Decision Procedures

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

Summer 2012

Organisation

Organisation

Dates

- Lecture is Tuesday 14–16 (c.t) and Thursday 14–15 (c.t).
- Tutorials will be given on Thursday 15–16.
  Starting next week (this week is a two hour lecture).
- Exercise sheets are uploaded on Tuesday.
  They are due on Tuesday the week after.

To successfully participate, you must

- prepare the exercises (at least 50 %)
- actively participate in the tutorial
- pass an oral examination

Literature

THE CALCULUS OF COMPUTATION:
Decision Procedures with
Applications to Verification

by
Aaron Bradley
Zohar Manna

Springer 2007

Motivation

Motivation

Decision Procedures are algorithms to decide formulae.

These formulae can arise

- in Hoare-style software verification.
- in hardware verification

Motivation (2)

Consider the following program:

```
for
   (int i := ℓ; i ≤ u; i := i + 1) {
   if ((a[i] = e))  {
      rv := true;
   }
}
```

Motivation (2)

Consider the following program:

```
for
  @ ℓ ≤ i ≤ u ∧ (rv ↔ ∃j. ℓ ≤ j < i ∧ a[j] = e)
  (int i := ℓ; i ≤ u; i := i + 1) {
  if ((a[i] = e))  {
    rv := true;
  }
}
```

Motivation (2)

Consider the following program:

```
for
  @ ℓ ≤ i ≤ u ∧ (rv ↔ ∃j. ℓ ≤ j < i ∧ a[j] = e)
  (int i := ℓ; i ≤ u; i := i + 1) {
  if ((a[i] = e)) {
    rv := true;
  }
}
```

How can we prove that the formula is a loop invariant?

Motivation (3)

Prove the Hoare triples (one for if case, one for else case)

$\texttt{assume}\ \ell \leq i \leq u \ \wedge\ (rv \ \leftrightarrow\ \exists j.\, \ell \leq j < i \ \wedge\ a[j] = e)$
$\texttt{assume}\ i \leq u$
$\texttt{assume}\ a[i] = e$
$rv := \texttt{true};$
$i := i + 1$
$\texttt{@}\ \ell \leq i \leq u \ \wedge\ (rv \ \leftrightarrow\ \exists j.\, \ell \leq j < i \ \wedge\ a[j] = e)$

$\texttt{assume}\ \ell \leq i \leq u \ \wedge\ (rv \ \leftrightarrow\ \exists j.\, \ell \leq j < i \ \wedge\ a[j] = e)$
$\texttt{assume}\ i \leq u$
$\texttt{assume}\ a[i] \neq e$
$i := i + 1$
$\texttt{@}\ \ell \leq i \leq u \ \wedge\ (rv \ \leftrightarrow\ \exists j.\, \ell \leq j < i \ \wedge\ a[j] = e)$

Motivation (4)

A Hoare triple {P} S {Q} holds, iff

$$P \rightarrow wp(S, Q)$$

(wp denotes is weakest precondition)

Motivation (4)

A Hoare triple {P} S {Q} holds, iff

$$P \;\rightarrow\; wp(S, Q)$$

(wp denotes is weakest precondition)
For assignments wp is computed by substitution:

$\texttt{assume}\ \ell \leq i \leq u \ \land\ (rv \ \leftrightarrow\ \exists j.\, \ell \leq j < i \ \land\ a[j] = e)$
$\texttt{assume}\ i \leq u$
$\texttt{assume}\ a[i] = e$
$rv := \texttt{true};$
$i := i + 1$
$@\ \ell \leq i \leq u \ \land\ (rv \ \leftrightarrow\ \exists j.\, \ell \leq j < i \ \land\ a[j] = e)$

---

holds if and only if:

$$\begin{aligned} &\ell \leq i \leq u \ \land\ (rv \ \leftrightarrow\ \exists j.\, \ell \leq j < i \ \land\ a[j] = e) \ \land\ i \leq u \ \land\ a[i] = e \\ \rightarrow\ &\ell \leq i+1 \leq u \ \land\ (\texttt{true} \ \leftrightarrow\ \exists j.\, \ell \leq j < i+1 \ \land\ a[j] = e) \end{aligned}$$

Motivation (5)

We need an algorithm that decides whether a formula holds.

$$\ell \leq i \leq u \ \wedge\ (rv \ \leftrightarrow\ \exists j.\, \ell \leq j < i \ \wedge\ a[j] = e) \ \wedge\ i \leq u \ \wedge\ a[i] = e$$
$$\rightarrow \ell \leq i+1 \leq u \ \wedge\ (\texttt{true} \ \leftrightarrow\ \exists j.\, \ell \leq j < i+1 \ \wedge\ a[j] = e)$$

Motivation (5)

We need an algorithm that decides whether a formula holds.

$$\ell \leq i \leq u \;\land\; (rv \;\leftrightarrow\; \exists j.\, \ell \leq j < i \;\land\; a[j] = e) \;\land\; i \leq u \;\land\; a[i] = e$$
$$\rightarrow \ell \leq i + 1 \leq u \;\land\; (\texttt{true} \;\leftrightarrow\; \exists j.\, \ell \leq j < i + 1 \;\land\; a[j] = e)$$

If the formula does not hold it should give a counterexample, e.g.:

$$\ell = 0, i = 1, u = 1, rv = \mathit{false}, a[0] = 0, a[1] = 1, e = 1,$$

Motivation (5)

We need an algorithm that decides whether a formula holds.

$$\ell \leq i \leq u \ \land \ (rv \ \leftrightarrow \ \exists j.\, \ell \leq j < i \ \land \ a[j] = e) \ \land \ i \leq u \ \land \ a[i] = e$$
$$\rightarrow \ell \leq i + 1 \leq u \ \land \ (\texttt{true} \ \leftrightarrow \ \exists j.\, \ell \leq j < i + 1 \ \land \ a[j] = e)$$

If the formula does not hold it should give a counterexample, e.g.:

$$\ell = 0, i = 1, u = 1, rv = \mathit{false}, a[0] = 0, a[1] = 1, e = 1,$$

This counterexample shows that $i + 1 \leq u$ can be violated.

Motivation (5)

We need an algorithm that decides whether a formula holds.

$$\ell \leq i \leq u \;\wedge\; (rv \;\leftrightarrow\; \exists j.\, \ell \leq j < i \;\wedge\; a[j] = e) \;\wedge\; i \leq u \;\wedge\; a[i] = e$$
$$\rightarrow \ell \leq i+1 \leq u \;\wedge\; (\texttt{true} \;\leftrightarrow\; \exists j.\, \ell \leq j < i+1 \;\wedge\; a[j] = e)$$

If the formula does not hold it should give a counterexample, e.g.:

$$\ell = 0, i = 1, u = 1, rv = \mathit{false}, a[0] = 0, a[1] = 1, e = 1,$$

This counterexample shows that $i + 1 \leq u$ can be violated.

This lecture is about algorithms checking for validity and producing these counterexamples.

Contents of Lecture

Topics

- Propositional Logic
- First-Order Logic
- First-Order Theories
- Quantifier Elimination
- Decision Procedures for Linear Arithmetic
- Decision Procedures for Uninterpreted Functions
- Decision Procedures for Arrays
- Combination of Decision Procedures
- DPLL(T)
- Craig Interpolants

Foundations: Propositional Logic

Syntax of Propositional Logic

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: Syntax

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

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

Formula F and Interpretation I is evaluated to a truth value 0/1
where 0 corresponds to value false
1 true

Interpretation $I : \{P \mapsto 1, Q \mapsto 0, \cdots\}$

Evaluation of logical operators:

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

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

$I : \{P \mapsto 1, Q \mapsto 0\}$

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

1 = true 0 = false

Example: Semantics

$F : P \wedge Q \rightarrow P \vee \neg Q$
$I : \{P \mapsto 1, Q \mapsto 0\}$

P	Q	$\neg Q$	$P \wedge Q$	$P \vee \neg Q$	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

$$\begin{array}{lllll} I & \models & F & \text{if } F \text{ evaluates to} & 1 \;/\; \text{true} & \text{under } I \\ I & \not\models & F & & 0 \;/\; \text{false} & \end{array}$$

Inductive Definition of PL's Semantics

$$
\begin{array}{llll}
I \models F & \text{if } F \text{ evaluates to} & 1 \;/\; \text{true} & \text{under } I \\
I \not\models F & & 0 \;/\; \text{false} &
\end{array}
$$

Base Case:

$$
\begin{array}{lll}
I \models \top & & \\
I \not\models \bot & & \\
I \models P & \text{iff} & I[P] = 1 \\
I \not\models P & \text{iff} & I[P] = 0
\end{array}
$$

Inductive Definition of PL's Semantics

$I \models F$ if F evaluates to 1 / true under I
$I \not\models F$ 0 / false

Base Case:

$I \models \top$
$I \not\models \bot$

$I \models P$ iff $I[P] = 1$
$I \not\models P$ iff $I[P] = 0$

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 $I \not\models F_2$

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

$$I : \{P \mapsto 1,\ Q \mapsto 0\}$$

$I \models P \quad I \not\models Q \quad I \models \neg Q$

$I \not\models P \land Q \quad I \models P \lor \neg Q$

$I \models P \land Q \rightarrow P \lor \neg Q$

Example: Inductive Reasoning

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

$$I: \{P \mapsto 1,\ Q \mapsto 0\}$$

1. $I \models P$ since $I[P] = 1$

Example: Inductive Reasoning

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

$$I : \{P \mapsto 1, Q \mapsto 0\}$$

1. $I \models P$ since $I[P] = 1$
2. $I \not\models Q$ since $I[Q] = 0$

Example: Inductive Reasoning

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

$$I: \; \{P \mapsto 1, \; Q \mapsto 0\}$$

1.	I	$\models$	P	since $I[P] = 1$
2.	I	$\not\models$	Q	since $I[Q] = 0$
3.	I	$\models$	$\neg Q$	by 2, $\neg$

Example: Inductive Reasoning

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

$$I : \{P \mapsto 1, Q \mapsto 0\}$$

1.	I	$\models$	P	since $I[P] = 1$
2.	I	$\not\models$	Q	since $I[Q] = 0$
3.	I	$\models$	$\neg Q$	by 2, $\neg$
4.	I	$\not\models$	$P \land Q$	by 2, $\land$

Example: Inductive Reasoning

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

$$I : \{P \mapsto 1, Q \mapsto 0\}$$

1.	I	$\models$	P	since $I[P] = 1$
2.	I	$\not\models$	Q	since $I[Q] = 0$
3.	I	$\models$	$\neg Q$	by 2, $\neg$
4.	I	$\not\models$	$P \land Q$	by 2, $\land$
5.	I	$\models$	$P \lor \neg Q$	by 1, $\lor$

Example: Inductive Reasoning

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

$$I: \; \{P \mapsto 1, \; Q \mapsto 0\}$$

1.	$I \models$	P	since $I[P] = 1$	
2.	$I \not\models$	Q	since $I[Q] = 0$	
3.	$I \models$	$\neg Q$	by 2, $\neg$	
4.	$I \not\models$	$P \land Q$	by 2, $\land$	
5.	$I \models$	$P \lor \neg Q$	by 1, $\lor$	
6.	$I \models$	F	by 4, $\rightarrow$	Why?

Example: Inductive Reasoning

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

$$I : \; \{P \mapsto 1, \; Q \mapsto 0\}$$

1.	I	$\models$	P	since $I[P] = 1$
2.	I	$\not\models$	Q	since $I[Q] = 0$
3.	I	$\models$	$\neg Q$	by 2, $\neg$
4.	I	$\not\models$	$P \wedge Q$	by 2, $\wedge$
5.	I	$\models$	$P \vee \neg Q$	by 1, $\vee$
6.	I	$\models$	F	by 4, $\rightarrow$ Why?

Thus, F is true under I.

Satisfiability and Validity

UNI FREIBURG

Definition (Satisfiability)

F is satisfiable iff there exists an interpretation I such that $I \models F$.

Definition (Validity)

F is valid iff for all interpretations I, $I \models F$.

F valid implies F satisfiable

F satisfiable iff $\exists I : I \models F$

iff $\neg \forall I : \neg (I \models F)$

iff $\neg \forall I : I \models \neg F$

iff $(\neg F)$ is not valid

Definition (Satisfiability)

F is satisfiable iff there exists an interpretation I such that $I \models F$.

Definition (Validity)

F is valid iff for all interpretations I, $I \models F$.

Note

F is valid iff $\neg F$ is unsatisfiable

Satisfiability and Validity

Definition (Satisfiability)

F is satisfiable iff there exists an interpretation I such that $I \models F$.

Definition (Validity)

F is valid iff for all interpretations I, $I \models F$.

Note

F is valid iff $\neg F$ is unsatisfiable

Decision Procedure: An algorithm for deciding validity or satisfiability.

Examples: Satisfiability and Validity

Now assume, you are a decision procedure.

Which of the following formulae is satisfiable, which is valid?

- $F_1 : P \wedge Q$
- $F_2 : \neg(P \wedge Q)$
- $F_3 : P \vee \neg P$
- $F_4 : \neg(P \vee \neg P)$
- $F_5 : (P \rightarrow Q) \wedge (P \vee Q) \wedge \neg Q$

Examples: Satisfiability and Validity

Now assume, you are a decision procedure.

Which of the following formulae is satisfiable, which is valid?

- $F_1 : P \wedge Q$
  satisfiable, not valid

  $I_1 := \{P \to 1, Q \to 1\}$. $I_1 \models F_1$

  $I_2 := \{P \to 0, Q \to 1\}$ $I_2 \not\models F_1$
- $F_2 : \neg(P \wedge Q)$
- $F_3 : P \vee \neg P$
- $F_4 : \neg(P \vee \neg P)$
- $F_5 : (P \to Q) \wedge (P \vee Q) \wedge \neg Q$

Examples: Satisfiability and Validity

Now assume, you are a decision procedure.

Which of the following formulae is satisfiable, which is valid?

- $F_1 : P \land Q$
  satisfiable, not valid
- $F_2 : \neg(P \land Q)$
  satisfiable, not valid
- $F_3 : P \lor \neg P$
- $F_4 : \neg(P \lor \neg P)$
- $F_5 : (P \to Q) \land (P \lor Q) \land \neg Q$

Examples: Satisfiability and Validity

Now assume, you are a decision procedure.

Which of the following formulae is satisfiable, which is valid?

- $F_1 : P \wedge Q$
  satisfiable, not valid
- $F_2 : \neg(P \wedge Q)$
  satisfiable, not valid
- $F_3 : P \vee \neg P$
  satisfiable, valid
- $F_4 : \neg(P \vee \neg P)$
- $F_5 : (P \rightarrow Q) \wedge (P \vee Q) \wedge \neg Q$

Examples: Satisfiability and Validity

Now assume, you are a decision procedure.

Which of the following formulae is satisfiable, which is valid?

- $F_1 : P \land Q$
  satisfiable, not valid
- $F_2 : \neg(P \land Q)$
  satisfiable, not valid
- $F_3 : P \lor \neg P$
  satisfiable, valid
- $F_4 : \neg(P \lor \neg P)$
  unsatisfiable, not valid
- $F_5 : (P \to Q) \land (P \lor Q) \land \neg Q$

Examples: Satisfiability and Validity

Now assume, you are a decision procedure.

Which of the following formulae is satisfiable, which is valid?

- $F_1 : P \land Q$
  satisfiable, not valid
- $F_2 : \neg(P \land Q)$
  satisfiable, not valid
- $F_3 : P \lor \neg P$
  satisfiable, valid
- $F_4 : \neg(P \lor \neg P)$
  unsatisfiable, not valid
- $F_5 : (P \rightarrow Q) \land (P \lor Q) \land \neg Q$
  unsatisfiable, not valid

Examples: Satisfiability and Validity

Now assume, you are a decision procedure.

Which of the following formulae is satisfiable, which is valid?

- $F_1 : P \land Q$
  satisfiable, not valid
- $F_2 : \neg(P \land Q)$
  satisfiable, not valid
- $F_3 : P \lor \neg P$
  satisfiable, valid
- $F_4 : \neg(P \lor \neg P)$
  unsatisfiable, not valid
- $F_5 : (P \rightarrow Q) \land (P \lor Q) \land \neg Q$
  unsatisfiable, not valid

Is there a formula that is unsatisfiable and valid?

Method 1: Truth Tables

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

P Q	$P \land Q$	$\neg Q$	$P \lor \neg Q$	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

Method 1: Truth Tables

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

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.

Method 1: Truth Tables

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

P	Q	$P \land Q$	$\neg Q$	$P \lor \neg Q$	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.

$F : P \lor Q \to P \land Q$

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

Method 1: Truth Tables

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

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.

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

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 (Semantic Tableaux)

- Assume F is not valid and I a falsifying interpretation: $I \not\models F$
- Apply proof rules.
- If no contradiction reached and no more rules applicable, F is invalid.
- If in every branch of proof a contradiction reached, F is valid.

Semantic Argument: Proof rules

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

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

$\nwarrow$ 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

Prove $F: P \land Q \rightarrow P \lor \neg Q$ is valid.

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

1. $I \not\models P \land Q \rightarrow P \lor \neg Q$	
2. $I \models P \land Q$	1. $\rightarrow$
3. $I \not\models P \lor \neg Q$	1. $\rightarrow$
4. $I \models P$	2. $\land$
5. $I \models Q$	2. $\land$
6. $I \not\models P$	3. $\lor$
7. $I \not\models \neg Q$	3. $\lor$
8. $I \models \bot$	4. 6. contradict

Example

Prove $F : P \land Q \rightarrow P \lor \neg Q$ is valid.

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

1. $I \not\models P \land Q \rightarrow P \lor \neg Q$ assumption

Example

Prove $F : P \land Q \rightarrow P \lor \neg Q$ is valid.

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

1.	I	$\not\models$	$P \land Q \rightarrow P \lor \neg Q$	assumption
2.	I	$\models$	$P \land Q$	1, Rule $\rightarrow$
3.	I	$\not\models$	$P \lor \neg Q$	1, Rule $\rightarrow$

Example

Prove $F: P \wedge Q \rightarrow P \vee \neg Q$ 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, Rule $\rightarrow$
3.	I	$\not\models$	$P \vee \neg Q$	1, Rule $\rightarrow$
4.	I	$\models$	P	2, Rule $\wedge$

Example

Prove $F: P \land Q \rightarrow P \lor \neg Q$ is valid.

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

1.	I	$\not\models$	$P \land Q \rightarrow P \lor \neg Q$	assumption
2.	I	$\models$	$P \land Q$	1, Rule $\rightarrow$
3.	I	$\not\models$	$P \lor \neg Q$	1, Rule $\rightarrow$
4.	I	$\models$	P	2, Rule $\land$
5.	I	$\not\models$	P	3, Rule $\lor$

Example

Prove $F : P \wedge Q \rightarrow P \vee \neg Q$ 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, Rule $\rightarrow$
3.	I	$\not\models$	$P \vee \neg Q$	1, Rule $\rightarrow$
4.	I	$\models$	P	2, Rule $\wedge$
5.	I	$\not\models$	P	3, Rule $\vee$
6.	I	$\models$	$\bot$	4 and 5 are contradictory

Example

Prove $F: P \wedge Q \rightarrow P \vee \neg Q$ 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, Rule $\rightarrow$
3.	I	$\not\models$	$P \vee \neg Q$	1, Rule $\rightarrow$
4.	I	$\models$	P	2, Rule $\wedge$
5.	I	$\not\models$	P	3, Rule $\vee$
6.	I	$\models$	$\perp$	4 and 5 are contradictory

Thus F is valid.

Example 2

Prove $F : (P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$ is valid.

Let's assume that F is not valid.

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

8a. $I \not\models P$ | 8b. $I \models Q$ — 6. $\rightarrow$

9a. $I \models \bot$ — 4, 8a | 9ba. $I \not\models Q$ | 9bb. $I \models R$ — 7. $\rightarrow$

$I \models \bot$ — 8b, 9ba | $I \models \bot$ — 5, 9bb

Example 2

Prove $F: (P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$ is valid.

Let's assume that F is not valid.

1. $I \not\models F$ assumption

Example 2

Prove $F : (P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$ 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, Rule $\rightarrow$
3.	I	$\not\models$	$P \rightarrow R$	1, Rule $\rightarrow$

Example 2

Prove $F: (P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$ 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, Rule $\rightarrow$
3.	I	$\not\models$	$P \rightarrow R$	1, Rule $\rightarrow$
4.	I	$\models$	P	3, Rule $\rightarrow$
5.	I	$\not\models$	R	3, Rule $\rightarrow$

Example 2

Prove $F: (P \rightarrow Q) \land (Q \rightarrow R) \rightarrow (P \rightarrow R)$ is valid.

Let's assume that F is not valid.

1.	I	$\not\models$	F	assumption
2.	I	$\models$	$(P \rightarrow Q) \land (Q \rightarrow R)$	1, Rule $\rightarrow$
3.	I	$\not\models$	$P \rightarrow R$	1, Rule $\rightarrow$
4.	I	$\models$	P	3, Rule $\rightarrow$
5.	I	$\not\models$	R	3, Rule $\rightarrow$
6.	I	$\models$	$P \rightarrow Q$	2, Rule $\land$
7.	I	$\models$	$Q \rightarrow R$	2, Rule $\land$

Example 2

Prove $F : (P \rightarrow Q) \land (Q \rightarrow R) \rightarrow (P \rightarrow R)$ is valid.

Let's assume that F is not valid.

1.	I	$\not\models$	F	assumption
2.	I	$\models$	$(P \rightarrow Q) \land (Q \rightarrow R)$	1, Rule $\rightarrow$
3.	I	$\not\models$	$P \rightarrow R$	1, Rule $\rightarrow$
4.	I	$\models$	P	3, Rule $\rightarrow$
5.	I	$\not\models$	R	3, Rule $\rightarrow$
6.	I	$\models$	$P \rightarrow Q$	2, Rule $\land$
7.	I	$\models$	$Q \rightarrow R$	2, Rule $\land$

$8a.\ I \not\models P$ | $8b.\ I \models Q$ $6 \rightarrow$

Example 2

Prove $F : (P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$ 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, Rule $\rightarrow$
3.	I	$\not\models$	$P \rightarrow R$	1, Rule $\rightarrow$
4.	I	$\models$	P	3, Rule $\rightarrow$
5.	I	$\not\models$	R	3, Rule $\rightarrow$
6.	I	$\models$	$P \rightarrow Q$	2, Rule $\wedge$
7.	I	$\models$	$Q \rightarrow R$	2, Rule $\wedge$

$8a.$	I	$\not\models$	P	$8b.$	I	$\models$	Q	$6 \rightarrow$
$9a.$	I	$\models$	$\perp$					

Example 2

Prove $F: (P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$ 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, Rule $\rightarrow$
3.	I	$\not\models$	$P \rightarrow R$	1, Rule $\rightarrow$
4.	I	$\models$	P	3, Rule $\rightarrow$
5.	I	$\not\models$	R	3, Rule $\rightarrow$
6.	I	$\models$	$P \rightarrow Q$	2, Rule $\wedge$
7.	I	$\models$	$Q \rightarrow R$	2, Rule $\wedge$

Branch a	Branch b	
$8a.\ I \not\models P$	$8b.\ I \models Q$ $6 \rightarrow$	
$9a.\ I \models \bot$	$9ba.\ I \not\models Q$	$9bb.\ I \models R$

Example 2

Prove $F : (P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$ 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, Rule $\rightarrow$
3.	I	$\not\models$	$P \rightarrow R$	1, Rule $\rightarrow$
4.	I	$\models$	P	3, Rule $\rightarrow$
5.	I	$\not\models$	R	3, Rule $\rightarrow$
6.	I	$\models$	$P \rightarrow Q$	2, Rule $\wedge$
7.	I	$\models$	$Q \rightarrow R$	2, Rule $\wedge$

8a. $I \not\models P$	8b. $I \models Q$ 6 $\rightarrow$	
9a. $I \models \bot$	9ba. $I \not\models Q$	9bb. $I \models R$
	10ba. $I \models \bot$	

Prove $F : (P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$ 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, Rule $\rightarrow$
3.	I	$\not\models$	$P \rightarrow R$	1, Rule $\rightarrow$
4.	I	$\models$	P	3, Rule $\rightarrow$
5.	I	$\not\models$	R	3, Rule $\rightarrow$
6.	I	$\models$	$P \rightarrow Q$	2, Rule $\wedge$
7.	I	$\models$	$Q \rightarrow R$	2, Rule $\wedge$

$8a.\ I \not\models P$ | $8b.\ I \models Q \quad 6 \rightarrow$

$9a.\ I \models \bot$

$9ba.\ I \not\models Q$ | $9bb.\ I \models R$

$10ba.\ I \models \bot$ | $10bb.\ I \models \bot$

Prove $F: (P \to Q) \land (Q \to R) \to (P \to R)$ is valid.

Let's assume that F is not valid.

1.	I	$\not\models$	F	assumption
2.	I	$\models$	$(P \to Q) \land (Q \to R)$	1, Rule $\to$
3.	I	$\not\models$	$P \to R$	1, Rule $\to$
4.	I	$\models$	P	3, Rule $\to$
5.	I	$\not\models$	R	3, Rule $\to$
6.	I	$\models$	$P \to Q$	2, Rule $\land$
7.	I	$\models$	$Q \to R$	2, Rule $\land$

$8a.\quad I \not\models P$
$9a.\quad I \models \bot$

$8b.\quad I \models Q \quad 6 \to$

$9ba.\quad I \not\models Q$
$10ba.\quad I \models \bot$

$9bb.\quad I \models R$
$10bb.\quad I \models \bot$

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

Example 3

Is $F: P \lor Q \to P \land Q$ valid?

Let's assume that F is not valid.

1. $I \not\models P \lor Q \to P \land Q$
2. $I \models P \lor Q$ — 1. $\to$
3. $I \not\models P \land Q$ — 1 $\to$

4.a $I \models P$ | 4.b $I \models Q$ — 2, $\lor$

5aa. $I \not\models P$, $I \models \bot$ | $I \not\models Q$ ↑ open | 5ba. $I \not\models P$ ↑ open | $I \not\models Q$, $I \models \bot$ — 3, $\land$

Example 3

Is $F : P \lor Q \rightarrow P \land Q$ valid?

Let's assume that F is not valid.

1. $I \not\models P \lor Q \rightarrow P \land Q$ assumption

Example 3

Is $F: P \lor Q \to P \land Q$ valid?

Let's assume that F is not valid.

1.	I	$\not\models$	$P \lor Q \to P \land Q$	assumption
2.	I	$\models$	$P \lor Q$	1 and $\to$
3.	I	$\not\models$	$P \land Q$	1 and $\to$

Example 3

Is $F : P \lor Q \to P \land Q$ valid?

Let's assume that F is not valid.

$$\begin{array}{llll} 1. & I & \not\models & P \lor Q \to P \land Q & \text{assumption} \\ 2. & I & \models & P \lor Q & \text{1 and } \to \\ 3. & I & \not\models & P \land Q & \text{1 and } \to \end{array}$$

$$4a. \quad I \models P \qquad \text{2 and } \lor$$

Example 3

Is $F: P \vee Q \rightarrow P \wedge Q$ valid?

Let's assume that F is not valid.

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

$$
\begin{array}{ll|l}
4a. & I \models P \quad 2 \text{ and } \vee & \\
5aa. & I \not\models P & 5ab. \; I \not\models Q \\
6aa. & I \models \bot &
\end{array}
$$

Example 3

Is $\quad F: P \lor Q \to P \land Q \quad$ valid?

Let's assume that F is not valid.

1.	I	$\not\models$	$P \lor Q \to P \land Q$	assumption
2.	I	$\models$	$P \lor Q$	1 and $\to$
3.	I	$\not\models$	$P \land Q$	1 and $\to$

Branch a	Branch b
$4a.\ I \models P$ — 2 and $\lor$	$4b.\ I \models Q$ — 2 and $\lor$
$5aa.\ I \not\models P$ | $5ab.\ I \not\models Q$	
$6aa.\ I \models \bot$	

Example 3

Is $F: P \lor Q \to P \land Q$ valid?

Let's assume that F is not valid.

$$\begin{array}{llll}
1. & I & \not\models & P \lor Q \to P \land Q & \text{assumption} \\
2. & I & \models & P \lor Q & 1 \text{ and } \to \\
3. & I & \not\models & P \land Q & 1 \text{ and } \to
\end{array}$$

$$\begin{array}{l|l}
4a.\ I \models P \quad 2 \text{ and } \lor & 4b.\ I \models Q \quad 2 \text{ and } \lor \\
\begin{array}{l|l} 5aa.\ I \not\models P & 5ab.\ I \not\models Q \\ 6aa.\ I \models \bot & \end{array} & \begin{array}{l|l} 5ba.\ I \not\models P & 5bb.\ I \not\models Q \\ & 6bb.\ I \models \bot \end{array}
\end{array}$$

Example 3

Is $\quad F: P \lor Q \rightarrow P \land Q \quad$ valid?

Let's assume that F is not valid.

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

$$
\begin{array}{l|l}
4a. \; I \models P \quad \text{2 and } \lor & 4b. \; I \models Q \quad \text{2 and } \lor \\
\begin{array}{l|l} 5aa. \; I \not\models P & 5ab. \; I \not\models Q \\ 6aa. \; I \models \bot & \end{array} &
\begin{array}{l|l} 5ba. \; I \not\models P & 5bb. \; I \not\models Q \\ & 6bb. \; I \models \bot \end{array}
\end{array}
$$

We cannot always derive a contradiction. F is not valid.

UNI FREIBURG

Is $F: P \lor Q \rightarrow P \land Q$ valid?

Let's assume that F is not valid.

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

$$
\begin{array}{ll|ll|ll|ll}
4a. & I \models P & & 2 \text{ and } \lor & 4b. & I \models Q & & 2 \text{ and } \lor \\
5aa. & I \not\models P & 5ab. & I \not\models Q & 5ba. & I \not\models P & 5bb. & I \not\models Q \\
6aa. & I \models \bot & & & & & 6bb. & I \models \bot
\end{array}
$$

We cannot always derive a contradiction. F is not valid.

<u>Falsifying interpretation</u>:

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

Example 3

Is $F: P \lor Q \rightarrow P \land Q$ valid?

Let's assume that F is not valid.

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

$$
\begin{array}{l|l}
4a.\ I \models P \quad 2 \text{ and } \lor & 4b.\ I \models Q \quad 2 \text{ and } \lor \\
\begin{array}{l|l} 5aa.\ I \not\models P & 5ab.\ I \not\models Q \\ 6aa.\ I \models \bot & \end{array} & \begin{array}{l|l} 5ba.\ I \not\models P & 5bb.\ I \not\models Q \\ & 6bb.\ I \models \bot \end{array}
\end{array}
$$

We cannot always derive a contradiction. F is not valid.

Falsifying interpretation:

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

We have to derive a contradiction in all 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!

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):

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

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

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

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

$\neg(P \rightarrow Q) \Leftrightarrow \neg(\neg P \vee Q) \Leftrightarrow \neg\neg P \wedge \neg Q$

$\Leftrightarrow P \wedge \neg Q$

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):

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

Example

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

Example

Convert $F: (Q_1 \lor \neg\neg R_1) \land (\neg Q_2 \to R_2)$ into DNF

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

The last formula is equivalent to F and is in DNF. Note that formulas can grow exponentially.

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):

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

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):

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

A disjunction of literals $P_1 \lor P_2 \lor \neg P_3$ is called a clause.

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):

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

A disjunction of literals $P_1 \lor P_2 \lor \neg P_3$ is called a clause.
For brevity we write it as set: $\{P_1, P_2, \overline{P_3}\}$.
A formula in CNF is a set of clauses (a set of sets of literals).

Equisatisfiability

Definition (Equisatisfiability)

F and F' are equisatisfiable, iff

$$F \text{ is satisfiable if and only if } F' \text{ is satisfiable}$$

Definition (Equisatisfiability)

F and F' are equisatisfiable, iff

$$F \text{ is satisfiable if and only if } F' \text{ is satisfiable}$$

Every formula is equisatifiable to either $\top$ or $\bot$.

Equisatisfiability

Definition (Equisatisfiability)

F and F' are equisatisfiable, iff

$$F \text{ is satisfiable if and only if } F' \text{ is satisfiable}$$

Every formula is equisatifiable to either $\top$ or $\bot$.
There is a efficient conversion of F to F' where

- F' is in CNF and
- F and F' are equisatisfiable

Equisatisfiability

Definition (Equisatisfiability)

F and F' are equisatisfiable, iff

$$F \text{ is satisfiable if and only if } F' \text{ is satisfiable}$$

Every formula is equisatifiable to either $\top$ or $\bot$.
There is a efficient conversion of F to F' where

- F' is in CNF and
- F and F' are equisatisfiable

Note: efficient means polynomial in the size of F.

Conversion to CNF

Basic Idea:

- Introduce a new variable P_G for every subformula G; unless G is already an atom.

Conversion to CNF

Basic Idea:

- Introduce a new variable P_G for every subformula G; unless G is already an atom.
- For each subformula $G: \ G_1 \circ G_2$ produce a small formula $P_G \ \leftrightarrow \ P_{G_1} \circ P_{G_2}$.

Conversion to CNF

Basic Idea:

- Introduce a new variable P_G for every subformula G; unless G is already an atom.
- For each subformula $G : G_1 \circ G_2$ produce a small formula $P_G \leftrightarrow P_{G_1} \circ P_{G_2}$.
- encode each of these (small) formulae separately to CNF.

Conversion to CNF

Basic Idea:

- Introduce a new variable P_G for every subformula G; unless G is already an atom.
- For each subformula $G : G_1 \circ G_2$ produce a small formula $P_G \leftrightarrow P_{G_1} \circ P_{G_2}$.
- encode each of these (small) formulae separately to CNF.

The formula

$$P_F \wedge \bigwedge_G CNF(P_G \leftrightarrow P_{G_1} \circ P_{G_2})$$

is equisatisfiable to F (Why?)

Conversion to CNF

Basic Idea:

- Introduce a new variable P_G for every subformula G; unless G is already an atom.
- For each subformula $G : \ G_1 \circ G_2$ produce a small formula $P_G \ \leftrightarrow \ P_{G_1} \circ P_{G_2}$.
- encode each of these (small) formulae separately to CNF.

The formula

$$P_F \wedge \bigwedge_G CNF(P_G \ \leftrightarrow \ P_{G_1} \circ P_{G_2})$$

is equisatisfiable to F (Why?)

The number of subformulae is linear in the size of F.

The time to convert one small formula is constant!

Example: CNF

Convert $F : P \lor Q \rightarrow P \land \neg R$ to CNF.

Example: CNF

Convert $F: P \lor Q \rightarrow P \land \neg R$ to CNF.
Introduce new variables: P_F, $P_{P \lor Q}$, $P_{P \land \neg R}$, $P_{\neg R}$.

Example: CNF

Convert $F : P \lor Q \to P \land \neg R$ to CNF.
Introduce new variables: P_F, $P_{P \lor Q}$, $P_{P \land \neg R}$, $P_{\neg R}$. Create new formulae and convert them to CNF separately:

- $P_F \leftrightarrow (P_{P \lor Q} \to P_{P \land \neg R})$ in CNF:

$$F_1 : \{\{\overline{P_F}, \overline{P_{P \lor Q}}, P_{P \land \neg R}\}, \{P_F, P_{P \lor Q}\}, \{P_F, \overline{P_{P \land \neg R}}\}\}$$

- $P_{P \lor Q} \leftrightarrow P \lor Q$ in CNF:

$$F_2 : \{\{\overline{P_{P \lor Q}}, P \lor Q\}, \{P_{P \lor Q}, \overline{P}\}, \{P_{P \lor Q}, \overline{Q}\}\}$$

- $P_{P \land \neg R} \leftrightarrow P \land P_{\neg R}$ in CNF:

$$F_3 : \{\{\overline{P_{P \land \neg R}} \lor P\}, \{\overline{P_{P \land \neg R}}, P_{\neg R}\}, \{P_{P \land \neg R}, \overline{P}, \overline{P_{\neg R}}\}\}$$

- $P_{\neg R} \leftrightarrow \neg R$ in CNF: $F_4 : \{\{\overline{P_{\neg R}}, \overline{R}\}, \{P_{\neg R}, R\}\}$

$\{\{P_F\}\} \cup F_1 \cup F_2 \cup F_3 \cup F_4$ is in CNF and equisatisfiable to F.

Davis-Putnam-Logemann-Loveland (DPLL) Algorithm

Decides the satisfiability of PL formulae in CNF

Decision Procedure DPLL: Given F in CNF

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

Unit Propagation (PROP)

If a clause contains one literal ℓ,

- Set ℓ to $\top$.
- Remove all clauses containing ℓ.
- Remove $\neg\ell$ in all clauses.

Unit Propagation (PROP)

If a clause contains one literal ℓ,

- Set ℓ to $\top$.
- Remove all clauses containing ℓ.
- Remove $\neg\ell$ in all clauses.

Based on resolution

$$\frac{\ell \qquad \neg\ell \lor C}{C} \leftarrow \text{clause}$$

Pure Literal Propagation (PLP)

If P occurs only positive (without negation), set it to $\top$.

Pure Literal Propagation (PLP)

If P occurs only positive (without negation), set it to $\top$.
If P occurs only negative set it to $\bot$.

Example

$$F: \; (\neg P \lor Q \lor R) \land (\neg Q \lor R) \land (\neg Q \lor \neg R) \land (P \lor \neg Q \lor \neg R)$$

Example

$F: (\neg P \lor Q \lor R) \land (\neg Q \lor R) \land (\neg Q \lor \neg R) \land (P \lor \neg Q \lor \neg R)$

Branching on Q

$F : (\neg P \lor Q \lor R) \land (\neg Q \lor R) \land (\neg Q \lor \neg R) \land (P \lor \neg Q \lor \neg R)$

Branching on Q

$$F\{Q \mapsto \top\} : (R) \land (\neg R) \land (P \lor \neg R)$$

By unit resolution

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

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

On the other branch

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

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

F is satisfiable with satisfying interpretation

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

Example

$$F: (\neg P \lor Q \lor R) \land (\neg Q \lor R) \land (\neg Q \lor \neg R) \land (P \lor \neg Q \lor \neg R)$$

F

$Q \mapsto \top$: $(R) \land (\neg R) \land (P \lor \neg R)$

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

$Q \mapsto \bot$: $(\neg P \lor R)$

$R \mapsto \top$: $\neg P$

$P \mapsto \bot$

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

Knight and Knaves

A island is inhabited only by knights and knaves. Knights always tell the truth, and knaves always lie. You meet four inhabitants: Alice, Bob, Charles and Doris.

- Alice says that Doris is a knave.
- Bob tells you that Alice is a knave.
- Charles claims that Alice is a knave.
- Doris tells you, ‘Of Charles and Bob, exactly one is a knight.’

Knight and Knaves

Let A denote that Alice is a Knight, etc. Then:

- $A \leftrightarrow \neg D$
- $B \leftrightarrow \neg A$
- $C \leftrightarrow \neg A$
- $D \leftrightarrow \neg(C \leftrightarrow B)$

Knight and Knaves

Let A denote that Alice is a Knight, etc. Then:

- $A \leftrightarrow \neg D$
- $B \leftrightarrow \neg A$
- $C \leftrightarrow \neg A$
- $D \leftrightarrow \neg(C \leftrightarrow B)$

In CNF:

- $\{\overline{A}, \overline{D}\}, \{A, D\}$
- $\{\overline{B}, \overline{A}\}, \{B, A\}$
- $\{\overline{C}, \overline{A}\}, \{C, A\}$
- $\{\overline{D}, \overline{C}, \overline{B}\}, \{\overline{D}, C, B\}, \{D, \overline{C}, B\}, \{D, C, \overline{B}\}$