Lecture 2

What have done so far?

- We have informally described the contents of the course.
- We have defined the syntax of Propositional Logic.
- We have defined the semantics of Propositional Logic.
- We have introduced the first semantic concepts: satisfiability, tautologies and contradictions.

Outline of Lecture 2

- We complete our crash course in Propositional Logic.
- We introduce vocabularies for first order structures.
- We introduce the syntax and semantics of First Order Logic.

Definition 18
Basic Semantic Concepts: Logical Equivalence

We say that two formulas ϕ_1, ϕ_2 are
logically equivalent
or **semantically equivalent**
if and only if for every
propositional assignement z

$$M_{PL}(\phi_1, z) = M_{PL}(\phi_2, z).$$

Examples 19

The following pairs of formulas are equivalent:

- $\neg\phi$ and $(\phi \to \mathbf{F})$.
- $(\neg\phi \vee \psi)$ and $(\phi \to \psi)$.
- $(\phi \vee \psi)$ and $((\phi \to \mathbf{F}) \to \psi)$.
- $(\phi \wedge \psi)$ and $\neg(\neg\phi \vee \neg\psi)$.

Use this to show the functional completeness of $\{\to, \mathbf{F}\}$, i.e.:

Proposition-Exercise 20
*For every truth table TT there as a formula $\phi \in$ **WFF**$_{\{\to,\mathbf{F}\}}$ such that $TT = TT_\phi$.*

Examples 21

- $\phi \in$ **WFF** is valid if and only if ϕ is logically equivalent to the formula $\mathbf{T}$.
- $\phi \in$ **WFF** is a contradiction if and only if ϕ is logically equivalent to the formula $\mathbf{F}$.
- $\phi \in$ **WFF** is valid if and only if $\neg\phi$ is logically equivalent to the formula $\mathbf{F}$.

Proposition-Exercise 22

(i) ϕ is a tautology if and only if TT_ϕ is the constant function with value 1.

(ii) ϕ is satisfiable if and only if there are $x_1, x_2, ..., x_n \in \{0, 1\}$ such that $TT_\phi(x_1, x_2, ..., x_n) = 1$.

(iii) Two well formed formulas $\phi, \psi \in$ **WFF** are logically equivalent if and only if they have the same truth tables associated with them, i.e. $TT_\phi = TT_\psi$.

Proposition-Exercise 23

Show that the following pairs of formulas ϕ_1, ϕ_2 are logically equivalent:

Commutativity:

$$\phi_1 = (\psi_1 \wedge \psi_2), \quad \phi_2 = (\psi_2 \wedge \psi_1);$$
$$\phi_1 = (\psi_1 \vee \psi_2), \quad \phi_2 = (\psi_2 \vee \psi_1);$$

Associativity:

$$\phi_1 = ((\psi_1 \wedge \psi_2) \wedge \psi_3), \quad \phi_2 = ((\psi_1 \wedge (\psi_2 \wedge \psi_3));$$
$$\phi_1 = ((\psi_1 \vee \psi_2) \vee \psi_3), \quad \phi_2 = ((\psi_1 \vee (\psi_2 \vee \psi_3));$$

Proposition-Exercise 24

Show that the following pairs of formulas ϕ_1, ϕ_2 are logically equivalent:

Distributivity:

$$\phi_1 = ((\psi_1 \wedge \psi_2) \vee \psi_3), \quad \phi_2 = ((\psi_1 \vee \psi_3) \wedge (\psi_2 \vee \psi_3));$$
$$\phi_1 = ((\psi_1 \vee \psi_2) \wedge \psi_3), \quad \phi_2 = ((\psi_1 \wedge \psi_3) \vee (\psi_2 \wedge \psi_3));$$

De Morgan's laws:

$$\phi_1 = \neg(\psi_1 \wedge \psi_2), \quad \phi_2 = (\neg\psi_1 \vee \neg\psi_2);$$
$$\phi_1 = \neg(\psi_1 \vee \psi_2), \quad \phi_2 = (\neg\psi_1 \wedge \neg\psi_2);$$

Double negation:

$$\phi_1 = \neg\neg\psi, \quad \phi_2 = \psi.$$

Definition 25

Basic Semantic Concepts: Logical Consequence

Let Σ be a (possibly infinite) set of well formed formulas in **WFF**, and let $\phi \in$ **WFF**.

We say that ϕ **is a logical (semantical) consequence of** Σ

or alternatively

Σ **logically (semantically) entails** ϕ

if and only if for every propositional assignement z such that

$$M_{PL}(\Sigma, z) = 1$$

we have also that

$$M_{PL}(\phi, z) = 1.$$

We write $\Sigma \models \phi$ for Σ entails ϕ.

Examples 26

(i) ϕ is valid if and only if
the empty set $\emptyset$ entails ϕ, i.e. $\emptyset \models \phi$;

(ii) $\{\phi\} \models \phi$;

(iii) more generally, if $\phi \in \Sigma$, then $\Sigma \models \phi$.

(iv) ϕ and ψ are logically equivalent,
if and only if
$\{\phi\} \models \psi$ and $\{\psi\} \models \phi$.

Proposition-Exercise 27

Some simple but useful properties of the logical consequence relation.

(i) (False implies everything)
For every $\phi \in$ **WFF** we have that $\{\mathbf{F}\} \models \phi$;

(ii) For every $\phi, \psi \in$ **WFF**
$\{\phi\} \models \psi$ iff $(\phi \to \psi)$ is a tautology;

(iii) (Modus Ponens)
For every Σ, ϕ, ψ we have that
$\Sigma \cup \{\phi, (\phi \to \psi)\} \models \psi$.

(iv) (Monotonicity)
If $\Sigma \subseteq \Sigma_1 \subseteq$ **WFF**,
$\phi \in$ **WFF** and $\Sigma \models \phi$ then also $\Sigma_1 \models \phi$.

(v) (Consequence)
$\Sigma \models (\phi \to \psi)$ iff $\Sigma \cup \{\phi\} \models \psi$.

Deciding logical consequence
(and validity)

In the following we sketch a semantic decision procedure for the logical consequence.

It is called **semantic,**
because it resorts to the truth tables
associated with the formulas involved.

A **syntactic** decision procedure is a
decision procedure which uses as its only data
the formulas themselves.

Syntactic decision procedures
will be discussed in a later section.

Theorem 28
Semantic decision procedure (algorithm) for logical consequences

---

Let Σ be a finite set of well formed formulas in **WFF** and $\phi \in$ **WFF**.
There is a decision procedure which decides whether $\Sigma \models \phi$.

Proof:
First we observe that $\Sigma \models \phi$ iff for every $\Sigma \cup \{\neg\phi\}$ is not satisfiable.

Let $\Sigma = \{\psi_1, \ldots, \psi_n\}$
Let TT be the truth table for

$$((\bigwedge_{i=1,\ldots,n} \psi_i) \wedge \neg\phi)$$

This truth table is well defined and finite.

$\Sigma \models \phi$ iff TT is constant with unique value 0. Q.E.D.

Cost of the decision procedure.

Let the Σ and ϕ have variables $p_{i_0}, p_{i_1}, \ldots, p_{i_n}$.
The truth tables has 2^{n+1} values.

Let the $k = rk(\phi) + \sum_{\psi \in \Sigma} rk(\psi)$.

Computing a line of the truth table uses at most 2^k boolean operations.

We have $k \geq n$.

So we get at least 2^{n+1} many boolean operations.

CAN WE DO BETTER ?

SAT: The most important open problem in Propositional Logic

Input: Given a finite set $\Sigma \in CNF$.

Question: Is Σ satsifiable.

Find **efficient** algorithms for SAT

Propositional Modal Logic

Propositional Logic analyses the words

and, or, not, if ... then

Modal Propositional Logic analyses additionally the words

possibly, necessarily

We study this in the course Logic II.

Propositional Temporal Logic

Propositional Logic analyses the words

and, or, not, if ... then

Temporal Propositional Logic analyses additionally the words

next time, previous time
some time in the future,
some time in the past,
always in the future,
always in the past,
until, since

We study this in the course Logic II.

Where do we use Propositional Logics

Propositional Logic (and its Modal and Temporal versions) are used in

- Hardware specification and verification.
- Software specification and verification.
- Automated reasoning and Artificial Intelligence (AI).

First Order Logic

First Order Logic

- Propositional Logic deals with propositions built using **propositional variables** p_i and the connectives

  and, or, not, implies

  and their **consequence relation**.

- Relational Calculus, or First Order Logic, deals with propositions built using additionally **relation symbols, individual variables** v_i and the **quantifiers**

  exists $\exists$**, for all** $\forall$

  and their **consequence relation**.

What do we talk about?

In Propositional Logic we **abstract** from the details of a sentence:

If $a \neq 0$ then
(there is an x with $ax^2 + bx + c = 0$ iff $b^2 \geq 4ac$)

This is of the form

$$(\phi_1 \to ((\phi_2 \to \phi_3) \wedge (\phi_3 \to \phi_2)))$$

with

$\phi_1 : a \neq 0$
ϕ_2 : there is an x with $ax^2 + bx + c = 0$
$\phi_3 : b^2 \geq 4ac$

either true or false.

Now we want to build a language where we can analyze the meaning of the ϕ_i more precisely.

Analyzing atomic sentences

We interpret the statement

If $a \neq 0$ then (there is an x with $ax^2 + bx + c = 0$ iff $b^2 \geq 4ac$)

spontaneously thinking of

addition, multiplication and **order**

which are then thought of as **functions** or **relations** over a set A, e.g. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$.

The truth now depends on the interpretation of $a, b, c \in A$ and the choice of A.

The Natural Numbers with Arithmetic

The structure of the Natural Numbers with Arithmetic

$$\mathfrak{N} = \langle \mathbb{N}, +_N, \times_N, <_N, 0_N, 1_N \rangle$$

consists of

the set $\mathbb{N}$ of natural numbers (with 0),
the **universe** of $\mathfrak{N}$, and
two **functions** *addition* and *multiplication*

$$+_N : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$\times_N : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

a **relation** *less than*

$$<_N \subseteq \mathbb{N} \times \mathbb{N}$$

and two **constants** *zero, one*

$$0_N \in \mathbb{N},\ 1_N \in \mathbb{N}$$

The Real Numbers with Arithmetic

The structure of the Real Numbers with Arithmetic

$$\mathfrak{R} = \langle \mathbb{R}, +_R, \times_R, <_R, 0_R, 1_R \rangle$$

consists of

the set $\mathbb{R}$ of natural numbers (with 0),
the **universe** of $\mathfrak{R}$, and
two **functions** *addition* and *multiplication*

$$+_R : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$
$$\times_R : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

a **relation** *less than*

$$<_R \subseteq \mathbb{R} \times \mathbb{R}$$

and two **constants** *zero, one*

$$0_R \in \mathbb{R},\ 1_R \in \mathbb{R}$$

Other structures with Arithmetic

We have more structures which are quite similar:

The structure of the Integers with Arithmetic

$$\mathfrak{Z} = \langle \mathbb{Z}, +_Z, \times_Z, <_Z, 0_Z, 1_Z \rangle$$

The structure of the Rational Numbers with Arithmetic

$$\mathfrak{Q} = \langle \mathbb{Q}, +_Q, \times_Q, <_Q, 0_Q, 1_Q \rangle$$

The structure of the Complex Numbers with Arithmetic is usually given **without** an order:

$$\mathfrak{C} = \langle \mathbb{C}, +_C, \times_C, 0_C, 1_C \rangle$$

Structures without arithmetic: Directed Graphs

A graph $G = \langle V, E \rangle$ consists of

- a **set** of vertices V, also called the **universe** of G;
- a set of edges E. We can identify an edge $e \in E$ with a pair $\langle v_1, v_2 \rangle$ of vertices and think of $E \subseteq V^2$. E is a **binary relation** on V.

Example:
$V = \{1, 3, 5, 12, 15, 27\}$
$E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$ with

$e_1 = (1, 3)$, $e_2 = (1, 5)$, $e_3 = (3, 12)$,
$e_4 = (5, 15)$, $e_5 = (12, 1)$, $e_6 = (15, 3)$

Structures as Interpretations of Relation (Function, Constant) Symbols

The general form of these structures is given by

$$\mathfrak{A} = \langle A, f_A, g_A, r_A, c_A, d_A \rangle$$

where A is the universe,
f_A, g_A are functions from A to A,
r_A is a binary relation on A ($r_A \subseteq A^2$), and
c_A, d_A are elements of A.

We give f_A, g_A, r_A, c_A, d_A names in a

formal language:

F and G are binary function symbols, with interpretations f_A and g_A respectively.
R is a binary relation symbol, with interpretation r_A
c and d are constant symbols with interpretation c_A and d_A respectively.

Vocabularies and Structures

Vocabularies are sets of

- relation symbols,
- function symbols and
- constant symbols.

Like in natural language, vocabularies for the

relational calculus = first order logic

are the building blocks of first order languages which are subject to various interpretations.

These interpretations are called

first order structures.

Zero order, first order, second order structures

- Propositions are true or false:
  Zero order
- Propositions speak of elements in a set A,
  First order
- Propositions speak of elements in a set A,
  and of subsets of A, A^2, A^3, ...
  which are elements in $\wp(A), \wp(A^2), \wp(A^3), \ldots$
  Second order
- Propositions speak of elements in a set A,
  in $\wp(A^n)$ **and** in $\wp(\wp(A^j)$
  Third order

The arity of a relation or function (symbol)

- Un-ary = with one argument:
  $sin(x)$ is a unary function
  Prime number is a unary relation (predicate).
  $\neg$ is a unary connective.
- Bin-ary = with two arguments:
  Addition is a binary function.
  Order is a binary relation.
  and is a binary connective.
- Tern-ary = with three arguments;
  Quatern-ary = with four arguments

Arity is the number of arguments the function, relation, connective has.

Definition 29
The countable universal vocabulary

The *countable universal vocabulary* τ_ω consists of the following:

(i) For every natural number n and α we have a *relation symbol* $R_{n,\alpha}$ of *arity* n and identification number α;

(ii) For every natural number n and α we have a *function symbol* $F_{n,\alpha}$ of *arity* n and identification number α;

(iii) For every natural number α we have a *constant symbol* c_α.

Definitions 30
Vocabularies

(i) A *vocabulary* is a subset of $\tau \subseteq \tau_\omega$. We usually denote vocabularies with the Greek letter τ or with τ_x where x can be any symbol serving as an index.

(ii) A vocabulary τ is called *finite (empty)* if it is a finite (empty) subset of τ_ω.

(iii) A vocabulary τ is *relational* if it does not contain any function symbol.

Examples 31

(i) $\tau_1 = \{R_{2,0}\}$ is a vocabulary which consists of one binary relation symbol with identification number 0.
τ_1 is relational and finite.

(ii) $\tau_{arith} = \{c_0, c_1, F_{2,0}, F_{2,1}, R_{2,0}\}$ consists of two constant symbols, two binary function symbols and one binary relation symbol.
τ_{arith} is finite but not relational.

Usually $F_{2,0}$ stands for addition, $F_{2,1}$ for multiplication and $R_{2,0}$ for an order relation, so we shall often write, for simplicity, but contrary to our convention,
$\tau_{arith} = \{c_0, c_1, F_+, F_*, R_<\}$.

Definition 32

Interpretations of a vocabulary τ are τ-structures.

Let **Var** be a dummy symbol, later to be used as the name of the set of variables. Let A be any non-empty set and let $\mathfrak{A}$ be a function from $\{\mathbf{Var}\} \cup \tau$ into $A \cup \bigcup_{n\in\mathbb{N}} \wp(A^n)$ such that

(i) $\mathfrak{A}(\mathbf{Var}) = A, A \neq \emptyset$;

(ii) For every constant symbol $c_\alpha \in \tau$ $\mathfrak{A}(c_\alpha) \in A$;

(iii) For every relation symbol $R_{n,\alpha} \in \tau$ $\mathfrak{A}(R_{n,\alpha}) \subseteq A^n$;

(iv) For every function symbol $F_{n,\alpha} \in \tau$ $\mathfrak{A}(F_{n,\alpha})$ is a function from A^n into A.

A is called the *universe* of $\mathfrak{A}$. We say also that $\mathfrak{A}$ is a τ-structure over the universe A.

Example 33

(i) Let $\tau = \emptyset$. Then a τ-structure $\mathfrak{A}$ over a universe A is just the set A.

(ii) Let $\tau = \tau_{arith}$. Let $\mathfrak{N}$ be the τ-structure with $\mathfrak{N}(\mathbf{Var}) = \mathbb{N}$ and with

(i) $\mathfrak{N}(c_0) = 0$, $\mathfrak{N}(c_1) = 1$,

(ii) $\mathfrak{N}(F_{2,0})(n, m) = n + m$,

(iii) $\mathfrak{N}(F_{2,1})(n, m) = n \cdot m$,

(iv) $(n, m) \in \mathfrak{N}(R_{2,0})$ iff $n < m$.

$\mathfrak{N}$ is called the *(standard) Arithmetic Structure of the Natural Numbers*.

If we chose for $\mathfrak{N}(R_{2,0})$ the relation $n \leq m$ we get a **different** structure.

Example 34

(iii) Again, let $\tau = \tau_{arith}$. Let $\mathcal{Z}$ be the τ-structure with $\mathcal{Z}(\mathbf{Var}) = \mathbb{Z}$, the integers, and with

(i) $\mathcal{Z}(c_0) = 0$, $\mathcal{Z}(c_1) = 1$,

(ii) $\mathcal{Z}(F_{2,0})(n, m) = n + m$,

(iii) $\mathcal{Z}(F_{2,1})(n, m) = n \cdot m$,

(iv) $(n, m) \in \mathcal{Z}(R_{2,0})$ iff $n < m$.

$\mathcal{Z}$ is called the *Arithmetic Structure of the Integers*.

If we had defined $(n, m) \in \mathcal{Z}(R_{2,0})$ iff $n \leq m$, again this would be a different structure.

Example 35

Funny structures

We can choose other interpretations, e.g.

(funny) Again, let $\tau = \tau_{arith}$. Let $\mathcal{Z}_{funny}$ be the τ-structure with $\mathcal{Z}(\mathbf{Var}) = \mathbb{Z}$, the integers, and with

(i) $\mathcal{Z}_{funny}(c_0) = 5$, $\mathcal{Z}(c_1) = 2^{1000}$,

(ii) $\mathcal{Z}_{funny}(F_{2,0})(n,m) = gcd(n,m)$,

(iii) $\mathcal{Z}_{funny}(F_{2,1})(n,m) = n^m$,

(iv) $(n,m) \in \mathcal{Z}_{funny}(R_{2,0})$ iff n divides m.

$\mathcal{Z}_{funny}$ was defined to show our freedom of definition. $\mathcal{Z}_{funny}$ is one possible τ_{arith}-structure.

Example 36

The Powerset Structures:

Let A be a set. $\mathcal{P}(A)$ is the τ_{arith}–structure given by

(i) $\mathcal{P}(A)(\mathbf{Var}) = \wp(A)$, the subsets of A;

(ii) $\mathcal{P}(A)(F_+)$ the usual union of two sets,

(iii) $\mathcal{P}(A)(F_*)$ the usual intersection of two sets,

(iv) $\mathcal{P}(A)(R_<)$ the usual inclusion relation between sets,

(v) $\mathcal{P}(A)(c_0) = \emptyset$, $\mathcal{P}(A)(c_1) = A$.

The structure $\mathcal{P}(A)$ is the
set algebra of subset of A.

More examples will be discussed in the sequel.

What we want to say, I

About (undirected) graphs:

- A graph is undirected, i.e. E is a symmetric relation.
- a is an E-neighbor of b, i.e. $(a,b) \in E$.
- Every vertex has exactly two E-neighbors.
- There are no vertices without E-neighbors.
- Every edge is part of a triangle:
  For every two vertices $a \neq b$ with $(a,b) \in E$ there is a vertex c with $c \neq a, c \neq b$ and $(a,c) \in E$ and $(b,c) \in E$.

What we want to say, II

About the natural numbers with arithmetic:

- There are infinitely many a, b, c with $a^2 + b^2 = c^2$.
- There are no a, b, c with $a^3 + b^3 = c^3$, unless $b = 0$.
- There are infinitely many primes p.
- There are infinitely many pairs of primes p, q.
- There are infinitely many pairs of primes p, q with $p - q = 2$.

What we want to say, III

About the rationals or reals with arithmetic:

- Between any two points there is a third point.
- Every polynomial of degree 17 has a zero.
- Every polynomial of degree 17 is a continuous function.
- Every polynomial of degree 17 has a local maximum.

We shall define a language where we can say all this.

What we will NOT be able to say in First Order Logic (but in Second Order Logic)

About the rationals or reals with arithmetic:

- For every **rational** number a there is **natural** number n which $a \leq n$.
- Every polynomial has a zero.
- Every polynomial is a continuous function.
- Every subset of natural numbers has a smallest element.

We shall be able to prove that we
cannot say these things in First Order Logic.

What we will NOT be able to say in First Order Logic (but in Second Order Logic)

About graphs

- A graph is connected.
- A graph is hamiltonian.
- A graph is eulerian
- A graph is planar.
- A graph is k-colorable.

We shall be able to prove that we
cannot say these things in First Order Logic.

Syntax of First Order Logic with Equality

Definition 37
Logical Symbols

Logical symbols are elements of the set
$Logsymb = \{\wedge, \vee, \rightarrow, \neg, \forall, \exists, \approx\}$.
Separator symbols are elements of the set
$Sepsymb = \{(,), ,\}$.

$\wedge$ is read as 'and',

$\vee$ is read as 'or',

$\neg$ is read as 'not',

Definition 38 (4.3.1, contd)
Logical Symbols

$\forall$ is read as 'for all' and is called
universal quantifier,

$\exists$ is read as 'there is' and is called
existential quantifier,

$\approx$ is read as 'equals' and

$\rightarrow$ is read as 'arrow'.
We avoid reading $\rightarrow$ as 'implies', as sometimes suggested in the literature.

Definition 39
(First order) variables

For every $i \in \mathbf{N}$, v_i is an *individual variable*. The set of all individial variables is denoted by **Var**. Note that **Var** is the dummy symbol we had introduced in definition of structures.

Well–formed formulas of First Order Logic are strings containing symbols which are in

$$Logsymb \cup Sepsymb \cup \mathbf{Var} \cup \tau_\omega$$

Definition 40
(Second order) variables

For every $j, \alpha \in \mathbf{N}$, $U_{j,\alpha}$ is an *j-ary relation variable*. The set of all variables is denoted by **RelVar**.

Well–formed formulas of First Order Logic are strings containing symbols which are in

$$Logsymb \cup Sepsymb \cup \mathbf{Var} \cup \mathbf{RelVar} \cup \tau_\omega$$

End of Lecture 2