Stubborn Sets for Standard Properties

Karsten Schmidt

Institut für Informatik, Humboldt-Universität zu Berlin, 10099 Berlin, Germany

Abstract. Stubborn sets are a tool for state space reduction preserving certain system properties. We present stubborn set approaches for all popular Petri net standard properties. This extends the list of properties that can be analysed successfully (including boundedness, reversibility). For other properties, our approach can lead to larger reductions (reachability) than previous ones. Furthermore, shortest and cheapest witness paths for several properties are now preserved.

Keywords: (Theory) Analysis of nets, Computer tools for nets

1 Introduction

Using stubborn sets, situations where sequences of transitions can fire in arbitrary order are detected. By firing as few as possible of the possible permutations, the size of state spaces can decrease significantly. Reduction is obtained by firing, at a marking $m$, only some transitions at each state, collected in the stubborn set $St(m)$. The art of stubborn sets is to keep the reduced size as small as possible, but large enough to preserve a given property of the underlying system.

The first, and still most popular, application field of stubborn sets was the dead marking problem [9]. Then, eliminating the problem of ignored transitions, other standard properties like liveness and dead transitions could be preserved [10]. The stubborn set concept was generalised to language preservation [10] and linear time temporal logic (LTL) model checking [11, 12, 6, 3]. These two approaches depend on the distinction between visible and invisible transitions, i.e. transitions that do or do not influence the desired property. The language of visible transitions is fully preserved while state space reduction concerns only invisible transitions. Though visibility can be relaxed in some situations [5, 17], the general approaches do not work very well for global or almost global properties (properties with a small number of invisible transitions). Furthermore, care must be taken to the ignoring problem.

Attempts to apply stubborn sets to model checking for the branching time logic CTL [2] lead to significantly stronger restrictions (i.e. larger stubborn sets) than LTL-preserving methods.

In [13–15], many derivatives of the stubborn set method are surveyed.

We propose another policy of stubborn set creation. Where most existing methods consider stubborn sets as a superset of a single enabled transition (arbitrarily chosen), our stubborn sets are supersets of attractor sets of transitions.
These attractor sets play a key role for directing the generation of the reduced graph into the desired direction. This concept is also present in the tester concept in [12] where the actions of the tester process are closely related to our attractor sets. However, the tester concept treats visible transitions in a similar way as language preserving stubborn sets and is therefore not suitable for global properties.

We present our method property by property. Thereby we start with boundedness and reachability. Having done this, we generalise the pattern of our methodology. Then we discuss invariance and satisfiability of state predicates on a more general level. We continue with the preservation of shortest and cheapest paths. After that we revisit the dead transition and dead marking problems. For preserving liveness and reversibility, we study stubborn sets in the context of strongly connected components of the reachability graph. We close our list of properties with the (more complicated) home state problem.

2 Petri nets

For the purpose of simplicity, we present the approach for place/transition nets. However, the idea can be easily transferred to other formalisms that have a concept of stubborn sets.

Definition 1 (Petri net). A tuple $N = [P, T, F, W, m_0]$ is a Petri net iff $P$ and $T$ are finite, nonempty, and disjoint sets (of places and transitions), $F \subseteq (P \times T) \cup (T \times P)$ (the set of arcs), $W : (P \times T) \cup (T \times P) \rightarrow \mathbb{N}$ such that $W([x, y]) > 0$ iff $[x, y] \in F$ (the arc multiplicities), and $m_0$ is a marking, i.e. a mapping $m_0 : P \rightarrow \mathbb{N}$.

For a place or transition $x$, $\bullet x = \{ y \mid [y, x] \in F \}$ denotes the pre-set of $x$, and $x^* = \{ y \mid [x, y] \in F \}$ denotes its post-set.

Definition 2 (Transition relation). We say: $t$ can fire at a marking $m$ yielding a marking $m'$ (written: $m \xrightarrow{t} R m'$) iff for all $p \in P$, $m(p) \geq W([p, t])$ and $m'(p) = m(p) - W([p, t]) + W([t, p])$.

If there exists a $m'$ to a given $m$ and $t$ such that $m \xrightarrow{t} R m'$, then we say: $t$ is enabled at $m$. We extend the transition relation to sequences of transitions. Define $m \xrightarrow{w} R m$ for arbitrary $m$ and the empty sequence $\varepsilon$, and $m \xrightarrow{w, t} R m'$ ($w$ being a transition sequence and $t$ a transition) iff there is a $m^*$ such that $m \xrightarrow{w} R m^*$ and $m^* \xrightarrow{t} R m'$. If there is a transition sequence $w$ such that $m \xrightarrow{w} R m'$, we write $m \xrightarrow{t} R m'$.

Definition 3 (Reachability graph). A directed labelled graph is the reachability graph of a Petri net $N = [P, T, F, W, m_0]$ iff its set of nodes is the set of all reachable markings, i.e. $\{ m \mid m_0 \xrightarrow{t} R m \}$, and $[m, m']$ is an edge labelled with $t$ iff $m \xrightarrow{t} R m'$. 