# Propositional Logic

Bow-Yaw Wang

Institute of Information Science
Academia Sinica, Taiwan

September 12, 2017

# Outline

- Consider the following arguments:

**Example**

若火車誤點且車站沒有計程車，則小明開會就遲到。小明開會並沒有遲到，而火車誤點。那麼車站就有計程車。

**Example**

如果下雨而且小華沒帶雨傘，則小華會淋溼。小華並沒有淋溼，而外面正在下雨。那麼小華一定帶了雨傘。

- Both examples have the same structure:

| | | |
|---|---|---|
| $p$ | 火車誤點 | 下雨 |
| $q$ | 車站有計程車 | 小華帶雨傘 |
| $r$ | 小明開會遲到 | 小華淋溼 |

If $p$ and not $q$, then $r$. Not $r$. $p$. Hence $q$.

（若$p$ 且非$q$，則$r$。非$r$，$p$。則$q$）

# Propositions

- We will develop a language to reason such arguments.
- Our langauge is based on propositions (or declarative sentences).
- Examples:
  - The sum of 3 and 5 equals 8.
  - Every even natural number is the sum of two prime numbers (Goldbach's conjecture).
  - All hobbits like mushrooms in their soup.
- A proposition can either be "true" or "false."
- Non-examples:
  - When will we have lunch?
  - Run!

# Atomic Sentences

- Certain sentences are the basic blocks of our language.
  - They are called atomic (or indecomposable) sentences.
- We will use $p, q, r, \ldots$ (possibly with sub- or super-scripts) to denote sentences.
- Examples:
  - Let $p$ denote "I won the lottery last week."
  - Let $q$ denote "I bought a lottery ticket."
  - Let $r$ denote "I won last week's grand prize."
- In fact, $p$, $q$, and $r$ are all atomic sentences.

# Sentences

- Let $p, q, r, \ldots$ be sentences.
  - $p$ : "I won the lottery last week."
  - $q$ : "I bought a lottery ticket."
  - $r$ : "I won last week's grand prize."
- We construct new sentences by the following connectives:
  - The negation of $p$ (denoted by $\neg p$).
    - ★ It is **not** true that "I won the lottery last week."
  - The disjunction of $p$ and $q$ (denoted by $p \vee q$).
    - ★ "I won the lottery last week" **or** "I won last week's grand prize."
  - The conjunction of $p$ and $q$ (denoted by $p \wedge q$).
    - ★ "I won the lottery last week" **and** "I bought a lottery ticket."
  - The implication of $r$ and $p$ (denoted by $r \implies p$).
    - ★ "I won last week's grand prize" **implies** "I won the lottery last week."

# Binding Priorities

- If $p, q, r$ are sentences, $p \land q$ and $(\neg r) \lor q$ are sentences.
- $(p \land q) \implies ((\neg r) \lor q)$ is also a sentence.
- To reduce the number of parentheses, we adopt the following conventions:
  **Convention**.

| strong | | weak |
|---|---|---|
| $\neg$ | $\{\lor, \land\}$ | $\implies$ |

- Hence $p \land q \implies \neg r \lor q$ is indeed $(p \land q) \implies ((\neg r) \lor q)$.

# Examples, Examples, Examples

- Let us rewrite our examples:

**Example**

若火車誤點且車站沒有計程車，則小明開會就遲到。小明開會並沒有遲到，而火車誤點。那麼車站就有計程車。

- We have the following atomic sentences:
  $p$ : 火車誤點 | $q$ : 車站有計程車 | $r$ : 小明開會遲到
- In our language, we write:
  - $p \land \neg q \implies r$ （若火車誤點且車站沒有計程車，則小明開會就遲到）
  - $\neg r$ （小明開會並沒有遲到）
  - $p$ （火車誤點）
  - Hence $q$ （車站就有計程車）

# Examples, Examples, Examples

- Let us rewrite our examples:

**Example**

如果下雨而且小華沒帶雨傘，則小華會淋溼。小華並沒有淋溼，而外面正在下雨。那麼小華一定帶了雨傘。

- We have the following atomic sentences:

| $p$ : 下雨 | $q$ : 小華帶雨傘 | $r$ : 小華淋溼 |
|---|---|---|

- In our language, we write:
  - $p \wedge \neg q \implies r$ （如果下雨而且小華沒帶雨傘，則小華會淋溼）
  - $\neg r$ （小華並沒有淋溼）
  - $p$ （外面正在下雨）
  - Hence $q$ （小華一定帶了雨傘）

# Outline

# Natural Deduction

- In our examples, we (informally) infer new sentences.
- In natural deduction, we have a collection of proof rules.
  - These proof rules allow us to infer new sentences logically followed from existing ones.
- Supose we have a set of sentences: $\phi_1, \phi_2, \ldots, \phi_n$ (called premises), and another sentence $\psi$ (called a conclusion).
- The notation

$$\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$$

  is called a sequent.
- A sequent is valid if a proof (built by the proof rules) can be found.
- We will try to build a proof for our examples. Namely,

$$\boxed{p \wedge \neg q \implies r, \neg r, p \vdash q.}$$

# Proof Rules for Natural Deduction – Conjunction

- Suppose we want to prove a conclusion $\phi \wedge \psi$. What do we do?
  - Of course, we need to prove both $\phi$ and $\psi$ so that we can conclude $\phi \wedge \psi$.
- Hence the proof rule for conjunction is

$$\frac{\phi \quad \psi}{\phi \wedge \psi} \wedge i$$

  - Note that premises are shown above the line and the conclusion is below. Also, $\wedge i$ is the name of the proof rule.
  - This proof rule is called "conjunction-introduction" since we introduce a conjunction ($\wedge$) in the conclusion.

# Proof Rules for Natural Deduction – Conjunction

- For each connective, we have introduction proof rule(s) and also elimination proof rule(s).
- Suppose we want to prove a conclusion $\phi$ from the premise $\phi \wedge \psi$. What do we do?
  - We don't do any thing since we know $\phi$ already!
- Here are the elimination proof rules:

$$\frac{\phi \wedge \psi}{\phi} \wedge e_1 \qquad\qquad \frac{\phi \wedge \psi}{\psi} \wedge e_2$$

- The rule $\wedge e_1$ says: if you have a proof for $\phi \wedge \psi$, then you have a proof for $\phi$ by applying this proof rule.
- Why do we need two rules?
  - Because we want to manipulate syntax only.

**Example**

Prove $p \wedge q, r \vdash q \wedge r$.

**Proof.**

We are looking for a proof of the form:

$$\begin{array}{c} p \wedge q \quad r \\ \vdots \\ q \wedge r \end{array}$$

$\square$

# Examples

## Example

Prove $p \wedge q, r \vdash q \wedge r$.

## Proof.

We are looking for a proof of the form:

$$\cfrac{\cfrac{p \wedge q}{q}\ \wedge e_2 \qquad r}{q \wedge r}\ \wedge i$$

We will write proofs in lines:

| | | |
|---|---|---|
| 1 | $p \wedge q$ | premise |
| 2 | $r$ | premise |
| 3 | $q$ | $\wedge e_2$ 1 |
| 4 | $q \wedge r$ | $\wedge i$ 3, 2 |

$\square$

# Proof Rules for Natural Deduction – Double Negation

- Suppose we want to prove $\phi$ from a proof for $\neg\neg\phi$. What do we do?
  - There is no difference between $\phi$ and $\neg\neg\phi$. The same proof suffices!
- Hence we have the following proof rules:

$$\boxed{\frac{\phi}{\neg\neg\phi}\ \neg\neg i} \qquad \boxed{\frac{\neg\neg\phi}{\phi}\ \neg\neg e}$$

# Examples

## Example

Prove $p, \neg\neg(q \wedge r) \vdash \neg\neg p \wedge r$.

## Proof.

We are looking for a proof like:

$$\begin{array}{c} p \quad \neg\neg(q \wedge r) \\ \vdots \\ \neg\neg p \wedge r \end{array}$$

$\square$

# Examples

## Example

Prove $p, \neg\neg(q \wedge r) \vdash \neg\neg p \wedge r$.

## Proof.

We are looking for a proof like:

$$\dfrac{\dfrac{p}{\neg\neg p}\ \neg\neg i \qquad \dfrac{\dfrac{\neg\neg(q \wedge r)}{q \wedge r}\ \neg\neg e}{r}\ \wedge e_2}{\neg\neg p \wedge r}\ \wedge i$$

$\square$

# Examples

## Example

Prove $p, \neg\neg(q \wedge r) \vdash \neg\neg p \wedge r$.

## Proof.

We are looking for a proof like:

| | | |
|---|---|---|
| 1 | $p$ | premise |
| 2 | $\neg\neg(q \wedge r)$ | premise |
| 3 | $\neg\neg p$ | $\neg\neg i$ 1 |
| 4 | $q \wedge r$ | $\neg\neg e$ 2 |
| 5 | $r$ | $\wedge e_2$ 4 |
| 6 | $\neg\neg p \wedge r$ | $\wedge i$ 3, 5 |

□

# Proof Rules for Natural Deduction – Implication

- Suppose we want to prove $\psi$ from proofs for $\phi$ and $\phi \implies \psi$. What do we do?
  - We just put the two proofs for $\phi$ and $\phi \implies \psi$ together.
- Here is the proof rule:

$$\frac{\phi \quad \phi \implies \psi}{\psi} \implies e$$

- This proof rule is also called *modus ponens*.
- Here is another proof rule related to implication:

$$\frac{\phi \implies \psi \quad \neg\psi}{\neg\phi}\ MT$$

- This proof rule is called *modus tollens*.

# Example

## Example

Prove $p \implies (q \implies r), p, \neg r \vdash \neg q$.

## Proof.

| | | |
|---|---|---|
| 1 | $p \implies (q \implies r)$ | premise |
| 2 | $p$ | premise |
| 3 | $\neg r$ | premise |
| 4 | $q \implies r$ | $\implies e$ 2, 1 |
| 5 | $\neg q$ | $MT$ 4, 3 |

$\square$

- Suppose we want to prove $\phi \implies \psi$. What do we do?
  - We assume $\phi$ to prove $\psi$. If succeed, we conclude $\phi \implies \psi$ without any assumption.
  - Note that $\phi$ is added as an assumption and then removed so that $\phi \implies \psi$ does not depend on $\phi$.
- We use "box" to simulate this strategy.
- Here is the proof rule:

$$\frac{\boxed{\begin{array}{c}\phi \\ \vdots \\ \psi\end{array}}}{\phi \implies \psi} \implies i$$

- At any point in a box, you can only use a sentence $\phi$ before that point. Moreover, no box enclosing the occurrence of $\phi$ has been closed.

# Example

## Example

Prove $\neg q \implies \neg p \vdash p \implies \neg\neg q$.

## Proof.

$$\dfrac{\boxed{\dfrac{\neg q \implies \neg p \quad \dfrac{p}{\neg\neg p}\,\neg\neg i}{\neg\neg q}\,MT}}{p \implies \neg\neg q} \implies i$$

| | | |
|---|---|---|
| 1 | $\neg q \implies \neg p$ | premise |
| 2 | $p$ | assumption |
| 3 | $\neg\neg p$ | $\neg\neg i$ 2 |
| 4 | $\neg\neg q$ | $MT$ 1, 3 |
| 5 | $p \implies \neg\neg q$ | $\implies i$ 2-4 |

# Theorems

## Example

Prove $\vdash p \implies p$.

## Proof.

$$\begin{array}{cll} 1 & \boxed{p \quad \quad \quad \text{assumption}} & \\ 2 & p \implies p & \implies i\ 1 - 1 \end{array}$$

$\square$

In the box, we have $\phi \equiv \psi \equiv p$.

## Definition

A sentence $\phi$ such that $\vdash \phi$ is called a theorem.

# Examples

## Example

Prove $p \wedge q \implies r \vdash p \implies (q \implies r)$.

## Proof.

| | | |
|---|---|---|
| 1 | $p \wedge q \implies r$ | premise |
| 2 | $p$ | assumption |
| 3 | $q$ | assumption |
| 4 | $p \wedge q$ | $\wedge i$ 2, 3 |
| 5 | $r$ | $\implies e$ 4, 1 |
| 6 | $q \implies r$ | $\implies i$ 3-5 |
| 7 | $p \implies (q \implies r)$ | $\implies i$ 2-6 |

$\square$

# Proof Rules for Natural Deduction – Disjunction

- Suppose we want to prove $\phi \vee \psi$. What do we do?
  - We can either prove $\phi$ or $\psi$.
- Here are the proof rules:

$$\frac{\phi}{\phi \vee \psi} \vee i_1 \qquad\qquad \frac{\psi}{\phi \vee \psi} \vee i_2$$

  - Note the symmetry with $\wedge e_1$ and $\wedge e_2$.

$$\frac{\phi \wedge \psi}{\phi} \wedge e_1 \qquad\qquad \frac{\phi \wedge \psi}{\psi} \wedge e_2$$

  - Can we have a corresponding symmetric elimination rule for disjunction? Recall

$$\frac{\phi \quad \psi}{\phi \wedge \psi} \wedge i$$

# Proof Rules for Natural Deduction – Disjunction

- Suppose we want to prove $\chi$ from $\phi \vee \psi$. What do we do?
  - We assume $\phi$ to prove $\chi$ and then assume $\psi$ to prove $\chi$.
  - If both succeed, $\chi$ is proved from $\phi \vee \psi$ without assuming $\phi$ and $\psi$.
- Here is the proof rule:

$$\dfrac{\phi \vee \psi \qquad \boxed{\begin{array}{c}\phi\\ \vdots\\ \chi\end{array}} \qquad \boxed{\begin{array}{c}\psi\\ \vdots\\ \chi\end{array}}}{\chi}\ \vee e$$

- In addition to nested boxes, we may have parallel boxes in our proofs.

# Example

Recall that our syntax does not admit commutativity.

## Example

Prove $p \lor q \vdash q \lor p$.

## Proof.

$$\dfrac{p \lor q \quad \boxed{\dfrac{p}{q \lor p}\ \lor i_2} \quad \boxed{\dfrac{q}{q \lor p}\ \lor i_1}}{q \lor p}\ \lor e$$

| | | | |
|---|---|---|---|
| 1 | $p \lor q$ | premise | |
| 2 | $p$ | assumption | |
| 3 | $q \lor p$ | $\lor i_2$ 2 | |
| 4 | $q$ | assumption | |
| 5 | $q \lor p$ | $\lor i_1$ 4 | |
| 6 | $q \lor p$ | $\lor e$ 1, 2-3, 4-5 | |

□

# Example

## Example

Prove $q \implies r \vdash p \vee q \implies p \vee r$.

## Proof.

| | | | |
|---|---|---|---|
| 1 | $q \implies r$ | premise | |
| 2 | $p \vee q$ | assumption | |
| 3 | $p$ | assumption | |
| 4 | $p \vee r$ | $\vee i_1$ 3 | |
| 5 | $q$ | assumption | |
| 6 | $r$ | $\implies e$ 5, 1 | |
| 7 | $p \vee r$ | $\vee i_2$ 6 | |
| 8 | $p \vee r$ | $\vee e$ 2, 3-4, 5-7 | |
| 9 | $p \vee q \implies p \vee r$ | $\implies i$ 2-8 | |

$\square$

# Example

## Example

Prove $p \wedge (q \vee r) \vdash (p \wedge q) \vee (p \wedge r)$.

## Proof.

| | | |
|---|---|---|
| 1 | $p \wedge (q \vee r)$ | premise |
| 2 | $p$ | $\wedge e_1$ 1 |
| 3 | $q \vee r$ | $\wedge e_2$ 1 |
| 4 | $q$ | assumption |
| 5 | $p \wedge q$ | $\wedge i$ 2, 4 |
| 6 | $(p \wedge q) \vee (p \wedge r)$ | $\vee i_1$ 5 |
| 7 | $r$ | assumption |
| 8 | $p \wedge r$ | $\wedge i$ 2, 7 |
| 9 | $(p \wedge q) \vee (p \wedge r)$ | $\vee i_2$ 8 |
| 10 | $(p \wedge q) \vee (p \wedge r)$ | $\vee e$ 3, 4-6, 7-9 |

$\square$

# Example

## Example

Prove $(p \land q) \lor (p \land r) \vdash p \land (q \lor r)$.

## Proof.

| | | |
|---|---|---|
| 1 | $(p \land q) \lor (p \land r)$ | premise |
| 2 | $p \land q$ | assumption |
| 3 | $p$ | $\land e_1$ 2 |
| 4 | $q$ | $\land e_2$ 2 |
| 5 | $q \lor r$ | $\lor i_1$ 4 |
| 6 | $p \land (q \lor r)$ | $\land i$ 3, 5 |
| 7 | $p \land r$ | assumption |
| 8 | $p$ | $\land e_1$ 7 |
| 9 | $r$ | $\land e_2$ 7 |
| 10 | $q \lor r$ | $\lor i_2$ 9 |
| 11 | $p \land (q \lor r)$ | $\land i$ 8, 10 |
| 12 | $p \land (q \lor r)$ | $\lor e$ 1, 2-6, 7-11 |

# Contradiction

## Definition

Contradictions are sentences of the form $\phi \wedge \neg\phi$ or $\neg\phi \wedge \phi$.

- Examples:
  - $p \wedge \neg p$, $\neg(p \vee q \implies r) \wedge (p \vee q \implies r)$.
- Logically, any sentence can be proved from a contradiction.
  - If $0 = 1$, then $100 \neq 100$.
- Particularly, if $\phi$ and $\psi$ are contradictions, we have $\phi \dashv\vdash \psi$.
  - $\phi \dashv\vdash \psi$ means $\phi \vdash \psi$ and $\psi \vdash \phi$ (called provably equivalent).
- Since all contradictions are equivalent, we will use the symbol $\bot$ (called "bottom") for them.
- We are now ready to discuss proof rules for negation.

# Proof Rules for Natural Deduction – Negation

- Since any sentence can be proved from a contradiction, we have

$$\frac{\bot}{\phi}\ \bot e$$

- When both $\phi$ and $\neg\phi$ are proved, we have a contradiction.

$$\frac{\phi \quad \neg\phi}{\bot}\ \neg e$$

    - The proof rule could be called $\bot i$. We use $\neg e$ because it eliminates a negation.

# Example

## Example

Prove $\neg p \vee q \vdash p \implies q$.

## Proof.

| | | | |
|---|---|---|---|
| 1 | $\neg p \vee q$ | premise | |
| 2 | $\neg p$ | assumption | |
| 3 | $p$ | assumption | |
| 4 | $\perp$ | $\neg e$ 3, 2 | |
| 5 | $q$ | $\perp e$ 4 | |
| 6 | $p \implies q$ | $\implies i$ 3-5 | |
| 7 | $q$ | assumption | |
| 8 | $p$ | assumption | |
| 9 | $q$ | copy 7 | |
| 10 | $p \implies q$ | $\implies i$ 8-9 | |
| 11 | $p \implies q$ | $\vee e$ 1, 2-6, 7-10 | |

# Proof Rules for Natural Deduction – Negation

- Suppose we want to prove $\neg\phi$. What do we do?
  - We assume $\phi$ and try to prove a contradiction. If succeed, we prove $\neg\phi$.
- Here is the proof rule:

$$\frac{\boxed{\begin{array}{c}\phi\\ \vdots\\ \bot\end{array}}}{\neg\phi}\ \neg i$$

# Example

## Example

Prove $p \implies q, p \implies \neg q \vdash \neg p$.

## Proof.

| | | | |
|---|---|---|---|
| 1 | $p \implies q$ | premise | |
| 2 | $p \implies \neg q$ | premise | |
| 3 | $p$ | assumption | ⌉ |
| 4 | $q$ | $\implies e$ 3, 1 | \| |
| 5 | $\neg q$ | $\implies e$ 3, 2 | \| |
| 6 | $\bot$ | $\neg e$ 4, 5 | ⌋ |
| 7 | $\neg p$ | $\neg i$ 3-6 | |

□

**Example**

Prove $p \land \neg q \implies r, \neg r, p \vdash q$.

**Proof.**

| | | | |
|---|---|---|---|
| 1 | $p \land \neg q \implies r$ | premise | |
| 2 | $\neg r$ | premise | |
| 3 | $p$ | premise | |
| 4 | $\neg q$ | assumption | ⌉ |
| 5 | $p \land \neg q$ | $\land i$ 3, 4 | \| |
| 6 | $r$ | $\implies e$ 5, 1 | \| |
| 7 | $\bot$ | $\neg e$ 6, 2 | ⌋ |
| 8 | $\neg\neg q$ | $\neg i$ 4-7 | |
| 9 | $q$ | $\neg\neg e$ 8 | |

□

# Derived Rules

- Some rules can actually be derived from others.

**Examples**

Prove $p \implies q, \neg q \vdash \neg p$ (modus tollens).

**Proof.**

| | | | |
|---|---|---|---|
| 1 | $p \implies q$ | premise | |
| 2 | $\neg q$ | premise | |
| 3 | $p$ | assumption | ⌉ |
| 4 | $q$ | $\implies e$ 3, 1 | \| |
| 5 | $\bot$ | $\neg e$ 4, 2 | ⌋ |
| 6 | $\neg p$ | $\neg i$ 3-5 | |

□

# Derived Rules

**Examples**

Prove $p \vdash \neg\neg p$ $(\neg\neg i)$

**Proof.**

| | | | |
|---|---|---|---|
| 1 | $p$ | premise | |
| 2 | $\neg p$ | assumption | ] |
| 3 | $\bot$ | $\neg e$ 1, 2 | ] |
| 4 | $\neg\neg p$ | $\neg i$ 2-3 | |

$\square$

- These rules can be replaced by their proofs and are not necessary.
  - They are just macros to help us write shorter proofs.

# Reductio ad absurdum (RAA)

## Example

Prove $\neg p \implies \bot \vdash p$ (RAA).

## Proof.

| | | | |
|---|---|---|---|
| 1 | $\neg p \implies \bot$ | premise | |
| 2 | $\neg p$ | assumption | ⌉ |
| 3 | $\bot$ | $\implies e$ 2, 1 | ⌋ |
| 4 | $\neg\neg p$ | $\neg i$ 2-3 | |
| 5 | $p$ | $\neg\neg e$ 4 | |

$\square$

# Tertium non datur, Law of the Excluded Middle (LEM)

## Example

Prove $\vdash p \lor \neg p$.

## Proof.

| | | |
|---|---|---|
| 1 | $\neg(p \lor \neg p)$ | assumption |
| 2 | $p$ | assumption |
| 3 | $p \lor \neg p$ | $\lor i_1$ 2 |
| 4 | $\bot$ | $\neg e$ 3, 1 |
| 5 | $\neg p$ | $\neg i$ 2-4 |
| 6 | $p \lor \neg p$ | $\lor i_2$ 5 |
| 7 | $\bot$ | $\neg e$ 6, 1 |
| 8 | $\neg\neg(p \lor \neg p)$ | $\neg i$ 1-7 |
| 9 | $p \lor \neg p$ | $\neg\neg e$ 8 |

□

# Proof Rules for Natural Deduction (Summary)

Conjunction ($\wedge$)

$$\frac{\phi \quad \psi}{\phi \wedge \psi} \wedge i \qquad \frac{\phi \wedge \psi}{\phi} \wedge e_1 \quad \frac{\phi \wedge \psi}{\psi} \wedge e_2$$

Disjunction ($\vee$)

$$\frac{\phi}{\phi \vee \psi} \vee i_1 \quad \frac{\psi}{\phi \vee \psi} \vee i_2 \qquad \frac{\phi \vee \psi \quad \boxed{\begin{array}{c}\phi \\ \vdots \\ \chi\end{array}} \quad \boxed{\begin{array}{c}\psi \\ \vdots \\ \chi\end{array}}}{\chi} \vee e$$

Implication ( $\implies$ )

$$\frac{\boxed{\begin{array}{c}\phi \\ \vdots \\ \psi\end{array}}}{\phi \implies \psi} \implies i \qquad \frac{\phi \quad \phi \implies \psi}{\psi} \implies e$$

# Proof Rules for Natural Deduction (Summary)

Negation ($\neg$)

$$\frac{\boxed{\begin{array}{c}\phi \\ \vdots \\ \bot\end{array}}}{\neg\phi}\ \neg i \qquad\qquad \frac{\phi \quad \neg\phi}{\bot}\ \neg e$$

Contradiction ($\bot$)

(no introduction rule)

$$\frac{\bot}{\phi}\ \bot e$$

Double negation ($\neg\neg$)

(no introduction rule)

$$\frac{\neg\neg\phi}{\phi}\ \neg\neg e$$

# Useful Derived Proof Rules

$$\frac{\phi \implies \psi \quad \neg\psi}{\neg\phi}\ MT \qquad \frac{\phi}{\neg\neg\phi}\ \neg\neg i$$

$$\frac{\boxed{\begin{array}{c}\neg\phi\\ \vdots\\ \bot\end{array}}}{\phi}\ RAA \qquad \boxed{\frac{}{\phi \vee \neg\phi}\ LEM}$$

# Provable Equivalence

- Recall $p \dashv\vdash q$ means $p \vdash q$ and $q \vdash p$.
- Here are some provably equivalent sentences:

$$
\begin{array}{rcl}
\neg(p \wedge q) & \dashv\vdash & \neg q \vee \neg p \\
\neg(p \vee q) & \dashv\vdash & \neg q \wedge \neg p \\
p \implies q & \dashv\vdash & \neg q \implies \neg p \\
p \implies q & \dashv\vdash & \neg p \vee q \\
p \wedge q \implies p & \dashv\vdash & r \vee \neg r \\
p \wedge q \implies r & \dashv\vdash & p \implies (q \implies r)
\end{array}
$$

- Try to prove them.

# Proof by Contradiction

- Although it is very useful, the proof rule RAA is a bit puzzling.

$$\frac{\boxed{\begin{array}{c}\neg\phi \\ \vdots \\ \bot\end{array}}}{\phi}\ RAA$$

- Instead of proving $\phi$ directly, the proof rule allows indirect proofs.
  - If $\neg\phi$ leads to a contradiction, then $\phi$ must hold.
- Note that indirect proofs are not "constructive."
  - We do not show why $\phi$ holds; we only know $\neg\phi$ is impossible.
- In early 20th century, some logicians and mathematicians chose not to prove indirectly. They are <u>intuitionistic</u> logicians or mathematicians.
- For the same reason, intuitionists also reject

$$\frac{}{\phi \vee \neg\phi}\ LEM \qquad\qquad \frac{\neg\neg\phi}{\phi}\ \neg\neg e$$

# Proof by Contradiction

**Theorem**

*There are $a, b \in \mathbb{R} \setminus \mathbb{Q}$ such that $a^b \in \mathbb{Q}$.*

**Proof.**

Let $b = \sqrt{2}$. There are two cases:

- If $b^b \in \mathbb{Q}$, we are done since $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.
- If $b^b \notin \mathbb{Q}$, choose $a = b^b = \sqrt{2}^{\sqrt{2}}$. Then $a^b = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2$. Since $\sqrt{2}^{\sqrt{2}}, \sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$, we are done.

$\square$

- An intuitionist would criticize the proof since it does not tell us what $a, b$ give $a^b \in \mathbb{Q}$.
  - We know $(a, b)$ is either $(\sqrt{2}, \sqrt{2})$ or $(\sqrt{2}^{\sqrt{2}}, \sqrt{2})$.

# Outline

# Well-Formedness

## Definition

A well-formed formula is constructed by applying the following rules finitely many times:

- atom: Every propositional atom $p, q, r, \ldots$ is a well-formed formula;
- $\neg$: If $\phi$ is a well-formed formula, so is $(\neg\phi)$;
- $\wedge$: If $\phi$ and $\psi$ are well-formed formulae, so is $(\phi \wedge \psi)$;
- $\vee$: If $\phi$ and $\psi$ are well-formed formulae, so is $(\phi \vee \psi)$;
- $\implies$: If $\phi$ and $\psi$ are well-formed formulae, so is $(\phi \implies \psi)$.

- More compactly, well-formed formulae are defined by the following grammar in Backus Naur form (BNF):

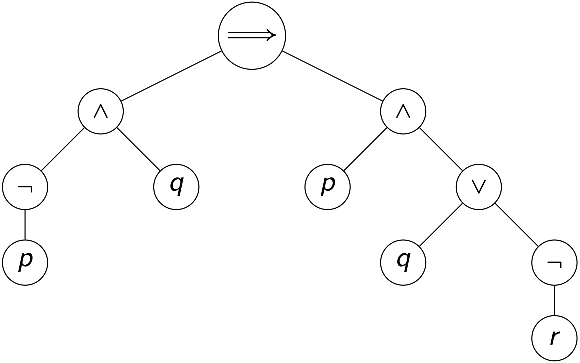
$$\phi ::= p \mid (\neg\phi) \mid (\phi \wedge \phi) \mid (\phi \vee \phi) \mid (\phi \implies \phi)$$

# Inversion Principle

- How do we check if $(((\neg p) \wedge q) \implies (p \wedge (q \vee (\neg r))))$ is well-formed?
- Although a well-formed formula needs five grammar rules to construct, the construction process can always be inverted.
  - This is called inversion principle.
- To show $(((\neg p) \wedge q) \implies (p \wedge (q \vee (\neg r))))$ is well-formed, we need to show both $((\neg p) \wedge q)$ and $(p \wedge (q \vee (\neg r)))$ are well-formed.
- To show $((\neg p) \wedge q)$ is well-formed, we need to show both $(\neg p)$ and $q$ are well-formed.
  - $q$ is well-formed since it is an atom.
- To show $(\neg p)$ is well-formed, we need to show $p$ is well-formed.
  - $p$ is well-formed since it is an atom.
- Similarly, we can show $(p \wedge (q \vee (\neg r)))$ is well-formed.

# Parse Tree

- The easiest way to decide whether a formula is well-formed is perhaps by drawing its parse tree.



# Subformulae

- Given a well-formed formula, its subformulae are the well-formed formulae corresponding to its parse tree.
- For instance, the subformulae of the well-formed formulae $(((\neg p) \wedge q) \implies (p \wedge (q \vee (\neg r))))$ are

$$
\begin{array}{l}
p \\
q \\
r \\
(\neg p) \\
(\neg r) \\
((\neg p) \wedge q) \\
(q \vee (\neg r)) \\
(p \wedge (q \vee (\neg r))) \\
(((\neg p) \wedge q) \implies (p \wedge (q \vee (\neg r))))
\end{array}
$$

# Outline

# From $\vdash$ to $\vDash$

- We have developed a calculus to determine whether $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$ is valid.
  - That is, from the premises $\phi_1, \phi_2, \ldots, \phi_n$, we can conclude $\psi$.
  - Our calculus is syntactic. It depends on the syntactic structures of $\phi_1, \phi_2, \ldots, \phi_n$, and $\psi$.
- We will introduce another relation between premises $\phi_1, \phi_2, \ldots, \phi_n$ and a conclusion $\psi$.

$$\phi_1, \phi_2, \ldots, \phi_n \vDash \psi.$$

  - The new relation is defined by 'truth values' of atomic formulae and the semantics of logical connectives.

# Truth Values and Models

**Definition**

The set of truth values is $\{\mathsf{F}, \mathsf{T}\}$ where F represents 'false' and T represents 'true.'

**Definition**

A valuation or model of a formula $\phi$ is an assignment from each proposition atom in $\phi$ to a truth value.

# Truth Values of Formulae

## Definition

Given a valuation of a formula $\phi$, the truth value of $\phi$ is defined inductively by the following truth tables:

| $\phi$ | $\psi$ | $\phi \land \psi$ |
|---|---|---|
| F | F | F |
| F | T | F |
| T | F | F |
| T | T | T |

| $\phi$ | $\psi$ | $\phi \lor \psi$ |
|---|---|---|
| F | F | F |
| F | T | T |
| T | F | T |
| T | T | T |

| $\phi$ | $\psi$ | $\phi \implies \psi$ |
|---|---|---|
| F | F | T |
| F | T | T |
| T | F | F |
| T | T | T |

| $\phi$ | $\neg\phi$ |
|---|---|
| F | T |
| T | F |

| $\top$ |
|---|
| T |

| $\bot$ |
|---|
| F |

# Example

- $\phi \wedge \psi$ is T when $\phi$ and $\psi$ are T.
- $\phi \vee \psi$ is F when $\phi$ or $\psi$ is T. wrong
- $\bot$ is always F; $\top$ is always T.
- $\phi \implies \psi$ is T when $\phi$ "implies" $\psi$.

## Example

Consider the valuation $\{q \mapsto \mathrm{T}, p \mapsto \mathrm{F}, r \mapsto \mathrm{F}\}$ of $(q \wedge p) \implies r$. What is the truth value of $(q \wedge p) \implies r$?

## Proof.

Since the truth values of $q$ and $p$ are T and F respectively, the truth value of $q \wedge p$ is F. Moreover, the truth value of $r$ is F. The truth value of $(q \wedge p) \implies r$ is T. □

# Truth Tables for Formulae

- Given a formula $\phi$ with propositional atoms $p_1, p_2, \ldots, p_n$, we can construct a truth table for $\phi$ by listing $2^n$ valuations of $\phi$.

## Example

Find the truth table for $(p \implies \neg q) \implies (q \vee \neg p)$.

## Proof.

| $p$ | $q$ | $\neg p$ | $\neg q$ | $p \implies \neg q$ | $q \vee \neg p$ | $(p \implies \neg q) \implies (q \vee \neg p)$ |
|---|---|---|---|---|---|---|
| F | F | T | T | T | T | T |
| F | T | T | F | T | T | T |
| T | F | F | T | T | F | F |
| T | T | F | F | F | T | T |

$\square$

# Outline

# Validity of Sequent Revisited

- Informally $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$ is valid if we can derive $\psi$ with assumptions $\phi_1, \phi_2, \ldots, \phi_n$.
  - We have formalized "deriving $\psi$ with assumptions $\phi_1, \phi_2, \ldots, \phi_n$" by "constructing a proof in a formal calculus."
- We can give another interpretation by valuations and truth values.
- Consider a valuation $\nu$ over all propositional atoms in $\phi_1, \phi_2, \ldots, \phi_n, \psi$.
  - By "assumptions $\phi_1, \phi_2, \ldots, \phi_n$," we mean "$\phi_1, \phi_2, \ldots, \phi_n$ are T under the valuation $\nu$.
  - By "deriving $\psi$,", we mean $\psi$ is also T under the valuation $\nu$.
- Hence, "we can derive $\psi$ with assumptions $\phi_1, \phi_2, \ldots, \phi_n$" actually means "if $\phi_1, \phi_2, \ldots, \phi_n$ are T under a valuation, then $\psi$ must be T under the same valuation.

# Semantic Entailment

## Definition

We say

$$\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$$

holds if for every valuations where $\phi_1, \phi_2, \ldots, \phi_n$ are T, $\psi$ is also T. In this case, we also say $\phi_1, \phi_2, \ldots, \phi_n$ semantically entail $\psi$.

- Examples
  - $p \wedge q \vDash p$. For every valuation where $p \wedge q$ is T, $p$ must be T. Hence $p \wedge q \vDash p$.
  - $p \vee q \nvDash q$. Consider the valuation $\{p \mapsto \mathrm{T}, q \mapsto \mathrm{F}\}$. We have $p \vee q$ is T but $q$ is F. Hence $p \vee q \nvDash q$.
  - $\neg p, p \vee q \vDash q$. Consider any valuation where $\neg p$ and $p \vee q$ are T. Since $\neg p$ is T, $p$ must be F under the valuation. Since $p$ is F and $p \vee q$ is T, $q$ must be T under the valuation. Hence $\neg p, p \vee q \vDash q$.
- The validity of $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$ is defined by syntactic calculus. $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$ is defined by truth tables. Do these two relations coincide?

# Soundness Theorem for Propositional Logic

## Theorem (Soundness)

*Let $\phi_1, \phi_2, \ldots, \phi_n$ and $\psi$ be propositional logic formulae. If $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$ is valid, then $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$ holds.*

## Proof.

Consider the assertion $M(k)$:

"For all sequents $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi (n \geq 0)$ that have a proof of length $k$, then $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$ holds."

$k = 1$. The only possible proof is of the form

$$1 \quad \phi \quad \text{premise}$$

This is the proof of $\phi \vdash \phi$. For every valuation such that $\phi$ is T, $\phi$ must be T. That is, $\phi \vDash \phi$.

# Soundness Theorem for Propositional Logic

## Proof (cont'd).

Assume $M(i)$ for $i < k$. Consider a proof of the form

$$\begin{array}{lll} 1 & \phi_1 & \text{premise} \\ 2 & \phi_2 & \text{premise} \\ & \vdots & \\ \text{n} & \phi_n & \text{premise} \\ & \vdots & \\ \text{k} & \psi & \text{justification} \end{array}$$

We have the following possible cases for justification:

i $\wedge i$. Then $\psi$ is $\psi_1 \wedge \psi_2$. In order to apply $\wedge i$, $\psi_1$ and $\psi_2$ must appear in the proof. That is, we have $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi_1$ and $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi_2$. By inductive hypothesis, $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi_1$ and $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi_2$. Hence $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi_1 \wedge \psi_2$ (Why?).

# Soundness Theorem for Propositional Logic

## Proof (cont'd).

ii $\vee e$. Recall the proof rule for $\vee e$:

$$\frac{\eta_1 \vee \eta_2 \quad \boxed{\begin{array}{c}\eta_1\\ \vdots\\ \psi\end{array}} \quad \boxed{\begin{array}{c}\eta_2\\ \vdots\\ \psi\end{array}}}{\psi} \vee e$$

In order to apply $\vee e$, $\eta_1 \vee \eta_2$ must appear in the proof. We have $\phi_1, \phi_2, \ldots, \phi_n \vdash \eta_1 \vee \eta_2$. By turning "assumptions" $\eta_1$ and $\eta_2$ to "premises," we obtain proofs for $\phi_1, \phi_2, \ldots, \phi_n, \eta_1 \vdash \psi$ and $\phi_1, \phi_2, \ldots, \phi_n, \eta_2 \vdash \psi$. By inductive hypothesis, $\phi_1, \phi_2, \ldots, \phi_n \vDash \eta_1 \vee \eta_2$, $\phi_1, \phi_2, \ldots, \phi_n, \eta_1 \vDash \psi$, and $\phi_1, \phi_2, \ldots, \phi_n, \eta_2 \vDash \psi$. Consider any valuation such that $\phi_1, \phi_2, \ldots, \phi_n$ evaluates to T. $\eta_1 \vee \eta_2$ must be T. If $\eta_1$ is T under the valuation, $\psi$ is also T (Why?). Similarly for $\eta_2$ is T. Thus $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$.

Proof (cont'd).

iii Other cases are similar. Prove the case of $\Longrightarrow e$ to see if you understand the proof.

□

- The soundness theorem shows that our calculus does not go wrong.
- If there is a proof of a sequent, then the conclusion must be true for all valuations where all premises are true.
- The theorem also allows us to show the non-existence of proofs.
- Given a sequent $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$, how do we prove there is no proof for the sequent?
  - Try to find a valuation where $\phi_1, \phi_2, \ldots, \phi_n$ are T but $\psi$ is F.

# Outline

# Completeness Theorem for Propositional Logic

- "$\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$ is valid" and "$\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$ holds" are very different.
  - "$\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$ is valid" requires proof search (syntax);
  - "$\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$ holds" requires a truth table (semantics).
- If "$\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$ holds" implies "$\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$ is valid," then our natural deduction proof system is complete.
- The natural deduction proof system is both sound and complete. That is

  $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$ is valid iff $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$ holds.

# Completeness Theorem for Propositional Logic

- We will show the natural deduction proof system is complete.
- That is, if $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$ holds, then there is a natural deduction proof for the sequent $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$.
- Assume $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$. We proceed in three steps:
  1. $\vDash \phi_1 \implies (\phi_2 \implies (\ldots(\phi_n \implies \psi)))$ holds;
  2. $\vdash \phi_1 \implies (\phi_2 \implies (\ldots(\phi_n \implies \psi)))$ is valid;
  3. $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$ is valid.

# Completeness Theorem for Propositional Logic (Step 1)

**Lemma**

*If* $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$ *holds, then* $\vDash \phi_1 \implies (\phi_2 \implies (\ldots(\phi_n \implies \psi)))$ *holds.*

**Proof.**

Suppose $\vDash \phi_1 \implies (\phi_2 \implies (\ldots(\phi_n \implies \psi)))$ does not hold. Then there is valuation where $\phi_1, \phi_2, \ldots, \phi_n$ is T but $\psi$ is F. A contradiction to $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$. □

**Definition**

Let $\phi$ be a propositional logic formula. We say $\phi$ is a tautology if $\vDash \phi$.

- A tautology is a propositional logic formula that evaluates to T for all of its valuations.

# Completeness Theorem for Propositional Logic (Step 2)

- Our goal is to show the following theorem:

**Theorem**

*If $\vDash \eta$ holds, then $\vdash \eta$ is valid.*

- Similar to tautologies, we introduce the following definition:

**Definition**

Let $\phi$ be a propositional logic formula. We say $\phi$ is a theorem if $\vdash \phi$.

- Two types of theorems:
  - If $\vdash \phi$, $\phi$ is a theorem proved by the natural deduction proof system.
  - The soundness theorem for propositional logic is another type of theorem proved by mathematical reasoning (less formally).

# Completeness Theorem for Propositional Logic (Step 2)

## Proposition

*Let $\phi$ be a formula with propositional atoms $p_1, p_2, \ldots, p_n$. Let $l$ be a line in $\phi$'s truth table. For all $1 \leq i \leq n$, let $\hat{p}_i$ be $p_i$ if $p_i$ is T in $l$; otherwise $\hat{p}_i$ is $\neg p_i$. Then*

1. $\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_n \vdash \phi$ *is valid if the entry for $\phi$ at $l$ is T;*
2. $\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_n \vdash \neg\phi$ *is valid if the entry for $\phi$ at $l$ is F.*

## Proof.

We prove by induction on the height of the parse tree of $\phi$.

- $\phi$ is a propositional atom $p$. Then $p \vdash p$ or $\neg p \vdash \neg p$ have one-line proof.
- $\phi$ is $\neg\phi_1$.
  - If $\phi$ is T at $l$. Then $\phi_1$ is F. By IH, $\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_n \vdash \neg\phi_1 (\equiv \phi)$.
  - If $\phi$ is F at $l$. Then $\phi_1$ is T. By IH, $\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_n \vdash \phi_1$. Using $\neg\neg i$, we have $\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_n \vdash \neg\neg\phi_1 (\equiv \neg\phi)$.

**Proof (cont'd).**

- $\phi$ is $\phi_1 \implies \phi_2$.
  - If $\phi$ is F at $l$, then $\phi_1$ is T and $\phi_2$ is F at $l$. By IH, $\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_n \vdash \phi_1$ and $\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_n \vdash \neg\phi_2$. Consider

| | | |
|---|---|---|
| 1 | $\phi_1 \implies \phi_2$ | assumption |
| | $\vdots$ | |
| i | $\phi_1$ | IH |
| i + 1 | $\phi_2$ | $\implies e$ i, 1 |
| | $\vdots$ | |
| j | $\neg\phi_2$ | IH |
| j + 1 | $\bot$ | ¬ e i+1, j |
| j + 2 | $\neg(\phi_1 \implies \phi_2)$ | ¬ i 1-(j+1) |

# Completeness Theorem for Propositional Logic (Step 2)

## Proof (cont'd).

- $\phi$ is $\phi_1 \implies \phi_2$.
  - If $\phi$ is T at $l$, we have three subcases. Consider the case where $\phi_1$ and $\phi_2$ are F at $l$. Then

| | | |
|---|---|---|
| 1 | $\phi_1$ | assumption |
| | $\vdots$ | |
| i | $\neg\phi_1$ | IH |
| i + 1 | $\bot$ | $\neg$ e 1, i |
| i + 2 | $\phi_2$ | $\bot$ e (i+1) |
| i + 3 | $\phi_1 \implies \phi_2$ | $\implies$ i 1-(i+2) |

The other two subcases are simple exercises.

# Completeness Theorem for Propositional Logic (Step 2)

## Proof (cont'd).

- $\phi$ is $\phi_1 \land \phi_2$.
  - If $\phi$ is T at $l$, then $\phi_1$ and $\phi_2$ are T at $l$. By IH, we have $\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_n \vdash \phi_1$ and $\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_n \vdash \phi_2$. Using $\land$ i, we have $\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_n \vdash \phi_1 \land \phi_2$.
  - If $\phi$ is F at $l$, there are three subcases. Consider the subcase where $\phi_1$ and $\phi_2$ are F at $l$. Then

| | | |
|---|---|---|
| 1 | $\phi_1 \land \phi_2$ | assumption |
| 2 | $\phi_1$ | $\land$ e$_1$ 1 |
| | $\vdots$ | |
| i | $\neg\phi_1$ | IH |
| i + 1 | $\bot$ | $\neg$ e 2, i |
| i + 2 | $\neg(\phi_1 \land \phi_2)$ | $\neg$ i 1-(i+1) |

The other two subcases are simple exercises.

**Proof.**

- $\phi$ is $\phi_1 \lor \phi_2$.
  - If $\phi$ is F at $l$, then $\phi_1$ and $\phi_2$ are F at $l$. Then

| | | |
|---|---|---|
| 1 | $\phi_1 \lor \phi_2$ | assumption |
| 2 | $\phi_1$ | assumption |
| | $\vdots$ | |
| i | $\neg\phi_1$ | IH |
| i + 1 | $\bot$ | $\neg$ e 2, i |
| i + 2 | $\phi_2$ | assumption |
| | $\vdots$ | |
| j | $\neg\phi_2$ | IH |
| j + 1 | $\bot$ | $\neg$ e i+2, j |
| j + 2 | $\bot$ | $\lor$ e 2-(i+1), (i+2)-(j+1) |
| j + 3 | $\neg(\phi_1 \lor \phi_2)$ | $\neg$i 1-(j+2) |

  - If $\phi$ is T at $l$, there are three subcases. All of them are simple exercises.

□

# Completeness Theorem for Propositional Logic (Step 2)

**Theorem**

*If $\phi$ is a tautology, then $\phi$ is a theorem.*

**Proof.**

Let $\phi$ have propositional atoms $p_1, p_2, \ldots, p_n$. Since $\phi$ is a tautology, each line in $\phi$'s truth table is T. By the above proposition, we have the following $2^n$ proofs for $\phi$:

$$
\begin{array}{rcl}
\neg p_1, \neg p_2, \ldots, \neg p_n & \vdash & \phi \\
p_1, \neg p_2, \ldots, \neg p_n & \vdash & \phi \\
\neg p_1, p_2, \ldots, \neg p_n & \vdash & \phi \\
& \vdots & \\
p_1, p_2, \ldots, p_n & \vdash & \phi
\end{array}
$$

We apply the rule LEM and the $\vee$e rule to obtain a proof for $\vdash \phi$. (See the following example.) $\square$

# Completeness Theorem for Propositional Logic (Step 2)

## Example

Observe that $\vDash p \implies (q \implies p)$. Prove $\vdash p \implies (q \implies p)$.

## Proof.

| | | |
|---|---|---|
| 1 | $p \vee \neg p$ | LEM |
| 2 | $p$ | assumption |
| 3 | $q \vee \neg q$ | LEM |
| 4 | $q$ | assumption |
| | $\vdots$ | |
| i | $p \implies (q \implies p)$ | $p, q \vdash p \implies (q \implies p)$ |
| i + 1 | $\neg q$ | assumption |
| | $\vdots$ | |
| j | $p \implies (q \implies p)$ | $p, \neg q \vdash p \implies (q \implies p)$ |
| j + 1 | $p \implies (q \implies p)$ | $\vee$e 3, 4-i, (i+1)-j |
| j + 2 | $\neg p$ | assumption |
| j + 3 | $q \vee \neg q$ | LEM |
| j + 4 | $q$ | assumption |
| | $\vdots$ | |
| k | $p \implies (q \implies p)$ | $\neg p, q \vdash p \implies (q \implies p)$ |
| k + 1 | $\neg q$ | assumption |
| | $\vdots$ | |
| l | $p \implies (q \implies p)$ | $\neg p, \neg q \vdash p \implies (q \implies p)$ |
| l + 1 | $p \implies (q \implies p)$ | $\vee$e (j+3), (j+4)-k, (k+1)-l |
| l + 2 | $p \implies (q \implies p)$ | $\vee$e 1, 2-(j+1), (j+2)-(l+1) |

□

# Completeness Theorem for Propositional Logic (Step 3)

## Lemma

*If* $\phi_1 \implies (\phi_2 \implies (\cdots(\phi_n \implies \psi)))$ *is a theorem, then* $\phi_1, \phi_2, \ldots, \phi_n \vdash \psi$ *is valid.*

## Proof.

Consider

| | | |
|---|---|---|
| 1 | $\phi_1$ | premise |
| 2 | $\phi_2$ | premise |
| | $\vdots$ | |
| n | $\phi_n$ | premise |
| | $\vdots$ | |
| i | $\phi_1 \implies (\phi_2 \implies (\cdots(\phi_n \implies \psi)))$ | theorem |
| i + 1 | $\phi_2 \implies (\cdots(\phi_n \implies \psi))$ | $\implies$e 1, i |
| i + 2 | $\phi_3 \implies (\cdots(\phi_n \implies \psi))$ | $\implies$e 2, (i+1) |
| | $\vdots$ | |
| i + n - 1 | $\phi_n \implies \psi$ | $\implies$e (n-1), (i+n-2) |
| i + n | $\psi$ | $\implies$e n, (i+n-1) |

□

# Outline

1. Introduction
2. Natural Deduction
3. Propositional logic as a formal language
4. Semantics of propositional logic
   - The meaning of logical connectives
   - Soundness of Propositional Logic
   - Completeness of Propositional Logic
5. Normal Forms
   - Semantic equivalence, satisfiability, and validity
   - Conjunctive normals forms and validity
   - Horn clauses and satisfiability
6. SAT Solvers

# Semantically Equivalence and Validity

- Consider two formulae $\phi_1 \land \phi_2$ and $\phi_2 \land \phi_1$.
- Intuitively, $\phi_1 \land \phi_2$ and $\phi_2 \land \phi_1$ should have the same "meaning."
- More formally, two formulae $\phi$ and $\psi$ have the same meaning if their truth tables coincide.

## Definition

Let $\phi$ and $\psi$ be propositional logic formulae. $\phi$ and $\psi$ are semantically equivalent (written $\phi \equiv \psi$) if both $\phi \vDash \psi$ and $\psi \vDash \phi$ hold.

- Examples

$$
\begin{array}{rcl}
p \implies q & \equiv & \neg q \implies \neg p \\
p \land q \implies p & \equiv & r \lor \neg r
\end{array}
\qquad
\begin{array}{rcl}
p \implies q & \equiv & \neg p \lor q \\
p \land q \implies r & \equiv & p \implies (q \implies r)
\end{array}
$$

- A formula $\phi$ is valid if it is a tautology.

## Definition

Let $\phi$ be a propositional logic formula. $\phi$ is valid if $\vDash \phi$.

**Lemma**

*Let $\phi_1, \phi_2, \ldots, \phi_n, \psi$ be propositional logic formulae. $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$ iff $\vDash \phi_1 \implies (\phi_2 \implies \cdots \implies (\phi_n \implies \psi))$.*

**Proof.**

Suppose $\vDash \phi_1 \implies (\phi_2 \implies \cdots \implies (\phi_n \implies \psi))$ Consider any valuation. If $\phi_1, \phi_2, \ldots, \phi_n$ evaluate to T under the valuation, $\phi$ must evaluate to T since $\vDash \phi_1 \implies (\phi_2 \implies \cdots \implies (\phi_n \implies \psi))$. Hence $\phi_1, \phi_2, \ldots, \phi_n \vDash \psi$.

The other direction is proved in Step 1 of the completeness theorem. □

# Conjunctive Normal Form (CNF)

**Definition**

A literal $L$ is either an atom $p$ or its negation $\neg p$. A clause $D$ is a disjunction of literals. A formula $C$ is in conjunctive normal form (CNF) if it is a conjunction of clauses.

$$
\begin{array}{rcl}
L & ::= & p \mid \neg p \\
D & ::= & L \mid L \vee D \\
C & ::= & D \mid D \wedge C
\end{array}
$$

- Examples: $(\neg q \vee p \vee r) \wedge (\neg p \vee r) \wedge q$, $(p \vee r) \wedge (\neg p \vee r) \wedge (p \vee \neg r)$

# Validity of CNF Formulae

## Lemma

*A clause $L_1 \vee L_2 \vee \cdots \vee L_m$ is valid iff there is a propositional atom $p$ such that $L_i$ is $p$ and $L_j$ is $\neg p$ for some $1 \leq i, j \leq m$.*

## Proof.

Without loss of generality, assume $L_1 = p$ and $L_2 = \neg p$. Then $p \vee \neg p \vee L_3 \vee \cdots \vee L_m$ evaluates to T for any valuation. The clause is valid. Conversely, consider the valuation where all literals evaluate to F. This is possible since every literal $L_i$ has no negation in the clause. The clause evaluates to F under the valuation. □

- Examples:
  - $p \vee q \vee q \vee \neg p \vee r$ is valid;
  - $p \vee \neg q \vee r \vee \neg q$ is not valid (consider $\{p \mapsto \mathrm{F}, q \mapsto \mathrm{T}, r \mapsto \mathrm{F}\}$).
- For any propositional logic formula $\phi$ in CNF, the validity of $\phi$ can be checked in linear time.

# Satisfiability of CNF Formulae

## Definition

Let $\phi$ be a propositional logic formula. $\phi$ is satisfiable if it evaluates to T under some valuation.

- Example: $p \vee q \implies p$ is satisfiable (consider $\{p \mapsto \mathrm{T}, q \mapsto \mathrm{T}\}$); it is not valid (consider $\{p \mapsto \mathrm{F}, q \mapsto \mathrm{T}\}$).

## Proposition

*Let $\phi$ be a propositional logic formula. $\phi$ is satisfiable iff $\neg\phi$ is not valid.*

## Proof.

Suppose $\phi$ evaluates to T under a valuation. Then $\neg\phi$ evaluates to F under the valuation. $\neg\phi$ is not valid.
Conversely, suppose $\neg\phi$ is not valid. Hence $\neg\phi$ evaluates to F under a valuation. Thus $\phi$ evaluates to T under the valuation. $\phi$ is satisfiable. $\square$

# From Truth Tables to Conjunctive Normal Form

- Suppose we have the truth table for a formula $\phi$ with propositional atoms $p_1, p_2, \ldots, p_n$.
- For each line $l$ where $\phi$ evaluates to F, construct a clause $\psi_l$ as follows.
  - $\psi_l = L_{l,1} \vee L_{l,2} \vee \cdots \vee L_{l,n}$ where $L_{l,j} = \neg p_j$ if $p_j$ is T at line $l$; otherwise $L_{l,j} = p_j$.
- Then $\phi \equiv \psi_1 \wedge \psi_2 \wedge \cdots \psi_m$ where $\psi_l$'s are contructed for every line evaluating $\phi$ to F.
- Observe that $\psi_1 \wedge \psi_2 \wedge \cdots \psi_m$ is F iff $\psi_l$ is F for some $1 \leq l \leq m$. $\psi_l = L_{l,1} \vee L_{l,2} \vee \cdots \vee L_{l,n}$ is F iff $L_{l,j}$ is F for every $1 \leq j \leq n$. $L_{l,j}$ is F iff $p_j$ has its truth value at line $l$.
- In other words, $\psi_1 \wedge \psi_2 \wedge \cdots \psi_m$ is F under a valuation iff the valuation evaluates $\phi$ to F in $\phi$'s truth table.

# From Truth Tables to Conjunctive Normal Form

## Example

Translate $p \vee q \implies q \wedge \neg r$ into CNF.

## Proof.

| $p$ | $q$ | $r$ | $p \vee q \implies q \wedge \neg r$ | $p$ | $q$ | $r$ | $p \vee q \implies q \wedge \neg r$ |
|---|---|---|---|---|---|---|---|
| F | F | F | T | T | F | F | F |
| F | F | T | T | T | F | T | F |
| F | T | F | T | T | T | F | T |
| F | T | T | F | T | T | T | F |

| $p$ | $q$ | $r$ | $\psi_l$ | $p$ | $q$ | $r$ | $\psi_l$ |
|---|---|---|---|---|---|---|---|
| F | T | T | $p \vee \neg q \vee \neg r$ | T | F | F | $\neg p \vee q \vee r$ |
| T | F | T | $\neg p \vee q \vee \neg r$ | T | T | T | $\neg p \vee \neg q \vee \neg r$ |

$$p \vee q \implies q \wedge \neg r \equiv (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee \neg r). \qquad \square$$

# Outline

# Validity Checking

- Given a propositional logic formula in conjunctive normal form, we can check the validity of the formula in linear time.
- Recall that a formula is valid iff it is a theorem.
- If we can translate any propositional logic formula into conjunctive normal form, we can check the validity of the formula!
- We know how to translate any logic formula to conjunctive normal form by its truth table.
  - This is not satisfactory. If we have to construct its truth table, we can check validity already.
- We will give an algorithm $\texttt{CNF}(\phi)$ to convert any propositional logic formula into conjunctive normal form without building its truth table.

# From Formula to Conjunctive Normal Form

- Any propositional logic formula can be transformed to conjunctive normal form by the following equivalences:

$$\phi \implies \psi \equiv \neg\phi \lor \psi$$

$$\neg(\phi \land \psi) \equiv \neg\phi \lor \neg\psi \qquad \neg(\phi \lor \psi) \equiv \neg\phi \land \neg\psi$$

$$\phi \land (\psi_1 \lor \psi_2) \equiv (\phi \land \psi_1) \lor (\phi \land \psi_2)$$

$$\phi \lor (\psi_1 \land \psi_2) \equiv (\phi \lor \psi_1) \land (\phi \lor \psi_2)$$

- The algorithm $\texttt{CNF}(\phi)$ hence consists of three steps:
  - Remove every implication ( $\implies$ ) from $\phi$ (Algorithm $\texttt{IMPL\_FREE}(\phi)$);
  - Push every negation ($\neg$) to literals (Algorithm $\texttt{NNF}(\phi)$);
  - Apply law of distribution (Algorithm $\texttt{CNF}(\phi)$).

# Algorithm IMPL_FREE($\phi$)

**Input:** $\phi$ : a logic formula
**Output:** $\phi'$ : all implications ($\implies$) in $\phi'$ are removed and $\phi' \equiv \phi$
**switch** $\underline{\phi}$ **do**

- **case** $\underline{\phi \text{ is a literal:}}$ **do return** $\underline{\phi}$;
- **case** $\underline{\phi \text{ is } \neg\phi_1:}$ **do return** $\underline{\neg\mathtt{IMPL\_FREE}(\phi_1)}$;
- **case** $\underline{\phi \text{ is } \phi_1 \wedge \phi_2:}$ **do return** $\underline{\mathtt{IMPL\_FREE}(\phi_1) \wedge \mathtt{IMPL\_FREE}(\phi_2)}$;
- **case** $\underline{\phi \text{ is } \phi_1 \vee \phi_2:}$ **do return** $\underline{\mathtt{IMPL\_FREE}(\phi_1) \vee \mathtt{IMPL\_FREE}(\phi_2)}$;
- **case** $\underline{\phi \text{ is } \phi_1 \implies \phi_2:}$ **do return** $\underline{\mathtt{IMPL\_FREE}(\neg\phi_1 \vee \phi_2)}$;
- **otherwise do** `assert(0)`;

**Algorithm 1:** IMPL_FREE($\phi$)

# Algorithm NNF($\phi$)

**Input:** $\phi$ : a logic formula without implication ( $\Longrightarrow$ )
**Output:** $\phi'$ : only propositional atoms in $\phi'$ are negated and $\phi' \equiv \phi$
**switch** $\phi$ **do**
- **case** $\phi$ is a literal: **do return** $\phi$;
- **case** $\phi$ is $\neg\neg\phi_1$: **do return** $\mathtt{NNF}(\phi_1)$;
- **case** $\phi$ is $\phi_1 \land \phi_2$: **do return** $\mathtt{NNF}(\phi_1) \land \mathtt{NNF}(\phi_2)$;
- **case** $\phi$ is $\phi_1 \lor \phi_2$: **do return** $\mathtt{NNF}(\phi_1) \lor \mathtt{NNF}(\phi_2)$;
- **case** $\phi$ is $\neg(\phi_1 \land \phi_2)$: **do return** $\mathtt{NNF}(\neg\phi_1 \lor \neg\phi_2)$;
- **case** $\phi$ is $\neg(\phi_1 \lor \phi_2)$: **do return** $\mathtt{NNF}(\neg\phi_1 \land \neg\phi_2)$;
- **otherwise do** $\mathtt{assert}(0)$;

**Algorithm 2:** $\mathtt{NNF}(\phi)$

## Definition

Let $\phi$ be a propositional logic formula. If only propositional atoms in $\phi$ are negated, $\phi$ is in negation normal form.

**Input:** $\phi$ : an NNF formula without implication ( $\implies$ )
**Output:** $\phi'$ : $\phi'$ is in CNF and $\phi' \equiv \phi$
**switch** $\underline{\phi}$ **do**
  **case** $\underline{\phi \text{ is a literal:}}$ **do return** $\underline{\phi}$;
  **case** $\underline{\phi \text{ is } \phi_1 \land \phi_2\text{:}}$ **do return** $\underline{\mathtt{CNF}(\phi_1) \land \mathtt{CNF}(\phi_2)}$;
  **case** $\underline{\phi \text{ is } \phi_1 \lor \phi_2\text{:}}$ **do return** $\underline{\mathtt{DISTR}(\mathtt{CNF}(\phi_1), \mathtt{CNF}(\phi_2))}$;

**Algorithm 3:** $\mathtt{CNF}(\phi)$

**Input:** $\eta_1, \eta_2$ : $\eta_1, \eta_2$ are in CNF
**Output:** $\phi'$ : $\phi'$ is in CNF and $\phi' \equiv \eta_1 \lor \eta_2$
**if** $\underline{\eta_1 \text{ is } \eta_{11} \land \eta_{12}}$ **then return** $\underline{\mathtt{DISTR}(\eta_{11}, \eta_2) \land \mathtt{DISTR}(\eta_{12}, \eta_2)}$ ;
**else if** $\underline{\eta_2 \text{ is } \eta_{21} \land \eta_{22}}$ **then return** $\underline{\mathtt{DISTR}(\eta_1, \eta_{21}) \land \mathtt{DISTR}(\eta_1, \eta_{22})}$ ;
**else return** $\underline{\eta_1 \lor \eta_2}$ ;

**Algorithm 4:** $\mathtt{DISTR}(\eta_1, \eta_2)$

# Satisfiability of Propositional Logic Formulae

- Let $\phi$ be a propositional logic formula. Consider the following algorithm for checking its satisfiability.
  1. Compute a CNF formula $\psi$ such that $\psi \equiv \neg\phi$.
  2. Check the validity of $\psi$.
  3. Return "$\phi$ is satisfiable" if $\psi$ is not valid; Return "$\phi$ is not satisfiable" if $\psi$ is valid.
- Recall that satisfiability of propositional logic formulae is an NP-complete problem.
- Is the above algorithm in polynomial time? Why?

# Outline

# Horn Clauses

- Given a propositional logic formula in CNF, it is easy to check its validity; it is "hard" to check its satisfiability.
- We will consider a subclass of CNF formulae whose satisfiability can be checked efficiently.

### Definition

A Horn formula is a propositional logic formula $\phi$ of the following form:

$$
\begin{array}{rcl}
P & ::= & \bot \mid \top \mid p \\
A & ::= & P \mid P \land A \\
C & ::= & A \implies P \\
H & ::= & C \mid C \land H.
\end{array}
$$

A clause of the form $C$ is called a Horn clause.

- Example: $(p \land q \land s \implies \bot) \land (q \land r \implies p) \land (\top \implies s)$
- Nonexample: $(p \land \neg q \land s \implies \bot) \land (q \land r \implies p \land s) \land (p \lor r \implies s)$

# Satisfiability of Horn Formulae

- Consider a Horn clause $P_1 \wedge P_2 \wedge \cdots \wedge P_n \implies Q$.
- If $P_1, P_2, \ldots, P_n$ are assigned to T, then $Q$ must be T; otherwise, $Q$ can be an arbitrary truth value.
- We hence have the following (informal) algorithm:
  1. Mark $\top$ if it occurs in the Horn formula $\phi$;
  2. If there is a Horn clause $P_1 \wedge P_2 \wedge \cdots \wedge P_n \implies Q$ in $\phi$ such that all $P_j$ for $1 \leq j \leq n$ are marked, mark $Q$;
  3. If $\bot$ is marked, print "The Horn formula $\phi$ is unsatisfiable."
  4. Print "The Horn formula $\phi$ is satisfiable."

**Input:** $\phi$: $\phi$ is a Horn formula
**Output:** "unsatisfiable" if $\phi$ is unsatisfiable; otherwise "satisfiable."
mark all occurrences of $\top$ in $\phi$;
**while** there is a Horn clause $P_1 \wedge P_2 \wedge \cdots \wedge P_n \implies Q$ in $\phi$ such that $P_j$ are all marked but $Q$ is not **do**
    mark $Q$;
**if** $\perp$ is marked **then** **return** "unsatisfiable" ;
**else** **return** "satisfiable" ;

**Algorithm 5:** Horn($\phi$)

# Satisfiability of Horn Formulae

**Theorem**

*Let $\phi$ be a Horn formula with $n$ propositional atoms.* $\texttt{Horn}(\phi)$ *runs at most $n+1$ iterations and decides the satisfiability of $\phi$ correctly.*

**Proof.**

At each iteration, an unmarked atom will be marked. Since there are $n$ atoms, there are at most $n+1$ iterations.

By induction on the number of iterations, we show that "all marked $P$ are true for all valuations where $\phi$ evaluates to T." At iteration 0 (before entering the loop), only $\top$ are marked. Clearly, $\top$ must be true for any valuation. At iteration $k+1$, consider a Horn clause $P_1 \wedge P_2 \wedge \cdots \wedge P_n \implies Q$ where $P_1, P_2, \ldots, P_n$ are marked but not $Q$. For a valuation $\nu$ where $\phi$ evaluates to T, $P_1 \wedge P_2 \wedge \cdots \wedge P_n \implies Q$ must evaluate to T. Since $P_1, P_2, \ldots, P_n$ are true in $\nu$ (by IH), $Q$ must be true in $\nu$.

# Satisfiability of Horn Formulae

**Proof (cont'd).**

We now prove `Horn`($\phi$) answers correctly. When `Horn`($\phi$) returns "unsatisfiable," there is a Horn clause $P_1 \land P_2 \land \cdots \land P_n \implies \bot$ where $P_1, P_2, \ldots, P_n$ are all marked. Suppose $\nu$ is a valuation where $\phi$ evaluates to T. Then $P_1, P_2, \ldots, P_n$ must be true in $\nu$. Hence $P_1 \land P_2 \land \cdots \land P_n \implies \bot$ evaluates to F. $\phi$ cannot evaluate to T under $\nu$. A contradiction.

When `Horn`($\phi$) returns "satisfiable," define a valuation $\nu$ where all marked propositional atoms are assigned to T and all unmarked atoms are F. We claim $\phi$ evaluates to T in $\nu$. Suppose not. There is a Horn clause $P_1 \land P_2 \land \cdots P_n \implies Q$ in $\phi$ which evaluates to F under $\nu$. That is, $P_1, P_2, \ldots, P_n$ are T but $Q$ is F under $\nu$. By the definition of $\nu$, $P_1, P_2, \ldots, P_n$ are marked by the algorithm. Hence $Q$ must also be marked by the algorithm. $Q$ cannot be F in $\nu$. A contradiction. □

# Outline

# SAT Solvers

- The satisfiability problem for propositional logic is to decide whether a propositional logic formula $\phi$ is satisfiable.
  - The satisfiability problem for propositional logic is an NP-complete problem (Cook's Theorem).
- Many SAT solvers are available for the problem.
- We will discuss algorithms for the satisfiability problem.
- For this topic, most materials are copied or modified from Prof. Sharad Malik's and Prof. Chung-Yang Huang's lecture notes.

# Equisatisfiable Propositional Logic Formulae

- Let $\phi$ and $\psi$ be propositional logic formulae.
- $\phi$ and $\psi$ are equisatisfiable if

$$\phi \text{ is satisfiable if and only if } \psi \text{ is satisfiable.}$$

- What is the difference between semantic equivalence and equisatisfiability?

# Tseitin Transformation

## Theorem

*For every propositional logic formula $\phi$, there is a propositional logic formula $\psi$ in CNF such that $\phi$ and $\psi$ are equisatisfiable.*

## Proof.

For every subformula $\alpha$ of $\phi$, $x_\alpha$ is $p$ if $\alpha$ is the atomic proposition $p$; $x_\alpha$ is $P_\alpha$ otherwise. For every non-atomic subformula $\alpha$, define $C_\alpha$ as follows.

| $\alpha$ | $C_\alpha$ | Remark |
|---|---|---|
| $\neg\beta$ | $(x_\alpha \vee x_\beta) \wedge (\neg x_\alpha \vee \neg x_\beta)$ | $x_\alpha \Leftrightarrow \neg x_\beta$ |
| $\beta_0 \vee \beta_1$ | $(x_\alpha \vee \neg x_{\beta_0}) \wedge (x_\alpha \vee \neg x_{\beta_1}) \wedge (\neg x_\alpha \vee x_{\beta_0} \vee x_{\beta_1})$ | $x_\alpha \Leftrightarrow x_{\beta_0} \vee x_{\beta_1}$ |
| $\beta_0 \wedge \beta_1$ | $(\neg x_\alpha \vee x_{\beta_0}) \wedge (\neg x_\alpha \vee x_{\beta_1}) \wedge (x_\alpha \vee \neg x_{\beta_0} \vee \neg x_{\beta_1})$ | $x_\alpha \Leftrightarrow x_{\beta_0} \wedge x_{\beta_1}$ |

Let $\psi = x_\phi \wedge \bigwedge\{C_\alpha : \alpha \text{ is a non-atomic subformula of } \phi\}$. Then $\phi$ and $\psi$ are equisatisfiable. $\square$

# Example

## Example

Transform $\phi = \neg(p \wedge \neg q)$ into an equisatisfiable propositional logic formula in CNF.

## Proof.

$\neg q, p \wedge \neg q, \phi$ are non-atomic subformulae of $\phi$.

$$
\begin{array}{rcl}
C_{\neg q} & \triangleq & (P_{\neg q} \vee q) \wedge (\neg P_{\neg q} \vee \neg q) \\
C_{p \wedge \neg q} & \triangleq & (\neg P_{p \wedge \neg q} \vee p) \wedge (\neg P_{p \wedge \neg q} \vee P_{\neg q}) \wedge (P_{p \wedge \neg q} \vee \neg p \vee \neg P_{\neg q}) \\
C_{\phi} & \triangleq & (P_{\phi} \vee P_{p \wedge \neg q}) \wedge (\neg P_{\phi} \vee \neg P_{p \wedge \neg q})
\end{array}
$$

$\phi$ and $P_{\phi} \wedge C_{\phi} \wedge C_{p \wedge \neg q} \wedge C_{\neg q}$ =
$P_{\phi} \wedge (P_{\phi} \vee P_{p \wedge \neg q}) \wedge (\neg P_{\phi} \vee \neg P_{p \wedge \neg q}) \wedge (\neg P_{p \wedge \neg q} \vee p) \wedge (\neg P_{p \wedge \neg q} \vee P_{\neg q}) \wedge$
$(P_{p \wedge \neg q} \vee \neg p \vee \neg P_{\neg q}) \wedge (P_{\neg q} \vee q) \wedge (\neg P_{\neg q} \vee \neg q)$ are equisatisfiable. $\square$

# Example

## Example

Transform $\phi = p \vee \neg(q \wedge (r \vee \neg s))$ into an equisatisfiable propositional logic formula in CNF.

## Proof.

$\neg s, r \vee \neg s, q \wedge (r \vee \neg s), \neg(q \wedge (r \vee \neg s)), \phi$ are non-atomic subformulae of $\phi$.

$$\begin{array}{rcl}
C_{\neg s} & \triangleq & (P_{\neg s} \vee s) \wedge (\neg P_{\neg s} \vee \neg s) \\
C_{r \vee \neg s} & \triangleq & (P_{r \vee \neg s} \vee \neg r) \wedge (P_{r \vee \neg s} \vee \neg P_{\neg s}) \wedge (\neg P_{r \vee \neg s} \vee r \vee P_{\neg s}) \\
C_{q \wedge (r \vee \neg s)} & \triangleq & (\neg P_{q \wedge (r \vee \neg s)} \vee q) \wedge (\neg P_{q \wedge (r \vee \neg s)} \vee P_{r \vee \neg s}) \wedge \\
 & & (P_{q \wedge (r \vee \neg s)} \vee \neg q \vee \neg P_{r \vee \neg s}) \\
C_{\neg(q \wedge (r \vee \neg s))} & \triangleq & (P_{\neg(q \wedge (r \vee \neg s))} \vee P_{q \wedge (r \vee \neg s)}) \wedge (\neg P_{\neg(q \wedge (r \vee \neg s))} \vee \neg P_{q \wedge (r \vee \neg s)}) \\
C_{\phi} & \triangleq & (P_{\phi} \vee \neg p) \wedge (P_{\phi} \vee \neg P_{\neg(q \wedge (r \vee \neg s))}) \wedge (\neg P_{\phi} \vee p \vee P_{\neg(q \wedge (r \vee \neg s))})
\end{array}$$

Then $\phi$ and $P_{\phi} \wedge C_{\phi} \wedge C_{\neg(q \wedge (r \vee \neg s))} \wedge C_{q \wedge (r \vee \neg s)} \wedge C_{r \vee \neg s)} \wedge C_{\neg s}$ is equisatisfiable. □

# Properties of Tseitin Transformation

- Let $\phi$ be a propositional logic formula.
- The size $|\phi|$ of $\phi$ is the number of symbols (atomic propositions, $\wedge$, $\vee$, $\neg$) in $\phi$.
  - Parentheses ("(" and ")") do not count.
  - $|\phi|$ is the number of nodes in the parsing tree of $\phi$.
- Tseitin Transformation of $\phi$ has
  - $|\phi|$ atomic propositions;
  - Each $C_\alpha$ has at most 3 clauses;
  - Each clause of $C_\alpha$ has at most 3 literals.
- Let $\phi = (p_{11} \wedge p_{12} \wedge \cdots p_{1m_1}) \vee (p_{21} \wedge p_{22} \wedge \cdots p_{2m_2}) \vee \cdots \vee (p_{n1} \wedge p_{n2} \wedge \cdots p_{nm_n})$. We obtain a semantic equivalent propositional logic formula $\psi$ by distributive law. What is the size of $\psi$?

# DIMACS SAT Format I

- DIMACS SAT format is a standard text format for CNF formulae.
- Most SAT solvers accept a simplified version of DIMACS SAT format.
- Here is the example from the SAT Competition home page.

```
c
c start with comments
c
c
p cnf 5 3
1 -5 4 0
-1 5 3 4 0
-3 -4 0
```

# DIMACS SAT Format II

- From the SAT Competition home page:
  - The file can start with comments, that is lines begining with the character `c`.
  - Right after the comments, there is the line `p cnf` *nbvar nbclauses* indicating that the instance is in CNF format; *nbvar* is the exact number of variables appearing in the file; *nbclauses* is the exact number of clauses contained in the file.
  - Then the clauses follow. Each clause is a sequence of distinct non-null numbers between *-nbvar* and *nbvar* ending with `0` on the same line; it cannot contain the opposite literals $i$ and $-i$ simultaneously. Positive numbers denote the corresponding variables. Negative numbers denote the negations of the corresponding variables.
- Following DIMACS SAT format, we will represent a propositional logic formula in CNF by a set of clauses.
  - $(\neg a \vee b \vee \neg c) \wedge (\neg b \vee d) \wedge (a \vee c \vee \neg d)$ is represented as

$$(\neg a \vee b \vee \neg c) \quad (\neg b \vee d) \quad (a \vee c \vee \neg d)$$

# SAT Algorithms

- Davis, Putnam, 1960
  - Explicit resolution based.
  - May explode in memory.
- Davis, Logemann, Loveland, (DLL) 1962
  - Search based.
  - Most successful, basis for almost all modern SAT solvers.
  - Learning and non-chronological backtracking, 1996.
- Stålmarcks algorithm, 1980s
  - Proprietary algorithm. Patented.
  - Commercial versions available
- Stochastic Methods, 1992
  - Unable to prove unsatisfiability, but may find solutions for a satisfying problem quickly.
  - Local search and hill climbing

# Resolution

- Consider the proof rule:

$$\frac{l_0 \lor l_1 \lor \cdots \lor l_m \lor k \quad \overline{k} \lor l'_0 \lor l'_1 \lor \cdots \lor l'_n}{l_0 \lor l_1 \lor \cdots \lor l_m \lor l'_0 \lor l'_1 \lor \cdots \lor l'_n} \ \textit{resolution}$$

  - $k$ and $\overline{k}$ are complementary literals.
  - We assume $\lor$ is commutative.
- For instance, we obtain $(a \lor \neg b \lor \neg d \lor f)$ from $(a \lor \neg b \lor \neg c)$ and $(\neg d \lor c \lor f)$ by resolution.

# Davis Putnam Algorithm

- Select a variable for resolution iteratively.
- Consider the following set of clauses:

$$\begin{array}{lll}
(a \vee b \vee c) & (b \vee \neg c \vee f) & (\neg b \vee e) \\
\hline
(a \vee c \vee e) & (\neg c \vee e \vee f) & \\
\hline
(a \vee e \vee f) & &
\end{array}$$

SAT!

- Consider the following set of clauses:

$$\begin{array}{llll}
(a \vee b) & (a \vee \neg b) & (\neg a \vee c) & (\neg a \vee \neg c) \\
\hline
(a) & (\neg a \vee c) & (\neg a \vee \neg c) & \\
\hline
(c) & (\neg c) & & \\
\hline
() & & &
\end{array}$$

UNSAT!

# Basic DLL I

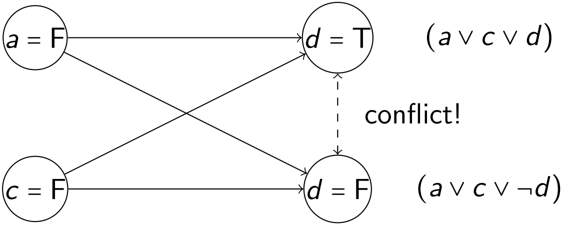
- Consider the following set of clauses:

$$(\neg a \lor b \lor c) \quad (a \lor c \lor d) \quad (a \lor c \lor \neg d) \quad (a \lor \neg c \lor d)$$
$$(a \lor \neg c \lor \neg d) \quad (\neg b \lor \neg c \lor d) \quad (\neg a \lor b \lor \neg c) \quad (\neg a \lor \neg b \lor c)$$

- We perform depth first search:

$$a = \mathrm{F} \quad b = \mathrm{F} \quad c = \mathrm{F}$$

and obtain a conflict:




  - This is an implication graph.

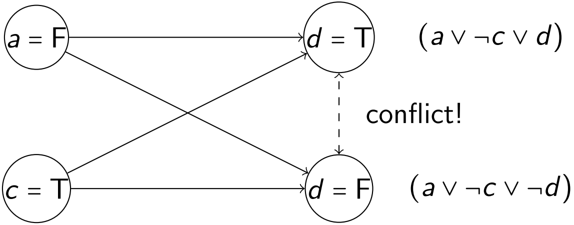
- Consider the following set of clauses:

$$(\neg a \lor b \lor c) \quad (a \lor c \lor d) \quad (a \lor c \lor \neg d) \quad (a \lor \neg c \lor d)$$
$$(a \lor \neg c \lor \neg d) \quad (\neg b \lor \neg c \lor d) \quad (\neg a \lor b \lor \neg c) \quad (\neg a \lor \neg b \lor c)$$

- Backtrack!

$$a = \mathrm{F} \quad b = \mathrm{F} \quad \cancel{c = \mathrm{F}}$$
$$c = \mathrm{T}(\text{forced})$$

and obtain a conflict:



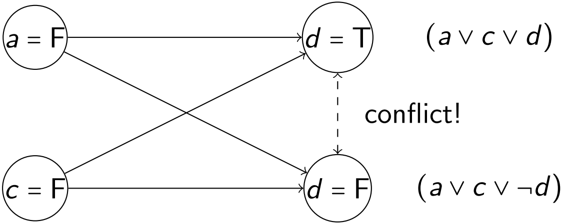
- Consider the following set of clauses:

$$
\begin{array}{cccc}
(\neg a \vee b \vee c) & (a \vee c \vee d) & (a \vee c \vee \neg d) & (a \vee \neg c \vee d) \\
(a \vee \neg c \vee \neg d) & (\neg b \vee \neg c \vee d) & (\neg a \vee b \vee \neg c) & (\neg a \vee \neg b \vee c)
\end{array}
$$

- Backtrack!

$$
\begin{array}{lll}
a = \mathrm{F} & \cancel{b = \mathrm{F}} & \\
 & b = \mathrm{T}(\text{forced}) & c = \mathrm{F}
\end{array}
$$

and obtain a conflict:



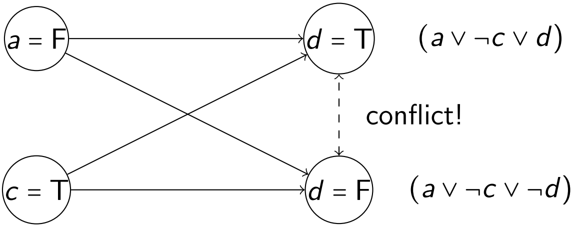
- Consider the following set of clauses:

$$\begin{array}{cccc} (\neg a \vee b \vee c) & (a \vee c \vee d) & (a \vee c \vee \neg d) & (a \vee \neg c \vee d) \\ (a \vee \neg c \vee \neg d) & (\neg b \vee \neg c \vee d) & (\neg a \vee b \vee \neg c) & (\neg a \vee \neg b \vee c) \end{array}$$

- Backtrack!

$$\begin{array}{lll} a = \mathrm{F} \quad \cancel{b = \mathrm{F}} & & \\ & b = \mathrm{T}(\text{forced}) \quad \cancel{c = \mathrm{F}} & \\ & & c = \mathrm{T}(\text{forced}) \end{array}$$

and obtain a conflict:



# Basic DLL V

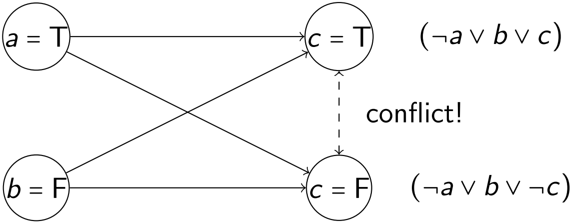
- Consider the following set of clauses:

$$
\begin{array}{cccc}
(\neg a \vee b \vee c) & (a \vee c \vee d) & (a \vee c \vee \neg d) & (a \vee \neg c \vee d) \\
(a \vee \neg c \vee \neg d) & (\neg b \vee \neg c \vee d) & (\neg a \vee b \vee \neg c) & (\neg a \vee \neg b \vee c)
\end{array}
$$

- Backtrack!

$$
\begin{array}{ll}
\cancel{a = \mathrm{F}} & \\
a = \mathrm{T}(\text{forced}) & b = \mathrm{F}
\end{array}
$$

and obtain a conflict:



# Basic DLL VI

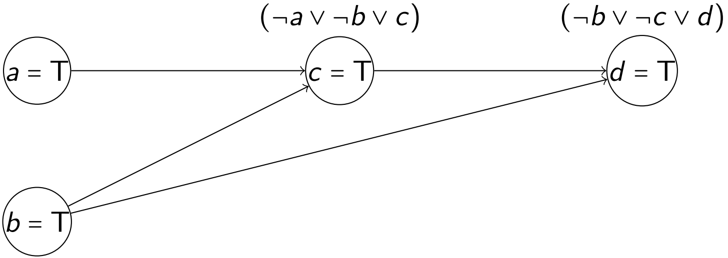
- Consider the following set of clauses:

$$
\begin{array}{cccc}
(\neg a \vee b \vee c) & (a \vee c \vee d) & (a \vee c \vee \neg d) & (a \vee \neg c \vee d) \\
(a \vee \neg c \vee \neg d) & (\neg b \vee \neg c \vee d) & (\neg a \vee b \vee \neg c) & (\neg a \vee \neg b \vee c)
\end{array}
$$

- Backtrack!

$$
\begin{array}{ll}
\cancel{a = \mathrm{F}} & \\
a = \mathrm{T}(\text{forced}) & \cancel{b = \mathrm{F}} \\
 & b = \mathrm{T}(\text{forced})
\end{array}
$$

and SAT!



# Conflict Driven Learning

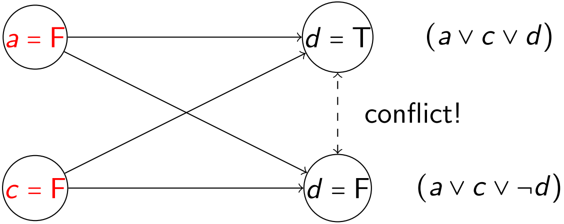
- When a conflict is encountered, add its cause to prevent it.
- Consider the following set of clauses:

$$\begin{array}{cccc} (\neg a \vee b \vee c) & (a \vee c \vee d) & (a \vee c \vee \neg d) & (a \vee \neg c \vee d) \\ (a \vee \neg c \vee \neg d) & (\neg b \vee \neg c \vee d) & (\neg a \vee b \vee \neg c) & (\neg a \vee \neg b \vee c) \end{array}$$

  and the following valuation:

$$a = \mathrm{F} \quad b = \mathrm{F} \quad c = \mathrm{F}$$

- The conflict is caused by $a = \mathrm{F}$ and $c = \mathrm{F}$:




- Hence we add a learned clause: $(a \vee c)$.

# Non-Chronological Backtracking

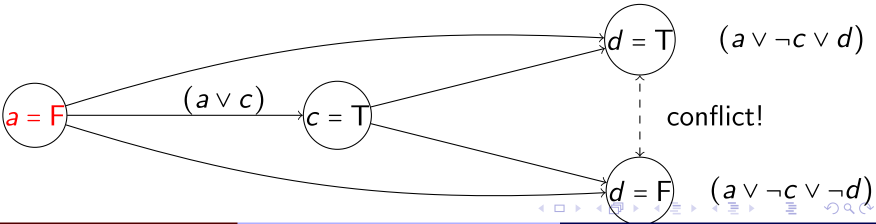
- When a learned clause is generated, backtrack to the next-to-the-last variable in the clause.
- Consider the following set of clauses:

$$\begin{array}{cccc} (\neg a \lor b \lor c) & (a \lor c \lor d) & (a \lor c \lor \neg d) & (a \lor \neg c \lor d) \\ (a \lor \neg c \lor \neg d) & (\neg b \lor \neg c \lor d) & (\neg a \lor b \lor \neg c) & (\neg a \lor \neg b \lor c) \\ {\color{magenta}(a \lor c)} & & & \end{array}$$

backtrack to $a$:

$$a = \mathrm{F}$$

obtain a conflict, and add a learned clause ${\color{magenta}(a)}$:



# DPLL I

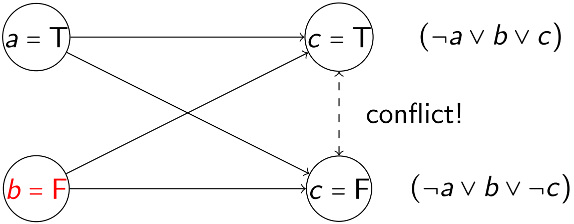
- Consider the following set of clauses:

$$
\begin{array}{cccc}
(\neg a \lor b \lor c) & (a \lor c \lor d) & (a \lor c \lor \neg d) & (a \lor \neg c \lor d) \\
(a \lor \neg c \lor \neg d) & (\neg b \lor \neg c \lor d) & (\neg a \lor b \lor \neg c) & (\neg a \lor \neg b \lor c) \\
(a \lor c) & (a) & &
\end{array}
$$

- backtrack all variables:

$$b = \mathrm{F}$$

obtain a conflict, and add a learned clause $(b)$:



- Consider the following set of clauses:

$$
\begin{array}{cccc}
(\neg a \vee b \vee c) & (a \vee c \vee d) & (a \vee c \vee \neg d) & (a \vee \neg c \vee d) \\
(a \vee \neg c \vee \neg d) & (\neg b \vee \neg c \vee d) & (\neg a \vee b \vee \neg c) & (\neg a \vee \neg b \vee c) \\
(a \vee c) & (a) & (b) &
\end{array}
$$

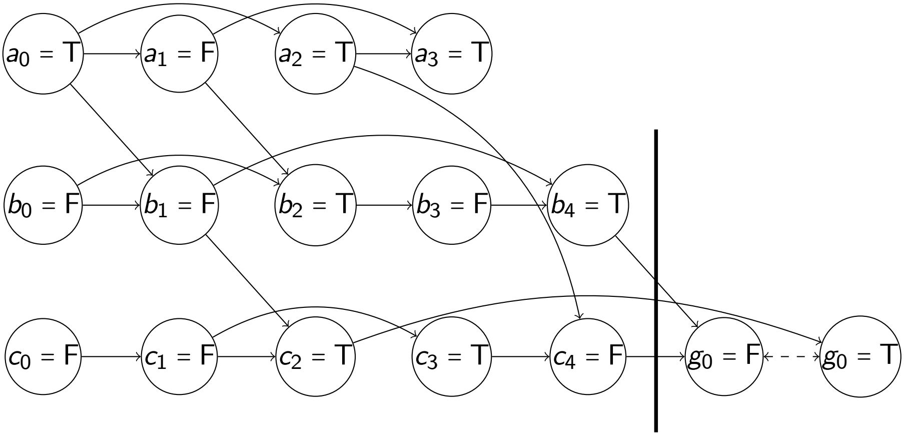
- and SAT!

$$
\begin{tikzcd}
 & (\neg a \vee \neg b \vee c) & (\neg b \vee \neg c \vee d) \\
a = \mathrm{T} \arrow[r] & c = \mathrm{T} \arrow[r] & d = \mathrm{T} \\
b = \mathrm{T} \arrow[ur] \arrow[urr] & &
\end{tikzcd}
$$

# Conflict Analysis I

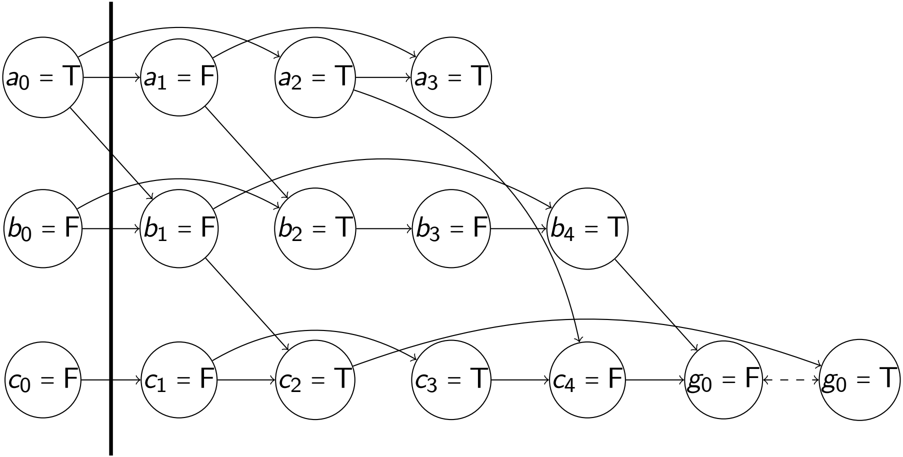
- When a conflict occurs, we would like to "learn" a clause to prevent the conflict from reoccurring.
- We hence would like to know what valuations cause the conflict.
- In an implication graph, any cut from root assignments to conflicting assignments is such a cause.

# Conflict Analysis II

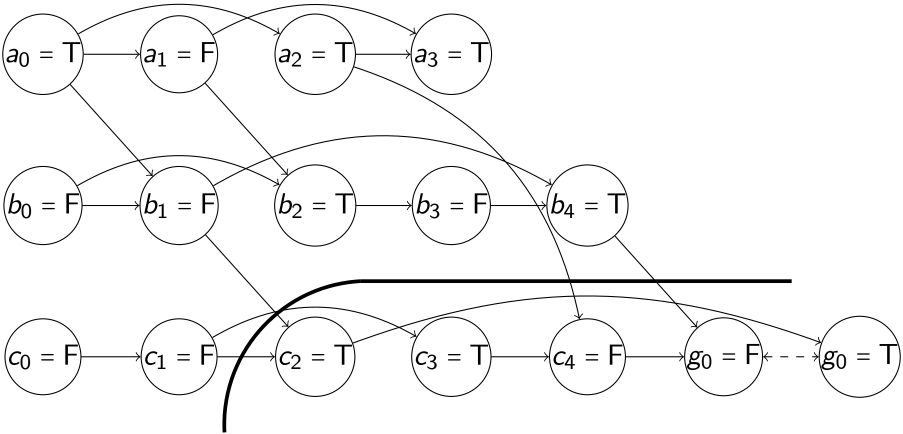



- $b_4 = \mathrm{T}$, $c_2 = \mathrm{T}$, and $c_4 = \mathrm{F}$ cause the conflict.
- Hence we can learn $(\neg b_4 \vee \neg c_2 \vee c_4)$.

# Conflict Analysis III




- $a_0 = \mathrm{T}$, $b_0 = \mathrm{F}$, and $c_0 = \mathrm{F}$ cause the conflict.
- Hence we can learn $(\neg a_0 \vee b_0 \vee c_0)$.

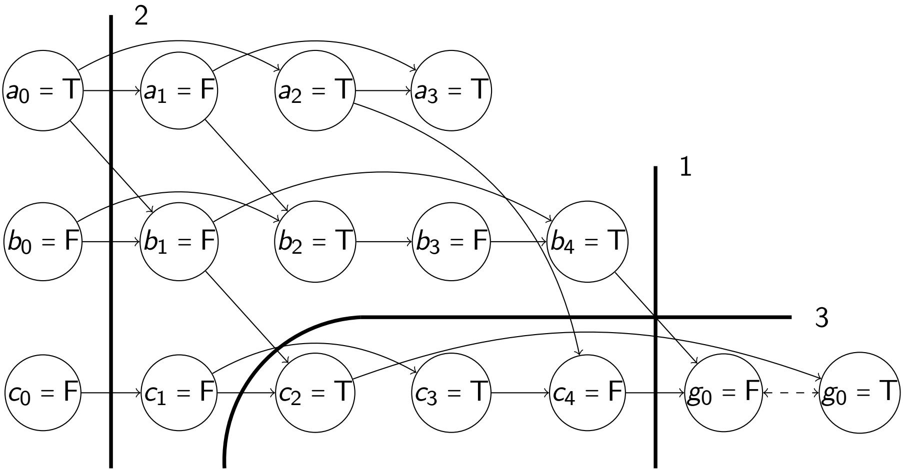



- $a_2 = \mathrm{T}$, $b_1 = \mathrm{F}$, $b_4 = \mathrm{T}$, and $c_1 = \mathrm{F}$ cause the conflict.
- Hence we can learn $(\neg a_2 \vee b_1 \vee \neg b_4 \vee c_1)$.

# Conflict Analysis V

- Clearly, there are several cuts in an implication graph.
- Each cut corresponds to a learned clause.
- Which one is the best?
- Idea: reverse exactly one truth value.
- Consider only cuts that has only one node in the same level as the conflict.
  - This is called a unique implication point (UIP).

# Conflict Analysis VI




- Cut 1 is not UIP. Cut 2 is the last UIP. Cut 3 is the first UIP.
  - Emperically, the first UIP is the best.

# Where to go?

- Contrary to general belief, SAT solvers are not impractical.
- Engineering ideas are essential to the real world.
  - When cleverly applied, they can even tackle hard theoretical problems such as satisfiability.
- We only discuss a clever idea in SAT solvers very briefly.
- There are certainly many more.
  - There are many interesting ideas for propagation, memory management, etc.
- MINISAT is an open-sourced fast SAT solver.
- Read its code. You will learn a lot more!