Logic Homework #1, 2020

Nelson-Oppen Combination

L3 Informatique, ENS Paris-Saclay
baelde@lsv.fr

Due by March 2, 2020

The satisfiability problem for first-order logic tends to be undecidable, even for simple languages. However, many interesting theories become decidable when restricting to quantifier-free formulas. For example, if one takes the equality theory $\mathrm{Eq}_{\Sigma,\mathcal{P}}$ over the language given by Σ and $\mathcal{P}$, the entailment problem $\mathrm{Eq}_{\Sigma,\mathcal{P}}, \models \phi$ is undecidable if the input ϕ is an arbitrary formula, but decidable if one restricts to quantifier-free inputs.

The quantifier-free case is also decidable for linear arithmetic, arrays, lists, etc. which are useful e.g. in software verification. But, given two decidable theories, it is not always the case that their combination remains decidable. Even when it is, obtaining a decision procedure for the combined theory from the individual decision procedures is not obvious. Hence the need for techniques for combining theories. Such techniques have been extensively researched and are a key to the construction of *SMT solvers* (Satisfiability Modulo Theories), which are very successful in all sorts of logic-based automated tasks, including software verification.

In this assignment you will discover the Nelson-Oppen combination technique (first part) and see a case where two decidable theories combine to an undecidable one (second part). These two parts can be tackled in any order.

In what follows, all theories are assumed to implicitly contain the theory of equality. This allows us to restrict our attention to structures where **the equality predicate is interpreted as equality over the structure's domain**. We will in fact only consider such structures, and we will describe a language $\Sigma, \mathcal{P}$ without giving equality as part of $\mathcal{P}$; we assume instead that is it part of the basic syntax of formulas.

We say that two languages $\Sigma_1, \mathcal{P}_1$ and $\Sigma_2, \mathcal{P}_2$ are **disjoint** when $\Sigma_1 \cap \Sigma_2 = \emptyset$ and $\mathcal{P}_1 \cap \mathcal{P}_2 = \emptyset$. In other words, the formulas over $\Sigma_1, \mathcal{P}_1$ and those over $\Sigma_2, \mathcal{P}_2$ do not share any function symbol and only share one predicate symbol: equality.

Recall that $\mathrm{fv}(\phi)$ is the set of all variables occuring free in ϕ, and that $D_{\mathcal{S}}$ is the domain of a structure $\mathcal{S}$. A **theory** is an arbitrary set of closed formulas, i.e.

formulas ϕ such that $\mathrm{fv}(\phi) = \emptyset$. When T is a theory, we say that a structure is a T-**interpretation** when it is a model of T (it satisfies all formulas of T). We say that a closed formula is T-**satisfiable** when it is satisfied by a T-interpretation. When a formula ϕ has free variables, we say that it is satisfied when there exists a structure $\mathcal{S}$ and σ such that $\mathcal{S}, \sigma \models \phi$. This extends naturally to the notion of T-satisfaction, and to satisfaction for sets of formulas.

1 Combining decidable theories

1.1 Preliminaries

When $\mathcal{S}$ and $\mathcal{S}'$ are $(\Sigma, \mathcal{P})$-structures, a $(\Sigma, \mathcal{P})$-isomorphism from $\mathcal{S}$ to $\mathcal{S}'$ is a bijective mapping $h : D_{\mathcal{S}} \to D_{\mathcal{S}'}$ such that:

- for any function symbol $f \in \Sigma$ of arity k, for any $(e_1, \ldots, e_k) \in D_{\mathcal{S}}$,

$$h(f_{\mathcal{S}}(e_1, \ldots, e_k)) = f_{\mathcal{S}'}(h(e_1), \ldots, h(e_k))$$

- for any predicate symbol $P \in \Sigma$ of arity k, for any $(e_1, \ldots, e_k) \in D_{\mathcal{S}}$,

$$(e_1, \ldots, e_k) \in P_{\mathcal{S}} \text{ iff } (h(e_1), \ldots, h(e_k)) \in P_{\mathcal{S}'}$$

Question 1
Let h be a $(\Sigma, \mathcal{P})$-isomorphism from $\mathcal{S}$ to $\mathcal{S}'$. Let $\sigma : \mathcal{X} \to D_{\mathcal{S}}$ and $\sigma' : \mathcal{X} \to D_{\mathcal{S}'}$ be two semantics assignments such that $\sigma'(x) = h(\sigma(x))$ for all variables $x \in \mathcal{X}$. Show that $\mathcal{S}, \sigma \models \phi$ iff $\mathcal{S}', \sigma' \models \phi$.

For this first question we expect you to include all formal details to your solution. Note, however, that you can consider wlog. only formulas built from atomic formulas and $\bot$ using only universal quantification and implication (why?).

For the rest of the section, we fix two theories T_1 and T_2 over disjoint languages $\Sigma_1, \mathcal{P}_1$ and $\Sigma_2, \mathcal{P}_2$.

Question 2
For each $i \in \{1, 2\}$, let E_i be a set of $(\Sigma_i, \mathcal{P}_i)$-formulas, possibly featuring quantifiers and free variables. Show that (1) and (2) are equivalent:

(1) There exists $\mathcal{S}$ and σ such that $\mathcal{S}, \sigma \models E_1 \cup E_2$.

(2) There exists $\mathcal{S}_1$ and $\mathcal{S}_2$ with the same domain, and σ such that $\mathcal{S}_1, \sigma \models E_1$ and $\mathcal{S}_2, \sigma \models E_2$.

Question 3
Show that condition (2) above is equivalent to the next one:

(3) There exists $\mathcal{S}_1$, $\mathcal{S}_2$, σ_1, σ_2 such that:

(a) $\mathcal{S}_1, \sigma_1 \models E_1$ and $\mathcal{S}_2, \sigma_2 \models E_2$,

(b) $D_{\mathcal{S}_1}$ and $D_{\mathcal{S}_2}$ have the same cardinality,

(c) $\sigma_1(x) = \sigma_1(y)$ iff $\sigma_2(x) = \sigma_2(y)$ for all $x, y \in \mathcal{X}$.

1.2 Separated forms

Question 4
Let Γ be a conjunction of litterals over the language $\Sigma_1 \cup \Sigma_2, \mathcal{P}_1 \cup \mathcal{P}_2$. Show that one can compute conjunctions of litterals Γ_1 and Γ_2, respectively over $\Sigma_1, \mathcal{P}_1$ and $\Sigma_2, \mathcal{P}_2$ such that:

$$\mathrm{Eq}_{\Sigma_1 \cup \Sigma_2, \mathcal{P}_1 \cup \mathcal{P}_2} \models (\exists x_1 \ldots \exists x_n.\ \Gamma) \Leftrightarrow (\exists y_1 \ldots \exists y_m.\ \Gamma_1 \wedge \Gamma_2)$$

Formulas in this form will be called **separated**.

For this question, you must present clearly your transformation; your are strongly encouraged to define it by means of rewrite rules. You must justify why the transformation computes formulas in the desired form, and argue (formally but without detailing everything) why the transformation of a formula yields a logically equivalent one.

1.3 The Nelson-Oppen method

A theory T is **stably infinite** when, for any quantifier-free T-satisfiable formula ϕ, there exists a T-interpretation that satisfies ϕ and whose domain is countably infinite. For example, the singleton theory $\{\forall x.\ x = a \vee x = b\}$ is not stably infinite, but elementary arithmetic is.

Question 5
Consider an arbitrary Σ, and $\mathcal{P} = \emptyset$. Show that the theory of equality is stably infinite: in other words, any quantifier-free formula ϕ has a model iff it has a

countably infinite model (recall that we only consider structures where equality is interpreted as equality over the structure's domain).

When $\mathcal{R}$ is a binary relation over a set of variables $V \subseteq \mathcal{X}$, we define its caracteristic set as follows:

$$E(\mathcal{R}, V) = \{x = y \mid x \mathcal{R} y\} \cup \{x \neq y \mid \neg(x \mathcal{R} y)\}$$

We will identify $E(\mathcal{R}, V)$ with the conjunction of its elements when V is finite.

Question 6
Assume that T_1 and T_2 are stably infinite, and that $\Gamma_1 \wedge \Gamma_2$ is a separated conjunction of litterals. Show that $\Gamma_1 \wedge \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable iff there exists an equivalence relation $\mathcal{R}$ over $V = \mathrm{fv}(\Gamma_1) \cap \mathrm{fv}(\Gamma_2)$ such that, for all $i \in \{1, 2\}$, $\Gamma_i \wedge E(\mathcal{R}, V)$ is T_i-satisfiable.

Question 7
Conclude that, if T_1 and T_2 are disjoint, decidable and stably infinite, the $(T_1 \cup T_2)$-satisfiability problem is still decidable for quantifier-free formulas.

It is normal to obtain an impractical decision procedure. Following this approach, one could obtain practical algorithms with a little bit more work, but this is beyond the scope of this assignment.

2 An Undecidable Combination

In this part, we exhibit two decidable theories that are disjoint, where one is not stably infinite, such that the combination of the two theories is undecidable.

We fix $\Sigma = \emptyset$ and consider predicate symbols P_M of arity 0 where M is a Turing machines:

$$\mathcal{P}_\mathcal{T} = \{P_M \mid M \text{ is a Turing machine}\}$$

Given a Turing machine, let $k(M)$ be the number of computation steps performed by M on the empty input before stopping, with $k(M) = \infty$ if the machine never stops. We define the Turing theory T_T as the set of all instances of the following axiom scheme:

$$P_M \Rightarrow \forall x_1 \ldots \forall x_m. \bigvee_{1 \leq i < j \leq m} x_i = x_j \quad \text{if } k(M) < m$$

Note that these axioms never mention a machine M for which $k(M) = \infty$.

Question 8
Given a conjunction ϕ of litterals over equality, show that one can compute a natural number n such that ϕ is satisfiable in all structures of cardinality at least n, and in no structure of lesser cardinality.

Question 9
Show that the T_T-satisfiability of conjunctions of litterals over $\mathcal{P}_\mathcal{T}$ is decidable (litterals over the equality predicate are still allowed).

Let $T_\mathbb{Z}$ be the theory over $\Sigma_\mathbb{Z} = \{0(0), s(1)\}$ and $\mathcal{P} = \emptyset$ formed of all formulas satisfied in the canonical structure of domain $\mathbb{Z}$. We admit that this theory is decidable — we will prove it during the week of May 11.

Question 10
Show the undecidability of the problem of $(T_T \cup T_\mathbb{Z})$-satisfiability for conjunctions of litterals.