Ve203 Discrete Mathematics

Lecturer: Zach McKenzie

University of Michigan - Shanghai Jiaotong University
Joint Institute

Summer Term 2018

Course Information

- **Lecturer:** Zach McKenzie
- **Room:** 441B
- **Email:** `zachiri.mckenzie@sjtu.edu.cn`
- **Office Hours:** Monday 10am- noon
- **Teaching Assistants:** See CANVAS for their contact information
- **Recitation classes:** Teaching Assistants will lead a weekly recitation class that begins in the second week.

Use of Wikipedia and Other Sources; Honor Code Policy

When faced with a particularly difficult problem, you may want to refer to other textbooks or online sources such as Wikipedia. Here are a few guidelines:

- Outside sources may treat a similar sounding subject matter at a much more advanced or a much simpler level than this course. This means that explanations you find are much more complicated or far too simple to help you. For example, when looking up the "induction axiom" you may find many high-school level explanations that are not sufficient for our problems; on the other hand, wikipedia contains a lot of information relating to formal logic that is far beyond what we are discussing here.
- If you do use any outside sources to help you solve a homework problem, you are not allowed to just copy the solution; this is considered a violation of the Honor Code.

Use of Wikipedia and Other Sources; Honour Code Policy

- The correct way of using outside sources is to understand the contents of your source and then to write in your own words and without referring back to the source the solution of the problem. Your solution should differ in style significantly from the published solution. If you are not sure whether you are incorporating too much material from your source in your solutions, then you must cite the source that you used.
- You may cooperate with other students in finding solutions to assignments, but you must write your own answers. Do not simply copy answers from other students. It is acceptable to discuss the problems orally, but you may not look at each others' written notes. Do not show your written solutions to any other student. This would be considered a violation of the Honour Code.

Course Grade

The course contains four grade components:

- Three examinations,
- Assignments

The course grade will be calculated from these components using the following weighting:

- First midterm exam: 25%
- Second midterm exam: 25%
- Final exam: 25%
- Assignments: 25% (details to follow)

LaTeX Policy and Textbook

As engineers, you are strongly encouraged to familiarise yourselves with a mathematical typesetting program called LaTeX. This is open-source software, and there are various implementations available. I suggest that you use Baidu or Google to find a suitable implementation for your computer and OS.

While the use of LaTeX is **optional**, there will be a **10% bonus to the awarded marks** for those assignments handed in as typed LaTeX manuscripts.

The main textbook for this course is

- Rosen, K. H., *Discrete Mathematics and its Applications*, 6^{th} Ed., McGraw-Hill International Edition 2007.

Logic

Mathematical Logic, developed in the mid-1800s, gives mathematicians the tools to mathematicaly analyse the structure of language and arguments, and even treat notions such as “arguments", “truth", and “proof", that seemingly belong to the realm of philosophy, as mathematical notions. The development of mathematical logic helped mathematicians identify the foundamental assumptions that underpin mathematics and what constitutes a rigorous “proof" of a mathematical statement. Today, mathematical logic has found wide ranging applications:

- It underpins much of the work that is done in computional liguistics (with applications like speach recognition software)
- It provides the basis for formal verification tools that are essential for checking the correctness of computer software and hardware.
- It has allowed us to treat notions such as “algorithm" and “proof" as mathematical objects giving us insight into the limitations of computers and mathematics.

The Natural Numbers

Despite the wide ranging applications of logic, this course will focus on using mathematical logic to analyse mathematical statements and arguments. For this reason, most of our examples will be based on numbers. For now, we assume that the set of natural numbers

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

has been constructed. In particular, we assume that we know what a *set* is!
If n is a natural number, we write $n \in \mathbb{N}$. (We will later discuss naive set theory and give a formal construction of the natural numbers.)
We also assume that on $\mathbb{N}$ we have defined the operations of addition $+ \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and multiplication $\cdot \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and that their various properties (commutativity, associativity, distributivity) hold.

The Natural Numbers

Definition

Let $m, n \in \mathbb{N}$ be natural numbers.

(i) *We say that n is greater than or equal to m, writing $n \geq m$, if there exists some $k \in \mathbb{N}$ such that $n = m + k$. If we can choose $k \neq 0$, we say n is greater than m and write $n > m$.*

(ii) *We say that m divides n, writing $m \mid n$, if there exists some $k \in \mathbb{N}$ such that $n = m \cdot k$.*

(iii) *If $2 \mid n$, we say that n is even.*

(iv) *If there exists some $k \in \mathbb{N}$ such that $n = 2k + 1$, we say that n is odd.*

(v) *Suppose that $n > 1$. If there does not exist any $k \in \mathbb{N}$ with $1 < k < n$ such that $k \mid n$, we say that n is prime.*

It can be proven that every number is either even or odd and not both. We also assume this for the purposes of our examples.

Integers, rational, real and complex numbers

You should also be familiar (at least intuitively) with the integers ($\mathbb{Z}$), rational numbers ($\mathbb{Q}$), real numbers ($\mathbb{R}$), and complex numbers ($\mathbb{C}$), and we will use these entities to build examples.

- $\mathbb{Z}$ is the collection (set) of negative and nonnegative whole numbers
- $\mathbb{Q}$ is the set of numbers that can be obtained by taking fractions of integers with nonzero denominator
- Both $\mathbb{Q}$ and $\mathbb{Z}$ are equipped with a natural order relation, written $\leq$, "... is less than or equal to ..."
- $\mathbb{R}$ is the "completion" of $\mathbb{Q}$ defined by ensuring that every nonempty bounded subset of $\mathbb{R}$ has a least upper bound (this is the **least upper bound principle** that you used to define $\mathbb{R}$ in Calculus)
- The order $\leq$ on $\mathbb{Q}$ and $\mathbb{Z}$ extends to $\mathbb{R}$
- $\mathbb{C}$ is the set of all numbers in the form $a + bi$ where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$
- You should also be familiar wit the basic open, closed and clopen intervals of $\mathbb{R}$: (a, b), $[a, b]$, $(a, b]$ and $[a, b)$

Propositional Logic

Propositional logic represents a first-attempt at analysing the structure of statements and arguments.

Definition

*A **proposition** is a declarative sentence. I.e. a statement that is either true (T) or false (F), but not both.*

Example

- *"$2 + 2 = 4$" is a true proposition*
- *"27 is a prime number" is a false proposition*
- *"$x > 5^3$" is NOT a proposition (the variable x is not specified)*
- *"$7 + 6$" is NOT a proposition*

Just as letters are used to represent variables in mathematical formulae, we will also use letters $(A, B, C, p, q, \ldots)$ in propositional logic to denote **propositional variables**.

Propositional Logic

Compound expressions, **compound propositions** or **well-formed formulae** are are built up from propositions using **connectives**. There are five conectives availble to us in propositional logic: one unary connective (the connective prefixes a single proposition) $\neg$ (not), and four binary connectives $\vee$ (disjunction), $\wedge$ (conjunction), $\Rightarrow$ (implication) and $\iff$ (biconditional). Propositional logic is **truth functional**, which means that the truth value (T or F) assigned to a compound expression is completely determined by the truth values of the propositions that appear in the compund expression.

Definition

Let A be a (compound) proposition. The proposition $\neg A$ (pronounced "It is not the case that A") is the statement that is true if A is false, and false if A is true.

Example

If A is the proposition A: $2 > 3$, then the negation of A is $\neg A$: $2 \not> 3$.

Negation and Conjunction

The behaviour of the connective $\neg$ is convieniently represented using a **truth table**:

A	$\neg A$
T	F
F	T

We can now use truth tables to define the behaviour of the remaining connectives.

Definition

Let A and B be two (compound) propositions. Then we define the **conjunction** *of A and B, written $A \wedge B$, by the following truth table:*

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction

Definition

Let A and B be two propositions. Then we define the **disjunction** *of A and B, written $A \vee B$, by the following truth table:*

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

The disjunction $A \vee B$ is spoken "A or B". It is true only if either A or B is true, false otherwise.

Example

- *Let A: $2 > 0$ and B: $1 + 1 = 1$. Then $A \wedge B$ is false and $A \vee B$ is true.*
- *Let A be a proposition. Then the compound expression "$A \vee (\neg A)$" is always true, and "$A \wedge (\neg A)$" is always false.*

Proofs using Truth Tables

How do we prove that "$A \vee (\neg A)$" is an always true expression? We are claiming that $A \vee (\neg A)$ will be a true expression, regardless of whether the proposition A is true or not. To prove this, we go through all possibilities using a truth table:

A	$\neg A$	$A \vee (\neg A)$
T	F	T
F	T	T

Since the column for $A \vee (\neg A)$ only lists T for "true", we see that $A \vee (\neg A)$ is always true. A compound expression that is always true is called a **tautology**.

Correspondingly, the truth table for $A \wedge (\neg A)$ is

A	$\neg A$	$A \wedge (\neg A)$
T	F	F
F	T	F

so $A \wedge (\neg A)$ is always false. A compound expression that is always false is called a **contradiction**.

Implication

Definition

Let A and B be two propositions. Then we define the **implication** *of B and A, written $A \Rightarrow B$, by the following truth table:*

A	B	$A \Rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

In the expression $A \Rightarrow B$, A is called the **antecedent** *and B is called the* **consequence***.*

We read "$A \Rightarrow B$" as "A implies B", "if A, then B" or "A only if B". (The last formulation refers to the fact that A can not be true unless B is true.) Note that an implication $A \Rightarrow B$ is false (F) only when the antecedent (A) is true (T) and the consequence (B) is false (F).

Implication

Example

Consider the following infinite list of implications:

$$A_n\colon n \text{ is prime} \Rightarrow n \text{ is odd}, \qquad n \in \mathbb{N}, \tag{1}$$

- A_2 *is the expression* $(2 \textit{ is prime}) \Rightarrow (2 \textit{ is odd})$*. Since "2 is prime" is true and "2 is odd" is false,* A_2 *is false*
- A_3 *is the expression* $(3 \textit{ is prime}) \Rightarrow (3 \textit{ is odd})$*. Since "3 is prime" is true and "3 is odd" is true,* A_3 *is true*
- A_4 *is the expression* $(4 \textit{ is prime}) \Rightarrow (4 \textit{ is odd})$*. Since "4 is prime" is false and "4 is odd" is false,* A_4 *is true*
- A_9 *is the expression* $(9 \textit{ is prime}) \Rightarrow (9 \textit{ is odd})$*. Since "9 is prime" is false and "9 is odd" is true,* A_9 *is true*

Biconditional

Definition

Let A and B be two propositions. Then we define the **biconditional** *of A and B, written $A \Leftrightarrow B$, by the following truth table:*

A	B	$A \Leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

We read "$A \Leftrightarrow B$" as "A is equivalent to B" or "A if and only if B". Some textbooks abbreviate "if and only if" by "iff". If A and B are both true or both false, then they are equivalent. Otherwise, they are not equivalent. In propositional logic, "equivalence" is the closest thing to the "equality" of arithmetic.

Equivalence

On the one hand, logical equivalence is strange; two propositions A and B do not need to have anything to do with each other to be equivalent. For example, the statements "$2 > 0$" and "$100 = 99 + 1$" are both true, so they are equivalent.

On the other hand, we use equivalence to manipulate compound propositions.

Definition

Two compound propositions A and B are called **logically equivalent** *if $A \Leftrightarrow B$ is a tautology. We then write $A \equiv B$.*

Example

The two de Morgan rules are the tautologies

$$\neg(A \vee B) \Leftrightarrow (\neg A) \wedge (\neg B), \qquad \neg(A \wedge B) \Leftrightarrow (\neg A) \vee (\neg B).$$

In other words, they state that $\neg(A \vee B)$ is logically equivalent to $(\neg A) \wedge (\neg B)$ and $\neg(A \wedge B)$ is logically equivalent to $(\neg A) \vee (\neg B)$.

Contraposition

An important tautology is the equivalence of the proposition $A \Rightarrow B$ with its **contrapositive**: $\neg B \Rightarrow \neg A$.

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A).$$

For example, for any natural number n, the statement "$n > 0 \Rightarrow n^3 > 0$" is equivalent to "$n^3 \not> 0 \Rightarrow n \not> 0$" This principle is used in proofs by contradiction.
We prove the contrapositive using a truth table:

A	B	$\neg A$	$\neg B$	$\neg B \Rightarrow \neg A$	$A \Rightarrow B$	$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

Some Logical Equivalences

The following logical equivalences can be established using truth tables or by using previously proven equivalences. Here T is the compound statement that is always true, $T: A \vee (\neg A)$ and F is the compound statement that is always false, $F: A \wedge (\neg A)$

Equivalence	Name
$A \wedge T \equiv A$	Identity for $\wedge$
$A \vee F \equiv A$	Identity for $\vee$
$A \wedge F \equiv F$	Dominator for $\wedge$
$A \vee T \equiv T$	Dominator for $\vee$
$A \wedge A \equiv A$	Idempotency of $\wedge$
$A \vee A \equiv A$	Idempotency of $\vee$
$\neg(\neg A) \equiv A$	Double negation

Some Logical Equivalences

Equivalence	Name
$A \wedge B \equiv B \wedge A$	Commutativity of $\wedge$
$A \vee B \equiv B \vee A$	Commutativity of $\vee$
$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$	Associativity of $\wedge$
$(A \vee B) \vee C \equiv A \vee (B \vee C)$	Associativity of $\vee$
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$	Distributivity
$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$	Distributivity
$A \vee (A \wedge B) \equiv A$	Absorption
$A \wedge (A \vee B) \equiv A$	Absorption

These laws include all that are necessary for a *boolean algebra generated by* $\wedge$ *and* $\vee$ (identity element, commutativity, associativity, distributivity). Hence the name *boolean logic* for this calculus of logical statements.

Some Logical Equivalences

We omitted de Morgan's laws from the previous table.We now list some equivalences involving the implication.

Equivalence
$A \Rightarrow B \equiv \neg A \vee B \equiv \neg B \Rightarrow \neg A$
$(A \Rightarrow B) \wedge (A \Rightarrow C) \equiv A \Rightarrow (B \wedge C)$ $(A \Rightarrow B) \vee (A \Rightarrow C) \equiv A \Rightarrow (B \vee C)$
$(A \Rightarrow C) \wedge (B \Rightarrow C) \equiv (A \vee B) \Rightarrow C$ $(A \Rightarrow C) \vee (B \Rightarrow C) \equiv (A \wedge B) \Rightarrow C$
$(A \Leftrightarrow B) \equiv ((\neg A) \Leftrightarrow (\neg B))$ $(A \Leftrightarrow B) \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$ $(A \Leftrightarrow B) \equiv (A \wedge B) \vee ((\neg A) \wedge (\neg B))$ $\neg(A \Leftrightarrow B) \equiv A \Leftrightarrow (\neg B)$

Manipulating propositional expressions

One of the first things one learns in mathematics is to manipulate mathematical expressions using equations. For example, using the equation $(x+1)^2 = x^2 + 2x + 1$, one can see that

$$x^2 + 3x + 1 = (x+1)^2 + x$$

Propositional expressions can be manipulated in the same fashion using known logical equivalences. This provides a way of proving new logical equivalences.

Example

$\neg(A \Rightarrow B)$ *is equivalent to* $A \wedge \neg B$ *because*

$$\begin{aligned} \neg(A \Rightarrow B) &\equiv \neg(\neg A \vee B) \\ &\equiv \neg\neg A \wedge \neg B \\ &\equiv A \wedge \neg B \end{aligned}$$

Manipulating propositional expressions

Example

The expression $(A \wedge B) \Rightarrow (A \vee B)$ *is a tautology:*

$$
\begin{aligned}
(A \wedge B) \Rightarrow (A \vee B) &\equiv \neg(A \wedge B) \vee (A \vee B) \\
&\equiv (\neg A \vee \neg B) \vee (A \vee B) \\
&\equiv (A \vee \neg A) \vee (B \vee \neg B) \\
&\equiv T \vee T \\
&\equiv T
\end{aligned}
$$

Note that the order of operation for the propositional connectives is: bracketed expressions, then $\neg$, then $\wedge$ and $\vee$, then $\Rightarrow$ and $\iff$. Brackets should always be used to distinguish between $\wedge$ and $\vee$, and $\Rightarrow$ and $\iff$.

Arguments in propositional logic

Propositional logic gives us a tool that we can use to analyse the structure of arguments. Consider:

$$\text{If } \sqrt{2} > \frac{3}{2}, \text{ then } (\sqrt{2})^2 > \left(\frac{3}{2}\right)^2. \text{ We know that } \sqrt{2} > \frac{3}{2}.$$

$$\text{Therefore } (\sqrt{2})^2 > \left(\frac{3}{2}\right)^2.$$

This is an example of an argument. We have asserted some facts, call premises, that we know to be true, and using these premises we determined that a new fact, called the conclusion, is true. It is enlightening to examine what this looks like in propositional logic. Let A be the proposition "$\sqrt{2} > \frac{3}{2}$" and let B be the proposition "$(\sqrt{2})^2 > \left(\frac{3}{2}\right)^2$".Then, the two premises of the argument are $A \Rightarrow B$ and A, and the conclusion is B.

$$\begin{array}{rl} & A \Rightarrow B \\ & A \\ \hline \therefore & B \end{array}$$

Arguments

Definition

An **argument** *is a finite sequence of propositions. All propositions except for the final statement are called* **premises** *while the final statement is called the* **conclusion***. We say that an argument is* **valid** *if the truth of all premises implies the truth of the conclusion.*

From the definition of an argument it is clear that an argument consisting of a sequence of premises $P_1, \ldots, P_n$ and a conclusion C is valid of and only if

$$(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \Rightarrow C \tag{2}$$

is a tautology, i.e., a true statement for any values of the premises and the conclusion.We can write this argument as:

$$\begin{array}{rl} & P_1 \\ & P_2 \\ & \vdots \\ & P_n \\ \hline \therefore & C \end{array}$$

Arguments

The symbol $\therefore$ is pronounced "therefore". You may only use this symbol when constructing a logical argument in the notation above. Do not use it as a general-purpose abbreviation of "therefore".

On an earlier slide we saw the argument:

$$\begin{array}{rl} & A \Rightarrow B \\ & A \\ \hline \therefore & B \end{array}$$

To check that this argument is valid we need to verify that $((A \Rightarrow B) \wedge A) \Rightarrow B$ is a tautology.

A	B	$A \Rightarrow B$	$(A \Rightarrow B) \wedge A$	$\big((A \Rightarrow B) \wedge A\big) \Rightarrow B$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Hypothetical Syllogisms

Certain basic valid arguments in mathematics are given latin names and called **rules of inference**. A **syllogism** is an argument that has exactly two premises. We first give three **hypothetical syllogisms**, i.e., syllogisms involving the implication "$\Rightarrow$".

Rule of Inference	Name
$\begin{array}{ll} & A \Rightarrow B \\ & A \\ \hline \therefore & B \end{array}$	Modus (Ponendo) Ponens *Mode that affirms (by affirming)*
$\begin{array}{ll} & A \Rightarrow B \\ & \neg B \\ \hline \therefore & \neg A \end{array}$	Modus (Tollendo) Tollens *Mode that denies (by denying)*
$\begin{array}{ll} & A \Rightarrow B \\ & B \Rightarrow C \\ \hline \therefore & A \Rightarrow C \end{array}$	Transitive Hypothetical Syllogism

Hypothetical Syllogisms

Example

(i) *Modus ponendo ponens:*

If 3 is both prime and greater than 2, then 3 is odd
3 is both prime and greater than 2

$\therefore$ *3 is odd.*

(ii) *Modus tollendo tollens:*

If 4 is both prime and greater than 2, then 4 is odd
4 is not odd

$\therefore$ *4 is not both prime and greater than 2.*

(iii) *Transitive hypothetical syllogism:*

If 5 is greater than 4, then 5 is greater than 3
If 5 is greater than 3, then 5 is greater than 2

$\therefore$ *If 5 is greater than 4, then 5 is greater than 2.*

Disjunctive and Conjunctive Syllogisms

There are two important syllogisms involving the disjunction "$\vee$" and the conjunction "$\wedge$":

Rule of Inference	Name
$\begin{array}{rl} & A \vee B \\ & \neg A \\ \hline \therefore & B \end{array}$	Modus Tollendo Ponens *Mode that affirms by denying*
$\begin{array}{rl} & \neg(A \wedge B) \\ & A \\ \hline \therefore & \neg B \end{array}$	Modus Ponendo Tollens *Mode that denies by affirming*
$\begin{array}{rl} & A \vee B \\ & \neg A \vee C \\ \hline \therefore & B \vee C \end{array}$	Resolution

Disjunctive and Conjunctive Syllogisms

Example

(i) *Modus tollendo ponens:*

$$\begin{array}{rl} & \textit{4 is odd or even} \\ & \textit{4 is not odd} \\ \hline \therefore & \textit{4 is even.} \end{array}$$

(ii) *Modus ponendo tollens:*

$$\begin{array}{rl} & \textit{4 is not both even and odd} \\ & \textit{4 is even} \\ \hline \therefore & \textit{4 is not odd.} \end{array}$$

(iii) *Resolution:*

$$\begin{array}{rl} & \textit{4 is even or 4 is greater than 2} \\ & \textit{4 is odd or 4 is prime} \\ \hline \therefore & \textit{4 is greater than 2 or 4 is prime.} \end{array}$$

Some Simple Arguments

Finally, we give some seemingly obvious, but nevertheless useful, arguments:

Rule of Inference	Name
$$\begin{array}{rl} & A \\ & B \\ \hline \therefore & A \wedge B \end{array}$$	Conjunction
$$\begin{array}{rl} & A \wedge B \\ \hline \therefore & A \end{array}$$	Simplification
$$\begin{array}{rl} & A \\ \hline \therefore & A \vee B \end{array}$$	Addition

Examples for these are left to the reader!

Validity and Soundness

The previous rules of inference are all *valid arguments*. In the examples we gave, the arguments always led to a correct conclusion. This was, however, only because all the premises were true statements. It is possible for a valid argument to lead to a wrong conclusion if one or more of its premises are false.

If, in addition to being valid, an argument has only true premises, we say that the argument is **sound**. In that case, its conclusion is true.

Example

The following argument is valid (it is based on the rule of resolution), but not sound:

$$\begin{array}{rl} & \textit{4 is even or 4 is prime} \\ & \textit{4 is odd or 4 is prime} \\ \hline \therefore & \textit{4 is prime.} \end{array}$$

(The second premise is false, so the conclusion doesn't have to be true.)

Non Sequitur

The term **non sequitur** (latin for "it does not follow") is often used to describe logical fallacies, i.e., inferences that invalid because they are not based on tautologies.Some common fallacies are listed below:

Rule of Inference	Name
$\begin{array}{rl} & B \\ & A \Rightarrow B \\ \hline \therefore & A \end{array}$	Affirming the Consequent
$\begin{array}{rl} & \neg A \\ & A \Rightarrow B \\ \hline \therefore & \neg B \end{array}$	Denying the Antecedent
$\begin{array}{rl} & A \vee B \\ & A \\ \hline \therefore & \neg B \end{array}$	Affirming a Disjunct

Non Sequitur

Example

(i) *Affirming the consequent:*

$$\begin{array}{rl} & \textit{If 9 is prime, then it is odd} \\ & \textit{9 is odd} \\ \hline \therefore & \textit{9 is prime.} \end{array}$$

(ii) *Denying the antecedent*

$$\begin{array}{rl} & \textit{If 9 is prime, then it is odd} \\ & \textit{9 is not prime} \\ \hline \therefore & \textit{9 is not odd.} \end{array}$$

(iii) *Affirming a disjunct:*

$$\begin{array}{rl} & \textit{2 is even or 2 is prime} \\ & \textit{2 is even} \\ \hline \therefore & \textit{2 is not prime.} \end{array}$$

Predicate Logic

Consider the following argument:

$$
\begin{array}{rl}
 & \text{every prime number that is greater than 2 is odd} \\
 & \text{7 is a prime number that is greater than 2} \\
\hline
\therefore & \text{7 is odd.}
\end{array}
$$

This looks like a valid argument. However, if we try to analyse this argument using propositional logic, then the best we can do is assign the propositional variables A, B and C to the statements "every prime number that is greater than 2 is odd", "7 is a prime number that is greater than 2" and "7 is odd" respectively. But then the argument looks like:

$$
\begin{array}{rc}
 & A \\
 & B \\
\hline
\therefore & C
\end{array}
$$

which is not a valid argument!

Propositional logic is not rich enough to formalise statements in the form "for every ..." and "there exists ...". To formalise these statements we need quantifiers and predicates.

Predicates

Definition

A **predicate** *is a declaritive sentence involving variables. I.e. a statement involving variables such that when the variables a substituted with appropriate individuals we obtain a proposition. The* **arity** *of a predicate is the number of distinct variables appearing in the predicate. We call a predicate of arity* 1 *a unary predicate, a predicate of arity* 2 *a binary predicate, . . .*

Example

- *"$x > 5$" is a unary predicate*
- *"$x^2 + y$" is NOT a predicate*
- *"x is the least prime greater than y" is a binary predicate*

Predicate logic

Predicate logic consists of **basic predicate variables** $A, B, P, Q, \ldots$, **variables** $x, y, z, \ldots$, and **constants** $a, b, c, \ldots$. If A is, for example, a binary predicate, then we write $A(x, y)$ to indicate that x and y are the variables appearing in A. The variables $x, y, z, \ldots$ take values from a universe called the **domain of discourse**. The constants $a, b, c, \ldots$ are specific individuals from the domian of discourse. Replacing all the variables by constants in a predicate or compound expression yields a declaritive statement (a proposition). Compound expressions in predicate logic are built-up by:

- Forming expressions using the connectives of propositional logic: $\neg$, $\wedge$, $\vee$, $\Rightarrow$ and $\iff$
- Replacing variables by constant symbols or other variables
- **Bounding** variables in a compound expression using the **logical quantifier** $\forall$, that reads "for all ...", or the **logical quantifier** $\exists$, that reads "there exists ..."

Predicate logic

Example

Let the domain of discourse be $\mathbb{N}$. Let $P(x)$ be the predicate "x is prime" and let $Q(x, y)$ be the predicate "$x < y$".

1. $P(y) \wedge Q(x, y)$ *is the expression "y is prime and $x < y$"*
2. $P(y) \wedge Q(100, y)$ *is the expression "y is prime and $100 < y$"*
3. $\exists y(P(y) \wedge Q(100, y))$ *is the expression "there exists y, such that y is prime and $100 < y$"*
4. $\forall x \exists y(P(y) \wedge Q(x, y))$ *is the expression "for all x, there exists y, such that y is prime and $x < y$"*

The expressions (1) and (2) involve variables that are not yet specified. Such expressions involving unspecified variables are called **compound predicates** or **formulae**. In expressions (3) and (4) all of the variables have been replaced by constants or bound by quantifiers. These expressions are propositions and are called **sentences**.

Predicate logic

In order to assess the truth or falsity of a sentence ϕ in predicate logic, we need to specify the domain of discourse M (a collection of objects or set) in which all of the basic predicates have an interpretation. On the previous slide, the domain of discourse was $\mathbb{N}$ and the interpreation of the two predicates $P(x)$ and $Q(x, y)$ were given at the beginnning of the course.

Definition

Let M be a domain and let $A(x)$ be a predicate or formula. We define the quantifier $\forall$ by

$$\forall x A(x) \text{ is true in } M \iff A(x) \text{ is true for all } x \in M$$

We define the quantifier $\exists$ by

$$\exists x A(x) \text{ is true in } M \iff A(x) \text{ is true for at least one } x \in M$$

We often abbreviate "$\forall x A(x)$ is true in M" and "$\exists x A(x)$ is true in M" by $(\forall x \in M)A(x)$ and $(\exists x \in M)A(x)$. This notation also allows us to further restrict the domain of the quantifiers.

Predicate logic

For example, if the domain of discourse is $\mathbb{R}$, then we can write $(\forall x \in \mathbb{Q})A(x)$ as an abbreviation for "for all x, if x is a rational number, then $A(x)$".

Example

Let the domain be the real numbers ($\mathbb{R}$). Then

- $\forall x(x > 0 \Rightarrow x^3 > 0)$ *is a true statement;*
- $\forall x(x > 0 \Leftrightarrow x^2 > 0)$ *is a false statement;*
- $\exists x(x > 0 \Leftrightarrow x^2 > 0)$ *is a true statement.*

Sometimes mathematicians put a quantifier at the end of a statement form; this is known as a **hanging quantifier**. Such a hanging quantifier will be interpreted as being located just before the expression:

$$\exists y(y + x^2 > 0) \qquad\qquad \forall x$$

is equivalent to $\exists y \forall x(y + x^2 > 0)$.

Contraposition and Negation of Quantifiers

We do not actually need the quantifier $\exists$ since

$$\begin{aligned} \exists x A(x) \text{ is true in } M \Leftrightarrow &\quad A(x) \text{ is true for at least one } x \in M \\ \Leftrightarrow &\quad A(x) \text{ is not false for all } x \in M \\ \Leftrightarrow &\quad \neg(\forall x \neg A(x)) \text{ is true in } M \end{aligned} \tag{3}$$

The equivalence (3) is called **contraposition of quantifiers**. It implies that the negation of $(\exists x \in M)A(x)$ is equivalent to $(\forall x \in M)\neg A(x)$. For example,

$$\neg\big((\exists x \in \mathbb{R})(x^2 < 0)\big) \qquad \Leftrightarrow \qquad (\forall x \in \mathbb{R})(x^2 \not< 0).$$

Conversely,

$$\neg(\forall x \in M)A(x) \qquad \Leftrightarrow \qquad (\exists x \in M)\neg A(x).$$

Vacuous Truth

If the domain of the universal quantifier $\forall$ is the empty set $M = \emptyset$, then the statement $(\forall x \in M)A(x)$ is defined to be true regardless of the predicate $A(x)$. It is then said that $A(x)$ is **vacuously true**.

Example

Let M be the set of real numbers x such that $x = x + 1$. Then the statement

$$(\forall x \in M)(x > x)$$

is true

This convention reflects the philosophy that a universal statement is true unless there is a counterexample to prove it false. While this may seem a strange point of view, it proves useful in practice.
This is similar to saying that “All pink elephants can fly" is a true statement, because it is impossible to find a pink elephant that can’t fly. It is also consistent with behaviour of compound expressions involving $\Rightarrow$, which are true if the antecedent is false, regardless of the consequence.

Quantifier order

Example

Let the domain be the real numbers ($\mathbb{R}$).

- $\forall x \forall y(x^2+y^2-2xy \geq 0)$ *is equivalent to* $\forall y \forall x(x^2+y^2-2xy \geq 0)$. *Therefore, one often writes* $\forall x, y(x^2+y^2-2xy \geq 0)$.
- $\exists x \exists y(x+y>0)$ *is equivalent to* $\exists y \exists x(x+y>0)$. *One often writes* $\exists x, y(x+y>0)$.
- $\forall x \exists y(x+y>0)$ *is a true statement.*
- $\exists x \forall y(x+y>0)$ *is a false statement.*

The order of the quantifiers is important if they are different.

Examples from Calculus

Let the domain of discourse be $\mathbb{R}$ and let I be an interval in $\mathbb{R}$. Then a function $f : I \longrightarrow \mathbb{R}$ is said to be **continuous** on I if and only if

$$(\forall \varepsilon > 0)(\forall x \in I)(\exists \delta > 0)(\forall y \in I)(|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon)$$

The function f is **uniformly continuous** on I if and only if

$$(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x \in I)(\forall y \in I)(|x - y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon)$$

It is easy to see that a function that is uniformly continuous on I must also be continuous on I.
If I is a closed interval, $I = [a, b]$, it can also be shown that a continuous function is also uniformly continuous. However, that requires techniques from calculus and is not obvious just by looking at the logical structure of the definitions.

Examples from Calculus

Negating complicated expressions can be done step-by-step. For example, the statement that f is not continuous on I is equivalent to

$$
\begin{aligned}
&\neg(\forall \varepsilon > 0)(\forall x \in I)(\exists \delta > 0)(\forall y \in I)(|x-y| < \delta \Rightarrow |f(x)-f(y)| < \varepsilon)\\
&\Leftrightarrow (\exists \varepsilon > 0)\neg(\forall x \in I)(\exists \delta > 0)(\forall y \in I)(|x-y| < \delta \Rightarrow |f(x)-f(y)| < \varepsilon)\\
&\Leftrightarrow (\exists \varepsilon > 0)(\exists x \in I)\neg(\exists \delta > 0)(\forall y \in I)(|x-y| < \delta \Rightarrow |f(x)-f(y)| < \varepsilon)\\
&\Leftrightarrow (\exists \varepsilon > 0)(\exists x \in I)(\forall \delta > 0)\neg(\forall y \in I)(|x-y| < \delta \Rightarrow |f(x)-f(y)| < \varepsilon)\\
&\Leftrightarrow (\exists \varepsilon > 0)(\exists x \in I)(\forall \delta > 0)(\exists y \in I)\neg(|x-y| < \delta \Rightarrow |f(x)-f(y)| < \varepsilon)\\
&\Leftrightarrow (\exists \varepsilon > 0)(\exists x \in I)(\forall \delta > 0)(\exists y \in I)(|x-y| < \delta \wedge |f(x)-f(y)| \geq \varepsilon)
\end{aligned}
$$

Examples from Calculus

Example

The Heaviside function $H : \mathbb{R} \longrightarrow \mathbb{R}$,

$$H(x) := \begin{cases} 1 & \text{if } x \geq 0, \\ 0 & \text{if } x < 0 \end{cases}$$

is not continuous on $I = \mathbb{R}$. *To see this, we need to show that there exists an* $\varepsilon > 0$ *(take* $\varepsilon = 1/2$*) and an* $x \in \mathbb{R}$ *(take* $x = 0$*) such that for any* $\delta > 0$ *there exists* $y \in \mathbb{R}$ *such that*

$$|x - y| = |y| < \delta \qquad \text{and} \qquad |H(x) - H(y)| = |1 - H(y)| \geq \varepsilon = \frac{1}{2}.$$

Given any $\delta > 0$ *we can choose* $y = -\frac{\delta}{2}$. *Then* $|y| = \frac{\delta}{2} < \delta$ *and* $|1 - H(y)| = 1 > \frac{1}{2}$. *This proves that* H *is not continuous on* $\mathbb{R}$.

Tautologies in predicate logic

Now that we are equipped with a calculus for compund expressions involving predicates and quantifiers, determining the truth or falsity of sentences becomes much more complicated. For example, the truth of a unary predicate bound by a quantifier depends on the truth of that predicate applied to individuals in the domain discourse. The following generalises the notion of tautology to sentences in predicate logic:

Definition

Let A be a predicate logic sentence. A is a **tautology** *if for every nonempty domain of of discourse M that is equipped with interpretations of the predicate symbols in A, A is true in M.*

Example

The sentence $A : \exists x \forall y Q(y, x)$ is not a tautology because A is not true in $\mathbb{N}$ with $Q(x, y)$ interpreted as "$x \leq y$".

Rules of inference for quantified expressions

Showing that sentences are tautologies of predicate logic is difficult, so instead we introduce rules of inference that allow us to deal with expressions involving quantifiers. These are taken as primitive (they are assumed):

Rule of Inference	Name
$\dfrac{\forall x P(x)}{\therefore\ P(x_0) \text{ for any } x_0 \text{ in the domain of discourse}}$	Universal Instantiation
$\dfrac{P(x) \text{ for any arbitrarily chosen } x \text{ in the domain of discourse}}{\therefore\ \forall x P(x)}$	Universal Generalisation
$\dfrac{\exists x P(x)}{\therefore\ P(x_0) \text{ for a certain (unknown) } x_0 \text{ in the domain of discourse}}$	Existential Instantiation
$\dfrac{P(x_0) \text{ for some (known) } x_0 \text{ in the domain of discourse}}{\therefore\ \exists x P(x)}$	Existential Generalisation

Rules of inference for quantified expressions

In addition to these rules of inference, every valid argument in propositional logic remains valid in predicate logic.

The fact these rules of inference yield all the tautologies of predicate logic, and conversely that all of these rules of inference are valid, are deep results of mathematical logic known as the Completeness and Soundness Theorems.

Rules of inference for quantified expressions

Example

$$\begin{array}{rl} & \exists x(P(x) \wedge \neg Q(x)) \\ & \forall x(P(x) \Rightarrow R(x)) \\ \hline \therefore & \exists x(R(x) \wedge \neg Q(x)) \end{array}$$

is a valid argument

1. $\exists x(P(x) \wedge \neg Q(x))$ *is a premise*
2. $P(a) \wedge \neg Q(a)$, *where a is some (unknown) element of the domain of discourse, by Existential Instantiation*
3. $P(a)$ *by Simplification of (2)*
4. $\forall x(P(x) \Rightarrow R(x))$ *is a premise*
5. $P(a) \Rightarrow R(a)$ *by Universal Instantiation of (4)*
6. $R(a)$ *by Modus Ponens from (5) and (3)*
7. $\neg Q(a)$ *by Simplification of (2)*
8. $R(a) \wedge \neg Q(a)$ *by Conjunction of (6) and (7)*
9. $\exists x(R(x) \wedge \neg Q(x))$ *by Existential Generalisation of (8)*

Tautologies in predicate logic

Example

Alternatively, to show that

$$\begin{array}{rl} & \exists x(P(x) \wedge \neg Q(x)) \\ & \forall x(P(x) \Rightarrow R(x)) \\ \hline \therefore & \exists x(R(x) \wedge \neg Q(x)) \end{array}$$

is a valid argument, we could show that

$$(\exists x(P(x) \wedge \neg Q(x)) \wedge \forall x(P(x) \Rightarrow R(x))) \Rightarrow \exists x(R(x) \wedge \neg Q(x))$$

is a tautology.
Suppose that $\mathscr{M}$ is a nonempty domain of discourse equipped with interpretations $P^{\mathscr{M}}$, $Q^{\mathscr{M}}$ and $R^{\mathscr{M}}$ of the unary predicates P, Q and R. Assume that

$$(\exists x(P(x) \wedge \neg Q(x)) \wedge \forall x(P(x) \Rightarrow R(x))) \Rightarrow \exists x(R(x) \wedge \neg Q(x))$$

is not true in $\mathscr{M}$.

Tautologies in predicate logic

Example

Therefore $(\exists x(P(x) \wedge \neg Q(x)) \wedge \forall x(P(x) \Rightarrow R(x)))$ *is true in* $\mathscr{M}$ *and* $\exists x(R(x) \wedge \neg Q(x))$ *is not true in* $\mathscr{M}$. *Therefore* $\exists x(P(x) \wedge \neg Q(x))$, $\forall x(P(x) \Rightarrow R(x))$, $\forall x(\neg R(x) \vee Q(x))$ *are all true in* $\mathscr{M}$. *Let* a *be an element of the domain* $\mathscr{M}$ *such that* $P(a) \wedge \neg Q(a)$ *is true in* $\mathscr{M}$. *Therefore both* $P(a)$ *and* $\neg Q(a)$ *are true in* $\mathscr{M}$. *Since* $\forall x(P(x) \Rightarrow R(x))$ *and* $\forall x(\neg R(x) \vee Q(x))$ *are true in* $\mathscr{M}$, *both* $P(a) \Rightarrow R(a)$ *and* $\neg R(a) \vee Q(a)$. *Therefore* $R(a)$ *and* $\neg R(a)$ *are both true in* $\mathscr{M}$, *which is a CONTRADICTION!*

Therefore if $\mathscr{M}$ *is a nonempty domain of discourse equipped with interpretations* $P^{\mathscr{M}}$, $Q^{\mathscr{M}}$ *and* $R^{\mathscr{M}}$ *of the unary predicates* P, Q *and* R, *then*

$$(\exists x(P(x) \wedge \neg Q(x)) \wedge \forall x(P(x) \Rightarrow R(x))) \Rightarrow \exists x(R(x) \wedge \neg Q(x))$$

is true in $\mathscr{M}$

Proofs in logic and proofs in mathematics

Given a mathematical argument (a proof), it should be possible to formalise this argument by identifying the premises (the assumptions that are being made), assigning predicate and constant symbols to the mathematical entities appearing in the argument, and verifying that the argument being made is logically valid. This process is often very tedious! That said, mathematical logic does reveal to us the structure and assumptions that underpin many arguments that we use in mathematics. There is an element of circularity in the fact that we are using mathematical arguments to analyse logic. Mathematical logic is riddled with subtleties that means that one need to be careful drawing conclusions about its mathematical and philosophical implications.

Naive Set Theory: Sets via Predicates

Set Theory is the study of collections of mathematical objects. A **set** is a collection of objects that contains no information about order, and in which repetitions of objects are ignored. In pure set theory every object is itself a set, but it is often useful, and formally harmless, to also think of other mathematical entities such as numbers and shapes, or even physical entities, as objects. We will see later that mathematical entities such as the natural numbers can be represented as sets, and mathematicians have provided evidence that every mathematical entity can be represented using sets.

We will see later that allowing any collection of objects (or sets) to be a set leads to an inconsistent theory. This means that if we were going to be rigorous we would need to set out rules that tell us which collections are sets. However, as collections that lead to inconsistency are not generally encountered in applications of set theory, in this course we will assume that every collection that can be desribed is set - this is called **Naive Set Theory**. In contrast, laying out definite rules for which collections are sets is referred to as **Axiomatic Set Theory**.

Curly brackets ($\{\ldots\}$) are used to indicate that some collection of objects are collected into a set.

Definition

Let X be a set and let x be an object. We write $x \in X$ to indicate that x is a member of X.

If $P(x)$ is predicate then the set of all objects x that satisfy $P(x)$ is written:

$$X = \{x \mid P(x)\}$$

I.e. $x \in X$ if and only if $P(x)$

Definition

Two sets X and Y are equal ($X = Y$) if for all x, $x \in X$ if and only if $x \in Y$.

Notation for Sets

We define the empty set $\emptyset = \{x \mid x \neq x\}$. The empty set has no elements, because the predicate $x \neq x$ is never true.

We may also use the notation $X = \{x_1, x_2, \dots, x_n\}$ to denote a set. In this case, X is understood to be the set

$$X = \{x \mid (x = x_1) \vee (x = x_2) \vee \cdots \vee (x = x_n)\}.$$

We will frequently use the convention

$$\{x \in A \mid P(x)\} = \{x \mid x \in A \wedge P(x)\}$$

Example

- *The set of even nonnegative integers is* $\{n \in \mathbb{N} \mid (\exists k \in \mathbb{N})(n = 2k)\}$
- $$\{x \in \mathbb{R} \mid x^3 + 2x^2 - 1 = 0\} = \left\{-1, \frac{-1+\sqrt{5}}{2}, \frac{-1-\sqrt{5}}{2}\right\}$$

Subsets

If every object $x \in X$ is also an element of a set Y, we say that X is a **subset** of Y, writing $X \subseteq Y$; in other words,

$$X \subseteq Y \Leftrightarrow \forall x (x \in X \Rightarrow x \in Y).$$

Note that $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$.

We say that X is a **proper subset** of Y if $X \subseteq Y$ but $X \neq Y$. In that case we write $X \subset Y$.

Some authors write $\subset$ for $\subseteq$ and $\subsetneq$ for $\subset$. Pay attention to the convention used when referring to literature.

Example

- *When* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *and* $\mathbb{C}$ *are thought of as sets of numbers,*

  $$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

  To see that each of these containments is proper note that $-1 \in \mathbb{Z}$ *and* $-1 \notin \mathbb{N}$, $\frac{1}{2} \in \mathbb{Q}$ *and* $\frac{1}{2} \notin \mathbb{Z}$, $\sqrt{2} \in \mathbb{R}$ *and* $\sqrt{2} \notin \mathbb{Q}$, *and* $\sqrt{-1} \in \mathbb{C}$ *and* $\sqrt{-1} \notin \mathbb{R}$

Examples of Sets and Subsets

Example

1. *For any set* X, $\emptyset \subseteq X$. *Since* $\emptyset$ *does not contain any elements, for every* x, *the antecedant of the implication* $x \in \emptyset \Rightarrow x \in X$ *is false. So, the implication is true, which shows that* $\emptyset \subseteq X$.
2. *Consider the set* $A = \{a, b, c\}$ *where* a, b, c *are arbitrary objects, for example, numbers. The set*

   $$B = \{a, b, a, b, c, c\}$$

   is equal to A,

   $$x \in A \quad \Leftrightarrow \quad (x = a) \vee (x = b) \vee (x = c) \quad \Leftrightarrow \quad x \in B.$$

   If $C = \{a, b\}$, *then* $C \subseteq A$ *and in fact* $C \subset A$. *Setting* $D = \{b, c\}$ *we have* $D \subset A$ *but* $C \not\subseteq D$ *and* $D \not\subseteq C$.
3. *Let* $A = \{\emptyset, \{\{\emptyset\}\}\}$, $B = \{\emptyset\}$ *and* $C = \{\{\emptyset\}\}$. $B \subseteq A$, *but* $B \notin A$, *and* $C \in A$, *but* $C \not\subseteq A$.

Powerset and Cardinality

If a set X has a finite number of elements, we define the **cardinality** of X to be this number, denoted by $\#X$, $|X|$ or $\mathrm{card}(X)$.

Definition

If X is a set, then the **powerset** *of X, denoted $\mathscr{P}(X)$, is the set of all subsets of X. I.e.*

$$\mathscr{P}(X) = \{A \mid A \subseteq X\}$$

This means the expressions "$A \in \mathscr{P}(X)$" and "$A \subseteq X$" are equivalent.

Example

The power set of $\{a, b, c\}$ is

$$\mathscr{P}(\{a, b, c\}) = \big\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\big\}.$$

$|\{a, b, c\}| = 3$ *and* $|\mathscr{P}(\{a, b, c\})| = 8$.

Operations on Sets

Let A and B be sets.

Definition

- *The* **union** *of A and B is the set:* $A \cup B = \{x \mid x \in A \vee x \in B\}$
- *The* **intersection** *of A and B is the set:* $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- *The* **difference** *is:* $A \backslash B = \{x \in A \mid x \notin B\}$ *some authors write this* $A - B$

If $A \subseteq M$, then $M \backslash A$ is called the complement of A. Some authors write this A^{c} when M is clear from the context.
If $A \cap B = \emptyset$, then we say that A and B are disjoint.

Example

Let $A = \{a, b, c\}$ *and* $B = \{c, d\}$. *Then*

$$A \cup B = \{a, b, c, d\}, \qquad A \cap B = \{c\}, \qquad A \setminus B = \{a, b\}.$$

Operations on Sets

Logical equivalences immediately lead to several rules for set operations. For example, the distributive laws for $\wedge$ and $\vee$ imply

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

Other such rules are, for example,

- $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$
- $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$
- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
- $A \setminus B = B^{\mathrm{c}} \cap A$
- $(A \setminus B)^{\mathrm{c}} = A^{\mathrm{c}} \cup B$

Some of these will be proved in the recitation class and the exercises.

Operations on Sets

Occasionally we will need the following notation for the union and intersection of a finite number $n \in \mathbb{N}$ of sets:

$$\bigcup_{k=0}^{n} A_k := A_0 \cup A_1 \cup A_2 \cup \cdots \cup A_n,$$
$$\bigcap_{k=0}^{n} A_k := A_0 \cap A_1 \cap A_2 \cap \cdots \cap A_n.$$

This notation even extends to $n = \infty$, but needs to be properly defined:

$$x \in \bigcup_{k=0}^{\infty} A_k \quad :\Leftrightarrow \quad (\exists k \in \mathbb{N})(x \in A_k),$$
$$x \in \bigcap_{k=0}^{\infty} A_k \quad :\Leftrightarrow \quad (\forall k \in \mathbb{N})(x \in A_k).$$

Operations on Sets

In particular,

$$\bigcap_{k=0}^{\infty} A_k \subseteq \bigcup_{k=0}^{\infty} A_k.$$

Example

Let $A_k = \{0, 1, 2, \ldots, k\}$ *for* $k \in \mathbb{N}$*. Then*

$$\bigcup_{k=0}^{\infty} A_k = \mathbb{N}, \qquad \bigcap_{k=0}^{\infty} A_k = \{0\}.$$

To see the first statement, note that $\mathbb{N} \subseteq \bigcup_{k=0}^{\infty} A_k$ *since* $x \in \mathbb{N}$ *implies* $x \in A_x$ *implies* $x \in \bigcup_{k=0}^{\infty} A_k$*. Furthermore,* $\bigcup_{k=0}^{\infty} A_k \subseteq \mathbb{N}$ *since* $x \in \bigcup_{k=0}^{\infty} A_k$ *implies* $x \in A_k$ *for some* $k \in \mathbb{N}$ *implies* $x \in \mathbb{N}$*.*

For the second statement, note that $\bigcap_{k=0}^{\infty} A_k \subseteq \mathbb{N}$*. Now* $0 \in A_k$ *for all* $k \in \mathbb{N}$*. Thus* $\{0\} \subseteq \bigcap_{k=0}^{\infty} A_k$*. On the other hand, for any* $x \in \mathbb{N} \setminus \{0\}$ *we have* $x \notin A_{x-1}$ *whence* $x \notin \bigcap_{k=0}^{\infty} A_k$*.*

Operations on Sets

More generally, if A is a set and $X \subseteq \mathscr{P}(A)$, then

$$\bigcup X = \{x \in A \mid (\exists y \in X)(x \in y)\} \text{ and } \bigcap X = \{x \in A \mid (\forall y \in X)(x \in y)\}$$

Example

Let

$$X = \{A \in \mathscr{P}(\mathbb{N}) \mid (\exists k \in \mathbb{N})(\forall n \in \mathbb{N})(n \in A \vee n = k)\}$$

Then

$$\bigcup X = \mathbb{N} \textit{ and } \bigcap X = \emptyset$$

Note here that $X \subseteq \mathscr{P}(A)$, but both $\bigcup X$ and $\bigcap X$ are subsets of A (these operations strip off $\{\cdots\}$).

Ordered Pairs

A set does not contain any information about the order of its elements, e.g.,

$$\{a, b\} = \{b, a\}.$$

Thus, there is no such a thing as the "first element of a set". However, sometimes it is convenient or necessary to have such an ordering. This is achieved by defining an **ordered pair**, denoted by

$$(a, b)$$

and having the property that

$$(a, b) = (c, d) \qquad \Leftrightarrow \qquad (a = c) \wedge (b = d). \tag{4}$$

We define

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

It is not difficult to see that this definition guarantees that (4) holds.

Cartesian Product of Sets

If A, B are sets and $a \in A$, $b \in B$, then we denote the set of all ordered pairs by

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

$A \times B$ is called the **cartesian product** of A and B.

Using ordered pairs, one can then define **ordered triples** and, more generally, ordered n**-tuples** of sets. For sets $x_0, \ldots, x_n$, define

$$(x_0, \ldots, x_n) = (x_0, (x_1, \ldots, x_n))$$

This is an example of a recursive definition (we will discuss definitions of this type in more detail later): Ordered n-tuples of sets are defined in terms of ordered $n-1$-tuples of sets. In particular, if x, y and z are sets, then

$$(x, y, z) = (x, (y, z)) = \{\{x\}, \{x, (y, z)\}\} = \{\{x\}, \{x, \{\{y\}, \{y, z\}\}\}\}$$

And, if A, B and C are sets, then the set of ordered triples with first element a member of A, second element a member of B, and third element a memeber of C, written $A \times B \times C$, is the set $A \times (B \times C)$

Cartesian Product of Sets

In general, if $A_1, \ldots, A_n$ are sets and $n \geq 2$, then the set of ordered n-tuples with first element from A_1, second element from A_2, ..., called the ***n*-fold cartesian product** and writen $A_1 \times \cdots \times A_n$, is the set

$$A_1 \times (A_2 \times \cdots (A_{n-1} \times A_n) \cdots)$$

If A is a set then the ***n*-fold cartesian product** of A, i.e. $A \times \cdots \times A$, is abreviated A^n.

Example

- $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N} = \{(a,b) \mid a \in \mathbb{N} \wedge b \in \mathbb{N}\}$
- *Let* $A = \{1,4,5\}$, $B = \{2,3\}$ *and* $C = \{0,2\}$.

$$A \times B \times C = A \times (B \times C) = \left\{ \begin{array}{c} (1,2,0),(1,2,2),(1,3,0),(1,3,2), \\ (4,2,0),(4,2,2),(4,3,0),(4,3,2), \\ (5,2,0),(5,2,2),(5,3,0),(5,3,2) \end{array} \right\}$$

We can see that $|A \times B \times C| = 3 \cdot 2 \cdot 2 = 12$

Problems in Naive Set Theory

The fact that Naive Set Theory allows the unrestricted formation of sets, means that a set A can be defined with the property that $A \in A$. For example: the set of all sets, the set of all infinite sets, ... Unrestricted self-reference has long been known to be problematic. For example,

- Epimenides Paradox (6^{th}-century BC)
- Barber Paradox: A male barber in a hamlet shaves all those, and only those, who do not shave themselves. Who shaves the barber?

In 1902 Bertrand Russell formalised these paradoxes in Naive Set Theory to show that Naive Set Theory is inconsistent.

Russell's Paradox

Theorem

The set of all sets that are not members of themselves is not a set. I.e.

$$R := \{x \mid x \notin x\} \text{ is not a set.}$$

Proof.

The proof is by contradiction. Suppose that R is a set. If $R \in R$, then $R \notin R$ by the definition of R, which is a contradiction. If $R \notin R$, then $R \in R$ by the definition of R, which is also a contradiction. □

Russell's Paradox

We will simply ignore the existence of such contradictions and build on Naive Set Theory. There are further paradoxes in naive set theory, such as **Cantor's Paradox** and the **Burali-Forti Paradox**. All of these are resolved if naive set theory is replaced by a modern axiomatic set theory such as **Zermelo-Fraenkel Set Theory**.

Further Information:

- *Set Theory*, Stanford Encyclopedia of Philosophy, `http://plato.stanford.edu/entries/set-theory/`
- P.R. Halmos, **Naive Set Theory**, Available here: `http://link.springer.com/book/10.1007/978-1-4757-1645-0`
- T. Jech, **Set Theory: The Third Millennium Edition, Revised and Expanded**, Available here: `http://link.springer.com/book/10.1007/3-540-44761-X`