School for Information Technology
Computer Science Technical Report

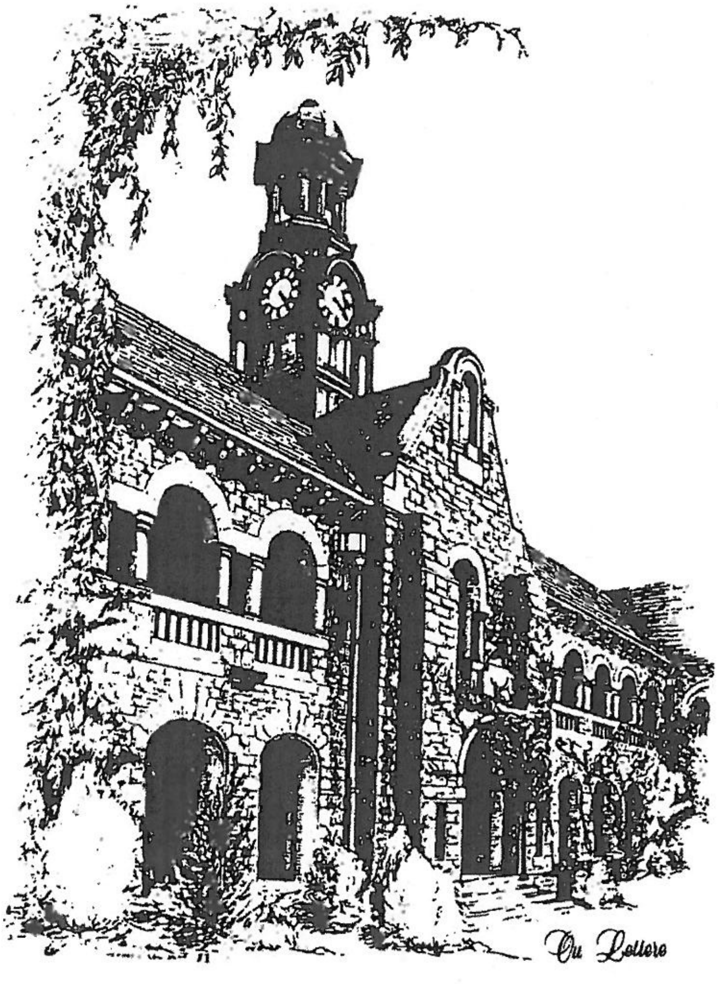
Parameterised Three-Valued Model Checking – Proofs

Nils Timm and Stefan Gruner

Department of Computer Science, University of Pretoria, South Africa
{ntimm,sgruner}@cs.up.ac.za

October 2, 2015

Abstract. In this technical report we prove Theorem 1 and Theorem 2 of the article *Parameterised Three-Valued Model Checking* submitted to the journal *Science of Computer Programming SI: SBMF 2014*.



University of Pretoria

Proof of Theorem 1

In the following we present the proof of Theorem 1 from Section 4. The proof was originally introduced in our SBMF 2014 paper where we used a slightly different but equivalent notation for Kripke structures: $M = (S, s_0, R, L)$ is the same as $K = (S, R, L)$ and $[M \models \psi]$ is the same as $[K, s_0 \models \psi]$. Hence, in this proof we explicitly refer to the initial state $s_0 \in S$ in the model checking problem $[K, s_0 \models \psi]$ instead of referring to s_0 in the tuple $K = (S, R, L)$, whereas in the current article it is vice versa. For our proof we use the following Proposition 1 from [8] (pp. 64-65) which establishes the relation between the two-valued Kripke structure K modelling the concrete system and the three-valued Kripke structure $K^\perp$ modelling the abstract system.

Proposition 1

Let $Sys = \|_{i=1}^{n}\ Proc_i$ be a concurrent system and $Spot = Spot(Proc) \cup Spot(Pred)$ be a given spotlight abstraction for Sys. Let $K = (S, R, L)$ over a set AP be a two-valued Kripke structure modelling the concrete state space of Sys, i.e. every temporal logic property over AP that holds for Sys also holds for K and vice versa. Let $K^\perp = (S^\perp, R^\perp, L^\perp)$ over $AP^\perp = Spot(Pred) \cup \{pc_i = j \mid Proc_i \in Spot(Proc) \wedge j \in Loc_i\}$ with $AP^\perp \subseteq AP$ be a pure three-valued Kripke structure modelling the abstract state space corresponding to $Spot$. Moreover, let $s_1 \in S$ and $s_1^\perp \in S^\perp$ be states representing the initial configuration of Sys in K resp. $K^\perp$ and let ψ over $AP^\perp$ be an LTL formula. Then the following holds:

1. $[K^\perp, s_1^\perp \models \psi] \ \leq_{\mathbb{K}_3}\ [K, s_1 \models \psi]$, *i.e. every definite verification result obtained for the pure three-valued Kripke structure $K^\perp$ can be transferred to the two-valued Kripke structure K,*
2. *for each path $\pi^\perp \in \Pi(K^\perp, s_1^\perp)$ there exists a path $\pi \in \Pi(K, s_1)$ with $\forall\, i > 0 : R^\perp(\pi_i^\perp, \pi_{i+1}^\perp) = true \ \Rightarrow\ R(\pi_i, \pi_{i+1}) = true \ \wedge\ \forall\, p \in AP^\perp : L^\perp(\pi_i^\perp, p) \ \leq_{\mathbb{K}_3}\ L(\pi_i, p)$,*
3. *for each path $\pi \in \Pi(K, s_1)$ there exists a path $\pi^\perp \in \Pi(K^\perp, s_1^\perp)$ with $\forall\, i > 0 : R(\pi_i, \pi_{i+1}) \neq false \ \Rightarrow\ R^\perp(\pi_i^\perp, \pi_{i+1}^\perp) \neq false \ \wedge\ \forall\, p \in AP^\perp : L^\perp(\pi_i^\perp, p) \ \leq_{\mathbb{K}_3}\ L(\pi_i, p)$.*

Hence, for each path in $K^\perp$ there exists a corresponding 'more or equal definite' path in K, and for each path in K there exists a corresponding 'less or equal definite' path in $K^\perp$. Based on this proposition we can prove Theorem 1.

Theorem 1

Let $Sys = \|_{i=1}^{n}\ Proc_i$ be a concurrent system and $Spot = Spot(Proc) \cup Spot(Pred)$ be a given spotlight abstraction for Sys. Let K over AP be a two-valued KS modelling the concrete state space of Sys and let $K^\perp$ over $AP^\perp = Spot(Pred) \cup \{pc_i = j \mid Proc_i \in Spot(Proc) \wedge j \in Loc_i\}$ with $AP^\perp \subseteq AP$ be a pure three-valued KS modelling the abstract state space corresponding to $Spot$. Moreover, let s_1 and $s_1^\perp$ be states representing the initial configuration of Sys in K resp. $K^\perp$. Then for any parameterisation $K^\perp(\overset{m}{x})$ of $K^\perp$ obtained by applying the *rules I and II, and for any safety or liveness LTL formula ψ over $AP^{\perp}$ the following holds:*

$$[K^{\perp}(\overset{m}{x}), s_1^{\perp} \models \psi] \quad \leq_{\mathbb{K}_3} \quad [K, s_1 \models \psi]$$

Proof. (Theorem 1)
Theorem 1 immediately follows from Lemma 1 where we split $[K^{\perp}(\overset{m}{x}), s_1^{\perp} \models \psi] \quad \leq_{\mathbb{K}_3} \quad [K, s_1 \models \psi]$ into two different cases:

Lemma 1
Let all definitions as in Theorem 1. Then the following holds:

(1) $[K^{\perp}(\overset{m}{x}), s_1^{\perp} \models \psi] = \mathit{true} \quad \Rightarrow \quad [K, s_1 \models \psi] = \mathit{true}.$

and

(2) $[K^{\perp}(\overset{m}{x}), s_1^{\perp} \models \psi] = \mathit{false} \quad \Rightarrow \quad [K, s_1 \models \psi] = \mathit{false}$

Proof. (Lemma 1)
The proof of Part (1) of Lemma 1 is as follows. We start with the following equivalent transformations (note that K is two-valued, whereas $K^{\perp}$ and $K^{\perp}(\overset{m}{x})$ are three-valued):

$$[K^{\perp}(\overset{m}{x}), s_1^{\perp} \models \psi] = \mathit{true} \;\Rightarrow\; [K, s_1 \models \psi] = \mathit{true}$$

$$\Leftrightarrow\; [K^{\perp}(\overset{m}{x}), s_1^{\perp} \models \psi] \neq \mathit{true} \;\vee\; [K, s_1 \models \psi] = \mathit{true}$$

$$\Leftrightarrow\; [K, s_1 \models \psi] = \mathit{true} \;\vee\; [K^{\perp}(\overset{m}{x}), s_1^{\perp} \models \psi] \neq \mathit{true}$$

$$\Leftrightarrow\; [K, s_1 \models \psi] = \mathit{false} \;\Rightarrow\; [K^{\perp}(\overset{m}{x}), s_1^{\perp} \models \psi] \neq \mathit{true}$$

$$\Leftrightarrow\; [K, s_1 \models \psi] = \mathit{false} \;\Rightarrow\; [K^{\perp}(\overset{m}{x}), s_1^{\perp} \models \psi] \in \{\mathit{false}, \perp\}$$

$$\Leftrightarrow\; [K, s_1 \models \psi] = \mathit{false} \;\Rightarrow\; \exists(\overset{m}{a}) \in \{t, f\}^m \,\exists \pi \in \Pi(K^{\perp}(\overset{m}{a}), s_1^{\perp}) : [\pi \models \psi] \in \{\mathit{false}, \perp\}$$

(compare Definition 4 and Definition 6 of the submitted paper)

Hence, we have to show that if checking $[K, s_1 \models \psi]$ yields *false*, then there exists an instantiation $K^{\perp}(\overset{m}{a})$ of $K^{\perp}(\overset{m}{x})$ such that checking $[K^{\perp}(\overset{m}{a}), s_1^{\perp} \models \psi]$ yields *false* or *unknown*, i.e. for some $K^{\perp}(\overset{m}{a})$ there exists a path π with $[\pi \models \psi] \in \{\mathit{false}, \perp\}$.

We know that for K and $K^{\perp}$ Proposition 1 holds and we have that ψ is of the form

(a) $\psi \equiv \mathbf{G}\neg p$ (safety)
i.e. a real counterexample for ψ would be of the form $\pi = (\pi_1 \dots \pi_k)$ with

$\forall\, 1 \leq i < k : R(\pi_i, \pi_{i+1}) = \mathit{true}$ and $L(\pi_k, p) = \mathit{true}$ (whereas an unconfirmed counterexample would be of a similar form but could also contain $\perp$-transitions and $\perp$-labellings)

or

(b) $\psi \equiv \mathbf{GF}p$ (liveness)
i.e. a real counterexample for ψ would be of the form $\pi = (\pi_1 \ldots \pi_{l-1}) \bullet (\pi_l \ldots \pi_k)^\omega$ with $\forall\, 1 \leq i < k : R(\pi_i, \pi_{i+1}) = \mathit{true}$, $R(\pi_k, \pi_l) = \mathit{true}$, and $\forall\, l \leq i \leq k : L(\pi_i, p) = \mathit{false}$ (whereas an unconfirmed counterexample would be of a similar form but could also contain $\perp$-transitions and $\perp$-labellings)

where $p \in AP^\perp$.

Thus, Lemma 1 Part (1) immediately follows from Lemma 2 where we distinguish the following cases:

Lemma 2
Let all definitions as in Theorem 1 and let $p \in AP^\perp$. Then the following holds:

(a) If there exists a path $\pi \in \Pi(K, s_1)$ and π is of the form $\pi = (\pi_1 \ldots \pi_k)$ with $\forall\, 1 \leq i < k : R(\pi_i, \pi_{i+1}) = \mathit{true}$ and $L(\pi_k, p) = \mathit{true}$, then there is an instantiation $K^\perp(\overset{m}{a})$ of $K^\perp(\overset{m}{x})$ such that there exists a path $\pi^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \ldots \pi_{k'}^\perp(\overset{m}{a}))$ with $\forall\, 1 \leq i < k' : R^\perp(\overset{m}{a})(\pi_i(\overset{m}{a}), \pi_{i+1}(\overset{m}{a})) \in \{\mathit{true}, \perp\}$ and $L^\perp(\overset{m}{a})(\pi_{k'}^\perp(\overset{m}{a}), p) \in \{\mathit{true}, \perp\}$.

(b) If there exists a path $\pi \in \Pi(K, s_1)$ and π is of the form $\pi = (\pi_1 \ldots \pi_{l-1}) \bullet (\pi_l \ldots \pi_k)^\omega$ with $\forall\, 1 \leq i < k : R(\pi_i, \pi_{i+1}) = \mathit{true}$, $R(\pi_k, \pi_l) = \mathit{true}$ and $\forall\, l \leq i \leq k : L(\pi_i, p) = \mathit{false}$, then there is an instantiation $K^\perp(\overset{m}{a})$ of $K^\perp(\overset{m}{x})$ such that there exists a path $\pi^\perp(\overset{m}{a}) \in \Pi(K^\perp(\overset{m}{a}), s_1^\perp)$ and $\pi^\perp(\overset{m}{a})$ is of the form $\pi^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \ldots \pi_{l'-1}^\perp(\overset{m}{a})) \bullet (\pi_{l'}^\perp(\overset{m}{a}) \ldots \pi_{k'}^\perp(\overset{m}{a}))^\omega$ with $\forall\, 1 \leq i < k' : R^\perp(\overset{m}{a})(\pi_i^\perp(\overset{m}{a}), \pi_{i+1}^\perp(\overset{m}{a})) \in \{\mathit{true}, \perp\}$, $R^\perp(\overset{m}{a})(\pi_{k'}^\perp(\overset{m}{a}), \pi_{l'}^\perp(\overset{m}{a})) \in \{\mathit{true}, \perp\}$ and $\forall\, l' \leq i \leq k' : L^\perp(\overset{m}{a})(\pi_i^\perp(\overset{m}{a}), p) \in \{\mathit{false}, \perp\}$.

Proof. (Lemma 2)
Case (a): Based on Proposition 1.3 we can conclude that in the pure three-valued Kripke structure $K^\perp$ there exists a path $\pi^\perp \in \Pi(K^\perp, s_1^\perp)$ which is of the form $\pi^\perp = (\pi_1^\perp \ldots \pi_{k'}^\perp)$ with $\forall\, 1 \leq i < k' : R^\perp(\pi_i^\perp, \pi_{i+1}^\perp) \in \{\mathit{true}, \perp\}$ and $L^\perp(\pi_{k'}^\perp, p) \in \{\mathit{true}, \perp\}$.

Without loss of generality we can assume that along $\pi^\perp$ each transition and state occurs at most once. Otherwise $\pi^\perp$ must contain cycles $(\pi_t^\perp \ldots \pi_r^\perp)^n$ that are left after a finite number of n run-throughs. We can remove such cycles by replacing $\pi^\perp = (\pi_1^\perp \ldots \pi_r^\perp) \bullet (\pi_t^\perp \ldots \pi_r^\perp)^n \bullet (\pi_{r+1}^\perp \ldots \pi_k^\perp)$ by $\pi^\perp =$

$(\pi_1^\perp \ldots \pi_r^\perp \pi_{r+1}^\perp \ldots \pi_{k'}^\perp)$, which is still a prefix with $\forall\, 1 \leq i < k' : R^\perp(\pi_i^\perp, \pi_{i+1}^\perp) \in \{\mathit{true}, \perp\}$ and $L^\perp(\pi_{k'}^\perp, p) \in \{\mathit{true}, \perp\}$.

Since $K^\perp(\overset{m}{x})$ is a parameterisation of $K^\perp$, there must exist and instantiation $K^\perp(\overset{m}{a})$ such that there exists a path $\pi^\perp(\overset{m}{a}) \in \Pi(K^\perp(\overset{m}{a}), s_1^\perp)$ with $\pi^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \ldots \pi_{k'}^\perp(\overset{m}{a}))$ with $\forall\, 1 \leq i < k' : R^\perp(\overset{m}{a})(\pi_i(\overset{m}{a}), \pi_{i+1}(\overset{m}{a})) \in \{\mathit{true}, \perp\}$ and $L^\perp(\overset{m}{a})(\pi_{k'}^\perp(\overset{m}{a}), p) \in \{\mathit{true}, \perp\}$.

The explanation is as follows: According to the definition of our parameterisation rules, the path $\pi^\perp \in \Pi(K^\perp, s_1^\perp)$ must have a corresponding path $\pi^\perp(\overset{m}{x}) \in \Pi(K^\perp(\overset{m}{x}), s_1^\perp)$ where some formerly *unknown* transitions and labellings might now be parameterised, and similar to $\pi^\perp$, each transition and state occurs at most once along $\pi^\perp(\overset{m}{x})$. We now choose $(\overset{m}{a}) \in \{\mathit{true}, \mathit{false}\}^m$ such that each parameterised transition along $\pi^\perp(\overset{m}{x})$ evaluates to *true* along $\pi^\perp(\overset{m}{a})$. This is possible because we have that each state occurs at most once along $\pi^\perp(\overset{m}{x})$. Hence, the starting state of a parameterised complementary branch can occur at most once, and thus, only one branch of each parameterised complementary branch can occur along $\pi^\perp(\overset{m}{x})$ at all. Moreover, if $L^\perp(\overset{m}{x})(\pi_{k'}^\perp(\overset{m}{x}), p)$ is parameterised, then we instantiate the labelling parameters such that $L^\perp(\overset{m}{a})(\pi_{k'}^\perp(\overset{m}{a}), p) = \mathit{true}$.

This implies Lemma 2 (a) and thus ends this case of the proof.

Case (b): Based on Proposition 1.3 we can conclude that in the pure three-valued Kripke structure $K^\perp$ there exists a path $\pi^\perp = (\pi_1^\perp \ldots \pi_{l'-1}^\perp) \bullet (\pi_{l'}^\perp \ldots \pi_{k'}^\perp)^\omega$ with $\forall\, 1 \leq i < k' : R^\perp(\pi_i^\perp, \pi_{i+1}^\perp) \in \{\mathit{true}, \perp\}$, $R^\perp(\pi_k^\perp, \pi_{l'}^\perp) \in \{\mathit{true}, \perp\}$ and $\forall\, l' \leq i \leq k' : L^\perp(\pi_i^\perp, p) \in \{\mathit{false}, \perp\}$.

Without loss of generality we can assume that along $\pi^\perp$'s finite unfolding $\pi^{\perp \mathit{fin}} = (\pi_1^\perp \ldots \pi_{l'-1}^\perp) \bullet (\pi_{l'}^\perp \ldots \pi_{k'}^\perp) \bullet (\pi_{l'}^\perp)$ each transition and state occurs at most once, except the state $\pi_{l'}^\perp$ which occurs twice. The explanation is the same as in Case (a). For $\pi^{\perp \mathit{fin}}$ we still have that $\forall\, 1 \leq i < k' : R^\perp(\pi_i^\perp, \pi_{i+1}^\perp) \in \{\mathit{true}, \perp\}$, $R^\perp(\pi_{k'}^\perp, \pi_{l'}^\perp) \in \{\mathit{true}, \perp\}$ and $\forall\, l' \leq i \leq k' : L^\perp(\pi_i^\perp, p) \in \{\mathit{false}, \perp\}$.

Since $K^\perp(\overset{m}{x})$ is a parameterisation of $K^\perp$, there must exist and instantiation $K^\perp(\overset{m}{a})$ such that there exists a path $\pi^\perp(\overset{m}{a}) \in \Pi(K^\perp(\overset{m}{a}), s_1^\perp)$ with $\pi^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \ldots \pi_{l'-1}^\perp(\overset{m}{a})) \bullet (\pi_{l'}^\perp(\overset{m}{a}) \ldots \pi_{k'}^\perp(\overset{m}{a}))^\omega$ with $\forall\, 1 \leq i < k' : R^\perp(\overset{m}{a})(\pi_i(\overset{m}{a}), \pi_{i+1}(\overset{m}{a})) \in \{\mathit{true}, \perp\}$ and $\forall\, l' \leq i \leq k' : L^\perp(\overset{m}{a})(\pi_i^\perp(\overset{m}{a}), p) \in \{\mathit{false}, \perp\}$

The explanation is as follows: According to the definition of our parameterisation rules, the path $\pi^\perp \in \Pi(K^\perp, s_1^\perp)$ must have a corresponding path $\pi^\perp(\overset{m}{x}) \in \Pi(K^\perp(\overset{m}{x}), s_1^\perp)$ where some formerly *unknown* transitions and labellings might now be parameterised, and similar to $\pi^\perp$, each transition and state occurs at most once along $\pi^\perp(\overset{m}{x})$'s finite unfolding $\pi^{\perp \mathit{fin}}(\overset{m}{x}) = (\pi_1^\perp(\overset{m}{x}) \ldots \pi_{l'-1}^\perp(\overset{m}{x})) \bullet (\pi_{l'}^\perp(\overset{m}{x}) \ldots \pi_{k'}^\perp(\overset{m}{x})) \bullet (\pi_{l'}^\perp(\overset{m}{x}))$, except the state $\pi_{l'}^\perp(\overset{m}{x})$ which occurs twice. We now choose $(\overset{m}{a}) \in \{\mathit{true}, \mathit{false}\}^m$ such that each parameterised transition along $\pi^{\perp \mathit{fin}}(\overset{m}{x})$ evaluates to *true* along $\pi^{\perp \mathit{fin}}(\overset{m}{a})$. This is possible because along $\pi^{\perp \mathit{fin}}(\overset{m}{x})$ each state s has a unique successor state s', and thus, at most one branch transition of each parameterised complementary branch can occur along $\pi^{\perp \mathit{fin}}(\overset{m}{x})$ at all. $\pi^{\perp \mathit{fin}}(\overset{m}{x})$ can be straightforwardly extended to an infinite path that repetitively runs through the same transitions. Thus, with our evaluation we also get the infinite path $\pi^{\perp}(\overset{m}{a}) = (\pi_1^{\perp}(\overset{m}{a}) \dots \pi_{l'-1}^{\perp}(\overset{m}{a})) \bullet (\pi_{l'}^{\perp}(\overset{m}{a}) \dots \pi_{k'}^{\perp}(\overset{m}{a}))^{\omega}$ where each formerly parameterised transition is now *true*.

It remains to show that we can choose $(\overset{m}{a}) \in \{\mathit{true}, \mathit{false}\}^m$ such that additionally $\forall\, l' \leq i \leq k' : L^{\perp}(\overset{m}{a})(\pi_i^{\perp}(\overset{m}{a}), p) \in \{\mathit{false}, \perp\}$ holds for the cycle part $(\pi_{l'}^{\perp}(\overset{m}{a}) \dots \pi_{k'}^{\perp}(\overset{m}{a}))$ of $\pi^{\perp}(\overset{m}{a})$. According to our rules, the parameterisation of predicates is always independent from the parameterisation of transitions. Thus, we can argument independently from our formerly chosen $(\overset{m}{a}) \in \{\mathit{true}, \mathit{false}\}^m$ for transitions here.

It is sufficient to show that along the cycle part $(\pi_{l'}^{\perp}(\overset{m}{x}) \dots \pi_{k'}^{\perp}(\overset{m}{x}))$ of the parameterised $\pi^{\perp}(\overset{m}{x})$ there exists no complementary parameterisation with regard to the predicate p, i.e. $\neg \exists\, l' \leq i, j \leq k'$ with $L^{\perp}(\overset{m}{x})(\pi_i^{\perp}(\overset{m}{x}), p) = b$ and $L^{\perp}(\overset{m}{x})(\pi_j^{\perp}(\overset{m}{x}), p) = \neg b$ where b is a logical expression over $\{x_1, \dots, x_m\}$.

Remember that K correctly represents the concrete state space of the considered system *Sys*, in K there exists the path $\pi = (\pi_1 \dots \pi_{l-1}) \bullet (\pi_l \dots \pi_k)^{\omega}$ with $\forall\, l \leq i \leq k : L(\pi_i, p) = \mathit{false}$, and $K^{\perp}$ is a corresponding sound abstract state space model (compare Proposition 1). The parameterisation of predicates in $K^{\perp}$ is always done *with respect to the systems operations associated with transitions* in $K^{\perp}$ (compare Rule II). Thus, in any parameterised Kripke structure $K^{\perp}(\overset{m}{x})$ constructed by the application of Rule II to $K^{\perp}$, there must be a cycle $(\pi_{l'}^{\perp}(\overset{m}{x}) \dots \pi_{k'}^{\perp}(\overset{m}{x}))$ corresponding to concrete cycle $(\pi_l \dots \pi_k)$ without a complementary parameterisation with regard to the predicate p.

This implies Lemma 2 (b) and thus ends the proof of Lemma 2.
□

The proof of Part (2) of Lemma 1 is analogous to the proof of Part (1) goes as follows. We start with the following equivalent transformation (note that K is two-valued, whereas $K^{\perp}$ and $K^{\perp}(\overset{m}{x})$ are three-valued):

$$[K^{\perp}(\overset{m}{x}), s_1^{\perp} \models \psi] = \mathit{false} \;\Rightarrow\; [K, s_1 \models \psi] = \mathit{false}$$

$\Leftrightarrow\; \forall(\overset{m}{a}) \in \{t, f\}^m\, \exists \pi \in \Pi(K^{\perp}(\overset{m}{a}), s_1^{\perp}) : [\pi \models \psi] = \mathit{false} \;\Rightarrow\; [K, s_1 \models \psi] = \mathit{false}$
(compare Definition 4 and Definition 6 of the submitted paper)

Hence, we have to show that if checking $[K^{\perp}(\overset{m}{a}), s_1^{\perp} \models \psi]$ yields *false* for all instantiations $K^{\perp}(\overset{m}{a})$ of $K^{\perp}(\overset{m}{x})$, then checking $[K, s_1 \models \psi]$ also yields *false*. I.e. if for all $K^{\perp}(\overset{m}{a})$ there exists a path $\pi^{\perp}$ with $[\pi^{\perp} \models \psi] = \mathit{false}$ then there exists a path π in K with $[\pi \models \psi] = \mathit{false}$.

We know that for K and $K^{\perp}$ Proposition 1 holds and we have that ψ is of the form

(a) $\psi \equiv \mathbf{G}\neg p$ (safety)
i.e. a real counterexample for ψ would be of the form $\pi = (\pi_1 \dots \pi_k)$ with $\forall\, 1 \leq i < k : R(\pi_i, \pi_{i+1}) = \mathit{true}$ and $L(\pi_k, p) = \mathit{true}$ (whereas an unconfirmed counterexample would be of a similar form but could also contain

$\perp$-transitions and $\perp$-labellings)

or

(b) $\psi \equiv \mathbf{GF}p$ (liveness)
i.e. a real counterexample for ψ would be of the form $\pi = (\pi_1 \dots \pi_{l-1}) \bullet (\pi_l \dots \pi_k)^\omega$ with $\forall\, 1 \leq i < k : R(\pi_i, \pi_{i+1}) = \mathit{true}$, $R(\pi_k, \pi_l) = \mathit{true}$, and $\forall\, l \leq i \leq k : L(\pi_i, p) = \mathit{false}$ (whereas an unconfirmed counterexample would be of a similar form but could also contain $\perp$-transitions and $\perp$-labellings)

where $p \in AP^\perp$.

Thus, Lemma 1 Part (2) immediately follows from Lemma 3 where we distinguish the following cases:

Lemma 3
Let all definitions as in Theorem 1 and let $p \in AP^\perp$. Then the following holds:

(a) If for all instantiations $K^\perp(\overset{m}{a})$ of $K^\perp(\overset{m}{x})$ there exists a path $\pi^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \dots \pi_{k'}^\perp(\overset{m}{a}))$ with $\forall\, 1 \leq i < k' : R^\perp(\overset{m}{a})(\pi_i(\overset{m}{a}), \pi_{i+1}(\overset{m}{a})) = \mathit{true}$ and $L^\perp(\overset{m}{a})(\pi_{k'}^\perp(\overset{m}{a}), p) = \mathit{true}$, then there exists a path $\pi \in \Pi(K, s_1)$ and π is of the form $\pi = (\pi_1 \dots \pi_k)$ with $\forall\, 1 \leq i < k : R(\pi_i, \pi_{i+1}) = \mathit{true}$ and $L(\pi_k, p) = \mathit{true}$.

(b) If for all instantiations $K^\perp(\overset{m}{a})$ of $K^\perp(\overset{m}{x})$ there exists a path $\pi^\perp(\overset{m}{a}) \in \Pi(K^\perp(\overset{m}{a}), s_1^\perp)$ and $\pi^\perp(\overset{m}{a})$ is of the form $\pi^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \dots \pi_{l'-1}^\perp(\overset{m}{a})) \bullet (\pi_{l'}^\perp(\overset{m}{a}) \dots \pi_{k'}^\perp(\overset{m}{a}))^\omega$ with $\forall\, 1 \leq i < k' : R^\perp(\overset{m}{a})(\pi_i^\perp(\overset{m}{a}), \pi_{i+1}^\perp(\overset{m}{a})) = \mathit{true}$, $R^\perp(\overset{m}{a})(\pi_{k'}^\perp(\overset{m}{a}), \pi_{l'}^\perp(\overset{m}{a})) = \mathit{true}$ and $\forall\, l' \leq i \leq k' : L^\perp(\overset{m}{a})(\pi_i^\perp(\overset{m}{a}), p) = \mathit{false}$, then there exists a path $\pi \in \Pi(K, s_1)$ and π is of the form $\pi = (\pi_1 \dots \pi_{l-1}) \bullet (\pi_l \dots \pi_k)^\omega$ with $\forall\, 1 \leq i < k : R(\pi_i, \pi_{i+1}) = \mathit{true}$, $R(\pi_k, \pi_l) = \mathit{true}$ and $\forall\, l \leq i \leq k : L(\pi_i, p) = \mathit{false}$.

Proof. (Lemma 3)
Case (a): Without loss of generality we can assume that along each $\pi^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \dots \pi_{k'}^\perp(\overset{m}{a}))$ each transition and state occurs at most once. Otherwise $\pi^\perp(\overset{m}{a})$ must contain cycles $(\pi_t^\perp(\overset{m}{a}) \dots \pi_r^\perp(\overset{m}{a}))^n$ that are left after a finite number of n run-throughs. We can remove such cycles by replacing $\pi^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \dots \pi_r^\perp(\overset{m}{a})) \bullet (\pi_t^\perp(\overset{m}{a}) \dots \pi_r^\perp(\overset{m}{a}))^n \bullet (\pi_{r+1}^\perp(\overset{m}{a}) \dots \pi_k^\perp(\overset{m}{a}))$ by $\pi^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \dots \pi_r^\perp(\overset{m}{a}) \pi_{r+1}^\perp(\overset{m}{a}) \dots \pi_{k'}^\perp(\overset{m}{a}))$, which is still a path prefix with $\forall\, 1 \leq i < k' : R^\perp(\overset{m}{a})(\pi_i^\perp(\overset{m}{a}), \pi_{i+1}^\perp(\overset{m}{a})) = \mathit{true}$ and $L^\perp(\overset{m}{a})(\pi_{k'}^\perp(\overset{m}{a}), p) = \mathit{true}$. We denote such paths as a *single-occurrence prefixes.*

Each $K^\perp(\overset{m}{a})$ is an instantiation of $K^\perp(\overset{m}{x})$, where $K^\perp(\overset{m}{x})$ is a parameterisation of $K^\perp$ obtained by the application of Rule I and Rule II. Moreover, for each single-occurrence prefix $\pi^{\perp}$ in $K^{\perp}$ there exists a single-occurrence prefix π in K with $\forall\, i > 0 : R^{\perp}(\pi_i^{\perp}, \pi_{i+1}^{\perp}) = \mathit{true} \;\Rightarrow\; R(\pi_i, \pi_{i+1}) = \mathit{true} \,\wedge\, \forall\, p \in AP^{\perp} : L^{\perp}(\pi_i^{\perp}, p) \;\leq_{\mathbb{K}_3}\; L(\pi_i, p)$ (Proposition 1.2). A parameterisation of $K^{\perp}$ only substitutes certain *unknowns* with boolean expressions over the set of parameters $\{x_1, \ldots, x_m\}$. Thus, for each parameterised single-occurrence prefix $\pi^{\perp}(\overset{m}{x})$ in $K^{\perp}(\overset{m}{x})$ there exists a single-occurrence prefix π in K with $\forall\, i > 0 : R^{\perp}(\overset{m}{x})(\pi_i^{\perp}(\overset{m}{x}), \pi_{i+1}^{\perp}(\overset{m}{x})) = \mathit{true} \;\Rightarrow\; R(\pi_i, \pi_{i+1}) = \mathit{true} \,\wedge\, \forall\, p \in AP^{\perp} : \left(L^{\perp}(\overset{m}{x})(\pi_i^{\perp}(\overset{m}{x}), p) \;\leq_{\mathbb{K}_3}\; L(\pi_i, p) \,\vee\, L^{\perp}(\overset{m}{x})(\pi_i^{\perp}(\overset{m}{x}), p) = b\right)$ where b s a boolean expression over $\{x_1, \ldots, x_m\}$.

We now show that we can instantiate the parameters $\{x_1, \ldots, x_m\}$ with truth values $\{a_1, \ldots, a_m\}$ such that for each single-occurrence prefix $\pi^{\perp}(\overset{m}{a}) = (\pi_1^{\perp}(\overset{m}{a}) \ldots \pi_k^{\perp}(\overset{m}{a}))$ in $K^{\perp}(\overset{m}{a})$ there exists a single-occurrence prefix $\pi = (\pi_1 \ldots \pi_k)$ in K with $\forall\, 0 < i < k : R^{\perp}(\overset{m}{a})(\pi_i^{\perp}(\overset{m}{a}), \pi_{i+1}^{\perp}(\overset{m}{a})) = R(\pi_i, \pi_{i+1}) \,\wedge\, \forall\, p \in AP^{\perp} : L^{\perp}(\overset{m}{a})(\pi_i^{\perp}(\overset{m}{a}), p) = L(\pi_i, p)$. The explanation is as follows: If $K^{\perp}(\overset{m}{x})$ would be a parameterisation of $K^{\perp}$ where each parameterised predicate in a state and each parameterised transition is associated with an *individual* parameter, then there exists an instantiation $K^{\perp}(\overset{m}{a})$ such that for each single-occurrence prefix $\pi^{\perp}(\overset{m}{a}) = (\pi_1^{\perp}(\overset{m}{a}) \ldots \pi_k^{\perp}(\overset{m}{a}))$ there exists a single-occurrence prefix $\pi = (\pi_1 \ldots \pi_k)$ in K with $\forall\, 0 < i < k : R^{\perp}(\overset{m}{a})(\pi_i^{\perp}(\overset{m}{a}), \pi_{i+1}^{\perp}(\overset{m}{a})) = R(\pi_i, \pi_{i+1}) \,\wedge\, \forall\, p \in AP^{\perp} : L^{\perp}(\overset{m}{a})(\pi_i^{\perp}(\overset{m}{a}), p) = L(\pi_i, p)$. This immediately follows from Proposition 1 together with the definitions 5 and 6 from the submitted paper and the fact that we are only considering single-occurrence prefixes.

We still have to show, that this also holds for parameterisations obtained by the application of Rule I and Rule II, which means each parameterised predicate in state and each parameterised transition is now not necessarily associated with an individual parameter. The application of Rule I associates complementary branches with complementary expressions over the set of parameters. The application of Rule II associates predicates in different states with the same parameter as long as the value of the predicate does not change between this states. This generally reduces the amount of parameters and thus the amount of possible instantiations in comparison to an individual parameterisation. However, the application of the rules solely leads to the exclusion of infeasible behaviour (e.g. that both branches of an *if*-statement are executable at the same time) of the original system in the Kripke structure. Feasible behaviour of the original system will be never excluded by applying the rules, since the application of the rules always takes the systems original program code into account. Thus, for a parameterisation $K^{\perp}(\overset{m}{x})$ of $K^{\perp}$ obtained by the application of the rules I and II there must also exist an instantiation $K^{\perp}(\overset{m}{a})$ of $K^{\perp}(\overset{m}{x})$ such that for each single-occurrence prefix $\pi^{\perp}(\overset{m}{a}) = (\pi_1^{\perp}(\overset{m}{a}) \ldots \pi_k^{\perp}(\overset{m}{a}))$ there exists a single-occurrence prefix $\pi = (\pi_1 \ldots \pi_k)$ in K with $\forall\, 0 < i < k : R^{\perp}(\overset{m}{a})(\pi_i^{\perp}(\overset{m}{a}), \pi_{i+1}^{\perp}(\overset{m}{a})) = R(\pi_i, \pi_{i+1}) \,\wedge\, \forall\, p \in AP^{\perp} : L^{\perp}(\overset{m}{a})(\pi_i^{\perp}(\overset{m}{a}), p) = L(\pi_i, p)$.

Hence, there exists one instantiation $K^{\perp}(\overset{m}{a})$ that exactly characterises single-occurrence prefixes of K. We can conclude that if a single-occurrence prefix of the form $\pi^{\perp}(\overset{m}{a}) = (\pi_1^{\perp}(\overset{m}{a}) \ldots \pi_{k'}^{\perp}(\overset{m}{a}))$ with $\forall\, 1 \leq i < k' : R^{\perp}(\overset{m}{a})(\pi_i(\overset{m}{a}), \pi_{i+1}(\overset{m}{a})) =$

true and $L^\perp(\overset{m}{a})(\pi^\perp_{k'}(\overset{m}{a}), p) = \mathit{true}$ exists in *all* instantiations $K^\perp(\overset{m}{a})$ of $K^\perp(\overset{m}{x})$, then it also exists in the one instantiation that exactly characterises single-occurrence prefixes of K, which immediately implies that a path of the form $\pi = (\pi_1 \dots \pi_k)$ with $\forall\, 1 \leq i < k : R(\pi_i, \pi_{i+1}) = \mathit{true}$ and $L(\pi_k, p) = \mathit{true}$ exists in K.

This implies Lemma 3 (a) and thus ends this case of the proof.

Case (b): Lemma 3 (a) together with Proposition 1 guarantees us that for $K^\perp(\overset{m}{x})$ there must be one instantiation $K^\perp(\overset{m}{a})$ such that each single-occurrence prefix[1] $\pi^\perp(\overset{m}{a}) = (\pi^\perp_1(\overset{m}{a}) \dots \pi^\perp_k(\overset{m}{a})) \in \Pi(K^\perp(\overset{m}{a}), s^\perp_1)$ has a corresponding single-occurrence prefix $\pi = (\pi_1 \dots \pi_k) \in \Pi(K, s_1)$ with $\forall\, 0 < i < k : R^\perp(\overset{m}{a})(\pi^\perp_i(\overset{m}{a}), \pi^\perp_{i+1}(\overset{m}{a})) = R(\pi_i, \pi_{i+1}) \wedge \forall\, p \in AP^\perp : L^\perp(\overset{m}{a})(\pi^\perp_i(\overset{m}{a}), p) = L(\pi_i, p)$. We say, $\pi^\perp(\overset{m}{a})$ can be *simulated* in K by π. The reason why we can simulate single-occurrence prefixes but not necessarily infinite paths is that we have abstract states in $K^\perp(\overset{m}{a})$ (resp. in $K^\perp(\overset{m}{x})$ and in $K^\perp$). An abstract state $s^\perp_i(\overset{m}{a})$ of $K^\perp(\overset{m}{a})$ may characterise two (or more) concrete states s_i and s'_i in K (i.e. $\forall\, p \in AP^\perp : L^\perp(\overset{m}{a})(s^\perp_i(\overset{m}{a}), p) \leq_{\mathbb{K}_3} L(s_i, p)$ and $L^\perp(\overset{m}{a})(s^\perp_i(\overset{m}{a}), p) \leq_{\mathbb{K}_3} L(s'_i, p)$). Thus, for an infinite path $\pi^\perp(\overset{m}{a}) = (\pi^\perp_1(\overset{m}{a}) \dots \pi^\perp_{l-1}(\overset{m}{a})) \bullet (\pi^\perp_l(\overset{m}{a}) \dots \pi^\perp_k(\overset{m}{a}))^\omega$ in $K^\perp(\overset{m}{a})$ with $\forall\, 1 \leq i < k : R^\perp(\overset{m}{a})(\pi^\perp_i(\overset{m}{a}), \pi^\perp_{i+1}(\overset{m}{a})) = \mathit{true}$, $R^\perp(\overset{m}{a})(\pi^\perp_k(\overset{m}{a}), \pi^\perp_l(\overset{m}{a})) = \mathit{true}$, and $\forall\, l \leq i \leq k : L^\perp(\overset{m}{a})(\pi^\perp_i(\overset{m}{a}), p) = \mathit{false}$ where abstract states and transitions occur multiple times, we can assume that the simulation of $\pi^\perp(\overset{m}{a})$ in K is only possible for a finite number of runs through the $\neg p$-cycle $(\pi^\perp_l(\overset{m}{a}) \dots \pi^\perp_k(\overset{m}{a}))$. I.e. we will find a prefix $\pi^{\mathit{fin}} = (\pi_1 \dots \pi_{l-1}) \bullet (\pi_l \dots \pi_{i-1}\pi_i\pi_{i+1} \dots \pi_k)^n \bullet (\pi_l \dots \pi_{i-1}\pi'_i)$ in K with $n > 0$ and $l \leq i \leq k$ which is equivalent (wrt. transition values and labellings) to the prefix of $\pi^\perp(\overset{m}{a})$ of the same length, but there is no transition $R(\pi'_i, \pi_{i+1})$, i.e. no way to continue the simulation of $\pi^\perp(\overset{m}{a})$ in K. Evidently, π_i and π'_i must be two different concrete states that are characterised by the same abstract state $\pi^\perp_i(\overset{m}{a})$ in $K^\perp(\overset{m}{a})$ (resp. in $K^\perp(\overset{m}{x})$ and in $K^\perp$). The only reason why the simulation of $\pi^\perp(\overset{m}{a})$ cannot be continued in K after a finite number of runs through the $\neg p$-cycle, is that $R^\perp(\overset{m}{a})(\pi^\perp_i(\overset{m}{a}), \pi^\perp_{i+1}(\overset{m}{a}))$ corresponds to a parameterised transition in $K^\perp(\overset{m}{x})$ and $R(\pi_i, \pi_{i+1}) = \mathit{true}$ but $R(\pi'_i, \pi_{i+1}) = \mathit{false}$ in the concrete K. Parameterised transitions only arise due to the application of Rule I. Hence, we must have that $R^\perp(\overset{m}{x})(\pi^\perp_i(\overset{m}{x}), \pi^\perp_{i+1}(\overset{m}{x})) = b$ with $b \in \{x_1, \dots, x_m, \neg x_1, \dots, \neg x_m\}$ and there must be also a transition $R^\perp(\overset{m}{x})(\pi^\perp_i(\overset{m}{x}), \pi'^\perp_{i+1}(\overset{m}{x})) = \neg b$. Thus, the simulation of $\pi^\perp(\overset{m}{a})$ by $\pi^{\mathit{fin}} = (\pi_1 \dots \pi_{l-1}) \bullet (\pi_l \dots \pi_{i-1}\pi_i\pi_{i+1} \dots \pi_k)^n \bullet (\pi_l \dots \pi_{i-1}\pi'_i)$ cannot be continued by a concrete transition corresponding to $R^\perp(\overset{m}{x})(\pi^\perp_i(\overset{m}{x}), \pi^\perp_{i+1}(\overset{m}{x}))$ but there must be a some concrete state π'_{i+1} and a concrete transition $R(\pi'_i, \pi'_{i+1})$ corresponding to $R^\perp(\overset{m}{x})(\pi^\perp_i(\overset{m}{x}), \pi'^\perp_{i+1}(\overset{m}{x}))$ (i.e. with $\forall\, p \in AP^\perp : L^\perp(\overset{m}{x})(\pi'^\perp_{i+1}(\overset{m}{x}), p)$

[1] Along a single-occurrence prefix $\pi = (\pi_1 \dots \pi_k)$ of a Kripke structure K, each state and each transition of K occurs at most once.

$\leq_{K_3} L(\pi'_{i+1}, p))$ that we can take next: $\pi^{fin} = (\pi_1 \dots \pi_{l-1}) \bullet (\pi_l \dots \pi_{i-1}\pi_i\pi_{i+1} \dots \pi_k)^n \bullet (\pi_l \dots \pi_{i-1}\pi'_i\pi'_{i+1})$. From π^{fin} we can derive the loop-free single-occurrence prefix $\pi^{fin'} = (\pi_1 \dots \pi_{l-1}) \bullet (\pi_l \dots \pi_{i-1}\pi'_i\pi'_{i+1})$. $\pi^{fin'}$ hints at a partial instantiation $K^\perp(\overset{m_1}{a}, \overset{m_2}{x})$ of the parameterised Kripke structure $K^\perp(\overset{m}{x})$ such that there exists a prefix $\pi'^\perp(\overset{m_1}{a}, \overset{m_2}{x}) = (\pi_1^\perp(\overset{m_1}{a}, \overset{m_2}{x}) \dots \pi_{l-1}^\perp(\overset{m_1}{a}, \overset{m_2}{x})) \bullet (\pi_l^\perp(\overset{m_1}{a}, \overset{m_2}{x}) \dots \pi_{i-1}^\perp(\overset{m_1}{a}, \overset{m_2}{x})\pi_i'^\perp(\overset{m_1}{a}, \overset{m_2}{x})\pi_{i+1}'^\perp(\overset{m_1}{a}, \overset{m_2}{x}))$ with $\forall 0 < j <| \pi^{fin'} |$: $R^\perp(\overset{m_1}{a}, \overset{m_2}{x})(\pi_j^\perp(\overset{m_1}{a}, \overset{m_2}{x}), \pi_{j+1}^\perp(\overset{m_1}{a}, \overset{m_2}{x})) = R(\pi_j, \pi_{j+1}) \ \wedge \ \forall p \in AP^\perp : L^\perp(\overset{m_1}{a}, \overset{m_2}{x})(\pi_j^\perp(\overset{m_1}{a}, \overset{m_2}{x}), p) = L(\pi_j, p)$ in $K^\perp(\overset{m_1}{a}, \overset{m_2}{x})$. According to the prerequisite of this lemma, there must be a complete instantiation $K^\perp(\overset{m}{a})$ of $K^\perp(\overset{m_1}{a}, \overset{m_2}{x})$ such that $\pi'^\perp(\overset{m_1}{a}, \overset{m_2}{x})$ can be extended to an infinite path $\pi'^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \dots \pi_{l'-1}^\perp(\overset{m}{a})) \bullet (\pi_{l'}^\perp(\overset{m}{a}) \dots \pi_{k'}^\perp(\overset{m}{a}))^\omega$ with $\forall 1 \leq i < k' : R^\perp(\overset{m}{a})(\pi_i^\perp(\overset{m}{a}), \pi_{i+1}^\perp(\overset{m}{a})) = \mathit{true}$, $R^\perp(\overset{m}{a})(\pi_{k'}^\perp(\overset{m}{a}), \pi_{l'}^\perp(\overset{m}{a})) = \mathit{true}$, and $\forall l \leq i \leq k' : L^\perp(\overset{m}{a})(\pi_i^\perp(\overset{m}{a}), p) = \mathit{false}$, and for the finite unfolding $(\pi_1^\perp(\overset{m}{a}) \dots \pi_{l'-1}^\perp(\overset{m}{a})\pi_l^\perp(\overset{m}{a}) \dots \pi_{k'}^\perp(\overset{m}{a})\pi_{l'}^\perp(\overset{m}{a}))$ of $\pi'^\perp(\overset{m}{a})$ there exists an equivalent single-occurrence prefix $(\pi_1 \dots \pi_{l'-1}\pi_{l'} \dots \pi_k\pi_{l'})$ in K. Either this single-occurrence prefix can be extended to the infinite path $\pi' = (\pi_1 \dots \pi_{l'-1}) \bullet (\pi_{l'} \dots \pi_{k'})^\omega$ in K, which means the lemma is proven. Or the prefix can only be extended to a prefix $\pi'^{fin} = (\pi_1 \dots \pi_{l'-1}) \bullet (\pi_{l'} \dots \pi_{i-1}\pi_i\pi_{i+1} \dots \pi_{k'})^n \bullet (\pi_{l'} \dots \pi_{i-1}\pi'_i)$ with $n > 0$ and $l' \leq i \leq k'$, but the simulation of the infinite path $\pi'^\perp(\overset{m}{a})$ of $K^\perp(\overset{m}{a})$ cannot be further continued in K. Then we can (repetitively) extend π'^{fin} as we have done it before to get π'^{fin} out of π^{fin}. After a finite number of repetitions, we will get a prefix that can be actually extended to an infinite path $\pi' = (\pi_1 \dots \pi_{l'-1}) \bullet (\pi_{l'} \dots \pi_{k'})^\omega$ in K, which means the lemma is proven. Otherwise there would exist a complete instantiation $K^\perp(\overset{m}{a})$ where no path $\pi^\perp(\overset{m}{a}) = (\pi_1^\perp(\overset{m}{a}) \dots \pi_{l-1}^\perp(\overset{m}{a})) \bullet (\pi_l^\perp(\overset{m}{a}) \dots \pi_k^\perp(\overset{m}{a}))^\omega \in \Pi(K^\perp(\overset{m}{a}), s_1^\perp)$ with $\forall 1 \leq i < k : R^\perp(\overset{m}{a})(\pi_i^\perp(\overset{m}{a}), \pi_{i+1}^\perp(\overset{m}{a})) = \mathit{true}$, $R^\perp(\overset{m}{a})(\pi_k^\perp(\overset{m}{a}), \pi_l^\perp(\overset{m}{a})) = \mathit{true}$, and $\forall l \leq i \leq k : L^\perp(\overset{m}{a})(\pi_i^\perp(\overset{m}{a}), p) = \mathit{false}$ exists - which however is be a contradiction to the prerequisite of Lemma 3 (b).

This implies Lemma 3 (b) and thus ends the proof of Lemma 3. Lemma 2 together with Lemma 3 establishes the correctness of Lemma 1 (a) and (b).
□

We now can immediately conclude that Theorem 1 holds.
□

Proof of Theorem 2

In the following we prove Theorem 2 from Section 6. We show that our algorithm *CheckFG(p)* is correct in the sense that for a parameterised three-valued Kripke structure $M(\overset{m}{x}) = (S, s_0, R, L)$ over AP with $p \in AP$ as input, its output corresponds to the result of checking $[M(\overset{m}{x}) \models_{\exists} \mathbf{FG}p]$. Our proof makes use of the following auxiliary definition:

Definition 8 (Path Constraint)
Let $M(\overset{m}{x}) = (S, s_0, R, L)$ be a parameterised three-valued Kripke structure over AP and X. Moreover, let $p \in AP$ and π be a path of the form $(s_0 \ldots s_{l-1}) \bullet (s_l \ldots s_k)^{\omega}$ in $M(\overset{m}{x})$. Then the path constraint *of π is defined as*

$$constraint(\pi) = \bigwedge_{i=0}^{k-1} R(s_i, s_{i+1}) \wedge \bigwedge_{i=l}^{k} L(s_i, p).$$

Hence, we extend our notion of propositional logic constraints to entire paths of Kripke structures, whereas in Section 6 we only defined and used this constraints for single states and strongly connected components. The theorem that we prove is the following:

Theorem 2
Let $M(\overset{m}{x}) = (S, s_0, R, L)$ be a parameterised three-valued Kripke structure over AP and X. Moreover, let $p \in AP$. Then after the termination of the algorithm CheckFG(p) *with input $M(\overset{m}{x})$ the following holds:*

$$\left[M(\overset{m}{x}) \models_{\exists} \mathbf{FG}p\right] = \begin{cases} \mathit{true} & \mathit{iff}\ \ constraint(s_0)\ \mathit{is\ tautological} \\ \mathit{false} & \mathit{iff}\ \ constraint(s_0)\ \mathit{is\ unsatisfiable} \\ \bot & \mathit{otherwise} \end{cases}$$

Proof. (Theorem 2)
We prove Theorem 2 by showing the following:

- $[M(\overset{m}{x}) \models_{\exists} \mathbf{FG}p] = \mathit{true}$ iff $constraint(s_0)$ is tautological *(Theorem 2.1)*

- $[M(\overset{m}{x}) \models_{\exists} \mathbf{FG}p] = \mathit{false}$ iff $constraint(s_0)$ is unsatisfiable *(Theorem 2.2)*

Proof. (Theorem 2.1)
The proof of Theorem 2.1 is as follows. We start with the following equivalent transformations.

$[M(\overset{m}{x}) \models_{\exists} \mathbf{FG}p] = \mathit{true}$ iff $\mathit{constraint}(s_0)$ is tautological

$\Leftrightarrow$ For all instantiations $M(\overset{m}{a})$ of $M(\overset{m}{x})$ there exists a path of the form $\pi = (s_0 \ldots s_{l-1}) \bullet (s_l \ldots s_k)^{\omega}$ in $M(\overset{m}{a})$ with $\forall\, 0 \leq i < k :$ $R(\overset{m}{a})(s_i, s_{i+1}) = \mathit{true}$ and $\forall\, l \leq i \leq k : L(\overset{m}{a})(s_i, p) = \mathit{true}$
iff
$\mathit{constraint}(s_0)$ is tautological

$\Leftrightarrow$ For all interpretations $I : X \rightarrow \{\mathit{true}, \mathit{false}\}$ of X there exists a path $\pi = (s_0 \ldots s_{l-1}) \bullet (s_l \ldots s_k)^{\omega}$ in $M(\overset{m}{x})$ with $I(\mathit{constraint}(\pi)) = \mathit{true}$
iff
for all interpretations $I : X \rightarrow \{\mathit{true}, \mathit{false}\} : I(\mathit{constraint}(s_0)) = \mathit{true}$

The correctness of this assertion now immediately follows from Lemma 4.

Lemma 4
Let $M(\overset{m}{x}) = (S, s_0, R, L)$ be a parameterised three-valued Kripke structure over AP and X. Moreover, let $I : X \rightarrow \{\mathit{true}, \mathit{false}\}$ be an arbitrary interpretation of X. Then the following holds:

1. *Let π be an arbitrary path of the form $(s_0 \ldots s_{l-1}) \bullet (s_l \ldots s_k)^{\omega}$ in $M(\overset{m}{x})$ with $I(\mathit{constraint}(\pi)) = \mathit{true}$. Then $I(\mathit{constraint}(s_0)) = \mathit{true}$ after the termination of* CheckFG(p).
2. *If $I(\mathit{constraint}(s_0)) = \mathit{true}$ after the termination of* CheckFG(p), *then there exists a path $\pi = (s_0 \ldots s_{l-1}) \bullet (s_l \ldots s_k)^{\omega}$ with $I(\mathit{constraint}(\pi)) = \mathit{true}$.*

Proof. (Lemma 4.1)
Our premise is $I(\mathit{constraint}(\pi)) = \mathit{true}$. Consequently, for all transitions (s, s') along the path π with $R(s, s') \in BE(X)$ we have that $I(R(s, s')) = \mathit{true}$, and for all states s along the strongly connected component C formed by $(s_l \ldots s_k)^{\omega}$ with $L(s, p) \in BE(X)$ we have that $I(L(s, p)) = \mathit{true}$ (Definition 8). Hence, after the execution of the lines 1 to 13 we have that $I(\mathit{constraint}(C)) = \mathit{true}$ and for all states s along C we have that $I(\mathit{constraint}(s)) = \mathit{true}$. After line 14, all states of C, in particular the state s_l, will be contained in the set T. Thus, during the execution of the *while*-loop, s_l will be eventually chosen in line 16. Consequently, s_l's predecessor state s_{l-1} along π will be contained in the set T' (line 18) and eventually selected in line 19. Now we distinguish the following mutually exclusive cases:

Case (a) The *if*-condition in line 20 holds, which means we have that $\neg(R(s_{l-1}, s_l) \wedge \mathit{constraint}(s_l)) \Rightarrow \mathit{constraint}(s_{l-1})$. Then $\mathit{constraint}(s_{l-1})$ is updated: $\mathit{constraint}(s_{l-1}) := \mathit{constraint}(s_{l-1}) \vee (R(s_{l-1}, s_l) \wedge \mathit{contstraint}(s_l))$. Now $I(\mathit{constraint}(s_{l-1})) = \mathit{true}$, since we already have that $I(R(s_{l-1}, s_l)) = \mathit{true}$ and $I(\mathit{contstraint}(s_l)) = \mathit{true}$. After the update of $\mathit{constraint}(s_{l-1})$ the state s_{l-1} will be added to the set T (line 22). If s_{l-1} is already the initial state of π we have that $I(constraint(s_0)) = true$, which completes the proof of Lemma 4.1.

Otherwise, in a later iteration of the *while*-loop the state s_{l-1} will be chosen from T in line 16 and its predecessor s_{l-2} will be contained in the set T' (line 18) and eventually selected in line 19. Now we can distinguish the cases (a) and (b) again with $l := l - 1$.

Case (b) The *if*-condition in line 20 does not hold, which means we have that $(R(s_{l-1}, s_l) \wedge constraint(s_l)) \Rightarrow constraint(s_{l-1})$. Since we already have that $I(R(s_{l-1}, s_l)) = true$ and $I(contstraint(s_l)) = true$, the premise of (b) allows us to conclude that $contstraint(s_{l-1}) \neq false$ and $I(contstraint(s_{l-1})) = true$. If s_{l-1} is already the initial state of π we have that $I(constraint(s_0)) = true$, which completes the proof of Lemma 4.1.

The body of the *if*-condition will not be executed, which means the state s_{l-1} is *not* added to the set T. However, since $constraint(s_{l-1})$ was initialised with *false* in line 3 and the premise of Case (b) implies that $constraint(s_{l-1}) \neq false$, $contstraint(s_{l-1})$ must have been updated and the state s_{l-1} must have been added to T at some point in the past. (Update and addition to T either had happened in lines 13 and 14, or in lines 21 and 22.) Thus, in some iteration of the *while*-loop the state s_{l-1} will be chosen from T in line 16 and its predecessor s_{l-2} will be contained in the set T' (line 18) and eventually selected in line 19. Now we can distinguish the cases (a) and (b) again with $l := l - 1$.

Proof. (Lemma 4.2)
We show that under the premise $I(constraint(s_0)) = true$ such a path π can be gradually constructed (i.e. found) in $M(\overset{m}{x})$. We initialise $\pi := (s_0)$, i.e. the finite prefix consisting of the state s_0. Moreover, we initialise a state variable $s_l := s_0$.

In accordance with the algorithm *CheckFG(p)*, $constraint(s_l)$ will be of the following form after termination: $constraint(s_l) = false \vee constraint(C_1) \vee \ldots \vee constraint(C_n) \vee (R(s_l, s_1) \wedge constraint(s_1)) \vee \ldots \vee (R(s_l, s_m) \wedge constraint(s_m))$ where $C_1, \ldots, C_n \in SCC$ and $s_1, \ldots, s_m \in S$. Our premise is $I(constraint(s_l)) = true$. Hence, there must exist a $C_i \in \{C_1, \ldots, C_n\}$ with $I(constraint(C_i)) = true$ or there must exist an $s_j \in \{s_1, \ldots s_m\}$ with $I(R(s_l, s_j) \wedge constraint(s_j)) = true$. Thus, at least one of the following cases holds:

Case (a) There exists a strongly connected component $C_i \in \{C_1, \ldots, C_n\}$ with $I(constraint(C_i)) = true$. Then s_l is a state along C_i. Let $s_l, \ldots, s_k$ be the states of C_i such that the sequence $(s_l \ldots s_k)$ forms a cycle $(s_l \ldots s_k)^\omega$ in $M(\overset{m}{x})$. Let the current prefix π be $\pi = \pi' \bullet (s_l)$. Then we set $\pi := \pi' \bullet (s_l \ldots s_k)^\omega$. We get that $I(constraint(\pi)) = true$ (Definition 8), which completes the proof of Lemma 4.2.

Case (b) There exists an $s_j \in \{s_1, \ldots s_m\}$ with $I(R(s_l, s_j) \wedge constraint(s_j)) = true$. The current π is a finite prefix whose last state is s_l. Now we set

$\pi := \pi \bullet (s_j)$ We get that for all transitions (s, s') along π : $I(R(s, s')) = true$. We set $s_l := s_j$. For the updated state s_l we again have that $I(constraint(s_l)) = true$ and $constraint(s_l)$ is of the form $constraint(s_l) = false \vee constraint(C_1) \vee \ldots \vee constraint(C_n) \vee (R(s_l, s_1) \wedge constraint(s_1)) \vee \ldots \vee (R(s_l, s_m) \wedge constraint(s_m))$ where $C_1, \ldots, C_n \in SCC$ and $s_1, \ldots, s_m \in S$. For the updated s_l we now distinguish the cases (a) and (b) as before.

Eventually Case (a) must hold because of the following: $constraint(s_l)$ and all other state constraints are initialised with *false* in *CheckFG(p)* (line 3). During the execution of the algorithm the state constraints are updated in line 13 and in line 21. In line 21 the updates happen dependent on other state constraints. Thus, if all updates of $constraint(s_l)$ and its subformulae would be based on line 21, then $constraint(s_l)$ would be still *false* after termination. In line 13 the updates happen dependent on constraints of strongly connected components. Since we have that $I(constraint(s_l)) = true$ and thus $constraint(s_l) \neq false$, $constraint(s_l)$ or a subformulae must have been updated dependent on the constraint of a strongly connected component C_i in line 13. Hence, at one point of our construction of π Case (a) will hold.

Proof. (Theorem 2.2)
The proof of Theorem 2.2 is as follows. We start with the following equivalent transformations.

$[M(\overset{m}{x}) \models_\exists \mathbf{FG}p] = false$ iff $constraint(s_0)$ is unsatisfiable

$\Leftrightarrow$ For all instantiations $M(\overset{m}{a})$ of $M(\overset{m}{x})$ there exists no path of the form $\pi = (s_0 \ldots s_{l-1}) \bullet (s_l \ldots s_k)^\omega$ in $M(\overset{m}{a})$ with $\forall\, 0 \leq i < k$: $R(\overset{m}{a})(s_i, s_{i+1}) = true$ and $\forall\, l \leq i \leq k : L(\overset{m}{a})(s_i, p) = true$
iff
$constraint(s_0)$ is unsatisfiable

$\Leftrightarrow$ For all interpretations $I : X \rightarrow \{true, false\}$ of X and all paths of the form $\pi = (s_0 \ldots s_{l-1}) \bullet (s_l \ldots s_k)^\omega$ in $M(\overset{m}{x}) : I(constraint(\pi)) = false$
iff
for all interpretations $I : X \rightarrow \{true, false\} : I(constraint(s_0)) = false$

The correctness of this assertion now immediately follows from Lemma 5.

Lemma 5
Let $M(\overset{m}{x}) = (S, s_0, R, L)$ be a parameterised three-valued Kripke structure over AP and X. Moreover, let $I : X \rightarrow \{true, false\}$ be an arbitrary interpretation of X. Then the following holds:

1. *If $I(constraint(\pi)) = false$ for all paths π of the form $(s_0 \ldots s_{l-1}) \bullet (s_l \ldots s_k)^\omega$ in $M(\overset{m}{x})$, then $I(constraint(s_0)) = false$ after the termination of* CheckFG(p).

2. *If $I(constraint(s_0)) = false$ after the termination of* CheckFG(p), *then $I(constraint(\pi)) = false$ for all paths π of the form $(s_0 \dots s_{l-1}) \bullet (s_l \dots s_k)^\omega$ in $M(\overset{m}{x})$.*

Proof. (Lemma 5)
Lemma 5 is an immediate consequence of Lemma 6.

Lemma 6
Let $M(\overset{m}{x}) = (S, s_0, R, L)$ be a parameterised three-valued Kripke structure over AP and X. Moreover, let $I : X \rightarrow \{true, false\}$ be an arbitrary interpretation of X. Then the following holds:

1. *If $I(constraint(s_0)) \neq false$ after the termination of* CheckFG(p), *then there exists a path $\pi = (s_0 \dots s_{l-1}) \bullet (s_l \dots s_k)^\omega$ with $I(constraint(\pi)) \neq false$.*
2. *Let π be an arbitrary path of the form $(s_0 \dots s_{l-1}) \bullet (s_l \dots s_k)^\omega$ in $M(\overset{m}{x})$ with $I(constraint(\pi)) \neq false$. Then $I(constraint(s_0)) \neq false$ after the termination of* CheckFG(p).

Proof. (Lemma 6)
The proof of Lemma 6.1 is analogous to the proof of Lemma 4.2 and the proof of Lemma 6.2 is analogous to the proof of Lemma 4.1.

This completes the proof of Theorem 2.