THE UNIVERSITY OF MELBOURNE

COMP30026
Models of Computation

Cezary Kaliszyk and William Umboh

Lecture 4

Resolution

Propositional Logic is Decidable

Valid/contingent/unsatisfiable? Decide with truth table.

Propositional Logic is Decidable

Valid/contingent/unsatisfiable? Decide with truth table.

Finite, but huge!

2^n rows where n is number of variables.

Either-Or Reasoning

If it is raining, I will bring an umbrella.
If it is not raining, I will have ice cream.

$\therefore$

Either-Or Reasoning

$$\begin{array}{ll} & \text{If it is raining, I will bring an umbrella.} \\ & \text{If it is not raining, I will have ice cream.} \\ \hline \therefore & \text{I will either bring an umbrella or have ice cream.} \end{array}$$

Either-Or Reasoning, Symbolically

$$\frac{\begin{array}{c} P \rightarrow F \\ \neg P \rightarrow G \end{array}}{F \vee G} \qquad\qquad \frac{\begin{array}{c} P \rightarrow \bot \\ \neg P \rightarrow \bot \end{array}}{\bot}$$

Resolution

Rewrite "$\rightarrow$" in terms of "$\neg$" and "$\vee$":

$$\frac{\neg P \vee F \qquad P \vee G}{F \vee G} \qquad\qquad \frac{\neg P \qquad P}{\bot}$$

This is resolution.

Resolution

Rewrite “→” in terms of “¬” and “∨”:

$$\frac{\neg P \lor F \qquad P \lor G}{F \lor G} \qquad\qquad \frac{\neg P \qquad P}{\bot}$$

This is resolution.

Exercise: check this is sound!

Resolution Graph Example

Graphical representation of proof:

$B \vee \neg A$ $\quad$ $B \vee A$ $\quad$ $\neg B$

Resolution Graph Example

Graphical representation of proof:

$$
\begin{tikzcd}[column sep=small]
B \vee \neg A & & B \vee A \arrow[dr, dash] & & \neg B \arrow[dl, dash] \\
 & & & A &
\end{tikzcd}
$$

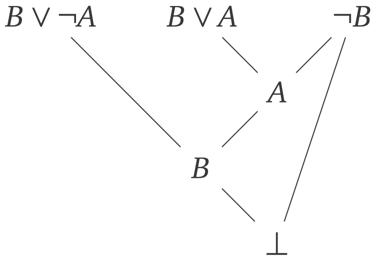
Resolution Graph Example

Graphical representation of proof:

$$
\begin{tikzcd}[arrows=dash]
B \lor \neg A \arrow[ddrr] & & B \lor A \arrow[dr] & & \neg B \arrow[dl] \\
& & & A \arrow[dl] & \\
& & B & &
\end{tikzcd}
$$

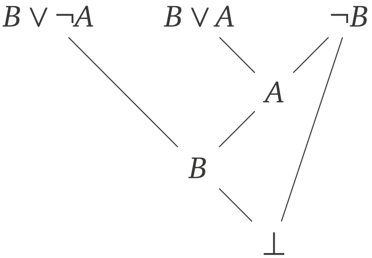
Resolution Graph Example

Graphical representation of proof:



Resolution Graph Example

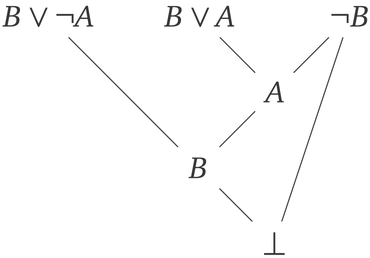
Graphical representation of proof:



A refutation of $(B \vee \neg A) \wedge (B \vee A) \wedge \neg B$

Resolution Graph Example

Graphical representation of proof:



A refutation of $(B \vee \neg A) \wedge (B \vee A) \wedge \neg B$ Showing that it is not true; deriving contradiction

How to Use Refutations

To show that F is valid, refute $\neg F$.

Theorem

$\models F$ *iff* $\neg F \models \bot$.

How to Use Refutations

To show that F is valid, refute $\neg F$.

Theorem

$\models F$ *iff* $\neg F \models \bot$.

To prove $F \models G$, refute $F \wedge \neg G$.

Theorem

$F \models G$ *iff* $F \wedge \neg G \models \bot$.

Resolution Proof Exercise

Refute:

$$P \lor \neg Q \qquad \neg P \qquad Q \lor \neg R \qquad Q \lor R \lor S \qquad \neg S$$

Resolution Proof Exercise

Refute:

$$P \vee \neg Q \qquad \neg P \qquad Q \vee \neg R \qquad Q \vee R \vee S \qquad \neg S$$

$$\neg Q \qquad\qquad\qquad\qquad Q \vee R$$

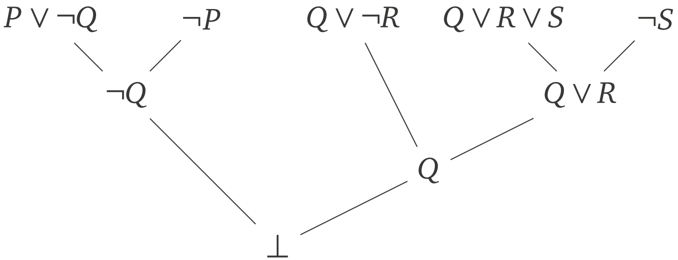
Resolution Proof Exercise

Refute:

$$
\begin{tikzcd}[arrows=dash]
P \lor \neg Q \arrow[dr] & & \neg P \arrow[dl] & Q \lor \neg R \arrow[ddrr] & & Q \lor R \lor S \arrow[dr] & & \neg S \arrow[dl] \\
& \neg Q & & & & & Q \lor R \arrow[dl] & \\
& & & & & Q & &
\end{tikzcd}
$$

Resolution Proof Exercise

Refute:



Resolution Proof Exercise

Derive R from the premises:

$$P \lor Q \qquad \neg P \lor R \qquad \neg Q \lor R \qquad S$$

Resolution Proof Exercise

Derive R from the premises:

$$\begin{array}{ccccccc} P \lor Q & & \neg P \lor R & & \neg Q \lor R & & S \\ & Q \lor R & & & & & \\ & & R & & & & \end{array}$$

Do Not Do This, Please

Do not cancel **multiple** variables at once!

Do Not Do This, Please

Do not cancel **multiple** variables at once!

$(P \lor Q) \land (\neg P \lor \neg Q)$ is **satisfiable**!!!

If you could cancel both, you would get $\bot$!!!

Do Not Do This, Please

Do not cancel **multiple** variables at once!

$(P \vee Q) \wedge (\neg P \vee \neg Q)$ is **satisfiable**!!!

If you could cancel both, you would get $\perp$!!!

This would not be sound!!!

Propositional Resolution Formally

Definition

A resolution proof of C_m from wffs $P_1, \ldots, P_n$ is a string of the form

$$P_1, \ldots, P_n \vdash C_1, \ldots, C_m$$

where each C_i is either a copy of some P_j, or otherwise follows by resolution from any two wffs earlier in the string.

Propositional Resolution Formally

Definition

A resolution proof of C_m from wffs $P_1, \ldots, P_n$ is a string of the form

$$P_1, \ldots, P_n \vdash C_1, \ldots, C_m$$

where each C_i is either a copy of some P_j, or otherwise follows by resolution from any two wffs earlier in the string.

Examples:

- "$P \vdash P$"
- "$P, \neg P \vdash \bot$"
- "$(P \vee Q), \neg P \vdash Q$"

Resolution System is Sound

We write "$\Sigma \vdash_R F$" to mean "there is a resolution proof of F from the set of premises Σ".

Resolution System is Sound

We write "$\Sigma \vdash_R F$" to mean "there is a resolution proof of F from the set of premises Σ".

Theorem (Soundness)

If $\Sigma \vdash_R F$, then $\Sigma \models F$.

Resolution System is Sound

We write "$\Sigma \vdash_R F$" to mean "there is a resolution proof of F from the set of premises Σ".

Theorem (Soundness)

If $\Sigma \vdash_R F$, then $\Sigma \models F$.

Proof (sketch).

Let x be a proof of F from Σ.
Let v be a model of Σ.
Let $C_1, \ldots, C_n$ be the wffs after the $\vdash$ in x.
Prove by induction that v satisfies each C_i. $\square$

Conjunctive Normal Form (CNF)

Literal: a propositional atom or its negation.

(Disjunctive) clause: disjunction ($\vee$) of literals.

CNF: conjunction ($\wedge$) of disjunctive clauses.

Conjunctive Normal Form (CNF)

Literal: a propositional atom or its negation.

(Disjunctive) clause: disjunction ($\vee$) of literals.

CNF: conjunction ($\wedge$) of disjunctive clauses.

Example

$$(A \vee \neg B) \wedge (B \vee C \vee D) \wedge A$$

Conjunctive Normal Form (CNF)

Literal: a propositional atom or its negation.

(Disjunctive) clause: disjunction ($\vee$) of literals.

CNF: conjunction ($\wedge$) of disjunctive clauses.

Example

$$(A \vee \neg B) \wedge (B \vee C \vee D) \wedge A$$

Theorem

Every propositional formula has an equivalent CNF.

Negation Normal Form (NNF) to CNF

NNF: Only connectives are $\neg$, $\wedge$ and $\vee$. $\neg$ only in front of variables.

Example

$$(\neg A \vee (B \wedge \neg C)) \vee (C \wedge (B \vee D))$$

Negation Normal Form (NNF) to CNF

NNF: Only connectives are $\neg$, $\wedge$ and $\vee$. $\neg$ only in front of variables.

Example

$$(\neg A \vee (B \wedge \neg C)) \vee (C \wedge (B \vee D))$$

To get NNF:

1. Eliminate $\leftrightarrow$ (rewrite using $\rightarrow$ and $\wedge$).
2. Eliminate $\rightarrow$ (rewrite using $\vee$ and $\neg$).
3. Push $\neg$ inward (use de Morgan's laws).
4. Eliminate $\neg\neg$.

Negation Normal Form (NNF) to CNF

NNF: Only connectives are $\neg$, $\wedge$ and $\vee$. $\neg$ only in front of variables.

Example

$$(\neg A \vee (B \wedge \neg C)) \vee (C \wedge (B \vee D))$$

To get NNF:

1. Eliminate $\leftrightarrow$ (rewrite using $\rightarrow$ and $\wedge$).
2. Eliminate $\rightarrow$ (rewrite using $\vee$ and $\neg$).
3. Push $\neg$ inward (use de Morgan's laws).
4. Eliminate $\neg\neg$.

To get CNF from NNF, distribute $\vee$ over $\wedge$.

Example Conversion to CNF

$(\neg P \land (\neg Q \to R)) \leftrightarrow S$

Example Conversion to CNF

$$
\begin{aligned}
& (\neg P \land (\neg Q \rightarrow R)) \leftrightarrow S \\
\equiv \quad & ((\neg P \land (\neg Q \rightarrow R)) \rightarrow S) \land (S \rightarrow (\neg P \land (\neg Q \rightarrow R))) \qquad (1)
\end{aligned}
$$

Example Conversion to CNF

$$
\begin{aligned}
& (\neg P \wedge (\neg Q \rightarrow R)) \leftrightarrow S \\
\equiv\ & ((\neg P \wedge (\neg Q \rightarrow R)) \rightarrow S) \wedge (S \rightarrow (\neg P \wedge (\neg Q \rightarrow R))) && (1) \\
\equiv\ & (\neg(\neg P \wedge (\neg Q \rightarrow R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (\neg Q \rightarrow R))) && (2)
\end{aligned}
$$

Example Conversion to CNF

$$
\begin{aligned}
& (\neg P \land (\neg Q \rightarrow R)) \leftrightarrow S \\
\equiv\ & ((\neg P \land (\neg Q \rightarrow R)) \rightarrow S) \land (S \rightarrow (\neg P \land (\neg Q \rightarrow R))) && (1) \\
\equiv\ & (\neg(\neg P \land (\neg Q \rightarrow R)) \lor S) \land (\neg S \lor (\neg P \land (\neg Q \rightarrow R))) && (2) \\
\equiv\ & (\neg(\neg P \land (\neg\neg Q \lor R)) \lor S) \land (\neg S \lor (\neg P \land (\neg\neg Q \lor R))) && (2)
\end{aligned}
$$

Example Conversion to CNF

$$
\begin{array}{rll}
& (\neg P \land (\neg Q \to R)) \leftrightarrow S & \\
\equiv & ((\neg P \land (\neg Q \to R)) \to S) \land (S \to (\neg P \land (\neg Q \to R))) & (1) \\
\equiv & (\neg(\neg P \land (\neg Q \to R)) \lor S) \land (\neg S \lor (\neg P \land (\neg Q \to R))) & (2) \\
\equiv & (\neg(\neg P \land (\neg\neg Q \lor R)) \lor S) \land (\neg S \lor (\neg P \land (\neg\neg Q \lor R))) & (2) \\
\equiv & ((\neg\neg P \lor (\neg\neg\neg Q \land \neg R)) \lor S) \land (\neg S \lor (\neg P \land (\neg\neg Q \lor R))) & (3)
\end{array}
$$

Example Conversion to CNF

$$
\begin{aligned}
& (\neg P \land (\neg Q \rightarrow R)) \leftrightarrow S \\
\equiv\ & ((\neg P \land (\neg Q \rightarrow R)) \rightarrow S) \land (S \rightarrow (\neg P \land (\neg Q \rightarrow R))) && (1) \\
\equiv\ & (\neg(\neg P \land (\neg Q \rightarrow R)) \lor S) \land (\neg S \lor (\neg P \land (\neg Q \rightarrow R))) && (2) \\
\equiv\ & (\neg(\neg P \land (\neg\neg Q \lor R)) \lor S) \land (\neg S \lor (\neg P \land (\neg\neg Q \lor R))) && (2) \\
\equiv\ & ((\neg\neg P \lor (\neg\neg\neg Q \land \neg R)) \lor S) \land (\neg S \lor (\neg P \land (\neg\neg Q \lor R))) && (3) \\
\equiv\ & ((P \lor (\neg Q \land \neg R)) \lor S) \land (\neg S \lor (\neg P \land (Q \lor R))) && (4)
\end{aligned}
$$

Example Conversion to CNF

$$
\begin{aligned}
& (\neg P \wedge (\neg Q \rightarrow R)) \leftrightarrow S \\
\equiv\ & ((\neg P \wedge (\neg Q \rightarrow R)) \rightarrow S) \wedge (S \rightarrow (\neg P \wedge (\neg Q \rightarrow R))) && (1) \\
\equiv\ & (\neg(\neg P \wedge (\neg Q \rightarrow R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (\neg Q \rightarrow R))) && (2) \\
\equiv\ & (\neg(\neg P \wedge (\neg\neg Q \vee R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (\neg\neg Q \vee R))) && (2) \\
\equiv\ & ((\neg\neg P \vee (\neg\neg\neg Q \wedge \neg R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (\neg\neg Q \vee R))) && (3) \\
\equiv\ & ((P \vee (\neg Q \wedge \neg R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (Q \vee R))) && (4) \\
\equiv\ & (((P \vee \neg Q) \wedge (P \vee \neg R)) \vee S) \\
& \quad \wedge((\neg S \vee \neg P) \wedge (\neg S \vee (Q \vee R))) && (5)
\end{aligned}
$$

Example Conversion to CNF

$$
\begin{aligned}
& (\neg P \wedge (\neg Q \rightarrow R)) \leftrightarrow S \\
\equiv\ & ((\neg P \wedge (\neg Q \rightarrow R)) \rightarrow S) \wedge (S \rightarrow (\neg P \wedge (\neg Q \rightarrow R))) && (1) \\
\equiv\ & (\neg(\neg P \wedge (\neg Q \rightarrow R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (\neg Q \rightarrow R))) && (2) \\
\equiv\ & (\neg(\neg P \wedge (\neg\neg Q \vee R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (\neg\neg Q \vee R))) && (2) \\
\equiv\ & ((\neg\neg P \vee (\neg\neg\neg Q \wedge \neg R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (\neg\neg Q \vee R))) && (3) \\
\equiv\ & ((P \vee (\neg Q \wedge \neg R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (Q \vee R))) && (4) \\
\equiv\ & (((P \vee \neg Q) \wedge (P \vee \neg R)) \vee S) \\
& \quad \wedge ((\neg S \vee \neg P) \wedge (\neg S \vee (Q \vee R))) && (5) \\
\equiv\ & (P \vee \neg Q \vee S) \wedge (P \vee \neg R \vee S) \\
& \quad \wedge (\neg S \vee \neg P) \wedge (\neg S \vee Q \vee R) && (5)
\end{aligned}
$$

Example Conversion to CNF

$$
\begin{aligned}
& (\neg P \wedge (\neg Q \rightarrow R)) \leftrightarrow S \\
\equiv\; & ((\neg P \wedge (\neg Q \rightarrow R)) \rightarrow S) \wedge (S \rightarrow (\neg P \wedge (\neg Q \rightarrow R))) && (1)\\
\equiv\; & (\neg(\neg P \wedge (\neg Q \rightarrow R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (\neg Q \rightarrow R))) && (2)\\
\equiv\; & (\neg(\neg P \wedge (\neg\neg Q \vee R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (\neg\neg Q \vee R))) && (2)\\
\equiv\; & ((\neg\neg P \vee (\neg\neg\neg Q \wedge \neg R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (\neg\neg Q \vee R))) && (3)\\
\equiv\; & ((P \vee (\neg Q \wedge \neg R)) \vee S) \wedge (\neg S \vee (\neg P \wedge (Q \vee R))) && (4)\\
\equiv\; & (((P \vee \neg Q) \wedge (P \vee \neg R)) \vee S) \\
& \quad \wedge ((\neg S \vee \neg P) \wedge (\neg S \vee (Q \vee R))) && (5)\\
\equiv\; & (P \vee \neg Q \vee S) \wedge (P \vee \neg R \vee S) \\
& \quad \wedge (\neg S \vee \neg P) \wedge (\neg S \vee Q \vee R) && (5)
\end{aligned}
$$

The result is in conjunctive normal form.

Resolution is Refutation-Complete

Theorem

Every unsatisfiable set of clauses has a resolution refutation.

In other words:

Theorem

Let Σ be a set of clauses.
If $\Sigma \models \bot$, then $\Sigma \vdash_R \bot$.

Satisfiability Algorithm

This gives us an algorithm:

1. Convert formula into suitable form.
2. Repeatedly apply resolution.
   - Derive $\bot$? Report unsatisfiable.
   - Cannot derive anything new? Report satisfiable.

Simplifying CNF

Common redundancies:

- Duplicate variables (e.g. $P \lor P$)
- Tautologies (e.g. $P \lor \neg P \lor Q$)
- Subsumptions (e.g. $(P \lor \neg Q \lor R) \land (P \lor R)$)

Simplifying CNF

Common redundancies:

- Duplicate variables (e.g. $P \lor P$)
- Tautologies (e.g. $P \lor \neg P \lor Q$)
- Subsumptions (e.g. $(P \lor \neg Q \lor R) \land (P \lor R)$)

Exercise: simplify this formula:

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

Simplifying CNF

Common redundancies:

- Duplicate variables (e.g. $P \vee P$)
- Tautologies (e.g. $P \vee \neg P \vee Q$)
- Subsumptions (e.g. $(P \vee \neg Q \vee R) \wedge (P \vee R)$)

Exercise: simplify this formula:

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

Note that CNF is not unique!

Clausal Form

Represent CNF as set of sets of literals.

Example

CNF:

$$(P \lor \neg Q \lor S) \land (P \lor \neg R \lor S) \land (\neg S \lor \neg P) \land (\neg S \lor Q \lor R)$$

Clausal form:

$$\{\{P, S, \neg Q\}, \{P, S, \neg R\}, \{\neg P, \neg S\}, \{Q, R, \neg S\}\}$$

We shall often treat these interchangeably.

Why? Simplifies reasoning.

Empty Disjunction

Let A and B be propositional variables.

- $\{A, B\}$ represents the clause $A \vee B$.
- $\{A\}$ represents the clause A.

Empty Disjunction

Let A and B be propositional variables.

- $\{A, B\}$ represents the clause $A \vee B$.
- $\{A\}$ represents the clause A.

What disjunctive clause does $\{\}$ represent?
($\{\}$ sometimes written $\emptyset$)

Empty Disjunction

Let A and B be propositional variables.

- $\{A, B\}$ represents the clause $A \vee B$.
- $\{A\}$ represents the clause A.

What disjunctive clause does $\{\}$ represent?
($\{\}$ sometimes written $\emptyset$)

Natural choice: $\bot$.

Empty Disjunction

Let A and B be propositional variables.

- $\{A, B\}$ represents the clause $A \vee B$.
- $\{A\}$ represents the clause A.

What disjunctive clause does $\{\}$ represent?
($\{\}$ sometimes written $\emptyset$)

Natural choice: $\bot$.

Disjunction is true iff at least one disjunct is true.

Empty Conjunction

Let C_1 and C_2 be clauses.

- $\{C_1, C_2\}$ represents the CNF formula $C_1 \land C_2$.
- $\{C_1\}$ represents the CNF C_1.

What CNF does $\{\}$ represent?

Empty Conjunction

Let C_1 and C_2 be clauses.

- $\{C_1, C_2\}$ represents the CNF formula $C_1 \land C_2$.
- $\{C_1\}$ represents the CNF C_1.

What CNF does $\{\}$ represent?

Natural choice: $\top$.

Empty Conjunction

Let C_1 and C_2 be clauses.

- $\{C_1, C_2\}$ represents the CNF formula $C_1 \wedge C_2$.
- $\{C_1\}$ represents the CNF C_1.

What CNF does $\{\}$ represent?

Natural choice: $\top$.

Conjunction is true iff every conjunct is true.

Empty Clauses and Formulas

- Empty conjunction ($\wedge$) is valid.
- Empty disjunction ($\vee$) is unsatisfiable.

Empty Clauses and Formulas

- Empty conjunction ($\wedge$) is valid.
- Empty disjunction ($\vee$) is unsatisfiable.

Thus:

- The empty set of clauses is valid.
- A set of clauses containing the empty clause is unsatisfiable.

Propositional Resolution for Clausal Form

Let P be a propositional variable.

Let C_1, C_2 be clauses without P or $\neg P$.

$$\frac{\begin{array}{c} C_1 \cup \{P\} \\ C_2 \cup \{\neg P\} \end{array}}{C_1 \cup C_2}$$