

# Introduction to formal methods

September 2, 2008



# Chapter 1

## Propositional logic

Propositional logic (PL) is briefly recapitulated, as all logics that will be discussed are extensions of propositional logic.

Propositional logic formalizes reasoning with “not” and “and” about the world at the level of propositions, i.e., atomic assertions that can be true or false.

### 1.1 Syntax

Formal names for propositions and symbols for “not” and “and” are provided. Inductive rules enable to form expressions with these symbols.

**Definition 1.1.1** *The language contains as symbols:*

- i) a countable set of propositional variables:  $PV = \{p, q, \dots\}$ ;*
- ii) logical connectives:  $\neg$  (logical “not”) and  $\wedge$  (logical “and”);*
- iii) auxiliary symbols: ( and ).*

*The set of formulas is the smallest set such that:*

- i) every element of  $PV$  is a formula;*
- ii) if  $\alpha$  is a formula, then so is  $\neg\alpha$ ;*
- iii) if  $\alpha$  and  $\beta$  are formula, then so is  $(\alpha \wedge \beta)$ .*

Where no confusion is likely, parentheses are omitted. Derived connectives are:

- $\alpha \vee \beta \stackrel{def}{=} \neg(\neg\alpha \wedge \neg\beta)$  (logical "or");
- $\alpha \Rightarrow \beta \stackrel{def}{=} \neg\alpha \vee \beta$  (logical "if ... then");
- $\alpha \equiv \beta \stackrel{def}{=} (\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$  (logical "if and only if").

## 1.2 Semantics

The situation in the world, i.e., the semantics of the propositional variables, is modelled as the truth values of the proposition variables. As only one world is considered, this world is not mentioned explicitly in the semantics.

**Definition 1.2.1** A model is a valuation function  $V : PV \longrightarrow \{tt, ff\}$  from the set of propositional variables to the set of logical values  $tt$  and  $ff$ .

The reasoning with "not" and "and", i.e., the semantics of  $\neg$  and  $\wedge$  is given as how the truth of a formula follows from the interpretation of the logical connectives.

**Definition 1.2.2** A model  $V$  satisfies a formula  $\alpha$  (denoted  $V \models \alpha$ ) is defined inductively:

- i)  $V \models p$  iff  $V(p) = tt$ , for  $p \in PV$ ;
- ii)  $V \models \neg\alpha$  iff not ( $V \models \alpha$ ) (denoted as  $V \not\models \alpha$ );
- iii)  $V \models \alpha \wedge \beta$  iff  $V \models \alpha$  and  $V \models \beta$ .

A formula  $\alpha$  is valid if all models satisfy it (denoted  $\models \alpha$ , the converse, invalidity, is denoted as  $\not\models \alpha$ ). A model  $V$  satisfies a set of formulas  $L$  (denoted  $V \models L$ ) if  $V \models \alpha$  for each  $\alpha \in L$ . A formula  $\alpha$  is a semantical consequence of a set of formulas  $L$  (denoted  $L \models \alpha$ ) if  $V \models L$  implies  $V \models \alpha$  for every model  $V$ .

**Example 1.2.1** Interpreting the formulas in the example with all possible combinations of truth values immediately yields the following results.

- i)  $p \vee \neg p$  is valid .
- ii)  $p \wedge q$  is satisfiable.
- iii)  $p \wedge \neg p$  is not satisfiable.

## 1.3 MUTEX

We can now formalize one of the three properties that we formulated about MUTEX.

- Mutual Exclusion: for all states (worlds)  $w$  in the model for MUTEX  
 $V(w) \models \neg(c_1 \wedge c_2)$ .



# Chapter 2

## Modal Propositional Logic

Modal propositional logic (MPL) formalizes reasoning about the situation in different worlds, some of which may be related. Apart from “not” and “and”, reasoning about “all reachable worlds” is now introduced. The level of reasoning remains that of propositions.

### 2.1 Syntax

The language of MPL contains the three symbols of PL, together with the symbol:

- iv) the modal operator  $\Box$  (in all reachable worlds).

The language of a modal system is given by the three formation rules for PL, together with the rule:

- iv) If  $\varphi$  is a formula, so is  $\Box\varphi$ .

The derived operators are as in the case of PL, together with the derived dual modality:  $\Diamond\varphi \stackrel{def}{=} \neg\Box\neg\varphi$  (there exists a reachable world).

### 2.2 Semantics

The fact that different worlds and their relationships are considered needs to be reflected in the interpretation. To this end frames are used. A *frame* is a pair  $(W, R)$ , where  $W$  is a non-empty set of worlds and  $R \subseteq W \times W$  is a binary (accessibility) relation on  $W$ . Like in the case of PL, the situation in

a world is reflected by assigning values to propositional variables. Again, but now for each world, these are given by a valuation function. This leads to the following notion of model.

**Definition 2.2.1** A model is a triple  $M = (W, R, V)$ .

1.  $W$  is a non-empty set of states (worlds).
2.  $R \subseteq W \times W$  is a binary (accessibility) relation on  $W$ .
3.  $PV$  a set of propositional variables.
4.  $V$  a valuation function  $V : W \times PV \longrightarrow \{tt, ff\}$ .

Note, that this is exactly the same model as used for the semantics of systems.

There are two different ways in which models are used as interpretations, influencing the notion of validity. For the simplest interpretation the notion of model defined so far suffices. For the other interpretation a small extension is necessary: A model  $M$  is *anchored* if there is one distinguished world  $w_0 \in W$ , called the *anchor* of  $M$ . If the second interpretation is used, this will be indicated explicitly.

**Definition 2.2.2** A formula  $\varphi$  is satisfied at a world  $w$  in a model  $M$  (denoted  $M, w \models \varphi$ ) is defined inductively:

- i)  $M, w \models p$  iff  $V(w, p) = tt$ , for  $p \in PV$ ,
- ii)  $M, w \models \neg\varphi$  iff  $M, w \not\models \varphi$ ,
- iii)  $M, w \models \varphi \wedge \psi$  iff  $M, w \models \varphi$  and  $M, w \models \psi$ ,
- iv)  $M, w \models \Box\varphi$  iff (for all  $w' \in W$ ) ( $w R w'$  implies  $M, w' \models \varphi$ ).

A formula is satisfiable if it is satisfied at some world in some model. A formula  $\varphi$  is valid in the model  $M$  (denoted  $M \models \varphi$ ) if it is satisfied at each world of  $M$ . A formula  $\varphi$  is valid (denoted  $\models \varphi$ ) if it is valid in all models.

Notions like the above and like those defined for PL will also be used relativized with respect to classes of models. Let  $\mathcal{M}$  be a class of models. A formula which is true at some world in some model from  $\mathcal{M}$  is called  $\mathcal{M}$ -satisfiable. A formula  $\varphi$  which is valid in all models from  $\mathcal{M}$  is called  $\mathcal{M}$ -valid (denoted  $\models_{\mathcal{M}} \varphi$ ).

Similar notions apply for the anchored interpretation. A formula which is true at the anchor of some anchored model is called *A-satisfiable*. A formula  $\varphi$  which is true at the anchor of an anchored model  $M$ , is called *A-valid in the model  $M$*  (denoted  $M \models^A \varphi$ ). A formula  $\varphi$  which is valid in all anchored models is called *A-valid* (denoted  $\models^A \varphi$ ). Again, the notions can be relativized. A formula which is true at the anchor of some anchored model in  $\mathcal{M}$  is called *A- $\mathcal{M}$ -satisfiable*. A formula  $\varphi$  which is A-valid in all models from a class of anchored models  $\mathcal{M}$  is called *A- $\mathcal{M}$ -valid* (denoted  $\models_{\mathcal{M}}^A \varphi$ ). Where no confusion seemed likely, indices are omitted. For the rest of this chapter the definitions for unanchored models are used.

## 2.3 MUTEX

We can now formalize the properties that we formulated about MUTEX to some extend.

- Mutual Exclusion:  $M \models \neg(c_1 \wedge c_2)$ .
- Eventual Access:  $M \models t_1 \Rightarrow \Box(c_1 \vee \Box(c_1 \vee \Box(c_1 \vee \Box c_1)))$  - “If  $t_1$  then in at most four steps  $c_1$ ”. (Not very nice: clumsy formula, and also counting steps.)
- Non-blocking:  $M \models n_1 \Rightarrow \Diamond t_1$ .



# Chapter 3

## Propositional linear time temporal logic

Linear time temporal logic (LTL) formalizes reasoning about different worlds that are related in a sequential order, which intuitively reflects one time line. This means, that models are limited to infinite linear ones. Apart from the “reachable in one step” operator, also operators that involve more steps are introduced. All of these operators are expressible via two newly added operators. The level of reasoning remains that of propositions.

### 3.1 Syntax of PLTL

For historical reasons, the “reachable” operator, denoted in modal logic with  $\Box$ , is in *LTL* denoted by  $\bigcirc$ , called “next”. Apart from this operator, also the binary operator  $U$  is now introduced.

The set of LTL *formulas* is defined inductively, given a set  $PV$  (of Propositional Variables, including special ones *true* and *false*).

- S1. every member of  $PV$  is a formula;
- S2. if  $\phi$  and  $\psi$  are formulas, then so are  $\neg\phi$  and  $\phi \vee \psi$ ;
- S3. if  $\phi, \psi$  are formulas, then so are  $\bigcirc\phi$  and  $(\phi U \psi)$ .

The connectives  $\wedge$  and  $\Rightarrow$  are defined in the standard way. The operators  $\diamond$  (eventually) and  $\square$  (always), (using the same  $\square$  notation as in modal logic for a different operator)! can be derived as follows:

- $\diamond\phi := trueU\phi$ ;

- $\Box\phi := \neg\Diamond\neg\phi$ .

## 3.2 Semantics of PLTL

We use a linear subset of the models for modal logic. To indicate this choice, we combine the information in the  $W$  and  $R$  part from the modal models  $(W, R, V)$  into an infinite path notation  $p = (w_0, w_1, \dots)$ . This leads to the following semantics.

Let  $M = \langle p, V \rangle$  be a *model*, i.e.,  $p = (w_0, w_1, \dots)$  and  $V : W \times PV \longrightarrow \{tt, ff\}$ . We denote the suffix  $(w_i, w_{i+1}, \dots)$  of  $p$  by  $p_i$ .

S1.  $M, w_i \models q$  iff  $V(w_i, q) = tt$ , for  $q \in PV$ ;

S2.  $M, w_i \models \neg\phi$  iff not  $M, w_i \models \phi$ ;

$M, w_i \models \phi \vee \psi$  iff  $M, w_i \models \phi$  or  $M, w_i \models \psi$ ;

S3.  $M, w_i \models \bigcirc\phi$  iff  $M, w_{i+1} \models \phi$ ;

$M, w_i \models (\phi U \psi)$  iff there is  $k \geq i$  such that  $M, w_k \models \psi$  and for all  $j$ ,  $i \leq j < k$ ,  $M, w_j \models \phi$ .

Validity in a model  $M$  or general validity is defined as for Modal logic.

The connection with systems is, that a property  $\varphi$  holds for a system  $S$  if it holds for all models that are paths in the transition system for that system. For that we write  $S \models \varphi$ .

## 3.3 MUTEX

We can now formalize the first and second properties that we formulated about MUTEX more properly.

- Mutual Exclusion:  $S \models \neg(c_1 \wedge c_2)$ .
- Eventual Access:  $S \models (t_1 \Rightarrow \Diamond c_1)$ .

Note, that in case of anchored validity, a property expressed by a formula *varphi* for the non-anchored case is expressed by prefixing the formula with a  $\Box$ , e.g., turning it into  $\Box\varphi$ .