Towards the Composition of Specifications in Event-B

Renato Silva¹,²

School of Electronics and Computer Science
University of Southampton
Southampton, UK

Abstract
The development of a system can start with the creation of a specification. Following this viewpoint, we claim that often a specification can be constructed from the combination of specifications which can be seen as composition. Event-B is a formal method that allows modelling and refinement of systems. The combination, reuse and validation of component specifications is not currently supported in Event-B. We extend the Event-B formalism using shared event composition as an option for developing (distributed) systems. Refinement is used in the development of specifications using composed machines and we prove that properties and proof obligations of specifications can be reused to ensure valid composed specifications. The main contributions of this work are the Event-B extension to support shared event composition and refinement including the proof obligations for a composed machine.

Keywords: composition, refinement, Event-B, development of specifications, formal methods

1 Introduction

Systems can often be seen as a combination and interaction of several sub-specifications (hereafter called sub-components) where each sub-component has its own functionality aspect. This view introduces modularity in the system: different sub-components represent a particular functionality and changes in the sub-components are accommodated more gracefully [12] in the system specification. We use composition to structure specifications through the interaction of sub-components seen as independent modules. This use of composition is not new in other formal notations: examples are [22,13,15].

¹ Part of this research was carried out within the European Commission ICT DEPLOY
² Email: ras07r@ecs.soton.ac.uk

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs
Here we express how we can use (and reuse) composition for building specifications in Event-B [2] through sub-components (modules) interaction, benefiting from their properties and proof obligations (POs). The interesting part of composition involves the interaction of sub-components which usually occurs by shared state [4], shared operations [7] or a combination of both (for example, fusion composition [15]). Although sub-components have states, we mainly focus on their (visible) events similar to CSP [11,14]: we follow a shared event composition approach where events are synchronised in parallel.

This document is structured as follows: Sect. 2 briefly describes Event-B. Section 3 introduces the notion and properties for shared event approach. Composed machine, POs and the monotonicity property are introduced in Sect. 4. Related work, conclusions and future work are drawn in Sect. 5.

2 Event-B Language

Event-B is a formal methodology that uses mathematical techniques based on set theory and first order logic supporting system development with abstract specification. An abstract Event-B specification is divided into a static part called context and a dynamic part called machine. A machine sees as many contexts as desired. A context consists of sets $s$ (collection of elements or a type definition), constants $c$ and axioms $A(\ldots)$ of the system. A machine contains the state (global) variables $v$ whose values are assigned in events. Events that can be parameterised (local variables $p$) occur when enabled by their guards $G(\ldots)$ being true and as a result actions $S(\ldots)$ are executed. Invariants $I(\ldots)$ define the dynamic properties of the specification and POs are generated to verify that these properties are always maintained. An event $evt$ is expressed by parameters $p$, by guards $G(s, c, p, v)$ and actions $S(s, c, p, v, v')$:

$$
evtx = \text{ANY } p \text{ WHERE } G(s, c, p, v) \text{ THEN } S(s, c, p, v, v') \text{ END.}
$$

When the guard $G(s, c, p, v)$ is true then the event $evt$ is enabled and therefore the action $S(s, c, p, v, v')$ updates the set of variables $v$ to $v'$ (value of $v$ after the assignment). An abstract Event-B specification can be refined with the introduction of more details and becoming closer to a concrete implementation. A context extends an abstract context by adding sets, constants or axioms. The abstract context properties are still assumed. Refinement of a machine consists of refining existing events. The relation between variables in the concrete and abstract model is given by a gluing invariant $J(\ldots)$. POs are generated to ensure that this invariant is preserved in the concrete model. New events can be added, refining $skip$ which may be declared as convergent, meaning they do not cause divergence. The convergence is proved if each new event decreases a variant. The variant must be well-founded and may be an integer or a finite set.
3 Shared Event Approach

Sub-component specifications that are part of a full system specification, deal with a particular part of the system being modelled. Sub-component interaction must be verified to comply with the desired behavioural semantic of the system. The interaction usually occurs as a shared state, shared event or a combination of both as described. Here we focus on the developments using shared event composition only where composition is treated as the conjunction of individual elements’ properties: conjunction of individual invariants, conjoining variables and synchronisation of events. Consider Fig. 1(a) where machine A has events $e1$ and $e2$ that use variable $v1$. Moreover machine B has events $e3$, $e4$ and $e5$ using variables $v2$ and $v3$. If events $e2$ and $e3$ occur in parallel, they can be synchronised: another option is to compose machines A and B by sharing events. For example, machine D in Fig. 1(c) where $e2$ from machine A and $e3$ from machine e3 are composed: $e2 \parallel e3$. The interaction of machines A and B through their events results in a composed event sharing two independent variables: $v1$ and $v2$. The parallel composition of events $e2$ and $e3$ from Fig. 1 is defined as Def. 3.1 [7]:

**Definition 3.1** Composition of events $e2$ and $e3$ with parameter $p$ results in:

\[
\begin{align*}
  e2 & \triangleq \text{ANY } p? , x \text{ WHERE } p? \in C \land G(p?, x, m) \text{ THEN } S(p?, x, m) \text{ END} \\
  e3 & \triangleq \text{ANY } p!, y \text{ WHERE } H(p!, y, n) \text{ THEN } T(p!, y, n) \text{ END} \\
  e2 \parallel e3 & \triangleq \text{ANY } p!, x, y \text{ WHERE } p! \in C \land G(p!, x, m) \land H(p!, y, n) \text{ THEN } S(p!, x, m) \parallel T(p!, y, n) \text{ END}
\end{align*}
\]

where $x, y, p$ are sets of parameters from each of the events $evt1$ and $evt2$. Event $evt1$ has $p?$ as an input parameter and $evt2$ has $p!$ as an output parameter and the resulting composition is $p!$ itself an output parameter (like in CSP). This property can be used to model message-passing systems: $evt2$ sends a message to $evt1$ using the parameter $p$. Communication between parameters of type input is also possible but not with both types output since this could lead to a deadlock state [7]. Event-B has the same semantic structure and refinement definitions as action systems [17]. It is possible to make a correspondence between parallel composition in CSP and an event-based view of parallel composition for action systems [9,6].

![Diagram of shared event composition](image-url)
Theorem 3.2 The shared event parallel composition of Event-B machines corresponds to CSP parallel-composition. The failure-divergence semantics of CSP can be applied to Event-B machines. The failure divergence semantics of machine $M$ in parallel with $N$, $M \parallel N$ is defined as:

$$[M \parallel N] = [M] \parallel [N]$$

where $[M]$ and $[N]$ are the failure divergence semantics of $M$ and $N$ respectively. The proof of this theorem can be found in [9].

The semantics of the parallel composition of machines $M$ and $N$ corresponds to the set of failure-divergence for each individual machine in parallel. From the correspondence between action systems and Event-B, machines $M$ and $N$ can be refined independently which is one of the most important and powerful properties that shared event composition in Event-B inherits from CSP. The monotonicity property for the shared event composition in Event-B is proved by means of proof obligation in Sect. 4.3. When sub-components are composed it is desirable to define properties that relate the individual sub-components allowing interactions. These properties are expressed by adding composition invariants $I_{CM}(s, c, v_1, \ldots, v_m)$ to the composed machine constraining the variables of all machines being composed.

Definition 3.3 The invariant of the parallel composition of machines $M_1$ to $M_n$ with variables $v_1$ to $v_n$ respectively is the conjunction of the individual invariants and the composition invariant $I_{CM}(s, c, v_1, \ldots, v_n)$:

$$I(M_1 \parallel \cdots \parallel M_n) = I_1(s, c, v_1) \land \cdots \land I_m(s, c, v_m) \land I_{CM}(s, c, v_1, \ldots, v_n).$$ (1)

In Fig. 1, composed machine $D$ has as invariant the conjunction of the individual invariants $I(A \parallel B) = I_A(s, c, v_1) \land I_B(s, c, v_2, v_3)$ plus possible composition invariant $I_{CM}(s, c, v_1, v_2, v_3)$. In a shared event composition the sub-components have independent state space (variables are unique to each machine). Consequently composition reasoning is simplified as there are no constraints between state spaces of sub-components.

4 Composed Machines: Composition and Refinement

We define a new construct composed machine, representing the shared event composition of Event-B machines. We aim to have a construct that remains reactive to changes in the sub-components. Consequently the composition is structural. The interaction of sub-components following a “top-down” approach, can represent a refinement of an existing abstraction. To formalise the composition, it is necessary to define composition and refinement POs. In the following sections, we introduce the structure of a composed machine, respective POs and prove the monotonicity property.
4.1 Structure of Composed Machines

A shared event composed machine is expressed as the parallel conjunction of sub-component properties. Machines are composed in parallel including their properties and events: $CM \equiv M_1 \parallel \cdots \parallel M_m$ as seen in Fig. 2. Moreover:

- The composed machine variables are all the sub-component variables ($v_1$ from $M_1$, $v_2$ from $M_2$, $\ldots$, $v_m$ from $M_m$) and are state-space disjoint.
- The invariants of the composed machine are defined as Def. 3.3.
- The composed events are defined according to Def. 3.1.

Next we present the required POs to verify composed machines.

4.2 Proof Obligations

POs play an important role in Event-B developments. POs are generated to verify the properties of a model. For simplicity we define POs in terms of a composition of two machines $M_1$ and $M_2$ that refine machine $M_0$, but the rules generalise easily to the composition of $n$ machines. Furthermore context elements in the formulas $(s, c, A(s, c))$ are not considered. The POs defined for standard machines (invariant preservation, well-definedness, refinement, etc) [2] are defined for composed machines. We simplify the composed machines POs by assuming that the POs of the individual machines hold. We define the additional POs necessary to ensure that the composed machine satisfies all the standard POs. We consider that the POs of the $M_0$, $M_1$ and $M_2$ hold. The respective composition POs are described as follows.

4.2.1 Consistency

Consistency POs are required to be always verified. Consistency is expressed by the feasibility and invariant preservation POs for each event. The feasibility proof obligation for the composed event $evt_1 \parallel evt_2$ is $FIS_{evt_1\parallel evt_2}$.

**Theorem 4.1** The individual $FIS$ PO for each event can be reused for proving feasibility for each composed event and that is enough to verify this prop-
tery. From [2]:

\[ FIS_{evt1} : I_1(v_1) \wedge G_1(p_1, v_1) \vdash \exists v'_1 \cdot (S_1(p_1, v_1, v'_1)) \]  
\[ FIS_{evt2} : I_2(v_2) \wedge G_2(p_2, v_2) \vdash \exists v'_2 \cdot (S_2(p_2, v_2, v'_2)) \]  
\[ FIS_{evt1||evt2} : IC_M(v_0, v_1, v_2) \wedge I_1(v_1) \wedge I_2(v_2) \wedge G_1(p_1, v_1) \wedge G_2(p_2, v_2) \wedge S_1(p_1, v_1, v'_1) \wedge S_2(p_2, v_2, v'_2). \]

Assume: FIS_{evt1} and FIS_{evt2}.

Proof. Assume the hypotheses of FIS_{evt1||evt2}. Prove: \( \exists v'_1, v'_2 \cdot (S_1(p_1, v_1, v'_1) \wedge S_2(p_2, v_2, v'_2)) \). The proof proceeds as follows:

\[
\exists v'_1 \cdot (S_1(p_1, v_1, v'_1)) \wedge \exists v'_2 \cdot (S_2(p_2, v_2, v'_2))  
\Rightarrow (FIS_{evt1} \wedge FIS_{evt2}).  
\]

\{(2),(3)+ hypotheses of (4)\}

\[ \square \]

In the composed machine, invariant preservation PO \( INV_{CM} \) corresponds to the invariant preservation in all events. The invariant preservation PO for the composed event \( evt1 || evt2 \) is \( INV_{evt1||evt2} \).

**Theorem 4.2** For each invariant \( i \) from the set of invariants \( I \) in a composed machine, composition invariant \( I_{CM}(v_0, v_1, v_2) \) needs to be verified. From [2]:

\[ INV_{evt1} : I_1(v_1) \wedge G_1(p_1, v_1) \wedge S_1(p_1, v_1, v'_1) \vdash i_1(v'_1) \]  
\[ INV_{evt2} : I_2(v_2) \wedge G_2(p_2, v_2) \wedge S_2(p_2, v_2, v'_2) \vdash i_2(v'_2) \]  
\[ INV_{evt1||evt2} : IC_M(v_0, v_1, v_2) \wedge I_1(v_1) \wedge I_2(v_2) \wedge G_1(p_1, v_1) \wedge G_2(p_2, v_2) \wedge S_1(p_1, v_1, v'_1) \wedge S_2(p_2, v_2, v'_2) \vdash i_1(v'_1) \wedge i_2(v'_2) \wedge i_{CM}(v_0, v'_1, v'_2). \]

Assume: \( INV_{evt1} \) and \( INV_{evt2} \).

Prove: \( INV_{evt1||evt2} \).

Proof. Assume the hypotheses of \( INV_{evt1||evt2} \). Prove: \( i_1(v'_1) \wedge i_2(v'_2) \wedge i_{CM}(v_0, v'_1, v'_2) \). The proof proceeds as follows:

\[
i_1(v'_1) \wedge i_2(v'_2) \wedge i_{CM}(v_0, v'_1, v'_2)  
\Leftrightarrow INV_{evt1} \wedge INV_{evt2} \wedge i_{CM}(v_0, v'_1, v'_2). \  
\]

\{(5),(6) and hypotheses of (7)\}

\[ \square \]

Well-definedness for expressions (guards, actions, invariants, etc) needs to be verified. These are verified by means of POs in Event-B [3]. For composed machines, well-definedness POs are only generated for \( I_{CM}(v_0, v_1, v_2) \). Other expressions are verified in the individual machines.

### 4.2.2 Refinement

Refinement POs are required when the composed machine refines an abstract machine. Machine \( M_0 \) with variables \( v_0, \) invariant \( I_0(v_0) \) and abstract event
\( \text{evt}_0 \) is refined by composed machine \( CM \) defined by machines \( M_1 \) with variables \( w_1 \), invariant \( I_1(w_1) \), event \( \text{evt}_1 \) and \( M_2 (w_2 ; I_2(w_2); \text{evt}_2) \) and composition invariant \( J_{CM}(v_0, w_1, w_2) \). The composed event \( \text{evt}_1 \parallel \text{evt}_2 \) refines the abstract event \( \text{evt}_0 \). A general refinement PO (\( \text{REF}_{\text{evt}_i} \)) for a machine \( M \) refining event \( \text{evt} \) follows from:

\[
\text{REF}_{\text{evt}_i} \equiv I_i(v_i) \land J_i(v_i, w_i) \land H_i(q_i, w_i) \land T_i(q_i, w_i, w_i') \vdash \exists v_i'. G_i(v_i) \land S_i(p_i, v_i, v_i') \land J_i(v_i', w_i')
\]  

(8)

**Theorem 4.3** For each composed event \( \text{evt}_1 \parallel \text{evt}_2 \), refining abstract event \( \text{evt}_0 \) through (gluing) composition invariant in a composed machine, the refinement \( \text{REF} \) PO consists in proving the guard strengthening of abstract guards, proving the simulation of the abstract variables \( (v_0') \) and preserving the gluing invariant \( (J_{CM}(v_0', w_1', w_2')) \). From [2] and (8):

\[
\begin{align*}
\text{INV}_{\text{evt}_1} : & \quad I_1(w_1) \land H_1(q_1, w_1) \land T_1(q_1, w_1, w_1') \vdash i_1(w_1') \\
\text{INV}_{\text{evt}_2} : & \quad I_2(w_2) \land H_2(q_2, w_2) \land T_2(q_2, w_2, w_2') \vdash i_2(w_2') \\
\text{REF}_{\text{evt}_0 \parallel \text{evt}_1 \parallel \text{evt}_2} : & \quad I_0(v_0) \land I_1(v_1) \land I_2(v_2) \\
& \land H_1(q_1, w_1) \land H_2(q_2, w_2) \land T_1(q_1, w_1, w_1') \land T_2(q_2, w_2, w_2') \\
& \vdash \exists v_0'. G_0(p_0, v_0) \land S_0(p_0, v_0, v_0') \land I_1(v_1') \land I_2(v_2') \land J_{CM}(v_0', w_1', w_2').
\end{align*}
\]

Assume: \( \text{INV}_{\text{evt}_1} \) (9) and \( \text{INV}_{\text{evt}_2} \) (10).

Prove: \( \text{REF}_{\text{evt}_0 \parallel \text{evt}_1 \parallel \text{evt}_2} \).

**Proof.** Assume the hypotheses of \( \text{REF}_{\text{evt}_0 \parallel \text{evt}_1 \parallel \text{evt}_2} \). Prove: \( \exists v_0'. G_0(p_0, v_0) \land S_0(p_0, v_0, v_0') \land I_1(v_1') \land I_2(v_2') \land J_{CM}(v_0', w_1', w_2'). \) The proof proceeds as follows:

\[
G_0(p_0, v_0) \land I_1(v_1') \land I_2(v_2') \\
\land \exists v_0'. (S_0(p_0, v_0, v_0') \land J_{CM}(v_0', w_1', w_2')) \\
\equiv G_0(p_0, v_0) \land \exists v_0'. (S_0(p_0, v_0, v_0') \land J_{CM}(v_0', w_1', w_2')) \quad \{ \text{from (9) + (10) for each } i_1(w_1'), i_2(w_2') \}
\]

\[\square\]

These are the required POs to verify composed machines. Next we show that composed machines are monotonic which allows to further refine individual machines preserving composition.

### 4.3 Monotonicity of Shared Event Composition for Composed Machines

An important property of the shared event composition in Event-B is monotonicity. We prove it by means of refinement POs confirming the result described by Butler [9] using actions systems and CSP. Figure 3 shows abstract component specification \( M_1 \) composed with other component specification \( N_1 \), creating a composed model \( M_1 \parallel N_1 \). \( M_1 \) is refined by \( M_2 \) and \( N_1 \) by \( N_2 \) respectively. Once we compose component specifications \( M_1 \) and \( N_1 \), discharge the required composed POs, \( M_1 \) and \( N_1 \) can be refined individually while the composition properties are preserved without the need to recompose refinements \( M_2 \) and \( N_2 \). We want to formally prove the monotonicity property through refinement POs between composed machines. Therefore if the refinement POs hold between \( CM_1 \) and \( CM_2 \), we can say that \( CM_2 \) refines \( CM_1 \): \( CM_1 \sqsubseteq CM_2 \). The gluing invariant of the refinement between
The proof proceeds as follows:

Assume:

Prove:

Assume the hypotheses of \( \text{evt}_{M2} \) and \( \text{evt}_{N2} \). We can derive the refinement PO between \( M2 \) and \( M1 \) for the concrete event \( \text{evt}_{M2} \) refining abstract event \( \text{evt}_{M1} \).

\[
\text{REF}_{\text{evt}_{M1} \subseteq \text{evt}_{M2}}: \quad I_M(v_M) \land J_M(v_M, w_M) \land G_M(p_M, v_M) \land H_M(q_M, w_M) \\
\land S_M(p_M, v_M, v'_M) \land T_M(q_M, w_M, w'_M) \\
\vdash \exists v'_M, G_M(p_M, v_M) \land S_M(p_M, v_M, v'_M) \land J_M(v'_M, w'_M). \tag{11}
\]

The refinement PO between \( N2 \) and \( N1 \) is similar. We refine an abstract event in \( \text{CM1} \) by a concrete one in \( \text{CM2} \) and verify that the refinement POs for each individual machine hold for the composition. Event \( \text{evt}_{M1} \) from machine \( M1 \) and event \( \text{evt}_{N1} \) from machine \( N1 \) are composed, resulting in the abstract composed event \( \text{evt}_{M1} \parallel \text{evt}_{N1} \) in \( \text{CM1} \) from Fig. 3. The gluing invariant relating the states of \( \text{CM1} \) and \( \text{CM2} \) is expressed as the conjunction of the gluing invariants between \( (M1 \) and \( M2) \) and \( (N1 \) and \( N2) \):

\[
J_{CM}(v_M, v_N, w_M, w_N) = J_M(v_M, w_M) \land J_N(v_N, w_N) \tag{12}
\]

**Theorem 4.4** The refinement POs for composed machines is expressed as the conjunction of the refinement POs for the individual machines. Therefore the monotonicity property holds if the refinement POs of individual machines hold. The refinement PO between concrete composed event \( \text{evt}_{M2} \parallel \text{evt}_{N2} \) and abstract composed event \( \text{evt}_{M1} \parallel \text{evt}_{N1} \) is expressed as:

\[
\text{REF}_{\text{evt}_{M1} \parallel \text{evt}_{N1}}: \quad I_M(v_M) \land J_M(v_M, w_M) \land J_{CM}(v_M, v'_M) \land J_{CM}(v'_M, v''_M) \\
\land H_M(q_M, w_M) \land H_N(q_N, w_N) \land T_M(q_M, w_M, w'_M) \land T_N(q_N, w_N, w''_N) \\
\vdash \exists v'_M, v'_N, G_M(p_M, v_M) \land G_N(p_N, v_N) \land S_M(p_M, v_M, v'_M) \land S_N(p_N, v_N, v'_N) \\
\land J_M(v'_M, w'_M) \land J_N(v'_N, w'_N). \tag{13}
\]

**Assume:** \( \text{REF}_{\text{evt}_{M1} \subseteq \text{evt}_{M2}} \) and \( \text{REF}_{\text{evt}_{N1} \subseteq \text{evt}_{N2}} \).

**Prove:** \( \text{REF}_{\text{evt}_{M1} \parallel \text{evt}_{N1}} \). **Prove:** \( \text{REF}_{\text{evt}_{M1} \parallel \text{evt}_{N1}} \).

The proof proceeds as follows:

\[
\exists v'_M, v'_N: G_M(p_M, v_M) \land G_N(p_N, v_N) \\
\land S_M(p_M, v_M, v'_M) \land S_N(p_N, v_N, v'_N) \\
\land J_M(v'_M, w'_M) \land J_N(v'_N, w'_N) \quad \{\text{expanding } J_{CM} \text{ from (12)}\}
\]

\[
\equiv \exists v'_M, v'_N: G_M(p_M, v_M) \land S_M(p_M, v_M, v'_M) \land J_M(v'_M, w'_M) \\
\land \exists v'_N, G_N(v_N) \land S_N(p_N, v_N, v'_N) \land J_N(v'_N, w'_N) \quad \{\text{disjoint } v'_M, v'_N\}
\]

\[
\iff \text{REF}_{\text{evt}_{M1} \subseteq \text{evt}_{M2}} \land \text{REF}_{\text{evt}_{N1} \subseteq \text{evt}_{N2}} \quad \{\text{(11) + hypotheses of (13)}\}
\]

8
We also need to prove the monotonicity for single (non-composed) events that appear at both levels of abstraction. We shall prove it using machines $M_1$ and $CM_2$. In this case, the gluing invariant described in (12) does not use neither the variables $(v_N)$ neither the invariants $(I_N)$ neither events $(evt_{N1})$ from $N_1$. Therefore it can be simplified and rewritten as:

$$J_{CM}(v_M, w_M, w_N) = J_M(v_M, w_M) \land J_N(w_N)$$  \hspace{1cm} (14)

**Theorem 4.5** An individual event $evt_{M1}$ in machine $M_1$ is refined by a composed event $evt_{M2} = evt_{N2}$ in composed machine $CM_2$. The monotonicity is preserved if the refinement PO between $M_1$ and $M_2$ hold in conjunction with the gluing invariant preservation PO for the composed event $evt_{M2} = evt_{N2}$. The refinement PO between concrete composed event $evt_{M2} = evt_{N2}$ and abstract non-composed event $evt_{M1}:

$$REF_{evt_{M1} \subseteq (evt_{M2} || evt_{N2})} : \quad J_M(v_M) \land J_{CM}(v_M, w_M, w_N) \land H_M(q_M, w_M) \land H_N(q_N, w_N)$$

$$\land T_M(q_M, w_M, w'_M) \land T_N(q_N, w_N, w'_N)$$

$$+ \exists v'_M G_M(p_M, v_M, w'_M) \land S_M(p_M, v_M, v'_M) \land J_{CM}(v'_M, w'_M, w'_N).$$  \hspace{1cm} (15)

**Assume:** $REF_{evt_{M1} \subseteq (evt_{M2} || evt_{N2})}$ and $INV_{evt_{M2} || evt_{N2}}$ (based on (7)).

**Prove:** $REF_{evt_{M1} \subseteq (evt_{M2} || evt_{N2})}$. 

**Proof.** Assume the hypotheses of $REF_{evt_{M1} \subseteq (evt_{M2} || evt_{N2})}$ and the hypotheses of $INV_{evt_{M2} || evt_{N2}}$. Prove: $\exists v'_M G_M(p_M, v_M, w'_M) \land S_M(p_M, v_M, v'_M) \land J_{CM}(v'_M, w'_M, w'_N)$. The proof proceeds as follows:

$$\exists v'_M G_M(p_M, v_M) \land S_M(p_M, v_M, v'_M) \land J_M(v'_M, w'_M) \land J_N(w'_N) \quad \text{(expanding } J_{CM} \text{ from (14))}$$

$$\equiv \exists v'_M G_M(p_M, v_M) \land S_M(p_M, v_M, v'_M) \land J_M(v'_M, w'_M) \land J_N(w'_N) \quad \text{(free } v'_N)$$

$$\Leftrightarrow REF_{evt_{M1} \subseteq (evt_{M2})} \land J_N(w'_N) \quad \text{((11) + hypotheses of (15))}$$

$$\Leftrightarrow REF_{evt_{M1} \subseteq (evt_{M2})} \land INV_{evt_{M2} || evt_{N2}} \quad \text{(7)}$$

New events can be added during refinement. They must respect the refinement POs. The refinement PO proof for new events is similar to the previous cases but applied to a single event refined by composed event. Due to the lack of space we do not present it here.

5 Related Work, Conclusions and Future Work

Composition allows the interaction of sub-components. Back [16], Abadi and Lamport[1] studied the interaction of components through shared variable composition. Jones [21] also proposes a shared variable composition for VDM by restricting the behaviour of the environment and the operation itself in order to consider the composition valid using rely-guarantee conditions. In Z, composition can be achieved by combining schemas [20] where variables within the same scope cannot have identical names or by views [12] allowing
the development of partial specifications that can interact through invariants that relate their state or by operations’ synchronisation. Although systems are developed in single machines in classical B, Bellergarde et al [5] suggest a composition by rearranging separated machines and synchronising their operations under feasibility conditions. The behaviour of a component composition is seen as a labelled transition system using weakest preconditions, where a set of authorised transitions are defined. The objective is to verify the refinement of synchronised parallel composition between components but it is limited to finite state transitions and a finite number of components. This work differs from ours as it uses a labelled transition system including a notion of refinement and variable sharing while we use synchronisation and communication in the CSP style. Butler and Walden [8] discuss a combination of action systems and classical B by composing machines using parallel systems in an action system style and preserving the invariants of the individual machines. This approach allows the classical B to derive parallel and distributed systems and since the parallel composition of action system is monotonic, the sub-systems in a parallel composition may be refined independently. This work is closely related to our work with similar underlying semantics and notion of refinement based on CSP. Abrial et al [4] propose a state-based decomposition for Event-B introducing the notion of shared variables and external events. Although it allows variable sharing, this approach is also monotonic but its respective nature is more suitable for parallel programs [10].

Our Event-B composition is based on the close relation between action systems and Event-B plus the correspondence between action systems and CSP [9]. Shared event composition is proved to be monotonic by means of POs. Refinement in a “top-down” style for developing specifications is allowed. Sub-components interact through event parameters by value-passing and can be further refined. We extend Event-B to support shared event composition, allowing combination and reuse of existing sub-components through the introduction of composed machines. Such an approach seems suitable for modelling (distributed) systems. This work is the result of the exploration of specifications’ composition. A methodology for the composition is defined including the verification of properties through the generation of POs. We do not address the step corresponding to the translation of this composition to an implementation. This study needs to be carried out in the future. A tool has been developed to support composition in the Rodin platform [18]. Some case studies have been applying composition with success in particular for distributed systems and as part of decomposition [19].

References


