Discrete Mathematics (80181)

Dr. Noa Nitzan

Moshe Krumbein

Fall 2021

Compiled: 2023-03-17 12:46:25

https://github.com/outofink/notes

CONTENTS

DISCRETE MATHEMATICS

1

INTRODUCTION TO SET THEORY AND LOGIC

Moshe Krumbein - Fall 2021

1.1 Sets

Definition (Discrete Sets)**.** A *discrete set* is a set that has a distinct, individualized parts.

Discrete sets may be finite or infinite (but countable).

Definition (Sets)**.** A *set* is a collection of objects.

A set of objects of does not have to contain objects of only one type.

A property of sets is that a set A has a *binary relation* between itself and an object o. Either A contains or does not contain o.

Example 1.1.1.

$$A = \{1, 4, 7, 8\}$$
$$B = \{a, b, c, d\}$$
$$C = \{x, y, z\}$$

$$1 \in A$$
$$2 \notin A$$

Additionally, a set that has multiple members of the same element is equivalent to a set that has one one of the element, due to the property of *binary relation*.

$$A = \{1, 4, 7, 8\} = \{1, 1, 4, 4, 4, 7, 8\}$$

Definition (Size of a Sets)**.** Number of (by definition, distinct) elements in a set.

$$|A| = 4$$

Definition (Conditional Set)**.**

$$\{x \mid \text{such that } x\}$$
$$B = \{a \in A \mid a < 5\}$$

Example 1.1.2. All of the whole numbers from 1 to 1000.

$$\{x \mid 1 < x < 1000, \text{ such that } x \text{ is whole } \}$$

Although the following set is small in size, it is easier to express it in the following fashion instead of explicitly:

$$\{x \mid x^5 - 4x^3 + 7x^2 - 11x + \sqrt{2} = 0\}$$

Symbol (Quantifiers).

$$\forall = \text{for all}$$
$$\exists = \text{exists}$$

1.1.1 Containment (Subset)

Definition (Containment)**.** B contains A when all elements in B are also in A.

$$B \subseteq A$$

Specifically if A and B are distinct:

$$B \subsetneq A$$

If two sets are *equivalent*: ($A \subseteq B, B \subseteq A$)

$$A = B$$

Example 1.1.3.

$$A = \{1, 3, 4, \{1\}, \{1, 2\}\}$$
$$|A| = 5$$
$$1 \in A$$
$$\{1\} \in A$$
$$\{1\} \subseteq A$$
(because of the first element)
$$\{\{1\}\} \subseteq A$$
(because of the forth element)
$$\{1, 2\} \in A$$
$$\{1, 2\} \nsubseteq A$$
$$\{1\} \subseteq A$$
$$\{1\} \subsetneq A$$

Note. $A \in B$: the *element* A is in *set* B. $A \subseteq B$: the contents of *set* A are all in *set* B.

1.1.2 Special Sets

$$\begin{aligned}
\emptyset =& \{\} && \text{(empty set)}\\
\mathbb{N} =& \{1, 2, 3, \ldots\} && \text{(natural numbers)}\\
\mathbb{Z} =& \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\} && \text{(whole numbers)}\\
\mathbb{Q} =& \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\} && \text{(rational numbers)}\\
\mathbb{R} & && \text{(real numbers)}
\end{aligned}$$

$$\emptyset \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

1.1.3 Binary operations on sets

$$\begin{aligned}
A \cup B =& \{a \mid a \in B \text{ or } a \in A\} && \text{(Union)}\\
A \cap B =& \{a \mid a \in B \text{ and } a \in A\} && \text{(Intersection)}\\
A \setminus B =& \{a \mid a \notin B \text{ and } a \in A\} && \text{(Difference)}\\
A \triangle B =& (A \cup B) \setminus (A \cap B) && \text{(Symmetrical Difference)}
\end{aligned}$$

1.1.4 Size of union of sets

$$|A \cup B| \stackrel{?}{=} |A| + |B|$$

Definition (Disjoint Sets)**.** A and B are *disjoint sets* if $A \cap B = \emptyset$.

If A and B are disjoint sets, then:

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

In general:

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

When A, B, C are *pairwise disjointed*:

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

1.1.5 Algebraic Properties

Commutative property:

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

Associative property:

$$(A \cup B) \cup C = A \cup (B \cup C)$$
$$(A \cap B) \cap C = A \cap (B \cap C)$$

Distributive property:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Given the sets $A_1, A_2 \ldots, A_n$:

$$[n] = \{1, 2, 3, \ldots, n\}, n \in \mathbb{N}, \quad |[n]| = n$$
$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n = \{x \mid \exists\, i \in [n] : x \in A_i\}$$
$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n = \{x \mid \forall\, i \in [n] : x \in A_i\}$$

Definition (Compliment)**.** For set U where $A \subseteq U$:

$$A^c = U \setminus A$$

Definition (De Morgan's Laws)**.** Given sets A, B:

$$(A \cup B)^c = A^c \cap B^c$$
$$(A \cap B)^c = A^c \cup B^c$$

1.2 Logic and Logical Relations

Axiom. Every claim is either *true* and *false*: $\{T, F\}$

$$1+1=2 \to T$$
$$1+1=0 \to F$$

1.2.1 Unary Operations - Negation

P	$\neg P$
T	F
F	T

Table 1.1: Negation

1.2.2 Binary Operations

P	Q	$P \vee Q$	$P \wedge Q$	$P \to Q$	$P \leftrightarrow Q$
T	T	T	T	T	T
T	F	T	F	F	F
F	T	T	F	T	F
F	F	F	F	T	T

Table 1.2: Binary Operations

Definition (Complex Statements)**.** Combination of logical relations in one statement.

Example 1.2.1.

$$\neg P \to Q$$

Relation between $\cup, \cap$ and $\vee, \wedge$

$$P : x \in A \quad Q : x \in B$$
$$P \vee Q : x \in A \cup B$$
$$P \wedge Q : x \in A \cap B$$

Definition (Logical Equivalency)**.** If two complex statements are made up of the same statements, then they are *logically equivalent.* ($\iff$)

$$1 < 2 \quad x < 2$$

We'll symbolize the statement P with the variable x for $P(x)$

Example: $P : (\forall\, x \in \mathbb{N} \quad x < 2)$

$$\forall\, x \in A \quad P(x)$$

is true if every $P(x)$ is true, and will be false if even one $P(x)$ is false.

$$\exists\, x \in A \quad P(x)$$

will be true if even one $P(x)$ is true, and will be false if all $P(x)$ is false.

Given $P(x), Q(x)$, the following logical statements can be constructed:

$$\begin{array}{lll} \forall\, x \in A & \forall\, y \in B & P(x) \wedge Q(y) \\ \exists\, x \in A & \exists\, y \in B & P(x) \wedge Q(y) \\ \exists\, x \in A & \forall\, y \in B & P(x) \wedge Q(y) \\ \forall\, x \in A & \exists\, y \in B & P(x) \wedge Q(y) \end{array}$$

1.3 Series

Definition. Given two sets A, B:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Note. The order of A, B does matter.

If A, B are *finite*:

$$|A \times B| = |A| \cdot |B|$$

Definition (Plane)**.**

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$$

If $A_1, \ldots, A_n$ are sets:

$$\bigtimes_{i=1}^{n} = A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid \forall\, i \in [n], a_i \in A_i\}$$

If $A_1, \ldots A_n$ are finite:

$$\left| \bigtimes_{i=1}^{n} A_i \right| = \prod_{i=1}^{n} |A_i|$$

Definition (Characteristics)**.**

$$\begin{gathered} A \times \emptyset = \emptyset \\ A \times A = A^2 \\ \underbrace{A_1 \times \ldots \times A_n}_{n \text{ times}} = A^n \end{gathered}$$

DISCRETE MATHEMATICS

2

FUNCTIONS AND PERMUTATIONS

Moshe Krumbein - Fall 2021

2.1 Functions

Given two sets A, B, function $f : A \mapsto B$, all $a \in A$ maps to $b \in B$.

A is called the *domain* and B is called the *range*.

$$f(a) = b$$

a is *a source* of b, and b is *the image* of a.

For $c \subset a$, the image of c is:

$$\begin{aligned} f(C) &= \{b \in B \mid a \in C : f(a) = b\} \subseteq B \\ &= \{f(a) \mid a \in C\} \end{aligned}$$

Example 2.1.1. Given $f : A \mapsto B$:

$$\operatorname{Im} f = f(A) \subseteq B$$

Given $D \subseteq B$, the source of D:

$$f^{-1}(D) = \{a \in A \mid f(a) \in D\}$$

1.

$$A \subseteq U$$
$$\mathbb{1} : U \mapsto \{0,1\}(\chi)$$
$$\forall\, a \in U, \mathbb{1}_A(a) = \begin{cases} 1 & a \in A \\ 0 & a \notin A \end{cases}$$

2.

$$A = \mathbb{Z}^k \quad B = \mathbb{Z}$$
$$f((a_1, \ldots, a_n)) = a_3$$

3.

$$\text{Given: } \{(a_1, \ldots, a_n)\} \subseteq \mathbb{Z}^k$$
$$f : \underbrace{[n]}_{\{1,2,\ldots,n\}} \mapsto \mathbb{Z}$$
$$\forall\, i \in [n] : f(i) = a_i$$

Claim. Given: $f : A \mapsto B$, $D_1, D_2 \subseteq B$:

$$f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2)$$
$$a \in f^{-1}(D_1 \cap D_2) \iff f(a) \in D_1 \cap D_2$$

Given: $C_1, C_2 \subseteq A$:

$$f(C_1 \cap C_2) \neq f(C_1) \cap f(C_2)$$

2.1.1 Characteristics of Functions

Given $f : A \mapsto B$:

f is *injective* (one-to-one) if:

$$\forall\, a_1, a_2 \in A : a_1 \neq a_2\ \exists\ f(a_1) \neq f(a_2)$$
$$\forall\, a_1, a_2 \in A \quad f(a_1) = f(a_2) \implies a_1 = a_2$$

f is *surjective* (onto) if:

$$\operatorname{Im} f = B$$

If f is injective: $|A| \leq |B|$.

If f is surjective: $|A| \geq |B|$.

If f is both injective and surjective, it is *bijective* (invertible) and: $|A| = |B|$. If we have two finite sets A, B, function $f : A \mapsto B$, and $C \subseteq A, D \subseteq B$:

1. $|f(c)| \leq |C|$
2. f is injective:
   (a) $|f(C)| = |C|$
   (b) $|f^{-1}(D)| = |D|$
3. f is surjective:
   (a) $|f^{-1}(D)| \geq |D|$
4. If f is injective and $|A| = |B|$, then it is also surjective.
5. If f is surjective and $|A| = |B|$, then we've learned nothing new.

2.1.2 Composing Functions

Given sets A, B, C:

$$f : A \mapsto B, \quad g : B \mapsto C$$
$$g \circ f : A \mapsto C : \forall\, a \in A :$$
$$(g \circ f)(a) = g(f(a))$$

2.1.3 Identity function

$$\mathrm{Id}_A : A \mapsto A$$
$$f \circ \mathrm{Id}_A : A \mapsto B$$
$$f \circ \mathrm{Id}_A : f$$
$$\mathrm{Id}_B \circ f : A \mapsto B$$
$$\mathrm{Id}_B \circ f : f$$

2.1.4 Inverse function

Given $f : A \mapsto B, g : B \mapsto C$:

g is the inverse of f if:

$$g \circ f = \mathrm{Id}_A$$
$$f \circ g = \mathrm{Id}_B$$

If the previous is true, then $g = f^{-1}$.

2.1.5 Examples

Example 2.1.2. Given $f : A \mapsto B, C_1, C_2 \subseteq A$:

1. If $C_1 \subseteq C_2$, then $f(C_1) \subseteq f(C_2)$.

   Yes.

   Suppose $a \in f(C_1) \implies b \in C_1$ such that $f(b) = a$. Since we also know $b \in C_2$, therefore $f(b) \subseteq f(C_2) \implies f(C_1) \subseteq f(C_2)$.

2. If $f(C_1) \subseteq f(C_2)$, then $f(C_1) \subseteq f(C_2)$.

   No.

   We define $A = \{1, 2\}, B = \{u\}$, $f(1) = f(2) = a$.

   item If f is injective, and $f(C_1) \subseteq f(C_2)$,then $C_1 \subseteq C_2$.

   Suppose $c \in C_1, c \notin C_2$.

   $f(c) \notin f(C_2)$

Example 2.1.3. Let $f : A \mapsto B, g : B \mapsto C$. Prove that if $g \circ f$ is injective then f is also injective.

Suppose $a_1, a_2 \in A, a_1 \neq a_2$.

$$g \circ f(a_1) \neq g \circ f(a_2)$$
$$f(a_1) \neq f(a_2)$$

Example 2.1.4. Let $f : A \mapsto B, g : B \mapsto A, h : B \mapsto A$:

1. $g \circ f = \mathrm{Id}_A$ and $h \circ f = \mathrm{Id}_A$, then $g = h$.

   False

2. $f \circ g = \mathrm{Id}_B$ and $h \circ f = \mathrm{Id}_A$, then $g = h$.

   True

2.2 Permutations

A *permutation* is a (possible) rearrangement of objects. For example, there are 6 permutations of the letters a, b, c:

$$abc, acb, bac, bca, cab, cba$$

Permutation on $[n]$ is $f : [n] \mapsto [n]$. For example $\mathrm{Id}_{[n]}$:

$$f : A \mapsto A$$
$$f^2 = f \circ f : A \mapsto A$$
$$f^m = \underbrace{f \circ f \circ f \ldots}_{m \text{ times}}$$

If $f \circ g$ is bijective, it is a permutation.

$$\sigma^6 = \mathrm{Id}_\sigma$$
$$\sigma^{100} = \mathrm{Id}_\sigma$$

Definition (Permutation)**.** Permutation of $[n]$ is $f : [n] \mapsto [n]$ is surjective and injective.

We symbolize the *collection* of permutations of $[n]$: S_n

If $f, g \in S_n$, then $g \circ f : [n] \mapsto [n]$.

If $g \circ f$ is *one-to-one*, then we see it's also *onto* $g \circ f \in S_n$.

Claim. If $f : A \to B$ is *one-to-one* and $g : B \to C$ is also *one-to-one*, then $g \circ fA \to C$ is also *one-to-one*.

Proof. Suppose $a_1, a_2 \in A$ such that $(g \circ f)(a_1) = (g \circ f)(a_2)$ (which means $a_1 = a_2$).

Given $g(f(a_1)) = g(f(a_2))$ is *one-to-one* $\implies$ $f(a_1) = f(a_2)$. f is also *one-to-one* $\implies$ $a_1 = a_2$. ■

Conclusion. $g \circ f$ is *one-to-one*.

Definition. Let $f : [n] \to [n]$ be the permutation of f, the minimal number of permutations k such that $f_k = \mathrm{Id}_{[n]}$.

We see that k is the *lowest common multiple* of the lengths of the sub-permutations.

DISCRETE MATHEMATICS

3

BINARY RELATIONS AND EQUIVALENCE RELATIONS

Moshe Krumbein - Fall 2021

3.1 Binary Relations

Definition (Binary Relation)**.** Given two sets A, B, all subsets $R \subseteq A \times B$ is called *binary relations* from A to B. If $(a, b) \in R$ we symbolize relations as aRb.

Example 3.1.1.

$$A = B = \mathbb{R} \quad R = \{(x, x^2) \mid x \in A\}$$

Definition. If $A = B$, then $R \subseteq A \times A$ is called a *relation on* A.

Example 3.1.2. $A = \{2, 3, 4, 5, 8, 12\}, R = \{(a, b) \mid a, b \in A, a|b\}$

$$R = \{(2, 4), (2, 8), (2, 12), (2, 2), (3, 3), (3, 12), \ldots\}$$

Definition. *Empty relation*: $R = \emptyset$

Definition. *Full (universal) relation*: $R = A \times A$

Definition (Power Set)**.** Given set A, we define the *power set* as being all the subsets of A:

$$2^A = P(A) = \{B \mid B \subseteq A\}$$
$$|P(A)| = 2^{|A|}$$

Example 3.1.3. $B = P(\{1, 2, 3\})$:

$$R = \{(A_1, A_2) \mid A_1, A_2 \in B, A_1 \subseteq A_2\}$$

3.1.1 Characteristics of Binary Relations

1. R is *reflexive* if for all $a \in A : (a, a) \in R$
2. R is *irreflexive* if for all $a \in A : (a, a) \notin R$
3. R is *symmetric* if for all $a, b \in A : (a, b) \in R \implies (b, a) \in R$
4. R is *antisymmetric* if for all $a, b \in A : (a, b), (b, a) \in R \implies a = b$
5. R is *transitive* if for all $a, b, c \in A : (a, b), (b, c) \in R \implies (a, c) \in R$

$A \neq \emptyset$ and not limited in size can have a relation that is reflexive, symmetric and antisymmetric: $R = \{(a, a) \mid a \in A\}$.

Example 3.1.4.

$$A \in \mathbb{Z}$$
$$a|x - y \iff xRy$$
$$(x, y), (y, z) \in R \implies (x, z) \in R$$
$$(x, y) \in R \implies \exists t_1 \in \mathbb{Z}, x - y = 2t_1$$
$$(y, z) \in R \implies \exists t_2 \in \mathbb{Z}, y - z = 2t_2$$
$$x - z = x - y + y - z = 2t_1 + 2t_2 = 2(t_1 + t_2) \implies (x, z) \in R$$

3.2 Equivalence Relations

Definition. R is a *equivalence relation* on A if R is *reflexive*, *symmetric*, and *transitive*.

Symbol. If R is a equivalence relation on A we sometimes symbolize $(x, y) \in R$ or $x \sim y$.

Definition. If R is a equivalence relation on A then for all $a \in A$ we define a *equivalence closure* to be:

$$[a]_R = \{b \in A \mid (a, b) \in R$$

Given set A the closure of A is the collection $\{A_i\}_{i \in I}$:

1. $\forall i \in I, A_i \neq \emptyset$
2. $\forall i, j \in I, A_i \neq A_j \implies A_i \cap A_j = \emptyset$
3. $\bigcup_{i \in I} A_i = A$

Example 3.2.1.

$$A = \mathbb{R} = \{(-\infty, -1), [-1, 1], (1, \infty)\}$$
$$B = \mathbb{N} = \{\{1, 3, 5, 7, \ldots\}, \{2, 4, 6, 8, \ldots\}\}$$

Claim. If R is a equivalence relation on A then the collection of all the equivalence closures:

$$\{[a]_R \mid a \in A\}$$

is a *partition* of A.

Symbol. Equivalence closures: A/R

$$A/R = \{[a]_R \mid a \in A\}$$

D is the *representative set* if:

$$\forall a \in A : |D \cap [a]_R| = 1$$

Example 3.2.2 (Identity relation).

$$\forall a \in A : [a]_R = \{a\}$$
$$A/R = \{\{a\}\}_{a \in A}$$
$$D = A$$

Example 3.2.3 (Universal Relation).

$$R = A \times A$$
$$A/R = \{A\}$$
$$\forall a \in A : D = \{a\}$$

Example 3.2.4.

$$A = \mathbb{Z}$$
$$R = \{(x, y) \mid x, y \in A, 2|x - y\}$$
$$[0]_R = \{-4, -2, 0, 2, 4, 6, \ldots\}$$
$$[1]_R = \{-3, -1, 1, 3, 5, \ldots\}$$
$$A/R = \{[0]_R, [1]_R\}$$
$$D = \{0, 1\}$$
(or any two even/odd numbers)

3.3 Binary Relations

Definition. $R \subseteq A \times A$

Binary relations are made up of pair from set A that fulfill certain parameters.

Example 3.3.1.

$$A = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$$
$$R = \{(m_1, n_1), (m_2, n_2) \mid m_1 n_2 = m_2 n_1\}$$

To prove that this relation is an equivalence relation, we have to prove that it is *reflexive*, *symmetric* and *transitive*.

DISCRETE MATHEMATICS

4

PARTIAL ORDERED RELATIONS

Moshe Krumbein - Fall 2021

4.1 Partial Ordered Relations

Given relation R on a set, then we say the R is a partial ordered relation if R is *reflexive*, *antisymmetric*, and *transitive*. In this case we say that A is a *partial ordered set*.

Definition. A partial ordered relation that exists for all $\forall x, y \in R \; \exists \; (x, y) \in R$ or $(y, x) \in R$ is called a *linear order*.

Suppose that R is a partial ordered relation on A:

$$(a, b) \in R \quad a \leq_R b$$

$x \in A$ is called the *maximum* if $\forall \; y \in A$, if $(x, y) \in R$, then $x = y$. (x has no arrows going out of it except for to itself).

$x \in A$ is called the *minimum* if $\forall \; y \in A$, if $(y, x) \in R$, then $x = y$. (x has no arrows going to it except for to itself).

4.2 Hasse Diagram

We'll say that pair $(x, y) \in R$ is "required" in a Hasse diagram if $x \neq y$, and therefore:

$$\forall z \in A(x, z), (z, y) \in R \implies z = x \text{ or } z = y$$

Essentially, we can get rid of all arrows that represent transitivity and reflexivity because they are assumed.

Claim. If R is a *linear ordered relation* on A, then there exists in A only one maximum and minimum.

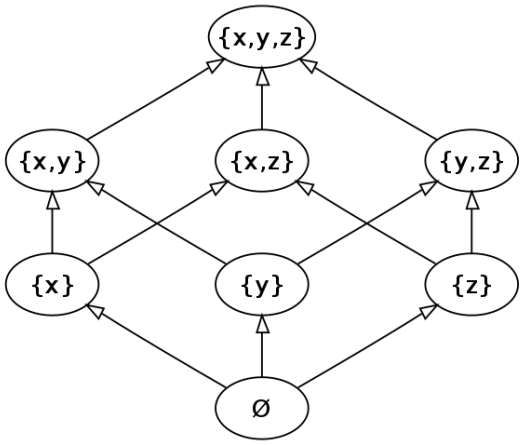

Figure 4.1: Example of a Hesse diagram

DISCRETE MATHEMATICS

5

COUNTING PROBLEMS

Moshe Krumbein - Fall 2021

5.1 Introduction

Essentially, there are four basic counting problems:

	Repeats	No Repeats
Order is important	?	?
Order is unimportant	?	?

Table 5.1: Types of counting problems

5.2 Order is important

5.2.1 Repeats

When order is important but there are repeats, we can simply express the number of ways to place n different balls in k places as:

$$n^k$$

5.2.2 No Repeats

If $n = k$, we get the number of permutations on $[n]$, which is $n!$.

$$D = \{f : [k] \to [n] \mid f \text{ is injective}, \forall i \in [k] : f(i) = n\}(n \notin Imf)$$

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

$$E = \{f : [k] \to [n] \mid f \text{ is injective}, \exists! i \in [k] : f(i) = n\}$$
$$\forall i \in [k] : E_i = \{f \in E \mid f(i) = n\}$$
$$|E_i| = \frac{(n-1)!}{n-1-(k-1)} = \frac{(n-1)!}{(n-k)!} \implies |E| = \frac{k(n-1)!}{(n-k)!} = \frac{n!}{(n-k)!} - \frac{(n-1)!}{(n-1-k)!}$$

Simply put, the number of ways to place n distinct balls in k places without repeats is:

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

5.3 Order is unimportant, without repeats

Instead of dealing with sequences, we're dealing with sets.

In essence, when order is unimportant, we just divide the answer where order is important by $k!$:

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

This is also known as the *binomial coefficient*, symbolized as:

$$\binom{n}{k}$$

5.3.1 Characteristics of binomial coefficients

1. $\binom{n}{0} = 1, \binom{n}{n} = 1, \binom{n}{1} = n = \binom{n}{n-1}$
2. $\binom{n}{k} \in \mathbb{N} \quad (n \in \mathbb{N} \cup \{0\}, 0 \leq k \leq n)$
3. Symmetry: $\binom{n}{k} = \binom{n}{n-k}$

   Symbol.

$$[n] = \{1, 2, \ldots, n\}, \binom{[n]}{k} = \{A \subseteq [n] \mid |A| = k\}$$
$$\left|\binom{[n]}{k}\right| = \binom{n}{k}$$

Proof.

$$f : \binom{[n]}{k} \to \binom{[n]}{n-k}$$
$$A \in \binom{[n]}{k}, \quad f(A) = ([n] \setminus A) \in \binom{[n]}{n-k}$$
$$f(f(A)) = A \quad B \in \binom{[n]}{n-k}, f(f(B)) = B$$

■

Algebraically:

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

Back to characteristics:

4. Pascal's rule:
$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$

5.4 Order is unimportant, with repeats

5.4.1 Multinomial Coefficients

If we had to order k_1 balls of the color 1, k_2 balls of color 2, $\dots k_m$ balls of color m, how many ways can we sort them (where the order of balls of the same color does not matter)?

$$n = \sum_{i=1}^{m} k_i, \quad \frac{n!}{k_1!k_2!\dots k_m!} = \binom{n}{k_1, k_2, \dots, k_m} - \textit{multinomial coefficient}$$

As a generalization:

$$\frac{(a+b+c)!}{a!\ b!\ c!} = \binom{a+b+c}{a,b,c} = \binom{a+b+c}{c} \cdot \binom{a+b}{b} \cdot \binom{a}{a}$$

If we apply Pascal's rule to multinomial coefficients, we receive the following generalization:

$$\binom{a+b+c}{a,b,c} = \binom{(a+b+c)-1}{a-1,b,c} + \binom{(a+b+c)-1}{a,b-1,c} + \binom{(a+b+c)-1}{a,b,c-1}$$

5.4.2 Different ways to ask the same question

1. How many ways can we distribute k items to n people?
2. How many ways can we pick k items from n different piles?
3. How many solutions (whole, positive) to the following equation:

$$x_1 + x_2 + \cdots + x_n = k$$

A helpful way to view this problem is by asking how many ways can we place $n-1$ dividers among between k places? (which really means if dividers take up space then how many ways to place $n-1$ items over $k+(n-1)$ places?)

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

5.5 Conclusion

	Repeats	No Repeats
Order is important	n^k	$\dfrac{n!}{(n-k)!}$
Order is unimportant	$\binom{n+k-1}{k}$	$\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$

Table 5.2: Our final table

DISCRETE MATHEMATICS

6

COMBINATORICS, PASCAL'S TRIANGLE, AND NEWTON'S BINOMIAL THEOREM

Moshe Krumbein - Fall 2021

6.1 Combinatorics

Question How many ways can we arrange:

- k black balls
- l white balls

such that no two black balls will be next to each other?

- If $l = k - 1$, then there is exactly 1 way to arrange the balls
- If $l = k$, then there are $k + 1$ ways to arrange the balls

General Case Within l balls, $k - 1$ within those have to "divide" k of those balls. There are $l - (k - 1)$ white balls remaining, which have to "fill" $k + 1$ spaces.

This is similar to our fourth problem, which can also take the form:

$$x_1 + x_2, \dots x_{k+1} = l - k + 1$$
$$\Downarrow$$
$$\binom{(k+1) + (l-k+1) - 1}{(k+1) - 1} = \binom{l+1}{k}$$

In other words, for all (k) black balls, we're going to "reserve" that many ($k - 1$) white balls (enough to fill in the gaps). With the remaining white balls, we can distribute them in any order throughout (around) the black balls ($k + 1$ places).

Alternate solution We'll first place the l white balls, creating $l+1$ spaces, and we have to distribute all k black balls (one per space maximum):

$$\binom{l+1}{k}$$

6.2 Pascal's Triangle

Reminder.

$$\binom{n}{0} = 1, \binom{n}{n} = 1$$
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

$$\binom{0}{0}$$
$$\binom{1}{0}\ \binom{1}{1}$$
$$\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2}$$
$$\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3}$$
$$\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4}$$
$$\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5}$$

Figure 6.1: Pascal's Triangle - Binomial Coefficients

```
                1
              1   1
            1   2   1
          1   3   3   1
        1   4   6   4   1
      1   5   10  10  5   1
    1   6   15  20  15  6   1
  1   7   21  35  35  21  7   1
```

Figure 6.2: Pascal's Triangle - Numbers

6.2.1 Characteristics

- We can see that each value is the sum of the two numbers above it.
- $\forall\ n \in \mathbb{N} : \binom{n}{0} = \binom{n}{n} = 1$
- $\forall\ n \in \mathbb{N}, 0 \leq k \leq n : \binom{n}{k} = \binom{n}{n-k}$

- *Unimodality*:

$$\binom{n}{k+1} \geq \binom{n}{k} \iff \frac{n!}{(k+1)!(n-k-1)!} \geq \frac{n!}{k!(n-k)!}$$
$$\Updownarrow$$
$$\frac{n-1}{2} \geq k$$

  In other words, the middle column of Pascal's Triangle always contains the highest value in its row and the values decrease going left and going right.

- The sum of row n is equal to 2^n

$$P([n]) \equiv \{A \mid A \subseteq [n]\}$$
$$|2^{[n]}| = |P([n])| = ?$$

Claim. $|P([n])| = 2^n$

Given $S \subseteq A$:

$$\chi_s : A \to \{0,1\}$$
$$\chi_s(a) = \begin{cases} 1 & a \in S \\ 0 & a \notin S \end{cases}$$

We want to find a set B such that $|B| = 2^n$ so that there exists a function $f : P([n]) \to B$ which is both *injective* and *surjective*.

Proof. We define $B = \{f : [n] \to \{0,1\}\}$, and we know that $|B| = 2^n$.

We define the function $T : P([n]) \to B$:

$$\forall A \subseteq P([n]) : A \in P([n])$$
$$T(A) = \chi_A = \begin{cases} 1 & a \in A \\ 0 & a \notin A \end{cases}$$

T is *one-to-one* and *onto*:

$$f \in B \quad T^{-1}(f) = \{k \in [n] \mid f(k) = 1\}$$

Conclusion.

$$|P([n])| = |B| = 2^n$$

■

6.3 Newton's Generalized Binomial Theorem

$$(a+b)^n$$

$$\begin{aligned}
(a+b)^1 &= a+b \\
(a+b)^2 &= \underbrace{\binom{2}{0}}_{1} b^2 + \underbrace{\binom{2}{1}}_{2} ab + \underbrace{\binom{2}{2}}_{1} a^2 \\
(a+b)^3 &= \underbrace{\binom{3}{0}}_{1} b^3 + \underbrace{\binom{3}{1}}_{3} ab^2 + \underbrace{\binom{3}{2}}_{3} a^2 b + \underbrace{\binom{3}{3}}_{1} a^3 \\
(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}
\end{aligned}$$

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}$$

Let's play with some more values for a and b:

$$(-1+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$$

$$\Downarrow$$

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^k \binom{n}{n} = 0$$

$$\Downarrow$$

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots$$

Conclusion. In other words, the number of subsets of $[n]$ of even size is equal to the number of subsets of $[n]$ of odd size.

We can show this easily if n is odd by showing that $\binom{n}{k} = \binom{n}{n-k}$, which allows us to draw a one-to-one symmetry from every term to its corresponding equivalent term.

Another proof Let there be A be a set with the size $n \in \mathbb{N}$ and $a \in A$.

$$F_1 = \{B \subseteq A \mid |B| \text{ is even}\}$$
$$F_2 = \{B \subseteq A \mid |B| \text{ is odd}\}$$

$$f : F_1 \to F_1 \quad \forall B \in F_1 :$$
$$f(B) = \begin{cases} B \setminus \{a\} & a \in B \\ B \cup \{a\} & a \notin B \end{cases}$$

We see that if $|B|$ is even, then $|f(B)|$ is odd and $f(f(B)) = B$. We also see that f is *invertible* as it's *one-to-one* and *onto*, and therefore we see that $|F_1| = |F_2|$.

6.3.1 Generalizing the Binomial Theorem

Example 6.3.1.

$$(a + b + c)^{17}$$

First, we know that for each term, the sum of powers of a, b and c will be 17. In regards to each term's coefficient, we can express it in the following way:

"What is the coefficient of $a^3b^6c^8$?" is equivalent to asking how many ways can we arrange in a row 3 as, 6 bs and 8 cs, which can be expressed by the following multinomial coefficient:

$$\binom{17}{3, 6, 8} = \frac{17!}{3!6!8!}$$

6.3.2 Multinomial Theorem

$$m \in \mathbb{N} \quad (x_1 + x_2 + x_3 + \cdots + x_n)^m$$
$$= \sum_{\substack{k_1, k_2, \ldots, k_n \in \mathbb{N} \cup \{0\} \\ k_1 + k_2 + \cdots + k_n = m}}^{n} \binom{m}{k_1, k_2, \ldots, k_n} x_1^{k_1} x_2^{k_2} x_3^{k_3} \ldots x_n^{k_n}$$

6.4 Paths on a Grid

Example 6.4.1. There are two delegates: A and B, with $2k$ ballots (k that have A and k ballots have B). How many ways can we order the $2k$ ballots such that there are never more ballots for A than B? ($B \geq A$)

Similar problems include the "line for the movies" problem and "number of balanced series of n parentheses" (computer science).

$$\underbrace{()(())}_{\text{balanced}} \quad \underbrace{())(()}_{\text{unbalanced}}$$

Algebraic expression:

$$A = \left\{ a \in \{-1,1\}^{2n} \mid \sum_{i=1}^{2n} a_i = 0 \right\} \quad |A| = \binom{2n}{n}$$

$$B = \left\{ a \in A \mid \forall k \in [2n] : \sum_{i=1}^{k} a_i \leq 0 \right\} \quad |B| = ?$$

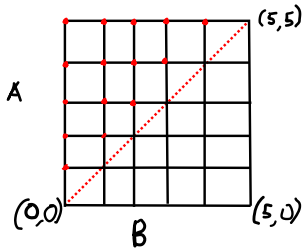

Figure 6.3: Grid expression where $k = 5$

Symbols

A - Total number of paths from $(0,0)$ to (n,n) where $|A| = \binom{2n}{n}$

B - Paths in A that do not go above the main diagonal

C - Paths that go above the main diagonal

$$B = A \setminus C$$
$$|B| = |A| - |C| \Leftarrow C \subseteq A$$

D - Total number of paths from $(0,0)$ to $(n-1, n+1)$ where $|D| = \binom{2n}{n-1}$

Claim. How many ways are there to go from $(0,0)$ until (n,n) without crossing the main diagonal?

$$\frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1}$$

$$|B| = |A| - |C| \underset{|C|=|D|}{=} |A| - |D| = \binom{2n}{n} - \binom{2n}{n+1}$$

We define $f : C \to D$:

Given $a \in C$, we symbolize $a = (a_1, a_2, \ldots, a_n)$:

$$A = \left\{ a \in \{-1,1\}^n \mid \sum a_i = 0 \right\}$$

Where -1 is a step right and 1 is a step up.

Where we need this to be true:

$$\sum_{i=1}^{k} a_i > 0$$

$$k = \min\left\{1 \le k \le 2n \mid \sum_{i=1}^{k} a_i > 0\right\}$$

$$(f(a))_i = \begin{cases} a_i & 1 \le i \le k \\ -a_i & k < i \end{cases}$$

We notice that for $f(a)$:

$$\sum_{i=1}^{2n} (f(a))_i = 2$$

Therefore we see that f expresses the path between $(0,0)$ to $(n-1, n+1)$. Notice that for all $a \in C$:

$$f(f(a)) = a \implies f \circ f|_C = \mathrm{Id}_C$$

Proof.

$$\implies f \text{ is } \textit{invertible}$$
$$\implies |C| = |D|$$
$$\implies |B| = C_n = \binom{2n}{n} - \binom{2n}{n+1}$$

■

DISCRETE MATHEMATICS

7

THE INCLUSION–EXCLUSION PRINCIPLE

Moshe Krumbein - Fall 2021

7.1 Summation Principle

Theorem. If $A_1, \ldots, A_n$ are *pairwise disjointed*, then:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|$$

However, there are $\binom{n}{2}$ conditions to check:

$$\forall a, j \in [n] : A_i \cap A_j = \emptyset$$

In General

$$\begin{aligned} n = 2: &\quad |A \cup B| = |A| + |B| - |A \cap B| \\ n = 3: &\quad |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| \\ &\quad + |A \cap B \cap C| \end{aligned}$$

Symbol. X is a finite set, and $A_1, \ldots A_n$ are subsets of X.

We symbolize $N = \{1, 2, \ldots, n\}$ for all $\emptyset \neq k \subseteq N$.

$$A(k) = \bigcap_{i \in k} A_i$$

For example:

$$k = \{1, 4, 5, 8\} \implies A(k) = A_1 \cap A_4 \cap A_5 \cap A_8$$

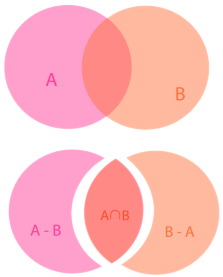

Figure 7.1: Visualization of $|A \cup B| = |A| + |B| - |A \cap B|$

Theorem (Inclusion-Exclusion Formula)**.**

$$\left|\bigcup_{i=1}^{n} A_i\right| = \underbrace{|A_1| + |A_2| + \cdots + |A_n|}_{\binom{n}{1}} - \underbrace{|A_1 \cap A_2|}_{\binom{n}{2}}$$
$$\cdots + (-1)^{n+1}|A_1 \cap A_2 \cap \cdots \cap A_n|$$
$$= \sum_{j=1}^{n} \sum_{\substack{k \subseteq N \\ |k|=j}} (-1)^{j-1}|A(k)|$$
$$= \sum_{k \subseteq N, k \neq \emptyset} (-1)^{|k|+1}|A(k)|$$
$$\boxed{\sum_{j=0}^{n} \sum_{\substack{k \subseteq N \\ |k|=j}} (-1)^{j}|A(k)|}$$

7.2 First Use

Question: Given S_n as permutations on $[n]$, and $\sigma \in S_n : 1 \leq i \leq n$ is a *fixed point*, if $\sigma(i) = i$, our question is: how many permutations x exist that do not contain a *fixed point*?

Solution:

$$x = S_n \quad |x| = n!$$
$$\forall 1 \le i \le n : A_i = \{\sigma \in S_n \mid \sigma(i) = i\}$$

$\bigcup_{i=1}^{n} A_i$ – all of the permutations that contain at least one fixed point.

$$|A_i| = (n-1)! \quad 1 \le i < j \le n : |A_i \cap A_j| = (n-2)!$$
$$\forall k \subseteq N : |k| = j : \quad |A(k)| = (n-j)!$$
$$\left| X \setminus \bigcup_{j=0}^{n} A_i \right| = \underbrace{\sum_{j=0}^{k} \sum_{\substack{k \subseteq N \\ |k|=j}} (-1)^j \underbrace{(n-j)!}_{|A(k)|}}_{\text{constant for all } |k|=j} = \sum_{j=0}^{n} \binom{n}{j} (n-j)!(-1)^j$$
$$= n! \sum_{j=0}^{n} \frac{(-1)^j}{j!} \xrightarrow{n \to \infty} n! \cdot \boxed{\frac{1}{e}}$$

7.3 Second Use

Given finite sets $D, R : |D| = d, |R| = r$.

$$|A| = |\{f : D \to R \mid f \text{ is onto } (\operatorname{Im} f = R)\}| = ?$$

If $d < r$, then $|A| = 0$, and if $d = r$, then $|A| = r!$.

We're going to subtract from the total number of functions, all of the functions that are not *onto*.

Solution

$$X = \{f : D \to R\} \quad |X| = r^d$$
$$\forall 1 \le i \le r : A_i = \{f \in X \mid i \notin \operatorname{Im} f\}$$

$\bigcup_{i=1}^{r} A_i$ – All of the functions that are not onto.

$$A = X \setminus \bigcup_{i=1}^{r} A_i$$
$$\forall 1 \le i \le r \quad |A_i| = (r-1)^d$$
$$\forall 1 \le i < j \le r \quad |A_i \cup A_j| = (r-2)^d$$
$$\forall k \subseteq R, |k| = j \quad |A(k)| = (r-j)^d$$
$$\left| X \setminus \bigcup_{i=1}^{r} A_i \right| = \sum_{j=0}^{r} \sum_{\substack{k \subseteq \{1,\dots r\} \\ |k|=j}} (-1)^j |A(k)| = \sum_{j=0}^{r} \binom{r}{j} (-1)^j (r-j)^d$$

7.4 Third Use

Claim. For all $n \in \mathbb{N}$ there exists a factorization to primes, in other words primes $p_1, \ldots, p_m$, $S_1, \ldots, S_m \in \mathbb{N}$, such that:

$$n = p_1^{S_1} p_2^{S_2} \ldots p_n^{S_n}$$

Definition. For $m, n \in \mathbb{N}$, we say that m and n are *relatively prime* or *coprime* if:

$$\gcd(m, n) = \max\{k \in \mathbb{N} \mid k|m, k|n\} = 1$$

In other words, they do not share any prime factors.

Claim. If $k, n \in \mathbb{N}$, then the number of terms between 1 and n that divides k is $\lfloor \frac{n}{k} \rfloor$.

In other words, $|\{1 \leq i \leq n \mid i \in \mathbb{N}, k|i\}| = \lfloor \frac{n}{k} \rfloor$

Explanation If we symbolize $l = \lfloor \frac{n}{k} \rfloor$, l is the largest integer such that $l \leq \frac{n}{k}$.

$$A = \{k, 2k, 3k, \ldots, lk\} \quad lk \leq \frac{n}{k} k = n$$
$$|A| = l = \left\lfloor \frac{n}{k} \right\rfloor$$

Question Given $n \in \mathbb{N}$ how many numbers $\{1, \ldots, n\}$ are *coprime* to n?

Definition (Euler's totient function)**.**

$$\varphi(n) = |\{x \in \mathbb{N} \mid x \leq n; x, n \text{ are } \textit{coprime}\}|$$

Example 7.4.1.

$$\varphi(12) = |\{1, 5, 7, 11\}| = 4$$

If p is prime, then $\varphi(p) = |\{1, 2, 3, \ldots, p-1\}| = p - 1$.

Theorem (Euler's totient function)**.** For $n \in \mathbb{N}$ if:

$$n = p_1^{s_1} p_2^{s_2} \ldots p_t^{s_t}$$

then:

$$\varphi(n) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right)$$

Example 7.4.2.

$$\varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$$

Proof. First, we notice that if $m \in \mathbb{N}$ is not *coprime* with n, then there exists some $1 \leq i \leq t$ such that $p_i | m$.

We define $x = [n]$.

$$\forall i : 1 \leq i \leq n : \quad A_i = \{x \in [n] \mid p_i | x\} \qquad |A_i| = \frac{n}{p_i}$$

$$1 \leq i < j \leq n : \quad A_i \cap A_j = \{x \in [n] \mid p_i | x, p_j | x\} \qquad |A_i \cap A_j| = \frac{n}{p_i p_j}$$

And in general:

$$k \subseteq \{1, \ldots, t\}$$

$$A(k) = \bigcap_{i \in k} A_i = \{x \in [n] \mid \forall i \in k : p_i | x\} = \left\{ x \in [n] \;\middle|\; \prod_{i \in k} p_i | x \right\}$$

$$|A(k)| = \frac{n}{\prod_{i \in k} p_i}$$

Based on our definition:

$$\begin{aligned} \varphi(n) = \left| X \setminus \bigcup_{i=1}^{t} A_i \right| &= \underbrace{n}_{|X|} - \sum_{i=1}^{t} \frac{n}{p_i} + \sum_{1 \leq i < j \leq n} \frac{n}{p_i p_j} - \sum_{1 \leq i < j < j \leq n} \frac{n}{p_i p_j p_k} + \ldots \\ &\quad + (-1)^j \sum_{\substack{k \subseteq \{1, \ldots, t\} \\ |k| = j}} \frac{n}{\prod_{i \in k} p_i} \\ &= n \sum_{j=0}^{n} (-1)^j \sum_{\substack{k \subseteq \{1, \ldots, t\} \\ |k| = j}} \frac{1}{\prod_{i \in k} p_i} \end{aligned}$$

With a little algebraic manipulation, we can see that our conclusion is indeed equal to:

$$n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i} \right)$$

■

DISCRETE MATHEMATICS

8

THE PIGEONHOLE PRINCIPLE AND INDUCTION

Moshe Krumbein - Fall 2021

8.1 The Pigeonhole Principle

8.1.1 Definition and Examples

Definition (The Pigeonhole Principle)**.** Given $m, n \in \mathbb{N}, m > n$, if we distribute m pigeons between n pigeonholes, then at least one hole with have at least two pigeons.

In other words, if $m > n$, then there does not exist $f : [m] \to [n]$ such that will be *injective*.

Claim (First Example). Suppose $A = \{0, 1, 2, \ldots, 11\}$. If we choose 7 numbers within A then we are guaranteed that there will be two numbers from our choice that will add to 11.

Proof. We define the following 6 sets:

$$\{0, 11\}, \{1, 10\}, \{2, 9\}, \{3, 8\}, \{4, 7\}, \{5, 6\}$$

where the sum of the elements of the set is equal to 11.

According to the *pigeonhole principle*, if we pick 7 numbers, we will certainly pick at least one of the 6 previously mentioned sets. ■

Claim (Second Example). If we choose 101 numbers from the set $\{1, 2, \ldots, 200\}$, we can be guaranteed that among the numbers we picked, one will divide another.

Proof. For all $1 \leq i \leq 100$, we define:

$$B_i = \{2i - 1, 2i\} \quad \bigcup_{i=1}^{100} B_i = [200]$$

Reminder. For all $n \in \mathbb{N}$, there exists a single prime factorization and specifically for $n \in [200]$, there exists a_n, b_n such that:

$$n = 2^{a_n} \cdot b_n$$

where $a_n \in \mathbb{N} \cup \{0\}, b_n \in \mathbb{N}$.

We notice that if $n \in [200]$ then $1 \leq b_n \leq 200$, or in other words: $b \in \{1, 3, 5, \ldots, 199\}$.

For all $j \in \{1, 3, 5, \ldots, 199\}$ we define:

$$B_j = \{n \in [200] \mid n = n^m \cdot j\}$$

In other words, the only odd factor in B_j will be j itself.

1. From the singularity of prime factorization:

$$j_1 \neq j_2 \implies B_{j_1} \cap B_{j_2} = \emptyset$$

2. $$\bigcup_{j \in \{1,3,5,\ldots,199\}} B_j = [200]$$

3. If $k, l \in B_j$ then we are guaranteed that one will divide another: (without loss of generality: $n_1 < n_2$)

$$k = 2^{n_1} \cdot j \quad l = 2^{n_2} \cdot j$$
$$2^{n_1} j | 2^{n_2} j \implies k | l$$

■

Claim (Third Example). Between all $n + 1$ different natural numbers, we can find 2 numbers such that their difference divides n without a remainder.

Proof.

Reminder. We have see that relation over the natural number defined as:

$$a \sim b : a - b = 0 \pmod{n}$$

Given $n + 1$ different natural numbers, as per the *pigeonhole principle*, 2 are part of the same *equivalence class*. ■

Claim (Fourth Example). If 13 natural numbers are written in a row, then there exists a run of adjacent numbers such that their sum divides by 13.

Proof. We define $1 \leq k \leq 13$ such that:

$$b_k = \sum_{i=1}^{k} a_i \quad b_0 = 0$$

From the previous claim, there exists $0 \leq i < j \leq 13$ such that:

$$b_j - b_i = 0 \pmod{13}$$

However:

$$b_j - b_i = \sum_{k=i+1}^{j} a_k$$

$$b_j - b_i = (a_1 + a_2 + \cdots + a_j) - (a_1 + a_2 + \cdots + a_i) = a_{i+1} + a_{i+2} + \cdots + a_j$$

■

8.1.2 Erdős–Szekeres theorem

Definition (Erdős–Szekeres theorem)**.** Sequence $(a_1, \ldots, a_n)$ is *monotonic* if $a_1 \leq a_2 \leq \cdots \leq a_n$ or $a_1 \geq a_2 \geq \cdots \geq a_n$

Given sequence $A = (a_1, a_2, \ldots, a_n)$, if $1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq k$ of k natural numbers, then $(a_{i_1}, a_{i_2}, \ldots a_{i_k})$ is a *subsequence* of length k of A.

Given series of $nm + 1$ distinct numbers then there exists a subsequence either *increasing* with length $n + 1$ or *decreasing* with the length $m + 1$.

Example 8.1.1 (Erdős–Szekeres theorem).

$$(1, 5, 0, 3, 2)$$

Length of: $2 \cdot 2 + 1$

There is a decreasing subsequence of length: $2 + 1$

Conclusion. For every sequence of the length $1 \cdot 11 + 1 = 12$ we can find a decreasing subsequence of length 2 or an increasing subsequence of length 2.

Proof. We define of all $i : 1 \leq i \leq nm + 1$:

p_1 - length of increasing subsequence with maximum length beginning with a_i.

q_1 - length of decreasing subsequence with maximum length beginning with a_i.

Proof by contradiction:

- If there does not exist a subsequence with length $m + 1$, then for all $i : 1 \leq p_i \leq m$.
- If there also isn't a decreasing subsequence with a length $n + 1$, then for all $i : 1 \leq q_i \leq n$.

Therefore, for all $1 \leq i \leq nm + 1$:

$$(p_i, q_i) \in [m] \times [n]$$
$$|[m] \times [n]| = mn$$

We have $nm + 1$ ordered pairs that are each part of a set with the size nm.

Per the *pigeonhole principle*, there exists $1 \leq i < j \leq nm + 1$ such that $(p_i, q_i) = (p_j, q_j)$. However, we know that $a_i \neq a_j$.

If $a_1 < a_j$, then $p_i > p_j$, which is a contradiction.

If $a_1 > a_j$, then $p_i < p_j$, which is a contradiction. ■

8.1.3 Generalized Pigeonhole Principle

If we distribute $ab + 1$ pigeons in a holes, then there is a hole that has at least $b + 1$ pigeons.

Proof. We will prove *by contradiction*:

We define c_i as the number of pigeons that come from the i^{th} hole.

According to the negative assumption, for all i, $c_i \leq b$, where we receive:

$$ab + 1 = \sum_{i=1}^{a} c_i \leq \sum_{i=1}^{a} b = ab$$

Which is a contradiction. ■

Example 8.1.2. For every group of 6 people, we will be able to find either 3 people who know one another or 3 people who do not know one another.

Proof. Suppose *Dani* is one of the people in a group.

Everyone else in the group can be split up into one of two groups:

A - People who know *Dani*.

B - People who don't know *Dani*.

Per the *generalized pigeonhole principle*, there will be a group containing 3 people.

If $|A| \geq 3$, if among set A there are at least 2 people who know each other, then along with *Dani*, we will find 3 people in the group who know one another. If there aren't, then we know there are 3 people in set A who do not know one another.

Similarly, if $|B| \geq 3$, if they don't know one another then there are 3 people know don't know each other and if they all know each other then that satisfies the requirement of having three people know each other.

$$5 = \underbrace{2}_{a} \cdot \underbrace{2}_{b} + 1$$

■

Example 8.1.3. A plane is colored with the colors green and white. Is is guaranteed that we will be able to find two *monochromatic* (the same color) points such that the distance between them is exactly 1?

Proof. Consider the vertices of an equilateral triangle of side length 1 on the plane. Per the *pigeonhole principle* at least two of the vertices will be the same color. ■

If we go up a dimension and consider a swimming pool colored with 3 different colors, we will still be able to find two monochromatic points at distance 1m from one another if we consider *tetrahedron* (three-sided pyramid) instead of a triangle in our previous proof.

8.2 Induction

8.2.1 What is induction?

Induction is proof technique regarding the natural numbers.

Axiom (Axiom of Induction)**.** For all $\emptyset \neq A \subseteq \mathbb{N}$, there exists a *minimum term.*

In other words:

$$\exists a_0 \in A \text{ s.t. } \forall a \in A : a_0 \leq a$$

Method of proving $p(n)$ using induction over the real numbers:

I. *Base case of induction.*

To show the statement holds for $p(1)$.

II. *Induction step.*

Posits that if $p(k)$ is true ($p \in \mathbb{N}$), then $p(k+1)$ will also be true.

If both steps are true, we can deduce that for $n \in \mathbb{N}$, $p(n)$ is true.

Proof. We will assume by counterexample that the two steps are true but not for all $n \in \mathbb{N}$, $p(n)$ is true.

We define $A = \{n \mid p(n) \text{ is false}\} \subseteq \mathbb{N}$. According to our assumption, $A \neq \emptyset$. As per the *axiom of induction*, there exists $n_0 = \min A$. We know that $1 \notin A$ and therefore $n_0 > 1$, $n_0 - 1 \notin A$, $n_0 - 1 \in \mathbb{N}$ and therefore $p(n_0 - 1)$ is true. Per *induction*, $p(n_0)$ must also be true, which is a contradiction. ■

8.2.2 Examples

Example 8.2.1.

$$1 + 3 + 5 + \cdots + (2n + 1) = \sum_{k=1}^{n} (2k - 1) = n^2$$

Proof. By induction:

I. $p(1)$:

$$1 = \sum_{k=1}^{1} 2k - 1 = 1 \qquad (\checkmark)$$

II. *Induction step*

Let's suppose $p(j)$ and prove $p(j + 1)$.

$$\sum_{k=1}^{j} (2k - 1) = j^2$$

$$\sum_{k=1}^{j+1} (2k - 1) = (j + 1)^2$$

$$\sum_{k=1}^{j+1} (2k - 1) = \sum_{k=1}^{j} (2k - 1) + 2(j + 1) - 1 = j^2 + 2j + 1 = (j + 1)^2 \qquad (\checkmark)$$

■

Example 8.2.2. For all $n \in \mathbb{N}$, $3|4^n - 1$.

Proof. By induction:

I.

$$3|4^1 - 1 \qquad (\checkmark)$$

II.

$$\exists t \in \mathbb{Z} \text{ s.t. } 4^k - 1 = 3t$$

$$4^{k+1} - 1 = 4 \cdot 4^k - 1 = 3 \cdot 4^k + 4^k - 1 = 3 \cdot 4^k + 3t = 3(4^k + 1)$$

$$4^k + 1 \in \mathbb{Z} \implies 3|4^{k+1} - 1 \qquad (\checkmark)$$

■

Example 8.2.3. For all $n \in \mathbb{N}$ it is possible to tile a grid of the size $2^n \times 2^n$ (excluding a 1×1 corner square) with "L" tiles (or any rotation of an "L" tile).

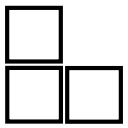

Figure 8.1: "L" tile

Proof. By induction:

I.
$$2^1 \times 2^1 - \text{ just place one "L" piece} \qquad (\checkmark)$$

II. $2^k \times 2^k$ works.

Given $2^{k+1} \times 2^{k+1}$, we can divide it into 4 smaller square of $2^k \times 2^k$.

■

8.2.3 Expansion on Induction

Theorem (Expansion of Induction)**.** Given $p(n), n \in \mathbb{N}$:

I. $p(n_0)$ is true for $n_0 \in \mathbb{N}$

II. $p(k) \implies p(k+1)$

Therefore, for all $n \in \mathbb{N}$ such that $n \geq n_0$, $p(n)$ is true.

Theorem (Complete Induction)**.** Given $p(n)$ over the natural numbers:

I. $p(1)$ is true.

II. $p(1) \wedge p(2) \wedge \cdots \wedge p(k) \implies p(k+1)$

Example 8.2.1. For all $n \in \mathbb{N}$, n can be expressed as a product of prime numbers.

Proof. By induction:

I. $p(1)$: 1 is a multiple of 0 primes.

II. Assuming $p(1), p(2), \ldots, p(k)$:

If $k+1$ is prime, we're done.

If not, then there exists $b, c \in \mathbb{N} \setminus \{1\}$ such that $bc = k+1$. Since $b, c < k+1$ through *complete induction*, we know that both b and c can be expressed as a product of primes, and therefore we see that $k+1$ can be expresses as the product of b and c's prime factors.

■

Example 8.2.2. For all $n \in \mathbb{N}$, there are n prime numbers.

Proof. By induction:

I.
$$n = 1 \qquad (\checkmark)$$

II. We suppose there exists k primes $p_1, p_2, p_3, \ldots p_k$ and we'll prove that there exists $k+1$ primes.

Consider $q = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$.

q isn't divisible by $p_1, p_2, \ldots p_k$.

If q is prime, we're done.

If q isn't prime, it still must have a prime factor, but since q isn't divisible by $p_1, p_2, \ldots p_k$, we know there are at least $k+1$ primes.

■

DISCRETE MATHEMATICS

9

RECURRENCE RELATIONS AND CATALAN NUMBERS

Moshe Krumbein - Fall 2021

9.1 Recurrence Relation

Definition (Recursion)**.** Sequence a_n is defined as *recursive* if there exists a function f such that for all $2 \leq n \in \mathbb{N}$:

$$a_n = \underbrace{f(a_1, a_2, \ldots, a_{n-1})}_{\text{recurrence relation}}$$

Definition (Recurrence Relation)**.** We say that a_n is defined as a *recurrence relation* of order k if for all $n > k$:

$$a_n = f(a_{n-1}, a_{n-2,\ldots,a_{n-k}})$$

Example 9.1.1 (Arithmetic Progression)*.*

$$\begin{gathered} a_1 = a \\ \forall n \geq 2 \quad a_n = a_{n-1} + d, d \in \mathbb{R} \\ a_n = a + (n-1)d \end{gathered}$$

Example 9.1.2 (Geometric Progression)*.*

$$\begin{gathered} a_1 = a \\ \forall n \geq 2 \quad a_n = a_{n-1} \cdot q \\ a_n = aq^{n-1} \end{gathered}$$

Example 9.1.3 (Tower of Hanoi)*.* What are the minimum number of a steps to move a tower of height n to the rightmost place?

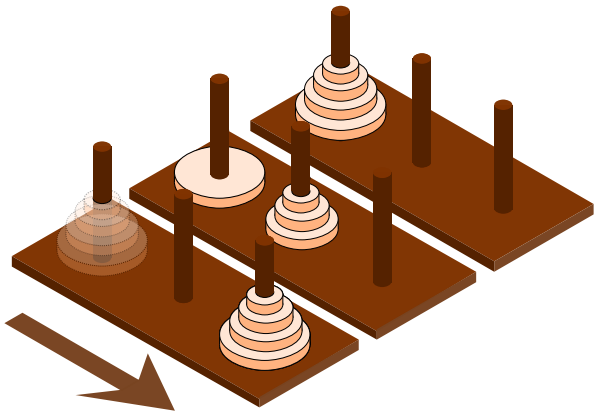

Figure 9.1: Tower of Hanoi

Base case: $a_1 = 1$.

In order to move the nth ring, we first have to move $n-1$ rings to the middle, move the nth ring, and then to move back all then $n-1$ rings.

$$a_n = 2a_{n-1} + 1$$

We see that $a_2 = 3$ and $a_3 = 7$. Maybe $a_n = 2^n - 1$?

Proof. Let us check using induction:

I.

$$a_1 = 1 \qquad (\checkmark)$$

II.

$$a_n = 2a_{n-1} + 1 = 2 \cdot (2^{n-1} - 1) + 1 = 2^n - 2 + 1 = 2^n - 1 \qquad (\checkmark)$$

■

Example 9.1.4 (Fibonacci Sequences). We have two newly-born rabbits.

- After a month of being born they become mature
- After a month of maturity they will give birth to a pair of baby bunnies
- Rabbits do not die.

$$f(0) = 1, f(1) = 1, f(2) = 2, f(3) = 3$$

Recurrence sequence (of order 2):

$$f(n) = \underbrace{f(n-2)}_{\text{just born}} + \underbrace{f(n-1)}_{\text{old rabbits}}$$

Symbol.

$$\varphi = \frac{1+\sqrt{5}}{2} \qquad \overline{\varphi} = \frac{1-\sqrt{5}}{2}$$

When are the solution to the following equation:

$$x^2 = x + 1$$

Claim. For all $n \in \mathbb{R} \cup \{0\}$:

$$f(n) = \frac{1}{\sqrt{5}}\left(\varphi^{n+1} - \overline{\varphi}^{n+1}\right) = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right)$$

Proof. Using induction:

I.

$$f(0) = 1, \quad f(1) = 1 \tag{✓}$$

II.

$$\begin{aligned} f(n+1) = f(n) + f(n-1) &= \frac{1}{\sqrt{5}}(\varphi^{n+1} - \overline{\varphi}^{n+1} + \varphi^n - \overline{\varphi}^n) \\ &= \frac{1}{\sqrt{5}}(\varphi^n(\varphi+1) - \overline{\varphi}^n(\overline{\varphi}+1)) \\ &= \frac{1}{\sqrt{5}}(\varphi^n\varphi^2 - \overline{\varphi}^n\overline{\varphi}^2) = \frac{1}{\sqrt{5}}(\varphi^{n+2} - \overline{\varphi}^{n+2}) \end{aligned} \tag{✓}$$

■

Example 9.1.5. We have a ladder with n rungs. In every step we can go up one or two rungs. $J(n)$ is the number of ways to up a ladder with n rungs.

$$\begin{aligned} &J(1) = 1, \quad J(2) = 2, \quad J(3) = 3 \\ J(n) = &\underbrace{J(n-1)}_{\text{the last step is to go up one rung}} + \underbrace{J(n-2)}_{\text{the last step is to go up two rungs}} \end{aligned}$$

Which is a *Fibonacci sequence* with the initial values of $J(1) = 1, J(2) = 2$.

Example 9.1.6. $g(n)$ is defined as the number of subsets of the set $\{1, \ldots, n\}$ that do not contain two consecutive numbers.

Essentially, this is another *Fibonacci sequence* with the initial values $g(0) = 1, g(1) = 2$.

9.2 Catalan numbers

Definition (Catalan numbers)**.** We define $C(n)$ as the number of paths on the grid from $(0,0)$ to (n,n) that do not cross the line $y=x$.

$$C(n)=\frac{1}{n+1}\binom{2n}{n}$$

Let us build a recursive definition for $C(n)$.

First, we see that our first step must be a step to the right and our last step must be a step up (this is obvious because we have already proved that the function is *invertible*). ($C(0)=1$)

We define for all $1\leq i\leq n$ set A_i as the number of paths from $(0,0)$ to (n,n) such that the first time we touch the line $y=x$ is at the point (i,i). Based on this we see:

$$\bigcup_{i=1}^{n}|A_i|=C(n)$$

The size of A_i can be defined as the number of legal paths from $(0,0)$ until (i,i) *without* touching $y=x$, which is essentially shifting our line to $y=x-1$ ($C(i-1)$), times the number of legal paths from (i,i) to (n,n) ($C(n-i)$).

$$|A_i|=C(i-1)\cdot C(n-i)$$

In conslusion, we receive the following *recurrence sequence*:

$$C(n)=\sum_{i=1}^{n}C(i-1)\cdot C(n-i)$$

Example 9.2.1. Thirding a polygon is done by going over all the diagonals that don't cross over each other.

How many ways are there to "third" a given polygon?

We symbolize with a_n the number of ways we can divide a polygon with $n+2$ sides into three parts.

$$a_1=1 \qquad a_2=2$$

We define A to be all of the ways we can divide the polygon into thirds:

A_1 - Set of all the thirds that contain the triangle $\{1,n+1,n+2\}$

$|A_1|=a_{n-1}$

A_2 - Set of all the thirds that contain the triangle $\{2,n+1,n+2\}$

$|A_1|=a_1a_{n-2}$

For all $1 \leq k \leq n$, we define:

A_k - Set of all the thirds that contain the triangle $\{k, n+1, n+2\}$

$$A = \bigcup_{k=1}^{n} A_k \implies a_n = |A| = |A_1| + |A_2| + \cdots + |A_n|$$

We will now find the size of A_k: each thirding in A_k divides the polygon into three parts: the triangle $\underbrace{\{k, n+1, n+2\}}_{\text{number of thirds}-1}$, the polygon $\underbrace{\{1, 2, 4, \ldots, k, n+1\}}_{\text{number of thirds}-a_{k-1}}$ and the polygon $\underbrace{\{k, k+1, \ldots, n+1\}}_{\text{number of thirds}-a_{n-k}}$.

$$|A_k| = a_{k-1}a_{n-k}$$

Conclusion.

$$a_n = \sum_{k=1}^{n} |A_k| = \sum_{k=1}^{n} a_{k-1}a_{n-k}$$
$$a_1 = 1 \qquad a_0 = 1$$

We see that this is exactly like the Catalan numbers:

$$a_1 = c(1) \qquad a_0 = c(0)$$
$$a_n = c(n)$$
$$\boxed{a_n = \frac{1}{n+1}\binom{2n}{n}}$$

DISCRETE MATHEMATICS

10

ASYMPTOTIC GROWTH

Moshe Krumbein - Fall 2021

10.1 Big O Notation

Definition. The sequence (a_n) is almost always positive if there exists $N_0 \in \mathbb{N}$ such that $n > N_0$, $a_n > 0$

Definition. Given sequences $(a_n)(b_n)$, they are almost always positive itself:

$$a_n = O(b_n)$$

($(a_n) = O((b_n))$) if there exists $N \in \mathbb{N}$, $0 < c \in \mathbb{R}$ such that $n \leq N$: $a_n \leq cb_n$.

Example 10.1.1.

$$a_n = 7n + 5 \qquad b_n = n^2$$
$$\underbrace{7n + 5}_{a_n} \leq 7n + 5n = 12n \leq 12n^2$$

We define $N = 1$, $c = 12$. For all $n \geq 1$:

$$a_n \leq 12b_n$$

10.1.1 Characteristics

1. If there exists $N \in \mathbb{N}$ such that for all $n \geq N$: $a_n \leq b_n$, then $a_n = O(b_n)$
2. If $a_n = O(b_n)$ and $0 < k \in \mathbb{R}$, then $ka_n = O(b_n)$
3. If $a_n = O(b_n)$, $a'_n = O(b_n)$, then $a_n + a'_n = O(b_n)$
4. If $a_n = O(b_n)$, $b_n = O(d_n)$, then $a_n = O(d_n)$

10.2 Claims about Asymptotic Growth

Claim. Suppose $k, l \in \mathbb{R}, k < n$, then:

1. $(n^k) = O(n^l)$
2. $(n^l) \neq O(n^k)$

Proof. 1. For all $n \in \mathbb{N}, n^k \leq n^l$. ✓

2. Suppose $n \geq N$: $n^l \leq cn^k \implies n^{l-k} \leq c$. If we define $n > c^{\frac{1}{l-k}}$ then:

$$c \geq n^{l-k} \geq \left(c^{\frac{1}{l-k}}\right)^{l-k} = c$$

Which is a contradiction. ✓

■

Claim. For $n \in \mathbb{N}$ we define $b_n = \underbrace{n(n-1)\dots(n-k+1)}_{\frac{n!}{(n-k)!}}$:

I. $n^k = O(b_n)$

II. $b_n = O(n^k)$

Proof. I. We need to prove $n^k = O(b_n)$:

$$\begin{array}{l|l} \frac{n}{2} \leq n-k < n-k+1 & n^k = 2^k \left(\frac{n}{2}\right)^k \\ \Updownarrow & \frac{n}{2} \leq n-k+1 \\ n \leq 2n-2k & \frac{n}{2} \leq n-k \\ \Updownarrow & \vdots \\ \boxed{2k \leq n} & \frac{n}{2} \leq n \end{array}$$

Therefore:

$$n^k \left(\frac{n}{2}\right)^k \leq 2^k n(n-1)\dots(n-k+1) = 2^k b_n$$

We choose $c = 2^k, N = 2k$, and therefore:

$$n^k \leq cb_n$$

II. $b_n = \underbrace{n(n-1)\dots(n-k+1)}_{k \text{ terms}} \leq n^k$

$(c = 1, N = 1 \implies b_n = O(a_n))$

■

Conclusion. From the claim and the characteristics:

$$n^k = O\binom{n}{k} \qquad \binom{n}{k} = O(n^k)$$
$$b_n = O\binom{n}{k} \qquad \binom{n}{k} = O(b_n)$$

Claim. Given $k \in \mathbb{N}$:

I. $n^k = O(2^k)$

II. $2^k \neq O(n^k)$

Proof. I.

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} \implies \forall n \geq k : \binom{n}{k} \leq 2^n$$
$$\implies N = k, c = 1 : \binom{n}{k} = O(2^n), n^k = O\binom{n}{k}$$

Conclusion.

$$n^k = O(2^n) \qquad (\checkmark)$$

II. Proof by contradiction:

There exists $k_o \in \mathbb{N}$ such that: $2^n = O(n^{k_0})$.

We already know that $n^{k_0+1} = O(2^n)$. Using the property of transitivity: $n^{k_0+1} = O(n^{k_0})$, but since $k_0 + 1 > k_0$, this contradicts our first claim.

■

Note. We can generalize this for all $\alpha > 1$:

I. $n^k = O(\alpha^k)$

II. $2^k \neq O(\alpha^k)$

10.3 Big Θ Notation

Definition (Big Θ Notation)**.** Given sequences $(a_n)(b_n)$, that are almost always positive, we define:

$$a_n = \Theta(b_n)$$

If:

$$a_n = O(b_n) \quad b_n = O(a_n)$$

Example 10.3.1.

$$n^k = \Theta\binom{n}{k}$$

Claim. Θ is an equivalence relation of the collection of all of the sequences that are almost always positive.

Proof. I. Reflexivity:

$$\forall n \quad a_n \leq a_n \implies a_n = O(a_n)$$
$$a_n = \Theta(a_n) \qquad (\checkmark)$$

II. Symmetry:

If $a_n\Theta(b_n)$, then $a_n = O(b_n)$ and $b_n = O(a_n)$, which implies that: $b_n = \Theta(a_n)$.

$(\checkmark)$

III. Transitivity:

Given $a_n = \Theta(b_n)$ and $b_n = \Theta(c_n)$:

$$a_n = \Theta(b_n) \to \quad a_n = O(b_n), a_n = O(a_n)$$
$$b_n = \Theta(c_n) \to \quad b_n = O(c_n), c_n = O(b_n)$$

$$\implies a_n = \Theta(c_n) \qquad (\checkmark)$$

■

Definition (Polynomial Growth)**.** Given a sequence (a_n) which is almost always positive, we say that for (a_n) has a *polynomial growth rate* if there exists $k \in \mathbb{N}$ such that $a_n = \Theta(n^k)$.

In this case we say that (a_n) has polynomial growth of order k.

Example 10.3.2. (2^n) does not have a polynomial growth rate.

Claim. Given:

$$p(n) = n^k + \sum_{i=0}^{k-1} t_i n^i$$

Therefore $(p(n))$ has a polynomial growth rate of order k.

Proof. $p_n = O(n^k)$.

$$\begin{aligned} p(n) = n^k + \sum_{i=0}^{k-1} t_i n^i &\leq \left| n^k + \sum_{i}^{k-1} t_i n^i \right| \leq n^k + \sum_{i=0}^{k-1} |t_i| n^i \\ &\leq n^k + \sum_{i=0}^{k-1} |t_i| n^k = n^k \underbrace{\left(1 + \sum_{i=0}^{k-1} |t_i|\right)}_{c} \end{aligned}$$

$p(n) = O(n^k)$.

Now to prove $n^k = O(p(n))$:

$$\begin{aligned} p(n) &= n^k + t_{k-1} n^{k-1} + k_{k-2} n^{k-2} + \cdots + t_1 n + t_0 \\ &= n^k \underbrace{\left(1 + \frac{t_{k-1}}{n} + \frac{t_{k-2}}{n^2} + \cdots + \frac{t_0}{n^k}\right)}_{k+1 \text{ addends}} \end{aligned}$$

For a large enough n, $p(n) > \frac{1}{2}$, and therefore $p(n) > \frac{1}{2} n^k \implies n^k < 2p(n)$.

Therefore, $n^k = O(p(n)) \implies p(n) = \Theta(n^k)$. ■

10.4 Examples

Example 10.4.1. a_n is the number of ways to place 100 distinct balls to n cells.

$$a_n = n^{100}$$

a_n has polynomial growth rate of order 100.

Example 10.4.2. a_n is the number of ways to place 100 distinct balls to n cells such that in each cell there contains at most one ball.

For all $n \geq 100$, $a_n > 0$, and therefore (a_n) is almost always positive.

$$a_n = \frac{n!}{(n-100)!}$$

a_n has polynomial growth rate of order 100.

Example 10.4.3. a_n is the number of ways to place n distinct balls to 100 cells.

$$a_n = 100^n$$

a_n does not have an polynomial growth rate.

Example 10.4.4. a_n is the number of ways to place n distinct balls to 100 cells such that in each cell there contains at most one ball.

For all $n > 100$, $a_n = 0$, which makes it not a sequence which is almost always positive.

Example 10.4.5. a_n is the number of ways to place 100 identical balls to n cells such that in each cell there contains at most one ball.

For all $n \geq 100$, $a_n > 0$, and therefore (a_n) is almost always positive.

$$a_n = \binom{n}{100}$$

a_n has polynomial growth rate of order 100.

Example 10.4.6. a_n is the number of ways to place 100 identical balls to n cells.

$$a_n = \binom{n+99}{100}$$

a_n has polynomial growth rate of order 100.

Example 10.4.7. a_n is the number of ways to place n identical balls to 100 cells.

$$a_n = \binom{n+99}{99}$$

a_n has polynomial growth rate of order 99.

Example 10.4.8. Find the order of polynomial growth k of a_n where a_n is the number of ways to place 100 distinct balls to n cells such that:

a. In the first cell there are exactly 4 balls:

$$a_n = \binom{100}{4}(n-1)^{96}$$

$k = 96$.

b. In the first cell there is at most 4 balls:

$$a_n \leq \text{total number of ways to place } 100 \text{ balls in } n \text{ cells} = n^{100}$$
$$a_n = O(n^{100}) \tag{I}$$
$$a_n \geq \text{total number of ways to place } 100 \text{ balls in } n-1 \text{ cells} = (n-1)^{100}$$
$$n^{100} = O(a_n) \tag{II}$$
$$a_n = \Theta(n^{100}), k = 100$$

c. There exists a cell that has exactly 4 balls:

$a_n \geq$ number of ways such that one cell has 4 balls and all other have at least one

$$= \underbrace{\binom{n}{1}\binom{100}{4}(n-1)(n-2)\dots(n-96)}_{\text{polynomial of degree 97}} \implies n^{97} = O(a_n) \tag{I}$$

We define A_k to be the number of ways such that in the k-th cell there are exactly 4 balls:

$$A_k = \binom{100}{4}(n-1)^{96}$$

$$a_n = \left|\bigcup_{k=1}^{n} A_k\right| \leq \left|\sum_{k=1}^{n} A_k\right| = n\binom{100}{4}(n-1)^{96} \implies a_n = O(n^{97})$$

$$a_n = \Theta(n^{97}), k = 97$$

d. There exists a cell that has at least 4 balls

$$c \leq d \implies n^{97} = O(a_n)$$

A_k - all the ways such that in the k-th cell there are at least 4 balls:

$$|A_k| = \binom{100}{4}n^{96}$$

$$a_n = \left|\bigcup_{k=1}^{n} A_k\right| \leq \sum_{k=1}^{n} |A_k| = n\binom{100}{n}n^{96} \implies a_n = O(n^{97})$$

$$a_n = \Theta(n^{97}), k = 97$$

DISCRETE MATHEMATICS

11

GRAPH THEORY

Moshe Krumbein - Fall 2021

11.1 Introduction

Definition ((Undirected) Graph)**.** Is a order pair $G = (V, E)$ such that:

V - Set of vertices - finite and not empty.

E - Set of edges - collection of the unordered pairs of distinct elements of V.

Given $u, v \in V$, if $\{u, v\} \in E$ we can also write $(u, v) \in E$ (even though in general we reserve parentheses for ordered pairs).

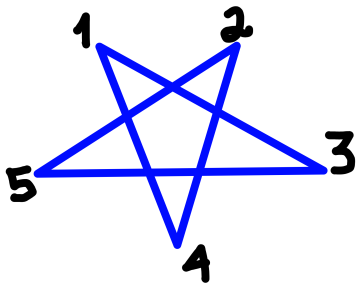

Figure 11.1: Example 11.1.1

Example 11.1.1.

$$V = \{1, 2, 3, 4, 5\}$$
$$E = \{(1, 3), (3, 5), (5, 2), (2, 4), (4, 1)\}$$

	1	2	3	4	5
1	0	0	1	1	0
2	0	0	0	1	1
3	1	0	0	0	1
4	1	1	0	0	0
5	0	1	1	0	0

Table 11.1: Example 11.1.1

11.2 Special Graphs

Definition (Empty/Null Graph (N_n))**.**

$$|V| = n \quad E = \emptyset$$

Definition (Complete Graph (K_n))**.**

$$|V| = n \quad E = \{(i, j) \mid 1 \leq i < j \leq n\}$$
$$|E| = \binom{n}{2}$$

How may different graphs are there with n vertices?

Every subset of the complete graph produces a different graph:

$$2^{\binom{n}{2}}$$

Definition (Circle Graph (C_n))**.**

$$|V| = n \quad E = \{(1, 2), (2, 3), \ldots, (n-1, n), (n, 1)\}$$
$$|E| = n$$

Definition (Neighbors)**.** Given $u, v \in V$, u and v are *neighbors* if $(u, v) \in E$.

Definition (Degree of a Vertex)**.** The *degree* of a vertex $u \in V$ is the number of *neighbors* of u.

$$\deg(u) = |\{v \in V \mid (u, v) \in E\}|$$

Claim. The sum of the degrees of all the vertices in a graph is equal to $2|E|$. In other words:

$$\sum_{v \in V} \deg(v) = 2|E|$$

Proof. We will symbolize for all $v \in V$, $e \in E$:

$$T(e,v) = \begin{cases} 1 & v \in e \\ 0 & v \notin e \end{cases}$$

$$\sum^{v \in V} \deg(v) = \sum_{v \in V} \sum_{e \in E} T(e,v) = \sum_{e \in E} \underbrace{\sum_{v \in V} T(e,v)}_{2} = \sum_{e \in E} 2 = 2|E|$$

■

Conclusion. The number of vertices that have have an odd degrees is even.

Definition (Path)**.** A *path* in graph $G = (V, E)$ is a sequence of vertices $(v_0, v_1, \ldots, v_n)$ such that for all $0 \leq i \leq n-1$: $(v_i, v_{i+1}) \in E$, which has a length of n.

Definition (Connectivity)**.** Graph $G = (V, E)$ is *connected* if for all $u, v \in V$ there exists a *path* $(v_0, v_1, \ldots, v_n)$ such that $v_0 = u$ and $v_n = v$.

Definition (Components)**.** We define relation R on V:

$(u, v) \in R \iff$ there exists a path $(v_0, \ldots, v_n)$ in the graph such that $v_0 = u$ and $v_n = v$.

Note. For all $v \in V$: (v) is a path.

Claim. This relation is an equivalence relation of V.

These equivalence classes are called *connected components* of G.

Claim. If G is *connected*, then the relation on V is the full/complete relation (in other words, for all $u, v \in V, (u, v) \in R$), and therefore we get one *connected component.*

For the empty graph N_n, we get n *components.*

Claim. The number of components in a graph $G = (V, E)$ is greater or equal to $|V| - |E|$.

Proof. Induction of the number of edges.

I. $|E| = 0$: Number of components $= n = |V| - |E|$

II. We assume induction for $|E| = k$ and we'll prove for $|E| = k + 1$: Our graph is $G = (E, v)$, $|V| = n$ and $|E| = k + 1$. We'll pick $e \in E$ and we'll define $G_0 = (V, E \setminus \{e\})$, which is a graph with n vertices and k edges.

   From the initial assumption, the number of components in $G_0 \geq n - k$.

   Suppose $e = (u, v)$. If in G_0, u and v belong to the same component, then the number of components in $G =$ the number of components in $G_0 \geq n - k > n - k - 1$.

   If u and v are not in the same component in G_0, then the number of components in $G =$ number of components in $G_0 - 1 \geq n - k - 1 = n - (k + 1)$.

■

Definition (Simple Path)**.** A path $(v_0, \ldots, v_n)$ is called a *simple path* if all the vertices $v_0, \ldots, v_n$ are different from each other.

Definition (Simple Circuit)**.** A path $(v_0, \ldots, v_n)$ is called a *simple circuit* if $v_1, \ldots, v_n$ are all different and $v_1 = v_n$ (where $n \geq 3$).

11.3 Trees

Definition (Tree)**.** A connected graph without any *simple circuits* is called a *tree*.

v is a *leaf* (external vertex) if $\deg(v) = 1$.

Lemma. Any *tree* that has more than one *vertex* has at least one *leaf*.

Proof. Given a tree $G = (V, E)$ and $v_0 \in V$. $\deg(v_0) \neq 0$, because that would with violate the requirement that trees are *connected* or the condition of having more than one vertex of the initial claim.

If $\deg(v_0) = 1$, we found a *leaf*.

If $\deg(v_0) > 1$ than it has part of a path that has an end vertex v_n such that $\deg(v_n) = 1$ (because there are no circuits in trees). ■

Claim. If $G = (V, E)$ is a tree, then $|V| - |E| = 1$.

Proof. Proof by induction on the number of vertices in the graph:

I. $|V| = 0$, and therefore $E = \emptyset$, and therefore $|V| - |E| = 1 - 0 = 1$.

II. We assume $|V| = n$ works, and we proof $|V| = n + 1$ also works:

As per the aforementioned lemma, there exists a leaf $v \in V$.

Let there be $e \in E$ such that $v \in e$. We then define $G' = (V \setminus \{v\}, E \setminus \{e\})$. We see that G' is a tree because it doesn't contain any *simple circuits* and is *connected*, because we removed only a *leaf* and its edge.

In addition, G' has $n = |V| - 1$ vertices and $|E| - 1$ edges. Therefore, G' fulfills our induction hypothesis and therefore:

$$|V| - |E| = (|V| - 1) - (|E| - 1) = |V \setminus \{v\}| - |E \setminus \{e\}| = 1$$

■

Claim. Given graph $G = (V, E)$ without *simple circuits* such that $|V| - |E| = 1$, then G is *connected*.

Proof. $V_1, V_2, \dots V_l$ are *connected components* of G.

For all $1 \leq i \leq l$:

$$E_i = \{\{u, w\} \in E \mid u, w \in V_i\}$$

Because *components* are *equivalence classes*, we know that $E_i \cap E_j = \emptyset$ and $E_1 \cap E_2 \cap \dots \cap E_l = E$. From here we see that $|E_1| + |E_2| + \dots + |E_l| = |E|$.

In addition, for all $1 \leq i \leq l$, the graph $G_i = (V_i, E_i)$ is a tree because it is *connected* and doesn't have any *simple circuits*. Therefore, as per the previous claim, $|V_i| - |E_i| = 1$.

$$1 = |V| - |E| = (|V_1| + \dots + |V_l|) - (|E_1| + \dots + |E_l|) = (|V_1| - |E_1|) + \dots + (|V_l| - |E_l|)$$
$$= \underbrace{1 + 1 + \dots + 1}_{l \text{ times}} = l \implies l = 1$$

Therefore, G has only one *connected component*, meaning G is *connected*. ■

Claim. If $G = (V, E)$ is a *connected* graph and $(v_0, \dots, v_n)$ is a simple circuit in G, then $G' = (V, E \setminus \{(v_0, v_1)\})$ is also *connected*.

Proof. Given $u, w \in V$. Given that G is *connnected*, there is a *path* $(u = w_0, w_1, \dots, w_k = w)$.

If for all $1 \leq i \leq k$: $(w_{i-1}, w_i) \neq (v_0, v_1)$, then this path is in G' and therefore u, w are connected in G'.

If there does exist $1 \leq i \leq k$: $(w_{i-1}, w_1) = (v_0, v_1)$, then either $w_{i-1} = v_0, w_i = v_1$ or $w_{i-1} = v_1, w_i = v_0$.

In the first case:

$$(u = w_0, w_1, \dots, w_{i-1} = v_n, v_{n-1}, \dots, v_2, v_1 = w_i, w_{i+1}, \dots, w_k = w)$$

Is a path in G' that connects u and w.

In the second case:

$$(u = w_0, w_1, \dots, w_{i-1} = v_1, v_2, \dots, v_{n-1}, v_n = v_0 = w_i, w_{i+1}, \dots, w_k = w)$$

Is a path in G' that connects u and w.

In all cases u and w are connected in G', which means G' is *connected*. ■

Claim. If $G = (V, E)$ is a *connected graph* such that $|V| - |E| = 1$, then G does not have any *simple circuits*.

Reminder. The number of *components* in any graph $G = (V, E)$ is greater than or equal to $|V| - |E|$.

Proof. We will prove by contradiction that G contains a *simple circuit* $(v_0, v_1, \ldots, v_n)$.

Per our previous claim, the graph $G = (V, E \setminus \{(v_0, v_1)\})$ is also connected, and $|E \setminus \{(v_0, v_1)\}| = |E| - 1$. Per the reminder about the relationship between the number of components in a graph and the number of vertices and edges it has, the number of components in G' is at least:

$$|V| - |E \setminus \{(v_0, v_1)\}| = |V| - (|E| - 1) = (|V| - |E|) + 1 = 1 + 1 = 2$$

which means that G' is not *connected*, which is a contradiction. ■

Theorem (Trees)**.** Let $G = (V, E)$ be a graph.

Any two of these conditions implies the third one to also be true:

1. G is *connected*
2. G does not contain any *simple circuits*
3. $|V| - |E| = 1$

11.4 Bigraphs

Definition (Two-sided (Bipartite) Graph)**.** Graph $G = (V, E)$ is a *bigraph* if we can express V as a *disjoint union* $V_1 \cup V_2$ such that for all $e \in E$ joins a vertex from V_1 with a vertex from V_2. In such a can we symbolize $G = (V_1, V_2, E)$.

Note. There may be more than one way to define V_1 and V_2.

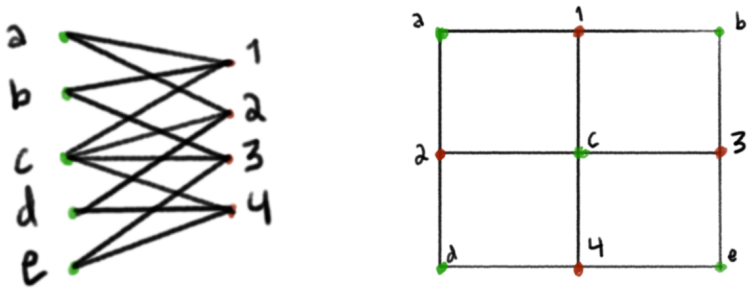

Figure 11.2: Example 11.4.1 of a two ways to express a *bigraph*

Example 11.4.1.

Definition (Cubic Graph (Q_3))**.**

$$V = \{0, 1\}^3 \quad |V| = 8$$
$$E = \{(a_1, b_1, c_1), (a_2, b_2, c_2) \mid |a_1 - a_2| + |b_1 - b_2| + |c_1 - c_2| = 1\}$$

How we define the two parts of the bigraph:

$$V_1 = \{(a,b,c) \mid a+b+c \text{ is even}\}$$
$$V_2 = \{(a,b,c) \mid a+b+c \text{ is odd}\}$$

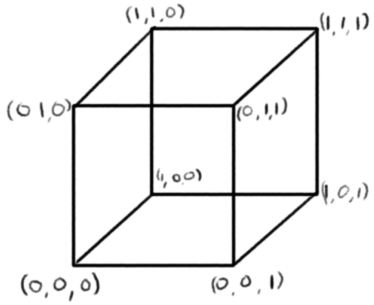

Figure 11.3: Example of a cubic graph

Definition (Complete Bigraph ($K_{n,m}$))**.**

$$|V_1| = m, |V_2| = n \quad V_1 \cap V_2 = \emptyset$$
$$E = \{\{v,u\} \mid v \in V_1, u \in V_2\}$$
$$|V| = m+n \quad |E| = mn$$

Claim. In a *bigraph* the number of vertices in a *simple circuit* is always even.

Definition (Regular Graph)**.** A graph $G = (V,E)$ is *d-regular* if from all $v \in V$, $\deg(v) = d$.

For example, Q_3 is 3-regular.

Claim. For a *regular* bigraph, $|V_1| = |V_2|$.

Proof.

$$|E| = d \cdot |V_1| = d \cdot |V_2| \implies |V_1| = |V_2|$$

■

11.5 Special Circuits

11.5.1 Hamiltonian Circuits

Definition (Hamiltonian Circuit)**.** A *simple circuit* is called a *Hamiltonian circuit* if it passes through each vertex of a graph exactly once.

In other words, $(v_0, v_1, \ldots, v_n = v_0)$ is a *Hamiltonian circuit* if for all $v \in V$ there exists $1 \leq i \leq n$ such that $v_i = v$.

Claim. If $G = (V_1 \cup V_2, E)$ is a *bigraph* and G contains a *Hamiltonian circuit*, then $|V_1| = |V_2|$.

Proof. We suppose $(v_0, v_1, \ldots, v_n = v_0)$ is a *Hamiltonian circuit* where:

$$v_0 \in V_1 \to v_1 \in V_2 \to v_2 \in V_1 \to v_3 \in V_2 \to \ldots$$

From this we see that n is even and that $|V_1| = |V_2|$. ■

Claim. For all $n \geq 2$, the graph Q_n contains a *Hamiltonian circuit.*

Definition (Hypercube Graph (Q_n))**.**

$$V = \{0,1\}^n \quad |V| = 2^n$$
$$E = \left\{ (a_1, \ldots, a_n), (b_1, \ldots, b_n) \;\middle|\; \sum_{i=1}^{n} |a_i - b_i| = 1 \right\}$$

Proof. We will use proof by induction:

I. $n = 2$ ✓

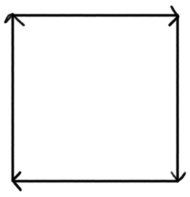

Figure 11.4: *Hamiltonian* graph of Q_2

II. We assume correctness on Q_{n-1} and will prove for Q_n:

$$A = \{(a_1, a_2, \ldots, a_{n-1}, 0) \mid \forall i \in [n-1], a_i \in \{0,1\}\}$$
$$B = \{(a_1, a_2, \ldots, a_{n-1}, 1) \mid \forall i \in [n-1], a_i \in \{0,1\}\}$$
$$V = A \cup B$$

Based on our assumption, A contains the following *Hamiltonian circuit*:

$$(v_0, v_1, \ldots, v_{2^{n-1}} = v_0) \quad v_0 = (0, 0, \ldots, 0)$$

And B contains the following *Hamiltonian circuit*:

$$(u_0, u_1, \ldots, u_{2^{n-1}} = u_0) \quad u_0 = (0, 0, \ldots, 1)$$

Note. We can go from v_i to u_i by changing the last number from 0 to 1.

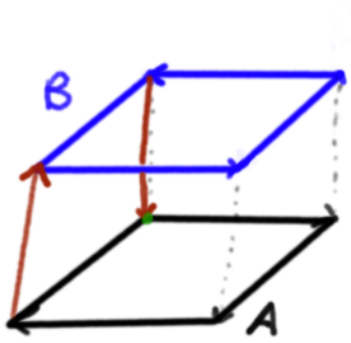

Figure 11.5: *Hamiltonian* graph of Q_3

Therefore, we can create the following *Hamiltonian circuit*:

$$(v_0, v_1, \ldots, v_{2^{n-1}-2}, v_{2^{n-1}-1}, u_{2^{n-1}-1}, u_{2^{n-1}-2}, \ldots, u_2, u_1, u_0, v_0)$$

Which is a *Hamiltonian circuit* in Q_n.

■

11.5.2 Eulerian Circuits

Definition (Eulerian Circuit)**.** Given connected graph G, a *circuit* (not necessarily *simple*) $(v_0, v_1, \ldots, v_n = v_0)$ is called an *Eulerian circuit* if for all $e \in E$ there exists a single $1 \leq i \leq n$ such that $e = \{v_i, v_{i+1}\}$.

In other words, an *Eulerian circuit* is circuit that visits each edge exactly once.

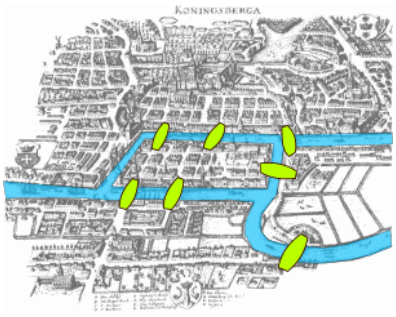

Figure 11.6: Map of Königsberg in Euler's time

Example 11.5.1 (Seven Bridges of Königsberg). The problem was to devise a *circuit* such that one could cross every bridge exactly once. Euler proved this to be impossible.

Theorem. Given a connected graph $G = (V, E)$, there exists an *Eulerian circuit* if and only if for all $v \in V$, $\deg(v)$ is even.

Proof. Being that we have to prove that this is $\iff$, we must prove both directions:

$\Leftarrow$ Given an *Eulerian circuit*, each visit to a vertex adds 2 to its degree. (This is also true for the vertex that we started from because we initially leave from it and must return to it in the end)

$\Rightarrow$ We will prove by induction on the number of edges $|E| = m$.

I. $m = 0$ ✓

II. We assume the statement holds for less than m edges:

G is connected, and for all $v \in V$, $\deg(v)$ is even. Therefore, G does not have any *leaves*, and is therefore not a *tree*. And since G is connected but isn't a *tree*, we know that it then must contain a *simple circuit* $(v_0, v_1, \ldots, v_n = v_0)$.

We define $G' = (V, E')$ as G without all the edges in its *simple circuit*. In other words:

$$E' = E \setminus \{\{v_i, v_{i+1}\} \mid 0 \leq i \leq n-1\}$$

In G', the degree of each vertex is even. However G' is not necessarily connected. We will define G''s *components* as $V_1, V_2, \ldots, V_l$, where for all $1 \leq i \leq l$: $G_i = (V_i, E_i)$.

For all G_i the number of edges is less than m. Therefore based on our induction hypothesis, G_i contains a *Eulerian circuit*.

We see that for all i: $V_i \cap \{v_0, v_1, \ldots, v_{n-1}\} \neq \emptyset$. In other words, for each *component* V_i, there is a representative from the original circuit.

Given $u \in V_i$, knowing that G is connected, there exists a *path* in G between v_0 and u.

$$(w_0 = v_0, w_1, w_2, \ldots, w_n = u)$$

$$j = \max\{i \mid w_i \in \{v_0, v_1, \ldots, v_{n-1}\}\}$$

We get that all the vertices $w_j, \ldots, w_k$ are all in V_i, and therefore w_j is part of the circuit and it is the representative of the circuit in *component* V_i. We see that we can chose a set of representatives from all of the *components* that are all in the set $\{v_0, \ldots, v_{n-1}\}$.

We will now build an *Eulerian circuit* for the graph G:

$$\forall\ 1 \leq i \leq l : f(i) = \min\{i \mid v_i \in V_i\}$$

We will begin with v_0. If there exists an i such that $v_0 = f(i)$, then we will cover *component* V_i by an *Eulerian circuit* that we got from our induction hypothesis. We now continue to v_1. If there exists an i such that $v_1 = f(i)$ we will cover V_i until we come back to v_1. Then we can continue to v_2 and so on until $v_n = v_0$.

■

11.6 Ramsey Theory

Coloring of graph $G = (V, E)$ with k colors $\{c_1, c_2, \ldots, c_k\}$ is essentially a function:

$$C : E \to \{c_1, c_2, \ldots, c_k\}$$

We will specifically we working with coloring graphs with two different colors, namely red and blue.

Claim. In coloring K_6 (the complete graph with six vertices), with two colors red and blue, we will be able to find a red K_3 or a blue K_3 (or both).

Proof. Suppose $v_0 \in V$. Given that our graph is complete, $\deg(v_0) = 5$. By the *pigeonhole principle*, there are at least three red edges or three blue edges emanating from v_0.

If v_0 emits three red edges we will label the vertices they connect to u_1, u_2, u_3. If there is $1 \leq i < j \leq 3$ such that (u_i, u_j) is red then v_0, u_i, u_j forms a red K_3. If there aren't any, then we know that u_1, u_2, u_3 forms a blue K_3.

Likewise, if v_0 emits three blue edges, the same can be said in reverse. ■

Definition (Ramsey's Theorem)**.** Given $s, t \in \mathbb{N}$, $R(s, t)$ is the smallest n such that when coloring K_n in red or blue, at least one of the following cases is true:

a. There is $S \subset V$, $|S| = s$ such that all edges between the vertices in S are red.
b. There is $T \subset V$, $|T| = t$ such that all edges between the vertices in T are blue.

In other words there is guaranteed to be a red K_s or a blue K_t (or both).

From our previous claim, $R(3, 3) \leq 6$. How can we prove that $R(3, 3) = 6$?

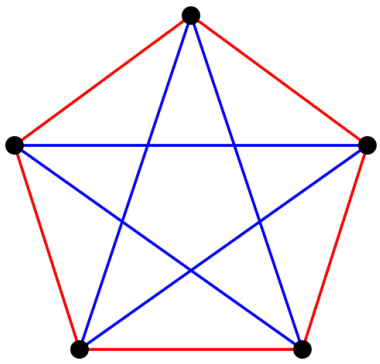

Figure 11.7: A coloring of K_5 with no monochromatic K_3

Since $R(3, 3) \neq 5$, $R(3, 3) = 6$.

For all s, t:

- $R(1,t) = 1$
- $R(s,1) = 1$
- $R(2,t) = t$
- $R(s,2) = s$
- $R(4,4) = 18$
- $R(5,5) =$ still unknown!

Lemma. For all $m, n \in \mathbb{N}$:

$$R(n,m) \leq \underbrace{R(n-1,m)}_{a} + \underbrace{R(n,m-1)}_{b}$$

Proof. For all colorings of K_{a+b} in red or blue we are guaranteed that there will be either a red K_n or a blue K_m.

Suppose $v \in V$. v emits $a+b-1$ edges. We are guaranteed one of the following cases:

a. From v emanates a red edges.
b. From v emanates b blue edges.

Suppose that case "a" is true:

We look at the a neighbors that are connected to v by red edges. We are guaranteed that between then there exists either a red K_{n-1} or a blue K_m. If there's a blue K_m, we're done. Otherwise there's a red K_{n-1} and we'll join v to them to create a red K_n.

If case "b" is true:

We look at the a neighbors that are connected to v by blue edges. We are guaranteed that between then there exists either a red K_n or a blue K_{m-1}. If there's a red K_n, we're done. Otherwise there's a blue K_{m-1} and we'll join v to them to create a blue K_m. ■

Example 11.6.1.

$$R(3,4) \leq 10$$

From our lemma:

$$R(3,4) \leq R(2,4) + R(3,3) = 4 + 6 = 10$$

How hard can it be to find $R(5,5)$? We know that the lower bound of $R(5,5)$ is 43, which is to say the number of edges in $K_{43} = \binom{43}{2} = 903$ and the number of different ways to color the edges is 2^{903} (!!!).

Theorem. For $m, n \geq 2$:

$$R(n,m) \leq \binom{n+m-2}{m-1}$$

Proof. We will prove by induction on $l = m + n$:

I. $l = 4 \implies m = n = 2$:

$$R(2,2) \leq \binom{2+2-2}{2-1} = \binom{2}{1} = 2 \qquad (\checkmark)$$

II. We assume $l - 1 \geq 4$, and we'll prove for l:

From our previous claim $R(m,n) \leq R(m-1,n) + R(m,n-1)$. $m + n - 1 = l - 1$, and therefore, from the induction hypothesis:

$$R(m-1,n) \leq \binom{n+m-3}{m-1} \qquad R(m,n-1) \leq \binom{n+m-3}{m-2}$$

Reminder (Pascal's Rule).

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

Therefore, we see that:

$$\begin{aligned} R(m,n) &\leq R(m-1,n) + R(m,n-1) \\ &\leq \binom{n+m-3}{m-1} + \binom{n+m-3}{m-1} = \binom{n+m-2}{m-1} \end{aligned} \qquad (\checkmark)$$

■

11.7 The Matching Problem

Let $G = (V_1 \cup V_2, E)$ be a *bipartite* graph.

Definition (Perfect Matching)**.** *Perfect matching* is a function $f : V_1 \to V_2$ *one-to-one* and *onto* such that for all $v \in V_1 : (v, f(v)) \in E$.

We are looking for conditions to guarantee *perfect matching* on G.

Initial condition: $|V_1| = |V_2|$.

Definition (Neighbors)**.** Given $S \subset V$:

$$\Gamma(S) = \{u \in V \mid \exists v \in S \text{ s.t. } (v,u) \in E\}$$

Required condition: for all v: $\deg(v) \geq 1$. In other words: $|\Gamma(\{v\})| \geq 1$. This is still not enough to guarantee *perfect matching*.

For all $S \subset V$ we expect that $|\Gamma(S)| \geq |S|$. In other words, every set S will collectively connected to at least $|S|$ vertices.

Theorem (Hall's Marriage Theorem)**.** Given $G = (V_1 \cup V_2, E)$ is a *bigraph* such that $|V_1| = |V_2|$, then there exists *perfect matching* in G if and only if for all $S \subset V_1$: $|\Gamma(S)| \geq |S|$.

Proof. Being that we have to prove that this is $\iff$, we must prove both directions:

- $\Rightarrow$ Assuming $f : V_1 \to V_2$ as required, for all $S \subset V_1$: $f(S) \subseteq \Gamma(S)$. f is *one-to-one* and *onto*, and therefore $|f(S) = |S| \implies |\Gamma(S)| \geq |S|$.
- $\Leftarrow$ Assuming that for all $S \subset V_1$: $|\Gamma(S)| \geq |S|$.

  We will prove the following using induction on $|V_1|$:

  I. $|V_1| = 1$

  II. Assuming correctness for $k < n$ and we will prove for n:

  a. Assuming for all $S \subsetneq V_1 \neq \emptyset$: $|\Gamma(S)| > |S|$.

  Choosing $u \in V_1$, u is connected to at least two vertices in V_2, and we will *match* it to w.

  We now consider the remaining graph: $G' = (V_1 \setminus \{u\} \cup V_2 \setminus \{w\}, E')$. G' is still a *bigraph* and $|V_1 \setminus \{u\}| = |V_2 \setminus \{w\}| = n - 1$.

  For all $S \subset V_1 \setminus \{u\}$: $|\Gamma(S)| > |S|$ and $|\Gamma'(S)| \geq |\Gamma(S)| - 1$, and therefore $|\Gamma'(S)| \geq |S|$.

  Based on the induction hypothesis, there exists *perfect matching* between $V_1 \setminus \{u\}$ and $V_2 \setminus \{w\}$, together with the pair (u, w), we get *perfect matching* on G.

  b. Suppose there exists $K \subsetneq V_1 \neq 0$ such that $|\Gamma(K)| = |K| = k < n$.

  We define $L = \Gamma(k)$, where $|L| = k$. We consider the *bi graph* $G'' = (K \cup L, E'')$. $|K| = |L| = k < n$. We notice that for all $u \in K$ if $(u, v) \in E$, then $(u, v) \in E''$, and therefore *Hall's condition* is maintained in G''. From our induction hypothesis, there exists *perfect matching* between K and L.

  We will now show that there is *perfect matching* between $V_1 \setminus K$ and $V_2 \setminus L$:

  $$|V_1 \setminus K| = |V_2 \setminus L| = n - k < n$$

  We define $G''' = G \setminus G''$, and we will that in G''' *Hall's condition* also applies. Let $S \subseteq V_1 \setminus K$, where $|S| = s$. We consider at $K \cup S$ and notice it is a *disjoint union* where $|K \cup S| = k + s$. $K + S$ is connected to at least $k + s$ vertices in V_2, and exactly k among them are part of L. Therefore, without them, S is connected to $V_2 \setminus L$ to least s vertices. From our induction hypothesis on G'' where there exists *perfect matching* between $V_1 \setminus K$ and $V_2 \setminus L$, all in all we have *perfect matching* on our entire original graph G.

■

Example 11.7.1. Consider the set $A = \{1, 2, 3, \ldots, n\}$. Given n subsets $A_1, A_2, \ldots, A_n \subseteq A$, and union of any k sets $A_1, \ldots, A_n$ contain at least k elements of A. Show that there exists $f : A \to \{A_1, \ldots, A_n\}$ such that for all $i \in A$, $i \in f(i)$.

We will define a graph $G = (V_1 \cup V_2, E)$ in the following way:

$$V_1 = \{A_1, \ldots, A_n\} \quad V_2 = A = \{1, \ldots, n\}$$
$$|V_1| = |V_2| = n$$
$$E = \{(A_j, i) \mid i \in A_j\}$$

For all $K \subseteq \{A_1, \ldots, A_n\}$:

$$\left|\bigcup_{i \in K} A_i\right| \geq |K| \implies |\Gamma(K)| \geq |K|$$

And therefore *Hall's condition* holds and therefore there is *perfect matching* in the graph. In other words there exists $f : \{A_1, \ldots, A_n\} \to \{1, \ldots, n\}$ *one-to-one* and *onto* such that for all $j \in [n]$: $f(j) \in A_j$.

Example 11.7.2. We distribute cards from a legal deck (52 cards) randomly into 13 piles of 4 cards each. Is it possible to pick a representative from each pile such that each representative will be a different value card $\{1, \ldots, 13\}$?

We define:

$$V_1 = \{1, \ldots, 13\} \quad V_2 = \{q_1, \ldots, q_{13}\}$$
$$E = \{\{i, q_j\} \mid \text{the number } i \text{ is in the pile } q_j\}$$

We notice that for all k numbers in V_1 there are $4k$ cards that show them, and therefore they are distributed among at lest k piles. *Hall's condition* holds and therefore there is *perfect matching*.

Reminder. G is a *d-regular* graph if for all $v \in V$, $\deg(v) = d$.

G is a *regular* graph if there exists d such that G is *d-regular*.

Claim. On a *d-regular bigraph*, there exists *complete matching*.

Reminder. On a *regular bigraph*, $|V_1| = |V_2|$.

Proof. Let $G = (V_1 \cup V_2, E)$ be a *regular bigraph*. We can derive that $|V_1| = |V_2|$ and we will prove that *Hall's condition* holds.

Let $S \subseteq V_1$, $|S| = s$. All ds edges exit from S are all in $\Gamma(S)$, and from $\Gamma(S)$ exit a total of $d|\Gamma(S)|$ edges. Therefore we get:

$$d|\Gamma(S)| \geq ds \implies |\Gamma(S)| \geq s = |S|$$

Hall's condition holds and therefore there exists *complete matching*. ■

11.7.1 Latin Rectangle

Definition (Latin Rectangle)**.** A *Latin rectangle* is a matrix $k \times n$ such that in every row and column there appears $\{1, \ldots, n\}$ distinctly. ($k \leq n$)

Claim. Given a *Latin rectangle* $k \times n$, we can expand it to a *Latin rectangle* $(k+1) \times n$.

Proof. We consider a *bigraph* such that its vertices are the columns $c_1, \ldots c_n$ and the set of edges being:

$$E = \{\{i, c_j\} \mid \text{ the number } i \text{ is not in } c_j\}$$

where the numbers are $\{1, \ldots, n\}$.

All $1 \leq i \leq n$, i appears in all k rows and doesn't appear in the column more than once. Therefore i appear exactly in k columns $\implies \deg(i) = n - k$.

In each column c_j there are k distinct numbers $\implies \deg(c_j) = n - k$.

Hall's condition holds and therefore there is *perfect matching*, which exactly constitutes row $k+1$. ■

DISCRETE MATHEMATICS

12

CARDINALITY

Moshe Krumbein - Fall 2021

12.1 Introduction

Reminder. For *finite* sets, A, B:

$$|A| = |B| \iff \exists f : A \to B \text{ that is } \textit{bijective}$$

Definition (Equinumerosity)**.** A, B have the same *cardinality* (*equinumerous*) if there exists an $f : A \to B$ that is *bijective*. We symbolize this as $A \sim B$.

12.2 Characteristics

1. For all A: $A \sim A$

   $$\mathrm{Id}_A : A \to A \text{ is } \textit{bijective}$$

2. For all A, B: if $A \sim B \to B \sim A$.

   $$f : A \to B \quad f^{-1} : B \to A$$

   Claim. Given sets A, B, C, $f : A \to B, g : B \to C$:

   - If f, g are *injective*, then $g \circ f : A \to C$ is *injective*
   - If f, g are *surjective*, then $g \circ f : A \to C$ is *surjective*

3. Given sets A, B, C:

   $$A \sim B, B \sim C \implies A \sim C$$

12.3 Countable Sets

Definition (Countable Sets)**.** A set A is called *countable* if $\mathbb{N} \sim A$. In other words, there exists a function $f : \mathbb{N} \to A$ that is *bijective*. In this case we symbolize $|A| = \aleph_0$.

Note. A is *countable* if there is a *sequence* which contains all the elements of A exactly once.

12.3.1 Hilbert's Hotel

There are a countably infinite number of rooms such that each room is labeled with a natural number.

Suppose all the rooms in Hilbert's hotel are full.

A new guest arrives and wants a room. To accommodate for him, we can move each occupant to the room immediately to his right and put our new guest in first room which is unoccupied.

Suppose a bus arrives containing an countably infinite number of guests. To accommodate for them, we can move each occupant to his room number times two, and place all the new guests in the now unoccupied odd-numbered rooms.

Suppose $\aleph_0$ buses arrive with $\aleph_0$ guests each. To accommodate for all the new guests we can move each occupant in room i to the room 2^i. For the first bus, we can send the i-th person the 3^i-th room. For each subsequent bus j we send guest i to room number j-th prime number to the i-th power.

Finally, a single bus arrives with all the numbers between 0 and 1. Unfortunately, given that there are an uncountably infinite number of new guests, we will not able about to make enough room for them.

12.3.2 Examples

Let us explore using more mathematical notion:

Example 12.3.1.

$$A = \mathbb{N} \cup \{0\}$$
$$f : \mathbb{N} \to A, \forall n \in \mathbb{N} : f(n) = n - 1$$
$$A \sim \mathbb{N} \implies |A| = \aleph_0$$

Example 12.3.2.

$$A = \mathbb{N} \times \{0\} \quad f : \mathbb{N} \to A$$
$$f(n) = \begin{cases} (\frac{n}{2}, 1) & n \text{ is even} \\ (\frac{n+1}{2}, 0) & n \text{ is odd} \end{cases}$$

Example 12.3.3.

$$A = \mathbb{Z} \quad f : \mathbb{N} \to \mathbb{Z}$$
$$f(n) = \begin{cases} \frac{n}{2} & n \text{ is even} \\ -\frac{n-1}{2} & n \text{ is odd} \end{cases}$$

Claim. If A is *countably infinite* and $B \subseteq A$, then B is either *finite* or *countably infinite*.

Proof. Since we know that A is *countably infinite*, there exists $f : \mathbb{N} \to A$ that is *bijective*. If B is not *finite*, we will prove that B is *countably infinite*.

We define $g : \mathbb{N} \to B$:

$$g(n) = f(\min\{m \in \mathbb{N} \mid f(m) \in B, \forall i \in [n-1] : g(i) \neq f(m)\})$$

In other words we can write A as $f(1), f(2), f(3), \ldots$ and B as $f(2), f(4), f(5), \ldots$, and therefore:

$$g(1) = f(2)$$
$$g(2) = f(4)$$
$$g(3) = f(5)$$
$$\vdots$$
$$g \text{ is } \textit{bijective} \implies \mathbb{N} \sim B \implies |B| = \aleph_0$$

Note. We can only define $g(n)$ after we define $g(1), g(2), \ldots, g(n-1)$.

■

Claim. If A is *countably infinite* and B is *finite*, then $A \cup B$ is *countably infinite*.

Note. In *Hilbert's hotel* if k new guests arrive we can move all currents guests k rooms to the right, thus freeing up rooms 1 through k.

Proof. We will split into two cases:

1. Suppose $A \cap B = \emptyset$, and $|B| = k$.

   There exists $f : \mathbb{N} \to A, g : [k] \to B$ that are both *bijective*.

   We define $h : \mathbb{N} \to A \cup B$:

   $$h(n) = \begin{cases} g(n) & n \in [k] \\ f(n-k) & n > k \end{cases}$$

   h is *surjective* and *injective* (because $A \cup B = \emptyset$).

2. In general:

$$A \cup B = (A \setminus B) \cup B$$

B is *finite* and $A \setminus B \subseteq A$.

$A \setminus B$ is not *finite* because otherwise $A = (A \setminus B) \cup (A \cap B)$ would be a *union* of *finite* sets which is *finite*, by contradiction (since we know A is *countably infinite*).

Therefore, $A \setminus B$ is *countably infinite* and we can finish with case 1.

■

Claim. If A, B are *countably infinite*, then $A \cup B$ is *countably infinite*.

Proof. Here too we will consider two different cases:

1. $A \cap B = \emptyset$:

There exists $f : \mathbb{N} \to A, g : \mathbb{N} \to B$ which are *bijective*. We can define $h : \mathbb{N} \to A \cup B$:

$$h(n) = \begin{cases} g(\frac{n}{2}) & n \text{ is even} \\ f(\frac{n+1}{2}) & n \text{ is odd} \end{cases} \implies A \cup B \sim \mathbb{N} \implies |A \cup B| = \aleph_0$$

2. In general:

$$A \cup B = (A \setminus B) \cup B$$

If $A \setminus B$ is *finite* we can use the previous claim to finish the proof.

If $A \setminus B$ is *countably infinite*, since $(A \setminus B) \cap B = \emptyset$, we can use the first case to finish the proof.

■

Conclusion. There are two conclusions that can be drawn from the aforementioned claims:

1. If sets $A_1, \ldots A_n$ are *countably infinite*, then $\bigcup_{i=1}^{n} A_i$ is also *countably infinite*.
2. If $A_1, \ldots A_n$ are sets such that for all $1 \leq i \leq n$: A_i is either *finite* or *countably infinite*, then $\bigcup_{i=1}^{k} A_i$ is either *finite* or *countably infinite*.

What if we take a *countably infinite* number of *countably infinite* sets, such as the *sequence* $A_1, A_2, \ldots$ such that for all $i \in \mathbb{N}$: A_i is *countably infinite*? Is $\bigcup_{i=1}^{\infty} A_i$ *countably infinite*?

Claim. $\mathbb{N} \times \mathbb{N}$ is *countably infinite*.

Proof.

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$f(m,n) = (1 + 2 + 3 + \cdots + (m + n - 2)) + n$$
$$\implies \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \implies |\mathbb{N} \times \mathbb{N}| = \aleph_0$$

■

Claim. Given sets $A_1, A_2, \ldots$ such that for all i: A_i is either *finite* or *countably infinite*, then $\bigcup_{i=1}^{\infty} A_i$ is *finite* or *countably infinite*.

Proof. We see that $\bigcup_{i=1}^{\infty} A_i$ is *equinumerous* to a subset of $\mathbb{N} \times \mathbb{N}$.

Given that all A_n is either *finite* or *countably infinite*, there exists a function $f_n : \mathbb{N} \to A_n$ that is *bijective* or $f_n : [m_n] \to A_n$ that is *bijective* in the case that $|A_n| = m_n$.

Now, we will define for all n: $g_n = (f_n)^{-1}$ and $h : \bigcup_{i=1}^{\infty} A_i \to \mathbb{N} \times \mathbb{N}$.

For all $x \in \bigcup_{i=1}^{\infty} A_i$, there exists $n \in \mathbb{N}$ such that $x \in A_n$. We therefore define $h(x) = (n, g_n(x))$. Now all we have to do is prove that h is *injective* and *bijective*.

h is *injective*: If $h(x) = h(y)$, then we can symbolize:

$$h(x) = (n_1, g_{n_1}(x)) \qquad h(y) = (n_2, g_{n_2}(y))$$

Therefore, we see that $n_1 = n_2$ and $g_{n_1}(x) = g_{n_1}(y)$, but since we know that g_{n_1} is *injective* $\implies x = y$.

We notice that $h : \bigcup_{i=1}^{\infty} A_1 \to \mathrm{Im}(h)$ is *bijective* and therefore $\bigcup A_i \sim \mathrm{Im}(h)$. However, we know that $\mathrm{Im}(h) \subseteq \mathbb{N} \times \mathbb{N}$, and that $\mathbb{N} \times \mathbb{N}$ is *countably infinite*, and therefore $\mathrm{Im}(h)$ is either *finite* or *countably infinite* $\implies \bigcup_{i=1}^{\infty} A_i$ is *finite* or *countably infinite*. ■

Note. If all A_i are *countably infinite*, then $\bigcup_{i=1}^{\infty} A_i$ is also *countably infinite*.

Alternatively, if one of the sets$A_j \in \{A_1, A_2, \ldots\}$ is *countably infinite*:

$$A_j \subseteq \bigcup_{i=1}^{\infty} A_i \implies \bigcup_{i=1}^{\infty} A_i \sim \aleph_0$$

12.3.3 Cardinality of the Rational Numbers ($\mathbb{Q}$)

Claim. $\mathbb{Q}$ is *countably infinite*.

Proof.

$$\mathbb{Q} = \left\{ \frac{m}{n} \;\middle|\; m \in \mathbb{Z}, n \in \mathbb{N} \right\}$$
$$Q_n = \left\{ \frac{m}{n} \;\middle|\; m \in \mathbb{Z} \right\}$$

For all n, Q_n is *countably infinite* since there exists $f_n : \mathbb{Z} \to Q_n$ which is *bijective*:

$$\forall m \in \mathbb{Z} : f_n(m) = \frac{m}{n}$$

$$\mathbb{Q} = \bigcup_{n \in \mathbb{N}} Q_n \implies \mathbb{Q} \sim \aleph_0$$

■

12.4 Uncountable Sets

Is the set of all the numbers between 0 and 1 *countable*?

Definition (Weak Inequality)**.** $|A| \leq |B|$ if there exists:

$$f : A \to B$$

that is *injective*.

Definition (Strong Inequality)**.** $|A| < |B|$ if $|A| \leq |B|$ and there does not exist:

$$g : A \to B$$

that is *surjective*.

Claim. $|\mathbb{N}| < |(0, 1)|$

Proof. This proof is famously known as *Cantor's diagonal argument*.

We define $f : \mathbb{N} \to (0, 1)$:

$$\forall n \in N : f(n) = \frac{1}{n} \implies f \text{ is } \textit{injective} \implies |\mathbb{N}| \leq |(0, 1)|$$

Now, we will prove by contradiction, supposing there does exist $g : \mathbb{N} \to (0, 1)$ that is *injective*.

We suppose that every number $(0, 1)$ has a unique expression as a decimal fraction.

We define:

$$\begin{aligned} g(1) &= 0.a_{11}a_{12}a_{13}a_{14}\ldots \\ g(2) &= 0.a_{21}a_{22}a_{23}a_{24}\ldots \\ g(3) &= 0.a_{31}a_{32}a_{33}a_{34}\ldots \\ &\vdots \end{aligned}$$

We want to show that there exists $b = 0.b_1b_2b_3b_4\cdots \in (0,1)$, such that $b \notin \mathrm{Im}(g)$. We define for all $i \in \mathbb{N}$:

$$b_i = \begin{cases} 4 & a_{ii} = 3 \\ 3 & a_{ii} \neq 3 \end{cases}$$

where for all $i \in \mathbb{N}$: $b_i \neq a_{ii}$, and therefore, $b \neq g(i)$. In other words, b does not have a source from the domain of g, which is contrary to the fact that g is *injective*. ■

We need a new *equivalence class* for $(0,1)$.

Symbol.

$$|(0,1)| = \aleph \text{ (or } \aleph_1)$$

- For all $a < b$: (a,b):
$$f(x) : (0,1) \to (a,b) \qquad f(x) = (b-a)x + a$$
- $\mathbb{R}$:
$$f(x) : (0,1) \to \mathbb{R} \qquad f(x) = \frac{1-2x}{x(1-x)}$$
- $(0,\infty)$:
$$f(x) : \mathbb{R} \to (0,\infty) \qquad f(x) = e^x$$
- $|(0,\infty)| = |(1,\infty)|$:
$$f(x) : (0,\infty) \to (1,\infty) \qquad f(x) = x + 1$$
- $|(1,\infty)| = |(0,1)|$:
$$f(x) : (1,\infty) \to (0,1) \qquad f(x) = \frac{1}{x}$$

$$\implies |(0,1)| = |(1,\infty)| = |\mathbb{R}| = \aleph_1$$

Claim (Continuum Hypnosis). There is no set A, such that:

$$\aleph_0 = |\mathbb{N}| < |A| < |\mathbb{R}| = \aleph_1$$

Theorem (Cantor's Theorem)**.** For any set A: $|A| < \underbrace{|P(A)|}_{2^A}$

Proof. We define $f : A \to P(A)$: $f(a) = \{a\}$. We can say that there is no function $g : A \to P(A)$ that is *injective*. We suppose by contradiction that there exists such a function g. We define:

$$B = \{a \in A \mid a \notin g(a)\} \subseteq A$$

There exists $b \in A$: $g(b) = B$, since g is *injective*:

$$b \in B \implies b \in g(b) \implies b \notin B$$
$$b \notin B \implies b \in g(b) \implies b \in B$$

Which is a contradiction. ■