CS2802: Discrete Structures - Honors

Welcome to the class!

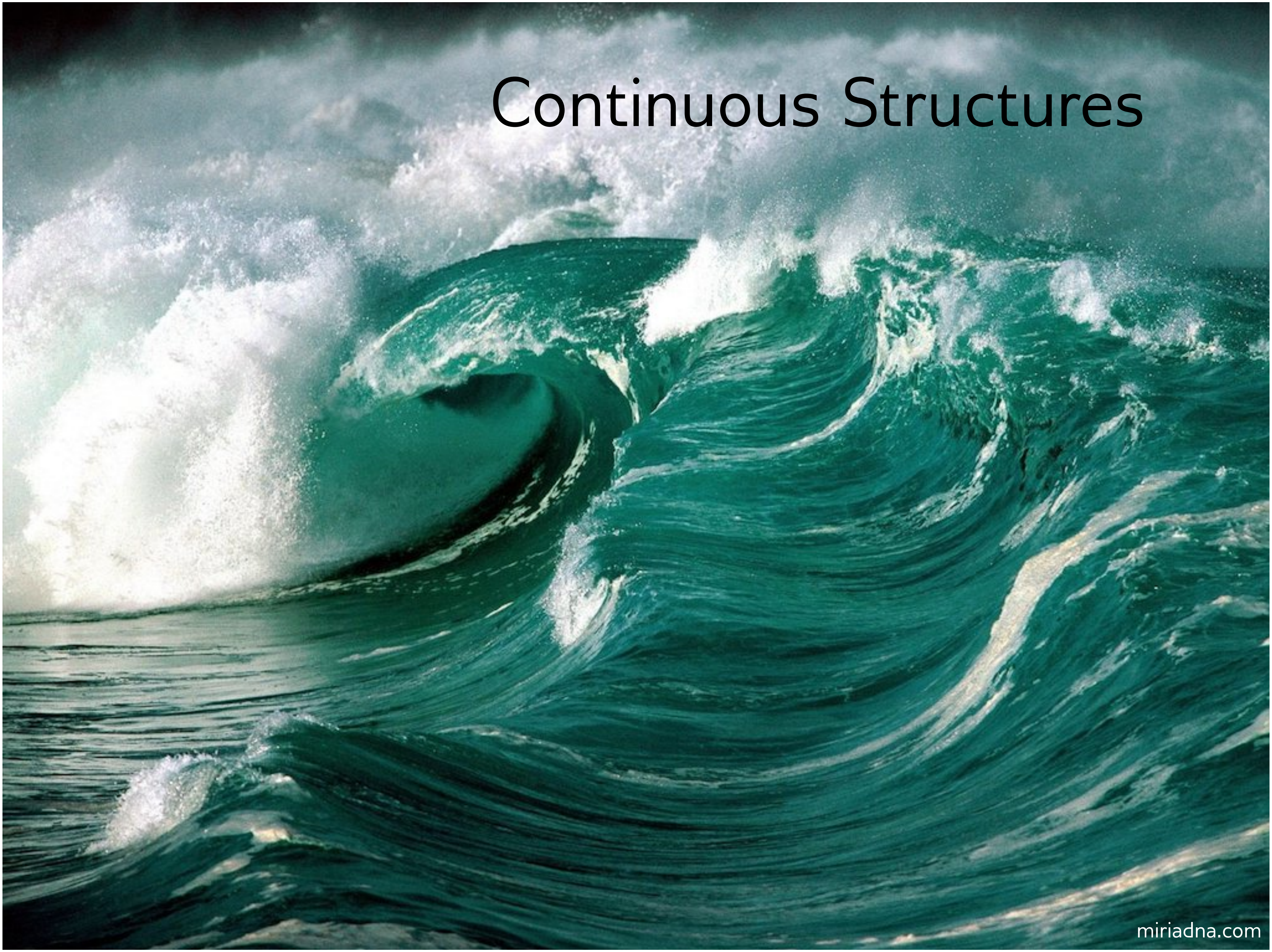
So What's "Discrete Structures" all about anyway?

- The following slides are largely taken from Sid Chaudhuri, with thanks.

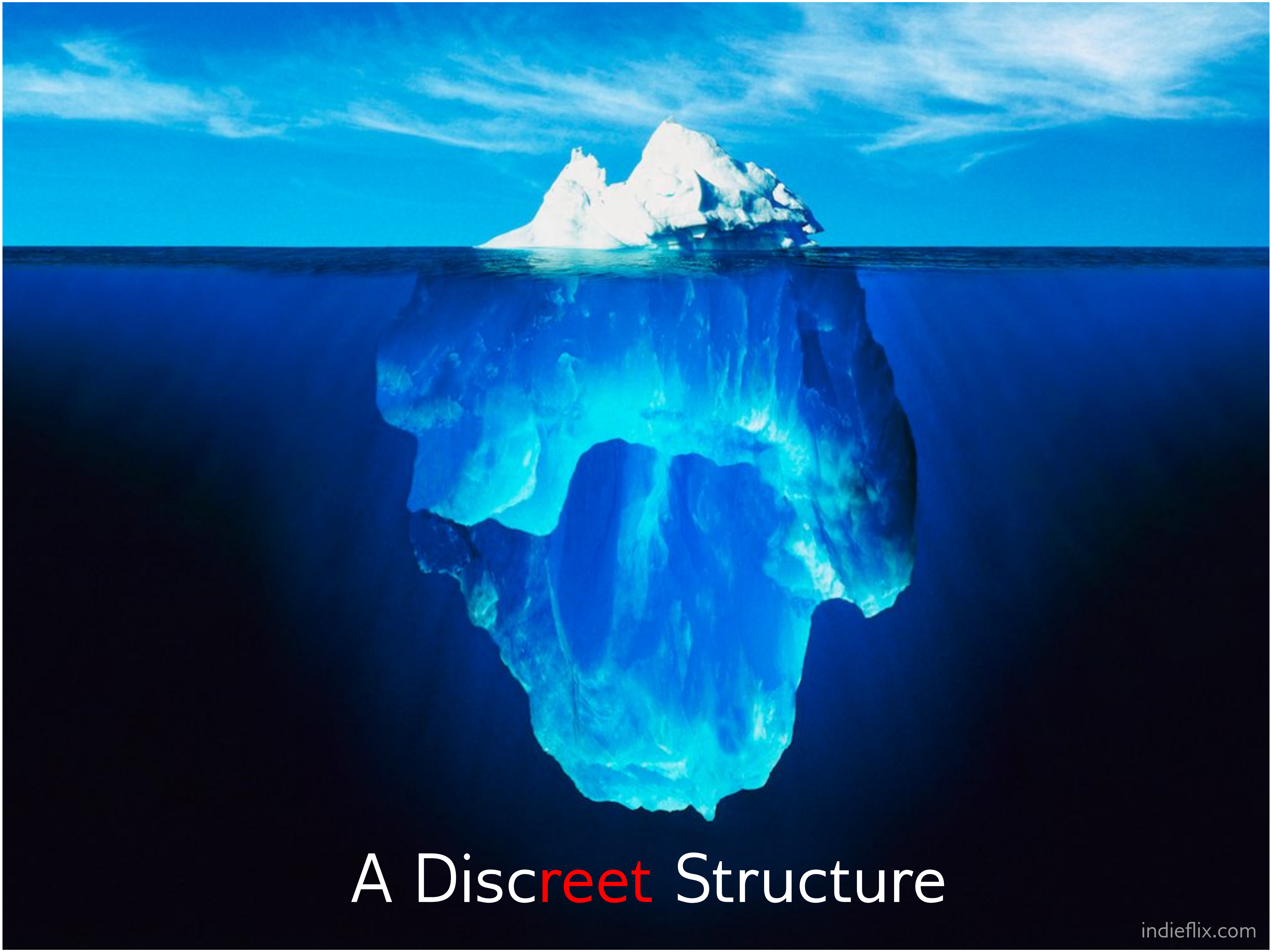
Discrete Structures

wallippo.com

Continuous Structures

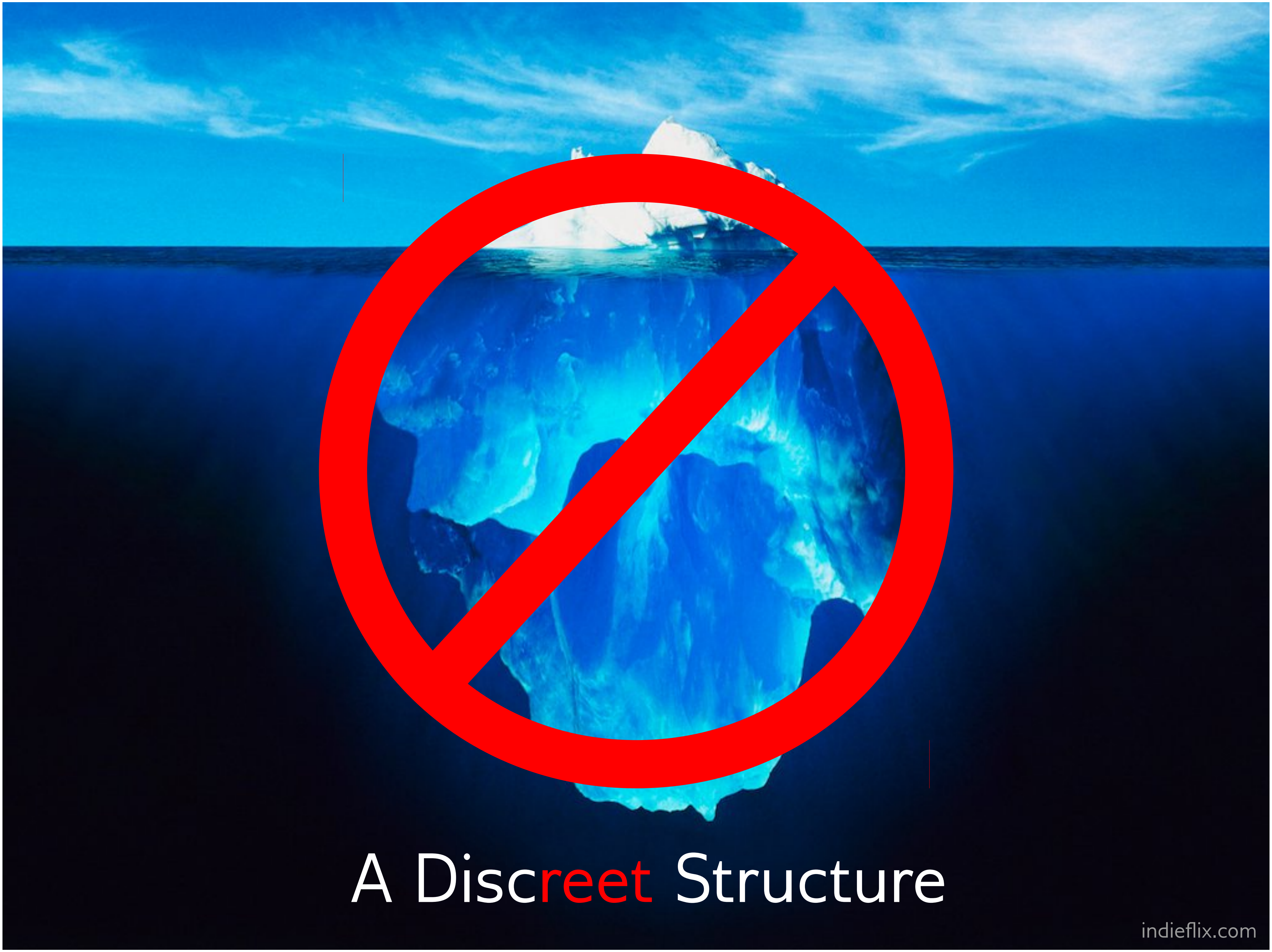


miriadna.com



A Discreet Structure

indieflix.com



A Discreet Structure

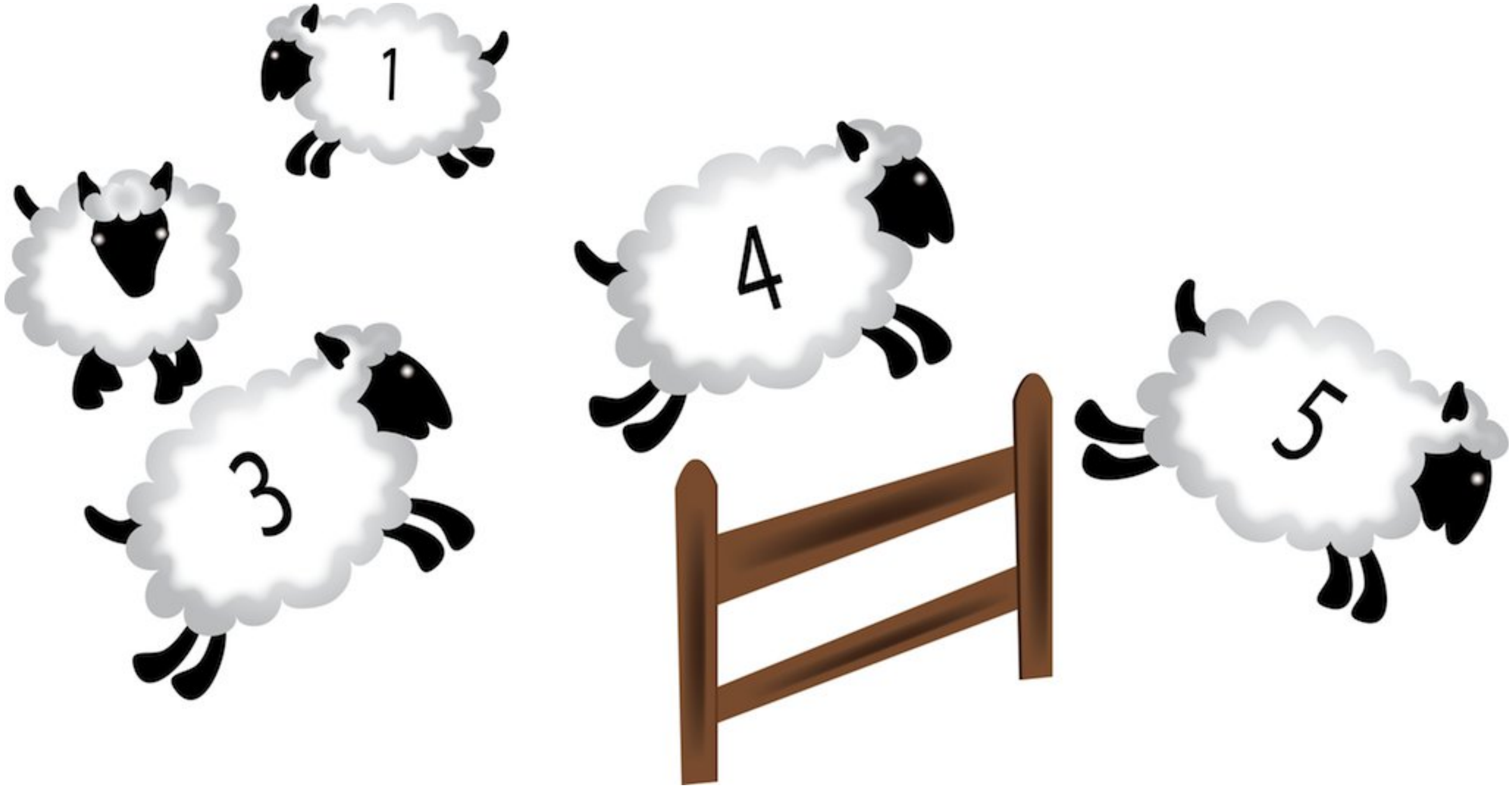
indieflix.com

- discrete: individually separate and distinct
- discreet
  - careful and circumspect in one's speech or actions, especially in order to avoid causing offense or to gain an advantage.
  - intentionally unobtrusive.

Things we can count with the integers

ser4kids.com

Things we can count with the integers

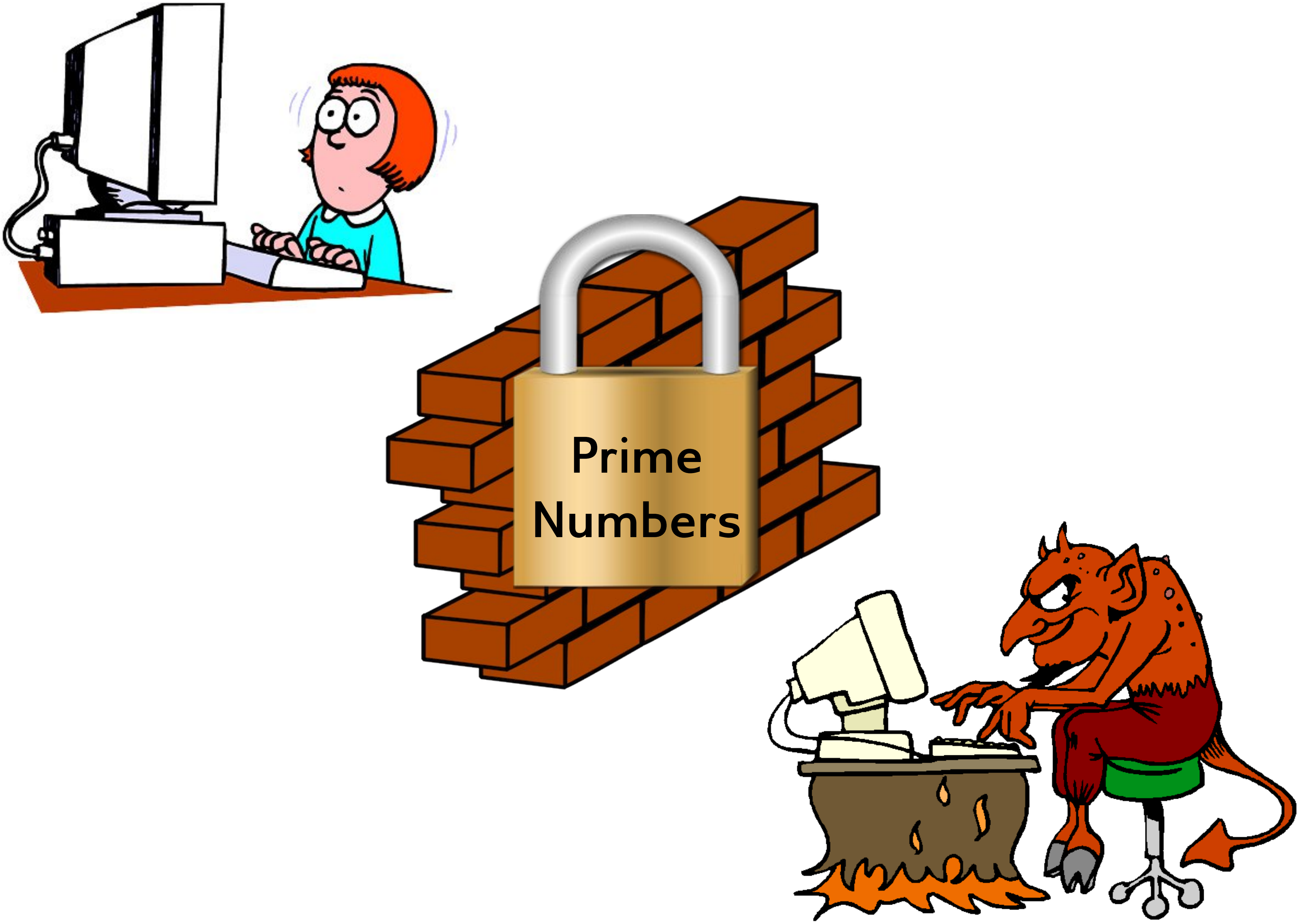


clipartpanda.com

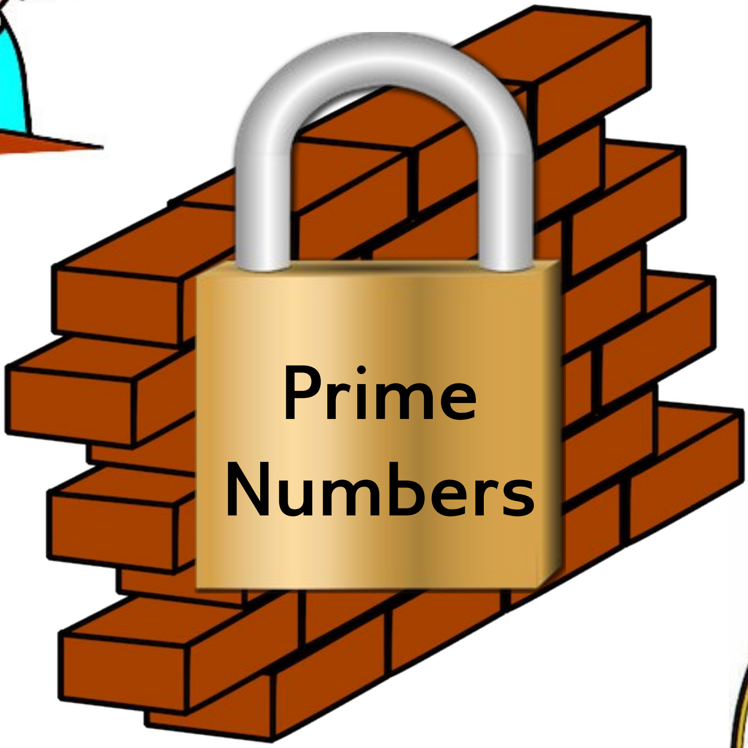
Prime Numbers

A number with exactly two divisors:
1 and **itself**

2, 3, 5, 7, 11, 13, 17...



eldhughes.com, pleasureinlearning.com


Prime
Numbers

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

How many prime numbers exist?

How many prime numbers exist?

1,000?

How many prime numbers exist?

1,000?

1,000,000?

How many prime numbers exist?

1,000?
1,000,000?
An infinite number?

How many prime numbers exist?

1,000?

1,000,000?

An infinite number

Euclid's Proof of Infinitude of Primes

(~300BC)

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p
- Consider $n = (1 \times 2 \times 3 \times \ldots \times p) + 1$

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p
- Consider $n = (1 \times 2 \times 3 \times ... \times p) + 1$
- n cannot be prime (p is the largest)

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p
- Consider $n = (1 \times 2 \times 3 \times \ldots \times p) + 1$
- n cannot be prime (p is the largest)
- Therefore it has a (prime) divisor $< n$

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p
- Consider $n = (1 \times 2 \times 3 \times \ldots \times p) + 1$
- n cannot be prime (p is the largest)
- Therefore it has a (prime) divisor $< n$
- But no number from 2 to p divides n

Euclid's Proof of Infinitude of Primes

- Suppose there is a finite number of primes
- Then there is a largest prime, p
- Consider $n = (1 \times 2 \times 3 \times \ldots \times p) + 1$
- n cannot be prime (p is the largest)
- Therefore it has a (prime) divisor $< n$
- But no number from 2 to p divides n
- So n has a prime divisor greater than p

Euclid's Proof of Infinitude of Primes

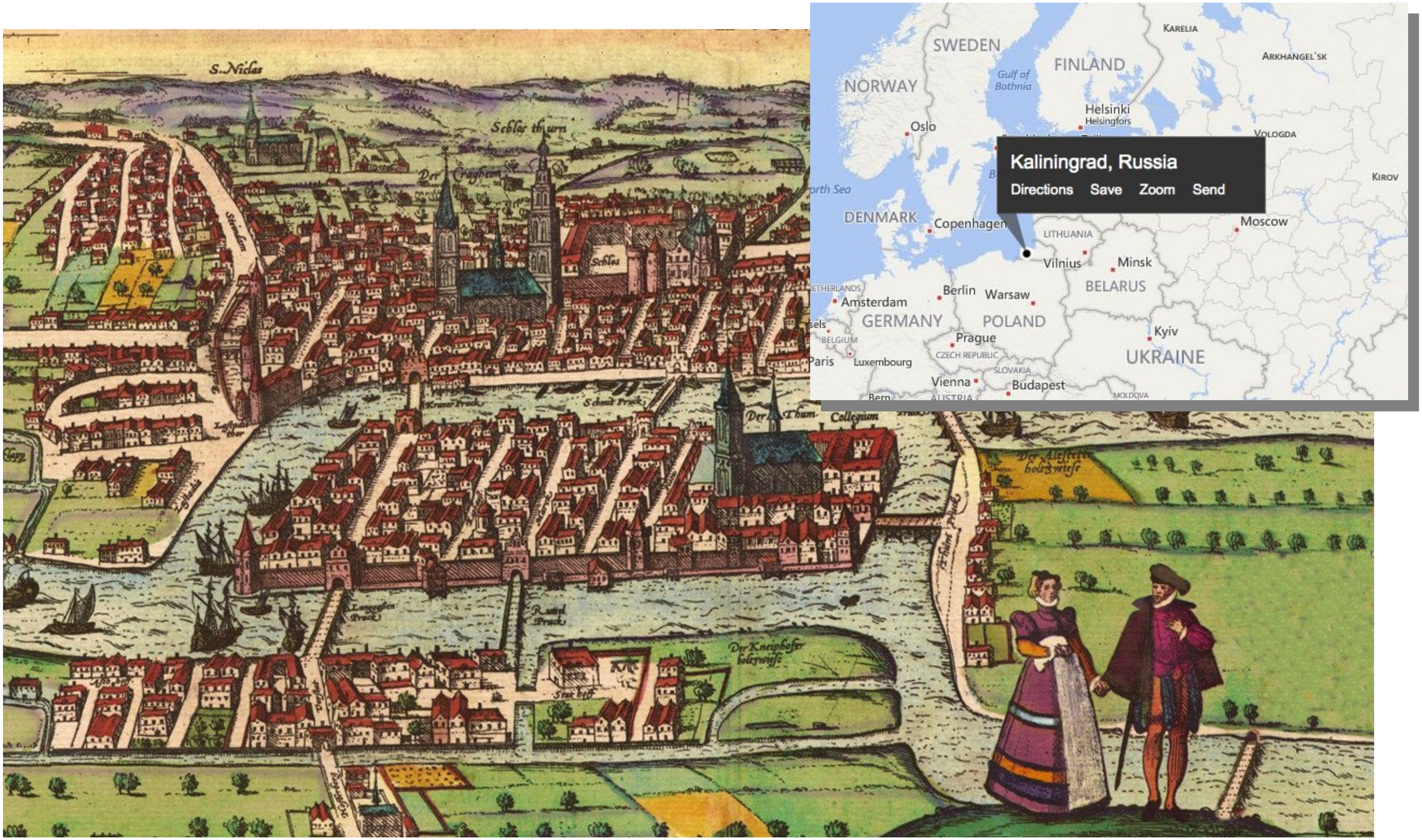
- Suppose there is a finite number of primes
- Then there is a **largest prime, p**
- Consider $n = (1 \times 2 \times 3 \times \ldots \times p) + 1$
- n cannot be prime (p is the largest)
- Therefore it has a (prime) divisor $< n$
- But no number from 2 to p divides n
- So n has a **prime divisor greater than p**

Contradiction!!!

Discrete Structures

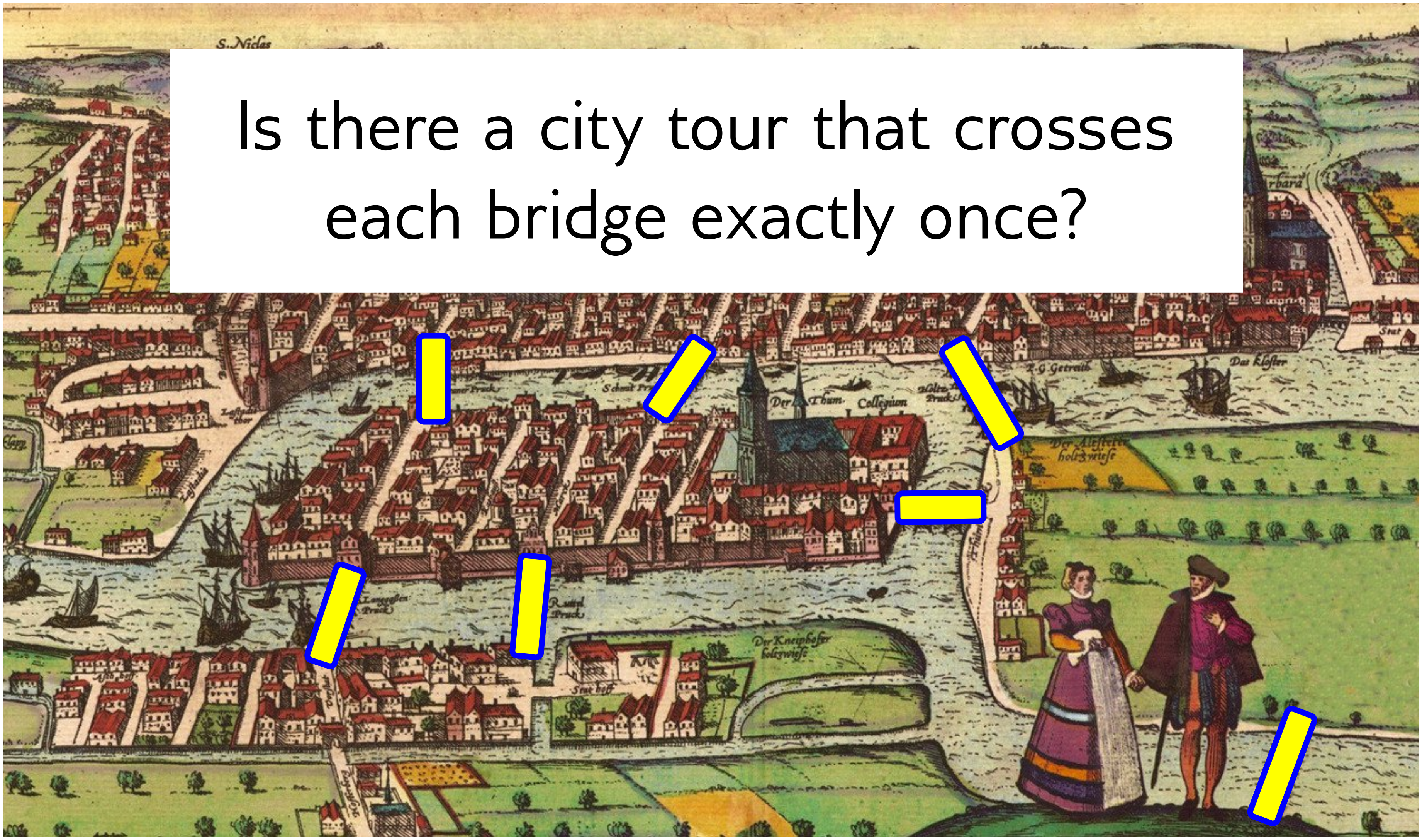
- Number theory
- Proof systems
- Sets, functions, relations
- Counting and probability

Bridges of Königsberg



Braun & Hogenberg, "Civitates Orbis Terrarum", Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

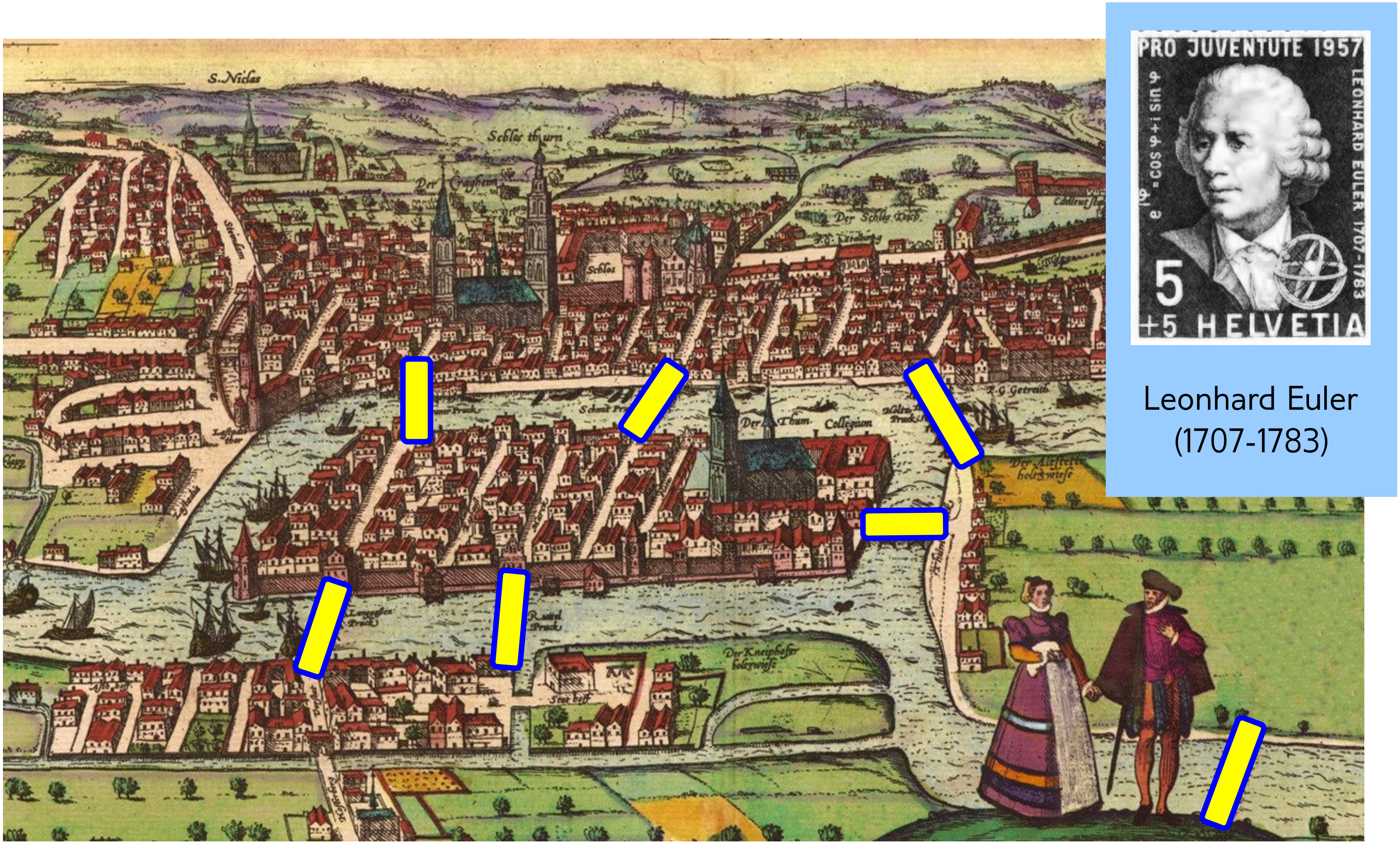
Bridges of Königsberg



Is there a city tour that crosses each bridge exactly once?

Braun & Hogenberg, “Civitates Orbis Terrarum”, Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

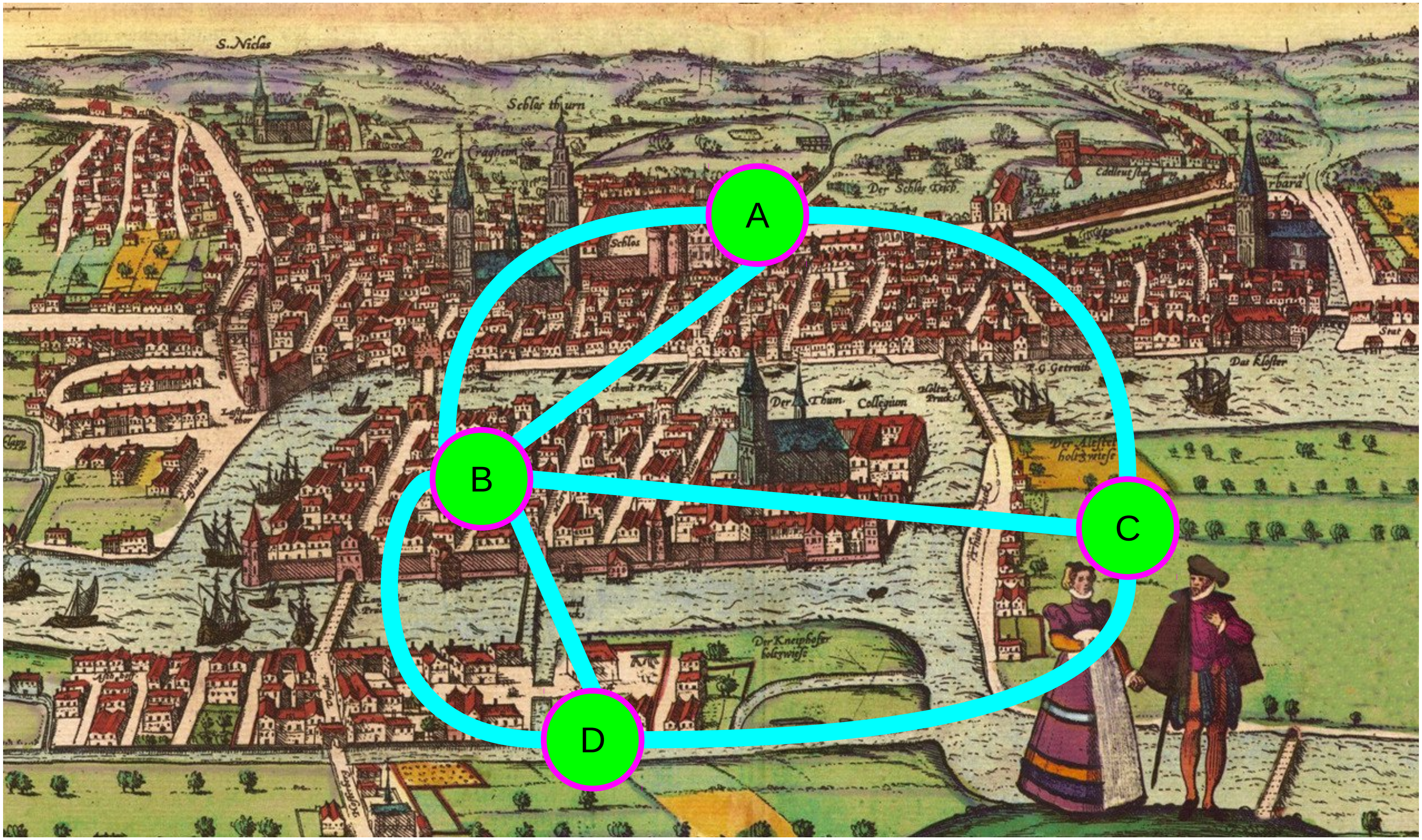
Bridges of Königsberg



Leonhard Euler
(1707-1783)

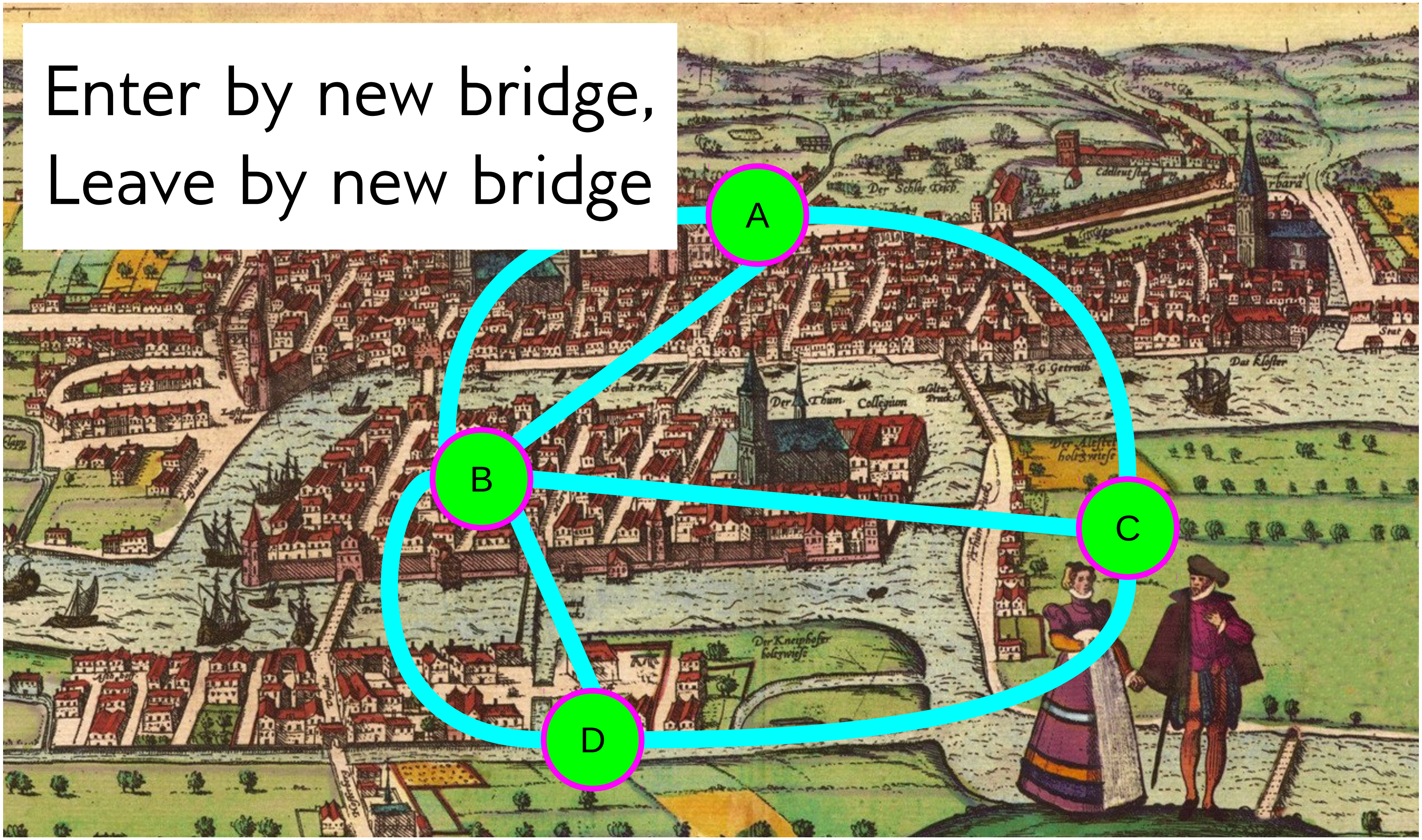
Braun & Hogenberg, “Civitates Orbis Terrarum”, Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

Bridges of Königsberg



Braun & Hogenberg, “Civitates Orbis Terrarum”, Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

Bridges of Königsberg

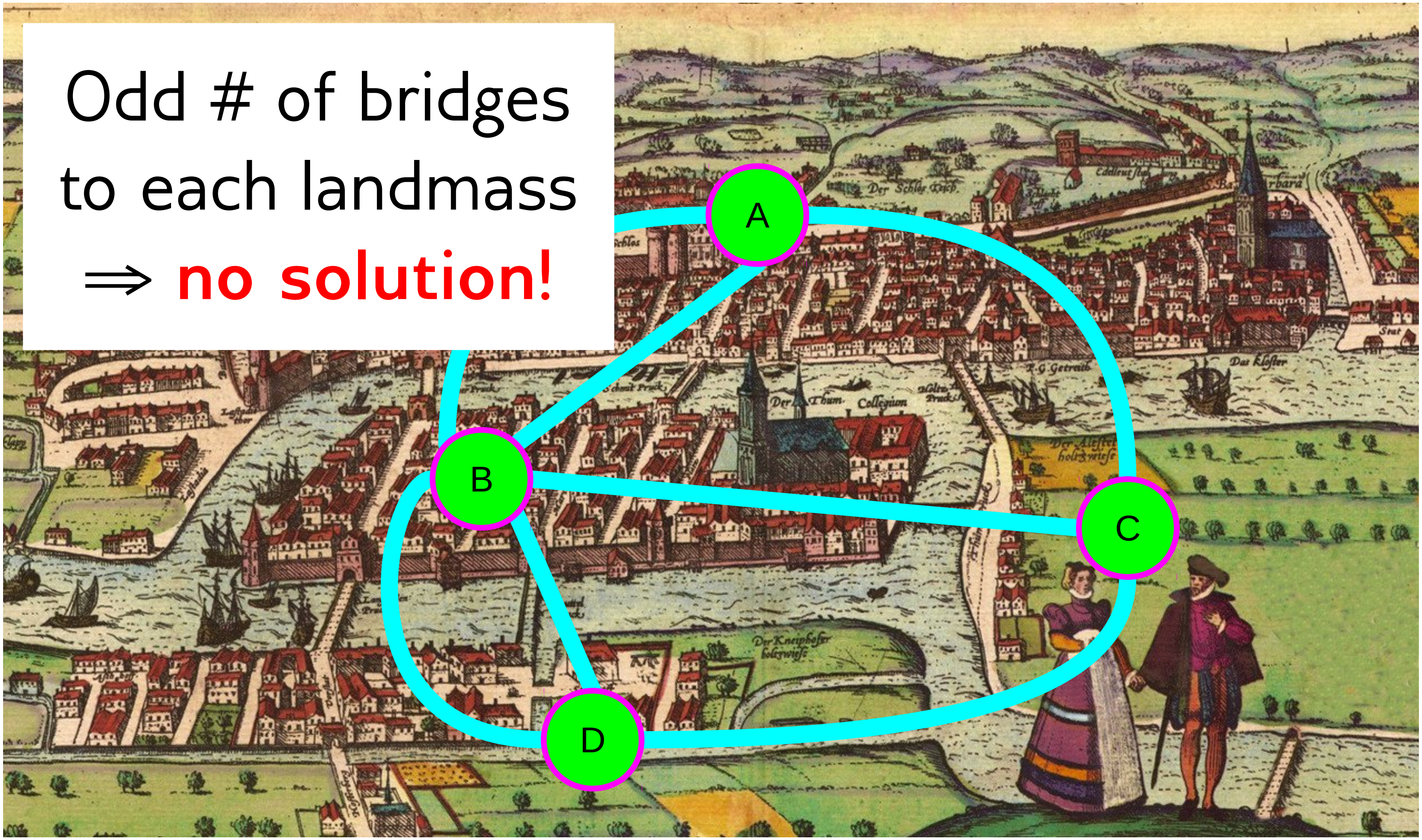


Enter by new bridge, Leave by new bridge

Braun & Hogenberg, "Civitates Orbis Terrarum", Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

Bridges of Königsberg

Odd # of bridges
to each landmass
⇒ **no solution!**

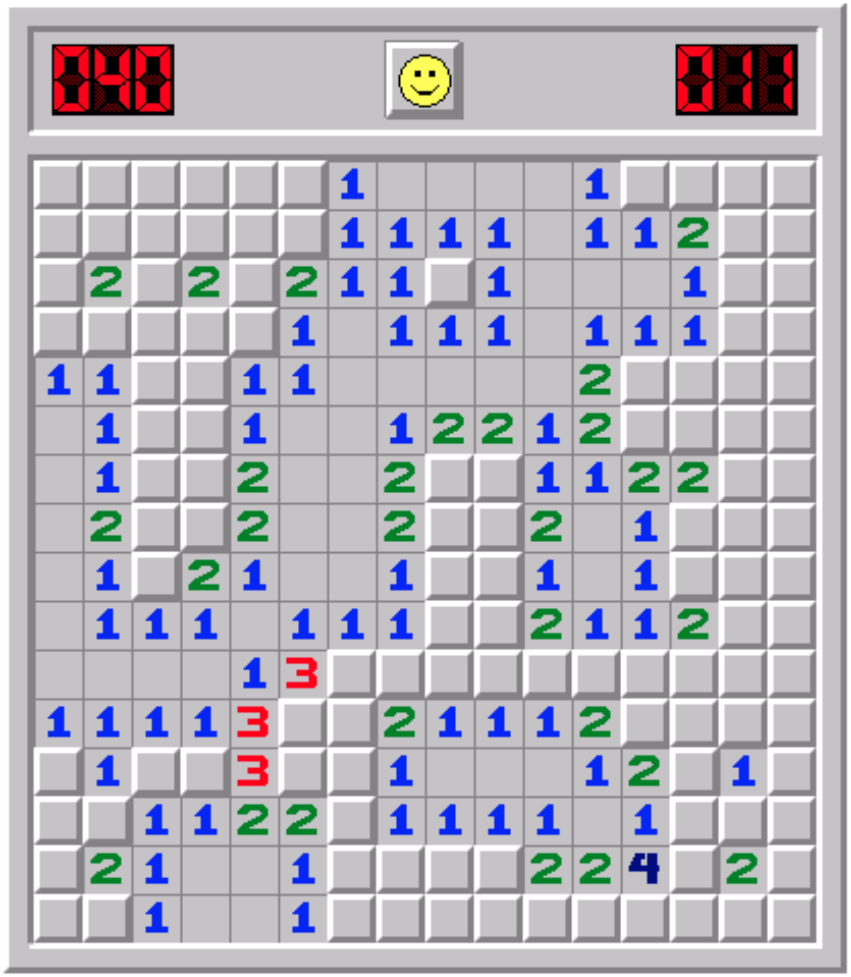


Braun & Hogenberg, “Civitates Orbis Terrarum”, Cologne 1585. Photoshopped to clean up right side and add 7th bridge.

Bridges of Königsberg

- Cross each bridge once: Euler Path
  - Easy for a computer to calculate
- Visit each landmass once: Hamiltonian Path
  - Probably very hard for a computer to calculate
  - If you can find an efficient solution, you will get $1M and undying fame (answers “P = NP?”)
  - (Will also break modern crypto, collapse the banking system, revolutionize automated mathematics and science, bring about world peace…)

You'll also be terrific at Minesweeper



Discrete Structures

- Number theory
- Proof systems
- Sets, functions, relations
- Counting and probability
- Graph theory
- Models of computation, automata, complexity

This sentence is false.

This sentence is false.

If true, it is false

If false, it is true

This sentence is false.

If true, it is false

If false, it is true

Discrete Structures

- Number theory
- Proof systems
- Sets, functions, relations
- Counting and probability
- Graph theory
- Models of computation, automata, complexity
- Logic
- Decidability, computability

warrenphotographic.co.uk, auntiedogmasgardenspot.wordpress.com

CS 2802 vs. CS 2800

All of the above applies to both CS 2800 and CS 2802

- Both CS 2802 and CS 2800 cover essentially the same material

So how do they differ?

- CS 2802 is an honors version of CS 2800. That means:
  - It will cover material in more depth
  - It will cover a few extra topics
  - You will be expected to be able to read the text and absorb some material on your own.
  - There will be less time on straightforward exercises.
    - Although both courses will courses will focus on writing proofs
  - Most people will find the homework in CS 2802 harder
- The courses will stay in synch up to the end of the add period (Feb. 4), to make it easy to transfer from CS 2802 to CS 2800

CS 2802 vs. CS 2800

All of the above applies to both CS 2800 and CS 2802

- Both CS 2802 and CS 2800 cover essentially the same material

So how do they differ?

- CS 2802 is an honors version of CS 2800. That means:
  - It will cover material in more depth
  - It will cover a few extra topics
  - You will be expected to be able to read the text and absorb some material on your own.
  - There will be less time on straightforward exercises.
    - Although both courses will courses will focus on writing proofs
  - Most people will find the homework in CS 2802 harder
- The courses will stay in synch up to the end of the add period (Feb. 4), to make it easy to transfer from CS 2802 to CS 2800

This is the second time that CS 2802 is being taught.

- It's still a work in progress!
- Feedback and suggestions are welcome!

Proofs

One running theme of the course:

- How to prove things
- How to write good proofs

That's what we'll be starting with.

What's a proof?

For our purposes, a proof is a chain of logical deductions, leading to the proposition in question (i.e., the thing you want to prove) from a base set of axioms (i.e., things you can assume without proving them).

- We'll later study axiomatic systems for deriving statements written in a formal logic, but when we talk about writing proofs in this course, we mean proofs that are largely English sentences.

What's a proof?

For our purposes, a proof is a chain of logical deductions, leading to the proposition in question (i.e., the thing you want to prove) from a base set of axioms (i.e., things you can assume without proving them).

- We'll later study axiomatic systems for deriving statements written in a formal logic, but when we talk about writing proofs in this course, we mean proofs that are largely English sentences.

So what counts as a "legal" chain of logical deductions? How big a step can you take?

- It's largely in the eye of the beholder
- You need to convince the graders that you've understood what's going on and haven't missed any essential details.

Proving Implications

There are standard techniques for proving things.
Suppose that we want to prove an implication of the form $P \Rightarrow Q$

- Read this as "If P is true then Q is true".

So you can assume P, and the prove Q using the fact that P is true in your proof.

Structure of Proof:

Assume P

...

Therefore Q.

Example: If n is odd, then so is n^2.
How do we even start the proof?

Example: If n is odd, then so is n^2.
How do we even start the proof?

- We need a formal definition of “odd”!

Example: If n is odd, then so is n^2.
How do we even start the proof?

- We need a formal definition of "odd"!

Proof: Assume that n is odd.
Since n is odd, $n = 2m + 1$ for some integer m.
Then $n^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$.
Therefore n^2 has the form $2m' + 1$ (where $m' = 2m^2 + 2m$), and must be odd. ■

Example: If n is odd, then so is n^2.
How do we even start the proof?

- We need a formal definition of "odd"!

Proof: Assume that n is odd.
Since n is odd, $n = 2m + 1$ for some integer m.
Then $n^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$.
Therefore n^2 has the form $2m' + 1$ (where $m' = 2m^2 + 2m$), and must be odd. ∎

The proof is trivial, but there are two key points:

- To prove the result carefully, you need a formal definition of odd.
- It has the right "structure".
  - The ∎ marks the end of a proof.

Proof by Contradiction:

Sometimes the best way to prove $P \Rightarrow Q$ is by contradiction:

- Show if Q is false, then P is also false (i.e., $\neg Q \Rightarrow \neg P$).
- In general $P \Rightarrow Q$ is equivalent to $\neg Q \Rightarrow \neg P$.
  - $\neg Q \Rightarrow \neg P$ is called the *contrapositive* of $P \Rightarrow Q$.

Proof by Contradiction:

Sometimes the best way to prove $P \Rightarrow Q$ is by contradiction:

- Show if Q is false, then P is also false (i.e., $\neg Q \Rightarrow \neg P$).
- In general $P \Rightarrow Q$ is equivalent to $\neg Q \Rightarrow \neg P$.
  - $\neg Q \Rightarrow \neg P$ is called the *contrapositive* of $P \Rightarrow Q$.

Example: If n^2 is odd, then so is n.

Proof: Suppose that n^2 is odd and (by way of contradiction) that n is not odd. Then it must be even.

- Why? How would you prove this formally?

Thus, $n = 2k$ for some k. This means that $n^2 = 4k^2 = 2(2k^2)$, so n^2 is even. - Contradiction

Therefore if n^2 is odd, then so is n. ∎

Theorem: $\sqrt{2}$ is irrational.
Proof: By contradiction. Suppose that $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$ for some $a, b \in \boldsymbol{N}^+$. We can assume that a/b is in lowest terms.

- Therefore, a and b can't both be even.

Squaring both sides, we get

$$2 = a^2/b^2$$

Thus, $a^2 = 2b^2$, so a^2 is even. This means that a must be even.

- Why? What does this follow from?

Theorem: $\sqrt{2}$ is irrational.
Proof: By contradiction. Suppose that $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$ for some $a, b \in \boldsymbol{N}^+$. We can assume that a/b is in lowest terms.

- Therefore, a and b can't both be even.

Squaring both sides, we get

$$2 = a^2/b^2$$

Thus, $a^2 = 2b^2$, so a^2 is even. This means that a must be even.

- Why? What does this follow from?

That means that $a = 2c$ for some integer c. Then $a^2 = 4c^2$.

Thus, $4c^2 = 2b^2$, so $b^2 = 2c^2$. This means that b^2 is even, and hence so is b.

Contradiction!

Thus, $\sqrt{2}$ must be irrational.
∎

Proving iff (if and only if)

Sometimes you want to prove $P \Leftrightarrow Q$. This is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

- One approach: prove $P \Rightarrow Q$ and $Q \Rightarrow P$ separately, as discussed above.
- Another approach: construct a chain of iffs:

$$\begin{array}{ll} & P \\ \text{iff} & P_1 \\ \ldots & \\ \text{iff} & P_n \\ \text{iff} & Q \quad \blacksquare \end{array}$$

See example in text.

Proving iff (if and only if)

Sometimes you want to prove $P \Leftrightarrow Q$. This is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

- One approach: prove $P \Rightarrow Q$ and $Q \Rightarrow P$ separately, as discussed above.
- Another approach: construct a chain of iffs:

$$\begin{array}{ll} & P \\ \text{iff} & P_1 \\ \ldots & \\ \text{iff} & P_n \\ \text{iff} & Q \quad \blacksquare \end{array}$$

See example in text.

Make sure you put in the iffs! Don't just write down a sequence of formulas without words between them.

- This is guaranteed to be an unacceptable proof!

Proof by cases

Splitting up a complex argument into cases can be a good strategy

Example: Show that every integer that is a perfect cube (i.e., has the form n^3) is either a multiple of 9, 1 more than a multiple of 9, or 1 less than a multiple of 9.

Proof by cases

Splitting up a complex argument into cases can be a good strategy

Example: Show that every integer that is a perfect cube (i.e., has the form n^3) is either a multiple of 9, 1 more than a multiple of 9, or 1 less than a multiple of 9.
Every number n is either a multiple of 3, 1 more than a multiple of 3, or 2 more than a multiple of 3, which means it's 1 less than a multiple of 3 ($3p + 2 = 3(p + 1) - 1$).

- Consider each case separately.
  - What's the form of n^3 if $n = 3p$, $n = 3p + 1$, and $n = 3p - 1$, respectively

Soon we'll get to a proof method that plays a major role in this course:

- Induction

But first we'll briefly cover a few other topics that are

(a) important and

(b) give us practice in writing proofs.

Soon we'll get to a proof method that plays a major role in this course:

- Induction

But first we'll briefly cover a few other topics that are

(a) important and

(b) give us practice in writing proofs.

- propositional logic
- sets
- relations
- graphs
- functions

Propositional Logic (A Very Brief Review)

I will assume that you've all seen propositional logic before.

- Whether or not you have, you should read Sections 3.1-3.5 in MCS
  - Section 3.6 talks about first-order (or predicate) logic; we'll talk more about that later in the course

I'll hit some highlights in the next few slides . . .

Propositional Logic: Syntax

The *syntax* of propositional logic tells us what formulas are legal:

- We with *primitive propositions*, basic statements like
  - It is now brillig
  - This thing is mimsy
  - It's raining in San Francisco
  - 4 is even
- We then form more complicated *compound propositions* using connectives like:
  - $\neg$: not
  - $\wedge$: and
  - $\vee$: or
  - $\Rightarrow$: implies
  - $\Leftrightarrow$: equivalent (if and only if)

Technically, we define more complicated formulas by induction.

Propositional Logic: Syntax

The *syntax* of propositional logic tells us what formulas are legal:

- We with *primitive propositions*, basic statements like
  - It is now brillig
  - This thing is mimsy
  - It's raining in San Francisco
  - 4 is even
- We then form more complicated *compound propositions* using connectives like:
  - $\neg$: not
  - $\wedge$: and
  - $\vee$: or
  - $\Rightarrow$: implies
  - $\Leftrightarrow$: equivalent (if and only if)

Technically, we define more complicated formulas by induction.

MCS uses English connectives (NOT, AND, OR, IMPLIES, IFF).

- I have no idea why!

I'll stick to the standard mathematical notation.

Propositional Logic: Semantics

Semantics tells you when a formula is true.

- I'll assume you how to define the truth value of compound propositions given the truth value of primitive propositions, using truth tables.

I want to focus on the truth table for ⇒:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	?
F	F	?

What should the truth value of $P \Rightarrow Q$ be when P is false?

Propositional Logic: Semantics

Semantics tells you when a formula is true.

- I'll assume you how to define the truth value of compound propositions given the truth value of primitive propositions, using truth tables.

I want to focus on the truth table for ⇒:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

- We take $P \Rightarrow Q$ to be true if P is false.
  - This definition gives what is called *material implication*

Why is this reasonable?

Propositional Logic: Semantics

Semantics tells you when a formula is true.

- I'll assume you how to define the truth value of compound propositions given the truth value of primitive propositions, using truth tables.

I want to focus on the truth table for $\Rightarrow$:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

- We take $P \Rightarrow Q$ to be true if P is false.
  - This definition gives what is called *material implication*

Why is this reasonable?

- This choice is mathematically convenient
- As long as Q is true when P is true, then $P \Rightarrow Q$ will be true no matter what.
  - It justifies what we did before: Assume P is true, then prove Q.

Problems with Material Implication

Although *material implication* is what we'll use in this course, it has some possibly unintended consequences.

- (elephants are pink $\Rightarrow$ the moon is made of green cheese) $\vee$ (the moon is made of green cheese $\Rightarrow$ elephants are pink) is valid

Problems with Material Implication

Although *material implication* is what we'll use in this course, it has some possibly unintended consequences.

- (elephants are pink $\Rightarrow$ the moon is made of green cheese) $\vee$ (the moon is made of green cheese $\Rightarrow$ elephants are pink) is valid

Perhaps a more serious problem: false formulas imply everything.

Suppose that we have a big database, and we want to query it.

- We want the database to return *true* to a query φ if the conjunction of facts in the database imply φ.
- But large databases almost surely have some inconsistency somewhere.
    - Just because a database has some inconsistency somewhere, we don't want to conclude that you are a student at Cornell, and a student at Harvard, and a student at North Dakota state!

Alternatives to Material Implication

Logicians have considered a number of different propositional logics, each with different notions of implication.

- *classical* (propositional) logic uses material implication.

But there are other propositional logics, including:

- *conditional logic*, which uses *conditional* (or *counterfactual*) implication
  - if the match were dry then it would light
- *intuitionistic logic*
  - $p \lor \neg p$ is not necessarily valid in intuitionistic logic
  - roughly speaking, p is valid in intuitionistic logic only if it has a constructive proof
- *relevance* logic, which uses *relevant implication*: $p \Rightarrow q$ is true only if q is true whenever p is, and p is “relevant” to q
  - in relevance logic, $p \land \neg p$ does not imply q, although it does in classical logic.
    - This deals with the database problem

Validity, Satisfiability, and Equivalence

- A formula φ is *valid* (also known as a *tautology*) if every truth assignment makes φ true.
- φ is *satisfiable* if some truth assignment makes φ true.
- Two formulas φ and ψ are *equivalent* if exactly the same truth assignments make both φ and ψ true.
- **Lemma:** φ and ψ are equivalent iff $\varphi \Leftrightarrow \psi$ is valid.
  - This will be homework

Examples:

- $\varphi \Rightarrow \psi$ is equivalent to $\neg\varphi \vee \psi$
- $\varphi \Rightarrow \psi$ is equivalent to $\neg\psi \Rightarrow \neg\varphi$.
  - This justifies proof by contradiction

First-Order Logic: Syntax

First-order (or predicate) logic extends propositional logic with

- Quantification: $\forall n P(n)$, $\exists x P(x)$.
  - The quantifier ranges over some *domain*
- *Predicates* that take arguments:
  - A *unary predicate* takes one argument
    - *Tall(Alice)*: *Tall* is a unary predicate
  - A *binary predicate* takes two argument:
    - *Loves(Alice,Bob)*
  - In general, we can have k-ary predicates
- *Function symbols* that take arguments (just like predicates): $+(2,3) = 5$
- *Constant* symbols: *Alice*, *Bob*

How do we prove for $\forall x P(x)$: i.e., that $P(x)$ is true for all values of x.

- Here P is a statement (often in English) that mentions x):
  - E.g., $\forall x(x^2 \geq x)$
- Whether $\forall x P(x)$ is true depends on what x ranges over (the *domain*)
  - $\forall x(x^2 \geq x)$ is false if x ranges over the real numbers.
    - $(1/2)^2 < 1/2$
  - It's true if x ranges over the integers.
- To prove it, we consider an arbitrary integer x, and show that $x^2 \geq x$ for that x.
- How do we do that?

How do we prove for $\forall x P(x)$: i.e., that $P(x)$ is true for all values of x.

- Here P is a statement (often in English) that mentions x):
    - E.g., $\forall x (x^2 \geq x)$
- Whether $\forall x P(x)$ is true depends on what x ranges over (the *domain*)
    - $\forall x (x^2 \geq x)$ is false if x ranges over the real numbers.
        - $(1/2)^2 < 1/2$
    - It's true if x ranges over the integers.
- To prove it, we consider an arbitrary integer x, and show that $x^2 \geq x$ for that x.
- How do we do that?
- Consider two cases: $x \geq 1$ and $x \leq 0$.

How do we prove $\forall x P(x)$: i.e., that $P(x)$ is true for all values of x.

- Whether $\forall x P(x)$ is true depends on what x ranges over (the *domain*)
  - $\forall x(x^2 \geq x)$ is false if x ranges over the real numbers.
    - $(1/2)^2 < 1/2$
  - It's true if x ranges over the integers.
- To prove it, we consider an arbitrary integer x, and show that $x^2 \geq x$ for that x.
- How do we do that?

How do we prove $\forall x P(x)$: i.e., that $P(x)$ is true for all values of x.

- Whether $\forall x P(x)$ is true depends on what x ranges over (the *domain*)
  - $\forall x(x^2 \geq x)$ is false if x ranges over the real numbers.
    - $(1/2)^2 < 1/2$
  - It's true if x ranges over the integers.
- To prove it, we consider an arbitrary integer x, and show that $x^2 \geq x$ for that x.
- How do we do that?
- Consider two cases: $x \geq 1$ and $x \leq 0$.

How do we prove $\forall x P(x)$: i.e., that $P(x)$ is true for all values of x.

- Whether $\forall x P(x)$ is true depends on what x ranges over (the *domain*)
  - $\forall x(x^2 \geq x)$ is false if x ranges over the real numbers.
    - $(1/2)^2 < 1/2$
  - It's true if x ranges over the integers.
- To prove it, we consider an arbitrary integer x, and show that $x^2 \geq x$ for that x.
- How do we do that?
- Consider two cases: $x \geq 1$ and $x \leq 0$.

How do we show that $\forall x P(x)$ is false?

How do we prove $\forall x P(x)$: i.e., that $P(x)$ is true for all values of x.

- Whether $\forall x P(x)$ is true depends on what x ranges over (the *domain*)
  - $\forall x(x^2 \geq x)$ is false if x ranges over the real numbers.
    - $(1/2)^2 < 1/2$
  - It's true if x ranges over the integers.
- To prove it, we consider an arbitrary integer x, and show that $x^2 \geq x$ for that x.
- How do we do that?
- Consider two cases: $x \geq 1$ and $x \leq 0$.

How do we show that $\forall x P(x)$ is false?

- Find a counterexample!
- E.g., to show that $\forall x(x^2 \geq x)$ is false when x ranges over the real numbers, just point out $(1/2)^2 < 1/2$.

Sets

I'm going to assume that you are familiar with with sets, set builder notation, and basic operations on sets

- $\cup$ (union)
- $\cap$ (intersection)
- $\bar{\ }$ (complementation)

You should read Section 4.1 in the text to review this material!

Sets and Propositions

There's a close connection between set operations and propositional connectives:

- $\cup$ and $\vee$
- $\cap$ and $\wedge$
- $\overline{\ }$ and $\neg$

What's the formal connection?

Sets and Propositions

There's a close connection between set operations and propositional connectives:

- $\cup$ and $\vee$
- $\cap$ and $\wedge$
- $\overline{}$ and $\neg$

What's the formal connection?

- The set of truth assignments that make $\varphi \vee \psi$ true is the union of the set of truth assignments that make φ true and the set that make ψ true.

Sets and Propositions

There's a close connection between set operations and propositional connectives:

- $\cup$ and $\vee$
- $\cap$ and $\wedge$
- $\overline{\ }$ and $\neg$

What's the formal connection?

- The set of truth assignments that make $\varphi \vee \psi$ true is the union of the set of truth assignments that make φ true and the set that make ψ true.
- The set of truth assignments that make $\varphi \wedge \psi$ true is the intersection of the set of truth assignments that make φ true and the set that make ψ true.
- The set of truth assignments that make $\neg\varphi$ true is the complement of the set that make φ true.

Sets and Propositions

There's a close connection between set operations and propositional connectives:

- $\cup$ and $\vee$
- $\cap$ and $\wedge$
- $\overline{\ }$ and $\neg$

What's the formal connection?

- The set of truth assignments that make $\varphi \vee \psi$ true is the union of the set of truth assignments that make φ true and the set that make ψ true.
- The set of truth assignments that make $\varphi \wedge \psi$ true is the intersection of the set of truth assignments that make φ true and the set that make ψ true.
- The set of truth assignments that make $\neg\varphi$ true is the complement of the set that make φ true.

There's also a connection between $\Rightarrow$ and $\subseteq$.

- $\varphi \Rightarrow \psi$ is valid iff the set of truth assignments that make φ true is a subset of the set that makes ψ true. (For homework.)

Proving Set Equality

One way to prove that $A = B$ (where A and B are sets).

- Prove that A and B have the same elements; that is
  - prove $x \in A$ iff $x \in B$.

  This may involve proving $A \subseteq B$ and $B \subseteq A$.
  - This is an analogous to proving $P \Leftrightarrow Q$ by proving $P \Rightarrow Q$ and $Q \Rightarrow P$.

  Similarly, to prove that $A \subseteq B$,
  - prove that $x \in A$ implies $x \in B$.

Sets vs. Sequences

We denote a sequence of objects as (a, b, c)

- the order matters: $(a, b, c) \neq (c, b, a)$
- elements can be repeated: (a, b, a) is a legitimate sequence of length 3.
- By way of contrast, with sets, order doesn't matter
  - $\{a, b, c\} = \{c, b, a\}$

  and we can't repeat elements
  - We don't write $\{a, b, a\}$ or $\{a, a, b\}$; we would just write $\{a, b\}$.
    - However, there is a notion of *multiset* where elements are repeated and the multiplicity matters
    - $\{\{a, a, b\}\}$ is a meaningful multiset

Relations

- **Cartesian product**:
  $S \times T = \{(s,t) : s \in S, t \in T\}$
  - $\{1,2,3\} \times \{3,4\} =$
    $\{(1,3),(2,3),(3,3),(1,4),(2,4),(3,4)\}$
  - $|S \times T| = |S| \times |T|$.
- A *relation* on S and T (or, on $S \times T$) is a subset of $S \times T$
- A *relation* on S is a subset of $S \times S$
  - *Taller than* is a relation on people: (Joe,Sam) is in the Taller than relation if Joe is Taller than Sam
  - *Greater than* is a relation on $\boldsymbol{R}$ (the real numbers):

    $$L = \{(x,y) : x, y \in R, x > y\}$$

  - *Divisibility* is a relation on $\boldsymbol{N}$ (the natural numbers):

    $$D = \{(x,y) : x, y \in \boldsymbol{N}, x|y\}$$

Notation: the book writes $a\,R\,b$ to denote that the pair $(a,b) \in R$. The latter notation is more standard, and that's what I will use.

- You can use either one.

Various Properties of Relations

- A relation R on S is *reflexive* if $(x, x) \in R$ for all $x \in S$.
    - $\leq$ is reflexive; $<$ is not

Various Properties of Relations

- A relation R on S is *reflexive* if $(x, x) \in R$ for all $x \in S$.
  - $\leq$ is reflexive; $<$ is not
- A relation R on S is *irreflexive* if $(x, x) \notin R$ for all $x \in S$.
  - $<$ is irreflexive; $\leq$ is not

Various Properties of Relations

- A relation R on S is *reflexive* if $(x, x) \in R$ for all $x \in S$.
  - $\leq$ is reflexive; $<$ is not
- A relation R on S is *irreflexive* if $(x, x) \notin R$ for all $x \in S$.
  - $<$ is irreflexive; $\leq$ is not
- A relation R on S is *symmetric* if $(x, y) \in R$ implies $(y, x) \in R$.
  - "sibling-of" is symmetric (what about "sister of")
  - $\leq$ is not symmetric

Various Properties of Relations

- A relation R on S is *reflexive* if $(x, x) \in R$ for all $x \in S$.
    - $\leq$ is reflexive; $<$ is not
- A relation R on S is *irreflexive* if $(x, x) \notin R$ for all $x \in S$.
    - $<$ is irreflexive; $\leq$ is not
- A relation R on S is *symmetric* if $(x, y) \in R$ implies $(y, x) \in R$.
    - "sibling-of" is symmetric (what about "sister of")
    - $\leq$ is not symmetric
- A relation R on S is *asymmetric* if $(x, y) \in R$ implies $(y, x) \notin R$.
    - $<$ and $>$ are asymmetric
    - $\leq$ and $\geq$ are not

Various Properties of Relations

- A relation R on S is *reflexive* if $(x, x) \in R$ for all $x \in S$.
  - $\leq$ is reflexive; $<$ is not
- A relation R on S is *irreflexive* if $(x, x) \notin R$ for all $x \in S$.
  - $<$ is irreflexive; $\leq$ is not
- A relation R on S is *symmetric* if $(x, y) \in R$ implies $(y, x) \in R$.
  - "sibling-of" is symmetric (what about "sister of")
  - $\leq$ is not symmetric
- A relation R on S is *asymmetric* if $(x, y) \in R$ implies $(y, x) \notin R$.
  - $<$ and $>$ are asymmetric
  - $\leq$ and $\geq$ are not
- A relation R on S is *antisymmetric* if $(x, y) \in R$ and $x \neq y$ implies $(y, x) \notin R$.
  - $\leq$ and $\geq$ are antisymmetric

Various Properties of Relations

- A relation R on S is *reflexive* if $(x, x) \in R$ for all $x \in S$.
    - $\leq$ is reflexive; $<$ is not
- A relation R on S is *irreflexive* if $(x, x) \notin R$ for all $x \in S$.
    - $<$ is irreflexive; $\leq$ is not
- A relation R on S is *symmetric* if $(x, y) \in R$ implies $(y, x) \in R$.
    - "sibling-of" is symmetric (what about "sister of")
    - $\leq$ is not symmetric
- A relation R on S is *asymmetric* if $(x, y) \in R$ implies $(y, x) \notin R$.
    - $<$ and $>$ are asymmetric
    - $\leq$ and $\geq$ are not
- A relation R on S is *antisymmetric* if $(x, y) \in R$ and $x \neq y$ implies $(y, x) \notin R$.
    - $\leq$ and $\geq$ are antisymmetric
- A relation R on S is *transitive* if $(x, y) \in R$ and $(y, z) \in R$ implies $(x, z) \in R$.
    - $\leq$, $<$, $\geq$, $>$ are all transitive;
    - "parent-of" is not transitive; "ancestor-of" is

Equivalence Relations

- A relation R is an *equivalence relation* if it is reflexive, symmetric, and transitive
  - $=$ is an equivalence relation
  - *Parity* is an equivalence relation on $\boldsymbol{N}$;
    $(x, y) \in \mathit{Parity}$ if $x - y$ is even

Equivalence Relations

- A relation R is an *equivalence relation* if it is reflexive, symmetric, and transitive
  - $=$ is an equivalence relation
  - *Parity* is an equivalence relation on $\boldsymbol{N}$; $(x, y) \in \mathit{Parity}$ if $x - y$ is even

An equivalence relation on S partitions S into *equivalence classes*:

- The equivalence class of s is denoted $[s]$.
  - $[s] = \{t : (s, t) \in R\}$

Theorem: Equivalences classes are either equal or disjoint: for all $s, s' \in S$, either $[s] = [s']$ or $[s] \cap [t] = \emptyset$.

Equivalence Relations

- A relation R is an *equivalence relation* if it is reflexive, symmetric, and transitive
  - $=$ is an equivalence relation
  - *Parity* is an equivalence relation on $\boldsymbol{N}$; $(x, y) \in \mathit{Parity}$ if $x - y$ is even

An equivalence relation on S partitions S into *equivalence classes*:

- The equivalence class of s is denoted $[s]$.
  - $[s] = \{t : (s, t) \in R\}$

Theorem: Equivalences classes are either equal or disjoint: for all $s, s' \in S$, either $[s] = [s']$ or $[s] \cap [t] = \emptyset$.

- What are the equivalence classes of the parity relation?

Transitive Closure

The *transitive closure* of a relation R is the least relation R^* such that

1. $R \subseteq R^*$
2. R^* is transitive (so that if $(u, v), (v, w) \in R^*$, then so is (u, w)).

Transitive Closure

The *transitive closure* of a relation R is the least relation R^* such that

1. $R \subseteq R^*$
2. R^* is transitive (so that if $(u, v), (v, w) \in R^*$, then so is (u, w)).

How do we know that there is a least relation R^* with these properties:

- "least" means that R^* must be a subset of any other relation with these properties;
- that is, if there is a relation R' such that that $R \subseteq R'$ and R' is transitive, then $R^* \subseteq R'$.

Transitive Closure

The *transitive closure* of a relation R is the least relation R^* such that

1. $R \subseteq R^*$
2. R^* is transitive (so that if $(u, v), (v, w) \in R^*$, then so is (u, w)).

How do we know that there is a least relation R^* with these properties:

- "least" means that R^* must be a subset of any other relation with these properties;
- that is, if there is a relation R' such that that $R \subseteq R'$ and R' is transitive, then $R^* \subseteq R'$.

Take R^* to be the intersection of all the transitive relations that contain R.

- We must check that the intersection contains R and is transitive.

Clearly R^* is a subset of any transtive relation R' that contains R.

Transitive Closure

The *transitive closure* of a relation R is the least relation R^* such that

1. $R \subseteq R^*$
2. R^* is transitive (so that if $(u, v), (v, w) \in R^*$, then so is (u, w)).

How do we know that there is a least relation R^* with these properties:

- "least" means that R^* must be a subset of any other relation with these properties;
- that is, if there is a relation R' such that that $R \subseteq R'$ and R' is transitive, then $R^* \subseteq R'$.

Take R^* to be the intersection of all the transitive relations that contain R.

- We must check that the intersection contains R and is transitive.

Clearly R^* is a subset of any transtive relation R' that contains R.

Example: Suppose $R = \{(1,2),(2,3),(1,4)\}$.

- $R^* = \{(1,2),(1,3),(2,3),(1,4)\}$
- we need to add $(1,3)$, because $(1,2),(2,3) \in R$

Note that we don't need to add (2,4).

- If (2,1), (1,4) were in R, then we'd need (2,4)
- (1,2), (1,4) doesn't force us to add anything (it doesn't fit the "pattern" of transitivity.

Note that if R is already transitive, then $R^* = R$.

Composing and Inverting Relations

If R is a relation on $A \times B$, then R^{-1} is a relation on $B \times A$:

$$(a, b) \in R \text{ iff } (b, a) \in R^{-1}.$$

Composing and Inverting Relations

If R is a relation on $A \times B$, then R^{-1} is a relation on $B \times A$:

$$(a, b) \in R \text{ iff } (b, a) \in R^{-1}.$$

If R is a relation on $B \times C$ and S is a relation on $A \times B$, then $R \circ S$ is a relation on $A \times C$:

$$(a, c) \in R \circ S \text{ iff } \exists b((a, b) \in S \text{ and } (b, c) \in R.$$

- Note the order of R and S on the right-hand side
- This is not a typo!

Composing and Inverting Relations

If R is a relation on $A \times B$, then R^{-1} is a relation on $B \times A$:

$$(a, b) \in R \text{ iff } (b, a) \in R^{-1}.$$

If R is a relation on $B \times C$ and S is a relation on $A \times B$, then $R \circ S$ is a relation on $A \times C$:

$$(a, c) \in R \circ S \text{ iff } \exists b((a, b) \in S \text{ and } (b, c) \in R.$$

- Note the order of R and S on the right-hand side
- This is not a typo!

Example: If $R = \{(n, n+1) : n \in \boldsymbol{N}\}$, then what's $R \circ R$?

Composing and Inverting Relations

If R is a relation on $A \times B$, then R^{-1} is a relation on $B \times A$:

$$(a, b) \in R \text{ iff } (b, a) \in R^{-1}.$$

If R is a relation on $B \times C$ and S is a relation on $A \times B$, then $R \circ S$ is a relation on $A \times C$:

$$(a, c) \in R \circ S \text{ iff } \exists b((a, b) \in S \text{ and } (b, c) \in R.$$

- Note the order of R and S on the right-hand side
- This is not a typo!

Example: If $R = \{(n, n+1) : n \in \boldsymbol{N}\}$, then what's $R \circ R$?

- $R \circ R = \{(n, n+2) : n \in \boldsymbol{N}\}$.
- How do you prove this?

Recall that $R = \{(n, n+1) : n \in \boldsymbol{N}\}$. Let $S = \{(n, n+2) : n \in \boldsymbol{N}\}$. We want to show $R \circ R = S$. One way to show that $A = B$ is to show that $A \subseteq B$ and $B \subseteq A$. That's what I'll do:

Recall that $R = \{(n, n+1) : n \in \mathbb{N}\}$. Let $S = \{(n, n+2) : n \in \mathbb{N}\}$. We want to show $R \circ R = S$. One way to show that $A = B$ is to show that $A \subseteq B$ and $B \subseteq A$. That's what I'll do:

- Suppose that $x \in S$. Then $x = (n, n+2)$ for some n.
- Note that $(n, n+1) \in R$ and $(n+1, n+2) \in R$.
- Thus, by definition $(n, n+2) \in R \circ R$; that is, $x \in R \circ R$.

This shows that $S \subseteq R \circ R$.

Recall that $R = \{(n, n+1) : n \in \mathbb{N}\}$. Let $S = \{(n, n+2) : n \in \mathbb{N}\}$. We want to show $R \circ R = S$. One way to show that $A = B$ is to show that $A \subseteq B$ and $B \subseteq A$. That's what I'll do:

- Suppose that $x \in S$. Then $x = (n, n+2)$ for some n.
- Note that $(n, n+1) \in R$ and $(n+1, n+2) \in R$.
- Thus, by definition $(n, n+2) \in R \circ R$; that is, $x \in R \circ R$.

This shows that $S \subseteq R \circ R$.

The other direction works essentially the same way:

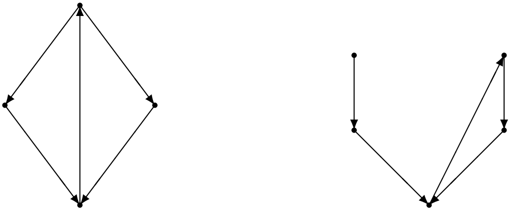
- Suppose that $(a, c) \in R \circ R$.
- Then (by definition), there is a b such that $(a, b) \in R$ and $(b, c) \in R$.
- Thus, $b = a + 1$ and $c = b + 1 = a + 2$.
- Thus $(a, c) = (a, a+2) \in S$.

This shows that $R \circ R \subseteq S$.

Graphs

A *graph* consists of nodes and edges between nodes.

A *directed graph* (*digraph*) is one where the edges have a direction, usually denoted with an arrow.



Graphs come up everywhere.

- We can view the internet as a graph (in many ways)
  - who is connected to whom
- Web search views web pages as a graph
  - who points to whom
- Niche graphs (Ecology):
  - The vertices are species
  - Two vertices are connected by an edge if they compete (use the same food resources, etc.)

  Niche graphs give a visual representation of competitiveness.
- Influence Graphs
  - The vertices are people
  - There is an edge from a to b if a influences b

  Influence graphs give a visual representation of power structure.

There are lots of other examples in all fields . . .

Terminology and Notation

An *undirected graph* G is a pair (V, E), where V is a set of *vertices* or *nodes* and E is a set of *edges* or *branches*; an edge is a set $\{v, v'\}$ of two not necessarily distinct vertices (i.e., $v, v' \in V$).

- We sometimes write $G(V, E)$ instead of G
- We sometimes write $V(G)$ and $E(G)$ if we want to emphasize the graph that the vertices and edges come from.

Terminology and Notation

An *undirected graph* G is a pair (V, E), where V is a set of *vertices* or *nodes* and E is a set of *edges* or *branches*; an edge is a set $\{v, v'\}$ of two not necessarily distinct vertices (i.e., $v, v' \in V$).

- We sometimes write $G(V, E)$ instead of G
- We sometimes write $V(G)$ and $E(G)$ if we want to emphasize the graph that the vertices and edges come from.

A *digraph* is a pair (V, E) where E is a set of *directed edges*

- A directed edge is a pair (v, v'), where $v, v' \in G$
- The order matters!

Terminology and Notation

An *undirected graph* G is a pair (V, E), where V is a set of *vertices* or *nodes* and E is a set of *edges* or *branches*; an edge is a set $\{v, v'\}$ of two not necessarily distinct vertices (i.e., $v, v' \in V$).

- We sometimes write $G(V, E)$ instead of G
- We sometimes write $V(G)$ and $E(G)$ if we want to emphasize the graph that the vertices and edges come from.

A *digraph* is a pair (V, E) where E is a set of *directed edges*

- A directed edge is a pair (v, v'), where $v, v' \in G$
- The order matters!
- A *walk* in a graph G is an alternating sequence of vertices and edges, starting and ending with a vertex, where, for every edge (u, v) on the walk, u is the preceding vertex and v is the following vertex.

Terminology and Notation

An *undirected graph* G is a pair (V, E), where V is a set of *vertices* or *nodes* and E is a set of *edges* or *branches*; an edge is a set $\{v, v'\}$ of two not necessarily distinct vertices (i.e., $v, v' \in V$).

- We sometimes write $G(V, E)$ instead of G
- We sometimes write $V(G)$ and $E(G)$ if we want to emphasize the graph that the vertices and edges come from.

A *digraph* is a pair (V, E) where E is a set of *directed edges*

- A directed edge is a pair (v, v'), where $v, v' \in G$
- The order matters!
- A *walk* in a graph G is an alternating sequence of vertices and edges, starting and ending with a vertex, where, for every edge (u, v) on the walk, u is the preceding vertex and v is the following vertex.
  - E.g., 1 (1,3), 3, (3,8), 8

Terminology and Notation

An *undirected graph* G is a pair (V, E), where V is a set of *vertices* or *nodes* and E is a set of *edges* or *branches*; an edge is a set $\{v, v'\}$ of two not necessarily distinct vertices (i.e., $v, v' \in V$).

- We sometimes write $G(V, E)$ instead of G
- We sometimes write $V(G)$ and $E(G)$ if we want to emphasize the graph that the vertices and edges come from.

A *digraph* is a pair (V, E) where E is a set of *directed edges*

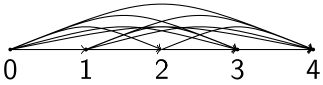
- A directed edge is a pair (v, v'), where $v, v' \in G$
- The order matters!
- A *walk* in a graph G is an alternating sequence of vertices and edges, starting and ending with a vertex, where, for every edge (u, v) on the walk, u is the preceding vertex and v is the following vertex.
    - E.g., 1 (1,3), 3, (3,8), 8
    - Yuck! (The vertices are redundant)
        - It's more standard to leave them out; the text includes them
- A *path* is a walk where all the vertices are different
- A cycle is a walk where all vertices are distinct except for the first and last one

Graphs and Relations

Given a relation R on $S \times T$, we can represent it by the directed graph $G(V, E)$, where

- $V = S \cup T$ and
- $E = \{(s, t) : (s, t) \in R\}$

Example: We can represent the $<$ relation on $\{0, 1, 2, 3, 4\}$ graphically.



How does the graphical representation show that a graph is

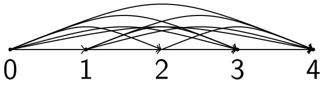
- reflexive?

Graphs and Relations

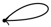
Given a relation R on $S \times T$, we can represent it by the directed graph $G(V, E)$, where

- $V = S \cup T$ and
- $E = \{(s, t) : (s, t) \in R\}$

Example: We can represent the $<$ relation on $\{0, 1, 2, 3, 4\}$ graphically.



How does the graphical representation show that a graph is

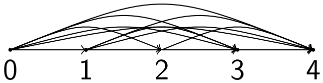
- reflexive? 

Graphs and Relations

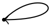
Given a relation R on $S \times T$, we can represent it by the directed graph $G(V, E)$, where

- $V = S \cup T$ and
- $E = \{(s, t) : (s, t) \in R\}$

Example: We can represent the $<$ relation on $\{0, 1, 2, 3, 4\}$ graphically.



How does the graphical representation show that a graph is

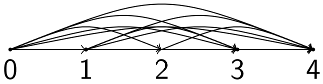
- reflexive? 
- symmetric?

Graphs and Relations

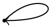
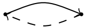
Given a relation R on $S \times T$, we can represent it by the directed graph $G(V, E)$, where

- $V = S \cup T$ and
- $E = \{(s, t) : (s, t) \in R\}$

Example: We can represent the $<$ relation on $\{0, 1, 2, 3, 4\}$ graphically.



How does the graphical representation show that a graph is

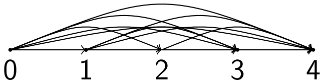
- reflexive? 
- symmetric? 

Graphs and Relations

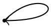
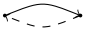
Given a relation R on $S \times T$, we can represent it by the directed graph $G(V, E)$, where

- $V = S \cup T$ and
- $E = \{(s,t) : (s,t) \in R\}$

Example: We can represent the $<$ relation on $\{0, 1, 2, 3, 4\}$ graphically.



How does the graphical representation show that a graph is

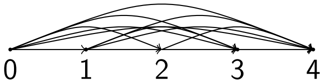
- reflexive? 
- symmetric? 
- transitive?

Graphs and Relations

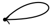
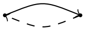
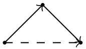
Given a relation R on $S \times T$, we can represent it by the directed graph $G(V, E)$, where

- $V = S \cup T$ and
- $E = \{(s, t) : (s, t) \in R\}$

Example: We can represent the $<$ relation on $\{0, 1, 2, 3, 4\}$ graphically.



How does the graphical representation show that a graph is

- reflexive? 
- symmetric? 
- transitive? 

Partial Orders

A relation is *strict partial order* if it is irreflexive and transitive.

- $<$ and $>$ are strict partial orders

A relation is *weak partial order* if it is reflexive, transitive, and antisymmetric

- $\leq$ and $\geq$ are weak partial orders

Functions

We think of a function $f : S \rightarrow T$ as providing a mapping from S to T. But ...

Formally, a *function* is a relation R on $S \times T$ such that for each $s \in S$, there is a unique $t \in T$ such that $(s, t) \in R$.

If $f : S \rightarrow T$, then S is the *domain* of f, T is the *codomain*; $\{y : f(x) = y \text{ for some } x \in S\}$ is the *range* or *image*.

Notation: S^T denotes the set of functions with domain T and range S.

- There's a reason that we use this "exponent" notation.
- We'll soon show that $|S^T| = |S|^{|T|}$

We often think of a function as being characterized by an algebraic formula

- $y = 3x - 2$ characterizes $f(x) = 3x - 2$.

It ain't necessarily so.

- Some formulas don't characterize functions:
  - $x^2 + y^2 = 1$ defines a circle; no unique y for each x
- Some functions can't be characterized by algebraic formulas
  - $f(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$

Function Terminology

Suppose $f : S \to T$

- f is *onto* (or *surjective*) if, for each $t \in T$, there is some $s \in S$ such that $f(s) = t$.
  - if $f : R^+ \to R^+$, $f(x) = x^2$, then f is onto
  - if $f : R \to R$, $f(x) = x^2$, then f is *not* onto
- f is *one-to-one* (1-1, *injective*) if it is not the case that $s \neq s'$ and $f(s) = f(s')$.
  - if $f : R^+ \to R^+$, $f(x) = x^2$, then f is 1-1
  - if $f : R \to R$, $f(x) = x^2$, then f is *not* 1-1.
- a function is *bijective* if it is 1-1 and onto.
  - if $f : R^+ \to R^+$, $f(x) = x^2$, then f is bijective
  - if $f : R \to R$, $f(x) = x^2$, then f is *not* bijective.

Inverse Functions

If $f : S \to T$, then f is *invertible* if there exists a function $g : T \to S$ such that

$$f(s) = t \text{ iff } g(t) = s.$$

- If f is invertible, then g is called the *inverse* of f
  - We usually denote the inverse of f as f^{-1}
- If f is invertible, then
  - for all $s \in S$, $(f^{-1} \circ f)(s) = s$
  - for all $t \in T$, $(f \circ f^{-1})(t) = t$
- If $(g \circ f)(s) = s$ for all $s \in S$, then g is a *left inverse* of f
- If $(f \circ g)(t) = t$ for all $t \in T$, then g is a *right inverse* of f

Inverse Functions

If $f : S \to T$, then f is *invertible* if there exists a function $g : T \to S$ such that

$$f(s) = t \text{ iff } g(t) = s.$$

- If f is invertible, then g is called the *inverse* of f
  - We usually denote the inverse of f as f^{-1}
- If f is invertible, then
  - for all $s \in S$, $(f^{-1} \circ f)(s) = s$
  - for all $t \in T$, $(f \circ f^{-1})(t) = t$
- If $(g \circ f)(s) = s$ for all $s \in S$, then g is a *left inverse* of f
- If $(f \circ g)(t) = t$ for all $t \in T$, then g is a *right inverse* of f
- **Theorem:** f is injective iff it has a left inverse.
- **Theorem:** f is surjective iff it has a right inverse.
- **Theorem:** f is a bijection iff it is invertible.

If f is not invertible, we still often abuse notation and view f^{-1} as a relation, taking

$$f^{-1}(s) = \{t : f(s) = t\}.$$

Cardinality

The cardinality of a finite set S, denoted $|S|$, is the number of element in S:

- $|\{1, 2, 7\}| = 3$

Cardinality

The cardinality of a finite set S, denoted $|S|$, is the number of element in S:

- $|\{1, 2, 7\}| = 3$

Theorem: If S and T are finite sets then:

(a) There is an injection from S to T iff $|S| \leq |T|$;

(b) There is a surjection from S to T iff $|S| \geq |T|$;

(c) There is a bijection from S to T iff $|S| = |T|$.

For these proofs, it is convenient that we can count the elements of a finite set and list them in the order that we count them.

Cardinality of Infinite Sets

What about infinite sets?

- How does the number of natural numbers compare to the number of even numbers?
  - (a) more
  - (b) less
  - (c) the same

Cardinality of Infinite Sets

What about infinite sets?

- How does the number of natural numbers compare to the number of even numbers?
  (a) more
  (b) less
  (c) the same
- Natural numbers vs. integers?
  (a) more
  (b) less
  (c) the same

Cardinality of Infinite Sets

What about infinite sets?

- How does the number of natural numbers compare to the number of even numbers?
  (a) more
  (b) less
  (c) the same
- Natural numbers vs. integers?
  (a) more
  (b) less
  (c) the same
- Natural numbers vs. rational numbers?
  (a) more
  (b) less
  (c) the same

Cardinality of Infinite Sets

What about infinite sets?

- How does the number of natural numbers compare to the number of even numbers?
  (a) more
  (b) less
  (c) the same
- Natural numbers vs. integers?
  (a) more
  (b) less
  (c) the same
- Natural numbers vs. rational numbers?
  (a) more
  (b) less
  (c) the same
- Rational numbers vs. irrational numbers?
  (a) more
  (b) less
  (c) the same

To answer these questions, we need some way to compare the sizes of infinite sets.

To answer these questions, we need some way to compare the sizes of infinite sets.

Idea: (Georg Cantor) use the characterization for finite sets as the definition:

Definition: $|S| \leq |T|$ if there is an injection from S to T

- For homework: there is an injection from S to T iff there is a surjection from T to S.

$|S| = |T|$ if there is a bijection from S to T.

- S and T have the same cardinality if you can match up their elements

To answer these questions, we need some way to compare the sizes of infinite sets.

Idea: (Georg Cantor) use the characterization for finite sets as the definition:

Definition: $|S| \leq |T|$ if there is an injection from S to T

- For homework: there is an injection from S to T iff there is a surjection from T to S.

$|S| = |T|$ if there is a bijection from S to T.

- S and T have the same cardinality if you can match up their elements

For this to be reasonable, we would expect that if $|S| \leq |T|$ and $|T| \leq |S|$, then $|S| = |T|$.

- That is, if there's an injection from S to T and an injection from T to S, then there's a bijection from S to T.
- This is true, but it's not obvious!

Theorem: [Schröder-Bernstein] If $|S| \leq |T|$ and $|T| \leq |S|$ iff $|S| = |T|$.

Proof coming soon.

Countable sets

Definition: If there is a bijection between $\mathbb{N}$ and S, then S is *countable*.

- The formal definition of countable is that a set S is countable iff there's an *injection* from S to $\mathbb{N}$. That means that finite sets are also countable.
    - After all, you can count them.
    - If there's a bijection from S to $\mathbb{N}$, then S is *countably infinite*.
- A bijection $f : \mathbb{N} \rightarrow S$ tells you how to count the elements of S.
    - $f(1)$ is the first element of S, $f(2)$ is the second element, ...

Theorem: The following sets are countable:

- The even numbers
- The multiples of three
- The integers
- $\mathbb{N} \times \mathbb{N}$
- The rational numbers

Diagonalization

So are all infinite sets countable?

Theorem: [Cantor] For all sets S, $|\mathcal{P}(S)| > |S|$.

- Recall: $\mathcal{P}(S)$, the *power set* of S, consists of all subsets of S
  - $\mathcal{P}(S)$ is sometimes denoted 2^S, for reasons that will become clearer when we do combinatorics.
  - The text writes pos(S) (which is quite nonstandard!)

Proof: There's an injection from S to $\mathcal{P}(S)$:

Diagonalization

So are all infinite sets countable?

Theorem: [Cantor] For all sets S, $|\mathcal{P}(S)| > |S|$.

- Recall: $\mathcal{P}(S)$, the *power set* of S, consists of all subsets of S
  - $\mathcal{P}(S)$ is sometimes denoted 2^S, for reasons that will become clearer when we do combinatorics.
  - The text writes pos(S) (which is quite nonstandard!)

Proof: There's an injection from S to $\mathcal{P}(S)$:

- $s \to \{s\}$

Diagonalization

So are all infinite sets countable?

Theorem: [Cantor] For all sets S, $|\mathcal{P}(S)| > |S|$.

- Recall: $\mathcal{P}(S)$, the *power set* of S, consists of all subsets of S
  - $\mathcal{P}(S)$ is sometimes denoted 2^S, for reasons that will become clearer when we do combinatorics.
  - The text writes pos(S) (which is quite nonstandard!)

Proof: There's an injection from S to $\mathcal{P}(S)$:

- $s \rightarrow \{s\}$

Now we have to show that there is no surjection from S to $\mathcal{P}(S)$.

Diagonalization

So are all infinite sets countable?
Theorem: [Cantor] For all sets S, $|\mathcal{P}(S)| > |S|$.

- Recall: $\mathcal{P}(S)$, the *power set* of S, consists of all subsets of S
  - $\mathcal{P}(S)$ is sometimes denoted 2^S, for reasons that will become clearer when we do combinatorics.
  - The text writes pos(S) (which is quite nonstandard!)

Proof: There's an injection from S to $\mathcal{P}(S)$:

- $s \rightarrow \{s\}$

Now we have to show that there is no surjection from S to $\mathcal{P}(S)$.
How are we going to do that?

- It's not enough to show that any specific function is not a surjection.
  - We have to show that there are no surjections.

We do a proof by contradiction. Suppose that $f : S \to \mathcal{P}(S)$. I will show that f is not a surjection by constructing a set A such that $f(s) \neq A$ for all $s \in S$.
Here's how A is defined:

- $s \in A$ iff $s \notin f(s)$.

We do a proof by contradiction. Suppose that $f : S \to \mathcal{P}(S)$. I will show that f is not a surjection by constructing a set A such that $f(s) \neq A$ for all $s \in S$.
Here's how A is defined:

- $s \in A$ iff $s \notin f(s)$.

Suppose that there is some s_0 such that $f(s_0) = A$.
Is $s_0 \in A$?

- If $s_0 \in A$, then $s_0 \in f(s_0)$ (because $f(s_0) = A$), but then $s_0 \notin A$ (by definition of A) - contradiction!
- If $s_0 \notin A$, then $s_0 \notin f(s_0)$, so $s_0 \in A$!

Bottom line: $s_0 \in A$ iff $s_0 \notin A$ - contradiction!
Conclusion: There is no s_0 such that $f(s_0) = A$. So there is no surjection from S to $\mathcal{P}(S)$. ∎

Why is this called a diagonalization? Consider the special case where $S = \boldsymbol{N}$:

- We can construct a matrix of 0s and 1s, where the *ij*th entry is 1 iff $j \in f(i)$.
- We can then construct a new set by flipping the elements of the diagonal: $A = \{i : i \notin f(i)\}$.
    - (This should make more sense when I discuss it in class and draw a picture.)

R is uncountable

Theorem: $\boldsymbol{R}$ is uncountable.

Proof: I'll show that $[0,1) = \{x \in \boldsymbol{R} : 0 \leq x < 1\}$ is uncountable.

Recall that a real number between 0 and 1 can be written as an infinite decimal:

$$0.x_0x_1x_2\ldots$$

Suppose, by way of contradiction, that $f : \boldsymbol{N} \to [0,1)$ is a surjection. I'll construct $x \in [0,1)$ that's not in the range of f. Define $x = .x_0x_1x_2\ldots$ as follows:

- To compute x_k, we consider $f(k)$.
  - $f(k) \in [0,1)$, so $f(k) = .y_0y_1y_2\ldots$
  - If $y_k = 0$, then $x_k = 1$; if $y_k \neq 0$, then $x_k = 0$.
  - **Bottom line:** $x_k \neq y_k$.

Claim: $x = .x_0x_1x_2\ldots$ is not in the range of f.

- The kth digit of x differs from the kth digit of $f(k)$, so $x \neq f(k)$.

$\boldsymbol{R}$ is uncountable

Theorem: $\boldsymbol{R}$ is uncountable.

Proof: I'll show that $[0,1) = \{x \in \boldsymbol{R} : 0 \leq x < 1\}$ is uncountable.

Recall that a real number between 0 and 1 can be written as an infinite decimal:

$$0.x_0x_1x_2\ldots$$

Suppose, by way of contradiction, that $f : \boldsymbol{N} \rightarrow [0,1)$ is a surjection. I'll construct $x \in [0,1)$ that's not in the range of f. Define $x = .x_0x_1x_2\ldots$ as follows:

- To compute x_k, we consider $f(k)$.
  - $f(k) \in [0,1)$, so $f(k) = .y_0y_1y_2\ldots$
  - If $y_k = 0$, then $x_k = 1$; if $y_k \neq 0$, then $x_k = 0$.
  - **Bottom line:** $x_k \neq y_k$.

Claim: $x = .x_0x_1x_2\ldots$ is not in the range of f.

- The kth digit of x differs from the kth digit of $f(k)$, so $x \neq f(k)$.
- E.g., $x \neq f(7)$, because if $f(7) = .y_0y_1...$, then $x_7 \neq y_7$.

Thus, $|\boldsymbol{N}| < |\boldsymbol{R}|$. ▮

Proof of Schröder-Bernstein

Theorem: [Schröder-Bernstein] If $|S| \leq |T|$ and $|T| \leq |S|$ iff $|S| = |T|$.

- In words: There is an injection from S to T and an injection from T to S iff there is a bijection from S to T.

Proof: Clearly if $|S| = |T|$ then $|S| \leq |T|$ and $|T| \leq |S|$. If f is a bijection from S to T, then there is an injection from S to T (f itself) and an injection from T to S:

Proof of Schröder-Bernstein

Theorem: [Schröder-Bernstein] If $|S| \leq |T|$ and $|T| \leq |S|$ iff $|S| = |T|$.

- In words: There is an injection from S to T and an injection from T to S iff there is a bijection from S to T.

Proof: Clearly if $|S| = |T|$ then $|S| \leq |T|$ and $|T| \leq |S|$. If f is a bijection from S to T, then there is an injection from S to T (f itself) and an injection from T to S: f^{-1}.

Now the hard part: Suppose that there is an injection $f : S \rightarrow T$ and an injection $g : T \rightarrow S$. We want to construct a bijection $h : S \rightarrow T$.

For simplicity, assume that S and T are disjoint ($S \cap T = \emptyset$).

- Can always rename the elements of T to ensure this.
  - Renaming is a bijection

Consider chains of elements alternating between elements of S and elements of G, where if $s \in S$ is on the chain and $t \in T$ is the next element, then $f(s) = t$; if u is the element after t, then $g(t) = u$.

$$\cdots \xrightarrow{g} s \xrightarrow{f} t \xrightarrow{g} s' \cdots$$

Because f and g are injections, there's a unique way to extend these chains both forwards and backwards as much as possible.
Claim 1: There are four possibilities for the chain:

Consider chains of elements alternating between elements of S and elements of G, where if $s \in S$ is on the chain and $t \in T$ is the next element, then $f(s) = t$; if u is the element after t, then $g(t) = u$.

$$\cdots \xrightarrow{g} s \xrightarrow{f} t \xrightarrow{g} s' \cdots$$

Because f and g are injections, there's a unique way to extend these chains both forwards and backwards as much as possible.

Claim 1: There are four possibilities for the chain:

- It is infinite in both the forward and backward directions
- It is a loop
- It is infinite in the forward direction and starts with an element of S
- It is infinite in the forward direction and starts with an element of T

Claim 2: The chains partition the elements of $S \cup T$:

- The chains are disjoint
- Every element is on some chain.

We can define a bijection $h : S \to T$ by defining it on each chain individually:

- For every chain except the last type, define $h = f$
- For the last type, define $h = g^{-1}$.

This gives a bijection! ∎

The Continuum Hypothesis

It's not hard to show that $\boldsymbol{N}$ is the smallest infinite set

- For all infinite sets A, there is an injection from $\boldsymbol{N}$ to A

The Continuum Hypothesis

It's not hard to show that $\boldsymbol{N}$ is the smallest infinite set

- For all infinite sets A, there is an injection from $\boldsymbol{N}$ to A

We know that $|\boldsymbol{N}| < |\mathcal{P}(\boldsymbol{N})| = |\boldsymbol{R}|$.

- Is there an infinite set X whose cardinality is between that of $\boldsymbol{N}$ and $\boldsymbol{R}$?
- Cantor conjectured that there wasn't.
  - This conjecture became known as the *continuum hypothesis*.
- You can't prove or disprove the continuum hypothesis using the standard axioms of mathematics.
  - That fact has been proved.
  - It follows from work of Kurt Gödel and Paul Cohen