02141 Computer Science Modeling
Solutions to Selected Exercises from Formal Methods Appetizer, Chapter 3

Essential Exercise 3.21 Show that $\mathcal{SP}(\mathbf{P})$ is finite whenever the partial predicate assignment $\mathbf{P}$ covers the program graph.

Solution: We prove this statement by a proof by contradiction. So assume that $\mathbf{P}$ covers the program graph (we will refer to this program graph as PG in the rest of the proof) and that $\mathcal{SP}(\mathbf{P})$ is infinite. Let $n \geq 0$ be the number of edges in PG. Since $\mathcal{SP}(\mathbf{P})$ is assumed to be infinite it must be the case that there exists edges $e_1, \ldots, e_\ell$ and nodes q_s, q_t in PG such that $\ell > n$ and $q_s \mathsf{a}(e_1) \ldots \mathsf{a}(e_\ell) q_t$ is a short path fragment with respect to $\mathbf{P}$ (so $q_s \mathsf{a}(e_1) \ldots \mathsf{a}(e_\ell) q_t \in \mathcal{SP}(\mathbf{P})$). Hence at least two of the edges in the sequence $e_1 \ldots e_\ell$ must be the same, because this sequence contains more edges than there are edges in the graph. Hence $e_1 \ldots e_\ell$ contains a proper loop (that is, the loop is not simply the entire path). By Definition 3.13 we know that $\mathsf{s}(e_1) = q_s$ and $\mathsf{t}(e_\ell) = q_t$ are the only nodes in the sequence $e_1 \ldots e_\ell$ that can also occur in the domain of $\mathbf{P}$ since $q_s \mathsf{a}(e_1) \ldots \mathsf{a}(e_\ell) q_t \in \mathcal{SP}(\mathbf{P})$. That is, $\{\mathsf{s}(e_i), \mathsf{t}(e_{i-1}) \mid i \in \{2, \ldots, \ell\}\} \cap \mathsf{dom}(\mathbf{P}) = \emptyset$. However, since $\mathbf{P}$ is assumed to cover PG we have by Definition 3.11 that each loop of PG contains a node in $\mathsf{dom}(\mathbf{P})$, contradicting the fact we just proved that no such node exists for the loop occurring in $e_1 \ldots e_\ell$. So we have derived a contradiction when we assumed that $\mathcal{SP}(\mathbf{P})$ is infinite, and we can therefore conclude that $\mathcal{SP}(\mathbf{P})$ must be finite. $\square$