite informal. Formally, counting is about bijections:

- Two sets have the same cardinality if there is a bijection between them
- A set has cardinality n if it has a bijection to $\{1, \ldots, n\}$.
- We count a set by showing a bijection to a set of known size.

One of the properties of counting is very large numbers of formulas. It is impossible to remember all of them. The key is to learn the principles, so the formulas can be rederived as necessary.

A special kind of *combinatorial proof* based on "thought experiments" is used frequently.

1.2 Rules of Sum and Product

1.2.1 Sum

Theorem 1.1 *If A and B are disjoint, then $|A \cup B| = |A| + |B|$.*

This can be rephrased in "thought experiment" language as: if there are n_A ways to choose an element of A and n_B ways to choose an element from B,. then there are $n_A + n_B$ ways to choose an element from A or B.

Proof. Let f be a bijection from A to $\{1, \ldots, n_A\}$, g from B to $\{1, \ldots, n_B\}$. Then define a function h on $A \cup B$ by

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

The function h is well-defined since A and B are disjoint. It is easy to see that h is a bijection with the inverse being

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

Since h is a bijection from $A \cup B$ to $\{1, \ldots, n_A + n_B\}$ we get that if A and B are disjoint, then $|A \cup B| = |A| + |B|$. ∎

1.2.2 Product

Theorem 1.2 $\|A \times B\| = \|A\| \cdot \|B\|$.

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 an element of $A \times B$.

Proof. Let f be a bijection from A to $\{1, \ldots, n_A\}$, g from B to $\{1, \ldots, n_B\}$. Then define a function h on $A \times B$ by

$$h((a, b)) = n_B(f(a) - 1) + g(b)$$

It is easy to see that h is a bijection with the inverse being

$$h^{-1}(n) = (f^{-1}(\lfloor \frac{n-1}{n_B} \rfloor + 1), g^{-1}((n - 1 \bmod n_B) + 1)).$$

Since h is a bijection from $A \times B$ to $\{1, \ldots, n_A \cdot n_B\}$ we get that $\|A \times B\| = \|A\| \times \|B\|$. ∎

Example 1 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.

How about any two books: pick first book 22 ways, next 21 ways, total of 462 ways.

Formally, what is going on here? We are counting via a thought experiment involving a sequence of choices:

1. give a choosing rule
2. show it's a bijection by showing each outcome results from exactly one choice sequence
3. count number of choice sequences, to get number of outcomes.

The sequence of branching choices yields a tree of outcomes.

Theorem 1.3 *r successive choices, with exactly n_k choices possible at the k^{th} step, can produce a total of exactly $n_1 n_2 \cdots n_r$ different results.*

Example 2 I have 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 3 How many binary numbers of length n? $T(1) = 2$. By product rule, $T(n) = 2T(n-1)$. So $T(n) = 2^n$.

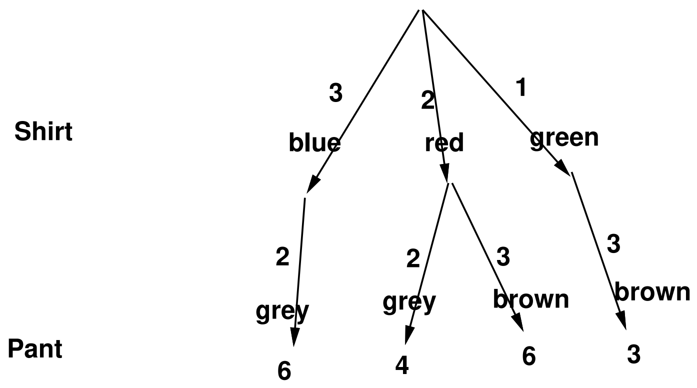

Figure 1: Tree of outcomes.

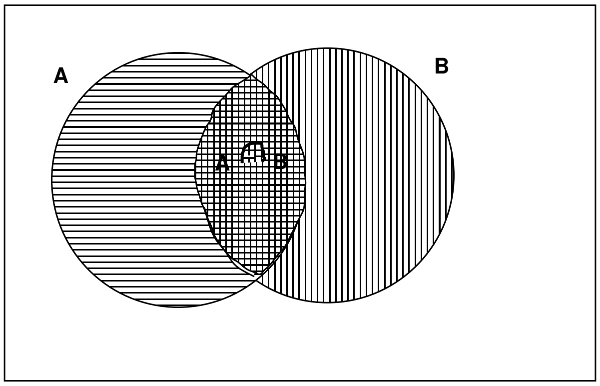

Figure 2: Venn diagram.

1.3 Inclusion Exclusion

$\|A \cup B\| = \|A\| + \|B\| - \|A \cap B\|$.

See Fig. 2.

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

1.4 Division Rule

If there is a k to 1 mapping from a set of size n to a set S, then S has n/k elements.

Example 5 How many length-n palindromes? We claim there are exactly $2^{\lceil n/2 \rceil}$ palindromes of length n over the alphabet $\{0, 1\}$.

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 will 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 Permutations and Combinations

There are two ways to select some elements of a group. Permutations apply when we care about the order of selection, combinations when we don't.

2.1 Permutations

An *r-permutation* of a set of n elements is an ordered arrangement of r of the n elements.

E.g. $S = \{A, B, C\}$. 2-permutations are $(A, B), (B, A), (A, C), (C, A), (B, C), (C, B)$.

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

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

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

A *permutation* of n elements is an n-permutation of them. $P(n, n) = n!$.

Example 6 How many ways can N people stand in a circle?

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

2.2 Combinations

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

E.G $S = \{A, B, C\}$ has 2-combs $\{A, B\}, \{A, C\}, \{B, C\}$.

How many r-combinations of an n-set?

- map each r-permutation to an r-combination by "unordering"
- 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, $C(n, r) = P(n, r)/r!$

Theorem 2.1 *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 7 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.