Chapter 6 / 5: Counting

general observation & recommendations:

- messing up while counting is hard to avoid
  (despite attempts to capture counting in “rules”)
- try smaller examples that keep essence
- check that answer makes sense
  (negative counts are usually incorrect)
- verify consistency between
  different ways to count the same

Prelude: counting using Chinese remaindering

to find the number C of people

- let p and q be coprime integers with $pq > C$
- form groups of p persons: find $C_p = C \bmod p$
- form groups of q persons: find $C_q = C \bmod q$
- thus $C = C_p + kp$ for unknown integer k
- to determine k, note that $C_p + kp = C_q \bmod q$ thus $k = (C_q - C_p)/p \bmod q$
- to calculate k we need s such that $sp = 1 \bmod q$ and thus $s = 1/p \bmod q$ (and $k = s(C_q - C_p) \bmod q$)
- finding s: with "$0 * p = q \bmod q$" and "$1 * p = p \bmod q$", perform the Euclidean algorithm on right hand sides until it equals 1

Warm-up: two simple counting rules

A and B are two different tasks,
with n ways to do A and m ways to do B

two scenarios:

1. task A must be done **followed by** task B

pages 375-376 /335-336

product rule:

n times m ways to do A and then B

2. task A **or** task B must be done (not both)

pages 379-380 /338-341

sum rule:

n plus m ways to do A or B

question:

how many ways to carry out each scenario?

Trivial example: pick two bits, a 1st & a 2nd

how many ways to pick the two bits?

task A: pick 1st bit; 2 ways to do so

task B: pick 2nd bit; 2 ways to do so

$\Rightarrow$ do task A followed by task B

thus $2 \times 2 = 4$ ways to do A followed by B

other way to define the tasks:

task A: 1st bit is 0; 2 ways to pick 2nd bit

task B: 1st bit is 1; 2 ways to pick 2nd bit

$\Rightarrow$ do task A or task B

thus $2 + 2 = 4$ ways to do A or B

(works because A and B are disjoint)

Common pitfall of sum rule

pages 382-383 /341-342

in how many ways can one pick seven bits such that last bit is 1 **or** the first 3 bits are 0?

A: pick last bit as 1; product rule: 64 ways
B: pick first 3 bits as 0; product rule: 16 ways
$\Rightarrow$ (sum rule?) 64 + 16 = 80 ways to do A **or** B

wrong because A and B are not disjoint:

- 8 of the ways under A have first 3 bits 0, or
- half the ways (i.e., 8) under B have last bit 1

$\Rightarrow$ either way, subtract 8 from 80: result 72

(remember principle of inclusion and exclusion: $|A \cup B| = |A| + |B| - |A \cap B|$)

(B': first 3 bits and last bit all zero, 8 total, is disjoint with A: $|A| + |B'| = 72$)

The first three of six simple examples

consider strings of length 6 over {a,b,c,…,y,z}

1. how many?

   26 choices for 1st, 26 choices for 2nd, 26 for 3rd, …, and 26 for 6th

   $\Rightarrow$ product rule: 26^6

2. how many begin with a vowel {a,e,i,o,u}?

   5 choices for 1st, 26 choices for 2nd – 6th

   $\Rightarrow$ product rule: $5*26^5$

3. how many begin and end with a vowel?

   5 choices for 1st and 6th, 26 for 2nd – 5th

   $\Rightarrow$ product rule: $5*26^4*5 = 5^2*26^4$

Fourth simple example

consider strings of length 6 over {a,b,c,…,y,z}

4. how many begin or end with a vowel?

   $5*26^5$ begin with vowel

   26^5*5 end with vowel

   $\Rightarrow 2*5*26^5$ begin or end with vowel

   but we counted "begin and end" twice

   $\Rightarrow 2*5*26^5 - 5^2*26^4 = 235*26^4$

   alternative calculation: complement of those that begin and end with consonant

   $\Rightarrow 26^6 - 21^2*26^4 = (26^2 - 21^2)*26^4$

use: $(c_1 = \text{vowel} \vee c_6 = \text{vowel}) \equiv \neg\,(c_1 \neq \text{vowel} \wedge c_6 \neq \text{vowel})$

$\equiv \neg\,(c_1 = \text{consonant} \wedge c_6 = \text{consonant})$

Fifth simple example

consider strings of length 6 over {a,b,c,…,y,z}

5. how many begin or end with a vowel, but not a vowel at begin and end?

   "begin or end" was $2*5*26^5 - 5^2*26^4$

   need to subtract "begin and end" again:

   $\Rightarrow 2*5*26^5 - 2*5^2*26^4 = 210*26^4$

   alternative calculation:

   begin vowel, end consonant: $5*26^4*21$

   begin consonant, end vowel: $21*26^4*5$

   these two possibilities are disjoint

   $\Rightarrow$ sum rule:

   $5*26^4*21+21*26^4*5 = 210*26^4$

Last simple example

consider strings of length 6 over {a,b,c,…,y,z}

6. how many have precisely one vowel?

   1st vowel, others consonants: $5*21^5$

   2nd vowel, others consonants: $21*5*21^4$

   3rd vowel, others consonants: 21^2*5*21^3

   …

   6th vowel, others consonants: 21^5*5

   (all possibilities disjoint)

   $\Rightarrow$ sum rule: $6*5*21^5$

Brief pigeonhole discussion

pages 388-390 /347-348

if N items are distributed over fewer than N bins, then there is a bin with at least two items ($N > 1$)

example: in any group of ≥ 2 persons there are at least 2 who have the same number of friends in the group ("being friends" is "symmetric"):

persons $p_1, p_2, \ldots, p_n$; $f(i)$: number of friends of p_i

bins $b_0, b_1, \ldots, b_{n-1}$; put person p_i in bin $b_{f(i)}$

$\Rightarrow$ n items in n bins: pigeonhole does not apply

- if b_0 is empty $\rightarrow$

  $p_1, p_2, \ldots, p_n$ assigned to $b_1, b_2, \ldots, b_{n-1}$
- if b_0 is not empty $\rightarrow$ (symmetry) b_{n-1} empty $\rightarrow$

  $p_1, p_2, \ldots, p_n$ assigned to $b_0, b_1, \ldots, b_{n-2}$

$\Rightarrow$ either way there is a "collision"

More general pigeonhole principle

pages 390-394 /349-353

with N items distributed over k bins,
there is a bin with at least $\lceil N/k \rceil$ items

select 8 different integers from $\{1,2,\ldots,12\}$,
then at least two pairs add up to precisely 13

bins are pairs adding up to 13, thus $k = 6$ bins:
(1,12), (2,11), (3,10), (4,9), (5,8), (6,7)

items are integers that are selected, thus $N = 8$
$\Rightarrow$ selection corresponds to a choice of bins
$\Rightarrow$ there is a bin with $\lceil N/k \rceil = \lceil 8/6 \rceil = 2$ items
$\Rightarrow$ at least one pair adds up to 13

remove it: $N = 6$, $k = 5$, $\lceil 6/5 \rceil = 2 \Rightarrow$ other pair

Related: cabling, and saving a few cables

page
395/354
exerc 30/34

connect p printers to d desktops ($d > p$) such that p desktops always connect to p distinct printers, but cheaper than running all pd cables

printers $P_1, P_2, \ldots, P_p$, desktops $D_1, D_2, \ldots, D_d$,

- for $1 \leq i \leq p$ connect D_i to P_i : p cables
- $p < k \leq d$ connect D_k to all P_is: $(d-p)p$ cables

$\Rightarrow$ total $(d-p)p+p$ cables (saving p^2-p cables)

works: D_i with $1 \leq i \leq p$ connects to P_i; if free printers then D_k ($k > p$) can connect to them

optimal: with $(d-p)p+p-1$ cables, there is a P_i
connected to $\leq d-p$ desktops, thus P_i not
connected to $\geq p$ desktops: let those print…

Permutations, combinations, etc

pages 395-425 /355-385

in how many different ways can *r* objects be selected from collection of *n* different objects?

have to distinguish different possibilities:

- may an object be selected more than once?

⇒ *replacement* (*repetition*) or not (if not: $r \leq n$)

- is the order of selection relevant?

⇒ *permutation* ("yes") or *combination* ("no")

⇒ 2×2 different possibilities to be considered:

1. permutation without replacement
2. combination without replacement
3. permutation with replacement
4. combination with replacement

Examples with $n = 10$, $r = 3$

pages
395-425
/355-385

1. permutation without replacement
   gold, silver, bronze medal among 10 players
2. combination without replacement
   select 3 representatives from class of 10
3. permutation with replacement
   select 3-digit PIN
4. combination with replacement
   select 3 cookies from 10 types of cookies
   or:
   number of nonnegative integer solutions
   to $x_1+x_2+\ldots+x_{10} = 3$ $(x_i \in \mathbf{Z}_{\geq 0})$

Simple formulas for general *n* and *r*

1. permutation without replacement: $P(n,r)$

pages 395-398 /355-357

n choices for 1^{st}, $n-1$ for 2^{nd}, …, $n-r+1$ for r^{th}

$$\Rightarrow P(n,r) = n(n-1)\ldots(n-r+1) = n!/(n-r)!$$

2. combination without replacement: $C(n,r)$

each combination can be ordered in $r!$ ways

pages 398-401 /357-360

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

(pronounced: "n choose r")

3. permutation with replacement

page 411/371

n choices for 1^{st}, n for 2^{nd}, …, n for r^{th}

$\Rightarrow$ in total n^r r-permutations with repetition

pages 411-415 /371-374

4. combination with replacement

(the only non-intuitive one – do this later)

Examples: combinations without replacement

pages 399-401 /358-359 433-434 /395-396

hands of five cards from standard deck:

52 cards: 13 “kinds” (valeurs) in 4 “suits” (couleurs)

(2,…,10, jack,queen,king,ace; spades,clubs,hearts,diamonds)

(2,…,10,valet,dame,roi,as; pique,trèfle,coeur,carreau)

- how many different hands?

  $$52 \text{ choose } 5 = C(52,5) = \binom{52}{5} = \frac{52!}{5!47!} = 2598960$$

- how many hands contain your favorite card (say 5 of clubs)?
  - pick it, left $\binom{51}{4} = 249900$ ($\Rightarrow$ almost 10%)
  - or: complement of not picking it:

    $$2598960 - \binom{51}{5} = 249900$$

  - or: $2598960 * (5/52) = 249900$

More card examples

pages
433-434
/395-396

- # hands containing your two favorite cards?
  - pick them, left $\binom{50}{3} = 19600$ ($\Rightarrow$ 0.75%)
  - or: complement of not picking them:
    $2598960 - \binom{50}{5} = 480200$
  - not the same, one must be wrong…
  - correct version of complement method uses inclusion&exclusion principle:
    $2598960 - \binom{51}{5} - \binom{51}{5} + \binom{50}{5} = 19600$
    (subtract card one excluded, subtract card two excluded, add back both excluded)

More card examples

pages 433-434 /395-396

- # hands containing five kinds?
  pick kinds ($C(13,5)$), four suits per kind:
  $C(13,5)4^5 = 1317888$ (51%)
- # hands with a flush, i.e., all same suit
  pick suit (4), pick 5 out of 13 ($C(13,5)$):
  $4C(13,5) = 5148$ (0.2%)
- # hands with four cards of one kind?
  pick kind ($C(13,1)$),
  pick the four cards of that kind ($C(4,4)=1$),
  and pick remaining card ($C(48,1)=48$):
  $13*48 = 624$ (0.024%)
- three of a kind: $C(13,1)*4*48*44/2$, (2.11%)
  (or: $C(12,2)*4^2$ instead of $48*44/2$)

Combinatorial and algebraic proofs

page
400/359

- combinatorial proof: formula holds based on counting argument or “insight”
- algebraic proof: usual math manipulations

Combinatorial and algebraic proofs

page 400/359 an r-combination from n without replacement
is equivalent to
an (n-r)-combination from n without replacement

$$\Rightarrow C(n,r) = C(n,n\text{-}r)$$

the above is example of a "combinatorial proof":
a counting argument that a formula holds

easily confirmed by a trivial algebraic proof:

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

$$= \binom{n}{n-r} = C(n,n-r)$$

More examples

page 336/292 exerc 10/14

1. splitting pile of n stones:
   - strong induction: total cost $n(n-1)/2$
   - "handshake" argument: same result

page 428/389 exerc 20/24

3. $P(n+1,r) = P(n,r)(n+1)/(n+1-r)$
   - algebraic proof immediate
   - combinatorial: argument:

$P(n+1,r+1) = (n+1)P(n,r)$:

take first from $n+1$, then r-perm from n

or

$P(n+1,r+1) = P(n+1,r)(n+1-r)$:

first take r-perm from $n+1$, then take last

More about *n* choose *r*: binomial coefficients

pages 403-409 /363-368

Pascal's identity ($0 < k \le n$): $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

- combinatorial proof:

pick k-combination from n+1 by fixing one element: include it (k-1 from n remain to be chosen) or don't (k from n remain to be chosen)

- algebraic proof:

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!}$$

$$= \frac{n!k}{k!(n-k+1)!} + \frac{n!(n-k+1)}{k!(n-k+1)!}$$

$$= \frac{n!k + n!(n-k+1)}{k!(n+1-k)!} = \frac{n!(n+1)}{k!(n+1-k)!} = \binom{n+1}{k}$$

Binomial theorem

page
404/363

for $n \geq 0$:

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

- combinatorial proof:
  expand product $(x+y)^n$: for the term $x^{n-k}y^k$
  the y needs to be chosen k out of n times
  (order irrelevant since $x^{n-k}y^k = yx^{n-k}y^{k-1} = \ldots = y^k x^{n-k}$)

$\Rightarrow$ coefficient of $x^{n-k}y^k$ must be n choose k

- algebraic proof:
  use mathematical induction
  and Pascal's identity

Algebraic proof of binomial theorem

let $P(n)$ be the assumption that $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

- $(x+y)^0 = 1 = \binom{0}{0} x^0 y^0 = \sum_{k=0}^{0} \binom{0}{k} x^{0-k} y^k$
  shows that $P(0)$ holds
- assume $P(n)$ holds for some $n \geq 0$. Then

$$(x+y)^{n+1} = (x+y)\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \text{ (used induction hypothesis)}$$

$$= \sum_{k=0}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1}$$

$$= \binom{n}{0} x^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1} + \binom{n}{n} y^{n+1}$$

$$= \binom{n+1}{0} x^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^{n+1-k} y^k + \sum_{k=1}^{n} \binom{n}{k-1} x^{n+1-k} y^k + \binom{n+1}{n+1} y^{n+1}$$

$$= \binom{n+1}{0} x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^{n+1-k} y^k + \binom{n+1}{n+1} y^{n+1} \text{ (Pascal's identity)}$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$$

Combinatorial and algebraic proofs

page 400/359

- combinatorial proof: formula holds based on counting argument or "insight"
- algebraic proof: usual math manipulations

seen both types of proofs for

pages 403-409 /363-368

- Pascal' identity ($0 < k \leq n$):

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

- binomial theorem: for $n \geq 0$

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

Consequence of binomial theorem

pages 405-406 /364-365

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

- algebraic proofs:
  - take $x = y = 1$ in binomial theorem
  - mathematical induction, Pascal's identity
- combinatorial proof:
  - 2^n is the number of length n bitstrings
  - write the number of length n bitstrings as $\sum_{k=0}^{n} C_i$, where C_i is the number of length n bitstrings with i bits "on", and note that C_i is n choose I

(or look at subsets and their cardinalities)

Another consequence of binomial theorem

pages 408-409 /367-368

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k} \text{ for } r < m, n$$

(Vandermonde's identity)

- algebraic proof:
  use $(x+y)^{m+n} = (x+y)^m (x+y)^n$
  with binomial theorem
  and compare the terms for $x^{m+n-r}y^r$

- combinatorial proof:
  count cardinality r subsets of
  cardinality $m+n$ set in different ways

- consequence: $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$

Final combinatorial $\leftrightarrow$ algebraic example

Page 409/369 exerc 14/22

$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k},\ 0 \le k \le r \le n$$

- combinatorial proof: suppose you need to pick a committee of r out of n, and a subcommittee of k out of those r (LHS). or pick the subcommittee of k first, then remaining r–k from remaining n–k (RHS)
- algebraic proof straightforward too:

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

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

Useful identity (for combination with repetition)

page
409/368
thm 4

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r} \text{ for } r \le n$$

- combinatorial proof: look at last "on" bit of r+1 "on" bits in n+1 positions

More precisely

page
409/368
thm 4

combinatorial proof of $\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}$ $(r \le n)$

pick r+1 out of $x_1, x_2, \ldots, x_{n+1}$,

All possibilities disjoint

- largest index is n+1
  n choose r ways to pick other r

or

- largest index is n
  n–1 choose r ways to pick other r

or

- largest index is n–1
  n–2 choose r ways to pick other r

or

- largest index is n–2
  n–3 choose r ways to pick other r

or

…

- largest index is r+1
  r choose r ways to pick other r

Useful identity

page
409/368
thm 4

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r} \text{ for } r \le n$$

- combinatorial proof: look at last "on" bit of r+1 "on" bits in n+1 positions
- proof by hand waving: repeatedly use Pascal's identity, walking up Pascal's triangle
- algebraic proof: use mathematical induction with respect to n (formalizing hand waving)
  - for $n = r$ identity holds
  - assume holds for n; then for n+1:

$$\binom{n+2}{r+1} = \binom{n+1}{r} + \binom{n+1}{r+1} \text{ (use Pascal's identity)}$$

$$= \binom{n+1}{r} + \sum_{j=r}^{n} \binom{j}{r} = \sum_{j=r}^{n+1} \binom{j}{r}$$

Back to counting formulas: pick *r* from *n*

1. permutation without replacement: $P(n,r)$

   $P(n,r) = n(n-1)\ldots(n-r+1) = n!/(n-r)!$

2. combination without replacement: $C(n,r)$

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

3. permutation with replacement

   $$n^r$$

pages 411-415 /371-374

4. combination with replacement

   still not done, and a bit less intuitive

Pick r-combination from n with replacement

pages 411-415 /371-374

to develop intuition, a few basic examples:

- given infinite supply of $n = 1$ cookie type, in how many ways can one pick r cookies? clearly only one way: r cookies of type 1

  $n = 1$: constant in r

- same question with $n = 2$ types of cookies: from 0 to r of type 1, others type 2: $r+1$ ways

  $n = 2$: linear in r

- same question with $n = 3$ types of cookies: s, $0 \leq s \leq r$, of type 1: $r-s$ of types 2 or 3, thus $\sum_{s=0}^{r}(r-s+1) = (r+1)(r+2)/2$ ways

  $n = 3$: quadratic in r

r-combination from n with replacement

pages 411-415 /371-374

observations we made:

- $n = 1$: 1 way
  $n = 2$: $r+1$ ways
  $n = 3$: $(r+1)(r+2)/2$ ways
  $\Rightarrow$suggests $(n+r-1)$ choose $n-1$ ways (*)

$\Rightarrow$ let $f(n,r)$ denote the number of r-combinations from n with replacement, then
$f(n,r) = f(n-1,0)+f(n-1,1)+\ldots+f(n-1,r)$:
take r of type 1, 0 left to take of $n-1$ types
take $r-1$ of type 1, 1 left to take of $n-1$ types
take $r-2$ of type 1, 2 left to take of $n-1$ types
…
take 0 of type 1, r left to take of $n-1$ types

r-combination from n with replacement

pages 411-415 /371-374

observations we made:

- $n = 1$: 1 way

  $n = 2$: $r+1$ ways

  $n = 3$: $(r+1)(r+2)/2$ ways

  $\Rightarrow$suggests $(n+r-1)$ choose $n-1$ ways (*)

$\Rightarrow$ let $f(n,r)$ denote the number of r-combinations from n with replacement, then

$f(n,r) = f(n-1,0)+f(n-1,1)+\ldots+f(n-1,r)$

- induction proof of *: basis $n = 1$ is okay;

$$f(n,r) = \sum_{s=0}^{r} f(n-1,s) = \sum_{s=0}^{r} \binom{n+s-2}{n-2}$$

page 409/368 thm 4

$$(\text{use } n+s-2 = j) \quad = \sum_{j=n-2}^{n+r-2} \binom{j}{n-2} = \binom{n+r-1}{n-1}$$

r-combination from *n* with replacement

why is the result so simple?

combinatorial proof that $f(n,r) = \binom{n+r-1}{n-1}$

uses $n+r-1$ positions $n-1$ of which are separators that "switch" to next type

note:

pages 413-414 /373-374

- $f(n,r)$ counts number of nonnegative integer solutions to $x_1+x_2+\ldots+x_n = r$ ($x_i \in \mathbf{Z}_{\geq 0}$)

  little tricks to deal with:
  - $x_i \geq b_i$ for bounds b_i: use $r - \sum_{i=1}^{n} b_i$
  - $x_1+x_2+\ldots+x_n \leq r$: use *slack variable* x_{n+1}

pages 415-419 /375-379

- $C(n,r)$ product for indistinguishable objects