Lecture 10

Herbrand's theorem and ground resolution

Introduction to Logic for Computer Science

Prof Hongseok Yang
KAIST

These slides are minor variants of those made by Prof Worrell and Prof Haase for their logic course at Oxford.

Recap

Let F be a quantifier-free formula.

Prenex form: $Q_1 x_1\, Q_2 x_2\, \cdots Q_n x_n\, F$, where $Q_i \in \{\forall, \exists\}$.

Skolem form: $\forall x_1\, \forall x_2\, \cdots \forall x_n\, F$.

Every first-order formula can be translated into an equi-satisfiable formula in Skolem form in poly. time.

Ground terms

Definition

Given a signature σ, a **ground term** is a σ-term in which no variable symbol appears.

Ground terms

Definition

Given a signature σ, a **ground term** is a σ-term in which no variable symbol appears.

Example

Let $\sigma = \langle c, d,\ f, g,\ P, Q\rangle$ with unary f and binary g, the set of ground terms is

$$\{c, d, f(c), f(d), g(c, c), g(c, d), g(d, c), g(d, d), f(f(c)), f(f(d)), \ldots\}.$$

Ground terms

Definition

Given a signature σ, a **ground term** is a σ-term in which no variable symbol appears.

Example

Let $\sigma = \langle c, d,\ f, g,\ P, Q\rangle$ with unary f and binary g, the set of ground terms is

$$\{c, d, f(c), f(d), g(c, c), g(c, d), g(d, c), g(d, d), f(f(c)), f(f(d)), \ldots\}.$$

Ex: Find a signature σ such that its set of ground terms is isomorphic to $\mathbb{N}$.

Herbrand structures

Definition

Let σ be a signature with at least one constant symbol. A σ-structure $\mathcal{H}$ is a **Herbrand structure** if the following hold:

- The universe $U_{\mathcal{H}}$ is the set of ground terms over σ.
- For every constant symbol c, we have $c_{\mathcal{H}} = c$.
- For every function symbol f, $f_{\mathcal{H}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$.

Herbrand structures

Definition

Let σ be a signature with at least one constant symbol. A σ-structure $\mathcal{H}$ is a **Herbrand structure** if the following hold:

- The universe $U_{\mathcal{H}}$ is the set of ground terms over σ.
- For every constant symbol c, we have $c_{\mathcal{H}} = c$.
- For every function symbol f, $f_{\mathcal{H}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$.

Proposition: For any Herbrand structure $\mathcal{H}$ and ground term t, $\mathcal{H}(t) = t$.

Herbrand structures

Definition

Let σ be a signature with at least one constant symbol. A σ-structure $\mathcal{H}$ is a **Herbrand structure** if the following hold:

- The universe $U_{\mathcal{H}}$ is the set of ground terms over σ.
- For every constant symbol c, we have $c_{\mathcal{H}} = c$.
- For every function symbol f, $f_{\mathcal{H}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$.

Proposition: For any Herbrand structure $\mathcal{H}$ and ground term t, $\mathcal{H}(t) = t$.

Ex1: Prove the proposition.

Herbrand structures

Definition

Let σ be a signature with at least one constant symbol. A σ-structure $\mathcal{H}$ is a **Herbrand structure** if the following hold:

- The universe $U_{\mathcal{H}}$ is the set of ground terms over σ.
- For every constant symbol c, we have $c_{\mathcal{H}} = c$.
- For every function symbol f, $f_{\mathcal{H}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$.

Proposition: For any Herbrand structure $\mathcal{H}$ and ground term t, $\mathcal{H}(t) = t$.

Ex1: Prove the proposition.

Translation Lemma: For all ground t, $\mathcal{H} \models F[t/x]$ iff $\mathcal{H}_{[x \mapsto t]} \models F$.

Herbrand structures

Definition

Let σ be a signature with at least one constant symbol. A σ-structure $\mathcal{H}$ is a **Herbrand structure** if the following hold:

- The universe $U_{\mathcal{H}}$ is the set of ground terms over σ.
- For every constant symbol c, we have $c_{\mathcal{H}} = c$.
- For every function symbol f, $f_{\mathcal{H}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$.

Proposition: For any Herbrand structure $\mathcal{H}$ and ground term t, $\mathcal{H}(t) = t$.

Ex1: Prove the proposition.

Translation Lemma: For all ground t, $\mathcal{H} \models F[t/x]$ iff $\mathcal{H}_{[x \mapsto t]} \models F$.

Ex2: Prove the lemma.

Jaques Herbrand (1908 – 1931)

Herbrand's theorem

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Herbrand's theorem

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Ex: Prove the theorem.

Herbrand's theorem

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Ex: Prove the theorem.

Hint1: It is sufficient to consider closed F only.

Herbrand's theorem

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Ex: Prove the theorem.

Hint1: It is sufficient to consider closed F only.

Hint2: The proof of the only-if direction goes like this.

Suppose $\mathcal{A} \models F$.

Herbrand's theorem

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Ex: Prove the theorem.

Hint1: It is sufficient to consider closed F only.

Hint2: The proof of the only-if direction goes like this.

Suppose $\mathcal{A} \models F$. Define a Herbrand model $\mathcal{H}$ by setting the interpretation of each predicate symbol P as follows:

$$(t_1, \ldots, t_k) \in P_{\mathcal{H}} \text{ iff } \mathcal{A} \models P(t_1, \ldots, t_k).$$

Herbrand's theorem

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Ex: Prove the theorem.

Hint1: It is sufficient to consider closed F only.

Hint2: The proof of the only-if direction goes like this.

Suppose $\mathcal{A} \models F$. Define a Herbrand model $\mathcal{H}$ by setting the interpretation of each predicate symbol P as follows:

$$(t_1, \ldots, t_k) \in P_{\mathcal{H}} \text{ iff } \mathcal{A} \models P(t_1, \ldots, t_k).$$

Now show that for all closed G in Skolem form, if $\mathcal{A} \models G$, then $\mathcal{H} \models G$. Use induction on the number of $\forall$ in G.

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Proof.

Assume that F is closed. Suppose $\mathcal{A} \models F$.

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ *be a formula in Skolem form. Then,* F *is satisfiable if and only if* F *has a Herbrand model.*

Proof.

Assume that F is closed. Suppose $\mathcal{A} \models F$.

Define $P_{\mathcal{H}}$ for each predicate symbol P:

$$(t_1, \ldots, t_k) \in P_{\mathcal{H}} \text{ iff } \mathcal{A} \models P(t_1, \ldots, t_k).$$

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Proof.

Assume that F is closed. Suppose $\mathcal{A} \models F$.

Define $P_{\mathcal{H}}$ for each predicate symbol P:

$$(t_1, \ldots, t_k) \in P_{\mathcal{H}} \text{ iff } \mathcal{A} \models P(t_1, \ldots, t_k).$$

We show that for all *closed* $G = \forall x_1 \forall x_2 \ldots \forall x_m G^*$ with quantifier free G^*, if $\mathcal{A} \models G$, then $\mathcal{H} \models G$. We use induction on m.

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Proof.

Assume that F is closed. Suppose $\mathcal{A} \models F$.

Define $P_{\mathcal{H}}$ for each predicate symbol P:

$$(t_1, \ldots, t_k) \in P_{\mathcal{H}} \text{ iff } \mathcal{A} \models P(t_1, \ldots, t_k).$$

We show that for all *closed* $G = \forall x_1 \forall x_2 \ldots \forall x_m G^*$ with quantifier free G^*, if $\mathcal{A} \models G$, then $\mathcal{H} \models G$. We use induction on m.

For $m = 0$, G is closed. Thus, it is a Boolean combination of $P(t_1, \ldots, t_k)$. By definition, $\mathcal{H} \models G$.

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Proof.

Assume that F is closed. Suppose $\mathcal{A} \models F$.

Define $P_{\mathcal{H}}$ for each predicate symbol P:

$$(t_1, \ldots, t_k) \in P_{\mathcal{H}} \text{ iff } \mathcal{A} \models P(t_1, \ldots, t_k).$$

We show that for all *closed* $G = \forall x_1 \, \forall x_2 \, \ldots \forall x_m \, G^*$ with quantifier free G^*, if $\mathcal{A} \models G$, then $\mathcal{H} \models G$. We use induction on m.

For $m = 0$, G is closed. Thus, it is a Boolean combination of $P(t_1, \ldots, t_k)$. By definition, $\mathcal{H} \models G$.

For $m > 0$, suppose $\mathcal{A} \models \forall x \, G'$. Note that x may appear free in G'.

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Proof.

Assume that F is closed. Suppose $\mathcal{A} \models F$.

Define $P_{\mathcal{H}}$ for each predicate symbol P:

$$(t_1, \ldots, t_k) \in P_{\mathcal{H}} \text{ iff } \mathcal{A} \models P(t_1, \ldots, t_k).$$

We show that for all *closed* $G = \forall x_1 \forall x_2 \ldots \forall x_m G^*$ with quantifier free G^*, if $\mathcal{A} \models G$, then $\mathcal{H} \models G$. We use induction on m.

For $m = 0$, G is closed. Thus, it is a Boolean combination of $P(t_1, \ldots, t_k)$. By definition, $\mathcal{H} \models G$.

For $m > 0$, suppose $\mathcal{A} \models \forall x\, G'$. Note that x may appear free in G'.

Translation Lemma gives $\mathcal{A} \models G'[t/x]$ iff $\mathcal{A}_{[x \mapsto \mathcal{A}(t)]} \models G'$ for all ground terms t.

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Proof.

Assume that F is closed. Suppose $\mathcal{A} \models F$.

Define $P_{\mathcal{H}}$ for each predicate symbol P:

$$(t_1, \ldots, t_k) \in P_{\mathcal{H}} \text{ iff } \mathcal{A} \models P(t_1, \ldots, t_k).$$

We show that for all *closed* $G = \forall x_1 \forall x_2 \ldots \forall x_m G^*$ with quantifier free G^*, if $\mathcal{A} \models G$, then $\mathcal{H} \models G$. We use induction on m.

For $m = 0$, G is closed. Thus, it is a Boolean combination of $P(t_1, \ldots, t_k)$. By definition, $\mathcal{H} \models G$.

For $m > 0$, suppose $\mathcal{A} \models \forall x\, G'$. Note that x may appear free in G'.

Translation Lemma gives $\mathcal{A} \models G'[t/x]$ iff $\mathcal{A}_{[x \mapsto \mathcal{A}(t)]} \models G'$ for all ground terms t. So, $\mathcal{H} \models G'[t/x]$ for all ground t by the ind. hypothesis.

Theorem

Let $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$ be a formula in Skolem form. Then, F is satisfiable if and only if F has a Herbrand model.

Proof.

Assume that F is closed. Suppose $\mathcal{A} \models F$.

Define $P_{\mathcal{H}}$ for each predicate symbol P:

$$(t_1, \ldots, t_k) \in P_{\mathcal{H}} \text{ iff } \mathcal{A} \models P(t_1, \ldots, t_k).$$

We show that for all *closed* $G = \forall x_1 \, \forall x_2 \, \ldots \forall x_m \, G^*$ with quantifier free G^*, if $\mathcal{A} \models G$, then $\mathcal{H} \models G$. We use induction on m.

For $m = 0$, G is closed. Thus, it is a Boolean combination of $P(t_1, \ldots, t_k)$. By definition, $\mathcal{H} \models G$.

For $m > 0$, suppose $\mathcal{A} \models \forall x \, G'$. Note that x may appear free in G'.

Translation Lemma gives $\mathcal{A} \models G'[t/x]$ iff $\mathcal{A}_{[x \mapsto \mathcal{A}(t)]} \models G'$ for all ground terms t. So, $\mathcal{H} \models G'[t/x]$ for all ground t by the ind. hypothesis.

But then $\mathcal{H} \models \forall x \, G'$. $\square$

Ground resolution

Herbrand expansion of $F = \forall x_1 \forall x_2 \dots \forall x_n F^*$:

$$E(F) := \{F^*[t_1/x_1][t_2/x_2] \dots [t_n/x_n] : t_1, \dots, t_n \text{ ground terms}\}.$$

Ground resolution

Herbrand expansion of $F = \forall x_1 \forall x_2 \dots \forall x_n F^*$:

$$E(F) := \{F^*[t_1/x_1][t_2/x_2]\dots[t_n/x_n] : t_1, \dots, t_n \text{ ground terms}\}.$$

Theorem (Ground Resolution)

A closed formula F in Skolem form is unsatisfiable if and only if there is a propositional resolution proof of $\square$ from $E(F)$.

Ground resolution

Herbrand expansion of $F = \forall x_1 \forall x_2 \dots \forall x_n F^*$:

$$E(F) := \{F^*[t_1/x_1][t_2/x_2]\dots[t_n/x_n] : t_1, \dots, t_n \text{ ground terms}\}.$$

Theorem (Ground Resolution)

A closed formula F in Skolem form is unsatisfiable if and only if there is a propositional resolution proof of $\square$ from $E(F)$.

Ex1: What does this imply in terms of developing a validity checker for first-order formulas?

Ground resolution

Herbrand expansion of $F = \forall x_1 \forall x_2 \ldots \forall x_n F^*$:

$$E(F) := \{F^*[t_1/x_1][t_2/x_2]\ldots[t_n/x_n] : t_1, \ldots, t_n \text{ ground terms}\}.$$

Theorem (Ground Resolution)

A closed formula F in Skolem form is unsatisfiable if and only if there is a propositional resolution proof of $\Box$ from $E(F)$.

Ex1: What does this imply in terms of developing a validity checker for first-order formulas?

Ex2: Prove the theorem.

Hint: Prove that Herbrand' theorem implies the following theorem. Then, use the Compactness theorem for propositional logic.

Theorem

A closed formula F in Skolem form is satisfiable iff $E(F)$ is satisfiable when considered as a set of propositional formulas.

Theorem

A closed formula F in Skolem form is satisfiable iff $E(F)$ is satisfiable when considered as a set of propositional formulas.

Proof.

By Herbrand's theorem, F is satisfiable if and only if F has a Herbrand model. Now

$$\begin{aligned}
\mathcal{H} \models F \text{ iff } & \mathcal{H}_{[x_1 \mapsto t_1]\cdots[x_n \mapsto t_n]} \models F^* \text{ for all ground terms } t_1, \ldots, t_n \\
\text{iff } & \mathcal{H} \models F^*[t_1/x_1] \ldots [t_n/x_n] \text{ for all ground } t_i \text{ (by Trans. Lemma)} \\
\text{iff } & \mathcal{H} \models E(F) \\
\text{iff } & E(F) \text{ as a set of prop. formulas is satisfied by } \mathcal{H}.
\end{aligned}$$

In the last line, we view $\mathcal{H}$ as an assignment to prop. variables of the form $P(t_1, \ldots, t_k)$. $\square$

Theorem (Ground Resolution)

A closed formula F in Skolem form is unsatisfiable if and only if there is a propositional resolution proof of $\Box$ from $E(F)$.

Proof.

By the Compactness theorem, $E(F)$ is unsatisfiable if and only if some finite subset of $E(F)$ is unsatisfiable. The latter happens if and only if $\Box$ can be derived from $E(F)$ using resolution. $\Box$