DM 551 Lecture 1 2/9 2021

6.1 Basic counting

why interesting for CS?

- determine # solutions to a problem
- complexity of algorithms
- list all subjects with given properties
- passwords

$$\boxed{\text{Product rule}: |A_1 \times A_2 \times \dots \times A_k| = \prod_{i=1}^{k} |A_i|}$$

In words: If a procedure can be broken into a sequence of k tasks such that there are n_i ways to perform task i, then there are $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ ways to do the procedure

Example 3 32 computers each with 24 ports
Find # of different ports in total

$A_1 = \{\text{computers}\}$ $A_2 = \{\text{ports}\}$

$(i,j) \sim$ port j on computer i

$$|A_1 \times A_2| = |A_1| \cdot |A_2| = 32 \cdot 24 = 768$$

Example 4 Find # of bit strings of length n

$A_i = \{0,1\}$ $i = 1, 2, \ldots, n$

$|A_1 \times A_2 \times \ldots \times A_n| = 2^n$

Example 6 # of functions $f: A \to B$ when $|A| = m$, $|B| = n$

Each of the m elements of A can map to any of the n elements of B so with

$A_i = \{$ possible images of element $i \}$ we have

$|A_i| = n$ and hence

Number of functions $= |A_1 \times A_2 \times \ldots \times A_n| = n^m$

Example 7 # of 1-1 functions $f: A \to B$ when $|A| = m$, $|B| = n$

Recall: f is 1-1 if $f(x) = f(y) \Rightarrow x = y$

Case 1 $m > n$: no solution (see next section pigeonhole principle)

Case 2 $m \le n$:

Say $A = \{a_1, a_2, \ldots, a_m\}$, then there are

n choices of image for a_1

$n-1$ —— " —— a_2

$\vdots$

$n-i+1$ a_i

So there are $n \cdot (n-1) \cdot \ldots (n-m+1) = \dfrac{n!}{(n-m)!}$

1-1 functions from A to B

Example 10 Number of subsets of an n-set A ($|A|=n$)

NB: This only depends on the size of A, not the type of elements!

$A = \{a_1, a_2, \dots, a_n\}$

There is a 1-1 correspondance between subsets of A and bit strings of length n:

$b_1 b_2 \cdots b_i \cdots b_n$ where $b_i = 1 \iff a_i \in A' = A'(b)$

We saw that there are 2^n bitstrings of length n so there are 2^n subsets of an n-set

$\emptyset \sim 000\cdots0$

$\{a_1\} \sim 1000\cdots0$

$\vdots$

$A \sim 1111\cdots1$

$$\boxed{\text{Sum rule} \quad A_1 \cap A_2 = \emptyset \Rightarrow |A_1 \cup A_2| = |A_1| + |A_2|}$$

In words: If a task can be done in either one of n_1 ways or in one of n_2 ways, where none of the n_1 ways is the same as one of the n_2 ways, then there are $n_1 + n_2$ ways to do the task

Example 12 Need a person for a committee

should be either a math faculty or $n_1 = 37$ such
a math student $n_2 = 83$ such

Then # choices is $37 + 83 = 120$

Generalized sum rule: If $A_i \cap A_j = \emptyset$ $\forall i \neq j$ then
$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|$$

Proof: by induction on n

$n = 2$ is the sum rule

- assume formula holds for $n-1$ sets satisfying the condition and let $C = A_1 \cup \dots \cup A_{n-1}$
- Then $C \cap A_n = \emptyset$ as $A_i \cap A_n = \emptyset$ so the

sum rule gives $|A_1 \cup A_2 \cup \dots \cup A_n| = |C \cup A_n| = |C| + |A_n|$

$$= |A_1| + \dots + |A_{n-1}| + |A_n| \qquad \square$$

Example 16 Passwords of length 6, 7 or 8 characters

Rules (i) each character $\in$ {uppercase letter} or {digit}

(ii) at least one digit

passwords $P = P_6 + P_7 + P_8$ P_i = # of pw of length i

↑

by the sum rule

Finding P_6 : difficult if we try different places for digits as we may double count! :(

instead count bad pw of length 6 (only uppercase letters)

By product rule there are 26^6 such pw

By product rule there are 36^6 strings of length 6

So $P_6 = 36^6 - 26^6$

similarly $P_7 = 36^7 - 26^7$ $P_8 = 36^8 - 26^8$

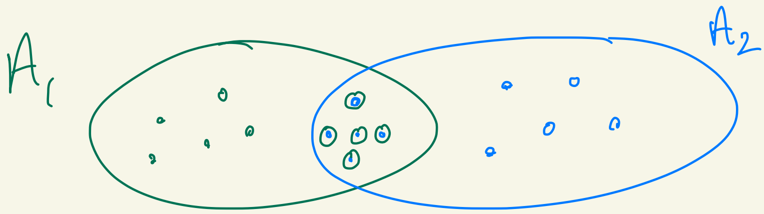
so $P = (36^6 - 26^6) + (36^7 - 26^7) + (36^8 - 26^8)$

Exact number NOT important here!

Inclusion-exclusion principle: $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

$\quad\quad\quad\quad\quad \|$

subtraction rule



$\odot$ counted twice in $|A_1| + |A_2|$

Example 18 # bitstrings of length 8 of the form

$1a_2 \ldots a_8$ or $a_1 a_2 \ldots a_6 00$

$A_1 = \{1a_2a_3 \ldots a_8 \mid a_i \in \{0,1\}, i = 2, \ldots 8\}$ $\quad |A_1| = 2^7 = 128$

$A_2 = \{a_1a_2 \ldots a_6 00 \mid a_i \in \{0,1\}, i = 1, \ldots 6\}$ $\quad |A_2| = 2^6 = 64$

$A_1 \cap A_2 = \{1a_2a_3 \ldots a_6 00 \mid a_i \in \{0,1\}\ i = 2, 3, \ldots 6\}$ $\quad |A_1 \cap A_2| = 2^5 = 32$

So $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 128 + 64 - 32 = 160$

Example 19 350 applicants for position

220 are CS majors $\quad A_1$

147 are business majors $\quad A_2$

51 are both CS and business majors $\quad A_1 \cap A_2$

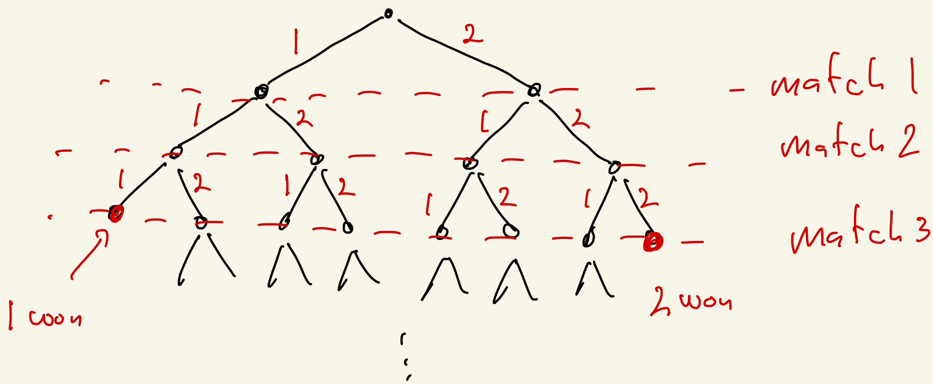
$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 220 + 147 - 51 = 316$

So $350 - |A_1 \cup A_2| = 350 - 316 = 34$ are neither CS major or business major

Tree diagrams (count using trees)

- branches at vertex = possible choices
- leaves = possible outcomes

Example: best of 5 game between two teams



see Figure 5 page 416.

6.2 The pigeonhole principle

Theorem 1 If k+1 objects are placed in k boxes then at least one box will have more than one element

proof (by contradiction)

suppose no box has more than 1 element, then there are at most $k \cdot 1 = k$ objects in total $\rightarrow \Leftarrow$

Theorem 2 If we place N objects in k boxes then some box has at least $\lceil \frac{N}{k} \rceil$ objects

proof (by contradiction)

suppose $\leq \lceil \frac{N}{k} \rceil - 1$ in each then

$$N = \#\text{object} \leq k \cdot \left(\lceil \tfrac{N}{k} \rceil - 1 \right) < k\left(\left(\tfrac{N}{k} + 1 \right) - 1 \right) = N \quad \rightarrow \Leftarrow$$

Example 4 For every integer n there exist integer k so that kN has only 0's and 1's in its decimal expansion

How to show this using

php = pigeonhole principle?

Given n consider the $n+1$ numbers with decimal representations

$$1, \quad 11, \quad 111, \quad \ldots, \quad \overbrace{111\cdots1}^{n+1}$$

$$N_1 \quad N_2 \quad N_3 \qquad\qquad N_{n+1}$$

There are only n remainders with respect to division by n $(0, 1, 2, \ldots n-1)$

PHP $\Rightarrow \exists\, i \neq j$ s.t. $i < j$ and

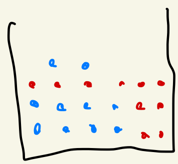
$$N_j \bmod n = N_i \bmod n$$

$$\Updownarrow$$

$$N_j - N_i = k \cdot n \text{ for some integer } k$$

and $N_j - N_i = \overbrace{11\cdots1}^{j-i}\overbrace{00\cdots0}^{i}$

Example (not in book)



A box contains 10 red and 10 blue balls
How many balls must we select to be sure to have at least 3 balls with the same colour?

Answer think of having two boxes B, R

and drop each red/blue ball picked up in R/B

If no box has at least 3, then we have taken at most $2 \times 2 = 4$ balls. 5 is the smallest N such that

$\left\lceil \frac{N}{2} \right\rceil \geq 3$ NB: the number of red/blue balls played no role

Example 11 $a_1, a_2, \dots, a_{n+1} \in \{1, 2, \dots, 2n\}$

$\Downarrow$

$\exists\, a_i, a_j$ such that a_i divides a_j

Proof Each integer a_i can be written as $a_i = 2^{k_i} q_i$

when q_i is an odd number

So $q_1, q_2, \dots q_{n+1}$ are all odd and there are only

n odd numbers in $\{1, 2, \dots, 2n\}$

By php we have $q_i = q_j$ for some pair $i \neq j$

without loss of generality $k_i \le k_j$ so we have

$a_i = 2^{k_i} \cdot q_i$ and $a_j = 2^{k_i} \cdot 2^{k_j - k_i} q_i$ so a_i divides a_j

$n+1$ is best possible:

if we let $a_i = n+i$ for $i = 1, 2, \dots, n$

then we have n numbers $a_1, a_2 \dots a_n \in \{1, 2, \dots, 2n\}$

so that no number divides another.

Example 12' (not same numbers as in book)

The sequence $3, 7, 1, 2, 4, 10, 11, 8, 12$

contains $a_{i_1}, a_{i_2}, a_{i_3}, a_{i_4}$ with $i_1 < i_2 < i_3 < i_4$

such that $a_{i_1} < a_{i_2} < a_{i_3} < a_{i_4}$ increasing sequence

But no sequence of four $j_1 < j_2 < j_3 < j_4$ s.t

$a_{j_1} > a_{j_2} > a_{j_3} > a_{j_4}$

Theorem Every sequence of n^2+1 distinct

real numbers $a_1, a_2, \ldots a_{n^2+1}$

contains $a_{i_1}, a_{i_2}, \ldots, a_{i_n}$ s.t $i_1 < i_2 < \ldots < i_n$

and either $a_{i_1} < a_{i_2} < \ldots < a_{i_n}$

or $a_{i_1} > a_{i_2} > \ldots > a_{i_n}$

Proof

let i_k = length of longest increasing sequence starting from a_k

$$a_k < \bigcirc < \bigcirc < \bigcirc < \cdots < \bigcirc$$

and d_k = length of longest decreasing sequence starting at a_k

$$a_k > \bigcirc > \bigcirc > \bigcirc \cdots \bigcirc$$

If the claim is false then for all $k \in \{1, 2, \dots n^2+1\}$ all the pairs (i_k, d_k) satisfy that $i_k, d_k \in \{1, 2, \dots, n\}$

There are n^2+1 such pairs so $\exists\, p, q$ s.t. $(i_q, d_q) = (i_p, d_p)$ where we can assume that $p < q$

If $a_p < a_q$ then $i_p > i_q$ $\rightarrow\leftarrow$

$$a_p < a_q < \bigcirc < \bigcirc \cdots < \bigcirc$$

If $a_p > a_q$ then $d_p > d_q$ $\rightarrow\leftarrow$

$$a_p > a_q > \bigcirc > \bigcirc > \cdots > \bigcirc$$

n^2+1 is best possible when $n = 2$:

5, 4, 7, 6 no $\nearrow$ length 3

no $\searrow$ length 3

Example 13 Ramsey theory

Given 6 persons which are pairwise either friends or enemies. There are always 3 persons who are all friends or 3 persons who are all enemies

proof represent as a coloured complete graph on 6 vertices

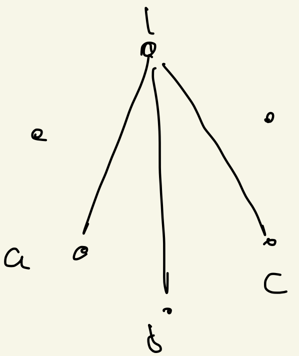
a o——o b = a and b are friends

a o——o b = a and b are enemies

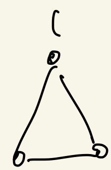
Fix person 1 and look at relation to persons 2,3,4,5,6

By php there are 3 persons among 2,3,4,5,6 who are all friends or all enemies with person 1

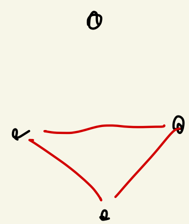
Without loss of generality we have



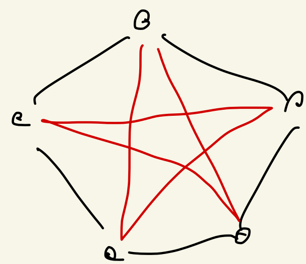
so either we get



or



6 is best possible:



6.3 Permutations and Combinations

r-permutation of an n-set S: pick r distinct elements $a_1 a_2 \dots a_r$ from S when the order matters

$P(n,r) = \#$ r-permutations of an n-set

$$\boxed{P(n,r) = n\cdot(n-1)\cdot \dots \cdot (n-r+1) = \frac{n!}{(n-r)!}}$$

<u>proof</u>: by product rule we have

n choices for a_1

$n-1$ — " — a_2

$\vdots$

$n-r+1$ - - - a_r $\square$.

Note $P(n,0)=1$ as there is exactly one way to choose 0 elements namely take the empty set

r-combination of an n-set S: pick r distinct elements $a_1 a_2 \dots a_r$ from S when order does not matter

$C(n,r) = \#$ r-combinations of an n-set

$$\boxed{C(n,r) = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}}$$

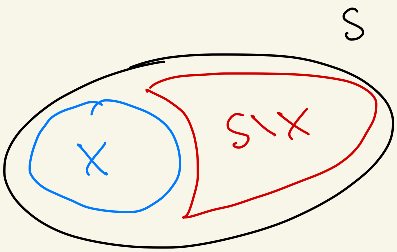
<u>proof</u> Each fixed r-permutation can be obtained from an r-combination by permuting the r elements. This can be done in $r!$ ways so $P(n,r) = r!\,C(n,r)$

Notation $C(n,r) \sim \binom{n}{r} = \frac{n!}{r!(n-r)!}$

Example 11 # poker hands from deck of 52 cards is $\binom{52}{5}$

Note that $\binom{n}{r} = \binom{n}{n-r}$ as $n-(n-r) = r$

Combinatorial proof of this (count elements on both sides of equality)



Each r-set X corresponds 1-1 to one $(n-r)$-set, namely $S \setminus X$

$\Downarrow$

r-sets in S $\binom{n}{r}$

$=$ # $(n-r)$-sets in S $\binom{n}{n-r}$

6.4 Binomial coefficients

$\binom{n}{r}$ also called a <u>binomial coefficient</u> because it occurs as a coefficient in the expansion of $(x+y)^n$.

$$(x+y)^2 = x^2 + 2xy + y^2$$
$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

Theorem $(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$ Binomial Theorem

proof: the terms are of the form $x^{n-j}y^j$ for $j = 0, 1, 2 \ldots n$ and the coefficient to $x^{n-j}y^j$ is the number of ways we can choose j y's from the n parantheses so it is $\binom{n}{j}$ $\square$

application of the binomial theorem

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \qquad (\text{take } x = y = 1)$$

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0 \qquad (\text{take } x = 1, y = -1)$$

Pascal's identity

$\forall n,k \in \mathbb{Z}$ s.t. $n \geq k$ $\quad \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$

proof: fix one element a in an $(n+1)$-set T and let $S = T \setminus \{a\}$

There are $\binom{n}{k}$ k-subsets of T which do not contain a

There are $\binom{n}{k-1}$ k-subsets of T that do contain a as the remaining $k-1$ elements form a $(k-1)$-subset of S $\square$

This and $\binom{n}{0} = \binom{n}{n} = 1$ gives a recursive formula for binomial coefficients using only addition

1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

Pascal's triangle

Vandermonde: when $r \leq \min\{n,m\}$

$$\binom{n+m}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}$$