Formale Methoden der Informatik

Block 2: Satisfiability Problems

3. Recap: First-order Logic and Theories

Uwe Egly

Knowledge-Based Systems Group
Institute of Information Systems
Vienna University of Technology

Why do we need first-order logic?

Goal of the SAT part

Provide necessary tools and background info to construct a decision procedure for equality logic with uninterpreted functions (EUF).

EUF is a restricted variant (or a fragment) of first-order logic. It uses the theory of equality.

Therefore, we need some definitions and notions from first-order logic extended by theories.

Disclaimer: The first slides recapitulate known material about first-order logic which you know from "Theoretische Informatik und Logik". The theory handling is new for (most of) you.

Outline

Signatures

- Signature Σ: countably infinite set of function symbols (FSs) or predicate symbols (PSs) together with their arity
- In propositional logic: Σ is the set of Boolean variables
- Elements from Σ are the building blocks for formulas.

$\Sigma = (\mathit{Func}, \mathit{Pred})$

- *Func*: set of function symbols (+ arity)
  - With arity 0: constant symbols (CSs)
  - With arity > 0: for building terms
- *Pred*: set of predicate symbols (+ arity)
  - For building atomic formulas

- Elements of Σ are often called the "non-logical symbols".

Terms

The definition of $Terms(\Sigma, Var)$

- Given a signature $\Sigma = (Func, Pred)$ and a set Var of (object) variables
- Variables are often denoted by $x, y, z, x_1, x', \ldots$

Definition

The set of terms, $Terms(\Sigma, Var)$, for given Σ and Var is defined inductively as follows:

B1: Every $x \in Var$ is a term.

B2: Every constant symbol from $Func$ in Σ is a term.

S1: If $t_1, \ldots, t_n$ are terms and f is a FS from $Func$ in Σ with arity $n > 0$, then $f(t_1, \ldots, t_n)$ is a term.

Terms: Some examples

Example

Given $Var = \{x\}$ and $Func = \{c/0, f/1\}$

$$Terms(\Sigma, Var) = \{x, c, f(x), f(c), f(f(x)), f(f(c)), \ldots\}$$

➥ The set of terms is infinite since there is a FS of arity > 0 in Σ.

Definition

A ground term is a term without variables.

Example

Given $Var = \{x\}$ and $Func = \{c/0, f/1\}$ as above. The set of ground terms from $Terms(\Sigma, Var)$ is

$$\{c, f(c), f(f(c)), f(f(f(c))), \ldots\}$$

First-order (FO) formulas

- Given a signature $\Sigma = (\mathit{Func}, \mathit{Pred})$ and Var
- Let p be a PS from Σ with arity $n \geq 0$ and $t_1, \ldots, t_n$ terms. Then $p(t_1, \ldots, t_n)$ is an atomic formula or atom.
- Ground atoms are atoms without variables.
- Inductive definition of the set of FO formulas for given Σ, Var

  B1: Every atom is a formula.

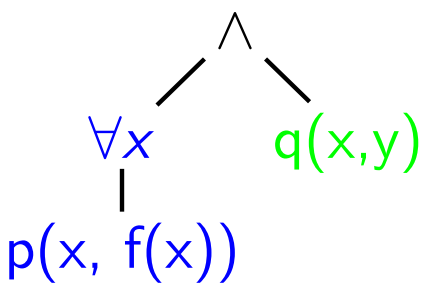
  B2: $\top$ (verum) and $\bot$ (falsum) are formulas.

  S1: For $\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \oplus$: same as for propositional logic.

  S2: If $x \in \mathit{Var}$ and φ is a formula, then so are $\forall x\, \varphi$ and $\exists x\, \varphi$.
- $\forall$ is the universal quantifier, $\exists$ is the existential quantifier
- In S2, φ is called the scope of the quantifier.

Formulas as trees

- First-order formulas can be depicted as formula trees.
- Example: $(\forall x\, p(x, f(x))) \wedge q(x, y)$



  - Var. occurrences can be free or bound.
  - Occurrences x are bound ($\forall x$ above!).
  - Occurrence x is free (no $\forall x$, $\exists x$ above).

- Formulas without free vars are called closed or sentences.

The free variables of a formula

Definition

The set of free variables of a term t, $free(t)$, is defined inductively:

B1: $free(t) = \{x\}$ if t is a variable x

B2: $free(t) = \{\}$ if t is a constant a

S1: $free(t) = \bigcup_{i=1}^{n} free(t_i)$ if t is a term $f(t_1, \ldots, t_n)$

Definition

The set of free variables of a formula λ, $free(\lambda)$, is defined inductively:

B1: $free(\lambda) = \bigcup_{i=1}^{n} free(t_i)$ if λ is an atom $p(t_1, \ldots, t_n)$

S1: $free(\lambda) = free(\varphi)$ if λ is $\neg\varphi$

S2: $free(\lambda) = free(\varphi) \cup free(\psi)$ if λ is $\varphi \circ \psi$ and $\circ \in \{\vee, \wedge, \rightarrow, \leftrightarrow, \oplus\}$

S3: $free(\lambda) = free(\varphi) \setminus \{x\}$ if λ is $Qx\,\varphi$ and $Q \in \{\forall, \exists\}$

Outline

The semantics of first-order logic

- Semantics of first-order logic more difficult than for propositional logic because of
  - the term structure,
  - the quantifiers, and
  - the free variables which can occur in formulas.
- A first-order (interpretation) structure wrt Σ consists of
  - a domain $\mathcal{U}$, i.e., a nonempty set of symbols and
  - the interpretation function $I(\cdot)$.
- $I(\cdot)$ has to satisfy the following conditions:
  1. For CS (0-ary FS) $c \in \mathit{Func}$: $I(c) \in \mathcal{U}$
  2. For n-ary FS $f \in \mathit{Func}$ (n>0): $I(f) : \mathcal{U}^n \mapsto \mathcal{U}$
  3. For n-ary PS $p \in \mathit{Pred}$: $I(p) \subseteq \mathcal{U}^n$

How to handle free variables?

- Free variables in a formula cause problems.
  What is the meaning of a free x?
- Two solutions possible:
  - Close a formula by $\forall$ (universal closure), or
  - interpret the formula modulo a variable assignment

$$\alpha : \mathit{Var} \mapsto \mathcal{U}$$

- We use variable assignments in the following.

The evaluation of a term

Definition (Evaluation of a term under I and α)

The evaluation of a term t under an interpretation structure $\mathcal{U}$, I and a variable assignment α (modulo the signature Σ), $I_{\mathcal{U},\Sigma,\alpha}(t)$, is defined inductively as follows:

B1: $I_\alpha(x) = \alpha(x)$ for $x \in \mathit{Var}$

B2: $I_\alpha(c) = I(c)$ for a constant symbol c (recall: $I(c) \in \mathcal{U}$)

S1: $I_\alpha(f(t_1, \ldots, t_n)) = I(f)(I_\alpha(t_1), \ldots, I_\alpha(t_n))$ for $f/n \in \mathit{Func}$ and $t_1, \ldots, t_n$ are terms

- We often write I_α instead of $I_{\mathcal{U},\Sigma,\alpha}(t)$ to improve readability!

The evaluation of a formula

Definition (Evaluation of a formula under I and α)

The evaluation of a formula under an interpretation structure $\mathcal{U}$, I and a variable assignment α (modulo the signature Σ) is defined inductively as follows:

B1: $I_\alpha(p(t_1, \ldots, t_n)) = 1$ iff $(I_\alpha(t_1), \ldots, I_\alpha(t_n)) \in I(p)$ where $p/n \in \mathit{Pred}$ and $t_1, \ldots, t_n$ are terms

S1: The connectives are handled like in propositional logic

S2: $I_\alpha(\forall x\, \varphi) = 1$ iff $I_{\alpha \cup \{x \leftarrow c\}}(\varphi) = 1$ for each $c \in \mathcal{U}$

S3: $I_\alpha(\exists x\, \varphi) = 1$ iff $I_{\alpha \cup \{x \leftarrow c\}}(\varphi) = 1$ for at least one $c \in \mathcal{U}$

- The evaluation of a first-order formula is undecidable.
- Notions like tautology, valid, (un)satisfiable, model, etc. remain essentially unchanged.

Example for an evaluation of a closed formula

Let φ be $\forall x\,(p(x) \rightarrow p(f(f(x))))$.

- Let $\mathcal{U} = \mathbb{N}$.
- Informally, the symbols f, p have the following meaning:
  - $f/1 \in \mathit{Func}$ with the intended meaning "successor of"
  - $p/1 \in \mathit{Pred}$ with the intended meaning "is odd number"
- φ's intended reading: for every odd no x, $x + 2$ is also odd
- Let $I(f) : \mathcal{U} \mapsto \mathcal{U}$ with $f(u) = u + 1$
- Moreover, $I(p) = \{(1), (3), (5), \ldots\} \subset \mathcal{U}$
- Since φ is closed, $\alpha = \{\}$ at the beginning

Example for an evaluation of a closed formula (cont'd)

- $I_{\{\}}(\varphi) = 1$ iff, for each $c \in \mathcal{U}$,
  $I_{\{x \leftarrow c\}}(p(x) \rightarrow p(f(f(x)))) = I_{\{\}}(p(c) \rightarrow p(f(f(c)))) = 1$
- Case distinction for c:
  1: c is odd (i.e., $(c) \in I(p)$):
  - $I_{\{\}}(p(c) \rightarrow p(f(f(c)))) = 1$ iff $(c) \notin I(p)$ or $I(f(f(c))) \in I(p)$
  - Since $I(f(f(c))) = I(c) + 2$, $(c) \in I(p)$ implies $I(f(f(c))) \in I(p)$
  - Since $(c) \in I(p)$, $I(f(f(c))) \in I(p)$ and the implication is true

  2: c is even (i.e., $(c) \notin I(p)$):
  - Then $p(c) \rightarrow p(f(f(c)))$ is true under I because $(c) \notin I(p)$
- Hence, φ is true under the chosen interpretation

Recall the notations

- $Mod(\psi)$ is the class of all models of ψ.
- φ is satisfiable if there is some $\mathcal{U}$, I_α that satisfies φ.
- φ is falsifiable if there is some $\mathcal{U}$, I_α that does not satisfy φ.
- φ is valid if every $\mathcal{U}$, I_α is a model of φ.
  - This means: for all $\mathcal{U}$, for all I and for all α!
- φ is unsatisfiable if φ is not satisfiable.
- Formulas φ and ψ are equivalent, denoted by $\varphi \equiv \psi$, iff they have exactly the same models, i.e., $Mod(\varphi) = Mod(\psi)$. In other words, for all $\mathcal{U}$, I_α, we have $I_\alpha \models \varphi$ iff $I_\alpha \models \psi$
- Note: $p(x) \not\equiv p(y)$ why?

Construct a counter-example to $p(x) \equiv p(y)$

(Slide added on students' request)

We know from the definition of $\equiv$ that

$$p(x) \equiv p(y) \qquad \text{if and only if} \qquad Mod(p(x)) = Mod(p(y))$$

We construct $\mathcal{U}$, I_α such that $I_\alpha \models p(x)$ but $I_\alpha \not\models p(y)$

Let $\mathcal{U} = \{0, 1\}$, let $I(p) = \{(0)\}$ and let α map x to 0 and y to 1.

Then $I_\alpha \models p(x)$ iff $I \models p(0)$ iff $(0) \in I(p)$. Therefore $I_\alpha \models p(x)$.

Then $I_\alpha \models p(y)$ iff $I \models p(1)$ iff $(1) \in I(p)$. Therefore $I_\alpha \not\models p(y)$.

We have constructed $\mathcal{U}$, I_α which is a model of $p(x)$ but not of $p(y)$. Therefore, $Mod(p(x)) \neq Mod(p(y))$. Consequently, the equivalence does not hold.

Example

- Let $\Sigma = \{\{a/0, b/0, \circ/2\}, \{\sim /2\}\}$
- Let φ: $\exists x\,(x \circ a \sim b)$ or $\exists x\,(\sim(\circ(x, a), b)))$
- Q: Can φ be satisfied over $\mathcal{U} = \mathbb{N}_0$?

Example

- Let $\Sigma = \{\{a/0, b/0, \circ/2\}, \{\sim /2\}\}$
- Let φ: $\exists x\,(x \circ a \sim b)$ or $\exists x\,(\sim(\circ(x, a), b)))$
- Q: Can φ be satisfied over $\mathcal{U} = \mathbb{N}_0$?
- A: It depends on the interpretation (function)!

Example

- Let $\Sigma = \{\{a/0, b/0, \circ/2\}, \{\sim /2\}\}$
- Let φ: $\exists x\,(x \circ a \sim b)$ or $\exists x\,(\sim(\circ(x, a), b)))$
- Q: Can φ be satisfied over $\mathcal{U} = \mathbb{N}_0$?
- A: It depends on the interpretation (function)!
- Possibility 1: Let $I(a) = 0, I(b) = 1$
- Interpret $\circ$ as multiplication and $\sim$ as equality, i.e.,

$$\begin{aligned} I(\circ) &= \{((n_1, n_2), n) \mid n_1, n_2, n \in \mathbb{N}_0 \wedge n = n_1 \cdot n_2\} \\ I(\sim) &= \{(n, n) \mid n \in \mathbb{N}_0\} \end{aligned}$$

☞ φ is false under the above interpretation! (Why?)

Example

- Let $\Sigma = \{\{a/0, b/0, \circ/2\}, \{\sim /2\}\}$
- Let φ: $\exists x\,(x \circ a \sim b)$ or $\exists x\,(\sim(\circ(x, a), b)))$
- Q: Can φ be satisfied over $\mathcal{U} = \mathbb{N}_0$?
- A: It depends on the interpretation (function)!
- Possibility 2: Let $I(a) = 0, I(b) = 1$
- Interpret $\circ$ as addition and $\sim$ as equality

$$\begin{aligned} I(\circ) &= \{((n_1, n_2), n) \mid n_1, n_2, n \in \mathbb{N}_0 \wedge n = n_1 + n_2\} \\ I(\sim) &= \{(n, n) \mid n \in \mathbb{N}_0\} \end{aligned}$$

☞ φ is true under the above interpretation! (Why?)

Entailment (or logical implication)

- So far, $\models$ relates an interpretation and a formula.
- We want to allow a set of formulas on the left side.
- Important: a set of formulas coincides with the conjunction of its elements, i.e., $\{\varphi_1, \ldots, \varphi_n\}$ is $\bigwedge_{i=1}^{n} \varphi_i$.
- Important: an empty conjunction is 1 in all interpretations i.e., it is equivalent to $\top$.
- Let W be a set of closed formulas. Then W entails φ,

  $$W \models \varphi, \qquad \text{if and only if} \qquad Mod(W) \subseteq Mod(\varphi)$$

Entailment is a very important concept, when we consider theories!

Check of an entailment

Show: $\varphi \models \psi$ with $\varphi\colon \exists x\,(p(x) \wedge (p(x) \rightarrow q(x)))$ and $\psi\colon \exists y\, q(y)$

- We show that each model of φ is also a model of ψ.
- Take an arbitrary domain $\mathcal{U}$ and let I be a model of φ.
- Then there is $c \in \mathcal{U}$, s.t. $I_{\{x \leftarrow c\}}(p(x) \wedge (p(x) \rightarrow q(x))) = 1$.
- Moreover, $(c) \in I(p)$ and $(c) \in I(q)$. why?
- Evaluate ψ under the model of φ.
- $I(\exists y\, q(y)) = 1$ iff $I_{\{y \leftarrow d\}}(q(y)) = 1$ for some $d \in \mathcal{U}$
- Let $d = c$ and observe that I is then also a model of ψ.

Construction of a counter-example to an entailment

(Slide added on students' request)

Show: $\varphi \models \psi$ with φ: $p(c) \wedge (p(c) \rightarrow q(c))$ and ψ: $\forall y\, q(y)$

- Let c be a constant. Then φ is closed.
- We construct a counter-example, i.e., we present an interpretation $\mathcal{U}$, I, such that $I \models \varphi$, but $I \not\models \psi$.
- Take $\mathcal{U} = \{0, 1\}$ as the domain.
- Let $I(c) = 0$ and let I make exactly $p(0)$ and $q(0)$ true, i.e., $I(p) = \{(0)\}$ and $I(q) = \{(0)\}$. Consequently, $I \models \varphi$ holds.
- Evaluate ψ under the model of φ:
  $I(\forall y\, q(y)) = 1$ iff $I_{\{y \leftarrow d\}}(q(y)) = 1$ for all $d \in \mathcal{U}$
- Since $q(1)$ is false under I, so is ψ.

➥ We have found $\mathcal{U}$, I, such that $I \models \varphi$, but $I \not\models \psi$. Hence, $Mod(\varphi) \not\subseteq Mod(\psi)$ and therefore $\varphi \not\models \psi$.

Outline

Motivation

- Reasoning about application domains like software or hardware requires structures to formalize important properties.
- E.g., programs manipulate numbers, lists, arrays, pointers, etc.

↪ First-order theories can be used for the formalization.

☹ Reasoning with theories is undecidable in general.

☺ Reasoning with "restricted" theories is often decidable!

The definition of a theory

Definition

A first-order theory, $\mathcal{T} = (\Sigma, \mathcal{A})$, is defined by its components:

1. its signature Σ,
2. its axioms as a set $\mathcal{A}$ of closed first-order formulas with function symbols (FSs) and predicate symbols (PSs) from Σ.

A theory is often identified

1. by its axioms (when Σ is clear from the context), or
2. by the set of all Σ-formulas, valid in the theory.

A Σ-formula is constructed from FSs and PSs from Σ, as well as variables, connectives and quantifiers. We often use formula instead of Σ-formula when Σ is clear from the context.

Some definitions

Definition

Given a theory $\mathcal{T} = (\Sigma, \mathcal{A})$.

1. A $\mathcal{T}$-interpretation I is an interpretation which satisfies $\mathcal{T}$'s axioms, i.e.,
$$I \models \varphi \qquad \text{for all } \varphi \in \mathcal{A}$$
2. A Σ-formula φ is valid in the theory $\mathcal{T}$, or $\mathcal{T}$-valid, if every $\mathcal{T}$-interpretation satisfies φ. Notation: $\mathcal{T} \models \varphi$
3. A Σ-formula φ is satisfiable in the theory $\mathcal{T}$, or $\mathcal{T}$-satisfiable, if some $\mathcal{T}$-interpretation satisfies φ.

When $\mathcal{T}$ is clear from the context, we often use interpretation, valid, satisfiable instead of $\mathcal{T}$-interpretation, $\mathcal{T}$-valid, $\mathcal{T}$-satisfiable

What is the connection to entailment, i.e., to $W \models \varphi$?

Properties of theories

Definition

A theory $\mathcal{T} = (\Sigma, \mathcal{A})$ is

1. complete, if for every closed Σ-formula φ, $\mathcal{T} \models \varphi$ or $\mathcal{T} \models \neg\varphi$;
2. consistent, if there is at least one $\mathcal{T}$-interpretation;
3. decidable, if $\mathcal{T} \models \varphi$ is decidable for every Σ-formula φ.

Formulas φ_1 and φ_2 are equivalent in $\mathcal{T}$ or $\mathcal{T}$-equivalent if $\mathcal{T} \models \varphi_1 \leftrightarrow \varphi_2$, i.e., $I \models \varphi_1$ iff $I \models \varphi_2$ holds for all $\mathcal{T}$-interpretations I.

Example of a complete theory: Presburger arithmetic [link]

Example of an incomplete theory: group theory [link]

Incompleteness of group theory

(Slide added on students' request)

Q: Why is group theory incomplete?

A: Because for the formula $\varphi\colon \forall x \forall y\, (x \cdot y \doteq y \cdot x)$, it holds that

$$\mathcal{T} \not\models \neg\varphi \qquad \text{and} \qquad \mathcal{T} \not\models \varphi.$$

The sentence $\neg\forall x \forall y\ (x \cdot y = y \cdot x)$ is not valid for groups. Take the abelian group $(\mathbb{Z}, +)$, i.e., use $\mathcal{U} = \mathbb{Z}$ and define I appropriately. Since addition in $\mathbb{Z}$ is commutative, $\forall x \forall y\ (x \cdot y = y \cdot x)$ is true under $\mathcal{U}$, I and therefore the negation is false. We have identified a model of the theory which is not a model of $\neg\forall x \forall y\ (x \cdot y = y \cdot x)$.

The sentence $\forall x \forall y\ (x \cdot y = y \cdot x)$ is not valid for groups. Simply take a non-commutative group (like the symmetric group S_n of degree $n \geq 3$) and proceed similarly.

Fragments of theories

A fragment of a theory $\mathcal{T}$ is a syntactically restricted subset of formulas of $\mathcal{T}$. A fragment of $\mathcal{T}$ is decidable if $\mathcal{T} \models \varphi$ is decidable for every Σ-formula φ from the fragment.

Example

1. The quantifier-free fragment of a theory $\mathcal{T}$ is the set of $\mathcal{T}$-valid formulas without quantifiers.

   NB Technically speaking, the "quantifier-free fragment" consists of valid formulas in which all variables are considered to be universally quantified!

2. The fragment of prenex conjunctive normal forms consists of valid formulas which have a quantifier prefix and a matrix in conjunctive normal form (CNF).

Combinations of theories

- The union $\mathcal{T}_1 \cup \mathcal{T}_2$ of two theories $\mathcal{T}_1$ and $\mathcal{T}_2$ with signatures Σ_1 and Σ_2 and axioms $\mathcal{A}_1$ and $\mathcal{A}_2$ has
  1. signature $\Sigma_1 \cup \Sigma_2$ and
  2. axioms $\mathcal{A}_1 \cup \mathcal{A}_2$.
- We restrict our attention here to combinations for which $\Sigma_1 \cap \Sigma_2 = \{\doteq\}$ holds.
- A $(\mathcal{T}_1 \cup \mathcal{T}_2)$-interpretation is both a $\mathcal{T}_1$-interpretation and a $\mathcal{T}_2$-interpretation, since it satisfies $\mathcal{A}_1 \cup \mathcal{A}_2$.

➥ A formula which is $\mathcal{T}_1$-valid or $\mathcal{T}_2$-valid is $(\mathcal{T}_1 \cup \mathcal{T}_2)$-valid.

➥ A formula which is $(\mathcal{T}_1 \cup \mathcal{T}_2)$-satisfiable is both $\mathcal{T}_1$-satisfiable and $\mathcal{T}_2$-satisfiable.

The theory of equality

- Σ_E consists of $\doteq$ together with FSs and other PSs.
- $\doteq$ is an interpreted symbol: the meaning is defined by the axioms of $\mathcal{T}_E$ ($\forall x_1, \ldots, x_n$ abbreviates $\forall x_1 \cdots \forall x_n$):
  1. $\forall x \; (x \doteq x)$ (reflexivity)
  2. $\forall x, y \; ((x \doteq y) \rightarrow (y \doteq x))$ (symmetry)
  3. $\forall x, y, z \; ((x \doteq y) \wedge (y \doteq z) \rightarrow (x \doteq z))$ (transitivity)
  4. Substitution axioms for each function symbol f of arity n:

$$\forall x_1, y_1, \ldots, x_n, y_n \left(\bigwedge_{i=1}^{n} x_i \doteq y_i \rightarrow f(x_1, \ldots, x_n) \doteq f(y_1, \ldots, y_n) \right)$$

  5. Substitution axioms for each predicate symbol p of arity n:

$$\forall x_1, y_1, \ldots, x_n, y_n \left(\bigwedge_{i=1}^{n} x_i \doteq y_i \rightarrow \left(p(x_1, \ldots, x_n) \leftrightarrow p(y_1, \ldots, y_n) \right) \right)$$

The theory of equality cont'd

- The axioms 1. to 3. state that $\doteq$ is an equivalence relation.
- The axioms 4. and 5. assert that $\doteq$ is a congruence relation.
- Functions (predicates) evaluate always to the same value (truth value) provided the same arguments are given.
- $\mathcal{T}_E$ is undecidable, but its quantifier-free fragment is decidable.

Example

Show: $\varphi\colon a \doteq b \wedge b \doteq c \rightarrow g(f(a), b) \doteq g(f(c), a)$ is $\mathcal{T}_E$-valid

The proof is by contradiction. Suppose there exists a $\mathcal{T}_E$-interpretation I with $I \not\models \varphi$.

1.	$I \not\models \varphi$	assumption
2.	$I \models a \doteq b \wedge b \doteq c$	1., semantics of $\rightarrow$
3.	$I \not\models g(f(a), b) \doteq g(f(c), a)$	1., semantics of $\rightarrow$
4.	$I \models a \doteq b$	2., semantics of $\wedge$
5.	$I \models b \doteq c$	2., semantics of $\wedge$
6.	$I \models a \doteq c$	4., 5., transitivity of $\doteq$
7.	$I \models f(a) \doteq f(c)$	6., substitution axiom for f
8.	$I \models b \doteq a$	4., symmetry of $\doteq$
9.	$I \models g(f(a), b) \doteq g(f(c), a)$	7., 8., substitution axiom for g
10.	$I \models \bot$	3., 9., contradiction

The assumption is false: φ is therefore $\mathcal{T}_E$-valid!

The theory of LISP-like lists: $\mathcal{T}_{cons}$

LISP-like lists have signature $\Sigma_{cons} = \{\{cons, car, cdr\}, \{atom, \doteq\}\}$

1. $cons$ is a binary function called the list constructor. $cons(a, b)$ represents the list constructed from a and b.
2. car is a unary function called the left projector. $car(cons(a, b)) \doteq a$
3. cdr is a unary function called the right projector. $cdr(cons(a, b)) \doteq b$
4. $atom$ is a unary predicate. $atom(x)$ is true iff x is a single-element list.
5. $\doteq$ is the binary predicate equality.

Examples of LISP-like lists

In the intended interpretations

- atoms are individual elements,
- while lists are functional structures with binary FS *cons*.

$cons(a, cons(b, c))$

- represents a list of three elements,
- a is its head and $cons(b, c)$ is its tail
- Examples:
  1. $car(cons(a, cons(b, c))) \mapsto a$
  2. $cdr(cons(a, cons(b, c))) \mapsto cons(b, c)$
  3. $cdr(cdr(cons(a, cons(b, c)))) \mapsto c$

The axioms of $\mathcal{T}_{cons}$

1. The axioms of reflexivity, symmetry, and transitivity
2. Substitution axioms (functional congruence) for *cons*, *car*, *cdr*
3. Substitution axioms (predicate congruence) for *atom*
4. $\forall x, y\ car(cons(x, y)) \doteq x$ (left projection)
5. $\forall x, y\ cdr(cons(x, y)) \doteq y$ (right projection)
6. $\forall x\ \neg atom(x) \rightarrow cons(car(x), cdr(x)) \doteq x$ (construction)
7. $\forall x, y\ \neg atom(cons(x, y))$ (atom)

The theory $\mathcal{T}_{cons}$: Some remarks

- There is no *NIL* value representing the empty list.
- The behavior of *car* and *cdr* on atoms is unspecified.
- $\mathcal{T}_{cons}$ is undecidable, but its quantifier-free fragment is decidable.

The theory $\mathcal{T}^E_{cons} = \mathcal{T}_{cons} \cup \mathcal{T}_E$

- Let $\mathcal{T}_{cons} = (\Sigma_{cons}, \mathcal{A}_{cons})$ and $\mathcal{T}_E = (\Sigma_E, \mathcal{A}_E)$.
- The signature of $\mathcal{T}^E_{cons}$ is $\Sigma_{cons} \cup \Sigma_E$.
- The set of axioms of $\mathcal{T}^E_{cons}$ is $\mathcal{A}_{cons} \cup \mathcal{A}_E$.
- $\mathcal{T}^E_{cons}$ has uninterpreted CSs, FSs, and PSs from Σ_E.
- $\mathcal{T}^E_{cons}$ is undecidable, but its quantifier-free fragment is decidable.
- Prove the following formula φ

  $$car(a) \doteq car(b) \wedge cdr(a) \doteq cdr(b) \wedge \neg atom(a) \wedge \neg atom(b) \rightarrow f(a) \doteq f(b)$$

  $\mathcal{T}^E_{cons}$-valid.

The theory $\mathcal{T}^E_{cons}$: The proof of φ

The proof is by contradiction. Suppose there exists a $\mathcal{T}^E_{cons}$-interpretation I with $I \not\models \varphi$.

1.	$I \not\models \varphi$	assumption
2.	$I \models car(a) \doteq car(b)$	1., semantics of $\rightarrow$, $\wedge$
3.	$I \models cdr(a) \doteq cdr(b)$	1., semantics of $\rightarrow$, $\wedge$
4.	$I \models \neg atom(a)$	1., semantics of $\rightarrow$, $\wedge$
5.	$I \models \neg atom(b)$	1., semantics of $\rightarrow$, $\wedge$
6.	$I \not\models f(a) \doteq f(b)$	1., semantics of $\rightarrow$
7.	$I \models cons(car(a), cdr(a)) \doteq cons(car(b), cdr(b))$	2., 3., functional congruence
8.	$I \models cons(car(a), cdr(a)) \doteq a$	4., construction
9.	$I \models cons(car(b), cdr(b)) \doteq b$	5., construction
10.	$I \models a \doteq b$	7., 8., 9., symmetry + transitivity
11.	$I \models f(a) \doteq f(b)$	10., functional congruence
10.	$I \models \bot$	6., 11., contradiction

The assumption is false: φ is therefore $\mathcal{T}^E_{cons}$-valid!

Further examples for theories

- Presburger arithmetic ($\Sigma = (\{0/0, 1/0, +/2\}, \{\doteq/2\})$)
- Peano arithmetic ($\Sigma = (\{0/0, 1/0, +/2, */2\}, \{\doteq/2\})$)
- Theory of integers
- Theory of reals
- Theory of arrays
- Theory of pointers
- Theory of recursive data structures
- and many more

Learning objectives

You should be able to

- explain the syntax and semantics of first-order logic,
- evaluate formulas under a given first-order structure,
- find models/falsifying interpretations for first-order formulas,
- evaluate entailments and provide proofs or counter-examples,
- motivate the use of theories,
- explain $\mathcal{T}$-validity and $\mathcal{T}$-satisfiability in detail,
- check them for a formula and a theory
  (including providing proofs or counter-examples for the answers),
- discuss the notion of decidability of a theory or one of its fragments.