hybr2d Theory of Hybrid Systems Informatik 2 | RWTH AACHEN UNIVERSITY

teaching@ths.rwth-aachen.de
https://ths.rwth-aachen.de/teaching/

Satisfiability Checking - WS 2023/2024

Series 4

Exercise 1

For each of the following theories, give their *signature* and *domain*, and state whether the theory is *decidable*.

Theory	Signature	Domain	Decidable?
Linear real arithmetic			
Linear integer arithmetic			
Nonlinear real arithmetic			
Nonlinear integer arithmetic			

Solution:

Theory	Signature	Domain	Decidable?
Linear real arithmetic	$\{0, 1, +, <\}$	$\mathbb{R}$	yes
Linear integer arithmetic	$\{0, 1, +, <\}$	$\mathbb{Z}$	yes
Nonlinear real arithmetic	$\{0, 1, +, \cdot, <\}$	$\mathbb{R}$	yes
Nonlinear integer arithmetic	$\{0, 1, +, \cdot, <\}$	$\mathbb{Z}$	no

Exercise 2

Assume a signature with the non-logical symbols: constants a, b; unary function f, binary function g; unary predicate p , binary predicate r, 3ary predicate q.

Say whether the following strings of symbols are well formed FOL Σ-formulas or terms:

1. $q(a)$
2. $p(y)$
3. $p(g(b))$
4. $\neg r(x, a)$
5. $q(x, p(a), b)$
6. $p(g(f(a), g(x, f(x))))$

7. $q(f(a), f(f(x)), f(g(f(z), g(a, b))))$
8. $r(a, r(a, a))$

Solution: Well formed formulas are 2, 4, 6, and 7. All other strings are NOT well formed FOL formulas nor terms:

- **??** $q(a)$: q needs three arguments
- **??** $p(g(b))$: g needs two arguments
- **??** $q(x, p(a), b)$: q needs theory expressions as arguments, but $p(a)$ is a Boolean expression
- **??** $r(a, r(a, a))$: r needs theory expressions as arguments, but $r(a, a)$ is a Boolean expression

Exercise 3

Assume a signature Σ with the non-logical symbols: constants a, b; unary function f, binary function g; unary predicate p , binary predicate r, 3ary predicate q.

Please specify all free variable occurrences in the following Σ-formulas:

1. $p(x) \wedge \neg r(y, a)$
2. $\exists x.\, r(x, y)$
3. $(\forall x.\, p(x)) \rightarrow (\exists y. \neg q(f(x), y, f(y)))$
4. $\forall x.\, \exists y.\, r(x, f(y))$
5. $\forall x.\, \exists y.\, (r(x, f(y)) \rightarrow r(x, y))$

   y开始　y结束　所以此处的y为free
6. $\forall x.\, ((\exists y.\, (r(x, f(y)))) \rightarrow r(x, y))$

   x作用范围开始　x作用范围结束

Solution:

1. x and y free
2. y free
3. the last occurrence of x free
4. no free variables
5. no free variables
6. the last occurrence of y free

Exercise 4

Define an appropriate signature Σ and formalize the following sentences using Σ-formulas:

1. All students are smart.
2. There exists a student.
3. There exists a smart student.
4. Every student loves some student.
5. Every student loves some other student.
6. There is a student who is loved by every other student.

7. Bill is a student.
8. Bill takes either Analysis or Geometry, but not both.
9. Bill takes Analysis and Geometry.
10. Bill doesn't take Analysis.
11. No student takes Geometry.

Solution: Σ contains the constants *Bill*, *Analysis* and *Geometry*; the unary predicates *Student* and *Smart*; the binary predicates *Takes* and *Loves*.

1. $\forall x. (\mathit{Student}(x) \rightarrow \mathit{Smart}(x))$
2. $\exists x. \mathit{Student}(x)$
3. $\exists x. (\mathit{Student}(x) \wedge \mathit{Smart}(x))$
4. $\forall x. (\mathit{Student}(x) \rightarrow \exists y. (\mathit{Student}(y) \wedge \mathit{Loves}(x, y)))$
5. $\forall x. (\mathit{Student}(x) \rightarrow \exists y. (\mathit{Student}(y) \wedge \neg(x = y) \wedge \mathit{Loves}(x, y)))$
6. $\exists x. (\mathit{Student}(x) \wedge \forall y. ((\mathit{Student}(y) \wedge \neg(x = y)) \rightarrow \mathit{Loves}(y, x)))$
7. $\mathit{Student}(\mathit{Bill})$
8. $\mathit{Takes}(\mathit{Bill}, \mathit{Analysis}) \leftrightarrow \neg \mathit{Takes}(\mathit{Bill}, \mathit{Geometry})$
9. $\mathit{Takes}(\mathit{Bill}, \mathit{Analysis}) \wedge \mathit{Takes}(\mathit{Bill}, \mathit{Geometry})$
10. $\neg \mathit{Takes}(\mathit{Bill}, \mathit{Analysis})$
11. $\neg \exists x. (\mathit{Student}(x) \wedge \mathit{Takes}(x, \mathit{Geometry}))$

Exercise 5

Minesweeper is a single-player computer game invented by Robert Donner in 1989. The game field is an $k \times k$ matrix of cells, out which $n \in [0, k^2]$ contain a mine. At the beginning, all cells are covered. Each covered cell can be uncovered by clicking on it. If a cell that contains a mine is clicked, the game is over. Otherwise, if the clicked cell does not contain a mine, one of two things happens:

i. A number between 1 and 8 appears indicating the amount of adjacent (including diagonally-adjacent) squares containing mines, or

ii. no number appears, in which case there are no mines in the adjacent cells.

The objective is to uncover each cell that does not contain a mine, without uncovering any cell with a mine in it.

Provide a signature for a first-order language that allows to formalize the knowledge of a player about a game state. In your language, formalize the following knowledge as axioms:

1. The minefield is a matrix of 8×8 cells.
2. For a given cell, its adjacent cells are its left, right, top, bottom and the four diagonal neightbours.

3. There are exactly n mines in the minefield.
4. If a cell contains the number 1, then there is exactly one mine in the adjacent cells.

Show by means of deduction that there must be a mine in the position $(3,3)$ (3rd row and 3rd column, counting from 1) of the game state depicted on the right.
Suggestion: define the predicate *adj*(x,y) to formalize the fact that two cells x and y are adjacent.

Solution: We define the signature Σ to consist of the following:

- Constants $c_{i,j}$ for $i,j \in \{1,\dots,8\}$ for the cells.
- A unary predicate *mine*, where *mine*(x) means that the cell x contains a mine.
- A binary predicate *adj*, where *adj*(x,y) means that the cell x is adjacent to the cell y.
- Unary predicates *contains*, where *contains*$_n(x)$ means that the cell x contains the number n for $n \in \{1,\dots,8\}$.

Axioms:

1. The minefield is a matrix of 8×8 cells.

$$(\forall x. \bigvee_{(i,j)\in[1,8]\times[1,8]} x = c_{i,j}) \wedge (\bigwedge_{\substack{(i,j),(i',j')\in[1,8]\times[1,8]\\ i\neq i',j\neq j'}} c_{i,j} \neq c_{i',j'})$$

2. For $(i,j) \in [1,8]\times[1,8]$, let

$$N(i,j) = \{(i',j') \in [1,8]\times[1,8] \mid i' \in [i-1,i+1] \wedge j' \in [j-1,j+1] \wedge (i \neq i' \vee j \neq j')\}\ .$$

For a given cell, its adjacent cells are its left, right, top, bottom and the four diagonal neightbours.

$$\bigwedge_{i=1}^{8}\bigwedge_{j=1}^{8}\left(\left(\bigwedge_{(i',j')\in N(i,j)} \mathit{adj}(c_{i,j},c_{i',j'})\right) \wedge \left(\bigwedge_{(i',j')\in([1,8]\times[1,8])\setminus N(i,j)} \neg\mathit{adj}(c_{i,j},c_{i',j'})\right)\right)$$

3. There are exactly n mines in the game.

$$\exists x_1.\ \dots \exists x_n.\ ((\bigwedge_{i,j=1,\dots,n,\ i\neq j} x_i \neq x_j) \wedge (\bigwedge_{i=1}^{n} \mathit{mine}(x_i)) \wedge (\forall y.\ (\mathit{mine}(y) \rightarrow \bigvee_{i=1}^{n} y = x_i)))$$

4. If a cell contains the number 1, then there is exactly one mine in the adjacent cells.

$$\forall x.\ (\mathit{contains}_1(x) \rightarrow \exists z.\ (\mathit{adj}(x,z) \wedge \mathit{mine}(z) \wedge \forall y.\ ((\mathit{adj}(x,y) \wedge \mathit{mine}(y)) \rightarrow y = z)))$$

We show by means of deduction that there must be a mine in the position $(3,3)$:

a) By state specification we have:

$$\mathit{contains}_1(c_{2,2})$$

b) By state specification we have:

$$\begin{array}{l}\neg\mathit{mine}(c_{1,1}) \wedge \neg\mathit{mine}(c_{1,2}) \wedge \neg\mathit{mine}(c_{1,3}) \wedge\\ \neg\mathit{mine}(c_{2,1}) \wedge \neg\mathit{mine}(c_{2,2}) \wedge \neg\mathit{mine}(c_{2,3}) \wedge\\ \neg\mathit{mine}(c_{3,1}) \wedge \neg\mathit{mine}(c_{3,2})\end{array}$$

c) From a) and Axiom 4 we can deduce:

$$\exists z.(\textit{adj}(c_{2,2}, z) \land \textit{mine}(z) \land \forall y.\,((\textit{adj}(c_{2,2}, y) \land \textit{mine}(y)) \to y = z))$$

d) From c) and the first two axioms we can deduce:

$$\textit{mine}(c_{1,1}) \lor \textit{mine}(c_{1,2}) \lor \textit{mine}(c_{1,3}) \lor \textit{mine}(c_{2,1}) \lor \textit{mine}(c_{2,3}) \lor \textit{mine}(c_{3,1}) \lor \textit{mine}(c_{3,2}) \lor \textit{mine}(c_{3,3})$$

e) From b) and d) we can deduce:

$$\textit{mine}(c_{3,3})$$

Exercise 6*

As help for understanding the definition of a theory. Not relevant for the exam. In this exercise, we give some more details on the concept of *logical theory* and how it is related to axioms.

We fix an arbitrary signature Σ and an arbitrary structure $\mathcal{S}$ over Σ. In the following, all sentences are over Σ and Φ[1] is a set of sentences. We use the following notation:

- $\mathcal{S} \models \varphi$: $\mathcal{S}$ is a model of a sentence φ.
- $\mathcal{S} \models \Phi$: $\mathcal{S}$ is a model of all sentences φ from the set Φ.

Definitions:

- A sentence φ **is a consequence of** Φ ($\Phi \models \varphi$) iff $\mathcal{S} \models \varphi$ for each model $\mathcal{S} \models \Phi$.
- $\Phi^{\models} := \{\varphi \mid \Phi \models \varphi\}$ denotes the **set of consequences of** Φ.
- Φ is called **consistent** if there is no sentence φ with $\Phi \models \varphi$ and $\Phi \models \neg\varphi$.
- A satisfiable set of sentences T is called a **theory** if for all sentences φ

$$T \models \varphi \quad \Longleftrightarrow \quad \varphi \in T.$$

- A theory T is **complete** iff for all sentences φ

$$\text{either} \quad \varphi \in T \quad \text{or} \quad \neg\varphi \in T.$$

Prove the following five statements.

1. Each theory T is consistent.
2. Let Φ be a set of sentences. Φ is consistent iff $\Phi^{\models}$ is a theory.
3. The set $\mathtt{Th}(\mathcal{S}) := \{\varphi \mid \mathcal{S} \models \varphi\}$ is a theory. It is called the **theory of** $\mathcal{S}$.
4. $\mathtt{Th}(\mathcal{S})$ is complete.
5. Let $\Sigma = \{+, \cdot, \leq, =\}$. Give one example each:
   (a) a complete Σ-theory T_1,
   (b) an incomplete Σ-theory T_2.

   Hint: You can use different ways to define a theory.

Solution:

[1] Imagine Φ to be a (finite) set of axioms.

1. Suppose there is a sentence φ with $T \models \varphi$ and $T \models \neg\varphi$. Let $\mathcal{S} \models T$. Because T is a theory, $\varphi \in T$ and $\mathcal{S} \models \varphi$. Likewise, $\neg\varphi \in T$ and $\mathcal{S} \not\models \varphi$. ↯ $\mathcal{S} \models \varphi$.

2. "$\Leftarrow$": Since $\Phi^{\models}$ is consistent as a theory, $\Phi \subseteq \Phi^{\models}$ is consistent.

   "$\Rightarrow$": Let Φ be consistent. It holds that

   $$\Phi^{\models} \models \varphi \;\Leftrightarrow\; \Phi \models \varphi \;\Leftrightarrow\; \varphi \in \Phi^{\models}.$$

   because $\models$ is transitive and by construction of $\Phi^{\models}$.

   It remains to prove that $\Phi^{\models}$ is satisfiable. For contradiction, we assume that $\Phi^{\models}$ is not satisfiable. By transitivity of $\models$, Φ is not satisfiable as well, i.e., Φ has no models. Therefore, $\Phi \models \psi$ for each Σ sentence ψ; in particular, there exists a Σ sentence φ such that $\Phi \models \varphi$ and $\Phi \models \neg\varphi$. ↯ Φ consistent.

3. Let $T := \mathsf{Th}(\mathcal{S})$. T is indeed satisfiable since $\mathcal{S} \models T$. It holds by transitivity of $\models$ and construction of T that

   $$T \models \varphi \Longleftrightarrow \mathcal{S} \models \varphi \Longleftrightarrow \varphi \in T.$$

4. Let $T := \mathsf{Th}(\mathcal{S})$. We assume that T is not complete. Therefore, a Σ sentence φ exists such that (1) $\varphi \notin T$ and (2) $\neg\varphi \notin T$. (1) implies that $\mathcal{S} \not\models \varphi$, i.e., there is no assignment from the domain of $\mathcal{S}$ to the variables of φ so that φ evaluates to true by the given interpretation of Σ in $\mathcal{S}$. Consequently, any such assignment satisfies $\neg\varphi$. Hence $\mathcal{S} \models \neg\varphi$. Thus, $\neg\varphi \in T$. ↯ (2).

5. (a) We define the theory of a structure, e.g., $T_1 = \mathsf{Th}(\ (\mathbb{N}, +, \cdot, \leq, =)\ )$, as proven in 4.

   (b) We define a theory by a set of axioms, e.g.,

   $$\begin{aligned} T_2 \;\; = \;\; & \{\forall x.\, \forall y.\, x \leq x, \\ & \forall x.\, \forall y.\, x \leq y \wedge y \leq x \rightarrow x = y, \\ & \forall x.\, \forall y.\, \forall z.\, x \leq y \wedge y \leq z \rightarrow x \leq z\ \}^{\models} \end{aligned}$$

   the theory of linear orders. It is true that, e.g., $(\mathbb{N}, +, \cdot, \leq, =) \models T_2$, but $\mathsf{Th}(\mathbb{N}, +, \cdot, \leq, =) \supsetneq T_2$. A witness for this issue is, e.g., the sentence

   $$\varphi \;\; = \;\; \forall x.\, x \leq x \cdot x.$$

   $\varphi \in T_1$, but neither $\varphi \in T_2$ nor $\neg\varphi \in T_2$, because multiplication $\cdot$ is not FO-definable within linear orderings.

   Another solution for T_2 is Presburger arithmetic, $T_2 = \mathsf{Th}(\ (\mathbb{N}, +, \leq, =)\ )$. Our incompleteness proof is based on decidability results:

   (1) satisfiability for Presburger arithmetic is decidable,

   (2) satisfiability for $T_1 = \mathsf{Th}(\ (\mathbb{N}, +, \cdot, \leq, =)\ )$ is undecidable.

   Firstly, we note that $T_2 \subseteq T_1$ because of the same interpretation of the signature.

   If we assume that T_2 is complete, we can define a formula $\varphi_{\cdot}(x, y, z)$ in T_2 so that $\varphi_{\cdot}(x, y, z) \equiv (x \cdot y = z)$ in T_1, i.e., we define multiplication in Presburger arithmetic. Thus, $T_2 \models T_1$, i.e., $T_2 = T_1$ because T_1 is complete due to part (a). This fact and (1) entail that T_1 must be decidable. Contradiction to (2).