

## A Deeper Look at Induction

Induction and recursion are *key* ideas in computer science.

I think it is worth taking a *deeper* look at the role of induction in mathematics.

The material today will be more abstract, but stick with me.

Today: Finish up induction and start graph theory.

## Examples of Orderings

1. The usual orderings  $\leq$  on  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  are total orderings.
2. The ordering  $\leq$  on  $\mathbb{Z}$  is **NOT** a well-ordering. For example,  $\mathbb{Z}$  itself does not have a least element.
3. Any total ordering on a finite set is a well ordering, e.g.  $S = \{x_1, x_2, x_3\}$  with  $x_1 \leq x_2 \leq x_3$ .

Subsets of $S$	Least Element
$\emptyset$	none
$\{x_1\}$	$x_1$
$\{x_2\}$	$x_2$
$\{x_3\}$	$x_3$
$\{x_1, x_2\}$	$x_1$
$\{x_1, x_3\}$	$x_1$
$\{x_2, x_3\}$	$x_2$
$\{x_1, x_2, x_3\}$	$x_1$

## When Does Induction Work?

We know that induction can be used to prove  $\forall n \in \mathbb{N} P(n)$ .

Can it be used to prove  $\forall x \in \mathbb{R} P(x)$ ? How about  $\forall x \in \mathbb{Q} P(x)$ ?

How might a proof by induction over the reals look like?

- ▶ In the inductive step, we need a method of going from one real number to the "next" real number.
- ▶  $P(x) \implies P(x+1)$  certainly does not hit all of  $\mathbb{R}$ . Neither does  $P(x) \implies P(x+\varepsilon)$  regardless of what  $\varepsilon$  is.
- ▶ Any way of getting to the "next" real number must *not* coincide with our usual notion of an ordering on  $\mathbb{R}$ .

## Well Ordering Principle for $\mathbb{N}$

**Well Ordering Principle for  $\mathbb{N}$ :** For any non-empty subset  $R \subseteq \mathbb{N}$ ,  $R$  has a least element. In other words,  $\mathbb{N}$  is well ordered under the usual ordering on  $\mathbb{N}$ .

*Proof.*

- ▶ Induction! On what?
- ▶ Induction on the size of  $R$  does not work. This can prove that all *finite* subsets of  $\mathbb{N}$  have a least element. . .
- ▶ but it does not work for the infinite subsets (like the set of even natural numbers).
- ▶ Specifically, induction on the size of  $R$  proves:

$$\forall n \in \mathbb{N} [((R \subseteq \mathbb{N}) \wedge (|R| = n) \wedge (R \neq \emptyset)) \implies Q(R)]$$

where  $Q(R)$  is " $R$  has a least element". The clause  $|R| = n$  means it only works for *finite*  $R$ .

## Well Orderings

Given a set  $S$ , a **total ordering**  $\leq$  on  $S$  is a relation which satisfies, for all  $x, y, z \in S$ :

- ▶ (Totality) We either have  $x \leq y$  or  $y \leq x$ .
- ▶ (Reflexivity) We have  $x \leq x$ .
- ▶ (Transitivity) If  $x \leq y$  and  $y \leq z$ , then  $x \leq z$ .
- ▶ (Antisymmetry) If  $x \leq y$  and  $y \leq x$ , then  $x = y$ .

Given a set  $S$ , a **well ordering**<sup>1</sup>  $\leq$  on  $S$  is a total ordering that also satisfies the following property:

**Well Ordering Property:** For any non-empty subset  $R \subseteq S$ ,  $R$  has a **least element**, that is, an element  $x$  such that  $x \leq y$  for all  $y \in R$ .

<sup>1</sup>Excuse the grammar, but this is the accepted terminology in mathematics.

## Proof of Well Ordering Principle for $\mathbb{N}$

**Well Ordering Principle for  $\mathbb{N}$ :** For any non-empty subset  $R \subseteq \mathbb{N}$ ,  $R$  has a least element.

*Proof.*

- ▶ Instead, try induction on *which* elements are in  $R$ .
- ▶ Inductive claim:  
 $P(n) = [((R \subseteq \mathbb{N}) \wedge (R \neq \emptyset) \wedge (n \in R)) \implies Q(R)]$ .
- ▶ Base case: For any  $R \subseteq \mathbb{N}$ , if  $0 \in R$ , then  $R$  has a least element. Namely, 0.
- ▶ Suppose that **if any of the elements  $0, 1, \dots, n$  are in  $R$ , then  $R$  has a least element.**
- ▶ Consider a set  $R$  containing  $n+1$ . If  $R$  also contains  $0, 1, \dots, n$ , then  **$R$  has a least element.**
- ▶ Otherwise,  $n+1$  must be the least element of  $R$ .  $\square$

## Well Ordering Is Equivalent to Induction

The Well Ordering Principle implies the Principle of Induction.

- ▶ Suppose  $P(0)$  and  $\forall n \in \mathbb{N} [P(n) \implies P(n+1)]$ . We want to show that  $\forall n \in \mathbb{N} P(n)$  holds.
- ▶ Assume, for the sake of contradiction, that for some  $n \in \mathbb{N}$ ,  $P(n)$  does **NOT** hold.
- ▶ Let  $R := \{n \in \mathbb{N} : P(n) \text{ does not hold}\}$ . By assumption,  $R$  is non-empty.
- ▶ By Well Ordering Principle,  $R$  has a least element  $n_0$ .
- ▶ Here  $n_0 \neq 0$  because we have proven  $P(0)$ .
- ▶ Consider  $P(n_0 - 1) \implies P(n_0)$ . Since  $n_0$  is the *least* element of  $R$ , then  $P(n_0 - 1)$  is True and  $P(n_0)$  is False.
- ▶ So,  $P(n_0 - 1) \implies P(n_0)$  is False, which is a **contradiction**.  
□

## Proof of the Division Algorithm

**Division Algorithm:** Given  $a, b \in \mathbb{Z}$  with  $b > 0$ , there exist unique integers  $q \in \mathbb{Z}$  and  $r \in \{0, 1, \dots, b-1\}$  with  $a = bq + r$ .

*Proof.*

- ▶ Consider the set  $S = \{a - bq : q \in \mathbb{Z} \text{ and } a - bq \geq 0\}$ .
- ▶  $S$  is non-empty, since we can make  $-bq$  arbitrarily large.
- ▶ Let  $r$  be the least element of  $S$  (**Well Ordering Property**).
- ▶ Then,  $r \geq 0$  and  $r = a - bq$  for some  $q \in \mathbb{Z}$ .
- ▶ **Claim:**  $r \leq b - 1$ . Indeed, if  $r \geq b$ , then  $a - (q+1)b$  would be a smaller element of  $S$ .
- ▶ So,  $a = bq + r$  for  $q \in \mathbb{Z}$  and  $r \in \{0, 1, \dots, b-1\}$ . □
- ▶ We will skip the proof that  $q$  and  $r$  are unique.

## Well Ordering Principle Conclusions

We can perform induction as long as we have a well ordering. A well ordering tells us what the “next” element is.

- ▶ Say we want to prove  $\forall x \in S, P(x)$ .
- ▶  $S$  has a least element  $x_0$ ; prove  $P(x_0)$ .
- ▶ Let  $R = S \setminus \{x_0\}$ ; then  $R$  has a least element  $x_1$ . Prove  $P(x_0) \implies P(x_1)$ .
- ▶ Continue...

So the question is: which sets can be well ordered?

- ▶ According to the axioms of set theory<sup>2</sup>, *all* of them!
- ▶ However, the well ordering on  $\mathbb{R}$  will be very *bizarre*, so trying to use induction on  $\mathbb{R}$  is not very useful.

The Well Ordering Principle can be used instead of induction.

<sup>2</sup>The standard axioms are called **ZFC**, for **Zermelo-Fraenkel with Choice**. If you want to learn more, take Math 135.

## The Puzzle of Green-Eyed Dragons

100 green-eyed dragons live on an island. They have a rule: if you find out that you have green eyes, you must commit ritual suicide. Despite this rule, they live in peace.

One day, a visitor comes to the island and says “I see a dragon here has green eyes”. The visitor leaves.

On day 100, every dragon commits suicide. **Why?**

## Division Algorithm

**Division Algorithm:** Given  $a, b \in \mathbb{Z}$  with  $b > 0$ , there exist unique integers  $q \in \mathbb{Z}$  and  $r \in \{0, 1, \dots, b-1\}$  with  $a = bq + r$ .

- ▶ In other words, we can divide  $a$  by  $b$  to get a quotient  $q$  and a remainder  $r$ .
- ▶ This humble theorem will be quite useful to us when we study modular arithmetic!
- ▶ Intuition: If  $a > 0$ , then we try to subtract as many copies of  $b$  as possible before we hit 0.
- ▶ Example: Let  $a = 40$  and  $b = 7$ . Consider

$$-9, -2, 5, 12, 19, 26, 33, 40, 47, 54, \dots$$

The Division Algorithm returns  $40 = 7 \cdot 5 + 5$ .

## The Dragons Took CS 70

**Claim:** For every positive integer  $n$ , if there are  $n$  green-eyed dragons on the island, they commit ritual suicide on day  $n$ .

*Proof.*

- ▶ Base case: There is one green-eyed dragon. After one day, the dragon performs the ritual.
- ▶ Inductive hypothesis: Assume the claim is true for  $n$  green-eyed dragons.
- ▶ Now consider an island of  $n+1$  green-eyed dragons.
- ▶ Inductive step: On day  $n+1$ , each green-eyed dragon sees  $n$  other green-eyed dragons.
- ▶ “If there were only  $n$  green-eyed dragons, they would have died on day  $n$ .”
- ▶ But they did not, so there are  $n+1$  green-eyed dragons. **Including me!** □

## Common Knowledge

Objection: The visitor did not tell the dragons anything new!

Consider the case of two green-eyed dragons.

- ▶ Each dragon knows the following fact:

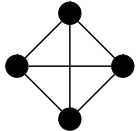
There is at least one dragon with green eyes. (\*)

- ▶ But does each dragon know that the other knows (\*)? **NO.** "If I have blue eyes, then the other does not know (\*)."
- ▶ After the visitor comes, each dragon knows (\*)... *and* each dragon knows that every other dragon knows (\*).
- ▶ The case of 100 dragons is 100-level nested thinking. "Does she know that I know that he knows..."

## Graph Terminology

An edge is a pair  $\{u, v\}$  where  $u, v \in V$ .

- ▶ Here, an edge has no *direction*. We call these graphs **undirected**. There are **directed graphs (digraphs)** too.
- ▶ The vertices  $u$  and  $v$  are called the **endpoints** of the edge.
- ▶ The edge  $\{u, v\}$  is **incident** to the vertices  $u$  and  $v$ .
- ▶ The **degree** of a vertex  $v$ ,  $\deg v$ , is the number of edges incident to it. Every vertex has degree 3:



- ▶ The **neighbors** of a vertex  $v$  are the vertices which are connected (via an edge) to  $v$ .

## Seven Bridges of Königsberg

New topic: graphs.

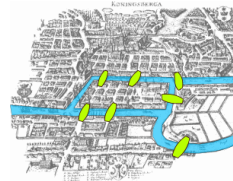


Figure: The figure is by Bogdan Giuscă (License).

Starting from anywhere, can you cross every bridge exactly once and end up where you started?

This problem was solved by Euler in 1736.

## Handshaking Lemma

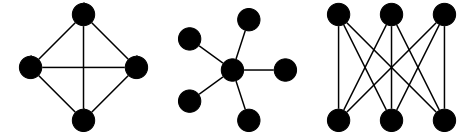
**Lemma:**  $\sum_{v \in V} \deg v = 2|E|$ .

*Proof.*

- ▶ Think of the vertices as people. **The edges are handshakes.**
- ▶ Then  $\deg v$  is the number of handshakes that  $v$  gives.
- ▶ Each handshake contributes 2 to the total degree.
- ▶ Total degree is twice the number of handshakes.  $\square$

## Graph Theory

Do not confuse "graphs" in graph theory with the graphs of *functions*.



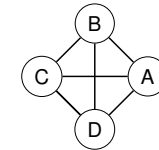
A **graph**  $G = (V, E)$  consists of:

- ▶  $V$ , a set of **vertices** or **nodes**, and
- ▶  $E \subseteq V \times V$ , a set of **edges**.

Graphs are visualized as *drawings*, where **nodes** are circles and **edges** are lines connecting their nodes.

We only consider finite graphs.

## Walks, Paths, Tours, Cycles



A **walk** is a sequence of edges  $\{v_0, v_1\}, \{v_1, v_2\}, \dots, \{v_{n-1}, v_n\}$ .

**Example:**  $\{A, B\}, \{B, D\}, \{D, B\}, \{B, C\}$ .

A **simple path** is a walk with no repeated edges, no repeated vertices.

**Example:**  $\{A, B\}, \{B, D\}$ .

A **tour** is a walk which starts and ends at the same vertex.

**Example:**  $\{A, B\}, \{B, A\}$ .

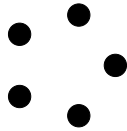
A **cycle** is a tour with no repeated edges.

**Example:**  $\{A, B\}, \{B, D\}, \{D, A\}$ .

## Connectivity

A graph is **connected** if for any pair of vertices, there exists a path between the vertices.

All the graphs we saw so far are connected. Here is one that is not connected:



These are called **isolated vertices**.

In the directed case, connectivity is not so simple. It may be possible to reach  $v$  from  $u$ , but not  $u$  from  $v$ .

## Conditions for Eulerian Tour

**Theorem:** A graph with no isolated vertices has an Eulerian tour iff it is connected and every vertex has even degree.

*Proof* ( $\implies$ ).

- ▶ Connected: The Eulerian tour connects all of the vertices.
- ▶ Even degree: Each time the tour visits a vertex, it must enter and exit through different edges.
- ▶ Each visit to the vertex contributes **two** to the degree of the vertex.
- ▶ The tour uses all edges.

## The Königsberg Graph

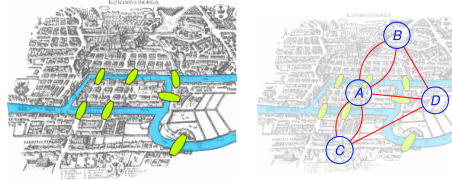


Figure: The figure on the left is by Bogdan Giuscă (License). The figure on the right is stolen from Satish Rao's slides.

We *abstract* out the unnecessary details to get a graph.

**Königsberg Bridges Problem:** Does there exist a tour in the graph which visits every edge exactly once?

## Conditions for Eulerian Tour

**Theorem:** A graph with no isolated vertices has an Eulerian tour iff it is connected and every vertex has even degree.

*Proof* ( $\Leftarrow$ ).

- ▶ Take a tour around the graph, just keep taking edges!
- ▶ Each vertex has **even degree**, so if you get stuck, you must be stuck at the vertex you started at.
- ▶ Remove the edges in the tour; the resulting graph has connected components.
- ▶ Each of these components must be connected and each vertex has even degree, so recursively find Eulerian tours.
- ▶ The original tour touches each of these Eulerian tours (original graph is **connected**), so "splice together" the tours. □

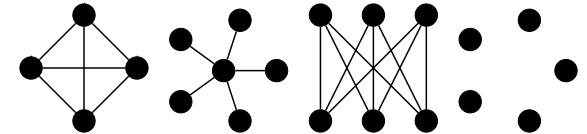
## Eulerian Tours

**Königsberg Bridges Problem:** Does there exist a tour in the graph which visits every edge exactly once?

In honor of Euler, we make the following definition:

**Definition:** An **Eulerian tour** is a tour which uses every edge exactly once.

Of the graphs we have seen so far, which have Eulerian tours?



## Solution to the Königsberg Bridges Problem

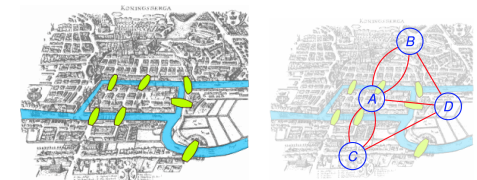


Figure: The figure on the left is by Bogdan Giuscă (License). The figure on the right is stolen from Satish Rao's slides.

Is the graph on the right **connected**, and does each vertex have **even degree**?

**NO.** There is no Eulerian tour!

## Summary

### Induction:

- ▶ Definitions of total ordering and well ordering.
- ▶ Well Ordering Principle for  $\mathbb{N}$ : The usual ordering on  $\mathbb{N}$  is a well ordering.
- ▶ The Well Ordering Principle is equivalent to induction.
- ▶ Green-eyed dragons: common knowledge is the key.

### Graph theory:

- ▶ Definitions: Graph, vertices, edges, endpoints, incidence, degree, neighbors, isolated vertices, connectedness, walks, paths, tours, cycles. . .
- ▶ Handshaking Lemma
- ▶ For graphs without isolated vertices, Eulerian tours exist iff the graph is connected and every vertex has even degree.