Formal Methods - 03_Temporal_Logics

Francesco Penasa

February 22, 2020

material lect 03 2020/02/21:
HANDOUTS : `http://disi.unitn.it/~rseba/DIDATTICA/fm2020/03_TEMPORAL_LOGICS_HANDOUT.pdf`
SLIDES : `http://disi.unitn.it/~rseba/DIDATTICA/fm2020/03_TEMPORAL_LOGICS_SLIDES.pdf`

1 Boolean logic

TRUE; FALSE;

1. Boolean formula: $\top = true \ \bot = false$
2. Atoms(ϕ): the set of atoms occurring in ϕ
3. Literal
4. Clause $\vee_j l_j$ (disjunction)
5. Cube $\wedge_j l_j$ (conjunction)

$$(A_1 \to A_2) \leftrightarrow (\neg A_1 \vee A_2)$$

$$XOR \Rightarrow \neg(A_1 \leftrightarrow A_2) \Leftrightarrow (A_1 \vee A_2) \wedge (\neg A_1 \vee \neg A_2)$$

Directed Acyclic Graph (DAG) representation of boolean formulas can be up to exponentially smaller than trees.

1.1 Basic notation & definitions

Total truth assignment: all atoms have to be assigned

Partial Truth assignment lazy evaluation of boolean, we just require to have the atoms needed for the satisfiability about the others we don't care. Actually, all of his extensions to total truth assignment satisfy the formula. ϕ is **satisfiable** iff $\mu \models \phi$ for some μ ϕ_1 **entails** ϕ_2 ($\phi_1 \models \phi_2$): iff $\mu \models \phi_1 \Rightarrow \mu \models \phi_2$ for every μ ϕ **is entails** ($\models \phi$): iff $\mu \models \phi$ for every μ ϕ is valid $\Leftrightarrow \neg\phi$ is not satisfiable

1.2 Equivalence and equi-satifsfiability

When we use **validity-preserving trasformation**
ϕ_1 and ϕ_2 are **equivalent** iff for **every** μ, $\mu \models \phi_1$ iff $\mu \models \phi_2$

When we use **satisfiability-preserving trasformation**
ϕ_1 and ϕ_2 are **equi-satisfiable** iff exists μ_1 s.t. $\mu_1 \models \phi_1$ iff exists μ_2 s.t. $\mu_2 \models \phi_2$
equi-satisfiable tells us nothing about the relations of the two models.

1.3 Complexity

For N variables, there are up to 2^N truth assignments to be checked

1.4 POLARITY

intuition: ϕ_1 occurs positively [negatively] in ϕ iff it occurs under the scope of an (implicit) even [odd] number of negations. **If we transform the formula, we watch where if there is a lnot or if it is positive.**
Polarity: the number of nested negations modulo 2

1.5 Substitution principle

$$\phi[\phi_1|\phi_2]$$

we substitute in ϕ, ϕ_2 over all occurrences of ϕ_1.

1. if equivalent then guess, it is easy
2. if entails, then it entails but only if applied on something that occurs only positively.

1.5.1 Negative normal form (NNF)

If it is formed only by $\wedge$ and $\vee$ to literals

1. 1) substitute all implications ($\rightarrow$ and $\leftrightarrow$)
2. 2) push down negations to the literals $\neg(A_1 \vee A_2) \Rightarrow (\neg A_1 \wedge \neg A_2)$

The reduction to NNF is linear if it is represented as a DAG and the equivalence is preserved.

1.5.2 Conjunctive normal form (CNF)

$$\wedge_{i=1}^{L} \vee_{j_i=1}^{Ki} l_{j_i}$$

Classic CNF conversion

1. convert to NNF
2. apply recursively the Demorgan's Rule:

$$(\phi_1 \wedge \phi_2) \vee \phi_3 \Rightarrow (\phi_1 \vee \phi_3) \wedge (\phi_2 \vee \phi_3)$$

3. exponential time
4. but equivalent

Labeling CNF conversion We use some alias to reduce the complexity

1. linear time
2. equi-satisfiable

Of course further optimizations can be executed.

2 Questions

POLARITY third point slide 14/108