Sept 24, 2013

LECTURE #4

PRINCIPLE OF EXTENSIONALITY:

$\omega : PV \to \{0,1\}$ ≡ Propositional Valuation.

Extend ω to all of $\mathcal{F}$, $\omega : \mathcal{F} \to \{0,1\}$

Truth value of a connected sentence depends only on the truth values of its constituent part.

$$\omega(\neg\alpha) = 1 - \omega(\alpha) = 1 - \omega\alpha$$
$$\omega(\alpha \wedge \beta) = \omega\alpha \cdot \omega\beta$$
$$\omega(\alpha \vee \beta) = \max(\omega\alpha, \omega\beta)$$

SEMANTIC EQUIVALENCE: (LOGICAL EQUIVALENCE)

$\alpha \equiv \beta$ ("α is semantically equivalent to β")

iff $\forall_{\text{valuation},\, \omega}\ \omega\alpha = \omega\beta$.

1. $\omega \neg\neg\alpha = 1 - \omega\neg\alpha = 1 - (1 - \omega\alpha) = \omega\alpha$

   $\alpha \equiv \neg\neg\alpha$

2. ASSOCIATIVITY:

   $\alpha \wedge (\beta \wedge \gamma) \equiv \alpha \wedge \beta \wedge \gamma$

   $\alpha \vee (\beta \vee \gamma) \equiv \alpha \vee \beta \vee \gamma$

3. COMMUTATIVITY:

   $\alpha \wedge \beta \equiv \beta \wedge \alpha$; $\alpha \vee \beta \equiv \beta \vee \alpha$

4. IDEMPOTENT:

   $\alpha \wedge \alpha \equiv \alpha$; $\alpha \vee \alpha \equiv \alpha$.

Conventions.

(C_1) The outermost parantheses may be omitted:

$((\alpha \wedge \beta) \vee \neg\alpha)$

$\equiv (\alpha \wedge \beta) \vee \neg\alpha$

(C_2) BINDING ORDER

In the order

$\neg, \wedge, \vee, \to, \leftrightarrow$

the former binds more strongly than the latter

$((\alpha \wedge \beta) \vee \neg\alpha)$

$\equiv \alpha \wedge \beta \vee \neg\alpha$

(C_3) $\to$ ≡ Right Associa[tive]

$\wedge, \vee$ ≡ Left Associative

$\alpha \to \beta \to \gamma \equiv \alpha \to (\beta \to \gamma)$

(5) ABSORPTION:

$$\alpha \wedge (\alpha \vee \beta) \equiv \alpha ; \quad \alpha \vee (\alpha \wedge \beta) \equiv \alpha$$

(6) $\wedge$-DISTRIBUTIVITY:

$$\alpha \wedge (\beta \vee \gamma) \equiv \alpha \wedge \beta \ \vee \ \alpha \wedge \gamma$$

(7) $\vee$-DISTRIBUTIVITY:

$$\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$$

(8) de Morgan's Rules:

$$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta ; \quad \neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta .$$

(9) $\alpha \vee \neg\alpha \equiv \top ; \quad \alpha \wedge \neg\alpha \equiv \bot$

$\alpha \wedge \top \equiv \alpha \vee \bot \equiv \alpha .$

How hard is it to test whether two formulas are equivalent?

$$\alpha \equiv \beta \ ?$$

$$\neg\alpha \equiv \alpha \vee \neg\alpha \Leftrightarrow \neg\alpha \equiv \top \Leftrightarrow \forall_\omega \ \omega\neg\alpha = 1 \Leftrightarrow \neg \exists_\omega \ \omega\neg\alpha = 0$$

$$\Leftrightarrow \neg \exists_\omega \ \omega\alpha = 1$$

$$\alpha \equiv (x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_2 \vee \bar{x}_3 \vee \bar{x}_4) \cdots (x_5 \vee \bar{x}_6 \vee x_7)$$

"SEMANTIC EQUIVALENCE" is an EQUIVALENCE RELATION.

(Reflexivity) $\forall_\alpha \quad \alpha \equiv \alpha$

(Symmetry) $\forall_{\alpha, \beta} \quad \alpha \equiv \beta \Rightarrow \beta \equiv \alpha$

(Transitivity) $\forall_{\alpha,\beta,\gamma} \quad \alpha \equiv \beta \wedge \beta \equiv \gamma \Rightarrow \alpha \equiv \gamma$

A CONGRUENCE RELATION

$$\forall_{\alpha,\alpha',\beta,\beta'} \quad \alpha \equiv \alpha' \wedge \beta \equiv \beta' \Rightarrow \alpha \circ \beta \equiv \alpha' \circ \beta' \quad \{ \circ \in \{\wedge, \vee\}$$

REPLACEMENT THEOREM:

$$\alpha \equiv \alpha' \Rightarrow \varphi \equiv \varphi[\alpha/\alpha']$$

↳ Obtained from φ by replacing one or several of the possible occurrences of the subformula α in φ by α'.

Every Boolean function can be represented by a BOOLEAN FORMULA $\in \mathcal{F}$.

NORMAL FORMS:

1) LITERALS:

Defn: Prime formulas and negations of prime formulas are called literals.

$$p_i \;,\; \neg p_i \;, \ldots$$

2) DISJUNCTIVE NORMAL FORMS (DNF)

Defn: A disjunction

$$\alpha_1 \vee \alpha_2 \vee \cdots \vee \alpha_n$$

where each α_i is a conjunction of literals, is called a ~~di~~ Disjunctive Normal Form (DNF).

3) CONJUNCTIVE NORMAL FORMS (CNF)

Defn: A conjunction

$$\beta_1 \wedge \beta_2 \wedge \cdots \wedge \beta_m$$

where each β_i is a disjunction of literals, is called a Conjunctive Normal Form (CNF).

THM (Constructive : Proof by Induction)

Every Boolean ~~formula~~ function f with

$$f \in \mathcal{B}_n \quad (n > 0)$$

is representable by a DNF, namely by

$$\alpha_f := \bigvee_{f\vec{x}=1} p_1^{x_1} \wedge \dots \; p_n^{x_n}$$

(Using de Morgan's Rule: At the same time f is representable by a CNF, namely by

$$\beta_f := \bigwedge_{f\vec{x}=0} p_1^{\neg x_1} \vee \dots \; p_n^{\neg x_n} \quad)$$

> **Notation:**
>
> $$p_i^1 := p_i \qquad p_i^0 := \neg p_i$$
>
> $$\omega(p_1^{x_1} \wedge p_2^{x_2}) = 1 \quad \text{iff} \quad \omega p_1 = x_1 \;\; \& \;\; \omega p_2 = x_2$$
>
> $$\omega(p_1^{\neg x_1} \vee p_2^{\neg x_2}) = 0 \quad \text{iff} \quad \omega p_1 = \neg x_1 \;\; \& \;\; \omega p_2 = \neg x_2$$

Example: $\quad f : \{0,1\}^2 \rightarrow \{0,1\}$

	x_1	x_2	f	
	0	0	1	←
←	0	1	0	
←	1	0	0	
	1	1	1	←

CNF

$$(p_1^1 \vee p_2^0) \wedge (p_1^0 \vee p_2^1)$$
$$\equiv (p_1 \vee \neg p_2) \wedge (\neg p_1 \vee p_2)$$
$$\equiv (p_2 \rightarrow p_1) \wedge (p_1 \rightarrow p_2)$$
$$\equiv p_1 \leftrightarrow p_2$$

DNF

$$(p_1^0 \wedge p_2^0) \vee (p_1^1 \wedge p_2^1)$$
$$\equiv (\neg p_1 \wedge \neg p_2) \vee (p_1 \wedge p_2)$$

Proof.

By defn of α_f

$$\omega(\alpha_f) = 1 \iff \exists \vec{x} \;\; f\vec{x} = 1 \;\wedge\; \omega(p_1^{x_1} \wedge p_2^{x_2} \wedge \cdots \wedge p_n^{x_n}) = 1$$

$$\iff \exists \vec{x} \;\; f\vec{x} = 1 \;\; \omega\vec{p} = \vec{x}$$

$$\iff f\,\omega\vec{p} = 1$$

$$\omega\alpha_f = 1 \quad \text{iff} \quad f\omega\vec{p} = 1$$

Since there are only two values:

$$\omega\alpha_f = 0 \quad \text{iff} \quad f\omega\vec{p} = 0$$

$$\therefore \quad \forall_\omega \;\; \omega\alpha_f \equiv f\omega\vec{p}$$

The rest follows from de Morgan's Law. $\square$

Corollary:

Each $\varphi \in \mathcal{F}$ is semantically equivalent to a DNF or a CNF.

FUNCTIONAL COMPLETENESS:

A logical signature is called functionally complete, if every Boolean formula is representable in this signature.

Examples:

(1) $\{\neg, \wedge, \vee\} \rightarrow$ CNF or DNF

(2) $\{\neg, \wedge\}$

(3) $\{\neg, \vee\}$ } $\rightarrow$ de Morgan's Law

(4) $\{\rightarrow, \bot\}$

$$\neg p \equiv p \rightarrow \bot$$
$$p \vee q \equiv \neg p \rightarrow q \equiv (p \rightarrow \bot) \rightarrow q$$

(5) $\{\downarrow\}$ NOR

$$\neg p \equiv p \downarrow p \equiv p \uparrow p$$
$$p \wedge q \equiv \neg p \downarrow \neg q \equiv (p \downarrow p) \downarrow (q \downarrow q)$$

(6) $\{\uparrow\}$ NAND

$$p \vee q \equiv \neg p \uparrow \neg q \equiv (p \uparrow p) \uparrow (q \uparrow q)$$

TAUTOLOGIES & LOGICAL CONSEQUENCES.

$\models$ "Satisfiability Relation"

$\boxed{\omega \models \alpha \quad \Leftrightarrow \quad \omega\alpha = 1}$ (ω satisfies α)

X = Set of formulas

$$\omega \models X \Leftrightarrow \forall_{\alpha \in X}\, \omega \models \alpha \Leftrightarrow \forall_{\alpha \in X}\, \omega\alpha = 1$$
$$\Leftrightarrow \left(\prod_{\alpha \in X} \omega\alpha \right) = 1.$$

We also say "ω is a (propositional) model of α."

A given α (resp. X) is <u>satisfiable</u> (SAT) if $\exists \omega : PV \to \{0,1\}$ with

$$\omega \models \alpha \quad (\text{or resp. } \omega \models X)$$

$p \in PV$

$$\omega \models p \Leftrightarrow \omega p = 1\,;$$
$$\omega \models \neg\alpha \Leftrightarrow \omega \not\models \alpha\,;$$
$$\omega \models \alpha \wedge \beta \Leftrightarrow \omega \models \alpha \text{ and } \omega \models \beta\,;$$
$$\omega \models \alpha \vee \beta \Leftrightarrow \omega \models \alpha \text{ or } \omega \models \beta.$$

Inductive Defn of Satisfiability

SAT.

<u>Given:</u> α (resp. X)

<u>Find:</u> A propositional valuation (or truth-assignment)

$$\omega : PV \to \{0, 1\}$$

s.t.

$$\omega \models \alpha \qquad (\text{resp. } \omega \models X).$$

<u>Defn</u> A wff α is called <u>logically valid</u> (or a <u>Tautology</u>)

$$\models \alpha$$

whenever $\omega \models \alpha$, for all valuations, ω.

In this case $\alpha \equiv \top$.

<u>Defn</u> A wff α is called a <u>Contradiction</u>

$$\not\models \alpha$$

whenever $\omega \not\models \alpha$ for all valuations, ω.

In this case $\alpha \equiv \bot$.

Examples:

$\models \alpha \vee \neg\alpha$ $\begin{cases} \text{Tertium non datur} \\ \text{Law of excluded middle} \end{cases}$

$\not\models \alpha \wedge \neg\alpha$ $\{$ Contradiction.

$\models \alpha \to \alpha$ Self-implication

$\models (p \to q) \to (q \to r) \to (p \to r)$ chain rule

$\models (p \to q \to r) \to (q \to p \to r)$ Exchange of premise

$$
*\begin{cases}
\models (p\to q\to r)\to (p\to q)\to(p\to r) & \text{(Frege's Formula)}\\
\models ((p\to q)\to p)\to p & \text{(Peirce's Formula)}\\
\models p\to q\to p & \text{(Premise charge)}
\end{cases}
$$

All tautologies in $\to$ alone derivable from $(*)$ $\{$Last 3 stmts.$\}$

LOGIC PROBLEMS

SAT	Is a formula satisfiable? $\exists_\omega \ \omega\models\alpha$	NP-complete
TAUT	Is a formula a tautology? $\forall_\omega \ \omega\models\alpha$	co-NP complete
EQUIV	Are two formulas semantically equivalent? $\forall_\omega \ \omega\models\alpha\leftrightarrow\beta$	co-NP complete

LOGICAL CONSEQUENCE

Defn: α is a logical consequence of X, written

$$X \models \alpha$$

if $\forall$ model ω of X $\quad \omega \models \alpha$

That is,

$$\forall \text{ valuation } \omega \quad \omega \models X \rightarrow \omega \models \alpha .$$

$$\phi \models \alpha \quad \triangleq \quad \alpha \text{ is a tautology.}$$

Given (α, X)
Decide if $X \models \alpha$ $\Big\}$ co-NP-complete.

Examples.

(i) $\alpha, \beta \models \alpha \wedge \beta \qquad \alpha \wedge \beta \models \alpha, \beta$

(ii) $\alpha, \alpha \rightarrow \beta \models \beta$ ← $\boxed{\text{Modus Ponen}}$

(iii) $X \models \bot \Rightarrow X \models \alpha$ for all α

(iv) $X, \alpha \models \beta \;\; \& \;\; X, \neg\alpha \models \beta$

$\Rightarrow X \models \beta.$

Properties of Satisfaction Relation ($\models$)

(R) Reflexivity $\quad \alpha \in X \quad X \models \alpha \quad$ (i.e. $\alpha \models \alpha$)

(M) Monotonicity $\quad X \models \alpha \;\; \& \;\; X \subseteq X'$

$\Rightarrow X' \models \alpha$

(T) Transitivity $\quad X \models Y \;\; \& \;\; Y \models \alpha$

$\Rightarrow X \models \alpha$

FINITARY

$X \models \alpha \Rightarrow$ For some finite subset $X_0 \subseteq X$
$X_0 \models \alpha$.

DEDUCTION THEOREM

$$(D) \qquad X, \alpha \models \beta \quad \Rightarrow \quad X \models \alpha \to \beta .$$

Proof: $X, \alpha \models \beta$; $\omega =$ Model for X, i.e. $\omega \models X$

(i) $\omega \models \alpha \Rightarrow \omega \models \beta \Rightarrow \cancel{\omega \not\models \alpha \text{ or } \omega \models \beta}$ $\omega \models \alpha \to \beta$
($\beta =$ true)
$\omega\beta = 1$

(ii) $\omega \not\models \alpha \Rightarrow \omega \models \alpha \to \beta$
($\alpha =$ false, $\omega\alpha = 0$)

$\Rightarrow \forall \omega \quad \omega \models X \Rightarrow \omega \models \alpha \to \beta$

Hence, $X \models \alpha \to \beta$. $\square$

Iterated Application of (D).

$\alpha_1, \alpha_2, \cdots, \alpha_n \models \beta$
$\Leftrightarrow \quad \models \alpha_1 \to \alpha_2 \to \cdots \to \alpha_n \to \beta$
$\Leftrightarrow \quad \models (\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n) \to \beta$

Example.

$p, q \models p$
$\Leftrightarrow \quad p \models q \to p$
$\Leftrightarrow \quad \models p \to q \to p$.

k-SAT $\rightarrow$ 3-SAT.

Clauses: $C = \{c_1, c_2, \cdots, c_m\}$

Variables: $U = \{u_1, u_2, \dots u_n\}$

$c_i \in C \rightarrow$ Literals $\rightarrow \{z_1, z_2, \dots, z_k\}$ $\quad z_j \in \{u_{jr}, \bar{u}_{jr}\}$

For each clause c_i introduce additional variables

$\{y_{i1}, y_{i2}, \cdots, y_{i,k-3}\}$ $k \geq 3$

$\{y_{i1}, y_{i2}\}$ $k \leq 3$

$k=1$ $\quad c_i = z_1$ $\quad c_i' = (z_1 \vee y_{i1} \vee y_{i2}) \wedge$
$(z_1 \vee \bar{y}_{i1} \vee y_{i2}) \wedge$
$(z_1 \vee y_{i1} \vee \bar{y}_{i2}) \wedge$
$(z_1 \vee \bar{y}_{i1} \vee \bar{y}_{i2})$

$k=2$ $\quad c_i = z_1 \vee z_2$ $\quad c_i' = (z_1 \vee z_2 \vee y_{i1}) \wedge$
$(z_1 \vee z_2 \vee \bar{y}_{i1})$

$k=3$ $\quad c_i = (z_1 \vee z_2 \vee z_3)$ $\quad c_i' = (z_1 \vee z_2 \vee z_3)$

$k>3$ $\quad c_i = (z_1 \vee z_2 \vee z_3 \vee \cdots \vee z_k)$

$c_i' = (z_1 \vee z_2 \vee y_{i1}) \wedge (\bar{y}_{i1} \vee z_3 \vee y_{i2}) \wedge$
$(\bar{y}_{i2} \vee z_4 \vee y_{i3}) \wedge \cdots$
$\wedge (\bar{y}_{i,l-2} \vee z_l \vee y_{i,l-1}) \wedge \cdots$
$\wedge (\bar{y}_{i,k-3} \vee z_{k-1} \vee z_k)$

a) $z_1 = T$ or $z_2 = T \Rightarrow \forall_j \; y_{ij} = F$

b) $z_{k-1} = T$ or $z_k = T \Rightarrow \forall_j \; y_{ij} = T$

c) $z_l = T \Rightarrow \forall_{j \leq l-2} \; y_{ij} = T$
$\; \& \; \forall_{j \geq l-1} \; y_{ij} = F$

d) $\forall_l \; z_l = F \Rightarrow c_i' \equiv \bot = y_{ik-3}$

$c_i' = y_{i1} \wedge (\bar{y}_{i1} \vee y_{i2}) \wedge (\bar{y}_{i2} \vee$
$\dots (\bar{y}_{ik2} \vee y_{i,k-3}) \wedge \bar{y}_{i,k}$
$\equiv y_{i1} \wedge (y_{i1} \rightarrow y_{i2}) \cdots (y_{ik2} \rightarrow y_{ik-3}) \wedge \bar{y}_{i}$