1 Problems

1. Assume that you are given a formula $\phi$ in CNF over the variables $X = \{x_1, x_2, \ldots, x_n\}$. Let $C_1 = (x_1 \lor P)$ and $C_2 = (\bar{x}_1 \lor Q)$ denote two clauses in $\phi$, where $P$ and $Q$ are arbitrary disjuncts over $X$. Let $\phi' = \phi \land (P \lor Q)$. The above process is called a resolution step on variable $x_1$.

   (i) Show that resolution steps are solution preserving.

   (ii) We can continue in this fashion resolving on $x_1$ and other variables, deriving a new formula at each time till no new clauses can be added. Call the final formula $\phi^*$. Show that $\phi$ is satisfiable if and only if $\phi^*$ does not contain the empty clause ($\square$). Note that $\square$ is the resolvent of the clauses $(x_i)$, $(\bar{x}_i)$, for any $i = 1, 2, \ldots, n$.

Solution:

(i) We need to show that $\phi$ is satisfiable if and only if $\phi'$ is.

   Clearly, if $\phi'$ is satisfiable, then so is $\phi$, since the clauses defining $\phi$ are a subset of the clauses defining $\phi'$.

Assume that $\phi$ is satisfiable and let $\vec{x}$ denote an assignment satisfying $\phi$. Since all the clauses in $\phi$ are satisfied, it must be the case that at least one of the literals in $(P \lor Q)$ is set to true. To see this, observe that if all the variables in $(P \lor Q)$ are set to false under $\vec{x}$, then regardless of the value assigned to $x_1$, either $C_1$ is falsified or $C_2$ is! It follows that $\phi'$ is satisfiable.

(ii) Using induction on the number of resolution steps, it is clear that $\phi$ is satisfiable if and only if $\phi^*$ is. Thus, if $\phi^*$ contains $\square$, then $\phi'$ is unsatisfiable and hence so if $\phi$. Now assume that $\phi$ is satisfiable; by the solution preserving nature of resolution, each derived formula including $\phi^*$ is satisfiable. Assume that $\phi^*$ contains $\square$. This means that in the step preceding the derivation of $\square$, the intermediate formula, say $\phi'$ had a pair of clauses $(x_i)(\bar{x}_i)$ for some $i = 1, 2, \ldots, n$. However, this implies that $\phi'$ is unsatisfiable and hence so is $\phi$, contradicting the hypothesis. It follows that if $\phi$ is satisfiable, then $\phi^*$ cannot contain $\square$.

2. Let $\Sigma_{EG}$ denote an enhanced vocabulary for graph theory. As with $\Sigma_G$, $\Sigma_{EG}$ does not have a function symbol. It has a single ternary relation, called $G_w$, in addition to the binary relation $=$. Typical expressions in the new vocabulary are: $G_w(x, y, 5)$, $G_w(y, z, -5)$, $(\forall z)(\exists y)G_w(z, y, \infty)$ and so on. Write a sentence in $\Sigma_{EG}$ which describes graphs containing negative cost cycles.

Solution: Consider the following formula:

$$\Phi = (\exists P)(\phi_1 \land \phi_2 \land \phi_3 \land \phi_4),$$

where,

(i) $\phi_1 = (\exists c)(\exists c_1)(G(x, y, c) \rightarrow P(x, y, c_1) \land (c_1 \leq c))$ represents the fact that if there is an edge from $x$ to $y$ of length $c$, then there exists a path from $x$ to $y$ of length at most $c$.,
(ii) \( \phi_2 = (\exists x)(\exists c)(P(x, x, c) \land (c < 0)) \) represents the fact that if there exists some vertex \( x \), such that there is a negative cost path from \( x \) to \( x \).

(iii) \( \phi_3 = (\forall u)(\forall v)(\exists c_1)(\exists c_2)(P(u, v, c_1) \land P(v, u, c_2) \rightarrow P(u, v, c_3) \land (c_3 \leq c_1 + c_2)) \) represents the fact that if there is a path of length \( c_1 \) from \( u \) to \( v \) and a path of length \( c_2 \) from \( v \) to \( u \), then there exists a path of length at most \( (c_1 + c_2) \) from \( u \) to \( v \).

(iv) \( \phi_4 = (\forall x)(\exists c)(\exists x_1)(\exists x_2)(P(x, x_1, c) \rightarrow (G_x(x, y, c) \lor (P(x, x_1, c) \land P(x, x_2, c) \land (c = c_1 + c_2)))) \)
represents the fact that if there is a path of length \( c \) from \( x \) to \( y \), then either there is an edge in the graph of length \( c \) or there exists a vertex \( w \), such that there is a path of length \( c_1 \) from \( x \) to \( w \) and a path of length \( c_2 \) from \( w \) to \( y \) and \( c = c_1 + c_2 \).

Technically speaking, we do have all constants in \( \mathcal{Z} \) in the vocabulary!

3. Let \( P_1 \) denote the statement: If \( \Delta \) is consistent, then \( \Delta \) has a model. Let \( P_2 \) denote the statement: If \( \Delta \models \phi \), then \( \Delta \vdash \phi \). Argue that \( P_1 \) and \( P_2 \) are equivalent.

Solution:

(i) \( P_1 \rightarrow P_2 \) - Assume that for all sets of sentences \( \Delta \), whenever \( \Delta \) is consistent, it has a model. Now consider a specific pair \( (\Delta_1, \phi_1) \) such that \( \Delta_1 \models \phi_1 \). Thus, any model satisfying all the expressions in \( \Delta_1 \) also satisfies \( \phi_1 \) and therefore falsifies \( \neg \phi_1 \). It follows that no model can satisfy \( \Delta_1 \cup \{\neg \phi_1\} \) and hence this set is inconsistent. We apply Theorem 5.4 of [Pap94] to conclude that \( \Delta_1 \models \phi_1 \).

(ii) \( P_2 \rightarrow P_1 \) - Assume that for all sets of sentences \( \Delta \) and all sentences \( \phi \), if \( \Delta \models \phi \) then \( \Delta \vdash \phi \). Now consider a specific set of sentences \( \Delta_1 \), such that \( \Delta_1 \) is consistent. We need to show that \( \Delta_1 \) has a model. Assume \( \Delta_1 \) does not have a model. It follows that for any expression \( \phi \), \( \Delta_1 \models \phi \). However, as per \( P_2 \), this implies that \( \Delta_1 \vdash \phi \), for any expression \( \phi \). The only conclusion from the previous statement is that \( \Delta_1 \) is inconsistent, which contradicts the hypothesis!

4. Show that for any first-order expression \( \phi \) over the vocabulary \( \Sigma_{GPHS} \), the property \( \phi - \text{GRAPH} \) can be tested in logarithmic space.

Solution: We simply use induction on the length of the expression \( \phi \). If the expression is atomic, i.e., of the form \( G(x, y) \) or \( G(y, x) \) it can be trivially checked in logarithmic space. We now consider the following cases:

(i) \( \phi = \neg \psi \) - By induction \( \psi \) can be decided in logarithmic space. The answer to \( \psi \) can be inverted to get the answer for \( \phi \).

(ii) \( \phi = \psi_1 \lor \psi_2 \) - By induction, \( \psi_1 \) can be decided in logarithmic space. If the answer to \( \psi_1 \) is \text{true}, then so is the answer to \( \phi \). Otherwise, the answer to \( \psi_1 \) is the answer to \( \phi \), which can be inductively determined in logarithmic space.

(iii) \( \phi = \psi_1 \land \psi_2 \) - The answer to \( \psi_1 \) can be determined inductively in logarithmic space. If this answer is \text{false}, so is the answer to \( \phi \). Otherwise, the answer to \( \phi \) is the answer to \( \psi_2 \), which can be inductively determined in logarithmic space.

(iv) \( \phi = (\forall x)\psi \) - Substitute each node of \( G \) in the expression \( \psi \) and inductively determine the corresponding answer in logarithmic space. If any answer is \text{false}, the answer to \( \phi \) is \text{false}!

5. Gödel’s incompleteness theorem is based on the fact that if number theory was axiomatizable, then it would be decidable. Curiously enough, group theory is axiomatizable, but still undecidable. How would you explain this discrepancy?

Solution: The axiomatization of number theory employed by Gödel, refers specifically to the model \( \mathcal{N} \) of non-negative integers. Consequently, any recursive axiomatization would imply the existence of a recursive procedure to decide the truth of a statement. In case of group theory, there are an infinite number of groups and hence axiomatization does not imply the existence of an algorithm to determine truth.
References