Automated Reasoning and Formal Verification

Diego Oniarti

Anno 2024-2025

Contents

1 25-02-2025

intro

Slides will be on his webpage along with the recordings.

The exam will consist of a script and an oral exam on the topics of the whole course.

boolean/propositional logic

A propositional **formula** can be:

- $\top$, $\bot$
- Propositional **atoms** $A_1, A_2, \ldots, A_n$
- A combination of other formulas. If ϕ_1 and ϕ_2 are formulas, so are:
  - $\neg\phi_1$
  - $\phi_1 \wedge \phi_2$
  - $\phi_1 \vee \phi_2$
  - $\phi_1 \rightarrow \phi_2$
  - $\phi_1 \leftarrow \phi_2$
  - $\phi_1 \leftrightarrow \phi_2$
  - $\phi_1 \oplus \phi_2$

We define a function $Atoms(\phi)$ representing the set $\{A_1, \ldots, A_n\}$ of atoms in ϕ

A **clause** is a disjunction of literals $\bigvee_j l_j$ or $(A_1 \vee \neg A_2 \vee ...)$

A **cube** is a conjunction of literals $\bigwedge_j l_j$ or $(A_1 \wedge \neg A_2 \wedge ...)$

trees and DAGS

A tree is a natural representation of an expression, but in the worst cases it can grow exponentially. The same information about the formula can be conveyed by a *Directed Acyclic Graph*, which can grow linearly in size.

Total Truth Assignment

They can also be abbreviated as *Total Assignment*.
A total truth assignment $\mu : Atoms(\phi) \mapsto \{\top, \bot\}$ represents *one* possible state of the formula.

Partial Truth Assignment

A partial truth assignment $\mu : \mathcal{A} \mapsto \{\top, \bot\}, \mathcal{A} \subset Atoms(\phi)$ represents 2^k total assignments, where k is the number of unassigned literals.

μ defined for total and partial truth assignments a can be seen as a set of literals (positive and negative ones) or a formula.

Set of models

$M(\phi) \triangleq \{\mu | \mu \models \phi\}$ is the set of all models of ϕ.

Properties

- ϕ is *valid* if every μ models ϕ
- ϕ valid $\iff$ $\neg\phi$ unsatisfiable
- $\alpha \models \beta \iff \alpha \to \beta$ valid Deduction theorem
- corollary $\alpha \models \beta \iff \alpha \wedge \neg\beta$ not satisfiable

Equivalence and Equi-satisfiability

α and β are *equivalent* if $\forall \mu . \mu \models \alpha \iff \mu \models \beta$.
In other terms, $M(\alpha) = M(\beta)$.

Equi-satisfiability $M(\alpha) \neq \emptyset \iff M(\beta) \neq \emptyset$. This property is mostly used when applying transformations to formulas $\beta \triangleq T(\alpha)$.

Transformations can be *validity preserving* if they preserve the validity of the formula they're being applied to, or *satisfiability preserving* if they preserve its satisfiability.

Shannon's expansion

$$\exists v.\phi := \phi|v = \bot \vee \phi|v = \top$$

The existential is a disjunction between two possible formulas. One where v is set to true, and one where it is set to false.

$$\forall v.\phi := \phi|v = \bot \wedge \phi|v = \top$$

The universal one is similar, with a conjunction between the two.

Polarity of subformulas

Polarity is a metric defined for each subformula of a formula ϕ that tells us under how many nested negations it occurs. It can either be positive, negative, or both in some cases.
The recursive rules to determine the polarity are shown in the image below

- φ occurs positively in φ;
- if $\neg\varphi_1$ occurs positively [negatively] in φ, then φ_1 occurs negatively [positively] in φ
- if $\varphi_1 \wedge \varphi_2$ or $\varphi_1 \vee \varphi_2$ occur positively [negatively] in φ, then φ_1 and φ_2 occur positively [negatively] in φ;
- if $\varphi_1 \rightarrow \varphi_2$ occurs positively [negatively] in φ, then φ_1 occurs negatively [positively] in φ and φ_2 occurs positively [negatively] in φ;
- if $\varphi_1 \leftrightarrow \varphi_2$ or $\varphi_1 \oplus \varphi_2$ occurs in φ, then φ_1 and φ_2 occur positively and negatively in φ;

If we assume $\top = 1, \bot = 0$ we can also see the polarity of a subformula as "how much it contributes to the overall value of the formula".

2 Normal forms

2.1 Negative Normal Form - NNF

A negative normal form is a formula in which each negations has been pushed down to the atoms. This implies that every subformula in $NNF(\phi)$ has positive polarity.

Properties

- Every formula can be made into negative normal form
- NNF transformation preserves equivalence

2.2 Conjunctive Normal Form - CNF

$$\bigvee_{i=1}^{L} \bigwedge_{j=1}^{K_i} l_{ij}$$

$$(l_{11} \wedge l_{12}) \vee (l_{21} \wedge l_{22} \wedge l_{23}) \vee (...) \vee ...$$

Every formula can be converted in *Conjunctive Normal Form*, but there are different ways to do so.

2.2.1 Naive CNF conversion

The more intuitive and straightforward method consist of:

1. Expanding implications and equivalences
2. Pushing down negations like in NNF
3. Recursively applying DeMorgan's rule to get the CNF shape

This method produces a CNF that is equivalent to the original formula and has the same atoms. It is however rarely used in practical applications because it can be up to exponentially larger than the original formula.

2.2.2 Labeling CNF conversion

This is a more efficient *bottom-up* approach, which can be executed while parsing the expression.
The main idea is that of introducing new variables that serve as "*labels*" for each subformula. The smaller formulas can be converted to CNF with the naive approach, and then assembled through the labels.

This method introduces new atoms, but $\exists(B_1, \ldots, B_k).CNF_l(\phi)$ equiv ϕ where $B_1, \ldots, B_k$ are the newly introduced variables. This means that ϕ and $CNF_l(\phi)$ are equisatisfiable.

The representation obtained from the CNF_l can be reduced further in size by using polarization to change some implications around.

3 Basic SAT-solving techniques