Software Analysis & Verification	**Due: Mar 31, 2020**

Homework 3

Instructor: Fei He
TA: Jianhui Chen, Fengmin Zhu
Guanlin Shen (2017013569)

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: Short-Answered Questions

1-1 First-order logic is "semidecidable" – which half is decidable?

Solution When F is valid/ not satisfiable, its validity/satisfiability is decidable. ■

1-2 Are the following statements about $T_{\mathbb{Z}}$ true? Briefly explain the reason (you may use conclusions from lectures).

(a) $T_{\mathbb{Z}}$ is decidable.

(b) $T_{\mathbb{Z}}$ is complete.

(c) If a formula ϕ is both a $\Sigma_{\mathbb{Z}}$-formula and a $\Sigma_{\mathbb{N}}$-formula, then: ϕ is $T_{\mathbb{N}}$-valid if and only if ϕ is $T_{\mathbb{Z}}$-valid.

Solution (a):True
(b):True
Since T_N us decidable and complete, and $T_{\mathbb{Z}}$ can be reduced to T_N,$T_{\mathbb{Z}}$ is decidable and complete.
(c):False
$(x + y = 0) \rightarrow (x = 0 \wedge y = 0)$ is valid in T_N but not valid in $T_{\mathbb{Z}}$.
■

1-3 Is the following formula T_A-valid? Briefly explain the reason:

$$(a[i] = x \wedge x = y) \rightarrow a\langle i \triangleleft y\rangle = a$$

Solution valid
1.$I \not\models F$,assumption
2.$I \models (a[i] = x \wedge x = y)$,1
3.$I \not\models a\langle i \triangleleft y\rangle = a$,1
4.$I \models a[i] = x$, 2
5.$I \models x = y$, 2
6.$a[i] = y$, 4,5,equality
7.$I \not\models \forall j(a\langle i \triangleleft y\rangle[j] = a[j])$, 2

8.$I[j \mapsto c_j] \not\models a\langle i \triangleleft y\rangle[j] = a[j]$,1,$\forall$
9.$I[j \mapsto c_j] \models a\langle i \triangleleft y\rangle[j] \neq a[j])$,8
10.$I[j \mapsto c_j] \models i = j$,9,r.o.w,2
11.$I[j \mapsto c_j] \models a[i] = a[j]$,10, congruence
12.$I[j \mapsto c_j] \models a\langle i \triangleleft y\rangle[j] = y$,11, r.o.w,1
13.$I[j \mapsto c_j] \models a\langle i \triangleleft y\rangle[j] = a[j]$,5,12, equality
14.$\perp$,8,13 ■

1-4 T_A is not convex – show that by providing a counterexample.

Solution $F : a\langle i \triangleleft v\rangle[j] = u$
$F \Rightarrow u = v \vee u = a[j]$
neither $F \Rightarrow u = v$ nor $F \Rightarrow u = a[j]$
■

Problem 2: Semantic Argument

Use the semantic method to check the validity of the following formulas. If not valid, please find a counterexample (a falsifying interpretation in its theory).

2-1 In T_E: $f(f(f(a))) = f(f(a)) \wedge f(f(f(f(a)))) = a \rightarrow (f(a) = a)$

Solution valid
1.$I \not\models F$,assumption
2.$I \models f(f(f(a))) = f(f(a)) \wedge f(f(f(f(a)))) = a$,1
3.$I \not\models f(a) = a$,1
4.$I \models f(f(f(a))) = f(f(a))$, 2
5.$I \models f(f(f(f(a)))) = a$, 2
6.$I \models f(f(f(f(a)))) = f(f(f(a)))$, 4,function congruence
7.$I \models f(f(f(f(a)))) = f(f(a))$,4,6,transitivity
8.$I \models a = f(f(a))$,5,7,transitivity
9.$I \models f(a) = f(f(f(a)))$, 8, function congruence
10.$I \models f(f(f(a))) = a$, 4,8,transitivity
11.$I \models a = f(a)$, 9,10,transitivity
12.$\perp$,3,11
■

2-2 In $T_{\mathbb{Z}}$: $(1 \leq x \wedge x \leq 2) \rightarrow (x = 1 \vee x = 2)$

Solution valid
1.$I \not\models F$,assumption
2.$I \models 1 \leq x \wedge x \leq 2$, 1
3.$I \not\models (x = 1 \vee x = 2)$, 1
4.$I \models 1 \leq x$, 2
5.$I \models x \leq 2$, 2
6.$I \not\models x = 1$, 3
7.$I \not\models x = 2$, 3
8.$\perp$,2,6,7,$T_{\mathbb{Z}}$
■

2-3 In T_A: $a\langle i \triangleleft e\rangle[j] = e \rightarrow a[j] = e$

Solution not valid:
e.g:$i = 1, j = 1, a[1] = 2, e = 3$
$a\langle i \triangleleft e\rangle[j] = 3 = e$,but $a[j] = a[1] = 2 \neq e$,invalid ■

Problem 3: Decision Procedure for Theories

3-1 Apply the decision procedure for quantifier-free T_E to the following Σ_E-formula:

$$p(x) \wedge f(f(x)) = x \wedge f(f(f(x))) = x \wedge \neg p(f(x))$$

Solution First, eliminate the quantifier p(x).

$$F : g(x) = \cdot \wedge f(f(x)) = x \wedge f(f(f(x))) = x \wedge g(f(x)) \neq \cdot$$

Then, build the subterm set

$$S_F = \{x, f(x), f^2(x), f^3(x), g(x), g(f(x)), \cdot\}$$

Then, initialize the congruence relation of S_F:

$$\{\{x\}, \{f(x)\}, \{f^2(x)\}, \{f^3(x)\}, \{g(x)\}, \{g(f(x))\}, \{\cdot\}\}$$

Then,merge $g(x)$ and $\cdot$, merge $f^3(x)$ and x, merge $f^2(x)$ and x, you can get

$$\{\{f(x)\}, \{x, f^2(x), f^3(x)\}, \{g(f(x))\}, \{g(x), \cdot\}\}$$

Then, from $x = f^2(x)$, propagate $f(x) = f^3(x)$, merge $f(x)$ to get

$$\{\{x, f(x), f^2(x), f^3(x)\}, \{g(f(x))\}, \{g(x), \cdot\}\}$$

Then, from $x = f^(x)$, propagate $g(x) = g(f(x))$, merge $f(f(x))$ to get

$$\{\{x, f(x), f^2(x), f^3(x)\}, \{g(x), g(f(x)), \cdot\}\}$$

Since $g(f(x)) \neq \cdot$, unsat. ■

3-2 Apply the decision procedure for quantifier-free T_A to the following Σ_A-formula:

$$a\langle i \triangleleft e\rangle\langle j \triangleleft f\rangle[k] = g \wedge j \neq k \wedge i = j \wedge a[k] \neq g$$

Solution First, eliminate the quantifier.Since $j \neq k$,we can get

$$a\langle i \triangleleft e\rangle[k] = g \wedge j \neq k \wedge i = j \wedge a[k] \neq g$$

Then, it can be splited into 2 cases

$$i = k : e = g \wedge i = k \wedge j \neq k \wedge i = j \wedge a[k] \neq g$$

$$i \neq k : a[k] = g \wedge i \neq k \wedge j \neq k \wedge i = j \wedge a[k] \neq g$$

Use $f(k)$ to subtitude $a[k]$, we get

$$i = k : e = g \wedge i = k \wedge j \neq k \wedge i = j \wedge f(k) \neq g$$

$$i \neq k : f(k) = g \wedge i \neq k \wedge j \neq k \wedge i = j \wedge f(k) \neq g$$

For case 1, build the subterm set

$$S_F = \{i, j, k, e, g, f(k)\}$$

Merge the equalities, we get

$$\{\{i, j, k\}, \{e, g\}, \{f(k)\}\}$$

Since $j \neq k$, it reaches a contradiction.
For case 2, $f(k) \neq g$ and $f(k) = g$ suddenly reachs a contradiction, unsat. ■

3-3 Apply the Nelson-Oppen method to the following formula in $T_{\mathbb{Z}} \cup T_A$:

$$a[i] \geq 1 \wedge a[i] + x \leq 2 \wedge x > 0 \wedge x = i \wedge a\langle x \triangleleft 2\rangle[i] \neq 1$$

Do it first using the nondeterministic version (i.e. guess and check), and then the deterministic version (i.e. equality propagation).

Solution First, purify the formula, use w_1, w_2 to replace 1,2,use v to replace a[i]

$$F_Z : x > 0 \wedge w_1 = 1 \wedge w_2 = 2 \wedge v \geq 1 \wedge v + x \leq 2$$

$$F_A : a\langle x \triangleleft w_2\rangle[i] \neq w_1 \wedge x = i \wedge a[i] = v$$

Shared variables:$\{w_1, w_2, x, v\}$

guess and check For convenience, since $w_1 = 1, w_2 = 2$, it is impossible that $w_1 = w_2$.
Since $v \geq 1, w_1 = 1$, it is impossible that $v = w_1$
Since $v \geq 1, x > 0, v + x \leq 2$, The only possibility is that $v = x = 1$.We can get that the only case satisfying F_Z is

$$\{w_1, v, x, w_2\}$$

First, eliminate the predicates of F_A: Consider x = i, and use f(i) to subtitude a[i],

$$F_A : w_2 \neq w_1 \wedge x = i \wedge f(i) = v$$

Then the subterm set

$$S_E = \{w_2, w_1, x, i, f(i), v\}$$

Accoring to the result of guess and check, we get

$$\{\{w_2\}, \{w_1, x, v\}, \{i\}, \{f(i)\}\}$$

Merging the equalities, we get

$$\{\{w_2\}, \{w_1, x, v, i, f(i)\}\}$$

It satisfies $w_2 \neq w_1$, the formula is satisfiable.

equality propagation From F_Z, you can get $x = w_1$. Then you can get $x = w_1 = v$, then you can get no conflicts in F_A, F_Z, and no more equalities will be get.Satisfiable. ■