Specification and verification of reconfiguration protocols in grid component systems.

Alessandro Basso¹
Alexander Bolotov¹
Artie Basukoski¹
Vladimir Getov¹
Ludovic Henrio²
Mariusz Urbanski³

¹ Harrow School of Computer Science
² CNRS/I3S/INRIA, Sophia Antipolis, France.
³ Institute of Psychology, Adam Mickiewicz University, Poznan, Poland.


This material is posted here with permission of the IEEE. Such permission of the IEEE does not in any way imply IEEE endorsement of any of the University of Westminster’s products or services. Internal or personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution must be obtained from the IEEE by writing to pubs-permissions@ieee.org. By choosing to view this document, you agree to all provisions of the copyright laws protecting it.

The WestminsterResearch online digital archive at the University of Westminster aims to make the research output of the University available to a wider audience. Copyright and Moral Rights remain with the authors and/or copyright owners. Users are permitted to download and/or print one copy for non-commercial private study or research. Further distribution and any use of material from within this archive for profit-making enterprises or for commercial gain is strictly forbidden.

Whilst further distribution of specific materials from within this archive is forbidden, you may freely distribute the URL of the University of Westminster Eprints (http://www.wmin.ac.uk/westminsterresearch).

In case of abuse or copyright appearing without permission e-mail wattsn@wmin.ac.uk.
Specification and Verification of Reconfiguration Protocols in Grid Component Systems

Alessandro Basso\textsuperscript{1}, Alexander Bolotov\textsuperscript{1}, Artie Basukoski\textsuperscript{1}, Vladimir Getov\textsuperscript{1}, Ludovic Henrio\textsuperscript{2} and Mariusz Urbanski\textsuperscript{3}

Abstract

In this work we present an approach for the formal specification and verification of the reconfiguration protocols in Grid component systems. We consider Fractal, a modular and extensible component model. As a specification tool we invoke a specific temporal language, separated clausal normal form, which has been shown to be capable of expressing any ECTL\textsuperscript{+} expression, thus, we are able to express the complex fairness properties of a component system. The structure of the normal enables us to directly apply the deductive verification technique, temporal resolution defined in the framework of branching-time temporal logic.

I. INTRODUCTION

There are two approaches to building long-lived and flexible Grid systems: exhaustive and generic. The former approach provides rich systems satisfying every service request from applications but consequently its implementation suffers from very high complexity. In the latter approach, we represent only the basic set of services (minimal and essential) and thus overcome the complexity of the exhaustive approach. However, to achieve the full functionality of the system, we must make this lightweight core platform reconfigurable and expandable. One of the possible solutions here is to identify and describe the basic set of features of the component model and to consider any other functions as pluggable components [30] which can be brought on-line whenever necessary [26].

Establishing the theoretical foundations of the generic processes involved in designing and functioning of such Grid systems is highly important. A significant part of this research lies in the area of formal specification and verification of the core component model and the properties of the desired Grid systems.

Among various approaches to representing a component model we pay specific attention to the Fractal component model [17]. The advantage of the Fractal framework is that it defines the structure of the components, gives a basic classification of components, and has the mathematical foundations, e.g., the Kell calculus [7]. The Fractal specification defines the basic (non-functional) controls which should be defined especially to enable dynamic reconfiguration of components, and a number of constraints on the interplay between functional and non-functional operations. The reconfiguration is obtained by triggering appropriate actions on specific types of the components' interfaces. These explicit dynamic properties of the Fractal component model are particularly suitable for Grid systems and environments. In this work we focus on predefined categories of reconfigurations and also on proving properties of these reconfigurations.

Given a formal specification of a distributed system there are two major approaches to formal verification of this specification: algorithmic and deductive [28]. While the algorithmic approach is fully automated, as in the case of model checking, its application, in general, is restricted to finite state systems. On the other hand, methods of the second, deductive approach, can handle arbitrary systems providing uniform proofs. To the best of our knowledge, the only technique currently used in the verification of distributed hierarchical components is model checking.

In our approach the components are modelled in a specific branching-time temporal logic, or SNF\textsubscript{CTL} (Separated Normal Form for Computation Tree Logic) [14], and then the temporal resolution is applied as a deductive verification tool.

SNF\textsubscript{CTL} initially developed for CTL has been shown to be able to express simple fairness constraints and their Boolean combinations [10], [11]. Furthermore, a clausal resolution over the set of SNF\textsubscript{CTL} clauses has been defined [9], [10] and recently the search strategies for this method were presented in [12]. These developments allow us to set up the following problem structure tackled in the paper:

\[
FCM \rightarrow SNF_{\text{ctl}}(FCM) \rightarrow BTR
\]

Here we suggest the translation of the Fractal component model (FCM) into the SNF\textsubscript{CTL}(FCM), the SNF\textsubscript{CTL} based formal specification of FCM, and to apply the 'branching temporal resolution' method (BTR), the temporal resolution technique defined over the set of SNF\textsubscript{CTL} clauses.

II. RECONFIGURATION SCENARIO

A. Component Model

Fractal is a modular and extensible component model. The Fractal specification defines a set of notions characterizing this model, an API (Application Program Interface), and an ADL (Architecture Description Language).

Components are characterized by their content and the membrane. The content of a component can be hidden (in which case it is simply a black box) or it can be constituted by a system of some other components (sub-
components). In the former case we would call a component primitive while the latter case represents a composite component. The membrane, or controller, controls the component. Controllers address non-functional aspects of the component.

Fractal is a multi-level specifications. Depending on their conformance level, Fractal components can feature introspection and/or configuration. The control interfaces are used in the Fractal model to allow configuration (reconfiguration), and are defined as non-functional. On the other hand, the functional interfaces of a component are associated with its functionalities. A functional interface can provide the required functionalities and we call it the server interface. Alternatively, a client interface requires some other functionalities.

Component interfaces are linked together by bindings. In this paper, we will only consider primitive bindings that are simple bindings transmitting invocations from the client interface to the connected server interface.

There are four controllers that have been already defined in Fractal (but others may be user-defined depending on the needs of the model):

- The attribute controller is used to configure a property within a component, when there is no need to take into consideration bindings of interfaces.
- The binding controller is used when the attribute controller is not applicable and actual binding/unbinding of interfaces is required.
- The content controller can be used to retrieve the representation of the sub components and add or remove them accordingly; note that if a sub component is shared by one or more other components, the scenario must be defined so that also these other components are taken into consideration.
- The life cycle controller allows to start and stop a component, it is used for dynamic reconfiguration so that all other controls can be applied safely to the component while the component is not in execution.

These are the basic controls which should be defined especially to be able to have dynamic reconfiguration of components.

The Fractal specification defines a number of constraints on the interplay between functional and non-functional operations:

- Content and binding control operations are only possible when the component is stopped.
- When stopped, a component does not emit invocations and must accept invocations through control interfaces; whether or not an invocation to a functional interface is possible is undefined.

B. Configuration/Reconfiguration Scenario

In general, the initial configuration of a Fractal component is given by the description of the component using Fractal ADL.

From this first state, reconfiguration is obtained by triggering appropriate actions on the the life-cycle, the binding, and the content control interfaces. A reconfiguration can be triggered by any component that has a reference to a correct non-functional interface.

In this work we focus on predefined categories of reconfigurations and on proving properties on these reconfigurations. As far as the reconfiguration is concerned we use the classical assumption that replacing a component by a similar one is safe for the system.

III. Specification of the Scenario in Temporal Logic Framework

A. Formal Specification and Verification of Components

We distinguish the specification of the primitives and of the composite component. The primitives are specified as a black box, usually in a programming language of our choice. The component composition is specified using Fractal ADL, and from this specifications it is possible to extract the bindings between interfaces of subcomponents and the controllers of the component itself.

B. Specification Language: Normal Form for ECTL+

The language of a normal form, SNFCTL developed for a number of branching-time logics, CTL [8], [14], ECTL [10] and ECTL+ [11], is based upon the extended set of classical logic operators \&, v, \rightarrow, \neg, the set of future time temporal operators[always], [sometime], [next time] and path quantifiers A (on all future paths) and E (on some future path), classically defined constants true and false, and a new operator, start (‘at the initial moment of time’ with the intended meaning that it is true only at the initial moment of time).

Underlying Tree Structures. Assuming familiarity of the reader with the basic tree structure concepts we preceede the presentation of the SNFCTL language by the introduction of the notation that we will utilise.

Definition 1 (Tree) A tree, T, is a pair (S, R), where S is a set of states and R ⊆ S × S is a relation between states of S such that (a) S0 ∈ S is a unique root node (b) for every s1 ∈ S there exists s2 ∈ S such that R(s1, s2); and (c) for every s1, s2, s3 ∈ S, if R(s1, s3) and R(s3, s2) then s1 = s2.

By s, we abbreviate a path departing from s1. A path s is called a fullpath. Let X be a family of all fullpaths of T. Given a path \chi, and a state sj ∈ \chi, (i < j) we term a finite subsequence \{si, sj\} = si, sj+1, ..., sj of \chi, a prefix of a path \chi, and an infinite subsequence sj, sj+1, sj+2, ..., of \chi, a suffix of a path \chi, abbreviated Snf(\chi, sj).

We assume that the underlying trees are countable ω-trees, i.e. any fullpath \chi ∈ X is isomorphic to natural numbers and every state s ∈ S has a countable number of successors.

Now we are ready to define the formal syntax and semantics for SNFCTL. A set of SNFCTL clauses is interpreted in a structure \(M = (S, R, s_0, X, L)\), where (S, R) is a countable \(\omega\) tree with a root \(s_0\), \(X\) is a set of all fullpaths and \(L\) is an interpretation function mapping atomic propositional symbols to truth values at each state and the following condition is satisfied: \(X\) is \(R\)-generable [19], i.e. for every state \(s_i \in S\), there exists \(\chi_j \in X\) such that \(s_i \in \chi_j\), and
for every sequence \( x_j = s_0, s_1, s_2, \ldots \), the following is true: 
\[ x_j \in X \text{ if, and only if, for every } i, R(s_i, s_{i+1}). \]

In our definition of an SNF\(_{\text{CTL}}\) model structure \( \mathcal{M} \) the set of full-paths \( X \) is \( R \)-generable. Therefore, following [19], it is suffix, fusion and limit closed.

**Syntax.** First, we fix a countable set, \( \text{Prop} = \{ x, y, z, \ldots \} \), of atomic propositions. The core idea of SNF\(_{\text{CTL}}\) is to represent temporal information in the following three types of constraints. *Initial constraints* represent information relevant to the initial moment of time, the root of the computation tree. *Step constraints* indicate what will happen at the successor state(s) given that some conditions are satisfied ‘now’. Finally, *Sometime constraints* keep track on any eventuality, again, given that some conditions are satisfied ‘now’. Additionally, to enable sound reasoning within a specific path context during the verification, we incorporate indices.

**Indices.** The language for indices is based on the set of terms \( \text{IND} = \{ f, g, h, (LC(f)), \{ LC(g) \}, (LC(h)) \ldots \} \), where \( f, g, h \ldots \) denote constants. Thus, \( E f g Q \) means that \( A \) holds on some path labelled as \( f \). A designated type of indices in SNF\(_{\text{CTL}}\) are indices \( \{ LC(\text{ind}) \} \) which represent a limit closure of prefixes associated with \( \text{ind} \). All Formulæ of SNF\(_{\text{CTL}}\) of the type \( P \Rightarrow E Q \) or \( P \Rightarrow EQ \), where \( Q \) is a purely classical expression, are labeled with some index.

**Definition 2.** (Separated Normal Form SNF\(_{\text{CTL}}\)) A set of SNF\(_{\text{CTL}}\) clauses is a set of formulæ \( \mathcal{A} \boxdot \{ P_i \Rightarrow F_i \} \) where each of the clauses \( P_i \Rightarrow F_i \) is further restricted as below, each \( \alpha_j, \gamma, \beta, \beta_0, \beta_1, \beta_2 \) is a literal, true or false and \( \text{ind} \in \text{IND} \) is some index.

\[
\begin{align*}
\text{start} & \Rightarrow \begin{array}{c}
\left[ \bigwedge_{i=1}^{k} \beta_i \right] \\
\end{array} \\
\Rightarrow & \begin{array}{c}
\alpha_j \Rightarrow \begin{array}{c}
A \bigcirc \left[ \bigwedge_{i=1}^{n} \beta_i \right] \\
\end{array} \\
\Rightarrow & \begin{array}{c}
p \Rightarrow \begin{array}{c}
E \bigcirc \left[ \bigwedge_{r=1}^{\gamma} \beta_r \right] \text{(ind)} \\
\end{array} \\
\Rightarrow & \begin{array}{c}
u \Rightarrow \begin{array}{c}
A \bigcirc \gamma \\
\end{array} \\
\Rightarrow & \begin{array}{c}
u \Rightarrow \begin{array}{c}
E \bigcirc \gamma \text{(ind)} \\
\end{array} \\
\end{array} \\
\end{array}
\end{array}
\end{align*}
\]

\( C. \) **Interpreting SNF\(_{\text{CTL}}\)**

We define a relation \( \models \) which evaluates the SNF\(_{\text{CTL}}\) clauses at a state \( s_i \) in a model \( \mathcal{M} \). The evaluation of the classical connectives in the states is standard. Below we represent the evaluation of the temporal operators and path quantifiers.

\[
\begin{align*}
\langle M, s_i \rangle & \models \Box B \iff \text{ for each } \chi_{x_i}, \langle M, \chi_{x_i} \rangle \models B. \\
\langle M, s_i \rangle & \models \Box B \iff \text{ there exists } \chi_{x_i} \\
\text{ such that } \langle M, \chi_{x_i} \rangle \models B. \\
\langle M, \chi_{x_i} \rangle & \models \Box B \iff \text{ for each } s_j \in \chi_{x_i}, \text{ if } i \leq j \\
\text{ then } \langle M, \text{Suf}[(\chi_{x_i}, s_j)] \rangle \models B. \\
\langle M, \chi_{x_i} \rangle & \models \Box B \iff \text{ there exists } s_j \in \chi_{x_i} \\
\text{ such that } i \leq j \text{ and } \langle M, \text{Suf}[(\chi_{x_i}, s_j)] \rangle \models B. \\
\langle M, \chi_{x_i} \rangle & \models \Box B \iff \text{ if } \langle M, \text{Suf}[(\chi_{x_i}, s_{i+1})] \rangle \models B. \\
\end{align*}
\]

**Definition 3.** (Satisfiability, validity) An SNF\(_{\text{CTL}}\) clause, \( C \), is satisfiable if, and only if, there exists a model \( \mathcal{M} \) such that \( \langle M, s_i \rangle \models C \). An SNF\(_{\text{CTL}}\) clause, \( C \), is valid if, and only if, it is satisfied in every possible model.

An initial SNF\(_{\text{CTL}}\) clause, \( \text{start} \Rightarrow F \), is understood as “\( F \) is satisfied at the initial state of some model \( \mathcal{M} \).” Any other SNF\(_{\text{CTL}}\) clause is interpreted taking also into account that it occurs in the scope of \( \Box \).

Thus, a clause \( \mathcal{A} \quad \Box (x \Rightarrow A P) \) is interpreted as “for any fullpath \( x \) and any state \( s_i \in \chi (0 \leq i) \), if \( x \) is satisfied at a state \( s_i \) then \( p \) must be satisfied at the moment, next to \( s_i \), along each path which starts from \( s_i \).

Next, a clause \( \mathcal{A} \quad \Box (x \Rightarrow E O q(\text{ind})) \) is interpreted as “for any fullpath \( x \) and any state \( s_i \in \chi (0 \leq i) \), if \( x \) is satisfied at a state \( s_i \) then \( q \) must be satisfied at the moment, next to \( s_i \), along a path which starts from \( s_i \) and which is associated with \( \text{ind} \).” Speaking informally, we interpret \( \mathcal{A} \quad \Box (x \Rightarrow E O q(\text{ind})) \) such that given a state in a model which satisfies \( x \) (the left hand side of the clause), the label, \( q(\text{ind}) \), indicates the direction, in which the successor state which satisfies \( q \) can be reached (see similar developments in the construction of logic \( \text{DCTL} \) [27]).

Finally, we would like to point out that our interpretation of an LC index corresponds to the concept of a linear interpretation [36].

Note that in the full \( \text{ECTL}^+ \) language the standard ‘until’ (\( \mathcal{U} \)) and ‘unless’ (\( \mathcal{W} \)) operators are used:

\[
\langle \mathcal{M}, s_i \rangle \models \mathcal{U} B \iff \text{ there exists } s_j \in \chi_{s_i} \text{ such that } i < j \text{ and } \langle M, \text{Suf}[(\chi_{s_i}, s_j)] \rangle \models B \text{ for each } s_k \in \chi_{s_i}, \text{ if } i < k < j \text{ then } \langle M, \text{Suf}[(\chi_{s_i}, s_k)] \rangle \models A. \\
\text{and } \mathcal{W} B = \Box \mathcal{A} \mathcal{V} \mathcal{U} B. \text{ In the SNF\(_{\text{CTL}}\) these operators are defined via the basic set of SNF\(_{\text{CTL}}\) operators [8]. For example, the following rules can be applied to remove the } \mathcal{W} \text{ operator in the scope of either of the path quantifiers [8] where } x \text{ is a new proposition:}
\]

**Removal of \( \mathcal{E} \text{W} \):**

\[
P \Rightarrow E(p \lor q)[(\text{LC}(\text{ind}))] \quad \text{x} \Rightarrow E O(q \lor (p \land x))[\text{(ind)}] \\
\]

**Removal of \( \mathcal{A} \text{W} \):**

\[
P \Rightarrow A(p \lor q) \quad x \Rightarrow E O(q \lor (p \land x)) \\
\]

**D. Example Specification**

Let us consider a simple printing queue component model which consists of a client and one printing queue component as primitives. The client interfaces of the client are of type \( \text{CL}_x \) and the server interfaces of the printing queue are of type \( \text{SL}_x \). Finally, we have a simplified version of a life-cycle controller that allows to safely add or remove a binding between a client and the printing queue.

**Formal specification of non-functional aspects.** In order to allow for reconfiguration, not only the scenario must be formally specified, but also everything else which allows dynamic reconfiguration. Although in the fractal model four controller interfaces are defined, for reasons of space, we will only specify the safe-unbinding part of a reduced Life-Cycle Controller (LCC) so that it can be used in the deductive reasoning. Note that it is always possible to create new controllers if needed, in this case an
appropriate set of formal specifications for each controller must be provided using a similar procedure. If a controller follows the standard Fractal model, a standard set of general temporal logic rules can be called and then modified to match the specification; otherwise, in the case of user-made definitions, the programmers themselves must provide the rules matching the criteria followed in the creation of the definition.

Next we let the propositions \( \text{Bound}_1, \ldots, \text{Bound}_n \) denote the bindings between components. The format that each may take is \( \text{Bound}_i(CI_a, SI_r) \) (1 \( \leq i \leq n \)) which is a proposition that (when true) specifies that a component with Client Interface \( CI_a \) is bound to the Server Interface \( SI_r \). In this example we have two primitive components, one for the Printing Queue and one for the Client using the Printing Queue. We would add as many of these propositions as necessary to describe the system.

\( LCC \) is a proposition which when true signifies that the Life Cycle Controller is active.

Before introducing the Life Cycle Controller Formula we would need to specify how components are started and stopped. However, for illustration in the context of this paper we will only provide a partial specification of the Life Cycle Controller and two primitive components; we only deal with the formula that captures the bindings of the two components. We will model the start of the components by attaching them to \textit{start}.

Now we introduce the formula for our version of the Simplified Life-Cycle Controller:

\[
-LCC \land -\text{Bound}_1(CI_a, SI_r) \lor \text{Bound}_2(CI_a, SI_r) \Rightarrow \text{Start} \Rightarrow (\text{Bound}_1(CI_a, SI_r) \land \text{Bound}_2(CI_a, SI_r))
\]

which states that if neither of the components are bound and the LCC is not active then in all possible computations when the LCC is active then we must have the two components bound.

In the following example the Client can send a request for printing: \( req(CI_a) \) abbreviated below as \( req \). When true, this proposition states that a printing request has been raised by the client which possesses the client interface \( CI_a \). Similarly \( print \) is a proposition stating that a printing request has been satisfied by the printer.

**Formal specification of reconfiguration scenarios.**

For this section, we consider a simple single printing queue component model (see figure 1) which consists of one client and one printing queue component as primitives. The client interface of the client is labelled \( CI_a \), and the server interfaces of the printing queue is labelled \( SI_r \). We will also consider a simplified life-cycle controller \( LCC \) that allows us to safely remove a binding between a client and the printing queue. This simple example is sufficient to demonstrate the potential of deductive reasoning, applied to a fractal model.

We will take in consideration the safety part of the specification and its requirements [29]. The Life-Cycle Controller \( LCC \) does not have a set specification being a non-functional component. We suggest that the system has a common protocol of communication (both Client and Printing Queue must follow a common process when a request is raised).

**Client specification:**

- (1) \( req \Rightarrow A(reqU(req \land print)) \) Request is kept until it is possible to execute it
- (2) \( req \Rightarrow A(\neg req2d print) \) There will be no other request until job is printed
- (3) \( req \Rightarrow A \diamond \neg req \) The request for print will be eventually released

The complete specification of the primitive:

\[
\text{Start} \Rightarrow \neg req \land (1) \land (2) \land (3)
\]

where \( \neg req \) defines the initial state for Client primitive.

**Printing queue specification:**

- (4) \( A \neg (\neg print \land print2) \) Mutual Exclusion property: at every point in time, the printer can perform at most one printing operation:
- (5) \( A(\neg print \lor req) \) There is no printing unless requested
- (6) \( print \Rightarrow A \diamond \neg print \) Printing will eventually end
- (7) \( req \Rightarrow A \diamond print \) The request for printing should be granted

The complete specification of the primitive:

\[
\text{Start} \Rightarrow \neg print \land (4) \land (5) \land (6) \land (7)
\]

Finally we specify the Life-Cycle Controller properties which affect the receiving of a printing request and the printing itself:

\[
\text{Start} \Rightarrow (\neg LCC \land \neg (req \lor print)) \Rightarrow A \Box (LCC \Rightarrow (req \land print))
\]

When the life-cycle controller is activated, it ensures that Client Interface and Server Interface are bound, therefore allowing for requests to be sent from the Client, and prints to be carried out by the Printing Queue, for the specific binding.

We believe that the branching-time framework is appropriate for our specification targets because of the following reasons. Assume that after unbinding a client CI, it has been removed forever. Now, from this moment of time it is true to say that \( A \Box \neg req \) (in all possible futures from now on, there will be no more requests from the Client Interface to the Server Interface) and therefore at the previous moment of time it was true to say that \( E \Box A \Box \neg req \) (in some future it will not be possible for the Client interface.

---

**Fig. 1. Example in Fractal: LC Controller**
to send a request to the Server Interface). The branching-time framework used shows how significant its use can be even in such simple example.

To apply deductive reasoning to this model, various properties could be taken into consideration. As a relatively simple example we consider the following property. Let \( p \) stands for \( \neg eq(C I_{s}, S I_{r}) \land \neg print(C I_{r}, S I_{r}) \). Assume now that during the reconfiguration of the system the following property should be verified:

\[
\vdash A( \Box \Diamond p \land \Box \neg p )
\]

In the next section we will show how this formula can be represented in terms of \( SNF_{CTL} \) and then apply to this specification the resolution technique as a verification method.

IV. The Verification Method - Clausal Temporal Resolution

A. Temporal Resolution Method for Branching-Time Logics

In order to achieve a refutation of the generated specification, we incorporate two types of resolution rules already defined in [8], [14]: step resolution (SRES) and temporal resolution (TRES). Step resolution is used between Formulae that refer to the same initial moment of time or same next moment along some or all paths. Two step resolution rules that will be used in our example are given below (where \( l \) is a literal and \( C \) and \( D \) are disjunctions of literals).

**SRES 1**

\[
\begin{align*}
\text{sstart} & \Rightarrow C \lor l \\
\text{start} & \Rightarrow D \lor \neg l \\
\text{start} & \Rightarrow C \land D
\end{align*}
\]

When an empty constraint is generated on the right hand side of the conclusion of the resolution rule, we introduce a constant \textbf{false} to indicate this terminating clause.

Now we present only two temporal resolution rules that will be used in our verification example. In the formulation of these rules below \( l \) is a literal and the first premises abbreviate the \( A \) and \( E \) loops in \( l \) [13], i.e. the situation where, given that \( P \) is satisfied at some point of time, \( l \) occurs always from that point on all or some path respectively.

**TRES 2**

\[
\begin{align*}
P & \Rightarrow A \Box A \square l \\
Q & \Rightarrow E \square \neg l_{(L C \text{ind})} \\
Q & \Rightarrow E (\neg P W \neg l)_{(L C \text{ind})}
\end{align*}
\]

**TRES 3**

\[
\begin{align*}
P & \Rightarrow E \Box E \square l_{(L C \text{ind})} \\
Q & \Rightarrow A \square l \\
Q & \Rightarrow A (\neg P W \neg l)
\end{align*}
\]

B. Example Verification

To verify \( \Box \) we apply the resolution method to the set of \( SNF_{CTL} \) clauses \( SNF_{CTL}(\Box) \). We commence the resolution proof presenting at steps 1 - 13 the clauses of \( SNF_{CTL}(\Box) \) in the following order: initial clauses, step clauses and, finally, any sometime clauses.

1. \textbf{start} \( \Rightarrow x \)
2. \textbf{start} \( \Rightarrow \neg x \lor y \)
3. \textbf{start} \( \Rightarrow \neg x \lor x_1 \)
4. \textbf{start} \( \Rightarrow \neg z \lor \neg p \)
5. \textbf{start} \( \Rightarrow \neg z \lor z_1 \)
6. \textbf{true} \( \Rightarrow A \square (\neg z \lor \neg p) \)
7. \textbf{true} \( \Rightarrow A \square (\neg z \lor z_1) \)

We apply step resolution rules between 2 and 7, 1 and 3. No more SRES rules are applicable. Formula 12 is an eventuality clause, and therefore, we are looking for a loop in \( \neg p \) (see [13] for the formulation of the loop searching procedure). The desired loop, \( E \Box E \square (\neg p)_{(L C \text{ind})} \) (given that condition \( z_1 \) is satisfied) can be found considering clauses 10 and 11. Thus, we apply the TRES 3 rule to resolve this loop and clause 12, obtaining 16. Next we remove \( EW \) from 16 deriving a purely classical Formula 17 (\( y \) is a new variable). Simplify the latter, apply TEMP (the temporalising rule), see [8], obtaining, in particular, 19 and 20, and then a series of SRES rules to newly generated clauses. Now, as no more SRES rules are applicable, we find another eventuality, Formula 13, and thus we next look for a loop in \( \neg z \). This loop can be found considering Formulae 9 and 26: \( A \Box A \square \neg z \) given that condition \( x_1 \) is satisfied. Thus, we can apply TRES 2 to resolve this loop and 13 deriving 27. Then we remove \( EW \) from the latter (on step 28, where \( w \) is a new variable, we use only one of its conclusions). Applying simplification and temporalising to 28 we obtain 29. The desired terminating clause \textbf{start} \( \Rightarrow \textbf{false} \) is deduced by applying SRES 1 to steps 15 and 23.

14. \textbf{start} \( \Rightarrow y \)
15. \textbf{start} \( \Rightarrow x_1 \)
16. \textbf{y} \( \Rightarrow A (\neg z_1 \lor p) \)
17. \textbf{y} \( \Rightarrow p \lor \neg z_1 \land v \)
18. \textbf{v} \( \Rightarrow A \square (p \lor \neg z_1 \land v) \)
19. \textbf{start} \( \Rightarrow \neg y \lor p \lor \neg z_1 \)
20. \textbf{true} \( \Rightarrow A \square (\neg p \lor \neg z_1) \)
21. \textbf{start} \( \Rightarrow p \lor \neg z_1 \)
22. \textbf{start} \( \Rightarrow p \lor \neg z \)
23. \textbf{start} \( \Rightarrow \neg z \)
24. \textbf{x} \( \Rightarrow A \square (p \lor \neg z_1) \)
25. \textbf{x} \( \Rightarrow A \square (p \lor \neg z) \)
26. \textbf{x} \( \Rightarrow A \square \neg z \)
27. \textbf{x} \( \Rightarrow E \square (\neg x_1 \lor \neg w)_{(L C \text{ind})} \)
28. \textbf{x} \( \Rightarrow z \lor \neg x_1 \land w \)
29. \textbf{start} \( \Rightarrow \neg x \lor z \lor \neg x_1 \)
30. \textbf{start} \( \Rightarrow \textbf{false} \)

We have found a contradiction, meaning that \( SNF_{CTL}(\Box) \), hence \( \Box \) itself is unsatisfiable.

V. Conclusions and Future Work

In this paper we have introduced a formal framework for the deductive verification of modular specification. As a specification tool we use the branching-time temporal logic. Specified properties and requirements of the system are then translated into the language of a normal form, \( SNF_{CTL} \), thus enabling the application of a powerful resolution method.
Future extensions of this work will be in the application of the Inferential Erotetic Logic (IEL) tools aiming at optimisation of the process of reconfiguration of a component model [15]. The Inferential Erotetic Logic (IEL) [31], [34] is a powerful tool in the area of analyzing and modelling such components of intelligent activity as planning, problem solving, and searching for information in massive data/knowledge bases [32]. Important developments within the framework of IEL are Eroetetic Search Scenarios (ESS) [33] and Socratic Proofs (SP) [35]. ESS is based on the idea of providing conditional instructions for solving an initial problem, informing us which questions should be asked and when they should be asked. Moreover, an erosetic search scenario shows where to go if a direct answer to a query appears to be acceptable and does so with respect to any direct answer to each query. SP is a very specific technique, which reduces the complexity of standard problem-solving methods by using pure questioning only.

REFERENCES