SMT-Based Diagnosis of Multi-Agent Temporal Plans

Gianluca Torta
Università di Torino, Dipartimento di Informatica
Torino, Italy
gianluca.torta@unito.it

Roberto Micalizio
Università di Torino, Dipartimento di Informatica
Torino, Italy
roberto.micalizio@unito.it

ABSTRACT

The paper proposes a model and methodology for diagnosing action failures in the execution of Temporal Multi-Agent Plans (TMAPs). Contrary to previous proposals in the literature, we characterize actions with a finite set of possible execution modes, where each mode prescribes not only the logic post-conditions of the actions, but also an interval of possible durations. Diagnoses are defined as assignments of modes to the actions that are consistent with the received observations and have the highest likelihood. We propose an algorithm that exploits a Satisfiability Modulo Theories (SMT) solver for the efficient computation of diagnoses. Preliminary experimental results are also presented.

KEYWORDS

Model-Based Diagnosis; Multi-Agent Plan; SMT

ACM Reference Format:

1 INTRODUCTION

The diagnosis of the execution of a multi-agent plan (MAP) - i.e., a plan assigned to a team of (cooperating) agents - has been addressed in a number of works (see e.g., [1, 6, 7]), proposing different notions of plan diagnosis and different diagnostic methodologies. These works assume that the MAP is correct, but during its execution action failures may happen as a consequence of unexpected events such as faults in the functionalities of the agents, or unpredictable changes in the environment. All these works do not consider the temporal dimension; that is, action delays are never taken into account as possible causes and effects of plan execution anomalies. In many practical situations this appears to be a strong limitation since the MAP is often enriched with a schedule, and hence intermediate deadlines and the temporal constraints between actions have to be satisfied at execution time.

Some recent approaches have started to address the temporal dimension in the diagnosis of MAPs [8–10]. However, all these works do not tackle action failures that miss the achievement of some expected effects. In this abstract, we propose a novel formalism for capturing action failures both as missing effects (i.e., logic conditions), and as temporal delays.

2 FORMALIZATION

The major contribution of this abstract is the extension of the formal definition of Temporal Multi-Agent Plan (TMAP) in order to support the diagnosis task. In particular, we define a TMAP as the tuple $(T, A, R, C, M)$, where:

- $T$ is the team of cooperating agents $a_1, a_2, \ldots$
- $A$ is the set of action instances $a_{c1}, a_{c2}, \ldots$ included in the plan, each of which is assigned to a specific agent $agent(ac)$.
- $R$ is a partial order relation over $A$ establishing the precedence constraints in the execution of actions;
- $C$ is a set of concurrency constraints of the form $ac, ac'$, where $agent(ac) \neq agent(ac')$, and whose meaning is: the two actions are performed simultaneously as a joint-action.
- $M$ is the set of all the possible behavioral modes that can be associated with the action instances in $A$. This is the novel element of our formalization that allows a knowledge engineer to define (anomalous) action behaviors according to the modality in which the action is performed. These behaviors encompass both delays in the completion of the action, as well as missing effects. Specifically, for each action $ac$ a set of modes $M[ac]$ is defined. Due to space reasons, we omit a rigorous formalization of the modes in $M[ac]$. We just say that the designer can specify a common set pre of pre-conditions for action $ac$, and for each mode $m \in M[ac]$:
  1. a time interval representing the possible range of duration of action $ac$ while performed in modality $m$, and
  2. a set eff of grounded literals resulting from the execution of $ac$. Therefore a modality is a (possibly faulty) action model, that is not used for the planning purpose, but for the diagnostic one, and hence it takes into account that actions may obtain different effects from the nominal, expected ones. More importantly, for each mode $m$ the engineer has also to specify its rank: a non-negative integer value representing the
order-of-magnitude probability of the mode [4]; lower ranks correspond to higher probabilities. Rank zero is associated with all and only the nominal modalities.

Example 2.1. Let us consider a simple case with two agents: \( T = \{ag1, ag2\} \) (see Figure 1). The set of actions is \( A = \{ac11, \ldots, ac15, ac21, \ldots, ac23\} \), with order relations \( R \) as shown in the figure by the arrows. The double arrow between \( ac11 \) and \( ac22 \) denotes a joint-action: the two agent actions must be performed simultaneously to push a heavy object. The eight actions are instances of just four types of actions: move, load, put, and pushHvy. This last action can be performed only by two agents together. That is, in the TMAP in Figure 1, the two agents have to cooperate for moving a heavy object \( o1 \) from location \( loc1 \) to location \( loc2 \). Note the precedence relations between \( ac22 \) and \( ac11 \), and between \( ac23 \) and \( ac12 \). These relations impose that actions \( ac11 \) and \( ac12 \) can start only when action \( ac21 \) and \( ac23 \), respectively, have ended.

The TMAP model specifies also nominal and fault models. For instance, in nominal mode \( (N) \), a move\((ag,p1,p2)\) requires the agent to be in place \( p1 \), causes the agent to arrive in place \( p2 \), and has an execution time in the interval \([1, 2]\). The rank is 0, meaning that the N mode is preferred in diagnostic explanations. In a faulty mode, say \( F3 \), the action has an execution time in the interval \([10, 25]\), a rank 3, and leaves the agent in \( p1 \).

3 PLAN EXECUTION FAILURE PROBLEM

We define a timed observation as a pair \( (e, t) \), where \( e \) is the observed event, and \( t \) is the time when \( e \) occurred.

Definition 3.1 (PEF problem). A Plan Execution Failure (PEF) problem is a pair \( (P, Obs) \) where \( P \) is a TMAP and \( Obs \) a set of timed observations.

We say that a mapping \( H : A \rightarrow M[A] \) is a hypothesis about the modes of actions in \( P \) that assigns each action \( ac \in A \) with a mode \( m \in M[ac] \). Since action modes are associated with time intervals and logic pre-/post-conditions, a hypothesis \( H \) can be used to estimate a set of possible executions of \( P \), that we call temporal execution profiles. We denote with \( TP(H) \) the space of possible temporal execution profiles for the plan \( P \) consistent with \( H \), and with \( TP(Obs) \) the profile space consistent with timed observations \( Obs \).

Definition 3.2 (PEF solution). Let \( (P, Obs) \) be a PEF problem, a solution to such a problem is a hypothesis \( H^{sol} \) such that:

1. \( TP(H^{sol}) \cap TP(Obs) \neq \emptyset \)
2. \( \text{rank}(H^{sol}) \) is minimal: no other hypothesis \( H' \) such that \( \text{rank}(H') < \text{rank}(H^{sol}) \) satisfies (1)

Example 3.3. With reference to the TMAP in Figure 1, let us consider the set of observations \( Obs^1 = \{(\text{holds}(ag1, o2), 15)\} \). In this case, three rank-one diagnoses are possible: it is sufficient to assume an \( F1 \) fault (which causes a delay in the interval \([3, 9]\)) to either one of \( ac21, ac22, \) and \( ac23 \), to explain the delay of \( o1 \) in leaving \( o1 \) at \( loc1 \). A rank-two diagnosis setting either \( ac11 \) or \( ac12 \) in mode \( F2 \) (delay \([10, 25]\)) would also be consistent with \( Obs^1 \), but it is discarded as it is not minimal.

Now, let us consider observations \( Obs^2 = \{(\text{holds}(ag1, o2), 15), (\text{at}(ag1, loc4), 15)\} \); the observation about the position of agent \( ag1 \) is sufficient to conclude that the only possible diagnosis is that action \( ac14 \) behaved with modality \( F2 \): the \( \text{put} \) of \( o2 \) by \( ag1 \) was unsuccessful in achieving the propositional effects. The latter case shows a diagnosis that not only explains a delay, but also an unexpected effect expressed as a propositional logic condition.

Given the encoding of a PEF problem in the input language of Z3, we compute the diagnoses exploiting the ability of Z3 to produce an unsat core every time it is invoked on an unsatisfiable instance. An unsat core is a set of assertions in the input to Z3 that cannot hold simultaneously and therefore require to withdraw at least one of them in order to get satisfiability. Given the set of unsat cores that is cumulatively produced during the search for the solutions, we can avoid to explore the parts of the search space that do not hit (i.e., withdraw at least an assignment from) all of them. Due to lack of space we omit details, but this technique is well known in diagnosis, also on approaches based on SMT [3, 5]. We will denote it as Conflict-based Best-First Search (CBFS).

4 EXPERIMENTAL EVALUATION

We have implemented the SMT-based approach to diagnosis described above as a Java program exploiting the Z3 solver. The tests were run on a virtual machine running Linux Ubuntu 14.04, equipped with an i7 M640 CPU at 2.80 GHz, and 4 GB RAM.

We have considered a Logistic domain which reflects the domain used in the examples. We have experimented our approach by running a number of software simulated tests under different configurations, defined by varying the number of agents #ag and number of actions #ac, and the ranks of injected failures.

In Table 1, we show results obtained with configurations including 2, 3, and 4 agents. The average times for finding a solution grow with the number of agents, number of actions per agent, and ranks of injected faults, as expected. We haven’t reported results in the last row, since several cases took more than a 1 hour timeout on the test machine.
REFERENCES


