Program Verification (CS1.303)

Monsoon 2021, IIIT Hyderabad
07 Jan, Friday (Lecture 2)

Taught by Prof. Venkatesh Choppella

Propositional Logic (contd.)

Before moving onto the semantics of propositional logic, we must make it clear that there are three languages involved here: the discourse language (English), the language of propositional logic expressions, and the language of booleans. The words *and*, *or*, *implies*, *not*, $=$, $\implies$ and $\iff$ belong to the first; the operators $\vee, \wedge, \rightarrow, \neg$ belong to the second; but we also have boolean operators $\overline{\vee}, \overline{\wedge}, \overline{\rightarrow}, \overline{\neg}$, which are binary functions on truth values and **not** expressions.

$$\overline{\wedge} : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$$
$$\overline{\vee} : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$$
$$\overline{\rightarrow} : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$$
$$\overline{\neg} : \mathbb{B} \rightarrow \mathbb{B}$$

Thus, the statements

$$b = 1 \iff \overline{\neg}(b) = 0$$
$$b = 0 \iff \overline{\neg}(b) = 1$$

are structural lemmas in the discourse language. We will call them $\overline{\neg}1$ and $\overline{\neg}0$ respectively.

Similarly, we have

$$a \overline{\wedge} b = 1 \iff a = 1 \text{ and } b = 1$$
$$a \overline{\wedge} b = 0 \iff a = 0 \text{ or } b = 0$$

named $\overline{\wedge}1$ and $\overline{\wedge}0$ respectively. We can also express $\overline{\wedge}0$ as two lemmas

$$a = 0 \implies a \overline{\wedge} b = 0 \forall b \in \mathbb{B}$$

$$b = 0 \implies a \overline{\wedge} b = 0 \forall a \in \mathbb{B}$$

named $\overline{\wedge}0L$ and $\overline{\wedge}0R$ respectively.

We also have the boolean equality lemmas, like

$$a_1 = a_2 \iff \overline{\neg} a_1 = \overline{\neg} a_2$$

$$a_1 = a_2 \text{ and } b_1 = b_2 \implies a_1 \mathbin{\overline{\wedge}} b_1 = a_2 \mathbin{\overline{\wedge}} b_2$$

named $\overline{\neg} \iff$ and $\overline{\wedge} \implies$ respectively.

These lemmas have **no** relation with propositional logic.

Semantics of Propositional Logic

Interpretation

An *interpretation* I is a map from Var to $\mathbb{B}$:

$$I : \text{Var} \to \mathbb{B}$$

For example, we could define $I_1 = \{p \to 0, q \to 1, r \to 0, ...\}$, and $I_2 = \{p \to 0, q \to 0, r \to 0, ...\}$. We say that these two interpretations *agree* on the variables p and r. Rigorously, if $X \subseteq \text{Var}$, and if $\forall p \in X, I_1(p) = I_2(p)$, then I_1 and I_2 agree on X, written $I_1 =_X I_2$.

Interpretations are also called *assignments*.

Valuation

A valuation is a fuction that takes an interpretation and an expression, and returns a boolean value:

$$\text{val} : \text{Interpretation} \times \text{Exp} \to \mathbb{B}$$

The interpretation gives a context in which the expression is evaluated.

$\text{val}(I, e)$ can be defined inductively:

$$\begin{aligned} \text{val}(I, p) &= I(p) \\ \text{val}(I, \neg e) &= \overline{\neg}\text{var}(I, e) \\ \text{val}(I, e_1 \wedge e_2) &= \text{val}(I, e_1) \mathbin{\overline{\wedge}} \text{val}(I, e_2) \\ \text{val}(I, e_1 \vee e_2) &= \text{val}(I, e_1) \mathbin{\overline{\vee}} \text{val}(I, e_2) \\ \text{val}(I, e_1 \to e_2) &= \text{val}(I, e_1) \mathbin{\overline{\to}} \text{val}(I, e_2) \end{aligned}$$

For example, $\text{val}(\{p \to 0, q \to 1, ...\}, p \vee q) = 1$.

Lemma. Let e be a propositional logic expression and I_1, I_2 be interpretations such that $I_1 =_{\text{vars}(e)} I_2$. Then $\text{val}(I_1, e) = \text{val}(I_2, e)$.
Informally, only the propositional variables of e are relevant in its evaluation.

We say that two expressions e_1, e_2 are equivalent, or $e_1 \equiv e_2$, iff $\forall I, \mathrm{val}(I, e_1) = \mathrm{val}(I, e_2)$. For example,

$$p \to q \equiv \neg p \vee q$$

$\equiv$ is a discourse symbol and **not** a propositional logic symbol.

We can define macros in propositional logic, treating them as constants. For example, we can let

$$T := p \vee \neg p$$
$$\perp := p \wedge \neg p$$

These macros are simply names for formulas; they embellish the syntax without adding any expressive capability to it.

Definition. A tautology is an expression e such that $\mathrm{val}(I, e) = 1$ for every interpretation I.
The macro T defined above is an example of a tautology.

Definition. An interpretation I is a model for an expression e, written $I \vDash e$ (or simply $\vDash e$), iff $\mathrm{val}(I, e) = 1$.