《软件分析与验证》第三次书面作业讲解

朱倖民

清华大学

2020 年 4 月

Contents

Contents

1-2

Question

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.

1-2

Question

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.

参考解答：

Solution (a), (b) 是对的，(c) 是错的。

$T_{\mathbb{Z}}$ 可以归结到 $T_{\mathbb{N}}$，由于 $T_{\mathbb{N}}$ 是 decidable, complete 的，因此 $T_{\mathbb{Z}}$ 也是 decidable, complete.

考虑公式 $\forall x, \neg(x+1=0)$，这既是 $T_{\mathbb{Z}}$ 也是 $T_{\mathbb{N}}$，但显然，在 $T_{\mathbb{N}}$ 上对任意取值都满足，是 valid；但在 $T_{\mathbb{Z}}$ 上，当 x 取 -1 时不满足，因此不是 valid。所以 $T_{\mathbb{Z}}$-valid 和 $T_{\mathbb{N}} - valid$ 并不等价。■

Question

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 Σ $\mathbb{Z}$-formula and a Σ $\mathbb{N}$-formula, then: ϕ is $T_{\mathbb{N}}$-valid if and only if ϕ is $T_{\mathbb{Z}}$-valid.

参考解答：

Solution (a), (b) 是对的，(c) 是错的。

$T_{\mathbb{Z}}$ 可以归结到 $T_{\mathbb{N}}$，由于 $T_{\mathbb{N}}$ 是 decidable, complete 的，因此 $T_{\mathbb{Z}}$ 也是 decidable, complete.

考虑公式 $\forall x, \neg(x+1=0)$，这既是 $T_{\mathbb{Z}}$ 也是 $T_{\mathbb{N}}$，但显然，在 $T_{\mathbb{N}}$ 上对任意取值都满足，是 valid；但在 $T_{\mathbb{Z}}$ 上，当 x 取 -1 时不满足，因此不是 valid。所以 $T_{\mathbb{Z}}$-valid 和 $T_{\mathbb{N}} - valid$ 并不等价。■

注意：自然数不包括负数！可归约不意味着二者完全等同！

1-3

Question

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

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

1-3

Question

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

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

错误解答:

Solution Yes.

1.	I	$\not\models (a[i] = x \wedge x = y) \rightarrow a\langle i \triangleleft y\rangle = a$	assumption
2.	I	$\models a[i] = x \wedge x = y$	1, $\rightarrow$
3.	I	$\models a[i] = x$	2, $\wedge$
4.	I	$\models x = y$	2, $\wedge$
5.	I	$\models a[i] = y$	3, 4, **(transitivity)**
6.	I	$\not\models a\langle i \triangleleft y\rangle = a$	1, $\rightarrow$
7.	I	$\models a\langle i \triangleleft y\rangle \neq a$	6, $\neg$
8.	I	$\models \neg(\forall j. a\langle i \triangleleft y\rangle[j] = a[j])$	7, **(extensionality)**
9.	I	$\not\models \forall j. a\langle i \triangleleft y\rangle[j] = a[j]$	8, $\neg$
10.	$I_1 : I \triangleleft \{j \mapsto j_0\}$	$\not\models a\langle i \triangleleft y\rangle[j] = a[j]$	9, $\forall$, for some $j_0 \in D_I$
11.	I_1	$\models a\langle i \triangleleft y\rangle[j] \neq a[j]$	10, $\neg$
12.	I_1	$\models i = j$	11, **(read-over-write 2)**
13.	I_1	$\models a[i] = a[j]$	12, **(array congruence)**
14.	I_1	$\models a\langle i \triangleleft y\rangle[j] = y$	12, **(read-over-write 1)**
15.	I_1	$\models y = a[i]$	5, **(symmetry)**
16.	I_1	$\models a\langle i \triangleleft y\rangle[j] = a[i]$	14, 15, **(transitivity)**
17.	I_1	$\models a\langle i \triangleleft y\rangle[j] = a[j]$	16, 13, **(transitivity)**
18.	I_1	$\models \perp$	11, 15 ■

1-3

Question

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

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

参考解答：

Solution 不是。原因：T_A 中等号只能作用在数组元素上。■

注意：T_A-valid 的公式必然是 T_A-公式！
回顾：L06 T_A Signature

1-4

Question

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

1-4

Question

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

回顾： L08 Convex Theory

1-4

Question

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

回顾： L08 Convex Theory

参考解答：

Solution Formula F:

$$a\langle i \triangleleft v\rangle[j] = a[i]$$

Then:

$$F \Rightarrow i = j \vee a[i] = a[j]$$

But neither $i = j$ nor $a[i] = a[j]$. ■

Contents

2-2

Question

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

2-2

Question

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

回顾：L02 Semantic Argument

2-2

Question

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

回顾： L02 Semantic Argument
参考解答：

Solution

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

2-2

Question

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

回顾：L02 Semantic Argument
参考解答：

Solution

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

注意：至少要写出所有与逻辑连接词相关的步骤、部分和 $T_{\mathbb{Z}}$ 相关的显而易见的结论可以跳步。

不太规范的解答

Solution

index	branch	rule
1	$I \not\models F$	(assum.)
2	$I \models 1 \leq x \wedge x \leq 2$	$1, \rightarrow$
3	$I \not\models x = 1 \vee x = 2$	$1, \rightarrow$
4	$I \models x \neq 1 \wedge x \neq 2$	$3, \vee$
5	$I \models x \neq 1$	$4, \wedge$
6	$I \models x \neq 2$	$4, \wedge$
7	$I \models x = 1 \vee x = 2$	$2, T_{\mathbb{Z}}$
8	$I \models x = 1$	$7, \vee$, case a
9	$I \models x = 2$	$7, \vee$, case b
10	$\perp$	5, 8, case a
11	$\perp$	6, 9, case b

Thus, F is $T_{\mathbb{Z}}$-valid. ■

不太规范的解答

Solution

index	branch	rule
1	$I \not\models F$	(assum.)
2	$I \models 1 \leq x \wedge x \leq 2$	1, $\rightarrow$
3	$I \not\models x = 1 \vee x = 2$	1, $\rightarrow$
4	$I \models x \neq 1 \wedge x \neq 2$	3, $\vee$
5	$I \models x \neq 1$	4, $\wedge$
6	$I \models x \neq 2$	4, $\wedge$
7	$I \models x = 1 \vee x = 2$	2, $T_{\mathbb{Z}}$
8	$I \models x = 1$	7, $\vee$, case a
9	$I \models x = 2$	7, $\vee$, case b
10	$\perp$	5, 8, case a
11	$\perp$	6, 9, case b

Thus, F is $T_{\mathbb{Z}}$-valid. ■

“case a, case b” 指什么？建议用 “left-hand side, right-hand size” 等更清晰的术语表达。（L02 也有这个问题）
其他写得很清楚。

Contents

3-2

Question

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

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

Question

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

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

错误解答 1:

Solution 因为 $i = j \land j \neq k$，所以 $a\langle i \triangleleft e\rangle\langle j \triangleleft f\rangle[k] = a[k]$，式子化为:

$$a[k] = g \land j \neq k \land i = j \land a[k] \neq g$$

显然不可满足。■

Question

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

错误解答 2:

Solution

1. Simplify F:

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

2. Obviously, F is T_A-unsatisfiable.

■

3-2

Question

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

错误解答 3：

Solution -

不可满足

根据F可知，$a\langle i \triangleleft e\rangle\langle j \triangleleft f\rangle[k] = g$

既有$a[k] = g$

但是与$a[k] \neq g$矛盾。

因此原式不可满足。 ■

3-2

Question

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

错误解答 3:

Solution -

不可满足

根据F可知，$a\langle i \triangleleft e\rangle\langle j \triangleleft f\rangle[k] = g$

既有$a[k] = g$

但是与$a[k] \neq g$矛盾。

因此原式不可满足。 ■

错误原因：没有用 decision procedure (L07) 或者步骤过于简略

再读一遍题目：

Question

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

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

参考解答：

Solution

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

Every branch reaches contradiction, so unsat. ■

Question

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

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

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

3-3

Question

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).

回顾： L08

Question

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

错误解答 1（只用了 guess and check）:

Solution -

将原式拆分为$T_{\mathbb{Z}}$和T_A两部分

$T_{\mathbb{Z}} : w_1 \geq 1 \land w_1 + x \leq 2 \land x > 0 \land w_2 = 2 \land w_3 = 1$

$T_A : w_1 = a[i] \land a\langle x \triangleleft w_2\rangle[i] \neq w_3 \land x = i$

$V = \{w_1, w_2, w_3, x\}$

猜测：$\{\{w_1, w_3, x\}, \{w_2\}\}$ 是可满足的。

$T_{\mathbb{Z}}$ 可得$w_1 = x = w_3$

代入T_A后不会产生矛盾，可满足。

■

Question

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

错误解答 2（概念性错误）:

Solution 设 $u = 0, v = 1, w = 2$, 则可以将原式化为两个论域下的式子:

$T_{\mathbb{Z}} : x = i \wedge x > 0 \wedge u = 0 \wedge v = 1 \wedge w = 2$ $T_A : a[i] \geq v \wedge a[i] + x \leq w \wedge a\langle x \triangleleft w\rangle[i] \neq v$ 共同变量为 x, i, u, v, w

1. 首先用 guess and check 方法，

令 x, i, v, u, w 为等价类，设 $a[1] = 1$, 原式成立

2. 用 equality propagation 方法

$x = i$ 得到 x, i, u, w, v

于是 $a[i] \geq 1$ 得到 $a[x] \geq 1$,$a[i] + x \leq 2$ 得到 $a[x] + x \leq 2$

又有 $x > 0$ 即 $x \geq 1$, 综合上述有 $2 \leq a[x] + x \leq 2$ 即 $a[x] = x = 1 = v$

此时等价类有 x, i, v, u, w 带入原式，没有矛盾。

因此原式可满足 ■

3-3

Question

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

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

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

认真审题！

参考解答：

Solution First purify F to obtain F_1 and F_2:

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

- 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

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

  Now no more equality can be drawn, so sat.

■

Contents

程序验证

核心问题：程序的行为是否符合预期？

程序验证

核心问题：程序的行为是否符合预期？

什么叫“程序的行为”？(形式语义)

程序验证

核心问题：程序的行为是否符合预期？
什么叫“程序的行为”？(形式语义)
什么叫“预期”？(用逻辑公式表达属性)

程序验证

核心问题：程序的行为是否符合预期？

什么叫“程序的行为”？(形式语义)

什么叫“预期”？(用逻辑公式表达属性)

什么叫“符合”？(推理、证明)

前半期主要内容

属性如何表达？Logic, or formal language!

- Propositional logic
- First-order logic and its fragments (quantifier-free, first-order theories)

前半期主要内容

属性如何表达？Logic, or formal language!

- Propositional logic
- First-order logic and its fragments (quantifier-free, first-order theories)

属性如何验证？Reduction, and searching!

- Semantic argument
- Resolution
- Decision procedure for first-order theory
- Decision procedure for combined theories (Nelson-Oppen)
- SAT (DPLL)
- SMT (DPLL(T))

理论概念

satisfiability v.s. validity

理论概念

satisfiability v.s. validity

soundness v.s. completeness

理论概念

satisfiability v.s. validity

soundness v.s. completeness

decidability

理论概念

satisfiability v.s. validity

soundness v.s. completeness

decidability

interpretation

理论概念

satisfiability v.s. validity

soundness v.s. completeness

decidability

interpretation

propositional v.s. first-order

复习建议

记住常用概念：记忆是理解的第一步

复习建议

记住常用概念：记忆是理解的第一步

搞清问题边界：什么问题不是我们要考虑的

复习建议

记住常用概念：记忆是理解的第一步

搞清问题边界：什么问题不是我们要考虑的

理解算法思想：领悟为什么这样设计就正确了（或者高效了）