9.0

Software Analysis & Verification **Due: Mar 3, 2020**

Homework 1

Instructor: Fei He Chenhao Li (2017011466)
TA: Jianhui Chen, Fengmin Zhu

Read the instructions below carefully before you start working on the assignment:

- Please typeset your answers in the attached LaTeX source file, compile it to a PDF, and finally hand the PDF to Tsinghua Web Learning *before the due date*.
- Make sure you fill in your *name* and *Tsinghua ID*, and replace all "`TODO`"s with your solutions.
- Any kind of dishonesty is *strictly prohibited* in the full semester. If you refer to any material that is not provided by us, you *must cite* it.

Problem 1: True of False

Are the following statements true or false? If false, provide a counterexample.

1-1 Given an arbitrary propositional logic formula, the problem of deciding its validity is decidable.

Solution True ■

1-2 If a propositional logic formula is not valid, then it is unsatisfiable.

Solution False
Counterexample: P is not valid, but it is satisfiable. ■

1-3 Every NNF is also a CNF.

Solution False
Counterexample: $(P \wedge Q) \vee R$ is a NNF, but is not a CNF. ■

1-4 A propositional logic formula φ is satisfiable if and only if for every interpretation I, $I \models \varphi$.

Solution False
φ is satisfiable if and only if there exists interpretation I, $I \models \varphi$. ■

1-5 If clause C is a unit under an interpretation I, then $I \not\models C$.

Solution False
The value of C is undefined under interpretation I. ■

Problem 2: Normal Forms

2-1 Convert the following formula into NNF and then DNF:

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

Solution

$$\begin{aligned}
&\neg(\neg(P \wedge Q) \to \neg R) \\
&= \neg((P \wedge Q) \vee \neg R) \\
&= \neg(P \wedge Q) \wedge R \\
&= (\neg P \vee \neg Q) \wedge R \cdots \text{NNF} \\
&= (\neg P \wedge R) \vee (\neg Q \wedge R) \cdots \text{DNF}
\end{aligned}$$

■

2-2 Convert the following formula into CNF with and without Tseitin's transformation:

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

Solution

1. With Tseitin's transformation

$$\begin{aligned}
F_1 &= T_1 \leftrightarrow \neg Q \wedge R = (\neg T_1 \vee \neg Q) \wedge (\neg T_1 \vee R) \wedge (T_1 \vee Q \vee \neg R) \\
F_2 &= T_2 \leftrightarrow P \to T1 = (\neg T_2 \vee \neg P \vee T_1) \wedge (T_2 \vee P) \wedge (T_2 \vee \neg T_1) \\
F_3 &= T_3 \leftrightarrow P \to \neg Q = (\neg T_3 \vee \neg P \vee \neg Q) \wedge (T_3 \vee P) \wedge (T_3 \vee Q) \\
F_4 &= T_4 \leftrightarrow T2 \wedge T3 = (\neg T_4 \vee T_2) \wedge (\neg T_4 \vee T_3) \wedge (T_4 \vee \neg T_2 \vee \neg T_3) \\
\text{CNF} &= T_4 \wedge F_1 \wedge F_2 \wedge F_3 \wedge F_4
\end{aligned}$$

2. Without Tseitin's transformation

$$\begin{aligned}
&(P \to (\neg Q \wedge R)) \wedge (P \to \neg Q) \\
&= (\neg P \vee (\neg Q \wedge R)) \wedge (\neg P \vee \neg Q) \\
&= (\neg P \vee \neg Q) \wedge (\neg P \vee R) \wedge (\neg P \vee \neg Q)
\end{aligned}$$

■

Problem 3: Validity & Satisfiability

3-1 Consider the following formula:

$$(P \to (Q \to R)) \to (\neg R \to (\neg Q \to \neg P))$$

Is it valid? If not, provide a falsifying interpretation. Moreover, is it satisfiable? If so, provide a satisfying interpretation.

Solution It is not valid. There exists interpretation $I = \{P \mapsto true, Q \mapsto false, R \mapsto false\}$, such that $I \not\models F$.

It is satisfiable. There exists interpretation $I = \{P \mapsto true, Q \mapsto true, R \mapsto false\}$, such that $I \models F$. ■

3-2 Show the validity of the following formula using the semantic argument method:

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

Solution

1. $I \not\models \neg(P \land Q) \leftrightarrow (\neg P \lor \neg Q)$
2. $I \models \neg(P \land Q) \land \neg(\neg P \lor \neg Q)$ (1 and $\leftrightarrow$, case A)
3. $I \models \neg(P \land Q)$ (2 and $\land$)
4. $I \models \neg(\neg P \lor \neg Q)$ (2 and $\land$)
5. $I \not\models P \land Q$ (4 and $\neg$)
6. $I \not\models P$ (5 and $\land$, case A)
7. $I \not\models \neg P \lor \neg Q$ (3 and $\neg$)
8. $I \not\models \neg P$ (7 and $\lor$)
9. $\perp$ (6 and 8)
10. $I \not\models Q$ (5 and $\land$, case B)
11. $I \not\models \neg Q$ (7 and $\lor$)
12. $\perp$ (10 and 11)
13. $I \models (P \land Q) \land \neg\neg(\neg P \lor \neg Q)$ (1 and $\leftrightarrow$, case B)
14. $I \models P \land Q$ (13 and $\land$)
15. $I \models P$ (14 and $\land$)
16. $I \models \neg\neg(\neg P \lor \neg Q)$ (13 and $\land$)
17. $I \not\models \neg(\neg P \lor \neg Q)$ (16 and $\neg$)
18. $I \models (\neg P \lor \neg Q)$ (17 and $\neg$)
19. $I \models \neg P$ (18 and $\lor$, case A)
20. $I \not\models P$ (19 and $\neg$)
21. $\perp$ (15 and 21)
22. $I \models Q$ (14 and $\land$)
23. $I \models \neg Q$ (18 and $\lor$, case B)
24. $I \not\models Q$ (23 and $\neg$)
25. $\perp$ (22 and 24)

Therefore, every branch reaches contradiction, so F is valid. ■

3-3 Show the satisfiability of the following formula by resolution:

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

Then, give a general form of all satisfying interpretations.

Solution

1. $\neg P \vee \neg Q$
2. $\neg P \vee R$
3. $Q \vee \neg R$
4. $\neg P \vee \neg R$ (1 and 3)
5. $\neg P \vee Q$ (2 and 3)
6. $\neg P$ (2 and 4)

Now there is no more possible resolvent, so F is satisfiable.
All satisfying interpretations have the form of $\{P \mapsto false, Q, R\}$, where $Q \vee \neg R = true$. ■

Problem 4: Modeling

A *nondeterministic finite automaton* (NFA) is given by a 5-tuple $(Q, \Sigma, \delta, I, F)$, where:

- Q is a finite set of states
- Σ is a finite alphabet
- $\delta : Q \times \Sigma \times 2^Q$ is a transition function
- $I \subseteq Q$ is a set of initial states
- $F \subseteq Q$ is a set of final (accepting) states

An NFA accepts a finite word (or, a char sequence) $w = [c_0, \dots, c_n]$, where $c_i \in \Sigma$, if and only if there is a sequence of states $q_0, \dots, q_n$, with $q_i \in Q$, such that:

- $q_0 \in I$
- For all $i \in \{1, \dots, n\}$, $q_i \in \delta(q_{i-1}, w_i)$
- $q_n \in F$

4-1 Given an NFA $M = (Q, \Sigma, \delta, I, F)$ and a fixed input string w, describe how to construct a propositional formula that is satisfiable if and only if M accepts w.

Hint Consider defining propositional variables that correspond to the initial states, final states, transition function, and alphabet symbols in w. Then think about "unwinding" the NFA on w. Do you need to define additional variables? How can you encode the fact that w is accepted?

Solution First define the following propositional variables:

- $I_i = true$ iff $q_i \in I$, where $q_i \in Q, i \in \{1, \dots, |Q|\}$
- $F_i = true$ iff $q_i \in F$, where $q_i \in Q, i \in \{1, \dots, |Q|\}$
- $T_{i,c,j} = true$ iff $q_j \in \delta(q_i, c)$, where $q_i, q_j \in Q, i, j \in \{1, \dots, |Q|\}, c \in \Sigma$

Then define formula:

$$AC = \bigvee_{i_0=1}^{|Q|} \bigvee_{i_1=1}^{|Q|} \dots \bigvee_{i_n=1}^{|Q|} I_{i_0} \wedge F_{i_n} \wedge \bigwedge_{j=1}^{n} T_{i_{j-1}, w_j, i_j}$$

Assert that $AC = true$ iff M accepts w. ■

4-2 Demonstrate your encoding on the NFA shown in Figure 1.

Solution

- $I_0 = true$
- $F_3 = true$
- $T_{0,0,0} = true, T_{0,0,1} = true, T_{0,1,0} = true, T_{0,1,2} = true$
- $T_{1,0,3} = true$
- $T_{2,1,3} = true$
- $T_{3,0,3} = true, T_{3,1,3} = true$

-1.0

Any defined but unlisted propositional variable has the value *false*. ■

$$
\begin{aligned}
Q &= \{q_0, q_1, q_2, q_3\} \\
\Sigma &= \{0, 1\} \\
\delta &= \{(q_0, 0) \mapsto q_0, \\
&\quad (q_0, 1) \mapsto q_0, \\
&\quad (q_0, 0) \mapsto q_1, \\
&\quad (q_0, 1) \mapsto q_2, \\
&\quad (q_1, 0) \mapsto q_3, \\
&\quad (q_2, 1) \mapsto q_3, \\
&\quad (q_3, 0) \mapsto q_3, \\
&\quad (q_3, 1) \mapsto q_3\} \\
I &= \{q_0\} \\
F &= \{q_3\}
\end{aligned}
$$

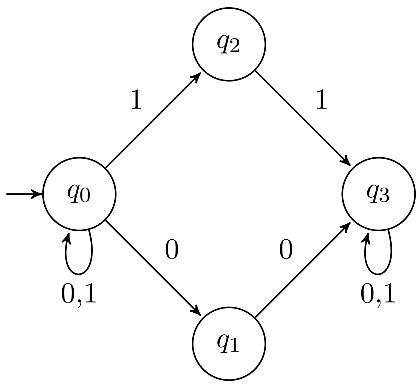

Figure 1: An NFA.