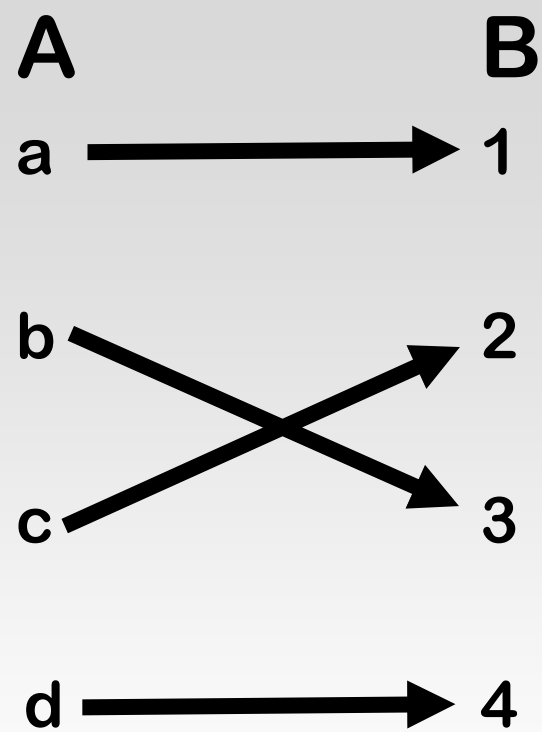
מתמטיקה בדידה
Discrete Math

Lecture 6

Counting one Thing by Counting Another

Recall: The Mapping Rule



If f: A $\rightarrow$ B is a bijection then |A| = |B|.

Example: Size of the Power Set

How many subsets of finite set A?

That is, what is |P(A)|?

A:	$\{a_1,$	$a_2,$	$a_3,$	$a_4,$	$a_5,$	… ,	$a_n\}$
subset:	$\{a_1,$		$a_3,$	$a_4,$		… ,	$a_n\}$
string:	1	0	1	1	0	…	1

This is a <u>bijection</u>

1. Every subset is mapped to an n-bit binary string.
2. Any n-bit binary string corresponds to a subset.

<u>Conclusion</u>: |P(A)| = |n-bit binary strings|

Example: Balls with Different Colors

How many ways to select 12 balls w/ 5 different colors?

A = all ways to select 12 balls w/ 5 different colors.

B = all 16-bit numbers with exactly 4 ones.

element of A: $\underbrace{00}_{\text{red}}\quad\underbrace{}_{\text{green}}\quad\underbrace{000000}_{\text{yellow}}\quad\underbrace{00}_{\text{blue}}\quad\underbrace{00}_{\text{white}}$

element of B: $\underbrace{00}_{\text{red}}\ 1\ \underbrace{}_{\text{green}}\ 1\ \underbrace{000000}_{\text{yellow}}\ 1\ \underbrace{00}_{\text{blue}}\ 1\ \underbrace{00}_{\text{white}}$

Balls with Different Colors II

A = all ways to select 12 balls w/ 5 different colors.

B = all 16-bit numbers with exactly 4 ones.

Bijection from A to B:

r red, g green, y yellow, b blue, w white

maps to

$$\underbrace{0\ldots0}_{r}\ 1\ \underbrace{0\ldots0}_{g}\ 1\ \underbrace{0\ldots0}_{y}\ 1\ \underbrace{0\ldots0}_{b}\ 1\ \underbrace{0\ldots0}_{w}$$

1. Sequence has always 16 bits and exactly 4 ones.
2. Every sequence corresponds to exactly one order of balls.

<u>Conclusion</u>: |A| = |B|

Counting a Thing by Counting Another

Counting rule relates |A| with |B|.

Once we figure out |B|, we will immediately know |A|.

Question: But how do we figure out |B|?

Answer: Sequences are easier to count…

General strategy:

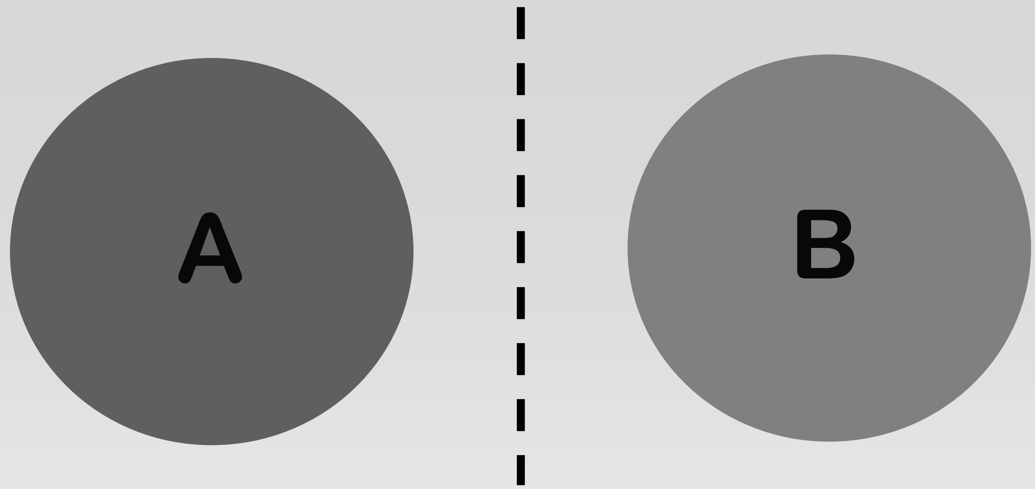
1. Get really good at counting sequences.
2. Use bijections to count everything else.

Given a set T:

1. Find bijection to set of sequences S.
2. Use counting skills to count |S|, which gives us |T|.

Rules for Counting

The Sum Rule

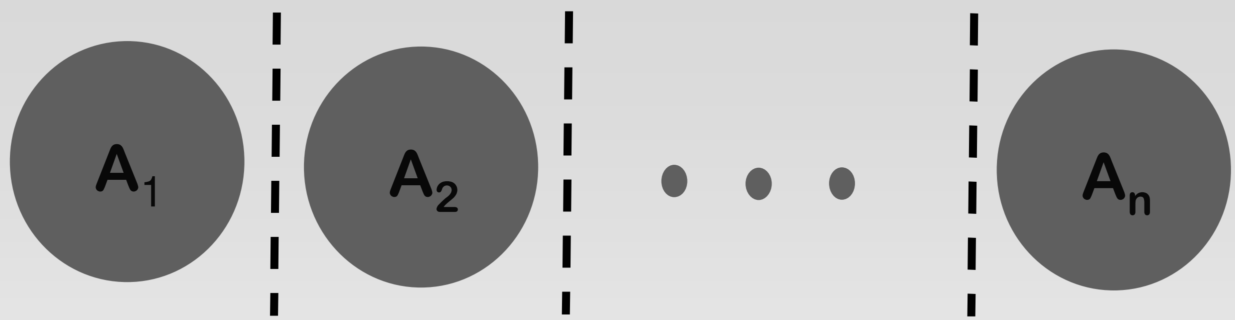


If sets A and B are disjoint, then

$$|A \cup B| = |A| + |B|$$

The sum rule כלל הסכום

More Generally



If sets $A_1, A_2, \ldots, A_n$ are <u>disjoint</u>, then

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

Sum Rule: Examples

Class has 11 women, 30 men so total enrollment is

$$11 + 30 = 41$$

26 Lower case letters, 26 upper case letters, and 10 digits, so total number of characters is

$$26 + 26 + 10 = 62$$

The Product Rule

If $P_1, P_2, \ldots, P_k$ are sets then

$$|P_1 \times P_2 \times \ldots \times P_k| = |P_1| \cdot |P_2| \cdot \cdot \cdot |P_k|$$

<u>Recall</u>:

$$P_1 \times P_2 \times \ldots \times P_k := \{(p_1, p_2, \ldots, p_k) \mid p_1 \in P_1, p_2 \in P_2, \ldots, p_n \in P_k\}$$

The Product Rule II

Unlike the sum rule, the product rule does not require the sets to be disjoint.

<u>Example</u>: If $|A| = m$ and $|B|=n$, then $|A \times B| = mn$

$A = \{a,b,c,d\}$, $B = \{a,2,3\}$

$$\begin{aligned} A \times B = \{&(a,a),(a,2),(a,3),\\ &(b,a),(b,2),(b,3),\\ &(c,a),(c,2),(c,3),\\ &(d,a),(d,2),(d,3)\} \end{aligned}$$

The Product Rule III

Counting strings:

Number of length-4 strings from alphabet $B := \{0,1\}$ is

$$|B \times B \times B \times B| = 2 \times 2 \times 2 \times 2 = 2^4$$

In particular,

$$|\{0,1\}^k| = 2^k$$

In general: Number of length-k strings from alphabet of size n is

$$n^k$$

Example: Counting Passwords

1. Between 6 and 8 characters long.
2. Starts with a letter.
3. Case sensitive.*
4. Other characters: digits or letters.

<u>Examples</u>: a5Tj6Vu5, sE5TG4

*Case sensitive – uppercase and lowercase are different.

Example: Counting Passwords II

$L := \{a,b,\ldots,z,A,B,\ldots,Z\}$

$D := \{0,1,\ldots,9\}$

$P_k :=$ length k passwords

<u>Question</u>: what is P_6?

<u>Answer</u>: Think of password as sequence

$$\text{sE5TG4} \leftrightarrow (\overbrace{s}^{L}, \overbrace{E, 5, T, G, 4}^{(L \cup D)})$$

$$P_6 = L \times (L \cup D) \times (L \cup D) \times (L \cup D) \times (L \cup D) \times (L \cup D)$$

$$= L \times (L \cup D)^5$$

Example: Counting Passwords III

$L := \{a,b,\ldots,z,A,B,\ldots,Z\}$

$D := \{0,1,\ldots,9\}$

$P_k :=$ length k passwords

$$P_k = L \times (L \cup D)^{k-1}$$

$$\begin{aligned} |L \times (L \cup D)^{k-1}| &= |L| \cdot |L \cup D|^{k-1} \\ &= |L| \cdot (|L| + |D|)^{k-1} \\ &= 52 \cdot 62^{k-1} \end{aligned}$$

Example: Counting Passwords IV

The set of passwords:

$$P = P_6 \cup P_7 \cup P_8$$

$$\begin{aligned} |P| &= |P_6| + |P_7| + |P_8| \\ &= 52 \cdot 62^5 + 52 \cdot 62^6 + 52 \cdot 62^7 \\ &= 186125210680448 \\ &\approx 19 \cdot 10^{14} \end{aligned}$$

String, Sequences and Functions

$$\underbrace{|B \times B \times \ldots \times B|}_{\text{k times}} = \underbrace{|B| \times |B| \times \ldots \times |B|}_{\text{k times}} = |B|^k$$

AKA: # sequences with repeats.

Corollary 1: # length-k strings from alphabet B of size n is n^k

Corollary 2: # length-k binary strings is $|\{0,1\}^k| = 2^k$

Note:

1. Length-k string and length-k sequence is the same thing
2. Length-|A| string from alphabet B and $f: A \to B$ is the same thing.

AKA "Also Known As"

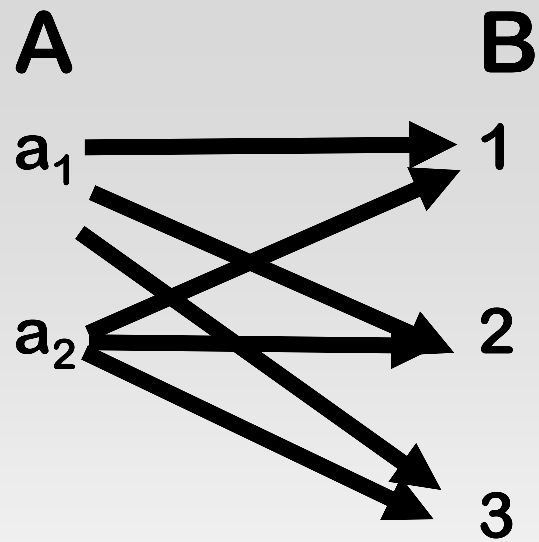
Example: Counting Functions

Let A,B be finite sets, and suppose that

$$|A| = k$$
$$|B| = n$$

<u>Q</u>: How <u>many</u> (total) functions f:A $\rightarrow$ B are there?

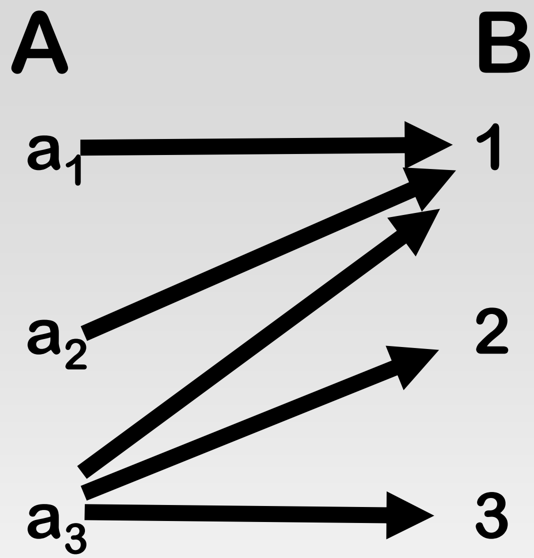
Example: $A=\{a_1,a_2\}$, $B=\{1,2,3\}$



For every choice for $f(a_1)$, there are 3 choices for $f(a_2)$

 # (total) functions $\{a_1, a_2\} \rightarrow \{1,2,3\} = 3 \times 3 = 3^2$

Example: A={a_1,a_2,a_3}, B={1,2,3}



For every choice for $f(a_1)$ and $f(a_2)$, there are 3 choices for $f(a_3)$

(total) functions $\{a_1, a_2, a_3\} \rightarrow \{1,2,3\} = 3 \times 3 \times 3 = 3^3$

So What is the General Rule?

(total) functions $\{a_1,a_2\} \rightarrow \{1,2,3\}$ = 3 x 3

$$= \underbrace{|B| \times |B|}_{|A|=2 \text{ times}}$$

(total) functions $\{a_1,a_2,a_3\} \rightarrow \{1,2,3\}$ = 3 x 3 x 3

$$= \underbrace{|B| \times |B| \times |B|}_{|A|=3 \text{ times}}$$

<u>The Rule</u>: $|B|^{|A|}$

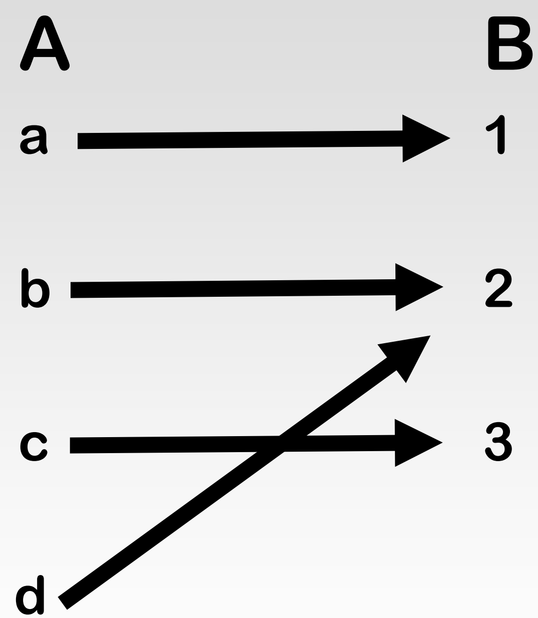
<u>The idea</u>: Think of f: A $\rightarrow$ B as a sequence of length |A| with elements from the alphabet B.

Generalized Counting Rules

The Pigeonhole Principle

If $\exists$ injection f: A $\to$ B then |A| ≤ |B|

<u>Equivalently:</u> if |A| > |B|, then $\nexists$ injection f: A $\to$ B



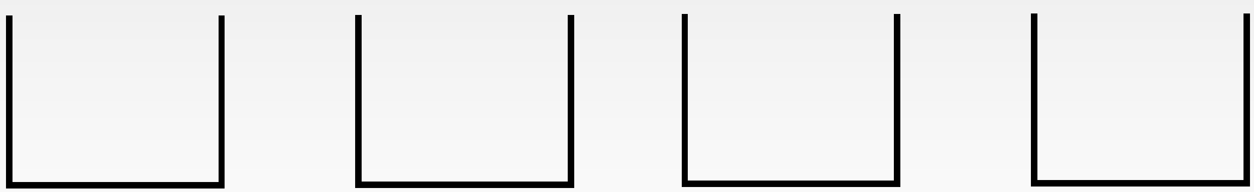
The pigeonhole principle עקרון שובך היונים

The Pigeonhole Principle

If $|A| > |B|$, then $\nexists$ injection $f\colon A \to B$

If more pigeons

Than pigeonholes



The Pigeonhole Principle II

Then some hole must have ≥ two pigeons!

Tip: when applying the pigeonhole principle, it is important to identify 3 things

1. The set A (the pigeons)
2. The set B (the pigeonholes)
3. The function f (rule of assigning pigeons to pigeonholes).

Example 1: Socks

A drawer in a dark room contains

1. red socks
2. green socks
3. blue socks.

Question: How many socks do you have to withdraw to be sure that you have a matching pair?

Answer: Let A := set of socks you withdraw

B := {red,green,blue}

Then if $|A| > |B| = 3$ at least two elements of A will have same color.

0204801353855029644448038	3171004832173501394113017	5763257331083479647409398	8247331000042995311646021
4894459918669156762409992	3208234421597368647019265	5800949123548989122628663	8496243997123475922766310
1082662032430379651370981	3437254656355157864869113	6042900801199280218026001	8518399140676002660747477
1178480894769706178994993	3574883393058653923711365	6116171789137737896701405	8543691283470191452333763
1253127351683239693851327	3644909946040480189969149	6144868973001582369723512	8675309258374137092461352
1301505129234077811069011	3790044132737084094417246	6247314593851169234746152	8694321112363996867296665
1311567111143866433882194	3870332127437971355322815	6814428944266874963488274	8772321203608477245851154
1470029452721203587686214	4080505804577801451363100	6870852945543886849147881	8791422161722582546341091
1578271047286257499433886	4167283461025702348124920	6914955508120950093732397	9062628024592126283973285
1638243921852176243192354	4235996831123777788211249	6949632451365987152423541	9137845566925526349897794
1763580219131985963102365	4670939445749439042111220	7128211143613619828415650	9153762966803189291934419
1826227795601842231029694	4815379351865384279613427	7173920083651862307925394	9270880194077636406984249
1843971862675102037201420	4837052948212922604442190	7215654874211755676220587	9324301480722103490379204
2396951193722134526177237	5106389423855018550671530	7256932847164391040233050	9436090832146695147140581
2781394568268599801096354	5142368192004769218069910	7332822657075235431620317	9475308159734538249013238
2796605196713610405408019	5181234096130144084041856	7426441829541573444964139	9492376623917486974923202
2931016394761975263190347	5198267398125617994391348	7632198126531809327186321	9511972558779880288252979
2933458058294405155197296	5317592940316231219758372	7712154432211912882310511	9602413424619187112552264
3075514410490975920315348	5384358126771794128356947	7858918664240262356610010	9631217114906129219461111
3111474985252793452860017	5439211712248901995423441	7898156786763212963178679	9908189853102753335981319
3145621587936120118438701	5610379826092838192760458	8147591017037573337848616	9913237476341764299813987
3148901255628881103198549	5632317555465228677676044	8149436716871371161932035	
3157693105325111284321993	5692168374637019617423712	8176063831682536571306791	

90 numbers – A = $\{a_1, a_2, \ldots, a_{90}\}$
25 digits each - $a_i \in \{0,\ldots,9\}^{25}$

Q: Are there two subsets of the numbers that have the same sum?

Example 2: Subset Sum

Q: Are there two subsets that have the same sum?

Note: the sum of any subset of numbers is $\leq 90 \cdot 10^{25}$

1. Let $X = P(\{a_1, a_2, \ldots, a_{90}\})$
2. Let $Y = \{0, 1, \ldots, 90 \cdot 10^{25}\}$
3. Let $f: X \to Y$ map each subset of numbers to its sum (in Y).

Now,

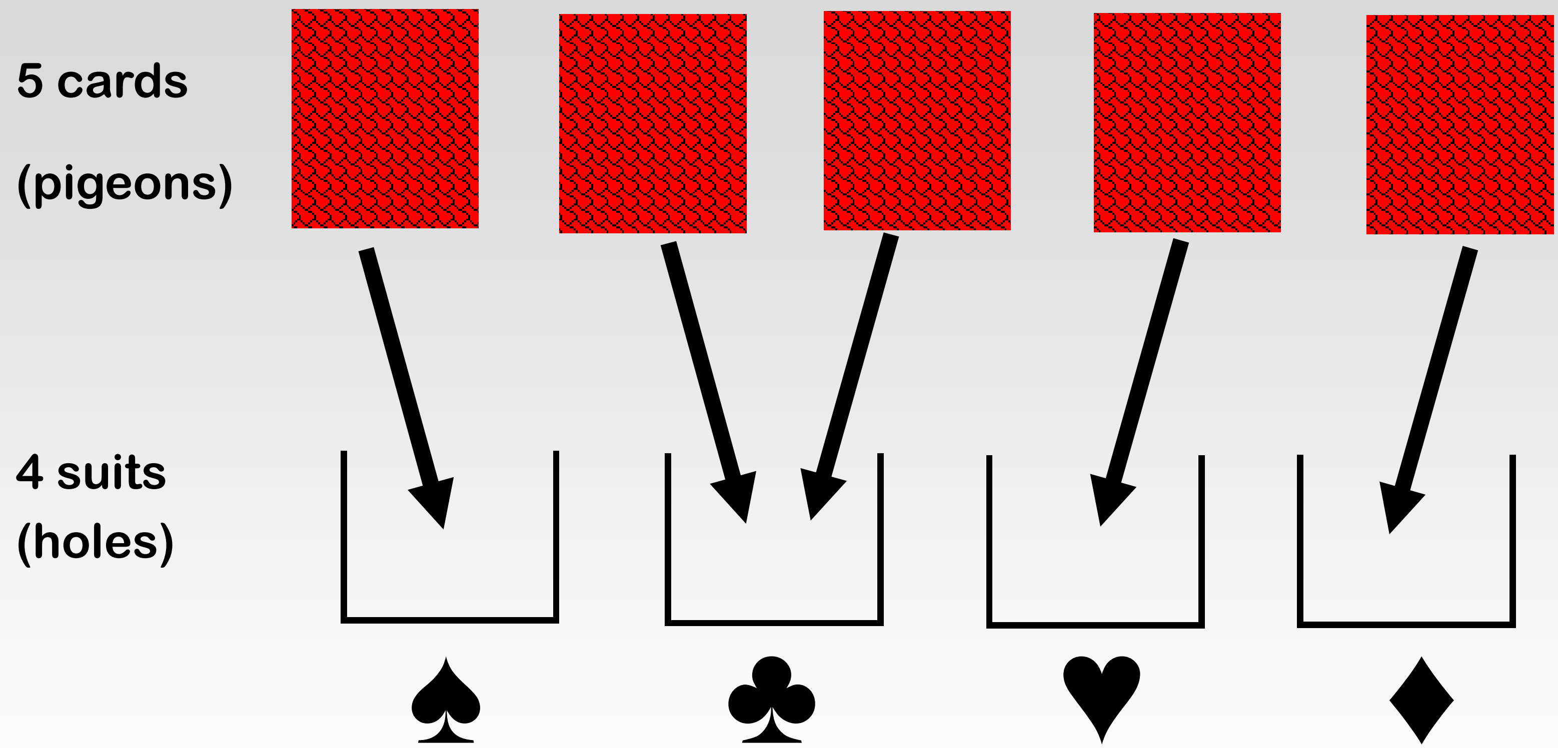
$|X| = 2^{90}$
$\geq 1.237 \times 10^{27}$

$|Y| = 90 \cdot 10^{25} + 1$
$\leq 0.901 \times 10^{27}$

By the pigeonhole principle, f maps at least two elements of X into the same element of Y!

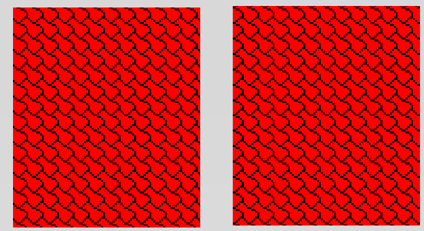
Remark: Proof is "nonconstructive" – gives no indication which two sets have the same sum…

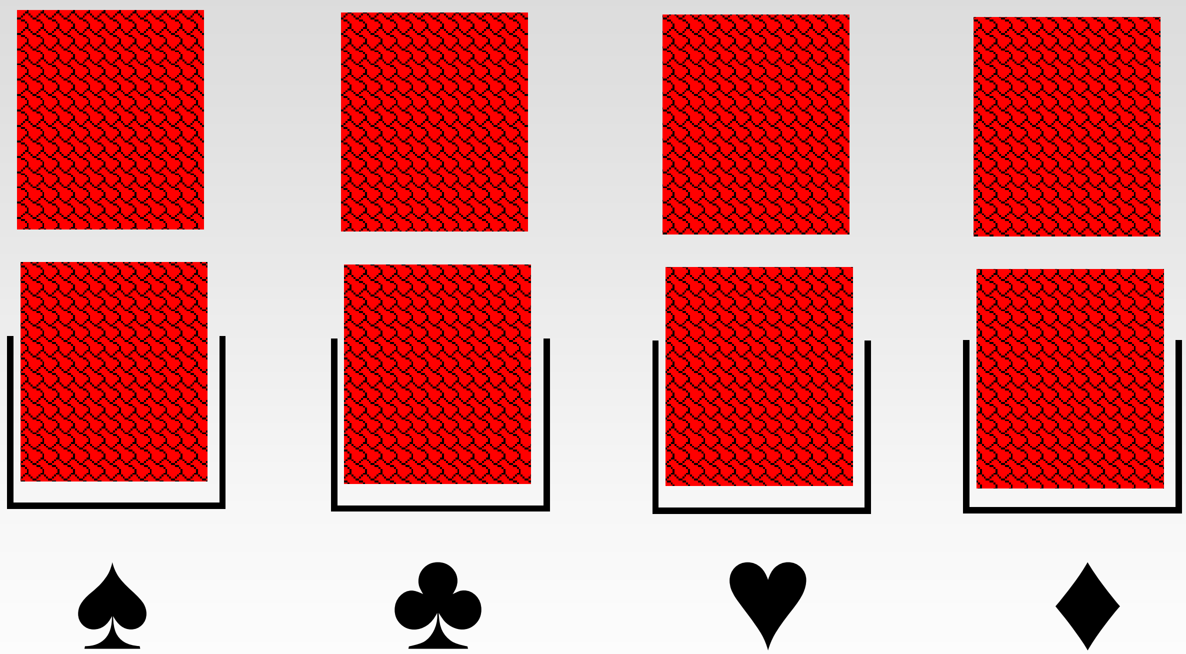
Example 3: 5 Card Draw



10 Card Draw

Cannot have < 3 cards in every hole





Generalized Pigeonhole Principle

cards with same suit $\geq$ 3

$$\left\lceil \frac{10}{4} \right\rceil = 3$$ cards with same suit

"ceiling" – means round up

<u>Generalized pigeonhole principle</u>: If n pigeons and h holes, then some hole has at least

$$\left\lceil \frac{n}{h} \right\rceil$$

pigeons.

<u>More formally</u>: If |A| > k · |B|, then every function f: A $\rightarrow$ B maps at least k+1 different elements of A to the same element of B.

Example: Hairs on Heads

Claim: There exist at least 3 people* in Tel Aviv that have exactly the same number of hairs on their heads.

1. Tel Aviv has about 500,000 non bald people
2. # hairs on a person's head is < 200,000

A := set of non bald people in Tel Aviv
B := {1,2,…,200,000}
f: A $\rightarrow$ B maps a person to # hairs on her head.

|A| > 2 · |B|, so by the generalized pigeonhole principle,
at least three people have the same number of hairs

*Not bald…

Advanced Comment: The "Birthday Paradox"

How many people in this class have the same birthday?

1. **41 students.**
2. **365 days in the year.**

Can we apply the pigeonhole principle?

<u>The lesson</u>: randomization is powerful!

Generalized Product Rule

<u>Question</u>: How many sequences of 5 students in class?

S := students in class $\qquad$ $|S| = 41$

|sequences of 5 students| = 41^5? $\qquad$ NO!

<u>We want</u>: $\quad$ |sequences in S^5 with no repeats|

No repeats $\qquad$ ללא חזרות

Generalized Product Rule II

|sequences in S^5 with no repeats|

41 choices for 1st student

40 choices for 2nd student

39 choices for 3rd student

38 choices for 4th student

37 choices for 5th student

so $41 \cdot 40 \cdot 39 \cdot 38 \cdot 37$

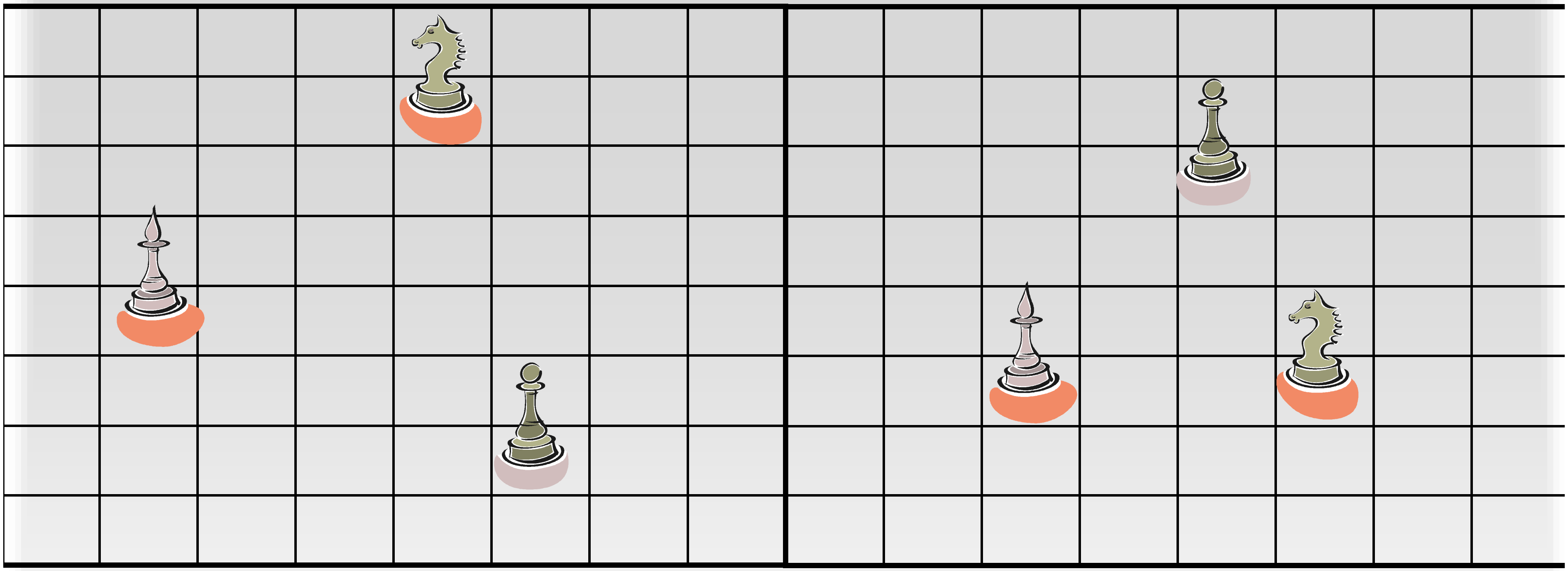
Generalized Product Rule III

The generalized product rule: Let S be a set of length-k sequences. If there are

- n_1 possible 1st entries,
- n_2 possible 2nd entries for each 1st entry,
- n_3 possible 3rd entries for each possible 1st and 2nd entries, etc.

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

Example: A Chess Problem



valid　　　　invalid

<u>Q</u>: In how many ways can we arrange knight, bishop and pawn so that no two pieces share a row or a column?

Example: A Chess Problem II

Let p – pawn, k – knight, b - bishop

First, notice that there is a bijection from configurations of the chessboard to sequences:

$$(r_p, c_p, r_k, c_k, r_b, c_b)$$

where r_p, r_k, r_b are distinct rows and c_p, c_k, c_b are distinct columns.

Now, using the generalized product rule:

r_p is one of 8 rows

c_p is one of 8 columns

r_k is one of 7 rows (any one but r_p)

c_k is one of 7 columns (any one but c_p)

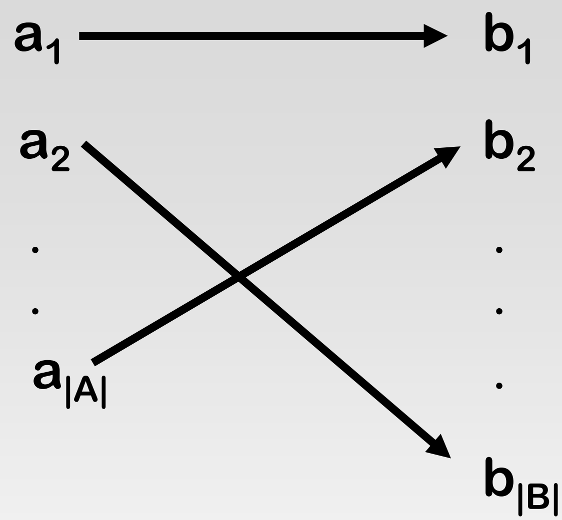
r_b is one of 6 rows (any one but r_p or r_k)

c_b is one of 6 columns (any one but c_p or c_k)

So the total number of configurations is $(8 \cdot 7 \cdot 6)^2$

Example: Counting Injective Functions

How many (total) injective functions from A to B?



- $|B|$ possible values for $f(a_1)$,
- $|B|$ - 1 possible values for $f(a_2)$, given $f(a_1)$
- $|B|$ - 2 possible values for $f(a_3)$, given $f(a_1)$ and $f(a_2)$ etc.

By generalized product rule: # injective functions f: A $\to$ B is

$$|B| \cdot (|B|-1) \cdot (|B|-2) \cdots (|B|-|A|+1)$$

Permutations

Definition: A permutation of a set S is a sequence that contains every element of S exactly once.

For example, the permutations of the set {a,b,c} are

(a,b,c) (a,c,b) (b,a,c)
(b,c,a) (c,a,b) (c,b,a)

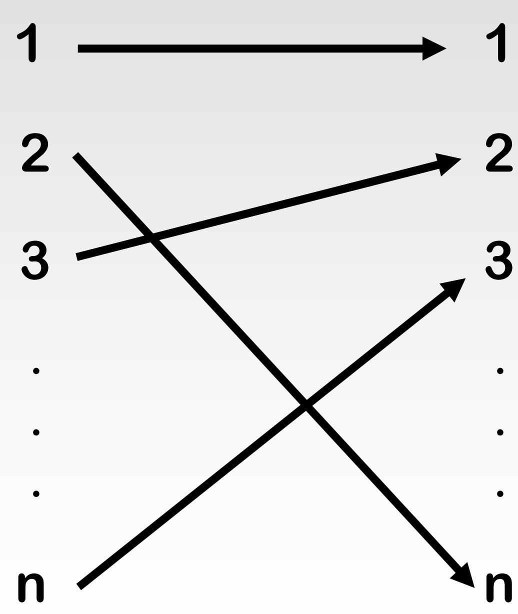
Permutation	תמורה
n factorial	n עצרת

Permutations as bijections

Typically: permutations on the set S = {1,2,…,n}

Notation: [n] := {1,2,…,n}

A permutation on [n] is a bijection π: [n] $\rightarrow$ [n]



Counting Permutations

A permutation is a bijection f: S $\to$ S.

<u>We saw before</u>: # injective functions f: A $\to$ B is

$$|B| \cdot (|B|-1) \cdot (|B|-2) \cdots (|B|-|A|+1)$$

<u>So</u>: # permutations on an n-element set

$$n! := n \cdot (n-1) \cdot (n-2) \cdot \cdot \cdot 3 \cdot 2 \cdot 1$$

(convention: $0! = 1$).

How Large is n!

Very large:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^{n}$$

This is known as Stirling's approximation.

#permutations vs. #functions

A permutation is a bijection π: [n] $\rightarrow$ [n].

Q: How many bijections π: [n] $\rightarrow$ [n] are there?

A: n!

Q: How many functions f: [n] $\rightarrow$ [n] are there?

A: n^n

By Stirling's approximation:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n = \frac{\sqrt{2\pi n}}{e^n} \cdot n^n$$

n! << n^n, but is still very large!

Quick Question

Q: How many functions f: A $\rightarrow$ B are not injective?

X – Set of all functions f: A $\rightarrow$ B ($|X| = |B|^{|A|}$)

Y – Set of all injective functions f: A $\rightarrow$ B

$$|Y| = |B| \cdot (|B|-1) \cdots (|B|-|A|+1)$$

Z – Set of all non-injective functions f: A $\rightarrow$ B

By sum rule: $|X| = |Y| + |Z|$

So $|Z| = |X| - |Y|$

$$= |B|^{|A|} - |B| \cdot (|B|-1) \cdots (|B|-|A|+1)$$

Strings with no Repeats

Let B be an alphabet of size n.

<u>By generalized product rule</u>: # length-k strings w/ <u>no repeats</u> with elements from B is

$$|B|\cdot(|B|-1)\cdot(|B|-2)\cdots(|B|-k+1)$$

<u>In other words</u>:

$$n\cdot(n-1)\cdots(n-k+1)=\frac{n\cdot(n-1)\cdots 2\cdot 1}{(n-k)\cdot(n-k-1)\cdots 2\cdot 1}$$

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

Summary so far

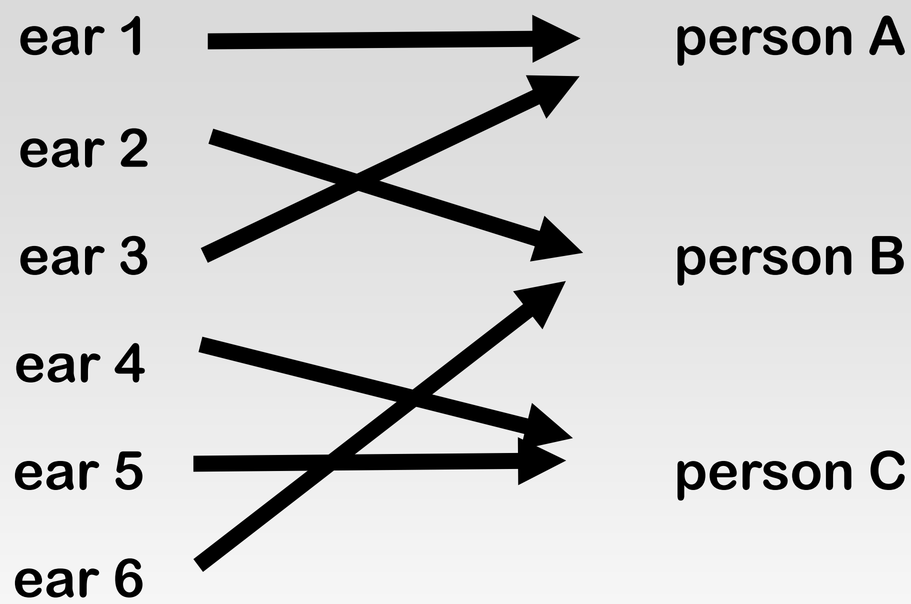
 # possibilities to choose k elements from a set of size n

	No repeats	**With repeats**
Order is important (sequence)	$\frac{n!}{(n-k)!}$	n^k
Order not important (subset)	**Next week**	**Next week**

The Division Rule

<u>Definition</u>: f: A $\rightarrow$ B is said to be <u>k-to-1</u> if it maps exactly k elements from A to every element in B.

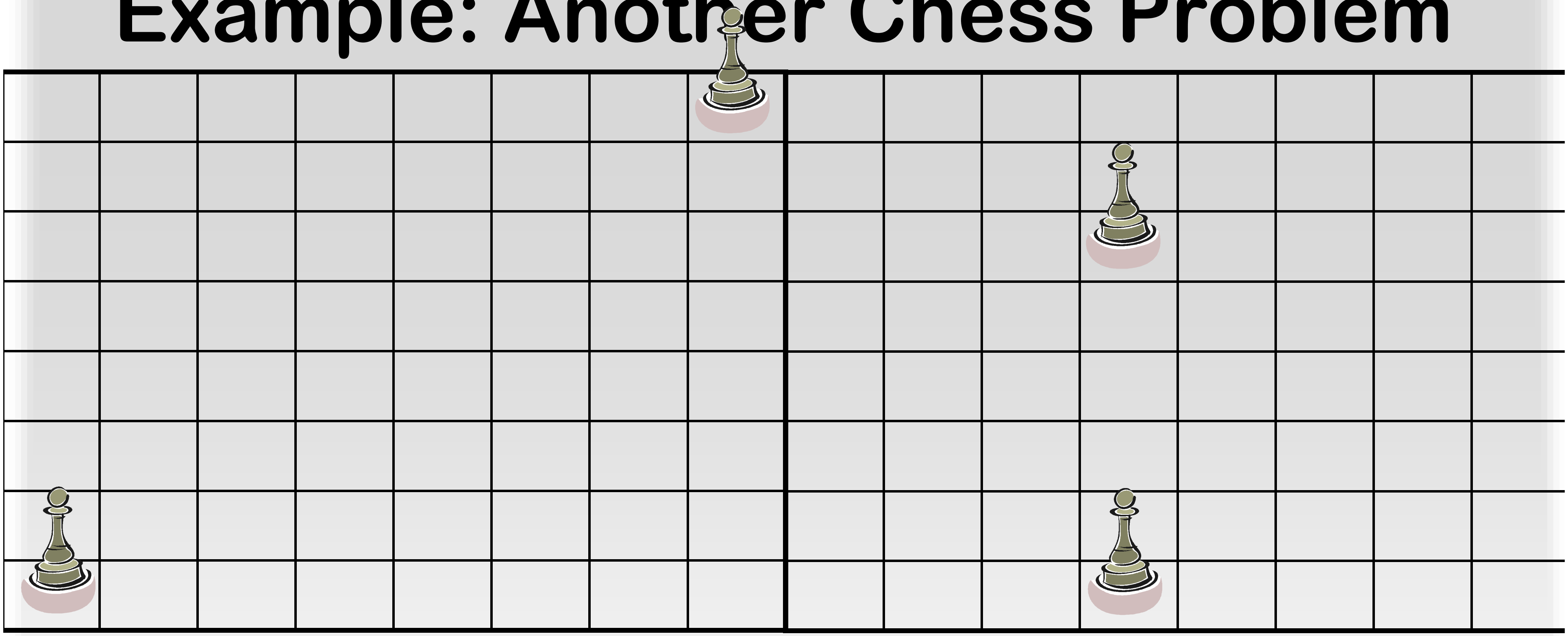
<u>Example</u>:



is a 2-to-1 function. Similarly a function mapping each finger to its owner is 10-to-1.

<u>The division rule</u>: If f: A $\rightarrow$ B is <u>k-to-1</u> then $|A| = k \cdot |B|$.

Example: Another Chess Problem



valid   invalid

Q: In how many ways can we place two identical pawns so that they do not share a row or a column?

Example: Another Chess Problem II

Let A be the set of all sequences (r_1, c_1, r_2, c_2) where r_1 and r_2 are distinct rows, and c_1, c_2 are distinct columns.

Let B be the set of all valid pawn configurations.

Let f: A $\rightarrow$ B t be a function that maps the sequence (r_1, c_1, r_2, c_2) to a configuration with one pawn in row r_1 column c_1 and the other pawn in row r_2 column c_2

Note: The sequences (1,1,8,8) and (8,8,1,1) map to the same configuration!

More generally: the function f maps exactly two sequences to every configuration. That is, f is 2-to1.

Conclusion: By the division rule, |A| = 2 · |B|. So,

$$|B| = |A|/2$$

$$= (8 \cdot 7)^2/2$$