Lecture 11
Applications of Herbrand's theorem
Ground resolution proofs, semi-decidability of validity

Print version of the lecture in *Introduction to Logic for Computer Science*

presented by Prof Hongseok Yang

These lecture notes are very minor variants of the ones made by Prof James Worrell and Prof Christoph Haase for their 'Logic and Proof' course at Oxford.

In this lecture, we show how to use the Ground Resolution Theorem, which is a consequence of Herbrand's theorem and was proved in the last lecture, to do some deduction in first-order logic. Moreover, we show that Herbrand's theorem allows us to conclude semi-decidability of validity of first-order logic. Finally, we show that validity and satisfiability are undecidable.

1 Ground Resolution Theorem

Recall that the process of eliminating existential quantifiers by introducing extra function and constant symbols is called *Skolemisation*. The extra symbols introduced are called *Skolem functions*. We begin with a slight generalisation of a theorem that was stated in the previous lecture. In this generalisation, we consider Skolemising a collection of formulas rather than a single formula.

Theorem 1. *Let $F_1, \ldots, F_n$ be closed rectified formulas in prenex form with respective Skolem forms $G_1, \ldots, G_n$. Assume that each G_i is constructed using a different set of Skolem functions. Then, $F_1 \wedge F_2 \wedge \ldots \wedge F_n$ is satisfiable if and only if $G_1 \wedge G_2 \wedge \ldots \wedge G_n$ is satisfiable.*

Recall that a ground term is a term that does not contain any variables. Given a quantifier-free formula F, a *ground instance* of F is a formula obtained by replacing all the variables in F with ground terms.

The following is a slight generalisation of the version of the Ground Resolution Theorem proved in the last lecture. Before we considered only a single formula in Skolem form. Here we consider a conjunction of such formulas, which is more convenient for the applications below.

Theorem 2 (Ground Resolution Theorem)**.** *Let $F_1, \ldots, F_n$ be closed formulas in Skolem form whose respective matrices $F_1^*, \ldots, F_n^*$ are in **CNF**. Then, $F_1 \wedge \ldots \wedge F_n$ is unsatisfiable if and only if there is a propositional resolution proof of $\square$ from the set of ground instances of clauses from $F_1^*, \ldots, F_n^*$.*

2 Examples

In this section, we give two examples of the use of the Ground Resolution Theorem.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\{\neg R(a), L(a)\} \quad \{\neg O(a), L(a), R(a), D(a)\}}{\{L(a), \neg O(a), D(a)\}} \quad \{\neg O(a), \neg L(a)\}}{\{\neg O(a), D(a)\}} \quad \{\neg D(a)\}}{\{\neg O(a)\}} \quad \{O(a)\}}{\square}$$

Figure 1: The nature of Oriel students

Example 3. We would like to formalise the following statements in first-order logic and to use ground resolution to show that (a), (b) and (c) together entail (d).

(a) Everyone at Oriel[1] is lazy, a rower or a drunk.
(b) All rowers are lazy.
(c) Someone at Oriel is not drunk.
(d) Someone at Oriel is lazy.

We translate (a), (b), (c) and the negation of (d) into closed formulas of first-order logic as follows.

$$\begin{aligned} F_1 &= \forall x\,(O(x) \to (L(x) \vee R(x) \vee D(x))) \\ F_2 &= \forall x\,(R(x) \to L(x)) \\ F_3 &= \exists x\,(O(x) \wedge \neg D(x)) \\ F_4 &= \neg\exists x\,(O(x) \wedge L(x)). \end{aligned}$$

Next we translate F_1, F_2, F_3 and F_4 to Skolem form. To do this, we bring all quantifiers to the outside, eliminate existential quantifiers by introducing Skolem functions, and finally bring the matrix of each formula into **CNF**. This yields

$$\begin{aligned} G_1 &= \forall x\,(\neg O(x) \vee L(x) \vee R(x) \vee D(x)) \\ G_2 &= \forall x\,(\neg R(x) \vee L(x)) \\ G_3 &= O(a) \wedge \neg D(a) \\ G_4 &= \forall x\,(\neg O(x) \vee \neg L(x)) \end{aligned}$$

where a is a fresh constant symbol.

Now we deduce the empty clause $\square$ from ground instances of clauses in the respective matrices of the Skolem-form formulas $G_1, \ldots, G_4$. Note that these formulas are defined over a signature with a single constant symbol a, which is therefore the only ground term. The proof is shown in Figure 1.

Example 4. Using ground resolution, we show that

$$F = \forall x\,\exists y\,(P(x) \to Q(y)) \to \exists y\,\forall x\,(P(x) \to Q(y))$$

is a valid sentence.

We can show this by showing that the negation is unsatisfiable. The negation can be written:

$$\forall x\,\exists y\,(P(x) \to Q(y)) \wedge \neg\exists y\,\forall x\,(P(x) \to Q(y)).$$

We bring each conjunction to Skolem form, yielding

$$\begin{aligned} F_1 &= \forall x\,(\neg P(x) \vee Q(f(x))) \\ F_2 &= \forall y\,(P(g(y)) \wedge \neg Q(y)). \end{aligned}$$

Note that F_1 and F_2 are defined over a signature with no constants and so there are no ground terms. We remedy this problem by introducing a single new constant symbol a. Now the set of ground terms is $\{a, f(a), g(a), f(f(a)), f(g(a)), \ldots\}$.

$$\dfrac{\dfrac{\{P(g(a))\} \qquad \{\neg P(g(a)), Q(f(g(a)))\}}{\{Q(f(g(a)))\}} \qquad \{\neg Q(f(g(a)))\}}{\square}$$

Figure 2: Ground Resolution proof for Example 4

We can now derive $\square$ by the propositional resolution proof in Figure 2 where every leaf is a ground instance of a clause from the respective matrices of F_1 and F_2.

Remark 5. Alternatively, it is of course also possible to show that F in Example 4 is valid via an application of the semantic definitions given for first-order logic. In particular, we have the following equivalence that transforms F into a rectified formula:

$$\begin{aligned}
F &= \forall x\, \exists y\, (P(x) \to Q(y)) \to \exists y\, \forall x\, (P(x) \to Q(y)) \\
&\equiv \neg(\forall x\, \exists y\, (P(x) \to Q(y))) \vee \exists y\, \forall x\, (\neg P(x) \vee Q(y)) \\
&\equiv \exists x\, \forall y\, \neg(\neg P(x) \vee Q(y)) \vee \exists y\, \forall x\, (\neg P(x) \vee Q(y)) \\
&\equiv \exists x\, \forall y\, (P(x) \wedge \neg Q(y)) \vee \exists y\, \forall x\, (\neg P(x) \vee Q(y)) \\
&\equiv \exists x\, \forall y\, (P(x) \wedge \neg Q(y)) \vee \exists u\, \forall v\, (\neg P(v) \vee Q(u)) \\
&\equiv \exists x\, \forall y\, (P(x) \wedge \neg Q(y)) \vee (\forall v\, \neg P(v)) \vee (\exists u\, Q(u)) \\
&\equiv ((\exists x\, P(x)) \wedge (\forall y\, \neg Q(y))) \vee (\forall v\, \neg P(v)) \vee (\exists u\, Q(u)).
\end{aligned}$$

Suppose $\mathcal{A}$ is an arbitrary σ-structure, we claim that $\mathcal{A} \models F$. To this end, we make a case distinction:

- Case $P_{\mathcal{A}} = \emptyset$: Then, $\mathcal{A} \models \forall v\, \neg P(v)$, and consequently $\mathcal{A} \models F$
- Case $Q_{\mathcal{A}} \neq \emptyset$: Then, $\mathcal{A} \models \exists u\, Q(u)$, and consequently $\mathcal{A} \models F$
- Case $P_{\mathcal{A}} \neq \emptyset$ and $Q_{\mathcal{A}} = \emptyset$: Then, $((\exists x\, P(x)) \wedge (\forall y\, \neg Q(y)))$, and consequently $\mathcal{A} \models F$.

At least one of those three cases will match for any σ-structure, and thus $\mathcal{A} \models F$ for all σ-structures $\mathcal{A}$, and thus F is indeed valid.

Example 6. Consider the following closed formulas, defined over a signature with constant symbol 0, unary function symbol s, and ternary relation Sum. Here $s^n(0)$ stands for the term $\underbrace{s(\ldots s(0)\ldots)}_{n}$.

$$\begin{aligned}
F_1 &= \forall x\, Sum(0, x, x) \\
F_2 &= \forall x\, \forall y\, \forall z\, (Sum(x, y, z) \to Sum(s(x), y, s(z))) \\
F_3 &= \exists x\, Sum(s^2(0), s^2(0), x)
\end{aligned}$$

We use ground resolution to show that $F_1, F_2 \models F_3$. To do this we show that $F_1 \wedge F_2 \wedge \neg F_3$ is unsatisfiable. The Skolem forms of F_1, F_2 and $\neg F_3$ are as follows:

$$\begin{aligned}
G_1 &= \forall x\, Sum(0, x, x) \\
G_2 &= \forall x\, \forall y\, \forall z\, (Sum(x, y, z) \to Sum(s(x), y, s(z))) \\
G_3 &= \forall x\, \neg Sum(s^2(0), s^2(0), x).
\end{aligned}$$

We can produce a *linear* resolution proof in this case, i.e., a proof in which the result of each step is a resolvent in the next step.

[1] Oriel is one of the oldest Oxford colleges. Oxford colleges are a bit like the four houses at the Harry Potter movie.

3 Semi-Decidability of Validity

The approach taken in the previous examples can be generalised in order to yield a semi-decision procedure for validity for first-order logic.

Theorem 7. *Validity of first-order formulas is semi-decidable.*

Proof. Recall that a semi-decision procedure for validity should halt and return "valid" when given a valid formula as input, but otherwise may compute forever. Such a procedure is as follows. (Note that there is no loss of generality in restricting to closed formulas since F is valid iff $\forall x F$ is valid.)

Semi-Decision Procedure for Validity
Input: Closed formula F
Output: Either that F is valid or compute forever
Compute a Skolem-form formula G equisatisfiable with $\neg F$
Let $G_1, G_2, \ldots$ be an enumeration of the Herbrand expansion $E(G)$
for $n = 1$ to ∞ **do**
begin
  if $\square \in \mathrm{Res}^*(G_1 \cup \ldots \cup G_n)$ **then** stop and output "F is valid"
end

The procedure relies on the fact that F is valid if and only if $\neg F$ is unsatisfiable. To show unsatisfiability of $\neg F$ we transform it into an equisatisfiable formula G in Skolem form. Then, by the refutation completeness of ground resolution, G is unsatisfiable iff there is a ground resolution refutation of G. If such a refutation exists it will eventually be discovered by the procedure. Note that for each n the set of clauses $\mathrm{Res}^*(G_1 \cup \ldots \cup G_n)$ that can be derived by resolution from $G_1 \cup \ldots \cup G_n$ is computable in a finite amount of time. (Here we regard each G_i as a set of clauses.) $\square$

In the above proof it was convenient to invoke the refutation completeness of ground resolution. However ultimately the result relies on Herbrand's Theorem and the Compactness Theorem for propositional logic, which together guarantee that F is valid if and only if some finite subset of $E(G)$ is unsatisfiable.

4 Undecidability of Validity and Satisfiability

We now show that both validity and satisfiability are undecidable. In particular, satisfiability is not semi-decidable. Intuitively, there need not be finite witness that a given formula is satisfiable. There are even satisfiable formulas that have no finite models! This is in contrast to propositional logic, where satisfiability was decidable.

In this section, we recall the definition of *Post's Correspondence Problem* (PCP), and show how to transform a given instance of this problem into a first-order formula such that the instance has a solution if and only if the formula is valid. PCP is one of the most well-known undecidable problems. Thus, it follows that the validity problem for first-order logic is undecidable.

An instance of Post's correspondence problem consists of a finite set of tiles. Each tile has a bit-string on the top and a bit-string on the bottom. For example, we could have tiles

$$\left\{ \begin{bmatrix} 1 \\ 101 \end{bmatrix}, \begin{bmatrix} 10 \\ 00 \end{bmatrix}, \begin{bmatrix} 011 \\ 11 \end{bmatrix} \right\}.$$

A solution to the problem is a sequence of tiles, allowing the same tile multiple times, such that the top string equals the bottom string. In the above example a

solution is

$$\left[\begin{array}{c} 1 \\ 101 \end{array}\right]\left[\begin{array}{c} 011 \\ 11 \end{array}\right]\left[\begin{array}{c} 10 \\ 00 \end{array}\right]\left[\begin{array}{c} 011 \\ 11 \end{array}\right],$$

because both the top and the bottom strings are 101110011.

In general, an instance of Post's correspondence problem is a finite set of pairs of bit-strings $\mathbf{P} = \{(x_1, y_1), \ldots, (x_k, y_k)\}$, where $x_i, y_i \in \{0,1\}^*$. A solution of $\mathbf{P}$ is a sequence $i_1, i_2, \ldots, i_n$ such that $x_{i_1} x_{i_2} \ldots x_{i_n} = y_{i_1} y_{i_2} \ldots y_{i_n}$. In the above example one solution is the sequence $1, 3, 2, 3$. Clearly for each particular PCP instance, the set of *potential solutions*, i.e., sequences of tiles is infinite. Thus solving an instance of PCP involves searching an infinite set.

We encode this problem in first-order logic using a signature with constant symbol e, two unary function symbols f_0, f_1 and a binary relation symbol P. The ground terms over this signature can be considered as bit-strings, e.g., the term $f_1(f_1(f_0(e)))$ represents the bit-string 110. In general, for a bit-string $b_1 \ldots b_t \in \{0,1\}^*$ we denote the term $f_{b_1}(\ldots(f_{b_t}(x))\ldots)$ by $f_{b_1 \ldots b_k}(x)$.

Our goal is to transform a given instance $\mathbf{P}$ of Post's correspondence problem into a closed formula F such that $\mathbf{P}$ has a solution if and only if F is valid. We first give the idea of the construction in the above example. Consider the following three formulas:

$$\begin{aligned} F_1 &= P(f_1(e), f_{101}(e)) \wedge P(f_{10}(e), f_{00}(e)) \wedge P(f_{011}(e), f_{11}(e)) \\ F_2 &= \forall u \forall v\, (P(u,v) \rightarrow P(f_1(u), f_{101}(v)) \wedge P(f_{10}(u), f_{00}(v)) \wedge P(f_{011}(u), f_{11}(v))) \\ F_3 &= \exists u\, P(u,u). \end{aligned}$$

We claim that $F_1 \wedge F_2 \rightarrow F_3$ is valid if and only if the PCP instance has a solution. Given a general instance $\mathbf{P} = \{(x_1, y_1), \ldots, (x_k, y_k)\}$ of PCP we have the formulas

$$\begin{aligned} F_1 &= \bigwedge_{i=1}^{k} P(f_{x_i}(e), f_{y_i}(e)) \\ F_2 &= \forall u \forall v \bigwedge_{i=1}^{k} (P(u,v) \rightarrow P(f_{x_i}(u), f_{y_i}(v))) \\ F_3 &= \exists u\, P(u,u). \end{aligned}$$

Proposition 8. $\mathbf{P}$ has a solution if and only if $F_1 \wedge F_2 \rightarrow F_3$ is valid.

Sketch. Suppose that $F_1 \wedge F_2 \rightarrow F_3$ is valid. Consider the Herbrand structure $\mathcal{H}$ for which

$$P_{\mathcal{H}} = \{(f_u(e), f_v(e)) : \exists i_1 \ldots \exists i_t.\, u = x_{i_1} \ldots x_{i_t} \text{ and } v = y_{i_1} \ldots y_{i_t}\}.$$

Clearly $\mathcal{H}$ satisfies $F_1 \wedge F_2$. Thus it must hold that $\mathcal{H}$ satisfies F_3. But this means that $\mathbf{P}$ has a solution.

Conversely suppose that $\mathbf{P}$ has a solution. We show that $F_1 \wedge F_2 \rightarrow F_3$ is valid. To this end, consider a structure $\mathcal{A}$ that satisfies $F_1 \wedge F_2$. Then, we can show by induction on t that for any sequence of tiles $i_1 \ldots i_t$, $\mathcal{A} \models P(f_u(e), f_v(e))$, where $u = x_{i_1} \ldots x_{i_t}$ and $v = y_{i_1} \ldots y_{i_t}$. But since $\mathbf{P}$ has a solution, $\mathcal{A} \models P(f_u(e), f_u(e))$ for some string u. Thus $\mathcal{A} \models F_3$. □

Theorem 9 (Church's Theorem (1936))**.** *The satisfiability and validity problems for first-order logic are undecidable.*

Proof. Undecidability of validity follows from undecidability of Post's Correspondence Problem (which may be shown in the *Computability Theory* course). Furthermore, since F is valid if and only if $\neg F$ is unsatisfiable, undecidability of satisfiability is immediate from undecidability of validity. □

It follows from semi-decidability of validity and Theorem 9 that satisfiability is not even semi-decidable. Indeed if satisfiability were semi-decidable then we could decide validity as follows. Given a formula F, either F is valid or $\neg F$ is satisfiable. Thus we could decide validity of F by simultaneously running a semi-decision procedure for validity on F and a semi-decision procedure for satisfiability on $\neg F$.

Corollary 10. *Satisfiability of first-order formulas is not semi-decidable.*