Scalable Redundancy Detection for Real-Time Requirements

Elisabeth Henkel  
University of Freiburg  
Freiburg, Germany  
0000-0003-3844-8292

Nico Hauff  
University of Freiburg  
Freiburg, Germany  
0000-0002-8972-2776

Lena Funk  
University of Freiburg  
Freiburg, Germany  
0009-0008-0216-0776

Vincent Langenfeld  
University of Freiburg  
Freiburg, Germany  
0000-0001-9835-6790

Andreas Podelski  
University of Freiburg  
Freiburg, Germany  
0000-0003-2540-9489

Abstract—Describing a system in a requirements specification demands correctness and conciseness. Requirements are redundant if they are stated multiple times throughout a specification (explicitly or implicitly). In contrast to vacuity, redundancies do not inherently indicate specification defects, and are sometimes even inevitable to adequately follow safety practices. However, intended redundancies have to be managed to avoid subsequent errors. Unintended redundancies often hint to defects in the requirements specification.

We present an analysis for redundancies in formal real-time requirements specifications based on automata theoretical model checking. To enable this analysis, we introduce a determinism preserving totalization and complement procedure for the timed automaton model of Phase Event Automata. We state the redundancy check for a set of real-time requirements as a program analysis task.

Benchmarks show the viability of our approach to analyse requirements sets of industrial size and complexity: the analysis scales well on industrial sets, interesting redundancies both from requirements and as a formalisation artefact were found.

Index Terms—Formal Requirements Analysis, Real-time Requirements, Redundancy, Vacuity, Phase Event Automata

I. INTRODUCTION

A requirements specification should describe a system that is to be built correctly, completely, and concisely. Requirements that are stated multiple times within a system specification are redundant. This may be because the requirement is stated multiple times identically, or because the conjunction of a set of requirements is already implied by the redundant requirement. While redundancy in itself is not necessarily bad, to some extent it may even increase readability of a requirements document, redundancies have to be managed in order to prevent defects during changes [1], [2]. Nonetheless, redundant requirements often hint to defects in the requirements. Redundancy in a requirements set may be caused by several defects:

A redundancy can be caused by a requirements precondition never being satisfied, caused by the sheer size of the system that is specified. This kind of defect, often called vacuity, can be detected by several requirements analysis tools [3], [4] and has been shown to be found in industry requirements [3]. This kind of redundancy is generally seen as a defect as vacuous requirements serve no function.

A redundancy can also be caused by a requirement being less restrictive than the composition of the remainder of the specification. This kind of redundancy may be intentional, e.g., for regulatory reasons, or due to including requirements from different stakeholders who want to know their specification to be covered. It might also stem from the intentional inclusion of requirements that prioritise over nuances of desirable system properties. The redundancy may also be non-intentional, i.e., hint to an oversight in the design or simple human error during documentation or even formalisation. Nonetheless, the redundancy has to be known, either to be managed during changes or for the requirements to be repaired. Analysis of requirements defects in industry projects has shown that the introduction of redundancies can be as simple as copy-and-paste errors and confusion of system variables can lead to a requirement specification being incomplete but redundant [5].

Formal requirements analysis tools analysing different properties such as consistency and vacuity have shown their usefulness in practical applications [6]–[9]. To our knowledge, none of these tools are able to detect arbitrary redundancy (i.e., more than vacuity, semantic equivalence or per-requirement equivalence) for formal temporal requirements.

In this paper, we present our scalable redundancy analysis for formal requirements in HANFORPL. To enable this analysis, we introduce a determinism preserving totalization and complement procedure for the timed automaton model of Phase Event Automata. Further, we state the redundancy check for a set of real-time requirements as a program analysis task.

A. Motivating example

In the following, we give a motivational example of two requirements where one is subsumed by the other requirement. The following set of requirements is given in the SPL-like [3] requirements language HANFORPL [10], [11]:

\[ r_0: \text{If } y \text{ holds, then } x \geq 5 \text{ holds after at most 3 time units.} \]
\[ r_1: \text{If } y \text{ holds, then } x \geq 5 \text{ holds after at most 5 time units.} \]

One can clearly see that requirement \( r_0 \) is a stronger restriction on the state space of the system than requirement \( r_1 \). This is, the requirements are equivalent except for a weaker time bound in \( r_1 \). It will therefore never have any influence on the state space of the system. Note that, although our example only regards subsumption because of time bounds, our approach is not limited to timing and detects any subsumption, e.g., due to constraints on observables or triviality of a requirement. Also, our approach is not limited to a pair of requirements, but

\[
\text{if } r_0 \text{ holds, then } r_1 \text{ holds after at most 5 time units.}
\]
checks subsumption of any requirement in a set of requirements against the remaining set.

The automatic detection of subsumption that we present in this paper is based on an automaton representation of the requirements. Each requirement in HANFORPL has an equivalent, so-called Phase Event Automaton (PEA). A PEA is a timed automaton over system variables (here a numeric \( x \) and a Boolean \( y \)) and clocks to measure time (\( c \) in Fig. 1). A PEA equivalent to a requirement accepts exactly the executions, i.e., sequences of valuations of system variables and their duration, that are permitted by the requirement. An example PEA of \( r_0 \) is shown in Fig. 1.

A run of a PEA is a sequence of configurations. Each configuration is a tuple of a location in the PEA, a valuation of system variables, a valuation of clocks to track time, and the duration spent in the current configuration. For example, a concrete (initial) configuration \((q_0, \beta_0, \gamma_0, t_0)\) of \( \mathcal{A}_r \) starts in the initial location \( q_0 \) (signified by the inbound arrow), has a valuation of system variables \( \beta_0 = \{x \mapsto 1, y \mapsto \text{false}\} \), has a valuation of clocks \( \gamma_0 \) that fulfils the clock invariant \( x \geq 5 \lor \neg y \), e.g., \( \gamma_0 = \{c \mapsto 0\} \), and a duration \( t_0 \) that does not extend any clock to violate a clock invariant, e.g., \( t_0 = 4.0 \). As the clock invariant is \( \text{true} \), \( t_0 \) does not have an upper bound in \( q_0 \).

To choose a successor configuration, we can either stay in \( q_0 \) by the self-loop, by choosing a similar valuation for variables and clocks, or we transition to location \( q_1 \), for example by choosing \( \beta_1 = \{x \mapsto 1, y \mapsto \text{true}\} \). In this example, we do the latter. Although time advancing by 4, the clock valuation is \( \gamma_1 = \{c \mapsto 0\} \) as the edge between \( q_0 \) and \( q_1 \) resets the clock (\( c := 0 \)). Location \( q_1 \) has the clock invariant \( c \leq 3 \), the duration \( t_1 \) has to be smaller than or equal to 3 as any higher number causes the clock to exceed the clock invariant. We choose \( t_1 = 3 \).

Any further extension of the current run has to set the variable \( x \) such that \( x \geq 5 \). This is because all edges leaving \( q_1 \) either are guarded by \( c < 3 \) guaranteeing that in any successor configuration there remains sufficient (i.e., non-zero) time to fulfil the requirement, which is already exceeded (as \( \gamma(c)_{1 + t_1} = 3 \)), or requires \( x \geq 5 \) as the only remaining edge is guarded by \( x' \geq 5 \) (here \( x' \) refers to the value of \( x \) in the successor configuration).

To demonstrate the redundancy check, we now observe the intersection of the automata \( \mathcal{A}_r \) and \( \mathcal{A}'_r \) (Fig. 1 and Fig. 2). We continue using the run \(((q_0, p_0), \beta_0, \gamma_0, t_0), ((q_1, p_1), \beta_1, \gamma_1, t_1)\) from the initial example. In the intersection, each location is
a tuple of the respective automata. The valuations of clocks and automata are checked against the location invariants, clock invariants and guards of the respective locations and transitions of each automaton. In the intersection, location \((q_1, p_1)\) is reachable. If requirement \(r_1\) is not redundant with \(r_0\), a run has to exist, that reaches \(p_{\perp}\), as it would be a violation of \(r_1\) that is not already prohibited by \(r_0\). All transitions to \(p_{\perp}\) are guarded by \(x' < 5 \land c \geq 5\). Contrary, a continuation of the above run in \(A_{r_0}\) is only possible if \(x \geq 5\) as long as \(c \leq 3\), i.e., there does not exist any extension of the run, that enters \(p_{\perp}\). As \(p_{\perp}\) is not reachable, there is no run in the intersection, and therefore \(r_1\) does not have any influence on the described behaviour of the requirements set \(\{r_1, r_0\}\).

The above search for an accepted word in the intersection can be reduced to a program analysis task where in a program, encoding the intersected automata, reachability of a statement is shown (Section IV). Scalability of this approach is demonstrated in the benchmarks in Section V.

II. PRELIMINARIES

As shown in Fig. 1 and 2, locations and transitions of PEAs are labelled with formulas. Before formally introducing PEAs, we define some notational shortcuts that are useful in this context:

By \(L(V)\), we denote the language of Boolean expressions with free variables in \(V\).

A clock constraint \(\delta_c\) is a formula of the form \(c < t\) or \(c \leq t\). By \(L(C)\), we denote the language of Boolean expressions with clock constraints on clocks in \(C\). A clock invariant \(I\) is the conjunction of clock constraints, i.e., \(I = \bigwedge \delta_c\). By \(I_c(p)\) and \(I_{\leq}(p)\), we denote the two functions that transform the clock invariant \(I\) of a location \(p\) into its strict and non-strict version, respectively. For example, for \(I(p) = c_0 < t_0 \land c_1 \leq t_1\), we get \(I_c(p) = c_0 < t_0 \land c_1 < t_1\) and \(I_{\leq}(p) = c_0 \leq t_0 \land c_1 \leq t_1\).

With a slight abuse of notation, we write \(\delta_c, I(p)\) to denote that clock constraint \(\delta_c\) appears as a conjunct in the clock invariant of location \(p\).

We write \(F = \{s \mapsto B(s) \mid s \in S\}\) to denote a function that maps each element in a set \(S\) to the Boolean predicate \(B(s)\). By \(\neg F\), we then abbreviate the function mapping each element in \(S\) to the negation of \(B(s)\), i.e., \(\neg F = \{s \mapsto \neg B(s) \mid s \in S\}\).

To denote the set of all outgoing transitions of location \(p\), we write \(E(p)\).

A Phase Event Automaton (PEA) is defined as a tuple \(A = (P, V, E, s, I, E_0)\) with the following components:\footnote{We slightly modify the definition of PEAs from [13] to use a set of initial edges instead of a set of initial locations, as we do not assume initial guards to be trivially true.}

- \(P\) being a finite set of locations,
- \(V\) being a finite set of typed variables,
- \(E\) being a finite set of clock variables,
- \(E \subseteq P \times L(V \cup C \cup V') \times Z \times P\) being a set of edges.

An edge is a tuple \((p, g, X, p')\), where \(p\) and \(p'\) represent source and target location, guard \(g\) is a Boolean expression over primed variables in \(V\) and unprimed clock variables in \(C\), and \(X \subseteq C\) is a set of clocks to be reset,

- \(s : P \to L(V)\) is a function labelling each location with a Boolean expression over variables in \(V\), called the location invariant,
- \(I : P \to L(C)\) is a function labelling each location with a Boolean expression over clock constraints, called the clock invariant,
- \(E_0\) being a set of initial edges of the form \((g, p')\) with guard \(g\) and target location \(p'\).

We call a location \(p_0 \in P\) an initial location if there is at least one initial edge \(e \in E_0\) such that \(p_0\) is the target location.

A configuration of a PEA is a tuple \((p, \beta, \gamma, t)\) with location \(p \in P\), variable valuation \(\beta\) for all variables \(v \in V\), clock valuation \(\gamma\) for all clock variables \(c \in C\), and a non-zero duration \(t\).

A run of a PEA is a finite sequence of configurations \(\sigma = (p_0, \beta_0, \gamma_0, t_0), ..., (p_n, \beta_n, \gamma_n, t_n)\). A run \(\sigma\) is accepting if there is an initial edge \((g, p_0) \in E_0\) such that

- the initial guard \(g\) is satisfied by the initial valuation \(\beta_0\) for primed variables and the initial clock valuation \(\gamma_0(c) = 0\), i.e., \(\beta_0, \gamma_0 \models g\),

and for each configuration

- the valuation satisfies the location invariant, i.e., \(\beta_i \models s(p_i)\),
- the clock valuation increased by the duration satisfies the location’s clock invariant, i.e., \(\gamma_i + t_i \models I(p_i)\),

and for every consecutive pair of configurations, there is an edge \((p_i, g, X, p_{i+1}) \in E\) such that

- the guard \(g\) is satisfied by the valuation \(\beta_i\) for unprimed variables, \(\beta_{i+1}^\prime\) for primed variables, and the valuation \(\gamma_i + t_i\) for clock variables, i.e., \(\beta_i, \beta_{i+1}^\prime, \gamma_i + t_i \models g\),
- the later clock valuation resets all clocks in \(X\) and increments all others by duration \(t_i\), i.e., \(\gamma_{i+1}(c) := 0\) if \(c \in X\) and \(\gamma_{i+1}(c) := \gamma_i(c) + t_i\) otherwise.

A sequence of configurations is stutter-free if it cannot be reduced by merging consecutive configurations. Two consecutive configurations \((p_i, \beta_i, \gamma_i, t_i)\) and \((p_{i+1}, \beta_{i+1}, \gamma_{i+1}, t_{i+1})\) can be merged to \((p_i, \beta_i, \gamma_i, t_i + t_{i+1})\) if their location and variable valuations coincide, i.e., if \(p_i = p_{i+1}\) and \(\beta_i = \beta_{i+1}\).

The language \(L(A)\) of a PEA \(A\) is defined as the set of all sequences of valuations and durations \(\pi = (\beta_0, t_0), ..., (\beta_n, t_n)\) corresponding to an accepting run \((p_0, \beta_0, \gamma_0, t_0), ..., (p_n, \beta_n, \gamma_n, t_n)\) in \(A\).

We call a PEA deterministic if and only if it satisfies the following two conditions:

1) for each valuation \(\beta'\), there is at most one initial edge \((g, p) \in E_0\) such that \(\beta' \models g\) and \(\beta' \models s(p)\);
2) for each location \(p \in P\) and pair of valuations \(\beta'\) and \(\gamma\), there is at most one edge \((p, g, X, p') \in E\) such that \(\beta', \gamma \models g\) and \(\beta' \models s(p')\) and \(\gamma \models X := 0\) \(\models I(p)\).

The parallel composition \([14]\) of two PEAs \(A_1\mid A_2\) is defined as the tuple \((P_1 \times P_2, V_1 \cup V_2, C_1 \cup C_2, E, s_1 \cup s_2, I_1 \cup I_2, E_0)\) with \((p_1, p_2), g_1 \land g_2, X_1 \land X_2, (p_1', p_2') \in E\) and \((g_1 \land g_2, (p_1, p_2)) \in E_0\) for every pair of edges in \(E_1\) and \(E_2\), and \(E_0,1\) and \(E_0,2\), respectively. Similarly, we build the parallel composition for more than two PEAs.
We define our notion of redundancy in the style of [15]: A requirement \( r \in \mathcal{R} \) is **redundant** in a set of requirements \( \mathcal{R} \), if
\[
\bigwedge_{\mathcal{R} \setminus \{ r \}} \models r
\]
i.e., the requirements set \( \mathcal{R} \setminus \{ r \} \) is a model for \( r \) without containing \( r \) itself. In other words, \( r \) does not impose any additional restriction on the models fulfilling \( \mathcal{R} \setminus \{ r \} \) already does.

For the remainder of this paper, we assume formal requirements to be written in the formal requirements pattern language HANFORPL. For brevity, we refer the reader to [3], [10] for further detail. Also, we will refer to the requirements only by their equivalent PEA i.e., the PEA accepting the same valuations of system variables over the same durations as the requirement.

### III. Redundancy Checking

In the following, a set of requirements is represented by a set of PEAs \( \mathcal{R} = \{ \mathcal{A}_1, \ldots, \mathcal{A}_m \} \). Thus, to restate the definition of **redundancy** in relation to automata: A requirement \( \mathcal{A}_i \) is redundant in \( \mathcal{R} \setminus \{ \mathcal{A}_i \} \), if it can be omitted, i.e., the system behaviour expressed by the PEAs in the set \( \mathcal{R} \) is equivalent to the system behaviour expressed by the PEAs in the set \( \mathcal{R} \setminus \{ \mathcal{A}_i \} \). This means that there exist PEAs \( \mathcal{A}_j \) with \( j \neq i \) in \( \mathcal{R} \) such that
\[
\bigcap_{\mathcal{A}_j \in \mathcal{R} \setminus \{ \mathcal{A}_i \}} \mathcal{L}(\mathcal{A}_j) \subseteq \mathcal{L}(\mathcal{A}_i).
\]

In order to check a set of requirements for redundancy, we restate **redundancy** as a classical automata theoretical model checking problem [12]:
\[
\overline{\mathcal{L}(\mathcal{A}_i)} \cap \bigcap_{\mathcal{A}_j \in \mathcal{R} \setminus \{ \mathcal{A}_i \}} \mathcal{L}(\mathcal{A}_j) = \emptyset.
\]
If this intersection is empty, \( \mathcal{A}_i \) is redundant since all executions that would be prohibited by \( \mathcal{A}_i \) are already prohibited by the rest of the set \( \mathcal{R} \) (cf. example in Section I-A). If this intersection is non-empty, there are executions exclusively prohibited by \( \mathcal{A}_i \). In that case, \( \mathcal{A}_i \) is **non-redundant**.

In order to perform the above emptiness check, a complement procedure for PEAs is required. The classical approach of negation of the underlying logical formula and transformation of the negated formula into an automaton is not feasible here, as the underlying fragment of Duration Calculus [16] is not closed under negation [14]. In the following, we present procedures to totalize and then complement PEAs. Both procedures preserve determinism of the input automaton.

#### A. Canonical Approach to PEA Totalization

The PEAs used to represent requirements reject any sequences of valuations and durations that would violate the requirement, so that any run of the automaton is an accepting run. For the complementation of a PEA, we need to capture both the accepted and unaccepted behaviour. We hence introduce the notion of a total PEA.

**Definition 1** (Total PEA). A PEA \( \mathcal{A} = (P, V, C, E, s, I, E_0) \) is called total if and only if it satisfies the following two conditions:

1) for each valuation \( \beta' \), there is exactly one initial edge \( (g, p) \in E_0 \) such that \( \beta' \models g \) and \( \beta' \models s'(p) \);
2) for each location \( p \in P \) and pair of valuations \( \beta' \) and \( \gamma \), there is exactly one edge \( (p, g, X, p') \in E \) such that \( \beta' \| \gamma \models g \) and \( \beta' \models s'(p') \) and \( \gamma[X := 0] \models I_\vartriangleleft(p') \).

In other words, a PEA \( \mathcal{A} \) is total if for every sequence of valuations and durations \( (\beta_0, t_0), \ldots, (\beta_n, t_n) \) there exists a unique, minimal sequence of configurations \( \sigma = (p_0, \beta_0, \gamma_0, t_0), \ldots, (p_n, \beta_n, \gamma_n, t_n) \) such that \( \sigma \) is a run of \( \mathcal{A} \). Note that, by definition, a total PEA is also deterministic.

To build a total PEA, we introduce a sink location \( p_\bot \) with the property that incoming transitions are only enabled, i.e., \( X = 0 \). The guard \( g_\bot \) for a transition from \( p \) to \( p_\bot \) is defined as:
\[
g_\bot(p) := \neg \bigcup_{(p, g, X, p') \in E} \left( g \land s'(p') \land \bigwedge_{(\delta, \delta_\vartriangleleft) \in I_\vartriangleleft(p') \land \forall \in X} \delta_\vartriangleleft \right).
\]

This guard ensures that \( p_\bot \) is only reachable when none of the original outgoing edges can be taken.

The set of all non-initial sink transitions is then given as \( \bigcup_{p \in P} \{ p, g_\bot(p), \emptyset, p_\bot \} \). Similarly, we define the guard \( g_\bot^{in} \) for the initial transition to the sink location as
\[
g_\bot^{in} := \neg \bigcup_{(g, p) \in E_0} (g \land s'(p)).
\]

This guard ensures that the sink location can only be entered initially, if none of the original initial locations can be entered.

As an example, consider again PEA \( \mathcal{A}_{15} \) from our running example. The respective total PEA is shown in Fig. 3, where the parts coloured in black correspond to the original PEA, and the extensions made for the totalization is coloured in red. It contains the sink location \( p_\bot \) where both the location and clock invariant are set to true, such that any continuation of a run is accepted. The sink location \( p_\bot \) cannot be entered initially since its initial guard \( g_\bot^{in} = \neg (x' \geq 5 \lor \neg y' \lor (y' \land x' < 5)) \) evaluates to false. Every location has a transition to the sink location labelled by the corresponding guard. For \( p_0 \), we have
\[
g_\bot(p_0) = \neg ((true \land (x' \geq 5 \lor \neg y') \land true) \lor (y' \land x' < 5)) = false.
\]

The guards \( g_\bot(p_1) \) and \( g_\bot(p_2) \) are computed analogously. In the graphical representation of a PEA, we usually omit transitions whose guard evaluates to false.
By definition, any location of a PEA is accepting. However, if we simply assume that the sink location is not accepting, then any run reaching the sink location is a non-accepting run. Introduction of a simple sink location is possible as requirements expressed by PEAs may only be safety requirements, i.e., requirements that prevent anything bad from happening (in contrast to liveness which is only fulfilled by a good thing eventually happening) [12]. Because of the safety limitation, any extension of a run reaching the sink is still a non-accepting run, thus any further extension has to stay in the sink location. It is hence not possible to leave the sink location once entered; the only outgoing edge is a self-loop whose guard evaluates to true. This edge is required for the parallel composition, i.e., to allow a product automaton to take a step although there exist component automata remaining in the same location. Further, as the prefix is already violating the property, the automaton may now just accept any valuation, therefore, both the state and clock invariant of the sink location are true.

Under the given assumption that the sink location is not accepting, the language of the totalized PEA is equivalent to the language of the original one, while not rejecting any sequences of valuations and duration.

### B. PEA Totalization

The totalization as described in the previous section is quite canonical. However, for locations with strict clock invariants, some runs are accepted erroneously. As an example, consider the requirement

\[ r_2: \text{Once } y \text{ holds, it holds for less than 5 time units.} \]

represented by the PEA in Fig. 4a. The PEA is called strict, since location \( p_1 \) contains the strict clock constraint \( c < 5 \) in its clock invariant. This strict clock constraint ensures that the duration of any interval in which \( y \) holds is strictly smaller than 5 time units. The strict clock invariant \( c < 5 \) enforces that location \( p_1 \) is left before \( c = 5 \) holds. The totalized PEA, following the procedure from Section III-A, is shown in Fig. 4b. Here, the sink location \( p_\perp \) is never reachable. The guard of its sink transition, \( c \geq 5 \), is never satisfied as the strict clock invariant \( c < 5 \) enforces that location \( p_1 \) is left before \( c = 5 \) holds.

We prevent non-accepting runs of strict PEAs to get stuck by replacing the strict clock constraint (after performing the hitherto described totalization) by its non-strict version (Fig. 4c). The sink location is now reachable; any run where \( y \) holds for more than 5 time units is captured within the sink location. However, even when assuming that the sink location is non-accepting, the language of the modified PEA is a superset of the language of the original one. Any run in which the observable \( y \) holds for exactly 5 time units, e.g., the run \( \{ p_1, \{ y \mapsto \text{true} \}, \{ c \mapsto 0 \}, 5 \} \), is erroneously accepted by the total PEA with the modified clock constraint.

We prevent this by introducing the notion of a conditional acceptance criterion for locations with strict clock invariants and combine it with the previous modification (Fig. 4d). The respective location is only accepting as long as the strict clock invariant holds and then gets non-accepting once the clock equals the exact clock limit, allowing to reach the sink location afterwards. In Fig. 4d, the conditional acceptance criterion for location \( p_1 \) is indicated by splitting the clock invariant into the strict clock invariant \( (c < 5) \) for which the location is considered to be accepting, and the equality \( c = 5 \) for which the location is considered to be non-accepting.

In a last step, we have to explicitly conjoin \( c < 5 \) to the guard of all outgoing transitions of \( p_1 \) that carry no constraint for the clock of the modified constraint (Fig. 4e). Before the modification, this constraint was implicitly given by the clock invariant, since the location had to be left before the limit of the clock constraint was reached.

With this extended totalization procedure and under the assumption that the sink location is non-accepting, the language of the totalized PEA \( \mathcal{A}_{r_2} \) is equivalent to the language of the original PEA \( \mathcal{A}_{r_1} \).

Since we need to distinguish accepting and non-accepting locations, possibly in dependence of the clocks, we introduce the notion of conditional PEAs (CPEAs).

**Definition 2** (Conditional PEA). A conditional PEA \( \mathcal{A} = (P, V, C, E, s, I, E_0, F) \) is a PEA \( (P, V, C, E, s, I, E_0) \) where \( F: P \rightarrow \mathcal{L}(C) \) is a function labelling each location with a Boolean expression over clock constraints over \( C \).

We call the clock constraint introduced by \( F \) the acceptance condition. The concept of totality for PEAs (Def. 1) can also be applied to CPEAs. We refine the definition of an accepting run for PEAs (cf. Section II) by adding the constraint that the final location in a run must be accepting at the end of the current configuration.

**Definition 3** (Accepting CPEA run). Let \( \mathcal{A} = (P, V, C, E, s, I, E_0, F) \) be a deterministic CPEA and let \( \sigma = (p_0, \beta_0, \gamma_0, t_0), \ldots, (p_n, \beta_n, \gamma_n, t_n) \) be a stutter free run of \( \mathcal{A} \). Run \( \sigma \) is accepting, if and only if it is an accepting run of the PEA \( (P, V, C, E, s, I, E_0) \) and if

\[ \gamma_n + t_n \models F(p_n). \]
The resulting totalized CPEA is formally defined as:

**Definition 4** (Totalized PEA). Given a deterministic PEA $A = (P, V, C, E, s, I, E_0, F)$, its totalized CPEA is given as $A^t = (P^t, V, C, E^t, s^t, I^t, E_0^t, F)$ where

- $P^t := P \cup \{p_\perp\}$,
- $E^t := (\bigcup_{p \in P} E^t(p)) \cup E_\perp$,
- $s^t := s \cup \{p_\perp \mapsto \text{true}\}$,
- $I^t := \{p \mapsto I_\perp(p) \mid p \in P\} \cup \{p_\perp \mapsto \text{true}\}$,
- $E_0^t := E_0 \cup \{(g_\perp^t, p_\perp)\}$, and
- $F := \{p \mapsto \bigwedge_{(c_i < t_i) \in I(p)} c_i < t_i \} \cup \{p_\perp \mapsto \text{false}\}$

where $I_\perp(p)$ is the non-strict version of the clock invariant $I(p)$ and where the transitions of the CPEA are defined as $E(p)$ if $I(p) = I_\perp(p)$,

$E^t(p) := \begin{cases} \{(p, g^t, X, p') \mid (p, g, X, p') \in E \text{ otherwise}, \} \\
\bigwedge_{(c_i < t_i) \in I(p)} g^t = g \bigwedge c_i < t_i \} \end{cases}$

and guards on the sink transitions are defined as $g_\perp(p) :=
\bigvee_{(p, g, X, p') \in E} \left(g \land s'(p') \land \bigwedge_{\delta \in I_\perp(p') \cap cX} \delta_c \right)$.

and the transitions to the sink location are defined as

$E_\perp := \bigcup_{p \in P} (p, g_\perp(p), \emptyset, p_\perp) \cup \{(p_\perp, \text{true}, \emptyset, p_\perp)\}$

and with initial guards of the sink location defined as

$g_\perp^{in} := \bigvee_{(g, p) \in E_0} (g \land s'(p))$.

For a totalized CPEA, we fix the acceptance condition $F$ such that it maps the original locations in $P$ with strict clock constraints to $\text{true}$, those with non-strict constraints to the conjunction of all modified clock constraints, and the sink location $p_\perp$ to $\text{false}$.

If a location’s clock invariant contains a combination of strict and non-strict clock constraints, the clock invariant of the accepting part will be the original clock invariant, while the clock invariant of the non-accepting part is the disjunction $\bigvee c_i = t_i$ of all non-strict clock constraints $c_i < t_i$ in the original clock invariant. For example, for location $p$ with clock invariant $I(p) = c_1 < 3 \land c_2 < 4 \land c_3 < 5$, the accepting part considers $I_\perp(p)$ while the non-accepting part considers $c_1 = 3 \lor c_3 = 5$.

**Theorem 1.** Given a deterministic PEA $A = (P, V, C, E, s, I, E_0)$, the totalized PEA $A^t$ (given in Def. 4) is total, and language preserving (i.e., $L(A^t) = L(A)$).

**Proof.** Let $A = (P, V, C, E, s, I, E_0, F)$ be a deterministic PEA and $A^t = (P^t, V, C, E^t, s^t, I^t, E_0^t, F)$ its totalized PEA.
We show totality of \( A^t \) by showing that there is exactly one initial transition enabled for every valuation \( \beta' \) and that in each location \( p \in P^t \) there is exactly one transition enabled for every pair of valuations \( \beta' \) and \( \gamma \).

As \( A \) is deterministic, for each location \( p \in P \) (and initially), there is at most one transition enabled for every pair of valuations \( \beta' \) and \( \gamma \). By definition of \( g^\text{in}_\perp \), the initial sink transition is enabled exactly if none of the original initial transitions is enabled, i.e., \( g^\text{in}_\perp \Leftrightarrow \neg \bigwedge_{(g,p) \in E_0} (g \wedge s'(p)) \).

For outgoing transitions of location \( p \), we make a case distinction on the type of \( p \). For \( p = p \perp \), the only outgoing transition \( (p \perp, \text{true}, \emptyset, p \perp_\perp) \) is enabled for all \( \beta', \gamma \).

For \( p \in P \): By definition of \( g_p(p) \), the guard of the sink transition \( (p, g_p(p), \emptyset, p \perp) \) is satisfied exactly if none of the original outgoing transitions of \( p \) is enabled, i.e.,

\[
g_p(p) \Leftrightarrow \neg \bigwedge_{(g,p,x,p') \in E} (g \wedge s'(p') \wedge \bigwedge_{\{\delta_i | \delta_i \in I \wedge (p',c \times g) \}} \delta_c).
\]

For non-strict locations, this coincides with the sink transition being enabled. However, for a strict location, this is not the case, as the strict clock invariant enforces that the location is left before the sink transition can be taken. By changing the strict clock invariant to its non-strict version, the sink transition can be taken. Implicit strict constraints are explicitly conjointed to the guards of all outgoing transitions that do not yet imply these strict constraints. Thus, after the modifications, the sink transition is enabled, exactly if none of the original outgoing transitions of \( p \) is enabled. There is hence exactly one (initial) transition enabled for all \( \beta' \) and \( \gamma \). Therefore, \( A^t \) is total.

We now show that the totalization is language preserving: Let \( \sigma = (p_0, \beta_0, \gamma_0, t_0), \ldots, (p_n, \beta_n, \gamma_n, t_n) \) be a stutter-free accepting run in \( A \). Then, \( \gamma + t_i \models I(p_i) \) for all \( i \in \{0, \ldots, n\} \), in particular, \( \gamma + t_n \models I(p_n) \). Since \( A^t \) is total, \( \sigma \) must be a run in \( A^t \). To show that \( \sigma \) is accepting in \( A^t \), we make a case distinction on the strictness of location \( p_n \). If \( p_n \) is a non-strict location, then \( F(p) = \text{true} \), hence \( \gamma + t_n \models F(p_n) \). Thus, \( \sigma \) is accepting in \( A^t \). Otherwise, if \( p_n \) is a strict location, \( F(p_n) = \wedge_{(c_1 < c_2) \in I(p)} c_2 = t_i \). By definition of the acceptance condition, \( I(p) \rightarrow F(p) \) for all \( p \neq p \perp \). Thus, \( \gamma + t_n \models F(p_n) \), and \( \sigma \) is accepting in \( A^t \). Therefore, \( L(A) \subseteq L(A^t) \).

For the second inclusion, let \( \sigma = (p_0, \beta_0, \gamma_0, t_0), \ldots, (p_n, \beta_n, \gamma_n, t_n) \) be a stutter-free accepting run in \( A^t \). Then \( \sigma \) is a stutter-free accepting run in \( A \), and hence \( L(A^t) \subseteq L(A) \). Therefore, \( L(A^t) = L(A) \).

Note, that the CPEA resulting from the described totalization procedure is still deterministic (as any total PEA is, by definition, deterministic).

\[ \text{C. PEA Complement} \]

A total PEA as constructed by the procedure given in Section III-A contains both accepted and unaccepted behaviour. To complement a PEA, we hence only need to switch accepting and non-accepting locations. Fig. 5 shows the complement \( A^c_{\perp 2} \) of the PEA equivalent to \( r_2 \).

**Theorem 2** (CPEA complement). Given a deterministic, totalized PEA \( A = (P, V, C, E, s, I, E_0, F) \), its complement automaton

\[ A^c = (P, V, C, E, s, I, E_0, \neg F) \]

represents the complement language of \( A \), i.e., \( L(A^c) = \overline{L(A)} \).

**Proof.** Let \( A^c = (P, V, C, E, s, I, E_0, \neg F) \) be the complement automaton of the totalized PEA \( A = (P, V, C, E, s, I, E_0, F) \).

By definition, the totalized PEA \( A \) does not reject any sequence of valuations and durations, such that all these sequences correspond to a run in \( A \). Since the totalization procedure preserves determinism, each sequence of valuations and durations corresponds to a unique stutter-free run.

A stutter-free run \( \sigma = (p_0, \beta_0, \gamma_0, t_0), \ldots, (p_n, \beta_n, \gamma_n, t_n) \) is accepting in \( A \) if \( \gamma + t_n \models F(p_n) \), and non-accepting if \( \gamma + t_n \models \neg F(p_n) \). Then, \( \sigma \) is accepting in the complement automaton \( A^c \) if \( \gamma + t_n \models F(p_n) \), i.e., if \( \gamma + t_n \models \neg F(p_n) \), and is non-accepting if \( \gamma + t_n \models \neg F(p_n) \), i.e., \( \gamma + t_n = F(p_n) \).

Thus, exactly the runs not-accepting in \( A \) are accepting in \( A^c \) and vice versa. Therefore, \( L(A^c) = \overline{L(A)} \).

**IV. IMPLEMENTATION**

In this section, we give an overview of the implementation of our redundancy check.

Our approach is implemented in the program analysis framework ULTIMATE [17], developed at the University of Freiburg as part of the requirements analysis tool ULTIMATE ReQCHECK. The implementation builds on an existing tool chain used for the analysis of consistency, vacuity [18] and rt-consistency [19]. The tool chain comprises several modules: A parser for the pattern language HANFORPL emitting PEAs. A transformer (Pea2Boogie) translating the PEAs into a program in the verification language Boogie [20]. The program is equivalent to the parallel product (i.e. intersection of languages) of the PEAs with added annotations relating to each analysis [13]. Reachability analysis of these annotations is performed by ULTIMATE AUTOMIZER [21]. The redundancy check is integrated into this requirement analysis tool chain as a fourth analysis option.
variables: The clocks of all PEAs are set to zero, as no time has elapsed, and clock invariant are satisfied. Because of the transitions for each current location of each PEA, if the state is non-deterministically assigned due to the boogie semantics, i.e., any run of the program reaching program location \(l_c\) is an initial configuration for the intersection of PEAs.

As transitions in a PEA may refer to the assignment of state variables in the successor configuration, primed copies of the state variables (e.g. \(x'\)) are non-deterministically assigned a suitable value.

In the following (sub program \(Edges\)), the program checks if transitions can be taken, i.e., if the source location is the current location and if the guard is fulfilled. According to the transitions, variables representing the current locations of the PEAs are changed accordingly.

The loop ends by assigning the future values for all state variables to the variables encoding the current state variables.

The loop then continues as for the initial configuration, with any execution of the program reaching location \(l_c\) for the \(n\)-th time, encoding a run of length \(n\) of the PEA intersection.

B. Encoding Redundancy

To explain the encoding of the PEA intersection, we ignored the double bordered locations. When input to a program analysis tool, the tool will try to find a run of the program, that ends in these so-called error locations. For example, the error locations in Fig. 6 are guarded by assumptions over some logical formulas. An error location can be reached exactly if there is a program execution that reaches \(l_c\) and fulfills the logical formula assumed at the edge.

The program \(\mathcal{P}(R)\) encoded for the redundancy check of the requirement \(r \in R\) is the parallel product of each totalized automaton

\[
\mathcal{P}(R) = \mathcal{A}^t_1 \parallel ... \parallel \mathcal{A}^t_n.
\]

As totalized CPEAs do not reject on any input, the encoding thus far does accept arbitrary runs. Recalling the definition of redundancy detection by model checking (Section III), a requirement is redundant if the intersection of its complement and all other requirements is empty. This is encoded in one annotation per requirement in a redundancy condition.

Definition 5 (Redundancy Condition). Let \(\mathcal{P}(R) = \mathcal{A}^t_1 \parallel ... \parallel \mathcal{A}^t_n\) be an encoding of totalized CPEAs with components \(\mathcal{A} = (P, V, C, E, s, I, E_0, F)\) and let \(pc_k\) be the program variable representing the automaton location. The redundancy condition for the \(k\)-th automaton is defined as

\[
Rdc(\mathcal{A}_k) := \left( \bigvee_{p_j \in P_k} pc_j = p_j \land \neg F(p_j) \right) \land
\]

\[
\bigwedge_{p_i \in \{p_1, ..., p_n\} \setminus \{p_k\}} \left( \bigvee_{p_j \in P_i} pc_j = p_j \land F(p_j) \right).
\]

As Theorem 2 shows, the complement of a CPEA is only dependent on the acceptance condition. Therefore, in the encoding, any automaton can serve as both, its totalized and its complement. In the redundancy condition, the first disjunction requires the \(k\)-th automaton to be the complement automaton by

Fig. 6: Overall structure of the program \(\mathcal{P}(A)\) encoding the parallel composition \(A = A^t_0 || A^t_1 || A^t_2\)

A. Intersection as a Boogie program

For a detailed explanation on the encoding, we refer the reader to [10], [13]. A schematic representation of the boogie encoding is shown in Fig. 6: States refer to relevant locations in the program, edges are labelled with the statement sequences between the locations and yellow boxes are sub programs abstracted for understandability. Error locations are marked by double border and can be ignored for now.

At the beginning (from \(l_0\) to \(l_{loop}\), the encoding initialises all variables: The clocks of all PEAs are set to zero, as no time has passed. The integer variables representing the current location of each PEA (e.g. \(pc_i\)) are set to an initial location. Note, that at this stage, all state variables of the PEAs (e.g. \(x\)) are non-deterministically assigned due to the boogie semantics, i.e. they have any possible value at once.

The encoding continues inside a loop starting in \(l_{loop}\) with each iteration referring to one configuration accepted by the current location of each PEA. The loop begins by choosing a positive non-zero duration (\(\delta\)) for the configuration non-deterministically. This duration is then used to advance the clock of each PEA by the same amount.

In the following (sub program \(State\ Invariants\)), the program checks for each current location of each PEA, if the state invariant and clock invariant are satisfied. Because of the nondeterministic assignment, any run of the program reaching program location \(l_c\) is an initial configuration for the intersection of PEAs.
negation of the acceptance condition, while any other automaton accepts normally.

To encode a redundancy analysis for each requirement, we add an error location and edge with the according redundancy condition to the monitor location \( l_r \).

It is worth noticing that our implementation requires each automaton to be included only once in the encoding as a totalized automaton. The semantics of each automaton can simply be altered by changing the accepting locations in the respective assertion (see Theorem 2). This allows us to encode all redundancy analyses for a whole requirements set without much overhead (apart from the unused sink locations).

**Theorem 3.** In a set of requirements \( \mathcal{R} \), a requirement \( r \in \mathcal{R} \) is not redundant, if in the encoding \( \mathcal{P}(\mathcal{R}) \) location \( l_r^2 \) is reachable.

The proof follows directly from model checking using automata (Section III-A) and the complement construction (Theorem 2). Existence of an execution of \( \mathcal{P}(\mathcal{R}) \) in which the complement of \( r \) as well as the remaining requirements accept the run is a witness for the non-emptiness of the intersection.

To clarify our approach, we now give an example of the encoding and redundancy condition for the running example. Let \( \{ A_{r_0}^l, A_{r_1}^l, A_{r_2}^l \} \) be the set of totalized CPEAs for the example requirements. In Fig. 6, the overall structure of the program \( \mathcal{P}(A) \) encoding the parallel composition \( A = A_{r_0}^l \parallel A_{r_1}^l \parallel A_{r_2}^l \) is shown. As stated previously, it is not necessary to explicitly construct the complement PEAs or to include them in the parallel composition, since we can express the intersection by just negating the acceptance condition of any \( A_i^l \). The \textit{assume} statement on the transition to location \( l_r^1 \) expresses the redundancy condition for requirement \( r_i \). For that, we assume that each location \( p_0, \ldots, p_n \) of a PEA \( A_i^l \) is represented by the integers \( 0, \ldots, n \) and the sink location \( p_{\perp} \) is represented by \( n + 1 \). We take a closer look at \( Rdc(A_{r_0}) \) on the edge to error location \( l_r^1 \).

\[
\begin{align*}
Rdc(A_{r_0}) &= (p_{c_{r_1}} = 3) \land
(p_{c_{r_1}} = 0 \lor p_{c_{r_1}} = 1 \lor p_{c_{r_2}} = 2) \land
(p_{c_{r_2}} = 0 \lor p_{c_{r_2}} = 1 \land c < 5) 
\end{align*}
\]

The error locations \( l_r^1 \) are reachable if the \textit{assume} statements are satisfied. Error location \( l_r^1 \) is reachable with the run corresponding to the sequence of valuations and durations

\[
\begin{align*}
\pi_0 &= \{(y \rightarrow false, x \rightarrow 3), 3\}, \quad \{(y \rightarrow true, x \rightarrow 3), 4\}, \\
\pi_1 &= \{(y \rightarrow true, x \rightarrow 6), 6\}.
\end{align*}
\]

This sequence represents prohibited system behaviour with respect to \( r_0 \), but permissible system behaviour with respect to \( r_1 \) and \( r_2 \). This means that requirements \( r_0 \) and \( r_2 \) are non-redundant. Location \( l_r^2 \) is not reachable for any run, since there is no sequence of valuations that is a word in \( \mathcal{L}(A_{r_0}) \cap \mathcal{L}(A_{r_1}) \) but not in \( \mathcal{L}(A_{r_1}) \). This means \( \mathcal{R} \setminus \{r_2\} \) prohibits the same unwanted behaviour that \( r_1 \) prohibits. Therefore, \( r_1 \) is redundant and can be omitted from the set of requirements \( \mathcal{R} \) without changing the specified system behaviour.

**V. Benchmarks**

We analysed several sets of requirements for redundancies to evaluate our implementation of the redundancy check.

**TABLE I: Redundancy analysis results of the replication package.** Columns show an identifier (ID), requirements count (R), real time requirements count (RT), number of variables (V), non-redundant (NO), redundant (Yes), time out (TO) and total analysis time (T).

<table>
<thead>
<tr>
<th>ID</th>
<th>R</th>
<th>RT</th>
<th>V</th>
<th>No</th>
<th>Yes</th>
<th>TO</th>
<th>T (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>dev-01</td>
<td>26</td>
<td>21</td>
<td>27</td>
<td>26</td>
<td>0</td>
<td>0</td>
<td>0.7</td>
</tr>
<tr>
<td>dev-02</td>
<td>50</td>
<td>47</td>
<td>53</td>
<td>49</td>
<td>1</td>
<td>0</td>
<td>5.8</td>
</tr>
<tr>
<td>dev-03</td>
<td>52</td>
<td>11</td>
<td>34</td>
<td>51</td>
<td>0</td>
<td>1</td>
<td>15.9</td>
</tr>
<tr>
<td>dev-04</td>
<td>58</td>
<td>53</td>
<td>53</td>
<td>57</td>
<td>1</td>
<td>0</td>
<td>7.2</td>
</tr>
<tr>
<td>dev-05</td>
<td>68</td>
<td>64</td>
<td>89</td>
<td>64</td>
<td>2</td>
<td>2</td>
<td>39.7</td>
</tr>
<tr>
<td>abz</td>
<td>83</td>
<td>52</td>
<td>52</td>
<td>78</td>
<td>5</td>
<td>0</td>
<td>23.3</td>
</tr>
<tr>
<td>dev-06</td>
<td>100</td>
<td>95</td>
<td>101</td>
<td>99</td>
<td>0</td>
<td>1</td>
<td>21.6</td>
</tr>
<tr>
<td>dev-07</td>
<td>107</td>
<td>80</td>
<td>172</td>
<td>107</td>
<td>0</td>
<td>0</td>
<td>3.5</td>
</tr>
<tr>
<td>dev-08</td>
<td>263</td>
<td>234</td>
<td>239</td>
<td>235</td>
<td>7</td>
<td>21</td>
<td>375.5</td>
</tr>
<tr>
<td>dev-09</td>
<td>407</td>
<td>358</td>
<td>326</td>
<td>396</td>
<td>4</td>
<td>7</td>
<td>464.1</td>
</tr>
<tr>
<td>dev-10</td>
<td>699</td>
<td>543</td>
<td>1003</td>
<td>589</td>
<td>7</td>
<td>8</td>
<td>819.2</td>
</tr>
</tbody>
</table>
TABLE II: Results of the analysis of industrial requirements sets. Columns show an identifier (ID), requirements count (R), real time requirements count (RT), non-redundant (NO), redundant (YES), time out (TO) and total analysis time (T). Some benchmarks reached the global timeout (24 h), marked as TO followed by the number of remaining checks. Reruns with a lower per-check time limit are marked with *

<table>
<thead>
<tr>
<th>ID</th>
<th>R</th>
<th>RT</th>
<th>V</th>
<th>NO</th>
<th>YES</th>
<th>TO (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>dev-a</td>
<td>45</td>
<td>37</td>
<td>68</td>
<td>44</td>
<td>1</td>
<td>3.9</td>
</tr>
<tr>
<td>dev-b</td>
<td>61</td>
<td>53</td>
<td>67</td>
<td>59</td>
<td>2</td>
<td>6.6</td>
</tr>
<tr>
<td>dev-c</td>
<td>62</td>
<td>30</td>
<td>76</td>
<td>62</td>
<td>0</td>
<td>2.8</td>
</tr>
<tr>
<td>dev-d</td>
<td>105</td>
<td>103</td>
<td>152</td>
<td>105</td>
<td>0</td>
<td>28.4</td>
</tr>
<tr>
<td>dev-e</td>
<td>115</td>
<td>112</td>
<td>156</td>
<td>115</td>
<td>0</td>
<td>35.6</td>
</tr>
<tr>
<td>dev-f</td>
<td>146</td>
<td>10</td>
<td>221</td>
<td>112</td>
<td>34</td>
<td>32.9</td>
</tr>
<tr>
<td>dev-g</td>
<td>185</td>
<td>151</td>
<td>180</td>
<td>256</td>
<td>4</td>
<td>45.2</td>
</tr>
<tr>
<td>dev-h</td>
<td>254</td>
<td>211</td>
<td>238</td>
<td>5</td>
<td>238</td>
<td>256.8</td>
</tr>
<tr>
<td>dev-i</td>
<td>368</td>
<td>328</td>
<td>383</td>
<td>437</td>
<td>55</td>
<td>29 (TO (185))</td>
</tr>
<tr>
<td>dev-j</td>
<td>703</td>
<td>620</td>
<td>985</td>
<td>557</td>
<td>49</td>
<td>59 (TO (63))</td>
</tr>
<tr>
<td>dev-k</td>
<td>763</td>
<td>394</td>
<td>561</td>
<td>437</td>
<td>55</td>
<td>29 (TO (242))</td>
</tr>
<tr>
<td>dev-i*</td>
<td>368</td>
<td>328</td>
<td>383</td>
<td>141</td>
<td>35</td>
<td>1318.7</td>
</tr>
<tr>
<td>dev-j*</td>
<td>703</td>
<td>620</td>
<td>985</td>
<td>609</td>
<td>5</td>
<td>1034.7</td>
</tr>
<tr>
<td>dev-k*</td>
<td>763</td>
<td>394</td>
<td>561</td>
<td>612</td>
<td>34</td>
<td>1296.0</td>
</tr>
</tbody>
</table>

Requirements stem from industry co-operations, mostly in the automotive domain. Formalisations were obtained from the industrial requirements as part of a formal analysis effort leading to, or following, the process described in [22]. The benchmarks were selected to cover requirements sets from different projects, as well as the whole range of sizes of requirements sets that were available to us. More precisely, requirements sets dev-01 to dev-10 (Table I) were from previous, publicly available benchmarks using requirements of BOSCH [13]. The remaining set (abc in Table I) is a previously formalised [10] set of pseudo realistic automotive requirements published by Houdek et al. [23] 2. We also analysed more recent sets of industrial requirements (Table II), also from the automotive domain (not publicly available). We included these requirements sets as they more accurately reflect the current state of requirements pattern in HANFORPL and the experience using the available patterns and scopes.

Benchmarks were executed using Linux-5.15 with Java OpenJDK 11.0.18 64bit on an AMD Ryzen 5 5600 6-Core CPU with 3.5 GHz and 48 GB RAM. Benchmarks were performed using the benchmarking tool benchexec 3.21. ULTIMATE ReqCheck was run in version 0.2.3-4f548f5. Each analysis was assigned 30 GB of RAM, four cores and a 15 min timeout per redundancy check as well as one day (24 h) overall timeout.

Tables I and II show the benchmark results. Each table has an identifier for the requirements set (ID), and the number of requirements (R). Additionally, the subset of real-time requirements (RT) and the number of variables used in the requirements (V) is given, as they might impact the analysis time. Result columns show the number of redundancy analysis runs separated into redundancies found (Yes), proofs that a requirement is not redundant (No), and timeouts of the model checker (TO), as well as the total analysis time (T).

For our benchmarks, we assumed the analysis to be embedded in some process governing the formalisation and subsequent analysis of the requirements as described by Dietsch et al. [22]. As this, the analysis should be able to run within a nightly analysis cycle, and provide at least partial results to be acted upon. Based on these assumptions, our redundancy analysis performed well. All requirements sets could be analysed successfully or at least with partial results, leading to the detection of redundancies (and a high number of non-redundancy proofs). While no analysis exceeded the memory limitation, a number of timeouts could be observed.

Especially the analysis of set dev-i (Table II) was stopped after analysing approx. half of the requirements set due to the 24 h timeout. A closer inspection of the requirements set showed, that it is close to an adversarial example with global clocks forcing the analysis to deal with uncommonly long runs. Additionally, the majority of requirements is using complex patterns and scopes, resulting in complex behaviour for each individual requirement. Nonetheless, even in this set, a number of redundancies was found.

The ability to produce partial results even for a complex input is a strength of our approach (as already shown in [13]). Embedded in an analyse and fix cycle, the partial results enable improvements in the requirements. In this context, timeouts may vanish in later iterations due to changes in other requirements, or higher analysis times may be allotted to further increase requirements quality. To demonstrate the viability of this approach, we re-run benchmarks dev-i to dev-k with a per-check timeout of five minutes. This timeout seems to be a practical default setting in the beginning of a project (see sets marked with * in Table II).

Note, that we assume that all requirements are already given as formal requirements in HANFORPL. Therefore, any redundancy found is a real redundancy in the requirements and any requirement proven to be non-redundant is necessary for system behaviour (see Theorem 3). For a discussion of the relation of defects found in a formal requirements analysis and natural language requirements as a basis for this analysis, we refer to the process discussion in Dietsch et al. [22].

VI. RELATED WORK

Redundancy in requirements is listed as a threat to the modifiability by IEEE-830 [1] as well as Davis et al. [2]. Redundancies are intentionally not listed as defects, but emphasize the necessity for careful management of requirements that are stated multiple times.

The notion of redundancy can also be found in the model checking community. Kupferman [24] argues, that a successful run of a model checker, i.e., the model checker proved that a model does not violate the specification, can give false security. The successful verification of the model may be due to an ineffective specification rather than due to the model adhering to the specification. More precisely, by a specification that

2A replication package for benchmarks in Table I can be found at doi.org/10.5281/zenodo.10999174
itself is vacuous [25] or may look thorough but is really just bloated by repetition.

In the requirements community, there is some work on the detection of redundancies in natural language requirements: Jürgens et al. [26] applied duplication detection methods taken from source code analysis. Their experimentation on real world documents lead them to conclude that one should assume around ten percent of duplication if no precautions to eliminate redundancy were taken. This number is much higher than we could replicate in our benchmarks, but this may be due to requirements in our analysis being taken from a safety domain, as well as obvious redundancies already being eliminated during the formalisation process [22]. In contrast to our approach, the approach of Jürgens et al. is purely syntactical, i.e., unable to detect requirements that are less restrictive than a combination of other requirements.

There exists a number of tools for the analysis of formal requirements, e.g. [6]–[9]. None of these have the capability to detect arbitrary redundancies. While they are able to detect different properties, such as consistency, reliability and more, none of these tools have the ability to detect redundancies in the requirements set.

Dokhanchi et al. [27] preset checks to assist the elicitation of specifications in Metric Interval Temporal Logic (MITL), including the detection of redundancy but only within one formula, i.e., not detecting redundancy within a whole specification.

The work of Post et al. [18] handles vacuity in real time requirements, and is the basis for the current implementation of our vacuity analysis [13]. The detection of vacuity in addition to redundancy is useful although a vacuous requirement will also always be detected as redundant. As a vacuity is almost always a defect, redundancies caused by vacuity can directly be reported as defects, whereas the root cause of a redundancy has to be analysed carefully.

An approach to model checking PEAs was presented by Meyer et al. [28]. They use so-called Test Automata that share the concept of a sink location with CPAs. However, Test Automata are only defined for non-strict clock constraints. Also, their model checking approach is based on the direct translation of special Duration Calculus formulas into Test Automata.

VIII. ACKNOWLEDGEMENTS

Funded by the Bundesministerium für Bildung und Forschung (BMBF, Federal Ministry of Education and Research, Germany) - 03VP11880 SystemValid.

VII. CONCLUSION

In this work, we presented a scalable approach to the redundancy analysis of real time requirements. This analysis is based on an automata theoretical approach that is enabled by the totalization and complement of an extension of the PEA timed automaton model that we introduce. We implemented the approach as a program analysis task solvable by reachability analysis. The benchmarks on industrial requirements sets show that our approach is fit for practical use. The analysis successfully uncovered redundancies on large real world requirements sets from industry projects.

In future research we will apply the redundancy analysis to industrial projects to evaluate the reasons behind, as well as the impact of, redundant requirements in large requirements specifications.

Investigating redundancies reported by our analysis is still time consuming as the analysis currently only indicates the existence but not the cause. In the future, we will work on the automatic extraction of reasons for the redundancies found.
REFERENCES


