Discrete Algebraic Structures

WiSe 2025/2026

Prof. Dr. Antoine Wiehe
Research Group for Theoretical Computer Science

Organizational things

- Registration for the exam is now open (until December 14)
  Register on TUNE
- Also register for the Studienleistung if not done already (and if you can)
- Exam on March 10 (whole day, in groups of ~ 100)

Exam has 2 parts:

- **Part 1** (around 100 points): mostly multiple choice questions + numerical questions
- Multiple choice questions: negative points for wrong answers
  DO NOT TRY TO GUESS

- Registration for the exam is now open (until December 14)
  Register on TUNE
- Also register for the Studienleistung if not done already (and if you can)
- Exam on March 10 (whole day, in groups of ~ 100)

Exam has 2 parts:

- **Part 1** (around 100 points): mostly multiple choice questions + numerical questions
- Multiple choice questions: negative points for wrong answers
  DO NOT TRY TO GUESS
- Also some questions with computations (just enter a number)
- **Part 2** (around 100 points): proofs

Strategy to not fail:

- Focus on Part 1: enough points to get a 2.0-2.3 if done perfectly
- Part 2 only for those of you who hope to get $1.x$
  Do not attempt if you are not confident with writing proofs (points are not easy to get)

- Countable sets, uncountable sets
- Countable sets = what can be represented exactly on a computer
- Combinatorial proofs as a way to prove equalities/inequalities about numbers using functions

$$\begin{aligned} \text{Injection } A \to B \quad &\leftrightarrow \quad |A| \leq |B| \\ \text{Surjection } A \to B \quad &\leftrightarrow \quad |A| \geq |B| \\ \text{Bijection } A \to B \quad &\leftrightarrow \quad |A| = |B| \end{aligned}$$

- Drawing a tuple/(multi)set with/without replacement
  n = size of the set we are drawing from
  k = number of draws

	Order matters	Order does not matter
Replacement	n^k	$\binom{n+k-1}{n-1}$
No replacement	$n^{\underline{k}}$	$\frac{n!}{k!(n-k)!}$

3 "advanced" proof techniques for counting:

- Double counting
- The inclusion-exclusion principle
- Application: counting partitions and surjective functions
- The pigeonhole principle and Ramsey's theorem

Talk about asymptotic growth of counting functions

Idea:

- we know if $f: A \to B$ is bijective, then $|A| = |B|$
- what can we do with relations instead of functions?

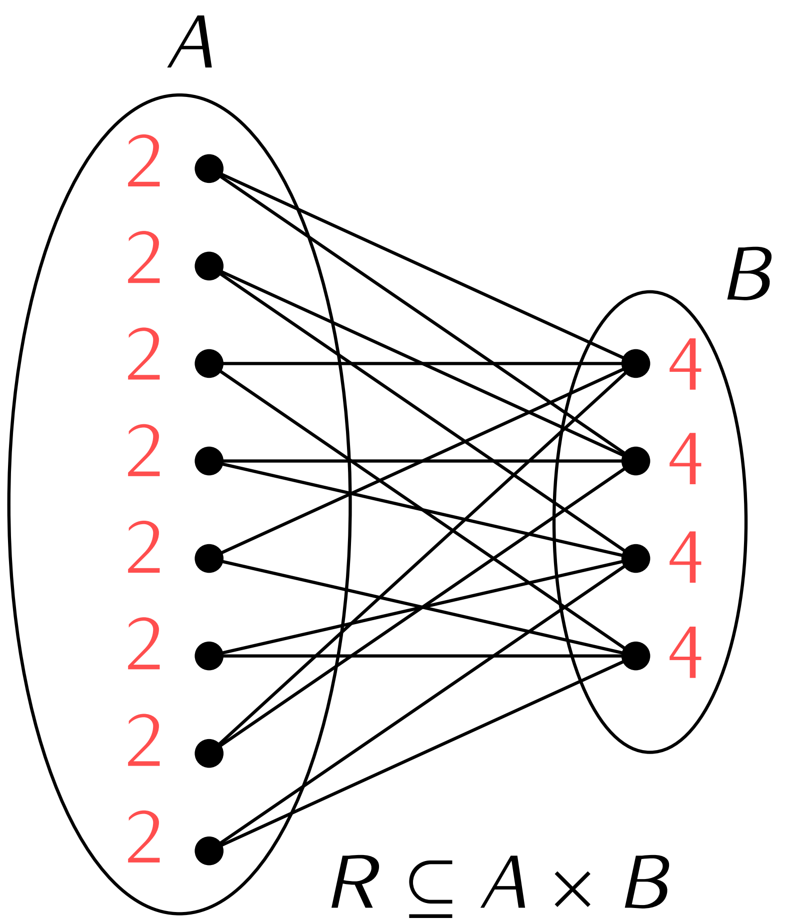
Definition. Let $R \subseteq A \times B$, $a \in A, b \in B$.

- $\deg(a) = |\{b \in B \mid (a, b) \in R\}|$
- $\deg(b) = |\{a \in A \mid (a, b) \in R\}|$

Theorem. $\sum_{a \in A} \deg(a) = |R| = \sum_{b \in B} \deg(b)$.

Proof. Theorem has a Σ $\rightsquigarrow$ partition R into subsets

- R_a: all edges "touching" a
- R_b: all edges "touching b



$\sum_{a \in A} \deg(a) = 16 = \sum_{b \in B} \deg(b)$

Idea:

- we know if $f : A \to B$ is bijective, then $|A| = |B|$
- what can we do with relations instead of functions?

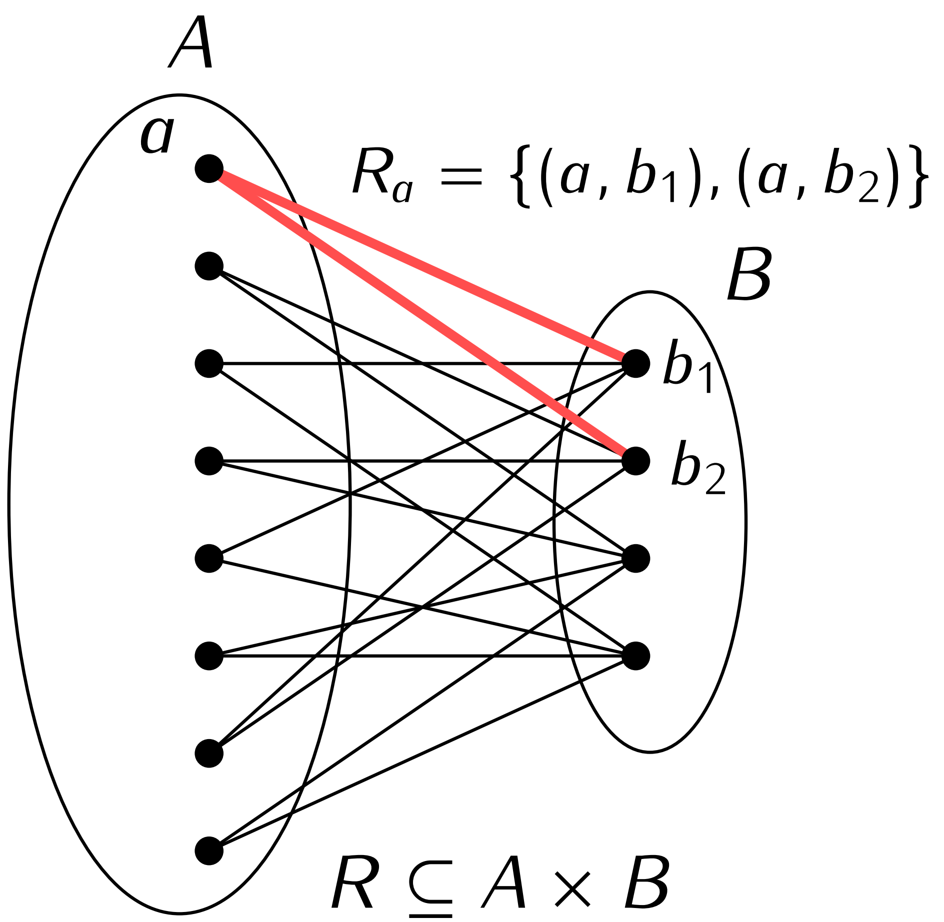
Definition. Let $R \subseteq A \times B$, $a \in A, b \in B$.

- $\deg(a) = |\{b \in B \mid (a, b) \in R\}|$
- $\deg(b) = |\{a \in A \mid (a, b) \in R\}|$

Theorem. $\sum_{a \in A} \deg(a) = |R| = \sum_{b \in B} \deg(b)$.

Proof. Theorem has a $\Sigma \rightsquigarrow$ partition R into subsets

- R_a: all edges "touching" a
- R_b: all edges "touching b



Idea:

- we know if $f: A \to B$ is bijective, then $|A| = |B|$
- what can we do with relations instead of functions?

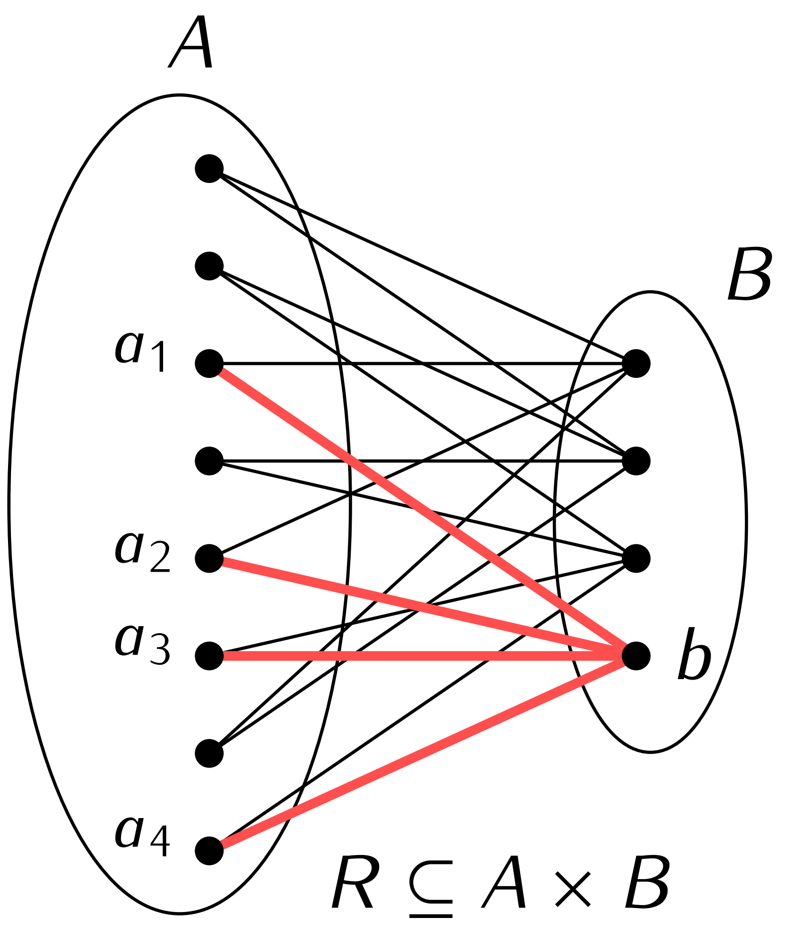
Definition. Let $R \subseteq A \times B$, $a \in A, b \in B$.

- $\deg(a) = |\{b \in B \mid (a, b) \in R\}|$
- $\deg(b) = |\{a \in A \mid (a, b) \in R\}|$

Theorem. $\sum_{a \in A} \deg(a) = |R| = \sum_{b \in B} \deg(b)$.

Proof. Theorem has a $\Sigma \rightsquigarrow$ partition R into subsets

- R_a: all edges "touching" a
- R_b: all edges "touching b



$R_b = \{(a_1, b), (a_2, b), (a_3, b), (a_4, b)\}$

Idea:

- we know if $f: A \to B$ is bijective, then $|A| = |B|$
- what can we do with relations instead of functions?

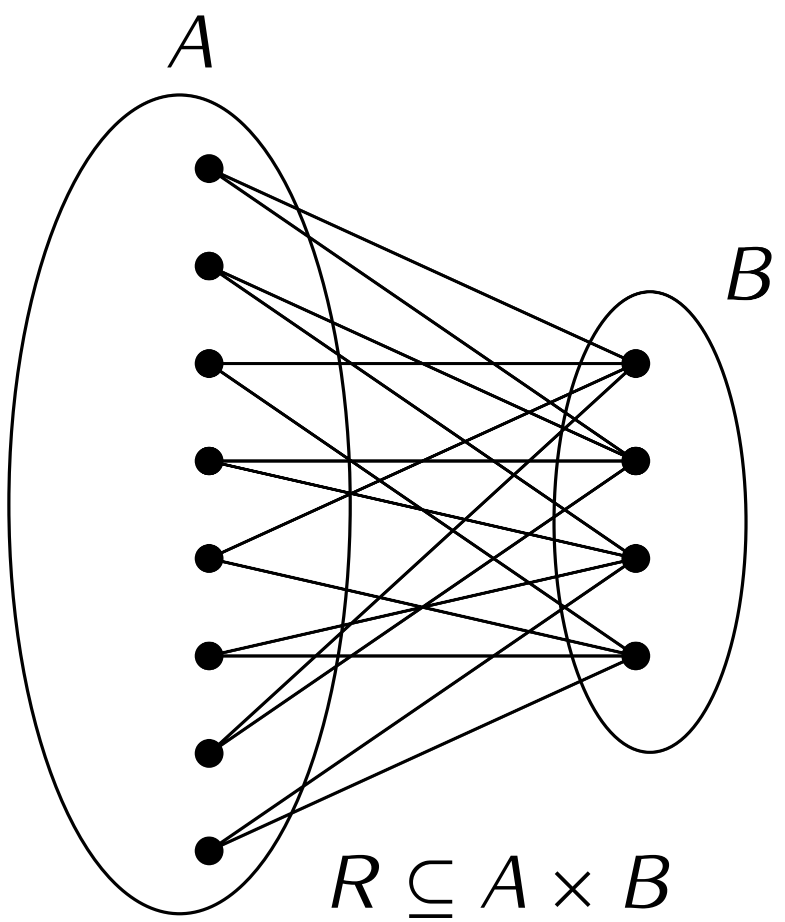
Definition. Let $R \subseteq A \times B$, $a \in A, b \in B$.

- $\deg(a) = |\{b \in B \mid (a, b) \in R\}|$
- $\deg(b) = |\{a \in A \mid (a, b) \in R\}|$

Theorem. $\sum_{a\in A} \deg(a) = |R| = \sum_{b\in B} \deg(b)$.

Proof. Theorem has a Σ $\rightsquigarrow$ partition R into subsets

- R_a: all edges "touching" a
- R_b: all edges "touching b
- Size of R_a? $\deg(a)$
- $R = \bigcup_{a\in A} R_a$
- $R_a \cap R_{a'} = \emptyset$ if $a \neq a'$
- By the union rule, $|R| = \sum_{a\in A} \deg(a)$. $\square$



When to use this?

If:

- The degrees are known
- $|A|$ is known

Then we can know $|B|$.

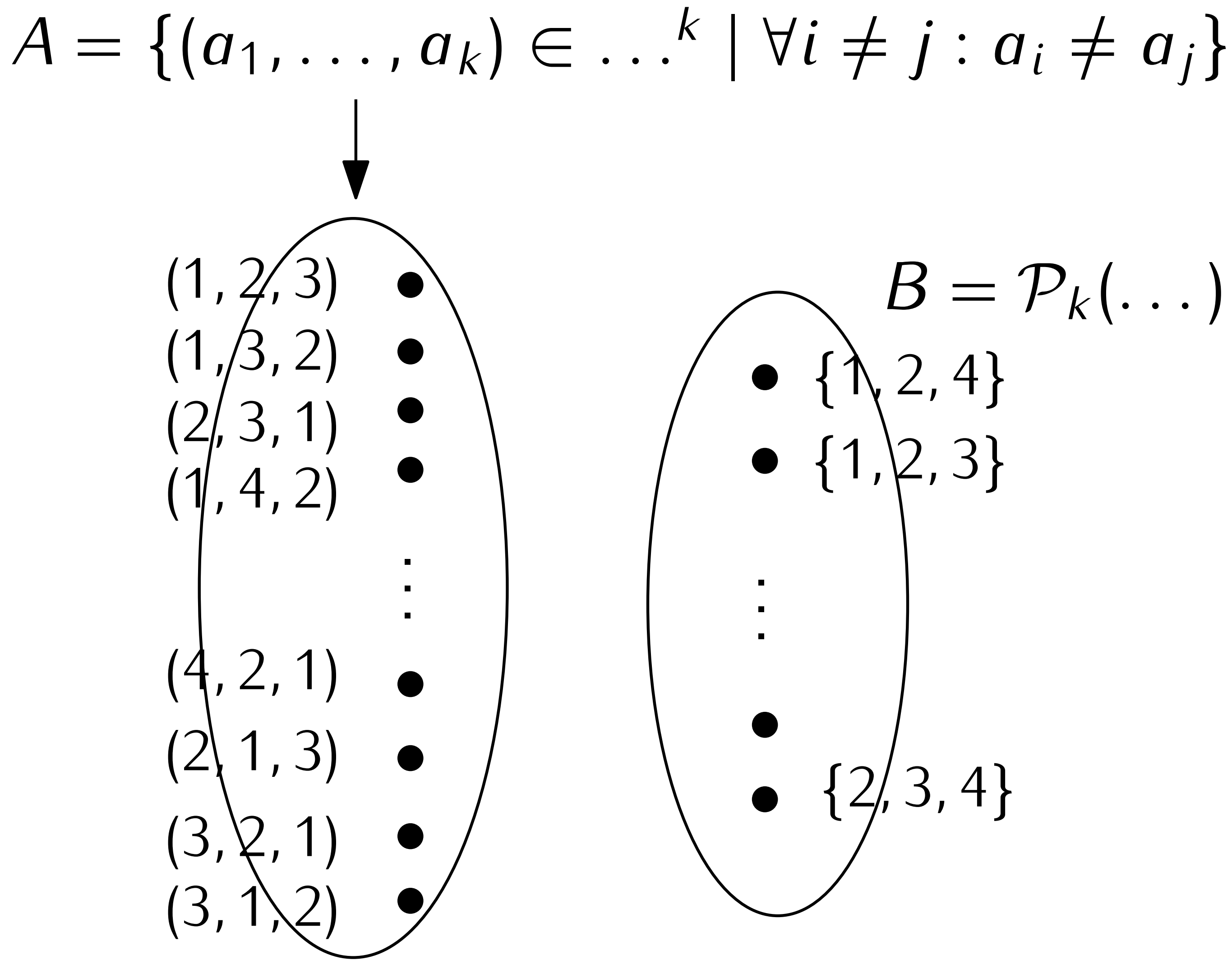
We have seen: $\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{k!(n-k)!}$

Proof using double counting:

- Want to know: $|\mathcal{P}_k(\{1, \dots, n\})|$
- Define $A = \{(a_1, \dots, a_k) \in \{1, \dots, n\}^k \mid \forall i \neq j : a_i \neq a_j\}$
- Define $R \subseteq A \times B$:
  $R = \{((a_1, \dots, a_k), T) \in A \times B \mid \{a_1, \dots, a_k\} = T\}$
- degree of elements of A?

What is $\deg(T)$ for every $T \in B$?

- 1
- $n!$
- $2k$
- $k!$



(For the example: $k = 3$)

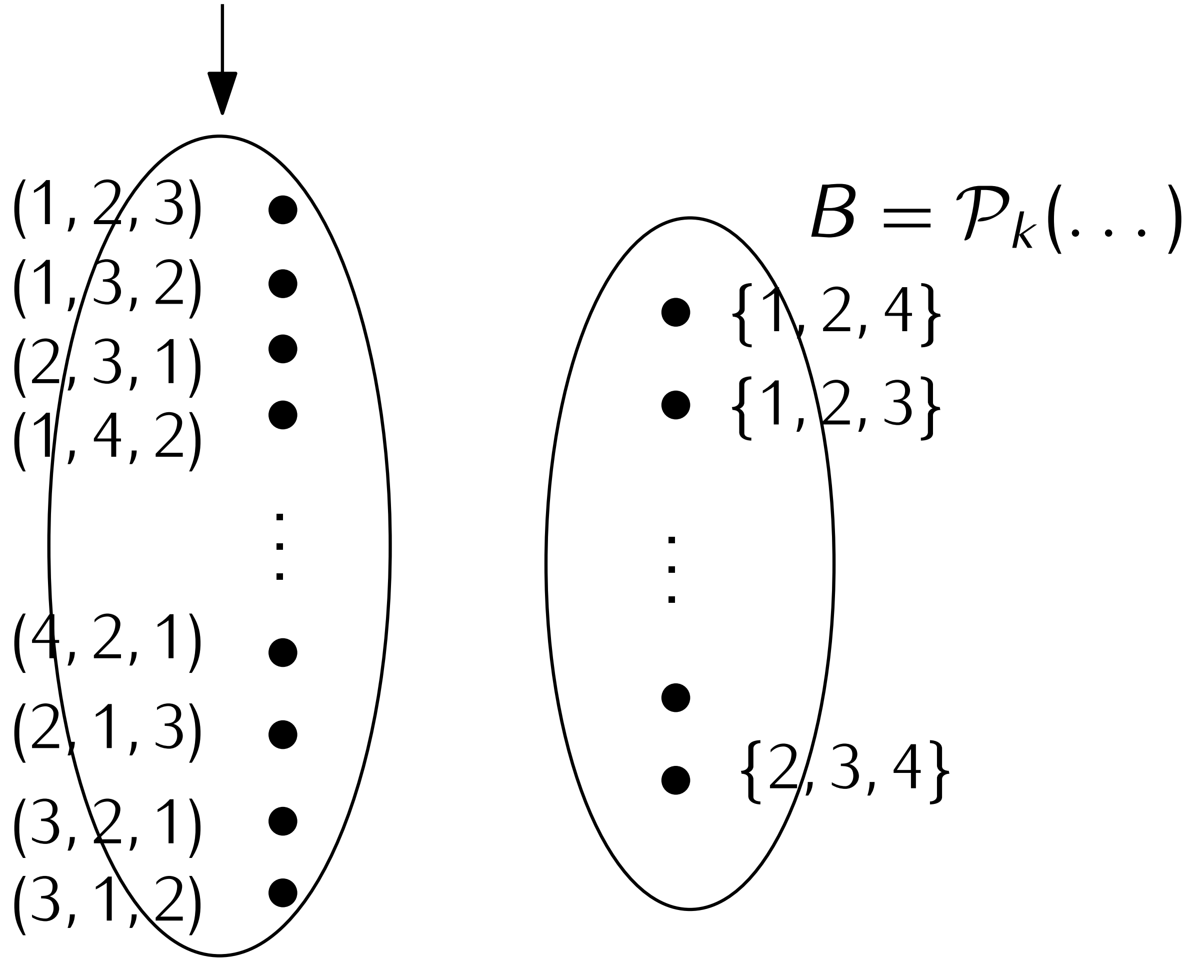
We have seen: $\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{k!(n-k)!}$

Proof using double counting:

- Want to know: $|\mathcal{P}_k(\{1,\ldots,n\})|$
- Define $A = \{(a_1,\ldots,a_k) \in \{1,\ldots,n\}^k \mid \forall i \neq j : a_i \neq a_j\}$
- Define $R \subseteq A \times B$:
  $R = \{((a_1,\ldots,a_k),T) \in A \times B \mid \{a_1,\ldots,a_k\} = T\}$
- degree of elements of A?
- degree of elements of B is $k!$

By double-counting:
$\sum_{a \in A} \deg(a) = \sum_{T \in B} \deg(T)$

$A = \{(a_1,\ldots,a_k) \in \ldots^k \mid \forall i \neq j : a_i \neq a_j\}$

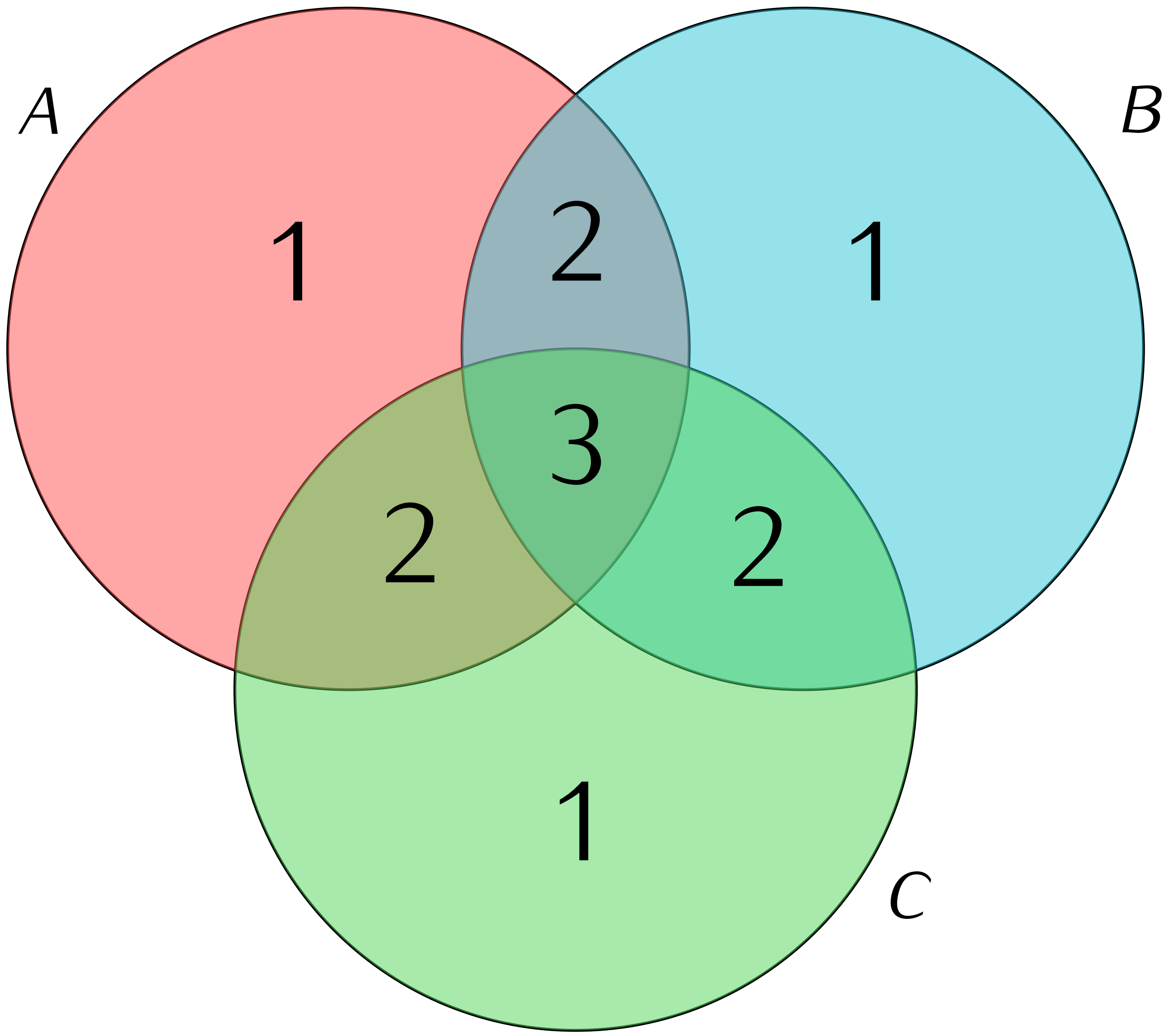


(For the example: $k = 3$)

Union rule: $|A \cup B| = |A| + |B| - |A \cap B|$

How to compute $|A \cup B \cup C|$?

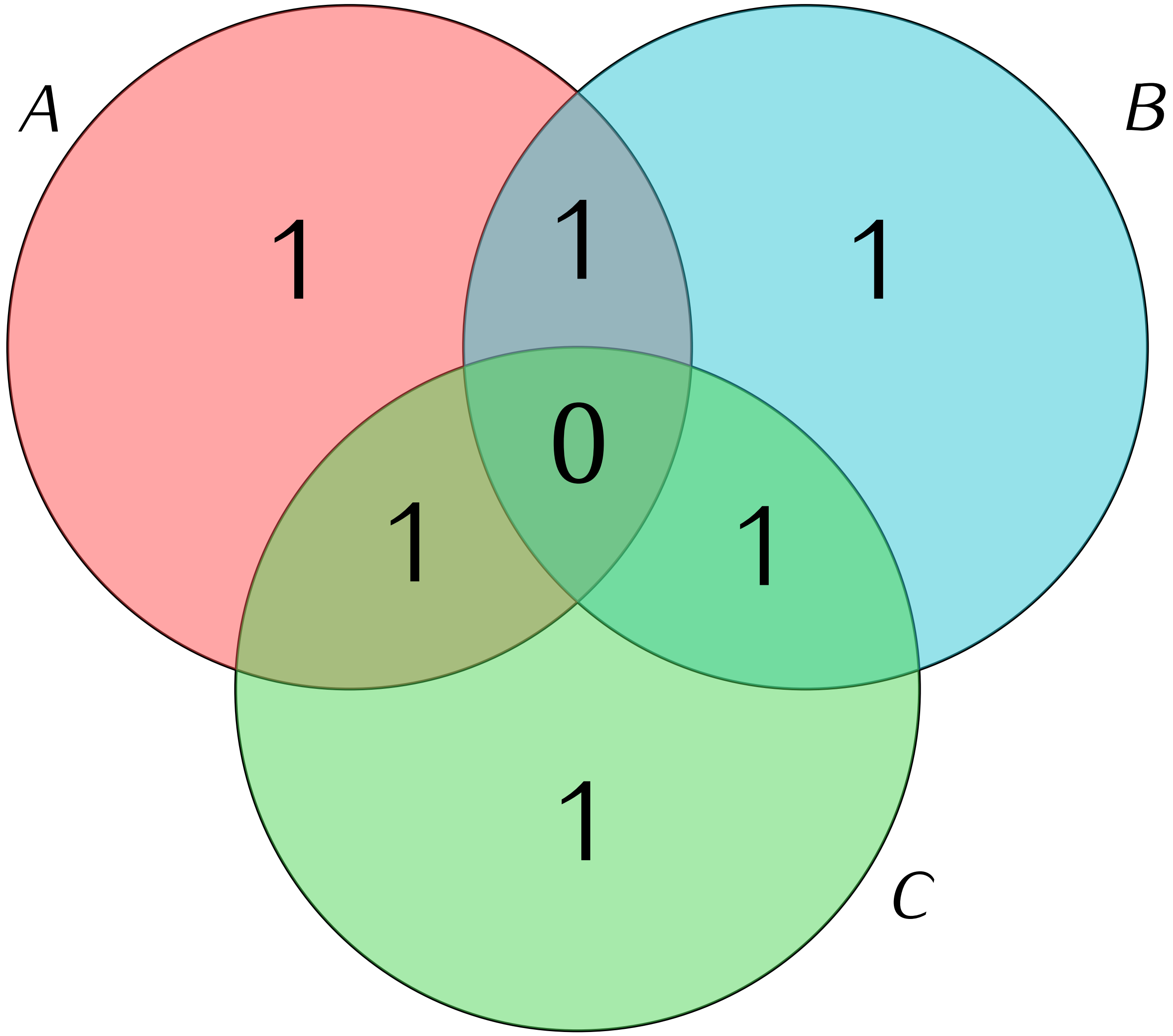
$|A| + |B| + |C|$



Union rule: $|A \cup B| = |A| + |B| - |A \cap B|$

How to compute $|A \cup B \cup C|$?

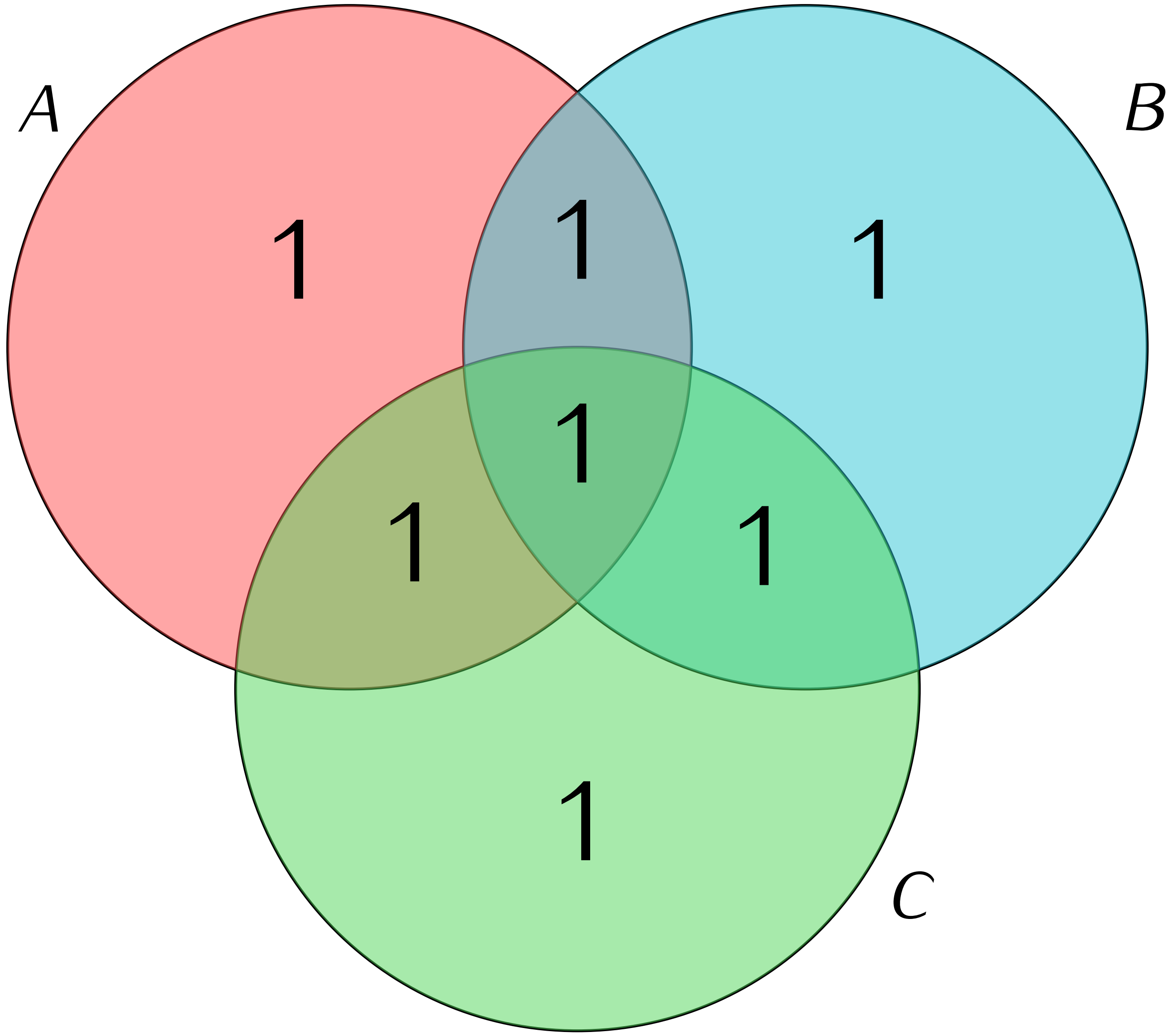
$|A| + |B| + |C|$ $-|A \cap B| - |A \cap C| - |B \cap C|$



Union rule: $|A \cup B| = |A| + |B| - |A \cap B|$

How to compute $|A \cup B \cup C|$?

$$|A| + |B| + |C| \quad -|A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| = |A \cup B \cup C|$$



This is called the **inclusion-exclusion principle**.

Ideally, one would like to be able to count more complicated expressions like $|A \cup B \cup C \cup D|$

sign alternates between $+$ and $-$

Theorem. If $A_1, \dots, A_n$ are finite sets, then

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r+1} \sum_{1 \le i_1 < i_2 < \cdots < i_r \le n} |A_{i_1} \cap \cdots \cap A_{i_r}|$$

Proof: by induction on $n \geq 2$, base case is the union rule

"Loop" over all subsets $\{i_1, \dots, i_r\}$ of $\{1, \dots, n\}$ with r elements

In some special cases, all the intersections $|A_{i_1} \cap \cdots \cap A_{i_r}|$ have the same size N_r, we then get:

Theorem. Let $A_1, \dots, A_n$ be finite sets and $N_1, \dots, N_n \in \mathbb{N}$ be such that for all $r \in \{1, \dots, n\}$ and all distinct $i_1, \dots, i_r \in \{1, \dots, n\}$, the intersection $A_{i_1} \cap \cdots \cap A_{i_r}$ has size N_r. Then

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r+1} \binom{n}{r} N_r$$

(From projecteuler.net)

At Least Four Distinct Prime Factors Less Than 100

Problem 268

It can be verified that there are 23 positive integers less than 1000 that are divisible by at least four distinct primes less than 100.

Find how many positive integers less than 10^{16} are divisible by at least four distinct primes less than 100.

Setup: $S = \{n \in \{1, \dots, 10^{16}\} \mid n \text{ is divisible by four distinct primes less than } 100\}$

$S = \bigcup_{p_1, p_2, p_3, p_4 \text{ distinct primes}} D_{p_1 p_2 p_3 p_4}$ where D_k = set of multiples of k smaller than 10^{16}

Naive attempt:

```
from itertools import combinations

smallPrimes = primes(100) # compute all primes up to 100
finalSet = set()
for (p1,p2,p3,p4) in                              :




print(len(finalSet))
```

(From projecteuler.net)

At Least Four Distinct Prime Factors Less Than 100

Problem 268

It can be verified that there are 23 positive integers less than 1000 that are divisible by at least four distinct primes less than 100.

Find how many positive integers less than 10^{16} are divisible by at least four distinct primes less than 100.

Setup: $S = \{n \in \{1, \dots, 10^{16}\} \mid n \text{ is divisible by four distinct primes less than } 100\}$

$S = \bigcup_{p_1,p_2,p_3,p_4 \text{ distinct primes}} D_{p_1p_2p_3p_4}$ where D_k = set of multiples of k smaller than 10^{16}

Naive attempt:

```
from itertools import combinations

smallPrimes = primes(100) # compute all primes up to 100
finalSet = set()
for (p1,p2,p3,p4) in combinations(smallPrimes,4):




print(len(finalSet))
```

(From projecteuler.net)

At Least Four Distinct Prime Factors Less Than 100

Problem 268

It can be verified that there are 23 positive integers less than 1000 that are divisible by at least four distinct primes less than 100.

Find how many positive integers less than 10^{16} are divisible by at least four distinct primes less than 100.

Setup: $S = \{n \in \{1, \dots, 10^{16}\} \mid n \text{ is divisible by four distinct primes less than } 100\}$
$S = \bigcup_{p_1, p_2, p_3, p_4 \text{ distinct primes}} D_{p_1 p_2 p_3 p_4}$ where D_k = set of multiples of k smaller than 10^{16}

Naive attempt:

```
from itertools import combinations

smallPrimes = primes(100) # compute all primes up to 100
finalSet = set()
for (p1,p2,p3,p4) in combinations(smallPrimes,4):
  # take all multiples of p1*p2*p3*p4 that are smaller than 10^16
  for k in range(10**16 / (p1*p2*p3*p4)):
    finalSet = finalSet | {p1*p2*p3*p4 * k}
print(len(finalSet)) # outputs the correct number
```

(From projecteuler.net)

At Least Four Distinct Prime Factors Less Than 100

Problem 268

It can be verified that there are 23 positive integers less than 1000 that are divisible by at least four distinct primes less than 100.

Find how many positive integers less than 10^{16} are divisible by at least four distinct primes less than 100.

Setup: $S = \{n \in \{1, \dots, 10^{16}\} \mid n \text{ is divisible by four distinct primes less than } 100\}$

$S = \bigcup_{p_1, p_2, p_3, p_4 \text{ distinct primes}} D_{p_1 p_2 p_3 p_4}$ where D_k = set of multiples of k smaller than 10^{16}

$|D_k| = 10^{16}/k$

$$|S| \stackrel{?}{=} \sum_{p_1, p_2, p_3, p_4 \text{distinct}} |D_{p_1 p_2 p_3 p_4}| -4 \sum_{p_1, p_2, p_3, p_4, p_5 \text{ distinct}} |D_{p_1 p_2 p_3 p_4 p_5}|$$

How many times did we count $2 \times 3 \times 5 \times 7 \times 11$? $\binom{5}{4} = 5$ times

How many times did we count $2 \times 3 \times 5 \times 7 \times 11 \times 13$? $\binom{6}{4} - 4\binom{6}{5} = -9$ times

(From projecteuler.net)

At Least Four Distinct Prime Factors Less Than 100

Problem 268

It can be verified that there are 23 positive integers less than 1000 that are divisible by at least four distinct primes less than 100.

Find how many positive integers less than 10^{16} are divisible by at least four distinct primes less than 100.

Setup: $S = \{n \in \{1, \dots, 10^{16}\} \mid n \text{ is divisible by four distinct primes less than } 100\}$

$S = \bigcup_{p_1,p_2,p_3,p_4 \text{ distinct primes}} D_{p_1p_2p_3p_4}$ where D_k = set of multiples of k smaller than 10^{16}

$|D_k| = 10^{16}/k$

$$|S| = \sum_{p_1,p_2,p_3,p_4 \text{distinct}} |D_{p_1p_2p_3p_4}| - 4 \sum_{p_1,p_2,p_3,p_4,p_5 \text{ distinct}} |D_{p_1p_2p_3p_4p_5}| + 10 \sum_{p_1,\dots,p_6 \text{ distinct}} |D_{p_1\cdots p_6}| - \dots$$

How many times did we count $2 \times 3 \times 5 \times 7 \times 11$? $\binom{5}{4} = 5$ times

How many times did we count $2 \times 3 \times 5 \times 7 \times 11 \times 13$? $\binom{6}{4} - 4\binom{6}{5} = -9$ times

How many times did we count $p_1 \times p_2 \times \cdots \times p_r$? $\boxed{1 - (-1)^r \binom{r-1}{3}}$ times

$$|S| = \sum_{p_1,p_2,p_3,p_4 \text{distinct}} |D_{p_1p_2p_3p_4}| - 4 \sum_{p_1,\dots,p_5 \text{ distinct}} |D_{p_1p_2p_3p_4p_5}| + \cdots + \boxed{(-1)^r \binom{r-1}{3}} \sum_{p_1,\dots,p_r \text{ distinct}} |D_{p_1\cdots p_r}|$$

```
from itertools import combinations # iterator on subsets
from math import comb # gives the binomial coefficients

smallPrimes = primes(100)
result = 0
N = 10**16
for r in range(4,len(smallPrimes)+1):
  sum_for_fixed_r = 0
  for combination_of_primes in combinations(smallPrimes,r):
    product = 1
    for p in combination_of_primes:
      product *= p
    sum_for_fixed_r += N//product
  result += (-1)**r * comb(r-1,3) * sum_for_fixed_r
print(result)
```

What we have seen so far: if A, B are finite, then there are:

- $|B|^{|A|}$ functions $f\colon A \to B$
- $|B|^{\underline{|A|}}$ injective functions $f\colon A \to B$

Ideas:

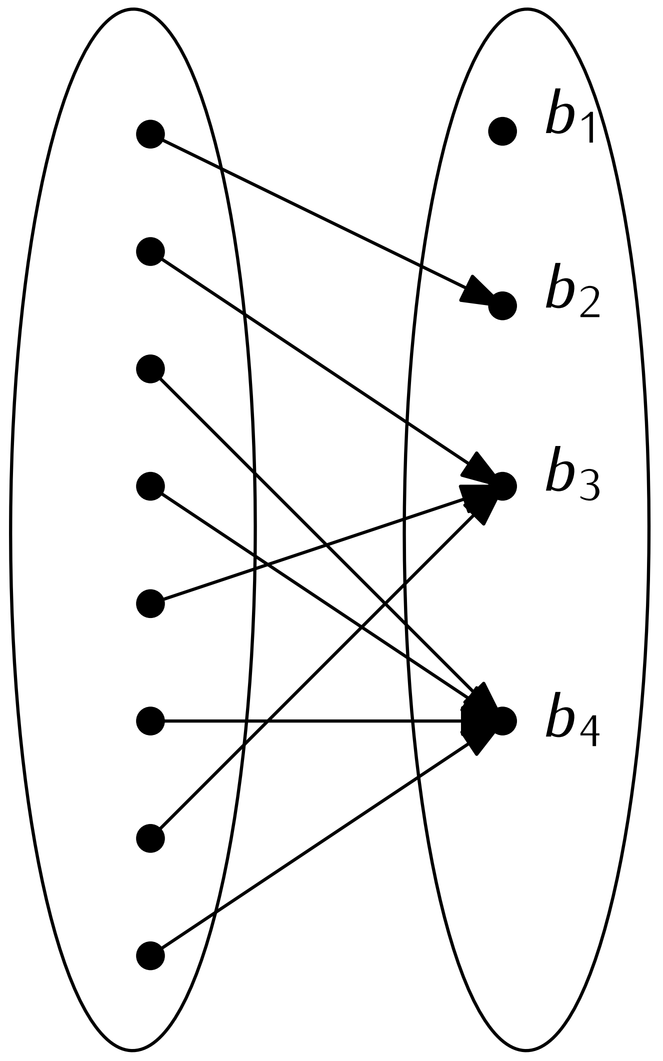
(1) If we know the number of functions that are not surjective, we know the number of surjective functions

(2) The set of not surjective functions is the union of simple sets

$$\text{Let } F_i = \{f\colon A \to B \mid b_i \notin f[A]\}$$

Suppose $|A| = 8$ and $|B| = 4$.
What is $|F_i|$?

- 4
- 4^7
- 3^8
- 3^7



A function in F_1

Application: counting surjective functions

What we have seen so far: if A, B are finite, then there are:

- $|B|^{|A|}$ functions $f\colon A \to B$
- $|B|^{\underline{|A|}}$ injective functions $f\colon A \to B$

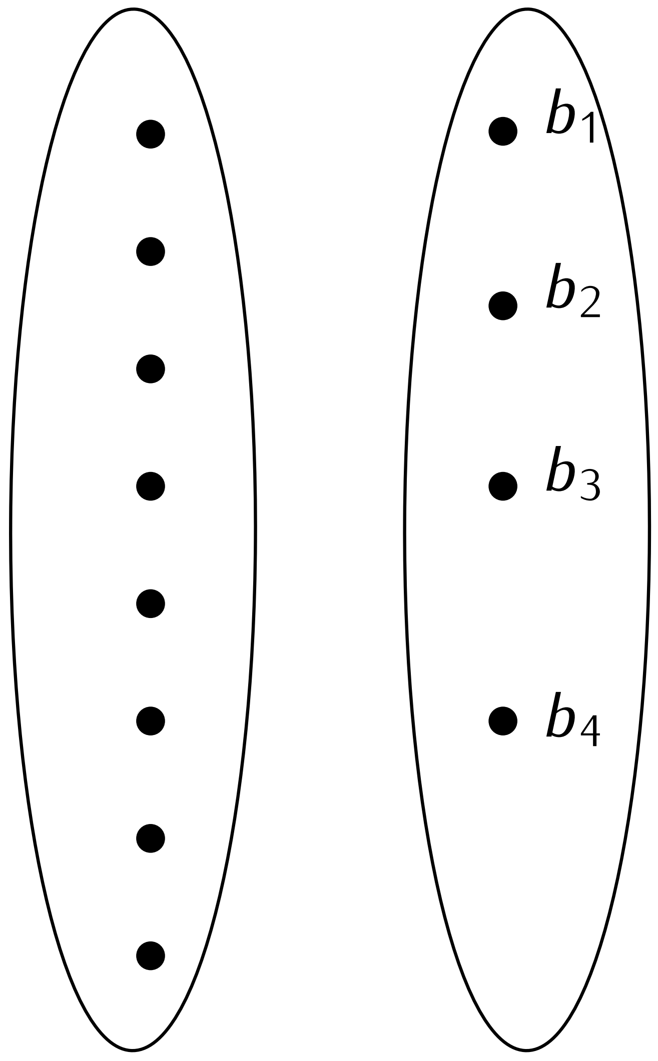
Ideas:

(1) If we know the number of functions that are not surjective, we know the number of surjective functions

(2) The set of not surjective functions is the union of simple sets

$$\text{Let } F_i = \{f\colon A \to B \mid b_i \notin f[A]\}$$

$$|F_i \cap F_j| = \qquad\qquad \text{if } i < j$$



A function in $F_1 \cap F_2$?

What we have seen so far: if A, B are finite, then there are:

- $|B|^{|A|}$ functions $f\colon A \to B$
- $|B|^{\underline{|A|}}$ injective functions $f\colon A \to B$

Ideas:

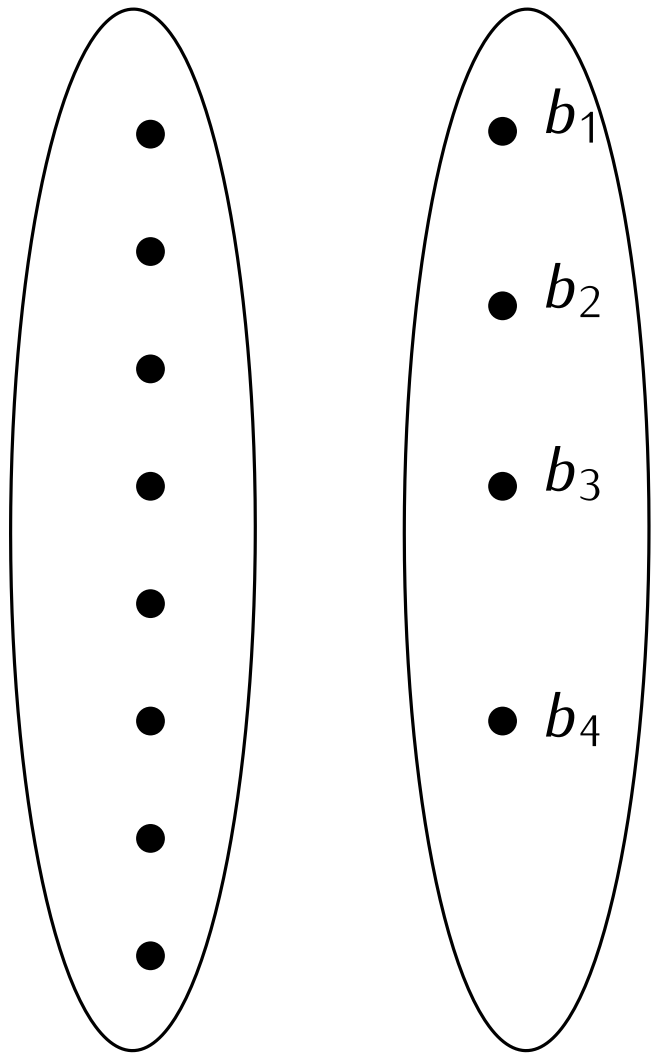
(1) If we know the number of functions that are not surjective, we know the number of surjective functions

(2) The set of not surjective functions is the union of simple sets

$$\text{Let } F_i = \{f\colon A \to B \mid b_i \notin f[A]\}$$

$$|F_i \cap F_j| = (|B|-2)^{|A|} \text{ if } i < j$$

$$|F_i \cap F_j \cap F_k| = \qquad\qquad \text{if } i < j < k$$



A function in $F_1 \cap F_2 \cap F_3$?

What we have seen so far: if A, B are finite, then there are:

- $|B|^{|A|}$ functions $f\colon A \to B$
- $|B|^{\underline{|A|}}$ injective functions $f\colon A \to B$

Ideas:

(1) If we know the number of functions that are not surjective, we know the number of surjective functions

(2) The set of not surjective functions is the union of simple sets

$$\text{Let } F_i = \{f\colon A \to B \mid b_i \notin f[A]\}$$

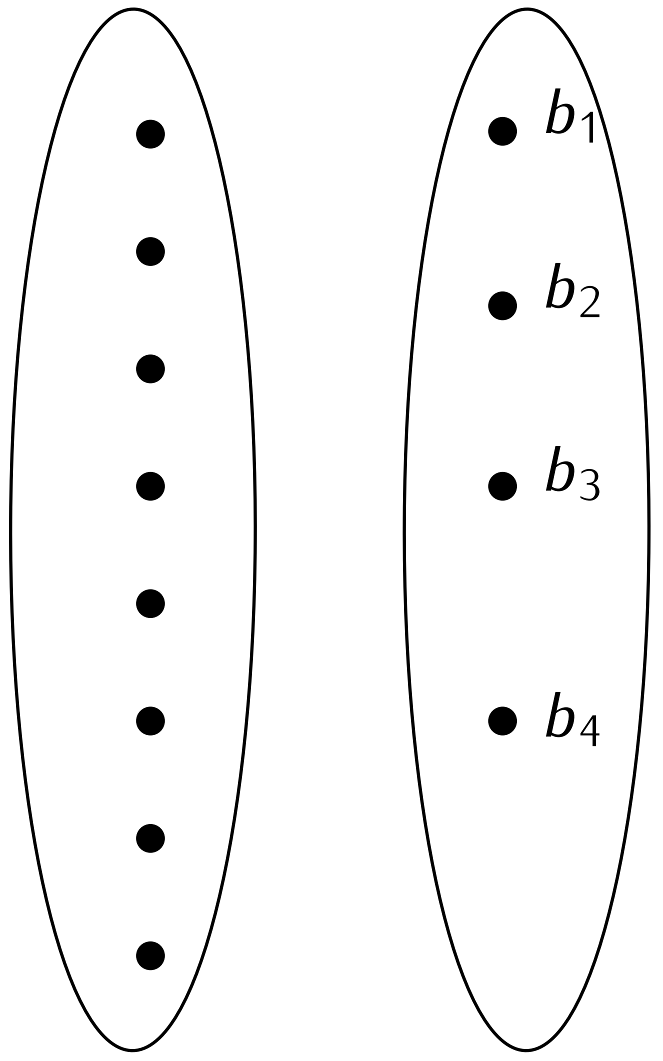
$$|F_i \cap F_j| = (|B| - 2)^{|A|} \text{ if } i < j$$

$$|F_i \cap F_j \cap F_k| = (|B| - 3)^{|A|} \text{ if } i < j < k$$

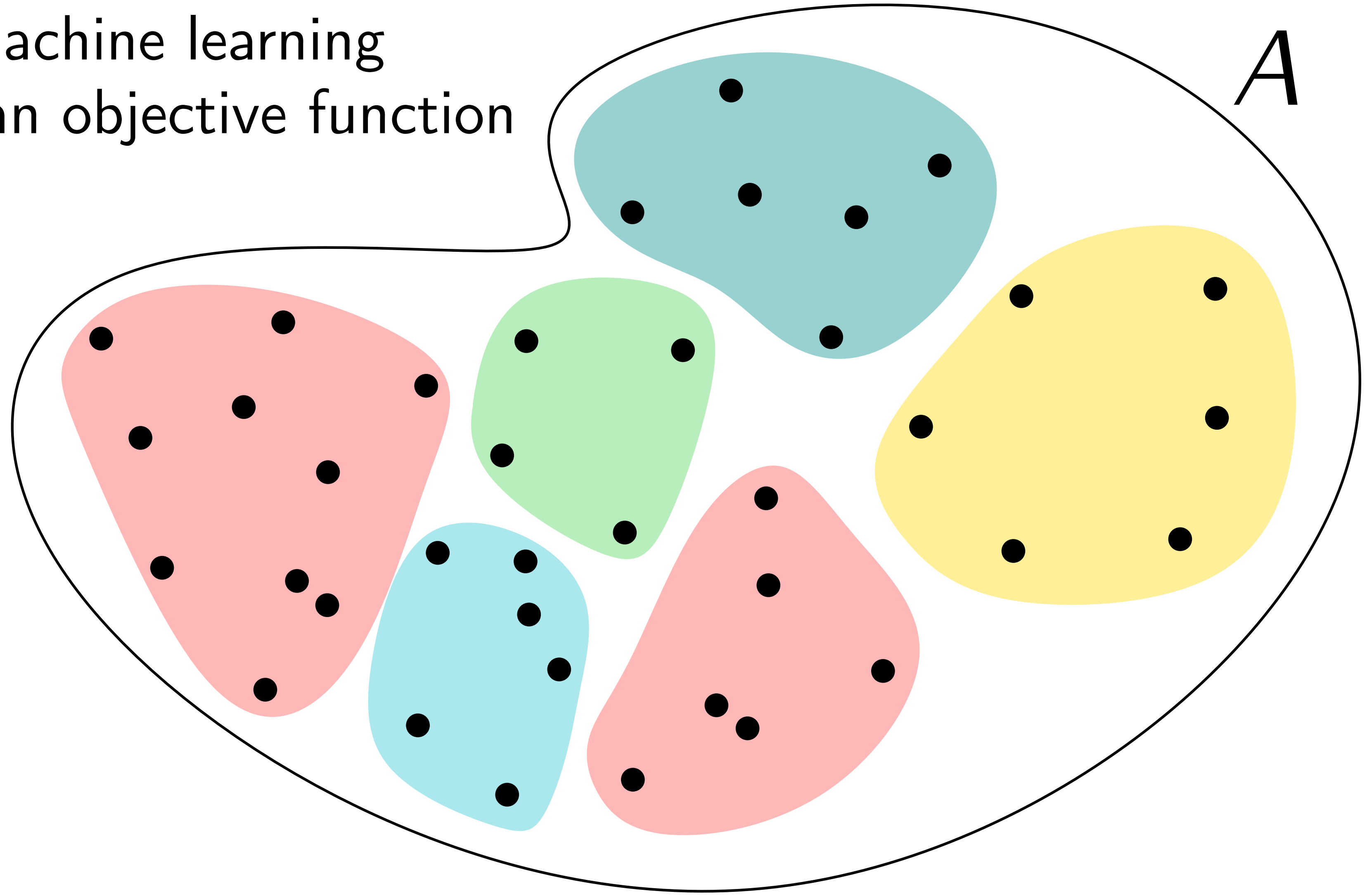
$$|F_{i_1} \cap \cdots \cap F_{i_r}| = (|B| - r)^{|A|} \text{ if } i_1 < \cdots < i_r$$

Theorem. The number of surjective functions $A \to B$ is given by

$$\sum_{r=0}^{|B|} (-1)^r \binom{|B|}{r} (|B| - r)^{|A|}$$

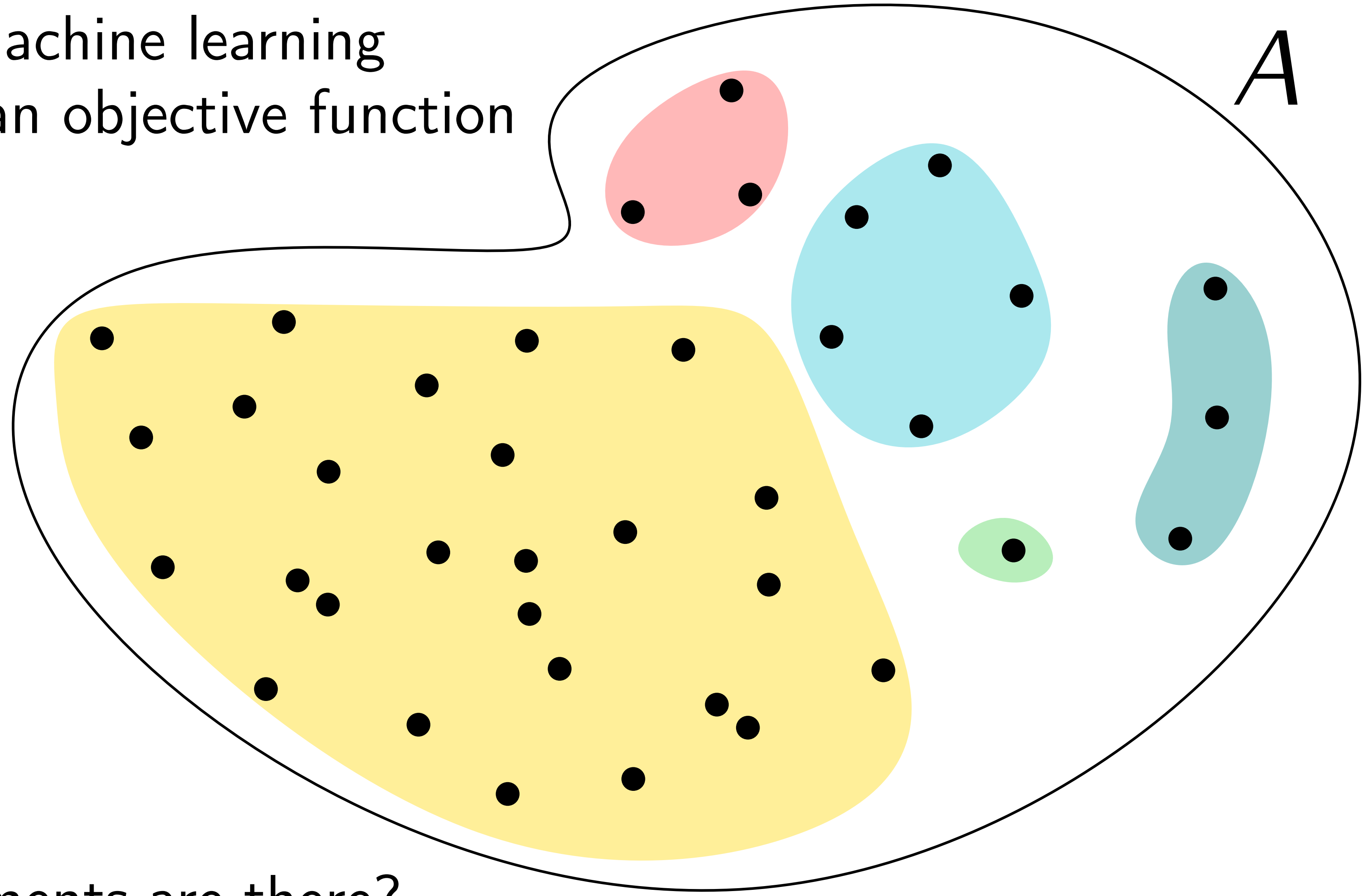


Clustering is an important problem in data science/machine learning
Goal: find a clustering of the points that minimizes an objective function



Clustering is an important problem in data science/machine learning

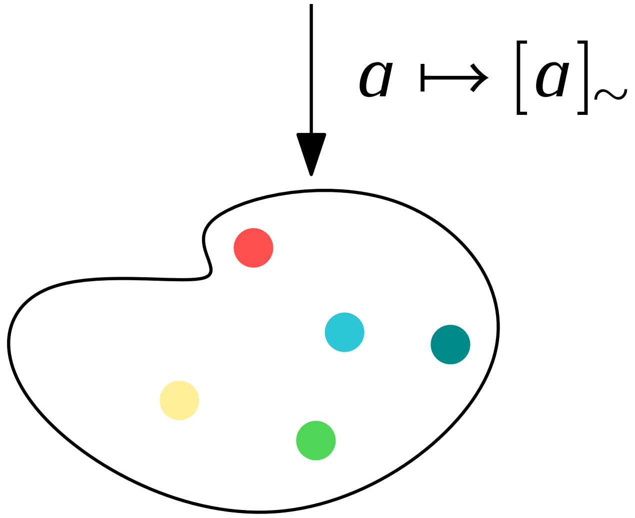
Goal: find a clustering of the points that minimizes an objective function




```
S = set_of_clusterings(nb_clusters=5)
for clustering in S:
  # check if this clustering
  # is good enough
```

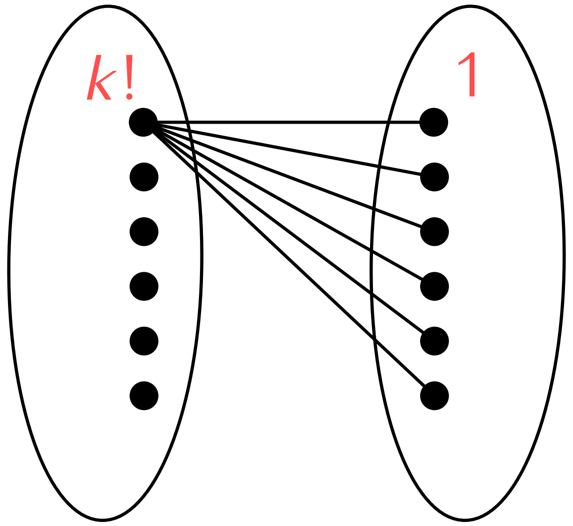
Clustering $\leftrightarrow$ partition of the set $\leftrightarrow$ eq. relation

cluster $\leftrightarrow$ part $\leftrightarrow$ eq. class



How many partitions with k parts of a set with n elements are there?

partitions of $\{1, \ldots, n\}$ in k parts

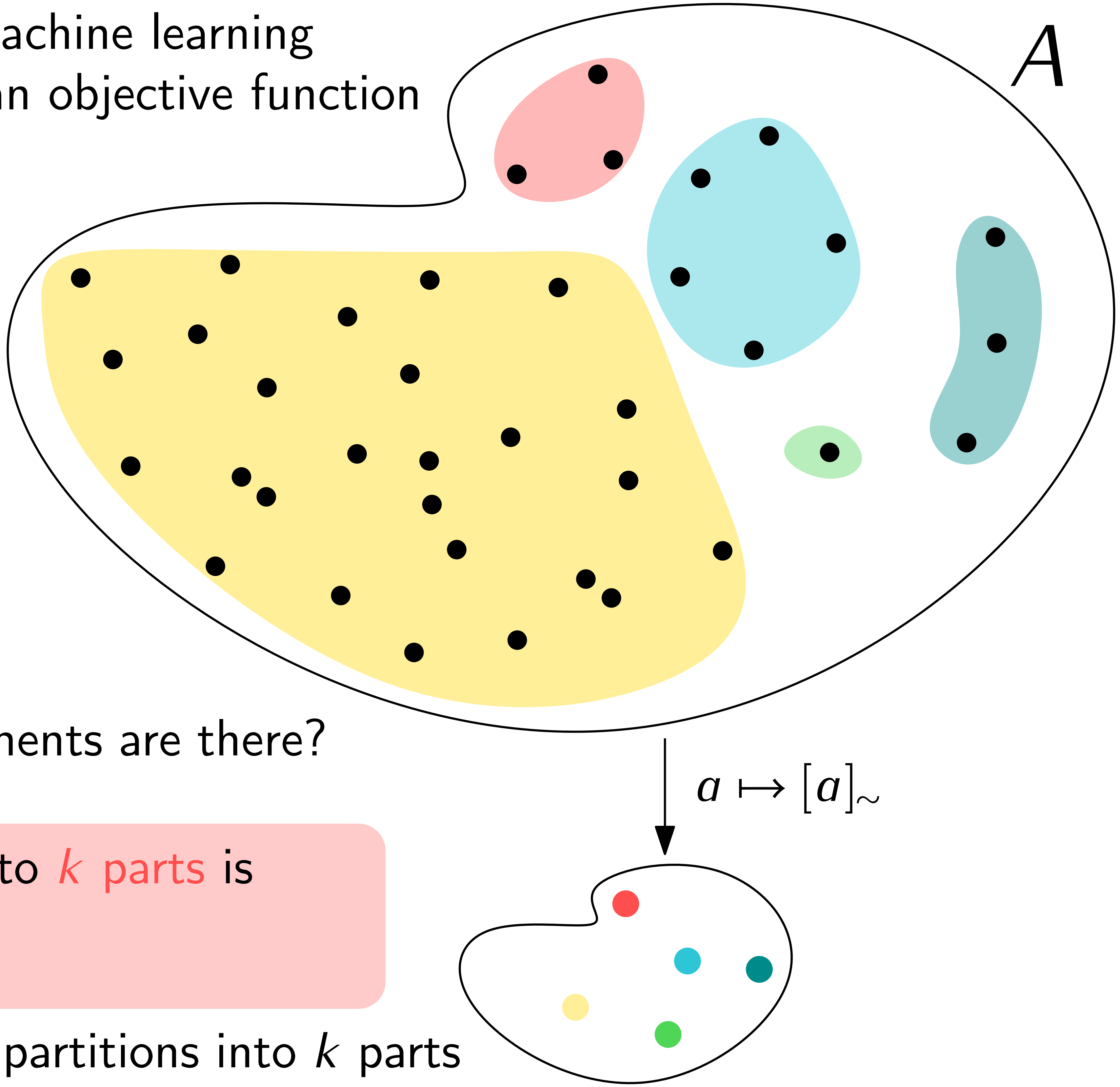


surjective functions

Clustering is an important problem in data science/machine learning
Goal: find a clustering of the points that minimizes an objective function

```
S = set_of_clusterings(nb_clusters=5)
for clustering in S:
  # check if this clustering
  # is good enough
```

Clustering $\leftrightarrow$ partition of the set $\leftrightarrow$ eq. relation
cluster $\leftrightarrow$ part $\leftrightarrow$ eq. class



How many partitions with k parts of a set with n elements are there?

Theorem. The number of partitions of $\{1, \ldots, n\}$ into k parts is

$$\frac{1}{k!}\sum_{r=0}^{k}(-1)^r\binom{k}{r}(k-r)^n$$

$n = 39, k = 5 \rightsquigarrow 18174782867968842219933192\,00$ partitions into k parts

Usually, to prove $\exists x\, \varphi$ one must give a concrete x that works
Sometimes, counting is enough:

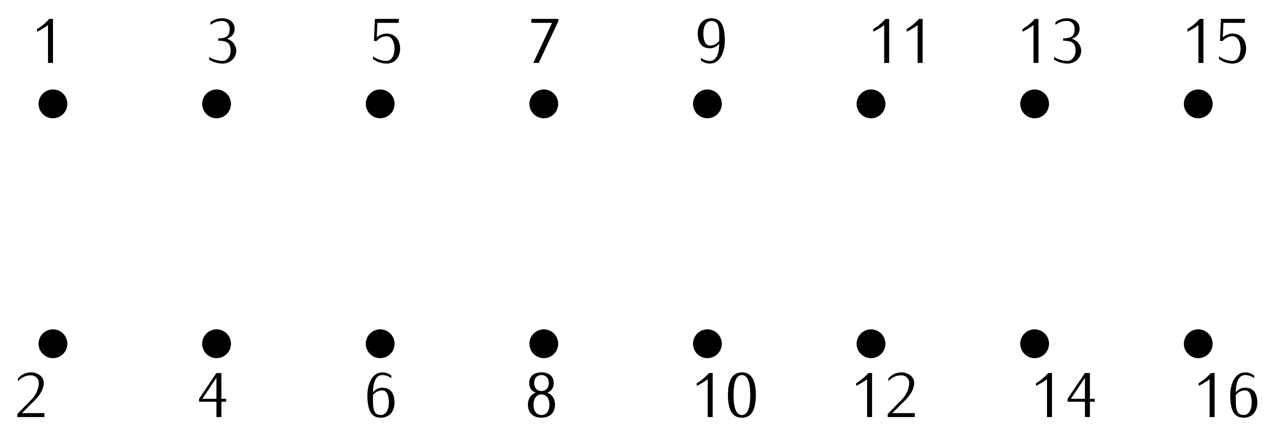
- Pigeonhole principle
- Ramsey theory
- Probabilistic method

Theorem. Suppose $f\colon A \to B$ is a function and $|A| > |B|$. Then there exist distinct $x, y \in A$ such that $f(x) = f(y)$.

In fact if A is much bigger than B, one can obtain more elements like this:

Theorem (Pigeonhole principle)**.** Suppose $f\colon A \to B$ is a function and $|A| > k|B|$ for some $k \in \mathbb{N}$. Then there exists distinct $x_1, \ldots, x_{k+1} \in A$ such that $f(x_i) = f(x_j)$ for all $i, j \in \{1, \ldots, k+1\}$.

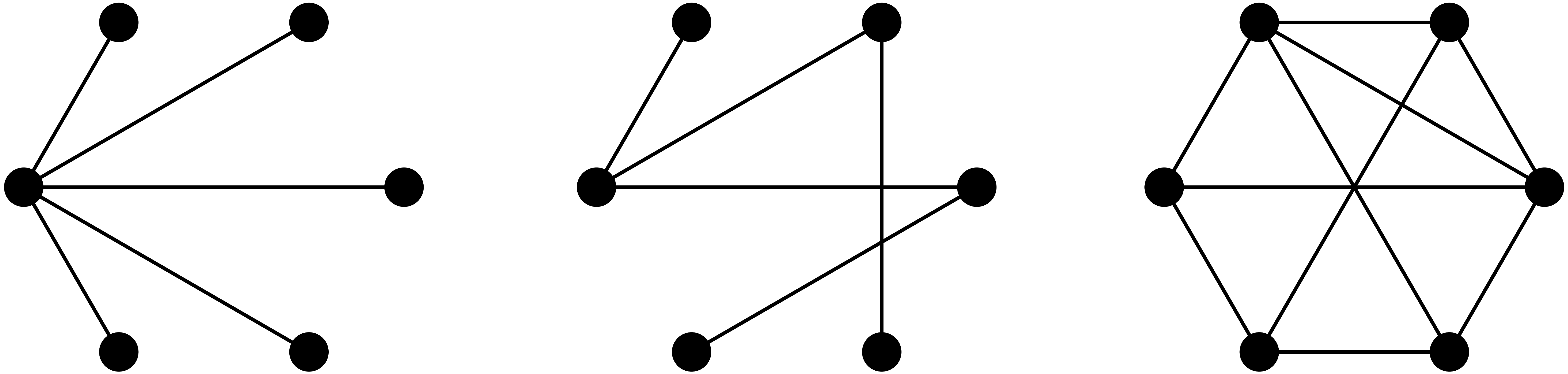
Example. For any 9 numbers $a_1, \ldots, a_9$ from $\{1, \ldots, 16\}$, two numbers are at distance exactly 2.



Theorem. Let $r \in \mathbb{N}$. There exists $n \in \mathbb{N}$ such that for every symmetric relation $R \subseteq A^2$, if $|A| \geq n$, there exist $a_1, \ldots, a_r \in A$ distinct such that either:

- $(a_i, a_j) \in R$ for all $i \neq j$.
- or $(a_i, a_j) \notin R$ for all $i \neq j$.

Example. We choose $r = 3$. Ramsey's Theorem gives us $n = 6$



For $r = 4$, $n = 18$ is enough
For $r = 5$, nobody knows what n is!