Atomicity Decomposition a Technique for Structuring Refinement in Event-B

Asieh Salehi Fathabadi, Michael Butler
University of Southampton
asf08r, mjb@ecs.soton.ac.uk

1 Introduction

Atomicity Decomposition [1] is a technique in the Event-B formal method, which augments Event-B refinement with additional structuring in a diagrammatic notation and supports clear view of event sequencing through refinement levels. Although the refinement technique in Event-B provides a flexible approach to modeling, it does not show all the relations between abstract events and concrete events. The atomicity decomposition approach is intended to make the relationships between abstract and concrete events clearer and easier to manage than simply using the standard Event-B refinement method.

We believe that reusability is very important specially in modeling of large and complex model. Using patterns in atomicity decomposition technique addresses this issue. The atomicity decomposition technique is applied to two complex case studies, multi media protocol [2] and an on-board instrument controller for a space craft and some new patterns are discovered during development of case studies.

Developing atomicity decomposition plug-in for Event-B toolkit (Rodin platform) helps developers to make Event-B models in a way that most of the modeling tasks can be done in a graphical environment which in particular shows sequential relationships between levels of refinement. The Rodin platform serves as a host for the plug-in developed to give tool support to atomicity decomposition technique.

2 Atomicity Decomposition Diagrams

The important contribution of the atomicity decomposition diagram is that it explicitly shows the relationship between abstract events and the corresponding concrete events, whereas the Event-B text is not able to show this sequential relationship between refinement levels. The sequencing in Event-B model is done with use of some control variables.

Consider an example that events E21, E22 should execute before event E23 in order to reach a state that enables event E23. This is implicitly done by some control variables in Event-B model. An Event-B model of this diagram is illustrated in Figure 1. VarE21, VarE22 and VarE23 are control variables. Event E22 is guarded by VarE21 which indicates the sequential execution of E21 and E22. Also event E23 is guarded by VarE22. Event E23 can be executed only when E22 has been executed, and event E22 can be executed only when E21 has been executed.

The atomicity decomposition diagram is used because it explicitly illustrates our intention that the effect achieved by E1 at the abstract level is realized at the refined level by execution of E21 followed by E22 followed by E23, Figure 2. The abstract atomic event, E1 in this case, appears in the root node, which is decomposed to sub-events in next refinement level. There is a sequential control from left to right between sub-events; in other words, they, E21, E22, E23 in this figure, are read from left to right. One important feature in the structure is types of lines, solid lines and dashed lines. The sub-event corresponding to dashed line, E21, E22, are new events which refine skip in abstract level. The child node with a solid line, E23, is a main event which should be proved to refine the abstract one, E1.

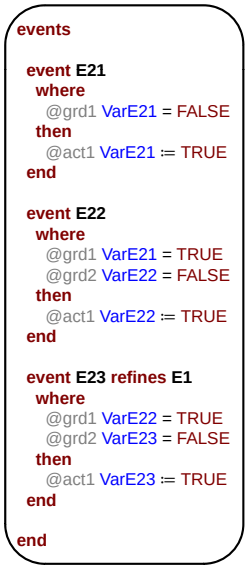

Figure 1: Event-B Model

In the standard Event-B method E21 and E22 are refinements of skip, and there is no explicit connection to E1. Technically, E23 is the only event that refines E1 but the diagram indicates that we break the atomicity of E1 into events E21, E2 and E23.

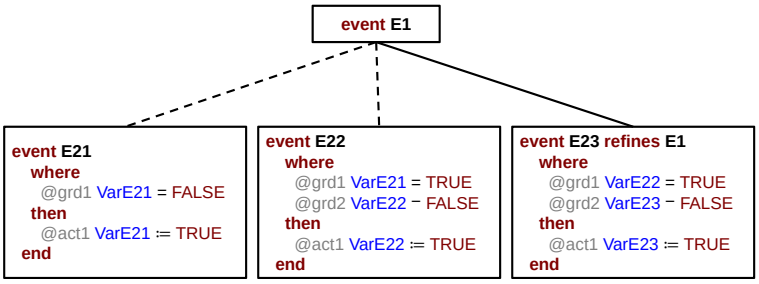

Figure 2: Atomicity Decomposition Diagram

This talk will outline the application of atomicity decomposition diagrams to two case studies, a multi media protocol and an on-board instrument controller for a space craft. It will also outline our on-going work on providing tool support for these diagrams as a Rodin plug-in.

References

[1] Michael Butler: Decomposition Structures for Event-B. In Integrated Formal Methods iFM2009, volume LNCS 5423. Springer, (2009)

[2] Asieh Salehi Fathabadi and Michael Butler: Applying Event-B Atomicity Decomposition to a Multi Media Protocol, In FMCO Formal Methods for Components and Objects, (2010)