Transition Invariants Revisited: Termination Witnesses and Their Validation (Supplementary Material)

Dirk Beyer, Marek Jankola, and Marian Lingsch-Rosenfeld

LMU Munich, Munich, Germany

1 Proofs for Chapter 4

1.1 Proof of Lemma 1

Proof. Direction $\Leftarrow$: Let us prove this direction by contradiction. Let T be a transition invariant that is well-founded on the reachable states and let P be non-terminating. Hence, there exists an infinite sequence $\langle s_0, s_1, \dots \rangle$ of states, such that $\mathit{Init}(s_0) \wedge \forall i \geq 0 : R(s_i, s_{i+1})$ holds. Since $\mathit{Init}(s_0)$, all the states from the sequence are reachable ($s_0, s_1, \dots \in \mathscr{R}$). Moreover, T is a transition invariant and therefore, $\forall i \geq 0 : (s_i, s_{i+1}) \in (T \cap (\mathscr{R} \times \mathscr{R}) \cap R^+)$ which is a contradiction to T being well-founded on the reachable states.

Direction $\Rightarrow$: The same argument as Podelski and Rybalchenko used in their proof that Theorem 1 holds [1]. $\square$

1.2 Proof of Lemma 2

Proof. If T is a disjunctively well-founded transition invariant of P, then P is terminating according to Theorem 1. Hence, the transitive closure of the transfer relation restricted to reachable states $R^+ \cap (\mathscr{R} \times \mathscr{R})$ of P is well-founded. Therefore, the relation $(T \cap (\mathscr{R} \times \mathscr{R}) \cap R^+)$ is also well-founded. $\square$

1.3 Proof of Lemma 3

Proof. Let L be a program loop, $\rho_0, \dots, \rho_k : S \to \mathbb{N}_0$ be functions and formula T be

$$T(s, s') \equiv \bigvee_{0 \leq i \leq k} (\rho_i(s) > \rho_i(s') \bigwedge_{0 \leq j < i} \rho_j(s) \geq \rho_j(s'))$$

Direction $\Rightarrow$: *Transition invariant:* This directly follows from the Definition 4. *Inductivity (the theorem can be extended with inductivity):* Let us assume that $T(s, s') \wedge R_L(s', s'')$ holds for some $s, s', s'' \in S$. In the following, we show that $T(s, s'')$ holds, as well. Since $T(s, s')$, then there exists such $0 \leq i \leq k$ that $\rho_i(s) > \rho_i(s') \bigwedge_{0 \leq j < i} \rho_j(s) \geq \rho_j(s')$. From Definition 4 and $R_L(s', s'')$, we know that there exists i' such that $\rho_{i'}(s') > \rho_{i'}(s'') \bigwedge_{0 \leq j < i'} \rho_j(s') \geq \rho_j(s'')$. We further divide the proof by the following cases:

- $i \leq i'$, it holds that $\rho_i(s) > \rho_i(s')$ and $\rho_i(s') \geq \rho_i(s'')$. Hence, it holds that $\rho_i(s) > \rho_i(s'')$.
- $i > i'$, it holds that $\rho_{i'}(s) \geq \rho_{i'}(s')$ and $\rho_{i'}(s') > \rho_{i'}(s'')$. Hence, it holds that $\rho_{i'}(s) > \rho_{i'}(s'')$.

Well-foundedness: We prove the property by contradiction. Let $s_0, s_1, \dots$ be an infinite sequence with $\forall i \geq 0 : T(s_i, s_{i+1})$. However, since $\rho_0, \dots, \rho_k$ map the states to $\mathbb{N}_0$ and for every transition $T(s_i, s_{i+1})$ at least one of them decreases, eventually, there is a state s_j in the sequence, which is mapped to a minimal value by every ranking function. Trivially, such a state does not have a successor in T.
Direction $\Leftarrow$: Let us prove this by contraposition. We assume that $\rho_0, \dots, \rho_k$ do not form a lexicographic ranking function for the loop L. Hence, there are states $(s, s') \in \mathscr{R} \times \mathscr{R}$ such that $R_L(s, s')$ and for all $0 \leq i \leq k$, it holds that $\rho_i(s) \leq \rho_i(s')$ or there is $0 \leq j < i$ such that $\rho_j(s) < \rho_j(s')$. Therefore, $T(s, s')$ also does not hold and therefore, T is not a transition invariant. □

1.4 Proof of Lemma 4

Proof. Direction $\Rightarrow$: *1-step invariant:* Assume two states $\widehat{s}, \widehat{s}' \in \mathscr{R}'$, such that $R'^{+}(\widehat{s}, \widehat{s}')$. Since we assume any combination of locations in I^t, it is not relevant what the variables *pc* and $\widehat{pc}$ are assigned to in $\widehat{s}'$. We distinguish two cases:

- $\widehat{s}'(\mathit{saved}) = 1$: It follows that $I^t(\widehat{s}') \equiv I(\widehat{s}')$ and $I(\widehat{s}')$ is satisfied because I is 1-step invariant.
- $\widehat{s}'(\mathit{saved}) = 0$: In this case, $\widehat{s}_{\downarrow X} = \widehat{s}'_{\downarrow \widehat{X}}$ because no state has been saved in $\widehat{s}_{\downarrow \widehat{X}}$. However, since both $\widehat{s}$ and $\widehat{s}'$ are reachable, there has to be a previous state $\widehat{s}''$ that can reach them both and $\widehat{s}_{\downarrow \widehat{X}} = \widehat{s}''_{\downarrow X}$. Hence, if we save this state, right after the first transition, states with the same mapping values as $\widehat{s}$ and $\widehat{s}'$, but with $\widehat{s}'(\mathit{saved}) = 1$ are still reachable from $\widehat{s}''$. Therefore, $I^t(\widehat{s}')$ also holds.

Safety: Let us assume $I(\widehat{s})$ holds, we show that $\neg\widehat{s}(\mathit{saved}) \vee \bigvee_{x \in X} \widehat{s}(x) \neq \widehat{s}(\widehat{x})$ is satisfied. The case $\widehat{s}(\mathit{saved}) = 0$ is trivial. If $\widehat{s}(\mathit{saved}) = 1$, then $I^t(\widehat{s}) = I(\widehat{s})$ and from the safety of I, we get that $\varphi'(\widehat{s})$ holds.

Direction $\Leftarrow$: Let $I^t \equiv \bigvee_{l, l' \in D_{pc}} I(\widehat{s}(\widehat{x}_0), \dots, \widehat{s}(\widehat{x}_{n-1}), l, \widehat{s}(x_0), \dots, \widehat{s}(x_{n-1}), l', 1)$ be an 1-step safe invariant of P'. Since I^t instantiates some of the variables of I but is the same otherwise, it holds that $I^t \Rightarrow I$. Therefore, I is an 1-step invariant, as well. Lastly, I is safe because I^t enumerates all the options for the *pc* variable in the disjunction and the only assignment it does not consider is $\mathit{saved} = 0$. However, in such case, the property is trivially satisfied, hence, I is safe. □

Fig. 1: A visual illustration of the first (left) and the second (right) case from the proof of transition invariance in Theorem 3. Every state from the instrumented program is divided into valuation of variables from X (up) and from $\widehat{X}$ (down).

1.5 Proof of Theorem 3

Proof. In this proof, R and R' are transition formulas of P and P', respectively. Direction $\Rightarrow$: Let I be a safe 1-step invariant of instrumented program P'.
Transition invariant: We have to show the following

$$\forall s, s' \in (\mathscr{R} \times \mathscr{R}) : (R^+(s, s') \Rightarrow T(s, s'))$$

Let $s, s' \in \mathscr{R} \times \mathscr{R}$ be states, such that $R^+(s, s')$ holds. Furthermore, let $\widehat{s}'$ be a state of instrumented program P' with $\widehat{s}'(\widehat{x}) = s(x)$ for all $\widehat{x} \in \widehat{X}$ and $\widehat{s}'(x) = s'(x)$ for all $x \in X$. In other words, it maps the ghost variables to the values assigned by s and the original variables to the values from s'. From the definition, if $I(\widehat{s}')$ holds, then we get $T(s, s')$. Hence, it is sufficient to show that $\widehat{s}'$ is reachable in at least one step in P'. Since, $s \in \mathscr{R}$, there are two cases possible (with a visual illustration in Fig. 1):

- $\mathit{Init}(s)$ holds: There is a state $\widehat{s}$, such that $\forall x \in X : \widehat{s}(x) = \widehat{s}(\widehat{x}) = s(x)$, $\widehat{s}(\mathit{saved}) = 0$ and hence $\mathit{Init}'(\widehat{s})$. More importantly, $\widehat{s} \in \mathscr{R}'$ and from the definition of R', $\widehat{s}$ can reach $\widehat{s}'$, i.e., $R'^+(\widehat{s}, \widehat{s}')$. The path from $\widehat{s}$ to $\widehat{s}'$ follows the transitions from the path given by $R^+(s, s')$ and saves s into the ghost variables in the first transition. Hence, it propagates s in the ghost variables from $\widehat{s}$ to $\widehat{s}'$. Lastly, from Definition 2, $I(\widehat{s}')$ holds.
- $\exists s_0, \ldots, s_k : \mathit{Init}(s_0) \wedge R(s_0, s_1) \wedge \ldots \wedge R(s_{k-1}, s) \wedge R(s, s_k)$ holds: Hence, there is a state $\widehat{s}_k$, such that $\forall x \in X : \widehat{s}_k(x) = s_k(x) \wedge \widehat{s}_k(\widehat{x}) = s(x)$, $\widehat{s}_k(\mathit{saved}) = 1$ and trivially, $\widehat{s}_k \in \mathscr{R}'$. Since $R(s, s_k)$, we can copy the state s into the ghost variables of $\widehat{s}_k$. Moreover, since $R^+(s, s')$, we can again pass s, further in the ghost variables and eventually reach $\widehat{s}'$. Therefore, $R'^+(\widehat{s}, \widehat{s}')$ and $I(\widehat{s}')$ is satisfied.

Well-foundedness on the reachable states: We show the property by contradiction. Let $\langle s_0, s_1, \ldots \rangle$ be an infinite sequence such that $\mathit{Init}(s_0) \wedge \forall i \geq 0 : T(s_i, s_{i+1}) \wedge R^+(s_i, s_{i+1})$ holds. The domains of all the variables in P are finite. Hence, the set S of all the states is finite. Therefore, there exist at least two indices $j < k$, such that $s_j = s_k = s$. Since s is repeating, without loss of generality, we can assume that the line number $s(pc)$ is a loop-head of some loop of P. Moreover, since $R^+(s_j, s_k)$, we can save the state s_j thanks to the transtition $R(s_j, s_{j+1})$ in the state of P'. Therefore, state $\widehat{s} \in S'$ with $\forall x \in X : \widehat{s}(x) = \widehat{s}(\widehat{x}) = s_j(x)$ and $\widehat{s}(\mathit{saved}) = 1$ is reachable. However, this implies $I(\widehat{s})$, which contradicts that I is a safe invariant.

Direction $\Leftarrow$: Let $T(s, s')$ be a transition invariant that is well-founded on the reachable states of P.
1-step invariant: Assume two states $\widehat{s}, \widehat{s}' \in \mathscr{R}'$, such that $R'^+(\widehat{s}, \widehat{s}')$. Since $\widehat{s}$ is reachable, there exists a sequence $\langle \widehat{s}_0, \ldots, \widehat{s}_j, \widehat{s}_{j+1}, \ldots, \widehat{s}_k \rangle$ of states, such that

$$\mathit{Init}'(\widehat{s}_0) \wedge R'(\widehat{s}_0, \widehat{s}_1) \wedge \ldots \wedge R'(\widehat{s}_j, \widehat{s}) \wedge R'(\widehat{s}, \widehat{s}_{j+1}) \ldots \wedge R'(\widehat{s}_k, \widehat{s}')$$

From the construction of $Init'$ and R' in Definition 1, it follows that there is a state $\widehat{s}''$ in the sequence, such that $\widehat{s}'$ maps the ghost variables to the same values as $\widehat{s}''$ maps the original variables. More formally, $\widehat{s}''$ is either $\widehat{s}$ or is equal to some $\widehat{s}_i$ from the sequence, and $\forall x \in X : \widehat{s}''(x) = \widehat{s}'(\widehat{x})$. Further, $R^+(\widehat{s}''_{\downarrow X}, \widehat{s}'_{\downarrow X})$ also follows from the definition of R'. Since T is a transition invariant of P, we get that $T(\widehat{s}''_{\downarrow X}, \widehat{s}'_{\downarrow X})$ also holds. Therefore, $I(\widehat{s}''(\widehat{x}_0), \ldots, \widehat{s}''(\widehat{x}_n), \widehat{s}'(x_0), \ldots, \widehat{s}'(x_n)) \equiv I(\widehat{s}'(\widehat{x}_0), \ldots, \widehat{s}'(\widehat{x}_n), \widehat{s}'(x_0), \ldots, \widehat{s}'(x_n)) \equiv I(\widehat{s}')$ holds.
Safe invariant: Analogous to the proof of the *well-foundedness.* □

1.6 Proof of Theorem 3 - Inductivity

Proof. Direction $\Rightarrow$: The 1-step invariance of I follows from Lemma 1 and the base version of Theorem 3. Let T be an inductive transition invariant. Further, let $\widehat{s}, \widehat{s}' \in S'$ be such that $I(\widehat{s}) \wedge R'(\widehat{s}, \widehat{s}')$. Transition $R'(\widehat{s}, \widehat{s}')$ implies $R(\widehat{s}_{\downarrow X}, \widehat{s}'_{\downarrow X})$ by Definition 1 and $I(\widehat{s}) \equiv T(\widehat{s}_{\downarrow \widehat{X}}, \widehat{s}_{\downarrow X})$. Our goal is to show that $T(\widehat{s}'_{\downarrow \widehat{X}}, \widehat{s}'_{\downarrow X})$ holds. By Definition 1 $\widehat{s}'_{\downarrow \widehat{X}}$ can be equal to

- $\widehat{s}_{\downarrow X}$ *due to transition of type (1) and (3)*: From inductiveness of T and $R(\widehat{s}_{\downarrow X}, \widehat{s}'_{\downarrow X})$, we get $T(\widehat{s}_{\downarrow X}, \widehat{s}'_{\downarrow X}) \equiv T(\widehat{s}'_{\downarrow \widehat{X}}, \widehat{s}'_{\downarrow X})$, which holds.
- $\widehat{s}_{\downarrow \widehat{X}}$ *due to transition of type (2)*: Again, from inductiveness of T, $T(\widehat{s}_{\downarrow \widehat{X}}, \widehat{s}_{\downarrow X})$ and $R(\widehat{s}_{\downarrow X}, \widehat{s}'_{\downarrow X})$, formula $T(\widehat{s}_{\downarrow \widehat{X}}, \widehat{s}'_{\downarrow X}) \equiv T(\widehat{s}'_{\downarrow \widehat{X}}, \widehat{s}'_{\downarrow X})$ holds.

Direction $\Leftarrow$: Let I be an inductive 1-step invariant of P'. Let $s, s', s'' \in \mathscr{R}$ be reachable states in P. To prove that T is an inductive transition invariant, we have to show two subgoals

- $R(s, s') \Rightarrow T(s, s')$. Since $R(s, s')$, then there exist states $\widehat{s}, \widehat{s}' \in S'$ such that $R'(\widehat{s}, \widehat{s}')$. Moreover, $\widehat{s}_{\downarrow X} = s$, $\widehat{s}'_{\downarrow X} = s'$ and we can save the state with $R'(\widehat{s}, \widehat{s}')$. In more details, $\widehat{s}(saved) = 0$ and $\widehat{s}'(saved) = 1$, therefore $\widehat{s}'_{\downarrow \widehat{X}} = \widehat{s}_{\downarrow X}$. Note that since $s, s' \in \mathscr{R}$, then $\widehat{s}, \widehat{s}' \in \mathscr{R}'$[1]. Finally, we get that $I(\widehat{s}') \equiv T(\widehat{s}'_{\downarrow \widehat{X}}, \widehat{s}'_{\downarrow X}) \equiv T(\widehat{s}_{\downarrow X}, \widehat{s}'_{\downarrow X}) \equiv T(s, s')$ holds.
- $T(s, s'') \wedge R(s'', s') \Rightarrow T(s, s')$. Due to $T(s, s'')$, there exists a state $\widehat{s} \in S'$ such that $\widehat{s}_{\downarrow \widehat{X}} = s$ and $\widehat{s}_{\downarrow X} = s''$, for which $I(\widehat{s})$ holds. Consider another state $\widehat{s}'$ such that $\widehat{s}'_{\downarrow \widehat{X}} = s$ and $\widehat{s}'_{\downarrow X} = s'$. Because of $R(s'', s')$, there exists a transition of type (2) $R'(\widehat{s}, \widehat{s}')$. Since I is inductive and $I(\widehat{s})$, we obtain $I(\widehat{s}') \equiv T(s, s')$. □

2 Proofs for Chapter 5

2.1 Proof of Lemma 5

Proof. Let R_L be a transition relation of loop L and let k be a number such that $1 \leq k$. Further, let us assume that the base-case and step-case formulas for the k

[1] We omit the proof of this here. However, it follows from the construction in Definition 1.

are valid. Consider an arbitrary sequence of reachable states $s'_0, \ldots, s'_m \in \mathscr{R}_L$, with $1 \leq m$ and $R(s'_0, s'_1) \wedge \ldots \wedge R(s'_{m-1}, s'_m)$ being valid. Since all the states $s'_0, \ldots, s'_m$ are reachable, $\bigwedge_{0 \leq j \leq m} I_L(s_j)$ holds. To prove that T is a transition invariant, we have to show that $T(s'_0, s'_m)$ holds. We divide the proof into two cases:

- $m \leq k$: In this case, we get that formula $\forall s_0, \ldots, s_m : R(s_0, s_1) \wedge \ldots \wedge R(s_{m-1}, s_m) \Rightarrow T(s_0, s_m)$ is valid due to the base case. If we substitute the universally quantifed states with $s'_0, \ldots, s'_m$, we get that $T(s'_0, s'_m)$ holds.
- $m > k$: Since both m and k are natural numbers, one of the foundational results from number theory tells us that there are two numbers $1 \leq l$ and $0 \leq r < k$, such that $m = l \cdot k + r$. We adjust the equation to an equivalent one and assume that $0 \leq l$ and $1 \leq r \leq k$. After substituting formula from the base case, we get that $R(s'_0, s'_1) \wedge \ldots \wedge R(s'_{r-1}, s'_r) \Rightarrow T(s'_0, s'_r)$, hence $T(s'_0, s'_r)$ holds. We can now substitute the step formula with $T(s'_0, s'_r) \wedge R(s'_r, s'_{r+1}) \wedge \ldots \wedge R(s'_{r+k-1}, s'_{r+k}) \Rightarrow T(s'_0, s'_{r+k})$. Therefore, $T(s'_0, s'_{r+k})$ holds. After substituting the formula l-times, we get that $T(s'_0, s'_{l \cdot k + r}) \equiv T(s'_0, s'_m)$ holds.

$\square$

2.2 Proof of Lemma 6

Proof. Let X be the set of variables that occur in T. Since all the variables from X have finite domains, then $S_{\downarrow X}$ is also finite. For contradiction, assume that T is not well-founded on the reachable states and `is_well_founded`(T, I_L) is valid. Then there exists an infinite sequence $s_0, s_1, \ldots \in S$ such that $\forall 0 \leq i : T(s_i, s_{i+1}) \wedge (s_i, s_{i+1}) \in \mathscr{R} \times \mathscr{R}$. Moreover, it holds that $\forall 0 \leq i : I_L(s_i)$ because I_L is the conjunction of the supporting invariants for L. Since $S_{\downarrow X}$ is finite, there exist two states s, s' from the sequence, such that $s_{\downarrow X} = s'_{\downarrow X}$. Let $succ(s) = \{s'' \in S \mid T(s, s'') \wedge I_L(s'')\}$, we show by induction the following: If $\forall 1 \leq k : T(s_1, s_2) \wedge \ldots \wedge T(s_k, s_{k+1}) \wedge \forall 1 \leq i \leq k+1 : I_L(s_i)$, then there exist at least k states that are in $succ(s_1)$ but are not in $succ(s_k)$.

- *Base Case:* Let $k = 1$ and $T(s_1, s_2) \wedge I_L(s_1) \wedge I_L(s_2)$ hold. Since the formula `is_well_founded`(T, I_L) is valid, then by definition of *succ*, it holds that there is a state s_0 such that $s_0 \in succ(s_1)$ and $s_0 \notin succ(s_2)$. Moreover, due to the second clause of the conjunction, $succ(s_2) \subseteq succ(s_1)$.
- *Step Case:* Let $k > 1$ and $T(s_1, s_2) \wedge \ldots \wedge T(s_k, s_{k+1}) \wedge \forall 1 \leq i \leq k+1 : I_L(s_i)$ hold. It follows, from the induction hypothesis, that there are at least $k - 1$ states that are in $succ(s_1)$ and not in $succ(s_k)$. Due to the validity of the formula `is_well_founded`(T, I_L), it holds that $succ(s_{k+1}) \subseteq succ(s_k)$ and therefore, these states are also not in $succ(s_{k+1})$. Moreover, there also exists a state s_0 that is in $succ(s_k)$ and not in $succ(s_{k+1})$. Hence, there exist at least $k + 1$ states that are in $succ(s_1)$ and not in $succ(s_{k+1})$.

Since T depends only on the variables from X, it holds that $succ(s) = succ(s')$. Therefore, the property that $succ(s)$ contains at least one state that is not in $succ(s')$, leads to a contradiction with $s_{\downarrow X} = s'_{\downarrow X}$. Hence, T must be well-founded on the reachable states. $\square$

2.3 Proof of Lemma 7

Proof. Let there exist formulas $C_1, \ldots, C_n$ such that $T = C_1 \vee \ldots \vee C_n$ and $\forall 1 \leq i \leq n :$ `is_disj_well_founded`(C_i, I_L). For the contradiction, let us assume that $R_L^+ \cap (\mathscr{R} \times \mathscr{R})$ is not well-founded. Since $R_L^+ \wedge (\mathscr{R} \times \mathscr{R})$ is not well-founded, there is exists an infinite sequence $s_0, s_1, \ldots \in \mathscr{R}$ such that $\forall 0 \leq i : R_L^+(s_i, s_{i+1})$. Let X be the set of variables used in T with finite domains. Due to the infinite sequence satisfying $R_L^+ \wedge (\mathscr{R} \times \mathscr{R})$, there exist two states in the sequence $s, s' \in \mathscr{R}$ such that $s_{\downarrow X} = s'_{\downarrow X}$ and $R_L^+(s, s')$. Since $R_L^+ \Rightarrow T$, then trivially $R_L^+ \cap (\mathscr{R} \times \mathscr{R}) \Rightarrow T$ holds as well. Hence, $T(s, s')$ and $T(s, s)$ hold because of the finiteness of X. There is a formula C_i from the sequence $C_1, \ldots, C_n$, such that $C_i(s, s)$ which is a contradiction with `is_disj_well_founded`(C_i, I_L). $\square$

2.4 Proof of Lemma 8

Proof. For the contradiction, let us assume that the overapproximating program is not terminating and T is well-founded. Hence, the transition relation R_T is not well-founded. Therefore, there exists an inifinite sequence $s_0, s_1, \ldots \in \mathscr{R}$, such that $\forall 0 \leq i : LC(s_i) \wedge I_L(s_i) \wedge I_L(s_{i+1}) \wedge T(s_i, s_{i+1})$. However, then T is also not well-founded, which is a contradiction. $\square$

References

1. Podelski, A., Rybalchenko, A.: Transition invariants. In: Proc. LICS. pp. 32–41. IEEE (2004). https://doi.org/10.1109/LICS.2004.1319598