MATH0005 Algebra 1

Fall 2022

Contents

1 Logic

1.1 Propositional calculus

Definition 1.1.1. A **proposition** is a mathematical statement which is either true or false.

Here are some example propositions:

- 123456 is a prime number.
- The function $f(x) = \sin x$ is continuous.
- $1 + 1 = 2$
- The Riemann hypothesis is false.

Proposition might be true or false. All the propositions have their *well-defined truth value*, even if we do not know what it is. One typical example showing a sentence is not a proposition is, "n is even", since it does not have a *well-defined truth value* until we know what n is.

Definition 1.1.2. **Truth value** is the attribute of a proposition as to whether the proposition is true or false.

Here is an example:

- The *truth value* for "7 is odd" is *true*, which can be denoted as **T**.
- The *truth value* for "7 is even" is *false*, which can be denoted as **F**.

1.2 Logical connectives

Definition 1.2.1. **Connectives** are symbols used to connect two or more propositional or predicate logics in such a manner that resultant logic depends only on the input logics and the meaning of the connective used.

The standard connectives introduced here are '*and*', '*or*', '*not*', '*implies*' and '*if and only if*' (iff, for short).

Here are some examples of propositions which contain connectives:

- **AND** "34043 is a sum of two squares *and* 34043 is divisible by 17"
- **OR** "34043 is a sum of two squares *or* 34043 is divisible by 17"
- **NOT** "It is *not* true that 34043 is a sum of two squares"
- **IMPLIES** "34043 is odd *implies* 34043 is divisible by 3"
- **IF AND ONLY IF** "An odd number is a sum of two squares, *if and only if* it leaves remainder 1 when you divide it by 4"

Notice that **implies** is often express as "**if** . . . **then**".

The sentence "34043 is odd *implies* 34043 is divisible by 3" could be written as "*If* 34043 is odd *then* 34043 is divisible by 3".

1.3 Well-formed formulae

1.3.1 Variables and connective symbols

Definition 1.3.1. Propositional variables are symbols that represent a proposition.

Traditionally, we use lower case English letters like $p, q, r, \dots$ or letters with subscripts p_1, p_2 to represent propositional variables.

For the logical connectives we discussed before, we also have symbols.

Connectives symbols

- $\wedge$ represents *and*.
- $\vee$ represents *or*.
- $\Rightarrow$ *or* $\rightarrow$ represents *implies*.
- $\neg$ represents *not*.
- Besides, we also use brackets: (and).

By collections of propositional variables, connectives and brackets, we could start to build formulae.

Note 1.3.1. Well-formed formulae are defined as the collections of those logical propositions with sensible meaning.

1.3.2 Definition of a well-formed formula

By definition, something is a **Well-formed formula**, or **WFF** for short, if and only if it can be constructed using these rules below:

Rules of WFFs

1. A propositional variable is a WFF.
2. If ϕ and ψ are any two WFFs, then
   (a) $(\phi \wedge \psi)$ is a WFF,
   (b) $(\phi \vee \psi)$ is a WFF,
   (c) $(\phi \Rightarrow \psi)$ is a WFF
   (d) $\neg\phi$ is a WFF.

1.3.3 WFF examples

Here are some examples of WFFs.
Suppose we have p and q as propositional variables. Then we have following WFFs:

- p is a WFF (from *Rule 1*).
- $(p \Rightarrow q)$ is a WFF (from *Rule 1 twice then Rule 2.c*).
- $\neg q$ is a WFF (from *Rule 1 then Rule 2.d*).
- $((p \Rightarrow q) \vee \neg q)$ is a WFF. Since $(p \Rightarrow q)$ and $\neg q$ are WFFs, and by *Rule 2.b* the whole thing is a WFF.
- $\neg\neg(p \Rightarrow q)$ is a WFF. Since $(p \Rightarrow q)$ is a WFF, by using *Rule 2.d* twice, the whole thing is a WFF.

Notice that things can be WFFs **only** when using those rules. Thereby formulae below are not WFFs:

- $p \vee q$, missing the brackets ().
- $(p \wedge q \wedge r)$. It should be corrected as $((p \wedge q) \wedge r)$ or $(p \wedge (q \wedge r))$.

1.4 Truth tables

Notice that a **Well-formed formula** like $(p \wedge q)$ is not true or false on its own: it totally depends on the truth or falsity of the statements represented by the propositional variables p and q. Once we decide the truth value of propositional variables in a WFF, we can give a truth value to the whole WFF.

Note 1.4.1. A **Truth-table** shows how the truth value of a WFF depends on its propositional variables and connectives.

1.4.1 Truth assignments for propositional variables

Definition 1.4.1. A **truth assignment** for a set V of propositional variables is a function $v : V \to \{T, F\}$.

Here and elsewhere, T represents true and F represents false.

Example 1.4.1. If p and q are propositional variables and $V = \{p, q\}$, then there is a truth assignment v for V such that $v(p) = T$ and $v(q) = F$.

1.4.2 Extending a truth assignment to WFFs

The truth assignment to WFF is more complex compared with assignments to propositional variables themselves, since it also depends on the intended meaning of the logical connectives.

Consider the following WFF:

$$((p \Rightarrow (q \vee r)) \Rightarrow (\neg p \vee q)) \tag{1}$$

Suppose that we somehow already knew the truth values of p, q, r, we still need to know about the truth value of formulae connected with those connectives $\wedge, \vee, \Rightarrow and \neg$.

Let us start with the connective $\wedge$ (and):

Since $\wedge$ represents the ordinary usage of the word "and", it would be sensible to assign $(\psi \wedge \psi)$ is true if and only if both ϕ and ψ are true.

Here we have the **truth table** for $\wedge$:

ϕ	ψ	$(\phi \wedge \psi)$
T	T	T
T	F	F
F	T	F
F	F	F

Table 1: Truth table for $\wedge$

By using the truth table above, we could assign the truth value to a WFF $(\phi \wedge \psi)$.

Here are some examples:

Example 1.4.2. If $v(\psi) = T$ and $v(\phi) = T$, then $v(\psi \wedge \phi)$ will be T.

Example 1.4.3. If the propositional variables "p : *Today is Thursday*" and "q : *Today is raining*" are true, then the proposition "*Today is Thursday and is raining*" is true.

Here are the truth tables for other connectives in our language.

ϕ	ψ	$(\phi \vee \psi)$
T	T	T
T	F	T
F	T	T
F	F	F

Table 2: Truth table for $\vee$

ϕ	ψ	$(\phi \Rightarrow \psi)$
T	T	T
T	F	F
F	T	T
F	F	T

Table 3: Truth table for $\Rightarrow$

ϕ	$(\neg\phi)$
T	F
F	T

Table 4: Truth table for $\neg$

Notices that for all truth assignments we could think about as a way to combine two truth values into another truth value, just like + combines two numbers into another number. Thereby we could have this conclusion:

- $T \wedge T = T$, $T \wedge F = F$, $F \wedge T = F$, $F \wedge F = F$
- $T \vee T = T$, $T \vee F = T$, $F \vee T = T$, $F \vee F = F$
- $T \Rightarrow T = T$, $T \Rightarrow F = F$, $F \Rightarrow T = T$, $F \Rightarrow F = T$
- $\neg T = F$, $\neg F = T$

1.5 Truth values for WFFs

For a truth assignment $v : V \to \{T, F\}$, we could extend the function v so that it gives a truth value to any WFF using the propositional variables V such that for any WFFs ϕ and ψ.

$$v((\phi \wedge \psi)) = v(\phi) \wedge v(\phi) \tag{2}$$
$$v((\phi \vee \psi)) = v(\phi) \vee v(\psi) \tag{3}$$
$$v((\phi \Rightarrow \psi)) = v(\phi) \Rightarrow v(\psi) \tag{4}$$
$$v((\neg\phi)) = \neg v(\phi) \tag{5}$$

This could support the idea that connective symbols are not just as parts of WFFs but as ways of combing truth values. Here are some examples:

Suppose $V \to \{\phi, \psi\}$ and $v(\phi) = T$, $v(\psi) = F$, we could have

Example 1.5.1.

$$\begin{aligned} v((\phi \wedge \psi)) &= v(\phi) \wedge v(\phi) \\ &= T \wedge F \\ &= F \end{aligned} \tag{6}$$

Example 1.5.2.

$$\begin{aligned} v((\neg\phi) \Rightarrow (\phi \vee \psi)) &= v(\neg\phi) \Rightarrow v(\phi \vee \psi) \\ &= \neg v(\phi) \Rightarrow (v(\phi) \vee v(\psi)) \\ &= F \Rightarrow (T \vee F) \\ &= F \Rightarrow T \\ &= T \end{aligned} \tag{7}$$

Example 1.5.3. Let $\alpha = ((p \wedge q) \vee (\neg p \wedge \neg q))$, $v(p) = T$, $v(q) = F$. Let us find $v(\alpha)$.
Firstly let expand $v(\alpha)$ as $v(((p \wedge q) \vee (\neg p \wedge \neg q))$,
We have:

$$\begin{aligned} v(\alpha) &= v(((p \wedge q) \vee (\neg p \wedge \neg q)) \\ &= v(p \wedge q) \vee v(\neg p \wedge \neg q) \\ &= (v(p) \wedge v(q)) \vee (v(\neg p) \wedge v(\neg q)) \\ &= (v(p) \wedge v(q)) \vee (\neg v(p) \wedge \neg v(q)) \\ &= (T \wedge F) \vee (\neg T \wedge \neg F) \\ &= F \vee (F \wedge T) \\ &= F \vee F \\ &= F \end{aligned} \tag{8}$$

Example 1.5.4. Consider a WFF $\phi = (p \Rightarrow (p \Rightarrow p))$ and $v(p) = T$. Let find $v(\phi)$. We have:

$$\begin{aligned} v(\phi) &= v(p \Rightarrow (p \Rightarrow p)) \\ &= v(p) \Rightarrow (v(p \Rightarrow p)) \\ &= v(p) \Rightarrow (v(p) \Rightarrow v(p)) \\ &= T \Rightarrow (T \Rightarrow T) \\ &= T \Rightarrow T \\ &= T \end{aligned} \tag{9}$$

If we work out the truth value of ϕ when $v(p) = F$, we would find the result of $v(\phi)$ is also T:

$$\begin{aligned} v(\phi) &= v(p \Rightarrow (p \Rightarrow p)) \\ &= v(p) \Rightarrow (v(p \Rightarrow p)) \\ &= v(p) \Rightarrow (v(p) \Rightarrow v(p)) \\ &= F \Rightarrow (F \Rightarrow F) \\ &= F \Rightarrow T \\ &= T \end{aligned} \tag{10}$$

We would observe the WFF ϕ is true for *every* truth assignment of its variables, and we call WFF with this property as **tautology**.

Definition 1.5.1. A formula of propositional logic is a **tautology** if the formula itself is always *true*, regardless of which valuation is used for the propositional variables.

Here are some examples of tautology:

- $(A \lor \neg A)$
- $((A \Rightarrow B) \land (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$

Similarly, we would have another kind of WFFs for which is false for *every* truth assignment of its variables, and we call WFF with this property as **contradiction**.

Definition 1.5.2. A formula of propositional logic is a **contradiction** if the formula itself is always *false*, regardless of which valuation is used for the propositional variables.

Here are some examples of tautology:

- $(A \land \neg A)$
- $\neg(p \Rightarrow (q \Rightarrow p))$

1.6 Logical equivalence

Consider the following two WFFs:

$$\phi = (p \wedge q) \tag{11}$$
$$\psi = (q \wedge p) \tag{12}$$

The formulae ϕ and ψ are *different* WFFs. However, no matter what truth assignment we give, the formulae ϕ and ψ could always get equal truth values. Here is the proof:

$$\begin{aligned} v(\phi) &= v(p \wedge q) \\ &= v(p) \wedge v(q) \end{aligned} \tag{13}$$

$$\begin{aligned} v(\psi) &= v(q \wedge p) \\ &= v(q) \wedge v(p) \end{aligned} \tag{14}$$

And no matter what $v(q)$ and $v(p)$ is, $v(p) \wedge v(q)$ always equals to $v(q) \wedge v(p)$.

Definition 1.6.1. Two WFFs ϕ and ψ are called **logically equivalent**, denoted as $\phi \equiv \psi$, if and only if they have the same truth value under every possible truth assignment.

The idea of logically equivalence is useful for us to prove something is true, because we can prove some logically equivalent formula instead if it is easier to interpret.

Theorem 1.6.1. *Let ϕ, ψ and θ be WFFs, then*

1. $(\phi \wedge \psi) \equiv (\psi \wedge \phi)$ *[Commutativity properties for $\wedge$]*
2. $(\phi \vee \psi) \equiv (\psi \vee \phi)$ *[Commutativity properties for $\vee$]*
3. $(\phi \wedge (\psi \wedge \theta) \equiv ((\psi \wedge \phi) \wedge \theta)$ *[Associativity Properties]*
4. $(\phi \vee (\psi \vee \theta) \equiv ((\psi \vee \phi) \vee \theta)$ *[Associativity Properties]*
5. $(\phi \wedge (\psi \vee \theta)) \equiv ((\phi \wedge \psi) \vee (\phi \wedge \theta)))$ *[Distributivity]*
6. $(\phi \vee (\psi \wedge \theta)) \equiv ((\phi \vee \psi) \wedge (\phi \vee \theta)))$ *[Distributivity]*

1.7 Double negation

Theorem 1.7.1. *Let ϕ be WFF, then*

$$\neg\neg\phi \equiv \phi \tag{15}$$

Proof. Define function $v : V \to \{T, F\}$.
If $v(\phi) = T$, then $v(\neg\neg\phi) = \neg(\neg v(\phi)) = \neg(\neg T) = \neg F = T$;
If $v(\phi) = F$, then $v(\neg\neg\phi) = \neg(\neg v(\phi)) = \neg(\neg F) = \neg T = F$.
Therefore under any truth assignment v we have $v(\phi) = v(\neg\neg\phi)$. □

1.8 De Morgan's Laws

Theorem 1.8.1. *Let ϕ and ψ be WFFs, then*

1. $\neg(\phi \wedge \psi) = (\neg\phi \vee \neg\psi)$
2. $\neg(\phi \vee \psi) = (\neg\phi \wedge \neg\psi)$

Proof. By checking the possibilities for the truth values of ϕ and ψ under any assignment. □

Notice that **De Morgan's Laws** can be generalised to more than two WFFs.

Theorem 1.8.2. *Let ϕ and ψ be WFFs, then*

1. $\neg(\phi_1 \wedge \cdots \wedge \phi_n) \equiv (\neg\phi_1 \vee \cdots \vee \neg\phi_n)$
2. $\neg(\phi_1 \vee \cdots \vee \phi_n) \equiv (\neg\phi_1 \wedge \ldots \neg\phi_n)$

1.9 Contrapositive

1.9.1 Equivalence between $\Rightarrow$ and combination of $\neg$ and $\vee$

Theorem 1.9.1. *Let ϕ and ψ be WFFs, then*

$$(\phi \Rightarrow \psi) \equiv (\neg\phi \vee \psi) \tag{16}$$

Proof.
Suppose that if ϕ is true, then $v(\phi \Rightarrow \psi) = T$ when $v(\psi) = T$, and $v(\phi \Rightarrow \psi) = F$ when $v(\psi) = F$. Similarly when ϕ is false, then $v(\phi \Rightarrow \psi) \equiv T$ regardless of the truth value of ψ.
On the other hand if ϕ is true, then $\neg\phi$ is false. When ψ is true $v(\neg\phi \vee \psi) = T$. When ψ is false $v(\neg\phi \vee \psi) = F$. Similarly when ϕ is false, $\neg\phi$ is true. Therefore no matter what the truth value of ψ is, $v(\neg\phi \vee \psi) \equiv T$.
Therefore,

$$(\phi \Rightarrow \psi) \equiv (\neg\phi \vee \psi) \tag{17}$$

□

1.9.2 Contrapositive

Definition 1.9.1. Contrapositive of an implication $A \Rightarrow B$ is defined as $\neg B \Rightarrow \neg A$.

Regardless of the truth value of A and B, the truth value of a proposition always equals to the truth value of its contrapositive proposition.
Here is a proof.

Proof.

$$\begin{aligned}(A \Rightarrow B) &\equiv (A \vee \neg B)\\ &\equiv ((\neg\neg A) \vee \neg B)\\ &\equiv (\neg A \Rightarrow \neg B)\end{aligned} \tag{18}$$

□

The equivalence between a proposition and its contrapositive proposition provides a useful tool to simplify some proof processes. It is sometimes easier to proof the contrapositive $\neg B \Rightarrow \neg A$ compared with the original one. We here have one example to support:

x^2 is an irrational number implies x is an irrational number.
$(\forall x^2 \in (\mathbb{R} - \mathbb{Q}) \Rightarrow x \in (\mathbb{R} - \mathbb{Q})\ )$

The contrapositive of this proposition is:

x is a rational number implies x^2 is a rational number.
$(\forall x \in \mathbb{R} \Rightarrow x^2 \in \mathbb{R})$

It is clear that the contrapositive is easier to prove because when x is a rational number we know $x = p/q$. Therefore $x^2 = p^2/q^2$ must be a rational number either.

1.9.3 Converse

Definition 1.9.2. **Converse** of an implication $A \Rightarrow B$ is defined as $B \Rightarrow A$.

Unlike contrapositive, the proposition and its converse is **not** in general logically equivalent. Here is a contradiction example:

Proof. Suppose $(A \Rightarrow B) \equiv (B \Rightarrow A)$*:* When $v(A) = T$ and $v(B) = F$,

$$v(A \Rightarrow B) = T \Rightarrow F = F. \tag{19}$$

But

$$v(B \Rightarrow A) = F \Rightarrow T = T. \tag{20}$$

Therefore, $(A \Rightarrow B) \not\equiv (B \Rightarrow A)$ □

1.10 Adequacy

Definition 1.10.1. A set of connectives is **adequacy** if every WFF is logically equivalent to one using only the connectives from the set.

Theorem 1.9.1. $(\phi \Rightarrow \psi) \equiv (\neg\phi \vee \psi)$ shows how we use $\neg$ and $\vee$ to replace the symbol $\Rightarrow$.

By using this theorem, all the occurrence of $p \Rightarrow q$ could be replaced by $(\neg p) \vee q$. This shows that the set $\{\wedge, \vee, \neg\}$ is adequate.

However, we could still find other even smaller adequate sets.

Theorem 1.10.1. $\{\vee, \neg\}$ is adequate.

Proof.
Since we have already know the set $\{\wedge, \vee, \neg\}$ is adequate, according to the **De Morgan's Laws**, all the occurrence of $(p \wedge q)$ could be replaced by $\neg((\neg p) \vee (\neg q))$, which only contains the symbols $\neg$ and $\vee$.
Therefore, $\{\vee, \neg\}$ is adequate. □

Here is an example:

Example 1.10.1. Consider a proposition:

$$p \Rightarrow (q \wedge r) \tag{21}$$

It could be replaced by the symbol $\vee$ and $\neg$.

$$\begin{aligned} p \Rightarrow (q \wedge r) &\equiv (\neg p) \vee (q \wedge r) \\ &\equiv (\neg p) \vee \neg((\neg q) \vee (\neg r)). \end{aligned} \tag{22}$$

Theorem 1.10.2. $\{\wedge, \neg\}$ is adequate.

Proof.
The proof of this theorem is similar with the one above.
According to **De Morgan's Laws**, all the occurrence of $(p \vee q)$ could be replaced by $\neg((\neg p) \wedge (\neg q))$. $\square$

1.10.1 Do we have sets of connectives that are not adequate?

It is clear the symbol $\wedge$, $\vee$ and $\Rightarrow$ is not adequate by themselves. But if we define new connectives like $p \uparrow q = \neg(p \wedge q)$ or $p \downarrow q = \neg(p \vee q)$, it can be shown that both $\{\uparrow\}$ and $\{\downarrow\}$ are adequate.

1.11 First order logic

First-order logic (or **predicate calculus**)is symbolized reasoning in which each sentence, or statement, is broken down into a subject and a predicate. Here are some examples:

Example 1.11.1.

- There *exists* a rational number x with $x^2 = 2$.
- *For all* natural number n, there *exists* a natural number m with $m > n$.

1.11.1 First order formulae

Here we would give an informal definition of first order formulae.

A simple example of a first order formula looks like this:

$$\forall x \exists y\, R(x, y) \tag{23}$$

The meaning of this equation refers to "*for all* x, there *exists* a y, such that x and y are related by the relation R". Like a WFF, this equation is not true or false at this moment. We need more information like what sort thing the xs and ys are and what the relation R is, to decide the truth value.

1.11.2 Construction of first order formulae

First order formulae are made up of:

- quantifiers $\forall$ and $\exists$
- logical connectives $\neg$, $\wedge$, $\vee$, $\Rightarrow$, and brackets
- variable symbols x, y, z, ...
- relation symbols R, Q, P, ...

For an indicator $R(x, y)$, it indicates that x and y are related by some relation R. It is a "two-variable relation" since it contains two variables x and y. Here are some examples of two-variable relation: $x = y$, $x > y$, $x \neq y$, etc. It can be true or false, depending on the variables themselves.

Relation are allowed on any number of things. Just like two-variable relation, we have "one-variable relation" like $R(x)$, which is just a true or false property of a single thing x. We also have "three-variable relation" like $R(x, y, z) : x + y = z$, and so on.

2 Interpretations

Definition 2.0.1. An **interpretation** of a first order formula consists of a set A, called the **domain** of the interpretation, and a relation on A for each relation symbol in the formula.

Variables can be elements of the domain A of the interpretation in an interpreted formula. We write $\forall x \in A$ to mean "*for all* x in A", and $\exists x \in A$ to mean "there *exists* an element $x \in A$".

Once we have interpreted a formula, we can try to decide the truth value.

Example 2.0.1. For a first order formula $\forall x \exists y\, R(x, y)$, we could some interpretations. Define the notation $\mathbb{N}$ as the set of all natural numbers $\{0, 1, 2, \dots\}$.

- Domain $\mathbb{N}$, relation R is $<$. The interpreted formula is written:
  $$\forall x \in N\ \exists y \in N\ x < y \tag{24}$$
  The interpreted formula is **true**, since for every natural number we could find a number greater than it by 1.
- Domain $\mathbb{N}$, relation R is $>$. The interpreted formula is written:
  $$\forall x \in N\ \exists y \in N\ x > y \tag{25}$$
  The interpreted formula is **false**, since it is not true for every natural number there exists a natural number smaller than it. For example, when $x = 0$, there *does not exist* a y as a natural number which satisfies $y < 0$.

We could provide another example:

Example 2.0.2. For a first order formula $\exists y \forall x\, R(x, y)$:

- Domain $\mathbb{N}$, relation R is $\leq$. The interpreted formula is written:

$$\exists y \in N\, \forall x \in N\, x \leq y \tag{26}$$

  This formula is **false** since there *does not exist* a y *for all* x such that $x \leq y$. Because for all y, there exists an x such that x is greater than y.

- Domain $\mathbb{N}$, relation R is $\geq$. The interpreted formula is written:

$$\exists y \in N\, \forall x \in N\, x \geq y \tag{27}$$

  This formula is **true** since when $y = 0$, *for all* x as natural number we have $x \geq y$.

2.0.1 Truth of quantified formulae

Rules for deciding whether a formula containing a quantifier is true in an interpretation with domain A are:

- An interpreted formula $\forall x \in A\, \phi$ is true, if for every element a of A, substituting a into ϕ in place of x gives a truth statement.
- An interpreted formula $\exists x \in A\, \phi$ is true, if there exists an element of a of A, substituting a into ϕ in place of x gives a truth statement.

2.1 First order equivalences

Definition 2.1.1. Two first order formulae F_1 and F_2 are called **logically equivalent** if and only if, in every interpretation, F_1 and F_2 have the same truth value. We write $F_1 \equiv F_2$ for two logically equivalent formulae.

2.1.1 Example of logically equivalent statements

lemma 2.1.1.

1. $\forall x \forall y\, P(x, y) \equiv \forall y \forall x\, P(x, y)$
2. $\forall x \exists y\, P(x, y) \not\equiv \exists y \forall x\, P(x, y)$

Proof.

1.

□