Resiliency

Alain Finkel Author: Please enter affiliation as second parameter of the author macro

Mathieu Hilaire ✉
Université Paris-Saclay
CNRS
ENS Paris-Saclay
Laboratoire Méthodes Formelles (LMF)
Gif-sur-Yvette, France

Abstract

Here goes the abstract.

2012 ACM Subject Classification Theory of computation → Automata over infinite objects; Theory of computation → Automata extensions

Keywords and phrases Author: Please fill in \keywords macro

Digital Object Identifier 10.4230/LIPIcs...70

Funding *Mathieu Hilaire*: This work was partly done while the author was supported by the Agence Nationale de la Recherche grant no. (numero de la grant BraVASS).

Acknowledgements The author would like to thank.

1 Definitions

In this section, we introduce general notations and preliminary definitions.

The model we are interested in is (S)WSTS (and later some particular instances, i.e. Timed/Counter Automata for instance).

1.1 Transition systems

▶ **Definition 1.** *A* labeled transition system *(LTS for short) is a tuple* $T = (S, \Lambda, \rightarrow)$ *where* S *is a set of* configurations, Λ *is a set of* labels, *and* $\rightarrow \subseteq S \times \Lambda \times S$ *is a ternary relation, denoted as the set of* labeled transitions.

We prefer to use infix notation and $(s, a, s') \in \rightarrow$ will be abbreviated as $s \xrightarrow{a} s'$ to represent a transition from configuration s to configuration s' with label a.

Labels can be used to represent the reading of an input, but also to represent an action performed during the transition or conditions that must hold in order to allow the use of the transition.

A *path* in a labeled transition system from a *source configuration* s_0 to a *target configuration* s_n is a sequence $\pi = s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} \cdots \xrightarrow{a_{n-1}} s_n$. We define the *concatenation* $\pi_1\pi_2$ of two paths π_1 and π_2 when the source configuration of π_2 is equal to the target configuration of π_1 as expected. The *length* of $\pi = s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} \cdots \xrightarrow{a_{n-1}} s_n$ is defined as $|\pi| = n$. We say the path is *labeled* by $a_0a_1, \ldots a_{n-1}$. For all $w \in \Lambda^*$, all $s, s' \in S$, we will write $s \xrightarrow{w} s'$ if there exists a path from s to s' labeled by w.

An *infinite path* is an infinite sequence $\pi = s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} \cdots$. For each infinite (resp. finite) path $\pi = s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} \cdots$ (resp. $\pi = s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} \cdots \xrightarrow{a_{n-1}} s_n$) and $i, j \in \mathbb{N}$ (resp. $i, j \in [0, n]$) with $i < j$ we denote by $\pi[i, j]$ the path $s_i \xrightarrow{a_i} s_{i+1} \xrightarrow{a_{i+1}} \cdots \xrightarrow{a_{j-1}} s_j$ and by $\pi[i]$ the configuration s_i. As expected, a *prefix* of a finite or infinite path π is a finite path of the

form $\pi[0, j]$, and a *suffix* of a finite path π is a path of the form $\pi[i, n]$.
Given an infinite path $\pi = s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} \cdots$ let $Inf(\pi) = \{s \in S \mid \forall i\ \exists j > i\ s_j = s\}$.
The set of *successors* of a configuration $s \in S$ is defined as $\textsc{Succ}(s) = \{s' \in S \mid \exists a \in \Lambda\ s \xrightarrow{a} s'\}$.
A configuration without successors is called a *dead end*.
The set of *predecessor* of a configuration $s \in S$ is defined as $\textsc{Pred}(s) = \{s' \in S \mid \exists a \in \Lambda\ s' \xrightarrow{a} s\}$.

A labeled transition system $(S, \Lambda, \to)$ is *deterministic* if for all configurations $s_1, s_2, s_3 \in S$ and all $a \in \Lambda$, $s_1 \xrightarrow{a} s_2$ and $s_1 \xrightarrow{a} s_3$ implies $s_2 = s_3$.

▶ **Definition 2.** *An* (unlabeled) transition system *is a pair* $T = (S, \to)$ *where* S *is a set of* configurations *and* $\to \subseteq S \times S$ *is a binary relation on the set of configurations, denoted as the set of* transitions.

We again prefer to use infix notation and write $s \to s'$ to denote a *transition* from configuration s to configuration s' (i.e., $(s, s') \in \to$).
Note that an unlabeled transition system can be seen as a labeled transition system where the set of labels consists of only one element. Determinism, (infinite) paths, their length, and concatenation in unlabeled transition systems are then defined as expected.

Thinking about whether or not it is pertinent to have LTS and not only TS. LTS can be usefull for TA because of the use of the guards/time as labels but it may be unecessary.

We write $\to^k$, $\to^+$, $\to^=$, $\to^*$ for the k-step iteration of $\to$, its transitive closure, its reflexive closure, its reflexive and transitive closure). We use similar notation for $\textsc{Succ}$ and $\textsc{Pred}$...

This makes sense for TS but not so much for LTS ...

A transition system is *finitely branching* if all $\textsc{Succ}(s)$ are finite. We restrict our attention to finitely branching TSs.

Alain: the forward coverability algorithm for infinitely branching TSs.; the backward cov algo may work for essentially finitely branching TSs. Not sure that TS induced by TA are finitely branching. Actually I believe they are not, i.e. for instance for a TA with one clock x, from a state q and clock x set at 0, if there is a transition e.g. $(q, x \geq 3, \varnothing, q')$ then the set of successors of $(q, 0)$ is $\{q'\} \times \{3, 4, 5, \ldots\}$. Need to check where finitely branching appears as an assumption/requirement.

1.2 Well-quasi-orderings

A *quasi-ordering* (a qo) is any reflexive and transitive relation $\leq$.

We abbreviate $x \leq y \nleq x$ by $x < y$.

Any qo induces an equivalence relation ($x \equiv y$ iff $x \leq y \leq x$).

We now recall a few results from the theory of well-orderings (add reference [...]).

▶ **Definition 3.** *A* well-quasi-ordering *(a wqo) is any quasi-ordering* $\leq$ *(over some set* X *) such that, for any infinite sequence* $x_0, x_1, x_2, \ldots$ *in* X*, there exist indexes* $i \leq j$ *with* $x_i \leq x_j$.

Notice that a wqo is well-founded, i.e. it admits no infinite strictly decreasing sequence $x_0 > x_1 > x_2 > \cdots$

▶ **Lemma 4.** *(Erdös and Rado). Assume* $\leq$ *is a wqo. Then any infinite sequence contains an infinite increasing subsequence:* $x_{i_0} \leq x_{i_1} \leq x_{i_2} \cdots$ *(with* $i_0 < i_1 < i_2 \cdots$*).*

Given $\leq$ a quasi-ordering over some set X, an *upward-closed set* is any set $I \subseteq X$ such that if $y \geq x$ and $x \in I$ then $y \in I$. A *downward-closed set* is any set $I \subseteq X$ such that if $y \leq x$ and $x \in I$ then $y \in I$. To any $A \subseteq X$ we associate the *upward-closure of* A $\uparrow A = \{x \in X \mid \exists a \in A\ y \geq a\}$

and the *downward-closure of* $A \downarrow A = \{x \in X \mid \exists a \in A\ y \leq a\}$. We abbreviate $\uparrow \{x\}$ (resp. $\downarrow \{x\}$) as $\uparrow x$ (resp. $\downarrow x$).

A *basis* of an upward-closed set I is a set I_b such that $I = \bigcup_{x \in I_b} \uparrow x$.

▶ **Lemma 5.** *(Higman [40]) If $\leq$ is a wqo; then any upward-closed I has a finite basis.*

Proof. The set of minimal elements of I is a basis because $\leq$ is well-founded. It only contains a finite number of non-equivalent elements otherwise they would make an infinite sequence contradicting the wqo assumption. ◀

Alain: non ceci est vrai seulement si le quasi ordre est un ordre cad antisymétrique. Mais ce n'est pas un pb. Relis mon papier de 2016 sur les well abstracted...

▶ **Lemma 6.** *If $\leq$ is a wqo; any infinite increasing sequence $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ of upward-closed sets eventually stabilizes; i.e. there is a $k \in N$ such that $I_k = I_{k+1} = I_{k+2} = \cdots$.*

Proof. Assue we have a counter-example. We extract an infinite subsequence where inclusion is strict: $I_{n_0} \subsetneq I_{n_1} \subsetneq I_{n_2} \cdots$. Now, for any $i > 0$, we can pick some $x_i \in I_{n_i} \setminus I_{n_{i-1}}$. The well-quasi-ordering hypothesis means that the infinite sequence of x_i's contains an increasing pair $x_i \leq x_j$ for some $i < j$. Because x_i belongs to an upward- closed set I_{n_i} we have $x_j \in I_{n_i}$, contradicting $x_j \notin I_{n_{j-1}}$. ◀

1.3 Well-structured transition systems

▶ **Definition 7.** *A* (resp. strongly) well-structured transition systems *(abbreviated as WSTS resp. SWSTS) is a TS $(S, \rightarrow, \leq)$ equipped with a wqo $\leq \subseteq S \times S$ between states such that the wqo is (resp. strongly) compatible with the transition relation, i.e., for all $s_1, t_1, s_2 \in S$ with $s_1 \leq t_2$ and $s_1 \rightarrow s_2$, there exists $t_2 \in S$ with $s_2 \leq t_2$ and $t_1 \rightarrow^* t_2$ (resp. $t_1 \rightarrow^1 t_2$).*

Several families of formal models of processes give rise to WSTSs in a natural way, e.g. Petri nets when inclusion between markings is used as the well-ordering.

▶ **Proposition 8.** *If S is an WSTS and $I \subseteq S$ is an upward-closed set of states, then $\text{PRED}^*(I)$ is upward- closed.*

▶ **Proposition 9.** *If S is an SWSTS and $I \subseteq S$ is an upward-closed set of states, then $\text{PRED}(I)$ is upward-closed.*

▶ **Definition 10.** *A WSTS has* effective pred-basis *if there exists an algorithm accepting any state $s \in S$ and returning $pb(s)$, a finite basis of $\uparrow \text{PRED}(\uparrow s)$.*

A downard-closed set J is *decidable* if, given $s \in S$, it is decidable whether $s \in J$. Since a downward-closed set does not have an "upward-basis" in general, we will demand that membership is decidable.

▷ Claim 11. (stability of ideals) Let $I, J \subseteq S$ be upward-closed. Then the sets $I \cup J$, and $I \cap J$ are upward-closed.

▶ **Fact 1.** *(i) For every upward-closed set $I \subseteq S$, there exists a finite basis B of I.*
(ii) Given a finite set $A \subseteq S$ with $I = \uparrow A$, we can compute a finite basis B of I.

▶ **Definition 12.** *(index). For an upward-closed set $I \subseteq S$ and $k \geq 0$, let $I^k = \bigcup_{0 \leq j \leq k} pre^j(I)$. The* index *$k(I)$ is the smallest k_0 s.t. $I^k = I^{k_0}$ for all $k \geq k_0$.*

▶ **Fact 2.** *Let $I \subseteq S$ be an upward-closed set and $k \geq 0$ s.t. $I^k = I^{k+1}$, then $I^\ell = I^k$ for all $\ell \geq k$, i.e., $k(I) \leq k$. This also implies that $pre^*(I) = I^k$.*

▶ **Lemma 13.** *Given a basis of an upward-closed set $I \subseteq S$, and a state s of a strongly well-structured transition system, we can decide whether we can reach I from s.*

Proof. We have to show that we can compute a basis of I^{k+1} if we are given a basis of I^k. Then the decidability of the stop condition follows directly. Let B be a basis of I^k. We have

$$I^{k+1} = I \cup pre(I^k) = I \cup \bigcup_{s' \in B} pre(\uparrow \{s'\}).$$

Since $pre(\uparrow \{s'\})$ is computable for any $s' \in S$ by definition, we obtain a finite generating set of I^{k+1} . By Fact 3, we can compute a basis of I^{k+1}. ◀

1.4 Defining resilience

1.4.1 TS resilience

Ask the question why use a set of propositions for $SAFE$ and BAD rather than use subsets of the set of configurations ?

We ask whether we can reach a state in $SAFE$ in a reasonable amount of time whenever we reach a state in BAD. From this we formulate two resilience problems. First consider the case where the recovery time is bound by a given natural number $k \geq 0$, i.e., the explicit resilience problem for TS.

TS k-RESILIENCE PROBLEM

INPUT: A state s of a TS $(S, \rightarrow)$, two disjoints subset of S $SAFE$ and BAD.
QUESTION: $\forall s' \in BAD\ (s \rightarrow^* s') \implies \exists s'' \in SAFE\ s' \rightarrow^{\leq k} s''$?

We can also ask whether there exists such a bound k. We call this problem the bounded resilience problem for TS.

TS BOUNDED RESILIENCE PROBLEM

INPUT: A state s of a TS $(S, \rightarrow)$, two disjoints subset of S $SAFE$ and BAD.
QUESTION: $\exists k \geq 0\ \forall s' \in BAD\ (s \rightarrow^* s') \implies \exists s'' \in SAFE\ s' \rightarrow^{\leq k} s''$?

1.4.2 WSTS resilience

Properties in well-structured transition systems are often given as upward- or downward closed sets [references]. Transfering the abstract resilience problems into this framework, it is therefore reasonable to demand that both propositions, SAFE and BAD, are given by upward-closed or downward-closed sets.

We assume that the safety property is given by an upward-closed set and the bad condition by a decidable downward-closed set.

From these considerations, we formulate instances of the abstract resilience problems for well- structured transition systems.

Again, we first consider the case where the recovery time is bounded by a $k \in \mathbb{N}$.

WSTS k-RESILIENCE PROBLEM

INPUT: A state s of a WSTS $(S, \rightarrow, \leq)$, an upward-closed set I with a given basis, a decidable downward-closed set J.

QUESTION: $\forall s' \in J\ (s \to^* s') \implies \exists s'' \in I\ s' \to^{\leq k} s''$?

Analogously, we formulate the bounded resilience problem for WSTSs.

WSTS bounded resilience problem

INPUT: A state s of a WSTS $(S, \to, \leq)$, an upward-closed set I with a given basis, a decidable downward-closed set J.

QUESTION: $\exists k \geq 0\ \forall s' \in J\ (s \to^* s') \implies \exists s'' \in I\ s' \to^{\leq k} s''$?

2 Decidability

▶ **Theorem 14.** SWSTS k-resilience *is decidable.*

Proof. Assume $(S, \to, \leq)$ is a SWSTS with upward compatibility, J is a decidable downward-closed subset of S, and I is an upward-closed set with a given basis.

We define inductively $I^k = \bigcup_{0 \leq j \leq k} pre^j(I)$. Note that for all $k \in \mathbb{N}$, I^k is upward-closed due to the strongly upward compatibility of $(S, \to, \leq)$.

The k-resilience property can be expressed as the formula $post^*(s) \cap J \subseteq I^k$. In order to decide whether the inclusion holds, we execute two procedures in parallel, one trying to prove $post^*(s) \cap J \subseteq I^k$ and one looking for a counter example.

In order to certify inclusion in I^k, we need to work with finite representations. The next lemma uses that I and J are upward- and downward-closed, respectively.

▶ **Lemma 15.** *Let $A \subseteq S$ be a set, $J \subseteq S$ downward-closed and $I \subseteq S$ upward-closed. Then $A \cap J \subseteq I \leftrightarrow (\uparrow A) \cap J \subseteq I$.*

▶ **Corollary 16.** *For all $k \in \mathbb{N}$, $post^*(s) \cap J \subseteq I^k \leftrightarrow (\uparrow post^*(s)) \cap J \subseteq I^k$.*

Assume k is fixed for now.

Procedure 1 enumerates inductive invariants in some fixed order D_1 , D_2 , ... , i.e. downward closed subsets $D_i \subseteq S$ such that $\uparrow post(D_i) \subseteq D_i$. Every inductive invariant D_i is an “over-approximation” of $\uparrow post^*(s)$ if it contains s. (on énumère des sur-approximations de la cloture par le haut de $post * (s)$ par leur bases finies). Each “over-approximation” D_i is given by its basis $b(D_i)$. Notice that, by standard monotonicity, $\uparrow post^*(s)$ is such an inductive invariant and may eventually be found.

Procedure 1 stops when it finds a basis $b(D)$ of an invariant D such that $b(D) \cap J \subseteq I^k$. Since $b(D)$ is finite and J is decidable, we can directly compute $b(D) \cap J$. We can compute a basis of I^{k+1} if we have a basis of I^k. Due to the Lemma, $b(D) \cap J \subseteq I^k$ implies $D \cap J \subseteq I^k$. Hence $b(D) \cap J \subseteq I^k$ implies $\uparrow post^*(s) \cap J \subseteq D \cap J \subseteq I^k$. (since D contains $\uparrow post^*(s)$).

The second procedure iteratively computes $post^{\leq n}(s) \cap J$ until it finds an element not in I^k.

```
(1)     i ← 0
(2)     while ¬(↑ post*(D_i) ⊆ D_i and
s ∈ D_i and b(D) ∩ J ⊆ I^k) loop
(3)         i ← i + 1
(4)     end loop
(5)     return false
```

Figure 1 Procedure 1: enumerates inductive invariants to find an inclusion certificate.

```
(1)     D ← {s}
(2)     while D ∩ J ⊆ I^k loop
(3)         D ← D ∪ post(D)
(4)     end loop
(5)     return false
```

Figure 2 Procedure 2: searches for a non-inclusion certificate.

We show that these two procedures are correct:

1. k-resilience holds if, and only if, Procedure 1 terminates.
2. k-resilience do not hold if, and only if, Procedure 2 terminates.

Proof:

1. By a simple induction, it can be shown that $\uparrow post^*(D) \subseteq D$ for every inductive invariant D. If Procedure 1 terminates, then $post^*(s) \cap J \subseteq \uparrow post^*(s) \cap J \subseteq D \cap J \subseteq I^k$ which implies that k-resilience holds.
   It remains to show that Procedure 1 terminates whenever k-resilience holds. To do so, it suffices to prove that $\uparrow post^*(s)$ is an inductive invariant. Indeed, this implies that $\uparrow post^*(s)$ is eventyally found by Procedure 1 when k-resilience holds.
   Formally, let us show that $\uparrow post(\uparrow post^*(s)) \subseteq \uparrow post^*(s)$. Let $b \in \uparrow post(\uparrow post^*(s))$ there exists a', a, b such that $s \to^* a'$, $a' \leq a$, $a \to b'$, and $b' \leq b$. By downward compatibility there exists $b'' \leq b'$ such that $a \to b''$. Therefore, $x \to^* b''$ and $b' \geq b$, hence $b \in \downarrow post^*(x)$.
2. Procedure 2 computes $post^{\leq n}(s) \cap J$ until it finds an element not in I^k.
   If Procedure 2 terminates, then k-resilience does not hold. It remains to show that Procedure 2 terminates whenever k-resilience does not hold. Assume $post^*(s) \cap J \nsubseteq I^k$, then there exists $a \in post^*(s) \cap J$ such that $a \notin I^k$. Since $post^*(s) = \bigcup_n post^{\leq n}(s)$, then $a \in post^*(s)$ implies there exists n_a such that $a \in post^{\leq n_a}(s)$. Hence, $post^{\leq n_a}(s) \cap J$ contains an element not in I^k, and Procedure 2 terminates.

◀

▶ **Theorem 17.** SWSTS RESILIENCE *is decidable.*

Proof. sketch

Iteratively check whether k-resilience holds. If this is the case, return $k_{min} = k$. Otherwise check whether $I^{k+1} = I^k$. If so, return -1 (false), otherwise continue. The stop condition is decidable and by Fact 4 also sufficient. ◀

3 Applications section

3.1 Timed Automata

Should be defined in a later 'application section' once we start writing any proof, for now I leave it there

A *guard* over a finite set of clocks Ω is a comparison of the form $\omega \bowtie c$, where $\omega \in \Omega$, $c \in \mathbb{N}$, and $\bowtie \in \{<, \leq, =, \geq, >\}$. We denote by $\textsc{Guards}(\Omega)$ the *set of guards* over the set of clocks Ω. The *size* of a guard $g = \omega \bowtie c$ is defined as $|g| = \log(c)$. A *clock valuation* is a function from Ω to $\mathbb{N}$; we write $\vec{0}$ to denote the clock valuation $\omega \mapsto 0$ whenever the set Ω is clear from the context. For each clock valuation v and each $t \in \mathbb{N}$ we denote by $v + t$ the clock valuation $\omega \mapsto v(\omega) + t$. For each guard $g = \omega \bowtie c$ with $c \in \mathbb{N}$, we write $v \models g$ if $v(\omega) \bowtie c$.

A timed automaton is a finite automaton extended with a finite set of clocks Ω that all progress at the same rate and that can individually be reset to zero. Moreover, every transition is labeled by a guard over Ω and by a set of clocks to be reset.

Formally, a *timed automaton* (*TA* for short) is a tuple $\mathcal{A} = (Q, \Omega, R, q_{init}, F)$, where

- Q is a non-empty finite *set of states*,
- Ω is a non-empty finite *set of clocks*,
- $R \subseteq Q \times \mathsf{G}(\Omega) \times \mathcal{P}(\Omega) \times Q$ is a finite *set of rules*,
- $q_{init} \in Q$ is an *initial state*, and
- $F \subseteq Q$ is a *set of final states*.

We also refer to $\mathcal{A}$ as an n-TA if $|\Omega| = n$. The *size* of $\mathcal{A}$ is defined as

$$|\mathcal{A}| \;=\; |Q| + |\Omega| + |R| + \sum_{(q,g,U,q') \in R} |g|.$$

Let $\mathsf{Consts}(\mathcal{A}) = \{c \in \mathbb{N} \mid \exists (q, g, U, q') \in R,\ \exists \omega \in \Omega, \bowtie \in \{<, \leq, =, \geq, >\} : g = \omega \bowtie c\}$ denote the set of constants that appear in the guards of the rules of $\mathcal{A}$.

By $\mathsf{Conf}(\mathcal{A}) = Q \times \mathbb{N}^{\Omega}$ we denote the set of *configurations* of $\mathcal{A}$. We prefer however to abbreviate a configuration (q, v) by $q(v)$.

A TA $\mathcal{A} = (Q, \Omega, R, q_{init}, F)$ induces the labeled transition system $T_{\mathcal{A}} = (\mathsf{Conf}(\mathcal{A}), \Lambda_{\mathcal{A}}, \rightarrow_{\mathcal{A}}$) where $\Lambda_{\mathcal{A}} = R \times \mathbb{N}$ and where $\rightarrow_{\mathcal{A}}$ is defined such that, for all $(\delta, t) \in R \times \mathbb{N}$ with $\delta = (q, g, U, q') \in R$, for all $q(v), q'(v') \in \mathsf{Conf}(\mathcal{A})$, $q(v) \xrightarrow{\delta,t}_{\mathcal{A}} q'(v')$ if $v + t \models g$, $v'(u) = 0$ for all $u \in U$ and $v'(\omega) = v(\omega) + t$ for all $\omega \in \Omega \setminus U$.

A *run* from $q_0(v_0)$ to $q_n(v_n)$ in $\mathcal{A}$ is a path in the transition system $T_{\mathcal{A}}$, that is, a sequence $\pi = q_0(v_0) \xrightarrow{\delta_1,t_1}_{\mathcal{A}} q_1(v_1) \cdots \xrightarrow{\delta_n,t_n}_{\mathcal{A}} q_n(v_n)$; it is called *reset-free* if for all $i \in \{1, \ldots, n\}$, $\delta_i = (g_i, \emptyset)$ for some guard g_i.

We say π is *accepting* if $q_0(v_0) = q_{init}(\vec{0})$ and $q_n \in F$.

It is worth mentioning that there are further modes of time valuations and guards which exist in the literature, we refer to [?] for a recent overview. Notably, we consider in this article only the case of timed automata over discrete time. It is worth mentioning that in the case of timed automata over continuous time (i.e. with clocks having values in $\mathsf{R}_{\geq 0}$), techniques [?, ?] exist for reducing the reachability problem to discrete time in the case of closed (i.e. non-strict) clock constraints ranging over integers.

<u>TA k-RESILIENCE PROBLEM</u>

INPUT: A state q of a TA (Q, X, Δ), a set $SAFE \subseteq Q$, a set $BAD \subseteq Q$.

QUESTION: $\forall q' \in BAD \forall v, v' \in \mathbb{N}^X \ (q(v) \to^* q'(v')) \implies \exists q'' \in SAFE \exists v'' \in \mathbb{N}^X \ q'(v') \to^{\leq k} q''(v'')$?

Analogously, we formulate the bounded resilience problem for WSTSs.

TA BOUNDED RESILIENCE PROBLEM

INPUT: A state q of a TA (Q, X, Δ), a set $SAFE \subseteq Q$, a set $BAD \subseteq Q$.
QUESTION: $\exists k \geq 0 \ \forall q' \in BAD \forall v, v' \in \mathbb{N}^X \ (q(v) \to^* q'(v')) \implies \exists q'' \in SAFE \exists v'' \in \mathbb{N}^X \ q'(v') \to^{\leq k} q''(v'')$?

I think there can be a discussion to be had here about how to quantify on the clock valuations

Here one thing that could be interesting to try to formalize is: how to enforce that the time that passes is less than k, rather than the number of transitions. This is tricky to deal with I find but it should be more doable if for instance we use one counter automata, where the counter effect of the sequence can be quantified more explicitly I suppose ? But here you could also use a kinda special clock x that is reset when you enter BAD and is not reset between a state in BAD and a state in $SAFE$, you could check that $x < k$.

... I guess if you use 0/1-TA then the problems become closer one to another ? Also of note is that 0/1-TA induces transition systems with bounded branching, so I guess it may be interesting to investigate these first ?

A 0/1 *timed automaton* (0/1-*TA* for short) is a tuple

$$\mathcal{B} = (Q, X, \Delta_0, \Delta_1, q_{init}, F),$$

where $\mathcal{B}_i = (Q, X, R_i, q_{init}, F)$ is a TA for all $i \in \{0, 1\}$. For simplicity we define its *size* as $|\mathcal{B}| = |\mathcal{B}_0| + |\mathcal{B}_1|$. We analogously denote the constants of $\mathcal{B}$ by $\mathsf{Consts}(\mathcal{B})$ and its configurations by $\mathsf{Conf}(\mathcal{B})$.

A 0/1 timed automaton $\mathcal{B} = (Q, X, R_0, R_1, q_{init}, F)$ induces the labeled transition system $T_{\mathcal{B}} = (\mathsf{Conf}(\mathcal{B}), \lambda_{\mathcal{B}}, \to_{\mathcal{B}})$ where $\lambda_{\mathcal{B}} = (R_0 \cup R_1) \times \{0, 1\}$ and where $\to_{\mathcal{B}}$ is defined such that for all $q(z), q'(z') \in \mathsf{Conf}(\mathcal{B})$, for all $(\delta, i) \in \lambda_{\mathcal{B}}$ with $\delta = (q, g, U, q') \in R_i$ $q(v) \xrightarrow{\delta, i}_{\mathcal{B}} q'(v')$ if $v + i \models g$, $v'(u) = 0$ for all $u \in U$ and $v'(\omega) = v(\omega) + i$ for all $\omega \in \Omega \setminus U$.

As expected, we write $q(v) \xrightarrow{\delta, i}_{\mathcal{B}} q'(v')$ if $q(v) \xrightarrow{\delta, i}_{\mathcal{B}} q'(v')$ for some $i \in \{0, 1\}$, and some $\delta \in R_i$.

3.2 One-Counter Automata

Should be defined in a later 'application section' once we start writing any proof, for now I leave it there

OCA k-RESILIENCE PROBLEM

INPUT: A state q of a OCA (Q, Δ), a set $SAFE \subseteq Q$, a set $BAD \subseteq Q$.
QUESTION: $\forall q' \in BAD \forall n, n' \in \mathbb{N} \ (q(n) \to^* q'(n')) \implies \exists q'' \in SAFE \exists n'' \in \mathbb{N} \ q'(n') \to^{\leq k} q''(n'')$?

OCA BOUNDED RESILIENCE PROBLEM

INPUT: A state q of a OCA (Q, Δ), a set $SAFE \subseteq Q$, a set $BAD \subseteq Q$.
QUESTION: $\exists k \geq 0 \ \forall q' \in BAD \forall n, n' \in \mathbb{N} \ (q(n) \to^* q'(n')) \implies \exists q'' \in SAFE \exists n'' \in \mathbb{N} \ q'(n') \to^{\leq k} q''(n'')$?

3.3 Vector Addition System with States

Should be defined in a later 'application section' once we start writing any proof, for now I leave it there

A Appendix thing if necessary