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

$\wedge$

Elec. engr.

Logician's view

Mathematician'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 $0, -1, 1, -2, 2, -3, 3, \ldots$

Suppose Σ is a finite alphabet.

Σ^* - set of finite strings over Σ

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

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

Σ^* is <u>countable</u>.

Fix $\mathcal{P}$, a countable set of propositions (or "propositional variables")

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

<u>Syntax of Prop logic</u>

Let WFF be the smallest set such that

- Every proposition $p \in \mathcal{P}$ is in WFF
- If φ and φ' are ~~but~~ in WFF, then $(\varphi \wedge \varphi')$, $(\varphi \vee \varphi')$, $(\neg \varphi)$ are also in WFF.

Grammar for WFF

$$\text{WFF} ::= p \mid (\varphi_1 \vee \varphi_2) \mid (\varphi_1 \wedge \varphi_2) \mid \neg \varphi_1$$

φ_1, φ_2 $\quad p \in \mathcal{P}$

Let $\mathcal{W}$ be the class of all sets that satisfies the properties

Let $W_0 = \bigcap \{ U \mid U \in \mathcal{W} \}$

W_0 satisfies the two properties and is the smallest.

$$WFF'_0 = P$$

wr

$$WFF'_{i+1} = WFF'_i \cup \{ (\varphi \wedge \varphi'), (\varphi \vee \varphi'), \neg \varphi \mid \varphi, \varphi' \in WFF'_i \}$$

$$WFF' = \bigcup_{\substack{n \geq 0 \\ n \in \mathbb{N}}} WFF'_n$$

U - any set satisfying the conditions

$WFF'_n \subseteq U$ for any n.

$$WFF_0' = \{ p_0, p_1, p_2 \ldots \}$$

$$WFF_1' = \{ p_0, p_1, \ldots \} \cup \{ (p_0 \wedge p_1), (p_5 \wedge p_6), (p_{11} \vee p_{13}) \ldots \}$$

$$WFF_2' = \{ \ldots \} \cup \{ \ldots \}$$

$$\cup \{ (p_0 \wedge p_1) \wedge (p_2 \wedge p_3), \ldots \}$$

All formulas in WFF have a property Q.

By <u>induction on n</u> that WFF_n' has property Q.

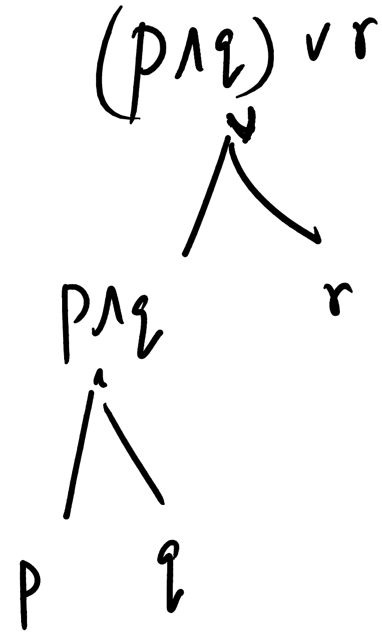
<u>Base case</u> : You show all propositions in P have property Q.

<u>Induction step</u>. Assume φ, φ' satisfy property Q.

Show $(\varphi \wedge \varphi')$, $(\varphi \vee \varphi')$, $\neg\varphi$ satisfy property Q

Parse tree

$(p \wedge q) \vee r$



Semantics

$(p \wedge q) \vee r$

Model : Think of this as a world that
or
Valuation   determines basic facts.

A valuation v is a function $v : \mathcal{P} \to \{\top, \bot\}$

Fix $v : P \to \{T, \bot\}$

Let $\hat{v} : \text{WFF} \to \{T, \bot\}$ defined as follows

- For every $p \in P$, $\hat{v}(p) = v(p)$
- For any $\alpha \in \text{WFF}$ of the form $\neg\beta$

$$\hat{v}(\alpha) = \begin{cases} T & \text{if } \hat{v}(\beta) = \bot \\ \bot & \text{if } \hat{v}(\beta) = T \end{cases}$$

- For any $\alpha \in \text{WFF}$ of the form $\beta \vee \gamma$

$$\hat{v}(\alpha) = \begin{cases} \bot & \text{if } \hat{v}(\beta) = \hat{v}(\gamma) = \bot \\ T & \text{o/w} \end{cases}$$

~~For~~

- For any $\alpha \in WFF$ of the form $\beta \wedge \gamma$

$$\hat{v}(\alpha) = \begin{cases} T & \text{if } \hat{v}(\beta) = \hat{v}(\gamma) = T \\ \perp & \text{o/w.} \end{cases}$$

A formula is valid (tautology)
if it evaluates to T in all models.

Eg $p \vee \neg p$

A formula is satisfiable
if there is some model where it evaluates to T

Eg. $p \wedge q$

$p \wedge \neg p$ is not satisfiable.

Thm α is valid

iff $\neg\alpha$ is <u>not</u> satisfiable.

$(\Rightarrow)$ α is valid

$\Leftrightarrow$ α is true in all models

$\Leftrightarrow$ $\neg\alpha$ is false in all models

$\Leftrightarrow$ $\neg\alpha$ is not satisfiable

$(\Leftarrow)$ $\neg\alpha$ is

SAT: Checking whether a given formula is satisfiable.

Relevance lemma M, M'

If two models, map the propositions occurring in a formula φ the same way then $M \models \varphi$ iff $M' \models \varphi$.

SAT problem : Given φ, is φ satisfiable?

Check if $M \models \varphi$ in every model M varying over the propositions occurring in φ.

Decision procedure

2^n models where $n = AP(\varphi)$
$= O(|\varphi|)$

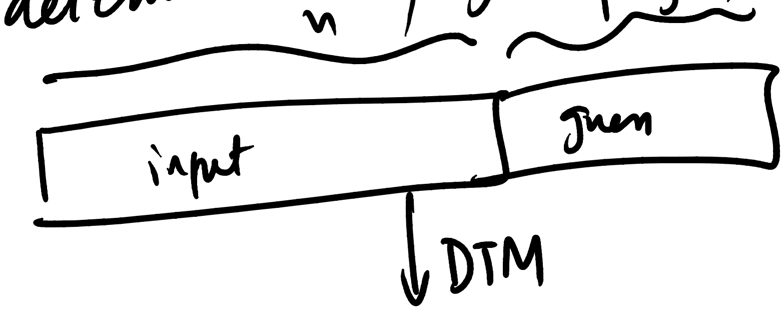
$\varphi : (p \wedge q) \vee \neg p$

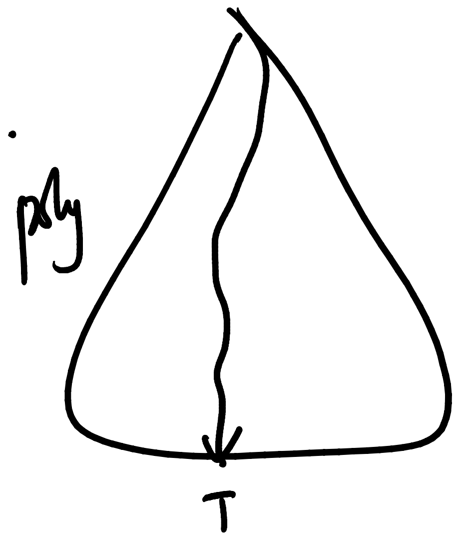
SAT: $O(2^n)$

$p : \top \quad q : \bot \qquad \varphi \mapsto \bot$

$p : \bot \quad q : \bot \qquad \varphi \mapsto \top$ ✓

NP: Nondeterministic polynomial time.





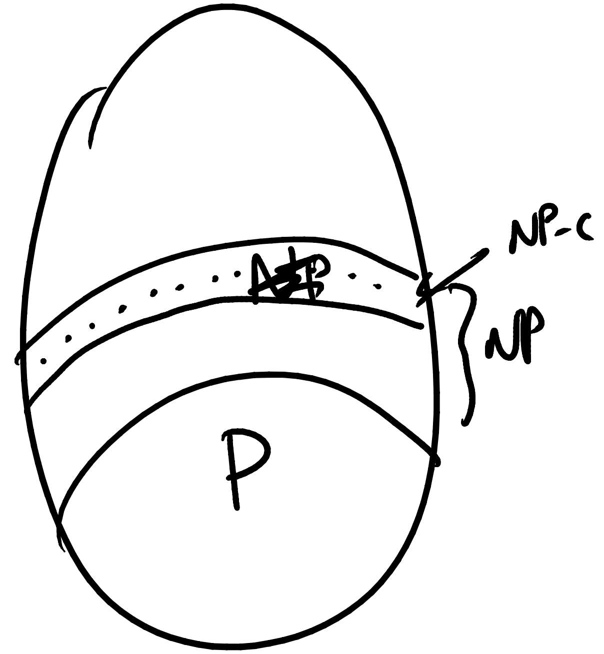
SAT $\in$ NP

Cook's theorem: SAT is NP-complete.

SAT solvers

Efficient-in-practice solvers for SAT.

Z3 @MSR



$$P \overset{?}{=} NP$$

$$\Updownarrow$$

$$SAT \in P$$

Validity

φ is ~~sat~~ valid

iff

$\neg\varphi$ is not ~~u~~ satisfiable

A SAT-solver is a validity solver as well.

Compactness theorem

Model-theoretic result

Let $X \subseteq$ Formulas

Then X is satisfiable iff every $Y \subseteq_{fin} X$ is satisfiable.

Here, a set S of formulas is satisfiable if there is a model/valuation M such that $M \models \varphi$ for any $\varphi \in S$.

$$X = \{ \underbrace{\underbrace{\underbrace{\underbrace{p \wedge q}_{M_1}, \; r \vee s}_{M_2}, \; p \vee r}_{M_3}, \; \dots \quad \dots}_{M} \}$$

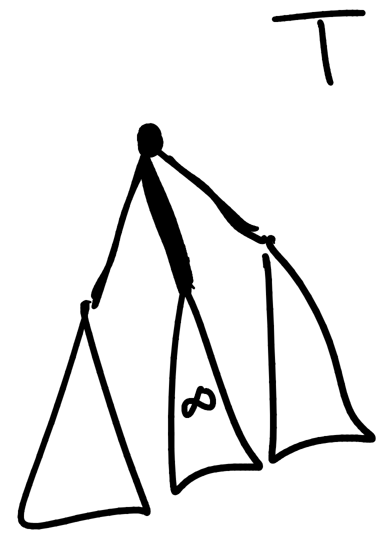
If X is <u>not</u> satisfiable then there exists a finite subset Y of X that is not satisfiable.

König's lemma :

Any infinite finitely-branching ~~branching~~ tree has an infinite path.

Proof

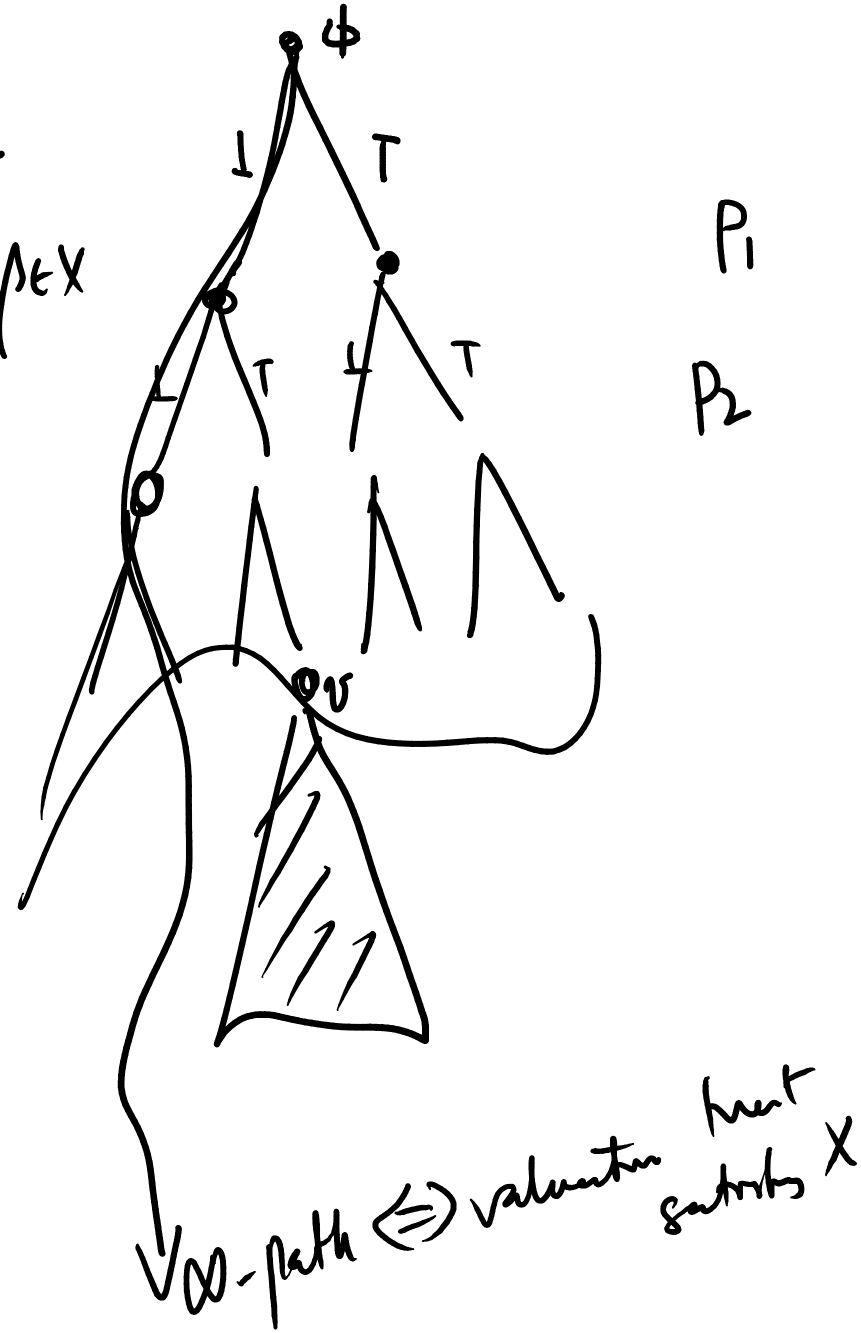
$x_0, x_1, x_2, x_3, \ldots$



X is not sat.

A node v in T is <u>bad</u>

if $v(\beta) = \bot$ for some $\beta \in X$



<u>Goal today</u>: The proof system we saw is <u>complete</u> for propositional logic.

$\models \alpha$ α is valid

$\vdash_{ps} \alpha$ α is provable in the proof system ps

$\vdash \alpha$

$\models \alpha$ iff $\vdash \alpha$

$\Leftarrow$ easy (soundness)

$\Rightarrow$ harder (completeness)

Suppose $\nvdash \alpha$

If $\vdash$ is complete then $\neg\alpha$ has a model

i.e. $\neg\alpha$ is satisfiable.

Consistent α is consistent if $\nvdash \neg\alpha$

α is a thesis if $\vdash \alpha$

Thesis

α is consistent if $\neg\alpha$ is not a thesis

$\alpha \vee \beta$ is consistent iff ~~either~~ α is consistent or β is consistent.

$$\Vert$$

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

$\nvdash \neg\alpha$ or $\nvdash \neg\beta$

$\alpha \wedge \beta$ is consistent then both α and β are consistent.

Converse does <u>not</u> hold.

Henkin's lemma

For all formulas β, if β is consistent then β is satisfiable.

Lemma $\Rightarrow$ Completeness. $(\vdash \beta$ iff $\vdash \neg\neg\beta)$

If $\nvdash \beta$, then $\neg\beta$ is consistent

then $\neg\beta$ is satisfiable (by lemma)

then β is not valid.

1. X is a set of formulas

X is finite: X is consistent if $\bigwedge_{\beta \in X} \beta$ is consistent.

X is infinite: X is consistent if all finite subsets $Y \subseteq_{fin} X$ are consistent.

Pf β is consistent

$\alpha_0, \alpha_1, \alpha_2 \ldots$ be an enumeration of the formulas

$$\{\beta\}$$

If $\{\beta, \alpha_0\}$ is consistent: $\{\beta, \alpha_0\}$

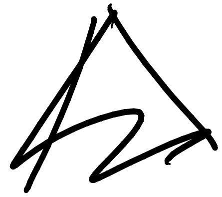
o/w α_0: $\{\beta\}$

$\vdots$

Let X be any finite consistent set.

$\alpha_0, \alpha_1, \alpha_2 \ldots$

X



$$X_0 = X$$

$$X_{i+1} = \begin{cases} X_i \cup \{\alpha_i\} & \text{if } X_i \cup \{\alpha_i\} \text{ is consistent} \\ X_i & \text{otherwise} \end{cases}$$

$$Y = \bigcup_{i \geq 0} X_i$$

Y is consistent.

Suppose Y is not consistent. Then $\exists Z \subseteq_{fin} Y$ that is not consistent.

$$Z = \{\alpha_{i_1}, \alpha_{i_2}, \ldots \alpha_{i_n}\}$$

$Z \subseteq X_{i_n+1}$ and X_{i_n+1} is consistent.

Z is inconsistent $\Leftrightarrow \vdash_T \neg(\alpha_{i_1} \wedge \ldots \alpha_{i_n})$

Z is incons $\Rightarrow$ X_{i_n} is inconsist. — contradiction

Y is maximal.

$Y \cup \{\alpha\}$ is not consistent for any $\alpha \notin Y$

$\alpha = \alpha_i$

$X_i \cup \{\alpha_i\}$ was inconsistent

So $Y \cup \{\alpha_i\}$ must be inconsistent as well.

$X_i \subseteq Y$

Lindenbaum's lemma

Every consistent set can be extended to a maximally consistent set.

Maximal consistent sets (MCS). Let X be an MCS.

- For any α, $\alpha \in X$ iff $\neg\alpha \notin X$
- For any α, β $\alpha \vee \beta \in X$ iff $\alpha \in X$ ~~or $\beta \in X$~~ or $\beta \in X$

$X = \{\beta\} \rightsquigarrow Y : MCS \rightsquigarrow$ Valuation/model that sat all formulas in Y!

$\rightsquigarrow \beta$ is satisfiable.

Y is an MCS

$V_Y(p) = T$ iff $p \in Y$

Let Υ be an MCS.

Then $v_\Upsilon \models \alpha$ iff $\alpha \in \Upsilon$.

Induction

- $\alpha = p$, $p \in P$, $v_\Upsilon \models p$ iff $p \in \Upsilon$ (by def.)

- $\alpha = \neg\beta$ $v_\Upsilon \models \neg\beta$

  iff $v_\Upsilon \not\models \beta$ (by ind. hypothesis)

  iff $\beta \notin \Upsilon$

  iff $\neg\beta \in \Upsilon$ (by property of MCS)

- $\alpha = \beta \vee \gamma$

$v_Y \models \beta \vee \gamma$ iff $v_Y \models \beta$ or $v_Y \models \gamma$

iff $\beta \in Y$ or $\gamma \in Y$ (by ind hypo).

iff $\beta \vee \gamma \in Y$ (by prop. of MCS)

$\square$

If α is consistent,

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

$v_Y \models \cancel{\alpha}\beta$ for every $\beta \in Y$

Hence $v_Y \models \alpha$

So α is satisfiable

So the proof system is complete.

How do we check φ is satisfiable?

- Truth-table technique

For every valuation $v : P(\varphi) \to \{\top, \bot\}$

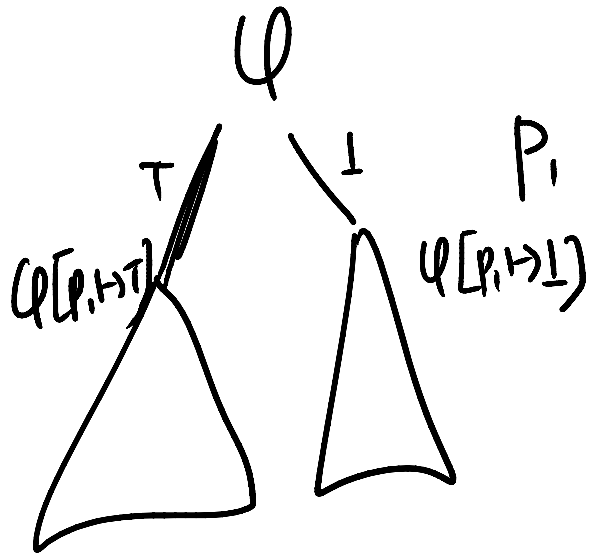
check if φ is sat.

$$\underline{\varphi \wedge S \wedge \neg S}$$

$\varphi \iff \varphi[p \mapsto \top] \vee \varphi[p \mapsto \bot]$

is sat iff is sat

Splitting method ~~[illegible]~~



SAT(φ):

~~Let p be in φ~~

If $\varphi = \top$ return $\top$

elif $\varphi = \bot$ return $\bot$

else if SAT($\varphi[p \mapsto \top]$)

ret true

else ~~ret~~

ret SAT($\varphi[p \mapsto \bot]$)

$\varphi \wedge p \longmapsto p$ must be true

~~φ~~ φ: p occurs "positively" in φ

CNF Conjunctive normal form.

$$\varphi \equiv C_1 \land C_2 \land \ldots C_n$$

$$C_n \equiv \cancel{\varphi}\ d_1 \lor d_2 \lor \ldots d_i$$

$$d_i : p \text{ or } \neg p \quad , p \in P$$

$$\varphi \rightsquigarrow \varphi' \text{ in CNF}$$

such that $\varphi \equiv \varphi'$

DNF : $D_1 \lor D_2 \ldots D_n$

$$D_i = d_1 \land d_2 \land \ldots d_i$$

$$d_i : p \text{ or } \neg p$$

$\varphi \rightsquigarrow \varphi'$ in CNF s.t. $\varphi \equiv \varphi'$

but <u>not</u> necessarily with poly blowup.

$\varphi \rightsquigarrow \varphi'$ in CNF

s.t. φ is sat iff φ' is sat

and $|\varphi'| = \mathrm{poly}(|\varphi|)$

$\varphi \rightsquigarrow \underset{\text{in CNF}}{\varphi'} \qquad \varphi \equiv \varphi'$

Pushing negation in &
~~used~~ using deMorgan laws

$$C_1 \wedge C_2 \ \ldots \ C_n \wedge p$$

Clearly p must be true

$$\frac{C_1[p \mapsto \top] \wedge C_2[p \mapsto \top] \wedge \ldots \wedge C_n[p \mapsto \top]}{C_1 \wedge \ldots \ C_n}$$

p occurs positively in all clauses

$p \mapsto \top$

p occurs negatively in all clauses

$p \mapsto \bot$

Resolution

$\varphi \rightarrow \text{CNF}$

$C_1 \wedge \dots \quad C_n \qquad \{C_1, \dots C_n\}$

$C_1 = \{d_1, \dots d_i\}$

$C_1 \dots \quad C_n$

$$\frac{\overset{C_1}{p_1 \vee p_2 \vee \ldots p_n \vee p \ldots} \qquad \overset{C_2}{q_1 \vee q_2 \vee \ldots q_m \vee \neg p}}{p_1 \vee p_2 \ldots \vee p_n \vee q_1 \vee q_2 \ldots q_m} \quad C_3$$

$$C_1 \wedge C_2 \Rightarrow C_3$$

C : false if $C = \phi$

$$\frac{\{p\} \qquad \{\neg p\}}{\emptyset}$$

$$\dfrac{\dfrac{\{p\} \qquad \{\neg p, q\}}{\{q\}} \qquad \{\neg q\}}{\emptyset}$$

$F|_\emptyset$ is refutable iff $\emptyset F$ is unsatisfiable

$(\Rightarrow)$ ✓ Induction on $|P(F|_\emptyset)|$

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

You can't refute

$F|_\emptyset = \emptyset$ and is satisfiable

$F = \{\emptyset\}$ is not satisfiable.

$$F = \{C_1, \dots C_n\}$$

$$R_p(F) = \cancel{\{\alpha \mid \alpha \in} \{C \mid C \in F \text{ and } p \text{ does not occur in } C\}$$

$$\cup \{\alpha \vee \beta \mid p \vee \alpha \in F \text{ and } \neg p \vee \beta \in F\}$$

<u>Lemma</u> If F is unsat then $R_p(F)$ is also unsat.

Let F be unsat and let $R_p(F)$ be sat.

τ be an assignment / valuation satisfying $R_p(F)$

(τ does not mention p)

$\tau_1 = \tau[p \mapsto 0]$ $\qquad$ $\tau_2 = \tau[p \mapsto 1]$

F is not ~~satisf~~ true in τ_1 and τ_2

There is a clause C_1 in F that has p

There is a clause C_2 in F that has $\neg p$

$p \vee \alpha$ $\qquad$ $\neg p \vee \beta$ $\qquad$ are in F

$\alpha \vee \beta \in R_p(F)$