CS498 MP
Logic in Computer Science
Spring 2017

Madhusudan Parthasarathy (Madhu)

Lectures: Tue / Thu 9:30am-10:45pm (1304 Siebel)
Website:  http://courses.engr.illinois.edu/cs498mp3/
Newsgroup(piazza):
Prerequisites:
  Mathematical maturity; some discrete math (CS173) and theory of computation (CS373) background.
  Come talk to me if you don’t have this background.
Propositional Logic

$
\land
$

Elec. eng.

Logician's view

Machinist's view
Countable set

S is countable (or countably infinite) if its elements can be enumerated as

\[ a_0, a_1, a_2, \ldots \]

\(\mathbb{Q}\) is countable

\(\mathbb{R}\) is not countable

\(\mathbb{N}\) is countable

\(\mathbb{Z}\) is countable 0, -1, 1, -2, 2, -3, 3, ...
Suppose $\Sigma$ is a finite alphabet.

$\Sigma^*$ - set of finite strings over $\Sigma$

$\Sigma = \{a, b, c\}$

$\Sigma^* = \{\varepsilon, a, b, c, aa, ab, ac, \ldots\}$

$\Sigma^*$ is countable.
Fix $\mathcal{P}$, a countable set of propositions (or "propositional variables")

$$\mathcal{P} = \{ p_0, p_1, p_2, \ldots \}$$

Syntax of Prop Logic

Let $WFF$ be the smallest set such that

- Every proposition $p \in \mathcal{P}$ is in $WFF$,
- If $\phi$ and $\phi'$ are in $WFF$,
  - then $(\phi \lor \phi')$, $(\phi \land \phi')$, $(\neg \phi)$ are also in $WFF$.\)
Grammar a for WFF

\[
\text{WFF} ::= \ \ p \ | \ (\phi \cup \psi_2) \ | \ (\phi \cap \psi_2) \ | \ \neg \phi, \\
\psi, \psi_2 \ in \ \mathcal{P}
\]

let \( W \) be the class of all sets that satisfy the propositional \( \psi \).

Let \( W_0 = \bigcup \{ \psi \mid \psi \in W \} \)

\( W_0 \) satisfies the two properties and is the smallest.
\[ WFF'_{0} = \emptyset \]

\[
WFF'_{i+1} = \left\{ \begin{array}{c}
\forall, \forall' \in WFF'_{i} \cup \\
\end{array} \right.
\begin{array}{c}
(\forall \land \forall'), (\forall \lor \forall'), \top \quad | \\
\forall, \forall' \in WFF'_{i}
\end{array}
\right\}
\]

\[
WFF' = \bigcup_{n \geq 0} WFF'_{n}
\]

\[
\forall n \in \mathbb{N} \quad WFF'_{n} \subseteq U
\]

- U - any set satisfying the conditions
\[\text{wff}_0' = \{ p_0, p_1, p_2, \ldots \} \]

\[\text{wff}_1' = \{ p_0, p_1, \ldots \} \cup \{(p_0 \wedge p_i), (p_i \wedge p_0), (p_i \vee p_3)\} \]

\[\text{wff}_2' = \{ \ldots \} \cup \{ \forall \}\]

\[\cup \{ (p_0 \wedge p_i) \wedge (p_i \wedge p_3), \ldots \} \]
All formulas in WFF have property Q.

By induction on n that WFF_n has property Q.

Base case: You show all properties in 0 have property Q.

Inductive step: Assume \( \phi, \phi' \) satisfy property Q.

Show \((\phi \lor \phi')\), \((\phi \land \phi')\), \(\forall \phi \) satisfy property Q.
Semantics

$\text{(p \lor q)} \nu r$

Model: Think of this as a world that

or

Valuation determines basic facts.

A valuation $\nu$ is a function $\nu : P \rightarrow \{\text{false}, \text{true}\}$
Fix \( \nu : \mathcal{P} \to \{ \top, \bot \} \)

Let \( \hat{\nu} : \text{WFF} \to \{ \top, \bot \} \) defined as follows.

1. For any \( p \in \mathcal{P} \), \( \hat{\nu}(p) = \nu(p) \)

2. For any \( \alpha \in \text{WFF} \) of the form \( \neg \beta \)
   \[
   \hat{\nu}(\alpha) = \begin{cases} 
   \top & \text{if } \hat{\nu}(\beta) = \bot \\
   \bot & \text{if } \hat{\nu}(\beta) = \top 
   \end{cases}
   \]

3. For any \( \alpha \in \text{WFF} \) of the form \( \beta \lor \gamma \)
   \[
   \hat{\nu}(\alpha) = \begin{cases} 
   \top & \text{if } \hat{\nu}(\beta) = \top \text{ and } \hat{\nu}(\gamma) = \bot \\
   \bot & \text{if } \hat{\nu}(\beta) = \bot \text{ and } \hat{\nu}(\gamma) = \top \\
   \top \lor \bot & \text{otherwise}
   \end{cases}
   \]
For any $\alpha \in WF \cap \mu$ for $\beta \wedge \gamma$

$\widehat{\beta}(\alpha) = \left\{ \begin{array}{ll} 1 & \text{if } \widehat{\beta}(\beta) = \widehat{\beta}(\gamma) = 1 \\ 0/1 & \text{o/w.} \end{array} \right.$
A formula is valid (tautology) if it evaluates to \( T \) in all models.

\[ \neg \neg p \quad \neg \neg p \]

A formula is satisfiable if there is some model where it evaluates to \( T \).

\[ p \lor q \]

\[ p \land \neg p \] in not satisfable.
Thm: \( \alpha \) is valid

iff \( \neg \alpha \) is not satisfiable.

\[ \Rightarrow \] \( \alpha \) is valid

\[ \Leftarrow \] \( \alpha \) is true in all models

\[ \Rightarrow \] \( \neg \alpha \) is false in all models

\[ \Rightarrow \] \( \neg \alpha \) is not satisfiable

SAT: Check whether a given formula is satisfiable.
Relevance lemma: \( M, M' \)

If two models map the propositional occurring in a formula \( \Phi \) the same way

then \( M \models \Phi \) iff \( M' \models \Phi \).

**SAT problem:** Given \( \Phi \), is \( \Phi \) satisfiable?

**Decision procedure:** Check if \( M \models \Phi \)

in every model \( M \) ranging over the propositional occurring in \( \Phi \).

\[ 2^n \text{ models where } n = \text{AP}(\Phi) = O(141) \]
\[ \phi: (p \lor q) \lor \neg p \]

\[ p: T \quad q: 1 \]

\[ \phi \Rightarrow T \]

\[ p: \bot \quad q: 1 \]

\[ \phi \Rightarrow T \]

**NP**: Nondeterministic polynomial time.

**SAT** \& **NP**

**Cook's theorem**: SAT is NP-complete.
SAT solvers

Efficient-in-practice solvers for SAT.

Z3 @ MSR

P = NP

SAT ∈ P
Validity

\[ \phi \text{ is valid} \iff \neg \phi \text{ is not satisfiable} \]

A satisfiable is a validity as well.
Compactness theorem

Let \( X \subseteq \text{Formulas} \)

Then \( X \) is satisfiable iff every \( Y \subseteq \text{Formulas} \) with \( \forall x \in X \) is satisfiable.

Here, a set \( S \) of formulas is satisfiable if there is a model/value assignment \( M \) such that \( M \models \phi \) for any \( \phi \in S \).
If $X$ is not satisfiable, then there exists a finite subset $Y$ of $X$ such that $Y$ is not satisfiable.
König's lemma:

Any infinite finitely branching tree has an infinite path.

Proof:

$x_0, x_1, x_2, x_3, \ldots$
X is not set.

A node $v$ in $T$ is bad if $v(\beta) = 1$ for some $\beta \in X$. 

VCC-path $\Leftrightarrow$ valuation $\Rightarrow$ met subspace $X$. 

\( T \)
Goal today: The proof system we saw is complete for propositional logic.

\[ \vdash \alpha \quad \alpha \text{ is valid} \]

\[ \vdash_{ps} \alpha \quad \alpha \text{ is provable in the proof system } ps \]

\[ \vdash \neg \alpha \quad \neg \alpha \text{ is provable in the proof system } ps \]

\[ \vdash \alpha \iff \vdash \neg \alpha \]

\[ \Leftarrow \quad \text{easy (soundness)} \]

\[ \Rightarrow \quad \text{harder (completeness)} \]
I suppose \( \Gamma \alpha \)

If \( \Gamma \alpha \) is consistent, then \( \Gamma \alpha \) has a model

i.e. \( \Gamma \alpha \) is satisfiable.

Consistent \( \alpha \) is consistent if \( \Gamma \vdash \alpha \)

Thesis \( \alpha \) is a thesis if \( \Gamma \vdash \alpha \)

\( \alpha \) is consistent if \( \Gamma \vdash \alpha \) is not a theorem
\( \alpha \lor \beta \) is consistent iff either \( \alpha \) is consistent or \( \beta \) is consistent.

\[ \neg \bot \lor (\alpha \lor \beta) \]

\( \alpha \lor \beta \) is consistent then both \( \alpha \) and \( \beta \) are consistent.

Common does not hold.
Henkin's lemma

For all formulas \( \beta \), if \( \beta \) is consistent, then \( \beta \) is satisfiable.

Lemma \( \Rightarrow \) Completeness.

If \( \not\vdash \beta \), then \( \neg \beta \) is consistent \((\vdash \beta \iff \vdash \neg \neg \beta)\).

Then \( \neg \beta \) is satisfiable (by lemma).

Then \( \beta \) is not valid.
$\emptyset$ $X$ is a set of formulas

$X$ is finite: $X$ is consistent if $\forall \beta \beta \in X$ is consistent.

$X$ is infinite: $X$ is consistent if all finite subsets $\exists \{F \subseteq X \}$ are consistent.
If \( \beta, \alpha_0 \) is constant

\[ \beta, \alpha_0 \]

\[ \beta \]

\[ \beta \]

\[ \alpha_0 \]

\[ \alpha_0, \alpha_1, \alpha_2, \ldots \]

be an enumeration of the functions
Let $X$ be any finite consistent set $\{x_0, x_1, x_2, \ldots\}$.

\[ X_0 = X \]
\[ X_{i+1} = \begin{cases} x_i \cup \{d_i\} & \text{if } x_i \cup \{d_i\} \text{ is countable} \\ x_i & \text{otherwise} \end{cases} \]

\[ Y = \bigcup_{i \geq 0} X_i \]
Y is constant

Suppose Y is not constant
Then \( \exists Z \subseteq Y \) that is not constant

\[ Z = \{ x_{i_1}, x_{i_2}, \ldots, x_{i_n} \} \]

\[ Z \subseteq X_{int} \quad \text{and} \quad X_{int} \text{ is constant} \]

\( Z \) is constant \( \iff \chi_{-1}(x_{i_1}, \ldots, x_{i_n}) \)

\( Z \) is \( mon \iff X_{in} \text{ is invariant. — contradiction} \)
$Y$ is maximal.

$Y \cup \{x\}$ is not connected for any $x \notin Y$

$\alpha = \alpha_i$

$X_i \cup \{x_i\}$ was connected

So $X \cup \{x_i\}$ must be connected as well. $X_i$
Lindenbaum's lemma

Every connected set can be extended to a maximally connected set.
Maximal commutant sets (MCS). Let $X$ be an MCS.

- For any $\alpha$, $\alpha \in X$ iff $\alpha \notin X$
- For any $\alpha, \beta$, $\alpha \vee \beta \in X$ iff $\alpha \in X$ or $\beta \in X$
\[ X = \{ \beta \} \quad \rightarrow \quad Y: \text{MCS} \quad \rightarrow \quad \text{Valuation model that sat all formulas in } Y \quad \rightarrow \quad \beta \text{ is satisfiable.} \]

\[ Y \text{ is an MCS} \]

\[ \nu_Y(P) = T \quad \text{iiff} \quad P \in Y \]
Let \( Y \) be an MCS. Then \( \forall Y \vdash \alpha \) iff \( \alpha \in \mathcal{S} \).

Induction:

\[
\overline{\alpha = p, \; p \in \Phi, \; \forall Y \vdash p \; \text{iff} \; \exists p \in Y \; \text{(by def.)}}
\]

\[\alpha = \neg \beta, \; \forall Y \vdash \neg \beta \]

\[\text{iff} \; \forall Y \not\vdash \beta \; \text{(by ind. hypothesis)}\]

\[\text{iff} \; \beta \notin Y \; \text{(by property of MCS)}\]

\[\text{iff} \; \neg \beta \in Y \; \text{(by property of MCS)}\]
\[ \alpha = \beta \nu Y \]
\[ \nu Y = \beta \nu Y \]
iff \[ \nu Y = \beta \] or \[ \nu Y = Y \]
iff \[ \beta \leq Y \] or \[ Y \in Y \]
(by ind hypothesis).
iff \[ \beta \nu Y \preceq \exists Y \]
(by prop. of MCS)
\[ \square \]
If $\alpha$ is consistent,

So $\{\alpha\}$ can be extended to an MCS $Y$.

Then $\forall Y \beta Y \Rightarrow \alpha$ for every $\beta Y$.

So $\alpha$ is satisfiable.

So the proof system is complete.
How do we check \( \varphi \) is satisfiable?

1. Truth-table technique

For every valuation \( \nu : \mathcal{P}(v) \rightarrow \{T, F\} \)

check if \( \varphi \) is sat.

\[ \varphi \wedge s \wedge \neg s \]
\[ \psi \equiv \psi[p \rightarrow T] \lor \psi[p \rightarrow T] \]

\[ \text{in } \psi \text{ is sat } \quad \text{is sat} \]

Splitting method

\[ \text{SAT}(\psi) : \]

\[ \text{Let } p \text{ be in } \psi \]

If \( \psi = T \) return \( T \)

Else if \( \psi = T \) return \( T \)

Else if \( \text{SAT}(\psi[p \rightarrow T]) \) return true

Else if \( \text{not SAT}(\psi[p \rightarrow T]) \) return false

Else return \( \psi[p \rightarrow T] \)
Λ p \rightarrow p

\text{where: } p \text{ occurs "potentially" in } \Lambda
CNF
Conjunctive normal form.

\[ \varphi' \equiv C_1 \land C_2 \land \ldots \land C_n \]

\[ C_n \equiv \bigwedge \text{ } d_1 \lor d_2 \lor \ldots \lor d_i \]

\[ d_i : \ p \lor \neg p \ , \ p \in \mathcal{P} \]

\[ (\varphi \equiv \varphi') \text{ in } \text{CNF}^2 \]

\[ \text{DNF} : D_1 \lor D_2 \lor \ldots \lor D_n \]

\[ D_i : d_1 \land d_2 \land \ldots \land d_i \]

\[ d_i : p \lor \neg p \]
\( \varphi \mapsto \varphi' \text{ in } \text{CNF} \), \( \varphi \equiv \varphi' \)

but not necessarily with poly blowup

\( \varphi \mapsto \varphi' \text{ in } \text{CNF} \)

\( \varphi \) is sat iff \( \varphi' \) is sat

and \(|\varphi'| = \text{poly}(|\varphi|)\)
\( \Phi \mapsto \Phi' \quad \varnothing \equiv \varnothing' \)

Punishing negation in \&

used only de Morgan laws
\( C_1 \land C_2 \ldots \land C_n \land p \)

Clearly \( p \) must be true

\[ C_1[p \rightarrow T] \land C_2[p \rightarrow T] \ldots \land C_n[p \rightarrow T] \]

\[ C_1 \land \ldots \land C_n \quad p \text{ occurs purely in all claim} \]

\[ p \text{ occurs regularly in all claim} \]

\[ p \rightarrow \bot \]
Resolution \[ U \rightarrow \text{CNF} \]

\[ C_1 \land \ldots \land C_n \]

\[ C_i = \{d_1, \ldots, d_i\} \]

\[ C_1, \ldots, C_n \]
\[ c_1 \cup \cup_{i=2}^{n} p_i \cup p \cup \cdots \]

\[ \cdots \]

\[ q_1 v q_2 v \cdots v q_m \cup \tau_p \]

\[ \underline{\text{\textbf{c_3}}} \]

\[ \text{c_1} \land \text{c_2} \Rightarrow \text{c_3} \]

\[ C : \text{false if } C = \emptyset \]
\[
\begin{array}{c}
\{ p \} \\
\{ q \}
\end{array}
\]

\frac{\phi}{\phi}
\[ \emptyset \subseteq \{q\} \subseteq \{q, p\} \subseteq \{p\} \]
$F \emptyset$ is refutable iff $\emptyset \not \in F$ in unsatisfiable

$(\Rightarrow)$ Induction on $|\emptyset F|$

$(\Leftarrow) |\emptyset F| = 0$

You can't refute $F \emptyset = \emptyset$ and is satisfiable

$F = \{ \emptyset \}$ is not satisfiable.
\[ F = \{ C_1, \ldots, C_n \} \]

\[ R_p(F) = \{ \alpha \} \cup \{ \delta \} \cup \{ C \mid C \in F \text{ and } p \text{ does not occur in } C \} \]

\[ \cup \{ \alpha \cup \beta \mid \nu \in F \text{ and } \nu \cup \beta \notin F \} \]

Lemma: If \( F \) is unat then \( R_p(F) \) is also unat.

Let \( F \) be unat and let \( R_p(F) \) be sat.

Let \( T \) be an assignment/valuation satisfying \( R_p(F) \) (it does not mention \( p \)
\[ T_1 = T[ϕ \rightarrow 0] \quad T_2 = T[ϕ \rightarrow 1] \]

F is not a tree in \( T_1 \) and \( T_2 \).

There is a clone \( C_1 \) in \( F \) that has \( ϕ \).

There is a clone \( C_2 \) in \( F \) that has \( \neg ϕ \).

\[ p \land \alpha \quad 7p \lor \beta \quad \alpha \lor \beta \in R_p(F) \]