Resilience and Home-Space for WSTS ⋆

Alain Finkel[1,2] and Mathieu Hilaire[1]

[1] Université Paris-Saclay, CNRS, ENS Paris-Saclay, LMF, Gif-sur-Yvette, France
[2] Institut Universitaire de France

Abstract. Resilience of unperfect systems is a key property for improving safety by insuring that if a system could go into a bad state in Bad then it can also leave this bad state and reach a safe state in Safe. We consider six types of resilience (one of them is the home-space property) defined by an upward-closed set or a downward-closed set Safe, and by the existence of a bound on the length of minimal runs starting from a set Bad and reaching Safe (Bad is generally the complementary of Safe).
We first show that all resilience problems are undecidable for effective Well Structured Transition Systems (WSTS) with strong compatibility. We then show that resilience is decidable for Well Behaved Transition Systems (WBTS) and for WSTS with adapted effectiveness hypotheses. Most of the resilience properties are shown decidable for other classes like WSTS with the downward compatibility, VASS, lossy counter machines, reset-VASS, integer VASS and continuous VASS.

Keywords: Verification, Resilience, Home-Space, Well-structured transition systems, Vector addition system with states

1 Introduction

Context. Resilience is a key notion for improving safety of unperfect systems and resilience engineering is a paradigm for safety management that focuses on systems coping with complexity and balancing productivity with safety [23]. Some systems are subjects at frequent intervals to accidents, attacks or changes. In such cases, a question that arises is that of whether the system can return to its normal (safe) behavior after an accident or attack pushed it towards some kind of 'error state' and, if it can, whether it can perform the return in a satisfactory timeframe.
Resiliences. Given a transition system whose set of states is S and let $X, H \subseteq S$, we say that (X, H) satisfies the *home-space* property [20] if the reachability set from X is included in the set of predecessors of H. In 1986, Memmi and Vautherin introduced the notion of home-space [20] in Petri nets for X a singleton. In 1989, de Frutos Escrig and Johnen proved that the home-space problem (for X a singleton and H a finite union of linear sets with the same period) was

⋆ This work was partly done while the authors were supported by the Agence Nationale de la Recherche grant BraVAS (ANR-17-CE40-0028).

decidable for VASS ([14]). In 2023, Jancar and Leroux proved the decidability of the (complete) semilinear home-space problem (X and H are both semilinear) in VASS [18].

A transition system is *resilient for* $(\mathit{Bad}, \mathit{Safe})$ if $(\mathsf{Bad}, \mathsf{Safe})$ satisfies the home-space property. A transition system is *resilient for* Safe if it is resilient for $(\mathsf{Bad}, \mathsf{Safe})$ with Bad is the complementary to Safe. It is *state-resilient* if it is resilient for $(\mathsf{Bad}, \mathsf{Safe})$ where Bad contains an unique state. The *k-resilience* problem, for $k \geq 0$, is to decide whether from any state is it always possible to reach Safe with a run of length smaller than k and the *bounded resilience* problem is to decide whether there exists an k such that the system is k-resilient.

State of the art.

In 2016, Prasad and Zuck introduced in [25] intuitions, definitions (without any connection to the concept of the home-space) and results (without detailed proofs) about resilience in the framework of process algebra. They show that resilience is decidable for effective Well Structured Transition Systems (WSTS) with both upward and reflexive downward compatibilities and some other technical conditions (that are defined in Section 2). In 2021, Özkan and Würdemann [22] and Özkan [21], in 2022, proved the decidability of the bounded state-resilience problem and the k-state-resilience problem for WSTS with strong compatibility (see Section 2) and with the supplementary (strong) hypothesis that there exists an algorithm that computes a finite basis of the upward-closure of the reachability set from s when Safe is upward-closed.

Our main contributions.

- Surprinsingly, the general undecidability statements about resilience were not known neither proved. We show that resilience and state-resilience (i.e. X a singleton) problems are both undecidable for WSTS with strong compatibility and for Safe upward-closed or downward-closed.
- In the subsequent three figures, we present the majority of our results pertaining to various models and resilience categories. The figures depict the boundaries of decidability within the context of well-known VASS and reset-VASS models.
- In particular, the three resilience problems are decidable for post-ideal-effective (Definition 5) Well Behaved Transition Systems (a generalisation of WSTS where the quasi-ordering is not necessarly well founded) with strong (upward) compatibility and when Safe is upward-closed (Theorem 4). Resilience is also decidable, when Safe is upward-closed, for effective pred-basis (Definition 5) WSTS with strong (upward) compatibility (Theorem 5).
- We clarify the different effectiness conditions on WBTS and WSTS (Definition 5) that allow the decidability of the six resilience.
- We generalize with Theorem 8 the main theorem of [22, 21] and we show that relaxing some hypothesis leads to undecidability (Proposition 5).
- We show that the three state-resilience problems are decidable for post-ideal-effective WBTS with downward and upward compatibilities and Safe downward-closed (Theorem 9 extends [25, Theorem 1]). The two other types

of resilience, k-state-resilience and bounded-state-resilience, are decidable for post-ideal-effective WBTS with strong downward compatibility.
– We study the resilience problems for VASS and variations of VASS where most of the resilience problems are shown decidable.

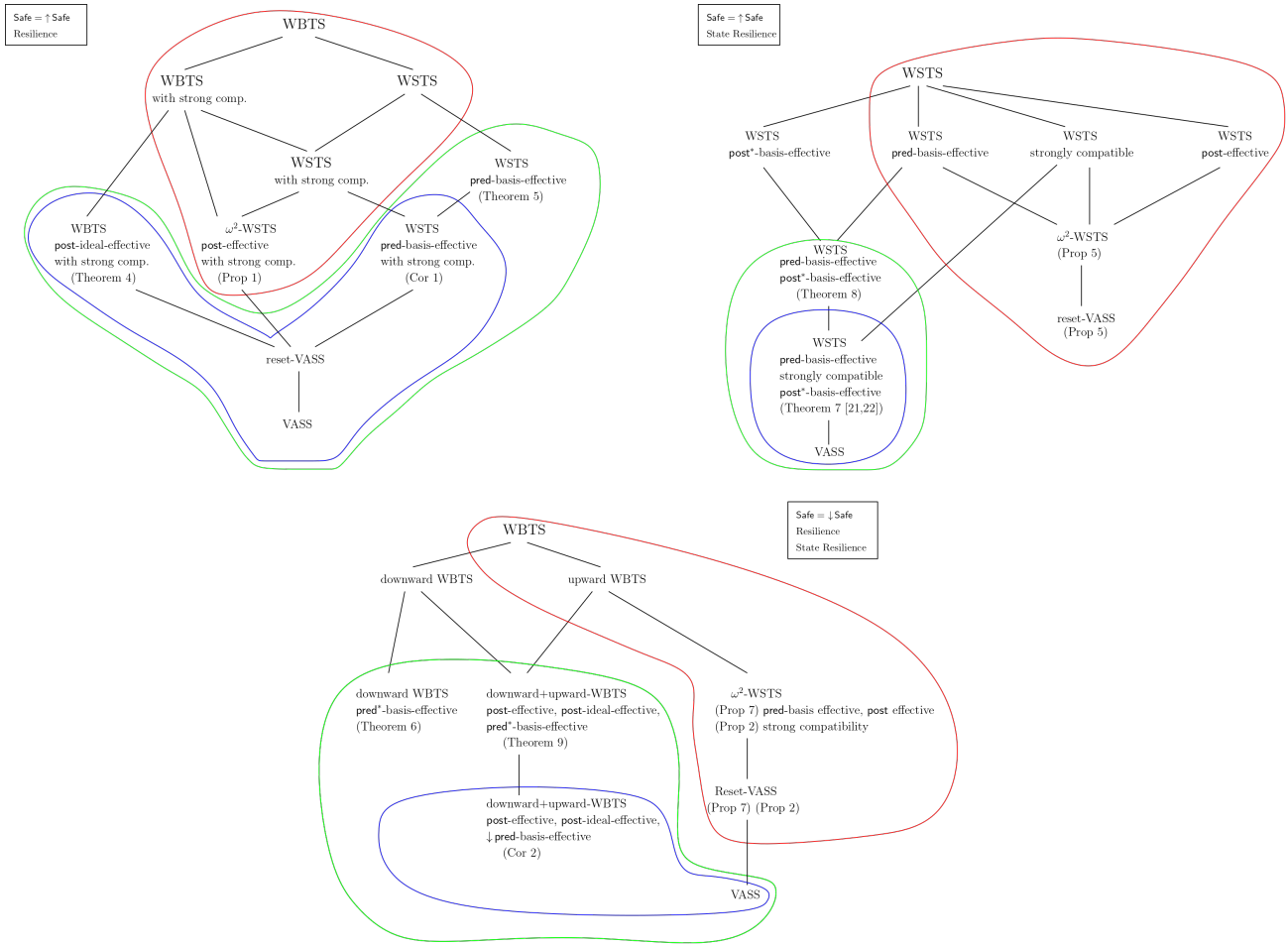

Fig. 1: Hasse diagram of some classes of transition systems, together with the decidability (in green) or undecidability (in red) of the resilience problems. Decidability of bounded resilience and $k-$resilience variants are indicated in blue.

Plan of the paper.

Section 2 introduces the necessary definitions of WSTS and variations as well as the different notions of effectivity. Section 3 and 4 are concerned with the general framework of WSTS and contain our results on the three resilience problems and the three state-resilience problems respectively. Lastly, Section 5 concerns itself with the resilience problems for VASS and variations of VASS.

2 Well-structured transition systems and VASS

A *transition system* is a pair $\mathscr{S} = (S, \to)$ where S is a set of *states* and $\to \subseteq S \times S$ is a binary relation on the set of states, denoted as the set of *transitions*. We write $s \to s'$ to denote $(s, s') \in \to$. 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. Let $X, Y \subseteq S$ and $k \in \mathbb{N}$; we denote $X \longrightarrow^* Y$ (resp. $X \longrightarrow^{\leq k} Y$) if from all states $x \in X$ there exists a path (resp. of length smaller than k) that reaches a state $y \in Y$. The set of *(immediate) successors* of a state $s \in S$ is defined as $\mathsf{post}_{\mathscr{S}}(s) = \{s' \in S \mid \ s \to s'\}$. The set of *(immediate) predecessors* of a state $s \in S$ is defined as $\mathsf{pred}_{\mathscr{S}}(s) = \{s' \in S \mid \ s' \to s\}$. To simplify the notations, we write without ambiguity $\mathsf{post}_{\mathscr{S}}(D)$ by $\mathsf{post}(D)$ and $\mathsf{pred}_{\mathscr{S}}(D)$ by $\mathsf{pred}(D)$. By iterating pred and post we obtain $\mathsf{post}^n(s) = \{s' \in S \mid \ s \to^n s'\}$ and $\mathsf{pred}^n(s) = \{s' \in S \mid \ s' \to^n s\}$. However, we are generally more interested in $\mathsf{post}^{\leq n}(s) = \bigcup_{1 \leq i \leq n} \mathsf{post}^i(s)$, $\mathsf{post}^*(s) = \bigcup_{1 \leq i} \mathsf{post}^i(s)$ and $\mathsf{pred}^{\leq n}(s) = \bigcup_{1 \leq i \leq n} \mathsf{pred}^i(s)$ and $\mathsf{pred}^*(s) = \bigcup_{1 \leq i} \mathsf{pred}^i(s)$. The *reachability problem* asks, given a transition system $\mathscr{S} = (S, \to)$, two states $s, t \in S$, whether $s \to^* t$.

A *quasi-ordering* (a qo) is any reflexive and transitive relation $\leq$ over some set X and we often write $(X, \leq)$. Given a quasi-ordering $(X, \leq)$, an *upward-closed set* is any set $U \subseteq X$ such that if $x \leq y$ and $x \in U$ then $y \in U$. A *downward-closed set* is any set $D \subseteq X$ such that if $y \leq x$ and $x \in D$ then $y \in D$. It is an *ideal* if it is also *directed*, i.e. it is nonempty and for every $a, b \in D$, there exists $c \in D$ such that $a \leq c$ and $b \leq c$. To any subset $A \subseteq X$, we may associate its *upward-closure*, $\uparrow A = \{x \in X \mid \exists a \in A \ a \leq x\}$ and its *downward-closure*, $\downarrow A = \{x \in X \mid \exists a \in A \ x \leq a\}$. We abbreviate $\uparrow\{x\}$ (resp. $\downarrow\{x\}$) as $\uparrow x$ (resp. $\downarrow x$). A *basis* of an upward-closed set U is a set U_b such that $U = \uparrow U_b$; similarly, a *basis* of a downward-closed set D is a set D_b such that $D = \downarrow D_b$.

A *well-quasi-ordering* (wqo) is any quasi-ordering $(X, \leq)$ such that, for any infinite sequence $x_0, x_1, x_2, ...$ in X, there exist indexes $i \leq j$ with $x_i \leq x_j$. This property is equivalent to the *finite decomposition* property : every upward-closed set $\emptyset \neq U \subseteq X$ admits a finite basis $B \subseteq X$ such that $U = \uparrow B$. Wqo admits many other equivalent formulations like : a qo $(X, \leq)$ is a wqo iff $(X, \leq)$ is well founded (i.e. there is no infinite strictly decreasing sequence of elements of X) and $(X, \leq)$ contains no infinite antichains (an antichain is a subset of mutually incomparable elements of X). See other equivalences in [16, 27]. As an example, $(\mathbb{N}^d, \leq)$, the set of vectors of d natural numbers (where d is finite) with component-wise order is a wqo.

Quasi-orderings that have no infinite antichains enjoy a similar *finite decomposition* property than wqo: every downward-closed subset $D \subseteq X$ can be decomposed into a *finite* set of ideals $J_1, J_2, \ldots, J_n$ such that $D = J_1 \cup J_2 \cup \ldots \cup J_n$ See for example [7]. In what follows, a downward-closed set D is represented by its finite set of ideals (or by the minimal elements of its upward-closed complement), and an upward-closed set U is represented by its finite set of minimal elements.

Let us now recall the (most general) definition of well-structured transition systems.

Definition 1 (Definition 3.10, [10]). *A* Well-Structured Transition System *(WSTS)* $\mathscr{S} = (S, \to, \leq)$ *is a transition system* $(S, \to)$ *equipped with a wqo* $\leq \subseteq S \times S$ *such that the transition relation* $\to$ *is (upward) compatible with* $\leq$*, i.e., for all* $s_1, t_1, s_2 \in S$ *with* $s_1 \leq s_2$ *and* $s_1 \to t_1$*, there exists* $t_2 \in S$ *with* $t_1 \leq t_2$ *and* $s_2 \to^* t_2$*.*

An (upward) compatible transition relation $\to$ is *reflexive* when the sequence $s_2 \to^* t_2$ is not empty: formally, for all $s_1, t_1, s_2 \in S$ with $s_1 \leq s_2$ and $s_1 \to t_1$, there exists $t_2 \in S$ with $t_1 \leq t_2$ and $s_2 \to^+ t_2$. We say that a WSTS $\mathscr{S}$ has *strong (upward) compatibility* when moreover for all $s_1, t_1, s_2 \in S$ with $s_1 \leq s_2$ and $s_1 \to t_1$, there exists $t_2 \in S$ with $t_1 \leq t_2$ and $s_2 \to t_2$.

Several families of formal models of processes [13] give rise to WSTSs in a natural way with disfferent compatibilities, e.g. compatible counter machines like VASS with d counters and Q a finite set of control-states (and equivalently Petri nets) data Petri nets, reset/transfer VASS are WSTS with strong compatibility for the usual ordering $= \times \leq^d$ on the set of states $S = Q \times \mathbb{N}^d$. Similarly, lossy channel systems with d channels and Q a finite set of control-states are WSTS (with a non-strong compatibility) for the ordering $= \times \sqsubseteq^d$ (where $\sqsubseteq$ is the subword ordering on Σ^*) on $S = Q \times (\Sigma^*)^d$.

But there is a more general class of (upward) compatible ordered transition systems than WSTS for which coverability is still decidable: recall that a Well Behaved Transition System (WBTS) [6] is an upward compatible ordered transition system $\mathscr{S} = (S, \to, \leq)$ where $(S, \leq)$ contains no infinite antichains (but it can be not well founded). The class of WBTS is strictly larger than WSTS: for example, $\mathbb{Z}^d-$VASS under the lexicographical ordering are WBTS but not WSTS [6].

By applying Proposition 4.3 from [11], we can reintroduce a straightforward definition of a specific proper subset of wqos that allow to construct coverability trees:

Definition 2. *A wqo* $(X, \leq)$ *is an* ω^2-wqo *if* $(Ideals(X), \subseteq)$ *forms a wqo.*

Although there exists wqo that are not ω^2-wqo (see the Rado ordering in [17]), all naturally occurring wqos are ω^2-wqo, perhaps to the notable exception of finite graphs well-quasi-ordered by the graph minor relation. The class of ω^2-wqo is robust because every datatype in the following list - natural number, finite

set, finite product, finite sum, finite disjoint sum, finite words, finite multisets and finite trees - is an ω^2-wqo [11, Proposition 4.5]. Now we are able to define ω^2-WSTS:

Definition 3. *(Finkel and Goubault-Larrecq [11]) A WSTS $\mathscr{S} = (S, \rightarrow, \leq)$ is an ω^2-WSTS if $(S, \leq)$ is an ω^2-wqo.*

Since almost of usual wqo are ω^2-wqo, all naturally occurring WSTS are in fact ω^2-WSTS: for example, reset/transfer VASS are ω^2-WSTS.

Let us recall that the *completion* [7] of a WSTS $\mathscr{S} = (S, \rightarrow, \leq)$ is the associated ordered transition system $\hat{\mathscr{S}} = (Ideals(S), \rightarrow, \subseteq)$ where $Ideals(S)$ is the set of ideals of S and $I \rightarrow J$ if J belongs to the finite ideal decomposition of $\downarrow \mathsf{post}_{\mathscr{S}}(I)$. The completion is always *finitely branching* but it is not necessarily a WSTS since $\subseteq$ is not necessarily a wqo. It is proved in [7] that $\hat{\mathscr{S}}$ is WSTS iff $\mathscr{S} = (S, \rightarrow, \leq)$ is ω^2-WSTS.

Another type of WSTS exists that enjoys downward compatibility.

Definition 4. *A* downward (compatible) WBTS (short, downward-WBTS) $\mathscr{S} = (S, \rightarrow, \leq)$ *is an ordered transition system $(S, \rightarrow, \leq)$ such that $\leq$ is without infinite antichains and the transition relation $\rightarrow$ is downward compatible with $\leq$, i.e., for all $s_1, t_1, s_2 \in S$ with $s_2 \leq s_1$ and $s_1 \rightarrow t_1$, there exists $t_2 \in S$ with $t_2 \leq t_1$ and $s_2 \rightarrow^* t_2$.*

A downward (compatible) WSTS (short, downward-WSTS) *[13, Definition 5.1] is a downward-WBTS where $\leq$ is a wqo.*

There are fewer downward-WSTS than WSTS, but we can still mention FIFO automata with insertion errors and Basic Process Algebra (BPA).

Let us reformulate the downward compatibility property.

Lemma 1. *For an ordered transition system $\mathscr{S} = (S, \rightarrow, \leq)$ (not necessarily a WSTS), the two following properties are equivalent: (1) $\mathscr{S} = (S, \rightarrow, \leq)$ is downward compatible ; (2) for every downward-closed set $D \subseteq S$, the set $\mathsf{pred}^*(D)$ is downward-closed.*

To obtain decidability results, we must introduce some notions of *effectiveness*. We use a mixture of the notions defined both by Blondin and al. in [6] and by Halfon in [16]. First, to simplify and w.l.o.g., we suppose that all classes of considered ordered transition systems $\mathscr{S} = (S, \rightarrow, \leq)$ satisfy the five following properties:

1. there exists an algorithm that decides whether $s \rightarrow t$ is true or not, for any states $s, t \in S$,
2. there is a computational representation for S for which membership in S is decidable,
3. $\leq$ is decidable,

4. there is a computational representation for $Ideals(S)$ for which membership in $Ideals(S)$ is decidable, and
5. inclusion of ideals is decidable.

Blondin and al. showed [6, Lemma 4.3] that under the previous hypotheses, one are able to enumerate *downward-closed sets* (by their finite decomposition in ideals), to decide inclusion between downward-closed sets and to decide if a state belongs to a given finite set of ideals. But the five properties are not sufficient to compute the complementary and the intersection of downward-closed sets. Halfon introduced *ideally-effective wqo* as wqo that essentially allow to compute representations of (principal) ideals $\downarrow s$, of the complementary of an ideal, of the complementary of filters (a filter is a set $\uparrow s$ for $s \in S$) and to compute representations of finite intersections of filters and finite intersections of ideals. Most well-known wqo are ideally-effective [16].

Starting now, we assume that all considered WBTS $\mathscr{S} = (S, \to, \leq)$ satisfy the five previous properties and that the wqo $\leq$ is ideally-effective. We refer to such WBTS as *effective*.

In order to construct algorithms, we also require effective hypotheses about the computations of certain sets of predecessors and successors. More precisely:

Definition 5. *We say that an ordered transition system $\mathscr{S} = (S, \to, \leq)$ is*

1. post-effective *if $\mathscr{S}$ is effective, and if there exists an algorithm that computes $|\mathsf{post}(s)| \in \mathbb{N} \cup \{\infty\}$ on input $s \in S$.*
2. post-ideal-effective *if $\mathscr{S}$ is effective and there exists an algorithm accepting any ideal $I \in Ideals(S)$ and returning $\downarrow \mathsf{post}(I)$, expressed as a finite union of (maximal) ideals.*
3. pred-basis-effective *[13, 1] if $\mathscr{S}$ is effective and there exists an algorithm accepting any state $s \in S$ and returning a finite basis of $\uparrow \mathsf{pred}(\uparrow s)$.*
4. post*-basis-effective *[21, 22] if $\mathscr{S}$ is effective and there exists an algorithm accepting any state $s \in S$ and returning a finite basis of $\uparrow \mathsf{post}^*(s)$.*
5. pred*-basis-effective *if $\mathscr{S}$ is effective and there exists an algorithm accepting any ideal $I \in Ideals(S)$ and returning a finite basis of $\downarrow \mathsf{pred}^*(I)$.*

Counter machines are effective but don't enjoy any other effectivities among the list of five. Reset VASS (hence VASS) and (front) lossy fifo automata are post-effective, post-ideal-effective, and pred-basis-effective. There exist post-effective WSTS that are not post-ideal-effective [7, Proposition 35]; there exist post-ideal-effective WSTS that are not post-effective [7, Proposition 36].There also exist WSTS that are not pred-basis-effective [7, Proposition 45]. Reset VASS are not post*-basis-effective since post*-basis-effectiveness allows to compute the finite set of the set of minimal reachable states, hence it would allow to decide the zero-reachability problem that is undecidable for reset-VASS. However, VASS are post*-basis-effective [21, Proposition 2] and LCS (with d fifo channels) are also post*-basis-effective because we have $(q, w_1, w_2, ..., w_d) \in \uparrow \mathsf{post}^*(q_0, u_1, u_2, ..., u_d)$ iff $(q, \epsilon, ..., \epsilon) \in \uparrow \mathsf{post}^*(q_0, u_1, u_2, ..., u_d)$ iff $(q, \epsilon, ..., \epsilon)$ is reachable from $(q_0, u_1, u_2, ..., u_d)$ that is decidable in LCS. Reset-VASS are not

pred^*-basis-effective because computing a finite basis of $\downarrow \mathsf{pred}^*(q, 0, ..., 0)$ would allow to decide whether $(q, 0, ..., 0)$ is reachable that is undecidable for reset-VASS. By using the decidability of reachability and [29, Theorem 3.11], we may prove that VASS are pred^*-basis-effective. A more complete study of these properties will be done in the long version of this paper.

Recall the *coverability problem* for ordered transition systems.

COVERABILITY PROBLEM

INPUT: An ordered transition system $\mathscr{S} = (S, \to, \leq)$ and two states $s_0, s \in S$.

QUESTION: $s_0 \in \mathsf{pred}^*(\uparrow s)$?

With the pred-basis-effective hypothesis, we obtain:

Theorem 1 (Theorem 3.6, [13], Theorem 4.1, [1]). *A finite basis of $\mathsf{pred}^*(U)$ is computable for any pred-basis-effective WSTS $\mathscr{S} = (S, \to, \leq)$ and any upward-closed set $U \subseteq S$ given with its finite basis. Hence coverability is decidable.*

With the post-ideal-effective hypothesis, we obtain the decidability of coverability for WBTS (without the pred-basis-effective hypothesis).

Theorem 2 (Corollaire 4.4, [6]). *Coverability is decidable for any post-ideal-effective WBTS.*

Downward-WSTS enjoy a powerfull property.

Theorem 3 (Proposition 5.4, [13]). *Finitely branching downward-WSTS with reflexive compatibility and post-effective are post^*-basis-effective.*

Let us recall the definition of vector addition system with (control-)states.

Definition 6. *A* vector addition system with (control-)states (VASS) *in dimension d (d-VASS for short) is a finite $\mathbb{Z}^d$-labeled directed graph $V = (Q, T)$, where Q is the set of* control-states*, and $T \subseteq Q \times \mathbb{Z}^d \times Q$ is the set of* control-transitions*.*

Subsetquently, $Q \times \mathbb{N}^d$ is the set of states of the transition system associated with a d-VASS V. For all states $p(\mathbf{u}), q(\mathbf{v}) \in Q \times \mathbb{N}^d$ and for every control-transition $t = (p, \mathbf{z}, q)$, we write $p(\mathbf{u}) \xrightarrow{t} q(\mathbf{v})$ whenever $\mathbf{v} = \mathbf{u} + \mathbf{z} \geq \mathbf{0}$. When in the context of a d-VASS, we denote 0^d by $\mathbf{0}$.

A *vector addition system (VAS)* in dimension d (d-VAS for short) is a d-VASS where the set of control-states is a singleton; hence one only needs T.

VASS can be extended with resets.

Definition 7. *A* reset-VASS *in dimension d is a finite labeled directed graph $V = (Q, T)$, where Q is the set of* control-states*, $T \subseteq Q \times Op \times Q$ is the set of* control-transitions*, and $Op = \{add(\boldsymbol{z}) \mid \boldsymbol{z} \in \mathbb{Z}^d\} \cup \{reset(i) \mid i \in \{1, \ldots, d\}\}$.*

For every states $p(\mathbf{u}), q(\mathbf{v}) \in Q \times \mathbb{N}^d$ and every control-transition t we write $p(\mathbf{u}) \xrightarrow{t} q(\mathbf{v})$ when

- $t = (q, add(\mathbf{z}), q') \in T$ and $\mathbf{u} + \mathbf{z} = \mathbf{v} \geq 0$,
- $t = (q, reset(i), q') \in T$ and $\mathbf{v}[i] = 0$, and $\mathbf{v}[i'] = \mathbf{u}[i']$ for all $i' \in \{1, \ldots, d\} \setminus i$.

As an example, let us remark that $(\mathbb{N}^d, \leq)$ is an ideally-effective wqo.

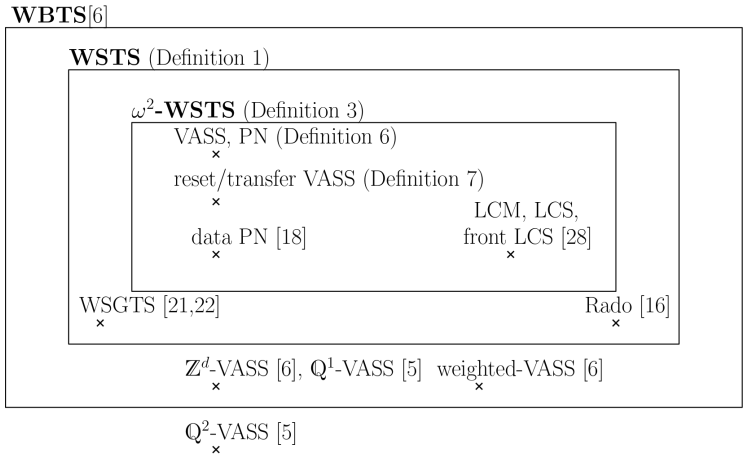

Fig. 2: A taxonomy of WSTS and variants.

3 Resilience for WSTS

In a (not necessarily ordered) transition system $\mathscr{S} = (S, \to)$, we consider a subset of states $\mathsf{Safe} \subseteq S$, and its complement, Bad. The *resilience problem* (resp. the *k-resilience problem*) for $(\mathscr{S}, \mathsf{Safe})$ is to decide whether from *any* state in S, *there exists* a path (resp. a path of length smaller than or equal to k) that reaches a state in Safe. Resilience is then akin to the Home-Space problem (defined in the introduction) for the set Safe. Resilience can also be viewed as a generalizeation of coverability, as it asks whether for *every* element of Bad it is possible to cover an element of the basis of Safe. We use the notation $S \longrightarrow^* \mathsf{Safe}$ (resp. $S \longrightarrow^{\leq k} \mathsf{Safe}$) for $\forall x \in S, \exists y \in \mathsf{Safe}$ such that $x \longrightarrow^* y$ (resp. $\forall x \in S, \exists y \in \mathsf{Safe}$ such that $x \longrightarrow^{\leq k} y$). In our framework, $\mathsf{Safe} \subseteq S$ is possibly infinite but must admit a computable finite representation : for example, downward-closed sets and upward-closed sets in wqos and semilinear sets in $\mathbb{N}^d$ have finite representations.

Let us formalize three resilience problems.

Resilience problems

INPUT: A transition system $\mathscr{S} = (S, \to)$, and a set $\mathsf{Safe} \subseteq S$.
QUESTION: (resilience problem (RP)) $\mathsf{Bad} \longrightarrow^* \mathsf{Safe}$?
(k-resilience problem (kRP)) $\mathsf{Bad} \longrightarrow^{\leq k} \mathsf{Safe}$?
(bounded resilience problem (BRP)) $\exists k \geq 0\ S \longrightarrow^{\leq k} \mathsf{Safe}$?

These three resilience problems are decidable for finite transition systems but undecidable for (general) infinite-state transition systems. So we restrict our framework to the class of infinite-state WSTS. Since most of decidable properties in WSTS rely on the computation of upward or downward-closed sets [1, 13], we consider upward-closed or downward-closed sets Safe. Since $\mathsf{Safe} \subseteq \mathsf{pred}^*(\mathsf{Safe})$, one only needs to decide whether the complement of Safe is in $\mathsf{pred}^*(\mathsf{Safe})$. From

now on, we use Bad to denote the complement of Safe.

Surprisingly, the general undecidability statement regarding resilience had neither been known nor proven (it is simply mentioned as a future work in the conclusion of [22]). We show that the resilience problem is undecidable for ω^2-WSTS with strong compatibility and natural effectiveness hypothesis.

Proposition 1. RESILIENCE *and* BOUNDED RESILIENCE *for post-effective* ω^2*-WSTS with strong compatibility, for upward closed sets* Safe *are undecidable.*

Proof. Indeed, consider the family $\{f_j : \mathbb{N}^2 \to \mathbb{N}^2\}$ of increasing recursive functions from [12] defined as

$$f_j(n,k) = \begin{cases} (n,0) & \text{if k=0 and TM}_j \text{ runs for more than n steps} \\ (n,n+k) & \text{otherwise,} \end{cases}$$

where TM_j is the j-th Turing machine (in a classical enumeration) which moreover begins by writing the integer j on its tape, and consider additionnally the function $g : \mathbb{N}^2 \to \mathbb{N}^2$ defined by $g(n,k) = (n+1,k)$. The transition system $S_j = (\mathbb{N}^2, \{f_j, g\}, \leq)$ is a post-effective ω^2-WSTS with strong compatibility and has the property that it is $\uparrow(1,1)$-resilient iff TM_j halts on input j, since $(1,1)$ is coverable from $(0,0)$ iff TM_j halts on input j. Hence there is no Turing machine which correctly determines resilience and halts whenever its input is a WSTS. Hence RESILIENCE for ω^2-WSTS with strong compatibility is undecidable. Furthermore, strong compatibility implies the existence of $k \in \mathbb{N}$ such that $\mathsf{pred}^*(\mathsf{Safe}) = \mathsf{pred}^{\leq k}(\mathsf{Safe})$, hence BOUNDED-RESILIENCE for ω^2-WSTS with strong compatibility is undecidable as well. □

Let us remark that the transition system $S_j = (\mathbb{N}^2, \{f_j, g\}, \leq)$ in the previous proof is not post-ideal-effective nor pred-basis-effective. Termination and boundedness are decidable for increasing recursive (functional) WSTS [12]; the decidability of coverability and place-boundedness depends on the effectiveness hypothesis on recursive functions.

We now prove that RESILIENCE is undecidable for reset-VASS when $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$ by a reduction from the undecidable [3] decision problem of *zero-reachability* in reset-VASS.

ZERO-REACHABILITY

INPUT: A reset-VASS $V = (Q,T)$ of dimension d, $q_f \in Q$, $p(\mathbf{u}) \in Q \times \mathbb{N}^d$.
QUESTION: $p(\mathbf{u}) \to^* q_f(\mathbf{0})$?

Proposition 2. RESILIENCE *is undecidable for reset-VASS, hence it is also undecidable for* post*-effective and* pred*-basis-effective* ω^2*-WSTS with strong compatibility and with* $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$.

Proof. Let V be a reset-VASS, $q_0(\mathbf{0})$ an initial state of V, and $q_f(\mathbf{0})$ a terminal state of V. We build V' from V by additionnally allowing from any control-state to get back to $q_0(\mathbf{0})$ by a transition reseting every counter and changing the control-state to q_0. Remark that the set of states reachable from $q_0(\mathbf{0})$ is the same

in V' and in V. Then $q_f(\mathbf{0})$ is reachable from $q_0(\mathbf{0})$ in V iff $q_f(\mathbf{0})$ is reachable from every state in V', which corresponds to RESILIENCE in V' for $\mathsf{Safe} = \{q_f(\mathbf{0})\}$. Indeed, if $q_f(\mathbf{0})$ is reachable from $q_0(\mathbf{0})$ in V, then, since $q_0(\mathbf{0})$ is reachable from every state in V', $q_f(\mathbf{0})$ is reachable from every state in V'. In the other direction, if $q_f(\mathbf{0})$ is reachable from every state in V', then in particular $q_f(\mathbf{0})$ is reachable from $q_0(\mathbf{0})$ in V', hence $q_f(\mathbf{0})$ is reachable from $q_0(\mathbf{0})$ in V.

3.1 Case: $\mathsf{Safe} = \uparrow\mathsf{Safe}$.

We start with the case $\mathsf{Safe} = \uparrow\mathsf{Safe}$, hence $\mathsf{Bad} = \downarrow\mathsf{Bad}$. Since Resilience is undecidable for ω^2-WSTS with strong compatibility (Theorem 1), we still consider WSTS, and even WBTS, with strong compatibility but by strengthening the assumptions of effectiveness (we now consider the post-ideal-effective hypothesis) and we demonstrate that the three resilience problems are now decidable.

Theorem 4. *Let $\mathscr{S} = (S, \to, \leq)$ be a post-ideal-effective WBTS with strong compatibility and a set $\mathsf{Safe} = \uparrow\mathsf{Safe}$.* RESILIENCE, BOUNDED RESILIENCE *and* k-RESILIENCE *are decidable.*

Proof. Let us first recall two results in [7] that are stated for WSTS but are also true for WBTS since the proofs rely only on compatibility and not on the property of wqo. [7, Proposition 30] establishes a strong relation between the runs of a WSTS $\mathscr{S} = (S, \to, \leq)$ and the runs of its completion $\hat{\mathscr{S}}$. It states that if $x \xrightarrow{k} y$ in $\mathscr{S}$ then for every ideal $I \supseteq \downarrow x$, there exists an ideal $J \supseteq \downarrow y$ such that $I \xrightarrow{k} J$ in $\hat{\mathscr{S}}$. [7, Proposition 29] establishes that if $I \xrightarrow{k} J$ in $\hat{\mathscr{S}}$ then for every $y \in J$, there exists $x \in I$ and $y' \geq y$ such that $x \xrightarrow{k'} y'$ in $\mathscr{S}$. Moreover, if $\mathscr{S}$ has transitive compatibility then $k' \geq k$; if $\mathscr{S}$ has strong compatibility then $k' = k$.

Let $\{s_1, s_2, ..., s_m\}$ be the (unique) minimal basis of Safe and $\{J_1, J_2, ..., J_n\}$ be the ideal decomposition of Bad. The resilience problem can be reduced to the following infinite number of instances of the coverability problem in $\mathscr{S}$: for all $x \in \mathsf{Bad}$ does there exist an j such that s_j is coverable from x. Let us show how this infinite set of coverability questions can be reduced to a *finite* set of coverability questions in the completion $\hat{\mathscr{S}} = (Ideals(S), \to, \subseteq)$ of $\mathscr{S} = (S, \to, \leq)$.

Let us prove that s_j is coverable from x in $\mathscr{S}$ if and only if $\downarrow s_j$ is coverable (for inclusion) from $\downarrow x$ in $\hat{\mathscr{S}}$. Suppose that s_j is coverable from x then there exists a run $x \xrightarrow{k} y \geq s_j$. From [7, Proposition 30], there exist an ideal J and a run $\downarrow x \xrightarrow{k} J$ where $J \supseteq \downarrow y \supseteq \downarrow s_j$ in $\hat{\mathscr{S}}$, hence $\downarrow s_j$ is covered from $\downarrow x$. Conversely, if $I \xrightarrow{k} J$ in $\hat{\mathscr{S}}$ with $\downarrow s_j \subseteq J$ then there exists $x \in I$ and $y' \geq s_j$ such that $x \xrightarrow{k} y' \geq s_j$ in $\mathscr{S}$ and then s_j is coverable from x in $\mathscr{S}$.

Hence we obtain: $\mathscr{S}$ is resilient iff for all $i = 1, .., n$ and $j = 1, ..m$, $\downarrow s_j$ is coverable from ideal J_i in $\hat{\mathscr{S}}$. Let us denote by $k_{i,j}$ the length of a covering sequence that covers $\downarrow s_j$ from J_i in $\hat{\mathscr{S}}$ and let $k_{i,j} \stackrel{\text{def}}{=} \infty$ if $\downarrow s_j$ is not coverable from J_i. Let us now define $K_{\mathscr{S}}(\mathsf{Safe}) = \max(k_{i,j} \mid i = 1, .., n \text{ and } j = 1, ..m)$.

We now have $\mathscr{S}$ is resilient iff $K_{\mathscr{S}}(\mathsf{Safe})$ is finite iff $\mathscr{S}$ is $K_{\mathscr{S}}(\mathsf{Safe})$-resilient with $K_{\mathscr{S}}(\mathsf{Safe})$ finite.

This implies that resilience and bounded resilience can be reduced to coverability. Since coverability is decidable for post-ideal-effective WBTS [7, Theorem 44], we deduce that both the resilience problem and the bounded resilience problem are decidable.

Let us now show that the k-resilience problem, with $k \in \mathbb{N}$, is also decidable. Let us denote by $k'_{i,j}$ the *minimal* length of a covering sequence that covers $\downarrow s_j$ from J_i in $\hat{\mathscr{S}}$ if it exists and let $k'_{i,j} \stackrel{\text{def}}{=} \infty$ if $\downarrow s_j$ is not coverable from J_i. If $\downarrow s_j$ is coverable from J_i, we first compute an $k_{i,j}$, and then we compute $k'_{i,j}$ by iteratively checking whether there exists a sequence of length $0, 1, ..., k_{i,j} - 1$ that covers $\downarrow s_j$ from J_i until we find the minimal one which is necessarly smaller (or equal to) than $k_{i,j}$.

Let us now define $K'_{\mathscr{S}}(\mathsf{Safe}) = \max(k'_{i,j} \mid i = 1, .., n \text{ and } j = 1, ..m)$ and we deduce that $\mathscr{S}$ is k-resilient iff $k \geq K'_{\mathscr{S}}(\mathsf{Safe})$. □

Theorem 5. *Let $\mathscr{S} = (S, \to, \leq)$ be a pred-basis-effective WSTS and a set $\mathsf{Safe} = \uparrow \mathsf{Safe}$.* Resilience *is decidable.*

Proof. The resilience problem can be reformulated as $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$ that is equivalent to $\mathsf{Bad} \cap (S \setminus \mathsf{pred}^*(\mathsf{Safe})) = \emptyset$. The set $\mathsf{pred}^*(\mathsf{Safe})$ is upward-closed, since Safe is upward-closed. Since $\mathscr{S} = (S, \to, \leq)$ is pred-basis-effective, we can compute a basis of $\mathsf{pred}^*(\mathsf{Safe})$. Since the wqo is ideally-effective, we can compute the intersection of Bad and $S \setminus \mathsf{pred}^*(\mathsf{Safe})$, which are both downward-closed, and test if this intersection is empty or not. Hence, the resilience problem is decidable. □

Strong compatibility implies furthermore the decidability of k-resilience and bounded-resilience.

Corollary 1. *Let $\mathscr{S} = (S, \to, \leq)$ be a pred-basis-effective WSTS with strong compatibility and a set $\mathsf{Safe} = \uparrow \mathsf{Safe}$.* Bounded resilience *and* k-resilience *are decidable.*

Proof. For strongly compatible WSTS, $\mathsf{pred}^k(\mathsf{Safe}) = \uparrow \mathsf{pred}^k(\mathsf{Safe})$, and hence $\mathsf{pred}^{\leq k}(\mathsf{Safe}) = \uparrow \mathsf{pred}^{\leq k}(\mathsf{Safe})$, when $\mathsf{Safe} = \uparrow \mathsf{Safe}$. Since $\mathscr{S} = (S, \to, \leq)$ is pred-basis-effective, we can compute a basis of $\uparrow \mathsf{pred}^{\leq k}(\mathsf{Safe}) = \mathsf{pred}^{\leq k}(\mathsf{Safe})$. Like above, we can test if the intersection of Bad and $S \setminus \mathsf{pred}^{\leq k}(\mathsf{Safe})$ is empty or not, hence k-resilience is decidable. To decide Bounded resilience, we check k-resilience starting with $k = 0$ until we find some k_0 such that either k_0-resilience holds, either $\mathsf{pred}^{\leq k_0}(\mathsf{Safe}) = \mathsf{pred}^{\leq k_0+1}(\mathsf{Safe})$, whichever comes first. The convergence of $(\mathsf{pred}^{\leq k}(\mathsf{Safe}))_{k \in \mathbb{N}}$ guarantees the latter eventually happens. □

Remark that the above proofs do not make use of the property that Bad is the complement of Safe, simply using $\mathsf{Bad} = \downarrow \mathsf{Bad}$ and $\mathsf{Safe} = \uparrow \mathsf{Safe}$, thus the above results still hold in the more general case where Bad and Safe are

not complements of each others. Remark furthermore that reset-VASS are pred-basis-effective hence satisfy the conditions from Theorem 5 which thus implies decidability of Resilience, Bounded resilience and k-resilience in reset-VASS in the case $\mathsf{Safe} = \uparrow \mathsf{Safe}$.

3.2 Case: $\mathsf{Safe} = \downarrow \mathsf{Safe}$.

Let us now consider the case $\mathsf{Safe} = \downarrow \mathsf{Safe}$ hence $\mathsf{Bad} = \uparrow \mathsf{Bad}$. It is of interest to note this case can be linked to the problem of mutual exclusion. Indeed the well-known mutual exclusion property can be modeled, in a d-VASS with d counters, by the property that a special counter c_{mutex} must be bounded by $k \geq 1$ which counts the (maximal) number of processes that are allowed to be simultaneously in the critical section. Then, the set $\mathsf{Safe} = \{c_{mutex} \leq k\} \times \mathbb{N}^{d-1}$ is downward-closed and $\mathsf{Bad} = \{c_{mutex} \geq k+1\} \times \mathbb{N}^{d-1}$ is the upward-closed complementary of Safe.

Theorem 6. Resilience *is decidable for pred^*-basis-effective downward-WBTS with $\mathsf{Safe} = \downarrow \mathsf{Safe}$.*

Proof. Let $\mathscr{S}$ be a pred^*-basis-effective downward-WBTS with $\mathsf{Safe} = \downarrow \mathsf{Safe}$. By Lemma 1, $\mathsf{pred}^*(\mathsf{Safe})$ is downward-closed; moreover, $\mathsf{pred}^*(\mathsf{Safe})$ is computable because $\mathscr{S}$ is pred^*-basis-effective. The resilience problem can be reformulated as $\mathsf{Bad} \cap (S \setminus \mathsf{pred}^*(\mathsf{Safe})) = \emptyset$. Since $\leq$ is ideally-effective, we can compute complementaries and intersections of upward and downward-closed subsets. Hence we can compute $S \setminus \mathsf{pred}^*(\mathsf{Safe})$ and then the intersection of Bad and $S \setminus \mathsf{pred}^*(\mathsf{Safe})$, which are both upward-closed. We may decide whether this intersection is empty, hence the resilience problem is decidable. □

In the case of a pred^*-basis-effective WBTS, not necesarly downward compatible, the above construction can provide a proof of non-resilience i.e. when $\mathsf{Bad} \cap (S \setminus \downarrow \mathsf{pred}^*(\mathsf{Safe})) \neq \emptyset$ then $\mathsf{Bad} \not\subseteq \downarrow \mathsf{pred}^*(\mathsf{Safe})$ and hence $\mathsf{Bad} \not\subseteq \mathsf{pred}^*(\mathsf{Safe})$. When $\mathsf{Bad} \cap (S \setminus \downarrow \mathsf{pred}^*(\mathsf{Safe})) = \emptyset$ however it is not enough to conclude.

Remark we did not make use of the property Bad complement of Safe, simply $\mathsf{Bad} = \uparrow \mathsf{Bad}$ and $\mathsf{Safe} = \downarrow \mathsf{Safe}$, thus the above results still hold in the more general case where Bad and Safe are not complements of each others.

4 State-resilience

Resilience is a strong property that implies that from every element there must exist a path to Safe. However, when one considers a system with an initial state s_0, it could be sufficient to only ask that from $\mathsf{post}^*(s_0)$, there must exist a path to Safe. The three previous problems become:

STATE RESILIENCE PROBLEMS

INPUT: A transition system $\mathscr{S} = (S, \rightarrow)$, $s \in S$, and a set $\mathsf{Safe} \subseteq S$.
QUESTION: (STATE-RESILIENCE PROBLEM (SRP)) $\mathsf{post}^*(s) \longrightarrow^* \mathsf{Safe}$?
(k-STATE-RESILIENCE PROBLEM (kSRP)) $\mathsf{post}^*(s) \longrightarrow^{\leq k} \mathsf{Safe}$?
(BOUNDED-STATE-RESILIENCE PROBLEM (BSRP)) $\exists k \geq 0$ such that $\mathsf{post}^*(s) \longrightarrow^{\leq k} \mathsf{Safe}$?

Remark that STATE-RESILIENCE is HOME-SPACE with input set Safe. Since these problems are undecidable for general infinite-state transition systems, we still restrict our study to WSTS. As in the Section 3, we study decidability results for Safe downward-closed and upward-closed.

4.1 Case: $\mathsf{Safe} = \uparrow\mathsf{Safe}$

We start with the case $\mathsf{Safe} = \uparrow\mathsf{Safe}$. Unfortunately, in this case STATE-RESILIENCE is undecidable for (general) WSTS even with strong upward-compatibility. This stems from the fact that it is undecidable in the particular case of reset-VASS, where t-liveness is both undecidable and reducible to STATE-RESILIENCE. This undecidability result furthermore implies the undecidability of the other two state resilience problems by straightforward reductions.

A control-transition t of a reset-VASS is *live* in a state $r(\mathbf{w})$ if for each $q(\mathbf{v}) \in \mathsf{post}^*(r(\mathbf{w}))$ there exists two states $p(\mathbf{u}), p'(\mathbf{u'})$ such that $q(\mathbf{v}) \rightarrow^* p(\mathbf{u}) \xrightarrow{t} p'(\mathbf{u'})$. We say that the whole reset-VASS is live if all its control-transitions are live. This leads to the following problem.

t-LIVENESS

INPUT: A reset-VASS $V = (Q, T)$ of dimension d, a transition $t \in T$, an initial state $s_0 \in Q \times \mathbb{N}^d$
QUESTION: Is t live in s_0 ?

Let us define the set of states, $\mathsf{pre}(t)$, from which a control-transition t is enabled: $\mathsf{pre}(t) = \{p(\mathbf{u}) \in Q \times \mathbb{N}^d \mid \exists q(\mathbf{v}) \in Q \times \mathbb{N}^d \text{ such that } p(\mathbf{u}) \xrightarrow{t} q(\mathbf{v})\}$. Remark that $\mathsf{pre}(t)$ is upward-closed.

Proposition 3. *t-LIVENESS is reducible to STATE-RESILIENCE in reset-VASS.*

Proof. We reformulate t-liveness in a reset-VASS (Q, T) with initial state s_0 as the following formula

$$\forall p(\mathbf{u}) \in Q \times \mathbb{N}^d,\ s_0 \rightarrow^* p(\mathbf{u}) \implies \exists q(\mathbf{v}) \in \mathsf{pre}(t),\ p(\mathbf{u}) \rightarrow^* q(\mathbf{v})$$

The previous formula reduces itself to STATE-RESILIENCE where $\mathsf{Safe} = \mathsf{pre}(t)$. □

It now remains to argue why t-LIVENESS is undecidable. Recall ZERO-REACHABILITY in reset-VASS is undecidable [3]. The following Proposition is a variation to reset-VASS of [24, Theorem 5.5] originally stated for Petri nets, whose proof can be seen in Appendix B.

Proposition 4. ZERO-REACHABILITY *can be reduced to* t-LIVENESS.

Since ZERO-REACHABILITY for reset-VASS is undecidable [8], the reduction implies t-LIVENESS is undecidable. We deduce undecidability by reduction to STATE-RESILIENCE, and straightforward reductions to the other two state resilience problems, as detailed in Appendix B.

Proposition 5. STATE-RESILIENCE, BOUNDED-STATE-RESILIENCE *and* k-STATE-RESILIENCE *are undecidable for reset-VASS, hence for strongly compatible,* post*-effective,* pred*-basis-effective* ω^2*-WSTS when* $\mathsf{Safe} = \uparrow \mathsf{Safe}$.

Recall that on the other hand RESILIENCE is decidable for reset-VASS when $\mathsf{Safe} = \uparrow \mathsf{Safe}$ by Theorem 5. This suggests that the undecidability of STATE-RESILIENCE comes more from the fact $\uparrow \mathsf{post}^*(s_0)$ is not constructible in reset-VASS - a consequence of the undecidability of reachability - rather than from the difficulties inherent in searching for paths from $\mathsf{post}^*(s_0)$ to Safe.

On the positive side, let us recall a result about BOUNDED-STATE-RESILIENCE (called resilience in [21, 22]).

Theorem 7 (Theorem 1, [21], Theorem 1, [22]). BOUNDED-STATE-RESILIENCE *and* k-STATE-RESILIENCE *are decidable for* pred*-basis-effective,* post**-basis-effective WSTS with strong compatibility when* $\mathsf{Safe} = \uparrow \mathsf{Safe}$.

The proof of Theorem 7 rely on the computability of $\uparrow \mathsf{post}^*(s)$ and on the following lemma.

Lemma 2. *Let* $A \subseteq S$, $D \subseteq S$ *be a downward-closed set and* $U \subseteq S$ *be an upward-closed set. Then* $A \cap D \subseteq U$ *iff* $(\uparrow A) \cap D \subseteq U$.

Özkan [21] argues that it is precisely the WSTS for which the following problem is decidable.

DOWNWARD-REACHABILITY PROBLEM

INPUT: A transition system $\mathscr{S} = (S, \to)$, $s \in S$ and a downward-closed set $D \subseteq S$.

QUESTION: $s \to^* D$?

Proposition 6 (Proposition 1, [21]). *For* post*-effective,* pred*-basis-effective finite-branching WSTS, a finite basis of* $\uparrow \mathsf{post}^*(s)$ *is computable for every state* s *iff the downward-reachability problem is decidable.*

The idea behind the proof is the following. For deciding whether a downward-closed set D is reachable from s, one checks whether $B_{\uparrow \mathsf{post}^*(s)} \cap D = \emptyset$, where $B_{\uparrow \mathsf{post}^*(s)}$ is a basis of $\uparrow \mathsf{post}^*(s)$, that is equivalent to $\mathsf{post}^*(s) \cap D = \emptyset$ by Lemma 2. For the converse direction, one computes the sequence of upward-closed sets $U_n = \uparrow \mathsf{post}^{\leq n}(s)$ until it becomes stationnary. Decidability of downward-reachability leads to the decidability of the following stop condition: asking whether $S \setminus U_n$ is reachable from s.

For instance, VASS are post^*-basis-effective WSTS [22]. It is well-known that VASS are WSTS with strong compatibility and since there is an algorithm that computes a finite basis of $\uparrow \mathsf{post}^*(s)$, [21] deduced that Bounded-state-resilience is decidable for VASS. Hence State-resilience is decidable for VASS.

However, the hypothesis that $\uparrow \mathsf{post}^*$ is computable cannot be tested in the general WSTS framework. Moreover there exist classes of WSTSs with strong compatibility for which there doesn't exist an algorithm computing a basis of $\uparrow \mathsf{post}^*$, such as reset-VASS.

Keeping the $\uparrow \mathsf{post}^*$ effectiveness hypothesis but *loosening* the strong compatibility one still yields some decidability result for the general State-resilience. Using the same proof structure as Theorem 1 from [22] we obtain:

Theorem 8. State-resilience *is decidable for* pred*-basis-effective,* post^**-basis-effective WSTS when* $\mathsf{Safe} = \uparrow \mathsf{Safe}$.

Proof. Let $\mathscr{S}$ be a pred-basis-effective, post^*-basis-effective WSTS. Since $\mathscr{S}$ is post^*-basis-effective, let $B_{\uparrow \mathsf{post}^*(s)}$ be a finite basis of $\uparrow \mathsf{post}^*(s)$, hence $\uparrow \mathsf{post}^*(s) = \uparrow B_{\uparrow \mathsf{post}^*(s)}$. Let B_{Safe} be a finite basis of Safe, hence $\mathsf{Safe} = . \uparrow B_{\mathsf{Safe}}$. Since $\mathscr{S}$ is pred-basis-effective, we may compute a finite basis $B_{\mathsf{pred}^*(\mathsf{Safe})}$ of $\mathsf{pred}^*(\mathsf{Safe})$ from B_{Safe}. By applying Lemma 2 twice, we obtain that

$$\mathsf{post}^*(s) \subseteq \mathsf{pred}^*(\mathsf{Safe}) \text{ iff } \uparrow \mathsf{post}^*(s) \subseteq \mathsf{pred}^*(\mathsf{Safe})$$

Now the last inclusion is equivalent to:

$$\uparrow B_{\uparrow \mathsf{post}^*(s)} \subseteq \uparrow B_{\mathsf{pred}^*(\mathsf{Safe})} \text{ iff } \forall b \in B_{\uparrow \mathsf{post}^*(s)} \exists b' \in B_{\mathsf{pred}^*(\mathsf{Safe})} \text{ such that } b' \leq b$$

Since both $B_{\uparrow \mathsf{post}^*(s)}$ and $B_{\mathsf{pred}^*(\mathsf{Safe})}$ are finite, State-resilience is decidable. □

However when removing strong compatibility, some precision is lost. Since $\mathsf{pred}(\uparrow \mathsf{Safe})$ is not necessarily upward-closed, it is possible to have $\uparrow \mathsf{post}^*(s) \cap S \not\subseteq \mathsf{pred}(\mathsf{Safe})$, despite having $\mathsf{post}^*(s) \cap S \subseteq \mathsf{pred}(\mathsf{Safe})$. In such a case, the algorithm in [21] would deduce that 1-state-resilience does not hold, which is incorrect.

Thus in case of post^*-basis-effective WSTS (when the compatibility is not strong), we don't know the decidability status of k-state-resilience and Bounded-state-resilience.

4.2 Case: $\mathsf{Safe} = \downarrow \mathsf{Safe}$

We now consider the case $\mathsf{Safe} = \downarrow \mathsf{Safe}$. Unfortunately State-resilience is undecidable in this case. This stems from undeciability of zero-reachability in reset-VASS, as seen in the reduction proof of Proposition 2.

Proposition 7. State-resilience *is undecidable for reset-VASS when* $\mathsf{Safe} = \downarrow \mathsf{Safe}$*, hence also for* post*-effective,* pred*-basis-effective* ω^2*-WSTS with strong compatibility.*

Despite this, it is possible to yield positive results. Indeed, in many ways the case where $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$ is symmetrical to the case $\mathsf{Safe} = {\uparrow}\mathsf{Safe}$. We will need the following lemma in order to obtain symmetrical results.

Lemma 3. *(Symmetrical from Lemma 2) Let $A \subseteq S$, $D \subseteq S$ be a downward-closed set and $U \subseteq S$ be an upward-closed set. Then $A \cap U \subseteq D$ iff $({\downarrow}A) \cap U \subseteq D$.*

In the case of a WBTS with *downward* compatibility, not necessarily strong, then Safe downward-closed implies $\mathsf{pred}^*(\mathsf{Safe})$ downward-closed and Lemma 3 can be used to show that if $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$, then $\mathsf{post}^*(s) \subseteq \mathsf{pred}^*(\mathsf{Safe})$ iff $({\downarrow}\mathsf{post}^*(s)) \subseteq \mathsf{pred}^*(\mathsf{Safe})$.

Theorem 9. STATE-RESILIENCE *is decidable for post-effective, post-ideal-effective and pred^*-basis-effective WBTS with downward and upward compatibilities and $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$.*

Proof. Since $\mathscr{S}$ is pred^*-basis-effective, $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$ and $\mathsf{pred}^*(\mathsf{Safe}) = {\downarrow}\mathsf{pred}^*(\mathsf{Safe})$, we may compute the finite decomposition in ideals of $\mathsf{pred}^*(\mathsf{Safe})$.

In order to decide whether $\mathsf{post}^*(s) \subseteq \mathsf{pred}^*(\mathsf{Safe})$, we execute two procedures in parallel, one looking for a resilience certificate and one looking for a non-resilience certificate.

Procedure 1 enumerates every downward-closed subsets in some fixed order D_1 , D_2 , ... by their ideal decomposition. The computability of the enumeration comes from the hypothesis that $\leq$ is ideally-effective (Lemma 4.3. from [6]). The procedure then checks for every downward-closed subset D_i whether ${\downarrow}\mathsf{post}(D_i) \subseteq D_i$ (this inclusion is decidable because $\mathscr{S}$ is post-ideal-effective). Every subset D_i such that ${\downarrow}\mathsf{post}(D_i) \subseteq D_i$ is an "over-approximation" of ${\downarrow}\mathsf{post}^*(s)$ if it contains s. Notice that, by upward compatibility, ${\downarrow}\mathsf{post}^*(s)$ is such a subset and may eventually be found.

Procedure 1 stops when it finds a downward-closed subset D such that ${\downarrow}\mathsf{post}(D) \subseteq D$, $s \in D$ and $D \subseteq \mathsf{pred}^*(\mathsf{Safe})$.

Indeed $D \subseteq \mathsf{pred}^*(\mathsf{Safe})$ implies ${\downarrow}\mathsf{post}^*(s) \subseteq \mathsf{pred}^*(\mathsf{Safe})$ since ${\downarrow}\mathsf{post}^*(s) \subseteq D$.

The second procedure iteratively computes $\mathsf{post}^{\leq n}(s)$ (this is effective because $\mathscr{S}$ is post-effective) until it finds an element not in $\mathsf{pred}^*(\mathsf{Safe})$.

If resilience hold, then procedure 1 terminates since it eventually finds $D = {\downarrow}\mathsf{post}^*(s)$ such that $D \subseteq \mathsf{pred}^*(\mathsf{Safe})$. If resilience does not hold, then procedure 2 terminates since there exists a witness that resilience does not hold which can eventually be found. □

In the case of strong downward compatibility, $\mathsf{pred}^{\leq k}(\mathsf{Safe})$ is downward-closed when Safe is. Hence, assuming a pred^*-basis-effective variation consisting in an algorithm accepting any ideal I and returning a finite basis of ${\downarrow}\mathsf{pred}(I)$, it becomes possible to perform the same procedures as above except with comparisons against $\mathsf{pred}^{\leq k}(\mathsf{Safe})$ rather than $\mathsf{pred}^*(\mathsf{Safe})$, and hence k-STATE-RESILIENCE and BOUNDED-STATE-RESILIENCE are decidable in this case.

Corollary 2. k-STATE-RESILIENCE *and* BOUNDED-STATE-RESILIENCE *are decidable for post-effective, post-ideal-effective WBTS, strong downward compatibility*

and upward compatibility when $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$ *and there exists an algorithm accepting any ideal* I *and returning a finite basis of* ${\downarrow}\mathsf{pred}(I)$.

post-effective, post-ideal-effective WSTS, strong downward compatibility and upward compatibility include for instance Lossy Channel Systems with insertions [2].

5 Resilience for VASS and variations

In this section we study VASS. Since they enjoy many properties of effectivity ($\leq$ is ideally-effective, VASS are post-effective, post-ideal-effective, pred-basis-effective, post^*-basis-effective), they inherit the decidability results for WSTS in the case $\mathsf{Safe} = {\uparrow}\mathsf{Safe}$. Lacking downward compatibility or a more relaxed hypothesis that for all downward-closed set D, the set $\mathsf{pred}^*(D)$ is downward-closed, VASS do not inherit the decidability results for WSTS in the case $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$. In this section, we work to re-establish decidability results for VASS when Safe is downward-closed and $\mathsf{Bad} = S \setminus \mathsf{Safe}$. We also extend decidability to resilience for semilinear sets rather than simply upward and downward-closed ones.

Surprisingly, when Safe is downward-closed, we have the following result for VAS (not VASS):

Proposition 8. Bounded resilience *and* k-resilience *never hold for* d*-VAS when* $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$ *and* $\mathsf{Safe} \neq \mathbb{N}^d$.

Proof. Consider a given $k \in \mathbb{N}$, $\mathsf{Safe} \subseteq \mathbb{N}^d$ is downward-closed such that its upward-closed complement $\mathsf{Bad} \subseteq \mathbb{N}^d$ is nonempty, and consider a given VAS V. Let us call $c_{\max}$ the maximal absolute value of a constant appearing in a coordinate of a transition of V. The set $\mathsf{Bad} \neq \emptyset$ admits a finite basis B_{Bad}. Consider the vector $\mathbf{v}_{\mathsf{Bad}}$ obtained by summing all members of the basis of Bad and then consider the vector $\mathbf{u}_k = \mathbf{v}_{\mathsf{Bad}} + (k+1) \cdot (c_{\max}, c_{\max}, \ldots, c_{\max})$.

All states reachable from $\mathbf{u}_k$ in k or less steps are above $\mathbf{v}_{\mathsf{Bad}}$ and thus, are in Bad, by upward-closedness. Hence Safe is not reachable from $\mathbf{u}_k$ in k or less steps and k-resilience does not hold. Since the reasoning hold for all $k \in \mathbb{N}$, Bounded-resilience does not hold either. □

This all changes when one considers VASS (having control-states). For a VASS $V = (Q, T)$, a set $\mathsf{Bad} = {\uparrow}\mathsf{Bad}$, for all $q \in Q$, either there is an element of the basis of Bad with control-state q — then $q(\mathbf{v})$ with $\mathbf{v} > \mathbf{v}_{\mathsf{Bad}}$ is necessarily in Bad by upward closure; if this hold for all $q \in Q$, then k-resilience does not hold — either there is none. If there is none, then ${\uparrow}q(\mathbf{0})$ is in the complement of Bad, i.e. Safe. Based on this, we partition Safe into two subsets: an upward-closed union of sets of the form ${\uparrow}q(\mathbf{0})$, and a remaining downward-closed subset. The key now is that there is only a finite number of elements of Bad of the form $p(\mathbf{v})$ with $\mathbf{v} \leq \mathbf{u}_k$ for all of which we will check reachability of Safe in k or less steps, while elements of Bad of the form $p(\mathbf{v})$ with $\mathbf{v} > \mathbf{u}_k$ can only potentially reach the upward-closed subset of Safe in k or less steps. Only being concerned by

the upward-closed subset of Safe in the latter case enable us to reuse techniques seen when Safe is upward-closed. Indeed we can compute the basis for the sets of elements from which our upward-closed subset of Safe is reachable in at most k steps. Substracting these predecessor from Bad yields either a finite number of elements from which one has to check Safe is reachable in at most k steps, either an infinite number of elements of which there is one which cannot reach Safe in at most k steps - for much the same reasons Bounded resilience and k-resilience never hold for VAS when $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$ and $\mathsf{Bad} = {\uparrow}\mathsf{Bad}$. We check the finiteness of the set by comparing the elements from the finite basis of both upward-closed sets. This leads to a decision procedure detailed in appendix C, which lead to the following decidability result:

Theorem 10. *k-resilience and Bounded resilience are decidable for VASS when $\mathsf{Safe} = {\downarrow}\mathsf{Safe}$.*

Let us now extend decidability of Resilience for semilinear sets and VASS variants. $\mathbb{Z}^d-$VASS (resp. $\mathbb{Z}-$VASS) [15] are d-VASS (resp. VASS) that are allowed to take values from the integers.

Theorem 11. Resilience *is decidable for VASS, and $\mathbb{Z}-$VASS, when Safe is a semilinear set.*

Proof. We consider the case where Safe is semilinear and $\mathsf{Bad} = S \setminus \mathsf{Safe}$ is semilinear too. We want to use the fact that, for VASS, it is decidable whether $\mathsf{post}^*(X) \subseteq \mathsf{pred}^*(Y)$ when X and Y are both semilinear sets [18]. Resilience asks whether $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$. We have $\mathsf{post}^*(\mathsf{Bad}) \setminus \mathsf{Safe} = \mathsf{Bad}$ by extension of $S \setminus \mathsf{Safe} = \mathsf{Bad}$. Thus $\mathsf{post}^*(\mathsf{Bad}) = \mathsf{Bad} \cup (\mathsf{Safe} \cap \mathsf{post}^*(\mathsf{Bad}))$. Since $(\mathsf{Safe} \cap \mathsf{post}^*(\mathsf{Bad})) \subseteq \mathsf{pred}^*(\mathsf{Safe})$, we have

$$\mathsf{post}^*(\mathsf{Bad}) \subseteq \mathsf{pred}^*(\mathsf{Safe}) \quad \text{iff} \quad \mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe}).$$

and hence, Resilience is decidable. The reachability relation of $\mathbb{Z}^d-$VASS is definable by a well-formed formula with no free variables in the first-order theory of the integers with addition and orders (Presburger arithmetic) in $\mathbb{Z}^{2d}$, hence $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$ is decidable when Safe and Bad are semilinear sets. □

Resilience is also decidable for other classes of counter machines for which the reachability relation can be expressed in a decidable logic. Recall that lossy counter machines (LCM) [28] are counter machines that may loose tokens in each control-state.

Resilience and the home-space problem are also linked to the model-checking of basic reachability and safety formulae. In particular [28] shows that the "from-all" formula $\forall s \in X\ \exists t \in Y\ s \to^* t$ is decidable for lossy counter machine when X and Y are semi-linear sets. Other decidable formulae include "one-to-one" ($\exists s \in X\ \exists t \in Y\ s \to^* t$), and "all-to-same" ($\exists t \in Y\ \forall s \in X\ s \to^* t$), whereas "one-to-all" ($\exists s \in X\ \forall t \in Y\ s \to^* t$), "all-to-all" ($\forall s \in X\ \forall t \in Y\ s \to^* t$) and "to-all" ($\forall t \in Y\ \exists s \in X\ s \to^* t$) are undecidable (again, for LCM).

Theorem 12. RESILIENCE *is decidable for lossy counter machines when* Safe *is a semilinear set.*

Proof. We deduce from [28, Theorem 3.6] that $\mathsf{pred}^*(\mathsf{Safe})$ is a computable semilinear set if Safe is semilinear. Hence since the inclusion between two semilinear sets is decidable, we deduce that $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$ is decidable if Bad is semilinear. □

$\mathbb{Q}^d$-VASS [5] (or continuous VASS) are a relaxation of classical (discrete) d-VASS in which transitions can be fired a fractional number of times, and consequently counters may contain a fractional number of tokens.

Theorem 13. RESILIENCE *is decidable for continuous VASS when* Safe *is definable in the existential theory of the rationals with addition and order.*

Proof. The reachability relation of continuous VASS is definable by a sentence of linear size in the existential theory of the rationals with addition and order whose complexity is EXPSPACE [5]. Hence, $\mathsf{Bad} \subseteq \mathsf{pred}^*(\mathsf{Safe})$ is decidable (and also in EXPSPACE). □

Remark that Theorem 12 (resp. Theorem 13) did not make use of the hypothesis that Bad is the complement of Safe, simply relying on the semilinearity of the set (resp. its definability in the existential theory of the rationals with addition and order). Thus the mentionned theorems still hold in the more general case where Bad and Safe are not complements of each others.

6 Conclusion and perspectives

We complemented previous results (decidability of two state-resilience problems for a restricted class of WSTS in [25, 22, 21]) by providing some undecidability proofs for resilience and state-resilience in general. We exhibited classes of WBTS, WSTS, VASS and extensions of VASS with decidable resilience.

Several questions still remain. For instance, we have been concerned with decidability only, and a detailed complexity analysis of the different resilience problems still remains to be done for concrete models. Another question could be to analyse the resilience in the framework of a controller and its environment. One could also extend upon the classes of set Safe considered. As with semilinear sets for VASS, one could study resilience for sets defined in a boolean logic on upward and downward-closed subsets [4]. Finally, while we mention VASS, a more detailed analysis of the resilience problems could be also done for other computational models such as pushdown automata, one-counter automata or timed automata.

Acknowledgements

We express our thanks to the reviewers of the VMCAI 2024 Conference for their numerous and relevant comments and improvement suggestions.

References

1. Abdulla, P.A., Cerans, K., Jonsson, B., Tsay, Y.: Algorithmic analysis of programs with well quasi-ordered domains. Inf. Comput. **160**(1-2), 109–127 (2000). https://doi.org/10.1006/inco.1999.2843, https://doi.org/10.1006/inco.1999.2843
2. Abdulla, P.A., Jonsson, B.: Verifying programs with unreliable channels. Inf. Comput. **127**(2), 91–101 (1996). https://doi.org/10.1006/inco.1996.0053, https://doi.org/10.1006/inco.1996.0053
3. Araki, T., Kasami, T.: Some decision problems related to the reachability problem for petri nets. Theoretical Computer Science **3**(1), 85–104 (1976)
4. Bertrand, N., Schnoebelen, P.: Computable fixpoints in well-structured symbolic model checking. Formal Methods Syst. Des. **43**(2), 233–267 (2013). https://doi.org/10.1007/s10703-012-0168-y, https://doi.org/10.1007/s10703-012-0168-y
5. Blondin, M., Finkel, A., Haase, C., Haddad, S.: The logical view on continuous petri nets. ACM Trans. Comput. Log. **18**(3), 24:1–24:28 (2017). https://doi.org/10.1145/3105908, https://doi.org/10.1145/3105908
6. Blondin, M., Finkel, A., McKenzie, P.: Well behaved transition systems. Log. Methods Comput. Sci. **13**(3) (2017). https://doi.org/10.23638/LMCS-13(3:24)2017, https://doi.org/10.23638/LMCS-13(3:24)2017
7. Blondin, M., Finkel, A., McKenzie, P.: Handling infinitely branching well-structured transition systems. Information and Computation **258**, 28–49 (2018). https://doi.org/10.1016/j.ic.2017.11.001
8. Dufourd, C., Finkel, A., Schnoebelen, P.: Reset nets between decidability and undecidability. In: International Colloquium on Automata, Languages, and Programming. pp. 103–115. Springer (1998)
9. Dufourd, C., Jancar, P., Schnoebelen, P.: Boundedness of reset P/T nets. In: Wiedermann, J., van Emde Boas, P., Nielsen, M. (eds.) Automata, Languages and Programming, 26th International Colloquium, ICALP'99, Prague, Czech Republic, July 11-15, 1999, Proceedings. Lecture Notes in Computer Science, vol. 1644, pp. 301–310. Springer (1999). https://doi.org/10.1007/3-540-48523-6_27, https://doi.org/10.1007/3-540-48523-6_27
10. Finkel, A.: Reduction and covering of infinite reachability trees. Inf. Comput. **89**(2), 144–179 (1990). https://doi.org/10.1016/0890-5401(90)90009-7, https://doi.org/10.1016/0890-5401(90)90009-7
11. Finkel, A., Goubault-Larrecq, J.: Forward analysis for wsts, part II: complete WSTS. Log. Methods Comput. Sci. **8**(3) (2012). https://doi.org/10.2168/LMCS-8(3:28)2012, https://doi.org/10.2168/LMCS-8(3:28)2012
12. Finkel, A., McKenzie, P., Picaronny, C.: A well-structured framework for analysing petri net extensions. Information and Computation **195**(1-2), 1–29 (2004)
13. Finkel, A., Schnoebelen, P.: Well-structured transition systems everywhere! Theor. Comput. Sci. **256**(1-2), 63–92 (2001). https://doi.org/10.1016/S0304-3975(00)00102-X, https://doi.org/10.1016/S0304-3975(00)00102-X
14. de Frutos Escrig, D., Johnen, C.: Decidability of home space property. Université de Paris-Sud. Centre d'Orsay. Laboratoire de Recherche en Informatique, Rapport de recherche n°503 (1989)
15. Haase, C., Halfon, S.: Integer vector addition systems with states. In: Ouaknine, J., Potapov, I., Worrell, J. (eds.) Reachability Problems - 8th International Workshop, RP 2014, Oxford, UK, September 22-24, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8762, pp. 112–124. Springer (2014). https://doi.org/10.1007/978-3-319-11439-2_9, https://doi.org/10.1007/978-3-319-11439-2_9

16. Halfon, S.: On Effective Representations of Well Quasi-Orderings. (Représentations Effectives des Beaux Pré-Ordres). Ph.D. thesis, University of Paris-Saclay, France (2018), https://tel.archives-ouvertes.fr/tel-01945232
17. Jancar, P.: A note on well quasi-orderings for powersets. Inf. Process. Lett. **72**(5-6), 155–160 (1999). https://doi.org/10.1016/S0020-0190(99)00149-0, https://doi.org/10.1016/S0020-0190(99)00149-0
18. Jancar, P., Leroux, J.: Semilinear home-space is decidable for petri nets. CoRR **abs/2207.02697** (2022). https://doi.org/10.48550/arXiv.2207.02697, https://doi.org/10.48550/arXiv.2207.02697
19. Lazic, R., Newcomb, T.C., Ouaknine, J., Roscoe, A.W., Worrell, J.: Nets with tokens which carry data. Fundam. Informaticae **88**(3), 251–274 (2008), http://content.iospress.com/articles/fundamenta-informaticae/fi88-3-03
20. Memmi, G., Vautherin, J.: Analysing nets by the invariant method. In: Brauer, W., Reisig, W., Rozenberg, G. (eds.) Petri Nets: Central Models and Their Properties, Advances in Petri Nets 1986, Part I, Proceedings of an Advanced Course, Bad Honnef, Germany, 8-19 September 1986. Lecture Notes in Computer Science, vol. 254, pp. 300–336. Springer (1986). https://doi.org/10.1007/BFb0046843, https://doi.org/10.1007/BFb0046843
21. Özkan, O.: Decidability of resilience for well-structured graph transformation systems. In: Behr, N., Strüber, D. (eds.) Graph Transformation - 15th International Conference, ICGT 2022, Held as Part of STAF 2022, Nantes, France, July 7-8, 2022, Proceedings. Lecture Notes in Computer Science, vol. 13349, pp. 38–57. Springer (2022). https://doi.org/10.1007/978-3-031-09843-7_3, https://doi.org/10.1007/978-3-031-09843-7_3
22. Özkan, O., Würdemann, N.: Resilience of well-structured graph transformation systems. In: Hoffmann, B., Minas, M. (eds.) Proceedings Twelfth International Workshop on Graph Computational Models, GCM@STAF 2021, Online, 22nd June 2021. EPTCS, vol. 350, pp. 69–88 (2021). https://doi.org/10.4204/EPTCS.350.5, https://doi.org/10.4204/EPTCS.350.5
23. Patriarca, R., Bergström, J., Di Gravio, G., Costantino, F.: Resilience engineering: current status of the research and future challenges. Safety Science **102** (02 2018). https://doi.org/10.1016/j.ssci.2017.10.005
24. Peterson, J.L.: Petri net theory and the modeling of systems. Prentice Hall PTR (1981)
25. Prasad, S., Zuck, L.D.: Self-similarity breeds resilience. In: Gebler, D., Peters, K. (eds.) Proceedings Combined 23rd International Workshop on Expressiveness in Concurrency and 13th Workshop on Structural Operational Semantics, EXPRESS/SOS 2016, Québec City, Canada, 22nd August 2016. EPTCS, vol. 222, pp. 30–44 (2016). https://doi.org/10.4204/EPTCS.222.3, https://doi.org/10.4204/EPTCS.222.3
26. Schmitz, S.: The complexity of reachability in vector addition systems. ACM SIGLOG News **3**(1), 4–21 (2016). https://doi.org/10.1145/2893582.2893585, https://doi.org/10.1145/2893582.2893585
27. Schmitz, S., Schnoebelen, P.: Algorithmic Aspects of WQO Theory (Aug 2012), https://cel.hal.science/cel-00727025, lecture
28. Schnoebelen, P.: Lossy counter machines decidability cheat sheet. In: Kucera, A., Potapov, I. (eds.) Reachability Problems, 4th International Workshop, RP 2010, Brno, Czech Republic, August 28-29, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6227, pp. 51–75. Springer (2010). https://doi.org/10.1007/978-3-642-15349-5_4, https://doi.org/10.1007/978-3-642-15349-5_4

29. Valk, R., Jantzen, M.: The residue of vector sets with applications to decidability problems in petri nets. Acta Informatica **21**, 643–674 (1985). https://doi.org/10.1007/BF00289715, https://doi.org/10.1007/BF00289715

A Proofs of technical lemmas

We have omitted proofs for Lemma 1 and Lemma 2 up until now since these are fairly straightforward technical proofs. We provide now both.

Lemma 1. *For an ordered transition system $\mathscr{S} = (S, \to, \leq)$ (not necessarily a WSTS), the two following properties are equivalent: (1) $\mathscr{S} = (S, \to, \leq)$ is downward compatible ; (2) for every downward-closed set $D \subseteq S$, the set $\mathsf{pred}^*(D)$ is downward-closed.*

Proof. Let us prove 1 $\implies$ 2. Let D be a downward-closed subset of S and let $x \in \downarrow \mathsf{pred}^*(D)$. By downward closure, there exists $y \in \mathsf{pred}^*(D)$ such that $x \leq y$. By definition of $\mathsf{pred}^*(D)$, there exists $d \in D$ such that: (1) either $y = d$ and then $x \in D \subseteq \mathsf{pred}^*(D)$ or (2) there exist $m \geq 0$ and $(a_i)_{0 \leq i \leq m+1} \in S^{m+2}$ such that $y = a_0 \to a_1 \to a_2 \to \cdots \to a_m \to a_{m+1} = d$. By downward compatibility $a_0 \to a_1$ implies that there exists $a'_1 \in S$ such that $a'_1 \leq a_1$ and $x \to^* a'_1$. More generally $a_i \to a_{i+1}$ and $a'_i \leq a_i$ implies the existence of $a'_{i+1} \in S$ with $a'_{i+1} \leq a_{i+1}$ and $a'_i \to^* a'_{i+1}$, and, by induction, $x \to^* a'_1 \to^* \cdots \to^* a'_m \to^* a'_{m+1} = d'$ with $d' \leq d$. Since d' belongs to D by downward closure of D, $x \in \mathsf{pred}^*(D)$ and then $\downarrow \mathsf{pred}^*(D) \subseteq \mathsf{pred}^*(D)$. Since $\mathsf{pred}^*(D) \subseteq \downarrow \mathsf{pred}^*(D)$ always hold, we deduce that $\mathsf{pred}^*(D) = \downarrow \mathsf{pred}^*(D)$ is downward-closed.

Let us prove 2 $\implies$ 1. Let $s_1, t_1, s_2 \in S$ with $s_2 \leq s_1$ and $s_1 \to t_1$, Since $s_1 \to t_1$ we deduce that $s_1 \in \mathsf{pred}^*(\downarrow t_1)$, and since $s_2 \leq s_1$ and $\mathsf{pred}^*(\downarrow t_1)$ is downward-closed, we also have $s_2 \in \mathsf{pred}^*(\downarrow t_1)$. This means that there exists $t_2 \leq t_1$ such that $s_2 \to^* t_2$. Hence, we proved that $\mathscr{S}$ is downward compatible. □

Lemma 2. *Let $A \subseteq S$, $D \subseteq S$ be a downward-closed set and $U \subseteq S$ be an upward-closed set. Then $A \cap D \subseteq U$ iff $(\uparrow A) \cap D \subseteq U$.*

Proof. Let us suppose that $A \cap D \subseteq U$. Then $\uparrow(A \cap D) \subseteq \uparrow U = U$. Let us show that $(\uparrow A) \cap D \subseteq \uparrow(A \cap D)$. Let $x \in (\uparrow A) \cap D$, then there exists $a \in A$ such that $x \geq a$. Since $x \in D$ and D is downward-closed, we also have $a \in D$. Hence $a \in A \cap D$ and then $x \in \uparrow(A \cap D)$. In the other direction, since $A \subseteq \uparrow A$, the inclusion $(\uparrow A) \cap D \subseteq U$ implies $A \cap D \subseteq (\uparrow A) \cap D \subseteq U$. □

B Reset-VASS and state-resilience

Let us recall the *zero-reachability* problem in (reset-)VASS.

ZERO-REACHABILITY

INPUT: A d-reset-VASS $V = (Q, T)$, $q_f \in Q$ and $p(\mathbf{u}) \in Q \times \mathbb{N}^d$.

QUESTION: $p(\mathbf{u}) \rightarrow^* q_f(\mathbf{0})$?

ZERO-REACHABILITY is decidable in VASS and it is undecidable in reset-VASS [3]. For a better representation, we will use reset Petri nets [8] rather than reset-VASS. A *reset Petri net* $N = (P, T, E, R, \mu)$ consists of a finite set of *places* $P = \{p_1, p_2, ...p_{|P|}\}$, a finite set of *transitions* $T = \{t_1, t_2, ..., t_{|T|}\}$, a finite set of *arcs* $E \subseteq (P \times T) \cup (T \times P)$, a finite set of *reset-arcs* $R \subseteq T \times P$, and an *initial marking* $\mu : P \rightarrow \mathbb{N}$. It is well-known that Petri nets and VASS are equivalents models with regards of the decidability of reachability problems: an d-VASS can be encoded into a Petri net with $d + 2$ places and conversely, a Petri net with p places can be encoded into a p-VASS [26]. The same equivalence hold between reset-VASS and reset Petri nets.

We will show that ZERO-REACHABILITY can be reduced to t-LIVENESS in reset Petri nets; this is done by "adjusting" a similar result for Petri nets [24, Theorem 5.5].

Proposition 4. *In reset Petri nets,* ZERO-REACHABILITY *can be reduced to* t-LIVENESS.

We may then deduce that:

Corollary *In reset-VASS,* ZERO-REACHABILITY *can be reduced to* t-LIVENESS.

Proof. If we wish to determine if a marking in which every place is empty is reachable for a reset Petri net $N_1 = (P_1, T_1, E_1, R_1, \mu_1)$ we construct a reset Petri net $N_2 = (P_2, T_2, E_2, R_2, \mu_2)$ which is live in N_2 if and only if the *zero marking*, which assigns 0 to every place of P_1, is not reachable from μ_1 in N_1.

Construction of N_2

The reset Petri net N_2 is constructed from N_1 by the addition of two places p_a and p_b and $|P_1| + 2$ transitions t_{p_a}, $\{t_p \mid p \in P_1\}$ and t_{p_b}. We first modify all transitions of N_1 to include p_a as both an input and an output. The initial marking μ_2 will include a token in p_a and no token in p_b. This new place p_a serve to mark that the run is ongoing. As long as it contains a token, the adjusted transitions of N_1 are live and can be used normally. Thus any marking which is reachable in the places of N_1 is also reachable in the corresponding places of N_2. We add an additional transition t_{p_a} which has p_a as an input and a null output. This allows to disable the transitions of N_1 and to "freeze" the marking of the places of P_1 in N_2. The place p_a and transition t_{p_a} allow the net N_2 to reach any reachable marking in N_1 and then for t_{p_a} to fire and freeze the net at that marking. We introduce a new place p_b and new transitions t_p, for all $p \in P_1$, which have p as input and p_b as output. Lastly, we add a transition t_{p_b} with p_b as its output and every place of P_2 as output, which "floods" the net with tokens, assuring that every transition is live in N_2 if a token is ever put in p_2.

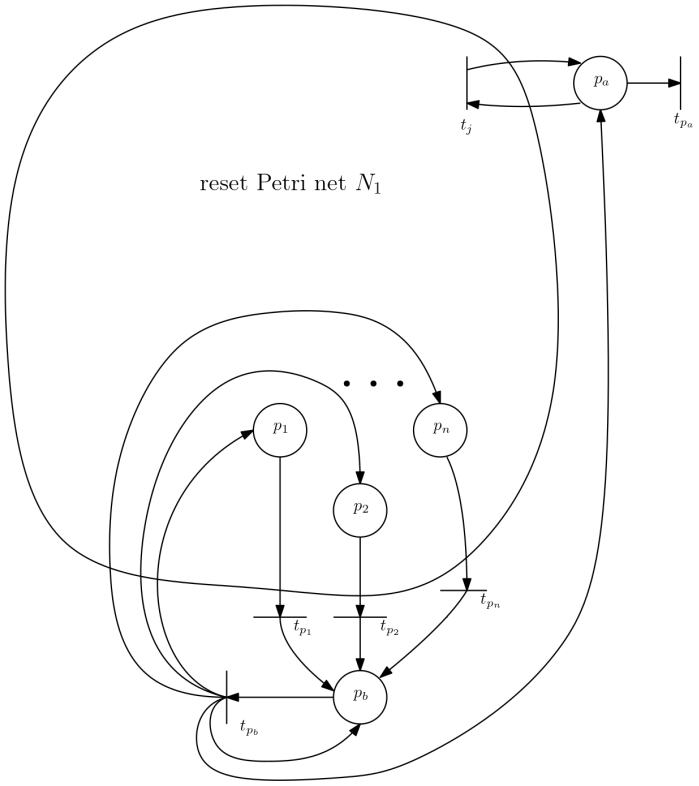

Fig. 3: Construction of N_2 from N_1.

Let us now prove that t_{p_2} is live in N_2 if and only if the zero marking is not reachable from μ_1 in N_1.

Suppose that the zero marking is reachable from μ_1 in N_1, then t_{p_2} is not live in N_2.

Indeed the marking with zero in every place of P_1 and in p_b is reachable in N_2, by executing the same sequence of transition firings. Then t_{p_a} can fire, leading to the marking which assigns zero to every place of P_2. From this marking the transitions t_p are not live and neither are the transitions inherited from N_1 nor t_{p_a}, and, finally, nor is t_{p_2}. Thus t_{p_2} is not live in N_2.

Suppose that t_{p_2} is not live in N_2, then the zero marking is reachable from μ_1 in N_1

Indeed, if t_{p_2} is not live in N_2, then a marking μ must be reachable in which $\mu(p_2) = 0$ and there is no reachable state in which p_2 has a token (in particular, since we do not allow token removal from p_2, the marking μ must be reached in a sequence of transitions that do not place any token in p_2). This means that no transition t_p is live in N_2 in μ since any transition t_p can place a token in p_2. Thus, every place of P_2 inherited from N_1 must be devoid of token. Moreover, since the marking μ must be reached in a sequence of transitions that do not place any token in p_2, it can be reached without using the transitions t_p or t_{p_2}. Since t_{p_a} do not modify the places inherited from P_1 nor does it enable new transitions, the reachability of μ implies the reachability of a marking where every place of P_2 inherited from P_1 is devoid of token using only the transitions inherited from N_1. Thus the zero marking is reachable from μ_1 in N_1.

Since ZERO-REACHABILITY for reset-VASS is undecidable, the reduction implies t-LIVENESS is undecidable as well. This leads to the undecidability of STATE RESILIENCE, BOUNDED-STATE-RESILIENCE and k-STATE-RESILIENCE. The first follows straight from Proposition 3, while the other two follow from straightforward reductions we nonetheless develop in more details here.

Proposition 5. STATE-RESILIENCE, BOUNDED-STATE-RESILIENCE *and* k-STATE-RESILIENCE *are undecidable for reset-VASS, hence for strongly compatible,* post*-effective,* pred*-basis-effective WSTS when* $\mathsf{Safe} = \uparrow \mathsf{Safe}$.

Proof. Since ZERO-REACHABILITY for reset-VASS is undecidable [8], the previous reduction (Proposition 4) implies t-LIVENESS is undecidable. Because t-LIVENESS is undecidable in reset-VASS and reducible to STATE-RESILIENCE, we also deduce that STATE-RESILIENCE is undecidable for reset-VASS, which are WSTS with strong compatibility. Additionally, in WSTS with strong compatibility and effective pred-basis, BOUNDED-STATE-RESILIENCE is reducible to k-STATE-RESILIENCE: since $\mathsf{Safe} = \uparrow \mathsf{Safe}$ and $\mathscr{S} = (S, \to, \leq)$ is a WSTS with strong compatibility, then $\mathsf{pred}^{\leq n}(\mathsf{Safe}) = \uparrow\ \mathsf{pred}^{\leq n}(\mathsf{Safe})$ for all $n \in \mathbb{N}$, and there exists $n_0 \in \mathbb{N}$ such that $\mathsf{pred}^{\leq n_0}(\mathsf{Safe}) = \uparrow \mathsf{pred}^{\leq n_0}(\mathsf{Safe}) = \uparrow \mathsf{pred}^*(\mathsf{Safe}) = \mathsf{pred}^*(\mathsf{Safe})$. We compute n_0, then iteratively check whether k-state-resilience hold for k from 0 to n_0. Furthermore, in WSTS with strong compatibility and effective pred-basis,

$\mathsf{Safe} = \uparrow \mathsf{Safe}$, Bounded-state-resilience is equivalent to State-resilience, since $\mathsf{pred}^{\leq n_0}(\mathsf{Safe}) = \uparrow \mathsf{pred}^{\leq n_0}(\mathsf{Safe}) = \uparrow \mathsf{pred}^*(\mathsf{Safe}) = \mathsf{pred}^*(\mathsf{Safe})$. Hence the undecidability of Bounded-state-resilience and k-state-resilience. □

C Decision procedure for VASS when $\mathsf{Safe} = \downarrow \mathsf{Safe}$

Theorem 10. *k-resilience and Bounded resilience are decidable for VASS when $\mathsf{Safe} = \downarrow \mathsf{Safe}$.*

Proof. Let V be a given d-VASS and consider a given $k \in \mathbb{N}$. Consider $\mathsf{Bad} \subseteq Q \times \mathbb{N}^d$ upward-closed and $\mathsf{Safe} = S \setminus \mathsf{Bad}$ downward-closed. Let us call $c_{\max}$ the maximal absolute value of a constant appearing in a coordinate of a transition.

The set Bad admits a finite basis $B_{\mathsf{Bad}} = \{q_{i_1}(\mathbf{v}_{i_1}), q_{i_2}(\mathbf{v}_{i_2}), \ldots, q_{i_m}(\mathbf{v}_{i_m})\}$. Consider the vector $\mathbf{v}_{\mathsf{Bad}} = \Sigma_{1 \leq j \leq m} \mathbf{v}_{i_j}$, and then consider the vector $\mathbf{u}_k = \mathbf{v}_{\mathsf{Bad}} + (k+1) \cdot (c_{\max}, c_{\max}, \ldots, c_{\max})$. For all $p \in Q$, all states reachable from $p(\mathbf{u}_k)$ in k or less steps are of the form $q(\mathbf{v})$ with $\mathbf{v} > \mathbf{v}_{\mathsf{Bad}}$.

For all $q \in Q$, either there is an element of the basis of Bad with state q — then $q(\mathbf{v})$ with $\mathbf{v} > \mathbf{v}_{\mathsf{Bad}}$ is necessarily in Bad by upward closure; if this hold for all $q \in Q$, then k-resilience does not hold — either there is none. If there is none, then $\uparrow q(\mathbf{0})$ is in the complement of Bad, i.e. Safe.

Let us assume from now on $\uparrow q_{j_1}(\mathbf{0}), \uparrow q_{j_2}(\mathbf{0}), \ldots \uparrow q_{j_\ell}(\mathbf{0})$ are all subsets of Safe and that their union contain all upward-closed subsets of Safe. Because these subsets are upward-closed, we can compute a basis of $\mathsf{pred}^{\leq k}(\uparrow q_{j_1}(\mathbf{0}))$, $\mathsf{pred}^{\leq k}(\uparrow q_{j_2}(\mathbf{0}))$, $\ldots$ $\mathsf{pred}^{\leq k}(\uparrow q_{j_\ell}(\mathbf{0}))$.

We now consider the set $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k}(\uparrow q_{j_\ell}(\mathbf{0})))$. We inductively check for any element in the set whether or not it is possible to reach from it the set Safe in k or less steps. If the set is finite then we stop the procedure once we have found a witness that k-resilience does not hold or once we have checked for every element, whichever comes first. If it is infinite then k-resilience does not hold, hence we eventually find a witness that k-resilience does not hold. Indeed, if $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k}(\uparrow q_{j_\ell}(\mathbf{0})))$ is infinite then there exists an element of the form $q(\mathbf{u})$ with $\mathbf{u} > \mathbf{v}_{\mathsf{Bad}} + (k+1) \cdot (c_{\max}, \ldots, c_{\max})$ that is in Bad but not in any of the $\mathsf{pred}^{\leq k}(\uparrow q_{j_i}(\mathbf{0}))$, and hence from which it is not possible at all to reach Safe in k or less steps. This also means that, even in the case where $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k}(\uparrow q_{j_\ell}(\mathbf{0})))$ is finite, we only need to check reachability of Safe in k or less steps for the elements with vectorial component at most $\mathbf{v}_{\mathsf{Bad}} + (k+1) \cdot (c_{\max}, \ldots, c_{\max})$. Binding the search space thus leads to an EXPSPACE upper bound for k-resilience.

In order to deal with Bounded resilience now, remark that there exists some $k_0 \in \mathbb{N}$ for which and hence $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k_0}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k_0}(\uparrow q_{j_\ell}(\mathbf{0})) = \mathsf{Bad} \setminus (\mathsf{pred}^*(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \mathsf{pred}^*(\uparrow q_{j_\ell}(\mathbf{0})))$. We start the decision procedure by checking k-resilience from 0 until k_0.

From k_0 onwards, $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k}(\uparrow q_{j_\ell}(\mathbf{0})) = \mathsf{Bad} \setminus (\mathsf{pred}^*(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \mathsf{pred}^*(\uparrow q_{j_\ell}(\mathbf{0})))$ is stationnary. We check the finiteness of the set by comparing the elements from the finite basis of Bad and $(\mathsf{pred}^{\leq k_0}(\uparrow q_{j_1}(\mathbf{0})) \cup$

$\ldots \cup \mathsf{pred}^{\leq k_0}(\uparrow q_{j_\ell}(\mathbf{0}))$. As an example, in dimension 2, for an upward-closed set U, $(\uparrow q(n,m)) \setminus U$ is finite if and only if U contains an element of the form $q(n',m')$ with $m' \geq m$ and $n' \leq n$, and one of the form $q(n'',m'')$ with $n'' \geq n$ and $m'' \leq m$. Indeed, if it does, then elements of $\uparrow q(n,m)$ with coordinates sufficiently large are greater than these and thus belong to U by upward-closedness. If not, then either the infinite set $\{q(n,m') \mid m' \geq m\}$ or the infinite set $\{q(n',m) \mid n' \geq n\}$ belong to $\uparrow q(n,m) \setminus U$ which is hence not finite.

If the set $\mathsf{Bad} \setminus (\mathsf{pred}^*(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \mathsf{pred}^*(\uparrow q_{j_\ell}(\mathbf{0})))$ is finite then we stop the procedure once we have checked for every element whether it is possible to reach Safe from it. If it is possible to reach Safe from every element then k_m-RESILIENCE hold for $k_m = \max(k_0, k_\pi)$ with k_π the maximum of the length of the paths from $\mathsf{Bad} \setminus (\mathsf{pred}^{\leq k_0}(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^{\leq k_0}(\uparrow q_{j_\ell}(\mathbf{0}))$ to Safe. If the set is infinite then for every $k \in \mathbb{N}$, k-resilience does not hold, and we eventually find a witness that k-resilience does not hold. Indeed, if $\mathsf{Bad} \setminus (\mathsf{pred}^*(\uparrow q_{j_1}(\mathbf{0})) \cup \ldots \cup \mathsf{pred}^*(\uparrow q_{j_\ell}(\mathbf{0})))$ is infinite then there exists an element of the form $q(\mathbf{u})$ with $\mathbf{u} > \mathbf{v}_{\mathsf{Bad}} + (k+1) \cdot (c_{\max}, \ldots, c_{\max})$ that is in Bad but not in any of the $\mathsf{pred}^{\leq k}(\uparrow q_{j_i}(\mathbf{0}))$, and hence from which it is not possible at all to reach Safe in k or less steps. □