Sujet : VMCAI 2024 notification for paper 30
De : “VMCAI 2024” <vmcai2024@easchair.org>
Date : 11/10/2023 17:25
Pour : Alain Finkel <alain.finkel@ens-paris-sacla.fr>

Dear Alain Finkel,

We are delighted to inform you that your submission titled

Resilience and Home-Space for WSTS

has been conditionally accepted to appear in VMCAI 2024 ***after an additional round of shepherding***.

This year we received 74 submissions of which 30 were accepted.

The reviewers of your paper requested significant changes. Therefore, we have assigned a shepherd to guide you through the process of incorporating those changes in the camera-ready version of your paper and to ensure those changes are made. We will follow up soon with details regarding the shepherding process.

Feel free to get in touch with us with any questions or concerns.

Kind regards,
Rayna Dimitrova
Ori Lahav
PC Chairs for VMCAI 2024

SUBMISSION: 30
TITLE: Resilience and Home-Space for WSTS

----------------------- REVIEW 1 ---------------------
SUBMISSION: 30
TITLE: Resilience and Home-Space for WSTS
AUTHORS: Alain Finkel and Mathieu Hilaire

----------- Overall evaluation -----------
SCORE: -1 (weak reject)
----- TEXT:
This paper addresses the problem of resilience in WSTS. Resilience can be formulated as follows: given a set SAFE of states, is it true that from any BAD (non-safe) state of a system one can reach SAFE ? The question can be made more precise, by specifying the initial state of the system. Bounded versions of resilience ask to return to SAFE in at most k steps, or ask if such a k exists.

This paper considers resilience for Well-Structured Transition Systems (WSTS), that is transitions systems equipped with a partial order relation on states that is compatible with the transition relation. Being Well-Structured is not sufficient to guarantee decidability of properties. For instance, decidability is usually achieved when the WSTS has effective algorithms to compute bases for upward or downward sets of predecessors. Former works [15,16] have proved decidability of resilience for WSTS with strong compatibility, upward closure of SAFE, downward closure of Bad states, and an additional hypothesis to guarantee effectiveness of a basis calculus for the upward closure of the set of successors of a state, but never addressed the general question of decidability of resilience in WSTS.

Two contributions of the paper are a proof that resilience is already undecidable for WSTS with strong compatibility, and
a demonstration that one needs additional hypotheses to get decidability.

The second section of the paper recalls basic definitions and results : Thm 1 recalls that coverability of an upward
closed set of states is decidable for effective WSTS with an effective pred basis calculus.
This is a standard decidable framework for WSTS.
Thm 2 recalls a similar result for ideal-effective WSTS when the ordering on states has only finite antichains.
The notion of ideal-effectiveness is less standard and is defined in three points: possibility to give a function to compute the ideal
of \downarrow(s), decidability of ideals inclusion, and possibility to encode \downarrow(Post(I)) with a finite union of ideals. If it
seems clear that such systems allow for calculus of coverings of sets of states via manipulation of finite sets of bases,
the type of models enjoying this property is less obvious, and an example would be welcome.

Section 2 addresses the resilience problem, first in a setting where Safe = \uparrow(safe) and bad = \downarrow(bad).

Thm 3 proves that resilience and its bounded variants are decidable for \omega^2-WSTS that are completion-post-effective
(this second property means that there exists algorithms to decompose the complement of an upward closed set into ideals).
However, the class of \omega^2-WSTS is not really defined. As this is a non-standard notion, this is really a miss, which makes
difficult to see which models are contained in this class. The second result of this part is that resilience is undecidable for WSTS
in general if the system does not satisfy completion-post-effectiveness. Surprisingly, this result is not presented as a theorem.

The next setting considered is when safe=\downarrow(safe).
Thm 4 shows that resilience is decidable for ideal-effective WSTS where downward closure is preserved by pred*(). A corollary is
that resilience is decidable for ideal-effective WSTS that are downward-compatible. Without the downward closure property,
resilience is undecidable. This is for instance the case for RESET-VASS. Remark that Reset-VASS have strong compatibility.
Here it would be interesting to locate this class in a detailed taxonomy of WSTS classes. The table provided at the end of
section 3 is not sufficent to establish such a taxonomy, and is rather misleading because results are presented depending
on the properties of the SAFE set. However characterisitics of WSTS classes yield dedicability or not, regardless of the
closure properties of SAFE.

Section 4 considers resilience when the initial state is specified, first for the case Safe =\uparrow(safe).
In RESET-VASS zero reachability can be reduced to this question, yielding undecidability of resilience for RESET-VASS and more
generally for WSTS with strong compatibility and an effective pred basis. Theorem 6 recalls that bounded state resilience is decidable
for WSTS with strong compatibility and where \uparrowpost*(s) is computable. This result extends to state resilience. However,
one cannot check in general if \uparrow post*(s) is computable.
Theorem establishes a more pragmatic result, showing that state resilience is decidable in the case safe =\uparrow(safe) for WSTS with an
effective calculus of a basis for \uparrow post*(s) (and one can notice that this result does not require strong compatibility).

The second part of section 4 considers the case safe=\downarrow(safe). Theorem 8 shows that state resilience is undecidable
for WSTS with strong compatibility. Theorem 9 shows that state resilience is decidable for ideal-effective WSTS with upward
and downward compatibility. Corollary 3 shows that bounded state resilience is also decidable for this class. Unfortunately the proof of theorem 9
builds on procedures that "enumerate inductive invariants" without explaining this notion nor

the procedure to compute them.
Again, the paper contains no example of models that satisfy the prerequisite of theorems 9 and corollary 3.

The last section of the paper considers resilience for VASS. Theorem 10 shows that resilience is decidable for VASS when safe is semilinear. This relies on results of [11] on reachability in RdPs. Theorem 11 shows that resilience is decidable for lossy counter machines when safe is semilinear, and Thm 12 for integer VASS. This property comes from the fact that accessibility can be described in Pressburger artihmetics.
Theorem 13 is its analogue for continuous VASS when SAfe is defined in the existential theory of reals with addition and order.

Proposition 4 shows that for VAS, bounded resilience never holds when safe is downward closed.
Finally, Theorem 14 shows that the bounded resilience is decidable for VASS when safe = \downarrow(safe)

Conclusion :
============

This paper presents numerous results (14 theorems and 4 propositions) but some choices in its organization make the article rather difficult to read and use.
The introduction is particularly technical, and accessible only to readers who have already read the article, or are already well familiar with WSTS and resilience.
Another criticism is that the paper initially presents the results as decidability in subclasses of WSTS for an upward / downward closed safe set. It then addresses resilience via decidabillity for particular models (VASS variants) with semi-linear safe sets, before returning to downward closed Safe sets. Overall, it is not easy to figure in which class of WSTS a particular model fits, nor how the models of a given class look like. This is especially the case for the class \omega^{2}
In the same way, we can consider that the example at the bottom of page 8, even if it is a WSTS, is a very particular case very different from VASS, lossy counter, Petri nets, communicating automata, etc. and wonder if classes containing such systems are interesting per se.
Clearly, a taxonomy of the subclasses and models presented in the article is missing.

The proofs of Theorems 9 and 14 in the article lack of details w.r.t. the decision procedures and their termination.

Verdict:
=========

Though I have no doubt on the presented results, I think this paper can be improved, and made more readable with a different organization, a taxonomy of WSTS classes, and a few corrections/precisions in proofs.

Detailed remarks:
==================

- Mainy notions used in the introduction are not yet defined : pre^*(X) post^*(X), upward and refelxive downward compatibilities, strong compatibility, \omega^{2}-WSTS and are only defined later in the paper
-Section 2, def. of upward and downward closure : shouldn't y \geq a be x \geq a ?
- Section 2, page 5. The various classes ou WSTS should be compared. What type of model

populates the class of ideal effective WSTS ?
- Section 3, page 7 : A simiar remark holds for the class od \$\omega^2-WSTS. First, no definition of \$\omega^2-WSTS is given. Then, in theorem 3 the decidability result holds for "completion-post-effective \omega^2-WSTS with strong compatibility. Again, what are the type of WSTS that lay in this class and not in others ?
- Section 3.2, page 9 : should "ideally effective " be ideal-effective ?
Regarding Thm 4 and its corollary, one would like to see non-trivial examples of systems that are ideal-effective,
meet conditions of theorem 4, and are not downward compatible.
- Page 10 : the table does not realy summarizes the result of the section, because the identfied subclasses of WSTS are not
mentionned. This makes the table rather ambiguous, because for instance in the safe=\downward safe case, resilience is decidable in some
classes, but undecidable for WSTS in general.
- page 12, propositions 1 & 2 : it is not clear why adressing t-liveness is required, since zero reachability is already undeidable
and reductions seem rather easy.
- page 14 in the table, 3rd column, according to thm 7 one should read \uparrow post * basis effective.

- proof of theorem 9: the proof is too fast. Procedure 1 enumerates inductive invariants : this notion was never addressed before,
so what is an invariant, and how is it computed ?
-Corollary 3 seems to be a consequence of thm 9. However downward compatibility is transformed into strong downward compatibility.
Is it a typo or is it on purpose ?

- Proof of theorem 14 and paragraph before : I found the explanations unclear. In the large, the decision procedure
either checks for a finite number of elements that Safe is reachable (no problem for this side) or from an infinite set of elements
that there exists one that cannot reach safe that can be found. The proof lack a detailed explanation on this procedure on infinite
sets of elements and on why it necessarily terminates.
----------- Reviewer's confidence -----------
SCORE: 3 ((medium))

----------------------- REVIEW 2 ---------------------
SUBMISSION: 30
TITLE: Resilience and Home-Space for WSTS
AUTHORS: Alain Finkel and Mathieu Hilaire

----------- Overall evaluation -----------
SCORE: 1 (weak accept)
----- TEXT:
The paper studies the verification of resilience properties for well-structured transition systems (WSTS). WSTS are a well-known programming model that, despite its expressiveness, admits decision procedures for important verification problems, notably for safety. The resilience problem asks wheter a system is able to recover: is it true that from every bad state there is a path to a good state? The resilience problem thus comes with a quantifier alternation that makes it difficult to apply techniques for safety verification.

The authors contribute a number of decidability and undecidability results for resilience verification on classes of WSTS. The results can be classified along the axes: notions of resilience, upward-/downward-closed/semi-linear sets of safe/bad states, updward/downward compatibility of WSTS transitions, strong/weak compatibility of WSTS transitions, effectiveness assumptions on WSTS. I should say that all effectiveness assumptions are known from the literature and well-justified. I cannot say whether the variants of the resilience problem are relevant.

I find the paper technically interesting but presentation-wise not well-done. It is technically interesting in that the arguments used in the (un)decidability proofs are non-trivial. I admit that these arguments are often rooted in known (and deep) results, and thus one could argue they are not that novel. I would like to see it differently, and take the paper as another demonstration of the versatility of these results. A highlight for me was the study of resilience for VAS and the insight that it never holds (I had not seen the argumentation before).

The presentation needs a major overhaul. There is a large number of typos and type-setting mistakes, some theorems rely on assumptions that are only mentioned in the proof (like bad having some shape), the same sentence is repeated in two consecutive paragraphs, there are two very similar proofs of auxiliary lemmas, and the introduction needs the concrete definition of resilience to be readable.

Hard to judge, I trust that the authors will carefully revise the paper to fix these issues, and then it is a weak accept to me.

Comments:

Proof of Theorem 14, Last Para: Don't you need to argue that this infinity is decidable?

Page 16: Definable by a sentence in Presburger => This is slang, please be more explicit.

Proposition 4: In this part of the paper, you use assumptions like Bad being uc that are not mentioned in the statement of the proposition.

Page 14: "For instance one can write the following lemma" => Rewrite this: we will need the following lemma for this and that.

Proof of Theorem 9, last para: Does the presentation of pred*(Safe) come from ideal effectiveness?

Lemmas 1 and 2 have similar proofs, skip one.

Proof of Theorem 10: Interesting but not well-structured 🙂 Explain the proof goal first.

Page 10: Reset-VASS can simulate Minsky machines: sure, but in a weak way. Why does this not matter for resilience.

k-Resilience on Page 6: Either you make k part of the input or you fix it in the problem statement.

Intro, Page 2: the process and its adversary => this is the first time you mention an adversary.

Proof of Theorem 3: Why are the elements in the basis of Safe denoted with a b while there is also the set of bad states?

You should remind the reader every now and then of the difference between compatibility and strong compatibility.

----------- Reviewer's confidence -----------

SCORE: 4 ((high))

----------------------- REVIEW 3 ---------------------

SUBMISSION: 30

TITLE: Resilience and Home-Space for WSTS

AUTHORS: Alain Finkel and Mathieu Hilaire

----------- Overall evaluation -----------

SCORE: 2 (accept)

----- TEXT:

Synopsis

This paper studies resilience problems over well-structured transition systems (WSTS).
The basic resilience problem asks, given a WSTS and a subset of so-called "safe states" if every state can reach a safe state. Two natural variants are studied: one which asks if there is a uniform bound k such that all state can reach a safe state in at most k steps ("bounded resilience"), and one for which k is part of the input ("k-resilience").
State-resiliency problems are defined analogously, except that the transition systems are equipped with an initial state, and the property of reachability in only required to be verified by states reachable from this initial state.
Trivially, these problems are decidable on finite transition systems, so the paper focuses on infinite ones. For the class of all WSTS (with mild computability assumption making the transition system effectively describable), these problems are easily shown to be undecidable by reduction from well-known problems (see end of §3 and §4-Theorem 5). The main contribution of the paper is to show decidability of some of these problems for subclasses of WSTS, namely:

- Resilience problems are decidable if the safe states are upward-closed and the transition system is an \omega^2-WSTS: thanks to the \omega^2-WSTS assumption, the transition system can be essentially simulated its "completion" (the WSTS of its ideals) ; in this latter system, the resilience problem of the original system can be expressed as a covering property, and is hence decidable.
- Resilience is decidable if the safe states are downward-closed, under some strong assumption on the computability of co-reachable states, by an elementary argument. The complexity for k-resilience and bounded resilience is not known in this case.
- It was already known that bounded-state-resilience and k-state-resilience is decidable for upward-closed safe states, under strong assumptions on the computability of reachable states.

The authors extend these results to show decidability of state-resilience under the same assumptions.

- For downward-closed safety sets, the problem is decidable (Theorem 9) assuming the transition system to be both upward- and downward-compatible, which essentially makes the "naive computation" effective.
- Lastly, the authors focus on VAS(S). They show that for a vector addition system (VAS) can never satisfy the bounded resiliency of k-resiliency property (Proposition 4) assuming the safety set to be downward-closed. I believe that there is a mistake there, and that the authors should furthermore assume the safety state to be distinct from the set of all states for the proof to go through.
- Then, they show (Theorem 14) these two problems to be decidable for VAS with states (VASS) with downward-closed safety set. Essentially, the property boils down to looking at each state of the VASS (of which there is finitely many) individually, and look at there safety set. Solving the problem for this single state is trivial by the previous point.

Recommendation

The resiliency problem seems to be a natural problem over transition systems, and (as often for verification problems) lives at the border between decidability and undecidability. The model studied (WSTS) are well-established models in the community.
I found the paper to be interesting, and I didn't find any major mistake. However, I thought the paper could greatly benefit from more care in the writing process, especially considering that the paper can fell catalogish at times (which is somewhat inevitable from the nature of the problem at hand) and that none of the proof introduce novel techniques. I believe the main strength of this paper is to draw a reasonably exhaustive landscape of the border between decidability and undecidability for resiliency problems: some efforts to make this picture as clear as possible (starting from the introduction) can only help the visibility of this work.
Overall, I recommend to accept the paper, but kindly ask the authors to consider the following suggestions.

Important suggestions & remarks for the authors

- please use $A = \mathop{\downarrow} B$ instead of $A = \downarrow B$: this dangling arrow is typographically horrific!
- Sometimes, your undecidability results are not stated as theorem.
- It would be clearer to only use "Theorem" for your main results, and Propositions/Lemma/etc. for intermediate results & results by other people.
- The tables you have in §3 and §4 are nice, but they are somewhat useless there. It would be much better to put a full table in the introduction, with pointers to the different theorems / sections (or other papers). Don't forget undecidability results. This way, it would be much easier to navigate the paper & understand what are your contributions.
- Proposition 4, p. 16: I believe the assumption Bad \neq \emptyset is needed.
- Section 1: I don't really like the use of the post and pre operation in the introduction; they are not introduced yet in the paper, and using plain english would make the whole thing more intuitive.
- p. 2 : cite the unpublished report even if it is unpublished (actually the paper is available online & backed on https://web.archive.org/
- How to improve your citations: https://www.mimuw.edu.pl/~bojan/posts/how-to-improve-your-citations-with-one-simple-trick

Typos & co.

- p. 2: weird vertical space after "Our contributions:"
- p. 4: in the def° of pred^{\leq n} and pred^* I believe i=0 should be allowed?
- p. 4: "Given X a quasi-ordering" -> "given a quasi-ordering X"
- p. 4: def° of upward-closure / downward-closure : y -> x
- p. 4: provide a ref for the "many equivalent charac of woos", e.g. Halfon's thesis
- p. 4: decomposition of downward-closed sets: ideals are downward-closed, so is there unions, so I do not understand why you used a downward-closure
- p. 5: provide a ref for "several families of formal models (…)"
- p. 5: I don't think coverability was introduced
- p. 6: missing dot in line 6 ; "wqo" -> "woos" ; "one only need" -> "only only needs"
- p. 9: "modelized" -> "modeled"
- p. 9, proof of Coro 1: I think you should allow the a-sequence to be empty
- p. 9, proof of Coro 1: conclude the proof by saying that you apply Theorem 4 to get the conclusion
- p. 10: why not choose \down{(0,0,0)} instead of \down{(1,1,0)}?
- p. 10, around Def 3: inconsistent notation for indices: it is sometimes \gamma, sometimes i
- p. 11: could not parse the end of the sentence beginning with "A control-transition t of a reset-VASS (…)"

- p. 11, following sentence: missing quantification over states
- p. 12, around Theorem 5: the § preceding the theorem & the beginning of the proof are very similar, maybe you can make the § before more concise
- p. 15, proof of Theorem 10: weird typography for "iff"

----------- Reviewer's confidence -----------

SCORE: 3 ((medium))