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

# Homework 1

*Instructor: Fei He* Charles Shen (2017013569)

*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.
Consider F=P, when P is False, F is False, F is not valid. But when P is True, F is True, F is satisfiable.
■

**1-3** Every NNF is also a CNF.

**Solution** False.
$(\neg P \land \neg Q) \lor R$ is a NNF, but not a CNF. ■

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

**Solution** False.
$\phi = P$ is satisfiable, since there exists $I = P \mapsto true, I \models \phi$.But there also exists $I = P \mapsto false, I \not\models \phi$.
■

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

**Solution** False.

Consider $C = P \vee Q, I = \{P \mapsto true, Q \mapsto undef\}$.

$C' = P, l = Q, C = C' \vee l, I \not\models C'$, C is unit under I, but $I \not\models C$ is not right in such case. ∎

# Problem 2: Normal Forms

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

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

**Solution** 1.$\neg((P \wedge Q) \vee \neg R)$
2.$\neg(P \wedge Q) \wedge R$
3.$(\neg P \vee \neg Q) \wedge R$, Now it is a NNF
4.$(\neg P \wedge R) \vee (\neg Q \wedge R)$,Now it is a DNF. ■

**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** No Tseitin:
1.$(\neg P \vee (\neg Q \wedge R)) \wedge (\neg P \vee \neg Q)$
2.$(\neg P \vee \neg Q) \wedge (\neg P \vee R) \wedge (\neg P \vee \neg Q)$
Tseitin:
$F1 = T1 \leftrightarrow \neg Q \wedge R$
$= (\neg T1 \vee \neg Q) \wedge (\neg T1 \vee R) \wedge (Q \vee \neg R \vee T1)$
$F2 = T2 \leftrightarrow P \to T1$
$= (\not T2 \vee \neg P \vee T1) \wedge (P \vee T2) \wedge (\neg T1 \vee T2)$
$F3 = T3 \leftrightarrow P \to \neg Q$
$= (\neg T3 \vee \neg P \vee \neg Q) \wedge (P \vee T3) \wedge (Q \vee T3)$
$F4 = T4 \leftrightarrow T2 \wedge T3$
$= (\neg T4 \vee T2) \wedge (\neg T4 \vee T3) \wedge (\neg T2 \vee \neg T3 \vee T4)$
$F = T4 \wedge F1 \wedge F2 \wedge F3 \wedge F4$
■

## 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** Not Valid, consider $I = \{P| \mapsto true, Q| \mapsto false, R| \mapsto false\}$
Satisfiable, consider $I = \{P| \mapsto true, Q| \mapsto true, R| \mapsto true\}$ ■

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

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

**Solution** $1.I \not\models \neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$
$2.I \models (P \wedge Q) \wedge (\neg P \vee \neg Q)(1, \leftrightarrow, caseA)$
$3.I \models \neg(P \wedge Q) \wedge (P \wedge Q)(1, \leftrightarrow, caseB)$
$4.I \models P \wedge Q(2, \wedge, caseA)$
$5.I \models \neg P \vee \neg Q(2, \wedge, caseA)$
$6.I \not\models P \wedge Q(5, \neg, caseA)$
For case A, 4 and 6 reach a contradiction.
$7.I \models \neg(P \wedge Q)(3, \wedge, caseB)$
$8.I \models (P \wedge Q)(3, \wedge, caseB)$
For case A, 7 and 8 reach a contradiction.
Since all the branches have reached contradiction, the formula given above 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** Round 1:
$F1 = \neg P \vee \neg Q$
$F2 = \neg P \vee R$
$F3 = Q \vee \neg R$
$F' =$
$F = \{F1, F2, F3\}$
Round 2:
$F4 = \neg P \vee \neg R(1\&3)$
$F5 = \neg P \vee Q(2\&3)$
$F' = \{F4, F5\}$

$F = \{F1, F2, F3, F4, F5\}$

Round 3:

$F6 = \neg P(1\&5)$

$F' = \{F4, F5, F6\}$

$F = \{F1, F2, F3, F4, F5, F6\}$

Round 4:

$F' = \{F4, F5, F6\}$

$F = \{F1, F2, F3, F4, F5, F6\}$

$F' \subseteq F$

Therefore, the formula is satisfiable.

The general form is $\{P \mapsto false, Q \mapsto true\} or \{P \mapsto false, R \mapsto false\}$.■

## 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
- $\Sigma$ 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) $w = [c_0, \ldots, c_n]$, where $c_i \in \Sigma$, if and only if there is a sequence of states $q_0, \ldots, q_n$, with $q_i \in Q$, such that:

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

**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** 为了避免空产生式带来的不利影响，我们首先把 NFA 转化为 DFA 进行处理。
假设 w 长度为 n，转化的 DFA 有 m 个状态:$q_0, q_1 ... q_{m-1}$, 其状态转移为 $\sigma$。输入串 w 在 DFA 中的路径为 $q_{s_0}, q_{s_1} ... q_{s_n}$
定义两种类型的文字：$S_{i,j}(0 \le i \le n; q_j \in Q)$ 代表已经输入 i 个字符后，状态为 $q_j$，特别的，i 为 0 代表初态为 $q_j$。$C_{i,j,k}(q_i, q_k \in Q; j \in \Sigma)$ 代表当前状态为 $q_i$ 时，输入 j，状态变为 $q_k$。
设计成这样：要保证所有的文字满足以下几点，才成立：
1. 初态正确：当且仅当 $q_j$ 为初态,$S_{0,j}$ 为真。这个规则是为了保证输入前状态在初态。
2. 终态正确：当且仅当 $q_j$ 为终态，$S_{n,j}$ 为真。这个规则是为了保证输入 w 完毕后状态可接受。
3. 转换正确：对于任意的 $1 \le t \le n; q_i, q_k \in Q, j \in \Sigma$，当仅当 $\sigma(q_i, j) = q_k$，有 $S_{t-1,i} \wedge S_{t,k} \wedge C_{i,j,k}$ 为真。这个规则是为了保证每一步转换严格按照自动机规则进行。
如果 w 可以被自动机接受，那么不会产生矛盾，这个式子可满足。
相反，如果 w 不可被自动机接受，那么规则 3 要求终态对应的 $S_{n,q_{s_n}}$ 为真，规则 2 要求终态对应的 $S_{n,q_{s_n}}$ 为假，矛盾，这个式子不可满足。$F = \bigwedge_{q_i \in I} S_{0,i}$
$\wedge \bigwedge_{q_i \notin I} \neg(S_{0,i})$
$\wedge \bigwedge_{q_i \in F} S_{n,i}$
$\wedge \bigwedge_{q_i \notin F} \neg(S_{n,i})$
$\wedge \bigwedge_{1 \le t \le n; q_{s_{t-1}}, q_{s_t} \in Q; \sigma(q_{s_{t-1}}, w_t) = q_{s_t}} (S_{t-1,s_{t-1}} \wedge C_{s_{t-1},w_t,s_t} \wedge S_{t,s_t})$
■

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

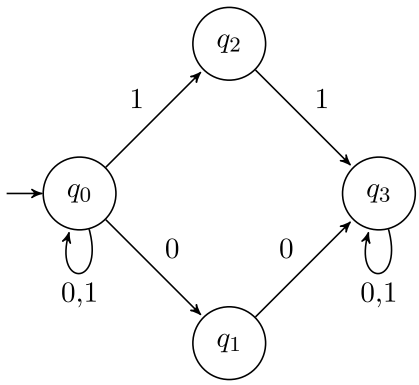


图 1: An NFA.

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

**Solution** 1. 将这个 NFA 转化为 DFA, 如下:
令 w = 00, 那么路径变为 $q_0, q_1, q_3$, 式子变为
$S_{00} \wedge \neg S_{01} \wedge \neg S_{02} \wedge \neg S_{03} \wedge \neg S_{04} \wedge S_{11} \wedge C_{001} \wedge C_{103} \wedge S_{23} \wedge S_{24}$
$land \neg S_{20} \wedge \neg S_{21} \wedge \neg S_{22}$ ■

$$
\begin{aligned}
Q &= \{q_0, q_1, q_2, q_3\ q_4\} \\
\Sigma &= \{0, 1\} \\
\delta &= \{(q_0, 0) \mapsto q_0, \\
&\qquad (q_0, 1) \mapsto q_2, \\
&\qquad (q_1, 0) \mapsto q_3, \\
&\qquad (q_1, 1) \mapsto q_2, \\
&\qquad (q_2, 0) \mapsto q_1, \\
&\qquad (q_2, 1) \mapsto q_4, \\
&\qquad (q_3, 0) \mapsto q_3, \\
&\qquad (q_3, 1) \mapsto q_4 \\
&\qquad (q_4, 0) \mapsto q_3 \\
&\qquad (q_4, 1) \mapsto q_4\} \\
I &= \{q_0\} \\
F &= \{q_3, q_4\}
\end{aligned}
$$

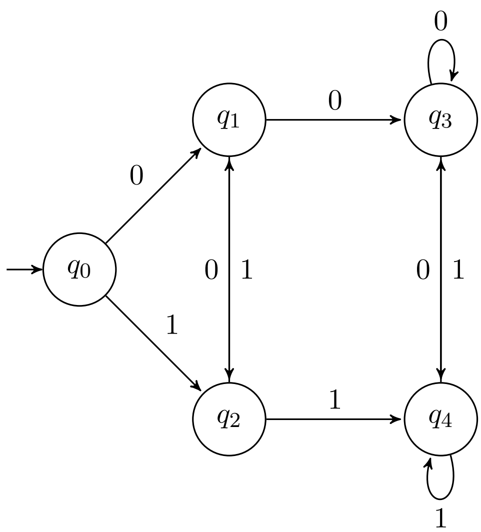


图 2: The DFA according to the problem.