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

Homework 3

Instructor: Fei He
TA: Jianhui Chen, Fengmin Zhu

Chenhao Li (2017011466)

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 The validity of any valid first-order formula can be decided in finite time. ■

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. A $T_{\mathbb{Z}}$-formula can be reduced into a $T_{\mathbb{N}}$-formula, and $T_{\mathbb{N}}$ is decidable.
(b) True. A $T_{\mathbb{Z}}$-formula can be reduced into a $T_{\mathbb{N}}$-formula, and $T_{\mathbb{N}}$ is complete.
(c) False. $\exists x. x+1=0$ is both a $\Sigma_{\mathbb{Z}}$-formula and a $\Sigma_{\mathbb{N}}$-formula, while it is $T_{\mathbb{Z}}$-valid but not $T_{\mathbb{N}}$-valid.

■

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 No. In T_A, equality is only captured between array elements, i.e., there is no axiom to decide the equality between arrays. ■

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

Solution Let $F : x = a\langle i \triangleleft y\rangle[j]$. It is easy to show that $F \Rightarrow x = a[j] \vee x = y$, but $F \not\Rightarrow x = a[j]$ and $F \not\Rightarrow x = y$. ■

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: $f(f(f(a))) = f(f(a)) \wedge f(f(f(f(a)))) = a \to (f(a) = a)$

Solution

1. $I \not\models F$
2. $I \models (f(f(f(a))) = f(f(a)) \wedge f(f(f(f(a)))) = a) \wedge \neg(f(a) = a)$, 1, $\to$
3. $I \models f(f(f(a))) = f(f(a)) \wedge f(f(f(f(a)))) = a$, 2, $\wedge$
4. $I \models \neg(f(a) = a)$, 2, $\wedge$
5. $I \models f(f(f(a))) = f(f(a))$, 3, $\wedge$
6. $I \models f(f(f(f(a)))) = a$, 3, $\wedge$
7. $I \models f(f(f(f(a)))) = f(f(f(a)))$, 5, cong.
8. $I \models f(f(f(a))) = f(f(f(f(a))))$, 7, symm.
9. $I \models f(f(f(a))) = a$, 6, 8, trans.
10. $I \models f(f(f(f(a)))) = f(a)$, 9, cong.
11. $I \models f(a) = f(f(f(f(a))))$, 10, symm.
12. $I \models f(a) = a$, 6, 11, trans.
13. $I \not\models f(a) = a$, 4, $\neg$
14. $I \models \perp$, 12, 13

So this formula is valid. ■

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

Solution

1. $I \not\models F$
2. $I \models (1 \leq x \wedge x \leq 2) \wedge \neg(x = 1 \vee x = 2)$, 1, $\to$
3. $I \models 1 \leq x \wedge x \leq 2$, 2, $\wedge$
4. $I \models \neg(x = 1 \vee x = 2)$, 2, $\wedge$
5. $I \not\models x = 1 \vee x = 2$, 4, $\neg$
6. $I \models \neg(x = 1)$, 5, $\vee$
7. $I \models \neg(x = 2)$, 5, $\vee$
8. $I \models 1 \leq x$, 3, $\wedge$
9. $I \models x \leq 2$, 3, $\wedge$
10. $I \models 1 < x$, 6, 8, $T_{\mathbb{Z}}$
11. $I \models x < 2$, 7, 9, $T_{\mathbb{Z}}$
12. $I \models x \leq 1$, 11, $T_{\mathbb{Z}}$
13. $I \models \perp$, 10, 12, $T_{\mathbb{Z}}$

So this formula is valid. ■

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

Solution

1. $I \not\models F$
2. $I \models a\langle i \triangleleft e\rangle[j] = e \land a[j] = e$, 1, $\rightarrow$
3. $I \models a\langle i \triangleleft e\rangle[j] = e$, 2, $\land$
4. $I \models a[j] = e$, 2, $\land$

No contradiction can be drawn, so this formula is not valid. A falsifying interpretation can be: $D = \{c_a, c_i, c_j, x, y\}$, $I = \{a \mapsto c_a, i \mapsto c_i, j \mapsto c_i, e \mapsto x\}$ and $c_a[c_i] = y$, $c_a[c_j] = x$. ■

Problem 3: Decision Procedure for Theories

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

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

Solution First transform it into an EUF-formula: $f_p(x) = \bullet \land f(f(x)) = x \land f(f(f(x))) = x \land f_p(f(x)) \neq \bullet$

$S_F = \{\bullet, x, f(x), f_p(x), f(f(x)), f_p(f(x)), f(f(f(x)))\}$

Step 0: $\{\{\bullet\}, \{x\}, \{f(x)\}, \{f_p(x)\}, \{f(f(x))\}, \{f_p(f(x))\}, \{f(f(f(x)))\}\}$

Step 1: From $f_p(x) = \bullet$, merge $\{\bullet\}$ and $\{f_p(x)\}$:
$\{\{\bullet, f_p(x)\}, \{x\}, \{f(x)\}, \{f(f(x))\}, \{f_p(f(x))\}, \{f(f(f(x)))\}\}$

Step 2: From $f(f(x)) = x$, merge $\{f(f(x))\}$ and $\{x\}$:
$\{\{\bullet, f_p(x)\}, \{x, f(f(x))\}, \{f(x)\}, \{f_p(f(x))\}, \{f(f(f(x)))\}\}$
From $f(f(x)) = x$, propagate $\{f(f(f(x)))\}$ and $\{f(x)\}$:
$\{\{\bullet, f_p(x)\}, \{x, f(f(x))\}, \{f(x), f(f(f(x)))\}, \{f_p(f(x))\}\}$

Step 3: From $f(f(f(x))) = x$, merge $\{x, f(f(x))\}$ and $\{f(x), f(f(f(x)))\}$:
$\{\{\bullet, f_p(x)\}, \{x, f(x), f(f(x)), f(f(f(x)))\}, \{f_p(f(x))\}\}$
From $f(x) = x$, propagate $f_p(x) = f_p(f(x))$:
$\{\{\bullet, f_p(x), f_p(f(x))\}, \{x, f(x), f(f(x)), f(f(f(x)))\}\}$

The final result is the congruence clusure of S_F. F asserts $f_p(f(x)) \neq \bullet$ while $f_p(f(x)) \sim \bullet$, so unsat. ■

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

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

Solution

- For F, assume $j = k$:
  $F_1 : f = g \land j \neq k \land i = j \land a[k] \neq g \land j = k$
  which has no write terms, so build a T_E-formula:
  $F_1' : f = g \land j \neq k \land i = j \land a(k) \neq g \land j = k$
  which is not satisfiable.
- For F, assume $j \neq k$:
  $F_2 : a\langle i \triangleleft e\rangle[k] = g \land j \neq k \land i = j \land a[k] \neq g \land j \neq k$
  - For F_2, assume $i = k$:
    $F_3 : e = g \land j \neq k \land i = j \land a[k] \neq g \land j \neq k \land i = k$
    which has no write terms, so build a T_E-formula:
    $F_3' : e = g \land j \neq k \land i = j \land a(k) \neq g \land j \neq k \land i = k$
    which is not satisfiable.
  - For F_2, assume $i \neq k$:
    $F_4 : a[k] = g \land j \neq k \land i = j \land a[k] \neq g \land j \neq k \land i \neq k$
    which has no write terms, so build a T_E-formula:
    $F_4' : a(k) = g \land j \neq k \land i = j \land a(k) \neq g \land j \neq k \land i \neq k$
    which is not satisfiable.

Every branch reaches contradiction, so 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 F to obtain F_1 and F_2:

$$\begin{aligned}
F &= w_1 \geq 1 \wedge w_1 + x \leq 2 \wedge x > 0 \wedge x = i \wedge w_2 \neq 1 \wedge a[i] = w_1 \wedge w_2 = a\langle x \triangleleft w_3\rangle[i] \wedge w_3 = 2 \\
F_1 &= w_1 \geq 1 \wedge w_1 + x \leq 2 \wedge x > 0 \wedge x = i \wedge w_2 \neq 1 \wedge w_3 = 2 \\
F_2 &= w_1 = a[i] \wedge w_2 = a\langle x \triangleleft w_3\rangle[i] \\
V &= free(F_1) \cap free(F_2) = \{w_1, w_2, w_3, x, i\}
\end{aligned}$$

- Guess-and-check method

  Enumerate all the equivalence relation E on V:

  1. $\{\{w_1, x, i\}, \{w_2, w_3\}\}$: sat.

  Maybe I am lucky enough to find the correct equivalence relation within one guess.

- Equality propagation method

$$\begin{aligned}
F_1 &\models x = i \\
F_2 \wedge x = i &\models w_2 = w_3 \\
F_2 \wedge w_2 = w_3 &\models x = w_1
\end{aligned}$$

  Now no more equality can be drawn, so sat.

■