Exercise 1: Counterexample-guided discovery of predicates

Consider the following program.

\[
\phi_{init} \equiv pc = \ell_0
\]

\[
\rho_1 \equiv (move(\ell_0, \ell_1) \land y \geq z \land skip(x, y, z))
\]

\[
\rho_2 \equiv (move(\ell_1, \ell_1) \land x + 1 \leq y \land x' = x + 1 \land skip(y, z))
\]

\[
\rho_3 \equiv (move(\ell_1, \ell_2) \land x \geq y \land skip(x, y, z))
\]

\[
\rho_4 \equiv (move(\ell_2, \ell_3) \land x \geq z \land skip(x, y, z))
\]

\[
\rho_5 \equiv (move(\ell_2, \ell_4) \land x + 1 \leq z \land skip(x, y, z))
\]

Let \( P \text{rds}_{pc} \) be the set of all predicates on the program counter.

\[
P \text{rds}_{pc} = \{ pc = \ell_1, pc = \ell_2, pc = \ell_3, pc = \ell_4, pc = \ell_5 \}
\]

(a) Given the path \( \rho_1 \rho_2 \rho_3 \rho_5 \), provide a set of predicates \( P \text{rds} \) such that \( P \text{rds} \cup P \text{rds}_{pc} \) is sufficient to prove safety of the program, i.e., every abstract state returned by \( \text{ABSTREACH}(P \text{rds} \cup P \text{rds}_{pc}) \) is disjoint from \( \phi_{err} \) (the set of error states \( \phi_{err} \) is \( pc = \ell_4 \)).

Show that the predicates returned by your algorithm are sufficient to prove safety of the program by providing the abstract reachability graph.

(b) On page 31 of the hand article you can find the (general) function \( \text{RefinePath} \) which is used in the function \( \text{ABSTREFINELOOP} \) and returns a set of predicates \( P \text{rds} \) given a path \( \rho_1, \ldots, \rho_n \).

Let us implement \( \text{RefinePath} \) using the following idea:

Let \( \phi_0 := \phi_{init} \) and for the other predicates use the result from the application of \( \text{post} \) (e.g., \( \phi_1 := \text{post}(\phi_0, \rho_1) \)).

Observe that the predicates satisfy the required constraints of \( \text{RefinePath} \).

Compute \( P \text{rds} \) for the above program and path \( \rho_1 \rho_2 \rho_3 \rho_5 \) using this algorithm. Are the predicates sufficient to prove safety?

(c) Imagine we had a smart implementation for \( \text{RefinePath} \) to find predicates sufficient to prove safety of any safe program. What are the implications? What can you conclude about the existence of such an algorithm?