Introduction to Discrete Math

Felipe P. Vista IV

Course Outline

- Mathematical Thinking
  - Convincing Arguments, Find Example, Recursion, Logic, Invariants
- Probability & Combinatronics
  - Counting, Probability, Random Variables
- Graph Theory
  - Graphs (cycles, classes, parameters)
- Number Theory & Cryptography
  - Arithmetic in modular form
  - Intro to Cryptography

Mathematical Thinking – Counting

BASIC COUNTING

- Why Counting
- Rule of Sum
- How not to use Rule of Sum
- Convenient Language: Sets
- Generalizing the Rule of Sum

Why Counting?

- Counting is one of the basic tasks in mathematics
- Goal
  - tell how many objects are there without actually counting them one by one
- Used a lot in other parts of mathematics and applications
- Important applications
  - count number of steps of an algorithm
  - compute probabilities

Why Counting?

We have already encountered counting in the previous lecture "What is a Proof?"

- Estimating the running time of algorithms
- Apply the pigeonhole principle

Real Life Example, a Preview

- Suppose a state introduces a new format license plate

https://upload.wikimedia.org/wikipedia/commons/thumb/e/ea/Russian_registration_2621.jpg/799px-Russian_registration_2621.jpg

- Take Russia for example:
  - A letter - three digits – two letters; 177 is regional code
- There are
  - 10 options for digits,
  - 12 options for letters (A, B, E, K, M, H, O, P, C, T, У, X)

Real Life Example, a Preview

- Suppose a state introduces a new format license plate

https://upload.wikimedia.org/wikipedia/commons/thumb/e/ea/Russian_registration_2621.jpg/799px-Russian_registration_2621.jpg

- Take Russia for example:
  - A letter - three digits – two letters; 177 is regional code

А	Б	В	Г	Д	Е
Ё	Ж	З	И	Й	К
Л	М	Н	О	П	Р
С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ъ	Ы	Ь
Э	Ю	Я			

https://en.wikipedia.org/wiki/Russian_alphabet#/media/File:00Russian_Alphabet_3.svg

- Why Counting
- Rule of Sum
- How not to use Rule of Sum
- Convenient Language: Sets
- Generalizing the Rule of Sum

Rule of Sum

If there are k objects of the first type and there are n objects of the second type, then there are $n + k$ objects of one of two types.

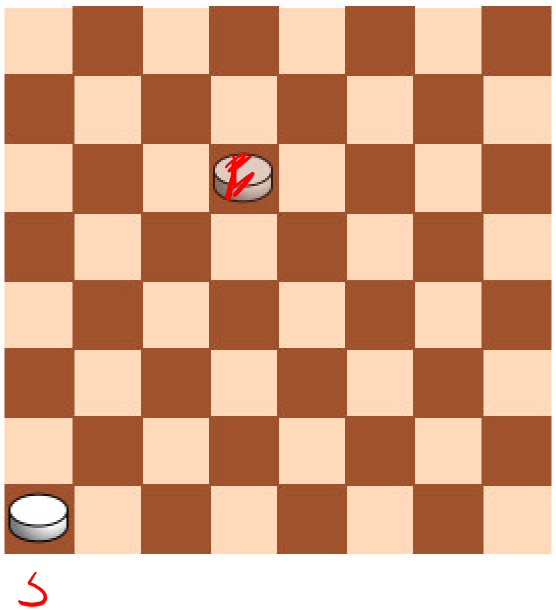
Pizza Parlor

Burger joint

5 + 7 = 12 places to eat in total

Piece on a Chessboard

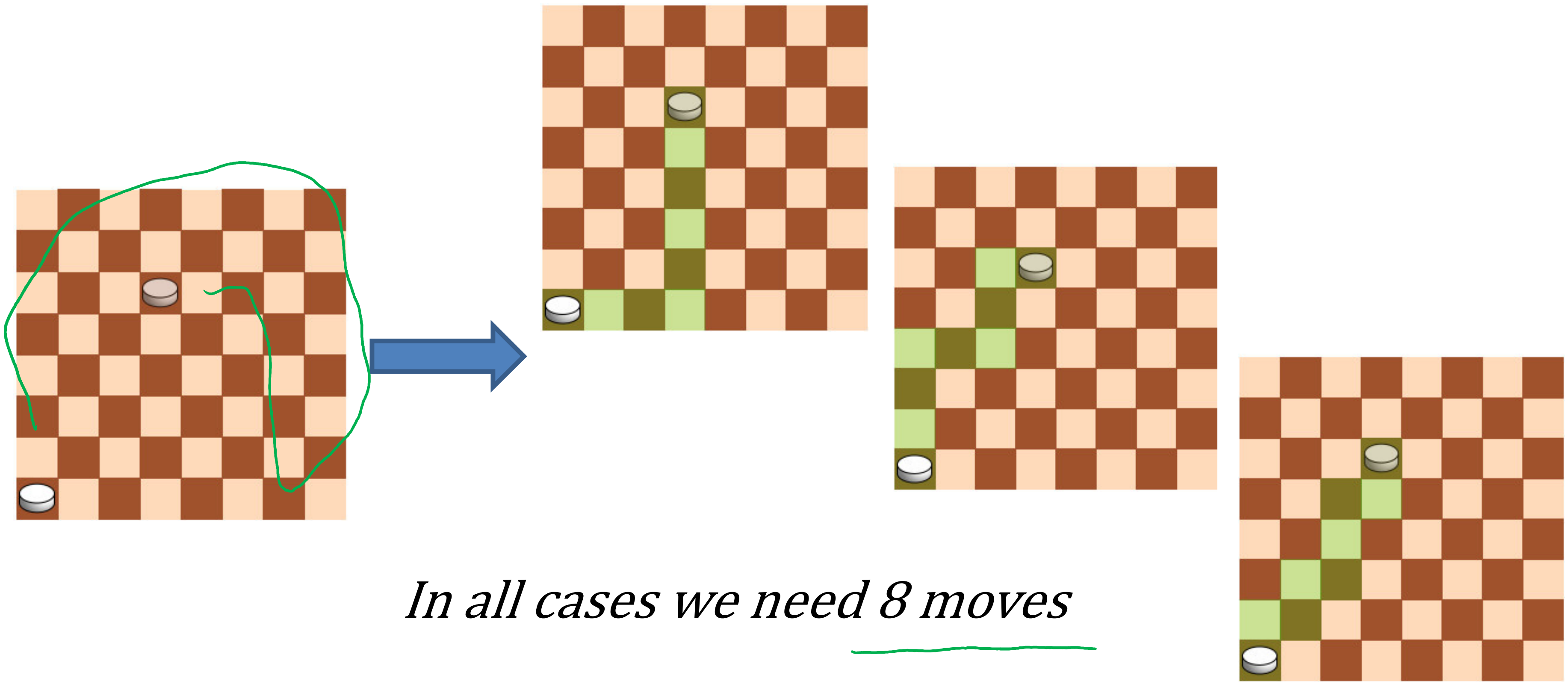
A piece stays in the bottom left corner of a chessboard. It can move one step to the right or one step up at a time. How many moves to get to the position shown?



We have seen this problem in previous lectures

Piece on a Chessboard

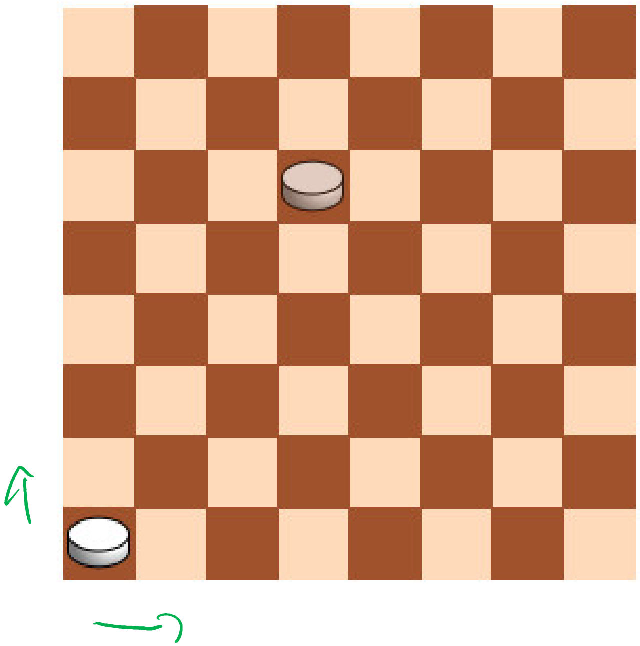
We can do it in several ways



In all cases we need 8 moves

Piece on a Chessboard

We can do it in several ways

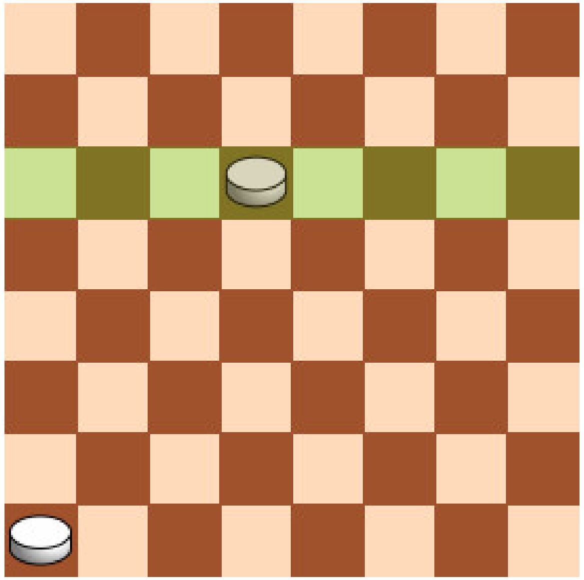


- In all cases we need 8 moves
- This is not a coincidence

1. There are two types of moves
   - go right, go up
2. In order to get to get to column 4
   - 3 moves to the right
3. In order to get to get to row 6
   - 5 moves going up
4. Total number of moves
   - $3 + 5 = 8$ moves

Piece on a Chessboard

We can do it in several ways

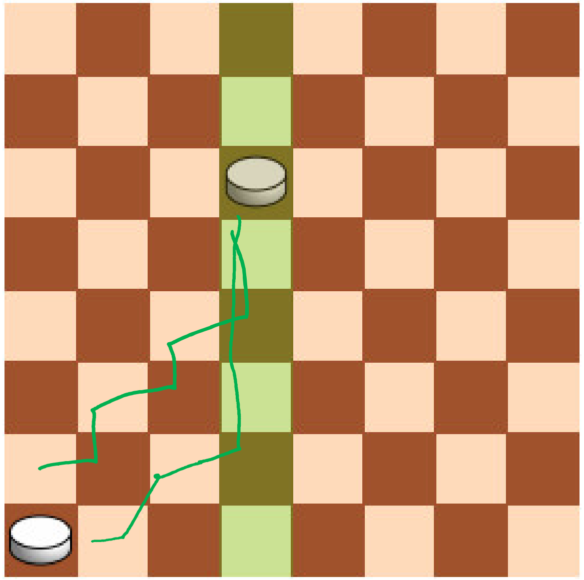


- In all cases we need 8 moves
- This is not a coincidence

1. There are two types of moves
   - go right, go up
2. In order to get to get to column 4
   - 3 moves to the right
3. In order to get to get to row 6
   - 5 moves going up
4. Total number of moves
   - $3 + 5 = 8$ moves

Piece on a Chessboard

We can do it in several ways



- In all cases we need 8 moves
- This is not a coincidence

1. There are two types of moves
   - go right, go up
2. In order to get to get to column 4
   - 3 moves to the right
3. In order to get to get to row 6
   - 5 moves going up
4. Total number of moves
   - 3 + 5 = 8 moves

- Why Counting
- Rule of Sum
- How not to use Rule of Sum
- Convenient Language: Sets
- Generalizing the Rule of Sum

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

- But what if we count directly?

1	2	3	4	5	6	7	8	9	10

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

- But what if we count directly?

1	2	3	4	5	6	7	8	9	10

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

- But what if we count directly?

1	2	3	4	5	6	7	8	9	10

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be 5 + 3 = 8

- But what if we count directly?

1	2	3	4	5	6	7	8	9	10

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

- But what if we count directly?

1	2	3	4	5	6	7	8	9	10

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

- But what if we count directly?

1	2	3	4	5	6	7	8	9	10

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

- But what if we count directly?

1	2	3	4	5	6	7	8	9	10

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

- But what if we count directly?

1	2	3	4	5	6	7	8	9	10

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

- But what if we count directly?
- The answer is 7!

1	2	3	4	5	6	7	8	9	10

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

- But what if we count directly?
- The answer is 7!
- Why??!

1	2	3	4	5	6	7	8	9	10

Divisibility by 2 or 3

Problem

Count all integers from 1 to 10 that are divisible by 2 or by 3…

- Let us attempt to apply the rule of sum
- There are five numbers divisible by 2: 2, 4, 6, 8, 10
- There are 3 numbers divisible by 3: 3, 6, 9
- The answer should be $5 + 3 = 8$

- But what if we count directly?
- The answer is 7!
- Why??! The problem lies with the number "6"

1	2	3	4	5	6	7	8	9	10

Rule of Sum

Revisiting

If there are k objects of the first type and there are n objects of the second type, then there are $n + k$ objects of one of two types.

- Important note re: Rule of Sum
- No object should belong to the same class! :D

- Why Counting
- Rule of Sum
- How not to use Rule of Sum
- Convenient Language: Sets
- Generalizing the Rule of Sum

Convenient Language: Sets

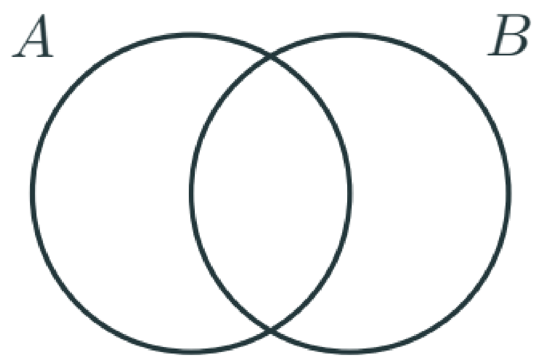
- Set is an arbitrary group of arbitrary objects
- We represent sets by capital letters: A, B, C, S, etc.
- Sets can be given by the list of their elements:
  - $S = \{0, 1, 2, 3\}$; this set consists of four elements: $0, 1, 2, 3$
- The order of elements is not important:
  - $\{0, 1, 2, 3\} = \{2, 0, 3, 1\}$
- Repetitions in the list of elements are not important:
  - $\{0, 1, 2, 3\} = \{1, 0, 1, 3, 2, 3\}$

Convenient Language: Sets

- For us, sets provide convenient language
- In mathematics, play important & fundamental role
- For us, sets can consist of anything:
  - $\mathcal{S} = \{0, \sqrt{2}, \textit{Isaac Newton}, \textit{a leprechaun}\}$
- However, there are pitfalls (danger/ difficulty)
  - "Set consisting of all sets" is a dangerous construction
- We will not encounter these difficulties in the course & will not discuss them

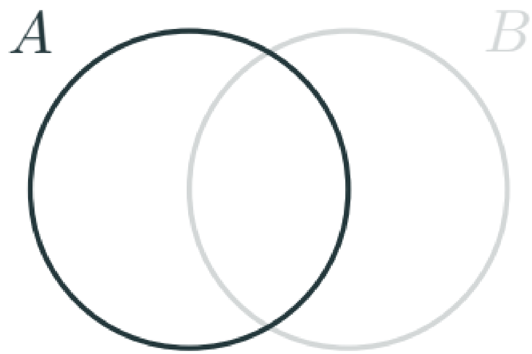
Venn Diagram

- Venn Diagrams
  - Convenient way to view/describe sets



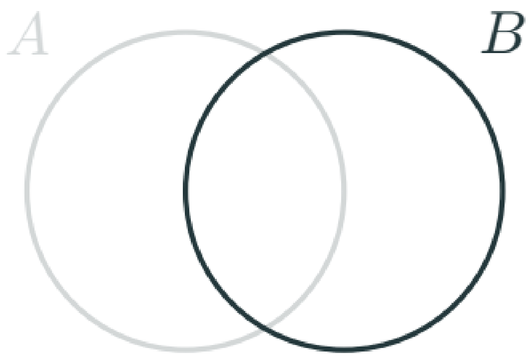
Venn Diagram

- Venn Diagrams
  - Convenient way to view/describe sets
- Elements of A are within the left circle



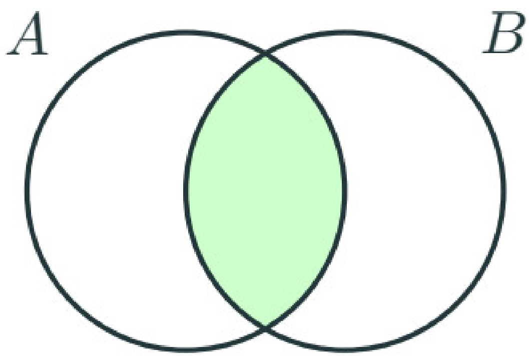
Venn Diagram

- Venn Diagrams
  - Convenient way to view/describe sets
- Elements of A are within the left circle
- Elements of B are within the right circle

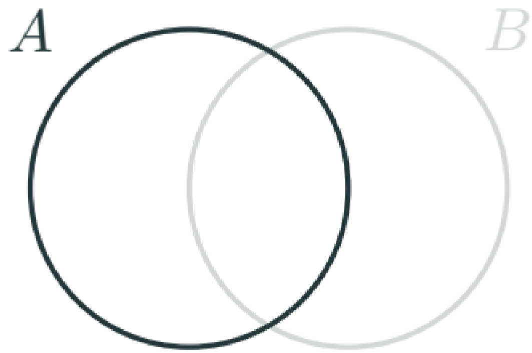


Venn Diagram

- Venn Diagrams
  - Convenient way to view/describe sets
- Elements of A are within the left circle
- Elements of B are within the right circle
- Intersection corresponds to elements belonging to both sets A & B

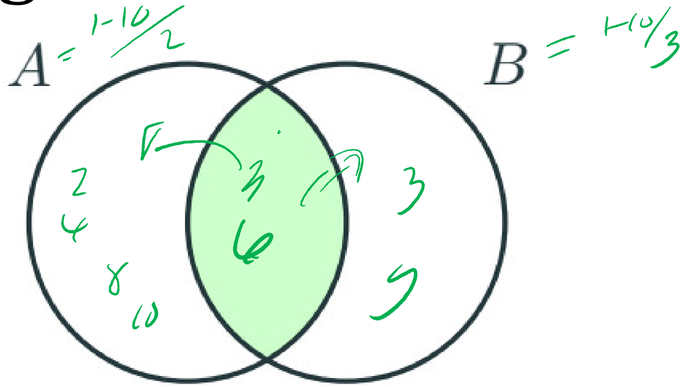


Venn Diagram – Useful Notations



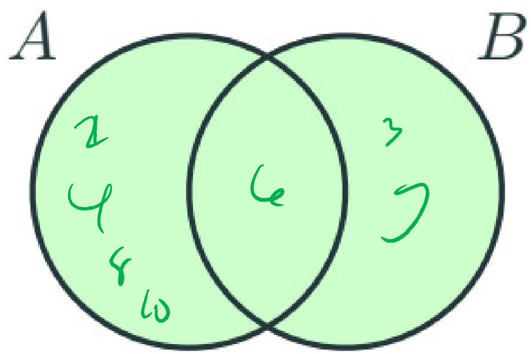
- Suppose we have two sets, A and B

Venn Diagram – Useful Notations



- Suppose we have two sets, A and B
- The set $\boldsymbol{A} \cap \boldsymbol{B}$ is an *intersection* of these sets
  - Consists of elements belonging to both sets

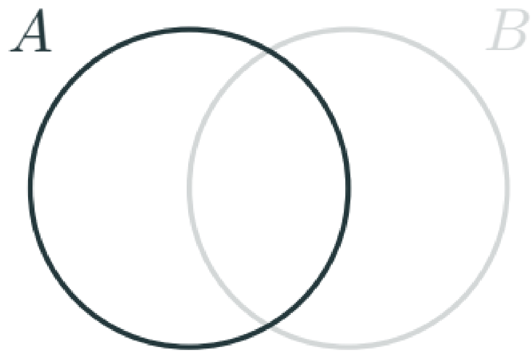
Venn Diagram – Useful Notations



1, 5, 7

- Suppose we have two sets, A and B
- The set $\boldsymbol{A} \cap \boldsymbol{B}$ is an *intersection* of these sets
  - Consists of elements belonging to both sets
- The set $\boldsymbol{A} \cup \boldsymbol{B}$ is a *union* of these sets
  - Consists of elements belong to at least one of the sets

Venn Diagram – Useful Notations



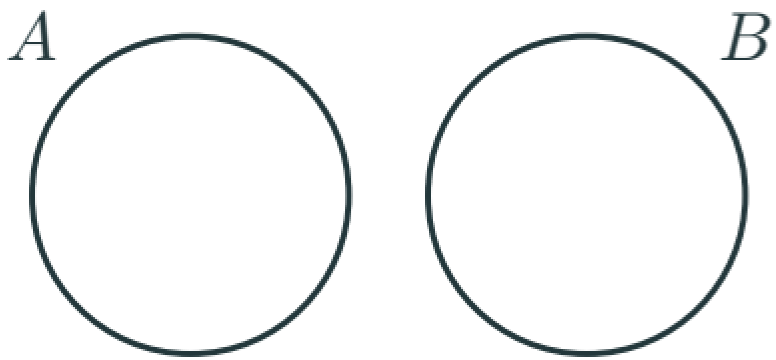
- Suppose we have two sets, A and B
- The set $\boldsymbol{A \cap B}$ is an *intersection* of these sets
  - Consists of elements belonging to both sets
- The set $\boldsymbol{A \cup B}$ is a *union* of these sets
  - Consists of elements belong to at least one of the sets
- Number of elements in Set A is |A|, can be infinite

- Why Counting
- Rule of Sum
- How not to use Rule of Sum
- Convenient Language: Sets
- Generalizing the Rule of Sum

Rule of Sum in the Set Language

Rule of Sum

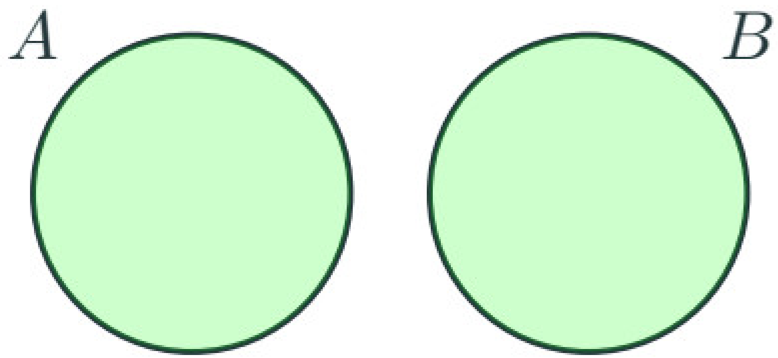
If there is a set A with k elements, a set B with n elements and these sets do not have common elements, then the set $A \cup B$ has $n + k$ elements



Rule of Sum in the Set Language

Rule of Sum

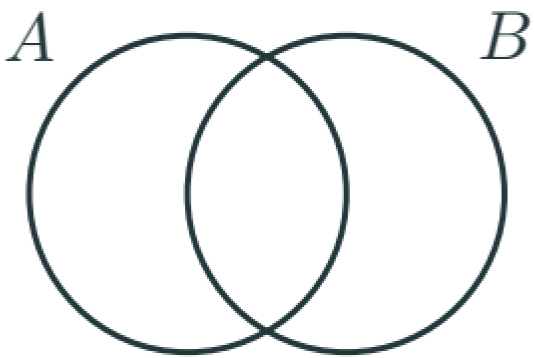
If there is a set A with k elements, a set B with n elements and these sets do not have common elements, then the set $A \cup B$ has $n + k$ elements



Generalized Rule of Sum

Rule of Sum

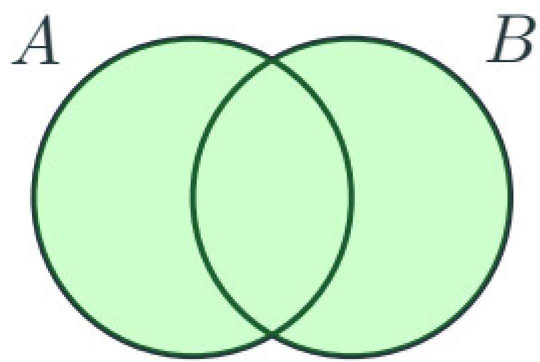
But what if we want to count $|A \cup B|$ as given below?



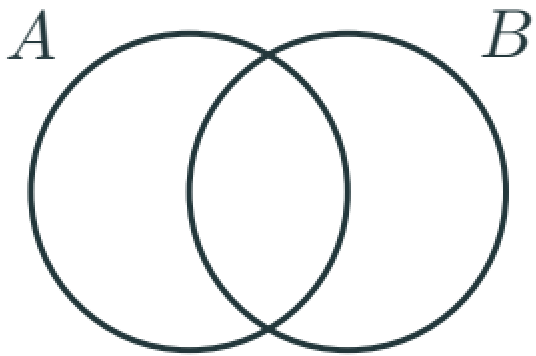
Generalized Rule of Sum

Rule of Sum

But what if we want to count $|A \cup B|$ as given below?

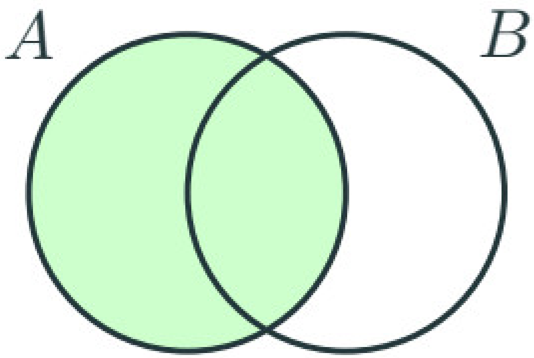


Generalized Rule of Sum



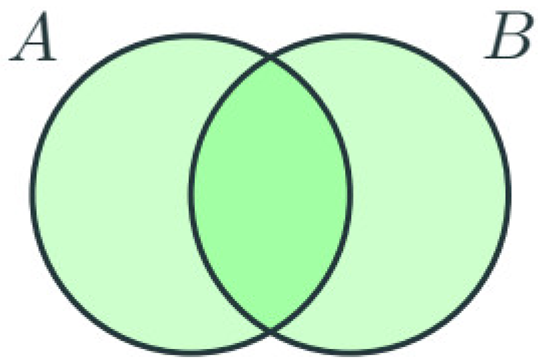
- If we just consider $|A| + |B|$ as in the rule of sum, then we will be wrong

Generalized Rule of Sum



- If we just consider $|A| + |B|$ as in the rule of sum, then we will be wrong

Generalized Rule of Sum



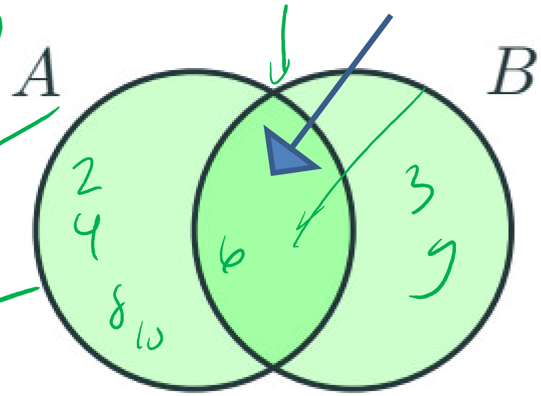
- If we just consider $|A| + |B|$ as in the rule of sum, then we will be wrong

Generalized Rule of Sum

$|A| - |B| = X =$ wrong

$|A| - |B| - |A \cap B| =$ ✓

$5 - 3 - 1 = 7$



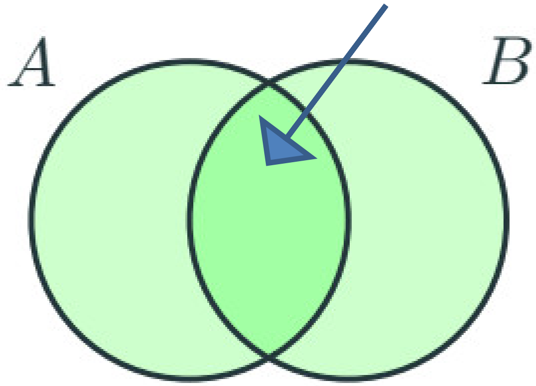
$|A| = 5$

$|B| = 3$

8

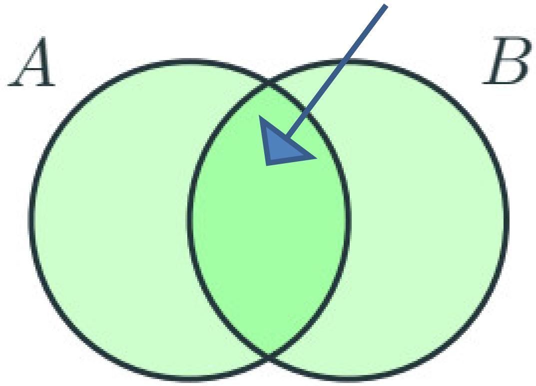
- If we just consider $|A| + |B|$ as in the rule of sum, then we will be wrong
- We will count elements that belong to both A and B twice

Generalized Rule of Sum



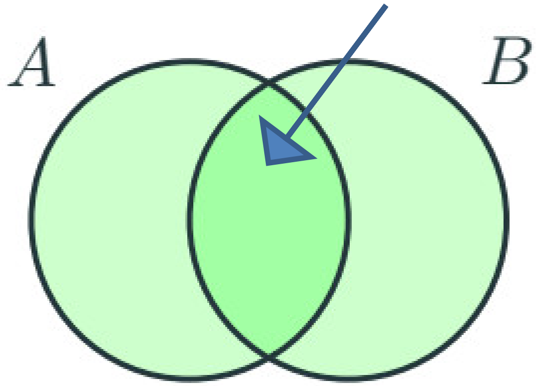
- If we just consider $|A| + |B|$ as in the rule of sum, then we will be wrong
- We will count elements that belong to both A and B twice
- So let's subtract them now!

Generalized Rule of Sum



- If we just consider $|A| + |B|$ as in the rule of sum, then we will be wrong
- We will count elements that belong to both A and B twice
- So let's subtract them now!
- This gives the right result:

Generalized Rule of Sum



- If we just consider $|A| + |B|$ as in the rule of sum, then we will be wrong
- We will count elements that belong to both A and B twice
- So let's subtract them now!
- This gives the right result:
  - $|A \cup B| = |A| + |B| - |A \cap B|$

Summary

- Counting starts with simple things
- But even rule of sum can be tricky
- Next, we will see how to build something more involved from the basic building blocks

Mathematical Thinking – Counting

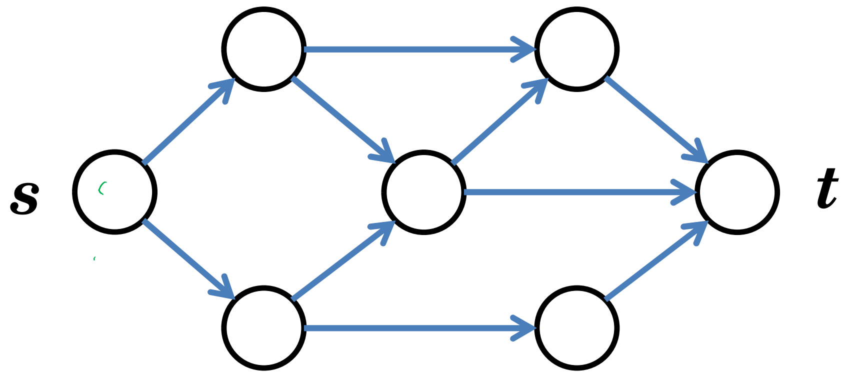
RECURSIVE COUNTING

- Number of Paths
- Rule of Product
- Back to Recursive Counting

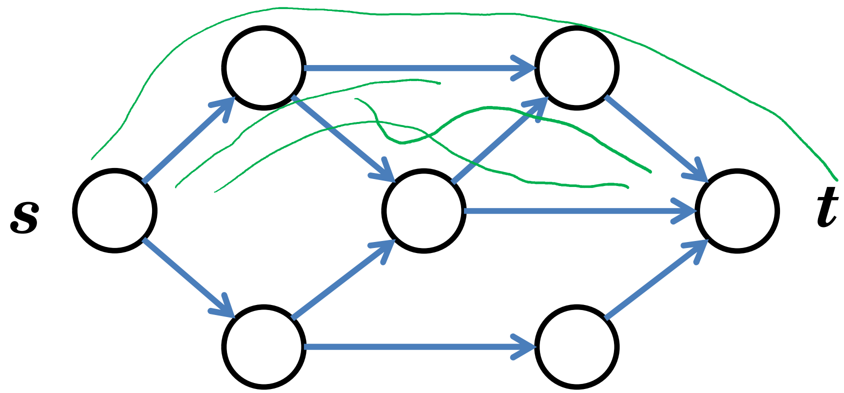
Number of Paths

Problem

- Suppose there are several points connected by arrows. There is a starting point s (called *source*) and a final point t (called *sink*). How many different ways are there to get from s to t?

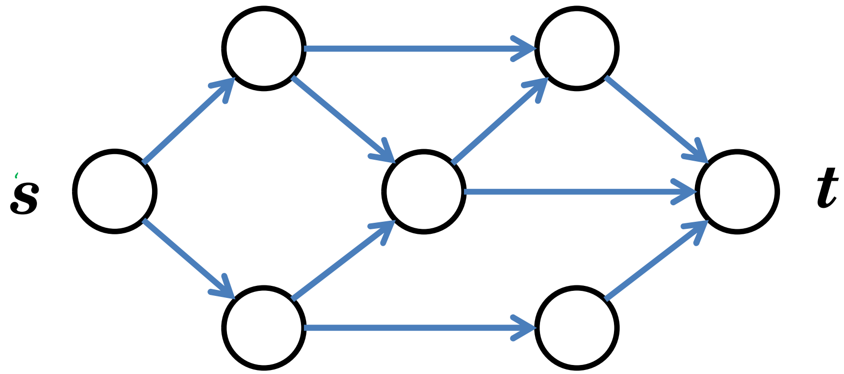


Number of Paths



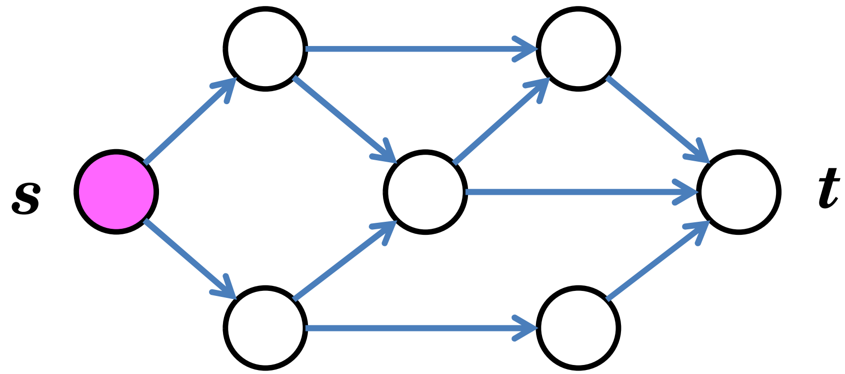
- There are several various paths
  - how not to miss anything when counting?

Number of Paths



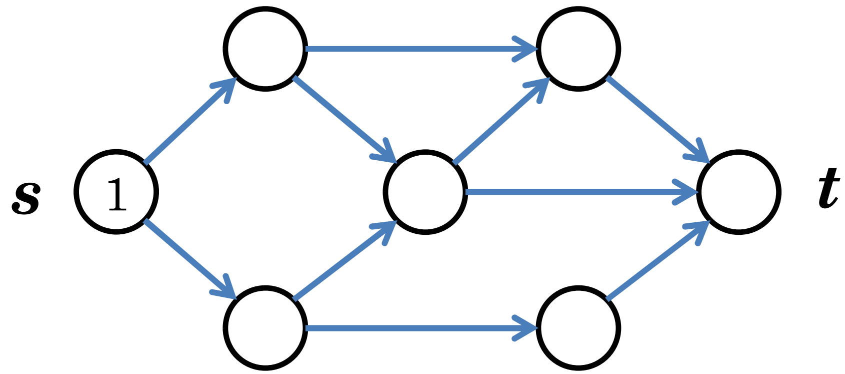
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from s to this node
- We use the rule of sum!

Number of Paths



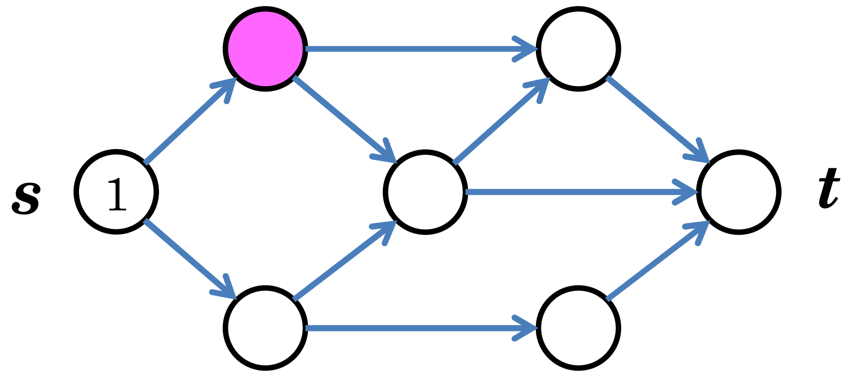
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from s to this node
- We use the rule of sum!

Number of Paths



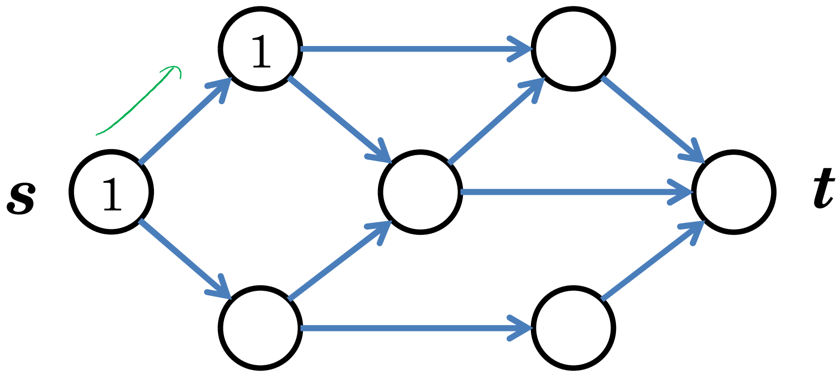
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from *s* to this node
- We use the rule of sum!

Number of Paths



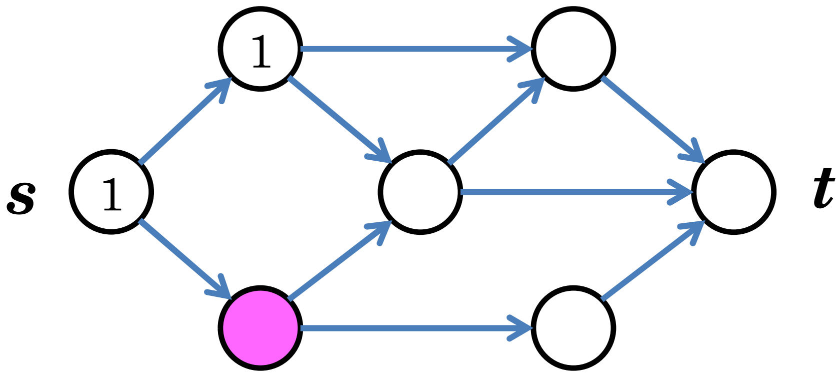
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from s to this node
- We use the rule of sum!

Number of Paths



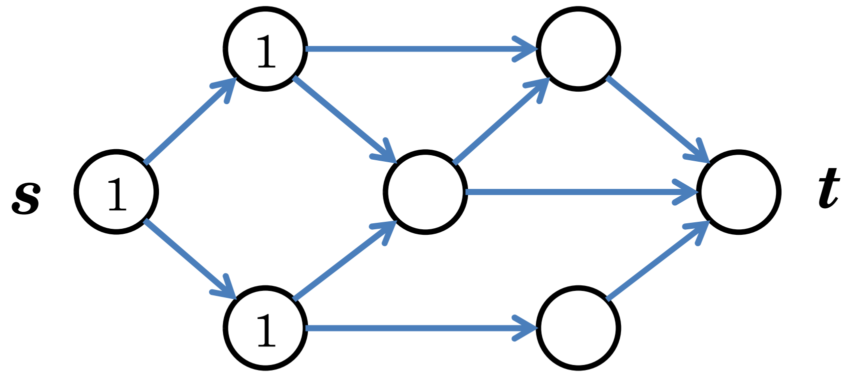
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from s to this node
- We use the rule of sum!

Number of Paths



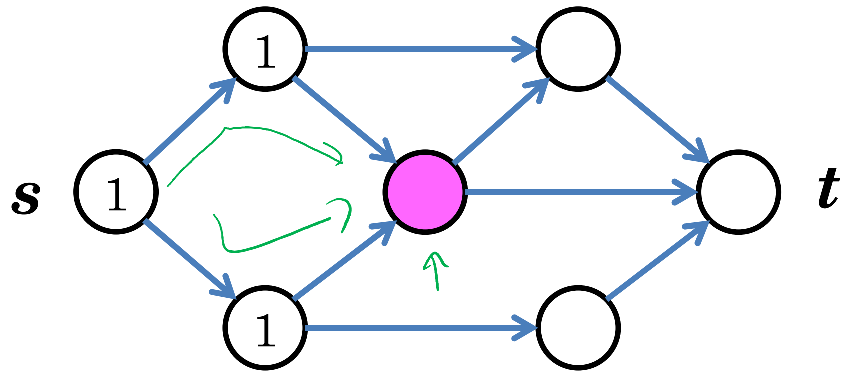
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from *s* to this node
- We use the rule of sum!

Number of Paths



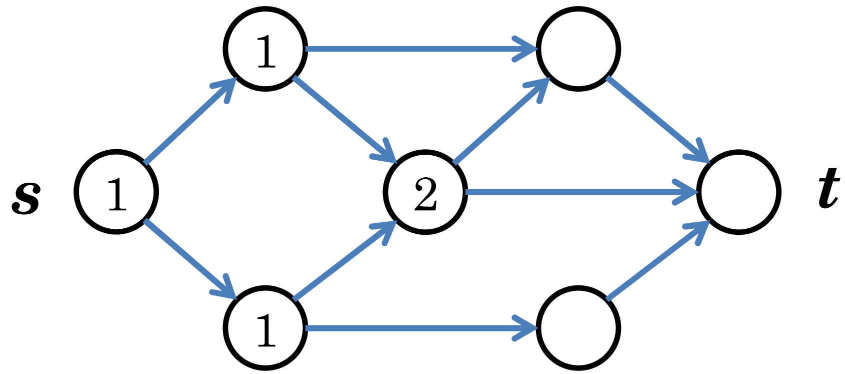
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from s to this node
- We use the rule of sum!

Number of Paths



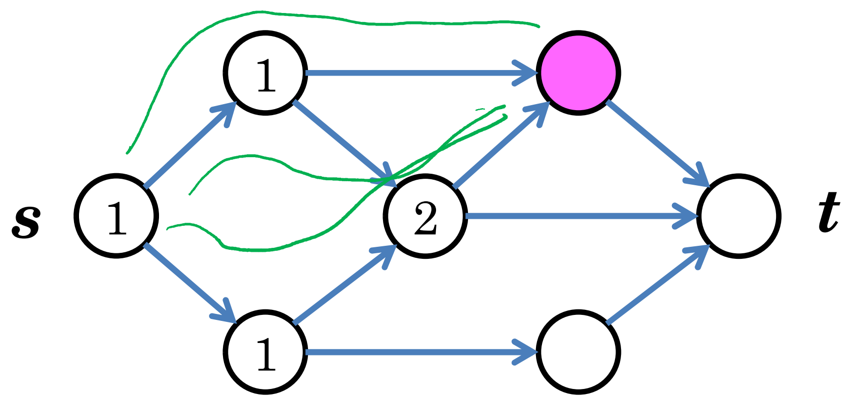
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from s to this node
- We use the rule of sum!

Number of Paths



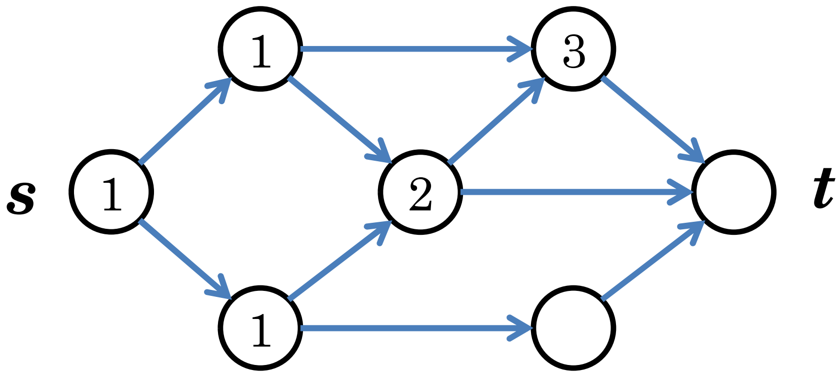
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from s to this node
- We use the rule of sum!

Number of Paths



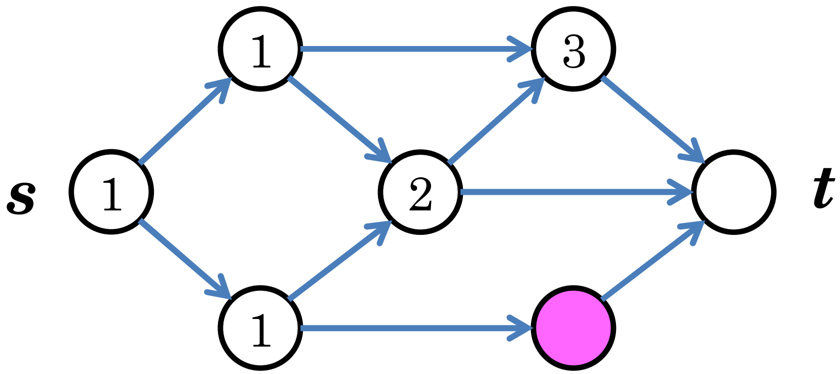
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from *s* to this node
- We use the rule of sum!

Number of Paths



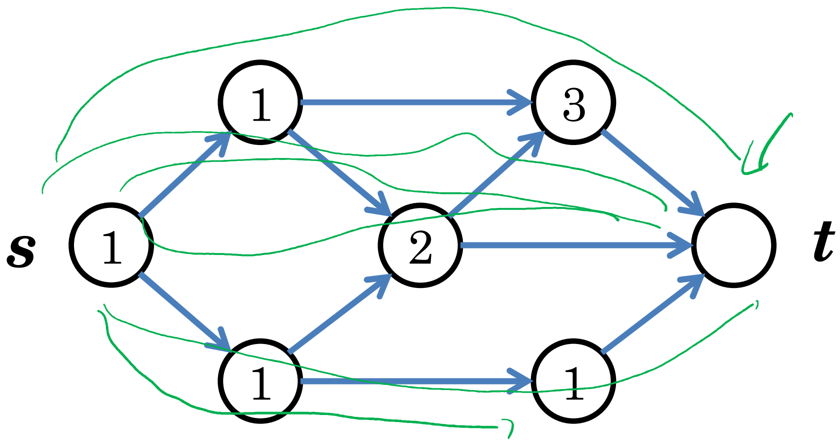
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from s to this node
- We use the rule of sum!

Number of Paths



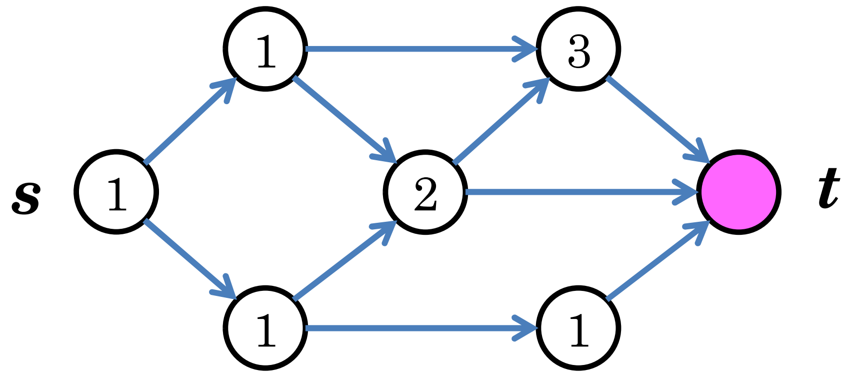
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from *s* to this node
- We use the rule of sum!

Number of Paths



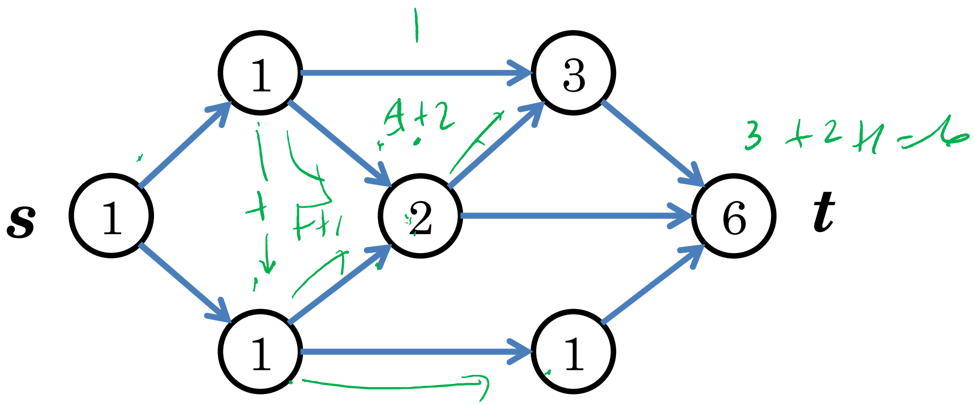
- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from *s* to this node
- We use the rule of sum!

Number of Paths



- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from *s* to this node
- We use the rule of sum!

Number of Paths



- There are several various paths
  - how not to miss anything when counting?
- We can count them **recursively**:
  - for each node count the number of paths from *s* to this node
- We use the rule of sum!

- Number of Paths
- Rule of Product
- Back to Recursive Counting

Rule of Product

Rule of Product

If there are k object of the first type and there are n object of the second type, then there are $k \times n$ pairs of objects, the first of the first type and the second of the second type

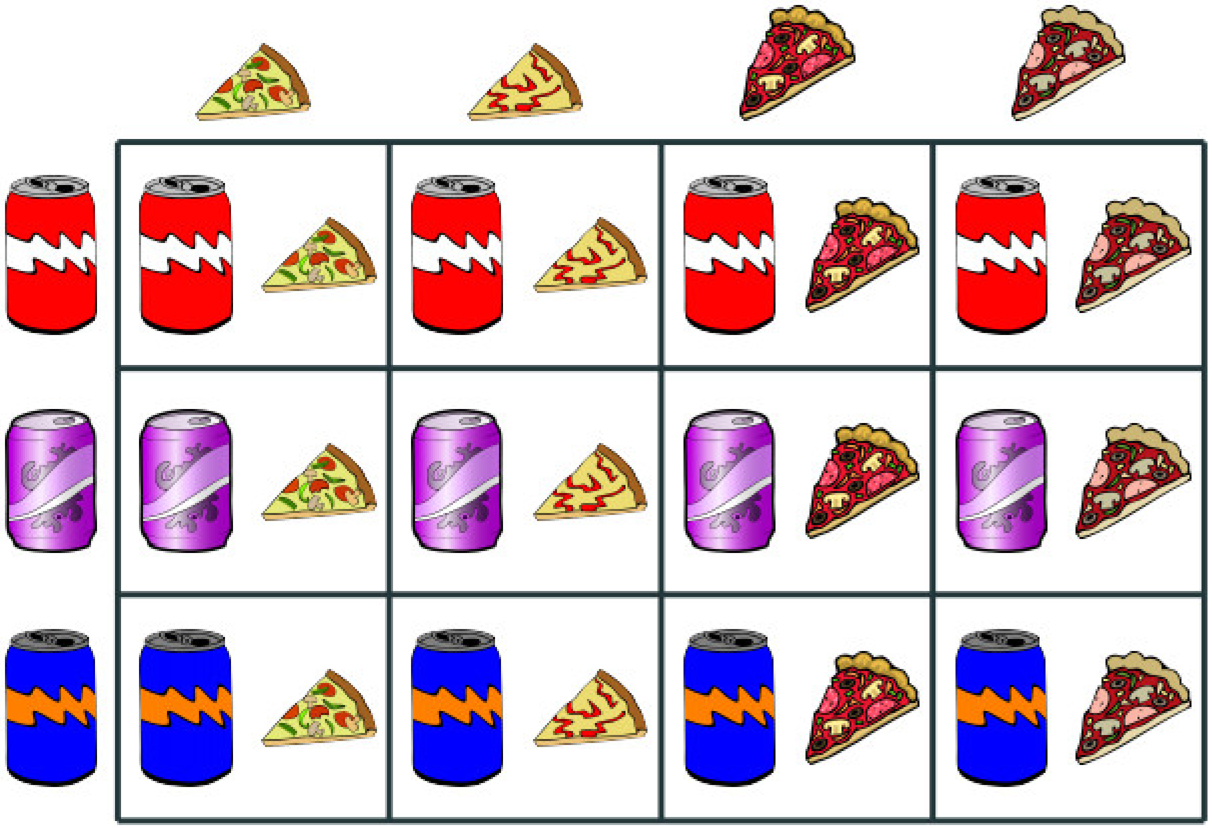
Pizza options

Soda options

4 x 3 = 12 combo options

Rule of Product

All the Combo Options



Rule of Product

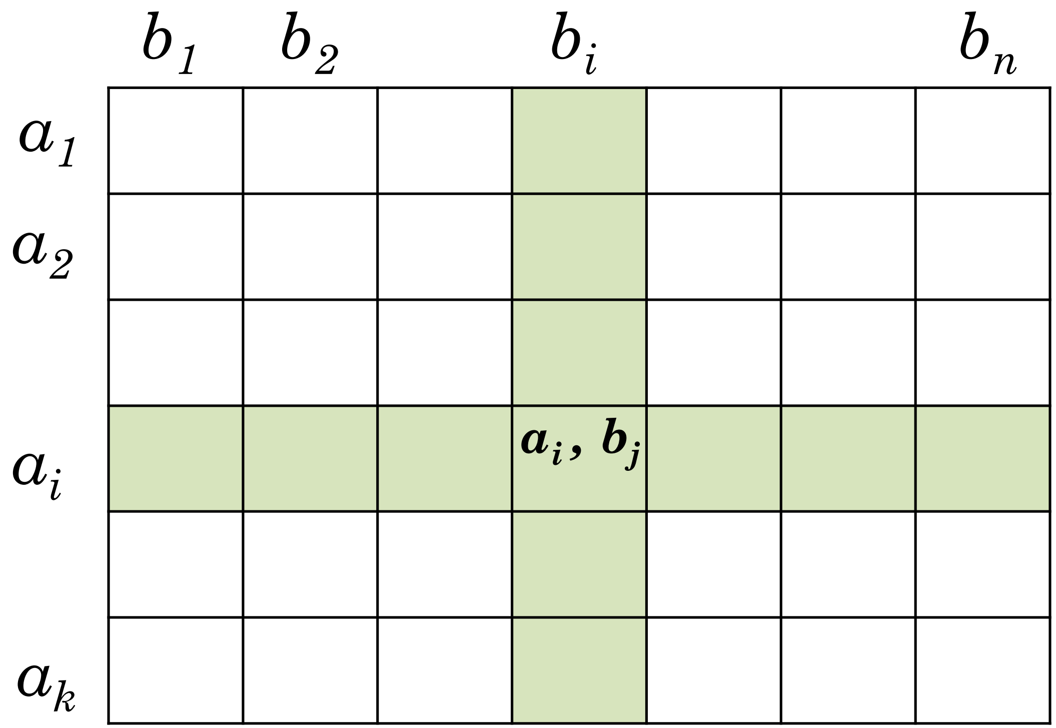
Rule of Product in the Set Language

If there is a finite set A and a finite set B, then there are $|A| \times |B|$ pairs of objects, the first from A and the second from B

Why the Rule of Product is True?

$$A = \{a_1, \cdots, a_k\}$$

$$B = \{b_1, \cdots . b_n\}$$



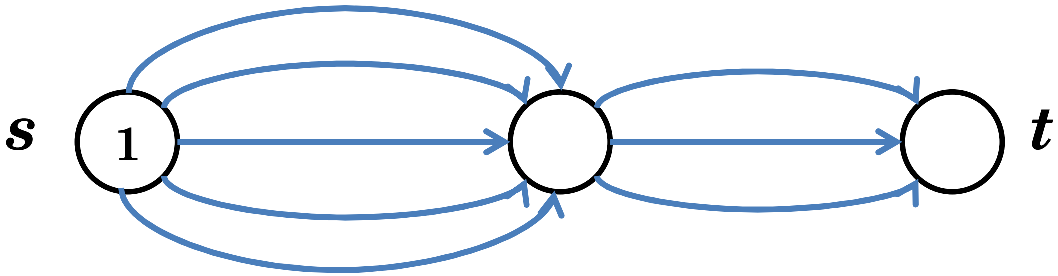
There are as many pairs as cells in this table

- Number of Paths
- Rule of Product
- Back to Recursive Counting

Back to Recursive Counting

Multiple Paths

How many possible paths from ~~*A*~~ s to ~~*B*~~ t?



Back to Recursive Counting

Rule of Product as the Number of Paths

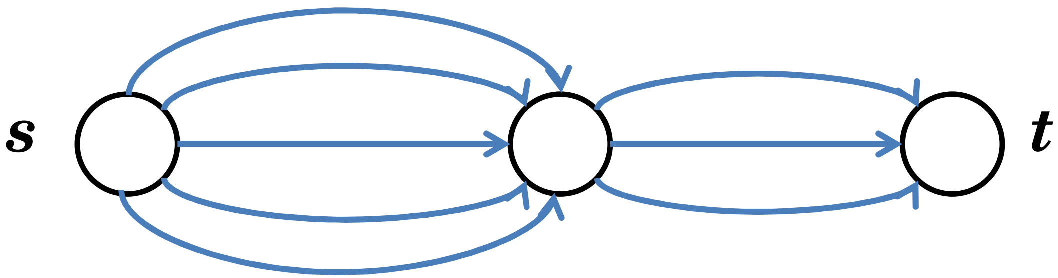
If there is a finite set A and a finite set B, then there are $|A| \times |B|$ pairs of objects, the first from A and the second from B

- Can we express this counting rule in terms of counting the number of paths?

Rule of Product as the Number of Paths

If there is a finite set A and a finite set B, then there are $|A| \times |B|$ pairs of objects, the first from A and the second from B.

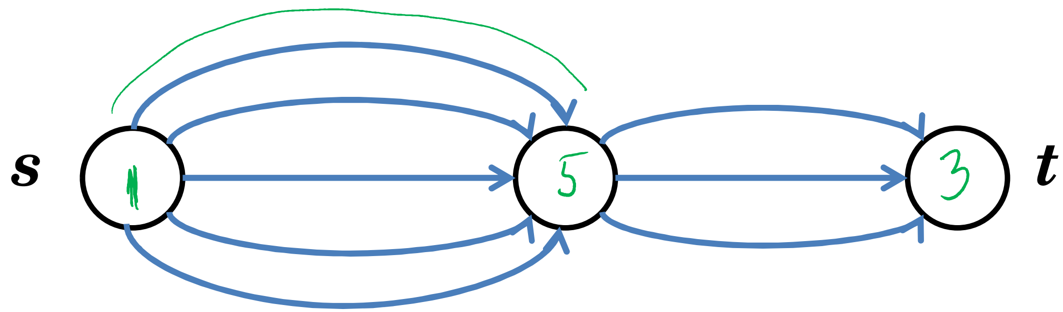
- Consider for simplicity $|A| = 5$ and $|B| = 3$



Rule of Product as the Number of Paths

If there is a finite set A and a finite set B, then there are $|A| \times |B|$ pairs of objects, the first from A and the second from B

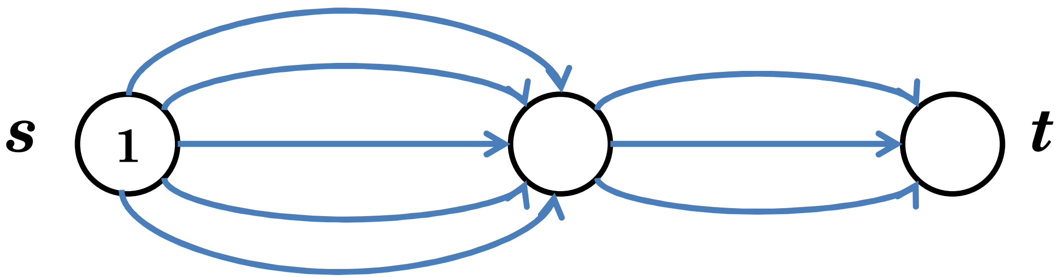
- Consider for simplicity $|A| = 5$ and $|B| = 3$



Rule of Product as the Number of Paths

If there is a finite set A and a finite set B, then there are $|A| \times |B|$ pairs of objects, the first from A and the second from B

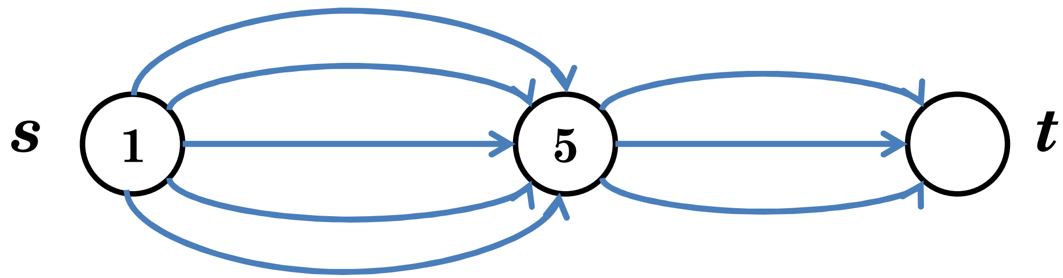
- Consider for simplicity $|A| = 5$ and $|B| = 3$



Rule of Product as the Number of Paths

If there is a finite set A and a finite set B, then there are $|A| \times |B|$ pairs of objects, the first from A and the second from B

- Consider for simplicity $|A| = 5$ and $|B| = 3$

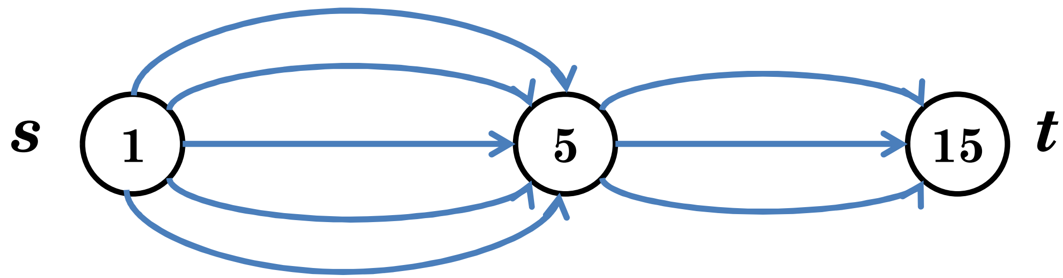


$1 + 1 + 1 + 1 + 1 = 5$

Rule of Product as the Number of Paths

If there is a finite set A and a finite set B, then there are $|A| \times |B|$ pairs of objects, the first from A and the second from B

- Consider for simplicity $|A| = 5$ and $|B| = 3$



5 + 5 + 5 = 5 x 3 = 15

Thank you.