PROPOSITIONAL LOGIC

VL Logik: WS 2018/19

(Version 2018.2)

Martina Seidl (martina.seidl@jku.at),
Armin Biere (biere@jku.at)
Institut für Formale Modelle und Verifikation
BOX Game: Rules

1. The game board consists of boxes with symbols. For example:

```
  ♥  ♦
  ♥   ♦
  ♥  □
  ♦  □
```
BOX Game: Rules

1. The game board consists of boxes with symbols. For example:

2. We chose two colors, for example purple and green.
   - One color is the winning color, for example purple.
   - Then the non-winning color is green.
BOX Game: Rules

1. The game board consists of boxes with symbols. For example:

   ♥ ♦
   □

2. We chose two colors, for example purple and green.
   - One color is the winning color, for example purple.
   - Then the non-winning color is green.

3. Now we can play: assign the two colors to each symbol such that its underlined and non-underlined occurrences have a different color.
BOX Game: Rules

1. The game board consists of boxes with symbols. For example:

```
  ♥ ♦
  □  ♦
```

2. We chose two colors, for example purple and green.
   □ One color is the winning color, for example purple.
   □ Then the non-winning color is green.

3. Now we can play: assign the two colors to each symbol such that its underlined and non-underlined occurrences have a different color.

4. If each box contains a symbol in purple you won.
Some Examples

- Wrong coloring!

![Images of card suits with incorrect coloring]
Some Examples

- Wrong coloring!

- Again a wrong coloring!
Some Examples

- Wrong coloring!

- Again a wrong coloring!

- Lost!
Some Examples

- Wrong coloring!
  
- Again a wrong coloring!
  
- Lost!
  
- Won!
Some Terminology

- From now on, we call a box a **clause**.
- We call a clause with **at least one** purple symbol **satisfied**.
- We call a clause with **all** symbols in green **falsified**.
- We call a clause with green and uncolored symbols **undecided**.

⇒ The game is won if all clauses are satisfied.
How Many Possibilities?

- 1 symbol, 2 possibilities
  1. 💖
  2. 💚
How Many Possibilities?

- 1 symbol, 2 possibilities
- 2 symbols, 4 possibilities
  1. ♠, ♦
  2. ♠, ♦
  3. ♠, ♦
  4. ♠, ♦
- 3 symbols, 8 possibilities
- 4 symbols, 16 possibilities
- 5 symbols, 32 possibilities
- 6 symbols, 64 possibilities
- ...
- 20 symbols, 1,048,576 possibilities
- 30 symbols, 1,073,741,824 possibilities
How Many Possibilities?

- 1 symbol, 2 possibilities
- 2 symbols, 4 possibilities
- 3 symbols, 8 possibilities
  1. ♠, ♢, □
  2. ♠, ♢, □
  3. ♠, ♢, □
  4. ♠, ♢, □
  5. ♠, ♢, □
  6. ♠, ♢, □
  7. ♠, ♢, □
  8. ♠, ♢, □
- 4 symbols, 16 possibilities
- 5 symbols, 32 possibilities
- 6 symbols, 64 possibilities
- ...
- 20 symbols, 1,048,576 possibilities
- 30 symbols, 1,073,741,824 possibilities
How Many Possibilities?

- 1 symbol, 2 possibilities
- 2 symbols, 4 possibilities
- 3 symbols, 8 possibilities
- 4 symbols, 16 possibilities
How Many Possibilities?

- 1 symbol, 2 possibilities
- 2 symbols, 4 possibilities
- 3 symbols, 8 possibilities
- 4 symbols, 16 possibilities
- 5 symbols, 32 possibilities
How Many Possibilities?

- 1 symbol, 2 possibilities
- 2 symbols, 4 possibilities
- 3 symbols, 8 possibilities
- 4 symbols, 16 possibilities
- 5 symbols, 32 possibilities
- 6 symbols, 64 possibilities
- ...
How Many Possibilities?

- 1 symbol, 2 possibilities
- 2 symbols, 4 possibilities
- 3 symbols, 8 possibilities
- 4 symbols, 16 possibilities
- 5 symbols, 32 possibilities
- 6 symbols, 64 possibilities
- ...

...
How Many Possibilities?

- 1 symbol, 2 possibilities
- 2 symbols, 4 possibilities
- 3 symbols, 8 possibilities
- 4 symbols, 16 possibilities
- 5 symbols, 32 possibilities
- 6 symbols, 64 possibilities
- ...
- 20 symbols, 1.048.576 possibilities
How Many Possibilities?

- 1 symbol, 2 possibilities
- 2 symbols, 4 possibilities
- 3 symbols, 8 possibilities
- 4 symbols, 16 possibilities
- 5 symbols, 32 possibilities
- 6 symbols, 64 possibilities
- ...
- 20 symbols, 1,048,576 possibilities
- 30 symbols, 1,073,741,824 possibilities
How Many Possibilities?

- 1 symbol, 2 possibilities
- 2 symbols, 4 possibilities
- 3 symbols, 8 possibilities
- 4 symbols, 16 possibilities
- 5 symbols, 32 possibilities
- 6 symbols, 64 possibilities
- ... 
- 20 symbols, 1.048.576 possibilities
- 30 symbols, 1.073.741.824 possibilities

\[ n \text{ symbols} \Rightarrow 2^n \text{ possibilities} \]
Guess & Check Problems

observation in our BOX game:

■ finding a solution is hard
  □ $2^n$ solution candidates have to be considered
  □ a good oracle is needed for guessing

■ verifying a given candidate solution is easy
  □ check that each box contains a purple symbol
Guess & Check Problems

observation in our BOX game:

■ finding a solution is hard
  □ $2^n$ solution candidates have to be considered
  □ a good oracle is needed for guessing

■ verifying a given candidate solution is easy
  □ check that each box contains a purple symbol

fundamental question in computer science:

The P = NP Question

Is searching for a solution harder than verifying a solution?
(unfortunately, the answer is not known)
Famous Guess & Check Problem: SAT

SAT is the decision problem of propositional logic:

- Given a Boolean formula, for example

\[ (\neg x \lor \neg y) \land (x \lor \neg y) \land (\neg x \lor z) \land (y \lor \neg z). \]

- Question: is the formula satisfiable?
  I.e., is there an assignment of truth values 1 (true), 0 (false) to the literals \( x, y, z, \neg x, \neg y, \neg z \) such that
  
  - for every variable \( v \in \{ x, y, z \} \) it holds that the truth value of \( v \) and the truth value of \( \neg v \) are different
  - each clause (...) contains at least one true literal
Famous Guess & Check Problem: SAT

SAT is the decision problem of propositional logic:

- Given a Boolean formula, for example
  \[(\neg x \lor \neg y) \land (x \lor \neg y) \land (\neg x \lor z) \land (y \lor \neg z)\].

- Question: is the formula satisfiable?
  I.e., is there an assignment of truth values 1 (true), 0 (false) to the literals \(x, y, z, \neg x, \neg y, \neg z\) such that
  - for every variable \(v \in \{x, y, z\}\) it holds that the truth value of \(v\) and the truth value of \(\neg v\) are different
  - each clause (...) contains at least one true literal

**Cook-Levin Theorem [71]:** SAT is NP-complete

Searching is as easy as checking if and only if it is for SAT.
Relating BOX and SAT

There is a correspondence between BOX and SAT, e.g., between

and \((\neg x \lor \neg y) \land (x \lor \neg y) \land (\neg x \lor z) \land (y \lor \neg z)\) :
Relating BOX and SAT

There is a correspondence between BOX and SAT, e.g., between

- $\heartsuit$ corresponds to $\diamondsuit$,
- $\neg x$ corresponds to $\heartsuit$,
- $\neg y$ corresponds to $\diamondsuit$,
- $\neg z$ corresponds to $\square$,
- purple/green coloring corresponds to assignment of literals to true/false ($1/0$)

and $(\neg x \lor \neg y) \land (x \lor \neg y) \land (\neg x \lor z) \land (y \lor \neg z)$:

- $x$ corresponds to $\heartsuit$,
- $\neg x$ corresponds to $\heartsuit$,
- $y$ corresponds to $\diamondsuit$,
- $\neg y$ corresponds to $\diamondsuit$,
- $z$ corresponds to $\square$,
- $\neg z$ corresponds to $\square$
Relating BOX and SAT

There is a correspondence between BOX and SAT, e.g., between

\[
\begin{array}{c}
\heartsuit \spadesuit \\
\heartsuit \spadesuit \\
\heartsuit \square \\
\spadesuit \square \\
\end{array}
\]

and \((¬x \lor ¬y) \land (x \lor ¬y) \land (¬x \lor z) \land (y \lor ¬z)\) :

- \(x\) corresponds to \(\heartsuit\), \(¬x\) corresponds to \(\heartsuit\)
- \(y\) corresponds to \(\spadesuit\), \(¬y\) corresponds to \(\spadesuit\)
- \(z\) corresponds to \(\square\), \(¬z\) corresponds to \(\square\)
- purple/green coloring corresponds to assignment of literals to true/false (1/0)

Note:
Relating BOX and SAT

There is a correspondence between BOX and SAT, e.g., between

\[
\begin{align*}
\heartsuit & \leftrightarrow \spadesuit \\
\heartsuit & \leftrightarrow \spadesuit \\
\heartsuit & \leftrightarrow \Box \\
\spadesuit & \leftrightarrow \Box 
\end{align*}
\]

and \((\neg x \lor \neg y) \land (x \lor \neg y) \land (\neg x \lor z) \land (y \lor \neg z)\):

- \(x\) corresponds to \(\heartsuit\), \(\neg x\) corresponds to \(\heartsuit\)
- \(y\) corresponds to \(\spadesuit\), \(\neg y\) corresponds to \(\spadesuit\)
- \(z\) corresponds to \(\Box\), \(\neg z\) corresponds to \(\Box\)
- purple/green coloring corresponds to assignment of literals to true/false (1/0)

Note:

- assignment of variables gives values of all literals
- if we can solve SAT, we can solve BOX (and vice versa)
Practical Applications of SAT Solving

- formal verification
- bioinformatics
- train safety
- planning & scheduling
- security
- theorem proving

encode -> SAT solver -> decode
Logics in this Lecture

In this lecture, we consider different logic-based languages:

- **propositional logic (SAT)**
  - simple language: only atoms and connectives
  - low expressiveness, low complexity
  - very successful in industry (e.g., verification)

- **first-order logic (predicate logic)**
  - rich language: predicates, functions, terms, quantifiers
  - great power of expressiveness, high complexity
  - many applications in mathematics and verification

- **satisfiability modulo theories (SMT)**
  - customizable language: user decides
  - as much expressiveness as required
  - as much complexity as necessary
  - very popular and successful in industry
Logic-Based Languages (Logics)

- A logic consists of
  - a set of symbols (like $\lor$, $\land$, $\neg$, $\top$, $\bot$, $\forall$, $\exists$, ...)
  - a set of variables (like $x$, $y$, $z$, ...)
  - concise syntax: well-formedness of expressions
  - concise semantics: meaning of expressions

- Logics support reasoning for
  - derivation of “new” knowledge
  - proving the truth/falsity of a statement (satisfiability checking)

- Different logics differ in their
  - truth values: binary (true, false), multi-valued (true, false, unknown), fuzzy (between 0 and 1, e.g., $[0, 1]$ as subset of the real numbers)
  - expressiveness (what can be formulated in the logic?)
  - complexity (how expensive is reasoning?)
PROPOSITIONAL LOGIC
Propositions

A proposition is an atomic statement that is either true or false.

Example:
- Alice comes to the party.
- It rains.

With connectives, propositions can be combined.

Example:
- Alice comes to the party, Bob as well, but not Cecile.
- If it rains, the street is wet.
Propositional Logic

- two truth values (Boolean domain): true/false, verum/falsum, on/off, 1/0
- language elements
  - atomic propositions (atoms, variables)
    - no internal structure
    - either true or false
  - logic connectives: not (¬), and (∧), or (∨), ...
    - operators for construction of composite propositions
    - concise meaning
    - argument(s) and return value from Boolean domain
  - parenthesis

**example:** formula of propositional logic: \((\neg t \lor s) \land (t \lor s) \land (\neg t \lor \neg s)\)

atoms: \(t, s\), connectives: \(\neg, \lor, \land\), parenthesis for structuring the expression
Background

- **historical origins**: ancient Greeks
- in philosophy, mathematics, and computer science
- two very basic principles:
  - **Law of Excluded Middle**: a proposition is true or its negation is true
  - **Law of Contradiction**: no expression is both true and false at the same time
- very simple language
  - no objects, no arguments to propositions
  - no functions, no quantifiers
- solving is easy (relative to other logics)
- many applications in industry
Syntax: Structure of Propositional Formulas

we build a propositional formula using the following components:

- **literals:**
  - variables $x, y, z, \ldots$
  - negated variables $\neg x, \neg y, \neg z, \ldots$
  - truth constants: $\top$ (verum) and $\bot$ (falsum)
  - negated truth constants: $\neg \top$ and $\neg \bot$

- **clauses:** disjunction ($\lor$) of literals
  - $x \lor y$
  - $x \lor y \lor \neg z$
  - $z$
  - $\top$
A propositional formula is a conjunction \((\land)\) of clauses.

**Examples of formulas:**

- \(\top\)
- \(\bot\)
- \(x\)
- \(\neg y\)
- \(x \land y \land z\)
- \((\neg x \lor y \lor \neg z) \land z\)
- \((x \lor \neg y) \land (x \lor \neg y \lor z) \land (y \lor \neg z)\)
- \(((l_{11} \lor \ldots \lor l_{1m_1}) \land \ldots \land (l_{n1} \lor \ldots \lor l_{nm_n}))\)

**Remark:** For the moment, we consider formulas of a restricted structure called CNF, e.g., we do not consider formulas like \((x \land y) \lor (\neg x \land z)\). Any propositional formula can be translated into this structure. We will relax this restriction later.
Conventions

we use the following conventions unless stated otherwise:

- $a, b, c, x, y, z$ denote variables and $l, k$ denote literals
- $\phi, \psi, \gamma$ denote arbitrary formulas
- $C, D$ denote clauses
- clauses are also written as sets
  - $\{l_1 \lor \ldots \lor l_n\} = \{l_1, \ldots, l_n\}$
  - to add a literal $l$ to clause $C$, we write $C \cup \{l\}$
  - to remove a literal $l$ from clause $C$, we write $C \setminus \{l\}$
- formulas in CNF are also written as sets of sets
  - $\{(l_{11} \lor \ldots \lor l_{1m_1}) \land \ldots \land (l_{n1} \lor \ldots \lor l_{nm_n})\} = \\{\{l_{11}, \ldots, l_{1m_1}\}, \ldots, \{l_{n1}, \ldots, l_{nm_n}\}\}$
  - to add a clause $C$ to CNF $\phi$, we write $\phi \cup \{C\}$
  - to remove a clause $C$ from CNF $\phi$, we write $\phi \setminus \{C\}$
Negation

- unary connective \( \neg \) (operator with exactly one argument)
- negating the truth value of its argument
- alternative notation: \( !x, \bar{x}, \neg x, NOT\, x \)

<table>
<thead>
<tr>
<th>( x )</th>
<th>( \neg x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**example:**
- If the atom “It rains.” is true then the negation “It does not rain.” is false.
- If the propositional variable \( a \) is true then \( \neg a \) is false.
- If the propositional variable \( a \) is false then \( \neg a \) is true.
Disjunction

- a disjunction is true iff at least one of the arguments is true
- alternative notation for $l \lor k$: $l \parallel k$, $l + k$, $l OR k$
- For $(l_1 \lor \ldots \lor l_n)$ we also write $\bigvee_{i=1}^n l_i$.

<table>
<thead>
<tr>
<th>$l$</th>
<th>$k$</th>
<th>$l \lor k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

truth table:

example:

- $(a \lor \neg a)$ is always true.
- $(\top \lor a)$ is always true.
- $(\bot \lor a)$ is true if $a$ is true.
Conjunction

- A conjunction is true iff both arguments are true.
- Alternative notation for $C \land D$: $C \&\& D$, $CD$, $C \ast D$, $C \cdot D$, $C \text{ AND } D$.
- For $(C_1 \land \ldots \land C_n)$ we also write $\land_{i=1}^n C_i$.

Truth table:

<table>
<thead>
<tr>
<th>$C$</th>
<th>$D$</th>
<th>$C \land D$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Example:

- $(a \land \neg a)$ is always false.
- $(\top \land a)$ is true if $a$ is true. $(\bot \land \phi)$ is always false.
- If $(a \lor b)$ is true and $(\neg c \lor d)$ is true then $(a \lor b) \land (\neg c \lor d)$ is true.
Properties of Connectives

- rules of precedence:
  - \( \neg \) binds stronger than \( \land \)
  - \( \land \) binds stronger than \( \lor \)

  example
  - \( \neg a \lor b \land \neg c \lor d \) is the same as \( (\neg a) \lor (b \land (\neg c)) \lor d \), but not 
    \( ((\neg a) \lor b) \land ((\neg c) \lor d) \)

  \( \Rightarrow \) put clauses into parentheses!

- associativity:
  - \( \land \) is associative and commutative
  - \( \lor \) is associative and commutative

  example
  - \( (a \land b) \land \neg c \) is the same as \( a \land (b \land \neg c) \)
  - \( (a \lor b) \lor \neg c \) is the same as \( a \lor (b \lor \neg c) \)
Assignment

- A variable can be assigned one of two values from the two-valued domain \( \mathbb{B} \), where \( \mathbb{B} = \{1, 0\} \).

- The mapping \( \nu : \mathcal{P} \to \mathbb{B} \) is called assignment, where \( \mathcal{P} \) is the set of atomic propositions.

- We sometimes write an assignment \( \nu \) as set \( V \) with \( V \subseteq \mathcal{P} \cup \{-x | x \in \mathcal{P}\} \) such that
  - \( x \in V \) iff \( \nu(x) = 1 \)
  - \( \neg x \in V \) iff \( \nu(x) = 0 \)

- For \( n \) variables, there are \( 2^n \) assignments possible.

- An assignment corresponds to one line in the truth table.
## Assignment: Example

\[ (x \lor y) \land \neg z \]

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
<th>$z$</th>
<th>$x \lor y$</th>
<th>$\neg z$</th>
<th>$(x \lor y) \land \neg z$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- **one assignment**: $\nu(x) = 1$, $\nu(y) = 0$, $\nu(z) = 1$
- **alternative notation**: $V = \{x, \neg y, z\}$
- **observation**: A variable assignment determines the truth value of the formulas containing these variables.
Semantics of Propositional Logic

Let $P$ be the set of atomic propositions (variables) and $L$ be the set of all propositional formulas over $P$ that are syntactically correct (i.e., all possible conjunctions of clauses over $P$).

Given assignment $\nu : P \rightarrow \mathbb{B}$, the interpretation $[.]_{\nu} : L \rightarrow \mathbb{B}$ is defined by:

- $[\top]_{\nu} = 1$, $[\bot]_{\nu} = 0$
- If $x \in P$ then $[x]_{\nu} = \nu(x)$
- $[-x]_{\nu} = 1$ iff $[x]_{\nu} = 0$
- $[C]_{\nu} = 1$ (where $C$ is a clause) iff there is at least one literal $l$ with $l \in C$ and $[l]_{\nu} = 1$
- $[\phi]_{\nu} = 1$ (where $\phi$ is in CNF) iff for all clauses $C \in \phi$ it holds that $[C]_{\nu} = 1$
Satisfying/Falsifying Assignments

- an assignment \( \nu \) is called
  - satisfying a formula \( \phi \) iff \([\phi]_\nu = 1\)
  - falsifying a formula \( \phi \) iff \([\phi]_\nu = 0\)

- a satisfying assignment for \( \phi \) is a model of \( \phi \)
- a falsifying assignment for \( \phi \) is a counter-model of \( \phi \)

example:

For formula \(((x \lor y) \land \neg z)\),
- \(\{x, y, z\}\) is a counter-model,
- \(\{x, y, \neg z\}\) is a model.
SAT-Solver Limboole

- available at [http://fmv.jku.at/limboole](http://fmv.jku.at/limboole)

- input:\(^1\)
  - variables are strings over letters, digits and \(-\_\).\([\[]\] \$ \@\)
  - negation symbol \(\neg\) is \(!\)
  - disjunction symbol \(\lor\) is \(|\)
  - conjunction symbol \(\land\) is \&

example

\((a \lor b \lor \neg c) \land (\neg a \lor b) \land c\) is represented as

\((a | b | !c) \& (!a | b) \& c\)

\(^1\)For now, we will only use subset of the language supported by Limboole.
Properties of Propositional Formulas (1/2)

- formula $\phi$ is **satisfiable** iff there exists an assignment $\nu$ with $[\phi]_{\nu} = 1$
  
  check with limboole -s

- formula $\phi$ is **valid** iff for all assignments $\nu$ it holds that $[\phi]_{\nu} = 1$
  
  check with limboole

- formula $\phi$ is **refutable** iff there exists an assignment $\nu$ with $[\phi]_{\nu} = 0$
  
  check with limboole

- formula $\phi$ is **unsatisfiable** iff for all assignments $\nu$ it holds that $[\phi]_{\nu} = 0$
  
  check with limboole -s
Properties of Propositional Formulas (2/2)

- A valid formula is called tautology.
- An unsatisfiable formula is called contradiction.

Example:
- $\top$ is valid.
- $a \lor \neg a$ is a tautology.
- $(a \lor \neg b) \land (\neg a \lor b)$ is refutable.
- $\bot$ is unsatisfiable.
- $a \land \neg a$ is a contradiction.
- $(a \lor \neg b) \land (\neg a \lor b)$ is satisfiable.
SAT: The Boolean Satisfiability Problem

Given a propositional formula $\phi$. Is there an assignment that satisfies $\phi$?

different formulation: can we find an assignment such that each clause contains at least one true literal?
Encoding the k-Coloring Problem

Given graph \((V, E)\) with vertices \(V\) and edges \(E\). Color each node with one of \(k\) colors, such that there is no edge \((v, w) \in E\), with vertices \(v\) and \(w\) colored in the same color.

encoding:

1. **propositional variables**: \(v_j\) ... node \(v \in V\) has color \(j\) \((1 \leq j \leq k)\)

2. each node has a color:

\[
\bigwedge_{v \in V} \left( \bigvee_{1 \leq j \leq k} v_j \right)
\]

3. each node has just one color: \((\neg v_i \lor \neg v_j)\) with \(v \in V, 1 \leq i < j \leq k\)

4. neighbors have different colors: \((\neg v_i \lor \neg w_i)\) with \((v, w) \in E, 1 \leq i \leq k\)
Encoding the k-Coloring Problem: Example

**task:** find 2-coloring of graph \((\{a, b, c\}, \{(a, b), (b, c)\})\) with SAT

**possible solution:**

- a
- b
- c

**encoding in SAT:**

\[
\begin{align*}
\text{variables:} & \quad a_1, a_2, b_1, b_2, c_1, c_2 \\
\text{clauses:} & \quad (a_1 \lor a_2), (b_1 \lor b_2), (c_1 \lor c_2) \\
& \quad (\neg a_1 \lor \neg a_2), (\neg b_1 \lor \neg b_2), (\neg c_1 \lor \neg c_2) \\
& \quad (\neg a_1 \lor \neg b_1), (\neg a_2 \lor \neg b_2), (\neg b_1 \lor \neg c_1), (\neg b_2 \lor \neg c_2)
\end{align*}
\]

**full formula:**

\[
(a_1 \lor a_2) \land (b_1 \lor b_2) \land (c_1 \lor c_2) \land (\neg a_1 \lor \neg a_2) \land (\neg b_1 \lor \neg b_2) \land (\neg c_1 \lor \neg c_2) \land (\neg a_1 \lor \neg b_1) \land (\neg a_2 \lor \neg b_2) \land (\neg b_1 \lor \neg c_1) \land (\neg b_2 \lor \neg c_2)
\]
Encoding the k-Coloring Problem: Example

task: find 2-coloring of graph \( \{a, b, c\}, \{(a, b), (b, c)\} \) with SAT

possible solution:

![Graph with nodes a, b, c connected by edges]

encoding in SAT:

- variables: \( a_1, a_2, b_1, b_2, c_1, c_2 \)
Encoding the k-Coloring Problem: Example

**task:** find 2-coloring of graph \( \{a, b, c\}, \{(a, b), (b, c)\} \) with SAT

**possible solution:**

encoding in SAT:

- **variables:** \( a_1, a_2, b_1, b_2, c_1, c_2 \)
- **clauses:**
  1. each node has a color: \( (a_1 \lor a_2), (b_1 \lor b_2), (c_1 \lor c_2) \)
  2. no node has two colors: \( (\neg a_1 \lor \neg a_2), (\neg b_1 \lor \neg b_2), (\neg c_1 \lor \neg c_2) \)
  3. connected nodes have a different color:
     \( (\neg a_1 \lor \neg b_1), (\neg a_2 \lor \neg b_2), (\neg b_1 \lor \neg c_1), (\neg b_2 \lor \neg c_2) \)
Encoding the k-Coloring Problem: Example

**task:** find 2-coloring of graph \( \{a, b, c\}, \{(a, b), (b, c)\} \) with SAT

**possible solution:**

![Graph with nodes a, b, c and edges (a, b) and (b, c)]

**encoding in SAT:**

- **variables:** \( a_1, a_2, b_1, b_2, c_1, c_2 \)
- **clauses:**
  1. each node has a color: \( (a_1 \lor a_2), (b_1 \lor b_2), (c_1 \lor c_2) \)
  2. no node has two colors: \( (\neg a_1 \lor \neg a_2), (\neg b_1 \lor \neg b_2), (\neg c_1 \lor \neg c_2) \)
  3. connected nodes have a different color:
     \[
     (\neg a_1 \lor \neg b_1), (\neg a_2 \lor \neg b_2), (\neg b_1 \lor \neg c_1), (\neg b_2 \lor \neg c_2)
     \]
- **full formula:**
  \[
  (a_1 \lor a_2) \land (b_1 \lor b_2) \land (c_1 \lor c_2) \land (\neg a_1 \lor \neg a_2) \land (\neg b_1 \lor \neg b_2) \land (\neg c_1 \lor \neg c_2) \land \\
  (\neg a_1 \lor \neg b_1) \land (\neg a_2 \lor \neg b_2) \land (\neg b_1 \lor \neg c_1) \land (\neg b_2 \lor \neg c_2)
  \]
Resolution

- The resolution calculus consists of the single resolution rule:

\[
\frac{x \lor C \quad \neg x \lor D}{C \lor D}
\]

- \(C\) and \(D\) are (possibly empty) clauses
- The clause \(C \lor D\) is called the resolvent
- Variable \(x\) is called the pivot
- Antecedent clauses \(x \lor C\) and \(\neg x \lor D\) are NOT tautological

- The resolution calculus works only on formulas in CNF
- If the empty clause can be derived, then the formula is unsatisfiable
- If the formula is unsatisfiable, then the empty clause can be derived
Examples of Applying the Resolution Rule

one application of resolution

\[
\begin{align*}
x \lor y \lor \neg z & \quad \neg x \lor y' \lor \neg z \\
\hline
y \lor \neg z \lor y' & \quad \neg y
\end{align*}
\]

derivation of empty clause:

\[
\begin{align*}
y & \quad \neg y \\
\hline
\bot
\end{align*}
\]

derivation of tautology:

\[
\begin{align*}
x \lor a & \quad \neg x \lor \neg a \\
\hline
a \lor \neg a
\end{align*}
\]

incorrect application of the resolution rule:

\[
\begin{align*}
x \lor a \lor \neg x & \quad \neg x \lor \neg a \\
\hline
\text{???
\end{align*}
\]
Resolution Example

We prove unsatisfiability of

\[\{(\neg x_1 \lor \neg x_5), (x_4 \lor x_5), (x_2 \lor \neg x_4), (x_3 \lor \neg x_4), (\neg x_2 \lor \neg x_3), (x_1 \lor x_4 \lor \neg x_6), (x_6)\}\]

as follows: