Quasi-Lexicographic Convergence

Stefan Hallerstede

Department of Engineering
Aarhus University
Denmark
sha@eng.au.dk

Abstract. Anticipation proof obligations for stated variants need to be proved in Event-B even if the variant has no variables in common with anticipated event. This often leads to models that are complicated by additional auxiliary variables and variants that need to take into account these variables. Because of such "encodings" of control flow information in the variants the corresponding proof obligations can usually not be discharged automatically.

We present a new proof obligation for anticipated events that does not have this defect and prove it correct. The proof is fairly intricate due to the nondeterminism of the simulations that link refinements. An informal soundness argument suggests using a lexicographic product in the soundness proof. However, it turns out that a weaker order is required which we call quasi-lexicographic product.

1 Introduction

Event-B provides some flexibility in termination proofs by means of the concept of anticipated events [3]. Anticipated events make it easier to formulate variants for complex models. Ample examples of their use can be found in [1].

The motivation for the work presented in this paper is best illustrated by way of an example. Consider the two fragments of some Event-B machine shown in Fig. 1. To simplify the presentation we have already included an abstract program counter P in the model. Assume

$$P = 3 \Rightarrow w \in 0\,..\,4$$

is an invariant of the machine. Concerning the right-hand side only we can prove convergence of event **three** using the variant $4 - w$. The Rodin tool [2] will do this automatically. However, if we also take the left-hand side into account we have to prove anticipation of event **one**

$$(P = 3 \Rightarrow w \in 0\,..\,4) \land P = 1 \land y < 2 \;\Rightarrow\; 4 - w \in \mathbb{N} \land 4 - w \leq 4 - w \ . \quad (1)$$

Now, we would fail to prove the first part $4 - w \in \mathbb{N}$ of the conclusion. A possible work-around would be to make the variant "global" using the set

$$(\{P\} \cap \{3\}) \times (0\,..\,4 - w) \ .$$

Y. Ait Ameur and K.-D. Schewe (Eds.): ABZ 2014, LNCS 8477, pp. 86–100, 2014.

```
anticipated event one
when
  $P = 1 \wedge y < 2$
then
  $y := y + 1$
end
event two
when
  $P = 1 \wedge y = 2$
then
  $x := y$
end
```

```
convergent event three
when
  $P = 3 \wedge w < 4$
then
  $w := w + 1$
end
event four
when
  $P = 3 \wedge w = 4$
then
  $v := w$
end
```

Fig. 1. Two non-interfering components

This solution is not satisfactory because it complicates the variant and the proof obligations. The proof involves set theory, finite sets and arithmetic and is not done automatically by Rodin tool. We consider tweaking the prover to deal with such instances a bad choice because it would not solve the problem in general and fail occasionally. As our first contribution we show instead that we can drop proof obligations such as (1) for anticipated events entirely. The second contribution concerns the nature of the invariant arising from the use of anticipated events. The soundness proof for the proof obligations requires a generalised form of lexicographic order. This is due to the nondeterminism inherent in the gluing invariant that relates abstract variables to concrete variables. Only special cases such as functional gluing invariants yield lexicographic products. The general case, however, does not.

The informal soundness argument in [3] depends on the abstract variables mentioned in a variant being kept in refinements. Hence, for those variables the refinements are functional; and the claim that termination can be demonstrated by means of a lexicographic product is correct under the given constraint. The only other (semi-) formal soundness proof we are aware of is presented in [8]. However, the proof glosses over a vital fact assuming an equality of abstract sets when only set inclusion is known (see Rem. 7). This way it also achieves to prove that anticipation yields a lexicographic variant.

Overview. We remind the reader of the important properties of well-founded relations in Section 2 and give a short introduction to the used concepts of Event-B in Section 3. The presentation of Event-B is purely set-theoretical and does not discuss Event-B syntax that is used in some examples. Syntax and set-theoretical semantics should be easy to relate though. Details can be found in [1,7]. Section 4 discusses a generalised form of anticipation and convergence based on the concept of quasi-stability. The idea behind quasi-stable relations is to replace the identity relation used in lexicographic products by a more general relation that must not "increase" the first component of the product. Section 5 presents the concept of quasi-lexicographic product that uses such a relation instead of the identity used in the soundness proof of Section 6 In Section 7 we suggest an improvement for the Rodin tool. Section 8 contains the conclusion.

2 Well-Founded Relations

We repeat the main facts about well-founded relations. Most interesting for us is their relationship to transitive closures.

Definition 1. *A predecessor relation m is called* well-founded *if all non-empty subsets z have minima with respect to m,*

$$\forall z \cdot z \neq \varnothing \Rightarrow \exists x \cdot x \in z \land \forall y \cdot y \in z \Rightarrow x \mapsto y \notin m \ . \tag{2}$$

Well-foundedness of m is denoted by $\boldsymbol{wf}\langle m\rangle$.

This is expressed more succinctly using set-theoretic notation (e.g. [1]),

$$\forall z \cdot z \subseteq m^{-1}[z] \Rightarrow z = \varnothing \ . \tag{3}$$

Whereas property (2) is easier to understand, the equivalent set-theoretic statement (3) is easier to apply in proofs.

Later we need well-founded relations that are also transitive. The easiest way to ensure transitivity is to use the transitive closure m^+ of a relation m.

Definition 2. *The* transitive closure m^+ *of a relation m is the smallest relation x satisfying the property $m \cup (m\,;x) \subseteq x$.*

Clearly, the transitive closure of a relation is a transitive relation.

Lemma 1. $m^+ \,; m^+ \subseteq m^+$

The proof obligations for anticipation and convergence only require the employed order m to be well-founded. Fortunately, transitive closures of well-founded relations are well-founded. This fact is well-known, e.g. [6].

Lemma 2. $\boldsymbol{wf}\langle m\rangle \ \Leftrightarrow \ \boldsymbol{wf}\langle m^+\rangle$.

Well-foundedness of relations of the shape $c \lhd m$ only concerns subsets of c. This property is sometimes useful in proofs.

Lemma 3. $\boldsymbol{wf}\langle c \lhd m\rangle \ \Leftrightarrow \ \forall z \cdot z \subseteq c \land z \subseteq m^{-1}[z] \Rightarrow z = \varnothing$.

Remark 1. Well-foundedness of $c \lhd m$ implies $c \lhd m$ is irreflexive. If $c \lhd m$ is well-founded and transitive, then $c \lhd m$ is a strict partial order. It is common to require stronger properties of $c \lhd m$ or m like strict partial orders for the loop proof rule in [4]. We aim to keep the number of proof obligations for candidates for m low, hence, we only require well-foundedness of $c \lhd m$, following the approach of [5].

3 Models, Consistency and Refinement

Event-B models are composed of *machines* that are related by *refinement*. A machine consists of a collection of *events* that describe the behaviour of the machine. An event is a relation of the shape $e = g \lhd s$ where g is a set called the *guard* of the event and s a relation called the *action* of the event. A dedicated event with the guard $g = {\sim}\varnothing$ is used for the initialisation of a machine.[1]

A machine has an *invariant* i. The invariant is a set that describes properties of the machine that are preserved by its events. This property is called *consistency* of the event, formally, $\boldsymbol{cns}\langle i, e\rangle$.

Definition 3. $\boldsymbol{cns}\langle i, e\rangle \;\Leftrightarrow\; e[i] \subseteq i.$

For event $e = g \lhd s$ we usually also require *feasibility*, that is, $i \cap g \subseteq \mathrm{dom}(s)$, or equivalently, $i \cap g \subseteq \mathrm{dom}(e)$. But we do not make use of it in this article.

A machine N *refines* another machine M if M can simulate the behaviour of N. In this relationship we call N the *concrete* machine and M the *abstract* machine. Machine N is related to machine M by means of a *gluing invariant*. The gluing invariant is a relation j that describes the simulation. Machine N refines M if each event e of M is refined by an event f of N, formally, $\boldsymbol{ref}\langle i, j, e, f\rangle$.

Definition 4. $\boldsymbol{ref}\langle i, j, e, f\rangle \;\Leftrightarrow\; (i \lhd j)\,;f \subseteq e\,;j.$

The concrete machine N may also introduce new events that are required to refine *skip*, the event that describes stuttering of M. The event *skip* is the identity relation id. Formally, the introduction of a new event corresponds to $\boldsymbol{ref}\langle i, j, \mathrm{id}, f\rangle$. Note that the invariant of the concrete machine N is $j[i]$.

Lemma 4. $\boldsymbol{cns}\langle i, e\rangle \;\wedge\; \boldsymbol{ref}\langle i, j, e, f\rangle \;\Rightarrow\; \boldsymbol{cns}\langle j[i], f\rangle.$

The relation $i \lhd j$ may also serve as the gluing invariant as implied by the following lemma.

Lemma 5. $\boldsymbol{cns}\langle i, e\rangle \;\wedge\; \boldsymbol{ref}\langle i, j, e, f\rangle \;\Rightarrow\; (i \lhd j)\,;f \subseteq e\,;(i \lhd j).$

Remark 2. Our presentation of the set-theoretical model of Event-B follows [1] by and large. In [1, Chapter 14] Abrial uses the relation $\rho = (i \lhd j)^{-1}$ in place of i and j as we do in Def. 4. Nonetheless, the formalisations are equivalent as indicated by Lemma 5 and inverting the relation ρ.

A tuple $\langle v, c, m\rangle$ where v is a partial function and $c \lhd m$ is a well-founded relation is called a *variant* and v is called the *variant function*. If we say informally "the variant has changed" refer to differing values of v in consecutive states. Let $\langle v, c, m\rangle$ be a variant. We say that event e is *anticipated* if $\boldsymbol{ant}\langle i, e, v, c, m\rangle$.

Definition 5. $\boldsymbol{ant}\langle i, e, v, c, m\rangle \;\Leftrightarrow\; i \lhd e \subseteq v\,;(\mathrm{id} \cup c \lhd m)\,;v^{-1}.$

We say that e is *convergent* if $\boldsymbol{cvg}\langle i, e, v, c, m\rangle$.

Definition 6. $\boldsymbol{cvg}\langle i, e, v, c, m\rangle \;\Leftrightarrow\; i \lhd e \subseteq v\,;c \lhd m\,;v^{-1}.$

[1] The set complement ${\sim}s$ is defined by $x \in {\sim}s \;\Leftrightarrow\; x \notin s$.

Remark 3. The original Event-B proof obligation for anticipated events is

$$i \lhd e \subseteq v \,;\, c \lhd (\mathrm{id} \cup m) \,;\, v^{-1} \ .$$

The new formulation of the proof obligation does not require the proof of membership in c if the e leaves the variant unchanged. In principle one could further generalise the proof obligation to

$$i \lhd e \subseteq v \,;\, \mathrm{id} \cup m \,;\, v^{-1}$$

but this would be traded against stronger constraints on m. Our intention is to make finding candidates for m as easy as possible, for instance, allowing a cyclic graph restricted to an acyclic tree. Constraining m would often necessitate the introduction of an auxiliary variable (e.g., for recording the acyclic tree directly). Using the new proof obligation of Def. 5 we have two ways to influence how m is used in case the anticipated event is interfering with the convergent event. One is the choice of the set c for determining a subset of m. The other is the function v. If we map all states that do not need to be considered for the convergence proof to the same element z outside c, then to prove $v(x) \mapsto v(y) \in \mathrm{id}$ we can use $v(x) = z$ and $v(y) = z$ in such cases. However, we would still need to verify $v(x) = z$ and $v(y) = z$.

The challenge of proving soundness of the anticipation and convergence proof obligations is clearly related to dealing with the gluing invariant. Fig. 2 shows an abstract and a concrete machine of a refinement. The variant for proving convergence of the abstract event **absc** is v, the only variable of the machine. In terms of our set-theoretical model the variant function is id. The set-theoretic gluing invariant is $\{v \mapsto w \mid w \subseteq \{x \mid x < v\} \land (v \in \mathbb{N}_1 \Rightarrow 0 \in w)\}$ establishing a many-to-many relationship between the abstract variable v and the concrete variable w. How to use variable w to express the variant in the concrete machine is not at all obvious. But it is necessary, in order to "forget" about the abstract machine and continue working solely with the concrete machine.

```
invariant $v \in \mathbb{Z}$

variant $v$

anticipated event absa
begin
  skip
end
convergent event absc
any $x$ when
  $v \in \mathbb{N}_1 \land x \in \mathbb{N}_1$
then
  $v := v - x$
end
```

```
invariant $w \subseteq \{x \mid x < v\} \land (v \in \mathbb{N}_1 \Rightarrow 0 \in w)$

anticipated event conca
any $x$ when
  $w \neq \varnothing \land x < \max(w)$
then
  $w := w \cup \{x\}$
end
convergent event concc
when
  $w \cap \mathbb{N} \neq \varnothing$
then
  $w := w \setminus \{\max(w)\}$
end
```

Fig. 2. A nondeterministic refinement with a simple variant

4 Convergence and Anticipation

The proof obligations ***ant*** and ***cvg*** stated in Section 3 are not suitable for the induction-based soundness proof of Section 6. We need a more general formulation based on the concept of quasi-stability.

Definition 7. *A relation r is called m-*quasi-stable*, $\boldsymbol{qs}\langle r, m\rangle$, if it is reflexive, transitive and for all predecessors y of x in r, all predecessors of y in m are also predecessors of x in m, that is, the following three conditions are satisfied*

$$\mathrm{id} \subseteq r \quad , \tag{4}$$

$$r\,;r \subseteq r \ , \tag{5}$$

$$\forall x, y \cdot x \mapsto y \in r \Rightarrow m[\{y\}] \subseteq m[\{x\}] \ . \tag{6}$$

Property (6) can be expressed more concisely using set-theoretic notation

$$(6) \ \Leftrightarrow \ \forall p \cdot (r\,; m)[p] \subseteq m[p] \ .$$

Whereas the set-theoretic formulation of well-foundedness is favourable for use in proof, this does not hold for (6). Instantiating x and y is usually straightforward. Dealing with the set p above easily leads astray when instantiated during a proof. Set-theoretic formulations are not invariably “better”.

An m-quasi-stable relation r is also $c \lhd m$-quasi-stable if the set c is invariant under the inverse of r.

Lemma 6. $\boldsymbol{qs}\langle r, m\rangle \ \wedge \ r^{-1}[c] \subseteq c \ \Rightarrow \ \boldsymbol{qs}\langle r, c \lhd m\rangle$.

Finally, for an m-quasi-stable relation r where m is a transitive relation, the transitive closure of $r \cup m$ is also m-quasi-stable.

Lemma 7. $\boldsymbol{qs}\langle r, m\rangle \ \wedge \ m\,; m \subseteq m \ \Rightarrow \ \boldsymbol{qs}\langle (r \cup m)^{+}, m\rangle$.

This is all we need to know about quasi-stable relations for now. We are ready to introduce quasi-variants.

Definition 8. *Let i be a set. A tuple $\langle v, r, m\rangle$ is called an i-*quasi-variant *iff v is a partial function with $i \subseteq \mathrm{dom}(v)$, m well-founded and r is m-quasi-stable. The i-quasi-variant $\langle v, r, m\rangle$ is called* transitive *if $m\,; m \subseteq m$.*

Using Def. 8 we define generalisations ***ANT*** and ***CVG*** of ***ant*** and ***cvg***. Let $V = \langle v, r, m\rangle$ be an i-quasi-variant in the following two definitions.

Definition 9. $\boldsymbol{ANT}\langle i, e, V\rangle \ \Leftrightarrow \ i \lhd e \subseteq v\,; (r \cup m)\,; v^{-1}$.

The generalisation only concerns the replacement of id in ***ant*** by an m-quasi-stable relation r in ***ANT***. The corresponding convergence proof obligation ***CVG*** has the same shape like ***cvg*** but uses a quasi-variant.

Definition 10. $\boldsymbol{CVG}\langle i, e, V\rangle \ \Leftrightarrow \ i \lhd e \subseteq v\,; m\,; v^{-1}$.

Remark 4. We have the obvious equivalences

$$\begin{aligned}&\boldsymbol{ANT}\langle i, e, \langle v, \mathrm{id}, c \lhd m\rangle\rangle \;\Leftrightarrow\; \boldsymbol{ant}\langle i, e, v, c, m\rangle \quad \text{and}\\ &\boldsymbol{CVG}\langle i, e, \langle v, \mathrm{id}, c \lhd m\rangle\rangle \;\Leftrightarrow\; \boldsymbol{cvg}\langle i, e, v, c, m\rangle \;.\end{aligned}$$

A consequence of this is that the proof obligations $\boldsymbol{ant}$ and $\boldsymbol{cvg}$ can serve as base cases in an inductive soundness proof using $\boldsymbol{ANT}$ and $\boldsymbol{CVG}$.

The transitive closure of a relation preserves quasi-stability. Combined with Lemma 7 this property permits to turn an m-quasi-stable relation r into an m^+-quasi-stable relation $(r \cup m)^+$ that matches the shape of the relation $r \cup m$ in Def. 9 and is transitive.

Lemma 8. $\boldsymbol{qs}\langle r, m\rangle \;\Rightarrow\; \boldsymbol{qs}\langle r, m^+\rangle$.

Remark 5. Any i-quasi-variant $V = \langle v, r, m\rangle$ has an associated transitive i-quasi-variant $W = \langle v, r, m^+\rangle$ by Lemmas 2 and 8. Furthermore, $\boldsymbol{ANT}\langle i, e, V\rangle$ implies $\boldsymbol{ANT}\langle i, e, W\rangle$, and $\boldsymbol{CVG}\langle i, e, V\rangle$ implies $\boldsymbol{CVG}\langle i, e, W\rangle$. Thus, using the equivalences of Rem. 4 we can use arbitrary quasi-variants on well-founded sets in specifications but assume that we have transitive quasi-variants available whenever needed.

5 Quasi-Lexicographic Products and Power Orders

The combination of refinement and anticipation produces quasi-lexicographic products on power orders. This complication is caused by the nondeterministic relationship between abstract and concrete states induced by the gluing invariant.

Definition 11. *The r-quasi-lexicographic product of two relations m and n, denoted $m \circledast_r n$, is defined as $(m \parallel {\sim}\varnothing) \cup (r \parallel n)$.*[2]

The relation $m \circledast_{\mathrm{id}} n$ is the lexicographic product of m and n. The identity keeps the first component "stable" while the second component changes. It breaks the symmetry of a plain union of m and n and as a result preserves well-foundedness. If we replace the identity by an m-quasi-stable relation we achieve the same.

If we unfold the set-theoretical definition of the r-quasi-lexicographic product, we obtain the more familiar formulation

$$m \circledast_r n = \{(p \mapsto x) \mapsto (q \mapsto y) \mid p \mapsto q \notin m \Rightarrow p \mapsto q \in r \land x \mapsto y \in n\} \;. \quad (7)$$

The following lemma provides the main insight of this section. The r-quasi-lexicographic product with an m-quasi-stable relation r of well-founded relations m and n is well-founded.

[2] In the Event-B notation the *parallel product* $r \parallel s$ of two relations r and s is defined by $(p \mapsto x) \mapsto (q \mapsto y) \in r \parallel s \;\Leftrightarrow\; p \mapsto q \in r \land x \mapsto y \in s$.

Lemma 9. $\boldsymbol{wf}\langle m\rangle \ \wedge\ \boldsymbol{qs}\langle r, m\rangle \ \wedge\ \boldsymbol{wf}\langle n\rangle \ \Rightarrow\ \boldsymbol{wf}\langle m \circledast_r n\rangle$.

The power order of a relation m is a relation over the subsets of its domain and range.

Definition 12. *The* power order *of a relation m, denoted by $\mathbb{O}\, m$, is defined as $\{p \mapsto q \mid p \subseteq m^{-1}[q] \wedge (p = \varnothing \Rightarrow q = \varnothing)\}$.*

Using the power order we could state well-foundedness (3) of a relation m in the form $\forall z \cdot z \mapsto z \in \mathbb{O}\, m \Rightarrow z = \varnothing$. Unfolding the set-theoretical notation the power order $\mathbb{O}\, m$ of a relation m has the following shape

$$\{p \mapsto q \mid (\forall x \cdot x \in p \Rightarrow \exists y \cdot y \in q \wedge x \mapsto y \in m) \wedge (p = \varnothing \Rightarrow q = \varnothing)\} \ . \qquad (8)$$

Power orders preserve many important properties of a relation such as transitivity, quasi-stability and well-foundedness on non-empty sets. This permits us to lift known well-founded orders to well-founded power orders.

Lemma 10. $r\,;r \subseteq r \ \Rightarrow\ (\mathbb{O}\, r)\,;(\mathbb{O}\, r) \subseteq \mathbb{O}\, r$.

If a relation r is m-quasi-stable, then $\mathbb{O}\, r$ is $\mathbb{O}\, m$-quasi-stable.

Lemma 11. $\boldsymbol{qs}\langle r, m\rangle \ \Rightarrow\ \boldsymbol{qs}\langle \mathbb{O}\, r, \mathbb{O}\, m\rangle$.

The empty set occurs in a power order only as the pair $\varnothing \mapsto \varnothing$. Hence, removing the empty set from the range of a power order also removes it from its domain. The following lemma is to be used with Lemma 6 and Lemma 13 below. It permits to remove the empty set from a power order while preserving quasi-stability.

Lemma 12. $(\mathbb{O}\, m)^{-1}[\sim\{\varnothing\}] \ \subseteq\ \sim\{\varnothing\}$.

Well-foundedness is only preserved when the empty set is excluded from the power order. In fact, the empty set is introduced for purely technical reasons in the definition of the power order. Removing it would complicate the definition of quasi-stability, in particular. In the soundness proof below the empty set is easily excluded to occur in all cases where well-foundedness of power orders is required.

Lemma 13. $\boldsymbol{wf}\langle m\rangle \ \Rightarrow\ \boldsymbol{wf}\langle \{\varnothing\} \lhd \mathbb{O}\, m\rangle$.

The following lemma permits to construct a quasi-stable quasi-lexicographic product from quasi-stable components. This construction facilitates the introduction of quasi-lexicographic products in refinements where the pair $\langle r, m\rangle$ is part of a quasi-variant of the abstract model and $\langle s, n\rangle$ is part of a quasi-variant of the concrete model.

Lemma 14. $\boldsymbol{qs}\langle r, m\rangle \ \wedge\ \boldsymbol{qs}\langle s, n\rangle \ \Rightarrow\ \boldsymbol{qs}\langle r \parallel s, m \circledast_r n\rangle$.

6 Soundness

Theorem 1 states the main condition for the termination proof in Event-B to be sound. It says that anticipation and convergence are preserved by refinement, and anticipation may be strengthened to convergence; and the variant function can be expressed in terms of concrete variables only.

Theorem 1. *For sets i, relation j, transitive i-quasi-variant V and $j[i]$-quasi-variant W there is a transitive $j[i]$-quasi-variant U such that*
(N) *for all relations f: if $\boldsymbol{ref}\langle i, j, \mathrm{id}, f\rangle$, then*
  (1) $\boldsymbol{ANT}\langle j[i], f, W\rangle$ *implies* $\boldsymbol{ANT}\langle j[i], f, U\rangle$,
  (2) $\boldsymbol{CVG}\langle j[i], f, W\rangle$ *implies* $\boldsymbol{CVG}\langle j[i], f, U\rangle$,
(R) *for all relations e, f: if $\boldsymbol{cns}\langle i, e\rangle$ and $\boldsymbol{ref}\langle i, j, e, f\rangle$, then*
  (1) $\boldsymbol{CVG}\langle i, e, V\rangle$ *implies* $\boldsymbol{CVG}\langle j[i], f, U\rangle$,
  (2) $\boldsymbol{ANT}\langle i, e, V\rangle$ *and* $\boldsymbol{ANT}\langle j[i], f, W\rangle$ *imply* $\boldsymbol{ANT}\langle j[i], f, U\rangle$,
  (3) $\boldsymbol{ANT}\langle i, e, V\rangle$ *and* $\boldsymbol{CVG}\langle j[i], f, W\rangle$ *imply* $\boldsymbol{CVG}\langle j[i], f, U\rangle$.

Proof. Let $V = \langle v, r, m\rangle$ and $W = \langle w, s, n\rangle$. In a refinement the abstract quasi-variant function v is only accessible by means of the gluing invariant $i \lhd j$; we define $\phi = v^{-1} \,;\, (i \lhd j)$. Let $U = \langle u, t, o\rangle$ be given by

$$\begin{aligned} u &= (\lambda x \cdot \top \mid \phi^{-1}[\{x\}] \mapsto w[\{x\}]) \\ t &= \mathbb{O}\,(r \cup m)^{+} \parallel \mathbb{O}\,s \\ o &= ((\{\varnothing\} \mathbin{⩤} \mathbb{O}\,m) \circledast_{\mathbb{O}\,(r \cup m)^{+}} (\{\varnothing\} \mathbin{⩤} \mathbb{O}\,n))^{+} \ . \end{aligned}$$

It is easy to verify that $j[i] \subseteq \mathrm{dom}(u)$. Furthermore, relation o is well-founded because

$$\begin{aligned} & \top \\ \Rightarrow \quad & \langle\ V \text{ is an } i\text{-quasi-variant}\ \rangle \\ & \boldsymbol{qs}\langle r, m\rangle \\ \Rightarrow \quad & \langle\ V \text{ is transitive and Lemma 7}\ \rangle \\ & \boldsymbol{qs}\langle (r \cup m)^{+}, m\rangle \\ \Rightarrow \quad & \langle\ \text{Lemma 11}\ \rangle \\ & \boldsymbol{qs}\langle \mathbb{O}\,(r \cup m)^{+}, \mathbb{O}\,m\rangle \\ \Rightarrow \quad & \langle\ \text{Lemma 12 and Lemma 6}\ \rangle \\ & \boldsymbol{qs}\langle \mathbb{O}\,(r \cup m)^{+}, \{\varnothing\} \mathbin{⩤} \mathbb{O}\,m\rangle \qquad (9) \\ \Rightarrow \quad & \langle\ \boldsymbol{wf}\langle m\rangle \text{ because } V \text{ is an } i\text{-quasi-variant, and Lemma 13}\ \rangle \\ & \boldsymbol{qs}\langle \mathbb{O}\,(r \cup m)^{+}, \{\varnothing\} \mathbin{⩤} \mathbb{O}\,m\rangle \wedge \boldsymbol{wf}\langle \{\varnothing\} \mathbin{⩤} \mathbb{O}\,m\rangle \\ \Rightarrow \quad & \langle\ \boldsymbol{wf}\langle n\rangle \text{ because } W \text{ is a } j[i]\text{-quasi-variant, and Lemma 13}\ \rangle \\ & \boldsymbol{qs}\langle \mathbb{O}\,(r \cup m)^{+}, \{\varnothing\} \mathbin{⩤} \mathbb{O}\,m\rangle \wedge \boldsymbol{wf}\langle \{\varnothing\} \mathbin{⩤} \mathbb{O}\,m\rangle \wedge \boldsymbol{wf}\langle \{\varnothing\} \mathbin{⩤} \mathbb{O}\,n\rangle \\ \Rightarrow \quad & \langle\ \text{Lemma 9}\ \rangle \end{aligned}$$

$\boldsymbol{wf}\langle(\{\varnothing\} ⩤ \mathbb{O}\,m) \circledast_{\mathbb{O}\,(r\cup m)^+} (\{\varnothing\} ⩤ \mathbb{O}\,n)\rangle$

$\Rightarrow$ ⟨ Lemma 2 ⟩

$\boldsymbol{wf}\langle o\rangle$. (10)

And, U is a transitive $j[i]$-quasi-variant because

$\top$

$\Rightarrow$ ⟨ $\boldsymbol{qs}\langle s, n\rangle$ because W is a $j[i]$-quasi-variant, and Lemma 11 ⟩

$\boldsymbol{qs}\langle \mathbb{O}\,s, \mathbb{O}\,n\rangle$

$\Rightarrow$ ⟨ Lemma 12 and Lemma 6 ⟩

$\boldsymbol{qs}\langle \mathbb{O}\,s, \{\varnothing\} ⩤ \mathbb{O}\,n\rangle$

$\Rightarrow$ ⟨ (9), Lemma 14, Lemma 8, def. of t and o ⟩

$\boldsymbol{qs}\langle t, o\rangle$

$\Rightarrow$ ⟨ (10) and Lemma 1, and $j[i] \subseteq \mathrm{dom}(u)$ ⟩

U is a transitive $j[i]$-quasi-variant .

Moreover, the $j[i]$-quasi-variant U satisfies the two conditions (N) and (R). Now, claims (N1) and (N2) are consequences of claims (R2) and (R3) with $e = \mathrm{id}$ because $\boldsymbol{cns}\langle i, \mathrm{id}\rangle$ and $\boldsymbol{ANT}\langle i, \mathrm{id}, V\rangle$, the latter being a consequence of $\mathrm{id} \subseteq r$. Thus, it only remains to be shown that U satisfies (R).

We begin with the proof of (R1). We have

$$
\begin{array}{lll}
 & (i \lhd j) \,;\, f & \langle\ \boldsymbol{cns}\langle i, e\rangle,\ \boldsymbol{ref}\langle i, j, e, f\rangle \text{ and Lemma 5 } \rangle \\
\subseteq & (i \lhd e) \,;\, (i \lhd j) & \langle\ \boldsymbol{CVG}\langle i, e, V\rangle\ \rangle \\
\subseteq & v \,;\, m \,;\, v^{-1} \,;\, (i \lhd j) & \langle \text{ def. of } \phi\ \rangle \\
\subseteq & v \,;\, m \,;\, \phi\ ,
\end{array}
$$

hence,

$$(i \lhd j) \,;\, f \ \subseteq\ v \,;\, m \,;\, \phi\ . \tag{11}$$

Using this,

$x \mapsto y \in j[i] \lhd f$

$\Rightarrow$ ⟨ Lemma 15 below with “$k := m$” ⟩

$\phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \mathbb{O}\,m$

$\Rightarrow$ ⟨ $\mathrm{dom}((i \lhd j) \,;\, f) \subseteq \mathrm{dom}(v)$ by (11) ⟩

$\phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \mathbb{O}\,m \wedge \phi^{-1}[\{x\}] \neq \varnothing$

$\Rightarrow$ ⟨ def. of ⩤ ⟩

$\phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \{\varnothing\} ⩤ \mathbb{O}\,m$

$\Rightarrow$ ⟨ def. of o ⟩

$$
\begin{array}{ll}
 & (\phi^{-1}[\{x\}] \mapsto w[\{x\}]) \mapsto (\phi^{-1}[\{y\}] \mapsto w[\{y\}]) \in o \\
\Leftrightarrow & \quad \langle \text{ def. of } u \ \rangle \\
 & x \mapsto y \in u \mathbin{;} o \mathbin{;} u^{-1} \ .
\end{array}
$$

Hence, (R1) holds. Claims (R2) and (R3) both assume $\boldsymbol{ANT}\langle i, e, V\rangle$. Thus, similarly to (11) we have

$$(i \lhd j) \mathbin{;} f \ \subseteq \ v \mathbin{;} (r \cup m) \mathbin{;} \phi \ . \tag{12}$$

Now,

$$
\begin{array}{ll}
 & x \mapsto y \in j[i] \lhd f \\
\Rightarrow & \quad \langle \text{ (12) and Lemma 15 below with ``}k := r \cup m\text{'' } \rangle \\
 & \phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \mathbb{O}(r \cup m) \\
\Rightarrow & \quad \langle \ r \cup m \subseteq (r \cup m)^{+} \text{ by def. of } ^{+} \ \rangle \\
 & \phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \mathbb{O}\,(r \cup m)^{+} \ . \qquad\qquad (13)
\end{array}
$$

As specified in (R2) and (R3) two cases can be distinguished according to $\boldsymbol{ANT}\langle j[i], f, W\rangle$ and $\boldsymbol{CVG}\langle j[i], f, W\rangle$. The former implies

$$x \mapsto y \in j[i] \lhd f \ \Rightarrow \ w(x) \mapsto w(y) \in s \vee w(x) \mapsto w(y) \in n \ . \tag{14}$$

and the latter

$$x \mapsto y \in j[i] \lhd f \ \Rightarrow \ w(x) \mapsto w(y) \in n \ . \tag{15}$$

Thus, (R3) follows because

$$
\begin{array}{ll}
 & (13) \\
\Rightarrow & \quad \langle \ x \mapsto y \in j[i] \lhd f \text{ and (15) } \rangle \\
 & \phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \mathbb{O}\,(r \cup m)^{+} \wedge w(x) \mapsto w(y) \in n \\
\Rightarrow & \quad \langle \ x \in \mathrm{dom}(w),\ y \in \mathrm{dom}(w) \text{ and } w \text{ is a function } \rangle \\
 & \phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \mathbb{O}\,(r \cup m)^{+} \wedge w[\{x\}] \mapsto w[\{y\}] \in \{\varnothing\} \mathbin{⩤} \mathbb{O}\,n \\
\Rightarrow & \quad \langle \text{ def. of } o \ \rangle \\
 & (\phi^{-1}[\{x\}] \mapsto w[\{x\}]) \mapsto (\phi^{-1}[\{y\}] \mapsto w[\{y\}]) \in o \\
\Leftrightarrow & \quad \langle \text{ def. of } u \ \rangle \\
 & x \mapsto y \in u \mathbin{;} o \mathbin{;} u^{-1} \ .
\end{array}
$$

Concerning (R2) observe that the case "$w(x) \mapsto w(y) \in n$" of (14) is already covered by the proof of (R3). With respect to the other case we have

$$
\begin{array}{ll}
 & (13) \\
\Rightarrow & \langle\ x \mapsto y \in j[i] \lhd f \text{ and } x \mapsto y \in j[i] \lhd f \Rightarrow w(x) \mapsto w(y) \in s\ \rangle \\
 & \phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \mathbb{O}\,(r \cup m)^{+} \wedge w(x) \mapsto w(y) \in s \\
\Rightarrow & \langle\ x \in \mathrm{dom}(w),\ y \in \mathrm{dom}(w) \text{ and } w \text{ is a function}\ \rangle \\
 & \phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \mathbb{O}\,(r \cup m)^{+} \wedge w[\{x\}] \mapsto w[\{y\}] \in \mathbb{O}\,s \\
\Rightarrow & \langle\ \text{def. of } t\ \rangle \\
 & (\phi^{-1}[\{x\}] \mapsto w[\{x\}]) \mapsto (\phi^{-1}[\{y\}] \mapsto w[\{y\}]) \in t \\
\Leftrightarrow & \langle\ \text{def. of } u\ \rangle \\
 & x \mapsto y \in u\,;t\,;u^{-1}\ \ .
\end{array}
$$

Finally, (R2) follows because

$$
\begin{array}{lll}
 & (13) & \langle\ \text{see above}\ \rangle \\
\Rightarrow & x \mapsto y \in u\,;t\,;u^{-1} \vee x \mapsto y \in u\,;o\,;u^{-1} & \langle\ \text{distributivity of } \cup \text{ and } ;\ \rangle \\
\Leftrightarrow & x \mapsto y \in u\,;(t \cup o)\,;u^{-1}\ \ . &
\end{array}
$$

This concludes the proof of Theorem 1. □

The following lemma shows how a concrete convergence or anticipation condition $(i \lhd j)\,;f \subseteq v\,;k\,;\phi$ induces a power ordering of the concrete event f.

Lemma 15. *Let* $\phi = v^{-1}\,;(i \lhd j)$ *and* $i \subseteq \mathrm{dom}(v)$*. Then*

$$
\begin{array}{ll}
 & (i \lhd j)\,;f \subseteq v\,;k\,;\phi \\
\Rightarrow & (\forall x, y \cdot x \mapsto y \in j[i] \lhd f \Rightarrow \phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \mathbb{O}\,k)\ \ .
\end{array}
$$

Proof. Starting from the premise we have

$$
\begin{array}{ll}
 & (i \lhd j)\,;f \subseteq v\,;k\,;\phi \\
\Rightarrow & \langle\ \text{def. of } \phi\text{, set theory}\ \rangle \\
 & \phi\,;f \subseteq v^{-1}\,;v\,;k\,;\phi \\
\Rightarrow & \langle\ v \text{ is a partial function}\ \rangle \\
 & \phi\,;f \subseteq k\,;\phi \\
\Leftrightarrow & \langle\ \text{def. of } \phi\ \rangle \\
 & \phi\,;(j[i] \lhd f) \subseteq k\,;\phi \\
\Leftrightarrow & \langle\ \text{def. of } \cup\text{, def. of } ;\ \rangle \\
 & (\forall p, y \cdot (\exists x \cdot p \mapsto x \in \phi \wedge x \mapsto y \in j[i] \lhd f) \Rightarrow p \mapsto y \in k\,;\phi) \\
\Leftrightarrow & \langle\ \text{predicate logic}\ \rangle \\
 & (\forall x, y \cdot x \mapsto y \in j[i] \lhd f \Rightarrow (\forall p \cdot p \mapsto x \in \phi \Rightarrow p \mapsto y \in k\,;\phi))\ \ . \qquad (16)
\end{array}
$$

Now,

$$
\begin{aligned}
& x \mapsto y \in j[i] \lhd f \\
\Rightarrow \quad & \langle\ (16)\ \rangle \\
& \forall p \cdot p \mapsto x \in \phi \Rightarrow p \mapsto y \in k \,;\, \phi \\
\Rightarrow \quad & \langle\ \text{def. of } ;\text{, set theory}\ \rangle \\
& \forall p \cdot p \in \phi^{-1}[\{x\}] \Rightarrow \exists q \cdot q \in \phi^{-1}[\{y\}] \wedge p \mapsto q \in k \qquad (17) \\
\Rightarrow \quad & \langle\ \text{shape (8) of } \mathbb{O}\text{, and } \phi^{-1}[\{x\}] \neq \varnothing \text{ because } i \subseteq \text{dom}(v)\ \rangle \\
& \phi^{-1}[\{x\}] \mapsto \phi^{-1}[\{y\}] \in \mathbb{O}\, k \ .
\end{aligned}
$$

Thus, Lemma 15 holds. □

Remark 6. In a functional refinement $(i \lhd j)^{-1}$ is a partial function, hence, ϕ^{-1} is a function. Now, because ϕ^{-1} is a function and $x \in \text{dom}(\phi^{-1})$ we have

$$
\begin{aligned}
& (17) \\
\Rightarrow\ & \phi^{-1}(x) \mapsto \phi^{-1}(y) \in k \quad \text{where } k = \text{id or } k = m.
\end{aligned}
$$

For refinements that are not functional we can only assume that ϕ^{-1} is a relation. This leads to the use of power sets and power orders and requires the generalisation to quasi-lexicographical products.

Remark 7. Continuing for relational refinements from (17) with $k = \text{id}$ would yield

$$
\begin{aligned}
& (17) \\
\Rightarrow \quad & \langle\ k = \text{id}\ \rangle \\
& \forall p \cdot p \in \phi^{-1}[\{x\}] \Rightarrow \exists q \cdot q \in \phi^{-1}[\{y\}] \wedge p \mapsto q \in \text{id} \\
\Rightarrow \quad & \langle\ \text{def. of id}\ \rangle \\
& \forall p \cdot p \in \phi^{-1}[\{x\}] \Rightarrow \exists q \cdot q \in \phi^{-1}[\{y\}] \wedge p = q \\
\Rightarrow \quad & \langle\ \text{one-point rule}\ \rangle \\
& \forall p \cdot p \in \phi^{-1}[\{x\}] \Rightarrow p \in \phi^{-1}[\{y\}] \\
\Rightarrow \quad & \langle\ \text{def. of } \subseteq\ \rangle \\
& \phi^{-1}[\{x\}] \subseteq \phi^{-1}[\{y\}]
\end{aligned}
$$

This gives an increasing sequence of sets, a candidate for a quasi-stable relation. Repeating the process with $k = \{p \mapsto q \mid p \subseteq q\}$ and proceeding similarly for the well-founded relation m indicates the need for the constructions presented in this article.

7 An Improved Proof Obligation for Anticipated Events

The current proof obligation for anticipated events could be rewritten in the following shape

$$x \mapsto y \in i \lhd e \wedge x \mapsto y \notin v \,;\, c \lhd \text{id} \,;\, v^{-1} \;\Rightarrow\; x \mapsto y \in v \,;\, c \lhd m \,;\, v^{-1}$$

Similarly the new proof obligation could be rewritten to

$$x \mapsto y \in i \lhd e \land x \mapsto y \notin v \mathbin{;} \mathrm{id} \mathbin{;} v^{-1} \;\Rightarrow\; x \mapsto y \in v \mathbin{;} c \lhd m \mathbin{;} v^{-1}$$

and further

$$x \mapsto y \in i \lhd e \land v(x) \neq v(y) \;\Rightarrow\; v(x) \in c \land v(x) \mapsto v(y) \in m \enspace .$$

And this proof obligation would only need to be generated when $x \neq y$. Following this approach no proof obligation would be generated in the situation described in the introductory example in place of (1).

8 Conclusion

The presented improvement of the anticipation proof obligation should be easy to incorporate into the Rodin tool. Fewer proof obligations need to be generated. The new proof obligation helps to keep models simple: by using the fact that some event is non-interfering on some set of variables we permit variants to be specified “locally” without referring to abstract program counters or similar constructs. This could also be useful for composing models where non-interference is common. (With the current proof rule we would have to change some variant expressions in order for termination claims to remain valid.)

We have also developed the concept of quasi-lexicographic product that is necessary for the soundness proof of anticipation and refinement. All lemmas mentioned in the paper have been proved with the Rodin tool. We are not sure whether a formalisation of Theorem 1 would be possible with reasonable effort in the tool. After all, it was never intended for deeper mathematical work.

Acknowledgement. I am grateful to the anonymous reviewers for their thorough work and constructive suggestions. I am particularly indebted to reviewer 2 who pointed out an error in the original proof of Theorem 1.

References

1. Abrial, J.-R.: Modeling in Event-B: System and Software Engineering. Cambridge University Press (2010)
2. Abrial, J.-R., Butler, M.J., Hallerstede, S., Hoang, T.S., Mehta, F., Voisin, L.: Rodin: an open toolset for modelling and reasoning in event-B. STTT 12(6), 447–466 (2010)
3. Abrial, J.-R., Cansell, D., Méry, D.: Refinement and Reachability in Event_B. In: Treharne, H., King, S., C. Henson, M., Schneider, S. (eds.) ZB 2005. LNCS, vol. 3455, pp. 222–241. Springer, Heidelberg (2005)
4. Apt, K.R., de Boer, F.S., Olderog, E.-R.: Verification of Sequential and Concurrent Programs. Texts in Computer Science. Springer (2009)

5. Dijkstra, E.W., Scholten, C.S.: Predicate Calculus and Program Semantics. Springer, NY (1990)
6. Dijkstra, E.W., van Gasteren, A.J.M.: Well-foundedness and the transitive closure, AvG88/EWD1079 (1990)
7. Hallerstede, S.: On the purpose of event-B proof obligations. Formal Asp. Comput. 23(1), 133–150 (2011)
8. Yilmaz, E.: Tool Support for Qualitative Reasoning in Event-B. Master's thesis, Department of Computer Science, ETH Zurich (2010)