First order theories

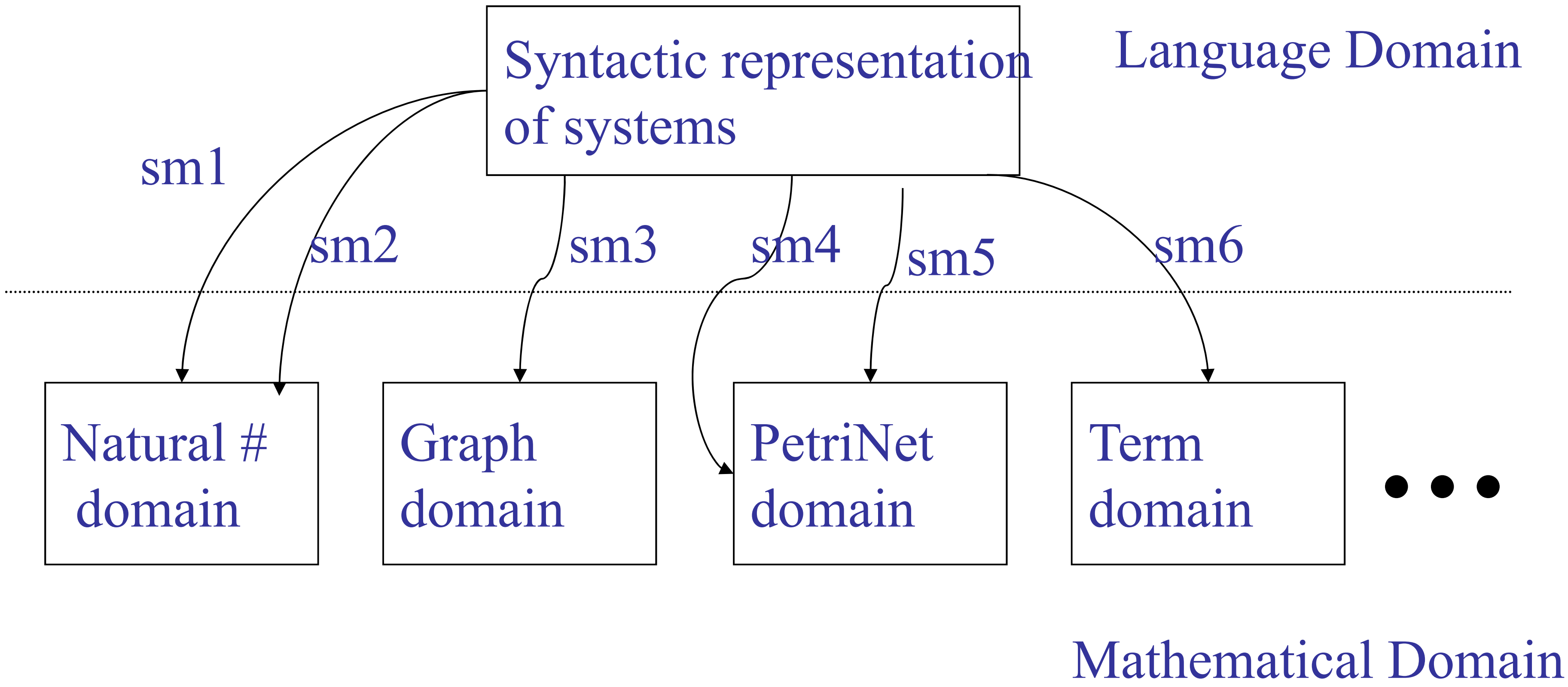
(Chapter 1, Sections 1.4 – 1.5)

From the slides for the book
“Decision procedures”
by D.Kroening and O.Strichman

Prelude: Syntax v.s. Semantic in Logic Framework

- An example of small language
  - Syntax
    - F := 0 | 1 | F + 1 | 1 + F
    - Ex. 0, 0+1+1, 1+0+1, but not 0+0
  - Possible semantics
    - 1 + 1 == 1 + 1 + 0 ?
      - Yes (interpreting formula as a natural #),
        - $[1 + 1]_{N1} = 2$, $[1 + 1 + 0]_{N1} = 2$ → $1 + 1 =_{N1} 1 + 1 + 0$
      - No (interpreting formula as string),
        - $[1+1]_S$="1+1",$[1+1+0]_S$="1+1+0"→ $1+1 \mathrel{!=_S} 1+1+0$
      - No (interpreting formula as a natural # of string length)
        - $[1 + 1]_{N2} = 3$, $[1 + 1 + 0]_{N2} = 5$ → $1 + 1 \mathrel{!=_{N2}} 1 + 1 + 0$

Examples of Semantic Mapping



First order logic

- A first order theory consists of
  - Variables
  - Logical symbols: — Æ = ; < `(' `)'
  - Non-logical Symbols ∑: Constants, predicate and function symbols
  - Syntax

Examples

- Σ = {0,1, '+', '>'}
  - '0','1' are constant symbols
  - '+' is a binary function symbol
  - '>' is a binary predicate symbol

- An example of a Σ-formula:

$$< y \;\, ; x.\ x > y$$

Examples

- $\Sigma = \{1$, ‘>’, ‘<’, ‘isprime’$\}$
  - ‘1’ is a constant symbol
  - ‘>’, ‘<‘ are binary predicates symbols
  - ‘isprime’ is a unary predicate symbol
- An example Σ-formula:

$$;n < p.\ n > 1\ \$\ \ \mathrm{isprime}(p) - n < p < 2n.$$

- Are these formulas valid ?
- So far these are only symbols, strings. No meaning yet.

Interpretations

- Let $\Sigma = \{0,1, \text{'+'}, \text{'='}\}$ where 0,1 are constants, '+' is a binary function symbol and '=' a predicate symbol.
- Let $\phi = <x.\ x + 0 = 1$
- Q: Is ϕ true in Q_0 ?
- A: Depends on the interpretation!

Structures

- A structure is given by:
  1. A domain
  2. An interpretation of the nonlogical symbols: i.e.,
     - Maps each predicate symbol to a predicate of the same arity
     - Maps each function symbol to a function of the same arity
     - Maps each constant symbol to a domain element
  3. An assignment of a domain element to each free (unquantified) variable

Structures

- Remember $\phi = \forall x.\ x + 0 = 1$
- Consider the structure S:
  - Domain: $\mathbb{Q}_0$
  - Interpretation:
    - '0' and '1' are mapped to 0 and 1 in $\mathbb{Q}_0$
    - '=' $\mapsto$ = (equality)
    - '+' $\mapsto$ * (multiplication)
- Now, is ϕ true in S ?

Satisfying structures

- Definition: A formula is satisfiable if there exists a structure that satisfies it

- Example: $\phi = < x.\ x + 0 = 1$ is satisfiable
- Consider the structure S':
  - Domain: Q_0
  - Interpretation:
    - '0' and '1' are mapped to 0 and 1 in Q_0
    - '=' $\mapsto$ = (equality)
    - '+' $\mapsto$ + (addition)
- S' satisfies ϕ. S' is said to be a model of ϕ.

First-order theories

- First-order logic is a framework.
- It gives us a generic syntax and building blocks for constructing restrictions thereof.
- Each such restriction is called a first-order theory.

- A theory defines
  - the signature Σ (the set of nonlogical symbols) and
  - the interpretations that we can give them.

Definitions

- Σ – the signature. This is a set of nonlogical symbols.
- Σ-formula: a formula over Σ symbols + logical symbols.
- A variable is free if it is not bound by a quantifier.
- A sentence is a formula without free variables.
- A Σ-theory T is defined by a set of Σ-sentences.

Definitions…

- Let T be a Σ-theory
- A Σ-formula ϕ is T-satisfiable if there exists a structure that satisfies both ϕ and the sentences defining T.
- A Σ-formula ϕ is T-valid if all structures that satisfy the sentences defining T also satisfy ϕ.

Example

- Let Σ = {0,1, '+', '='}
- Recall ϕ = <x. x + 0 = 1
- ϕ is a Σ-formula.
- We now define the following Σ-theory:
  - ;x. x = x // '=' must be reflexive
  - ;x,y. x + y = y + x // '+' must be commutative
- Not enough to prove the validity of ˙ !

Theories through axioms

- The number of sentences that are necessary for defining a theory may be large or infinite.
- Instead, it is common to define a theory through a set of axioms.
- The theory is defined by these axioms and everything that can be inferred from them by a sound inference system.

Example 1

- Let $\Sigma = \{\text{'='}\}$
  - An example Σ-formula is $\phi = ((x = y) \land \neg(y = z)) \rightarrow \neg(x = z)$
- We would now like to define a Σ-theory T that will limit the interpretation of '=' to equality.
- We will do so with the equality axioms:
  - $\forall x.\ x = x$ (reflexivity)
  - $\forall x,y.\ x = y \rightarrow y = x$ (symmetry)
  - $\forall x,y,z.\ x = y \land y = z \rightarrow x = z$ (transitivity)
- Every structure that satisfies these axioms also satisfies ϕ above.
- Hence ϕ is T-valid.

Example 2

- Let $\Sigma = \{‘<’\}$
- Consider the Σ-formula $\varphi: \forall x \exists y.\ y < x$
- Consider the theory T:
  - $\forall x,y,z.\ x < y \wedge y < z \rightarrow x < z$ (transitivity)
  - $\forall x,y.\ x < y \rightarrow \neg(y < x)$ (anti-symmetry)

Example 2 (cont'd)

- Recall: ˙: ;x <y. y < x

- Is ˙ T-satisfiable?
- We will show a model for it.
  - Domain:]
  - '<' $\mapsto$ <
- Is ˙ T-valid ?
- We will show a structure to the contrary
  - Domain: Q 0
  - '<' $\mapsto$ <

Fragments

- So far we only restricted the nonlogical symbols.
- Sometimes we want to restrict the grammar and the logical symbols that we can use as well.
- These are called logic fragments.
- Examples:
  - The quantifier-free fragment over Σ = {'=', '+',0,1}
  - The conjunctive fragment over Σ = {'=', '+',0,1}

Fragments

- Let $\Sigma = \{\}$
  - (T must be empty: no nonlogical symbols to interpret)
- Q: What is the quantifier-free fragment of T ?
- A: propositional logic

- Thus, propositional logic is also a first-order theory.
  - A very degenerate one.

Theories

- Let $\sum = \{\}$
  - (T must be empty: no nonlogical symbols to interpret)
- Q: What is T ?
- A: Quantified Boolean Formulas (QBF)

- Example:
  - $;x_1 < x_2\ ;x_3.\ x_1 \rightarrow (x_2 \text{ Æ } x_3)$

Some famous theories

- Presburger arithmetic: Σ = {0,1, ‘+’, ‘=’}
- Peano arithmetic: Σ = {0,1, ‘+’, ‘*’, ‘=’}
- Theory of reals
- Theory of integers
- Theory of arrays
- Theory of pointers
- Theory of sets
- Theory of recursive data structures
- …

The algorithmic point of view...

- It is also common to present theories NOT through the axioms that define them.

- The interpretation of symbols is fixed to their common use.
  - Thus '+' is plus, ...

- The fragment is defined via grammar rules rather than restrictions on the generic first-order grammar.

The algorithmic point of view...

- Example: equality logic (= “the theory of equality”)
- *Grammar:*

formula : *formula* Æ *formula* | = *formula* | *atom*

atom : term-variable = term-variable

| term-variable = constant | Boolean-variable

- Interpretation:

‘=’ is equality.

The algorithmic point of view...

- This simpler way of presenting theories is all that is needed when our focus is on decision procedures specific for the given theory.

- The traditional way of presenting theories is useful when discussing generic methods (for any decidable theory T)
  - Example 1: algorithms for combining two or more theories
  - Example 2: generic SAT-based decision procedure given a decision procedure for the conjunctive fragment of T.

Expressiveness of a theory

- Each formula defines a language:
  the set of satisfying assignments ('models') are the words accepted by this language.

- Consider the fragment '2-CNF'

  formula : (*literal* $\vee$ *literal*) | *formula* $\wedge$ *formula*

  literal: Boolean-variable | $\neg$Boolean-variable

$$(x_1 \vee \neg x_2) \wedge (\neg x_3 \vee x_2)$$

Expressiveness of a theory

- Now consider a Propositional Logic formula

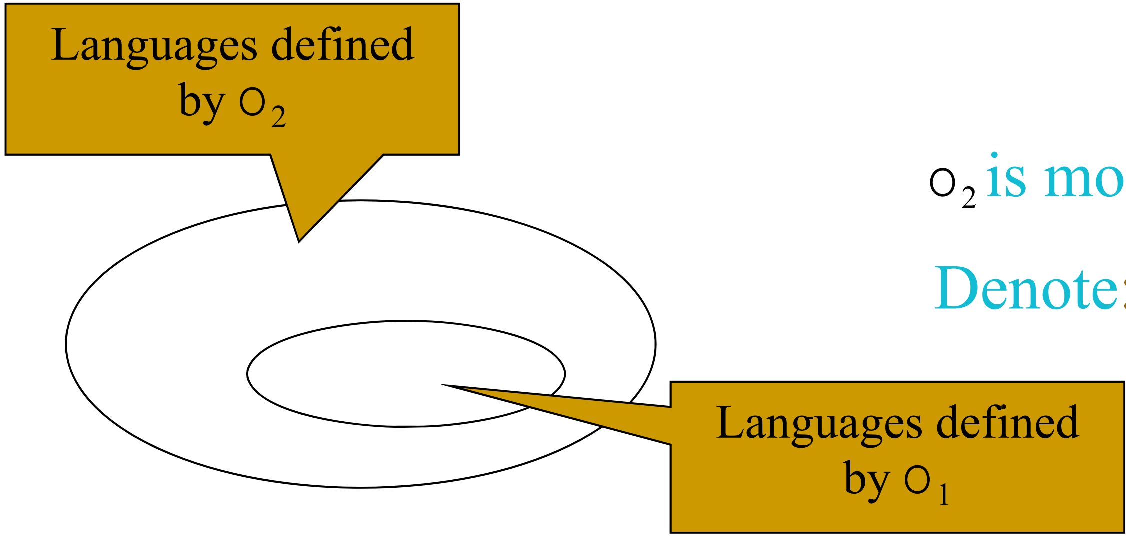
  ϕ: $(\{_1$ Æ $\{_2$ Æ $\{_3)$.

- Q: Can we express this language with 2-CNF?
- A: No.

  Proof:

  - The language accepted by ϕ has 7 words: all assignments other than $\{_1 = \{_2 = \{_3 = F$.
  - The first 2-CNF clause removes ¼ of the assignments, which leaves us with 6 accepted words. Additional clauses only remove more assignments.

Expressiveness of a theory



o₂ is more expressive than o₁.

Denote: o₁ ˚ o₂

- *Claim*: 50F Q I ˚ Surrsvlwlrqdo#Orjlf
- J hqhudoo|#wkhuh#lv#rqo|#d#sduwldo#rughu ehwz hhq##wkhrulhv1

The tradeoff

- So we see that theories can have different expressive power.

- Q: why would we want to restrict ourselves to a theory or a fragment ? why not take some ‘maximal theory’…

- A: Adding axioms to the theory may make it harder to decide or even undecidable.

Example: Hilbert axiom system (K)

- Let K be (M.P) + the following axiom schemas:

$$A \mathbin{\$} (B \mathbin{\$} A) \qquad \text{(H1)}$$

$$((A \mathbin{\$} (B \mathbin{\$} C)) \mathbin{\$} ((A \mathbin{\$} B) \mathbin{\$} (A \mathbin{\$} C)) \qquad \text{(H2)}$$

$$({=}B \mathbin{\$} \#{=}A) \mathbin{\$} \#(A \mathbin{\$} B) \qquad \text{(H3)}$$

- K is sound and complete
- This means that with K we can prove any valid propositional formula, and only such formulas. The proof is finite.

Example

- But there exists first order theories defined by axioms which are not sufficient for proving all T-valid formulas.

Example: First Order Peano Arithmetic

- $\Sigma = \{0, 1, \text{‘+’}, \text{‘*’}, \text{‘=’}\}$
- Domain: Natural numbers

Undecidable!

- Axioms (“semantics”):
  1. $; x : (0 \neq x + 1)$
  2. $; x : ; y : (x \neq y) \, \$ \, (x + 1 \neq y + 1)$
  3. Induction
  4. $; x : x + 0 = x$
  5. $; x : ; y : (x + y) + 1 = x + (y + 1)$
  6. $; x : x * 0 = 0$
  7. $; x ; y : x * (y + 1) = x * y + x$

$+ \left\{ \text{axioms 4–5} \right.$

$* \left\{ \text{axioms 6–7} \right.$

These axioms define the semantics of ‘+’

Example: First Order Presburger Arithmetic

- Σ = {0,1,‘+’, ~~‘*’~~, ‘=’}
- Domain: Natural numbers

decidable!

- Axioms (“semantics”):
  1. ; x : (0 $\neq$ x + 1)
  2. ; x : ; y : (x $\neq$ y) $ (x + 1 $\neq$ y + 1)
  3. Induction

+

  4. ; x : x + 0 = x
  5. ; x : ; y : (x + y) + 1 = x + (y + 1)

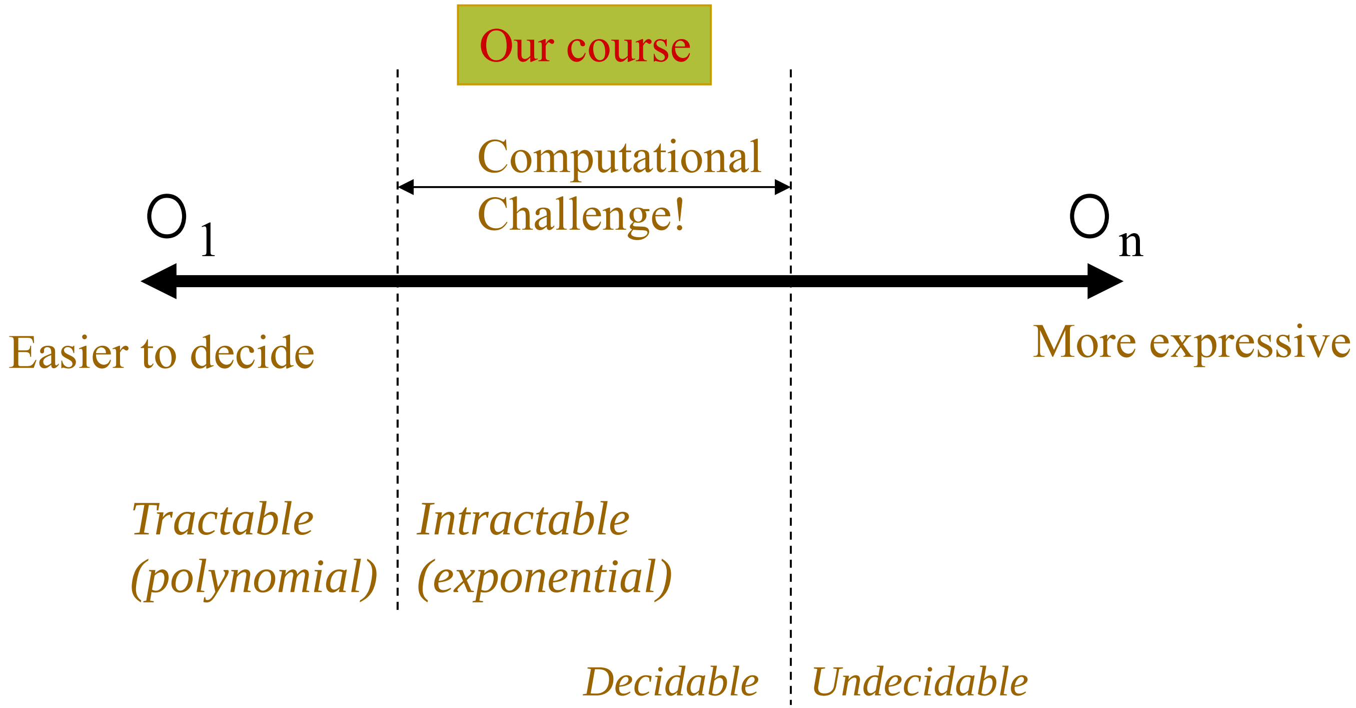
These axioms define the semantics of ‘+’

*

  6. ~~; x : x * 0 = 0~~
  7. ~~; x ; y : x * (y + 1) = x * y + x~~

Tradeoff: expressiveness/computational hardness.

- Assume we are given theories O_1 ° … ° O_n



When is a specific theory useful?

1. Expressible enough to state something interesting.
2. Decidable (or semi-decidable) and more efficiently solvable than richer theories.
3. More expressible, or more natural for expressing some models in comparison to ‘leaner’ theories.