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 $F : (P \wedge Q) \rightarrow (\top \vee \neg Q)$
atoms: $P, Q, \top$
literal: $\neg Q$
subformulas: $P \wedge Q$, $\top \vee \neg Q$
abbreviation
$F : P \wedge Q \rightarrow \top \vee \neg Q$

PL Semantics (meaning)

Sentence F + Interpretation I = Truth value (true, false)

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:

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

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

1 = true 0 = false

F evaluates to true under I

Inductive Definition of PL's Semantics

$I \models F$ if F evaluates to true under I
$I \not\models F$ false

Base Case:

$I \models \top$
$I \not\models \bot$
$I \models P$ iff $I[P] = \text{true}$
$I \not\models P$ iff $I[P] = \text{false}$

Inductive Case:

$I \models \neg F$ iff $I \not\models F$
$I \models F_1 \wedge F_2$ iff $I \models F_1$ and $I \models F_2$
$I \models F_1 \vee F_2$ iff $I \models F_1$ or $I \models F_2$
$I \models F_1 \rightarrow F_2$ iff, if $I \models F_1$ then $I \models F_2$
$I \models F_1 \leftrightarrow F_2$ iff, $I \models F_1$ and $I \models F_2$, or $I \not\models F_1$ and $I \not\models F_2$

Note:

$I \not\models F_1 \rightarrow F_2$ iff $I \models F_1$ and $I \not\models F_2$

Example:

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

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

1. $I \models P$ since $I[P] = \text{true}$
2. $I \not\models Q$ since $I[Q] = \text{false}$
3. $I \models \neg Q$ by 2 and $\neg$
4. $I \not\models P \wedge Q$ by 2 and $\wedge$
5. $I \models P \vee \neg Q$ by 1 and $\vee$
6. $I \models F$ by 4 and $\rightarrow$ Why?

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, $I \models F$.

F is valid iff $\neg F$ is unsatisfiable

Method 1: Truth Tables

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

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 $F : P \vee Q \rightarrow P \wedge Q$

P	Q	$P \vee Q$	$P \wedge Q$	F	
0	0	0	0	1	← satisfying I
0	1	1	0	0	← falsifying I
1	0	1	0	0	
1	1	1	1	1	

Thus F is satisfiable, but invalid.

Method 2: Semantic Argument

Proof rules

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

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

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

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

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

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

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	$\models$	$\bot$	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

8a.	I	$\not\models$	P	6 and $\rightarrow$
9a.	I	$\models$	$\bot$	4 and 8a are contradictory

and

8b.	I	$\models$	Q	6 and $\rightarrow$

Two cases from 7

9ba.	I	$\not\models$	Q	7 and $\rightarrow$
10ba.	I	$\models$	$\bot$	8b and 9ba are contradictory

and

9bb.	I	$\models$	R	7 and $\rightarrow$
10bb.	I	$\models$	$\bot$	5 and 9bb are contradictory

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.

1.	I	$\not\models$	$P \vee Q \rightarrow P \wedge Q$	assumption
2.	I	$\models$	$P \vee Q$	1 and $\rightarrow$
3.	I	$\not\models$	$P \wedge Q$	1 and $\rightarrow$

Two options

4a.	I	$\models$	P	2 and $\vee$	4b.	I	$\models$	Q	2 and $\vee$
5a.	I	$\not\models$	Q	3 and $\wedge$	5b.	I	$\not\models$	P	3 and $\wedge$

We cannot derive a contradiction. F is not valid.

Falsifying interpretation:
$I_1: \{P \mapsto \text{true}, Q \mapsto \text{false}\}$ $I_2: \{Q \mapsto \text{true}, P \mapsto \text{false}\}$
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. Negation Normal Form (NNF)

   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):

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

Example: Convert $F : \neg(P \rightarrow \neg(P \wedge Q))$ to NNF

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

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):

   $$\left.\begin{array}{lcl}(F_1 \vee F_2) \wedge F_3 & \Leftrightarrow & (F_1 \wedge F_3) \vee (F_2 \wedge F_3) \\ F_1 \wedge (F_2 \vee F_3) & \Leftrightarrow & (F_1 \wedge F_2) \vee (F_1 \wedge F_3)\end{array}\right\} \textit{dist}$$

Example: Convert

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

$$\begin{array}{lll} F' : (Q_1 \vee Q_2) \wedge (R_1 \vee R_2) & & \text{in NNF} \\ F'' : (Q_1 \wedge (R_1 \vee R_2)) \vee (Q_2 \wedge (R_1 \vee R_2)) & & \text{dist} \\ F''' : (Q_1 \wedge R_1) \vee (Q_1 \wedge R_2) \vee (Q_2 \wedge R_1) \vee (Q_2 \wedge R_2) & & \text{dist} \end{array}$$

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):

   $$\begin{array}{lcl}(F_1 \wedge F_2) \vee F_3 & \Leftrightarrow & (F_1 \vee F_3) \wedge (F_2 \vee F_3) \\ F_1 \vee (F_2 \wedge F_3) & \Leftrightarrow & (F_1 \vee F_2) \wedge (F_1 \vee F_3)\end{array}$$

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

```
let rec DPLL F =
  let F' = BCP F in
  if F' = ⊤ then true
  else if F' = ⊥ then false
  else
     let P = CHOOSE vars(F') in
     (DPLL F'{P ↦ ⊤}) ∨ (DPLL F'{P ↦ ⊥})
```

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

Boolean Constraint Propagation (BCP)

Based on unit resolution

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

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

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

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

On the other branch

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

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

F is satisfiable with satisfying interpretation

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