CMPS 217 – Logic in Computer Science

https://courses.soe.ucsc.edu/courses/cmps217/Spring13/01

Lecture #18

Validities

Theorem (Gödel's Completeness Theorem):
The Validity Problem is semi-decidable.
Equivalently, there is an algorithm that enumerates all valid FO-sentences.

- In what follows, we will give a proof of this theorem for the special case of FO-sentences without the equality symbol =.

- The proof will be carried out in three steps.
  Step 1: We will prove Skolem's Theorem for FO-sentences.

  Step 2: We will prove Herbrand's Theorem for FO-sentences without the equality symbol =

  Step 3: We will show that the semi-decidablity of the Validity Problem for FO-sentences without the equality symbol follows from Step 1, Step 2, and the Compactness Theorem for Propositional Logic.

Skolem's Theorem

Theorem:

- There is a polynomial-time algorithm such that, given a FO-sentence φ, it returns a Π_1-sentence $\varphi*$ over a signature expanded with additional function symbols $f_1, f_2, \ldots, f_k$ such that

$$\varphi \equiv \exists f_1 \exists f_2 \ldots \exists f_k \varphi^*.$$

  - In particular, φ is satisfiable if and only if φ^* is satisfiable.
- Moreover, if the equality symbol = does not occur in φ, then it does not occur in φ^* either.

Proof:

Step 1: Bring φ to prenex normal form.

Step 2: If φ begins with $\forall$, then apply repeatedly the transformation

$$\forall x_1 \ldots \forall x_k \exists y\, \theta \equiv \exists f \forall x_1 \ldots \forall x_k\, \theta(y/f(x_1,\ldots,x_k)).$$

Step 3: If φ begins with $\exists$, then apply the transformation

$$\exists z\, \theta \equiv \exists f \forall w\, \theta(z/f(w))$$

(to see that these two formulas are logically equivalent:

- left to right: take a witness c for z and let f be the constant function f(w) = c.

- right to left: if b is any element, then f(b) is a witness for z.)

Herbrand Universe and Herbrand Structures

Definition. Let ψ be a FO-sentence.

- The Herbrand Universe U(ψ) of ψ is the set of all possible terms obtained from the function symbols and the constant symbols occurring in ψ.
  - If ψ has no function or constant symbols, then U(ψ) consists of a new constant symbol c and all terms obtained from c and the function symbols occurring in ψ.
- A Herbrand structure associated with ψ is a structure **A** such that
  - the universe of **A** is the Herbrand universe U(ψ).
  - the terms are interpreted on **A** by themselves
  - there no restrictions on the relations of **A**.
- Thus, to define a Herbrand structure, it suffices to define its relations.

Herbrand Structures

Example: Let ψ be the formula $\forall$ x (R(x,c) $\vee$ R(x,f(d))

- The Herbrand Universe is the following infinite set
  U(ψ) = { c, d, f(c), f(d), f(f(c)), f(f(d)), f(f(f(c))), …}

- Herbrand Structure **A** = (U(ψ), R′, f′, c, d) with
  - f′(c) = f(c), f′(d) = f(d), …
    (more generally, f′(t) = f(t)).
  - R′ = {(c,c), (d,c)}

- Different Herbrand structures can be obtained by changing the relation R′, while keeping everything else the same.
  - For example, consider the Herbrand structure **B** in which the relation symbol R is interpreted by the relation
    R″ = {(c,d), (d,d), (d, f(d)), (f(f(c)), f(f(f(d)))}

Herbrand Structures

Theorem A: Let ψ be a Π_1-sentence without equality. Then the following statements are equivalent:

1. ψ is satisfiable.
2. ψ is satisfiable by some Herbrand structure.

Proof: Only the direction 1. ⇒ 2. is not obvious.

Let $f_1,\dots,f_n$, $R_1,\dots,R_m$, $c_1,\dots,c_k$ be the non-logical symbols occurring in ψ.

Assume that there is a structure

$\mathbf{A} = (A, f^*_1, \dots, f^*_n, R^*_1,\dots,R^*_m, c^*_1,\dots,c^*_k)$ such that $\mathbf{A} \models \psi$.

Let $\mathbf{B}$ be the Herbrand structure with universe $U(\psi)$ and with relations $R'_1,\dots,R'_m$ defined as follows:

if R_i is a relation symbol of arity r and $t_1,\dots,t_r$ are closed terms, then

$$(t_1,\dots t_r) \in R'_i \text{ if and only if } \mathbf{A} \models R^*_i(t^{\mathbf{A}}_1,\dots,t^{\mathbf{A}}_r),$$

where $t^{\mathbf{A}}_j$ is the interpretation of the term t_j on $\mathbf{A}$.

We will show that $\mathbf{B} \models \psi$.

Herbrand Structures

Lemma: Let θ be a quantifier-free formula with variables $x_1,\ldots x_n$ and without equality =. For all closed terms $t_1,\ldots,t_n$, the following statements are equivalent:

1. $\mathbf{B} \models \theta(x_1/t_1,\ldots,x_n/t_n)$
2. $\mathbf{A} \models \theta(x_1/t^{\mathbf{A}}{}_1,\ldots,x_n/t^{\mathbf{A}}{}_n)$.

Proof: By induction on the construction of quantifier-free formulas. The base case of atomic formulas is true because of the way **B** was defined.

Note: This lemma fails if we equalities = are allowed.
For example, **A** may satisfy $c^*_1 = f^*_2(c_2)$, while **B** does not.

Herbrand Structures

Proof (continued):

Since ψ is a Π_1-sentence, it is of the form $\forall x_1 \ldots \forall x_n\ \theta$, where θ is quantifier-free. We have to show that **B** $\models \forall x_1 \ldots \forall x_n\ \theta$.

- Take n elements from the universe U(ψ) of **B**. They must be closed terms $t_1, \ldots, t_n$.
- Since **A** $\models \forall x_1 \ldots \forall x_n\ \theta$, we have that **A** $\models \theta(x_1/t^{\mathbf{A}}_1, \ldots, x_n/t^{\mathbf{A}}_n)$.
- Hence, by the Lemma, we have that **B** $\models \theta(x_1/t_1, \ldots, x_n/t_n)$.
- This completes the proof that **B** $\models \forall x_1 \ldots \forall x_n\ \theta$.

Illustration

Example (continued): Let ψ be the formula $\forall$ x (R(x,c) $\vee$ R(x,f(d))

- The Herbrand Universe is the following infinite set

  U(ψ) = { c, d, f(c), f(d), f(f(c)), f(f(d)), f(f(f(c))), …}

- ψ is satisfiable.

  For example, **A** $\models \psi$, where **A** = ({a}, f*, R*, a ,a), f*(a) = a, and

  R* = {(a,a)}. Note that f*(f*(a)) = a, f*(f*(f*(a))) = a, etc.

  Thus, for every closed term t, we have that $t^{\mathbf{A}}$ = a.

- Let **B** = (U(ψ), f′, R′, c, d) be the Herbrand model such that

  $(t_1,t_2) \in R'$ if and only if $(t^{\mathbf{A}}_1,t^{\mathbf{A}}_2) \in R^*$.

  This means that R′ = {(t_1,t_2): t_1, t_2 are closed terms}.

- Clearly, **B** $\models \psi$.

Herbrand's Theorem

Recall that our goal is to establish

Herbrand's Theorem:

- For every Π_1-sentence ψ without the equality symbol =, there is a (perhaps infinite) set H(ψ) of propositional formulas such that

  ψ is satisfiable if and and only if H(ψ) is satisfiable.
- Moreover, there is an algorithm that, given ψ, it enumerates H(ψ) (i.e., it produces a list of all elements of H(ψ).

Definition: Let ψ is a Π_1-sentence of the form $\forall\, x_1 \ldots \forall\, x_n\, \theta$, where θ is quantifier-free. The Herbrand expansion H(ψ) of ψ is the set

$$H(\psi) = \{ \theta(x_1/t_1,\ldots,x_n/t_n):\ t_1,\ldots,t_n \text{ are in } U(\psi) \}$$

Herbrand Expansions

Definition: Let ψ is a Π_1-sentence of the form $\forall$ x_1 …$\forall$ x_n θ, where θ is quantifier-free. The Herbrand expansion H(ψ) of ψ is the set

$$H(\psi) = \{ \theta(x_1/t_1,\ldots,x_n/t_n): t_1,\ldots, t_n \text{ are in } U(\psi) \}$$

Note: On the face of it, H(ψ) is a set of quantifier-free sentences. However, it can be identified, and it will be identified, with a set of propositional formulas obtained from the sentences of H(ψ) by replacing each distinct atomic sentence $R(t_1,\ldots,t_m)$ by a distinct propositional variable.

Fact: There is an algorithm that, given a Π_1-sentence ψ, it enumerates all members of the Herbrand expansion H(ψ) of ψ.

Herbrand Expansions

Example 1: Let ψ be the formula $\forall$ x (R(c,x) $\vee$ R(x,f(c))

H(ψ) contains the quantifier-free sentences:

- R(c,c) $\vee$ R(c,f(c)) x/c
- R(c,f(c)) $\vee$ R(f(c),f(c)) x/f(c)
- R(c,f(f(c)) $\vee$ R(f(f(c)), f(c)) x/f(f(c))
- …

As a set of propositional formulas, H(ψ) contains the formulas

- $P_1 \vee P_2$
- $P_2 \vee P_3$
- $P_4 \vee P_5$
- …

Herbrand Expansions

Example 2: Let ψ be the formula $\forall x\,(P(x) \vee \neg P(f(c))$

$H(\psi)$ contains the quantifier-free sentences:

- $P(c) \vee \neg P(f(c))$ x/c
- $P(f(c)) \vee \neg P(f(c))$ x/f(c)
- $P(f(f(c)) \vee \neg P(f(c))$ x/f(f(c))
- …

As a set of propositional formulas, $H(\psi)$ contains the formulas

- $P_1 \vee \neg P_2$
- $P_2 \vee \neg P_2$
- $P_3 \vee \neg P_2$
- …

Herbrand's Theorem

Herbrand's Theorem:

Let ψ be a Π_1-sentence ψ without the equality symbol = and let H(ψ) be its Herbrand expansion. Then the following statements are equivalent

- ψ is satisfiable
- H(ψ) is satisfiable (as a set of propositional formulas)

Proof:

By Theorem A, ψ is satisfiable if and only if ψ is satisfiable by some Herbrand structure **A**. Recall that in defining a Herbrand structure **A**, we need only define the relations of **A**. This means that we only need to decide which atomic sentences $R(t_1,\ldots,t_n)$ are true on **A** or, equivalently, we need to decide the truth values of the propositional variables occurring in H(ψ).

It follows that the Herbrand structures that satisfy ψ are in a one-to-one correspondence with the satisfying truth assignments of H(ψ).

In particular, ψ is satisfiable if and only if H(ψ) is satisfiable.

Herbrand' Theorem: Illustration

Example: Let ψ be the formula $\forall$ x (P(x) $\vee$ $\neg$ P(f(c))

H(ψ) contains the quantifier-free sentences:

- R(c,c) $\vee$ R(c,f(c)),
- R(c,f(c)) $\vee$ R(f(c),f(c))
- R(c,f(f(c)) $\vee$ R(f(f(c)), f(c))
- …

As a set of propositional formulas, H(ψ) contains the formulas

- $P_1 \vee \neg P_2$
- $P_2 \vee \neg P_2$
- $P_3 \vee \neg P_2$
- …

- H(ψ) is satisfiable
  - The truth assignment s with $s(P_i) = 1$, for all i, satisfies H(ψ).
  - Also, any truth assignment with $s(P_2) = 0$ satisfies H(ψ)
- ψ is satisfiable.

Herbrand’s Theorem: Illustration

Example: Let ψ be the Π_1-sentence $\forall$ x(P(x) $\wedge$ $\neg$ P(f(c)).

The Herbrand expansion H(ψ) of ψ contains the sentence

- P(f(c)) $\wedge$ $\neg$ P(f(c))

or, equivalently, the propositional formula

- $P_2 \wedge \neg P_2$.

Therefore,

- H(ψ) is unsatisfiable
- ψ is unsatisfiable.

Herbrand's Theorem

Herbrand's Theorem:

Let ψ be a Π_1-sentence ψ without the equality symbol = and let H(ψ) be its Herbrand expansion. Then the following are equivalent:

- ψ is satisfiable
- H(ψ) is satisfiable (as a set of propositional formulas).

Corollary:

Let ψ be a Π_1-sentence ψ without the equality symbol = and let H(ψ) be its Herbrand expansion. Then the following are equivalent:

- ψ is unsatisfiable.
- H(ψ) is unsatisfiable (as a set of propositional formulas)
- There is a finite subset H_0 of H(ψ) that is unsatisfiable.

The Completeness Theorem for First-Order Logic

Theorem (Gödel's Completeness Theorem): The Validity Problem is semi-decidable. Equivalently, there is an algorithm that enumerates all valid FO-sentences.

Proof: We will give the proof for FO-sentences without equality =.

Let φ be a FO-sentence without =. We now have that:

- φ is valid

  if and only if
- $(\neg \varphi)$ is unsatisfiable

  if and only if (by Skolem's Theorem)
- $(\neg \varphi)^*$ is unsatisfiable

  if and only if (by Herbrand's Theorem)
- $H((\neg \varphi)^*)$ is unsatisfiable

  if and only if (by the Compactness Theorem for Prop. Logic)
- there is a finite subset H_0 of $H((\neg \varphi)^*)$ that is unsatisfiable.

The Completeness Theorem for First-Order Logic

Theorem (Gödel's Completeness Theorem): The Validity Problem is semi-decidable. Equivalently, there is an algorithm that enumerates all valid FO-sentences.

Proof (continued): So, the algorithm for the semi-decidability of valid FO-sentences without equality is as follows.

Given a FO-sentence φ without equality, do:

- Construct the Π_1 sentence $(\neg\, \varphi)^*$ (using Skolem's Theorem)
- Generate the Herbrand expansion $H((\neg\, \varphi)^*)$ of $(\neg\, \varphi)^*$, say,

  $$H((\neg\, \varphi)^*) = \{\psi_1, \psi_2, \ldots, \psi_n, \ldots\}$$
- While generating $H((\neg\, \varphi)^*)$, use the resolution algorithm to test each finite set $\{\psi_1, \psi_2, \ldots, \psi_n\}$, $n \geq 1$, for unsatisfiabiliy.
- If, for some n, the set $\{\psi_1, \psi_2, \ldots, \psi_n\}$ is found to be unsatisfiable, then stop and return "φ is valid".

The Completeness Theorem for First-Order Logic

Remarks:

- Here, we gave the proof for FO-sentences without equality =. The proof can be extended to arbitrary FO-sentences by forming structures that are obtained from Herbrand structures via taking the equivalence classes of terms according to the equalities between them in some structure satisfying the FO-sentence at hand.
- Here, we used the resolution procedure only for formulas of propositional logic. The resolution procedure can be extended to FO-formulas using unification of terms.
- There are other proofs of Gödel's Completeness Theorem in which one gives a proof system consisting of an explicit set of axioms and rules of inference for FO-formulas and then one shows that a FO-sentence is valid if and only if it can derived from this proof system.
- However, from an algorithmic viewpoint, all these approaches yield the same algorithmic result, namely, the Validity Problem is semi-decidadble, which means that *the set of valid FO-sentences is recursively enumerable.*

The Compactness Theorem for First-Order Logic

Theorem: Let Σ be a set of FO-sentences. Then the following statements are equivalent:

1. Σ is satisfiable.
2. Σ is finitely satisfiable, i.e., every finite subset of Σ is satisfiable.

Proof: The non-trivial direction is 2. ⇒ 1.
Assume that Σ is finitely satisfiable.
For every $\psi \in \Sigma$, let H(ψ*) be the Herbrand expansion of the Π_1-sentence ψ* given by Skolem's Theorem.
Let T be the union of all Herbrand expansions H(ψ*), for $\psi \in \Sigma$.
Since Σ is finitely satisfiable, it is easy to see that T is finitely satisfiable (as a set of formulas of propositional logic).
By the Compactness Theorem for propositional logic, T is satisfiable.
It follows that Σ is satisfiable.

The Compactness Theorem for First-Order Logic

Note:

The Compactness Theorem for first-order logic is one of the most useful tools in studying the expressive power of this logic. In particular, it can be used to show that none of the following properties is FO-expressible (see Lecture #13):

- The universe A of **A** is a finite set
- The graph **G** = (V,E) is connected
- The graph **G** = (V,E) is acyclic
- The graph **G** = (V,E) is k-colorable, for a fixed $k \geq 2$.
- The graph **G** = (V,E) is planar
- The graph **G** = (V,E) is Hamiltonian
- **P** = (A, ≤) is a well-ordered linear order
- The Least Upper Bound property of a linear order **P** = (A, ≤)

The Compactness Theorem for First-Order Logic

Theorem: There is no FO-sentence ψ such that for every structure **A**, we have that **A** $\models \psi$ if and only if the universe A of **A** is finite.

Proof: Towards a contradiction, assume that such a FO-sentence ψ exists.

Let σ_n be a FO-sentence asserting that "there are at least n distinct elements". Let $\Sigma = \{\psi\} \cup \{\sigma_n : n \geq 1\}$.

Then Σ is finitely satisfiable (why?). Hence, by the Compactness Theorem for first-order logic, Σ is satisfiable by some structure **A**.

We now have that

- The universe A of **A** is finite because **A** $\models \psi$.
- The universe A of **A** is infinite, because **A** $\models \sigma_n$, for every n.

The Compactness Theorem for First-Order Logic

Theorem: There is no FO-sentence ψ such that for every graph **G** = (V,E), we have that **G** $\models \psi$ if and only **G** is connected.

Proof: Towards a contradiction, assume that such a FO-sentence ψ exists. Let c, d be two constant symbols, and let σ_n be a FO-sentence asserting that "there is no path of length n from c to d".

Let $\Sigma = \{\psi\} \cup \{\sigma_n : n \geq 1\}$.

Then Σ is finitely satisfiable (why?). Hence, by the Compactness Theorem for first-order logic, Σ is satisfiable by some graph **G***.

Let c* and d* be the nodes of **G*** that interpret the constant symbols c and d, respectively. We now have that

- There is a path from c* to d* in **G***, since **G*** $\models \psi$.
- There is no path from c* to d* in **G***, since **G*** $\models \sigma_n$, for all $n \geq 1$.

The Compactness Theorem for First-Order Logic

Theorem: There is no FO-sentence ψ such that for every graph **G** = (V,E), we have that **G** $\models \psi$ if and only **G** contains a cycle.

Proof: Towards a contradiction, assume that such a FO-sentence ψ exists. Let σ_n be a FO-sentence asserting that "there is no cycle of length n".

Let Σ = $\{\psi\} \cup \{\sigma_n$: n $\geq$ 1$\}$.

Then Σ is finitely satisfiable (why?). Hence, by the Compactness Theorem for first-order logic, Σ is satisfiable by some graph **G***.

We now have that

- There is a cycle in **G***, since **G*** $\models \psi$.
- There is no cycle in **G***, since **G*** $\models \sigma_n$, for all n $\geq$ 1.

The Compactness Theorem for First-Order Logic

Theorem: There is no FO-sentence ψ such that for every structure **A** = (A, $\leq$), we have that **A** $\models \psi$ if and only **A** is a well-ordering.

Proof: Towards a contradiction, assume that such a FO-sentence ψ exists. Let c_1, c_2, …,c_n, … be an infinite sequence of constant symbols and let σ_n be a FO-sentence asserting that "$c_1 > c_2 > \ldots > c_n$".
Let $\Sigma = \{\psi\} \cup \{\sigma_n\colon n \geq 1\}$.
Then Σ is finitely satisfiable (why?). Hence, by the Compactness Theorem for first-order logic, Σ is satisfiable by some structure **A***.
Let c^*_1, c^*_2, …, c^*_n, … be the elements of A interpreting the constant symbols c_1, c_2, …, c_n, …
We now have that

- The set $\{c^*_1, c^*_2, \ldots, c^*_n, \ldots\}$ has a least element, since since **A*** $\models \psi$.
- The set $\{c^*_1, c^*_2, \ldots, c^*_n, \ldots\}$ has **no** least element, since **A*** $\models \sigma_n$, for all $n \geq 1$.

Compactness vs. Ehrenfeucht-Fraïssé Games

- Both the Compactness Theorem and Ehrenfeucht-Fraïssé Games can be used to analyze the expressive power of First-Order Logic.

- As a general rule, the Compactness Theorem is easier to use because one does not need to describe winning strategies for the Duplicator, which may be cumbersome.

- However, unless more sophisticated arguments are used, the Compactness Theorem typically proves that a property is not FO-expressible over all structures, but the proof does not yield that the property is not FO-expressible over all finite structures.

- In contrast, Ehrenfeucht-Fraïssé Games typically show that a property is not FO-expressible over all finite structures, which is a stronger result.

The Compactness Theorem

Fact:

- The Compactness Theorem for First-Order Logic **fails** if we restrict ourselves to finite structures.
- This means that there is a set Σ of FO-sentences such that
  - Every finite subset of Σ is satisfiable by a finite structure (hence, Σ is satisfiable by some structure).
  - No finite structure satisfies Σ.

Proof: Let Σ = {σ_n: n$\geq$ 1}, where σ_n is a FO-sentence asserting "there are at least n distinct elements.

The Compactness Theorem

Fact: The Compactness Theorem for Second-Order Logic **fails**.
Proof: Let ψ be a sentence of Second-Order Logic asserting that "the universe of the structure is finite" (this is expressed by saying that, for every unary function f, if f is one-to-one, then it is also onto").
Let $\Sigma = \{\psi\} \cup \{\sigma_n : n \geq 1\}$, where σ_n is a FO-sentence asserting "there are at least n distinct elements.
Then:

- Every finite subset of Σ is satisfiable (Why?)
- Σ is **not** satisfiable.

Conclusion:
The Compactness Theorem for a logic cannot be taken for granted.

Course Highlights: Propositional Logic

- Propositional Logic: Structural Properties
  - Relevance Theorem
  - Tautologies and satisfiable formulas
  - Conjunctive and Disjunctive Normal Forms
  - Complete sets of connectives, Post's Lattice
  - Compactness Theorem and its applications.

- Propositional Logic: Algorithms and Complexity
  - Sum-of-products algorithm
  - Resolution
  - Unit Resolution

Course Highlights: Propositional Logic

Satisfiability Problem	Computational Complexity
2SAT	NLOGSPACE-complete
Horn SAT	P-complete
SAT, 3SAT, 1-in-3-SAT, …	NP-complete
QBF	PSPACE-complete

Course Highlights: First-Order Logic

- First-Order Logic: Structural Properties and uses
  - Relevance Theorem
  - Valid sentences, Finitely valid sentences
  - Prenex Normal Form
  - Skolem's Theorem
  - First-order logic as a specification language
    - Definability on a fixed structure
    - Uniform definability on all structures or on a class of structures
    - First-order logic as a database query language
  - Ehrenfeucht-Fraïssé games and their applications.
  - Compactness Theorem and its applications

Course Highlights: First-Order Logic

- First-Order Logic: Algorithmic Properties
  - The set of valid sentences is semi-decidable, but its complement is not.
  - The set of finitely valid sentences is not semi-decidable, but its complement is semi-decidable.
  - Neither Th(**N**) nor its complement is semi-decidable.
  - Th(**R**) is decidable (in EXPSPACE; also, PSPACE-hard)
  - Th(**A**) is PSPACE-complete for every non-trivial finite structure **A**.

Moral: First-Order Logic is much more expressive than Propositional Logic, but this expressive power comes at a cost: Determining first-order "truth" is computationally much more difficult.