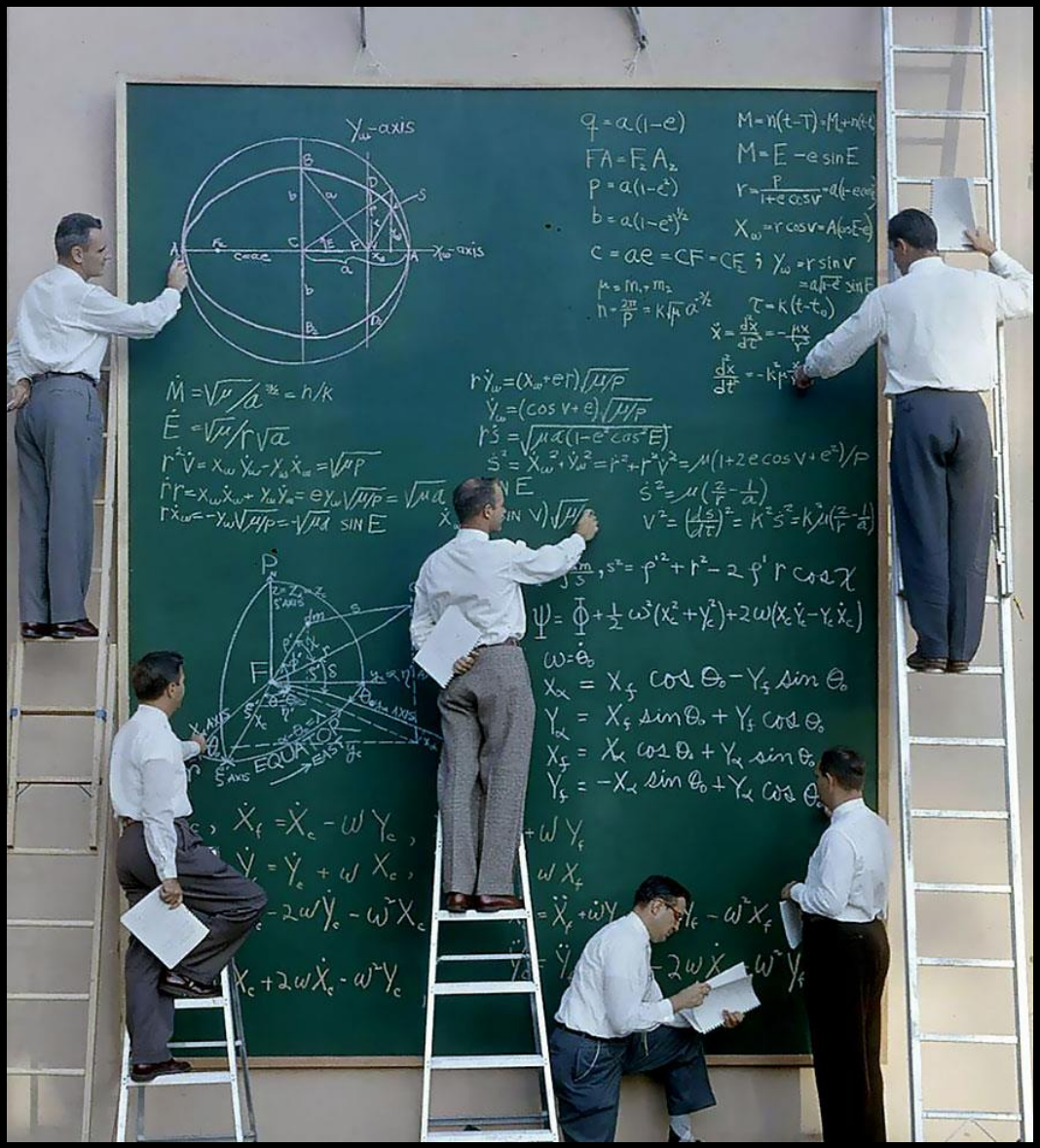


Preliminaries for the Theory of Computation

Contents

- Automata, Computability, and Complexity
- Sets and Elementary Set Theory
- Sequences and Tuples
- Functions
- Graphs
- Strings and Languages
- Boolean Logic
- Logic, Conditionals and Valid Arguments
- Proof Techniques: Direct Proof, Contrapositive, Proof by Cases, Contradiction, Induction
- Cantor's Methods: Infinities and Diagonalization

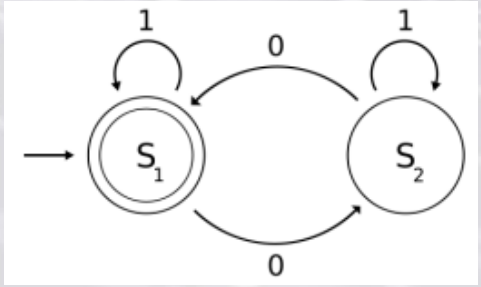
Automata, Computability, and Complexity

• The Theory of Computation encompasses (3) central domains of study: *Automata*, *Computability,* and *Complexity*.

Automata Theory

• Automata theory deals with properties of hierarchically related abstract models of computation. These models play key roles in several applied areas of computer science, including text and natural language processing, compilers, hardware design, programming languages and artificial intelligence.

• Classic models falling under the umbrella of automata theory include: **deterministic finite state automata**, **non-deterministic finite state automata**, **pushdown automata**, and **context-free grammars**.



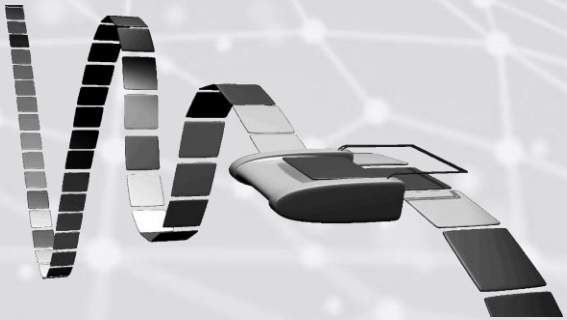
Automata, Computability, and Complexity

• The Theory of Computation encompasses (3) central domains of study: *Automata*, *Computability,* and *Complexity*.

Computability Theory

• Computability theory centers around the fundamental question: *What is (and isn't) computable*? The fact that some problems defy solution by any computer (now or in the future!) is a profound idea. The historical codification of theoretical models of computation – particularly the Turing machine – led, somewhat paradoxically, to the invention of physically realizable computers.

• The pinnacle of computability theory is the **Church-Turing Thesis** which asserts the equivalence of "effectively calculable" algorithms (i.e. paper-and-pencil methods) with algorithms that run on Turing Machines.



Automata, Computability, and Complexity

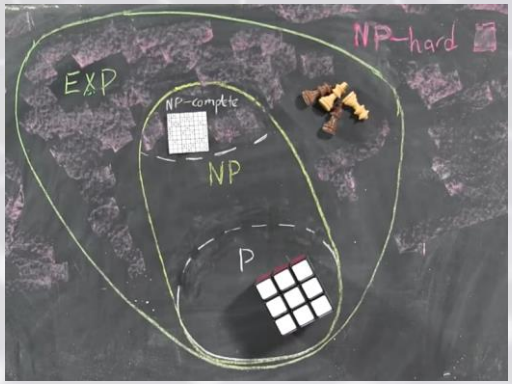
• The Theory of Computation encompasses (3) central domains of study: *Automata*, *Computability,* and *Complexity*.

(Computational) Complexity Theory

• Complexity Theory pertains to classifying computational problems according to their inherent difficulty, and relating these classes to one another.

• Computational complexity theory formalizes this intuition by quantifying the amount of resources required by models of computation needed to solve a given problem, such as time and storage. introducing mathematical models of computation. A problem is regarded as inherently difficult if its solution requires significant resources, whatever the algorithm used.

• The greatest unsolved problem in theoretical computer: **P vs. NP** asks whether every problem whose solution can be "efficiently" verified can be "efficiently" solved.



Sets

• A **set** is a group of objects represented as a unit. Sets may contain any type of object, including numbers, symbols and even other sets.

• The object in a set are called its **elements** or **members**.

• Sets may be described in several ways:

Set notation – in which the elements of the set are listed, separated by commas: $A = \{1,2,3\}$.

Set-builder notation – in which we describe how to "build" elements of the set: $A = \{x | 0 < x < 1\}$.

Sets

• **Membership** in a set is denoted: $1 \in \{1,2,3\}, 14 \notin \{1,2,3\}$.

• For two sets, we say ***A* is a subset of *B***, written $A \subseteq B$ if every member of A is also a member of B. We say that **A is a proper subset of B**, written $A \subsetneq B$ if A is a subset of B – but A is not equal to B.

• To prove that two sets are equal $(A = B)$, we prove both properties: $A \subseteq B$ and $B \subseteq A$.

• The **order** or **cardinality** of a set connotes the size of the set and is written $|A|$. For finite sets, the order of the set is equal to the number of elements contained in the set, e.g., $|\{a, b, c, d\}| = 4$. An infinite set contains infinitely-many elements.

• The set consisting of no elements is called the **empty set**, written: $\emptyset$; note that $\{\emptyset\} \neq \emptyset$. Note that for all sets A, $\emptyset \subseteq A$ holds.

Sets

• The **natural numbers** (or "counting numbers") are defined as the infinite array of non-negative integers:

$$\mathbb{N} = \{1,2,3, \dots\}$$

• The **set of integers** is defined as the doubly-infinite array:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

• The set of all **rational numbers** (i.e. fractions) is defined:

$$\mathbb{Q} = \left\{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\right\}$$

• The **set of all reals** $\mathbb{R}$ forms a continuum and is defined as the union (see below) of $\mathbb{Q}$ with the set of irrational numbers (i.e. numbers with non-terminating, non-repeating decimal expansions).

• Notice that: $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$.

Sets

• As with sets, sequences may be finite or infinite. Finite sequences are often called **tuples**; a sequence with k elements is called a **k-tuple**: $(7,21,3)$ is a 3-tuple; order pairs are 2-tuples.

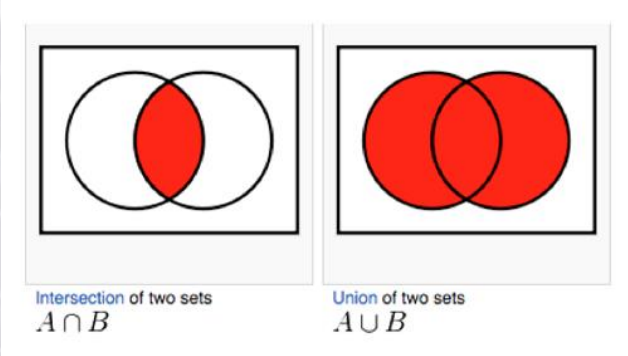
• The **power set** of a set A, expressed $\mathbb{P}(A)$ is defined as the set of all subsets of A. For example, $\mathbb{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$. When, $|A| < \infty, |\mathbb{P}(A)| = 2^{|A|}$, why?

• The **Cartesian Product** of sets A and B, is defined $A \times B = \{(a,b) | a \in A, b \in B\}$. The Cartesian product can be extended for more than two sets in a natural way; for example: $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3 = \{(a,b,c) | a,b,c \in \mathbb{R}\}$.

Sets

• There exist two common binary operations on sets: **union** and **intersection**. The union of sets A and B, written: A$\cup B$ is defined as the set of all elements either in A or B (or both); the intersection of sets, expressed: A$\cap B$ is defined as the set of all elements in both A and B:

$$A \cup B = \{x | x \in A \; or \; x \in B\}, A \cap B = \{x | x \in A \; and \; x \in B\}$$



• The unary operation **complement**, written $\bar{A}$, is defined as the set of all elements under consideration that are not in A.

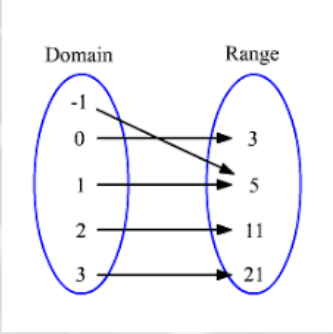
Functions & Relations

• A **relation** R is a set of ordered pairs over a non-empty Domain set D. If for elements $a, b \in D$, "a related to b", we write: $a\ R\ b$; equivalently we can express this relation as the ordered pair (a, b). For example if $D = \mathbb{Z}$ and R is the "less than" relation (i.e. <); it follows that $1\ R\ 2$ is True, but $10\ R\ 7$ is False.

• A **function** (also called a **mapping**) is an object that maps elements from one set (**Domain**) to another set (**Co-Domain**); in this way a function determines an element-wise correspondence between sets. The image of the function is referred to as the **Range** of the function, notice that $\text{Range(f)} \subseteq \text{CoDomain(f)}$, necessarily**.**

• The structure of a function is more stringent than that of a relation; **a function additionally requires that each input element is mapped to only one co-domain element**.

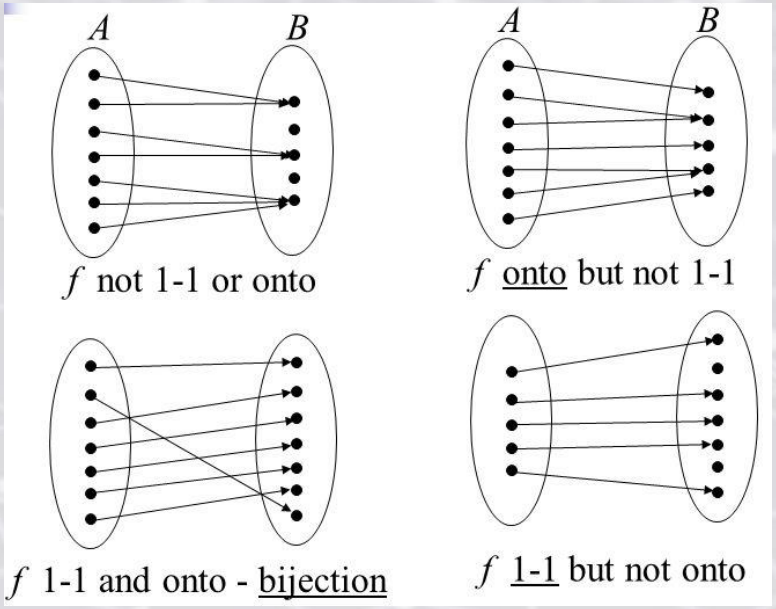
• Functions can be represented in a variety of ways, including as a set of ordered pairs, e.g., $\{(-1,5), (0,3), (1,5), (2,11), (3,21)\}$, or, alternatively using a function diagram or table.



Functions & Relations

• A function is called **injective** (1-1) if each input element maps to a unique output; a function is said to be **surjective** (onto) if Range(f) = CoDomain(f) – in other words, each element in the range of f is mapped "onto" by an element in the domain.

• If a function is both injective and surjective we call it a **bijection** (equivalently: f defines a "one-to-one correspondence").



Functions & Relations

• When a function takes single arguments as input, we call it a **unary function**. Otherwise, if a function takes sequences of dimension k (also: vectors) as input, we call it a **k-ary function**.

• Here is an example of a 2-ary function $g: Z_4 \times Z_4 \longrightarrow Z_4$ that defines addition modulo 4.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

For example, $g(3,1) = 0$.

Functions & Relations

• Relations are called **equivalence relations** if they satisfy the following (3) properties:

(1) R is **reflexive** if for every x in D, xRx
(2) R is **symmetric** if for every x and y in D, xRy implies yRx
(3) R is **transitive** if for every x, y and z in D, xRy and yRZ implies xRz.

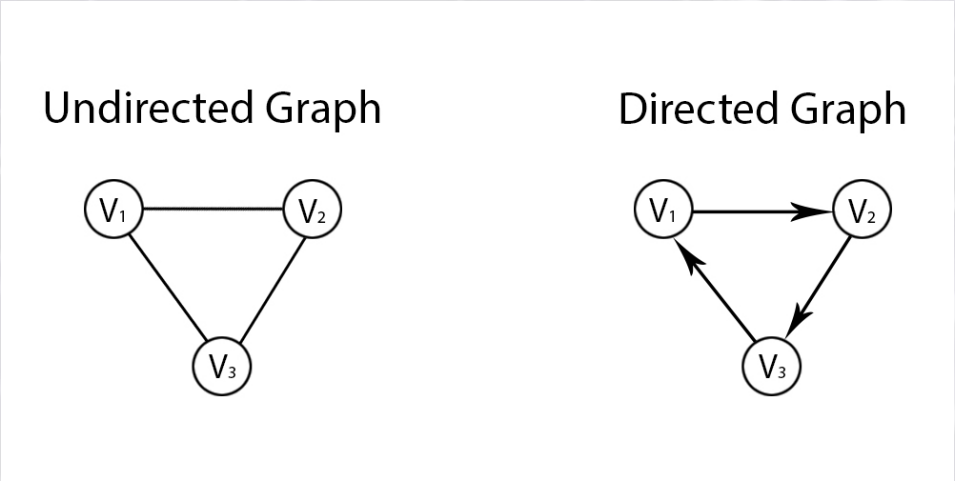
For example, the relation 'equality' for $D = \mathbb{Z}$ defines an equivalence relation.

Graphs

• Graphs are one of the most common structures encountered in computer science. A **graph G** is a collection of **vertices** (sometimes called nodes) (V) and **edges** (E), so a graph is a 2-tuple, defined: $G = (V, E)$. Graphs fundamentally describe relations (i.e. whether there is an edge or not) over a set of objects (i.e. the vertices).

• An **undirected graph** (or simple a graph) is a set of points with lines connecting some of the points; the edges are undirected in this case. **Simple graphs** have no **self-loops** (i.e. an edge connecting a vertex to itself) and no **multi-edges** (i.e. more than one edge connecting the same pair of vertices). Usually we simply refer to a simple graph as a "graph."

• Directed graphs contain oriented edges; typically an oriented edge is expressed as an ordered pair (v_1, v_2), where v_1 is the *source vertex* and v_2 is the *sink/terminal vertex* .

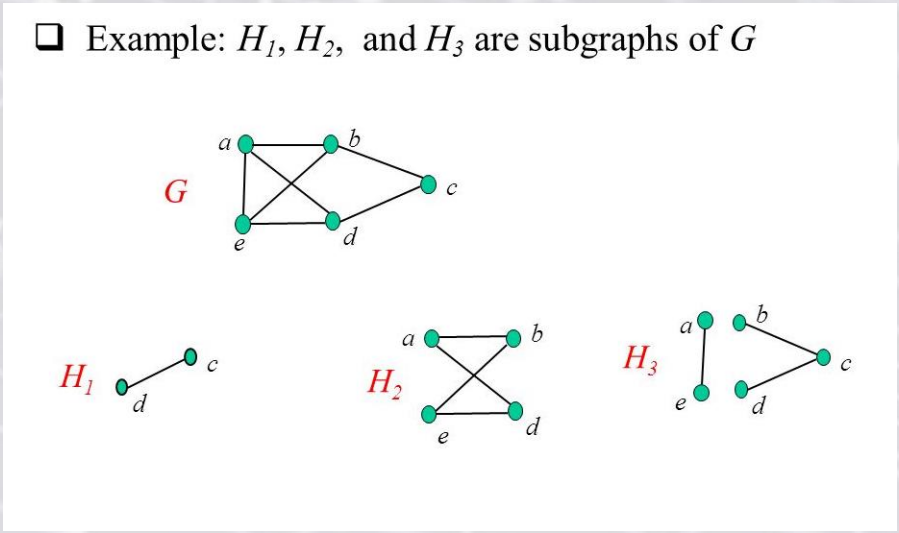


Graphs

• The **degree of a vertex** is defined as the number of edges emanating from a vertex. A graph is **regular** if all of the vertices have the same degree. For undirected graphs, we commonly specify two measures related to degree: **indegree(v)** and **outdegree(v)**.

• We say that a graph **H is a subgraph of a graph G** if the nodes of H are a subset of the nodes of G, and the edges of H are the edges of G on the corresponding nodes, i.e. $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$.

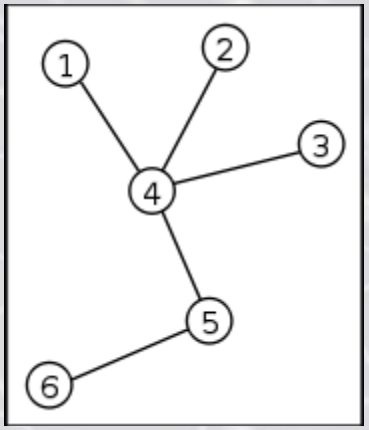
❑ Example: H_1, H_2, and H_3 are subgraphs of G



Graphs

• A **path** in a graph is a sequence of nodes connected by edges. A graph is **connected** if, for any two vertices in the graph, there exists a path between them. A **cycle** is a path that starts and ends at the same vertex. A **simple cycle** is one that contains at least three vertices and repeats only the first and last vertices.

• A **tree** is a connected graph with no simple cycles. A tree can be thought of as a minimally connected graph (with respect to the vertex set). A tree admits of a *topological ordering*, where a vertex is specially designated as the **root**; aside from the root, all vertices of degree 1 in a tree are referred to as the **leaves** of the tree.



• In a directed graph G, we say G is **strongly connected** if a directed path connects every two nodes.

Strings and Languages

• **Strings** of characters are fundamental building blocks in computer science. The alphabet over which strings are defined may vary with the application.

• We define an **alphabet** to be any non-empty finite set, usually we reserve the letters Σ and Γ for alphabets, e.g. $\Sigma = \{0,1\}$; the members of the alphabet are the **symbols** of the alphabet.

• A **string over an alphabet** is a finite sequence of symbols from that alphabet; for example $cbbabcaca$ is a string over the alphabet $\Sigma = \{a, b, c\}$.

• If w is a string over Σ, the length of w, written, $|w|$, is the number of symbols that it contains. The string of length zero is called the **empty string** and is denoted ε.

• The **reverse of a string w**, written w^R, is the string obtained by writing w in the opposite order, e.g. if $w = (w_1, \dots, w_n)$, then $w^R = (w_n, \dots, w_1)$.

Strings and Languages

• String z is a s**ubstring** of w if z appears consecutively within it. For example, cad is a substring of abracadabra.

• If we have a string x of length m and a string y of length n, the **concatenation** of x and y, written xy, is the string obtained by appending x to the end of y, yielding: $\mathrm{xy} = (x_1, \ldots, x_m, y_1, \ldots, y_m)$,

• The **lexicographic order** of strings it the same as the familiar dictionary order; **shortlex order** (or simply **string order**) is identical to lexicographic order, except that shorter strings precede longer strings. Thus the string ordering of all strings over the $\Sigma = \{0,1\}$ is:

$$\{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$$

• We say that string x is a **prefix** of string y if a string z exists where $\mathrm{x}z = y$ and that x is a **proper prefix** of y if in addition $\mathrm{x} \neq y$.

• A **language** is a set of strings. A language is **prefix-free** if no member is a proper prefix of another member.

Boolean Logic

- **Boolean Logic** is a mathematical system built around two values: TRUE and FALSE.

- We can manipulate Boolean values with Boolean operations, including: **negation** ⌐ (i.e. NOT), **conjunction** ⋀ (AND), and **disjunction** ⋁ (OR).

These Boolean operations can be summarized as follows:

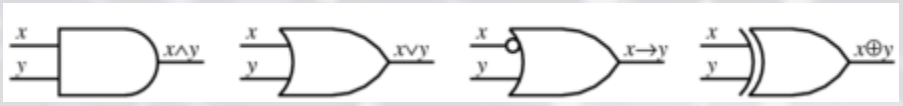
$0 \wedge 0 = 0$	$0 \vee 0 = 0$	$\neg 0 = 1$
$0 \wedge 1 = 0$	$0 \vee 1 = 1$	$\neg 1 = 0$
$1 \wedge 0 = 0$	$1 \vee 0 = 1$	
$1 \wedge 1 = 1$	$1 \vee 1 = 1$	

Boolean Logic

• Several other Boolean operations occasionally appear: the **exclusive or** $\oplus$ (XOR), which is 1 if either but not both of its operands is 1; and the **equality** $\leftrightarrow$ (IFF) which is 1 if both of its operands have the same value; lastly, **implication** $(\rightarrow)$ is 0 if its first operand is 1 and its second operand is 0, otherwise is 1. In summary:

$0 \oplus 0 = 0$	$0 \leftrightarrow 0 = 1$	$0 \rightarrow 0 = 1$
$0 \oplus 1 = 1$	$0 \leftrightarrow 1 = 0$	$0 \rightarrow 1 = 1$
$1 \oplus 0 = 1$	$1 \leftrightarrow 0 = 0$	$1 \rightarrow 0 = 0$
$1 \oplus 1 = 0$	$1 \leftrightarrow 1 = 1$	$1 \rightarrow 1 = 1$

• There exists a natural correspondence between Boolean operations and set operations. The set of Boolean operations can be reduced, equivalently, to expressions which only involve AND, OR and NOT. In this way, logic circuits representing wffs (well-formed formulas) can be expressed using combinations consisting of only these three Boolean operations.



$P \vee Q$ is equivalent to: $\neg(\neg P \wedge \neg Q)$

$P \rightarrow Q$ is equivalent to: $\neg P \vee Q$

$P \leftrightarrow Q$ is equivalent to: $(P \rightarrow Q) \wedge (Q \rightarrow P)$

$P \oplus Q$ is equivalent to: $\neg(P \leftrightarrow Q)$

Conditional Statements

• Conditional statements are statements of the form: "if P, then Q" (where P and Q are called *predicates*, i.e. Boolean-valued functions); P is referred to as the *antecedent* and Q is called the *consequent* of the conditional statement.. We commonly write a conditional statement using the implication symbol: $\mathrm{P} \longrightarrow Q$.

• There are <u>three additional related forms of a conditional statement $\mathrm{P} \longrightarrow Q$</u>.

• The **inverse** of the corresponding conditional state is defined: $\neg\mathrm{P} \longrightarrow \neg\mathrm{Q}$; the **converse**: $\mathrm{Q} \longrightarrow P$ and the **contrapositive**: $\neg Q \longrightarrow \neg\mathrm{P}$. Note that the **contrapositive is logically equivalent to its corresponding conditional statement**; however, the <u>converse is not logically equivalent to its corresponding conditional statement</u>. The <u>inverse and converse statements for a corresponding conditional statement are logically equivalent</u>.

• The logical equivalences mentioned above can be verified using logical rules of deduction – or equivalently, via *truth tables*.

				Conditional	Converse	Inverse	Contrapositive
P	Q	~P	~Q	P→Q	Q→P	~P→~Q	~Q→~P
T	T	F	F	T	T	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

Conditional Statements

• The **inverse** of the corresponding conditional state is defined: $\neg P \longrightarrow \neg Q$; the **converse**: $Q \longrightarrow P$ and the **contrapositive**: $\neg Q \longrightarrow \neg P$. Note that the **contrapositive is logically equivalent to its corresponding conditional statement**; however, the converse is not logically equivalent to its corresponding conditional statement. The inverse and converse statements for a corresponding conditional statement are logically equivalent.

• Note that most theorems in mathematics and computer science are expressed naturally as conditional statements. In these cases we can always construct the contrapositive of the theorem to generate a logically equivalent statement – frequently, this contrapositive variant of the theorem is additionally informative/useful. For example, from calculus we have the following theorem:

Theorem: "If the real-valued function $f(x)$ is differentiable at a point $x = p$ (i.e. $f'(p)$ is defined), then $f(x)$ is continuous at $x = p$."

Contrapositive: "If the real-valued function $f(x)$ is discontinuous at the point $x = p$, then $f(x)$ is not differentiable at $x = p$, i.e. (i.e.$f'(p)$ is undefined)"

Valid Arguments

• An **argument** in logic is a sequence of statements, where we assert that one of these statements (called the **conclusion**) follows from a subset of these statements (called the **premises**). The argument is deemed **valid** if the conclusion can be deduced from the premises using a sequence of "valid argument forms."

• Importantly, the abstract power of logic follows from the fact that if a valid argument contains true premises, then the conclusion is necessarily true. An argument is called **sound** if and only if it is valid and all of its premises are true.

• Here is a summary of common valid argument forms:

Modus Ponens	$p \to q$ p $\therefore q$	**Elimination**	**a.** $p \vee q$ $\sim q$ $\therefore p$ **b.** $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \to q$ $\sim q$ $\therefore \sim p$	**Transitivity**	$p \to q$ $q \to r$ $\therefore p \to r$
Generalization	**a.** p $\therefore p \vee q$ **b.** q $\therefore p \vee q$	**Proof by Division into Cases**	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$
Specialization	**a.** $p \wedge q$ $\therefore p$ **b.** $p \wedge q$ $\therefore q$		
Conjunction	p q $\therefore p \wedge q$	**Contradiction Rule**	$\sim p \to c$ $\therefore p$

Valid Arguments

Modus Ponens	$p \to q$ p $\therefore q$	**Elimination**	**a.** $p \vee q$ $\sim q$ $\therefore p$ **b.** $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \to q$ $\sim q$ $\therefore \sim p$	**Transitivity**	$p \to q$ $q \to r$ $\therefore p \to r$
Generalization	**a.** p $\therefore p \vee q$ **b.** q $\therefore p \vee q$	**Proof by Division into Cases**	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$
Specialization	**a.** $p \wedge q$ $\therefore p$ **b.** $p \wedge q$ $\therefore q$		
Conjunction	p q $\therefore p \wedge q$	**Contradiction Rule**	$\sim p \to c$ $\therefore p$

• Consider the following example, which we show is a valid argument:

Premise #1: If at least one of these two numbers is even, then the product of these two numbers is even.
Premise #2: Neither of these two numbers is even.
Conclusion: The product of these two numbers is odd.

• Premise #1 can be expressed: $E1 \vee E2 \longrightarrow PE$ (where AOE denotes "at least one is even" and PE denotes "product is even"). Premise #2 can be expressed $\neg E1 \wedge \neg E1$.

• The argument is valid, which we argue as follows:

$$(1) E_1 \vee E_2 \to PE \quad \text{(premise \#1)}$$
$$(2) \neg E_1 \wedge \neg E_2 \quad \text{(premise \#2)}$$
$$\therefore (3) \neg PE \quad \text{(modus tollens)}$$

Proof Techniques

• A **proof** is a convincing logical argument that a statement is true – the conclusion must follow in a valid way from the premises. In mathematics, an argument must be airtight; that is, convincing in an absolute sense.

• A **theorem** is a mathematical statement proved true. Generally, we reserve the use of that word for statements of special interest.

• Occasionally we prove statements that are interesting only because they assist in the proof of another, more significant statement. Such statements are called **lemmas**. Occasionally a theorem or its proof may allow us to conclude easily that other, related statements are true. These statements are called **corollaries** of the theorem.

• Sometimes the parts of a multi-part statement are not immediately evident. One frequently encountered type of multi-part statement has the form "**P if and only if (iff) Q**," where both P and Q are mathematical statements. In this case we must prove, in two separate cases, both implications: $P \longrightarrow Q$ and $Q \longrightarrow P$.

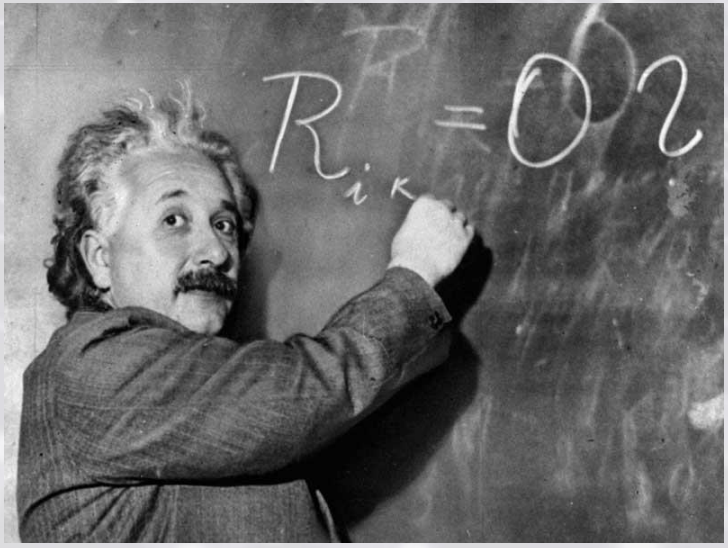
• To disprove a mathematical statement, one needs to produce a single **counterexample**.

Proof Techniques

• Unfortunately, **there is no generalizable procedure for constructing mathematical proofs** (Turing proved the impossibility of this endeavor!).

• Nevertheless, it is helpful to consider the following general tips: *be patient*, *come back to it*, *be neat and precise*, *be concise* – also, of course, practice makes perfect! Some proofs can be quite challenging and have known to baffle the greatest minds in science for years (even centuries in some cases).

• Let's begin by practicing a few proof examples, using a technique known as **direct proof** – meaning state the premises, and follow them (using any appropriate definitions and valid argument deductions) to their logical conclusion, i.e. we show $P \longrightarrow Q$ (where P indicates the set of premises and Q denotes the conclusion).



Proof Techniques: Direct Proof

Theorem: for any two sets A and B, $\overline{A \cup B} = \bar{A} \cap \bar{B}$.

Pf. (Direct) First, try and get an intuitive sense of why this property holds (imagine, for instance, a Venn diagram "argument"). Recall that in order to prove two sets are equal, we need to show that both subset containment arguments hold.

(1) We show: $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$. Let $x \in \overline{A \cup B}$, then x is not in the union of A and B from the definition of the completement of a set. Hence, x is not in A and x is not in B. This indicates that $x \in \bar{A} \cap \bar{B}$. Thus $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$ follows, as we have shown that any arbitrary element in $\overline{A \cup B}$ is necessarily in $\bar{A} \cap \bar{B}$.

(2) Next, we show: $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$. Let $x \in \bar{A} \cap \bar{B}$, then x is not in A and x is not in B. Thus, x is in the completement of the union of A and B, i.e., $x \in \overline{A \cup B}$. This proves $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$, as desired.

Since $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$ and $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$ both hold, we conclude that: $\overline{A \cup B} = \bar{A} \cap \bar{B}$.

QED (*quod erat demonstrandum*)

Proof Techniques: Direct Proof

Theorem: For every (simple) graph G, the sum of the degrees of all the nodes in G is an even number.

Pf. (Direct) Every edge is connected to two nodes; each edge contributes 1 to the degree of each node to which it is connected. Therefore, each edge contributes 2 to the sum of the degrees of all nodes. Consequently, if G contains e edges, then the sum of the degrees of all nodes of G is 2e, which is an even number. QED

Corollary: We refer to an **odd component** of a graph G as a *maximally connected component* with an odd number of vertices; similarly, we refer to an **even component** of a graph G as a maximally connected component with an even number of vertices.

Corollary: Every graph has an odd number of odd components. Why?

Proof Techniques: Contrapositive

• Another standard proof technique is **proof by contrapositive**. When tasked with proving the implication: $P \longrightarrow \mathrm{Q}$ we can equivalently prove the contrapositive statement: $\neg \mathrm{Q} \longrightarrow \neg P$. Oftentimes the it is easier to prove the contrapositive of a conditional statement in lieu of the original statement.

Claim: For any integer k, if 3k+1 is even, then k is odd.

• Notice that this statement is awkward to prove in its original form, because we're trying to use information about a derived quantity to prove something about a more basic one.

Pf. (Contrapositive) The contrapositive variant of the original conditional statement reads: if k is even, then 3k+1 is odd.

Assume that k is even, so $k = 2j$ for some $j \in \mathbb{Z}$. Now consider the expression:

$$3k + 1 = 3(2j) + 1 = 2(3j) + 1$$

Any integer of the form $2m + 1$ with $m \in \mathbb{Z}$ is necessarily odd, so $3k + 1$ is odd. QED

Proof Techniques: Cases

• **Proof by cases** is an essential proof method that entails partitioning the problem space into (natural) cases; we show that the required conclusion holds in all cases.

Theorem: If q is not divisible by 3, then $q^2 \equiv 1(mod\ 3)$.

• We consider the problem with respect to modulus 3. If q is not divisible by 3 , then either: $q \equiv 1(mod\ 3)\ or\ q \equiv 2(mod\ 3)$; our proof accounts for these two cases.

Pf. (Cases) Assume that q is not divisible by 3, so either: $q \equiv 1(mod\ 3)\ or\ q \equiv 2(mod\ 3)$.

Case 1: Assume that $q \equiv 1(mod\ 3)$, so $q = 3j + 1$ for some $j \in \mathbb{Z}$. Then:

$$q^2 = (3j + 1)^2 = 9j^2 + 6j + 1 = 3(3j^2 + 2j)\ + 1 \equiv 1(mod\ 3)$$

Case 2: Assume that $q \equiv 2(mod\ 3)$, so $q = 3j + 2$ for some $j \in \mathbb{Z}$. Then:

$$q^2 = (3j + 2)^2 = 9j^2 + 12j + 4 = 3(3j^2 + 4j + 1) + 1 \equiv 1(mod\ 3)$$

QED

Proof Techniques: Contradiction

• **Proof by contradiction** is among the most powerful elementary proof techniques – so much so that every mathematician and computer science student should be conversant with it.

• The general construct for proof by contradiction is as follows: to show $P \longrightarrow Q$ we proceeed in two steps: (1) First, "suppose not" and **assume** $\neg P$; (2) Next, from $\neg P$ **derive an (inexorable) contradiction** (e.g. Q and $\neg Q$).

Proof Techniques: Contradiction

Theorem: $\sqrt{2} \notin \mathbb{Q}$ (Euclid).

Pf. (Contradiction) Suppose not, and suppose instead that $\sqrt{2} \in \mathbb{Q}$; this implies that $\sqrt{2} = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ with $b \neq 0$.

Note that since all rational numbers admit of a "most simplified form", we can furthermore assume, **without loss of generality** (WLOG), that $GCD(a, b) = 1$ (i.e. a and b are *relatively prime*). Next, consider the following argument:

$$\sqrt{2} = \frac{a}{b} \underbrace{\leftrightarrow}_{iff}$$

$$\sqrt{2}b = a \leftrightarrow$$

$$\left(\sqrt{2}b\right)^2 = a^2 \leftrightarrow$$

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

Observe that the left-hand side of the last line represents an even number; ergo, a^2 is even, ergo a is even (why?). But if a is even and $a^2 = 2b^2$, then $4 \mid 2b^2$ which implies that $2 \mid b^2$ (why?), indicating b is also even. Thus, $GCD(a, b) > 1$, a contradiction. It therefore follows that $\sqrt{2} \notin \mathbb{Q}$.

QED

Proof Techniques: Contradiction

• Recall that a prime number $p > 1$ is an integer whose only positive factors are 1 and itself. All integers beginning with 2 are either prime or *composite* (meaning they consist of a product of only primes); the **Fundamental Theorem of Arithmetic (FTA)** states furthermore that all such integers greater than 1 admit of a unique prime factorization.

Theorem: There exists an infinite number of primes. (Euclid)

Pf. (Contradiction) Suppose not and so we assume there are only a finite number of primes. If this is the case, then we can list and order (in ascending fashion) the set of all primes P:

$$P = \{p_1, p_2, \dots, p_N\}$$

Now consider the integer: $p^* = p_1 \cdot p_2 \cdots p_N + 1$. Due to the FTA, because $p^* > 1$, either p^* is prime or it is compositive (but not both and not neither). **We show that p^* is neither** – a contradiction (of the FTA).

Continued…

Proof Techniques: Contradiction

Theorem: There exists an infinite number of primes. (Euclid)

Pf. (Contradiction) Suppose not and so we assume there are only a finite number of primes. If this is the case, then we can list and order (in ascending fashion) the set of all primes P:

$$P = \{p_1, p_2, \dots, p_N\}$$

Now consider the integer: $p^* = p_1 \cdot p_2 \cdots p_N + 1$. Due to the FTA, because $p^* > 1$, either p^* is prime or it is compositive (but not both and not neither). **We show that p^* is neither** – a contradiction (of the FTA).

Case #1: Assume that p^* is prime. Upon reflection, this cannot be the case, because $p^* > p_N$ where p_N is the largest extant prime! (What happens if we revise P so that $P = \{p_1, p_2, \dots, p_N, p^*\}$?)

Therefore, p^* cannot be prime.

Continued…

Proof Techniques: Contradiction

Theorem: There exists an infinite number of primes. (Euclid)

Pf. (Contradiction) Suppose not and so we assume there are only a finite number of primes. If this is the case, then we can list and order (in ascending fashion) the set of all primes P:

$$P = \{p_1, p_2, \dots, p_N\}$$

Now consider the integer: $p^* = p_1 \cdot p_2 \cdots p_N + 1$. Due to the FTA, because $p^* > 1$, either p^* is prime or it is compositive (but not both and not neither). **We show that p^* is neither** – a contradiction (of the FTA).

Case #2: Assume that p^* is composite. Upon reflection, this also cannot be the case, because, by construction, p^* is not divisible by any prime number (when dividing by a prime it always returns remainder 1), and thus p^* does not admit of a prime factorization. This result contradicts the FTA, so p^* is neither composite nor prime!

Conclusion: In either case, when we assume the set of primes is finite we reach a contradiction. It therefore follows that there exists an infinite number of primes.

QED

Proof Techniques: Induction

• Like proof by contradiction, **proof by induction** is an invaluable proof technique, particularly in computer science. Proof by induction is generally applicable in cases where we wish to show that all elements of an infinite set (e.g. $\mathbb{Z}$, $\mathbb{N}$) have a specified property.

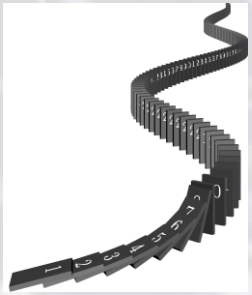
• Proof by induction works as follows: suppose we wish prove a property, call it P, to be true for every natural number $k \in \{1,2,3, \dots\}$. Concretely, our goal is to prove $P(k)$ is true for all k, i.e. we show $P(1)$ is true, as well as $P(2), P(3), P(4)$, and so on.

The general flow of proof by induction is as follows:

(1) **Basis Step**: Prove that $P(1)$ is true.

(2) **Induction Step**: For each $k \geq 1$, assume that $P(k)$ holds and use this assumption to show that $P(k+1)$ is also true. (we refer to the assumption that $P(k)$ is true as the **inductive hypothesis**).

• Why does induction work? Think of an infinite set of dominos labeled $\{1,2,3, \dots\}$. In (1) we show that the first domino "falls" (i.e. P(1) is true); in (2) we show that whenever a domino falls, the next domino adjected to it also falls. In this way all the dominos fall!



Proof Techniques: Induction

Theorem: For all $n \geq 1$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

• Consider the formula: $\mathrm{P}(k) \leftrightarrow \sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, so that $\mathrm{P}(k)$ is true when the formula holds for k.

Pf. (Induction)

(1) **Basis Step**: $\mathrm{P}(1) \leftrightarrow \sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$, so $\mathrm{P}(1)$ holds.

(2) **Induction Step**: Assume $\mathrm{P}(k)$ is true for some arbitrary $\mathrm{k} \in \{1,2,3, \ldots\}$. Now we must show that $\mathrm{P}(k+1)$ is also true.

We begin with the left-hand side of the formula $\mathrm{P}(k+1)$:

$$\sum_{i=1}^{k+1} i = 1 + 2 + \cdots + k + (k+1)$$

$$= \frac{k(k+1)}{2} + (k+1) \qquad \text{(by the inductive hypothesis)}$$

$$= \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{(k+1)(k+2)}{2} \leftrightarrow \mathrm{P}(k+1) \text{ is true.}$$

QED

Proof Techniques: Induction

Theorem: $5|(7^n - 2^n)\ \forall\ n \geq 0$.

• Consider the formula: $\mathrm{P}(k) \leftrightarrow 5|(7^k - 2^k)$, so that $\mathrm{P}(k)$ is true when the formula holds for k.

Pf. (Induction)

(1) **Basis Step**: $\mathrm{P}(0) \leftrightarrow 5|(7^0 - 2^0)$, and $5|0$, since $0 = 5 \cdot 0$.

(2) **Induction Step**: Assume $\mathrm{P}(k)$ is true for some arbitrary $\mathrm{k} \in \{0,1,2, \ldots\}$. Now we must show that $\mathrm{P}(k+1)$ is also true.

The inductive hypothesis assumes that $\mathrm{P}(k)$ is true, which implies that $5|(7^k - 2^k)$ so $7^k - 2^k = 5j$ for some $\mathrm{k} \in \mathbb{Z}$.

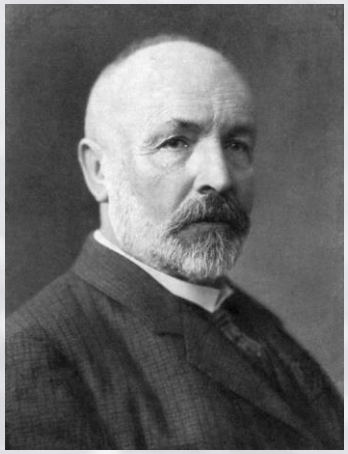
Next, we consider the expression $7^{k+1} - 2^{k+1}$; if we can show this expression is divisible by 5 under the assumption that $\mathrm{P}(k)$ is true, we are done.

Notice that:
$$\begin{aligned} 7^{k+1} - 2^{k+1} &= 7 \cdot 7^k - 2 \cdot 2^k \\ &= 7 \cdot 7^k + 5 \cdot 2^k - 7 \cdot 2^k \\ &= 7(7^k - 2^k) + 5 \cdot 2^k = 7(5j) + 5 \cdot 2^k \quad \text{(by the inductive hypothesis)} \\ &= 5(7j + 2^k) \leftrightarrow \mathrm{P}(k+1) \text{ is true.} \end{aligned}$$

QED

*Bonus problem: Prove that the sum of the interior angels of an n-sided polygon equals $180(\mathrm{n} - 2)\ \forall\ n \geq 3$.

Cantor's Methods



• At the end of the 19th century, the German mathematician **Gregor Cantor** developed several remarkable results regarding infinite sets which shook the foundation of the discipline and had a subsequent impact upon both Gödel and Turing – and the theory of computation more generally. **In particular, Cantor demonstrated that there exist infinite degrees of infinity**!

• Cantor began by investigating the cardinality of infinite sets (following from Galileo's own musings).

• We say that **two sets have the same cardinality (i.e. they are the same "size") iff there exists a bijection between them**.

• For finite sets, nothing here is remarkable; for example $|\{1,2,3\}| = |\{a, b, c\}|$, and one possible bijection between these sets is: $1 \leftrightarrow a, 2 \leftrightarrow b, 3 \leftrightarrow c$.

Cantor's Methods

• We say that **two sets have the same cardinality (i.e. they are the same "size" or "equinumerous") iff there exists a bijection between them**. Notice that cardinality defines an equivalence relation over sets.

• The case is, however, less straightforward and intuitive for infinite sets. First, notice the self-evident assertion that if A and B are finite sets with $\mathrm{A} \subsetneq B$, then $|A| < |B|$. For infinite sets A and B the claim is weaker, namely: if $\mathrm{A} \subsetneq B$ then $|A| \leq |B|$.

• Now define $2\mathbb{Z}$ as the set of all even integers, then $2\mathbb{Z}$ is a proper subset of $\mathbb{Z}$ (i.e., $2\mathbb{Z} \subsetneq \mathbb{Z}$) but as Cantor showed, $|2\mathbb{Z}| < |\mathbb{Z}|$, because one can define the bijection $\mathrm{f}: \mathbb{Z} \longrightarrow 2\mathbb{Z}, \mathrm{f}(i) = 2i \ \ \forall i \in \mathbb{Z}$.

• Far from being an anomalous example, Cantor in fact demonstrated that this property was a defining feature of all infinite sets: namely, **every infinite set contains a proper subset (also infinite) such that the subset has the same cardinality of the superset**.

• Following this reasoning and proof technique, one can readily show: $|\mathbb{N}| = |2\mathbb{N}| = |\mathbb{Z}|$.

Cantor's Methods

• Following this reasoning and proof technique, one can readily show: $|\mathbb{N}| = |2\mathbb{N}| = |\mathbb{Z}|$.

• Recalling that $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q}$, it is natural to wonder whether $|\mathbb{Z}| = |\mathbb{Q}|$. **The answer is in fact yes**.

Theorem. $|\mathbb{N}| = |\mathbb{Q}^+|$, where $\mathbb{Q}^+$ denotes the set of non-negative rationals.

Pf. We directly construct a bijection between the two sets to prove that they are equinumerous.
Define $f: \mathbb{Q}^+ \longrightarrow \mathbb{N}$, with $f(m/n) = 2^m 3^n$ (you should be able to prove that this is a bijection).

QED

• From here, it is not difficult to show that $|\mathbb{Q}^+| = |\mathbb{Q}|$, and thus: $|\mathbb{Z}| = |\mathbb{Q}|$ by the transitivity of the cardinality equivalence relation.

Cantor's Methods

• Recapping, we have shown that $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$, and $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$. Cantor next wondered whether all infinite sets are equinumerous.

• More specifically, does $|\mathbb{Q}| = |\mathbb{R}|$? Remarkably, the answer is **no**!

• Before proving the extraordinary result $|\mathbb{Q}| < |\mathbb{R}|$, let's first address some of the remarkable quirks surrounding the "algebra of infinities."

Cantor's Methods

• We say that a set is **countable** if it is either finite or is equinumerous with $\mathbb{N}$. Symbolically we denote the **uncountably infinite quantity** $\aleph_0$ (pronounced: "aleph-naught" or "aleph-zero", after aleph, the Hebrew letter). Thus: $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$.

• Observe that if we denote the even natural as $2\mathbb{N}$ and the odd naturals as O, since $|2\mathbb{N}| = |O| = |\mathbb{Z}|$ (why?) and $2\mathbb{N} \cup O = \mathbb{Z}$, it follows that $\aleph_0 + \aleph_0 = \aleph_0$ -- a strange result indeed.

• In fact, one can show, by extension that: $\aleph_0 + \cdots + \aleph_0 = \aleph_0$; moreover, since $|\mathbb{Q}| = |\mathbb{N}| \cdot |\mathbb{N}|$, we can also conclude that ${\aleph_0}^2 = \aleph_0$, astonishingly, in general we have: ${\aleph_0}^n = \aleph_0 \; \forall n \in \mathbb{N}$.

• The seemingly bizarre nature of this "algebra of infinites" imparted Cantor and his theories a dubious reputation during his lifetime; however, today Cantor's theories are considered some of the most profound and beautiful results in modern mathematics. Notably, the importance of these results appreciated subsequently by both Gödel or Turing.

Cantor's Methods: Diagonalization

• We now show that other orders of infinity exist, and that, in particular: $|\mathbb{Q}| < |\mathbb{R}|$.

• To prove this claim we utilize Cantor's famous **diagonalization argument**. We begin with the related claim $|\mathbb{Q}| < |(0,1)|$, which is to say that the cardinality of the open interval (0,1) is strictly larger than that of the cardinality of $\mathbb{Q}$ (this proof is somewhat cleaner than the direct proof of $|\mathbb{Q}| < |\mathbb{R}|$).

Theorem. $|\mathbb{Q}| < |(0,1)|$

Pf. (By contradiction, using diagonalization). Suppose not, and suppose instead that $|\mathbb{Q}| = |(0,1)|$, which is to say we assume that $(0,1)$ is *countable*. If $(0,1)$ is countable, then we may enumerate its members: $\{r_1, r_2, r_3 \ldots, \}$.

Each of the numbers r_i can be written as a decimal. We will use the following notational convention for these decimals:

$$r_1 = 0.a_{11}a_{12}a_{13} \ldots$$
$$r_2 = 0.a_{21}a_{22}a_{23} \ldots$$
$$r_3 = 0.a_{31}a_{32}a_{33} \ldots$$

and so on.

Cantor's Methods : Diagonalization

Theorem. $|\mathbb{Q}| < |(0,1)|$

Pf. (By contradiction, using diagonalization). Suppose not, and suppose instead that $|\mathbb{Q}| = |(0,1)|$, which is to say we assume that $(0,1)$ is *countable*. If $(0,1)$ is countable, then we may enumerate its members: $\{r_1, r_2, r_3 \ldots, \}$.

Each of the numbers r_i can be written as a decimal. We will use the following notational convention for these decimals:

$$r_1 = 0.a_{11}a_{12}a_{13} \ldots$$
$$r_2 = 0.a_{21}a_{22}a_{23} \ldots$$
$$r_3 = 0.a_{31}a_{32}a_{33} \ldots$$

and so on.

Writing this in a vertical list gives:

$$r_1 = 0.\boldsymbol{a_{11}}a_{12}a_{13} \ldots$$
$$r_2 = 0.a_{21}\boldsymbol{a_{22}}a_{23} \ldots$$
$$r_3 = 0.a_{31}a_{32}\boldsymbol{a_{33}} \ldots$$
$$\vdots$$
$$r_i = 0.a_{i1}a_{i2}a_{i3} \ldots \boldsymbol{a_{ii}} \ldots$$
$$\vdots$$

Cantor's Methods : Diagonalization

Theorem. $|\mathbb{Q}| < |(0,1)|$

Pf. (By contradiction, using diagonalization). Suppose not, and suppose instead that $|\mathbb{Q}| = |(0,1)|$, which is to say we assume that $(0,1)$ is *countable*. If $(0,1)$ is countable, then we may enumerate its members: $\{r_1, r_2, r_3 \ldots,\}$.

$$r_1 = 0.\boldsymbol{a_{11}}a_{12}a_{13} \ldots$$
$$r_2 = 0.a_{21}\boldsymbol{a_{22}}a_{23} \ldots$$
$$r_3 = 0.a_{31}a_{32}\boldsymbol{a_{33}} \ldots$$
$$\vdots$$
$$r_i = 0.a_{i1}a_{i2}a_{i3} \ldots \boldsymbol{a_{ii}} \ldots$$
$$\vdots$$

Now construct a real number $\mathrm{b} = 0.b_1b_2b_{i3} \ldots b_i$ in the following way. Choose b_1 to be 4 unless $a_{11} = 4$ in which case let $b_1 = 3$. Similarly, choose b_2 to be 4 unless $a_{22} = 4$ in which case let $b_2 = 3$, continue in this fashion. The idea is that we look at the diagonal elements in the list and choose b_i in such a way that it differs from the *i*th diagonal digit.

Notice that $\mathrm{b} \in (0,1)$; we also claim that b is not a member of the table from above. Why?

Cantor's Methods : Diagonalization

Theorem. $|\mathbb{Q}| < |(0,1)|$

Pf. (By contradiction, using diagonalization). Suppose not, and suppose instead that $|\mathbb{Q}| = |(0,1)|$, which is to say we assume that $(0,1)$ is *countable*. If $(0,1)$ is countable, then we may enumerate its members: $\{r_1, r_2, r_3 \ldots,\}$.

$$r_1 = 0.\boldsymbol{a_{11}}a_{12}a_{13} \ldots$$
$$r_2 = 0.a_{21}\boldsymbol{a_{22}}a_{23} \ldots$$
$$r_3 = 0.a_{31}a_{32}\boldsymbol{a_{33}} \ldots$$
$$\vdots$$
$$r_i = 0.a_{i1}a_{i2}a_{i3} \ldots \boldsymbol{a_{ii}} \ldots$$
$$\vdots$$

Now construct a real number $\mathrm{b} = 0.b_1b_2b_{i3} \ldots b_i$ in the following way. Choose b_1 to be 4 unless $a_{11} = 4$ in which case let $b_1 = 3$. Similarly, choose b_2 to be 4 unless $a_{22} = 4$ in which case let $b_2 = 3$, continue in this fashion. The idea is that we look at the diagonal elements in the list and choose b_i in such a way that it differs from the *i*th diagonal digit.

Notice that $\mathrm{b} \in (0,1)$; moreover, b is not on the above (why can't we simply add it to the list?). This is a contradiction, since we claimed that $(0,1)$ is countable (and thus enumerable). So no bijection exists between a countable set and $(0,1)$, so $|\mathbb{Q}| < |(0,1)|$.

QED

Cantor's Methods

• Now that we have proven $|\mathbb{Q}| < |(0,1)|$, we want to show the "big reveal", i.e. $|\mathbb{Q}| < |\mathbb{R}|$.

• This should seem intuitive given since $(0,1) \subsetneq \mathbb{R}$. Formally, one can show that $|(0,1)| = |\mathbb{R}|$ by constructing an appropriate bijection. Thus, $|\mathbb{Q}| < |\mathbb{R}|$ holds by transitivity of the cardinality equivalence relation.

• Because $|\mathbb{Q}| < |\mathbb{R}|$, we have that $\aleph_0 < |\mathbb{R}|$, meaning that we have discovered an additional order of infinity!

• Cantor's subsequent investigation (which he never resolved – and which was identified as one of Hilbert's *millennium problems*) was whether there exists a "next" magnitude of infinity, call it $\aleph_1$, where $\aleph_0 < \aleph_1 < |\mathbb{R}|$ (note the strict inequalities).

Cantor's Methods

• The famous **Continuum Hypothesis** (1878) asks whether any such cardinality $\aleph_1$, exists where:

$$\aleph_0 < \aleph_1 < |\mathbb{R}|$$

• In 1940, Gödel proved that the negation of the continuum hypothesis could not be proved in standard set theory; in 1963 Paul Cohen established the unprovability o the non-existence of such a set. In conclusion, **the continuum hypothesis is undecidable**.

• Finally, now that we have discovered a new magnitude of infinity, it is natural to wonder whether we have stumbled upon something "special" – are these the only two infinities? Are there more? Is there a finite number – or perhaps an infinite number of infinities?! As we now argue, **there are an infinite number of orders of infinity** (what a time to be alive!).

Cantor's Methods

• One of Cantor's additional celebrated results is the following: For any set $S, |S| < |\mathbb{P}(S)|$, where $\mathbb{P}(\cdot)$ denotes the *power set*.

• We omit the proof for brevity (it is not difficult). Observe that the result is unremarkable when S is finite, since $S \subsetneq \mathbb{P}(S)$ and $|S| < |\mathbb{P}(S)|$, automatically.

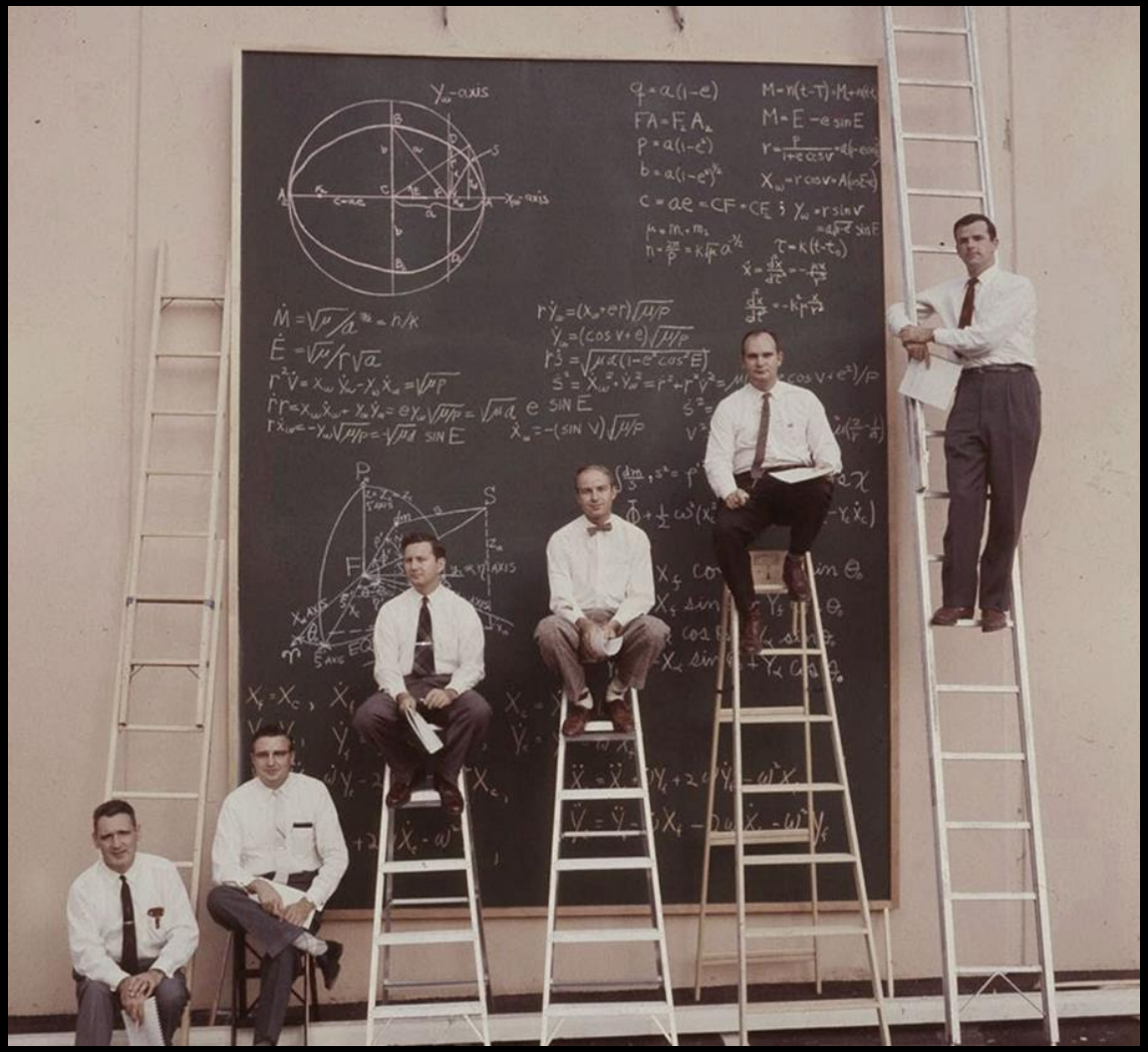
• However, recall that in general for S infinite, $S \subsetneq \mathrm{A}$ need not imply $|S| < |A|$ (consider $S = \mathbb{N}$ and $A = \mathbb{Q}$ as a counter-example).

• Now we see the significance of this result. It says that for any set, we can always find one with a strictly larger cardinality – just construct the power set of this set.

• It necessarily follows that there exists an infinite number of magnitudes of infinity! Why? Consider $|\mathbb{Q}| < |\mathbb{R}| < |\mathbb{P}(\mathbb{R})| < |\mathbb{P}(\mathbb{P}(\mathbb{R}))| < |\mathbb{P}(\mathbb{P}(\mathbb{P}(\mathbb{R})))| < \cdots$

QED

Fin


Y_w-axis
X_w-axis
$q = a(1-e)$
$FA = F_2 A_2$
$p = a(1-e^2)$
$b = a(1-e^2)^{1/2}$
$c = ae = CF = CE$
$M = n(t-T)$
$M = E - e \sin E$
$r = \frac{p}{1+e\cos v}$
$X_w = r\cos v$
$Y_w = r\sin v$
$\tau = k(t-t_0)$
$\dot{M} = \sqrt{\mu}/a^{3/2} = n/k$
$\dot{E} = \sqrt{\mu}/r\sqrt{a}$
$r^2\dot{v} = X_w\dot{Y}_w - Y_w\dot{X}_w = \sqrt{\mu p}$
$r\dot{r} = X_w\dot{X}_w + Y_w\dot{Y}_w = e Y_w\sqrt{\mu/p} = \sqrt{\mu a}\, e \sin E$
$r\dot{Y}_w = (X_w + er)\sqrt{\mu/p}$
$\dot{Y}_w = (\cos v + e)\sqrt{\mu/p}$
$r\dot{s} = \sqrt{\mu a(1-e^2\cos^2 E)}$
$\dot{X}_w = -(\sin v)\sqrt{\mu/p}$
P
S
F
S AXIS
EQ