The Calculus of Computation: Decision Procedures with Applications to Verification

by
Aaron Bradley
Zohar Manna

Springer 2007

Part I: FOUNDATIONS

1. Propositional Logic(PL)

Propositional Logic(PL)

PL Syntax

Atom	truth symbols $\top$("true") and $\bot$("false")
	propositional variables $P, Q, R, P_1, Q_1, R_1, \cdots$
Literal	atom α or its negation $\neg\alpha$
Formula	literal or application of a
	logical connective to formulae F, F_1, F_2

$\neg F$	"not"	(negation)
$F_1 \wedge F_2$	"and"	(conjunction)
$F_1 \vee F_2$	"or"	(disjunction)
$F_1 \rightarrow F_2$	"implies"	(implication)
$F_1 \leftrightarrow F_2$	"if and only if"	(iff)

Example:

formula $F : (P \land Q) \rightarrow (\top \lor \neg Q)$
atoms: $P, Q, \top$
literal: $\neg Q$
subformulas: $P \land Q, \quad \top \lor \neg Q$
abbreviation

$$F : P \land Q \rightarrow \top \lor \neg Q$$

PL Semantics (meaning)

$$\text{Sentence } F + \text{Interpretation } I = \begin{array}{l}\text{Truth value}\\ \text{(true, false)}\end{array}$$

Interpretation

$$I : \{P \mapsto \text{true}, Q \mapsto \text{false}, \cdots\}$$

Evaluation of F under I:

F	$\neg F$
0	1
1	0

where 0 corresponds to value false
1 true

F_1	F_2	$F_1 \wedge F_2$	$F_1 \vee F_2$	$F_1 \rightarrow F_2$	$F_1 \leftrightarrow F_2$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Example:

$F : P \land Q \rightarrow P \lor \neg Q$
$I : \{P \mapsto \text{true}, Q \mapsto \text{false}\}$

P	Q	$\neg Q$	$P \land Q$	$P \lor \neg Q$	F
1	0	1	0	1	1

$1 = \text{true}$ $\qquad$ $0 = \text{false}$

F evaluates to true under I

Inductive Definition of PL's Semantics

$$
\begin{array}{lll}
I \models F & \text{if } F \text{ evaluates to} & \text{true} \quad \text{under } I \\
I \not\models F & & \text{false}
\end{array}
$$

<u>Base Case</u>:

$$
\begin{array}{l}
I \models \top \\
I \not\models \bot
\end{array}
$$

$$
\begin{array}{lll}
I \models P & \text{iff} & I[P] = \text{true} \\
I \not\models P & \text{iff} & I[P] = \text{false}
\end{array}
$$

<u>Inductive Case</u>:

$$
\begin{array}{ll}
I \models \neg F & \text{iff } I \not\models F \\
I \models F_1 \wedge F_2 & \text{iff } I \models F_1 \text{ and } I \models F_2 \\
I \models F_1 \vee F_2 & \text{iff } I \models F_1 \text{ or } I \models F_2 \\
I \models F_1 \rightarrow F_2 & \text{iff, if } I \models F_1 \text{ then } I \models F_2 \\
I \models F_1 \leftrightarrow F_2 & \text{iff, } I \models F_1 \text{ and } I \models F_2, \\
 & \quad \text{or } I \not\models F_1 \text{ and } I \not\models F_2
\end{array}
$$

<u>Note</u>:

$$
I \not\models F_1 \rightarrow F_2 \quad \text{iff} \quad I \models F_1 \text{ and } I \not\models F_2
$$

Example:

$$F:\ P \land Q \rightarrow P \lor \neg Q$$

$$I:\ \{P \mapsto \text{true},\ Q \mapsto \text{false}\}$$

$$\begin{array}{lllll}
1. & I & \models & P & \text{since } I[P] = \text{true} \\
2. & I & \not\models & Q & \text{since } I[Q] = \text{false} \\
3. & I & \models & \neg Q & \text{by 2 and } \neg \\
4. & I & \not\models & P \land Q & \text{by 2 and } \land \\
5. & I & \models & P \lor \neg Q & \text{by 1 and } \lor \\
6. & I & \models & F & \text{by 4 and } \rightarrow \qquad \text{Why?}
\end{array}$$

Thus, F is true under I.

Satisfiability and Validity

F satisfiable iff there exists an interpretation I such that $I \models F$.
F valid iff for all interpretations I, $I \models F$.

$$\boxed{F \text{ is valid iff } \neg F \text{ is unsatisfiable}}$$

Method 1: Truth Tables

Example $\quad F : P \wedge Q \rightarrow P \vee \neg Q$

P	Q	$P \wedge Q$	$\neg Q$	$P \vee \neg Q$	F
0	0	0	1	1	1
0	1	0	0	0	1
1	0	0	1	1	1
1	1	1	0	1	1

Thus F is valid.

Example $F : P \lor Q \rightarrow P \land Q$

P	Q	$P \lor Q$	$P \land Q$	F	
0	0	0	0	1	$\leftarrow$ satisfying I
0	1	1	0	0	$\leftarrow$ falsifying I
1	0	1	0	0	
1	1	1	1	1	

Thus F is satisfiable, but invalid.

Method 2: Semantic Argument

Proof rules

$$\frac{I \models \neg F}{I \not\models F} \qquad\qquad \frac{I \not\models \neg F}{I \models F}$$

$$\frac{I \models F \wedge G}{\begin{array}{l} I \models F \\ I \models G \end{array}} \leftarrow\text{and} \qquad\qquad \frac{I \not\models F \wedge G}{I \not\models F \quad \mid \quad I \not\models G}$$

$\nwarrow$or

$$\frac{I \models F \vee G}{I \models F \quad \mid \quad I \models G} \qquad\qquad \frac{I \not\models F \vee G}{\begin{array}{l} I \not\models F \\ I \not\models G \end{array}}$$

$$\frac{I \models F \rightarrow G}{I \not\models F \quad \mid \quad I \models G} \qquad\qquad \frac{I \not\models F \rightarrow G}{\begin{array}{l} I \models F \\ I \not\models G \end{array}}$$

$$\frac{I \models F \leftrightarrow G}{I \models F \wedge G \quad \mid \quad I \not\models F \vee G} \qquad \frac{I \not\models F \leftrightarrow G}{I \models F \wedge \neg G \quad \mid \quad I \models \neg F \wedge G}$$

$$\frac{\begin{array}{l} I \models F \\ I \not\models F \end{array}}{I \models \bot}$$

Example 1: Prove

$$F : \; P \wedge Q \rightarrow P \vee \neg Q \quad \text{is valid.}$$

Let's assume that F is not valid and that I is a falsifying interpretation.

1.	I	$\not\models$	$P \wedge Q \rightarrow P \vee \neg Q$	assumption
2.	I	$\models$	$P \wedge Q$	1 and $\rightarrow$
3.	I	$\not\models$	$P \vee \neg Q$	1 and $\rightarrow$
4.	I	$\models$	P	2 and $\wedge$
5.	I	$\not\models$	P	3 and $\vee$
6.	I	$\models$	$\perp$	4 and 5 are contradictory

Thus F is valid.

Example 2: Prove

$$F : (P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R) \quad \text{is valid.}$$

Let's assume that F is not valid.

1.	I	$\not\models$	F	assumption
2.	I	$\models$	$(P \rightarrow Q) \wedge (Q \rightarrow R)$	1 and $\rightarrow$
3.	I	$\not\models$	$P \rightarrow R$	1 and $\rightarrow$
4.	I	$\models$	P	3 and $\rightarrow$
5.	I	$\not\models$	R	3 and $\rightarrow$
6.	I	$\models$	$P \rightarrow Q$	2 and of $\wedge$
7.	I	$\models$	$Q \rightarrow R$	2 and of $\wedge$

Two cases from 6

$$\begin{array}{lllll} 8a. & I & \not\models & P & \text{6 and } \rightarrow \\ 9a. & I & \models & \bot & \text{4 and 8a are contradictory} \end{array}$$

and

$$\begin{array}{lllll} 8b. & I & \models & Q & \text{6 and } \rightarrow \end{array}$$

Two cases from 7

$$\begin{array}{lllll} 9ba. & I & \not\models & Q & \text{7 and } \rightarrow \\ 10ba. & I & \models & \bot & \text{8b and 9ba are contradictory} \end{array}$$

and

$$\begin{array}{lllll} 9bb. & I & \models & R & \text{7 and } \rightarrow \\ 10bb. & I & \models & \bot & \text{5 and 9bb are contradictory} \end{array}$$

Our assumption is incorrect in all cases — F is valid.

Example 3: Is

$$F: \; P \vee Q \rightarrow P \wedge Q \quad \text{valid?}$$

Let's assume that F is not valid.

$$\begin{array}{llll l}
1. & I & \not\models & P \vee Q \rightarrow P \wedge Q & \text{assumption} \\
2. & I & \models & P \vee Q & \text{1 and } \rightarrow \\
3. & I & \not\models & P \wedge Q & \text{1 and } \rightarrow
\end{array}$$

Two options

$$\begin{array}{lllll lllll}
4a. & I & \models & P & \text{2 and } \vee & 4b. & I & \models & Q & \text{2 and } \vee \\
5a. & I & \not\models & Q & \text{3 and } \wedge & 5b. & I & \not\models & P & \text{3 and } \wedge
\end{array}$$

We cannot derive a contradiction. F is not valid.

Falsifying interpretation:

$I_1 : \{P \mapsto \text{true}, \; Q \mapsto \text{false}\}$ $\quad$ $I_2 : \{Q \mapsto \text{true}, \; P \mapsto \text{false}\}$

We have to derive a contradiction in both cases for F to be valid.

Equivalence

F_1 and F_2 are equivalent ($F_1 \Leftrightarrow F_2$)
iff for all interpretations I, $I \models F_1 \leftrightarrow F_2$

To prove $F_1 \Leftrightarrow F_2$ show $F_1 \leftrightarrow F_2$ is valid.

F_1 implies F_2 ($F_1 \Rightarrow F_2$)
iff for all interpretations I, $I \models F_1 \rightarrow F_2$

$F_1 \Leftrightarrow F_2$ and $F_1 \Rightarrow F_2$ are not formulae!

Normal Forms

1. <u>Negation Normal Form (NNF)</u>

   Negations appear only in literals. (only $\neg$, $\wedge$, $\vee$)

   To transform F to equivalent F' in NNF use recursively the following template equivalences (left-to-right):

$$\neg\neg F_1 \Leftrightarrow F_1 \qquad \neg\top \Leftrightarrow \bot \qquad \neg\bot \Leftrightarrow \top$$

$$\left.\begin{array}{l}\neg(F_1 \wedge F_2) \Leftrightarrow \neg F_1 \vee \neg F_2 \\ \neg(F_1 \vee F_2) \Leftrightarrow \neg F_1 \wedge \neg F_2\end{array}\right\}\text{De Morgan's Law}$$

$$F_1 \rightarrow F_2 \Leftrightarrow \neg F_1 \vee F_2$$

$$F_1 \leftrightarrow F_2 \Leftrightarrow (F_1 \rightarrow F_2) \wedge (F_2 \rightarrow F_1)$$

<u>Example</u>: Convert $F : \neg(P \rightarrow \neg(P \wedge Q))$ to NNF

$$\begin{array}{rll} F' : & \neg(\neg P \vee \neg(P \wedge Q)) & \rightarrow \text{ to } \vee \\ F'' : & \neg\neg P \wedge \neg\neg(P \wedge Q) & \text{De Morgan's Law} \\ F''' : & P \wedge P \wedge Q & \neg\neg \end{array}$$

F''' is equivalent to F ($F''' \Leftrightarrow F$) and is in NNF

2. Disjunctive Normal Form (DNF)

Disjunction of conjunctions of literals

$$\bigvee_i \bigwedge_j \ell_{i,j} \quad \text{for literals } \ell_{i,j}$$

To convert F into equivalent F' in DNF,
transform F into NNF and then
use the following template equivalences (left-to-right):

$$\left.\begin{array}{lcl} (F_1 \lor F_2) \land F_3 & \Leftrightarrow & (F_1 \land F_3) \lor (F_2 \land F_3) \\ F_1 \land (F_2 \lor F_3) & \Leftrightarrow & (F_1 \land F_2) \lor (F_1 \land F_3) \end{array}\right\} \mathit{dist}$$

Example: Convert

$$F : (Q_1 \lor \neg\neg Q_2) \land (\neg R_1 \rightarrow R_2) \text{ into DNF}$$

$$\begin{array}{rll} F' & : (Q_1 \lor Q_2) \land (R_1 \lor R_2) & \text{in NNF} \\ F'' & : (Q_1 \land (R_1 \lor R_2)) \lor (Q_2 \land (R_1 \lor R_2)) & \text{dist} \\ F''' & : (Q_1 \land R_1) \lor (Q_1 \land R_2) \lor (Q_2 \land R_1) \lor (Q_2 \land R_2) & \text{dist} \end{array}$$

F''' is equivalent to F ($F''' \Leftrightarrow F$) and is in DNF

3. Conjunctive Normal Form (CNF)

Conjunction of disjunctions of literals

$$\bigwedge_i \bigvee_j \ell_{i,j} \quad \text{for literals } \ell_{i,j}$$

To convert F into equivalent F' in CNF,
transform F into NNF and then
use the following template equivalences (left-to-right):

$$\begin{array}{rcl} (F_1 \land F_2) \lor F_3 & \Leftrightarrow & (F_1 \lor F_3) \land (F_2 \lor F_3) \\ F_1 \lor (F_2 \land F_3) & \Leftrightarrow & (F_1 \lor F_2) \land (F_1 \lor F_3) \end{array}$$

Davis-Putnam-Logemann-Loveland (DPLL) Algorithm

Decides the satisfiability of PL formulae in CNF

In book, efficient conversion of F to F' where

F' is in CNF and
F' and F are equisatisfiable (F is satisfiable iff F' is satisfiable)

Decision Procedure DPLL: Given F in CNF

$$
\begin{array}{l}
\texttt{let rec}\ \text{DPLL}\ F = \\
\quad \texttt{let}\ F' = \text{BCP}\ F\ \texttt{in} \\
\quad \texttt{if}\ F' = \top\ \texttt{then true} \\
\quad \texttt{else if}\ F' = \bot\ \texttt{then false} \\
\quad \texttt{else} \\
\qquad \texttt{let}\ P = \text{CHOOSE}\ \mathsf{vars}(F')\ \texttt{in} \\
\qquad (\text{DPLL}\ F'\{P \mapsto \top\})\ \lor\ (\text{DPLL}\ F'\{P \mapsto \bot\})
\end{array}
$$

Don't CHOOSE only-positive or only-negative variables for splitting.

Boolean Constraint Propagation (BCP)

Based on unit resolution

$$\frac{\ell \qquad C[\neg\ell]}{C[\bot]} \leftarrow \text{clause} \qquad \qquad \textit{where } \ell = P \textit{ or } \ell = \neg P$$

throughout

Example:

$$F:\ (\neg P \vee Q \vee R) \wedge (\neg Q \vee R) \wedge (\neg Q \vee \neg R) \wedge (P \vee \neg Q \vee \neg R)$$

Branching on Q

$$F\{Q \mapsto \top\}:\ (R) \ \wedge\ (\neg R) \ \wedge\ (P \ \vee\ \neg R)$$

By unit resolution

$$\frac{R \qquad (\neg R)}{\bot}$$

$$F\{Q \mapsto \top\} \ = \ \bot \ \Rightarrow \ \text{false}$$

On the other branch

$F\{Q \mapsto \bot\} : (\neg P \vee R)$

$F\{Q \mapsto \bot,\ R \mapsto \top,\ P \mapsto \bot\} = \top \Rightarrow \text{true}$

F is satisfiable with satisfying interpretation

$$I : \{P \mapsto \text{false},\ Q \mapsto \text{false},\ R \mapsto \text{true}\}$$