Probability theory

Prof.dr.hab. Viorel Bostan

Technical University of Moldova

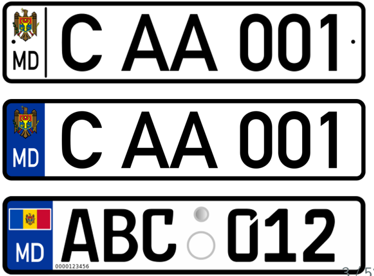
viorel.bostan@adm.utm.md

Lecture 4

Previous Lecture Outline

- General concept of probability;
- Sample space and probability distribution;
- Axioms and properties of probability;
- Conditional probability;
- A posteriori probability.

Next few lectures we will talk about this ...



Informal definition

Combinatorics is the area of mathematics concerned with counting.

- How difficult is counting? It's challenging! And it depends on you.
- Counting is a practical skill like integration.
- Just need to *translate* the problem to a math problem that you know how to solve.

A problem appearing on one of the oldest survived mathematics manuscripts of about 1650 BC was translated as:

Houses	7
Cats	49
Mice	343
Wheat	2401
Hekat	16807
	19607

Counting. A little bit of history

An example of counting principle can be traced to at least 1730 in a popular poem:

As I was going to St.Ives,
I met a man with seven wives,
Each wife had seven sacks,
Each sack had seven cats,
Each cat had seven kits.
Kits, cats, sacks and wives,
How many were going to St.Ives?

The correct answer is , **one!**
The others are going in the opposite direction.

You might have heard this old poem before. Where?

Memory cinephilia quiz

Die Hard 3

Counting example

7820480135385502964448038	3171004832173501394113017	5763257331083479647409398	8247331000042995311646021
4894459918669156762409921	3208234421597368647019265	5800949123548989122628663	8496243997123475922766310
1082662032430379651370981	3437254656355157864869113	6042900801199280218026001	8518399140676002660747477
1178480894769706178994993	3574883393058653923711651	6116171789137737896701405	8543691283470191452333763
1253127351683239693851327	3644909946040480189969149	6144868973001582369735121	8675309258374137092461352
1301505129234077811069011	3790044132737084094417246	6247314593851169234746152	8694321112363996862966665
1311567111143866433882194	3870332127437971355322815	6814428944266874963488274	8772321203608477245851154
1470029452721203876862144	4080505804577801451363100	6870852945543886849147881	8791422161722582546341091
1578271047286257499433886	4167283461025723481249203	6914955508120950093732397	9062628024592126283973285
1638243921852176243192354	4235996831123777788211249	6949632451369871524235413	9137845566925526349897794
1763580219131985963102365	4670939445749439042111220	7128211143613619828415650	9153762966031892919344419
1826227795601842231029694	4815379351865384279613427	7173920083651862307925394	9270880194077636406984249
1843971826751020372014203	4837052948212922604442190	7215654874211755676220587	9324301480722103490379204
2396951193722134526177237	5106384238550185506715309	7256932847164391040233050	9436090832146695147140581
2781394568268599801096354	5142368192004769218069910	7332226570752354316203178	9475308159734538249013238
2796605196713610405408019	5181234096130144084041856	7426441829541573444964139	9423766239174869749232202
2931016394761975263190347	5198267398125617994391348	7632198126531809327186321	9511972558779880288252979
9334580582944051551972967	5317592940316231219758372	7712154432211912882310511	9602413424619187112552264
3075514410490975920315344	5384358126771794128356947	7858918664240262356610010	9631217114906129219461111
3111474985252793452860017	5439211712248901995423417	7898156786763212963178679	9908189853102753335981319
3145621587936120118438701	5610379826092838192760458	8147591017037573337886166	9913237476341764299813987
3148901255628881103198549	5632317555465228677676044	8149436716871371161932035	3157693105325111283219930
	5692168374637019617423712	8176063831682536571306791	

Two different subsets of the ninety 25-digit numbers shown above have the same sum!

Where counting is used?

Counting seems easy: Just count $1, 2, 3, 4, \ldots$

The explicit approach works well for counting simple things like your fingers and for extremely complicated things for which there is no identifiable structure.

The number of different ways to select a dozen doughnuts when there are five varieties available.

The number of 16-bit numbers with exactly 4 ones.

Counting is useful in computer science for several reasons:

- To compute the time and storage necessary in solving a computational problem.
- To find the best algorithm for a specific task.
- To find the winning strategy in games.
- Counting is extensively used in graph theory.
- Counting is the foundation of the probability theory, especially the discrete one.
- Several proof techniques rely on counting.

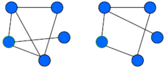
Given n numbers: $a_1, a_2, a_3, \ldots, a_n$ it is necessary to sort them, i.e., to put them in increasing (or decreasing) order: for. ex. input $4, 7, 6, 1, 3, 1, 9, 5$ gives an output $1, 1, 3, 4, 5, 6, 7, 9$.

- What is the minimum number of binary comparisons needed to sort n numbers?
- What is the fastest way any algorithm could possibly sort?

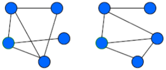
The probability of an event in a uniform sample space is $\frac{\text{nr. of event outcomes}}{\text{nr. of all outcomes}}$.

- What is the probability of a full house in poker?
- What is the probability of having two people with the same birthday in a room with n people?
- What is the probability that a thief will "guess" your bank card PIN number?
- What is the probability to have a profit of 100$ playing roulette in a Las Vegas casino if you have 500$ to ~~play~~ lose ?

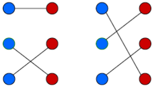
Where counting is used: Graph theory and Game theory



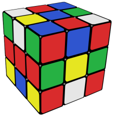
- How many different n-node graphs are there?
- How many different mappings need to be checked to see if two arbitrary n-node graphs are isomorphic (similar)?

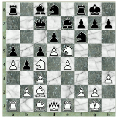


- How many different pairings between n boys and n girls are there?



- How many different configurations exist for a Rubik's cube?
- How many different chess positions can exist after n moves?
- How many weighing are needed to find the one counterfeit coin among 12 coins?





Count one thing by counting another

There are several rules for counting, most of them being intuitive.

How do you count people in a room? For example, you can count the heads since for each person there is **exactly** one head. Or you can count hands and divide by two.

Counting General Principle

Count one thing by counting another!

Counting General Principle Rephrased

Find the cardinality of a set X by finding the cardinality of a related set Y.

Theorem (Mapping Rule)

1. *If $f : X \to Y$ is surjective, then $|X| \geqslant |Y|$.*
2. *If $f : X \to Y$ is injective, then $|X| \leqslant |Y|$.*
3. *If $f : X \to Y$ is bijective, then $|X| = |Y|$.*

Doughnuts example

Example

Consider two sets:

$$\begin{aligned} A = \{&\text{all ways to choose 12 doughnuts from 5 available varieties :}\\ &\text{chocolate, lemon, vanilla, raspberry and hazelnut}\};\\ B = \{&\text{all 16-bit sequences with exactly 4 ones}\}.\\ &\text{E.g : 0110001000001000, 1000100100000001, 0001001000100010.} \end{aligned}$$

Consider a particular selection of 12 doughnuts:

$$\underbrace{00}_{\text{chocolate}} \quad \underbrace{}_{\text{lemon}} \quad \underbrace{000000}_{\text{vanilla}} \quad \underbrace{00}_{\text{raspberry}} \quad \underbrace{00}_{\text{hazelnut}}.$$

$$\underbrace{00}_{\text{chocolate}} \quad 1 \quad \underbrace{}_{\text{lemon}} \quad 1 \quad \underbrace{000000}_{\text{vanilla}} \quad 1 \quad \underbrace{00}_{\text{raspberry}} \quad 1 \quad \underbrace{00}_{\text{hazelnut}}$$

Doughnuts example

Example (Contd.)

$$\underbrace{00}_{\text{c}} \quad 1 \quad \underbrace{}_{\text{l}} \quad 1 \quad \underbrace{000000}_{\text{v}} \quad 1 \quad \underbrace{00}_{\text{r}} \quad 1 \quad \underbrace{00}_{\text{h}}.$$

We just formed a 16-bit sequence containing exactly 4 ones:

$$0011000000100100$$

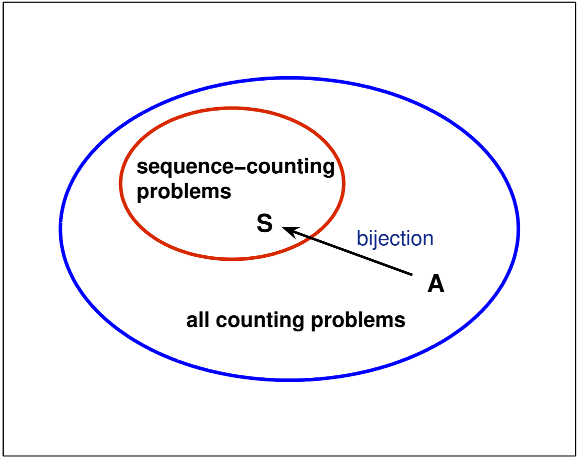
There is a bijection from set A to set B: map 12 doughnuts consisting of c chocolate, l lemon, v vanilla, r raspberry and h hazelnut to the sequence

$$\underbrace{0\dots0}_{\text{c}}1\underbrace{0\dots0}_{\text{l}}1\underbrace{0\dots0}_{\text{v}}1\underbrace{0\dots0}_{\text{r}}1\underbrace{0\dots0}_{\text{h}},$$

a sequence containing 16 bits and 4 ones.

By **Mapping Rule** we have $|A| = |B|$.

Previous example and **Mapping Rule** suggest the following: learn to count really well just few things and then use bijections to count everything else.



- A set is an **unordered** collection of **distinct** elements.

  For example $\{a, b, c\}$ is a set, and $\{c, a, b\}$ is the same set.
  On the other hand $\{a, b, a\}$ is not a set since a appears twice.

- A sequence is an **ordered** collection of elements (called *components* or *terms*) that are **not necessarily distinct**.

  For example, (a, b, c) and (c, a, b) are two different sequences. Moreover, (a, b, a) is a valid 3-element sequence.

Definition

A $k-$**sequence** is a sequence containing exactly k terms. A $2-$sequence is also called a pair.
A $3-$sequence is called a triple.
A $k-$**bit sequence** is a $k-$sequence whose terms are bits, either 0 or 1.

Sum rule

Example

A good computer science student has 10 books on math, 35 books on programming and 15 books on algorithms. How many books does he/she have?

Let set M to be the set of math books, P be the set of programming books and A be the set of of books on algorithms. In these notations, we are asked to find $|M \cup P \cup A|$.

Theorem (Sum Rule)

If $A_1, A_2, \ldots, A_n$ are **disjoint** *sets, then*

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

$$|M \cup P \cup A| = |M| + |P| + |A| = 10 + 35 + 15 = 60.$$

Product rule

Definition

Let P_1, P_2, ..., P_n be sets, then **cartesian product** of theses sets is

$$P_1 \times P_2 \times \ldots \times P_n = \{(p_1, p_2, \ldots, p_n) \mid p_i \in P_i\}.$$

Theorem (Product Rule)

If P_1, P_2, ..., P_n are sets, then

$$|P_1 \times P_2 \times \ldots \times P_n| = |P_1| \cdot |P_2| \cdot \ldots \cdot |P_n|.$$

Product rule does not require the sets to be disjoint.

Product rule

Example

Suppose that a daily student diet consists of breakfast selected from list B, a lunch selected from list L and a dinner from set D:
$B = \{$pancakes, scrambled eggs, sandwich, cereals$\}$;
$L = \{$soup, garden salad, schnitzel and fries, coffee and coffee$\}$;
$D = \{$pasta and fish, pizza, fried pork and mashed potatoes, burger and fries, polenta$\}$

Then $B \times L \times D$ is the set of all possible daily diets.

Here are some sample daily diets:
(scrambled eggs, soup, pizza);
(cereals, garden salad, polenta and stuff);
(sandwich, coffee and coffee, fried pork and mashed potatoes).

Thus, according to **Product Rule**, we have

$$|B \times L \times D| = 4 \cdot 4 \cdot 5 = 80.$$

Product rule

How many different 7-digit phone numbers

can be created?

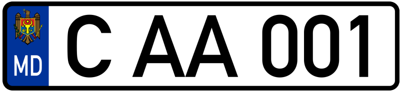
Keep in mind that a phone number can't start with digit 0.

Define sets:

$$F = \{1, \dots, 9\},$$
$$D = \{0, 1, \dots, 9\}.$$

Answer:

$$\left|F \times D^6\right| = 9 \cdot 10^6.$$



How many different plates in this format can be issued in R. Moldova?

$$C = \{\text{all counties}\},$$
$$S = \{A, B, \dots, Z\},$$
$$D = \{001, 002, \dots, 999\}.$$

$$\begin{aligned}\left|C \times S^2 \times D\right| &= 43 \cdot 26^2 \cdot 999 \\ &= 29038932.\end{aligned}$$

Putting rules together. Password example

Example

On a computer system a valid password is a sequence of between 6 and 8 symbols. 1st symbol must be a letter (lowercase or uppercase), remaining are either letters or digits. How many different passwords are possible? Define sets:

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

Set of all possible passwords is (disjoint union): $\left(F \times S^5\right) \cup \left(F \times S^6\right) \cup \left(F \times S^7\right)$.

$$\begin{aligned} \left|\left(F \times S^5\right) \cup \left(F \times S^6\right) \cup \left(F \times S^7\right)\right| &= \left|F \times S^5\right| + \left|F \times S^6\right| + \left|F \times S^7\right| \\ &= 52 \cdot 62^5 + 52 \cdot 62^6 + 52 \cdot 62^7 \\ &\approx 1.8 \cdot 10^{14} \text{ different passwords.} \end{aligned}$$

Worst passwords in UK (2006)

Here is the list:

- 10. thomas (0.99%)
- 9. arsenal (1.11%)
- 8. monkey (1.33%)
- 7. charlie (1.39%)
- 6. qwerty (1.41%
- 5. 123456 (1.63%)
- 4. letmein (1.76%)
- 3. liverpool (1.82%)
- 2. password (3.78%)
- 1. 123 (3.784%)

- If you are using any of these please turn off your computer immediately, go take a nap and then change your password to a smarter one. Or use one of existing programs to generate it.
- If you are stubborn and/or in love with your password, then go out and hand in your wallet to the first pickpocket thief!

Worst passwords by Forbes (2019)

Here is the list:

- 10. qwerty
- 9. asdf
- 8. g_czechout
- 7. zinch
- 6. 12345678
- 5. password
- 4. test1
- 3. 123456789
- 2. 123456
- 1. 12345

- Just remember that with a small investment of 500 Euro and a simple program you can check up to $8.2 \cdot 10^9$ passwords per second.
- And guess what passwords will be checked first ...

Subsets of an n-element set

How many different subsets of an n-element set X are there?

There is a natural bijection from subsets of X to $n-$bit sequences.

Let $X = \{x_1, x_2, \ldots x_n\}$.

Then a particular subset of X maps to the sequence $(b_1, b_2, \ldots, b_n)$, where $b_i = 1$ if and only if x_i is in that subset, and $b_i = 0$ otherwise.

For example, if there are 10 elements in set X, then

$$\{x_2, x_3, x_6, x_9\} \rightarrow 0110010010.$$

There are as many subsets as different $n-$bit sequences.
How many such sequences do exist?

If $B = \{0, 1\}$, then the set of all $n-$bit sequences is

$$\underbrace{B \times B \times \ldots \times B}_{n \text{ times}} = B^n,$$

$$|B^n| = |B|^n = 2^n \qquad \text{by Product Rule.}$$

Pigeonhole Principle

Old puzzle: *A drawer in a dark room contains red socks, green socks and blue socks. How many socks must you withdraw to be sure that you have a matching pair?*

Clearly, picking out three socks is not enough. You might end up with one red, one green and one blue socks.

The solution of this and many other problems rely on the **Dirichlet Principle** or **Pigeonhole Principle**, which is a consequence of the Mapping Rule.

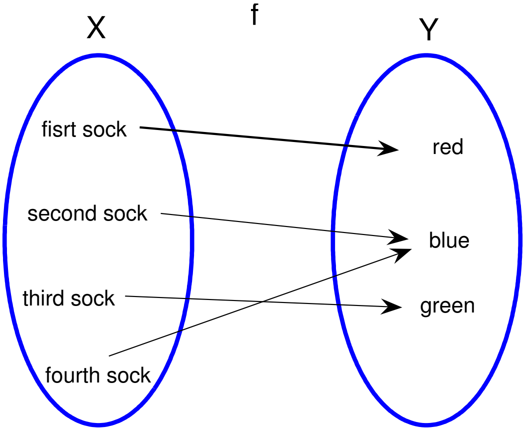
Pigeonhole or Dirichlet Principle

If $|X| > |Y|$, then for every function $f : X \to Y$, there exist two different elements of X that are mapped to the same element of Y.

Pigeonhole Principle. Not so many pigeons

Pigeonhole Principle. Too many pigeons

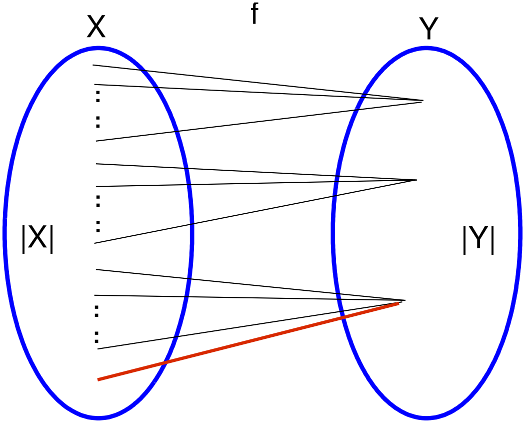
Let X be the set of socks and Y be the set of available colors.



The Pigeonhole Principle states that if $|X| > |Y| = 3$, then at least 2 elements of X must be mapped to the same element of Y.

Generalized Pigeonhole Principle

If $|X| > k \cdot |Y|$, then every function $f : X \to Y$ maps at least $k+1$ different elements of X that are mapped to the same element of Y.



Hairs on heads problem

If you pick two people at random, surely, there are extremely small chances that they have the same amount of hairs on their heads.

However, in Chisinau, there are actually four people who have exactly the same amount of hairs!

Chisinau has about $700,000$ non-bald people, and the number of hairs on a person's head is at most 200000.

Let X be the set of non-bold people in Chisinau and $Y = \{1, 2, \ldots, 200000\}$ and let f map each person to the number of hairs on his/her head.

Since $|X| > 3\,|Y|$, the Generalized Pigeonhole Principle implies that at least four people will have the same number of hairs.

I don't know them, but I know for sure that they exist!

Counting example revisited

7820480135385502964448038	3171004832173501394113017	5763257331083479647409398	8247331000042995311646021
4894459918669156762409921	3208234421597368647019265	5800949123548989122628663	8496243997123475922766310
1082662032430379651370981	3437254656355157864869113	6042900801199280218026001	8518399140676002660747477
1178480894769706178994993	3574883393058653923711651	6116171789137737896701405	8543691283470191452333763
1253127351683239693851327	3644909946040480189969149	6144868973001582369735121	8675309258374137092461352
1301505129234077811069011	3790044132737084094417246	6247314593851169234746152	869432111236399686296665
1311567111143866433882194	3870332127437971355322815	6814428944266874963488274	8772321203608477245851154
1470029452721203876862144	4080505804577801451363100	6870852945543886849147881	8791422161722582546341091
1578271047286257499433886	4167283461025723481249203	6914955508120950093732397	9062628024592126283973285
1638243921852176243192354	4235996831123777788211249	6949632451369871524235413	9137845566925526349897794
1763580219131985963102365	4670939445749439042111220	7128211143613619828415650	915376296603189291934419
1826227795601842231029694	4815379351865384279613427	7173920083651862307925394	9270880194077636406984249
1843971826751020372014203	4837052948212922604442190	7215654874211755676220587	9324301480722103490379204
2396951193722134526177237	5106384238550185506715309	7256932847164391040233050	9436090832146695147140581
2781394568268599801096354	5142368192004769218069910	7332226570752354316203178	9475308159734538249013238
2796605196713610405408019	5181234096130144084041856	7426441829541573444964139	942376623917486974923202
2931016394761975263190347	5198267398125617994391348	7632198126531809327186321	9511972558779880288252979
9334580582944051551972967	5317592940316231219758372	7712154432211912882310511	9602413424619187112552264
3075514410490975920315344	5384358126771794128356947	7858918664240262356610010	9631217114906129219461111
3111474985252793452860017	5439211712248901995423417	7898156786763212963178679	9908189853102753335981319
3145621587936120118438701	5610379826092838192760458	8147591017037573337886166	9913237476341764299813987
3148901255628881103198549	5632317555465228677676044	8149436716871371161932035	315769310532511128321993

5692168374637019617423712 8176063831682536571306791

Two different subsets of the ninety 25-digit numbers shown above have the same sum!

Counting example revisited

Let X be the collection of all subsets of the 90 numbers in the list.

Every 25$-$digit number is less than 10^{25}. Therefore, the sum of any subset of those 90 numbers is at most $90 \cdot 10^{25}$.

So, let $Y = \left\{0, 1, 2, \ldots, 90 \cdot 10^{25}\right\}$.

Let $f : X \to Y$ that maps any subset of numbers (in X) to its sum (in Y).

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

On the other hand $|Y| = 90 \cdot 10^{25} + 1 \leq 0.901 \cdot 10^{27}$.

Both numbers are enormous, but $|X|$ is a little bit bigger than $|Y|$. By Pigeohole Principle, f maps at least two elements of X to the same element of Y.

In other words, two different subsets must have the same sum!

Binary Search

Here is a game: I think of an animal.
You can ask me 20 questions that take an yes/no answer such as:

- "Does this animal have fur?"
- "Is this animal eating people?"

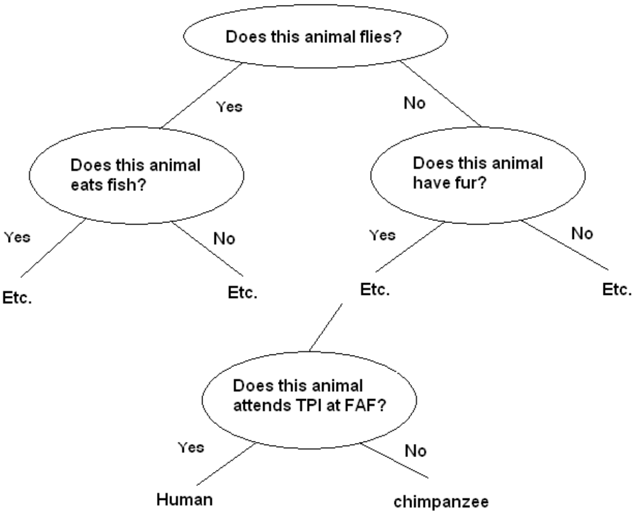
To win the game, you must ask a question like:

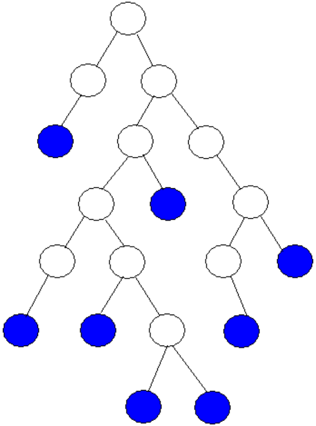
- "Is the animal a dog?"
- "Is this a shark?"
- "Is this animal a human?"

and receive the answer "Yes".

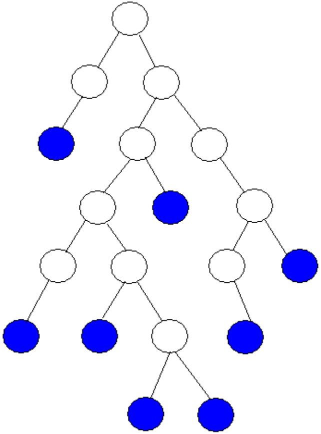
In effect, you have 19 questions to determine the animal I am thinking of, and then you must ask the final question to confirm your guess. Suppose I know a million animals.

Can you always determine which animal I am thinking of?





Any questioning strategy can be represented in a form of a **binary tree**.



Any questioning strategy can be represented in a form of a **binary tree**.

Each internal node in the tree represents a question, and each leaf (vertex of degree 1) represents a final guess.

The binary tree on the left, is of depth six and has eight leaves.

A tree of depth m will have at most 2^m leaves.
Can be proved using mathematical induction over m.

Thus, a depth 19 binary tree can have at most $2^{19} = 524,288$ leaves, and we can use any of 10^6 animals.

There are at most 524288 leaves, and 1000000 animals.

But each animal must be associated to one leaf.

By the Pigeonhole Principle, at least **two** animals must be associated with some leaf in the tree.

Therefore, you can't always determine the animal using only 19 questions.

Generaly, if n animals are known, then $m = \lceil \log_2 n \rceil$ questions are necessary to identify the animal.

Why? (since $2^m = n$).

Otherwise, a binary tree of lower depth must have fewer than n leaves, and some animals will remain unidentified.

Weighing Coins

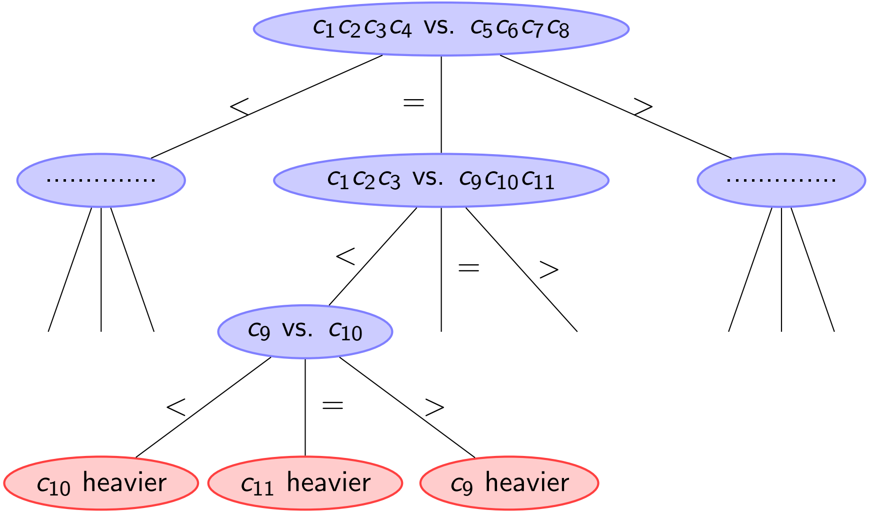
Let's consider the problem of identifying an off-weight counterfeit coin among a collection of coins using a balance scale.

Consider 12 coins of which 11 have the same weight and a counterfeit coin with a different weight.

Using only **three** weighings you must identify the counterfeit coin and determine whether it is lighter or heavier than the rest of the coins.

The strategy can be represented by a ternary tree (next page).

Weighing Coins



Each internal node represents a weighing, and the leaves represent the result.
A run of this algorithm corresponds to a path from the root to a leaf.

In a ternary tree of depth 3 (3 weighing) there are at most $3^3 = 27$ leaves.
For the counterfeit coin we have 2 possible answers: *is it lighter or heavier*.

There are 24 ($2 \cdot 12$ coins) possibilities for 27 leaves. Such a strategy exists.

Can the weighing problem be solved for 14 **coins and** 3 **weighing?**

Since any of the 14 coins could be the counterfeited one, there are 28 possible situations.

We have 28 **pigeons** and 27 **holes** in any strategy ternary tree of depth 3.

Since there are more pigeons than holes, the Pigeonhole Principle implies that some leaf is not associated to a unique situation and for any weighing strategy, there is a pair of cases that this strategy can not distinguish.

Weighing Coins

In general, suppose we have n coins and w weighing.

For a correct weighing strategy to exist, there must be as many leaves as situations.

That is $3^w \geq 2n$, or equivalently $w \geq \log_3(2n)$.

For example, $3 \not\geq \log_3(2 \cdot 14) = \log_3 28 \approx 3.033$

Note that Pigeonhole Principle also implies that for 13 coins and 3 weighing a strategy **may** exist.

It does not exclude the case that the solution can fail to exist.

Actually, the solution does not exist in this case.

Basic strategy for counting

Recall our basic strategy for counting:

1. Learn to count sequences.
2. Translate everything else into a sequence-counting problem via bijection.
3. Just don't be lost in translation!

Generalized Product Rule

Consider a $k-$sequence:

$$\Big(\underbrace{\quad}_{1st \text{ entry}}, \underbrace{\quad}_{2nd \text{ entry}}, \underbrace{\quad}_{3rd \text{ entry}}, \ldots, \underbrace{\quad}_{k-th \text{ entry}} \Big)$$

Theorem (Generalized Product Rule)

Let S be a set of $k-$sequences. If there are:

> n_1 *possible first entries;*
>
> n_2 *possible second entries for each first entry;*
>
> n_3 *possible third entries for each combination of 1st and 2nd entries;*
>
> *etc*

Then,

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

UTM alphabet

How many words of length 3 can be formed from alphabet $\{U, T, M\}$?

By product rule we can form $3^3 = 27$ different words:

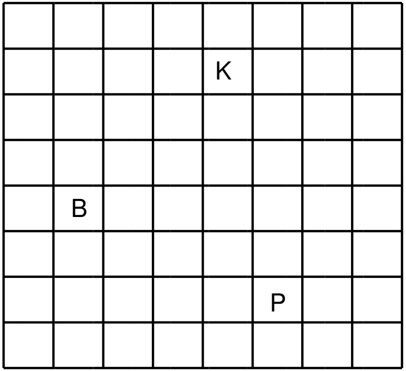
$$UUU, UUT, UUM, UTU, UTT, \ldots, UTM, \ldots, MMM$$

Now, how many words of length 3 can be formed from alphabet $\{U, T, M\}$ such that all letters are different?

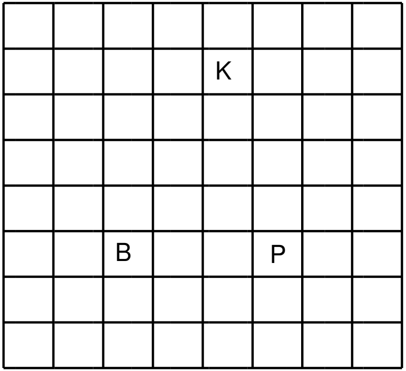
By generalized product rule, we can form $3 \cdot 2 \cdot 1 = 6$ different words:

$$UTM, UMT, TUM, TMU, MUT, MTU$$

In how many ways can we place a pawn, a knight and a bishop on a chessboard such that no two pieces share a row or column?



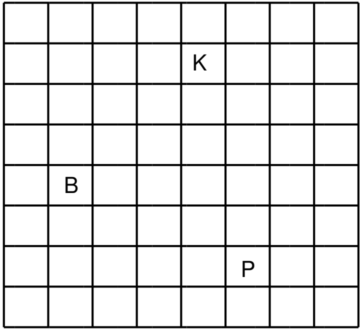
Valid configuration



Invalid configuration

A chess problem

Map this problem to a question about sequences: How many sequences $(r_p, c_p, r_k, c_k, r_b, c_b,)$ exist such that r_p, r_k and r_b are distinct rows and c_p, c_k and c_b are distinct columns.



The above configuration is mapped to $(7, 6, 2, 5, 5, 2)$.
It is a bijection. By **Mapping Rule**, the number of valid configurations is the same as the number of valid sequences.

A chess problem

Count the number of valid sequences using the Generalized Product Rule:

- r_p is one of the 8 rows.
- c_p is one of the 8 columns.
- r_k is one of the 7 rows (any row except the row r_p).
- c_k is one of the 7 columns (any column except c_p).
- r_b is one of the 6 rows (any one but r_p and r_k).
- c_b is one of the 6 columns (any one but c_p and c_k).

Total number of valid configurations is

$$8 \cdot 8 \cdot 7 \cdot 7 \cdot 6 \cdot 6 = 112896.$$

Definition

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

For example, here are all permutations of the set $\{a, b, c\}$:

$$(a, b, c) \quad (a, c, b) \quad (b, a, c) \quad (b, c, a) \quad (c, a, b) \quad (c, b, a).$$

How many permutations of an $n-$element set are there?
For example, as we can see there are 6 permutations of a 3-element set.
Let set S contain n elements and consider an n-sequence:

$$(\underbrace{\quad}_{1st}, \underbrace{\quad}_{2nd}, \underbrace{\quad}_{3rd}, \ldots, \underbrace{\quad}_{n-th})$$

For the $1st$ element in the sequence there are n choices,
for the $2nd$, there are $n-1$ choices (since we can't repeat elements),
for the $3rd$, there are $n-2$ choices, and so forth.

There are $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = \boxed{n!}$ permutations for an n-element set.

Definition

A *k*-**permutation** of a set is a sequence of k distinct elements of that set.

Consider $S = \{a, b, c, d\}$. Then, there are 12 2-permutations of set S:

$$(a, b)\ (a, c)\ (a, d)\ (b, a)\ (b, c)\ (b, d)\ (c, a)\ (c, b)\ (c, d)\ (d, a)\ (d, b)\ (d, c)$$

How many k-permutations of an n-element set are there?

There are n ways to select the 1st element,
$n-1$ ways to select the 2nd element,
$n-2$ to select the 3rd element,
. . . .
$n-k+1$ ways to select the k-th element.

Thus, there are $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1) = \boxed{\frac{n!}{(n-k)!}}$ k-permutations of an $n-$element set.

k-Permutations

Example

How many sequences of six letters with no repetitions are there?
QWERTY is such a sequence.
These sequences are exactly 6-permutations of the set of 26 letters of English alphabet:

$$\tfrac{26!}{20!} = 165\,765\,600.$$

Example

How many injective functions are from set A ($|A| = n$) to set B ($|B| = m$)?
Of course, $n \leqslant m$. Why?See Mapping Rule!
The number of injection functions is (show it!)

$$\frac{m!}{(n-m)!}.$$

Birthday Problem

In a room with k people, what is the probability that at least two people will have the same birthday?

Compute probability that in a room with k people, all people have different birthdays.

Assume that there are 365 possible birthdays. Order people from 1 to k.

The list of their birthdays will be a sequence of length k whose entries will be numbers from the set $S = \{1, 2, \ldots 365\}$.

The number of such sequences by Product Rule is 365^k.

Count the number of $k-$sequences with different entries:
For the 1st entry we have 365 possibilities,
for the 2nd entry we have 364,
for the 3rd entry we have 363,
for the last k-th choice we have $365 - k + 1$ possible values.

By Generalized Product Rule, $365 \cdot 364 \cdot 363 \cdot \ldots \cdot (365 - k + 1) = \frac{365!}{(365-k)!}$.

Problem

Suppose you are entering a room, and making a bet that among those present in the room, at least two will have the same birthday.

How many people should be in a room, such that your bet will be favorable ($P \geqslant 0.5$)?

The probability that in a room with k people at least two people will have the same birthday:

$$P = 1 - \frac{365 \cdot 364 \cdot 363 \cdot \ldots \cdot (365-k+1)}{365^k} = 1 - \frac{365!}{365^k (365-k)!}.$$

k	P
20	0.4114384
21	0.4436883
22	0.4756953
23	0.5072972
24	0.5383443
25	0.5686997

In order to make a favorable bet that in a room with k people, two will have the same birthday, we need 23 people in that room.

Lecture Outline

- Counting General Principle;
- Mapping Rule;
- Sum Rule;
- Product Rule;
- Pigeonhole Principle;
- Generalized Pigeonhole Principle;
- Generalized Product Rule;
- Permutations;
- k- permutations.

There are 3 kind of people:
those who can count and those who can't ...

(Math joke)

There are 10 kind of people:
those who know binary and those who don't ...

(Computer Science joke)

Cei patru apostoli erau următorii trei: Luca și Matei.

(Romanian joke)