Exercises on Inductive Invariants, with Solutions

Grégoire Sutre

http://www.labri.fr/~sutre/Teaching/SV/

Recall that an *inductive invariant* is a set Inv of configurations that (1) contains all initial configurations, and (2) is closed under Post, i.e., $\mathrm{Post}(Inv) \subseteq Inv$. To simplify notation, the set Inv will be given by formulas with free variables X, namely, one formula φ_q for each location $q \in Q$. The resulting set Inv is the set

$$Inv \;=\; \bigcup_{q \in Q} \{q\} \times [\![\varphi_q]\!] \;=\; \{(q,\rho) \mid q \in Q \wedge \rho \models \varphi_q\}$$

The definition of inductive invariants is transposed to formulas as follows. A collection of formulas $(\varphi_q)_{q \in Q}$ denotes an inductive invariant if, and only if, the formulas

$$\begin{array}{rcll} \mathbf{true} & \Rightarrow & \varphi_{q_{in}} & \\ \varphi_p \wedge \langle\!\langle \mathtt{op} \rangle\!\rangle & \Rightarrow & \varphi_q^{\langle 1 \rangle} & (\text{for all } p \xrightarrow{\mathtt{op}} q) \end{array}$$

are all logically valid (in the theory of integers). Recall that, for any formula φ with free variables X, the formula $\varphi^{\langle 1 \rangle}$ is obtained from φ by replacing each free variable x by x'. The formula $\langle\!\langle \mathtt{op} \rangle\!\rangle$ has free variables $X \cup X'$ and is defined as follows:

$$\begin{array}{rcl} \langle\!\langle g \rangle\!\rangle & \stackrel{\text{def}}{=} & \mathrm{side}(g) \;\wedge\; g \;\wedge \bigwedge_{z \in X} z' = z \\ \langle\!\langle x := e \rangle\!\rangle & \stackrel{\text{def}}{=} & \mathrm{side}(e) \;\wedge\; (x' = e) \;\wedge \bigwedge_{z \in X, z \neq x} z' = z \end{array}$$

where $\mathrm{side}(g)$ and $\mathrm{side}(e)$ are side-conditions that ensure that no division by zero occurs in the evaluation of g and e, respectively.

Exercise 1 *Consider the control-flow automaton depicted below, with variables $X = \{\mathtt{x}, \mathtt{y}\}$, both ranging over integers, with initial location q_0 and bad location q_{bad}.*

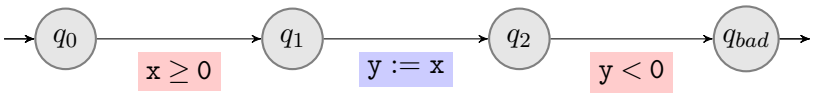

Exhibit an inductive invariant that is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$.

Solution. Choose the set Inv defined by the formulas $(\varphi_q)_{q \in Q}$ given hereafter:

$$\begin{array}{rcl} \varphi_{q_0} & = & \mathbf{true} \\ \varphi_{q_1} & = & \mathtt{x} \geq 0 \\ \varphi_{q_2} & = & \mathtt{y} \geq 0 \\ \varphi_{q_{bad}} & = & \mathbf{false} \end{array}$$

Obviously, the set Inv is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$. Let us show that the collection $(\varphi_q)_{q \in Q}$ denotes an inductive invariant.

- It holds that $\textbf{true} \Rightarrow \varphi_{q_0}$ since $\varphi_{q_0} = \textbf{true}$.
- $q_0 \xrightarrow{\mathtt{x} \geq \mathtt{0}} q_1$. Let ψ denote the formula $(\varphi_{q_0} \wedge \langle\!\langle \mathtt{x} \geq \mathtt{0} \rangle\!\rangle) \Rightarrow \varphi_{q_1}^{\langle 1 \rangle}$. We have:

$$\psi \quad = \quad \big(\textbf{true} \wedge \mathtt{x} \geq 0 \wedge \mathtt{x}' = \mathtt{x} \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \mathtt{x}' \geq 0$$

  which is logically valid.
- $q_1 \xrightarrow{\mathtt{y} := \mathtt{x}} q_2$. Let ψ denote the formula $(\varphi_{q_1} \wedge \langle\!\langle \mathtt{y} := \mathtt{x} \rangle\!\rangle) \Rightarrow \varphi_{q_2}^{\langle 1 \rangle}$. We have:

$$\psi \quad = \quad \big(\mathtt{x} \geq 0 \wedge \mathtt{y}' = \mathtt{x} \wedge \mathtt{x}' = \mathtt{x}\big) \;\Rightarrow\; \mathtt{y}' \geq 0$$

  which is logically valid.
- $q_2 \xrightarrow{\mathtt{y} < \mathtt{0}} q_{bad}$. Let ψ denote the formula $(\varphi_{q_2} \wedge \langle\!\langle \mathtt{y} < \mathtt{0} \rangle\!\rangle) \Rightarrow \varphi_{q_{bad}}^{\langle 1 \rangle}$. We have:

$$\psi \quad = \quad \big(\mathtt{y} \geq 0 \wedge \mathtt{y} < 0 \wedge \mathtt{x}' = \mathtt{x} \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \textbf{false}$$

  which is logically valid.

We have shown that Inv is an inductive invariant that is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$. ■

Exercise 2 *Consider the control-flow automaton depicted below, with variables $X = \{\mathtt{x}, \mathtt{y}\}$, both ranging over integers, with initial location q_0 and bad location q_{bad}.*

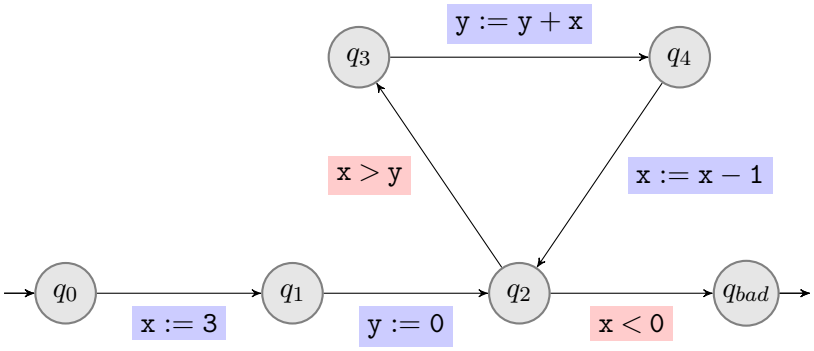

Exhibit an inductive invariant that is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$.

Solution. Choose the set Inv defined by the formulas $(\varphi_q)_{q \in Q}$ given hereafter:

$$\begin{array}{lcl} \varphi_{q_0} & = & \textbf{true} \\ \varphi_{q_1} & = & \mathtt{x} \geq 0 \\ \varphi_{q_2} & = & (\mathtt{x} \geq 0) \wedge (\mathtt{y} \geq 0) \\ \varphi_{q_3} & = & (\mathtt{x} > 0) \wedge (\mathtt{y} \geq 0) \\ \varphi_{q_4} & = & (\mathtt{x} > 0) \wedge (\mathtt{y} \geq 0) \\ \varphi_{q_{bad}} & = & \textbf{false} \end{array}$$

Obviously, the set Inv is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$. Let us show that the collection $(\varphi_q)_{q \in Q}$ denotes an inductive invariant.

- It holds that $\mathbf{true} \Rightarrow \varphi_{q_0}$ since $\varphi_{q_0} = \mathbf{true}$.
- $q_0 \xrightarrow{\mathtt{x := 3}} q_1$. Let ψ denote the formula $(\varphi_{q_0} \wedge \langle\!\langle \mathtt{x} := 3 \rangle\!\rangle) \Rightarrow \varphi_{q_1}^{\langle 1 \rangle}$. We have:
$$\psi \quad = \quad \big(\mathbf{true} \wedge \mathtt{x}' = 3 \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \mathtt{x}' \geq 0$$
which is logically valid.
- $q_1 \xrightarrow{\mathtt{y := 0}} q_2$. Let ψ denote the formula $(\varphi_{q_1} \wedge \langle\!\langle \mathtt{y} := 0 \rangle\!\rangle) \Rightarrow \varphi_{q_2}^{\langle 1 \rangle}$. We have:
$$\psi \quad = \quad \big(\mathtt{x} \geq 0 \wedge \mathtt{y}' = 0 \wedge \mathtt{x}' = \mathtt{x}\big) \;\Rightarrow\; \big(\mathtt{x}' \geq 0 \wedge \mathtt{y}' \geq 0\big)$$
which is logically valid.
- $q_2 \xrightarrow{\mathtt{x > y}} q_3$. Let ψ denote the formula $(\varphi_{q_2} \wedge \langle\!\langle \mathtt{x} > \mathtt{y} \rangle\!\rangle) \Rightarrow \varphi_{q_3}^{\langle 1 \rangle}$. We have:
$$\psi \quad = \quad \big(\mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0 \wedge \mathtt{x} > \mathtt{y} \wedge \mathtt{x}' = \mathtt{x} \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \big(\mathtt{x}' > 0 \wedge \mathtt{y}' \geq 0\big)$$
which is logically valid.
- $q_3 \xrightarrow{\mathtt{y := y + x}} q_4$. Let ψ denote the formula $(\varphi_{q_3} \wedge \langle\!\langle \mathtt{y} := \mathtt{y} + \mathtt{x} \rangle\!\rangle) \Rightarrow \varphi_{q_4}^{\langle 1 \rangle}$. We have:
$$\psi \quad = \quad \big(\mathtt{x} > 0 \wedge \mathtt{y} \geq 0 \wedge \mathtt{y}' = \mathtt{y} + \mathtt{x} \wedge \mathtt{x}' = \mathtt{x}\big) \;\Rightarrow\; \big(\mathtt{x}' > 0 \wedge \mathtt{y}' \geq 0\big)$$
which is logically valid.
- $q_4 \xrightarrow{\mathtt{x := x - 1}} q_2$. Let ψ denote the formula $(\varphi_{q_4} \wedge \langle\!\langle \mathtt{x} := \mathtt{x} - 1 \rangle\!\rangle) \Rightarrow \varphi_{q_2}^{\langle 1 \rangle}$. We have:
$$\psi \quad = \quad \big(\mathtt{x} > 0 \wedge \mathtt{y} \geq 0 \wedge \mathtt{x}' = \mathtt{x} - 1 \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \big(\mathtt{x}' \geq 0 \wedge \mathtt{y}' \geq 0\big)$$
which is logically valid (since $\mathtt{x}$ ranges over $\mathbb{Z}$).
- $q_2 \xrightarrow{\mathtt{x < 0}} q_{bad}$. Let ψ denote the formula $(\varphi_{q_2} \wedge \langle\!\langle \mathtt{x} < 0 \rangle\!\rangle) \Rightarrow \varphi_{q_{bad}}^{\langle 1 \rangle}$. We have:
$$\psi \quad = \quad \big(\mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0 \wedge \mathtt{x} < 0 \wedge \mathtt{x}' = \mathtt{x} \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \mathbf{false}$$
which is logically valid.

We have shown that Inv is an inductive invariant that is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$. ■

Exercise 3 *Consider the control-flow automaton depicted below, with variables $X = \{\mathtt{x}, \mathtt{y}\}$, both ranging over integers, with initial location q_0 and bad location q_{bad}.*

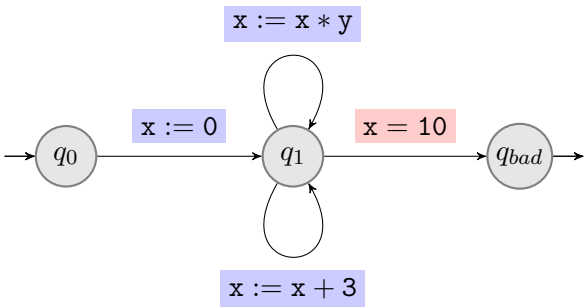

Exhibit an inductive invariant that is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$.

Solution. Choose the set Inv defined by the formulas $(\varphi_q)_{q \in Q}$ given hereafter:

$$\begin{array}{lcl} \varphi_{q_0} & = & \textbf{true} \\ \varphi_{q_1} & = & \exists k \in \mathbb{Z} \cdot (\mathtt{x} = 3k) \\ \varphi_{q_{bad}} & = & \textbf{false} \end{array}$$

Obviously, the set Inv is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$. Let us show that the collection $(\varphi_q)_{q \in Q}$ denotes an inductive invariant. For simplicity, we write $\mathtt{x} \in 3\mathbb{Z}$ in place of $\exists k \in \mathbb{Z} \cdot (\mathtt{x} = 3k)$.

- It holds that $\textbf{true} \Rightarrow \varphi_{q_0}$ since $\varphi_{q_0} = \textbf{true}$.
- $q_0 \xrightarrow{\mathtt{x} := 0} q_1$. Let ψ denote the formula $(\varphi_{q_0} \wedge \langle\!\langle \mathtt{x} := 0 \rangle\!\rangle) \Rightarrow \varphi_{q_1}^{\langle 1 \rangle}$. We have:
$$\psi \quad = \quad \big(\textbf{true} \wedge \mathtt{x}' = 0 \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \mathtt{x}' \in 3\mathbb{Z}$$
which is logically valid.
- $q_1 \xrightarrow{\mathtt{x} := \mathtt{x} * \mathtt{y}} q_1$. Let ψ denote the formula $(\varphi_{q_1} \wedge \langle\!\langle \mathtt{x} := \mathtt{x} * \mathtt{y} \rangle\!\rangle) \Rightarrow \varphi_{q_1}^{\langle 1 \rangle}$. We have:
$$\psi \quad = \quad \big(\mathtt{x} \in 3\mathbb{Z} \wedge \mathtt{x}' = \mathtt{x} \cdot \mathtt{y} \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \mathtt{x}' \in 3\mathbb{Z}$$
which is logically valid (since $\mathtt{y}$ ranges over $\mathbb{Z}$).
- $q_1 \xrightarrow{\mathtt{x} := \mathtt{x} + 3} q_1$. Let ψ denote the formula $(\varphi_{q_1} \wedge \langle\!\langle \mathtt{x} := \mathtt{x} + 3 \rangle\!\rangle) \Rightarrow \varphi_{q_1}^{\langle 1 \rangle}$. We have:
$$\psi \quad = \quad \big(\mathtt{x} \in 3\mathbb{Z} \wedge \mathtt{x}' = \mathtt{x} + 3 \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \mathtt{x}' \in 3\mathbb{Z}$$
which is logically valid.
- $q_1 \xrightarrow{\mathtt{x} = 10} q_{bad}$. Let ψ denote the formula $(\varphi_{q_1} \wedge \langle\!\langle \mathtt{x} = 10 \rangle\!\rangle) \Rightarrow \varphi_{q_{bad}}^{\langle 1 \rangle}$. We have:
$$\psi \quad = \quad \big(\mathtt{x} \in 3\mathbb{Z} \wedge \mathtt{x} = 10 \wedge \mathtt{x}' = \mathtt{x} \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \textbf{false}$$
which is logically valid (since $\mathtt{x}$ ranges over $\mathbb{Z}$).

We have shown that Inv is an inductive invariant that is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$. ■

Exercise 4 *Consider the control-flow automaton depicted below, with variables* $X = \{\mathtt{x}, \mathtt{y}\}$, *both ranging over integers, with initial location* q_0 *and bad location* q_{bad}.

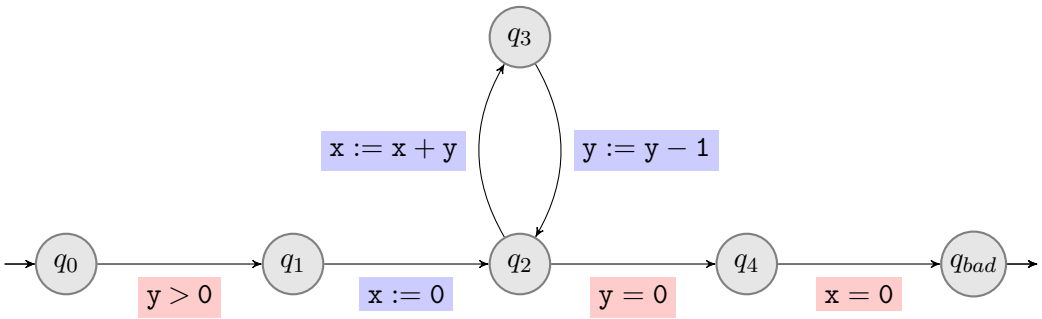

Exhibit an inductive invariant that is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$.

Tentative Solution. Choose the set Inv defined by the formulas $(\varphi_q)_{q \in Q}$ given hereafter:

$$\begin{array}{lcl} \varphi_{q_0} & = & \textbf{true} \\ \varphi_{q_1} & = & \mathtt{y} > 0 \\ \varphi_{q_2} & = & (\mathtt{y} = 0) \Rightarrow (\mathtt{x} > 0) \\ \varphi_{q_3} & = & (\mathtt{y} \geq 0) \Rightarrow (\mathtt{x} > 0) \\ \varphi_{q_4} & = & \mathtt{x} > 0 \\ \varphi_{q_{bad}} & = & \textbf{false} \end{array}$$

The set Inv is *not* an inductive invariant, since $\mathrm{Post}(Inv) \not\subseteq Inv$. Let us explain why. The problem arises from the transition $q_2 \xrightarrow{\mathtt{x} := \mathtt{x} + \mathtt{y}} q_3$. For Inv to be an inductive invariant, the formula $(\varphi_{q_2} \wedge \langle\!\langle \mathtt{x} := \mathtt{x} + \mathtt{y} \rangle\!\rangle) \Rightarrow \varphi_{q_3}^{\langle 1 \rangle}$ must be logically valid. But this is not the case: pick for instance the valuation $\{\mathtt{x} \mapsto -2, \mathtt{y} \mapsto 1, \mathtt{x}' \mapsto -1, \mathtt{y}' \mapsto 1\}$. An equivalent explanation is that the operational semantics of the control-flow automaton contains the step $(q_2, \rho_2) \xrightarrow{\mathtt{x} := \mathtt{x} + \mathtt{y}} (q_3, \rho_3)$ where $\rho_2 = \{\mathtt{x} \mapsto -2, \mathtt{y} \mapsto 1\}$ and $\rho_3 = \{\mathtt{x} \mapsto -1, \mathtt{y} \mapsto 1\}$. But $(q_2, \rho_2) \in Inv$ and $(q_3, \rho_3) \notin Inv$. Hence, $\mathrm{Post}(Inv) \not\subseteq Inv$.

The problem exhibited above comes from the transition $q_2 \xrightarrow{\mathtt{x} := \mathtt{x} + \mathtt{y}} q_3$. Informally, φ_2 was not strong enough to ensure that φ_3 holds after this transition. We may try to correct the chosen set Inv, by making φ_{q_2} stronger, as follows:

$$\varphi_{q_2} \quad = \quad (\mathtt{y} \geq 0) \Rightarrow (\mathtt{x} > 0)$$

This fixes the problem that we had before with the transition $q_2 \xrightarrow{\mathtt{x} := \mathtt{x} + \mathtt{y}} q_3$. Indeed, the formula $(\varphi_{q_2} \wedge \langle\!\langle \mathtt{x} := \mathtt{x} + \mathtt{y} \rangle\!\rangle) \Rightarrow \varphi_{q_3}^{\langle 1 \rangle}$ now becomes

$$\big((\mathtt{y} \geq 0) \Rightarrow (\mathtt{x} > 0) \ \wedge \ \mathtt{x}' = \mathtt{x} + \mathtt{y} \ \wedge \ \mathtt{y}' = \mathtt{y}\big) \quad \Rightarrow \quad \big((\mathtt{y}' \geq 0) \Rightarrow (\mathtt{x}' > 0)\big)$$

which is logically valid. However, it introduces an other problem: φ_{q_2} is now too strong. Indeed, the formula $(\varphi_{q_1} \wedge \langle\!\langle \mathtt{x} := 0 \rangle\!\rangle) \Rightarrow \varphi_{q_2}^{\langle 1 \rangle}$ has become invalid. In fact, this choice of φ_{q_2} cannot be correct: it does not capture the configuration $(q_2, \{\mathtt{x} \mapsto 0, \mathtt{y} \mapsto 1\})$, which belongs to the reachability set Post^*.

Solution. Choose the set Inv defined by the formulas $(\varphi_q)_{q \in Q}$ given hereafter:

$$\begin{array}{lcl} \varphi_{q_0} & = & \textbf{true} \\ \varphi_{q_1} & = & \mathtt{y} > 0 \\ \varphi_{q_2} & = & (\mathtt{y} \geq 0) \Rightarrow (\mathtt{x} + \mathtt{y} > 0) \\ \varphi_{q_3} & = & (\mathtt{y} \geq 0) \Rightarrow (\mathtt{x} > 0) \\ \varphi_{q_4} & = & \mathtt{x} > 0 \\ \varphi_{q_{bad}} & = & \textbf{false} \end{array}$$

Obviously, the set Inv is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$. Let us show that the collection $(\varphi_q)_{q \in Q}$ denotes an inductive invariant.

- It holds that $\textbf{true} \Rightarrow \varphi_{q_0}$ since $\varphi_{q_0} = \textbf{true}$.

- $q_0 \xrightarrow{\mathtt{y} > \mathtt{0}} q_1$. Let ψ denote the formula $(\varphi_{q_0} \wedge \langle\!\langle \mathtt{y} > \mathtt{0} \rangle\!\rangle) \Rightarrow \varphi_{q_1}^{\langle 1 \rangle}$. We have:

$$\psi \;=\; \big(\mathbf{true} \wedge \mathtt{y} > 0 \wedge \mathtt{x}' = \mathtt{x} \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \mathtt{y}' > 0$$

  which is logically valid.

- $q_1 \xrightarrow{\mathtt{x} := \mathtt{0}} q_2$. Let ψ denote the formula $(\varphi_{q_1} \wedge \langle\!\langle \mathtt{x} := \mathtt{0} \rangle\!\rangle) \Rightarrow \varphi_{q_2}^{\langle 1 \rangle}$. We have:

$$\psi \;=\; \big(\mathtt{y} > 0 \wedge \mathtt{x}' = 0 \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \big((\mathtt{y}' \geq 0) \Rightarrow (\mathtt{x}' + \mathtt{y}' > 0)\big)$$

  which is logically valid.

- $q_2 \xrightarrow{\mathtt{x} := \mathtt{x} + \mathtt{y}} q_3$. Let ψ denote the formula $(\varphi_{q_2} \wedge \langle\!\langle \mathtt{x} := \mathtt{x} + \mathtt{y} \rangle\!\rangle) \Rightarrow \varphi_{q_3}^{\langle 1 \rangle}$. We have:

$$\psi \;=\; \big((\mathtt{y} \geq 0) \Rightarrow (\mathtt{x} + \mathtt{y} > 0) \wedge \mathtt{x}' = \mathtt{x} + \mathtt{y} \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \big((\mathtt{y}' \geq 0) \Rightarrow (\mathtt{x}' > 0)\big)$$

  which is logically valid.

- $q_3 \xrightarrow{\mathtt{y} := \mathtt{y} - \mathtt{1}} q_2$. Let ψ denote the formula $(\varphi_{q_3} \wedge \langle\!\langle \mathtt{y} := \mathtt{y} - \mathtt{1} \rangle\!\rangle) \Rightarrow \varphi_{q_2}^{\langle 1 \rangle}$. We have:

$$\psi \;=\; \big((\mathtt{y} \geq 0) \Rightarrow (\mathtt{x} > 0) \wedge \mathtt{y}' = \mathtt{y} - 1 \wedge \mathtt{x}' = \mathtt{x}\big) \;\Rightarrow\; \big((\mathtt{y}' \geq 0) \Rightarrow (\mathtt{x}' + \mathtt{y}' > 0)\big)$$

  which is logically valid.

- $q_2 \xrightarrow{\mathtt{y} = \mathtt{0}} q_4$. Let ψ denote the formula $(\varphi_{q_2} \wedge \langle\!\langle \mathtt{y} = \mathtt{0} \rangle\!\rangle) \Rightarrow \varphi_{q_4}^{\langle 1 \rangle}$. We have:

$$\psi \;=\; \big((\mathtt{y} \geq 0) \Rightarrow (\mathtt{x} + \mathtt{y} > 0) \wedge \mathtt{y} = 0 \wedge \mathtt{x}' = \mathtt{x} \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \mathtt{x}' > 0$$

  which is logically valid.

- $q_4 \xrightarrow{\mathtt{x} = \mathtt{0}} q_{bad}$. Let ψ denote the formula $(\varphi_{q_4} \wedge \langle\!\langle \mathtt{x} = \mathtt{0} \rangle\!\rangle) \Rightarrow \varphi_{q_{bad}}^{\langle 1 \rangle}$. We have:

$$\psi \;=\; \big(\mathtt{x} > 0 \wedge \mathtt{x} = 0 \wedge \mathtt{x}' = \mathtt{x} \wedge \mathtt{y}' = \mathtt{y}\big) \;\Rightarrow\; \mathbf{false}$$

  which is logically valid.

We have shown that Inv is an inductive invariant that is disjoint from $\{q_{bad}\} \times \mathbb{Z}^X$. ■