Homework 1

Computer Aided Verification

Author:
Kidus Workneh

September 12, 2023

1

QUESTION 1

Prove Lemma 2 in Appendix B of the notes on first-order logic. That is, prove that in Peano arithmetic,

$$\forall x, y, z \;.\; x + z = y + z \leftrightarrow x = y$$

SOLUTION:

$P(z) = \forall x, y, z \;.\; x + z = y + z \leftrightarrow x = y$

1. $P(0) = x + 0 = y + 0 \leftrightarrow x = y$
   $x = y \leftrightarrow x = y$
2. $P(s(z)) \Leftrightarrow P(z)$
   $\Leftrightarrow \forall x, y \;.\; x + z = y + z \leftrightarrow x = y$
   $\Leftrightarrow \forall x, y \;.\; s(x + z) = s(y + z) \leftrightarrow x = y$
   $\Leftrightarrow \forall x, y \;.\; x + s(z) = y + s(z) \leftrightarrow x = y$
   $\Leftrightarrow P(s(z))$

2

QUESTION 2

Write a first-order sentence in the language of graphs (that is, the lan- guage with one binary relation symbol E) that says that every vertex of a graph has exactly one incoming edge; that is, that for vertex x there is exactly one vertex y such that E(y, x) is true.

SOLUTION:

$$\forall x, \exists y \;.\; E(y, x) \wedge \forall z, \;.\; E(z, x) \rightarrow y = z$$

3

QUESTION 3

Draw a model of your sentence for Problem 2; that is, draw a graph for which your sentence is true. Clearly, you can find a model of any given size (any given number of vertices). Corollary 1 from the notes then guarantees the existence of an infinite model. Describe one such model with a countable number of vertices. [Hint: Could you force your infinite model to be a strongly connected graph? Should you?]

SOLUTION:

With a finite Domain of three vertices $D = \{x1, x2, x3\}$

$$
\begin{tikzcd}
 & x_2 \arrow[d] \\
x_1 \arrow[ur] & \\
 & x_3 \arrow[ul]
\end{tikzcd}
$$

With an infinite model we can not circle back so we can not force it to be a strongly connected graph. A model that relates every number of the Natural numbers with an edge is one such model that can not be forced to be a strongly connected graph.

4

QUESTION 4

Section 4 of the notes on first-order logic, group theory is used as an example of first-order theory. The chosen signature contains the group operation symbol (binary function symbol), the equality symbol (binary relation symbol), and the identity symbol (constant symbol). How would you change the axioms if the identity symbol were excluded from the signature?

SOLUTION:

1. $\exists y \;.\; \forall x \;.\; xoy = yox = x$
2. $\exists y \;.\; \forall x \;.\; \exists z \;.\; xoy = yox = x \wedge xoz = zox = y$

5
QUESTION 5

Use the semantic tableau approach to prove the validity of

$$\forall x \,.\, \forall y \,.\, \phi(x, y) \rightarrow \forall v \,.\, \forall u \,.\, \phi(u, v)$$

1. $\neg[\forall x \,.\, \forall y \,.\, \phi(x, y) \rightarrow \forall v \,.\, \forall u \,.\, \phi(u, v)]$
2. $\forall x \,.\, \forall y \,.\, \phi(x, y)$
3. $\neg[\forall v \,.\, \forall u \,.\, \phi(u, v)]$
4. $\phi(a, b)$
5. $\neg\phi(a, b)$ $\qquad contradiction$