Formal Methods for High-Assurance Software Engineering

HomeWork Assignment 04

Shahin Roozkhosh
shahin@bu.edu
U01670169

September 2020

Problem 1. From Lecture Slides 11, entitled Quantified Boolean Formulas (QBF's):
part 1 Do the exercise on page 31.

Solution. We prove these equivalencies semantically, rather than providing a theoretical proof. Starting with the case that all wff's are quantifier-free.

$\Phi = (\phi \vee \psi_1) \wedge (\phi \vee \psi_2) \wedge (\phi \vee \psi_3)$
$\Psi = \exists y.(y \leftrightarrow \phi) \wedge (y \vee \psi_1) \wedge (y \vee \psi_2) \wedge (y \vee \psi_3)$

In order to show $\Phi \equiv \Psi$ it is sufficient to, semantically speaking, compare the last column of their truth tables and as you can see below, last columns of the truth tables for Φ and Ψ are exactly compatible, hence they are equivalent.

truth-table for WFF $\Phi = (\phi \vee \psi_1) \wedge (\phi \vee \psi_2) \wedge (\phi \vee \psi_3)$

ϕ	ψ_1	ψ_2	ψ_3	$\phi \vee \psi_1$	$\phi \vee \psi_2$	$\phi \vee \psi_3$	Φ
F	**F**	**F**	**F**	**F**	**F**	**F**	**F**
F	**F**	**F**	**T**	**F**	**F**	**T**	**F**
F	**F**	**T**	**F**	**F**	**T**	**F**	**F**
F	**F**	**T**	**T**	**F**	**T**	**T**	**F**
F	**T**	**F**	**F**	**T**	**F**	**F**	**F**
F	**T**	**F**	**T**	**T**	**F**	**T**	**F**
F	**T**	**T**	**F**	**T**	**T**	**F**	**F**
F	**T**	**T**	**T**	**T**	**T**	**T**	**T**
T	**F**	**F**	**F**	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**T**	**T**	**T**	**T**
T	**F**	**T**	**F**	**T**	**T**	**T**	**T**
T	**F**	**T**	**T**	**T**	**T**	**T**	**T**
T	**T**	**F**	**F**	**T**	**T**	**T**	**T**
T	**T**	**F**	**T**	**T**	**T**	**T**	**T**
T	**T**	**T**	**F**	**T**	**T**	**T**	**T**
T	**T**	**T**	**T**	**T**	**T**	**T**	**T**

truth-table for WFF $\Psi = \exists y.(y \leftrightarrow \phi) \wedge (y \vee \psi_1) \wedge (y \vee \psi_2) \wedge (y \vee \psi_3)$ (next page)

ϕ	ψ_1	ψ_2	ψ_3	$[y=0] \leftrightarrow \phi$	$[y=1] \leftrightarrow \phi$	$[y=0] \leftrightarrow \psi_1$	$[y=1] \leftrightarrow \psi_1$	$[y=0] \leftrightarrow \psi_2$	$[y=1] \leftrightarrow \psi_2$	$[y=0] \leftrightarrow \psi_3$	$[y=1] \leftrightarrow \psi_3$	$\Psi[y=0]$	$\Psi[y=1]$	Ψ
F	**F**	**F**	**F**	**T**	**F**	**F**	**T**	**F**	**T**	**F**	**T**	**F**	**F**	**F**
F	**F**	**F**	**T**	**T**	**F**	**F**	**T**	**F**	**T**	**T**	**T**	**F**	**F**	**F**
F	**F**	**T**	**F**	**T**	**F**	**F**	**T**	**T**	**T**	**F**	**T**	**F**	**F**	**F**
F	**F**	**T**	**T**	**T**	**F**	**F**	**T**	**T**	**T**	**T**	**T**	**F**	**F**	**F**
F	**T**	**F**	**F**	**T**	**F**	**T**	**T**	**F**	**T**	**F**	**T**	**F**	**F**	**F**
F	**T**	**F**	**T**	**T**	**F**	**T**	**T**	**F**	**T**	**T**	**T**	**F**	**F**	**F**
F	**T**	**T**	**F**	**T**	**F**	**T**	**T**	**T**	**T**	**F**	**T**	**F**	**F**	**F**
F	**T**	**T**	**T**	**T**	**F**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**F**	**T**
T	**F**	**F**	**F**	**F**	**T**	**F**	**T**	**F**	**T**	**F**	**T**	**F**	**T**	**T**
T	**F**	**F**	**T**	**F**	**T**	**F**	**T**	**F**	**T**	**T**	**T**	**F**	**T**	**T**
T	**F**	**T**	**F**	**F**	**T**	**F**	**T**	**T**	**T**	**F**	**T**	**F**	**T**	**T**
T	**F**	**T**	**T**	**F**	**T**	**F**	**T**	**T**	**T**	**T**	**T**	**F**	**T**	**T**
T	**T**	**F**	**F**	**F**	**T**	**T**	**T**	**F**	**T**	**F**	**T**	**F**	**T**	**T**
T	**T**	**F**	**T**	**F**	**T**	**T**	**T**	**F**	**T**	**T**	**T**	**F**	**T**	**T**
T	**T**	**T**	**F**	**F**	**T**	**T**	**T**	**T**	**T**	**F**	**T**	**F**	**T**	**T**
T	**T**	**T**	**T**	**F**	**T**	**T**	**T**	**T**	**T**	**T**	**T**	**F**	**T**	**T**

part 2 Do the exercise on page 32.

Problem 3. LCS 2.3.3 on page 160
Write down a sentence of predicate logic which intuitively holds in a model iff the model has (respectively):

part a) exactly three distinct elements:

Solution.

$$\exists x \exists y \exists z (((\neg(x = y) \wedge \neg(x = z)) \wedge \neg(y = x)) \wedge \forall t (((t = x) \vee (t = y)) \vee (t = z))) \tag{1}$$

part b) At most three distinct elements:

Solution. The answer is:

$$\phi_1 \wedge \phi_2 \wedge \phi_3 \tag{2}$$

As defined bellow:
ϕ_1 describes Model with exactly one element as:

$$\phi_1 = \exists x \forall t (t = x) \tag{3}$$

ϕ_2 describes Models with exactly two element:

$$\phi_2 = \exists x \exists y (\neg(x = y)) \wedge \forall t ((t = x) \vee (t = y)) \tag{4}$$

ϕ_3 describes M_3 as:

$$\phi_3 = \exists x \exists y \exists z (((\neg(x = y) \wedge \neg(x = z)) \wedge \neg(y = x)) \wedge \forall t (((t = x) \vee (t = y)) \vee (t = z))) \tag{5}$$

part c) Write down an infinite set of FO sentences which hold in a model iff the model has infinitely many distinct elements.

Solution. We define model $M_{k(k=0,\cdots,\infty)}$ such that the model M_k is a set of models with **exactly** k distinct elements. These models definately exist and could be constructed following the approach we took at section (a) as an example for **exactly** 3 elements. Then the answer to this part would be a logical or over all formulas of ϕ_i where ϕ_i describes M_i.

$$\bigwedge_{i \geq 1} \phi_i \tag{6}$$

For example:

ϕ_1 describes M_1 as:

$$\phi_1 = \exists x \forall t (t = x) \tag{7}$$

ϕ_2 describes M_2 as:

$$\phi_2 = \exists x \exists y (\neg(x = y)) \wedge \forall t ((t = x) \vee (t = y)) \tag{8}$$

ϕ_3 describes M_3 as:

$$\phi_3 = \exists x \exists y \exists z (((\neg(x = y) \wedge \neg(x = z)) \wedge \neg(y = x)) \wedge \forall t (((t = x) \vee (t = y)) \vee (t = z))) \tag{9}$$

Problem 4. LCS 2.3.9 on page 161
Prove the validity of the following sequents in predicate logic, where F , G, P , and Q have arity 1, and S has arity 0 (a 'propositional atom'):

part a

Solution.

$$\exists (S \to Q(x)) \vdash S \to \exists x\, Q(x) \tag{10}$$

1	$\exists(S \to Q(x))$	premise
2	S	assume
3	x_0	
4	$S \to Q(x_0)$	assume
5	$Q(x_0)$	$\to$e$4, 2$
6	$\exists x Q(x)$	$\exists x$i$, 5$
7	$\exists Q(x)$	$\exists x$e$, 1, 3-6$
8	$Q(x)$	$\to$i $2-7$

part b

Solution.

$$S \to \exists x Q(x) \vdash \exists x(S \to Q(x)) \tag{11}$$

1	$S \to \exists x Q(x)$	premise
2	$S \vee \neg S$	LEM
3	S	assume
4	$\exists x Q(x)$	$\to$e$1, 5$
5	$\neg S \vee \exists x Q(x)$	$\vee$i$_2, 6$
6	$\neg S$	assume
7	$\neg S \vee \exists x Q(x))$	$\vee$i$_1, 3$
8	$\neg S \vee \exists x Q(x)$	$\vee$e$2, 3-4, 5-7$
9	$\neg S$	assume
10	S	assume
11	$\bot$	$\neg$e$9, 10$
12	$Q(x_0)$	$\bot$e11
13	$S \to Q(x_0)$	$\to$i$10-12$
14	$\exists x(S \to Q(x))$	$\exists x$i13
15	$\exists x Q(x)$	assume
16	x_0	
17	$Q(x_0)$	assume
18	S	assume
19	$Q(x_0)$	17
20	$S \to Q(x_0)$	$\to$i$17-18$
21	$\exists x(S \to Q(x))$	$\exists x$i19
22	$\exists x(S \to Q(x))$	$\exists x$e$15, 17-20$
23	$\exists x(S \to Q(x))$	$\vee$e$8, 9-14, 15-21, 1, 3-6$

part c

Solution.

$$\exists x P(x) \to S \vdash \forall x(P(x) \to S) \tag{12}$$

1	$\exists x P(x) \rightarrow S$	premise
2	x_0	
3	$P(x_0)$	assume
4	$\exists x P(x)$	$\exists x$i 3
5	S	$\rightarrow$e $1, 4$
6	$P(x_0) \rightarrow S$	$\rightarrow$i $3 - 5$
7	$\forall x (P(x) \rightarrow S)$	$\forall x$i $2 - 6$

---

part d

Solution.

$$\forall x P(x) \rightarrow S \vdash \exists x (P(x) \rightarrow S) \tag{13}$$

1	$\forall x P(x) \to S$	premise
2	$\neg \exists x (P(x) \to S)$	assume
3	x_0	
4	$\neg P(x_0)$	assume
5	$P(x_0)$	assume
6	$\bot$	$\neg$e4, 5
7	S	$\bot$e6
8	$P(x_0) \to S$	$\to$i5 $-$ 7
9	$\exists x (P(x) \to S)$	$\exists x$i, 8
10	$\bot$	$\neg$e9, 2
11	$\neg\neg P(x_0)$	$\neg$i, 4 $-$ 10
12	$P(x_0)$	$\neg\neg$e, 11
13	$\forall x P(x)$	$\forall x$i, 3 $-$ 12
14	S	$\to$e1, 13
15	$P(x)$	assume
16	S	14
17	$P(x) \to S$	$\to$i15 $-$ 16
18	$\exists x (P(x) \to S)$	$\exists x$i, 17
19	$\bot$	$\neg$e2, 18
20	$\neg\neg \exists x (P(x) \to S)$	$\neg$i2 $-$ 19
21	$\exists x (P(x) \to S)$	$\neg\neg$e20

Problem 5.

Solution. `https://github.com/ro0zkhosh/CS511/blob/master/HW4/shahin_streamroller.py`

Problem 6.

Solution. https://github.com/ro0zkhosh/CS511/blob/master/HW4/shahin_whokilledaunty.in

Who killed Aunt Agatha? Buttler did! Here's the output of the prover8:

```
============================== PROOF =================================

% Proof 1 at 0.01 (+ 0.01) seconds.
% Length of proof is 16.
% Level of proof is 6.
% Maximum clause weight is 12.000.
% Given clauses 15.

1 (exists x (LivesIn(x,D) & Killed(x,A))) # label(non_clause).  [assumption].
2 LivesIn(A,D) & LivesIn(B,D) & LivesIn(C,D) & (all x (LivesIn(x,D) -> x = A | x = B | x = C)) # label(non_clause).  [assumption].
9 (exists x ((x = A | x = C | x = B) & Killed(x,A))) # label(non_clause) # label(goal).  [goal].
12 LivesIn(c1,D).  [clausify(1)].
13 Killed(c1,A).  [clausify(1)].
17 -LivesIn(x,D) | A = x | B = x | C = x.  [clausify(2)].
25 A != x | -Killed(x,A).  [deny(9)].
26 C != x | -Killed(x,A).  [deny(9)].
27 B != x | -Killed(x,A).  [deny(9)].
29 c1 = A | c1 = B | c1 = C.  [resolve(17,a,12,a),flip(a),flip(b),flip(c)].
34 c1 != A.  [resolve(25,b,13,a),flip(a)].
36 c1 = B | c1 = C.  [back_unit_del(29),unit_del(a,34)].
37 c1 != C.  [resolve(26,b,13,a),flip(a)].
39 c1 = B.  [back_unit_del(36),unit_del(b,37)].
41 Killed(B,A).  [back_rewrite(13),rewrite([39(1)])].
42 $F.  [ur(27,a,xx),unit_del(a,41)].

============================== end of proof ==========================
```

According to the line 41, Buttler is the killer.

First Order formulas:

1. Someone who lives in Dreadbury Mansion killed Aunt Agatha.

$$\exists x(LivesIn(x,D) \wedge Killed(x,A)) \tag{14}$$

2. Agatha, the butler, and Charles live in Dreadbury Mansion, and are the only people who live therein.

$$\begin{aligned} LivesIn(A,D) \wedge LivesIn(B,D) \wedge LivesIn(C,D) \\ \wedge(\forall x(LivesIn(x,D) \rightarrow ((x=A) \vee (x=B) \vee (x=C))) \end{aligned} \tag{15}$$

3. A killer always hates his victim, and is never richer than his victim.

$$\forall x\ Killed(x,y) \rightarrow (Hates(x,y) \wedge \neg(RicherThan(x,y))) \tag{16}$$

4. Charles hates no one that Aunt Agatha hates.

$$\forall x\ Hates(A,x) \rightarrow \neg Hates(C,x) \tag{17}$$

5. Agatha hates everyone except the butler.

$$\forall x(\neg(x = B) \rightarrow Hates(A, x)) \tag{18}$$

6. The butler hates everyone not richer than Aunt Agatha.

$$\forall x(\neg RicherThan(x, A) \rightarrow Hates(B, x)) \tag{19}$$

7. The butler hates everyone Aunt Agatha hates.

$$\forall x\ (Hates(A, x) \rightarrow Hates(B, x)) \tag{20}$$

8. No one hates everyone.

$$\forall y(\exists x\ \neg Hates(y, x)) \tag{21}$$

9. Agatha is not the butler.

$$\neg(A = B) \tag{22}$$