Solving Finite-Linear-Path CTL-Formulas Using the CEGAR Approach

Torsten Liebke(✉) and Karsten Wolf

Universität Rostock, Institut für Informatik, Rostock, Germany
{torsten.liebke,karsten.wolf}@uni-rostock.de

Abstract. Petri nets are an established formal method for modelling and verifying asynchronous, concurrent and distributed systems. To verify a specification, given as a temporal logic formula, state space methods often encounter the state space explosion problem. We propose a verification technique to solve the CTL query E (ϕ U ψ) using the *Petri net state equation* with a *counterexample guided abstraction refinement* (CEGAR) approach. As a side product we show that $(\text{EX})^k\phi$ formulas can be solved with the CEGAR approach as well. We use these special formulas as building bricks to solve the class of finite-linear-path CTL-formulas. The proposed techniques are strong at invalidating infeasible behaviour. In addition to this it will often terminate quickly. We are also introducing quick-checks for solving EG ϕ under certain circumstances.

Keywords: Petri nets · Verification · Structural analysis · CEGAR · ILP

1 Introduction

Explicit model checking algorithms encounter the state space explosion problem. A different concept to verify the reachability problem was introduced in [8] and extended by [3,4]. This concept is based on the structure of Petri nets and decreases the state space explosion problem significantly. It transforms the problem to an integer linear programming (ILP) problem, which runs iteratively based on counterexample guided abstraction refinement, proposed in [2].

Due to the fact that ILP-problems can become infeasible, the CEGAR approach is especially good to verify negative results. This makes it a valuable complement to explicit model checking algorithms, which are in general good for verifying positive results, due to the on-the-fly effect.

In [6] it is shown that it is beneficial to use specialized routines for common formulas to increase the number of verifiable problems. We propose two techniques to solve the CTL queries E(ϕ U ψ) and $(\text{EX})^k\phi$ with the CEGAR approach for Petri nets. Using well known tautologies, also A(ϕ R ψ) and $(\text{AX})^k\phi$ are solvable with these techniques. [6] also shows that only 62.3% of the E(ϕ U ψ)/A(ϕ R ψ) formulas from the Model Checking Contest 2018 [1] are solved using the explicit model checker LoLA 2 [9]. This is due to the reason that the

M. Koutny et al. (Eds.): ToPNoC XV, LNCS 12530, pp. 150–164, 2021.
https://doi.org/10.1007/978-3-662-63079-2_7

on-the-fly effect has no or very limited impact in some cases, e.g. when $\phi \wedge \neg\psi$ holds in the entire state space. For this case, the CEGAR approach we are introducing will terminate very quickly, stating that the ILP-problem is infeasible and thus the result of the formula is false.

We use these specialized routines as building bricks to solve a much bigger class of formulas, namely the finite-linear-path CTL-formulas. This class is characterized by two facts: First, the formulas are ending in a final marking, hence, they are finite and secondly, they have a linear witness path without branching. Using tautologies we can again check both the existential and the universal finite-linear-path formulas.

One drawback is that termination of the introduced approach is not guaranteed, which makes the procedure incomplete [8]. This drawback vanishes if a portfolio approach is applied where traditional algorithms are combined with the newly introduced methods.

We also introduce some quick-checks for verifying EG ϕ using the presence of deadlocks or the absence of certain transition invariants.

2 Basic Definitions

We consider place/transition Petri nets.

Definition 1 (place/transition net). *A* place/transition net $[P, T, F, W, m_0]$ *consists of a finite set* P *of* places*, a finite set* T *of* transitions*, a set* $F \subseteq (P \times T) \cup (T \times P)$ *of* arcs*, a mapping* $W : (P \times T) \cup (T \times P) \longrightarrow \mathbb{N}$ *where* $[x, y] \notin F$ *if and only if* $W([x, y]) = 0$*, and an* initial marking m_0*. A* marking *is a mapping* $m : P \longrightarrow \mathbb{N}$*.*

Transition t *is* enabled *in marking* m *if, for all* $p \in P$*,* $m(p) \geq W([p, t])$*. Firing an enabled transition in* m *yields the marking* m' *where, for all* p*,* $m'(p) = m(p) - W([p, t]) + W([t, p])$*. This is denoted* $m \xrightarrow{t} m'$*.*

Every Petri net defines a labeled transition system where the set of markings reachable from m_0 form the set of states, m_0 is the initial state, and the firing relation just defined forms the labeled transition relation. We restrict our considerations to Petri nets where the related transition system is finite.

The *incidence matrix* of a Petri net N is a matrix $C_N : P \times T \longrightarrow \mathbb{Z}$ where, for all $p \in P, t \in T$, $C_N(p, t) = W(t, p) - W(p, t)$. The incidence matrix is involved in important and well-known results of Petri net theory. If it is clear to which Petri net the incidence matrix belongs then we only write C.

Definition 2 (Reachability problem). *Given is a tuple* (N, m, m') *consisting of a Petri net* N *and two markings* m, m'*. A marking* m' *is* reachable *from marking* m *in a Petri net* N*, if there exists a firing sequence* $w \in T^*$ *with* $m \xrightarrow{w} m'$*. The set of all reachable markings in* N *starting in* m *is written as* $R_N(m)$*. The question whether* $m' \in R_N(m)$ *is called the* reachability problem*.*

The feasibility of the Petri net state equation is a necessary condition for a positive answer to this question.

Proposition 1 (Petri net state equation). *Let $w \in T^*$ be a firing sequence of N, that is, the sequence of labels on a path from some marking m to a marking m' in the transition system corresponding to N. Then it holds*

$$m + C \cdot \wp(w) = m'$$

where $\wp(w)$ is a vector and $|\wp(w)(t)|$ is the number of occurrences of t in the sequence w.

In the sequel, we shall refer to $\wp(w)$ as the *Parikh vector* of w.

Definition 3 (T-invariant). *A Parikh vector $\wp(w)$ is called a T-*invariant *if $C \cdot \wp(w) = \mathbf{0}$. If the firing sequence w is executable, we call $\wp(w)$ realizable.*

A realizable T-invariant is a cycle in the state space and will not change the marking.

Definition 4 (Solution space). *The solution of the Petri net state equation $m + C \cdot \wp(w) = m'$ can be written as the sum of a base solution and a period vector, which is a linear combination of T-invariants: $\wp(w) = b + \sum_i n_i y_i$, where $b \in \mathbb{N}^T$ is the base solution and $n_i \in \mathbb{N}$ is the coefficient of the T-invariant $y_i \in \mathbb{N}^T$ [3,8].*

3 Increasing and Decreasing Transitions

Consider a formal sum $s = k_1 p_1 + \cdots + k_n p_n$, which we also call atomic proposition. Every marking m turns this sum into the integer number $v_s(m) = k_1 m(p_1) + \cdots + k_n m(p_n)$. We can immediately derive from the firing rule of Petri nets:

Definition 5 (Delta). *Let s be a formal sum and t a transition, then $\Delta_{t,s}$ is defined as $\Delta_{t,s} = k_1 C(p_1, t) + \cdots + k_n C(p_n, t)$.*

Lemma 1. *For all markings m, $m \xrightarrow{t} m'$ implies $v_s(m) + \Delta_{t,s} = v_s(m')$.*

Proof. Apply the Petri net state equation. □

As we assume the transition system to be finite, there is only a finite range of values that $v_s(m)$ can take. Call an integer number k a *lower bound* for formal sum s if, for any reachable marking m, $v_s(m) \geq k$, and *upper bound* for s if, for any reachable m, $v_s(m) \leq k$. There exist several approaches in Petri net theory for computing bounds. As an example, we can solve the following optimisation problem where s is the objective function (to be minimised or maximised) and the state equation serves as side condition. If the problem yields a solution with non-diverging value for the objective function, that value is a lower (resp. upper) bound for s.

Based on Lemma 1, we can identify increasing and decreasing transitions.

Definition 6 (Increasing, decreasing). *Given an atomic proposition of the form $s \leq k$. Let L be a lower bound and U an upper bound for s. We call transition t w.r.t. the formal sum s:*

1. weakly increasing *iff* $\Delta_{t,s} < 0$
2. weakly decreasing *iff* $\Delta_{t,s} > 0$
3. strongly increasing *iff there is an upper bound U for s where $\Delta_{t,s} \leq k - U$*
4. strongly decreasing *iff there is a lower bound L for s where $\Delta_{t,s} > k - L$.*

The terminology may sound strange at first glance. However, increasing transitions have the tendency to turn a false proposition into a true one while decreasing transitions help turning a true proposition into a false one.

Let $p \leq 0$ be an atomic proposition where p is the number of tokens on place p in a Petri net. Then all transitions in the preset of p are strongly decreasing.

Lemma 2. *Consider markings m and m', transition t with $m \xrightarrow{t} m'$ and atomic proposition $s \leq k$.*

1. If $s \leq k$ is false in m and true in m' then t is weakly increasing w.r.t. s.
2. If $s \leq k$ is true in m and false in m' then t is weakly decreasing w.r.t. s.
3. If t is strongly increasing w.r.t. $s \leq k$ then $s \leq k$ is true in m'.
4. If t is strongly decreasing w.r.t. $s \leq k$ then $s \leq k$ is false in m'.

Proof. Regarding 1, we have $v_s(m) > k$ and $v_s(m') \leq k$. By Lemma 1, we conclude $\Delta_{t,s} < 0$. Regarding 3, we have $v_s(m) \geq L$ (since L is a lower bound). Hence, $v_s(m') = v_s(m) + \Delta_{t,s} \leq L + \Delta_{t,s}$ and, according to Definition 6, $v_s(m') \leq k$. □

4 CEGAR Approach for Reachability Analysis in Petri Nets

Abstraction is a powerful method for verifying systems. It omits irrelevant details of the system behaviours, to simplify the analysis and verification. Finding the right abstraction is hard. If it is too coarse, the verification might fail and if it is too fine, the state space explosion problem might occur. A solution is to use some initial abstraction [2], which is an overapproximation of the original system and then iteratively refine the abstraction based on spurious counterexamples.

In our case, the Petri net state equation is the initial abstraction for the reachability problem. Solving the state equation is a non-negative integer linear programming problem. The objective function for the ILP-problem is the shortest firing sequence of the Parikh vector $f(w) = \sum_{t \in T} |\wp(w)(t)|$ leading from the initial marking m to the final marking m'.

The feasibility of this linear system is a necessary condition for reachability, but not a sufficient one. We distinguish between three different situations:

- If the linear system is infeasible, the necessary condition is violated and the final marking is not reachable.

- If the linear system has a realizable solution, then the final marking is reachable.
- If the linear system has an unrealizable solution, which is a counterexample, then the abstraction has to be refined.

If we have an unrealizable solution, then there exists at least one $t \in T$ which fired less than $|\wp(w)(t)|$ times. To produce a new solution which avoids the spurious one, we build a refined abstraction using inequalities for the ILP-problem.

Definition 7 (Constraints). *We define two types of constraints, both being linear inequalities over transitions [8].*

- *Jump constraints have the form $|t_i| < n$, with $n \in \mathbb{N}$ and $t_i \in T$ where $|t_i|$ represents the firing count of transition t. Using the fact that base solutions are pairwise incomparable, jump constraints intend to generate a new base solution.*
- *Increment constraints have the form $\sum_{i=1}^{k} n_i|t_i| \geq n$ with $n_i \in \mathbb{Z}$, $n \in \mathbb{N}$, and $t_i \in T$. Increment constraints are used to get a new non-base solution, i.e., T-invariants are added, since their interleaving with another sequence w may turn w from unrealizable to realizable.*

Adding the two types of constrains to existing solutions we can traverse through the solution space and check whether the unrealizable solution of our linear system becomes realizable or whether the ILP-problem becomes infeasible.

Definition 8 (Partial solutions). *Let $N = (P, T, F, W, m)$ be a Petri net and $m' \in R_N(m)$ a reachability problem. A* partial solution *is a tuple $ps = (\Gamma, \wp(w), \sigma, r)$ with:*

- *Γ is the set of jump and increment constraints. Together with the state equation they form the ILP-problem.*
- *$\wp(w)$ is the minimal solution fulfilling the ILP-problem.*
- *σ is a firing sequence with $m \xrightarrow{\sigma}$ and $\wp(\sigma) \leq \wp(w)$.*
- *r is the remainder with $r = \wp(w) - \wp(\sigma)$ and $\forall t \in T : (r(t) > 0 \Longrightarrow \neg m \xrightarrow{\sigma t})$.*

Partial solutions are produced during the examination of the solution $\wp(w)$ of the ILP-problem by exploring the state space of N. For this an explicit model checking algorithm with reachability preserving stubborn sets [7] can be used to build a tree of reachable markings, such that for all transitions $t \in T$ it holds that they only occur $|\wp(w)(t)|$ times. Stubborn sets, which are concerned with only one ordering of transitions, are very useful here, to avoid the explosion of the solution space. Each path to a leaf represents a maximal firing sequence of a new partial solution. If a partial solution has an empty remainder $r = 0$, it is a full solution and the reachability problem is satisfied. If no full solution exists, $\wp(w)$ might be realizable by another firing sequence σ', or by adding a jump constraint to get to a new base solution, or by adding an increment constraint to get additional tokens for transitions with $r(t) > 0$. If all possible partial solutions are explored and no full solution is found, the reachability problem can not be satisfied.

Theorem 1 (Reachability of solutions). *If the reachability problem has a solution, a realizable solution of the state equation can be reached by constantly appending the minimal solution with constraints [8].*

As stated in [3] it is an open question, whether this procedure always terminates.

5 Solving E (ϕ U ψ) with the CEGAR Approach

Definition 9 (E(ϕ U ψ)). *Let $N = (P, T, F, W, m)$ be a Petri net and ϕ and ψ two propositions. $m \models \mathrm{E}(\phi \text{ U } \psi) \iff \exists w \in T^* : m \xrightarrow{w} m'$, with $\exists i \in \mathbb{N}\ \forall j < i : (m_j \models \phi) \wedge (m_i \models \psi)$. Which means that in every state along path w, ϕ is true until a state is reached where ψ is true.*

It is well known that EF ψ can be rewritten as E (true U ψ). To solve E(ϕ U ψ), where ϕ and ψ are atomic propositions, we solve EF ψ with the CEGAR approach. In addition to this we introduce additional (balance) constraints to keep ϕ true along the path. Furthermore we cut-off paths in the exploration of partial solutions, whenever states are reached where both ϕ and ψ are false.

Definition 10 (Balance constraints). *Given a Petri net $N = (P, T, F, W, m)$ and an atomic proposition ψ and $\phi = s_0 \leq k_0 \wedge s_1 \leq k_1 \wedge \cdots \wedge s_n \leq k_n$, where s_i is a formal sum, $0 \leq i \leq n$ and $i, k, n \in \mathbb{N}$. $T_i = \{t \in T | \Delta_{t,s_i} \neq 0\}$ is the set of transitions which can change the value of s_i. It contains all weakly/strongly increasing/decreasing transitions w.r.t. to s_i. We call $T_{i,\psi} \subseteq T_i$ the set of decreasing transitions w.r.t s_i, which are at the same time increasing w.r.t ψ: $T_{i,\psi} = \{t \in T_i | \Delta_{t,s_i} > 0 \wedge \Delta_{t,\phi} < 0\}$. We define variables δ_i, which are 0, if $T_{i,\psi} = \emptyset$ and otherwise are $MAX(\Delta_{t,s_i} | t \in T_{i,\psi})$. The δ_i-offset is the maximum arc weight of all transitions that can change the value of $s_i \leq k_i$ from true to false and ψ from false to true. Let $\theta_i = k_i - v_{s_i}(m)$ be the offset, which is the number of tokens that can be consumed from the initial marking and still leave the truth value of $s_i \leq k_i$ unchanged. We call $\forall s_i : \sum_{t \in T_i} \Delta_{t,s_i} \leq \theta_i + \delta_i$* balance constraints *w.r.t. s_i and m.*

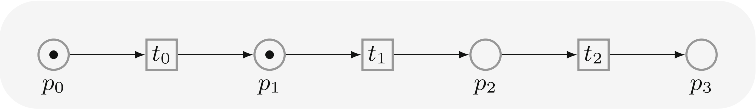

Fig. 1. The minimal solution for this Petri net and the formula E ($p_1 > 0$) U ($p_3 > 0$) is $t_1 t_2$. Since t_1 is weakly decreasing w.r.t. $p_1 > 0$, the balance constraint adds the weakly increasing transition t_0 to the solution.

As an example, consider Fig. 1 and the formula E ($p_1 > 0$) U ($p_3 > 0$). Note that this formula and every other formula can be rewritten into the required

$s \leq k$-format: E $(-p_1 \leq -1)$ U $(-p_3 \leq -1)$. To satisfy the formula, we check EF $p_3 > 0$, while keeping $p_1 > 0$ true along the path. The minimal solution to the ILP would be the firing vector (t_1, t_2), $m \xrightarrow{t_1 t_2} m'$, where m' satisfies $p_3 > 0$. But after firing the weakly decreasing transition t_1 w.r.t. $p_1 > 0$, a marking $m'' = (p_0, p_2)$ is reached that does neither satisfy $p_3 > 0$ nor $p_1 > 0$. To avoid this marking, the balance constraint would add the weakly increasing transition t_0 to the solution vector, $m \xrightarrow{t_0 t_1 t_2} m'$, to keep $p_1 > 0$ true.

Balance constraints in general ensure that the sum of all increasing and decreasing transitions w.r.t. a formal sum s is smaller than the offset, which is based on the initial marking and the maximal arc weight of all transitions $t \in T_{i,\psi}$. In case the offset θ_i is negative, ϕ is violated and E$(\phi$ U $\psi)$ has the value of ψ. We detect this case in the initial marking, before we compute the balance constraints and can return with a definitive answer directly in the beginning. Balance constraints make sure that ϕ is not violated and ψ is true in the final marking. The only transitions which are allowed to violate ϕ are in the set $T_{i,\psi}$ and they have also the effect to turn ψ to true. Due this effect, if such transitions exist, they tend to occur at the end of the firing sequence, but not exclusively. We add the balance constraints to our initial abstraction, the state equation and run the CEGAR algorithm for EF ψ.

Lemma 3. *Given a Petri net $N = (P, T, F, W, m)$ and formula $\phi = s_0 \leq k_0 \wedge s_1 \leq k_1 \wedge \cdots \wedge s_n \leq k_n$, where s_i is a formal sum and $k \in \mathbb{N}$ and $m \models \phi$. Adding to the ILP-problem all balance constraints for ϕ and checking that $\theta_i \geq 0$, then it is guaranteed that after executing the entire firing sequence given as a solution $\wp(w)$ to the ILP-problem that ψ is true. It also ensures that if a complete firing sequence exists, ϕ is true along the path and is only violated, if at all, in the final marking, where ψ holds.*

Proof. Regarding the second claim, we know, based on Definition 6, that only increasing/decreasing transitions affect $s_i \leq k_i$. The offset θ_i ensures that the truth value of $s_i \leq k_i$ stays unchanged. The balance constraint ensures that ϕ is not violated minus the δ_i-offset, which ensures the possibility of a firing sequence which does not violate ϕ along the path, until ψ holds.

If the set $T_{i,\psi}$ is not empty, the δ_i-offset based on the maximum of Δ_{t,s_i} ensures that transitions are not ignored in the balance constraint that violate ϕ but also turn ψ to true. The additional offset, which is the maximal arc weight of the transitions in the set, is enough to make sure that only one transition is allowed to fire, with the effect of making ϕ false and ψ true. We use the maximum, since an arc weight, which is not the maximum, will have a smaller effect and will not change the outcome. Transitions from the set $T_{i,\psi}$ can also fire, if they are in a different context, i.e. when they do not turn ϕ to false.

Theorem 1 ensures that if the complete solution $\wp(w)$ is fired, we get to the final marking m' which satisfies ψ. □

Lemma 3 only ensures that $m' \models \psi$, where m' is the final marking after firing the entire solution $\wp(w)$. But it does not guarantee that intermediate markings satisfy ϕ. This is due to the fact that also decreasing transitions w.r.t. ϕ are allowed to fire.

Lemma 4. *In the exploration of the solution space cutting off paths in markings m^*, with $m^* \models \neg\phi \wedge \neg\psi$ results in keeping only partial solutions which can become full solutions.*

Proof. Based on Definition 9, marking $m^* \models \neg\phi \wedge \neg\psi$ violates the property $\mathrm{E}(\phi \text{ U } \psi)$. All paths extending m^* are also violating $\mathrm{E}(\phi \text{ U } \psi)$ and no extension to the path can make the property true. □

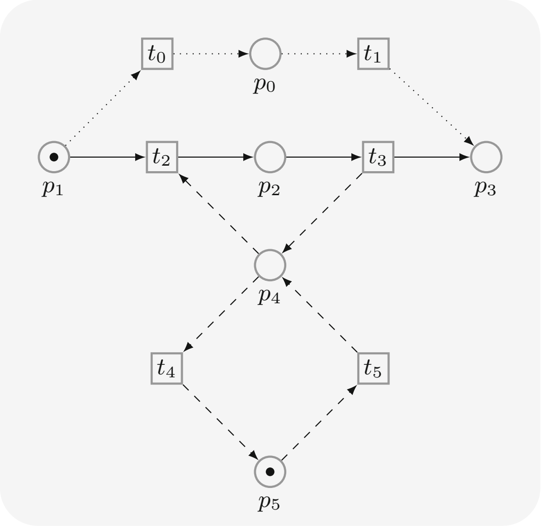

Fig. 2. For the given Petri net and the formula E $(p_1 + p_2 > 0)$ U $(p_3 > 0)$, the minimal solution (t_0, t_1) is cut off. With the CEGAR approach we jump to the next base solution (t_2, t_3), which is only a partial one. The T-invariant (t_4, t_5) is added with the next CEGAR step and provides a full solution, $m \xrightarrow{t_5 t_2 t_3 (t_4)} m'$.

Consider, for example, the Petri net in Fig. 2 and the formula E $(p_1 + p_2 > 0)$ U $(p_3 > 0)$. The minimal solution to the ILP is (t_0, t_1). After firing t_0, a marking $m' = (p_0, p_5)$ is reached that violates $p_1 + p_2 > 0$ and $p_3 > 0$. Lemma 4 ensures that this solution is cut off. There are also no increasing transitions we can add to this solution. Using the CEGAR approach, we jump to a new base solution, (t_2, t_3). But this solution is only a partial solution due to the fact that neither t_2 nor t_3 can fire. At this point, the CEGAR approach adds the T-invariant (t_4, t_5) from which tokens can be borrowed. Now we have a full solution and we get the path $m \xrightarrow{t_2 t_3 t_4 (t_5)} m'$ which satisfies $p_1 + p_2 > 0$ until $(p_3 > 0)$ is satisfied.

Theorem 2. *Let $N = (P, T, F, W, m)$ be a Petri net, ψ an atomic proposition and ϕ a proposition of the form $\phi = s_0 \leq k_0 \wedge s_1 \leq k_1 \wedge \cdots \wedge s_n \leq k_n$, where s_i is a formal sum and $i, k, n \in \mathbb{N}$ and it holds that $m \models \phi$. If* E(ϕ U ψ) *has a realizable solution in the solution space, it can be reached by solving* EF ψ *using the* CEGAR *approach from* [8] *and by adding all* balance constraints *to the initial abstraction and* cutting-off *all paths in m^* in the exploration of the solution space, whenever m^* with $m^* \models \neg\phi \wedge \neg\psi$ is reached.*

Proof. In [8] EF ψ is proved. We constantly add jump and increment constraints to get to a full solution, such that the final marking m' of this solution satisfies ψ, $m' \models \psi$. Lemma 3 ensures that we only get solutions, such that after firing the complete solution $\wp(w)$, ϕ holds. Lemma 4 makes sure that ϕ is not violated along the path. □

6 Solving (EX)$^k\phi$ with the CEGAR Approach

Definition 11 ((EX)$^k\phi$). *Given a Petri net $N = (P, T, F, W, m)$, a proposition ϕ and $k \in \mathbb{N} \setminus \{0\}$. $m \models (EX)^k\phi \iff \exists w \in T^k : m \xrightarrow{w} m_k \wedge m_k \models \phi$. This means there exists a path $m \xrightarrow{w} m_k$ with $|w| = k$ transitions in it and $m_k \models \phi$.*

For example for $k = 2$ this means $(\mathrm{EX})^2\phi = \mathrm{EX}\ \mathrm{EX}\ \phi \iff \exists t_1 t_2 \in T^2 : m \xrightarrow{t_1 t_2} m_k \wedge m_k \models \phi$. To solve (EX)$^k\phi$, we solve EF ϕ. In addition to this we introduce an additional (length) constraint which ensures that the length of sequence w of the ILP-problem solution $\wp(w)$ is equal to k.

Definition 12 (Length constraint). *Given a proposition of the form (EX)$^k\phi$ with $k \in \mathbb{N} \setminus \{0\}$ and an atomic proposition ϕ. We call $\sum_{t \in T} |\wp(w)(t)| = k$ a* length constraint*.*

The sum of the number of occurrences of all transitions in the Parikh vector $\wp(w)$ should exactly be k. To make the proposition true, marking m_k, which is reached after firing k transitions, must satisfy ϕ.

Theorem 3. *Given a Petri net $N = (P, T, F, W, m)$ and proposition (EX)$^k\phi$ with $k \in \mathbb{N} \setminus \{0\}$. If* (EX)$^k\phi$ *has a realizable solution in the solution space, it can be reached by solving* EF ϕ *using the CEGAR approach from [8] and by adding the* length constraint *to the initial abstraction.*

Proof. Based on Definition 11, $m \models (\mathrm{EX})^k\phi \iff \exists w \in T^k \wedge m \xrightarrow{w} m' \wedge m' \models \phi$. The length constraint $\sum_{t \in T} |\wp(w)(t)| = k$ from Definition 12 ensures that only solutions $\wp(w)$ of the ILP-problem are found, such that the length of the firing sequence is exactly k and results in the final marking $m_k \models \phi$. □

7 Solving Finite-linear-path CTL-formulas with the CEGAR Approach

Theorems 1-3 are solving simple CTL-formulas. They all have in common that they have a linear and finite witness path. We use this building bricks to solve a larger class of CTL-formulas with the CEGAR approach. Namely the class of finite-linear-path formulas.

Definition 13 (Existential finite-linear-path formula). *If ϕ and ψ are existential finite-linear-path formulas and ρ is an atomic proposition, then the following formulas are existential finite-linear-path formulas:*

- *ρ (the base of the inductive definition);*
- *EF ϕ;*
- *EX ϕ;*
- *E(ρ U ϕ);*
- *$\phi \vee \psi$;*
- *$\phi \wedge \rho$;*

The existentially quantified formulas are paired with the universally quantified formulas. These two formulas can be reduced to each other by negation. Hence, they permit the application of the same verification techniques. The class of CTL-formulas is extended to the universal finite-linear-path formulas, which use the path as a counterexample. The class is defined accordingly:

Definition 14 (Universal finite-linear-path formula). *If ϕ and ψ are universal finite-linear-path formulas and ρ is an atomic proposition, then the following formulas are universal finite-linear-path formulas:*

- *ρ (the base of the inductive definition);*
- *AG ϕ;*
- *AX ϕ;*
- *A(ρ R ϕ);*
- *$\phi \wedge \psi$;*
- *$\phi \vee \rho$;*

It is easy to see that the negation of an existential finite-linear-path formula is indeed a universal finite-linear-path formula and vice versa. That is, we may restrict subsequent considerations to existential finite-linear-path formulas. Universal finite-linear-path formulas can be verified by checking their negation.

We introduce the concept of how to solve this class of formulas with an example. The interesting part of this class are formulas which have nested CTL-operators, e.g. E (ρ_1 U (E (ρ_2 U ϕ))). The idea is to use for each CTL-operator one state equation with its own set of variables and constraints and then solve the entire ILP-problem.

In our example the first objective would be to solve the left/outer EU-formula. That is, we have to reach a marking $m' \models \rho_2$ while keeping ρ_1 true. For this we have to solve the ILP-problem consisting of the state equation

$m + C \cdot \wp(w)_1 = m'$ and the balance constraints for ρ_1. The second objective is to solve the right/inner EU-formula. Here we are doing the same things as before, that is, we have to reach a marking $m'' \models \phi$ while keeping ρ_2 true. We now add to the ILP-problem a slightly different state equation, $m' + C \cdot \wp(w)_2 = m''$, where we start in the marking m', which we reached from the first state equation and furthermore we introduce a new set of variables $\wp(w)_2$ for our second Parikh vector to reach the final marking m''. The balance constraints to keep ρ_2 true are added as well. Both state equations can be linked together into one equation, $m + C \cdot \wp(w)_1 + C \cdot \wp(w)_2 = m''$.

Definition 15 (ILP-problem for existential finite-linear-path formula). *Let $N = (P, T, F, W, m)$ be a Petri net and ϕ be an existential finite-linear-path formula, which contains $i \in \mathbb{N}$ CTL-operators. We call the following an* ILP-problem for an existential finite-linear-path formula *or in short ILP_ϕ:*

For all CTL-operators add a new set of variables for the Parikh vector $\wp(w)_i$ and the product of $C \cdot \wp(w)_i$ to the state equation:

$$m + C \cdot \wp(w)_1 + \ldots + C \cdot \wp(w)_i = m'.$$

Also add for all EU-operators balance constraints and for EX-operators length constraints based on their corresponding variables.

Once we build the initial ILP-problem we can use the CEGAR approach to find either a realizable solution or to add enough constraints to make the ILP-problem infeasible to verify that no solution exists. While realizing the solution it is important to first use all the transitions from the first Parikh vector $\wp(w)_1$ to keep the structure of the formula in place. $\wp(w)_1$ keeps ρ_1 true until ρ_2 is reached. If all transitions from $\wp(w)_1$ are used in the realization we can start with the transitions of $\wp(w)_2$.

Definition 16 (Realization ordering). *Let $N = (P, T, F, W, m)$ be a Petri net, ϕ an existential finite-linear-path formula, which contains $i \in \mathbb{N}$ CTL-operators and ILP_ϕ the corresponding ILP-problem. To keep the structure of ϕ in place while realizing a solution of ILP_ϕ it must hold that $\forall j, k \in \mathbb{N} : 0 \leq j < k \leq i$ the transitions from $\wp(w)_j$ must be realized before the transitions of $\wp(w)_k$. We call this the* realization ordering.

Theorem 4. *Let $N = (P, T, F, W, m)$ be a Petri net, ϕ be an existential finite-linear-path formula and ILP_ϕ be an ILP-problem for the existential finite-linear-path formula ϕ based on Definition 15. If ϕ has a realizable solution in the solution space, it can be reached by using Theorems 1–3 with ILP_ϕ as the initial ILP-problem and using the realization ordering based on Definition 16 for finding a realizable solution.*

Proof. We proceed by induction, according to Definition 13.
Case ρ (atomic proposition): In CTL an atomic proposition is satisfied, if it holds in the initial marking. Based on Definition 15 and the fact that no CTL-operator is present, no product of $C \cdot \wp(w)$ is added to the equation. It follows

that $m = m'$, which means that the atomic proposition must hold in the initial marking.
Case EF ϕ: This case can be traced back to Case E(ρ U ϕ) using the tautology EF $\phi \iff$ E(TRUE U ϕ).
Case EX ϕ: Definition 15 ensures that $C \cdot \wp(w)$ is added to the state equation and that the length constraint for EX ϕ is added to the ILP-problem. A witness path for EX ϕ is an existential finite-linear-path to the next marking which satisfies ϕ. The path extended by a witness path for ϕ at the final marking (which exists by induction hypothesis) yields a witness path for EX ϕ. Theorem 3 makes sure that if a realizable solution exists, the witness path for EX ϕ is found and Definition 16 ensures that the witness path is added at the correct position to keep the structure of the formula in place.
Case E(ρ U ϕ): This case is similar to the previous one. Definition 15 ensures that $C \cdot \wp(w)$ is added to the state equation and that the balance constraints are added to the ILP-problem. A witness path for E(ρ U ϕ) is an existential finite-linear-path where ρ is true in every marking until a marking is reached where ϕ holds. Theorem 2 makes sure that if a realizable solution exists, the witness path for E(ρ U ϕ) is found and Definition 16 ensures that the witness path is added at the correct marking (which exists by induction hypothesis) to keep the structure of the formula in place.
Case $\phi \vee \psi$: If ϕ is satisfied then there exists a witness path for ϕ for which the induction hypothesis may be applied. Otherwise, there is a witness path for ψ for which again the induction hypothesis applies. A formula like EX $\phi \vee \psi$ is rewritten to EX $\phi \vee$ EX ψ and both sides are verified separately.
Case $\phi \wedge \rho$: In this case, ϕ and ρ are satisfied. Since ρ is an atomic proposition, only the initial marking of the path is concerned. Hence, the induction hypothesis applied to ϕ yields the desired result. □

8 Partially Solving EG ϕ with the CEGAR Approach

Definition 17 (EG ϕ). *Let $N = (P, T, F, W, m)$ be a Petri net and ϕ a propositions. $m \models$ EG $\phi \iff \exists w \in T^* : m \xrightarrow{w} m'$, with $\forall i \in \mathbb{N} : (m_i \models \phi)$. This means that in every state along a path w, ϕ is true.*

Definition 18 (DEADLOCK). *Given a Petri net $N = (P, T, F, W, m)$. N has a* deadlock *if there exist a reachable marking from m in which no transition is activated.*

ϕ is true along a path w, if at least one of two conditions is fulfilled. Either there exists an infinite path containing a cycle or the path ends in a deadlock. Precisely:

1. If the path is infinite then there exists a cycle and the path can be split into two parts $w_1 w_2$ with $m \xrightarrow{w_1} m' \xrightarrow{w_2} m'$, where w_1 is a path leading to a marking m', from which a cycle starts, namely w_2, which goes back to m'. Each state in both w_1 and w_2 satisfies ϕ and w_2 can be repeated infinitely often.

2. If the paths ends in a deadlock every state including the last one, the deadlock state, must satisfy ϕ.

In both cases we can use the knowledge about the existence of a deadlock to create necessary or sufficient quick-checks to solve EG ϕ. If the Petri net has no deadlocks, the only possibility to satisfy EG ϕ is if a cycle can be reached while ϕ stays true and the cycle keeps ϕ also true in every state. The cycle is basically a T-invariant and we can reformulate the problem of solving EG ϕ into solving the state equation once and finding a T-invariant while keeping ϕ true, $m \xrightarrow{m+C\cdot\wp(w_1)=m'} m' \xrightarrow{C\cdot\wp(w_2)=\mathbf{0}} m'$.

Solving the first part, the state equation, is problematic due to fact that m' is not known. The reason for this is that there can be exponentially many T-invariants which keep ϕ true in every state. In addition to this we would have to solve the problem of finding a minimal marking to fire a T-invariant, where minimal is in regard to the entire token number in the marking. It would also make no difference if minimal is in regard to the componentwise comparison of markings, meaning that no more token can be removed. To the best of our knowledge there is no polynomial algorithm known for this problem. We could use a brute-force-method where we calculate for every sequence of a T-invariant, which are all permutations, the minimal required markings to fire completely. All markings can then be compared and we can search for the minimal markings. The runtime for this method would be exponential. This, in connection with the possibility of exponentially many T-invariants, is not a suitable approach to solve EG ϕ.

But on the other hand the second part can be used to build a necessary condition check. If no T-invariant exists that keeps ϕ true and the Petri net has no deadlocks we know that EG ϕ can never be true. To check this we can add to the ILP-problem for finding an invariant an adjusted version of the balance constraint from Definition 10.

Definition 19 (Minimum constraints). *Let $N = (P, T, F, W, m)$ be a Petri net and a proposition $\phi = s_0 \leq k_0 \wedge s_1 \leq k_1 \wedge \cdots \wedge s_n \leq k_n$, where s_i is a formal sum, $0 \leq i \leq n$ and $i, k, n \in \mathbb{N}$. $T_i = \{t \in T | \Delta_{t,s_i} \neq 0\}$ is the set of transitions which can change the value of s_i. It contains all weakly/strongly increasing/decreasing transitions w.r.t. to s_i. We call $\forall s_i : \sum_{t\in T_i} \Delta_{t,s_i} \leq 0$* minimum constraints *w.r.t. s_i.*

These constraints ensure that the sum of all increasing and decreasing transitions is smaller than or equal to zero. Otherwise the truth value of the proposition will be changed.

Proposition 2. *Given a Petri net $N = (P, T, F, W, m)$ and a proposition $\phi = s_0 \leq k_0 \wedge s_1 \leq k_1 \wedge \cdots \wedge s_n \leq k_n$, where s_i is a formal sum and $i, k, n \in \mathbb{N}$ and it holds that $m \models \phi$. If the Petri net has no deadlocks and if the ILP-problem for finding a T-invariant, $C \cdot \wp(w) = \mathbf{0}$ in addition with the minimum constraints has no solution, then* EG ϕ *is also false, $m \not\models$ EG ϕ.*

Proof. Based on Definition 17 if the Petri net has no deadlocks then the only way to satisfy EG ϕ is to find a cycle which keeps ϕ true in every state. If there exists such a cycle it must be a T-invariant and based on Definition 3 the equation $C \cdot \wp(w) = \mathbf{0}$ must have a solution. The minimum constraints based on Definition 19 ensure that ϕ stays true in the cycle. If the ILP-problem, $C \cdot \wp(w) = \mathbf{0}$ plus the minimum constraints, is infeasible, then no T-invariant, therefore no cycle exists, that keeps ϕ true. It follows that EG ϕ can never be true. □

In case the Petri net has deadlocks we can build a sufficient quick-check. We use the fact that EG ϕ is true if the path ends in a deadlock and every state along the path satisfies ϕ. In CTL this condition can be rewritten to E(ϕ U ($\phi \wedge$ DEADLOCK)), where the DEADLOCK predicate can be easily expressed as a conjunction of disjunctions over atomic propositions.

Proposition 3. *Given a Petri net $N = (P, T, F, W, m)$ with deadlocks and an atomic proposition ϕ. If the ILP-problem for E(ϕ U ($\phi \wedge$ DEADLOCK)) has a realizable solution, then EG ϕ is true, $m \models$ EG ϕ.*

Proof. If the Petri net has deadlocks, then based on Definition 17 EG ϕ is among others true, if a path which satisfies ϕ in every state ends in a deadlock. Definition 9 states that ϕ is true until ψ holds and ψ is in this case $\phi \wedge$ DEADLOCK. □

9 Conclusion and Future Work

We proposed two promising techniques to solve E(ϕ U ψ) and $(\mathrm{EX})^k\phi$ with the CEGAR approach for Petri nets and used this as building bricks to solve the class of finite-linear-path CTL-formulas. The main concept is to use constraints on the Parikh vector. We refine the over approximation iteratively until it becomes a realizable solution or infeasible. We also introduced quick-checks for solving EG ϕ under certain circumstances.

To solve E(ϕ U ψ), we solve EF ψ and keep ϕ true in every state along the path. To keep ϕ true, we introduced the concept of balance constraints for the ILP-problem to ensure that an atomic proposition is true after firing the entire solution vector. Furthermore we used a cut-off criterion to ensure that ϕ is also true in every state along the path. For solving $(\mathrm{EX})^k\phi$ we introduced the concept of a length constraint, which makes sure that we only get solutions of length k. The finite-linear-path formulas are using the proposed techniques for solving E(ϕ U ψ) and $(\mathrm{EX})^k\phi$ in addition to an ILP-problem that is build dependent on the CTL-operators contained in the finite-linear-path formula. To verify EG ϕ with a necessary quick-check in the absence of deadlocks we proposed a minimum constraints which ensure that when no T-invariant is found, EG ϕ must be false. As a sufficient quick-check in the presence of deadlocks we introduced the deadlock-constraint and check if E(ϕ U ($\phi \wedge$ DEADLOCK)) has a realizable solution. All proposed techniques are based on solving ILP-problems and thus avoiding the state space explosion problem.

These techniques will be implemented in LoLA 2 [9]. LoLA 2 is an explicit model checker and is every year on the podium of the Model Checking Contest for Petri nets. Once implemented we expect that the proposed approach will increase the verification performance for this formulas significantly. Especially in case of a negative result, the procedure will terminate quickly, due to the fact that the ILP-problem will become infeasible. We expect a similar performance increase as it was the case for the CEGAR approach for reachability analysis, where the performance of LoLA 2 increased from solving under 80% to over 90% in the Model Checking Contest.

Acknowledgements. This study is an extended version of [5]. We thank the anonymous reviewers of both PNSE and ToPNoC for their comments.

References

1. Amparore, E.G., et al.: Presentation of the 9th edition of the model checking contest. In: Tools and Algorithms for the Construction and Analysis of Systems - 25 Years of TACAS: TOOLympics, Held as Part of ETAPS 2019, 6–11 April 2019, Prague, Czech Republic, Proceedings, Part III, pp. 50–68 (2019)
2. Clarke, E.M., Grumberg, O., Jha, S., Lu, Y., Veith, H.: Counterexample-guided abstraction refinement. In: Computer Aided Verification, 12th International Conference, CAV 2000, 15–19 July 2000, Chicago, IL, USA, Proceedings, pp. 154–169 (2000)
3. Hajdu, Á., Vörös, A., Bartha, T.: New Search strategies for the petri net CEGAR approach. In: Devillers, R., Valmari, A. (eds.) PETRI NETS 2015. LNCS, vol. 9115, pp. 309–328. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-19488-2_16
4. Hajdu, Á., Vörös, A., Bartha, T., Mártonka, Z.: Extensions to the CEGAR approach on Petri nets. Acta Cybern. **21**(3), 401–417 (2014)
5. Liebke, T., Wolf, K.: Solving E (ϕ U ψ) using the CEGAR approach. In: Moldt, D., Kindler, E., Wimmer, M. (eds.) Petri Nets and Software Engineering. International Workshop, PNSE 2019, Aachen, Germany, June 24, 2019. CEUR Workshop Proceedings. CEUR-WS.org, vol. 2424, pp. 47–56 (2019)
6. Liebke, T., Wolf, K.: Taking some burden off an explicit CTL model checker. In: Donatelli, S., Haar, S. (eds.) PETRI NETS 2019. LNCS, vol. 11522, pp. 321–341. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-21571-2_18
7. Schmidt, K.: Stubborn sets for standard properties. In: Application and Theory of Petri Nets 1999, 20th International Conference, ICATPN 1999, 21–25 June 1999, Williamsburg, Virginia, USA, Proceedings, pp. 46–65 (1999)
8. Wimmel , H., Wolf, K.: Applying CEGAR to the Petri net state equation. In: Tools and Algorithms for the Construction and Analysis of Systems - 17th International Conference, TACAS 2011, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2011, 26 March – 3 April, Saarbrücken, Germany, 2011. Proceedings, pp. 224–238 (2011)
9. Wolf, K.: Petri net model checking with LoLA 2. In: Application and Theory of Petri Nets and Concurrency - 39th International Conference, PETRI NETS 2018, 24–29 June 2018, Bratislava, Slovakia, Proceedings, pp. 351–362 (2018)