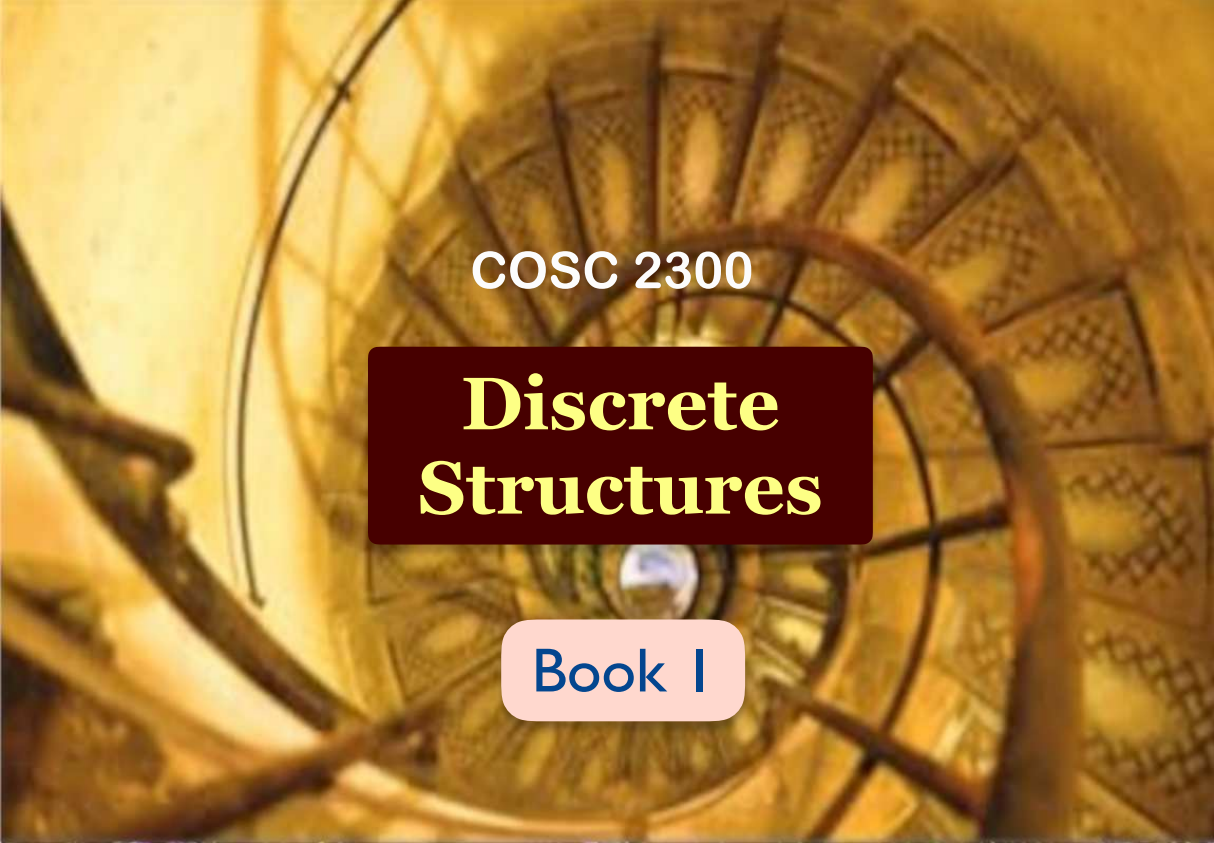
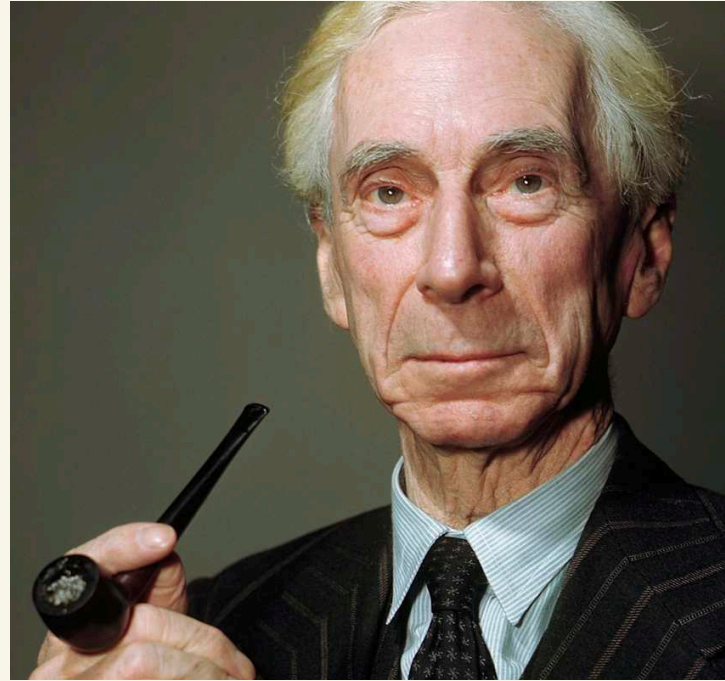




COSC 2300

# Discrete Structures

Book I



Bertrand Russell (1872-1970)

In a particular village there is a gentleman barber who shaves every gentleman who does not shave himself.

Does the barber shave himself?

No true/false answer can be given that is consistent.  
This is an example of Russell's Paradox.

Other forms:

P: The statement P (ie. this statement) is false.

---

Avoiding self-referential statements:

A: The statement B is true.

B: The statement A is false.

Propositional Logic (Propositional Calculus)

- R: Bertrand Russell was born in 1872. (True)  
M: Mars is the second planet from the sun. (False)  
J: January is the first month of the calendar year. (True)  
T: A triangle has four sides. (False)

Syntactic vs. Semantic features language  
syntax (symbolic)      meaning (semantics)  
true/false



R: Bertrand Russell was born in 1872.

(True)

M: Mars is the second planet from the sun.

(False)

J: January is the first month of the calendar year.

(True)

T: A triangle has four sides. (False)

"Exclusive or" of T and T is F. Avoid!

$R \vee M$  is True

↑  
"or"  
"join"  
"disjunction"

$R \wedge M$  is False

↑  
"and"  
"meet"  
"conjunction"

Truth Table: for two statements P, Q  
(atomic propositions)

| P | $\neg P$ |
|---|----------|
| T | F        |
| F | T        |

Conditional Statements  $P \rightarrow Q$  ("P implies Q")  
(implication) ("If P then Q")

$R \rightarrow M$  is false  
 $J \rightarrow R$  is true.  
 $T \rightarrow M$  is true.

$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$   
↑  
equivalence of propositions  
 $P \wedge Q \equiv Q \wedge P$

$P \rightarrow Q \equiv (\neg P) \vee Q$

| P | Q | $P \rightarrow Q$ | $\neg P$ | $(\neg P) \vee Q$ |
|---|---|-------------------|----------|-------------------|
| T | T | T                 | F        | T                 |
| T | F | F                 | F        | F                 |
| F | T | T                 | T        | T                 |
| F | F | T                 | T        | T                 |

"inclusive" or

| P | Q | $P \vee Q$ | $P \wedge Q$ |
|---|---|------------|--------------|
| T | T | T          | T            |
| T | F | T          | F            |
| F | T | T          | F            |
| F | F | F          | F            |

| P | Q | $P \rightarrow Q$ |
|---|---|-------------------|
| T | T | T                 |
| T | F | F                 |
| F | T | T                 |
| F | F | T                 |

$$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$$

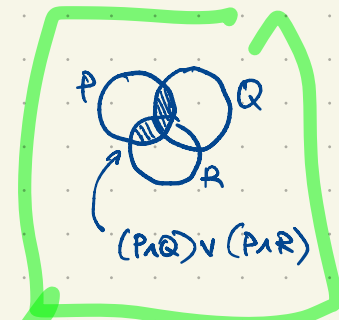
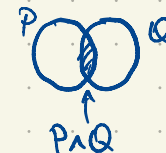
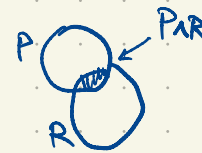
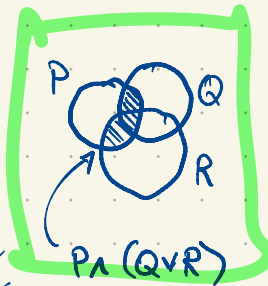
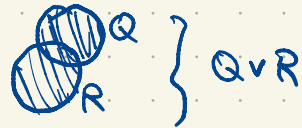
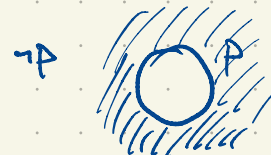
$$a(b+c) = ab+ac$$

$$a+bc \neq (a+b)(a+c)$$

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

This can be verified using a truth table (with eight rows)  
or using Venn diagram



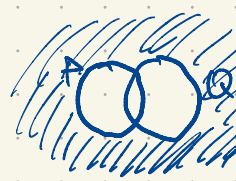
$$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$$

"P and Q are not both true, i.e. at least one of P and Q fails"



$$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$$

"Neither P nor Q is true; both are false"



De Morgan's Rules

$$\neg(P_1 \wedge P_2 \wedge P_3 \wedge \dots \wedge P_k) \equiv (\neg P_1) \vee (\neg P_2) \vee \dots \vee (\neg P_k)$$

$P_i$ : the  $i$ th student is wearing red  
 $P_1 \wedge P_2 \wedge \dots \wedge P_k$ : all  $k$  students are wearing red  
 $\neg(P_1 \wedge P_2 \wedge \dots \wedge P_k)$ : not all  $k$  students are wearing red  
 i.e. at least one of the  $k$  students

$$\neg(P_1 \vee P_2 \vee \dots \vee P_k) \equiv (\neg P_1) \wedge (\neg P_2) \wedge \dots \wedge (\neg P_k)$$

is not wearing red.  
 none of the  $k$  students are wearing red.

"All the students are not wearing red." Ambiguous: which of the above does the person mean?

$$P \vee (\neg P)$$

| P | $\neg P$ | $P \vee (\neg P)$ |
|---|----------|-------------------|
| T | F        | T                 |
| F | T        | T                 |



$P \vee (\neg P)$  is a tautology: its truth value is always true regardless of P.

P: "There exist integers  $x, y, z$  such that  $x^3 + y^3 + z^3 = 42$ ."

$P \vee (\neg P)$  says that P is either true or false.

$P \wedge (\neg P)$  is a contradiction

| P | $\neg P$ | $P \wedge (\neg P)$ |
|---|----------|---------------------|
| T | F        | F                   |
| F | T        | F                   |

$P \wedge (Q \vee R)$  is neither a tautology nor a contradiction: it depends on P, Q, R (it is a contingent proposition).

$P \rightarrow (Q \wedge (\neg Q))$  cannot be true unless P is false.

$$P \rightarrow (Q \wedge (\neg Q)) \equiv \neg P$$

$P \rightarrow (Q \vee (\neg Q))$  is a tautology.

| $P \rightarrow Q$<br>Conditional statement<br>"If P then Q"<br>or "P implies Q"<br>"Q whenever P" | P | Q | $P \rightarrow Q$ | Biconditional statement<br>$P \leftrightarrow Q$<br>$P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$ | P | Q | $P \leftrightarrow Q$ |
|---------------------------------------------------------------------------------------------------|---|---|-------------------|-----------------------------------------------------------------------------------------------------------------------------|---|---|-----------------------|
|                                                                                                   | T | T | T                 |                                                                                                                             | T | T | T                     |
|                                                                                                   | T | F | F                 |                                                                                                                             | T | F | F                     |
|                                                                                                   | F | T | T                 |                                                                                                                             | F | T | F                     |
|                                                                                                   | F | F | T                 |                                                                                                                             | F | F | T                     |

$P \rightarrow Q$  is equivalent to

$$(\neg P) \vee Q$$

$$P \rightarrow Q \equiv (\neg P) \vee Q$$

"x is even"  $\leftrightarrow$  " $x^2$  is even"  
 "P if and only if Q"  
 "P iff Q"

This is a true statement for integers.  
 The conditional statement  
 $Q \rightarrow P$   
 is the converse of  $P \rightarrow Q$ .

In order to prove  $P \rightarrow Q$ , one typically does so by assuming  $P$  and then proceeding to prove  $Q$  as a consequence.

In order to prove  $P \leftrightarrow Q$ , one typically proves  $P \rightarrow Q$  and then also prove  $Q \rightarrow P$ .

Sets e.g. the set  $A = \{1, 2, 5\}$  contains three <sup>(members)</sup> elements 1, 2, 5:

$1 \in A$   
 $2 \in A$   
 $5 \in A$   
 $7 \notin A \equiv \neg (7 \in A)$

$\in$  epsilon

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$

$\{\} = \emptyset$   
the empty set

nothing

$B = \{1, 4, \{1, 7\}, \{1, 2, 4\}, \{2\}\}$  has 5 elements

$1 \in B$   
 $2 \notin B$   
 $\{2\} \in B$   
 $7 \notin B$   
 $13 \notin B$

$\{1, 1, 3\} = \{1, 3\}$   
 $= \{3, 1\}$

A set is completely specified by its elements.

Discrete vs. Continuous

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$   $\mathbb{R}$   $[5, 8] = \{x \in \mathbb{R} \mid 5 \leq x \leq 8\}$

$1 \in \{1, 7\} \in B$

If  $A$  and  $B$  are sets then their <sup>5</sup>union is  $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

<sup>8</sup>intersection:  $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

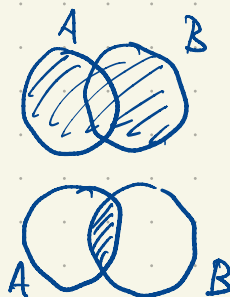
$A \subseteq B$  means  $x \in B$  for all  $x \in A$ . (Every element of  $A$  is an element of  $B$ .)

" $A$  is a subset of  $B$ "

If  $A = B$  then  $A \subseteq B$ . (Not conversely!)

$A = B$  is equivalent to  $A \subseteq B$  and  $B \subseteq A$ .

$\subsetneq \subsetneq \subsetneq$  



Warning:  $A \subset B$  can mean "A is a proper subset of B" but some people use it to just mean "A is a subset of B".

(A is a subset of B but not equal to B)  
Is there any confusion between  $x < y$  and  $x \leq y$ ?



$$\{\} = \emptyset$$

The power set of a set  $A$  is the set of all subsets of  $A$ :

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

$$\mathcal{P}(\{2, 5\}) = \{\emptyset, \{2\}, \{5\}, \{2, 5\}\}$$

$$\{2\} \subseteq \{2, 5\}$$

$$\{2\} \neq \{2, 5\}$$

$$2 \in \{2, 5\}$$

$$\{2\} \in \mathcal{P}(\{2, 5\})$$

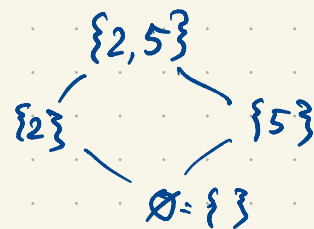
Can a set be an element of itself?

Let  $S = \{x \mid x \text{ is a set, } x \notin x\}$

Does  $S \in S$ ? If  $S \in S$  then  $S \notin S$ .  
If  $S \notin S$  then  $S \in S$ .

Russell's Paradox

$\mathcal{P}(A)$



If  $S$  has  $n$  elements then  $\mathcal{P}(S)$  has  $2^n$  elements

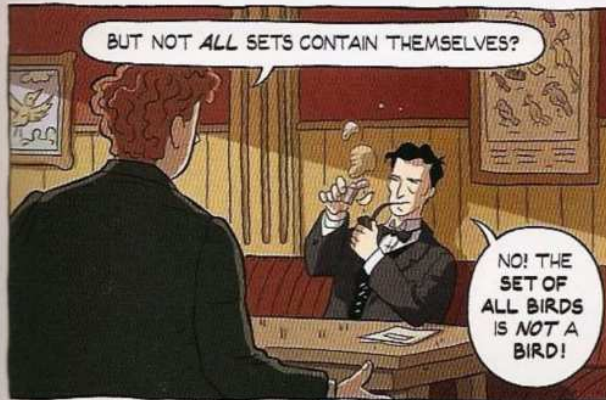
$\emptyset = \{\}$  has no elements

$$\mathcal{P}(\emptyset) = \{\emptyset\} = \{\{\}\} \quad \text{" 1 element"}$$

$A = \{\emptyset\}$  has one element

$$\Rightarrow \mathcal{P}(A) = \{\emptyset, A\} = \{\emptyset, \{\emptyset\}\} = \{\{\}, \{\{\}\}\}$$

$A$   
|  
 $\emptyset$



An alphabet is a (usually finite) set of symbols

eg.  $\{a, b, c, \dots, z\}$  (lower case Roman letters)

$\{0, 1\}$  (binary alphabet)

$\{0, 1, 2, \dots, 9, A, B, C, D, E, F\}$  (hexadecimal alphabet)

ASCII

$$A = \{a, b, c, \dots, z\} \quad |A| = 26$$

A word of length  $n$  over  $A$  is a string of letters, eg. 'dqqjl' is a word (string) of length 5.

$A^n$  = set of all words of length  $n$  over the alphabet  $A$ .  $|A^n| = |A|^n = 26^n$

There are  $26^n$  words of length  $n$  over  $A$ .

$$a_0 + a_1 + a_2 + \dots = \sum_{n=0}^{\infty} a_n$$

$$A^0 = \{''\}$$

$$A^* = A^0 \cup A^1 \cup A^2 \cup A^3 \cup \dots = \bigcup_{n=0}^{\infty} A^n$$
$$= \underbrace{\{''\}}_{A^0}, \underbrace{\{a, b, c, \dots, z\}}_{A^1}, \underbrace{\{aa, ab, \dots, az, ba, bb, \dots, bz, \dots, za, zb, \dots, zz\}}_{A^2}, \dots$$

The union of three sets  $A, B, C$  can be written as  $A \cup B \cup C$

If  $A \cap B = \emptyset$  and  $A \cap C = \emptyset$  and  $B \cap C = \emptyset$  then  $A, B, C$  are disjoint sets

$$\text{and } |A \cup B \cup C| = |A| + |B| + |C|$$

$|A|$  = size of  $A$  = number of elements of  $A$  = cardinality of  $A$ .

Early 20<sup>th</sup> century: axioms for set theory (ZFC = Zermelo-Fraenkel + Choice)

$\emptyset$  is a set. From  $\emptyset$  we recursively build new sets from old sets

$\mathbb{R}$  is a set.  $[5, 8] = \{x \in \mathbb{R} \mid 5 \leq x \leq 8\}$

"set-builder notation" for constructing sets

↑ or colon

Example: Truth-table for  $(P \wedge Q) \rightarrow R$  and  $P \wedge (Q \rightarrow R)$

| P | Q | R | $P \wedge Q$ | $(P \wedge Q) \rightarrow R$ | $Q \rightarrow R$ | $P \wedge (Q \rightarrow R)$ |
|---|---|---|--------------|------------------------------|-------------------|------------------------------|
| T | T | T | T            | T                            | T                 | T                            |
| T | T | F | T            | F                            | F                 | F                            |
| T | F | T | F            | T                            | T                 | T                            |
| T | F | F | F            | T                            | T                 | T                            |
| F | T | T | F            | T                            | T                 | F                            |
| F | T | F | F            | T                            | F                 | F                            |
| F | F | T | F            | T                            | T                 | F                            |
| F | F | F | F            | T                            | T                 | F                            |

Cardinality of sets:

$|A| = |B|$  means there is a one-to-one correspondence between the two sets.

$|A| \leq |B|$  means there is a one-to-one correspondence between elements of A and elements of a subset of B.

There is no such thing (in ZFC set theory) as the "set of all sets"

as this leads back to a contradiction (one guise of Russell's Paradox)

If  $U = \{x \mid x \text{ is a set}\}$  is a set then  $S = \{x \in U \mid x \notin x\}$  would be a set.

$\{x \mid x \text{ is a set}\}$  (in ZFC) is a "class" but not a set (a "proper class")

Kurt Gödel

Incompleteness Theorem: Axioms cannot be strong enough to do useful things and be provably free from inconsistency.



Quantifiers in logic: universal and existential quantifiers

For every real number  $x$ ,  $x^2 \geq 0$ .

universal quantifier  
 $x^2 \geq 0$  whenever  $x \in \mathbb{R}$ .

If  $x$  is a real number then  $x^2 \geq 0$ .

Here the universal quantifier "for all" or "for every" or "always" or "whenever" or ...

Let  $x$  be a real number. Then  $x^2 \geq 0$ .

$$(\forall x \in \mathbb{R})(x^2 \geq 0)$$

→  $(\forall x)(x^2 \geq 0)$  example of  $(\forall x)(P(x))$

There exists a real number  $x$  such that  $x^2 = 2$ .

existential quantifier  
 $x^2 = 2$  for some  $x \in \mathbb{R}$ .

There is an  $x \in \mathbb{R}$  such that  $x^2 = 2$ .

$$(\exists x \in \mathbb{R})(x^2 = 2) \quad \text{or} \quad (\exists x)(P(x))$$

→  $(\exists x)(x^2 = 2)$

$$(x+y)^2 = x^2 + 2xy + y^2$$

(for all  $x$  and  $y$  in  $\mathbb{R}$ )

$$(x+y)^2 = x^2 + y^2$$

for some  $x$  and  $y$  in  $\mathbb{R}$

permissible only if  $\mathbb{R}$  is understood from context



$\neg (\forall x)(P(x))$  is equivalent to  $(\exists x)(\neg P(x))$  de Morgan's rules  
 $(\forall x)(\neg P(x)) \quad \dots \quad \neg (\exists x)(P(x))$

eg.  $x \in \{\text{students in this room}\}$

Every student in this room is wearing blue. To say this is false (i.e. to negate the statement) is equivalent to saying that there is at least one student in the room not wearing blue.

$(\exists! x)(P(x))$  says there exists one and only one  $x$  (in the "universe") for which  $P(x)$

$P$ : Every elephant in this room weighs three pounds. This is true. (true in the vacuous sense)

$\neg P$ : Not every elephant in this room weighs three pounds.  
 i.e. there exists an elephant in this room weighing something other than three pounds.

If  $\neg P$  is false (which it certainly is) then  $P$  must be true.

$(\forall x \in \emptyset)(x = x+1)$  is true vacuously.

de Morgan's laws for set theory:

Let  $A$  be a set and  $C = \{X_a \mid a \in X\}$  be a collection of sets  $X_a$  indexed by  $a \in A$ .

eg.  $A = \mathbb{R}$ ,  $C = \{[a, \infty) : a \in \mathbb{R}\}$

$$[a, \infty) = \{x \in \mathbb{R} \mid x \geq a\} \quad \xrightarrow{\quad} \quad a$$

$$\bigcup_{a \in \mathbb{R}} [a, \infty) = \mathbb{R}$$

$$\bigcap_{a \in \mathbb{R}} [a, \infty) = \emptyset$$

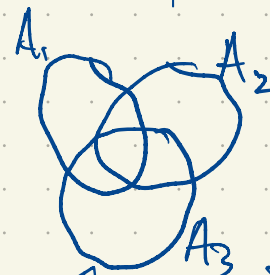
$$\bigcup_{a \in \mathbb{R}} (-\infty, a) = \mathbb{R} = \overline{\bigcap_{a \in \mathbb{R}} (-\infty, a)} = \overline{\emptyset}$$



$$\bar{A} = A^c = \{x \mid x \notin A\}$$

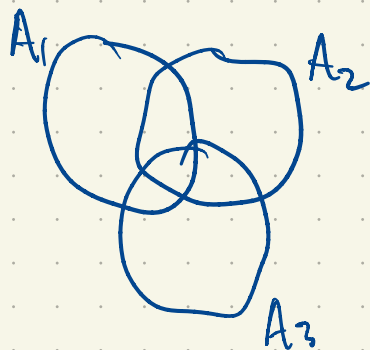
$$\overline{\bigcup_{c \in C}} = \bigcap_{c \in C} \bar{c}$$

$$\overline{\bigcap_{c \in C}} = \bigcup_{c \in C} \bar{c}$$

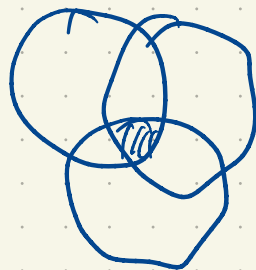


$$C = \{A_1, A_2, A_3\}$$





$$\mathcal{C} = \{A_1, A_2, A_3\}$$



$$\bigcap_{C \in \mathcal{C}} C$$

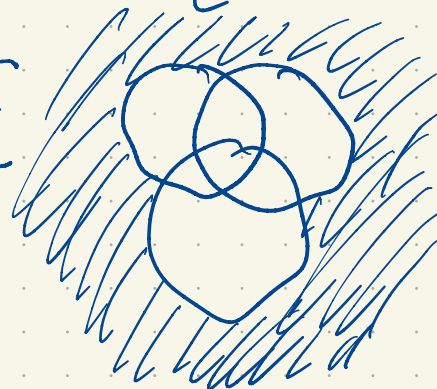


$$\overline{\bigcap_{C \in \mathcal{C}} C} = \bigcup_{C \in \mathcal{C}} \bar{C}$$

$$\bigcup_{C \in \mathcal{C}} C$$

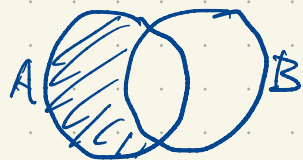


$$\overline{\bigcup_{C \in \mathcal{C}} C}$$



$$= \bigcap_{C \in \mathcal{C}} \bar{C}$$

Difference operation for two sets A, B



$$A - B = \{x \in A \mid x \notin B\}$$

or  $A \setminus B$   
or  $A \backslash B$

↪ backslash not / "slash"

$$\bar{A} = \{x \mid x \notin A\} \quad \{x \in U \mid x \notin A\}$$

The symmetric difference of two sets A, B

$$A \Delta B = B \Delta A$$

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

(the set-theoretic analogue of exclusive "or")

$$A \Delta B = \{x \in A \cup B \mid x \notin A \cap B\}$$



Nested quantifiers

$$\begin{aligned} &(\forall x)(\forall y)(P(x,y)) \\ &(\exists x)(\exists y)(P(x,y)) \\ &(\forall x)(\exists y)(P(x,y)) \\ &(\exists x)(\forall y)(P(x,y)) \end{aligned}$$

$$x \in \mathbb{Z}$$

$$(\forall x)(P(x)) \equiv (\forall u)(P(u))$$

If  $P(x)$ :  $x$  is either even or odd.

$(\forall x)(P(x))$ : Every integer is either even or odd.

$(\forall u)(P(u))$ :

Go back to  $\mathbb{R}$ :

$$P(x,y): x^2 + y^2 \geq 0$$

$(\forall x)(\forall y)(x^2 + y^2 \geq 0)$  is true.

$(\forall x)(\forall y)(x^2 + y^2 > 0)$  is false.  $(x,y) = (0,0)$  is a counterexample.

$(\forall x)(x^2 + y^2 > 0)$  depends on  $y$ .

If  $y \neq 0$  then  $(\forall x)(x^2 + y^2 > 0)$  is true.

If  $y = 0$  then  $(\forall x)(x^2 + y^2 > 0)$  is false.

( $x=0$  is a counterexample)

$$(\forall x)(\forall y)(P(x,y)) \equiv (\forall y)(\forall x)(P(x,y))$$

We sometimes write  $(\forall x,y)(P(x,y))$

$$(\exists x)(\exists y)(P(x,y)) \equiv (\exists y)(\exists x)(P(x,y))$$

$(\exists x,y)(P(x,y))$

$$(\exists x)(\exists y)(x^2 + y^2 = 0)$$

true if  $(x,y) = (0,0)$

true if  $x=0$

true.

$x, y, z, \dots$  real variables  
 $k, l, m, n, \dots$  integer variables

$(\forall k \geq 0)(\exists l)(k^2 = l)$  is true (in  $\mathbb{Z}$ )

$(\forall k \geq 0)(\exists l)(k = l^2)$  is false

$(\forall x \geq 0)(\exists y)(y^2 = x)$  is true (in  $\mathbb{R}$ ).

$(\exists l)(\forall k \geq 0)(k^2 = l)$  is false

$\int f(x,y) dy$  is a function of  $x$

$\int (\int f(x,y) dy) dx$  is a constant.

$$\int_0^1 (x+y)^2 dx = \frac{1}{3}(x+y)^3 \Big|_{x=0}^{x=1} = \frac{1}{3}(y+1)^3 - \frac{1}{3}y^3$$

$$\int_0^1 (\dots) dy = \text{number}$$

$(\forall x)(\exists y)(x < y)$  is true  
 $(\exists y)(\forall x)(x < y)$  is false

Suppose  $f: \mathbb{R} \rightarrow \mathbb{R}$  ( $f$  is a function having real number inputs and outputs).  
 To say  $f$  is continuous (everywhere) means, by definition:

For all  $x, a \in \mathbb{R}$  and for all  $\varepsilon > 0$ , there exists  $\delta > 0$  such that  $|f(x) - f(a)| < \varepsilon$  whenever  $|x - a| < \delta$ .

$$(\forall x \in \mathbb{R})(\forall a \in \mathbb{R})(\forall \varepsilon > 0)(\exists \delta > 0) \left( \underbrace{|x - a| < \delta}_{x \in (a - \delta, a + \delta)} \rightarrow \underbrace{|f(x) - f(a)| < \varepsilon}_{f(x) \in (f(a) - \varepsilon, f(a) + \varepsilon)} \right) \quad \leftarrow \text{Property of } f$$

Continuity at  $a \in \mathbb{R}$ :

$$(\forall x \in \mathbb{R})(\forall \varepsilon > 0)(\exists \delta > 0)(|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon). \quad \leftarrow \text{Property of } f \text{ which depends on } a.$$

$$(\exists \delta > 0)(P(\delta)) \quad \text{means} \quad (\exists \delta)(\delta > 0 \wedge P(\delta))$$

$$(\forall \delta > 0)(P(\delta)) \quad \text{means} \quad (\forall \delta)(\delta > 0 \rightarrow P(\delta))$$

A function  $f: A \rightarrow B$  allows us to input values in a set  $A$  with values (outputs) in a set  $B$ .

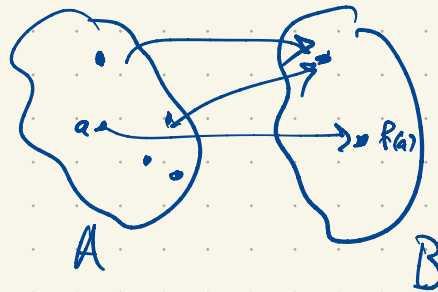
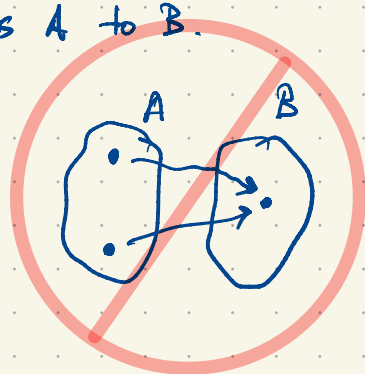
Note: ' $\rightarrow$ ' is 'to'.  $f$  maps  $A$  to  $B$ .

We write  $f: a \mapsto f(a)$

We say  $f$  is one-to-one if  
 no two points of  $A$  go to the  
 same point of  $B$

$$\text{i.e. } (\forall a, a' \in A)(f(a) = f(a') \rightarrow a = a')$$

$$\equiv (\forall a, a' \in A)(a \neq a' \rightarrow f(a) \neq f(a'))$$



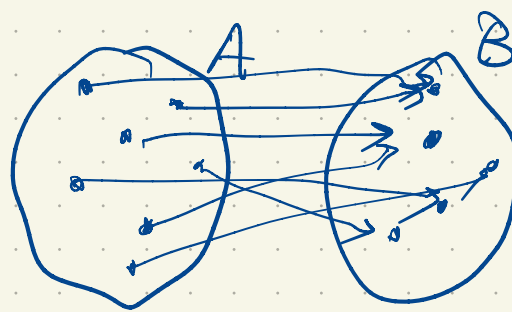
$Q \rightarrow P$  is the converse of  $P \rightarrow Q$   
 $(\neg Q) \rightarrow (\neg P)$  ... contrapositive of  $P \rightarrow Q$ .

$$(\neg Q) \rightarrow (\neg P) \equiv P \rightarrow Q$$

When is  $f: A \rightarrow B$  onto?

$f$  is onto  $B$  if every element of  $B$  is the value of  $f(a)$  for some  $a \in A$ .

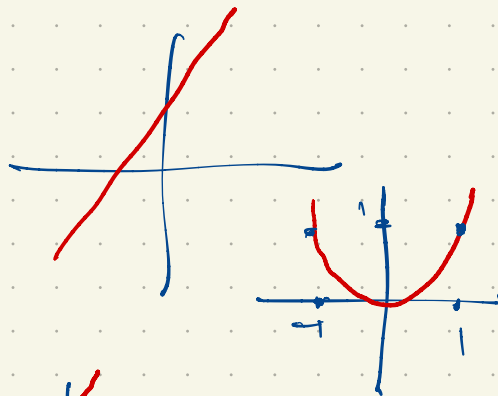
$$(\forall b \in B)(\exists a \in A)(f(a) = b).$$



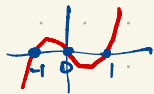
In Calculus,  $f: \mathbb{R} \rightarrow \mathbb{R}$

$f(x) = 3x + 1$  is one-to-one and onto

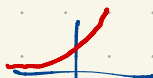
$f(x) = x^2$  is neither one-to-one nor onto



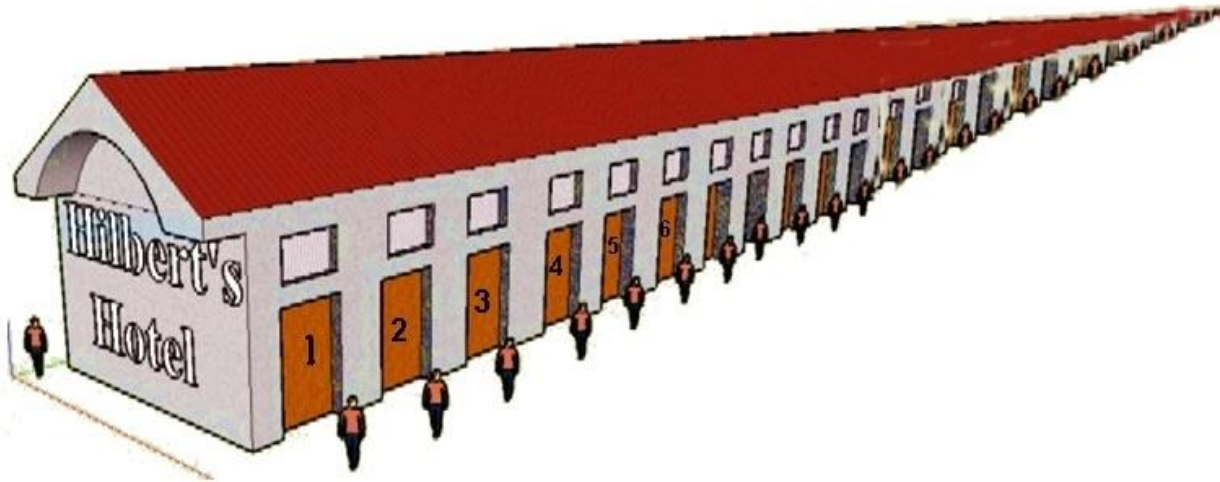
$f(x) = x^3 - x$  is onto but not one-to-one



$f(x) = e^x$  is one-to-one but not onto.



# Hilbert's Hotel



The sets that can be accommodated in Hilbert's Hotel are countable.

Two sets  $A, B$  have the same size (cardinality) if there exists a bijection  $f: A \rightarrow B$  (i.e.  $f$  is one-to-one and onto); in other words, we can match up the elements of  $A$  with the elements of  $B$ , i.e. there is a "one-to-one correspondence" between  $A$  and  $B$ . (We write  $|A| = |B|$ .)

We say  $|A| \leq |B|$  if  $A$  has the same size as some subset of  $B$ , i.e.  $|A| = |C|$  for some  $C \subseteq B$ , i.e. there exists a function  $f: A \rightarrow B$  which is one-to-one (not necessarily onto).

eg.  $|\mathbb{Z}| \leq |\mathbb{R}|$

$$|\mathbb{Z}| \leq |\mathbb{Q}|$$

$$|\{\text{even integers}\}| \leq |\mathbb{Z}|$$

$$2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, 6, \dots\}$$

Whenever  $A \subseteq B$ ,  $|A| \leq |B|$ .

Theorem If  $A, B$  are sets such that  $|A| \leq |B|$  and  $|B| \leq |A|$  then  $|A| = |B|$ . The Cantor-Schröder-Bernstein Theorem.

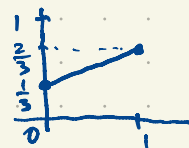
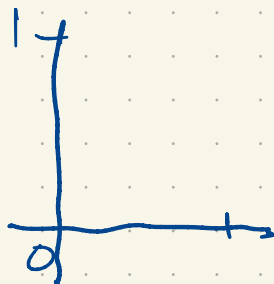
Example:  $|[0, 1]| = |(0, 1)|$  because  $|(0, 1)| \leq |[0, 1]|$

The function  $f: (0, 1) \rightarrow [0, 1]$

$f(x) = x$  is one-to-one (not onto)

A function  $g: [0, 1] \rightarrow (0, 1)$  that is also one-to-one is

eg.  $g(x) = \frac{x+1}{3}$  so  $|[0, 1]| \leq |(0, 1)|$





$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$$

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

$|\mathbb{N}| = |\mathbb{Z}|$  using the bijection

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots\}$$

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, 4, -4, 5, -5, \dots\}$$

$$\mathbb{N} \cup \{0\} = \{0, 1, 2, 3, 4, 5, 6, \dots\}$$

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, \dots\}$$

If  $|A| = |B|$  and  $|B| = |C|$  then  $|A| = |C|$ .

If  $|A| \leq |B|$  and  $|B| \leq |C|$  then  $|A| \leq |C|$ .

$|\mathbb{N}| = |\mathbb{Q}|$  A grid showing every rational number exactly once:

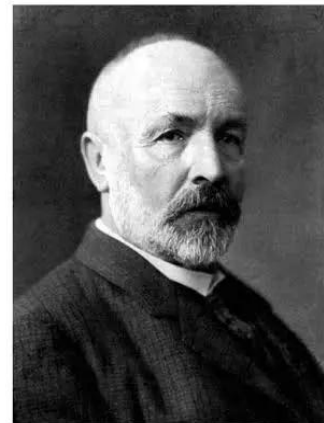
|     |      |     |      |     |      |     |      |     |      |      |     |
|-----|------|-----|------|-----|------|-----|------|-----|------|------|-----|
| 0   | 1    | -1  | 2    | -2  | 3    | -3  | 4    | -4  | 5    | -5   | ... |
| 1/2 | -1/2 | 3/2 | -3/2 | 5/2 | -5/2 | 7/2 | -7/2 | 9/2 | -9/2 | 11/2 | ... |
| 1/3 | -1/3 | 2/3 | -2/3 | 4/3 | -4/3 | 5/3 | -5/3 | 7/3 | -7/3 | 8/3  | ... |
| 1/4 | -1/4 | 3/4 | -3/4 | 5/4 | -5/4 | 7/4 | -7/4 | 9/4 | -9/4 | 11/4 | ... |
| 1/5 | -1/5 | 2/5 | -2/5 | 3/5 | -3/5 | 4/5 | -4/5 | 6/5 | -6/5 | ...  | ... |
| 1/6 | -1/6 | 5/6 | -5/6 | 7/6 | -7/6 | ... | ...  | ... | ...  | ...  | ... |
| 1/7 | -1/7 | 2/7 | -2/7 | 3/7 | -3/7 | ... | ...  | ... | ...  | ...  | ... |
| 1/8 | -1/8 | 3/8 | -3/8 | ... | ...  | ... | ...  | ... | ...  | ...  | ... |
| ... | ...  | ... | ...  | ... | ...  | ... | ...  | ... | ...  | ...  | ... |

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, \dots\}$$

$$\mathbb{Q} = \{0, \frac{1}{2}, 1, -1, -\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, -\frac{1}{3}, \dots\}$$

Georg  
Cantor

1845-1918



A set  $S$  is countable if it can be listed as

finite  $\rightarrow S = \{a_1, a_2, \dots, a_n\}$  for some  $n$

or countably infinite  $\rightarrow S = \{a_1, a_2, a_3, a_4, a_5, \dots\}$   
 $= \{a_n \mid n \in \mathbb{N}\}$

$\mathbb{R}$  is uncountable: its elements cannot be listed in this way.

Theorem (Cantor) If  $S$  is any set, then  $\mathcal{P}(S) = \{\text{all subsets of } S\}$  satisfies  $|\mathcal{P}(S)| > |S|$ .

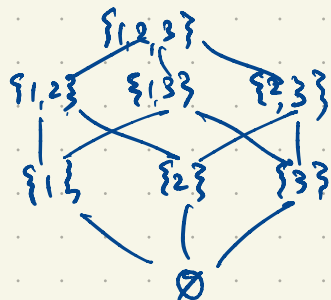
If  $|S| < \infty$ , say  $|S| = n$ , then  $|\mathcal{P}(S)| = 2^n > n$ .

If  $S$  is any set,  $|S| \leq |\mathcal{P}(S)|$

There is a one-to-one function  $S \rightarrow \mathcal{P}(S)$   
 $a \mapsto \{a\}$  (singleton sets, i.e. sets of cardinality 1).

$$\mathcal{P}(\{1,2,3\}) =$$

$$S = \{1,2,3\}$$



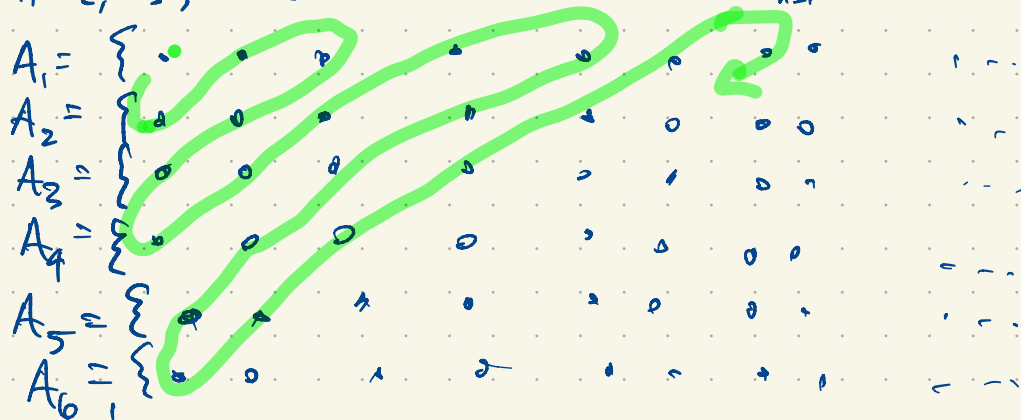
Why is  $|S| < |\mathcal{P}(S)|$ ?

We must show  $|S| \neq |\mathcal{P}(S)|$

Suppose  $|S| = |\mathcal{P}(S)|$  i.e. there is a bijection  $f: S \rightarrow \mathcal{P}(S)$ . For every  $a \in S$ ,  $f(a) \subseteq S$   
 and every subset  $B \subseteq S$  has the form  $B = f(a)$  for some  $a \in S$ . We need a contradiction.  
 Consider the subset  $B \subseteq S$  defined by  $B = \{a \in S : a \notin f(a)\}$ . We must have  $B = f(b)$  for some  $b \in S$ .  
 Does  $b \in B = f(b)$ ? If so,  $b \in f(b) = B$  then  $b \notin f(b)$ .  
 If not,  $b \notin f(b)$  then  $b \in B = f(b)$ .

This is a contradiction.

If  $A_1, A_2, A_3, \dots$  are countable sets then  $\bigcup_{n=1}^{\infty} A_n = A_1 \cup A_2 \cup A_3 \cup \dots$  is countable.



An infinite set is a set with infinitely many elements.

Bitstrings (binary strings / binary words / words over the alphabet  $\{0, 1\}$ , the binary alphabet)  
 Eg. words of finite length form a countable set: there are only countably many words of finite length over any finite alphabet.

If we consider infinitely long strings over a finite alphabet such as the binary alphabet, then we have uncountably many such infinite strings.

$$\{1, 5, 6, 8, 11, 13, 19, 20, 21, \dots\} \leftrightarrow 1000110100101 \dots$$

Uncountably many infinite strings of 0's and 1's.

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| \text{ is countable}$$

Another proof that  $\mathbb{R}$  is uncountable:  $|\mathbb{R}| = |(0, 1)|$

Suppose the elements of  $(0, 1)$  can be listed in an infinite list as

$$(0, 1) = \{a_1, a_2, a_3, a_4, a_5, \dots\}$$

$$a_1 = 0.a_{11} a_{12} a_{13} a_{14} a_{15} a_{16} a_{17} \dots$$

$$a_2 = 0.a_{21} a_{22} a_{23} a_{24} a_{25} \dots$$

$$a_3 = 0.a_{31} a_{32} a_{33} a_{34} a_{35} \dots$$

$$a_4 = 0.a_{41} a_{42} a_{43} a_{44} a_{45} \dots$$

$$a_5 = 0.a_{51} a_{52} a_{53} a_{54} a_{55} \dots$$

$a_{ij} \in \{0, 1, 2, \dots, 9\} \quad i \geq 1, j \geq 1$   
 (the  $j^{\text{th}}$  decimal digit of the  $i^{\text{th}}$  number in my list)

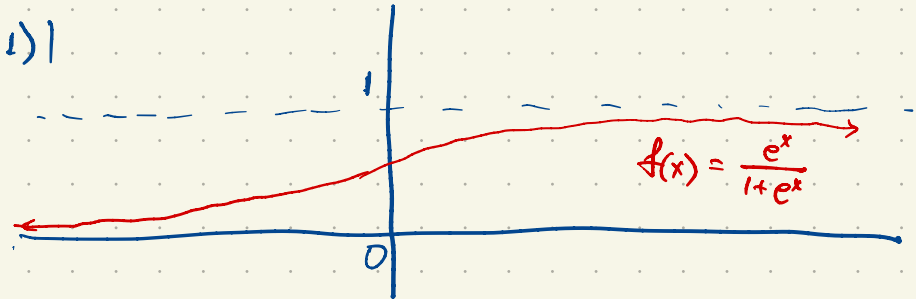
I give a number  $b \in (0, 1)$  which is not in this list, hence we have a contradiction.

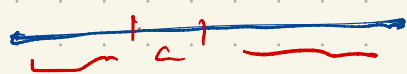
Take  $b = 0.b_1 b_2 b_3 b_4 b_5 \dots$   $b_j \in \{0, 1, 2, \dots, 9\}$  defined as:

$$b_j = \begin{cases} 3 & \text{if } a_{jj} \neq 3 \\ 7 & \text{if } a_{jj} = 3 \end{cases}$$

so  $b_j \neq a_{jj}$  for any  $j$ .

$b \neq a_i$  because they don't have the same  $i^{\text{th}}$  digit.





Flip a fair coin repeatedly until we get heads (H).  
 How many times will we flip the coin waiting for this to happen?  
 With probability  $\frac{1}{2}$ , only 1 flip is needed.

With probability  $\frac{1}{4}$ , it takes 2 flips TH

With probability  $\frac{1}{8}$ , it takes 3 flips TTH

With probability  $\frac{1}{2^n}$ , it takes n flips

With probability 0, we never get H: TTTTTT...

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots = 1$$

$$|\{11, 13, 18\}| = 3$$

$$V_3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$

$$V_0 = \emptyset, V_1 = \{V_0\}, V_2 = V_1 \cup \{V_1\} = \{\emptyset, \{\emptyset\}\}$$

John Von Neumann:  $V_0, V_1, V_2, V_3, \dots$   
 $V_\omega = \bigcup_{n=0}^{\infty} V_n$   
 $V_{\omega+1} = V_\omega \cup \{V_\omega\}$   
 $|V_n| = n$

- Proofs :
- creating proofs
  - reading/checking proofs.

Some instructive examples of proofs:

## Proof by contradiction

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

Theorem  $\sqrt{2}$  is irrational, i.e.  $\sqrt{2} \notin \mathbb{Q}$ .

Proof Suppose  $\sqrt{2} \in \mathbb{Q}$ , say  $\sqrt{2} = \frac{a}{b}$ ,  $a, b$  positive integers in lowest terms. Then  $2 = \frac{a^2}{b^2}$  so  $a^2 = 2b^2$  is even so  $a$  is even; say  $a = 2c$  for some positive integer  $c$ . Then  $2c^2 = b^2$ , so  $b$  is even, i.e.  $b = 2s$  for some integer  $s$ . Then the fraction  $\frac{a}{b}$  was not reduced, a contradiction. Therefore  $\sqrt{2} \notin \mathbb{Q}$ .  $\square$

Structure of a proof of  $P$  by contradiction: Start by declaring the assumption  $\neg P$  and deriving a contradiction from this. Thereby claim the conclusion that  $P$  is true.

Theorem  $2=1$ .

Proof Suppose  $a=b$ . Multiply both sides by  $b$  to get  $ab=b^2$ . So  $ab-a^2=b^2-a^2$  and  $a(b-a) = (b+a)(b-a)$  so  $a = b+a$  i.e.  $b = b+b = 2b$  so  $1=2$ .  $\square$

$$a(b-a) = (b+a)(b-a)$$

$$5x = 5y \Rightarrow x = y$$

$$5x = 5y \Rightarrow \frac{5x}{5} = \frac{5y}{5} \Rightarrow x = y$$

$$\frac{0 \cdot 8}{0} = \frac{0 \cdot 11}{0}$$

$$0 \cdot 8 = 0 \cdot 11$$

You cannot divide by 0.

For  $k, l, m, n, \dots \in \mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ , we say  $k$  is even if it's divisible by 2, i.e.  $k = 2l$  for some  $l \in \mathbb{Z}$ . An integer  $k$  is odd if

(I)  $k$  is not even; equivalently,

(II)  $k$  is 1 more than an even integer i.e.  $k = 2l+1$  for some  $l \in \mathbb{Z}$ .

The equivalence of (I) and (II) is subtle. We will prove  $(\forall k \in \mathbb{Z})(P(k) \leftrightarrow Q(k))$ .

$$P(k) : (\forall l)(\neg(k=2l))$$

$$Q(k) : (\exists l)(k=2l+1)$$

Theorem Let  $k \in \mathbb{Z}$ . If  $k^2$  is even, then  $k$  is even.  
the proof uses "proof by contrapositive".  $\square$

The contrapositive of a conditional statement  $P \rightarrow Q$  is  $(\neg Q) \rightarrow (\neg P)$ .  
... converse — — —  $P \rightarrow Q$  is  $\equiv P \rightarrow Q$   
 $\neq Q \rightarrow P$

Proof We prove the contrapositive: if  $k$  is odd then  $k = 2l+1$  for some  $l \in \mathbb{Z}$  so  
 $k^2 = 2(2l^2 + 2l) + 1$  is odd.  $\square$ .

$$k = 2l+1$$

$$k^2 = (2l+1)^2$$

$$k^2 = (2l)^2 + 2 \cdot 2l \cdot 1 + 1^2$$

$$k^2 = 4l^2 + 4l + 1$$

$$k^2 = 2(2l^2 + 2l + 1)$$

~~Leave this out please~~

$$\begin{aligned} k^2 &= (2l+1)^2 = (2l)^2 + 2 \cdot 2l \cdot 1 + 1^2 \\ &= 4l^2 + 4l + 1 \\ &= 2(2l^2 + 2l) + 1 \end{aligned}$$



If  $x, y \in \mathbb{R}$ , then the average or mean or arithmetic mean of  $x$  and  $y$  is  $\frac{x+y}{2}$ .

Assuming  $x, y > 0$ , their geometric mean is  $\sqrt{xy}$ .

eg. the arithmetic mean of 3 and 5 is  $\frac{3+5}{2} = 4$ ; the geometric mean of 3 and 5 is  $\sqrt{3 \cdot 5} = \sqrt{15} \approx 3.872983$ .

Theorem If  $x, y > 0$  then  $\underbrace{\sqrt{xy}}_{\text{geometric mean}} \leq \underbrace{\frac{x+y}{2}}_{\text{arithmetic mean}}$ . Moreover, equality holds iff  $x=y$ .

Proof Since  $(x-y)^2 \geq 0$  we have  $x^2 - 2xy + y^2 \geq 0$  so  $x^2 + 2xy + y^2 \geq 4xy$  i.e.  $(x+y)^2 \geq 4xy$ .  
So  $x+y \geq \sqrt{4xy} = 2\sqrt{xy}$ . Finally,  $\frac{x+y}{2} \geq \sqrt{xy}$ .  $\square$

This is a direct proof... but where did the idea come from?