Synthesis of Poka Yoke Activity Diagrams

Version 0.1 (June 2024)

1 Introduction

2 Preliminaries

2.1 Formalisms

Our activity synthesis algorithm deals with various different formalisms that each have their own terminology. Here is a high-level overview.

Finite automata. Finite automata are finite directed graphs consisting of *locations* and *edges*. Locations can be marked *initial* when they are 'starting' locations. Locations can also be *marked* when they are accepting locations, with the standard meaning of acceptance from automata theory.

Extended finite automata (EFA). EFAs are finite automata that are used in the presence of *state*, i.e., variables that have a value. The edges of EFAs have *guards*, which is a state predicate, and *updates*, which is a state transformer.

(UML) Model. A UML Model may consist of a number of UML enum declaration, and consists of a single UML Class, which may contain:

- A number of UML properties, whose type is either Boolean, bounded integer or an enum as is defined in the UML model.
- A number of UML opaque behaviors that have a *guard* and zero or more *effects*. These opaque behaviors model *actions* to be performed in the synthesized activities. In case such an action has at most one effect we say the action is *deterministic*, and otherwise it is *nondeterministic*. The execution semantics of nondeterministic actions is that by executing the action, one of its effects is nondeterministically chosen and executed.
- A number of UML constraints that model the requirements for synthesis.

- An abstract UML activity, with preconditions, postconditions, and optimality constraints. Optimality contraints are roughly of the form 'action A must happen at least M times and at most N times' and thus limit the number of occurrences of some action in a to-be-synthesized activity. Abstract UML activities are 'empty' in the sense that they contain no nodes and no control flow.

We will only consider UML models that are *valid* with respect to the Poka Yoke validator (see the code implementation).

(UML) Activity. Activities are finite directed graphs consisting of *nodes* and *control flow*[1]. A node can either be a *control node* (initial, final, fork, join, decision, or merge node), or an *call opaque behavior node* which executes an action by calling an opaque behavior[2]. The goal of the activity synthesis algorithm is to synthesize (concrete) UML activities for the specified abstract UML activities in UML models, and updating the UML model by replacing these abstract activities by the concrete syntehsized ones.

Petri Net. A Petri Net is a finite directed graphs consisting of *places*, *transitions*, and *arcs*. Any place in a Petri Net can have at most one *token*. Transitions in a Petri Net can be *fired* to move tokens around between adjacent places. If some transition can fire, we say that it is *enabled*. Any arc in a Petri Net must be connecting a place with a transition. That is, there cannot be an arc from a place to some other place, or from a transition to some other transition. Further details on Petri Nets can be found in the standard literature.

2.2 Tooling and standards

2.3 Supervisory controller synthesis

2.4 Petri Net synthesis

3 Activity Synthesis

Algorithm 1 shows the high-level activity synthesis algorithm. This algorithm is a sequence of operations performed on some input UML model, *umlModel*, containing an abstract activity, to produce a UML model, $umlModel_{concr}$, where the abstract activity is replaced by a synthesized concrete activity. The remainder of this section explains these operations and their preconditions and guarantees.

[1]The UML2 metamodel uses ActivityNode and ActivityEdge, but here it may be better to talk about control flow rather than edges due to the possible ambiguity with automata edges.

[2]Technically there are other types of activity nodes that are supported by our formalim as well, like UML opaque actions and other types of call behavior nodes. But for the purpose of this document and understanding the synthesis algorithm, let us keep those out of scope.

Algorithm 1: Synthesis of Poka Yoke activity diagrams

```
1  procedure activity-synthesis(umlModel)
       // Synthesize a CIF supervisor using data-based synthesis.
2      cifSpec := transform-uml-to-cif(umlModel);
3      cifSupervisor := data-based-synthesis(cifSpec);
       // Generate the CIF state space as a minimal DFA.
4      cifStatespace := generate-statespace(cifSupervisor);
5      cifStatespace := ensure-single-source-and-sink(cifStatespace);
6      cifStatespace_proj := event-based-projection(cifStatespace);
7      cifStatespace_min := dfa-minimization(cifStatespace_proj);
       // Synthesize a minimal Petri Net.
8      (petriNet, regionMapping) :=
        petrinet-synthesis(cifStatespace_min);
       // Transform the Petri Net to an UML activity without edge guards.
9      umlActivity := transform-to-activity(petriNet);
       // Compute the edge guards for the UML decision nodes.
10     cifStatespace_red := reduce-state-annotations(cifStatespace);
11     umlActivity_guards := compute-edge-guards(cifStatespace_red, ...);
       // Post-process the synthesized activity.
12     umlActivity_post := postprocess-activity(umlActivity_guards);
       // Replace abstract UML activity by the synthesized one.
13     umlModel_concr := replace-abstract-activity(umlActivity_post);
14     return umlModel_concr;
```

3.1 Operations

This section describes the operations performed by activity synthesis. For every operation in Algorithm 1 a short explanation is given, followed by the motivation for having that operation, followed by its preconditions and postconditions.

3.1.1 Transforming UML to CIF

The `transform-uml-to-cif`(*umlModel*) operation translates a given UML model, *umlModel*, to a CIF specification to be used for synthesis.

Motivation. With respect to synthesis, the UML model specifies the plant (i.e., UML opaque behaviors) and requirements (i.e, UML constraints). These are translated one-to-one to CIF, to enable data-based synthesis.

Preconditions. This operation requires:

- The input UML model to be valid. See also Section 2.
- The input UML model to contain exactly one UML class.

- The single class within the UML model to have a classifier behavior that is an abstract activity, without nodes and control flow.

Postconditions. This operation produces a CIF specification that:

- For every UML enum declaration, contains a corresponding CIF enum declaration.
- Contains a CIF plant for the single UML class. This plant is a flower automaton, containing one location and only self-loops.
- Contains discrete variables for every UML class property. If a UML class property has a default value, then this value is translated as the default value of the CIF variable. If not, then the corresponding CIF variable is specified to have any value initially, with the 'in any' CIF construct.
- Contains CIF event declarations corresponding to all defined UML opaque behaviors. All opaque behaviors that model deterministic actions are translated as a single controllable event. All opaque behaviors that model non-deterministic actions are translated to multiple CIF events, namely a controllable one for starting the action, and uncontrollable ones for each of its non-deterministic effects to end the action. Such separate uncontrollable events must be defined, since data-based synthesis in CIF disallows controllable events that can happen non-deterministically. So, for data-based synthesis, we need a controllable event to (controllably) start some non-deterministic action, and uncontrollable events for the non-deterministic effects. Moreover, in case the UML model contains non-deterministic actions, an internal *atomicity variable* is declared and maintained in the CIF specification, to ensure that no event may occur between the start and end event of a non-deterministic action.
- Contains an 'initial' predicate from the conjunction of all translated preconditions of the classifier behavior activity of the single UML class. There may be multiple preconditions defined for this activity. Each of these preconditions are translated as Boolean algebraic variables in CIF, for better traceability. The conjunction of all these Boolean algebraic variables then forms the activity precondition, for which an algebraic variable is created as well. This algebraic variable is then used as the 'initial' predicate, which limits the number of initial states to only the ones satisfying the precondition.
- Contains a 'marked' predicate from the conjunction of all translated postconditions of the classifier behavior activity of the single UML class. There may be multiple postconditions defined for this activity. Each of these postconditions are translated as Boolean algebraic variables in CIF, for better traceability. The conjunction of all these Boolean algebraic variables then forms the activity precondition, for which an algebraic variable is created as well. Moreover, in case there are non-deterministic actions, an

extra implicit postcondition is generated, stating that no non-deterministic action must be active (with respect to the atomicity variable explained earlier) for the postcondition to hold. This combined postcondition is then used as the 'marked' predicate.

- Contains requirement invariants stating that the postcondition disables any CIF event. In other words, if you reach a state where the activity postcondition holds, then no further actions have to be taken as they will not contribute to coming closer to a postcondition state. These requirements can be seen as an optimization for synthesis and later state space generation, to avoid considering irrelevant actions/events.

- Contains an edge in the flower automaton plant for every defined UML opaque behavior. An edge is defined for all declared CIF events, both controllable and uncontrollable ones. All controllable CIF events correspond one-to-one to UML opaque behavior definitions, and thus their edge guards are the translated action guard. Moreover, in case of a deterministic action, the edge updates are the translated action effect. In case of a non-deterministic action, the action effects (plural, as in, more than one) are translated on the corresponding uncontrollable events instead. These edge guards and updates also correctly handle and maintain the atomicity variable, as explained before.

- Contains requirement automata for the optimality constraints defined in the UML model[3]. Optimality contraints are roughly of the form 'action A must happen at least M times and at most N times'. Such constraints are translated as requirement automata, containing a discrete variable that maintains how often the action has already occurred. This variable can then be incremented every time the action occurs, and via edge guards and marked predicates the requirement can be enforced.

3.1.2 Data-based synthesis

The operation `data-based-synthesis`(*cifSpec*) executes the data-based supervisory controller synthesis tool that comes with ESCET/CIF. Data-based synthesis is thereby configured to do forward reachability (`--forward-reach=true`) for performance reasons, and to do no BDD predicate simplification (i.e., removing all simplifications from `--bdd-simplify`).

Motivation. Our goal of performing data-based synthesis is to compute all extra restrictions on actions that must be considered by the to-be-synthesized activity to never violate a specified requirement. Data-based synthesis computes a minimally restrictive supervisor for going from a state that satisfies the activity precondition, to a state that satisfies the postcondition, without violating requiements, running into deadlocks, etc. We will later make the behavior of

[3]Note that optimality constraints are temporary, and intended to be removed.

this supervisor explicit (Section 3.1.3), to be able to synthesize a compact Petri Net for it (Section 3.1.7) that is then transformed to an activity (Section 3.1.8).

Once we have the UML activity structure, we need to compute the guards of the outgoing edges of its decision nodes (see Section 3.1.10). To be able to do that, we need to configure data-based synthesis to disable all BDD predicate simplifications. Otherwise, the extra synthesized conditions would be simplified with respect to specified requirements (and probably other things as well), so that the conditions become smaller while the requirements are explicit in the CIF supervisor. Instead, we want the synthesized conditions to completely capture all imposed restrictions, including requirements.

Forward reachability is configured simply for performance reasons, and might make synthesized conditions smaller. We should later evaluate if, and how much, forward reachability actually contributes to that.

Preconditions. All preconditions of the Data-Based Synthesis tool apply[4].

Postconditions. All guarantees of the Data-Based Synthesis tool apply. Moreover, since BDD predicate simplification is disabled, the resulting CIF supervisor contains no requirement invariants. These requirements are instead included in the synthesized conditions.

3.1.3 State space generation

The operation `generate-statespace`(*cifSupervisor*) executes the CIF Explorer tool that comes with Eclipse ESCET[5]. This tool unfolds the state space expressed by the given CIF specification.

Motivation. We need to explicitly unfold the (safe) state space of the synthesized supervisor to be able to construct input for Petri Net synthesis, in order to later synthesize an activity. The state space that is generated from the synthesized supervisor expresses all possible orderings of events, taking into account the synthesized guards and the original action guards as specified in the UML model. The goal of Petri Net synthesis is then to find a compact Petri Net representation of all these possible orderings, whose structure can then relatively easily be translated to a UML activity.

As a side remark; state space generation could later become a performance bottleneck, e.g., in case there are many initial states or large diamond patterns. If this problem materializes, then we could consider symbolic state space generation instead of explicit state space generation, and possibly adapting the Petri Net synthesis algorithms to directly use these symbolic specifications.

Preconditions. Since state space generation uses the CIF Explorer tool that comes with Eclipse ESCET, all preconditions from that tool apply.

[4]See https://eclipse.dev/escet/cif/tools/datasynth.
[5]See https://eclipse.dev/escet/cif/tools/explorer.html.

Postconditions. All guarantees of the CIF Explorer tool from Eclipse ESCET apply. Noteworthy is that the CIF state space will have state annotations, `@state(...)`, that indicate the values of all variables in every location. This information will later be used for computing edge guards (see Section 3.1.10).

Moreover, due to the way our UML/CIF input for synthesis is constructed (e.g., by Section 3.1.1), the resulting state space has the following properties:

- All initial locations in the state space correspond to states that satisfy the precondition of the to-be-synthesized activity.
- All marked locations in the state space correspond to states that satisfy the postcondition of the to-be-synthesized activity.
- Marked locations do not have outgoing edges. This is because it does not make sense to perform further actions after the activity postcondition has been satisfied.
- The state space is deadlock-free. That is, any path from any location in the state space will either end up in a marked location, or will loop forever. In other words, the only locations from which no further edges can be taken are the marked locations.
- Unless the supervisor was empty (in which case the synthesis chain will have crashed already before generating the state space), there is at least one initial location and at least one marked location.
- For every location is holds that all events on outgoing edges are either all controllable, or all uncontrollable. This property is a consequence of the atomic execution semantics of actions. If a nondeterministic action is being executed in some location in the CIF state space, then by the atomicity constraint the only thing that could happen is an uncontrollable event to finish the atomic action. And conversely, if no nondeterministic action were being executed, then only controllable events can be executed to start some new action (assuming the location is not marked).

3.1.4 Ensuring a single source and sink location

The operation `ensure-single-source-and-sink`(*cifStatespace*) transforms the single automaton in the given CIF specification, *cifStatespace*, to ensure it has exactly one initial (source) location and exactly one marked (sink) location.

Motivation. Having exactly one initial location is required for the event-based projection and DFA minimization, described in Section 3.1.5 and Section 3.1.6.

Moreover, having exactly one initial location makes it easier to synthesize activities that must handle multiple initial states. To elaborate on that, we would like to synthesize activities that have exactly one initial node and exactly one final node (in order to keep the activities themselves, as well as their execution semantics, understandable). However, it may happen that *cifStatespace*

has multiple initial locations, for example when the activity precondition allows having more than one initial state. In such cases, we want the synthesized activity to have one initial node, and from there have a decision node that has outgoing edges for the multiple things that can happen. Thus, the single CIF initial location that is guaranteed by `ensure-single-source-and-sink` will then directly correspond to the single initial node in the synthesized activity.

The situation is likewise for final locations. The single CIF final location that is guaranteed by `ensure-single-source-and-sink` will directly correspond to the single final node in the synthesized activity. In case the to-be-synthesized activity has multiple different ways to satisfy the activity post-condition, then this single final node will be preceded by a merge node. So `ensure-single-source-and-sink` ensures that the CIF specification already has the right structure with respect to that.

Preconditions. The input CIF specification is required to:

- Not contain any CIF initialization predicates nor any CIF marker predicates. (This is ensured if *cifStatespace* is generated by the CIF Explorer.)
- Contain exacty one automaton with an explicit alphabet.
- Not contain declarations/identifiers with the names `__init`, `__done`, `__start`, or `__end`. These will be the names of the new initial (source) location, the new marked (sink) location, and the auxiliary events that connect these locations to the original initial/marked locations.

Postconditions. This operation guarantees that:

- The resulting CIF specification has two new declared controllable events, `__start` and `__end`, which have been added to the automaton alphabet.
- The resulting CIF specification has a single initial location named `__init`, even when it already had a single initial location. Auxiliary edges with event `__start` have been added that go from `__init` to all original initial locations. The original initial locations are now no longer initial.
- The resulting CIF specification has a single marked location named `__done`, even when it already had a single marked location. Auxiliary edges with event `__end` have been added that go from all original marked locations to `__done`. The original marked locations are now no longer marked.
- Apart from initial/marked locations, the CIF specification is unchanged.

3.1.5 Event-based projection

The operation `event-based-projection`(*cifStatespace*) projects the single automaton in the given CIF specification for all controllable events. This means that all uncontrollable events are projected away, i.e., *cifStatespace* is transformed to a DFA without keeping any uncontrollable events.

Motivation. Recall that uncontrollable CIF events were created for nondeterministic actions, to model the nondeterministic execution of their effects. However, these uncontrollable events and their corresponding edges are an internal, intermediate step that should not be visible in the synthesized UML activity. So at some point, these uncontrollable events have to be eliminated. This elimination should be done before Petri Net synthesis, due to the atomicity constraint. The goal of Petri Net synthesis is to find a minimal Petri Net whose behavior is trace equivalent to the CIF state space that was given as input to Petri Net synthesis. While doing so, Petri Net synthesis aims to reduce diamond pattern in the state space to fork/join constructs in Petri Nets as much as possible. However, due to the atomicity constraint, the uncontrollable events do not give perfect diamond patterns, since whenever some nondeterministic action is being executed, the atomicity constraint enforces that no other action can be performed, thus impacting interleaving. Therefore, we perform event-based projection on the CIF state space, to restore the diamond patterns that got disrupted by the atomicity constraint, before doing Petri Net synthesis.

Note that Petrify, which is the tool we use for Petri Net synthesis, also has a built-in option `--hide` to hide a list of given events. In earlier versions of our implementation, we used this option instead of doing event-based projection on the level of CIF. However, Petrify's hiding option seems broken, in the sense that we observed that Petrify does not always hide all events in the specified list. This further motivates doing this on the level of CIF instead.

Preconditions. Since `event-based-projection` uses the automaton projection tool that comes with Eclipse ESCET[6], all preconditions from that tool apply. Notably, the input should be a valid CIF specification (e.g., it does not accept automata where some locations have state annotations and some do not) that contains a single automaton, which in our case is the CIF state space. Moreover, this single automaton must have a single initial location.

Postconditions. All guarantees of the automaton projection tool from Eclipse ESCET apply. Notably, event-based projection guarantees that the resulting automaton after projection is a DFA that contains only the projected events, and that is language equivalent to the input specification with respect to those events. In our case, this means that the resulting CIF specification no longer contains the uncontrollable events, and is language equivalent to the input modulo those events. The resulting DFA is not guaranteed to be minimal.

3.1.6 DFA minimization

The `dfa-minimization`($cifStatespace_{proj}$) operation minimizes the single deterministic automaton in the given CIF specification, $cifStatespace_{proj}$.

[6] See https://eclipse.dev/escet/cif/tools/eventbased/projection.html.

Motivation. We use DFA minimization to minimize the input for Petri Net synthesis, to avoid unnecessary work and possibly non-optimal results.

Moreover, note that Petrify, which is the tool we use for Petri Net synthesis, also has a built-in option `--mints` to minimize the input graph modulo trace equivelance. From the documentation of Petrify[7] this option seems to have some interaction with the `--hide` option. However, as explained in Section 3.1.5, `--hide` does not seem to always work. Therefore, in addition to event-based projection, we also do the minimization on the level of CIF.

Preconditions. Since `dfa-minimization` uses the Event-based DFA minimization tool that comes with Eclipse ESCET[8], all preconditions from that tool apply. Notably, the input should be a CIF specification containing one deterministic automaton with a (single) initial location. In our case this is the CIF state space. Note that the previous steps of the activity synthesis algorithm ensure that the input we give to `dfa-minimization` is deterministic and has exactly one initial location.

Postconditions. All guarantees of the Event-based DFA minimization tool from Eclipse ESCET apply. Notably, the result is a minimal DFA that has the same language as the input DFA. (Minimal DFAs are also unique in the sense that there cannot exist two different minimal DFAs with the same language. But at the moment we do not make use of this uniqueness property.)

The resulting automaton has exactly one initial location due to it being a DFA. Moreover, this operation preserves the property from Section 3.1.4 that there is exactly one marked (sink) location. To see why, suppose that event-based projection and/or DFA minimization would somehow have split-up the single marked location into multiple ones. Let us take two of them and refer to these locations as m_1 and m_2. Neither m_1 nor m_2 can have outgoing edges. But then there can be no word in the automaton language that would distinguish m_1 and m_2. Hence they must be the same location.

3.1.7 Petri Net synthesis

The operation `petrinet-synthesis`(*cifStatespace*$_{min}$) performs Petri Net synthesis to compute a minimal free-choice Petri Net whose behavior is trace equivalent to the single automaton in the given CIF specification, *cifStatespace*$_{min}$. Moreover, this operation produces a *region mapping*, which is a mapping that relates the input specification *cifStatespace*$_{min}$ to the synthesized Petri Net.

We use the Petrify tool for performing Petri Net synthesis[9]. We thereby use the following options of Petrify: `-opt` to try to find the best possible result; `-fc` to synthesize a free-choice Petri Net; `-ip` to produce a Petri Net with

[7] Which is included in the distribution that can be downloaded from https://www.cs.upc.edu/~jordicf/petrify/distrib.

[8] See https://eclipse.dev/escet/cif/tools/eventbased/dfa-minimize.html.

[9] See https://www.cs.upc.edu/~jordicf/petrify.

intermediate places (otherwise certain places could be omitted to make the result a bit smaller for visualization purposes); and `-log` to generate a log file.

In our synthesis algorithm, we use PNML[10] as the intermediate format for representing Petri Nets. Therefore, part of the `petrinet-synthesis` operation is to translate $cifStatespace_{min}$ to the input language of Petrify, and transforming the output of Petrify to PNML.

Moreover, although Petrify constructs a region mapping internally, there is no way to retrieve this region mapping by, e.g., some command-line option. The developers of Petrify recommended us to write a separate algorithm to 'recover' this region mapping, by co-simulating the input and output of Petrify to find out which CIF locations correspond to which Petri Net places. Therefore, the implementation of `petrinet-synthesis` also required recovering this region mapping, at least as long a Petrify is being used.

Motivation. By having computed a CIF state space, $cifStatespace_{min}$, we are still quite distant from an UML activity. The main reason is that concurrency can more concisely be represented in UML activities, via their fork and join nodes, with respect to state machines and automata. In contrast, $cifStatespace_{min}$ has all concurrent interleaving explicitly unfolded as diamond patterns. We now somehow have to detect all (diamond) patterns of concurrent interleaving in $cifStatespace_{min}$ and translate those to fork/join patterns in the to-be-synthesized activity. This is done by means of Peri Net synthesis, which is a field of research aiming to do exactly that, but then on Petri Nets rather than (UML) activities. Nevertheless, Petri Nets and activities are quite closely related, in the sense that the semantics of activities is usually defined as a Petri Net semantics. Moreover, there are particular classes of Petri Nets, in particular *free-choice* Petri Nets, that can relatively straightforwardly be translated to activities. Our main strategy is therefore to synthesize a minimal free-choice Petri Net from $cifStatespace_{min}$, and translate that to an UML activity. We thus use Petri Nets as an intermediate formalism in our activity synthesis algorithm.

However, translating a free-choice Petri Net to an UML activity is not yet sufficient: we then still have to compute the edge guards for the decision nodes of the synthesized UML activity. This step must be done separately (see Section 3.1.10), since to the best of our knowledge, Petri Net synthesis with data/state is an open research field for which tooling is not available. Therefore, we must be able to relate the output of Petri Net synthesis to the input specification, $cifStatespace_{min}$. Such a relation is (or should be) produced by the Petri Net synthesis algorithm, and is called a *region mapping*. The reason for this, is that Petri Net synthesis is based on the *theory of regions*. Without going too deep into this theory; the main idea is to group locations from $cifStatespace_{min}$ together so that every such group (roughly) corresponds to a Petri Net place. These groups are then called *regions*. So the Petri Net algorithm can produce a mapping from Petri Net places to the regions from which they are formed, thereby providing an input-output relation. With this relation,

[10] See https://pnml.lip6.fr.

we can later find the relevant data/state and synthesized guards on the level of CIF, for the Petri Net places that will become UML decision nodes, and from those calculate the edge guards. Section 3.1.10 explains this further.

Preconditions. todo

Postconditions. todo

3.1.8 Transform Petri Net to activity

3.1.9 Reduce state annotations

The operation `reduce-state-annotations`(*cifStatespace*) removes all state annotations, `@state(...)`, from locations in the given CIF state space, *cifStatespace*, in which a nondeterministic action is being executed.

Recall that, during the UML-to-CIF conversion, all nondeterministic actions are 'split' into controllable and uncontrollable events, to start and end the action, respectively. Moreover, an atomicity constraint is imposed, stating that no action can happen while some other nondeterministic action is being executed. Of course, in the to-be-synthesized activity, we do not want to see such 'splitted' nondeterministic actions, but we want to see them as single nodes instead. Therefore, we need to get rid of all these uncontrollable events, so that by the time we do Petri Net synthesis, we just have single events for the nondeterministic actions. The 'getting rid of uncontrollable events' step is done by another operation, called event-based projection. However,

3.1.10 Compute edge guards