Math. Struct. in Comp. Science (2015), *vol.* 25, *pp.* 135–202. © Cambridge University Press 2014
doi:10.1017/S0960129514000061

Retrenchment and refinement interworking: the tower theorems

RICHARD BANACH and CZESŁAW JESKE

School of Computer Science, University of Manchester,
Oxford Road, Manchester, M13 9PL, U.K.
Email: banach@cs.man.ac.uk;jeske@xsys.org.uk

Received 31 August 2010; revised 27 March 2013

Retrenchment is a flexible model evolution formalism that compensates for the limitations imposed by specific formulations of refinement. Its refinement-like proof obligations feature additional predicates for accommodating design data describing the model change. The best results are obtained when refinement and retrenchment cooperate, the paradigmatic scheme for this being the commuting square or tower, in which 'horizontal retrenchment rungs' commute with 'vertical refinement columns' to navigate through a much more extensive design space than permitted by refinement alone. In practice, the navigation is accomplished through 'square completion' constructions, and we present and prove a full suite of square completion theorems.

1. Introduction

As a design and development technique, model-based refinement (see, for example, de Roever and Engelhardt (1998) for a survey) has proved its worth on many occasions. Despite the broad reluctance among mainstream developers to embrace as mathematical an approach to development as refinement proposes, a number of well-known industrial-scale developments have demonstrated the enhanced dependability that accrues from using a technique enjoying such a level of rigour. See, for instance: Stepney *et al.* (1998) and Stepney *et al.* (2000) for a public presentation of the Mondex formal development in Z, and Jones and Woodcock (2008) for a more recent reappraisal of it in the context of the Verification Grand Challenge (Jones *et al.* 2006; Woodcock 2006; Woodcock and Banach 2007); and Behm *et al.* (1999) and Behm *et al.* (2000) for the use of the B-Method in the development of MÉTÉOR, and its subsequent further development in projects such as Roissy-VAL (Badeau and Amelot 2005). In niche areas, where the benefits of the aforementioned dependability has been appreciated, these techniques continue to be applied, though it is often the case that little appears in the public domain for reasons of commercial confidentiality[†].

[†] For example, the proceedings of FM 2005 (*Springer-Verlag Lecture Notes in Computer Science* **3582**) contain a collection of short papers documenting the Industry Day, whereas the proceedings of FM 2011 (*Springer-Verlag Lecture Notes in Computer Science* **6664**) do not have any Industry Day papers since in that year the day was confined to oral presentations only.

As a design and development technique, a given, specific, incarnation of model-based refinement can sometimes fall short of what is desired, as regards treating specific requirements issues in the most faithful way possible. Retrenchment was introduced as a means of addressing such awkward requirements issues, with the aim of allowing them to be treated in a formal manner, whilst at the same time not interfering with the benefits of a possibly over-idealised refinement development. Banach *et al.* (2007a) provides a comprehensive and broadly based overview of retrenchment, with an extensive discussion of the background and context, a description of some key issues arising with retrenchment and an exploration of some case studies[†]. Moving on from that starting point, the current paper is concerned with a key technical topic: *viz.* the interworking of retrenchment and refinement.

The issue is that retrenchment, as conventionally presented, is extremely permissive (and deliberately so). Hence, using it as the sole formal technique in a development process can let through a whole host of design deviations that might be considered undesirable, and could derail the development process. This possibility can in turn require considerable self-discipline and intensive investment in validation to ensure that the development stays on track. However, using retrenchment in a controlled way in concert with refinement can considerably alleviate this situation, since a good deal of what would otherwise be validation burden can be delegated to the guarantees that (some particular notion of) model-based refinement offers, especially when backed up by the use of an appropriate tool.

How then can we arrange for such fruitful cooperation between the two notions? The paradigm investigated in the current paper views retrenchment and refinement as orthogonal directions in a development landscape that enjoys a higher 'dimensionality' than one in which refinement is seen as being the only possible means of progress. Thus, we can visualise refinement as proceeding 'downwards' from abstract to concrete (this being the only possible means of progress in a conventional formal development world), and retrenchment as proceeding 'horizontally', bridging between refinement strands that would remain isolated from one another without the use of retrenchment. This architecture is given solidity by demanding that diverse paths through this two dimensional landscape between the same two system models should be related in a composable and understandable way. And this in turn can be realised if we establish a sufficient store of 'square completion' constructions, each of which fills in a missing piece in an incomplete square of horizontal retrenchments and vertical refinements. One thing that this achieves is to allow us to interchange suitable retrenchment/refinement pairs, and thus, by repeated application, to morph one path between the two system models into a different one. Going further, the automatic construction of systems afforded by such square completion constructions widens the scope for 'system building by theorem' from the pure refinement

[†] See the Retrenchment homepage at `http://www.cs.man.ac.uk/~banach/retrenchment/` for the latest developments.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

paradigm[†] to a wider range of requirements issues that include ones that become formally addressable only by means of retrenchment. This is the aim of the current paper.

1.1. *Organisation of the paper*

In Section 2, we give a broad informal overview of retrenchment and describe some of the case studies and scenarios in which it has been employed. In Section 3, we change from an informal to a technically rigorous orientation, recalling the basics of retrenchment, and give a fairly general purpose formulation of refinement for interworking with it. The refinement notion is one that can be instantiated to capture a range of existing refinement formulations in the literature[‡]. In Section 4, we cover the compositions of retrenchments and refinements that we will need later in the paper.

In Section 5, we outline the main results of the rest of the paper, summarising the theorems and indicating their use in the tower pattern (Banach *et al.* 2005) – this section can be used as convenient overview. The following sections focus on the technical details of each of the specific theorems: Section 6 covers the Lifting Theorem; Section 7 covers the Lowering Theorem; Section 8 covers the Postjoin Theorem; and Section 9 covers the Prejoin Theorem. Since we adhere to a rather categorical paradigm, all of these results are proved up to notions of equivalence: specifically, these amount to inter-simulability, inter-retrenchability and inter-refinability, as appropriate, and as described in detail for each theorem as required. This gives a precise definition of the way that each of the results obtained is characterised beyond the details of the explicit construction given. This, in turn, helps when replacing the explicit construction by something equally useful, but more appealing from a system requirements point of view. Those unconcerned with the technical details can skip over the proofs in Sections 6–9.

In Section 10, we discuss associativity, general tower constructions and system engineering, and give a sketch of how the technical material presented earlier might be applied. Finally, we present our conclusions in Section 11.

1.2. *Background*

The current paper looks again at the results and constructions originally investigated in depth in Jeske (2005). The results in that paper took a particular stance on how the constructions should be approached, and strove to achieve the greatest degree of generality possible from that perspective. While this aim appeared at the outset to be innocuous

[†] This is exemplified at the time of writing by toolsets such as Rodin (for further details, see `http://www.event-b.org/`, `http://www.rodintools.org/` and `http://sourceforge.net/projects/rodin-b-sharp/`) and others, each of which is designed for the formal development of systems using (some specific notion of) refinement.

[‡] In a further paper, Banach (2009), we examine a number of specific real-world refinement formulations in order to infer the most appropriate way to design retrenchment notions, and the insights of the current paper are used to reinforce the conclusions drawn. In turn, the formulation of refinement used here is designed to be capable of realising various specific notions examined in Banach (2009). Thus, although the current paper is technically self-contained, it has benefited from strong conceptual cross-fertilisation between it, Banach (2009) and Banach *et al.* (2007b).

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

enough, it led, in the end, to some ferociously complicated results, and the overwhelming technical convolutedness of those results certainly proved to be an impediment to their widespread application. The aim of the current paper is to revisit the same issues, but employing the wisdom of hindsight, and thereby to give counterparts that are much more approachable and thus more readily applicable. Although a comparison of the present work with Jeske (2005) would show extensive detailed technical differences, the debt the current paper owes to Jeske (2005) for illuminating the consequences of the earlier approach cannot be overstated.

Assumptions 1.1. We work in a set theoretic and relational framework in which relations are manipulated using logical operations on the predicates that define their bodies. To avoid a proliferation of pathological cases, we assume that any set or relation mentioned in the hypotheses of a construction or theorem is non-empty, so that, for example, a mentioned putative choice of some element from the set or relation can actually be made.

Notation 1.2. We write X^T for the transpose of a relation X (that is, $x\,X\,x'$ if and only if $x'\,X^T\,x$). We write $Z \lhd X$ for the domain restriction of a relation X, that is,

$$Z \lhd X \equiv X \cap ((Z \cap \mathrm{dom}(X)) \times rng(X)).$$

2. Retrenchment, an overview

What we now refer to as model-based refinement had its origins in the work of Wirth, Dijkstra and Hoare in papers such as Wirth (1971), Dijkstra (1972) and Hoare (1972). In those days, the message was straightforward enough in that refinement was a process whereby a piece of abstract program could be replaced by a piece of more concrete program without changing the observable behaviour. If, for some set of sufficient conditions, it could be proved that observations were unchanged, those conditions could be adopted as a general purpose working method for establishing refinement.

As with any technique that gets fixed *a priori*, but deals with problems expressible in a ‘general purpose programming-like notation’, as problem instances of increasing size are tackled, complexity eventually rears its head and becomes an issue to contend with. In the case of notions of refinement, there is not only the complexity of problem descriptions in the sense of some formal complexity measure or other, as one would normally understand such a concept, but there is also complexity of a less precisely defined kind that has its roots in various ‘management level’ concerns that have an impact during the development of real-world applications.

Thus, applying some particular flavour of model-based refinement to a real application ‘out of the box’ may become infeasible, not only because the problem instance becomes too big according to some objective formal measure, but also, and at an earlier stage, because modelling at the level needed to take proper account of all the relevant requirements concerns increases the model (and development) complexity to a level unacceptable from a management perspective: for instance, because the resulting model is not clear enough

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

to be understood, or for other reasons emerging from the wider problem context or the real-world system construction context.

Retrenchment, which we will cover in some detail later in the paper (see Banach *et al.* (2007b), Banach *et al.* (2008) and Banach and Jeske (2010), and other work available from the Retrenchment homepage at `http://www.cs.man.ac.uk/~banach/retrenchment/`) was introduced to address the issues mentioned in the previous paragraph. The idea was to introduce a notion that would accommodate departures from the exigencies of formal refinement, yet would be capable of smooth interworking with refinement when circumstances allowed. Informally, if we say that the core idea of model-based refinement is captured in a 'forward simulation' proof obligation of the form

$$G \wedge stp_{Op_C} \Rightarrow (\exists stp_{Op_A} \wedge G') \tag{1}$$

where:

- G is a retrieve, or gluing relation;
- the prime decoration refers to after states; and
- stp_{Op_C} and stp_{Op_A} are concrete and abstract steps of the operation Op;

then the form adopted for the corresponding proof obligation of retrenchment is

$$G \wedge P_{Op} \wedge stp_{Op_C} \Rightarrow (\exists stp_{Op_A} \wedge ((G' \wedge O_{Op}) \vee C_{Op})) \tag{2}$$

where:

- P_{Op} is the within, or provided relation, tightening the scope of the proof obligation;
- O_{Op} is the output relation allowing strengthening of the claim made by the PO; and, crucially,
- C_{Op} is the concedes relation, which allows arbitrary departures from refinement-like behaviour, which is the essential characteristic of retrenchment.

The broad similarity between the shapes of (1) and (2) leads us to conjecture that a mathematically rigorous integration of refinement and retrenchment ought to be possible, and, indeed, this is the main topic of the current paper.

Of course, being construed in a similar way to model-based refinement (that is, as a more or less fixed scheme for relating system models and for generating proof obligations regarding such relationships), retrenchment ultimately suffers from similar complexity challenges to those already described. Nevertheless, being a weaker notion than refinement (in the sense of offering weaker guarantees than refinement typically does), it is hoped that the point at which the complexity issues start to defeat development strategies that employ suitable combinations of retrenchment alongside refinement lies considerably further out, which should considerably increase the number of real-world developments that can be feasibly given a formal treatment.

Giving a precise meaning to the phrase 'suitable combinations' is the main technical contribution of the current paper, and we will discuss this extensively below. For now, we will just describe how these techniques have already been used fruitfully in the development of some applications.

The most visible use of the technology proposed here has been in the treatment of a number of requirements issues in the Mondex formal development. The Mondex Purse

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

is a smartcard based electronic purse, whose security architecture permits payments from person to person using a wallet device or telephone line without the need for separate authorisation. The Mondex project was one of the earliest formal development exercises in which refinement played a central role (Stepney *et al.* 1998; Stepney *et al.* 2000). In seeking to keep the refinement tractable, a number of requirements issues were deliberately simplified and then treated informally outside the formal development. Subsequently, these were revisited using retrenchment to integrate a more formal treatment with the existing idealised development.

One such issue was the boundedness of Mondex sequence numbers. For the usual security reasons, Mondex transactions need to have unique sequence numbers. For simplicity, these were modelled as natural numbers in Stepney *et al.* (2000), though, in practice, they are obviously bounded. The difference between idealised and realistic sequence numbers, and its consequences, was treated in a retrenchment in Banach *et al.* (2005).

Another issue was the boundedness of Mondex error logs. For predictable reasons connected with transaction recovery, Mondex purses need to log various kinds of failed transaction. For simplicity, these logs were modelled as unbounded sets in Stepney *et al.* (2000), though, in practice, they are obviously bounded. For implementation reasons, the size of the log is rather small, which imposes a collection of requirement issues quite different from those connected with the finiteness of the sequence number bound. These issues were treated in a retrenchment in Banach *et al.* (2006a).

Yet another issue was connected with the properties of a hash function used during Mondex transaction recovery. For simplicity, and, more importantly, to make the security proof go through at all, this hash function was modelled as an injective function, though in practice any real hash function is obviously going to be many-to-one. This opens up interesting security repercussions, which were treated in a retrenchment in Banach *et al.* (2006b).

Finally, for subtle reasons connected with the use of backward refinement in the Mondex development, an operation as simple as a purse balance enquiry could not be modelled in the original development. The whole issue was revisited and a satisfactory resolution developed using retrenchment in Banach *et al.* (2007a). This later led to an abstract development of protocol refinement in general in Banach and Schellhorn (2010).

All of the above were treated using the precursor of the theory of the current paper, namely, using the theory in Jeske (2005). Given that the details of the theorems of Jeske (2005) differ from those in the current paper, it is worth asking how these earlier Mondex retrenchments might be affected if redone using the revised theory. The good news is that they are not affected at all because of the extreme simplicity of the relevant refinements in Stepney *et al.* (2000) through which the retrenchments of interest were pulled: these refinements are, in fact, injections on the state space, and when applied to such simple refinements, the theorems of Jeske (2005) have the same effects as the theorems developed in the current paper. Therefore, the earlier case studies serve just as well as confirmations of the utility of the revised theory as they did as confirmations of the earlier theory.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

Looking beyond the applications just described:

- Jeffords *et al.* (2009) adapted the basic retrenchment idea and, by adding a suitable collection of additional conditions (policed by corresponding proof obligations within the tool), was able to formally introduce faulty behaviours into the system model that depart from and subsequently rejoin (a refinement of) the nominal abstract behaviour.
- Banach (2011) introduced an extension of the Event-B formalism to include retrenchment development steps (precisely along the lines of the theory expounded in the current paper). Some of the ramifications of this are being explored in the ADVANCE project[†].
- Banach *et al.* (2012) showed that the greater flexibility of retrenchment can be extremely useful in accommodating variable discrepancies between abstract continuous model behaviour and concrete discretised model behaviour in situations where these cannot be statically bounded. Again, cooperation between refinement and retrenchment aspects is policed using the theoretical ideas of the current paper.

We can foresee there being many further applications of a similar kind.

3. Transition systems, retrenchment and refinement

In this section we present our basic definitions and notation. At any single moment in a development activity, we will typically be dealing with a pair of systems, with the first in some sense more ‘abstract’ than the second, which is more ‘concrete’. We model systems as transition systems, which are organised as follows.

An abstract system Abs has a set of operation names Ops_A, with typical element Op_A. An operation Op_A works on the abstract state space U having typical element u (the before state), and on an input space I_{Op_A} with typical element i. The operation Op_A will produce an after state typically written u' and once more in U, and an output o drawn from an output space O_{Op_A}. Initial states satisfy the predicate $Init_A(u')$, which allows initial states to be viewed as results of an initialisation operation if need be.

Individual steps of Op_A are written $u \text{-}(i, Op_A, o)\twoheadrightarrow u'$. Taken together, they constitute the step relation $stp_{Op_A}(u, i, u', o)$ of Op_A. Aggregating over all of Ops_A, we obtain the complete transition relation for the Abs system:

$$stp_A = \bigcup_{Op_A \in \mathsf{Ops}_A} stp_{Op_A},$$

where the union is necessarily disjoint since the relevant Op_A name is part of every execution step.

Later, we will have several systems in play simultaneously, and we will use similar notational conventions for them. We will set out our generic notions using a pair of concrete systems, which we name Conc_T and Conc_F. For Conc_T:

[†] Advanced Design and Verification Environment for Cyber-physical System Engineering – ADVANCE is an FP7 Information and Communication Technologies (ICT) Project funded by the European Commission (grant number 287563). For details, see `//http://www.advance-ict.eu/`.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

— the operation names are $Op_C \in \mathsf{Ops}_C$;
— the states are $v \in \mathsf{V}$;
— the inputs are $j \in \mathsf{J}_{Op_C}$;
— the outputs are $p \in P_{Op_C}$;
— the initial states satisfy $Init_C(v')$;
— the transitions are $v \mathrel{\text{-}(j, Op_C, p)\!\!\twoheadrightarrow} v'$, which are elements of the complete step relation $stp_{Op_C}(v, j, v', p)$.

For Conc_F, we assume:

— the operation names are also $Op_C \in \mathsf{Ops}_C$; but
— the variables are $w \in \mathsf{W}$;
— the inputs are $k \in \mathsf{K}_{Op_C}$;
— the outputs are $q \in \mathsf{Q}_{Op_C}$; and
— the rest are the obvious counterparts.

3.1. *Retrenchment*

Given the above context, a retrenchment from Abs to Conc_T is defined by three facts:

(1) We have

$$\mathsf{Ops}_A \cap \mathsf{Ops}_C = \mathsf{Ops}_{AC} \neq \varnothing,$$

that is, the abstract and concrete operation name sets have some elements in common.

(2) We have a collection of relations as follows:

— a retrieve relation $G(u, v)$ between abstract and concrete state spaces;
— for each common operation name $Op \in \mathsf{Ops}_{AC}$, a family of within, output and concedes relations:

$$\begin{aligned}
&P_{Op}(i, j, u, v)\\
&O_{Op}(o, p; u', v', i, j, u, v)\\
&C_{Op}(u', v', o, p; i, j, u, v),
\end{aligned}$$

respectively[†].

These relations are over the variables shown: specifically, the within relations involve the inputs and before states, while the output and concedes relations predominantly involve the outputs and after states, though inputs and before states can also feature if required (the semicolon is used to separate these additional possibilities cosmetically). The relations are collectively referred to as the retrenchment data, and, for brevity, we will refer to the retrenchment as *G,P,O,C*. Note that we suppress the '*A*' and

[†] The notation here confirms that the 'A' and 'C' and (later) similar subscripts on operation names are meta-level tags, which will be suppressed if it is convenient to do so and does not cause confusion. $\mathsf{Ops}_A \subseteq \mathsf{Ops}_C$ is usually assumed, but we will be more general here. Also, nothing prevents arbitrary correspondences between (otherwise unrelated) names in Ops_A and Ops_C being set up using suitable mappings, and though it would just add unnecessary theoretical clutter, such a property is highly desirable to add flexibility in the context of an industrial-strength tool.

'C' subscripts on Op in these relations since they concern both levels of abstraction equally.

(3) The following collection of properties must hold (these are the proof obligations or POs):

— The initial states must satisfy

$$Init_C(v') \Rightarrow (\exists u' \bullet Init_A(u') \wedge G(u', v')); \tag{3}$$

— for every corresponding operation pair Op_A and Op_C, the abstract and concrete step relations must satisfy the operation PO:

$$\begin{aligned} G(u, v) \wedge P_{Op}(i, j, u, v) \wedge stp_{Op_C}(v, j, v', p) \Rightarrow \\ (\exists u', o \bullet stp_{Op_A}(u, i, u', o) \\ \wedge ((G(u', v') \wedge O_{Op}(o, p; u', v', i, j, u, v)) \\ \vee C_{Op}(u', v', o, p; i, j, u, v))). \end{aligned} \tag{4}$$

For an $Op \in \mathsf{Ops}_{AC}$, an important counterfoil to the operation PO is the operation's simulation relation. This holds for an abstract step $u \text{-}(i, Op_A, o)\!\twoheadrightarrow u'$ and a corresponding concrete step $v \text{-}(j, Op_C, p)\!\twoheadrightarrow v'$, the two steps being in simulation if and only if

$$\begin{aligned} G(u, v) \wedge P_{Op}(i, j, u, v) \wedge stp_{Op_C}(v, j, v', p) \wedge stp_{Op_A}(u, i, u', o) \wedge \\ ((G(u', v') \wedge O_{Op}(o, p; u', v', i, j, u, v)) \vee C_{Op}(u', v', o, p; i, j, u, v)) \end{aligned} \tag{5}$$

holds.

A retrenchment (with retrenchment data as above) is a biretrenchment if and only if, in addition to (3) and (4), we also have

$$Init_A(u') \Rightarrow (\exists v' \bullet Init_C(v') \wedge G(u', v')) \tag{6}$$

and

$$\begin{aligned} G(u, v) \wedge P_{Op}(i, j, u, v) \wedge stp_{Op_A}(u, i, u', o) \Rightarrow \\ (\exists v', j \bullet stp_{Op_C}(v, j, v', p) \\ \wedge ((G(u', v') \wedge O_{Op}(o, p; u', v', i, j, u, v)) \\ \vee C_{Op}(u', v', o, p; i, j, u, v))). \end{aligned} \tag{7}$$

Thus, we can exchange the roles of abstract and concrete systems in a biretrenchment with impunity using the same data.

Going further, if we only have (6) and (7) (and not (3) and (4)), we call such a setup a converse retrenchment – that is, a converse retrenchment is characterised by having the signatures of the constituent relations the opposite way round to what we would normally expect.

Finally, suppose we simply have some relations defined on two transition systems and appropriately indexed by operation names as above, which have the signatures required to qualify as retrenchment data, but we cannot (or choose not to try to) establish (3) and

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

(4). Then the relations $G(u,v)$ and

$$\begin{aligned}&G(u,v)\wedge\\&P_{Op}(i,j,u,v)\wedge\\&((G(u',v')\wedge O_{Op}(o,p;u',v',i,j,u,v))\vee C_{Op}(u',v',o,p;i,j,u,v))\end{aligned}\tag{8}$$

(the latter from u,i,u',o, to v,j,v',p, with $Op\in\mathsf{Ops}_{AC}$) constitute a pseudoretrenchment. So, in a pseudoretrenchment, we have the simulation relations (5) without the abstract and concrete transitions.

3.2. *Refinement*

Given two systems Abs and Conc_F, we will now set up refinement as a relationship between the operations with identical names. In the current paper, we will assume that the abstract and concrete operations' name sets are identical for a refinement[†]. The refinement data will consist of a retrieve relation $G(u,w)$ and a family of input and output relations for each common $Op\in\mathsf{Ops}$: $In_{Op}(i,k)$ and $Out_{Op}(o,q)$. These latter relations are over the variables shown, that is, just the I/O variables. For brevity, we will refer to the refinement as *G,In,Out*.

The POs are:

— for initialisation

$$Init_C(w')\Rightarrow(\exists u'\bullet Init_A(u')\wedge G(u',w'));\tag{9}$$

— for the operations

$$\begin{aligned}&G(u,w)\wedge In_{Op}(i,k)\wedge stp_{Op_C}(w,k,w',q)\Rightarrow\\&\qquad(\exists u',o\bullet stp_{Op_A}(u,i,u',o)\wedge G(u',w')\wedge Out_{Op}(o,q)).\end{aligned}\tag{10}$$

Many notions of refinement feature additional criteria in addition to (9) and (10), and these are typically expressed using subsets of the before spaces and input spaces, and control the detailed semantics of operations. They often have names such as domain conditions, preconditions or guards. To mimic these generically, we let each common operation $Op\in\mathsf{Ops}$ have an associated applicability set, with $\textsc{app}_{Op_A}$ for Op_A and $\textsc{app}_{Op_C}$ for Op_C. Since some theories insist on weakening and others on strengthening such applicability criteria, typical conditions that such sets have to satisfy are either

$$\textsc{app}_{Op_A}(u,i)\wedge G(u,w)\wedge In_{Op}(i,k)\Rightarrow\textsc{app}_{Op_C}(w,k)\tag{11}$$

or

$$\textsc{app}_{Op_A}(u,i)\Leftarrow G(u,w)\wedge In_{Op}(i,k)\wedge\textsc{app}_{Op_C}(w,k).\tag{12}$$

As a shorthand, we will refer to both (11) and (12) using the notation

$$\textsc{app}_{Op_A}(u,i)\wedge G(u,w)\wedge In_{Op}(i,k)\overset{\Leftarrow}{\Rightarrow}G(u,w)\wedge In_{Op}(i,k)\wedge\textsc{app}_{Op_C}(w,k),\tag{13}$$

[†] We could, of course, opt for greater generality here along the lines of the footnote on page 142.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

where the symbol $\overset{\Leftarrow}{\Rightarrow}$ represents the two separate cases in (11) and (12). Thus (9), (10) and (13) represent three species of refinement theory: the first has (9) and (10); the second has (9), (10) and (11); and the third has (9), (10) and (12).

The simulation relation corresponding to these notions of refinement is

$$\begin{aligned}&G(u,w) \land In_{Op}(i,k) \land [\textsc{app}_{Op_A}(u,i) \land \textsc{app}_{Op_C}(w,k)] \land \\ &stp_{Op_C}(w,k,w',q) \land stp_{Op_A}(u,i,u',o) \land G(u',w') \land Out_{Op}(o,q),\end{aligned} \tag{14}$$

and again we say that the two steps are in simulation. The term

$$[\textsc{app}_{Op_A}(u,i) \land \textsc{app}_{Op_C}(w,k)]$$

in (14) is bracketed to indicate that it is not relevant for the simple formulation of refinement.

As with retrenchment, if in addition to (9) and (10), we also have

$$Init_A(u') \Rightarrow (\exists w' \bullet Init_C(w') \land G(u',w')) \tag{15}$$

and

$$\begin{aligned}&G(u,w) \land In_{Op}(i,k) \land stp_{Op_A}(u,i,u',o) \Rightarrow \\ &\qquad\qquad (\exists w',q \bullet stp_{Op_C}(w,k,w',q) \land G(u',w') \land Out_{Op}(o,q)),\end{aligned} \tag{16}$$

then the refinement is a birefinement. If we are dealing with a notion of refinement requiring the use of $\textsc{app}$ sets, then in the corresponding notion of birefinement we also insist on

$$\textsc{app}_{Op_A}(u,i) \land G(u,w) \land In_{Op}(i,k) \Leftrightarrow G(u,w) \land In_{Op}(i,k) \land \textsc{app}_{Op_C}(w,k). \tag{17}$$

Going further, if we only have (15) and (16), and the converse of (13) if appropriate (and not (9) and (10), and (13) if appropriate), then we call such a setup a converse refinement.

Finally, if we have three relations defined on two transition systems that are appropriately indexed by operation names and have the signatures required to qualify as refinement data, but we cannot (or choose not to try to) establish (9) and (10) (and (13) if appropriate), then the relations $G(u,w)$ and

$$G(u,w) \land In_{Op}(i,k) \land [\textsc{app}_{Op_A}(u,i) \land \textsc{app}_{Op_C}(w,k)] \land G(u',w') \land Out_{Op}(o,q), \tag{18}$$

with the latter from u,i,u',o, to w,k,w',q, with $Op \in \mathsf{Ops}$, are referred to as a pseudorefinement. As with a pseudoretrenchment, a pseudorefinement omits the transitions from the simulation relation.

4. Compositions

We will make much use later in the paper of compositions of relationships between systems. The relationships are retrenchments, refinements, their converses, their pseudo-analogues, and so on. Various notions of composition involving the basic retrenchment and refinement concepts were thoroughly studied in Banach *et al.* (2008), so we will just review the relevant results here. It turns out that these notions of composition are all based

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

on various compositions of relations, so they can be readily extended to the converse and pseudo variants. We will principally need vertical composition of retrenchments (and refinements) and disjunctive fusion composition.

4.1. *Vertical composition*

Suppose we have a system Sys_0 that is retrenched to a system Sys_1, and that Sys_1 is further retrenched to a system Sys_2. Assuming that the granularity of the individual transitions in these models does not change, Sys_0 and Sys_2 are related by a vertical composition. Subscripting the retrenchment data for the two original retrenchments with '1' and '2', respectively, and subscripting the retrenchment data for the composition with '(1, 2)', we find

$$G_{(1,2)} \equiv G_1 \mathbin{;} G_2 \tag{19}$$

$$P_{Op,(1,2)} \equiv (G_1 \wedge P_{Op,1}) \mathbin{;} (G_2 \wedge P_{Op,2}) \tag{20}$$

$$O_{Op,(1,2)} \equiv O_{Op,1} \mathbin{;} O_{Op,2} \tag{21}$$

$$C_{Op,(1,2)} \equiv (G'_1 \wedge O_{Op,1} \mathbin{;} C_{Op,2}) \vee (C_{Op,1} \mathbin{;} G'_2 \wedge O_{Op,2}) \vee (C_{Op,1} \mathbin{;} C_{Op,2}) \tag{22}$$

where the forward relational composition $\mathbin{;}$ is through the relevant variables of the intermediate system. Thus:

— The composed retrieve and the composed output relations are just the composition of the two retrieves and the two outputs, respectively.

— The composed within relation is the composition of the two withins, but strengthened by the composed retrieve.

— The composed concession has a more complex form and is one of:

(a) the after state retrieve and output relations for the first retrenchment, composed with the concession for the second; or

(b) the converse of (a); or

(c) the composition of the two concessions.

Since much will depend on this composition, we will give a precise statement, which also explains what me meant when we wrote 'we find' just before (19) – it referred to a soundness result, since the proof of Proposition 4.1 requires that the hypothesised retrenchment data do in fact satisfy the POs (3) and (4).

Proposition 4.1. Let Sys_0 (with variables u_0, i_0, o_0) be retrenched to Sys_1 (with variables u_1, i_1, o_1) using

$$G_1, \{P_{Op,1}, O_{Op,1}, C_{Op,1} | Op \in \mathsf{Ops}_{01}\},$$

and Sys_1 be retrenched to Sys_2 (with variables u_2, i_2, o_2) using

$$G_2, \{P_{Op,2}, O_{Op,2}, C_{Op,2} | Op \in \mathsf{Ops}_{12}\}.$$

Then Sys_0 is retrenched to Sys_2 using retrieve, within and concedes relations

$$G_{(1,2)}, \{P_{Op,(1,2)}, O_{Op,(1,2)}, C_{Op,(1,2)} | Op \in \mathsf{Ops}_{01} \cap \mathsf{Ops}_{12}\},$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

where[†]:

$$G_{(1,2)}(u_0,u_2) \equiv (\exists u_1 \bullet G_1(u_0,u_1) \land G_2(u_1,u_2)) \tag{23}$$

$$\begin{aligned} P_{Op,(1,2)}(i_0,i_2,u_0,u_2) \equiv (\exists u_1, i_1 \bullet\ & G_1(u_0,u_1) \land G_2(u_1,u_2) \land \\ & P_{Op,1}(i_0,i_1,u_0,u_1) \land \\ & P_{Op,2}(i_1,i_2,u_1,u_2)) \end{aligned} \tag{24}$$

$$\begin{aligned} O_{Op,(1,2)}(o_0,o_2;u'_0,u'_2,i_0,i_2,u_0,u_2) \equiv (\exists u'_1, o_1, u_1, i_1 \bullet\ & \\ & O_{Op,1}(o_0,o_1;u'_0,u'_1,i_0,i_1,u_0,u_1) \land \\ & O_{Op,2}(o_1,o_2;u'_1,u'_2,i_1,i_2,u_1,u_2)) \end{aligned} \tag{25}$$

$$\begin{aligned} C_{Op,(1,2)}(u'_0,u'_2,o_0,o_2;i_0,i_2,u_0,u_2) \equiv (\exists u'_1, o_1, u_1, i_1 \bullet\ & \\ & \{[G_1(u'_0,u'_1) \land \\ & \quad O_{Op,1}(o_0,o_1;u'_0,u'_1,i_0,i_1,u_0,u_1) \land \\ & \quad C_{Op,2}(u'_1,u'_2,o_1,o_2;i_1,i_2,u_1,u_2)] \lor \\ & [C_{Op,1}(u'_0,u'_1,o_0,o_1;i_0,i_1,u_0,u_1) \land \\ & \quad G_2(u'_1,u'_2) \land \\ & \quad O_{Op,2}(o_1,o_2;u'_1,u'_2,i_1,i_2,u_1,u_2)] \lor \\ & [C_{Op,1}(u'_0,u'_1,o_0,o_1;i_0,i_1,u_0,u_1) \land \\ & \quad C_{Op,2}(u'_1,u'_2,o_1,o_2;i_1,i_2,u_1,u_2)]\}). \end{aligned} \tag{26}$$

So far we have considered the composition of two retrenchments. The composition of a retrenchment (first) with a refinement (second) follows by defaulting the data for the second retrenchment. In more detail:

— the retrieve relation is the same as (23);

— we get the counterpart of (24) by replacing $P_{Op,2}$ by $In_{Op,2}$, which is the relevant input relation;

— we get the counterpart of (25) by replacing $O_{Op,2}$ by

$$Out_{Op,2} \land G'_2 \land In_{Op,2} \land G_2,$$

which is the relevant output relation strengthened by the retrieve relation (in both the after and before values) and the input relation – we do all this to match all of the '1' variables of $O_{Op,1}$;

— we get the counterpart of (26) by setting $C_{Op,2}$ to false and replacing $O_{Op,2}$ as in the previous point.

[†] In (26), and later in the paper, we use braces to delimit large disjunctions (especially those which are not at top level), with the individual large disjuncts delimited by square brackets.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

We can summarise the result as:

$$G_{(1,2)} \equiv G_1 \fatsemi G_2 \tag{27}$$

$$P_{Op,(1,2)} \equiv (G_1 \wedge P_{Op,1}) \fatsemi (G_2 \wedge In_{Op,2}) \tag{28}$$

$$O_{Op,(1,2)} \equiv O_{Op,1} \fatsemi (Out_{Op,2} \wedge G_2' \wedge In_{Op,2} \wedge G_2) \tag{29}$$

$$C_{Op,(1,2)} \equiv C_{Op,1} \fatsemi (Out_{Op,2} \wedge G_2' \wedge In_{Op,2} \wedge G_2). \tag{30}$$

Note that the result is a retrenchment, so there is no $\textsc{app}_{Op}$ data to worry about – the $\textsc{app}_{Op}$ from the refinement (if applicable) is simply discarded.

If we have a refinement (first) composed with a retrenchment (second), we simply interchange the roles of the two in the preceding discussion.

If we have two refinements, the reasoning is relatively familiar, and it is easy to prove that the following data yield a sound composed refinement:

$$G_{(1,2)} \equiv G_1 \fatsemi G_2 \tag{31}$$

$$In_{Op,(1,2)} \equiv In_{Op,1} \fatsemi In_{Op,2} \tag{32}$$

$$Out_{Op,(1,2)} \equiv Out_{Op,1} \fatsemi Out_{Op,2}. \tag{33}$$

From these, it is also easy to show that for any relevant '$\textsc{app}_{Op}$' criteria, either two instances of (11) or two instances of (12) compose in a sound way.

4.2. *Disjunctive fusion composition*

The fact that retrenchment is described using a PO whose top level structure is an implication, together with the fact that $A \Rightarrow B$ and $C \Rightarrow D$ implies

$$A \vee C \Rightarrow B \vee D,$$

yields a strategy for composing different retrenchments for the same pair of abstract and concrete systems, which we call disjunctive fusion composition[†].

If the retrenchment data for the first retrenchment are subscripted with '1' and for the second with '2', we will subscript the composed data with '(1∨2)'. In outline, the retrenchment data for disjunctive fusion composition is

$$G_{(1\vee 2)} \equiv G_1 \vee G_2 \tag{34}$$

$$P_{Op,(1\vee 2)} \equiv (G_1 \vee P_{Op,2}) \wedge (P_{Op,1} \vee G_2) \wedge (P_{Op,1} \vee P_{Op,2}) \tag{35}$$

$$O_{Op,(1\vee 2)} \equiv (G_1' \vee O_{Op,2}) \wedge (O_{Op,1} \vee G_2') \wedge (O_{Op,1} \vee O_{Op,2}) \tag{36}$$

$$C_{Op,(1\vee 2)} \equiv C_{Op,1} \vee C_{Op,2}. \tag{37}$$

In more detail, the basic soundness result is stated in the following proposition.

Proposition 4.2. Let Abs be retrenched to Conc using

$$G_1, \{P_{Op,1}, O_{Op,1}, C_{Op,1} | Op \in \mathsf{Ops}_{AC}\}$$

[†] Since we could replace '∨' by '∧' in this statement, there is also a conjunctive variant, but it will play a much smaller role than the disjunctive case, and we will just mention it in a couple of places when required.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

(with the usual variables). Let Abs also be retrenched to Conc using

$$G_2, \{P_{Op,2}, O_{Op,2}, C_{Op,2} | Op \in \mathsf{Ops}_{AC}\}$$

(with the usual variables). Then Abs can also be retrenched to Conc using

$$G_{(1\vee 2)}, \{P_{Op,(1\vee 2)}, O_{Op,(1\vee 2)}, C_{Op,(1\vee 2)} | Op \in \mathsf{Ops}_A\}$$

where:

$$G_{(1\vee 2)}(u,v) \equiv G_1(u,v) \vee G_2(u,v) \tag{38}$$

$$\begin{aligned} P_{Op,(1\vee 2)}(i,j,u,v) \equiv\ & (G_1(u,v) \vee P_{Op,2}(i,j,u,v)) \wedge \\ & (P_{Op,1}(i,j,u,v) \vee G_2(u,v)) \wedge \\ & (P_{Op,1}(i,j,u,v) \vee P_{Op,2}(i,j,u,v)) \end{aligned} \tag{39}$$

$$\begin{aligned} O_{Op,(1\vee 2)}(o,p;u',v',i,j,u,v) \equiv\ & (G_1(u',v') \vee O_{Op,2}(o,p;u',v',i,j,u,v)) \wedge \\ & (O_{Op,1}(o,p;u',v',i,j,u,v) \vee G_2(u',v')) \wedge \\ & (O_{Op,1}(o,p;u',v',i,j,u,v) \vee \\ & \ O_{Op,2}(o,p;u',v',i,j,u,v)) \end{aligned} \tag{40}$$

$$\begin{aligned} C_{Op,(1\vee 2)}(u',v',o,p;i,j,u,v) \equiv\ & C_{Op,1}(u',v',o,p;i,j,u,v) \vee \\ & C_{Op,2}(u',v',o,p;i,j,u,v). \end{aligned} \tag{41}$$

5. Square completions

In this section we give a schematic outline of the main results of the next four sections to help make the details more easily digestible.

The main idea is ‘square completion’. Consider the left-hand side of Figure 1, which consists of two triangles. The upper triangle has two solid boxes, which represent the two given systems, and the solid arrow is a retrenchment between them (with given retrenchment data). The third, hollow, box in the triangle represents another system: it is drawn hollow to represent the fact that it is to be constructed from the given data. The Lifting Theorem (see Section 6) shows that we can indeed construct this system from the given data in a generic way, and that, moreover, it can be connected to the given systems through the dashed arrows, the horizontal arrow being a retrenchment and the vertical one being a refinement (with the retrenchment and refinement data for these again being constructed from the given data in a generic way). Not only this, but the constructed retrenchment and refinement can be composed using (27)–(30) to yield an equivalent of the original (solid) retrenchment. Furthermore, the construction is unique up to inter-refinability: this fact is important since the generically constructed system (in this and subsequent theorems) is frequently rather unnatural-looking from an application perspective, so the opportunity to replace it with something that is theoretically equivalent but more intuitively appealing with respect to the application is highly desirable from a

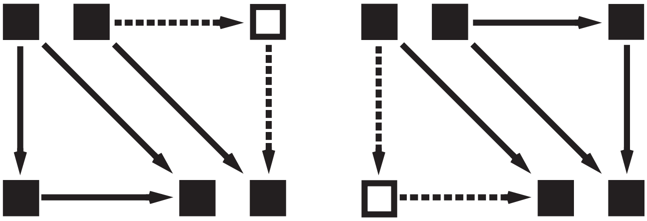

Fig. 1. Illustration of the lifting and lowering constructions – the vertical arrows are refinements and the horizontal arrows are retrenchments

systems engineering vantage point – see Section 10 for a more extensive discussion of this point.

Now consider the lower triangle of the left-hand side of Figure 1. It shows a vertical refinement followed by a horizontal retrenchment. The composition of these (using the dual of (27)–(30)) yields a retrenchment represented by the hypotenuse of the lower triangle. We may suppose that this retrenchment is the starting point of the construction we have just discussed in the upper triangle. Therefore, the Lifting Theorem enables us to complete the 'L shape' in the lower triangle to a square. This allows us to interchange the order of a refinement and retrenchment in a composition in such a way that the result of the two compositions, either way round, yields the same retrenchment (that is, the diagonal). The fact that the construction only requires the diagonal as input data means that many of the details of the specific refinement and retrenchment are irrelevant for the carrying out of the interchange.

We will now consider the right-hand side of Figure 1, which also consists of two triangles. The lower triangle has two solid boxes, which again represent two given systems, and the solid arrow is a retrenchment between them (with given retrenchment data). The third, hollow, box in the triangle again represents another system that is to be constructed from the given data. The Lowering Theorem (Section 7) shows that we can indeed construct this system from the given data in a generic way, and that, moreover, it can be connected to the given systems through the dashed arrows, the horizontal arrow being a retrenchment and the vertical one being a refinement (with the retrenchment and refinement data for these again being constructed from the given data in a generic way). Again, the constructed refinement and retrenchment can be composed using the dual of (27)–(30) to yield an equivalent of the original (solid) retrenchment. As before, the construction is unique up to inter-refinability, and this is again useful for the reasons previously stated. The upper triangle of the right-hand side of Figure 1 plays the same role as the lower triangle of the left-hand side of Figure 1, so we have another square completion, and we can interchange the order of a refinement and retrenchment in a composition, but this time in the other direction, with the same retrenchment resulting.

We have now covered the first two major results of the paper. For the remaining results, consider Figure 2. The square on the left-hand side has two solid sides and two dashed ones. As before, the horizontal arrows are retrenchments and the vertical arrows are refinements, with the dashed arrows to be constructed out of the (given) solid arrows. The

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

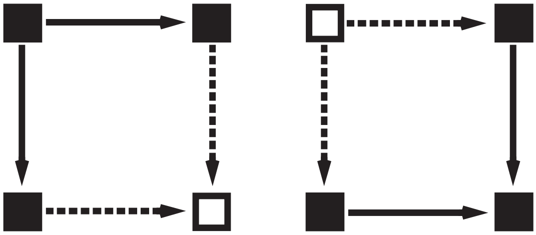

Fig. 2. Illustration of the postjoin and prejoin constructions – the vertical arrows are refinements and the horizontal arrows are retrenchments

Postjoin Theorem (see Section 8) shows that there is a generic construction that allows this to be done in such a way that the composition of the given retrenchment with the constructed refinement combines with the composition of the given refinement with the constructed retrenchment (using disjunctive fusion composition) to yield a retrenchment (which is not shown explicitly in the figure) from the top left system to the bottom right (constructed) system. The construction of the dashed system in the bottom right corner is again unique, but up to a weaker notion (inter-simulability in the sense defined in Section 3), which subsumes inter-refinability (hence, using inter-refinability to police the replacement of the generically constructed system by one closer to application concerns remains acceptable). We thus obviously have another square completion.

The square on the right-hand side of Figure 2 is the dual of this construction. It shows that if we are given a (vertical) refinement and (horizontal) retrenchment that converge to the same system, we can complete the square generically to create a system, together with a suitable refinement and retrenchment, such that the dual properties of the postjoin construction hold. Thus, we again have a retrenchment from top left to bottom right given by a fusion composition of the two routes round the square, and the universality of the basic construction is again characterised by inter-simulability, which again strengthens under suitable circumstances to inter-refinability.

6. The Lifting Theorem

In this section we consider the Lifting Theorem in detail. The relevant part of Figure 1 is elaborated in Figure 3. The given systems are *Abs* and *Conc*, with the usual retrenchment between them. The constructed system is *Univ*, and the universal nature of its relationship with *Abs* and *Conc* is expressed by saying that whenever there is a system *Xtra* enjoying similar properties to *Univ*, then *Xtra* is more abstract than *Univ*, that is, there is a refinement from *Xtra* to *Univ*.

Theorem 6.1. Let *Abs* (with variables u, i, o) and *Conc* (with variables v, j, p) be two systems, and let there be a retrenchment from *Abs* to *Conc* with retrenchment data

$$G,\ \{P_{Op}, O_{Op}, C_{Op} | Op \in \mathsf{Ops}_{AC}\}$$

where Ops_{AC} is the set of common names of related operations of *Abs* and *Conc*.

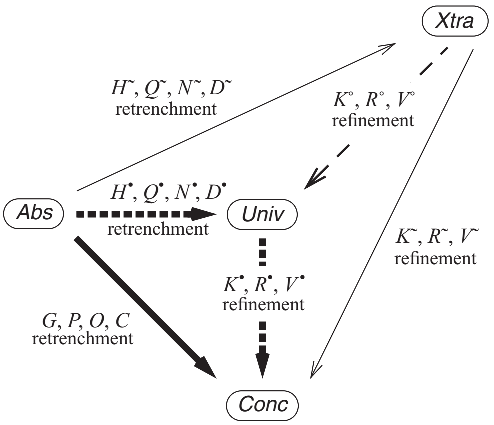
Xtra
$H^{\sim}, Q^{\sim}, N^{\sim}, D^{\sim}$
retrenchment
$K^{\circ}, R^{\circ}, V^{\circ}$
refinement
Abs
$H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$
retrenchment
Univ
$K^{\sim}, R^{\sim}, V^{\sim}$
refinement
$K^{\bullet}, R^{\bullet}, V^{\bullet}$
refinement
G, P, O, C
retrenchment
Conc

Fig. 3. The lifting construction in detail.

Then we have:

(1) There is a system *Univ* (with variables t, h, n) with operation name set Ops_U, where $\mathsf{Ops}_U = \mathsf{Ops}_C$, such that:

(i) there is a retrenchment from *Abs* to *Univ* with retrenchment data, say

$$H^{\bullet}(u,t),\ \{Q^{\bullet}_{Op}, N^{\bullet}_{Op}, D^{\bullet}_{Op} | Op \in \mathsf{Ops}_{AU}\};$$

(ii) there is a refinement from *Univ* to *Conc* with refinement data, say

$$K^{\bullet}(t,v),\ \{R^{\bullet}_{Op}, V^{\bullet}_{Op} | Op \in \mathsf{Ops}_U\},$$

which is a birefinement;

(iii) the composition (in the sense of (27)–(30)) of the retrenchment $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ and the refinement $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ yields the retrenchment G,$G \wedge P$,O,C;

(iv) if the notion of refinement in question requires the use of $\textsc{app}_{Op}$ sets, then the $\textsc{app}_{Op}$ sets of *Univ* are given by

$$\textsc{app}_{Op_U}(t,h) \equiv (\exists v, j \bullet K^{\bullet}(t,v) \wedge R^{\bullet}_{Op}(h,j) \wedge \textsc{app}_{Op_C}(v,j)). \tag{42}$$

(2) Whenever there is

— a system *Xtra* (with variables $t^{\sim}, h^{\sim}, n^{\sim}$), with operation name set Ops_X where $\mathsf{Ops}_X = \mathsf{Ops}_C$,

— a retrenchment from *Abs* to *Xtra* given by $H^{\sim}, Q^{\sim}, N^{\sim}, D^{\sim}$, and

— a refinement from *Xtra* to *Conc* given by $K^{\sim}, R^{\sim}, V^{\sim}$,

where the composition of $H^{\sim}, Q^{\sim}, N^{\sim}, D^{\sim}$ and $K^{\sim}, R^{\sim}, V^{\sim}$ yields G,$G \wedge P$,O,C, we have:

(i) there is a refinement from *Xtra* to *Univ* with refinement data, say

$$K^{\circ}(t^{\sim}, t),\ \{R^{\circ}_{Op}, V^{\circ}_{Op} | Op \in \mathsf{Ops}_U\};$$

(ii) we have

$$\begin{aligned} H^{\sim} \fatsemi K^{\circ} &\Leftarrow H^{\bullet} \\ (H^{\sim} \wedge Q^{\sim}) \fatsemi (K^{\circ} \wedge R^{\circ}) &\Leftarrow (H^{\bullet} \wedge Q^{\bullet}) \\ N^{\sim} \fatsemi (K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) &\Leftarrow N^{\bullet} \\ D^{\sim} \fatsemi (K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) &\Leftarrow D^{\bullet}; \end{aligned}$$

(iii) we have

$$\begin{aligned} K^{\circ} \fatsemi K^{\bullet} &= K^{\sim} \\ R^{\circ} \fatsemi R^{\bullet} &= R^{\sim} \\ V^{\circ} \fatsemi V^{\bullet} &= V^{\sim}. \end{aligned}$$

(3) If a system *Univ** has the properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are inter-refinable.

Proof.

(1) We start by completing the details of *Univ*, the retrenchment $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$ and the refinement $K^{\bullet}, R^{\bullet}, V^{\bullet}$. Assuming the usual conventions for *Abs* and *Conc*, the state space of *Univ* is $t \in \mathsf{T} = \mathsf{U} \times \mathsf{V}$. There are two cases for the input and output spaces of *Univ*:

— If $Op \in \mathsf{Ops}_{AU}$ (in other words $Op \in \mathsf{Ops}_{AC}$), then we have

$$\begin{aligned} h &\in \mathsf{H}_{Op} = \mathsf{I}_{Op} \times \mathsf{J}_{Op} \\ n &\in \mathsf{N}_{Op} = \mathsf{O}_{Op} \times \mathsf{P}_{Op}. \end{aligned}$$

— If $Op \in \mathsf{Ops}_{U \setminus AU}$ (in other words $Op \in \mathsf{Ops}_C - \mathsf{Ops}_{AC} = \mathsf{Ops}_{C \setminus AC}$), then

$$\begin{aligned} h &\in \mathsf{H}_{Op} = \mathsf{J}_{Op} \\ n &\in \mathsf{N}_{Op} = \mathsf{P}_{Op}. \end{aligned}$$

Initialisation in *Univ* is given by

$$Init_U(t') \equiv (t' = (u', v') \wedge Init_A(u') \wedge Init_C(v') \wedge G(u', v')). \tag{43}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

The operations of Univ are given by

$$
stp_{Op_U}(t,h,t',n) \equiv
\begin{cases}
\begin{array}{l}
(t' = (u',v') \wedge n = (o,p) \wedge \\
\ h = (i,j) \wedge t = (u,v) \wedge \\
\ \{[G(u,v) \wedge P_{Op}(i,j,u,v) \wedge \\
\qquad stp_{Op_A}(u,i,u',o) \wedge stp_{Op_C}(v,j,v',p) \wedge \\
\qquad ((G(u',v') \wedge O_{Op}(o,p;u',v',i,j,u,v)) \vee \\
\qquad\quad C_{Op}(u',v',o,p;i,j,u,v))] \vee \\
\quad [\neg(G(u,v) \wedge P_{Op}(i,j,u,v)) \wedge \\
\qquad stp_{Op_C}(v,j,v',p)]\})
\end{array} & \text{if } Op \in \mathsf{Ops}_{AU} \\[2ex]
\begin{array}{l}
(t' = (u',v') \wedge n = p \wedge \\
\ h = j \wedge t = (u,v) \wedge \\
\ stp_{Op_C}(v,j,v',p))
\end{array} & \text{if } Op \in \mathsf{Ops}_{U \setminus AU}.
\end{cases}
\tag{44}
$$

The retrenchment $H^{\bullet},Q^{\bullet},N^{\bullet},D^{\bullet}$ is given by the data[†]

$$H^{\bullet}(u,t) \equiv (t = (u,v) \wedge G(u,v)) \tag{45}$$

$$Q^{\bullet}_{Op}(i,h,u,t) \equiv (h = (i,j) \wedge t = (u,v) \wedge P_{Op}(i,j,u,v)) \tag{46}$$

$$
\begin{aligned}
N^{\bullet}_{Op}(o,n;u',t',i,h,u,t) \equiv (&t' = (u',v') \wedge n = (o,p) \wedge \\
&h = (i,j) \wedge t = (u,v) \wedge \\
&O_{Op}(o,p;u',v',i,j,u,v))
\end{aligned}
\tag{47}
$$

$$
\begin{aligned}
D^{\bullet}_{Op}(o,n,u',t';i,h,u,t) \equiv (&t' = (u',v') \wedge n = (o,p) \wedge h = (i,j) \wedge \\
&t = (u,v) \wedge C_{Op}(o,p,u',v';i,j,u,v)).
\end{aligned}
\tag{48}
$$

The refinement $K^{\bullet},R^{\bullet},V^{\bullet}$ is given by the data

$$K^{\bullet}(t,v) \equiv (t = (u,v)) \tag{49}$$

$$
R^{\bullet}_{Op}(h,j) \equiv
\begin{cases}
(h = (i,j)) & \text{if } Op \in \mathsf{Ops}_{AU} \\
(h = j) & \text{if } Op \in \mathsf{Ops}_{U \setminus AU}
\end{cases}
\tag{50}
$$

$$
V^{\bullet}_{Op}(n,p) \equiv
\begin{cases}
(n = (o,p)) & \text{if } Op \in \mathsf{Ops}_{AU} \\
(n = p) & \text{if } Op \in \mathsf{Ops}_{U \setminus AU}.
\end{cases}
\tag{51}
$$

We will now prove parts (i)–(iv):

(i) We need to check that $H^{\bullet},Q^{\bullet},N^{\bullet},D^{\bullet}$ is a retrenchment.

It is easy to check that with the G,P,O,C retrenchment initialisation PO, (43) and (45) give the required $H^{\bullet},Q^{\bullet},N^{\bullet},D^{\bullet}$ initialisation PO. For the operation PO, we

[†] Equation (45) is in fact an abbreviation of

$$H^{\bullet}(u,t) \equiv (t = (\underline{u},v) \wedge u = \underline{u} \wedge G(\underline{u},v))$$

with an application of the one-point rule. We will use this kind of short-cut extensively in the rest of the paper.

assume $H^\bullet, Q^\bullet_{Op}$, and the $Op \in \mathsf{Ops}_{AU}$ case of (44) (for which we only need the $G \wedge P_{Op}$ subcase). It is easy to see that we can produce a u' and an o (the u' and o inside the t' and n in (44)) for which both stp_{Op_A} and

$$(G' \wedge O_{Op}) \vee C_{Op}$$

(which are also in the $G \wedge P_{Op}$ subcase) hold. Repackaging the $G' \wedge O_{Op}$ into $H^{\bullet\prime} \wedge N^\bullet_{Op}$, and repackaging C_{Op} into $D^\bullet_{Op}$, we then get what we need.

(ii) We need to check that $K^\bullet, R^\bullet, V^\bullet$ is a refinement.
For the initialisation PO, we assume $Init_C(v')$. By (3), we have $v' \in \mathrm{ran}(G)$, so we can find a u', and hence a t', that makes (43) true – this t' is obviously related to v' by $K^\bullet$.
There are two cases for the operation PO:

— Case $Op \in Ops_{AU}$:
We assume $K^\bullet$, $R^\bullet_{Op}$ and stp_{Op_C}.
Given $K^\bullet \wedge R^\bullet_{Op}$, there are two subcases:

– $G \wedge P_{Op}$ (for the i, j, u, v, inside the t and h chosen for $K^\bullet \wedge R^\bullet_{Op}$):
Since we have $G \wedge P_{Op} \wedge stp_{Op_C}$, we can apply the G,P,O,C retrenchment's operation PO (4) to get u' and o values that make the G,P,O,C retrenchment's simulation condition

$$G \wedge P_{Op} \wedge stp_{Op_A} \wedge stp_{Op_C} \wedge ((G' \wedge O_{Op}) \vee C_{Op})$$

true, which gives us a stp_{Op_U} transition for this subcase.

– $\neg(G \wedge P_{Op})$:
The $\neg(G \wedge P_{Op})$ subcase of (44) offers us a stp_{Op_U} transition

$$\neg(G \wedge P_{Op}) \wedge stp_{Op_C}$$

based on the stp_{Op_C}, which we assumed.

In either case, all that we require of this transition is the projection $K^{\bullet\prime} \wedge V^\bullet_{Op}$, which is immediate given the first two clauses of (44).

— Case $Op \in Ops_{U \setminus AU}$:
The argument for this case is similar to the previous one, except that the $K^{\bullet\prime} \wedge V^\bullet_{Op}$ projection is simpler.

For the birefinement claim, we need to check the converse refinement. For the initialisation PO, we assume $Init_U(t')$. The t' obviously projects under $K^\bullet$ to a v' for which $Init_C(v')$ holds.
For the operation PO, let $t \text{-}(h, Op_U, n)\!\twoheadrightarrow t'$ be a step of Univ. If t and h project to v and j under $K^{\bullet\prime} \wedge R^\bullet_{Op}$, then t' and n project to v' and p under $K^{\bullet\prime} \wedge V^\bullet_{Op}$, and (44) confirms that $v \text{-}(j, Op_C, p)\!\twoheadrightarrow v'$ is a step of Conc since every case of (44) includes stp_{Op_C}, thereby discharging the PO.

(iii) We need to check that the composition of $H^\bullet, Q^\bullet, N^\bullet, D^\bullet$ and $K^\bullet, R^\bullet, V^\bullet$ (according to (27)–(30)) yields $G, G \wedge P, O, C$. But this is obvious given that $K^\bullet, R^\bullet, V^\bullet$ are simple projections.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

(iv) Note that since $K^{\bullet} \wedge R^{\bullet}_{Op}$ is a total function from $\mathsf{T} \times \mathsf{H}_{Op}$ onto $\mathsf{V} \times \mathsf{J}_{Op}$, it follows that

$$(K^{\bullet T} \wedge R^{\bullet T}_{Op}) \mathbin{;} (K^{\bullet} \wedge R^{\bullet}_{Op}) = \mathrm{Id}_{\mathsf{V} \times \mathsf{J}_{Op}}.$$

Consequently, the definition of the $\textsc{app}_{Op}$ sets of *Univ* in (42) satisfies the stipulation in (17) regarding the $K^{\bullet}, R^{\bullet}, V^{\bullet}$ birefinement.

This completes the proof of part (1).

(2) We start with the data for the refinement $K^{\circ}, R^{\circ}, V^{\circ}$, which is given by

$$K^{\circ}(t^{\sim}, t) \equiv (\exists v \bullet K^{\sim}(t^{\sim}, v) \wedge K^{\bullet}(t, v)) \tag{52}$$

$$R^{\circ}_{Op}(h^{\sim}, h) \equiv (\exists j \bullet R^{\sim}{}_{Op}(h^{\sim}, j) \wedge R^{\bullet}_{Op}(h, j)) \tag{53}$$

$$V^{\circ}_{Op}(n^{\sim}, n) \equiv (\exists p \bullet V^{\sim}{}_{Op}(n^{\sim}, p) \wedge V^{\bullet}_{Op}(n, p)). \tag{54}$$

We will now prove parts (i)–(iii):

(i) We start with the initialisation PO and assume $Init_U(t')$, which gives $Init_C \wedge G'$, which then gives $Init_C \wedge K^{\bullet\prime}$ when projected to *Conc*. From $Init_C$, we can then derive $Init_X \wedge K^{\sim\prime}$ from the $K^{\sim}, R^{\sim}, V^{\sim}$ refinement initialisation PO. So we have $Init_X \wedge (K^{\sim\prime} \wedge K^{\bullet\prime})$, which gives $Init_X \wedge K^{\circ\prime}$, which is what we need.

For the operation PO, we argue as follows. We let $t \mathrel{\text{-}(h, Op_U, n)\!\twoheadrightarrow} t'$ be a step of *Univ*, and suppose that

$$K^{\circ}(t^{\sim}, t) \wedge R^{\circ}_{Op}(h^{\sim}, h)$$

holds. This implies:

— $K^{\sim}(t^{\sim}, v) \wedge K^{\bullet}(t, v)$ for the unique v that t projects to under $K^{\bullet}$;

— $R^{\sim}{}_{Op}(h^{\sim}, j) \wedge R^{\bullet}_{Op}(h, j)$ for the unique j that h projects to under $R^{\bullet}$.

As in the birefinement proof above, we derive a $v \mathrel{\text{-}(j, Op_C, p)\!\twoheadrightarrow} v'$ step of *Conc* to which $t \mathrel{\text{-}(h, Op_U, n)\!\twoheadrightarrow} t'$ projects. With this, and $K^{\sim} \wedge R^{\sim}{}_{Op}$, and the $K^{\sim}, R^{\sim}, V^{\sim}$ refinement operation PO, we derive a $t^{\sim} \mathrel{\text{-}(h^{\sim}, Op_X, n^{\sim})\!\twoheadrightarrow} t^{\sim\prime}$ step of *Xtra* such that $K^{\sim\prime} \wedge V^{\sim}{}_{Op}$ holds for $t^{\sim\prime}$ and $n^{\sim}$. Putting this all together, we have now derived from step $t \mathrel{\text{-}(h, Op_U, n)\!\twoheadrightarrow} t'$ and $K^{\circ} \wedge R^{\circ}_{Op}$ the step $t^{\sim} \mathrel{\text{-}(h^{\sim}, Op_X, n^{\sim})\!\twoheadrightarrow} t^{\sim\prime}$ such that

$$K^{\sim\prime} \wedge K^{\bullet\prime} \wedge V^{\sim}{}_{Op} \wedge V^{\bullet}_{Op}$$

holds, in other words, $K^{\circ\prime} \wedge V^{\circ}_{Op}$ holds, which is what we need.

Going beyond this, if the notion of refinement requires the use of $\textsc{app}_{Op}$ sets, we must show that if a dependency like (11) or (12) holds between the $\textsc{app}_{Op}$ sets of *Conc* and those of *Xtra* in the context of the $K^{\sim}, R^{\sim}, V^{\sim}$ refinement, then a similar dependency holds between the $\textsc{app}_{Op}$ sets of *Univ* and those of *Xtra* in the context of the $K^{\circ}, R^{\circ}, V^{\circ}$ refinement. To do this, we first note that the stipulation (17) means that, for an (11) type dependency, if

$$\textsc{app}_{Op_X}(t^{\sim}, h^{\sim}) \wedge K^{\sim}(t^{\sim}, v) \wedge R^{\sim}{}_{Op}(h^{\sim}, j) \Rightarrow \textsc{app}_{Op_C}(v, j)$$

holds, then

$$\textsc{app}_{Op_X}(t^{\sim}, h^{\sim}) \wedge K^{\circ}(t^{\sim}, t) \wedge R^{\circ}_{Op}(h^{\sim}, h) \Rightarrow \textsc{app}_{Op_U}(t, h)$$

will also hold by composing $K^{\sim} \wedge R^{\sim}{}_{Op}$ with $K^{\bullet T} \wedge R^{\bullet T}_{Op}$. Similarly, for a (12) type dependency, again by composing $K^{\sim} \wedge R^{\sim}{}_{Op}$ with $K^{\bullet T} \wedge R^{\bullet T}_{Op}$, if

$$\mathrm{APP}_{Op_X}(t^{\sim}, h^{\sim}) \Leftarrow K^{\sim}(t^{\sim}, v) \wedge R^{\sim}{}_{Op}(h^{\sim}, j) \wedge \mathrm{APP}_{Op_C}(v, j)$$

holds, then

$$\mathrm{APP}_{Op_X}(t^{\sim}, h^{\sim}) \Leftarrow K^{\circ}(t^{\sim}, t) \wedge R^{\circ}_{Op}(h^{\sim}, h) \wedge \mathrm{APP}_{Op_U}(t, h)$$

will also hold.

(ii) Since $K^{\circ} = K^{\sim} \fatsemi K^{\bullet T}$ and $H^{\sim} \fatsemi K^{\sim} = G$, we have

$$H^{\sim} \fatsemi K^{\circ} = H^{\sim} \fatsemi K^{\sim} \fatsemi K^{\bullet T} = G \fatsemi K^{\bullet T} \Leftarrow H^{\bullet},$$

where the last implication holds because, while every $t = (u, v)$ with $\neg G(u, v)$ is in $\mathrm{ran}(K^{\bullet T})$, no such t is in $\mathrm{ran}(H^{\bullet})$.

The proofs of the other results are similar.

(iii) Since $K^{\circ} = K^{\sim} \fatsemi K^{\bullet T}$, we have

$$K^{\circ} \fatsemi K^{\bullet} = K^{\sim} \fatsemi K^{\bullet T} \fatsemi K^{\bullet} = K^{\sim} \fatsemi \mathrm{Id}_{\mathsf{V}} = K^{\sim}$$

(since $K^{\bullet T}$ is an inverse function).

The proofs of the other results are similar.

This completes the proof of part (2).

(3) Note that *Univ* itself satisfies the criteria required for *Xtra*, so if we have a system *Univ** with the properties (1) and (2) of *Univ*, then *Univ** satisfies the criteria required for *Xtra* too. Hence, we can construct two instances of Figure 3 as follows. In the first, *Univ* is in its conventional place and *Univ** replaces *Xtra*, and there is a refinement $K^{\circ}, R^{\circ}, V^{\circ}$, from *Univ** to *Univ*. In the second instance, *Univ** replaces *Univ*, and *Univ* replaces *Xtra*, and there is a refinement K^{*}, R^{*}, V^{*}, from *Univ* to *Univ**. So *Univ* and *Univ** are inter-refinable. □

6.1. *Remarks*

Remark 6.2. Referring to the last clause of Theorem 6.1, the composition of K^{*}, R^{*}, V^{*} with $K^{\circ}, R^{\circ}, V^{\circ}$ yields a refinement from *Univ* to itself (and similarly for *Univ**). However, this refinement is not required to be the identity. In particular, if the *Univ* system contains internal symmetries of a suitable kind, $K^{*} \fatsemi K^{\circ}$ may permute 'similar' states, or worse, map some of them to the same state, and so on. Our notion of 'inter-refinable' does not prevent this. Of course, if it is a permutation, composing it suitably with one of the two refinements will yield a birefinement.

Remark 6.3. The last clause of Theorem 6.1 presents, in effect, a notion of system equivalence, namely 'inter-refinability'. It is important to be aware that this is potentially a rather weak notion of equivalence, related to notions of bisimilarity, and much weaker than, say, a set theoretic isomorphism of transition systems. Much hinges on the strength or weakness of the retrieve relation connecting the state spaces. If it is strong, and relates

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

a state in one system to only a few states in the other, then the correspondence established can be precise and informative. However, if it is weak, and relates a state in one system to many states in the other, then the correspondence established can be rather vague. In our particular case, we had a retrieve relation that was a projection – such a relation completely ignores what may or may not be going on in the 'orthogonal' component of the projected system. As a consequence of all this, the fact that a certain system might be appropriate for a certain set of requirements does not automatically imply that a system inter-refinable with it is equally appropriate for those requirements – unless we take great care over what we mean by 'requirements' and 'appropriate'.

Remark 6.4. It is tempting to think[†] that the $K^\circ, R^\circ, V^\circ$ arrow in Figure 3 is the wrong way round. Looking at the diagram, and the relative dispositions of *Abs* and *Conc* within it, it seems that the most natural property we should ask of the *Univ* system is that it furnishes the most abstract system that accomplishes the factorisation. In such a case, there ought to be a refinement from *Univ* to the system *Xtra* that accomplishes any alternative factorisation. This was the strategy pursued in Jeske (2005) and earlier investigations. However, looking into the mathematics of this approach, the details are neither simple, nor do they suggest a straightforward integration with the other results we pursue in the current paper in terms of characterising the notion of universality that composite constructions might enjoy.

The alternative, described here, focuses on the most concrete system that accomplishes the factorisation. With this, the technical difficulties that plagued the earlier approaches just melt away. Furthermore, the composite constructions that we might imagine are much more understandable. For instance, imagine a commuting square of retrenchments and refinements (as in Figure 2) abutting the *Abs* to *Univ* retrenchment of Figure 3. Then, in a natural way, *Univ* refines the system (call it *Xtra*) directly above it. Composing the converse refinement directly above *Abs* with the retrenchment across the top of the square yields, in benign cases, a retrenchment from *Abs* to *Xtra* that, with the *Xtra* to *Univ* refinement, can be understood to yield an instance of Figure 3. The alternative approach, with *Univ* as the most abstract system, does not enjoy such natural properties.

Another reason to prefer the current approach is that it allows a very natural decoupling of the APP_{Op} sets discussion from the remainder of the construction, thereby giving a very generic feel to this aspect of the theory. Again, this smooth genericness does not emerge using alternative approaches. In the end, the argument between 'most abstract' and 'most concrete' is not one that can be resolved unequivocally using meta-criteria alone, and it is the persuasiveness of the mathematics that sways our treatment in the current paper.

7. The Lowering Theorem

In this section we consider the Lowering Theorem in detail. It can be viewed as the dual, in a suitable sense, of the Lifting Theorem. The relevant part of Figure 1 is elaborated

[†] Translation: 'For a long time the authors thought' .

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

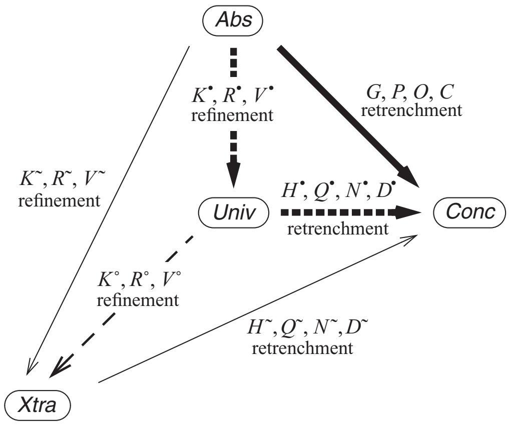
Abs
$K^\bullet, R^\bullet, V^\bullet$
refinement
G, P, O, C
retrenchment
$K^\sim, R^\sim, V^\sim$
refinement
Univ
$H^\bullet, Q^\bullet, N^\bullet, D^\bullet$
retrenchment
Conc
$K^\circ, R^\circ, V^\circ$
refinement
$H^\sim, Q^\sim, N^\sim, D^\sim$
retrenchment
Xtra

Fig. 4. The lowering construction in detail.

in Figure 4, where the given systems are *Abs* and *Conc*, with the usual retrenchment between them. The constructed system is *Univ* again, and the universal nature of its relationship with *Abs* and *Conc* is expressed by saying that whenever there is a system *Xtra* enjoying similar properties to *Univ*, then *Xtra* is more concrete than *Univ*, that is, there is a refinement from *Univ* to *Xtra*.

Theorem 7.1. Let *Abs* (with variables u, i, o) and *Conc* (with variables v, j, p) be two systems, and let there be a retrenchment from *Abs* to *Conc* with retrenchment data

$$G,\ \{P_{Op}, O_{Op}, C_{Op} | Op \in \mathsf{Ops}_{AC}\}$$

where Ops_{AC} is the set of common names of related operations of *Abs* and *Conc*. Then we have the following:

(1) There is a system *Univ* (with variables t, h, n), with operation name set Ops_U, where $\mathsf{Ops}_U = \mathsf{Ops}_A$, such that:

(i) there is a refinement from *Abs* to*Univ* with refinement data, say

$$K^\bullet(u,t),\ \{R^\bullet_{Op}, V^\bullet_{Op} | Op \in \mathsf{Ops}_A\},$$

which is a birefinement;

(ii) there is a retrenchment from *Univ* to *Conc* with retrenchment data, say

$$H^\bullet(t,v),\ \{Q^\bullet_{Op}, N^\bullet_{Op}, D^\bullet_{Op} | Op \in \mathsf{Ops}_{UC}\};$$

(iii) the composition (in the sense of the dual of (27)–(30)) of the refinement $K^\bullet, R^\bullet, V^\bullet$ and retrenchment $H^\bullet, Q^\bullet, N^\bullet, D^\bullet$ yields the retrenchment $G, G \wedge P, O, C$;

(iv) if the notion of refinement in question requires the use of $\textsc{app}_{Op}$ sets, then the $\textsc{app}_{Op}$ sets of *Univ* are given by

$$\textsc{app}_{Op_U}(t,h) \equiv (\exists u, i \bullet K^\bullet(u,t) \wedge R^\bullet_{Op}(i,h) \wedge \textsc{app}_{Op_A}(u,i)). \tag{55}$$

(2) Whenever there is:

— a system *Xtra* (with variables $t^{\sim}, h^{\sim}, n^{\sim}$), with operation name set Ops_X where $\mathsf{Ops}_X = \mathsf{Ops}_A$;

— a refinement from *Abs* to *Xtra* given by $K^{\sim}, R^{\sim}, V^{\sim}$; and

— a retrenchment from *Xtra* to *Conc* given by $H^{\sim}, Q^{\sim}, N^{\sim}, D^{\sim}$

where the composition of $K^{\sim}, R^{\sim}, V^{\sim}$ and $H^{\sim}, Q^{\sim}, N^{\sim}, D^{\sim}$ yields $G, G \wedge P, O, C$, we have:

(i) there is a refinement from *Univ* to *Xtra* with refinement data, say

$$K^{\circ}(t, t^{\sim}), \{R^{\circ}_{Op}, V^{\circ}_{Op} | Op \in \mathsf{Ops}_U\};$$

(ii) we have

$$\begin{aligned} K^{\circ} \mathbin{⨟} H^{\sim} &\Leftarrow H^{\bullet} \\ (K^{\circ} \wedge R^{\circ}) \mathbin{⨟} (H^{\sim} \wedge Q^{\sim}) &\Leftarrow (H^{\bullet} \wedge Q^{\bullet}) \\ (K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) \mathbin{⨟} N^{\sim} &\Leftarrow N^{\bullet} \\ (K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) \mathbin{⨟} D^{\sim} &\Leftarrow D^{\bullet}; \end{aligned}$$

(iii) we have

$$\begin{aligned} K^{\bullet} \mathbin{⨟} K^{\circ} &= K^{\sim} \\ R^{\bullet} \mathbin{⨟} R^{\circ} &= R^{\sim} \\ V^{\bullet} \mathbin{⨟} V^{\circ} &= V^{\sim}. \end{aligned}$$

(3) If a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are inter-refinable.

Proof.

(1) We start by completing the details of *Univ*, and of the refinement $K^{\bullet}, R^{\bullet}, V^{\bullet}$ and retrenchment $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$. Assuming the usual conventions for *Abs* and *Conc*, the state space of *Univ* is $t \in \mathsf{T} = \mathsf{U} \times \mathsf{V}$. There are two cases for the input and output spaces of *Univ*:

— If $Op \in \mathsf{Ops}_{UC}$ (in other words $Op \in \mathsf{Ops}_{AC}$, then

$$\begin{aligned} h &\in \mathsf{H}_{Op} = \mathsf{I}_{Op} \times \mathsf{J}_{Op} \\ n &\in \mathsf{N}_{Op} = \mathsf{O}_{Op} \times \mathsf{P}_{Op}. \end{aligned}$$

— If $Op \in \mathsf{Ops}_{U \setminus UC}$ (in other words $Op \in \mathsf{Ops}_A - \mathsf{Ops}_{AC} = \mathsf{Ops}_{A \setminus AC}$), then

$$\begin{aligned} h &\in \mathsf{H}_{Op} = \mathsf{I}_{Op} \\ n &\in \mathsf{N}_{Op} = \mathsf{O}_{Op}. \end{aligned}$$

Initialisation in *Univ* is given by

$$Init_U(t') \equiv (t' = (u', v') \wedge Init_A(u')). \tag{56}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

The operations of *Univ* are given by

$$stp_{Op_U}(t,h,t',n) \equiv \begin{cases} (t' = (u',v') \wedge n = (o,p) \wedge \\ \; h = (i,j) \wedge t = (u,v) \wedge & \text{if } Op \in \mathsf{Ops}_{UC} \\ \; stp_{Op_A}(u,i,u',o)) \\ (t' = (u',v') \wedge n = p \wedge \\ \; h = j \wedge t = (u,v) \wedge & \text{if } Op \in \mathsf{Ops}_{U \setminus UC}. \\ \; stp_{Op_A}(u,i,u',o)) \end{cases} \tag{57}$$

The refinement $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ is given by the data

$$K^{\bullet}(u,t) \equiv (t = (u,v)) \tag{58}$$

$$R^{\bullet}_{Op}(i,h) \equiv \begin{cases} (h = (i,j)) & \text{if } Op \in \mathsf{Ops}_{UC} \\ (h = i) & \text{if } Op \in \mathsf{Ops}_{U \setminus UC} \end{cases} \tag{59}$$

$$V^{\bullet}_{Op}(o,n) \equiv \begin{cases} (n = (o,p)) & \text{if } Op \in \mathsf{Ops}_{UC} \\ (n = o) & \text{if } Op \in \mathsf{Ops}_{U \setminus UC}. \end{cases} \tag{60}$$

The retrenchment $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ is given by the data

$$H^{\bullet}(t,v) \equiv (t = (u,v) \wedge G(u,v)) \tag{61}$$

$$Q^{\bullet}_{Op}(h,j,t,v) \equiv (h = (i,j) \wedge t = (u,v) \wedge P_{Op}(i,j,u,v)) \tag{62}$$

$$\begin{aligned} N^{\bullet}_{Op}(n,p;t',v',h,j,t,v) \equiv (t' = (u',v') \wedge n = (o,p) \wedge h = (i,j) \wedge \\ t = (u,v) \wedge O_{Op}(o,p;u',v',i,j,u,v)) \end{aligned} \tag{63}$$

$$\begin{aligned} D^{\bullet}_{Op}(t',v',n,p;h,j,t,v) \equiv (t' = (u',v') \wedge n = (o,p) \wedge h = (i,j) \wedge \\ t = (u,v) \wedge C_{Op}(o,p,u',v';i,j,u,v)). \end{aligned} \tag{64}$$

We will now prove parts (i)–(iv):

(i) We need to check that $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ is a refinement.
For the initialisation PO, suppose $Init_U(t')$ holds. Since this implies $Init_A(u')$ for the u' inside t', and $K^{\bullet}$ projects t' to u', the PO is discharged.
For the operation PO, suppose we have a step $t \text{-}(h,Op_U,n)\!\twoheadrightarrow t'$ of *Univ* and

$$K^{\bullet}(u,t) \wedge R^{\bullet}_{Op}(i,h).$$

The *Univ* step clearly contains an *Abs* step $u \text{-}(i,Op_A,o)\!\twoheadrightarrow u'$ in which u' and o are the projections of t' and n under $K^{\bullet\prime} \wedge V^{\bullet}_{Op}$. The latter is the case regardless of whether the projections $R^{\bullet}_{Op}$ and $V^{\bullet}_{Op}$ belong to the $Op \in Ops_{UC}$ or $Op \in Ops_{U \setminus UC}$ cases. This gives us the required result.

For the birefinement claim, for the initialisation PO, we let $Init_A(u')$ hold. Then $K^{\bullet}(u',t')$ holds for any v' where $t' = (u',v')$, which is enough for (56), thereby discharging the PO.

For the operation PO, suppose we have a step $u \text{-}(i, Op_A, o)\!\twoheadrightarrow u'$ of *Abs*, and

$$K^{\bullet}(u,t) \wedge R^{\bullet}_{Op}(i,h).$$

The *Abs* step extends to any *Univ* step $t \text{-}(h, Op_U, n)\!\twoheadrightarrow t'$ such that t' and n project through $K^{\bullet\prime} \wedge V^{\bullet}_{Op}$ to u' and o, thereby discharging the PO. This again works regardless of whether the projections $R^{\bullet}_{Op}$ and $V^{\bullet}_{Op}$ belong to either the $Op \in Ops_{UC}$ or $Op \in Ops_{U \setminus UC}$ case.

(ii) We need to check that $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$ is a retrenchment.
For the initialisation PO, we suppose $Init_C(v')$ holds. Then, by (3), there is a u' such that

$$Init_A(u') \wedge G(u', v')$$

holds. But this is equivalent to

$$Init_U(t') \wedge H^{\bullet}(t', v')$$

for the obvious t', thereby discharging the PO.
For the operation PO, suppose we have $H^{\bullet}$ and $Q^{\bullet}_{Op}$ and stp_{Op_C}. Then we combine the G and P_{Op} inside $H^{\bullet}$ and $Q^{\bullet}_{Op}$ with stp_{Op_C} and the G,P,O,C retrenchment operation PO (4) to derive a step $u \text{-}(i, Op_A, o)\!\twoheadrightarrow u'$ of the *Abs* system for which

$$(G' \wedge O_{Op}) \vee C_{Op}$$

holds. Repackaging the $G' \wedge O_{Op}$ into $H^{\bullet\prime} \wedge N^{\bullet}_{Op}$, and repackaging C_{Op} into $D^{\bullet}_{Op}$, we get the required result.

(iii) We need to check that the composition of $K^{\bullet}, R^{\bullet}, V^{\bullet}$ and $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$ (according to the dual of (27)–(30)) yields $G, G \wedge P, O, C$.
This is obvious given that $K^{\bullet}, R^{\bullet}, V^{\bullet}$ are simple projections.

(iv) Since $K^{\bullet T} \wedge R^{\bullet T}_{Op}$ is a total function from $\mathsf{T} \times \mathsf{H}_{Op}$ onto $\mathsf{U} \times \mathsf{I}_{Op}$, we have

$$(K^{\bullet} \wedge R^{\bullet}_{Op}) \fatsemi (K^{\bullet T} \wedge R^{\bullet T}_{Op}) = \mathrm{Id}_{\mathsf{U} \times \mathsf{I}_{Op}}.$$

Consequently, the definition of the $\textsc{app}_{Op}$ sets of *Univ* in (55) satisfies the stipulation in (17) for the $K^{\bullet}, R^{\bullet}, V^{\bullet}$ birefinement.

This completes the proof of part (1).

(2) We start with the data for the refinement $K^{\circ}, R^{\circ}, V^{\circ}$, which is given by

$$K^{\circ}(t, t^{\sim}) \equiv (\exists u \bullet K^{\bullet}(u,t) \wedge K^{\sim}(u, t^{\sim})) \tag{65}$$

$$R^{\circ}_{Op}(h, h^{\sim}) \equiv (\exists i \bullet R^{\bullet}_{Op}(i,h) \wedge R^{\sim}{}_{Op}(i, h^{\sim})) \tag{66}$$

$$V^{\circ}_{Op}(n, n^{\sim}) \equiv (\exists o \bullet V^{\bullet}_{Op}(o,n) \wedge V^{\sim}{}_{Op}(o, n^{\sim})). \tag{67}$$

We will now prove parts (i)–(iii):

(i) We must show that $K^{\circ}, R^{\circ}, V^{\circ}$ is a refinement.
For the initialisation PO, we assume $Init_X(t^{\sim\prime})$. Since $K^{\sim}, R^{\sim}, V^{\sim}$ is a refinement, there is a u' for which

$$Init_A(u') \wedge K^{\sim}(u', t^{\sim\prime})$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

holds. Since $Init_A(u')$ holds, taking any v' and setting $t' = (u',v')$, we get $Init_U(t')$ by (56). We also have $K^{\bullet}(u',t')$, so $K^{\circ}(t',t^{\sim\prime})$ holds by (65) and we are done.
For the operation PO, let $t^{\sim}\text{-}(h^{\sim},Op_X,n^{\sim})\twoheadrightarrow t^{\sim\prime}$ be a step of Xtra such that

$$K^{\circ}(t,t^{\sim}) \wedge R^{\circ}_{Op}(h,h^{\sim})$$

also holds. From $K^{\circ}\wedge R^{\circ}_{Op}$, which is

$$K^{\bullet}\wedge K^{\sim}\wedge R^{\bullet}_{Op}\wedge R^{\sim}{}_{Op},$$

we get a u and i such that

$$K^{\sim}\wedge R^{\sim}{}_{Op}$$

holds. Hence, since $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ is a refinement, there is a step $u\text{-}(i,Op_A,o)\twoheadrightarrow u'$ of Abs such that

$$K^{\sim\prime}\wedge V^{\sim}{}_{Op}$$

holds for u' and o. This Abs step, and

$$K^{\bullet}\wedge R^{\bullet}_{Op},$$

can be combined with the fact that $K^{\bullet}$,$R^{\bullet}_{Op}$,$V^{\bullet}_{Op}$ is a birefinement to derive a Univ step $t\text{-}(h,Op_U,n)\twoheadrightarrow t'$ for which

$$K^{\bullet\prime}\wedge V^{\bullet}_{Op},$$

and hence

$$K^{\circ\prime}\wedge V^{\circ}_{Op},$$

holds for t' and n, which discharges the PO.

Going beyond this, if the notion of refinement requires the use of APP_{Op} sets, we must show that if a dependency like (11) or (12) holds between the APP_{Op} sets of Abs and those of Xtra in the context of the $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ refinement, then a similar dependency holds between the APP_{Op} sets of Univ and those of Xtra in the context of the K°,R°,V° refinement.
To do this, we note that the stipulation (17) means that for an (11) type dependency, if

$$\text{APP}_{Op_A}(u,i) \wedge K^{\sim}(u,t^{\sim}) \wedge R^{\sim}{}_{Op}(i,h^{\sim}) \Rightarrow \text{APP}_{Op_X}(t^{\sim},h^{\sim})$$

holds, then

$$\text{APP}_{Op_U}(t,h) \wedge K^{\circ}(t,t^{\sim}) \wedge R^{\circ}_{Op}(h,h^{\sim}) \Rightarrow \text{APP}_{Op_X}(t^{\sim},h^{\sim})$$

will also hold by composing

$$K^{\sim T}\wedge R^{\sim}{}^{T}_{Op}$$

with

$$K^{\bullet}\wedge R^{\bullet}_{Op}.$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

Similarly, for a (12) type dependency, by composing

$$K^{\sim\,T} \wedge R^{\sim\,T}_{Op}$$

with

$$K^{\bullet} \wedge R^{\bullet}_{Op},$$

we again have that if

$$\mathrm{APP}_{Op_A}(u,i) \Leftarrow K^{\sim}(u,t^{\sim}) \wedge R^{\sim}{}_{Op}(i,h^{\sim}) \wedge \mathrm{APP}_{Op_X}(t^{\sim},h^{\sim})$$

holds, then

$$\mathrm{APP}_{Op_U}(t,h) \Leftarrow K^{\circ}(t,t^{\sim}) \wedge R^{\circ}_{Op}(h,h^{\sim}) \wedge \mathrm{APP}_{Op_X}(t^{\sim},h^{\sim})$$

will also hold.

(ii) Since

$$K^{\circ} = K^{\bullet T} \fatsemi K^{\sim}$$
$$K^{\sim} \fatsemi H^{\sim} = G,$$

we have

$$K^{\circ} \fatsemi H^{\sim} = K^{\bullet T} \fatsemi K^{\sim} \fatsemi H^{\sim} = K^{\bullet T} \fatsemi G \Leftarrow H^{\bullet},$$

where the last implication holds because, while every $t = (u,v)$ with $\neg G(u,v)$ is in $\mathrm{dom}(K^{\bullet T})$, no such t is in $\mathrm{dom}(H^{\bullet})$.

The proofs of the remaining results are similar.

(iii) Since $K^{\circ} = K^{\bullet T} \fatsemi K^{\sim}$, we have

$$K^{\bullet} \fatsemi K^{\circ} = K^{\bullet} \fatsemi K^{\bullet T} \fatsemi K^{\sim} = \mathrm{Id}_{\mathrm{T}} \fatsemi K^{\sim} = K^{\sim}$$

since $K^{\bullet T}$ is a function.

The proofs of the remaining results are similar.

This completes the proof of part (2).

(3) Note that *Univ* itself satisfies the criteria required of *Xtra*. Therefore, if we have a system *Univ** with the properties (1) and (2) of *Univ*, then *Univ** also satisfies the criteria required of *Xtra*. Hence, we can construct two instances of Figure 4 as follows. In the first instance, *Univ* is in its conventional place and *Univ** replaces *Xtra*, and there is a refinement K°,R°,V°, from *Univ* to *Univ**. In the second instance, *Univ** replaces *Univ*, and *Univ* replaces *Xtra*, and there is a refinement $K*$,$R*$,$V*$, from *Univ** to *Univ*. So *Univ* and *Univ** are inter-refinable. □

7.1. *Remarks*

The following remarks are similar to the corresponding remarks in Section 6, so are stated briefly.

Remark 7.2. As in Remark 6.2, the composition of K^*,R^*,V^* with K°,R°,V° need not be the identity. As before, if it happens to be a permutation, we can recover a birefinement.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

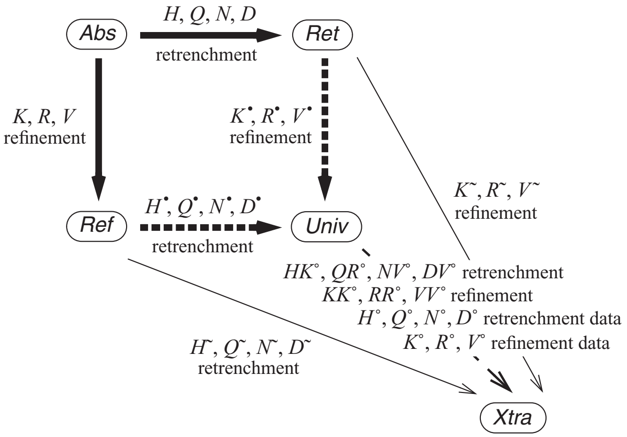

Fig. 5. The postjoin construction in detail – the pseudoretrenchment $G^{\times}$,$G^{\times}\wedge P^{\times}$,$O^{\times}$,$C^{\times}$ (not shown) connects *Ret* to *Ref*.

Remark 7.3. As in Remark 6.3, the 'inter-refinability' notion of equivalence is weaker than a given requirements context might need, so it should be used with care in an applications scenario.

Remark 7.4. As in Remark 6.4, it is tempting to think that the K°,R°,V° arrow in Figure 4 is the wrong way round. However, the comments in Remark 6.4 apply just as strongly here, though in a suitably dual sense.

8. The Postjoin Theorem

In this section we consider the Postjoin Theorem in detail. The relevant part of Figure 2 is elaborated in Figure 5, where the given systems are *Abs* together with *Ret* and *Ref*. There is a retrenchment from *Abs* to *Ret* and a refinement from *Abs* to *Ref*, the data for these being the usual ones. The constructed system is *Univ*, with a retrenchment from *Ref* to *Univ* and a refinement from *Ret* to *Univ*. The universal nature of the relationship between *Univ* and the other systems is expressed by saying that whenever there is a system *Xtra* enjoying similar properties to *Univ*, then *Xtra* is more concrete than *Univ*, witnessed by 'in simulation' relationships between the transitions of *Univ* and *Xtra*, strengthened under relatively benign conditions, to a retrenchment – and still further to a refinement – from *Univ* to *Xtra*.

Theorem 8.1. Let *Abs* (with variables u, i, o, operation names Ops_A), *Ret* (with variables v, j, p, operation names Ops_T) and *Ref* (with variables w, k, q, operation names Ops_F) be three systems. Let there be a retrenchment from *Abs* to *Ret* with retrenchment data

$$H,\ \{Q_{Op}, N_{Op}, D_{Op} | Op \in \mathsf{Ops}_{AT}\}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

where Ops_{AT} is the set of the common names of related operations of *Abs* and *Ret*. Let there be a refinement from *Abs* to *Ref* with refinement data

$$K,\ \{R_{Op}, V_{Op} | Op \in \mathsf{Ops}_A = \mathsf{Ops}_F\}$$

where Ops_A is the set of operation names of both *Abs* and *Ref*. Finally, suppose, for all Op, that $H \wedge Q_{Op}$ is a non-empty relation.

Then we have the following:

(1) There is a system *Univ* (with variables t, h, n), with operation name set Ops_U, where $\mathsf{Ops}_U = \mathsf{Ops}_T$, such that:

(i) there is a refinement from *Ret* to *Univ* with refinement data, say

$$K^{\bullet}(v,t),\ \{R^{\bullet}_{Op}, V^{\bullet}_{Op} | Op \in \mathsf{Ops}_T = \mathsf{Ops}_U\};$$

(ii) there is a retrenchment from *Ref* to *Univ* with retrenchment data, say

$$H^{\bullet}(w,t),\ \{Q^{\bullet}_{Op}, N^{\bullet}_{Op}, D^{\bullet}_{Op} | Op \in \mathsf{Ops}_{FU}\};$$

(iii) the composition of the pseudoretrenchment H^T,Q^T,N^T,D^T with the refinement K,R,V yields a pseudoretrenchment $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$, which is also given by the composition of the refinement $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ with the pseudoretrenchment $H^{\bullet T}$,$Q^{\bullet T}$, $N^{\bullet T}$,$D^{\bullet T}$;

(iv) each transition of *Univ* is in simulation with a transition of *Ret*, and if $Op \in \mathsf{Ops}_{FU}$, it is also in simulation with a transition of *Ref*, and in the latter case, any such pair of *Ret* and *Ref* transitions are in simulation through the pseudoretrenchment $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$;

(v) if the notion of refinement in question requires the use of $\textsc{app}_{Op}$ sets, then the $\textsc{app}_{Op}$ sets of *Univ* are given by

$$\textsc{app}_{Op_U}(t,h) \equiv (\exists v, j \bullet K^{\bullet}(v,t) \wedge R^{\bullet}_{Op}(j,h) \wedge \textsc{app}_{Op_T}(v,j)). \tag{68}$$

(2) Whenever there is

— a system *Xtra* (with variables $t^{\sim}, h^{\sim}, n^{\sim}$), with operation name set Ops_X where $\mathsf{Ops}_X = \mathsf{Ops}_T$,

— a refinement from *Ret* to *Xtra* given by $K^{\sim}$,$R^{\sim}$,$V^{\sim}$, and

— a retrenchment from *Ref* to *Xtra* given by $H^{\sim}$,$Q^{\sim}$,$N^{\sim}$,$D^{\sim}$,

where:

— the composition of the refinement

$$K^{\sim},R^{\sim},V^{\sim}$$

with the pseudoretrenchment

$$H^{\sim T},Q^{\sim T},N^{\sim T},D^{\sim T}$$

yields the pseudoretrenchment

$$G^{\times},G^{\times} \wedge P^{\times},O^{\times},C^{\times},$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

— each transition of *Xtra* is in simulation with a transition of *Ret*, and if $Op_X \in \mathsf{Ops}_{FX}$, then it is also in simulation with a transition of *Ref*, and where in the latter case any such pair of *Ret* and *Ref* transitions are in simulation through the pseudoretrenchment

$$G^{\times}, G^{\times} \wedge P^{\times}, O^{\times}, C^{\times},$$

then:

(i) There exist refinement data, say

$$K^{\circ}(t, t^{\sim}), \{R^{\circ}_{Op}, V^{\circ}_{Op} | Op \in \mathsf{Ops}_U\},$$

from *Univ* to *Xtra*, through which every transition of *Xtra* is in simulation with a transition of *Univ*.

(ii) There exist retrenchment data, say

$$H^{\circ}(t, t^{\sim}), \{Q^{\circ}_{Op}, N^{\circ}_{Op}, D^{\circ}_{Op} | Op \in \mathsf{Ops}_U\},$$

from *Univ* to *Xtra*, through which every $Op_X \in \mathsf{Ops}_{FX}$ transition of *Xtra* is in simulation with a transition of *Univ*, and if

$$\forall v \bullet \exists u, w \bullet \neg H(u, v) \wedge K(u, w)$$

also holds, then every other transition of *Xtra* is also in simulation with a transition of *Univ*.

(iii) We have

$$K^{\bullet} \fatsemi K^{\circ} = K^{\sim}$$
$$R^{\bullet} \fatsemi R^{\circ} = R^{\sim}$$
$$V^{\bullet} \fatsemi V^{\circ} = V^{\sim}.$$

(iv) We have

$$H^{\bullet} \fatsemi H^{\circ} = H^{\sim}$$

and for $Op_X \in \mathsf{Ops}_{FX}$,

$$(H^{\bullet} \wedge Q^{\bullet}) \fatsemi (H^{\circ} \wedge Q^{\circ}) = (H^{\sim} \wedge Q^{\sim})$$
$$N^{\bullet} \fatsemi N^{\circ} = N^{\sim}$$
$$D^{\bullet} \fatsemi D^{\circ} \Leftarrow D^{\sim}.$$

(v) There exist retrenchment data, say

$$HK^{\circ}(t, t^{\sim}), \{QR^{\circ}_{Op}, NV^{\circ}_{Op}, DV^{\circ}_{Op} | Op \in \mathsf{Ops}_U\},$$

from *Univ* to *Xtra*, through which every transition of *Xtra* is in simulation with a transition of *Univ*.

(3) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are inter-simulable.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

(4) There is a retrenchment from *Abs* to *Univ* with retrenchment data, say

$$G(u,t), \{P_{Op}, O_{Op}, C_{Op} | Op \in \mathsf{Ops}_{AU}\},$$

given by the disjunctive fusion composition of two retrenchments (a) and (b), where:

(a) is the vertical composition of H,Q,N,D with $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$;

(b) is the vertical composition of K,R,V with $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$.

(5) If we assume

$$\begin{aligned}
&(\mathrm{dom}(K \wedge R \wedge K' \wedge V) \lhd H \wedge Q \wedge H' \wedge N)(\underline{u}, v, \underline{i}, j, u', v', o, p) \wedge \\
&(\mathrm{dom}(H \wedge Q \wedge H' \wedge N) \lhd K \wedge R \wedge K' \wedge V)(\underline{u}, w, \underline{i}, k, u', w', o, q) \wedge \\
&(\mathrm{dom}(K \wedge R) \lhd H \wedge Q)(i, j, u, v) \wedge (\mathrm{dom}(H \wedge Q) \lhd K \wedge R)(i, k, u, w) \Rightarrow \\
&\qquad (\mathrm{dom}(K \wedge R \wedge K' \wedge V) \lhd H \wedge Q \wedge H' \wedge N)(u, v, i, j, u', v', o, p) \wedge \\
&\qquad (\mathrm{dom}(H \wedge Q \wedge H' \wedge N) \lhd K \wedge R \wedge K' \wedge V)(u, w, i, k, u', w', o, q)
\end{aligned} \tag{69}$$

$$\begin{aligned}
&(\mathrm{dom}(K \wedge R \wedge K' \wedge V) \lhd H \wedge Q \wedge D)(\underline{u}, v, \underline{i}, j, u', v', o, p) \wedge \\
&(\mathrm{dom}(H \wedge Q \wedge D) \lhd K \wedge R \wedge K' \wedge V)(\underline{u}, w, \underline{i}, k, u', w', o, q) \wedge \\
&(\mathrm{dom}(K \wedge R) \lhd H \wedge Q)(i, j, u, v) \wedge (\mathrm{dom}(H \wedge Q) \lhd K \wedge R)(i, k, u, w) \Rightarrow \\
&\qquad (\mathrm{dom}(K \wedge R \wedge K' \wedge V) \lhd H \wedge Q \wedge D)(u, v, i, j, u', v', o, p) \wedge \\
&\qquad (\mathrm{dom}(H \wedge Q \wedge D) \lhd K \wedge R \wedge K' \wedge V)(u, w, i, k, u', w', o, q),
\end{aligned} \tag{70}$$

then there is a retrenchment from *Univ* to *Xtra*, with the data given in part (2).(v)[†].

(6) Referring to the data given in (2).(v), if in addition to (69) and (70), we have

$$\begin{aligned}
&(\exists \tilde{t}, \tilde{h}, \tilde{n} \bullet stp_{Op_X}(\tilde{t}, \tilde{h}, \tilde{t}', \tilde{n})) \wedge \\
&(\exists \underline{t}' \bullet HK^{\circ}(\underline{t}', \tilde{t}')) \wedge \\
&(\exists t, \tilde{t}, h, \tilde{h}, n, \tilde{n} \bullet DV^{\circ}_{Op}(t', \tilde{t}', n, \tilde{n}\, ; h, \tilde{h}, t, \tilde{t})) \;\Rightarrow HK^{\circ}(t', \tilde{t}'),
\end{aligned} \tag{71}$$

then:

(i) the retrenchment of (5).(i) from *Univ* to *Xtra*, strengthens to a refinement with refinement data, say

$$KK^{\circ}(t, \tilde{t}), \{RR^{\circ}_{Op}, VV^{\circ}_{Op} | Op \in \mathsf{Ops}_{U}\};$$

(ii) if the notion of refinement in question requires the use of $\textsc{app}_{Op}$ sets, then the $\textsc{app}_{Op}$ sets of *Xtra* must satisfy

$$\begin{aligned}
&\textsc{app}_{Op_U}(t, h) \wedge KK^{\circ}(t, \tilde{t}) \wedge RR^{\circ}_{Op}(h, \tilde{h}) \overset{\Leftarrow}{\Rightarrow} \\
&\qquad\qquad KK^{\circ}(t, \tilde{t}) \wedge RR^{\circ}_{Op}(h, \tilde{h}) \wedge \textsc{app}_{Op_X}(\tilde{t}, \tilde{h}).
\end{aligned} \tag{72}$$

(7) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, and in addition the properties noted in (69)–(70), then *Univ* and *Univ** are inter-retrenchable, and if it also has the properties in (71), and if needed, (72), then they are also inter-refinable.

[†] Note that if the relations mentioned in (69) and (70) are functions (with *Ret* and *Ref* values as domain and *Abs* values as range), then (69) and (70) are satisfied.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

Proof.

(1) We start by completing the details of *Univ*, the refinement $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ and the retrenchment $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$. Adapting the usual notational conventions in the obvious way for *Ret* and *Ref*, the state space of *Univ* is $t \in \mathsf{T} = \mathsf{U} \times \mathsf{V} \times \mathsf{W}$ (where U is the state space of *Abs*, V is the state space of *Ret* and W is the state space of *Ref*). There are two cases for the input and output spaces of *Univ*:

— If $Op \in \mathsf{Ops}_{FU} = \mathsf{Ops}_{AT}$, then

$$h \in \mathsf{H}_{Op} = \mathsf{I}_{Op} \times \mathsf{J}_{Op} \times \mathsf{K}_{Op}$$
$$n \in \mathsf{N}_{Op} = \mathsf{O}_{Op} \times \mathsf{P}_{Op} \times \mathsf{Q}_{Op}.$$

— If $Op \in \mathsf{Ops}_{U \setminus FU}$, then

$$h \in \mathsf{H}_{Op} = \mathsf{J}_{Op}$$
$$n \in \mathsf{N}_{Op} = \mathsf{P}_{Op}.$$

We start by giving the data for the refinement and retrenchment.
The refinement $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ is given by the data:

$$K^{\bullet}(v,t) \equiv (t = (u,v,w) \wedge K(u,w)) \tag{73}$$

$$R^{\bullet}_{Op}(j,h) \equiv \begin{cases} (h = (i,j,k) \wedge R_{Op}(i,k)) & \text{if } Op \in \mathsf{Ops}_{FU} \\ (h = j) & \text{if } Op \in \mathsf{Ops}_{U \setminus FU} \end{cases} \tag{74}$$

$$V^{\bullet}_{Op}(p,n) \equiv \begin{cases} (n = (o,p,q) \wedge V_{Op}(o,q)) & \text{if } Op \in \mathsf{Ops}_{FU} \\ (n = p) & \text{if } Op \in \mathsf{Ops}_{U \setminus FU}. \end{cases} \tag{75}$$

The retrenchment $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ is given by the data:

$$H^{\bullet}(w,t) \equiv (t = (u,v,w) \wedge H(u,v)) \tag{76}$$

$$Q^{\bullet}_{Op}(k,h,w,t) \equiv (h = (i,j,k) \wedge t = (u,v,w) \wedge Q_{Op}(i,j,u,v)) \tag{77}$$

$$\begin{aligned} N^{\bullet}_{Op}(q,n;w',t',k,h,w,t) \equiv (t' &= (u',v',w') \wedge n = (o,p,q) \wedge \\ h &= (i,j,k) \wedge t = (u,v,w) \wedge \\ &N_{Op}(o,p;u',v',i,j,u,v)) \end{aligned} \tag{78}$$

$$\begin{aligned} D^{\bullet}_{Op}(w',t',q,n;k,h,w,t) \equiv (t' &= (u',v',w') \wedge n = (o,p,q) \wedge \\ h &= (i,j,k) \wedge t = (u,v,w) \wedge \\ &D_{Op}(u',v',o,p;i,j,u,v)). \end{aligned} \tag{79}$$

We need these relations to define the *Univ* system itself, so we will start by checking part 1.(iii).

(iii) We first calculate $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$ for $Op \in \mathsf{Ops}_{FU}$ as the composition of the pseudoretrenchment H^{T},Q^{T},N^{T},D^{T} with the refinement K,R,V. The fact that the result is also equal to the composition of the refinement $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ with the

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

pseudoretrenchment $H^{\bullet T}$,$Q^{\bullet T}$,$N^{\bullet T}$,$D^{\bullet T}$ follows by inspection.

$$\begin{aligned} G^{\times}(v,w) &\equiv H^{T} \fatsemi K \\ &= (\exists u \bullet H(u,v) \wedge K(u,w)) \\ &= K^{\bullet} \fatsemi H^{\bullet T}. \end{aligned} \tag{80}$$

$$\begin{aligned} & G^{\times}\wedge P^{\times}_{Op}\wedge((G^{\times\prime}\wedge O^{\times}_{Op})\vee C^{\times}_{Op})(v,w,j,k,v',w',p,q) \\ &\quad \equiv (H^{T}\wedge Q^{T}_{Op}\wedge((H^{T\prime}\wedge N^{T}_{Op})\vee D^{T}_{Op})) \fatsemi (K\wedge R_{Op}\wedge K'\wedge V_{Op}) \\ &\quad = (\exists u,i,u',o \bullet H(u,v) \wedge Q_{Op}(i,j,u,v) \wedge \\ &\qquad\quad ((H(u',v') \wedge N_{Op}(o,p;u',v',i,j,u,v)) \vee \\ &\qquad\qquad D_{Op}(u',v',o,p;i,j,u,v)) \wedge \\ &\qquad\quad K(u,w) \wedge R_{Op}(i,k) \wedge K(u',w') \wedge V_{Op}(o,q)) \\ &\quad = (K^{\bullet}\wedge R^{\bullet}_{Op}\wedge K^{\bullet\prime}\wedge V^{\bullet}_{Op}) \fatsemi \left(H^{\bullet T}\wedge Q^{\bullet T}_{Op}\wedge\left(\left(H^{\bullet T\prime}\wedge N^{\bullet T}_{Op}\right)\vee D^{\bullet T}_{Op}\right)\right). \end{aligned} \tag{81}$$

The *Univ* system itself is now given as follows.
Initialisation in *Univ* is given by

$$\begin{aligned} Init_{U}(t') \equiv (t' = (u',v',w') \wedge \\ Init_{T}(v') \wedge K^{\bullet}(v',t') \wedge \\ Init_{F}(w') \wedge H^{\bullet}(w',t')). \end{aligned} \tag{82}$$

The operations of *Univ* are given by

$$stp_{Op_U}(t,h,t',n) \equiv$$
$$\begin{cases} \begin{array}{l} (t = (u,v,w) \wedge h = (i,j,k) \wedge \\ \;t' = (u',v',w') \wedge n = (o,p,q) \wedge \\ \;[stp_{Op_T}(v,j,v',p) \wedge K^{\bullet}(v,t) \wedge \\ \;\;R^{\bullet}_{Op}(j,h) \wedge K^{\bullet}(v',t') \wedge V^{\bullet}_{Op}(p,n)] \wedge \\ \;[stp_{Op_F}(w,k,w',q) \wedge H^{\bullet}(w,t) \wedge \\ \;\;Q^{\bullet}_{Op}(k,h,w,t)\wedge \\ \;\;((H^{\bullet}(w',t') \wedge \\ \;\;\;\;N^{\bullet}_{Op}(q,n;w',t',k,h,w,t)) \vee \\ \;\;\;D^{\bullet}_{Op}(w',t',q,n;k,h,w,t))]) \end{array} & \text{if } Op \in \mathsf{Ops}_{FX} \\ \\ \begin{array}{l} (t = (u,v,w) \wedge h = j \wedge \\ \;t' = (u',v',w') \wedge n = p \wedge \\ \;[stp_{Op_T}(v,j,v',p) \wedge \\ \;\;\;K^{\bullet}(v,t) \wedge R^{\bullet}_{Op}(j,h) \wedge \\ \;\;\;K^{\bullet}(v',t') \wedge V^{\bullet}_{Op}(p,n)]) \end{array} & \text{if } Op \in \mathsf{Ops}_{X\setminus FX}. \end{cases} \tag{83}$$

(i) We need to check that $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ is a refinement.
For the initialisation PO, suppose we have $Init_{U}(t')$. Then by (82), we have $Init_{T}(v') \wedge K^{\bullet}(v',t')$ for the v' in t', which is enough.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

For the operation PO, suppose $Op \in \mathsf{Ops}_{FU}$. Then, if we assume

$$K^{\bullet}(v,t) \wedge R^{\bullet}_{Op}(j,h) \wedge stp_{Op_U}(t,h,t',n),$$

we can see that (83) furnishes us a $stp_{Op_T}(v,j,v',p)$ (with $K^{\bullet}(v',t') \wedge V^{\bullet}_{Op}(p,n)$ holding as required), which is what we need.

The argument is similar if $Op \in \mathsf{Ops}_{U \setminus FU}$.

(ii) We need to check that $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ is a retrenchment.

For the initialisation PO, suppose we have $Init_U(t')$. Then by (82), we have

$$Init_F(w') \wedge H^{\bullet}(w',t')$$

for the w' in t', which is enough.

For the operation PO, if we assume

$$H^{\bullet}(w,t) \wedge Q^{\bullet}_{Op}(k,h,w,t) \wedge stp_{Op_U}(t,h,t',n),$$

we can see that (83) furnishes us a $stp_{Op_F}(w,k,w',q)$ (with $(H^{\bullet\prime} \wedge N^{\bullet}_{Op}) \vee D^{\bullet}_{Op}$ holding as required), which is what we need.

(iv) It is clear from the arguments above that each step $t \,\text{-}(h,Op_U,n)\!\twoheadrightarrow t'$ of *Univ* is in simulation with (in the refinement sense) its constituent stp_{Op_T} transition, and, provided $Op \in \mathsf{Ops}_{FU}$, it is in simulation with (in the retrenchment sense) its constituent stp_{Op_F} transition (these stp_{Op_T} and stp_{Op_F} transitions are obviously unique since the data for the $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ retrenchment and the $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ refinement are functional from *Univ* to *Ref* and *Ret*, respectively). When $Op \in \mathsf{Ops}_{FU}$, the fact that these stp_{Op_T} and stp_{Op_F} transitions are in simulation through the pseudoretrenchment $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$ is evident since the data for the latter is directly present in (83).

(v) Since $K^{\bullet T} \wedge R^{\bullet T}_{Op}$ is a function (in general, a partial function) from $\mathsf{T} \times \mathsf{H}_{Op}$ onto $\mathsf{V} \times \mathsf{J}_{Op}$, we have

$$(K^{\bullet} \wedge R^{\bullet}_{Op}) \fatsemi (K^{\bullet T} \wedge R^{\bullet T}_{Op}) = \mathrm{Id}_{\mathsf{V} \times \mathsf{J}_{Op}}.$$

Consequently, the definition of the $\textsc{app}_{Op}$ sets of *Univ* in (68) satisfies the condition in (17) for the $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ refinement, and consequently satisfies an $\textsc{app}_{Op}$ requirement that has the form of either (11) or (12).

This completes the proof of part (1).

(2) (i) We start with the refinement data K°,R°,V°, which is given by

$$K^{\circ}(t,t^{\sim}) \equiv (\exists v \bullet K^{\bullet}(v,t) \wedge K^{\sim}(v,t^{\sim})) \tag{84}$$

$$R^{\circ}_{Op}(h,h^{\sim}) \equiv (\exists j \bullet R^{\bullet}_{Op}(j,h) \wedge R^{\sim}{}_{Op}(j,h^{\sim})) \tag{85}$$

$$V^{\circ}_{Op}(n,n^{\sim}) \equiv (\exists p \bullet V^{\bullet}_{Op}(p,n) \wedge V^{\sim}{}_{Op}(p,n^{\sim})). \tag{86}$$

We must show that every transition of *Xtra* is in simulation with a transition of *Univ* through (84)–(86). We consider two cases:

— Case $Op \in \mathsf{Ops}_{FX}$:

Let $t^{\sim} \,\text{-}(h^{\sim},Op_X,n^{\sim})\!\twoheadrightarrow t^{\sim\prime}$ be a step of *Xtra*, which, by assumption, is in simulation with some step of *Ret*, say $v \,\text{-}(j,Op_T,p)\!\twoheadrightarrow v'$, through $K^{\sim}$,$R^{\sim}$,$V^{\sim}$, and is also in simulation with some step of *Ref*, say $w\,\text{-}(k, Op_F, q)\!\twoheadrightarrow w'$, through $H^{\sim}$,$Q^{\sim}$,$N^{\sim}$,$D^{\sim}$. Again by assumption, these two steps are in simulation through $G^{\times}$,$G^{\times}\wedge P^{\times}$,$O^{\times}$,$C^{\times}$. But this means that they also determine a step of *Univ*, say $t\,\text{-}(h, Op_U, n)\!\twoheadrightarrow t'$, by (83), as seen above. This *Univ* step is in simulation with the *Ret* and *Ref* steps through the $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ refinement and the $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ retrenchment. Finally, composing the $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ simulation with the $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ simulation yields the required result.

— Case $Op \in \mathsf{Ops}_{X \setminus FX}$:
Let $t^{\sim}\,\text{-}(h^{\sim}, Op_X, n^{\sim})\!\twoheadrightarrow t^{\sim\prime}$ be a step of *Xtra*, which, by assumption, is in simulation with some step of *Ret*, say $v\,\text{-}(j, Op_T, p)\!\twoheadrightarrow v'$, through $K^{\sim}$,$R^{\sim}$,$V^{\sim}$. To get a simulation with a *Univ* step, referring to the $Op \in \mathsf{Ops}_{U \setminus FU}$ case of (83), it is sufficient to establish

$$K^{\bullet} \wedge R^{\bullet}_{Op} \wedge K^{\bullet\prime} \wedge V^{\bullet}_{Op}$$

for the *Ret* step. For this, it is enough to find any u, w, u', w' such that $K(u, w)$ and $K(u', w')$ hold (whence we can get $K^{\bullet} \wedge K^{\bullet\prime}$ through (83)). Beyond this, $v\,\text{-}(j, Op_T, p)\!\twoheadrightarrow v'$ gives us j, p (whence we can get $R^{\bullet}_{Op} \wedge V^{\bullet}_{Op}$ through the $Op \in \mathsf{Ops}_{X \setminus FX}$ cases of (74) and (75)). Composing the $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ simulation with the $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ simulation now yields the result.

(ii) We start with the retrenchment data H°,Q°,N°,D°. This is the vertical composition of the $H^{\sim}$, $Q^{\sim}$,$N^{\sim}$,$D^{\sim}$ and $H^{\bullet T}$,$Q^{\bullet T}$,$N^{\bullet T}$,$D^{\bullet T}$ data, suitably modified by the refinement data K°,R°,V° just above. It is given by

$$\begin{aligned} H^{\circ}(t, t^{\sim}) \equiv {} & [(\exists w \bullet H^{\bullet}(w, t) \wedge H^{\sim}(w, t^{\sim}))] \vee \\ & [\neg(\exists w \bullet H^{\bullet}(w, t)) \wedge \neg(\exists w \bullet H^{\sim}(w, t^{\sim})) \wedge \\ & \quad (\exists v \bullet K^{\bullet}(v, t) \wedge K^{\sim}(v, t^{\sim}))] \end{aligned} \tag{87}$$

$$Q^{\circ}_{Op}(h, h^{\sim}, t, t^{\sim}) \equiv \\ \begin{cases} (\exists k, w \bullet H^{\bullet}(w, t) \wedge H^{\sim}(w, t^{\sim}) \wedge \\ \quad Q^{\bullet}_{Op}(k, h, w, t) \wedge Q^{\sim}{}_{Op}(k, h^{\sim}, w, t^{\sim})) & \text{if } Op \in \mathsf{Ops}_{FX} \\ (\exists j \bullet R^{\bullet}_{Op}(j, h) \wedge R^{\sim}{}_{Op}(j, h^{\sim})) & \text{if } Op \in \mathsf{Ops}_{X \setminus FX} \end{cases} \tag{88}$$

$$N^{\circ}_{Op}(n, n^{\sim}; t', t^{\sim\prime}, h, h^{\sim}, t, t^{\sim}) \equiv \\ \begin{cases} (\exists w, k, w', q \bullet & \\ \quad N^{\bullet}_{Op}(q, n; w', t', k, h, w, t) \wedge & \text{if } Op \in \mathsf{Ops}_{FX} \\ \quad N^{\sim}{}_{Op}(q, n^{\sim}; w', t^{\sim\prime}, k, h^{\sim}, w, t^{\sim})) & \\ (\exists p \bullet V^{\bullet}_{Op}(p, n) \wedge V^{\sim}{}_{Op}(p, n^{\sim})) & \text{if } Op \in \mathsf{Ops}_{X \setminus FX} \end{cases} \tag{89}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

$$
\begin{array}{ll}
D^{\circ}_{Op}(t', t^{\sim\prime}, n, n^{\sim}; h, h^{\sim}, t, t^{\sim}) \equiv & \\
\left\{
\begin{array}{lll}
(\exists w, k, w', q \bullet & & \\
\quad \{[H^{\bullet}(w', t') \wedge & & \\
\qquad N^{\bullet}_{Op}(q, n; w', t', k, h, w, t) \wedge & & \\
\qquad D^{\sim}_{Op}(w', t^{\sim\prime}, q, n^{\sim}; k, h^{\sim}, w, t^{\sim})] \vee & & \\
\quad [D^{\bullet}_{Op}(w', t', q, n; k, h, w, t) \wedge & \text{if } Op \in \mathsf{Ops}_{FX} & (90) \\
\qquad H^{\sim}(w', t^{\sim\prime}) \wedge & & \\
\qquad N^{\sim}_{Op}(q, n^{\sim}; w', t^{\sim\prime}, k, h^{\sim}, w, t^{\sim})] \vee & & \\
\quad [D^{\bullet}_{Op}(w', t', q, n; k, h, w, t) \wedge & & \\
\qquad D^{\sim}_{Op}(w', t^{\sim\prime}, q, n^{\sim}; k, h^{\sim}, w, t^{\sim})]\}) & & \\
\mathsf{false} & \text{if } Op \in \mathsf{Ops}_{X \setminus FX}. &
\end{array}
\right. &
\end{array}
$$

We must show that every step of *Xtra* is in simulation with a step of *Univ* through (87)–(90). We consider the two cases separately:

— Case $Op \in \mathsf{Ops}_{FX}$:
Let $t^{\sim}\text{-}(h^{\sim}, Op_X, n^{\sim})\!\twoheadrightarrow t^{\sim\prime}$ be a step of *Xtra*, which, by assumption, is in simulation with a step of *Ret*, say $v\text{-}(j, Op_T, p)\!\twoheadrightarrow v'$, through $K^{\sim}, R^{\sim}, V^{\sim}$, and is also in simulation with a step of *Ref*, say $w\text{-}(k, Op_F, q)\!\twoheadrightarrow w'$, through $H^{\sim}, Q^{\sim}, N^{\sim}, D^{\sim}$. Again by assumption, these two steps are in simulation through $G^{\times}, G^{\times} \wedge P^{\times}, O^{\times}, C^{\times}$, so, as we saw above, they determine a step of *Univ*, say $t\text{-}(h, Op_U, n)\!\twoheadrightarrow t'$, by (83). This *Univ* step is in simulation with the *Ret* and *Ref* steps through the $K^{\bullet}, R^{\bullet}, V^{\bullet}$ refinement and the $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$ retrenchment. Composing the $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$ simulation with the $H^{\sim}, Q^{\sim}, N^{\sim}, D^{\sim}$ simulation now yields a formula of the shape

$$H^{\bullet} \wedge Q^{\bullet}_{Op} \wedge H^{\sim} \wedge Q^{\sim}_{Op} \wedge ((H^{\bullet\prime} \wedge N^{\bullet}_{Op}) \vee D^{\bullet}_{Op}) \wedge ((H^{\sim\prime} \wedge N^{\sim}) \vee D^{\sim}_{Op})$$

which relates the *Univ* and *Xtra* steps. We now apply the distributive law to the last two conjuncts to give

$$
\begin{aligned}
&(H^{\bullet\prime} \wedge N^{\bullet}_{Op} \wedge H^{\sim\prime} \wedge N^{\sim}_{Op}) \vee \\
&\qquad\qquad (H^{\bullet\prime} \wedge N^{\bullet}_{Op} \wedge D^{\sim}_{Op}) \vee (H^{\sim\prime} \wedge N^{\sim}_{Op} \wedge D^{\bullet}_{Op}) \vee (D^{\bullet}_{Op} \wedge D^{\sim}_{Op}).
\end{aligned}
$$

The last three disjuncts of this yield D°_{Op}, the first disjunct gives $H^{\circ\prime} \wedge N^{\circ}_{Op}$ (utilising the first disjunct in (87) for $H^{\circ\prime}$) and the rest of the earlier formula gives $H^{\circ} \wedge Q^{\circ}_{Op}$ (again utilising the first disjunct in (87) for H°). So we have what we need.

— Case $Op \in \mathsf{Ops}_{X \setminus FX}$:
Let $t^{\sim}\text{-}(h^{\sim}, Op_X, n^{\sim})\!\twoheadrightarrow t^{\sim\prime}$ be a step of *Xtra*. We must now do two things:

(a) First we must find some suitable values t, h, t', n such that they make a *Univ* transition for the $Op \in \mathsf{Ops}_{X \setminus FX}$ case. For this it is enough (according to (83)) to establish $stp_{Op_T}(v, j, v', p)$ for the v, j, v', p in t, h, t', n, and also that

$$K^{\bullet} \wedge R^{\bullet}_{Op} \wedge K^{\bullet\prime} \wedge V^{\bullet}_{Op}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

holds for t, h, t', n – the latter splits into four independent subproblems, one each for $K^{\bullet}$, $R^{\bullet}_{Op}$, $K^{\bullet\prime}$, $V^{\bullet}_{Op}$, since (83) does not otherwise constrict the values in the $Op \in \mathsf{Ops}_{X \setminus FX}$ case.

(b) Then, for these same values t, h, t', n, we must establish the simulation relation,

$$H^{\circ} \wedge Q^{\circ}_{Op} \wedge H^{\circ\prime} \wedge N^{\circ}_{Op}$$

(since D°_{Op} being false in the $Op \in \mathsf{Ops}_{X \setminus FX}$ case precludes establishing the concession variant) – noting that, through (88)–(89), Q°_{Op} and N°_{Op} only depend on inputs and outputs, respectively, in the $Op \in \mathsf{Ops}_{X \setminus FX}$ case, again splits this into four independent subproblems, one each for H°, Q°_{Op}, $H^{\circ\prime}$, N°_{Op}.

By assumption, the step $t^{\sim} \mathrel{-\!(h^{\sim}, Op_X, n^{\sim})\!\!\rightarrow} t^{\sim\prime}$ of *Xtra* is in simulation with a step of *Ret*, say $v \mathrel{-\!(j, Op_T, p)\!\!\rightarrow} v'$, through $K^{\sim}, R^{\sim}, V^{\sim}$ (which gives us the first thing we need for (83)). Noting that

$$R^{\bullet}_{Op}(j, h) \equiv (h = j)$$
$$V^{\bullet}_{Op}(p, n) \equiv (n = p),$$

together with $R^{\sim}$ and $V^{\sim}$ and (88)–(89), gives us $R^{\bullet}_{Op}$ and $V^{\bullet}_{Op}$ and Q°_{Op} and N°_{Op}, just leaving us with $K^{\bullet}$, $K^{\bullet\prime}$, H°, $H^{\circ\prime}$ to do. We consider $K^{\bullet}$ and H°, since the argument for $K^{\bullet\prime}$ and $H^{\circ\prime}$ will be similar. For the *Xtra* step, we have $K^{\sim}(v, t^{\sim})$ already. Now either $H^{\sim}(w, t^{\sim})$ holds for some w, or not:

- Suppose $H^{\sim}(w, t^{\sim})$ holds for some w:
  Then $H^{\sim}(w, t^{\sim})$ and $K^{\sim}(v, t^{\sim})$ compose to give $G^{\times}(v, w)$, so by (80), there is a u such that both $K(u, w)$ and $H(u, v)$ hold. The latter is enough to give $H^{\bullet}(w, t)$, where $t = (u, v, w)$. Composing $H^{\sim}(w, t^{\sim})$ and $H^{\bullet}(w, t)$ gives the desired $H^{\circ}(t, t^{\sim})$ through the first disjunct of (87). Since $G^{\times}(v, w)$ also gives $K^{\bullet}(v, t)$ and $H^{\bullet}(w, t)$, we have the desired $K^{\bullet}(v, t)$ too, completing this case.

- Suppose $H^{\sim}(w, t^{\sim})$ does not hold for any w:
  In this case, we have to establish the second disjunct of (87). This means that as well as $\neg(\exists w \bullet H^{\sim}(w, t^{\sim}))$, which we assume, we have to prove

  $$\neg(\exists w \bullet H^{\bullet}(w, t)) \wedge (\exists v \bullet K^{\bullet}(v, t) \wedge K^{\sim}(v, t^{\sim}))$$

  for suitable w and t. To do this, we use the additional assumption

  $$\forall v \bullet \exists u, w \bullet \neg H(u, v) \wedge K(u, w).$$

  Since we know $K^{\sim}(v, t^{\sim})$, we use the assumption to choose u and w such that $\neg H(u, v)$ and $K(u, w)$ both hold. From this, setting $t = (u, v, w)$, we deduce first that $\neg(\exists w \bullet H^{\bullet}(w, t))$ holds from (76), and then that $K^{\bullet}(v, t)$ holds from (73). This discharges the second disjunct of (87) and completes this case.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

(iii) Since $K^{\circ} = K^{\bullet T} \fatsemi K^{\sim}$, we have

$$\begin{aligned} K^{\bullet} \fatsemi K^{\circ} &= K^{\bullet} \fatsemi K^{\bullet T} \fatsemi K^{\sim} \\ &= \mathrm{Id}_{\mathsf{V}} \fatsemi K^{\sim} \\ &= K^{\sim} \end{aligned}$$

(since $K^{\bullet T}$ is a partial function).
The other results are similar.

(iv) Since

$$H^{\circ} = [(H^{\bullet T} \fatsemi H^{\sim}) \vee ((\neg H^{\bullet T} \fatsemi \neg H^{\sim}) \wedge (K^{\bullet T} \fatsemi K^{\sim}))],$$

we can derive that

$$\begin{aligned} H^{\bullet} \fatsemi H^{\circ} &= H^{\bullet} \fatsemi [(H^{\bullet T} \fatsemi H^{\sim}) \vee ((\neg H^{\bullet T} \fatsemi \neg H^{\sim}) \wedge (K^{\bullet T} \fatsemi K^{\sim}))] \\ &= \mathrm{Id}_{\mathsf{W}} \fatsemi H^{\sim} \\ &= H^{\sim} \end{aligned}$$

(since $H^{\bullet T}$ is a partial function, and $H^{\bullet}$... and $\neg H^{\bullet T}$... are disjoint). The derivation of $N^{\bullet} \fatsemi N^{\circ} = N^{\sim}$ is similar to that of the results in (2).(iii). We now consider $D^{\bullet} \fatsemi D^{\circ}$, where D° is given by (90). The term $D^{\bullet T} \wedge D^{\sim}$, which occurs disjunctively in (90), shows that $D^{\bullet} \fatsemi D^{\circ}$ contains

$$\begin{aligned} D^{\bullet} \fatsemi D^{\bullet T} \fatsemi D^{\sim} &= \mathrm{Id}_{\mathsf{W} \times \mathsf{K}_{Op} \times \mathsf{W} \times \mathsf{Q}_{Op}} \fatsemi D^{\sim} \\ &= D^{\sim}. \end{aligned}$$

Since (90) also contains other disjuncts, we derive $D^{\bullet} \fatsemi D^{\circ} \Leftarrow D^{\sim}$. Finally, by assumption, $H \wedge Q$ is a non-empty relation. This makes $H^{\bullet T} \wedge Q^{\bullet T}$ a non-empty (partial) function, which is onto $\mathsf{W} \times \mathsf{K}_{Op}$. Therefore, we can show

$$(H^{\bullet} \wedge Q^{\bullet}) \fatsemi (H^{\circ} \wedge Q^{\circ}) = (H^{\sim} \wedge Q^{\sim})$$

in the same way as other similar results, such as $N^{\bullet} \fatsemi N^{\circ} = N^{\sim}$ and the ones in (2).(iii)[†].

(v) We start with the retrenchment data $HK^{\circ}, QR^{\circ}, NV^{\circ}, DV^{\circ}$, which is given by (91)–(94). Note that, aside from the retrieve relation HK°, which is disjunctive in structure and simpler than just a combination of the retrieve relations (84) and (87), the remaining data is a suitable conjunction of the data in (84)–(86) with the data in (87)–(90). We have

$$\begin{aligned} HK^{\circ}(t, t^{\sim}) \equiv (t = (u, v, w) \wedge \\ \{[H^{\bullet}(w, t) \wedge H^{\sim}(w, t^{\sim})] \vee [K^{\bullet}(v, t) \wedge K^{\sim}(v, t^{\sim})]\}) \end{aligned} \tag{91}$$

[†] For other similar results, the non-emptiness of the partial function follows from the assumed non-emptiness of the underlying relation through Assumption 1.1. However, for $H \wedge Q$, non-emptiness does not follow from non-emptiness of H and Q individually.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

$$QR^{\circ}_{Op}(h,h^{\sim},t,t^{\sim})$$

$$\equiv \begin{cases} \begin{array}{l} (t=(u,v,w)\wedge h=(i,j,k)\wedge \\ \quad H^{\bullet}(w,t)\wedge H^{\sim}(w,t^{\sim})\wedge \\ \quad Q^{\bullet}_{Op}(k,h,w,t)\wedge \\ \quad Q^{\sim}_{Op}(k,h^{\sim},w,t^{\sim})\wedge \\ \quad K^{\bullet}(v,t)\wedge K^{\sim}(v,t^{\sim})\wedge \\ \quad R^{\bullet}_{Op}(j,h)\wedge R^{\sim}_{Op}(j,h^{\sim})) \end{array} & \text{if } Op\in\mathsf{Ops}_{FX} \\ \\ \begin{array}{l} (t=(u,v,w)\wedge h=j\wedge \\ \quad K^{\bullet}(v,t)\wedge K^{\sim}(v,t^{\sim})\wedge \\ \quad R^{\bullet}_{Op}(j,h)\wedge R^{\sim}_{Op}(j,h^{\sim})) \end{array} & \text{if } Op\in\mathsf{Ops}_{X\setminus FX} \end{cases} \tag{92}$$

$$NV^{\circ}_{Op}(n,n^{\sim};t',t^{\sim\prime},h,h^{\sim},t,t^{\sim})$$

$$\equiv \begin{cases} \begin{array}{l} (t=(u,v,w)\wedge h=(i,j,k)\wedge \\ \quad t'=(u',v',w')\wedge n=(o,p,q)\wedge \\ \quad N^{\bullet}_{Op}(q,n;w',t',k,h,w,t)\wedge \\ \quad N^{\sim}_{Op}(q,n^{\sim};w',t^{\sim\prime},k,h^{\sim},w,t^{\sim})\wedge \\ \quad K^{\bullet}(v,t)\wedge R^{\bullet}_{Op}(j,h)\wedge \\ \quad K^{\bullet}(v',t')\wedge V^{\bullet}_{Op}(p,n)\wedge \\ \quad K^{\sim}(v,t^{\sim})\wedge R^{\sim}_{Op}(j,h^{\sim})\wedge \\ \quad K^{\sim}(v',t^{\sim\prime})\wedge V^{\sim}_{Op}(p,n^{\sim})) \end{array} & \text{if } Op\in\mathsf{Ops}_{FX} \\ \\ (n=p\wedge V^{\bullet}_{Op}(p,n)\wedge V^{\sim}_{Op}(p,n^{\sim})) & \text{if } Op\in\mathsf{Ops}_{X\setminus FX} \end{cases} \tag{93}$$

$$DV^{\circ}_{Op}(t',t^{\sim\prime},n,n^{\sim};h,h^{\sim},t,t^{\sim})$$

$$\equiv \begin{cases} \begin{array}{l} (t=(u,v,w)\wedge h=(i,j,k)\wedge \\ \quad t'=(u',v',w')\wedge n=(o,p,q)\wedge \\ \quad \{[H^{\bullet}(w',t')\wedge N^{\bullet}_{Op}(q,n;w',t',k,h,w,t)\wedge \\ \qquad D^{\sim}_{Op}(w',t^{\sim\prime},q,n^{\sim};k,h^{\sim},w,t^{\sim})]\vee \\ \quad\ [D^{\bullet}_{Op}(w',t',q,n;k,h,w,t)\wedge \\ \qquad H^{\sim}(w',t^{\sim\prime})\wedge \\ \qquad N^{\sim}_{Op}(q,n^{\sim};w',t^{\sim\prime},k,h^{\sim},w,t^{\sim})]\vee \\ \quad\ [D^{\bullet}_{Op}(w',t',q,n;k,h,w,t)\wedge \\ \qquad D^{\sim}_{Op}(w',t^{\sim\prime},q,n^{\sim};k,h^{\sim},w,t^{\sim})]\}\wedge \\ \quad K^{\bullet}(v,t)\wedge R^{\bullet}_{Op}(j,h)\wedge \\ \quad K^{\bullet}(v',t')\wedge V^{\bullet}_{Op}(p,n)\wedge \\ \quad K^{\sim}(v,t^{\sim})\wedge R^{\sim}_{Op}(j,h^{\sim})\wedge \\ \quad K^{\sim}(v',t^{\sim\prime})\wedge V^{\sim}_{Op}(p,n^{\sim})) \end{array} & \text{if } Op\in\mathsf{Ops}_{FX} \\ \\ \mathsf{false} & \text{if } Op\in\mathsf{Ops}_{X\setminus FX}. \end{cases} \tag{94}$$

In the terminology of Banach *et al.* (2008), and aside from the properties of the retrieve relation already noted, the composition of (91)–(94) is a blend of

— on the one hand, conjunctive fusion composition (since the state and the I/O spaces are (partly) the same); and,

— on the other hand, synchronous parallel composition (since the state and the I/O spaces are (partly) different)

of the refinement data (84)–(86) and the retrenchment data (87)–(90).

With the retrenchment data in place, the argument is now largely a replay of the proofs of (2).(i) and (2).(ii).

Starting with an $Op \in \mathsf{Ops}_{FX}$ step of *Xtra*, we infer *Ret* and *Ref* steps from the refinement and retrenchment from *Ret* and *Ref* to *Xtra*. These are in simulation through $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$ by assumption, and determine a step of *Univ* as before. The conjunction of all the facts established along the way, through both *Ret* and *Ref*, then establishes the simulation between the *Univ* and *Xtra* steps through (91)–(94). The $Op \in \mathsf{Ops}_{X \setminus FX}$ case is a simplification of the analogous case in (2).(ii) because of the simpler structure of the retrieve relation here – it is sufficient to rely on the truth of $K^{\bullet}$ and $K^{\sim}$, without having to worry about whether $H^{\bullet}$ and $H^{\sim}$ do or do not hold for particular values of w.

This completes the proof of part (2).

(3) Note that *Univ* itself satisfies the criteria required for *Xtra*. Therefore, if we have a system *Univ** with the properties (1) and (2) of *Univ*, then *Univ** also satisfies the criteria required for *Xtra*. Hence, we can construct two instances of Figure 5 as follows:

(a) In the first, *Univ* is in its conventional place and *Univ** replaces *Xtra*, and there are refinement data K°,R°,V° and retrenchment data H°,Q°,N°,D° from *Univ* to *Univ**.

(b) In the second, *Univ** replaces *Univ*, and *Univ* replaces *Xtra*, and there are refinement data K^{*},R^{*},V^{*} and retrenchment data H^{*},Q^{*},N^{*},D^{*} from *Univ** to *Univ*.

So *Univ* and *Univ** are inter-simulable by the arguments above.

(4) We just observe that disjunctive fusion composition of retrenchments, and the vertical composition between retrenchments and refinements (both ways round) are sound composition mechanisms. For the record, the composed retrenchment data is

$$G(u,t) \equiv (t = (\underline{u},v,w) \wedge \{[H(u,v) \wedge K(\underline{u},w)] \vee [K(u,w) \wedge H(\underline{u},v)]\}) \tag{95}$$

$$\begin{aligned} &P_{Op}(i,h,u,t) \\ &\qquad \equiv (h = (\underline{i},j,k) \wedge t = (\underline{u},v,w) \wedge \\ &\qquad\qquad \{[K(\underline{u},w) \wedge R_{Op}(\underline{i},k) \wedge H(u,v) \wedge Q_{Op}(i,j,u,v)] \vee \\ &\qquad\qquad\quad [K(u,w) \wedge R_{Op}(i,k) \wedge H(\underline{u},v) \wedge Q_{Op}(\underline{i},j,\underline{u},v)]\}) \end{aligned} \tag{96}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

$$\begin{aligned}
&O_{Op}(o,n;u',t',i,h,u,t)\\
&\quad\equiv (t=(\underline{u},v,w)\wedge h=(\underline{i},j,k)\wedge\\
&\qquad t'=(\underline{u}',v',w')\wedge n=(\underline{o},p,q)\wedge\\
&\qquad \{[H(\underline{u}',v')\wedge K(u,w)\wedge R_{Op}(i,k)\wedge K(u',w')\wedge\\
&\qquad\quad V_{Op}(o,q)\wedge N_{Op}(\underline{o},p;\underline{u}',v',\underline{i},j,\underline{u},v)]\vee\\
&\qquad [H(u',v')\wedge K(\underline{u},w)\wedge R_{Op}(\underline{i},k)\wedge K(\underline{u}',w')\wedge\\
&\qquad\quad V_{Op}(\underline{o},q)\wedge N_{Op}(o,p;u',v',i,j,u,v)]\vee\\
&\qquad [K(u,w)\wedge R_{Op}(i,k)\wedge K(u',w')\wedge\\
&\qquad\quad V_{Op}(o,q)\wedge N_{Op}(\underline{o},p;\underline{u}',v',\underline{i},j,\underline{u},v)\wedge\\
&\qquad\quad N_{Op}(o,p;u'v',i,j,u,v)\wedge K(\underline{u},w)\wedge\\
&\qquad\quad R_{Op}(\underline{i},k)\wedge K(\underline{u}',w')\wedge V_{Op}(\underline{o},q)]\})
\end{aligned} \tag{97}$$

$$\begin{aligned}
&C_{Op}(u',t',o,n;i,h,u,t)\\
&\quad\equiv(t=(\underline{u},v,w)\wedge h=(\underline{i},j,k)\wedge\\
&\qquad t'=(\underline{u}',v',w')\wedge n=(\underline{o},p,q)\wedge\\
&\qquad \{[D_{Op}(u',v',o,p;i,j,u,v)\wedge K(\underline{u},w)\wedge\\
&\qquad\quad R_{Op}(\underline{i},k)\wedge K(\underline{u}',w')\wedge V_{Op}(\underline{o},q)]\vee\\
&\qquad [K(u,w)\wedge R_{Op}(i,k)\wedge K(u',w')\wedge\\
&\qquad\quad V_{Op}(o,q)\wedge D_{Op}(\underline{u}',v',\underline{o},p;\underline{i},j,\underline{u},v)]\}).
\end{aligned} \tag{98}$$

For the rest of the theorem, we will work under the additional assumptions given in the statement of (5) and (6).

(5) We need to show that the retrenchment data in (91)–(94) supports an actual retrenchment from *Univ* to *Xtra*. So we must prove that the initialisation PO and the retrenchment operation PO both hold with (91)–(94).
For the initialisation PO, we assume $Init_X(t^{\sim\prime})$ and need to find a t' such that

$$Init_U(t')\wedge HK^{\circ}(t',t^{\sim\prime})$$

holds. Since $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ is a refinement, there is a v' for which

$$Init_T(v')\wedge K^{\sim}(v',t^{\sim\prime})$$

holds. Also, since $H^{\sim}$, $Q^{\sim}$,$N^{\sim}$,$D^{\sim}$ is a retrenchment, there is a w' for which

$$Init_F(w')\wedge H^{\sim}(w',t^{\sim\prime})$$

holds. Since we have

$$K^{\sim}(v',t^{\sim\prime})\wedge H^{\sim}(w',t^{\sim\prime}),$$

we also have $G^{\times}(v',w')$ by assumption. So there is a u' such that

$$H(u',v')\wedge K(u',w')$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

holds by (80), so, for this u', we have

$$K^{\bullet}(v',t') \wedge H^{\bullet}(w',t')$$

holds, where $t' = (u',v',w')$. So we have $Init_U(t')$ by (82). We have now established

$$K^{\bullet}(v',t') \wedge K^{\sim}(v',t^{\sim\prime}) \wedge H^{\bullet}(w',t') \wedge H^{\sim}(w',t^{\sim\prime}),$$

which, with $t' = (u',v',w')$, gives both disjuncts of $HK^{\circ}(t',t^{\sim\prime})$. So we are done.

For the operation PO, we consider the two cases separately:

— Case $Op \in \mathsf{Ops}_{FX}$:
We assume

$$HK^{\circ}(t,t^{\sim}) \wedge QR^{\circ}_{Op}(h,h^{\sim},t,t^{\sim}) \wedge stp_{Op_X}(t^{\sim},h^{\sim},t^{\sim\prime},n^{\sim}).$$

We need a *Univ* step $t \text{ -}(h,Op_U,n)\twoheadrightarrow t'$ such that

$$((HK^{\circ}(t',t^{\sim\prime}) \wedge NV^{\circ}_{Op}(n,n^{\sim};t',t^{\sim\prime},h,h^{\sim},t,t^{\sim})) \vee \\ DV^{\circ}_{Op}(t',t^{\sim\prime},n,n^{\sim};h,h^{\sim},t,t^{\sim}))$$

holds. Suppose $t = (u,v,w)$ and $h = (i,j,k)$. Our assumption

$$HK^{\circ}(t,t^{\sim}) \wedge QR^{\circ}_{Op}(h,h^{\sim},t,t^{\sim})$$

gives us

$$K^{\sim}(v,t^{\sim}) \wedge R^{\sim}{}_{Op}(j,h^{\sim}).$$

Since $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ is a refinement, from $stp_{Op_X}(t^{\sim},h^{\sim},t^{\sim\prime},n^{\sim})$, we can get a *Ret* step, say $v \text{ -}(j,Op_T,p)\twoheadrightarrow v'$, such that

$$K^{\sim}{\wedge}R^{\sim}{}_{Op}{\wedge}K^{\sim\prime}{\wedge}V^{\sim}{}_{Op}$$

holds. Also, since

$$HK^{\circ}(t,t^{\sim}) \wedge QR^{\circ}_{Op}(h,h^{\sim},t,t^{\sim})$$

gives us

$$H^{\sim}(w,t^{\sim}) \wedge Q^{\sim}{}_{Op}(k,h^{\sim},w,t^{\sim}).$$

Since $H^{\sim}$,$Q^{\sim}$,$N^{\sim}$,$D^{\sim}$ is a retrenchment, we get a *Ref* step, say $w \text{ -}(k,Op_F,q)\twoheadrightarrow w'$, such that

$$H^{\sim}{\wedge}Q^{\sim}{}_{Op}{\wedge}((H^{\sim\prime}{\wedge}N^{\sim}{}_{Op}){\vee}D^{\sim}{}_{Op})$$

holds. Since

$$K^{\sim}{\wedge}R^{\sim}{}_{Op}{\wedge}K^{\sim\prime}{\wedge}V^{\sim}{}_{Op}$$

together with

$$H^{\sim}{\wedge}Q^{\sim}{}_{Op}{\wedge}((H^{\sim\prime}{\wedge}N^{\sim}{}_{Op}){\vee}D^{\sim}{}_{Op})$$

leads to

$$G^{\times}{,}G^{\times}{\wedge}P^{\times}{,}O^{\times}{,}C^{\times}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

as we saw above, which is witnessed by some *Abs* values $\underline{u}, \underline{i}, u', o$, the two *Ret* and *Ref* steps produce a *Univ* step, say $\underline{t}\,\text{-}(\underline{h}, Op_U, n)\!\twoheadrightarrow t'$, for which

$$HK^{\circ} \wedge QR^{\circ}_{Op} \wedge ((HK^{\circ\prime} \wedge NV^{\circ}_{Op}) \vee DV^{\circ}_{Op})$$

holds, as in the proof of (2).(v), where we have

$$\underline{t} = (\underline{u}, v, w)$$
$$\underline{h} = (\underline{i}, j, k).$$

To establish the retrenchment, it is now enough to show that we can safely replace $\underline{u}$ and $\underline{i}$ by the u and i we assumed to start with.
We now note that either

$$HK^{\circ} \wedge QR^{\circ}_{Op} \wedge HK^{\circ\prime} \wedge NV^{\circ}_{Op}$$

or

$$HK^{\circ} \wedge QR^{\circ}_{Op} \wedge DV^{\circ}_{Op}$$

holds. If the first of these holds, then, unravelling the assumed $HK^{\circ} \wedge QR^{\circ}_{Op}$ for t, h, and unravelling

$$HK^{\circ} \wedge QR^{\circ}_{Op} \wedge HK^{\circ\prime} \wedge NV^{\circ}_{Op}$$

for $\underline{t}, \underline{h}, t', n$, we see that we have the assumptions of (69). This allows us to replace $\underline{u}, \underline{i}$, by u, i, in

$$HK^{\circ} \wedge QR^{\circ}_{Op} \wedge HK^{\circ\prime} \wedge NV^{\circ}_{Op}$$

(and in the *Univ* step $\underline{t}\,\text{-}(\underline{h}, Op_U, n)\!\twoheadrightarrow t'$) as desired, completing the argument.
The argument for the $HK^{\circ} \wedge QR^{\circ}_{Op} \wedge DV^{\circ}_{Op}$ case is similar, but using (70) instead of (69).

— Case $Op \in \mathsf{Ops}_{X \backslash FX}$:
We assume

$$HK^{\circ}(t, t^{\sim}) \wedge QR^{\circ}_{Op}(h, h^{\sim}, t, t^{\sim}) \wedge stp_{Op_X}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim}).$$

It will be enough to find a *Univ* step $t\,\text{-}(h, Op_U, n)\!\twoheadrightarrow t'$ such that

$$HK^{\circ}(t', t^{\sim\prime}) \wedge NV^{\circ}_{Op}(n, n^{\sim}; t', t^{\sim\prime}, h, h^{\sim}, t, t^{\sim})$$

holds. The assumption

$$HK^{\circ}(t, t^{\sim}) \wedge QR^{\circ}_{Op}(h, h^{\sim}, t, t^{\sim})$$

yields

$$K^{\sim}(v, t^{\sim}) \wedge R^{\sim}{}_{Op}(j, h^{\sim})$$

for suitable v and j. Since $K^{\sim}, R^{\sim}, V^{\sim}$ is a refinement, from $stp_{Op_X}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})$, we can get a *Ret* step, say $v\,\text{-}(j, Op_T, p)\!\twoheadrightarrow v'$, such that

$$K^{\sim} \wedge R^{\sim}{}_{Op} \wedge K^{\sim\prime} \wedge V^{\sim}{}_{Op}$$

holds. If we now fix $n = p$ for the *Univ* step, then noting that

$$V^{\bullet}_{Op}(p, n) \equiv (p = n),$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

and that $V^{\sim}{}_{Op}(p,n^{\sim})$ holds, we can deduce $NV^{\circ}_{Op}(\ldots)$, since $NV^{\circ}_{Op}(\ldots)$ is

$$V^{\bullet}_{Op}(p,n) \wedge V^{\sim}{}_{Op}(p,n^{\sim}).$$

We now have to find t' to show that $HK^{\circ}(t',t^{\sim\prime})$ holds and to show that t,h,t',n constitute a *Univ* step. For the retrieve relation, we already have $K^{\sim}(v',t^{\sim\prime})$. So if we choose u',w' such that $K(u',w')$ holds, then by (73), $K^{\bullet}(v',t')$ also holds, where $t' = (u',v',w')$, and this yields $HK^{\circ}(t',t^{\sim\prime})$ through the second disjunct of (91). Finally, to show that t,h,t',n constitute a *Univ* step, we note that, by (83), we just need

$$K^{\bullet} \wedge R^{\bullet}_{Op} \wedge K^{\bullet\prime} \wedge V^{\bullet}_{Op}.$$

But we have $K^{\bullet} \wedge R^{\bullet}_{Op}$ from $HK^{\circ} \wedge QR^{\circ}_{Op}$, and have deduced $K^{\bullet\prime} \wedge V^{\bullet}_{Op}$, so we are done.

(6) (i) We start with the refinement data $KK^{\circ}, RR^{\circ}, VV^{\circ}$, which is given by (99)–(102):

$$KK^{\circ}(t,t^{\sim}) \equiv HK^{\circ}(t,t^{\sim}) \vee ZZ^{\circ}(t,t^{\sim}) \tag{99}$$

where

$$\begin{aligned} ZZ^{\circ}(t,t^{\sim}) \equiv\ & (\exists \underline{t}^{\sim}, h^{\sim}, n^{\sim} \bullet stp_{Op_X}(\underline{t}^{\sim}, h^{\sim}, t^{\sim}, n^{\sim})) \wedge \\ & \neg(\exists \underline{t} \bullet HK^{\circ}(\underline{t}, t^{\sim})) \wedge \\ & (\exists \underline{t}, \underline{t}^{\sim}, h, h^{\sim}, n, n^{\sim} \bullet DV^{\circ}_{Op}(t, t^{\sim}, n, n^{\sim}; h, h^{\sim}, \underline{t}, \underline{t}^{\sim})) \end{aligned} \tag{100}$$

$$RR^{\circ}(h,h^{\sim}) \equiv (\forall t, t^{\sim} \bullet HK^{\circ}(t,t^{\sim}) \Rightarrow QR^{\circ}_{Op}(h,h^{\sim},t,t^{\sim})) \tag{101}$$

$$\begin{aligned} VV^{\circ}(n,n^{\sim}) \equiv (\exists t, t^{\sim}, h, h^{\sim}, t', t^{\sim\prime} \bullet & \\ & NV^{\circ}_{Op}(n,n^{\sim};t',t^{\sim\prime},h,h^{\sim},t,t^{\sim}) \vee \\ & DV^{\circ}_{Op}(t',t^{\sim\prime},n,n^{\sim};h,h^{\sim},t,t^{\sim})). \end{aligned} \tag{102}$$

In order to prove the refinement, we begin with the initialisation PO, which follows along much the same lines as the analogous PO for the retrenchment $HK^{\circ}, QR^{\circ}, NV^{\circ}, DV^{\circ}$ given in part (5).
For the operation PO, we assume

$$KK^{\circ}(t,t^{\sim}) \wedge RR^{\circ}_{Op}(h,h^{\sim}) \wedge stp_{Op_X}(t^{\sim},h^{\sim},t^{\sim\prime},n^{\sim}),$$

and need to prove there are values t',n such that $stp_{Op_U}(t,h,t',n)$ and

$$KK^{\circ\prime} \wedge VV^{\circ}_{Op}$$

hold. To begin, we note that by the assumptions of part (2), every step of *Xtra* is in simulation with at least one step of *Ret*. Therefore, every before state of an *Xtra* transition is related to some *Univ* state through HK°, and, consequently, no before state of an *Xtra* transition can be in the range of ZZ° because of the middle conjunct of (100). Thus, from

$$KK^{\circ}(t,t^{\sim}) \wedge RR^{\circ}_{Op}(h,h^{\sim}),$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

we can deduce that

$$HK^{\circ}(t,\tilde{t}) \wedge QR^{\circ}_{Op}(h,\tilde{h},t,\tilde{t}) \wedge stp_{Op_X}(\tilde{t},\tilde{h},\tilde{t}',\tilde{n})$$

covers all the ways of making the operation PO hypothesis true. But this is the hypothesis of the operation PO for the HK°,QR°,NV°,DV° retrenchment, so we can deduce

$$(HK^{\circ\prime} \wedge NV^{\circ}_{Op}) \vee DV^{\circ}_{Op}.$$

We consider two cases:

— $HK^{\circ\prime} \wedge NV^{\circ}_{Op}$ holds:
  Then so does $KK^{\circ\prime} \wedge VV^{\circ}_{Op}$ (since $HK^{\circ\prime}$ is a disjunct of $KK^{\circ\prime}$ and NV°_{Op} is a disjunct of VV°_{Op}), and we are done.

— $HK^{\circ\prime} \wedge NV^{\circ}_{Op}$ does not hold:
  Then we must have that

$$DV^{\circ}_{Op}(t',\tilde{t}',n,\tilde{n};h,\tilde{h},t,\tilde{t})$$

  holds instead. In that case, either $\tilde{t}'$ is in the range of HK° or it is not:

  - If it is, we use (71) to deduce $HK^{\circ}(t',\tilde{t}')$ (after which we get $KK^{\circ}(t',\tilde{t}')$ through (99)), and then use (102) to deduce $VV^{\circ}_{Op}(n,\tilde{n})$, and we are done.
  - Otherwise, $\tilde{t}'$ is not in the range of HK° and we use (100) to deduce $ZZ^{\circ}(t',\tilde{t}')$ (after which we get $KK^{\circ}(t',\tilde{t}')$ through (99)), and then use (102) to deduce $VV^{\circ}_{Op}(n,\tilde{n})$, and again we are done.

(ii) We just note that the condition stated in (42) is just the requirement from (13), so we are done.

(7) The proof is just a matter of replaying the arguments given for part (3), but using the stronger relationships between *Univ* and *Xtra* afforded by the stronger assumptions in force. □

8.1. *Remarks*

Some of the following are similar to the corresponding remarks made earlier, so are only stated briefly; new observations related to the postjoin construction are discussed in more detail.

Remark 8.2. Observing that (given our formulation of refinement and retrenchment), every refinement K,R,V yields a retrenchment K,R,V,false, simply by reinterpreting the input and output relations in the obvious way, and adding a trivial concession (see Banach *et al.* (2007b) for a more extensive discussion), we can see that we could readily have extended the retrenchment data H°,Q°,N°,D° in (2).(ii) of the theorem to all operations simply by reinterpreting the refinement data K°,R°,V° from (2).(i) and adding a false concession. However, while valid, this would not have been very interesting. Another way of achieving the same thing would have been to consider the pseudoretrenchment data

$$H^{\circ} \vee K^{\circ}, Q^{\circ} \vee R^{\circ}, N^{\circ} \vee V^{\circ}, D^{\circ}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

instead. This would have worked for the stated claim in (2).(ii) because that claim only mentions the simulation relation (permitting the choice of the most convenient disjunct from the enlarged relations for each case). The main reason this approach was not pursued for (2).(ii) was that it would have spoiled the relative cleanness of the composition results in (2).(iv).

The same approach to simulation would also have worked for the simulation relation of the data in (2).(v), but we avoided it to avoid excessive clutter. However, the approach would not have worked for the retrenchment claim in (5) since there we need to prove the result for every way of satisfying the hypotheses, and the disjunctions introduce additional cases, which are not provable without additional assumptions. However, the approach based on overriding that we adopted avoids all these difficulties, though at the price of a little more complexity.

Remark 8.3. As a corollary, we note that if the vertical composition of concessions in (90) had satisfied the conditions of being compatibly tidy (in the terminology of Banach and Jeske (2010)), then we could have strengthened the

$$D^{\bullet} \fatsemi D^{\circ} \Leftarrow D^{\sim}$$

implication in (2).(iv) to an equality since the other two disjuncts of D° would have been absent. We again omitted the details to avoid excessive clutter.

Remark 8.4. In part (4) of the theorem, we highlighted disjunctive fusion composition, since it is valid without restriction. The corresponding conjunctive composition is not as generally applicable (it requires a ‘close to cosimulation’ criterion to hold), which is not true in general under our hypotheses – see Banach *et al.* (2008) for details. The easiest way to get the required criterion is to require that the *Abs* system is deterministic, that is, that there is a unique after state and output for each before state and input. An alternative involves the use of conditions like (69) and (70), but this time permitting the replacement of after states and outputs rather than before states and inputs. We have omitted the details.

Remark 8.5. As in earlier remarks, the composition of K^{*},R^{*},V^{*} with K°,R°,V° need not be the identity; still less the composition of H°,Q°,N°,D° and H^{*},Q^{*},N^{*},D^{*}.

Remark 8.6. It is tempting to think that[†] the construction of *Univ* should involve the free use of the components of *Ret* and *Ref* alone (with *Univ* expected to play a more veiled role, with its components typically existentially bound). The treatment in Jeske (2005) was developed from this point of view, and shows just how arduous it is to obtain a postjoin result from such a perspective. More seriously, that treatment required numerous restrictions to hold, and was tied to a particular use of APP$_{Op}$ sets, something that a general account should strive to avoid if at all possible – all this certainly left the authors

[†] The translation is again ‘For a long time the authors thought’.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

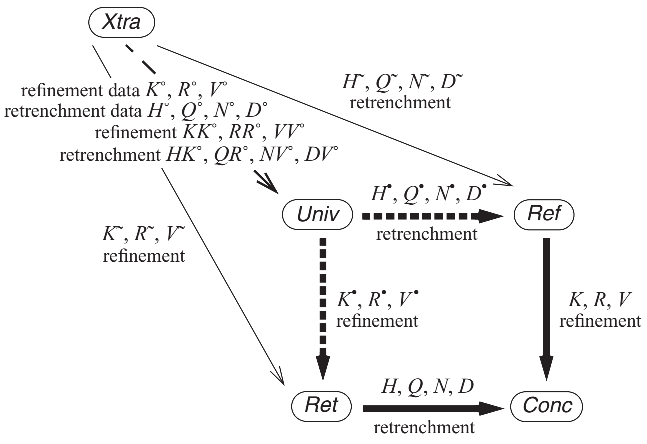
Xtra
refinement data K°, R°, V°
retrenchment data H°, Q°, N°, D°
refinement KK°, RR°, VV°
retrenchment HK°, QR°, NV°, DV°
$H^{\sim}$, $Q^{\sim}$, $N^{\sim}$, $D^{\sim}$
retrenchment
$K^{\sim}$, $R^{\sim}$, $V^{\sim}$
refinement
Univ
$H^{\bullet}$, $Q^{\bullet}$, $N^{\bullet}$, $D^{\bullet}$
retrenchment
Ref
$K^{\bullet}$, $R^{\bullet}$, $V^{\bullet}$
refinement
K, R, V
refinement
Ret
H, Q, N, D
retrenchment
Conc

Fig. 6. The prejoin construction in detail – the pseudoretrenchment $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$ (not shown) connects *Ret* to *Ref*.

thinking that 'there must be a better way'. The clean, unrestricted and general nature of the construction of Theorem 8.1 confirms that the authors' earlier beliefs about the structure of the *Univ* system were less than ideal, and that a reappraisal of the whole issue, undertaken, as here, with the wisdom of hindsight, was thoroughly justified.

9. The Prejoin Theorem

In this section, we consider the Prejoin Theorem in detail. The relevant part of Figure 2 is elaborated in Figure 6. The given systems are *Ret* and *Ref*, together with a system *Conc*. There is a retrenchment from *Ret* to *Conc* and a refinement from *Ref* to *Conc*, the data for these being adapted from the usual notation (note that because of the geometrical arrangement of the three systems, our previous notational conventions cannot be fully maintained, so care should be taken to allow for the differences). The constructed system is *Univ*, with a retrenchment from *Univ* to *Ref* and a refinement from *Univ* to *Ret*. The universal nature of the relationship between *Univ* and the other systems can be expressed by saying that whenever there is a system *Xtra* enjoying similar properties to *Univ*, then *Xtra* is more abstract than *Univ*, which is witnessed by 'in simulation' relationships between the transitions of *Xtra* and *Univ* that can be strengthened under relatively benign conditions to a retrenchment – and still further to a refinement – from *Xtra* to *Univ*.

In contrast to our preceding results, which assumed arbitrary refinements and retrenchments in their hypotheses, for Theorem 9.1, we will need a mild additional assumption about the hypothesised retrenchment. For this, we will revert to the notation of Section 3 and say that a retrenchment G,P,O,C is accommodating if and only if

$$\begin{aligned} & G(u,v) \wedge P_{Op}(i,j,u,v) \Rightarrow \\ & \qquad \exists u',v',o,p \bullet ((G(u',v') \\ & \qquad \wedge O_{Op}(o,p;u',v',i,j,u,v)) \\ & \qquad \vee C_{Op}(u',v',o,p;i,j,u,v)). \end{aligned} \tag{103}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

Note that any retrenchment may be made accommodating by weakening the concession sufficiently.

Theorem 9.1. Let *Ret* (with variables v, j, p, operation names Ops_T) and *Ref* (with variables w, k, q, operation names Ops_F) and *Conc* (with variables u, i, o, operation names Ops_C) be three systems. Let there be a retrenchment from *Ret* to *Conc* with retrenchment data

$$H, \{Q_{Op}, N_{Op}, D_{Op} | Op \in \mathsf{Ops}_{TC}\}$$

where Ops_{TC} is the set of common names of related operations of *Ret* and *Conc*. Let there be a refinement from *Ref* to *Conc* with refinement data

$$K, \{R_{Op}, V_{Op} | Op \in \mathsf{Ops}_F = \mathsf{Ops}_C\}$$

where Ops_F is the set of operation names of both *Ref* and *Conc*. Suppose, for all Op, that $H \wedge Q_{Op}$ is a non-empty relation, and that the retrenchment is accommodating. Then:

(1) There is a system *Univ* (with variables t, h, n), with operation name set Ops_U, where $\mathsf{Ops}_U = \mathsf{Ops}_T$, such that:

(i) there is a refinement from *Univ* to *Ret* with refinement data, say

$$K^{\bullet}(t, v), \{R^{\bullet}_{Op}, V^{\bullet}_{Op} | Op \in \mathsf{Ops}_U = \mathsf{Ops}_T\};$$

(ii) there is a retrenchment from *Univ* to *Ref* with retrenchment data, say

$$H^{\bullet}(t, w), \{Q^{\bullet}_{Op}, N^{\bullet}_{Op}, D^{\bullet}_{Op} | Op \in \mathsf{Ops}_{UF}\};$$

(iii) composing the retrenchment H,Q,N,D with the pseudrefinement K^T,R^T,V^T gives a pseudoretrenchment $G^{\times},G^{\times}\wedge P^{\times},O^{\times},C^{\times}$, which is also given by composing the pseudrefinement $K^{\bullet T},R^{\bullet T},V^{\bullet T}$ with the retrenchment $H^{\bullet},Q^{\bullet},N^{\bullet},D^{\bullet}$;

(iv) each transition of *Univ* is in simulation with a transition of *Ret*, or with a transition of *Ref*, or both, and in the last case, any such pair of *Ret* and *Ref* transitions are in simulation through the pseudoretrenchment $G^{\times},G^{\times}\wedge P^{\times},O^{\times},C^{\times}$;

(v) if the notion of refinement in question requires the use of $\textsc{app}_{Op}$ sets, then the $\textsc{app}_{Op}$ sets of *Univ* are given by

$$\textsc{app}_{Op_U}(t, h) \equiv (\exists v, j \bullet K^{\bullet}(t, v) \wedge R^{\bullet}_{Op}(h, j) \wedge \textsc{app}_{Op_T}(v, j)). \tag{104}$$

(2) If

— we have a system *Xtra* (with variables $t^{\sim}, h^{\sim}, n^{\sim}$),

— with operation name set Ops_X where $\mathsf{Ops}_X = \mathsf{Ops}_T$,

— with a refinement from *Xtra* to *Ret* given by $K^{\sim},R^{\sim},V^{\sim}$,

— with a retrenchment from *Xtra* to *Ref* given by $H^{\sim},Q^{\sim},N^{\sim},D^{\sim}$,

— where the composition of the pseudorefinement $K^{\sim T},R^{\sim T},V^{\sim T}$ with the retrenchment $H^{\sim},Q^{\sim},N^{\sim},D^{\sim}$ yields the pseudoretrenchment $G^{\times},G^{\times}\wedge P^{\times},O^{\times},C^{\times}$,

— where each transition of *Xtra* is in simulation with a transition of *Ret*, with a transition of *Ref*, or both, and where in the last case any such pair of *Ret* and *Ref* transitions are in simulation through the pseudoretrenchment $G^{\times},G^{\times}\wedge P^{\times},O^{\times},C^{\times}$,

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

then:

(i) There exist refinement data, say

$$K^{\circ}(t^{\sim}, t), \{R^{\circ}_{Op}, V^{\circ}_{Op} | Op \in \mathsf{Ops}_U\},$$

from *Xtra* to *Univ*, through which every transition of *Xtra* that is in simulation with a transition of *Ret* is in simulation with a transition of *Univ*.

(ii) There exist retrenchment data, say

$$H^{\circ}(t^{\sim}, t), \{Q^{\circ}_{Op}, N^{\circ}_{Op}, D^{\circ}_{Op} | Op \in \mathsf{Ops}_U\},$$

from *Xtra* to *Univ*, through which every transition of *Xtra* that is in simulation with a transition of *Ref* is in simulation with a transition of *Univ*.

(iii) We have

$$K^{\circ} \fatsemi K^{\bullet} = K^{\sim}$$
$$R^{\circ} \fatsemi R^{\bullet} = R^{\sim}$$
$$V^{\circ} \fatsemi V^{\bullet} = V^{\sim}.$$

(iv) We have

$$H^{\circ} \fatsemi H^{\bullet} = H^{\sim}$$

and for $Op_X \in \mathsf{Ops}_{XF}$,

$$(H^{\circ} \wedge Q^{\circ}) \fatsemi (H^{\bullet} \wedge Q^{\bullet}) = (H^{\sim} \wedge Q^{\sim})$$
$$N^{\circ} \fatsemi N^{\bullet} = N^{\sim}$$
$$D^{\circ} \fatsemi D^{\bullet} \Leftarrow D^{\sim}.$$

(v) There exist retrenchment data, say

$$HK^{\circ}(t^{\sim}, t), \{QR^{\circ}_{Op}, NV^{\circ}_{Op}, DV^{\circ}_{Op} | Op \in \mathsf{Ops}_U\},$$

from *Xtra* to *Univ*, through which every transition of *Xtra* that is in simulation with a transition of *Ret* or in simulation with a transition of *Ref* is in simulation with a transition of *Univ*.

(3) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are inter-simulable.

(4) There is a retrenchment from to *Univ* to *Conc* with retrenchment data, say

$$G(t, u), \{P_{Op}, O_{Op}, C_{Op} | Op \in \mathsf{Ops}_{UC}\},$$

given by the disjunctive fusion composition of two retrenchments (a) and (b), where:

(a) is the vertical composition of $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$ with K, R, V;

(b) is the vertical composition of $K^{\bullet}, R^{\bullet}, V^{\bullet}$ with H, Q, N, D.

(5) There is a retrenchment from *Xtra* to *Univ* with retrenchment data, say

$$HH^{\circ}(t^{\sim}, t), \{QQ^{\circ}_{Op}, NN^{\circ}_{Op}, DD^{\circ}_{Op} | Op \in \mathsf{Ops}_U\};$$

(6) Referring to the data given in (5), if

$$
\begin{aligned}
&((\exists t^{\sim}, h^{\sim}, n^{\sim} \bullet stp_{Op_X}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})) \wedge \\
&\ (\exists t^{\sim}, t, h^{\sim}, h, n^{\sim}, n \bullet DD^{\circ}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t))) \Rightarrow HH^{\circ}(t^{\sim\prime}, t'),
\end{aligned}
\tag{105}
$$

then:

(i) the retrenchment of (5) from *Xtra* to *Univ*, strengthens to a refinement with refinement data, say

$$KK^{\circ}(t^{\sim}, t), \{RR^{\circ}_{Op}, VV^{\circ}_{Op} | Op \in \mathsf{Ops}_U\};$$

(ii) if the notion of refinement in question requires the use of $\textsc{app}_{Op}$ sets, then the $\textsc{app}_{Op}$ sets of *Xtra* need to satisfy

$$
\begin{aligned}
&\textsc{app}_{Op_U}(t, h) \wedge KK^{\circ}(t^{\sim}, t) \wedge RR^{\circ}_{Op}(h^{\sim}, h) \overset{\Leftarrow}{\Rightarrow} \\
&\qquad\qquad KK^{\circ}(t^{\sim}, t) \wedge RR^{\circ}_{Op}(h^{\sim}, h) \wedge \textsc{app}_{Op_X}(t^{\sim}, h^{\sim}).
\end{aligned}
\tag{106}
$$

(7) If a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are inter-retrenchable, and if the property noted in (105) also holds, then they are also inter-refinable.

Proof.

(1) We will begin by completing the details of the refinement $K^{\bullet}, R^{\bullet}, V^{\bullet}$ and the retrenchment $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$. Adapting the usual conventions for *Ret* and *Ref*, the state space of *Univ* is $t \in \mathsf{T} = \mathsf{U} \times \mathsf{V} \times \mathsf{W}$ (where U is the state space of *Conc*, V is the state space of *Ret* and W is the sate space of *Ref*). There are two cases for the input and output spaces of *Univ* :

— If $Op \in \mathsf{Ops}_{UF} = \mathsf{Ops}_{TC}$, then

$$
\begin{aligned}
h &\in \mathsf{H}_{Op} = \mathsf{I}_{Op} \times \mathsf{J}_{Op} \times \mathsf{K}_{Op} \\
n &\in \mathsf{N}_{Op} = \mathsf{O}_{Op} \times \mathsf{P}_{Op} \times \mathsf{Q}_{Op}.
\end{aligned}
$$

— If $Op \in \mathsf{Ops}_{U \setminus UF}$, then

$$
\begin{aligned}
h &\in \mathsf{H}_{Op} = \mathsf{J}_{Op} \\
n &\in \mathsf{N}_{Op} = \mathsf{P}_{Op}.
\end{aligned}
$$

The refinement $K^{\bullet}, R^{\bullet}, V^{\bullet}$ is given by the data

$$K^{\bullet}(t, v) \equiv (t = (u, v, w) \wedge K(w, u)) \tag{107}$$

$$
R^{\bullet}_{Op}(h, j) \equiv \begin{cases} (h = (i, j, k) \wedge R_{Op}(k, i)) & \text{if } Op \in \mathsf{Ops}_{UF} \\ (h = j) & \text{if } Op \in \mathsf{Ops}_{U \setminus UF} \end{cases}
\tag{108}
$$

$$
V^{\bullet}_{Op}(n, p) \equiv \begin{cases} (n = (o, p, q) \wedge V_{Op}(q, o)) & \text{if } Op \in \mathsf{Ops}_{UF} \\ (n = p) & \text{if } Op \in \mathsf{Ops}_{U \setminus UF}. \end{cases}
\tag{109}
$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

The retrenchment $H^\bullet$,$Q^\bullet$,$N^\bullet$,$D^\bullet$ is given by the data

$$H^\bullet(t,w) \equiv (t=(u,v,w) \wedge H(u,v)) \tag{110}$$

$$Q^\bullet_{Op}(h,k,t,w) \equiv (h=(i,j,k) \wedge t=(u,v,w) \wedge Q_{Op}(j,i,v,u)) \tag{111}$$

$$\begin{aligned} N^\bullet_{Op}(n,q;t',w',h,k,t,w) \equiv (&t'=(u',v',w') \wedge n=(o,p,q) \wedge \\ &h=(i,j,k) \wedge t=(u,v,w) \wedge \\ &N_{Op}(p,o;v',u',j,i,v,u)) \end{aligned} \tag{112}$$

$$\begin{aligned} D^\bullet_{Op}(t',w',n,q;h,k,t,w) \equiv (&t'=(u',v',w') \wedge n=(o,p,q) \wedge \\ &h=(i,j,k) \wedge t=(u,v,w) \wedge \\ &D_{Op}(v',u',p,o;j,i,v,u)). \end{aligned} \tag{113}$$

Since we need these relations to define the *Univ* system itself, we will begin by checking part (1).(iii) before going on to parts (i) and (ii).

(iii) We first calculate $G^\times$,$G^\times \wedge P^\times$,$O^\times$,$C^\times$ for $Op \in \mathsf{Ops}_{UF}$ as the composition of the retrenchment H,Q,N,D with the pseudorefinement K^T,R^T,V^T. The fact that the result is also equal to the composition of the pseudorefinement $K^{\bullet T}$,$R^{\bullet T}$,$V^{\bullet T}$ with the retrenchment $H^\bullet$,$Q^\bullet$,$N^\bullet$,$D^\bullet$ follows by inspection.

$$\begin{aligned} G^\times(v,w) &\equiv H \fatsemi K^T \\ &= (\exists u \bullet H(v,u) \wedge K(w,u)) \\ &= K^{\bullet T} \fatsemi H^\bullet \end{aligned} \tag{114}$$

$$\begin{aligned} &G^\times \wedge P^\times_{Op} \wedge ((G^{\times\prime} \wedge O^\times_{Op}) \vee C^\times_{Op})(v,w,j,k,v',w',p,q) \\ &\quad \equiv (H \wedge Q_{Op} \wedge ((H' \wedge N_{Op}) \vee D_{Op})) \fatsemi (K^T \wedge R^T_{Op} \wedge K^{T\prime} \wedge V^T_{Op}) \\ &\quad = \exists u,i,u',o \bullet H(v,u) \wedge Q_{Op}(j,i,v,u) \wedge \\ &\qquad\quad ((H(v',u') \wedge N_{Op}(p,o;v',u',j,i,v,u)) \vee \\ &\qquad\qquad D_{Op}(v',u',p,o;j,i,v,u)) \wedge \\ &\qquad\quad K(w,u) \wedge R_{Op}(k,i) \wedge K(w',u') \wedge V_{Op}(q,o) \\ &\quad = (K^{\bullet T} \wedge R^{\bullet T}_{Op} \wedge K^{\bullet T\prime} \wedge V^{\bullet T}_{Op}) \fatsemi (H^\bullet \wedge Q^\bullet_{Op} \wedge ((H^{\bullet\prime} \wedge N^\bullet_{Op}) \vee D^\bullet_{Op})). \end{aligned} \tag{115}$$

The *Univ* system itself is now given as follows. Initialisation in *Univ* is given by

$$\begin{aligned} Init_U(t') \equiv (&t'=(u',v',w') \wedge \\ &\{[Init_T(v') \wedge K^\bullet(t',v')] \vee [Init_F(w') \wedge H^\bullet(t',w')]\}). \end{aligned} \tag{116}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

The operations of Univ are given by

$$stp_{Op_U}(t,h,t',n)$$

$$\equiv \begin{cases} (t=(u,v,w)\wedge h=(i,j,k)\wedge \\ \quad t'=(u',v',w')\wedge n=(o,p,q)\wedge \\ \quad \{[stp_{Op_T}(v,j,v',p)\wedge K^\bullet(t,v)\wedge \\ \qquad R^\bullet_{Op}(h,j)\wedge K^\bullet(t',v')\wedge V^\bullet_{Op}(n,p)]\vee \\ \quad [stp_{Op_F}(w,k,w',q)\wedge H^\bullet(t,w)\wedge \\ \qquad Q^\bullet_{Op}(h,k,t,w)\wedge \\ \qquad ((H^\bullet(t',w')\wedge N^\bullet_{Op}(n,q;t',w',h,k,t,w))\vee \\ \qquad\quad D^\bullet_{Op}(t',w',n,q;h,k,t,w))]\}) & \text{if } Op\in \mathsf{Ops}_{UF} \\ \\ (t=(u,v,w)\wedge h=j\wedge \\ \quad t'=(u',v',w')\wedge n=p\wedge \\ \quad [stp_{Op_T}(v,j,v',p)\wedge K^\bullet(t,v)\wedge \\ \quad R^\bullet_{Op}(h,j)\wedge K^\bullet(t',v')\wedge V^\bullet_{Op}(n,p)]) & \text{if } Op\in \mathsf{Ops}_{U\setminus UF}. \end{cases} \tag{117}$$

(i) We need to check that $K^\bullet$,$R^\bullet$,$V^\bullet$ is a refinement.

For the initialisation PO, suppose we have $Init_T(v')$. We then just need to find w',u' such that $K(w',u')$ holds, and then we can set $t'=(u',v',w')$, after which we will have

$$Init_T(v')\wedge K^\bullet(t',v'),$$

which gives

$$Init_U(t')\wedge K^\bullet(t',v'),$$

thereby discharging the PO.

For the operation PO, we consider the case $Op\in \mathsf{Ops}_{UF}$, and assume

$$K^\bullet(t,v)\wedge R^\bullet_{Op}(h,j)\wedge stp_{Op_T}(v,j,v',p).$$

Then we just need to find w',u' such that $K(w',u')$ holds, and q,o such that $V_{Op}(q,o)$ holds, and then we can set

$$t'=(u',v',w')$$
$$n=(o,p,q),$$

after which we will have enough for the first disjunct in the $Op\in \mathsf{Ops}_{UF}$ case of (117).

The argument for the $Op\in \mathsf{Ops}_{U\setminus UF}$ case is similar.

(ii) We need to check that $H^\bullet$,$Q^\bullet$,$N^\bullet$,$D^\bullet$ is a retrenchment.

For the initialisation PO, suppose we have $Init_F(w')$. Then we just need to find v',u' such that $H(v',u')$ holds, and then we can set

$$t'=(u',v',w'),$$

after which we will have

$$Init_F(w')\wedge H^\bullet(t',w'),$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

which gives

$$Init_U(t') \wedge H^\bullet(t', w'),$$

discharging the PO. For the operation PO, we assume

$$H^\bullet(t, w) \wedge Q^\bullet_{Op}(h, k, t, w) \wedge stp_{Op_F}(w, k, w', q).$$

Then $H^\bullet \wedge Q^\bullet_{Op}$ gives us

$$H(v, u) \wedge Q_{Op}(j, i, v, u).$$

Since the retrenchment H,Q,N,D is accommodating, (103) implies that we can find values v', u', p, o such that

$$(H(v', u') \wedge N_{Op}(p, o; v', u', j, i, v, u)) \vee D_{Op}(v', u', p, o; j, i, v, u)$$

holds, after which we can set

$$\begin{aligned} t' &= (u', v', w') \\ n &= (o, p, q), \end{aligned}$$

and we will then have enough for the second disjunct in the $Op \in \mathsf{Ops}_{UF}$ case of (117).

(iv) It is clear from the arguments above that each step $t \text{-}(h, Op_U, n)\!\!\rightarrow t'$ of *Univ* is either:

— in simulation with (in the refinement sense) its constituent stp_{Op_T} transition if the first disjunct of the $Op \in \mathsf{Ops}_{UF}$ case of (117) holds or we are in the $Op \in \mathsf{Ops}_{U \setminus UF}$ case; or

— in simulation with (in the retrenchment sense) its constituent stp_{Op_F} transition if the second disjunct of the $Op \in \mathsf{Ops}_{UF}$ case of (117) holds.

If both disjuncts hold, then the *Ret* and *Ref* transitions are evidently in simulation through the pseudoretrenchment $G^\times$,$G^\times \wedge P^\times$,$O^\times$,$C^\times$ because of the values of u, i, u', o that are common to the two transitions.

(v) Since $K^\bullet \wedge R^\bullet_{Op}$ is a (partial) function from $\mathsf{T} \times \mathsf{H}_{Op}$ onto $\mathsf{V} \times \mathsf{J}_{Op}$, we have

$$(K^{\bullet T} \wedge R^{\bullet T}_{Op}) \mathbin{⨾} (K^\bullet \wedge R^\bullet_{Op}) = \mathrm{Id}_{\mathsf{V} \times \mathsf{J}_{Op}}.$$

Consequently, the definition of the $\textsc{app}_{Op}$ sets of *Univ* in (104) satisfies the condition in (17) for the $K^\bullet$,$R^\bullet$,$V^\bullet$ refinement, and consequently satisfies an $\textsc{app}_{Op}$ requirement of either the form (11) or (12).

(2) (i) We start with the refinement data K°,R°,V°, which is given by

$$K^\circ(t^\sim, t) \equiv (\exists v \bullet K^\bullet(t, v) \wedge K^\sim(t^\sim, v)) \tag{118}$$

$$R^\circ_{Op}(h^\sim, h) \equiv (\exists j \bullet R^\bullet_{Op}(h, j) \wedge R^\sim{}_{Op}(h^\sim, j)) \tag{119}$$

$$V^\circ_{Op}(n^\sim, n) \equiv (\exists p \bullet V^\bullet_{Op}(n, p) \wedge V^\sim{}_{Op}(n^\sim, p)). \tag{120}$$

We must show that every transition of *Xtra* that is in simulation with a transition of *Ret* is in simulation with a transition of *Univ* through (118)–(120). Suppose

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

we have an *Xtra* step, say $t^{\sim}\text{-}(h^{\sim}, Op_X, n^{\sim})\!\twoheadrightarrow t^{\sim\prime}$, that is in simulation with some step of *Ret*, say $v\text{-}(j, Op_T, p)\!\twoheadrightarrow v'$, through $K^{\sim}, R^{\sim}, V^{\sim}$. Since $K^{\bullet}, R^{\bullet}, V^{\bullet}$ is a refinement, and $K^{\bullet} \wedge R^{\bullet}_{Op}$ is onto $\mathsf{V} \times \mathsf{J}_{Op}$, the step $v\text{-}(j, Op_T, p)\!\twoheadrightarrow v'$ will be in simulation with some step of *Univ*, say $t\text{-}(h, Op_U, n)\!\twoheadrightarrow t'$. Composing the $K^{\bullet}, R^{\bullet}, V^{\bullet}$ simulation with the $K^{\sim}, R^{\sim}, V^{\sim}$ simulation then yields the result.

(ii) We start with the retrenchment data $H^{\circ}, Q^{\circ}, N^{\circ}, D^{\circ}$. This is the vertical composition of the $H^{\sim}, Q^{\sim}, N^{\sim}, D^{\sim}$ and $H^{\bullet T}, Q^{\bullet T}, N^{\bullet T}, D^{\bullet T}$ data, and is given by

$$H^{\circ}(t^{\sim}, t) \equiv (\exists w \bullet H^{\bullet}(t, w) \wedge H^{\sim}(t^{\sim}, w)) \tag{121}$$

$$\begin{aligned} Q^{\circ}_{Op}(h^{\sim}, h, t^{\sim}, t) \equiv (\exists k, w \;\bullet H^{\bullet}(t, w) \wedge H^{\sim}(t^{\sim}, w) \wedge \\ Q^{\bullet}_{Op}(h, k, t, w) \wedge \\ Q^{\sim}{}_{Op}(h^{\sim}, k, t^{\sim}, w)) \end{aligned} \tag{122}$$

$$\begin{aligned} N^{\circ}_{Op}(n^{\sim}, n; t^{\sim\prime}, t', h^{\sim}, h, t^{\sim}, t) \equiv (\exists w, k, w', q \bullet \\ N^{\bullet}_{Op}(n, q; t', w', h, k, t, w) \wedge \\ N^{\sim}{}_{Op}(n^{\sim}, q; t^{\sim\prime}, w', h^{\sim}, k, t^{\sim}, w)) \end{aligned} \tag{123}$$

$$\begin{aligned} D^{\circ}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t) \equiv (\exists w, k, w', q \;\bullet \\ \{[H^{\bullet}(t', w') \wedge N^{\bullet}_{Op}(n, q; t', w', h, k, t, w) \wedge \\ D^{\sim}{}_{Op}(t^{\sim\prime}, w', n^{\sim}, q; h^{\sim}, k, t^{\sim}, w)] \vee \\ [D^{\bullet}_{Op}(t', w', n, q; h, k, t, w) \wedge H^{\sim}(t^{\sim\prime}, w') \wedge \\ N^{\sim}{}_{Op}(n^{\sim}, q; t^{\sim\prime}, w', h^{\sim}, k, t^{\sim}, w)] \vee \\ [D^{\bullet}_{Op}(t', w', n, q; h, k, t, w) \wedge \\ D^{\sim}{}_{Op}(t^{\sim\prime}, w', n^{\sim}, q; h^{\sim}, k, t^{\sim}, w)]\}). \end{aligned} \tag{124}$$

We must show that every transition of *Xtra* that is in simulation with a transition of *Ref* is in simulation with a transition of *Univ* through (121)–(124). Suppose we have an *Xtra* step, say $t^{\sim}\text{-}(h^{\sim}, Op_X, n^{\sim})\!\twoheadrightarrow t^{\sim\prime}$, that is in simulation with some step of *Ref*, say $w\text{-}(k, Op_F, q)\!\twoheadrightarrow w'$, through $H^{\sim}, Q^{\sim}, N^{\sim}, D^{\sim}$. Since, by assumption, $H \wedge Q_{Op}$ is a non-empty relation, $H^{\bullet} \wedge Q^{\bullet}_{Op}$ is necessarily a non-empty (partial) function onto $\mathsf{W} \times \mathsf{K}_{Op}$. Therefore, since $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$ is a retrenchment, the *Ref* transition $w\text{-}(k, Op_F, q)\!\twoheadrightarrow w'$ will be in simulation with some *Univ* step, say $t\text{-}(h, Op_U, n)\!\twoheadrightarrow t'$. Composing the $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$ simulation with the $H^{\sim}, Q^{\sim}, N^{\sim}, D^{\sim}$ simulation now yields the desired result through the distributive law applied to

$$((H^{\sim\prime} \wedge N^{\sim}) \vee D^{\sim}) \wedge ((H^{\bullet\prime} \wedge N^{\bullet}) \vee D^{\bullet}).$$

(iii) Since

$$K^{\circ} = K^{\sim} \fatsemi K^{\bullet T},$$

we have

$$\begin{aligned} K^{\circ} \fatsemi K^{\bullet} &= K^{\sim} \fatsemi K^{\bullet T} \fatsemi K^{\bullet} \\ &= K^{\sim} \fatsemi \mathrm{Id}_{\mathsf{V}} \\ &= K^{\sim} \end{aligned}$$

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

(since $K^{\bullet}$ is a partial function).
The remaining results are similar.

(iv) Since

$$H^{\circ} = H^{\sim} \fatsemi H^{\bullet T},$$

we have

$$\begin{aligned} H^{\circ} \fatsemi H^{\bullet} &= H^{\sim} \fatsemi H^{\bullet T} \fatsemi H^{\bullet} \\ &= H^{\sim} \fatsemi \mathrm{Id}_{\mathsf{W}} \\ &= H^{\sim} \end{aligned}$$

(since $H^{\bullet}$ is a partial function).
The derivation of $N^{\circ} \fatsemi N^{\bullet} = N^{\sim}$ is similar.
Now, consider $D^{\circ} \fatsemi D^{\bullet}$ where D° is given by (124). The term $D^{\sim} \wedge D^{\bullet T}$, which occurs disjunctively in (124), shows that $D^{\circ} \fatsemi D^{\bullet}$ contains

$$\begin{aligned} D^{\sim} \fatsemi D^{\bullet T} \fatsemi D^{\bullet} &= D^{\sim} \fatsemi \mathrm{Id}_{\mathsf{W} \times \mathsf{K}_{Op} \times \mathsf{W} \times \mathsf{Q}_{Op}} \\ &= D^{\sim}. \end{aligned}$$

The other disjuncts in (124) lead to

$$D^{\circ} \fatsemi D^{\bullet} \Leftarrow D^{\sim}.$$

Finally, by assumption, $H \wedge Q$ is a non-empty relation. This makes $H^{\bullet T} \wedge Q^{\bullet T}$ a non-empty (partial) function onto $\mathsf{W} \times \mathsf{K}_{Op}$, so we can show

$$(H^{\circ} \wedge Q^{\circ}) \fatsemi (H^{\bullet} \wedge Q^{\bullet}) = (H^{\sim} \wedge Q^{\sim})$$

in the same way as the other similar results[†].

(v) We begin with the retrenchment data $HK^{\circ}, QR^{\circ}, NV^{\circ}, DV^{\circ}$ given by (125)–(128). Note that this is a kind of disjunction of the data in (118)–(120) with the data in (121)–(124):

$$\begin{aligned} HK^{\circ}(t^{\sim}, t) \equiv (t = (u, v, w) \wedge \\ \{[H^{\bullet}(t, w) \wedge H^{\sim}(t^{\sim}, w)] \vee [K^{\bullet}(t, v) \wedge K^{\sim}(t^{\sim}, v)]\}) \end{aligned} \tag{125}$$

$$QR^{\circ}_{Op}(h^{\sim}, h, t^{\sim}, t) \equiv$$
$$\begin{cases} (t = (u, v, w) \wedge h = (i, j, k) \wedge \\ \quad \{[H^{\bullet}(t, w) \wedge H^{\sim}(t^{\sim}, w) \wedge Q^{\bullet}_{Op}(h, k, t, w) \wedge \\ \qquad Q^{\sim}_{Op}(h^{\sim}, k, t^{\sim}, w)] \vee & \text{if } Op \in \mathsf{Ops}_{UF} \\ \quad [K^{\bullet}(t, v) \wedge K^{\sim}(t^{\sim}, v) \wedge R^{\bullet}_{Op}(h, j) \wedge R^{\sim}_{Op}(h^{\sim}, j)]\}) \\ (t = (u, v, w) \wedge h = j \wedge \\ \quad K^{\bullet}(t, v) \wedge K^{\sim}(t^{\sim}, v) \wedge R^{\bullet}_{Op}(h, j) \wedge R^{\sim}_{Op}(h^{\sim}, j)) & \text{if } Op \in \mathsf{Ops}_{U \setminus UF} \end{cases} \tag{126}$$

[†] For the other similar results, the non-emptiness of the partial function follows from the assumed non-emptiness of the underlying relation using Assumption 1.1, but the non-emptiness for $H \wedge Q$ does not follow from non-emptiness of H and Q individually.

$$NV^{\circ}_{Op}(n^{\sim},n;t^{\sim\prime},t',h^{\sim},h,t^{\sim},t) \equiv$$

$$\begin{cases} \begin{aligned} &(t=(u,v,w)\wedge h=(i,j,k)\wedge \\ &\;t'=(u',v',w')\wedge n=(o,p,q)\wedge \\ &\;\{[H^{\bullet}(t',w')\wedge H^{\sim}(t^{\sim\prime},w')\wedge \\ &\qquad N^{\bullet}_{Op}(n,q;t',w',h,k,t,w)\wedge \\ &\qquad N^{\sim}{}_{Op}(n^{\sim},q;t^{\sim\prime},w',h^{\sim},k,t^{\sim},w)]\vee \\ &\quad[K^{\bullet}(t',v')\wedge K^{\sim}(t^{\sim\prime},v')\wedge \\ &\qquad V^{\bullet}_{Op}(n,p)\wedge V^{\sim}{}_{Op}(n^{\sim},p)]\}) \end{aligned} & \text{if } Op\in \mathsf{Ops}_{UF} \\ (n=p\wedge V^{\bullet}_{Op}(n,p)\wedge V^{\sim}{}_{Op}(n^{\sim},p)) & \text{if } Op\in \mathsf{Ops}_{U\setminus UF} \end{cases} \tag{127}$$

$$DV^{\circ}_{Op}(t^{\sim\prime},t',n^{\sim},n;h^{\sim},h,t^{\sim},t) \equiv$$

$$\begin{cases} \begin{aligned} &(t=(u,v,w)\wedge h=(i,j,k)\wedge \\ &\;t'=(u',v',w')\wedge n=(o,p,q)\wedge \\ &\;\{[H^{\bullet}(t',w')\wedge N^{\bullet}_{Op}(n,q;t',w',h,k,t,w)\wedge \\ &\qquad D^{\sim}{}_{Op}(t^{\sim\prime},w',n^{\sim},q;h^{\sim},k,t^{\sim},w)]\vee \\ &\quad[D^{\bullet}_{Op}(t',w',n,q;h,k,t,w)\wedge H^{\sim}(t^{\sim\prime},w')\wedge \\ &\qquad N^{\sim}{}_{Op}(n^{\sim},q;t^{\sim\prime},w',h^{\sim},k,t^{\sim},w)]\vee \\ &\quad[D^{\bullet}_{Op}(t',w',n,q;h,k,t,w)\wedge \\ &\qquad D^{\sim}{}_{Op}(t^{\sim\prime},w',n^{\sim},q;h^{\sim},k,t^{\sim},w)]\}) \end{aligned} & \text{if } Op\in \mathsf{Ops}_{UF} \\ \mathsf{false} & \text{if } Op\in \mathsf{Ops}_{U\setminus UF}. \end{cases} \tag{128}$$

In the terminology of Banach *et al.* (2008), the composition of (125)–(128) is a kind of blend of

— disjunctive fusion composition (since the state and I/O spaces are (partly) the same), and

— synchronous parallel composition (since the state and I/O spaces are (partly) different)

of the refinement data (118)–(120) and the retrenchment data (121)–(124).

With the retrenchment data in place, we can now adapt the argument of the proofs of (2).(i) and (2).(ii). Let $t^{\sim}\text{-}(h^{\sim},Op_X,n^{\sim})\!\rightarrow t^{\sim\prime}$ be a step of *Xtra*. By assumption, it is in simulation with a transition of *Ret* or with a transition of *Ref*. By (2).(i) and (2).(ii), this extends to the step $t^{\sim}\text{-}(h^{\sim},Op_X,n^{\sim})\!\rightarrow t^{\sim\prime}$ being in simulation with a transition of *Univ* through either the refinement data (118)–(120) or the retrenchment data (121)–(124). In the former case, it is easy to see that $K^{\circ}\wedge R^{\circ}_{Op}$ implies $HK^{\circ}\wedge QR^{\circ}_{Op}$ and that $K^{\circ\prime}\wedge V^{\circ}_{Op}$ also implies $HK^{\circ\prime}\wedge NV^{\circ}_{Op}$, as in (2).(i). In the latter case, it is easy to see that $H^{\circ}\wedge Q^{\circ}_{Op}$ implies $HK^{\circ}\wedge QR^{\circ}_{Op}$ and that

$$(H^{\circ\prime}\wedge N^{\circ}_{Op})\vee D^{\circ}_{Op}$$

also implies

$$(HK^{\circ\prime}\wedge NV^{\circ}_{Op})\vee DV^{\circ}_{Op},$$

as in (2).(ii).

This completes the proof of part (2).

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

(3) Note that *Univ* itself satisfies the criteria required of *Xtra*. Therefore, if we have a system *Univ** with the properties (1) and (2) of *Univ*, then *Univ** also satisfies the criteria required for *Xtra*. Hence, we can construct two instances of Figure 6 as follows:

— In the first, *Univ* is in its conventional place and *Univ** replaces *Xtra*, and there are refinement data $K^\circ, R^\circ, V^\circ$ and retrenchment data $H^\circ, Q^\circ, N^\circ, D^\circ$ from *Univ** to *Univ*.

— In the second, *Univ** replaces *Univ*, and *Univ* replaces *Xtra*, and there are refinement data K^*, R^*, V^* and retrenchment data H^*, Q^*, N^*, D^* from *Univ* to *Univ**.

So *Univ* and *Univ** are inter-simulable by the arguments above.

(4) For this we just observe that disjunctive fusion composition of retrenchments, and the vertical composition between retrenchments and refinements (both ways round) are sound composition mechanisms. For the record, the composed retrenchment data are

$$\begin{aligned} G(t,u) \equiv{}& (t = (\underline{u},v,w) \wedge \\ & \{[H(v,u) \wedge K(w,\underline{u})] \vee [K(w,u) \wedge H(v,\underline{u})]\}) \end{aligned} \tag{129}$$

$$\begin{aligned} P_{Op}(h,i,t,u) \equiv{}& (h = (\underline{i},j,k) \wedge t = (\underline{u},v,w) \wedge \\ & \{[K(w,\underline{u}) \wedge R_{Op}(k,\underline{i}) \wedge \\ & \quad H(v,u) \wedge Q_{Op}(j,i,v,u)] \vee \\ & \;[K(w,u) \wedge R_{Op}(k,i) \wedge H(v,\underline{u}) \wedge \\ & \quad Q_{Op}(j,\underline{i},v,\underline{u})]\}) \end{aligned} \tag{130}$$

$$\begin{aligned} O_{Op}(n,o;t',u',h,i,t,u) \equiv{}& (t = (\underline{u},v,w) \wedge h = (\underline{i},j,k) \wedge \\ & t' = (\underline{u}',v',w') \wedge n = (\underline{o},p,q) \wedge \\ & \{[H(v',\underline{u}') \wedge K(w,u) \wedge R_{Op}(k,i) \wedge \\ & \quad K(w',u') \wedge V_{Op}(q,o) \wedge \\ & \quad N_{Op}(p,\underline{o};v',\underline{u}',j,\underline{i},v,\underline{u})] \vee \\ & \;[H(v',u') \wedge K(w,\underline{u}) \wedge R_{Op}(k,\underline{i}) \wedge \\ & \quad K(w',\underline{u}') \wedge V_{Op}(q,\underline{o}) \wedge \\ & \quad N_{Op}(p,o;v',u',j,i,v,u)] \vee \\ & \;[K(w,u) \wedge R_{Op}(k,i) \wedge K(w',u') \wedge \\ & \quad V_{Op}(q,o) \wedge N_{Op}(p,\underline{o};v',\underline{u}',j,\underline{i},v,\underline{u}) \wedge \\ & \quad N_{Op}(p,o;v',u',j,i,v,u) \wedge K(w,\underline{u}) \wedge \\ & \quad R_{Op}(k,\underline{i}) \wedge K(w',\underline{u}') \wedge V_{Op}(q,\underline{o})]\}) \end{aligned} \tag{131}$$

$$\begin{aligned} C_{Op}(t',u',n,o;h,i,t,u) \equiv{}& (t = (\underline{u},v,w) \wedge h = (\underline{i},j,k) \wedge \\ & t' = (\underline{u}',v',w') \wedge n = (\underline{o},p,q) \wedge \\ & \{[D_{Op}(v',u',p,o;j,i,v,u) \wedge K(w,\underline{u}) \wedge \\ & \quad R_{Op}(k,\underline{i}) \wedge K(w',\underline{u}') \wedge V_{Op}(q,\underline{o})] \vee \\ & \;[K(w,u) \wedge R_{Op}(k,i) \wedge K(w',u') \wedge \\ & \quad V_{Op}(q,o) \wedge D_{Op}(v',\underline{u}',p,\underline{o};j,\underline{i},v,\underline{u})]\}). \end{aligned} \tag{132}$$

(5) We begin with the retrenchment data HH°,QQ°,NN°,DD°, which is given by (133)–(136) below. Note that the only difference between this and the earlier retrenchment data HK°,QR°,NV°,DV° in (125)–(128) is the replacement of the disjunction in the within relation QR° by a conjunction in the within relation QQ°.

$$HH^{\circ}(t^{\sim}, t) \equiv HK^{\circ}(t^{\sim}, t) \tag{133}$$

$$QQ^{\circ}_{Op}(h^{\sim}, h, t^{\sim}, t) \equiv$$
$$\begin{cases} \begin{aligned} &(t = (u, v, w) \wedge h = (i, j, k) \wedge \\ &\ \{[H^{\bullet}(t, w) \wedge H^{\sim}(t^{\sim}, w) \wedge \\ &\qquad Q^{\bullet}_{Op}(h, k, t, w) \wedge Q^{\sim}{}_{Op}(h^{\sim}, k, t^{\sim}, w)] \wedge \\ &\quad [K^{\bullet}(t, v) \wedge K^{\sim}(t^{\sim}, v) \wedge \\ &\qquad R^{\bullet}_{Op}(h, j) \wedge R^{\sim}{}_{Op}(h^{\sim}, j)]\}) \end{aligned} & \text{if } Op \in \mathsf{Ops}_{UF} \\ \\ \begin{aligned} &(t = (u, v, w) \wedge h = j \wedge \\ &\ K^{\bullet}(t, v) \wedge K^{\sim}(t^{\sim}, v) \wedge \\ &\ R^{\bullet}_{Op}(h, j) \wedge R^{\sim}{}_{Op}(h^{\sim}, j)) \end{aligned} & \text{if } Op \in \mathsf{Ops}_{U \setminus UF} \end{cases} \tag{134}$$

$$NN^{\circ}_{Op}(n^{\sim}, n; t^{\sim\prime}, t', h^{\sim}, h, t^{\sim}, t) \equiv NV^{\circ}_{Op}(n^{\sim}, n; t^{\sim\prime}, t', h^{\sim}, h, t^{\sim}, t) \tag{135}$$

$$DD^{\circ}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t) \equiv DV^{\circ}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t). \tag{136}$$

We begin with the initialisation. Suppose $Init_U(t')$ in (116) and the

$$[Init_T(v') \wedge K^{\bullet}(t', v')]$$

disjunct of $Init_U(t')$ holds. From $Init_T(v')$, because $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ is a refinement, we can find a $t^{\sim\prime}$ such that

$$Init_X(t^{\sim\prime}) \wedge K^{\sim}(t^{\sim\prime}, v')$$

holds. Composing $K^{\sim}$ and $K^{\bullet}$ gives the second disjunct of HH°, so we have

$$Init_X(t^{\sim\prime}) \wedge HH^{\circ}(t^{\sim\prime}, t')$$

as required.
The argument is analogous if we alternatively suppose the $H^{\bullet}$ disjunct of $Init_U(t')$ holds, and we are done.

For the operation PO, suppose we have

$$HH^{\circ} \wedge QQ^{\circ}_{Op} \wedge stp_{Op_U}.$$

It is evident that QQ° strengthens HH°. We consider two cases:

— Suppose the $stp_{Op_T} \wedge K^{\bullet}$ disjunct of stp_{Op_U} is true (whether for the $Op \in \mathsf{Ops}_{UF}$ or the $Op \in \mathsf{Ops}_{U \setminus UF}$ case).
So we have $HH^{\circ} \wedge QQ^{\circ}_{Op}$ factors uniquely through v, j, in *Ret*, and the *Univ* step, say $t \text{ -}(h, Op_U, n)\!\twoheadrightarrow t'$, projects through $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ to its enclosed *Ret* step, say $v \text{ -}(j, Op_T, p)\!\twoheadrightarrow v'$. If we now extract $K^{\sim} \wedge R^{\sim}{}_{Op}$ from our assumed $HH^{\circ} \wedge QQ^{\circ}_{Op}$, then,

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

with $v \text{-}(j, Op_T, p)\!\twoheadrightarrow v'$, we can apply the $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ refinement operation PO to derive a step of *Xtra*, say $t^{\sim} \text{-}(h^{\sim}, Op_X, n^{\sim})\!\twoheadrightarrow t^{\sim\prime}$, for which

$$K^{\sim\prime} \wedge V^{\sim}_{Op},$$

and thus

$$K^{\bullet\prime} \wedge K^{\sim\prime} \wedge V^{\bullet}_{Op} \wedge V^{\sim}_{Op},$$

so

$$HH^{\circ\prime} \wedge NN^{\circ}_{Op},$$

all hold. The last of these discharges our goal.

— Alternatively, suppose the $stp_{Op_F} \wedge H^{\bullet}$ disjunct of stp_{Op_U} is true (which can only be for the $Op \in \mathsf{Ops}_{UF}$ case).
We can use a similar argument in this case, except that the unique factorisation is through w, k, in *Ref*, we have a *Ref* step $w \text{-}(k, Op_F, q)\!\twoheadrightarrow w'$, we use the $H^{\sim}$,$Q^{\sim}$,$N^{\sim}$,$D^{\sim}$ retrenchment, and we derive an *Xtra* step $t^{\sim} \text{-}(h^{\sim}, Op_U, n^{\sim})\!\twoheadrightarrow t^{\sim\prime}$, for which

$$((H^{\sim\prime} \wedge N^{\sim}_{Op}) \vee D^{\sim}_{Op}),$$

and thus

$$((H^{\sim\prime} \wedge N^{\sim}_{Op}) \vee D^{\sim}_{Op}) \wedge ((H^{\bullet\prime} \wedge N^{\bullet}_{Op}) \vee D^{\bullet}_{Op})$$

hold. We can then rearrange the last of these to give

$$(HH^{\circ\prime} \wedge NN^{\circ}_{Op}) \vee DD^{\circ}_{Op},$$

which discharges our goal.

(6) We work under the additional assumption stated and start with the refinement data KK°,RR°,VV° given by

$$KK^{\circ}(t^{\sim}, t) \equiv HH^{\circ}(t^{\sim}, t) \tag{137}$$

$$RR^{\circ}_{Op}(h^{\sim}, h) \equiv (\forall t^{\sim}, t \bullet HK^{\circ}(t^{\sim}, t) \Rightarrow QQ^{\circ}_{Op}(h^{\sim}, h, t^{\sim}, t)) \tag{138}$$

$$\begin{aligned} VV^{\circ}_{Op}(n^{\sim}, n) \equiv (\exists t^{\sim\prime}, t', h^{\sim}, h, t^{\sim}, t \bullet \\ NN^{\circ}_{Op}(n^{\sim}, n; t^{\sim\prime}, t', h^{\sim}, h, t^{\sim}, t) \vee \\ DD^{\circ}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t)). \end{aligned} \tag{139}$$

(i) To prove the refinement, we start with the initialisation PO. This goes in just the same way as the analogous PO for the retrenchment HH°,QQ°,NN°,DD° in part (5).
For the operation PO, we assume

$$KK^{\circ}(t^{\sim}, t) \wedge RR^{\circ}_{Op}(h^{\sim}, h) \wedge stp_{Op_U}(t, h, t', n),$$

and must prove there are values $t^{\sim\prime}, n^{\sim}$ such that $stp_{Op_X}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})$ and

$$KK^{\circ\prime} \wedge VV^{\circ}_{Op}$$

hold.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

Consider $KK^{\circ}{\wedge}RR^{\circ}_{Op}$. This implies $HH^{\circ}{\wedge}QQ^{\circ}_{Op}$. With $stp_{Op_U}(t, h, t', n)$, we have the hypothesis of the operation PO of the HH°,QQ°,NN°,DD° retrenchment. Therefore, we can deduce

$$(HH^{\circ\prime}{\wedge}NN^{\circ}_{Op}){\vee}DD^{\circ}_{Op}.$$

We consider cases:

— If $HH^{\circ\prime}{\wedge}NN^{\circ}_{Op}$ holds, then so does

$$KK^{\circ\prime}{\wedge}VV^{\circ}_{Op}$$

since

$$HH^{\circ\prime} = KK^{\circ\prime}$$

and NN°_{Op} is a disjunct of VV°_{Op}, and we are done.

— If $HH^{\circ\prime}{\wedge}NN^{\circ}_{Op}$ does not hold, we must have

$$DD^{\circ}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t)$$

instead. In that case, (105) allows us to deduce $HH^{\circ}(t^{\sim\prime}, t')$ (which gives $KK^{\circ}(t^{\sim\prime}, t')$), and then we use (139) to deduce $VV^{\circ}_{Op}(n^{\sim}, n)$, and we are done.

(ii) Note that the condition stated in (104) is just the requirement from (13), so we are done.

(7) The proof of this part is just a matter of replaying the arguments of part (3) using the stronger relationships between *Univ* and *Xtra* afforded by the stronger assumptions in force. □

9.1. *Remarks*

Remark 9.2. In part (4) of the theorem we used disjunctive fusion composition, as in the Postjoin Theorem since it is valid without restriction. Again as in the Postjoin Theorem, the corresponding conjunctive composition requires a 'close to cosimulation' criterion to hold.

Remark 9.3. Note the close structural similarity between HH° and QQ°_{Op} in (133)–(134) and HK° and QR°_{Op} in (91)–(92) of the Postjoin Theorem. The tempting alternative of making QQ°_{Op} disjunctive as in (134) generates, through the distributive law, a plethora of pathological and exceptional cases in the analysis of

$$HH^{\circ}{\wedge}QQ^{\circ}_{Op}{\wedge}stp_{Op_U}$$

since the terms containing $K^{\bullet}$, say in each of the contributing HH°, QQ°_{Op}, stp_{Op_U}, are different – similar observations obviously apply to $H^{\bullet}$. However, hedging against the shortcomings of all of these possibilities is not elegant, succinct or useful, particularly in view of the remarks regarding the Prejoin Theorem made in the next section.

Remark 9.4. As in earlier remarks, the composition of K^{*},R^{*},V^{*} with K°,R°,V° need not be the identity; still less need the composition of H°,Q°,N°,D° and H^{*},Q^{*},N^{*},D^{*} be.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

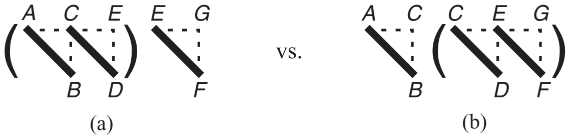

Fig. 7. Different association orders for the lifting construction.

10. Associativity, general tower constructions, and system engineering

If we reinterpret the 'diagonal factorising' lifting and lowering constructions as square completions in their own right (which is what results when we view the composition of a refinement and retrenchment round an 'L' shape as a retrenchment – see Figure 1), we now have a full set of square completion results available. (Equally, we can view the postjoin and prejoin constructions as 'co-diagonal factorising' constructions that pull apart the pseudoretrenchment across the co-diagonal, and we can thus say that we have a full suite of those too.)

From an applications perspective, the lifting and postjoin constructions are unquestionably more significant than the other square completions. This is because they deal with their constituent retrenchments in a 'forwards' manner – the others, the lowering and prejoin constructions, work, in essence, with converse retrenchments. Using a converse retrenchment during system construction amounts to a form of 'undevelopment' since the retrenchment relationship was deliberately designed to be used during development in the forwards direction (see the discussion in Banach *et al.* (2007b, Section 4.1) on this point). As a result, we would expect that were the results of the current paper to be mechanised, the focus would be on the lifting and postjoin constructions, since these would most obviously repay the investment of effort needed.

One notable aspect of our work is that everything has been reduced to the composition of (collections of) relations. Composing relations is associative, so we can expect that our constructions themselves will compose associatively – up to the appropriate notion of equivalence. We can illustrate this on a specific construction. Consider the lifting construction of Figure 3. The state and I/O spaces of this construction are just cartesian products made from the abstract and concrete constituent spaces. Likewise, the transitions in (44) are made up out of pairs of abstract and concrete constituent transitions. Consider Figure 7, which illustrates applying the construction using two different association orders.

We will focus first on Figure 7.(a), which shows the leftmost A-to-B retrenchment lifted to C, which is followed by the middle lifting, which lifts the C-to-D retrenchment to E. System E gives the result of the parenthesised liftings in Figure 7.(a). The construction can be repeated to include the third piece of Figure 7.(a), finally giving system G. A little thought shows that the state and I/O spaces of the result will be the cartesian products of the constituents, bracketed leftmost-innermost. Similar remarks apply to the core part of the transition relation, which will contain all the step relations from all the constituent systems, with their logical definitions bracketed in an analogous leftmost-innermost way.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

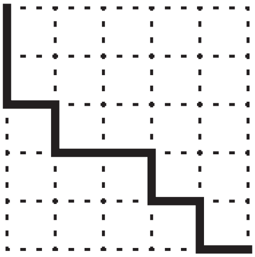

Fig. 8. Illustrating the lifting and lowering constructions – vertical lines are refinements and horizontal lines are retrenchments.

We will now turn to Figure 7.(b). Inside the parentheses, we have a combined lifting, as above, consisting of the lifting of the C-to-D retrenchment to E, followed by the lifting of the E-to-F retrenchment to give G. System G coincides with the system constructed by lifting the A-to-B retrenchment to give C, and identifying C with the starting system of the parenthesised lifting just described. Thus, when the leftmost lifting is combined with the retrenchment constructed in the parentheses, we get another result for the overall construction. However, a moment's thought shows that this turns out to be the same as the previous case, but bracketed rightmost-innermost, for both the state and I/O spaces and the core part of the transition relation. These rebracketings amount to set theoretic isomorphism, which is a much stronger notion of equivalence than either inter-refinability or the even weaker equivalence notions we encountered above. Similar remarks apply to the other constructions, to vertical as well as horizontal association and to combinations of constructions of various kinds. However, an exhaustive treatment of all the cases would be truly exhausting.

The good behaviour just noted allows us to envision a system development process built out of refinements and retrenchments aided by the constructions made available to us in the current paper: 'system development via theorem'. Figure 8 shows a schematic example. The development starts at the top left-hand corner with the most abstract model. Two refinement stages follow, after which more detailed requirement considerations necessitate a sideways jump, through a retrenchment, onto a lower level refinement strand. The square completion constructions, here lifting, permit the new low-level detail to be exhibited at a level of abstraction comparable with the initial model. This might be required, for example, in order to check abstract formulations of the requirements properties that the low-level system model modifications described by the retrenchment were intended to address. There then follows another refinement stage, followed by another retrenchment stage and then another retrenchment stage – the two separate retrenchments permitting piecemeal validation of the issues they were introduced to address. In the same manner, the process concludes with a further refinement, retrenchment, refinement and a final retrenchment.

Now suppose the user environment changes, and the previously developed system is no longer adequate. Suppose the requirements addressed up to the end of the third retrenchment still hold good, but that the remainder of the development needs to be

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

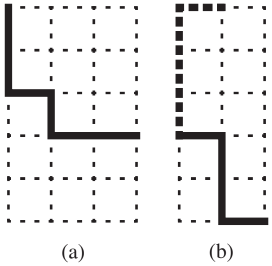

Fig. 9. Illustrating the postjoin and prejoin constructions – the vertical lines are refinements and the horizontal lines are retrenchments.

modified. Figure 9 shows what might happen next. The retained part of the original development is in Figure 9.(a). Its right vertical side, a refinement path from most abstract level down to where the thick development path reaches the edge, gives the interface from the retained part of the original development to the new activity. This, reproduced as the heavy dashed vertical line in Figure 9.(b), is the starting point for the new development.

If we suppose the new requirements have been described at the most abstract level, there will be a retrenchment, shown by the heavy dashed horizontal line in Figure 9.(b), from the starting abstract model to a modified abstract model. Assuming the three earlier refinements have been composed into one with the help of our square completion results (giving the heavy dashed vertical line in Figure 9.(b)), an application of the postjoin construction then embeds the new requirements into the current development level. The development can subsequently be completed through two further stages of refinement and a final retrenchment.

11. Conclusions

We have introduced retrenchment and some context for its applications (including applications of the theory treated in detail in the current paper). We have motivated the need for square completion constructions in the context of retrenchment and refinement interworking, and then formulated and proved the theorems relating to the four relevant completions. These were designed with simplicity and composability in mind, and we drew extensively, and with the experience of hindsight, on the theorems reported in Jeske (2005). The accompanying remarks to our four main theorems indicate that small variations on the results given are perfectly feasible. We also outlined how such constructions could be used in a large-scale formal development process to allow greater flexibility in dealing with requirements issues than is possible with the use of refinement alone.

In all of this, we pursued a resolutely one-to-one operation correspondence strategy. That is to say, a single abstract step always corresponds to a single concrete step. However, this is too restrictive for many practical applications. A ‘quick fix’ involves treating paths through the transition system as the individual steps of an associated system. The simple way in which we have formulated our systems and our relationships between systems guarantees that this approach will go through without any problems, given the usual

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

care and attention to 'plumbing' considerations. Of course, more detailed treatments of such 'coarse-grained versus fine-grained' formulations can uncover issues going beyond simple path-oriented reuse of the one-to-one results, but such issues remain as work for the future, and will be addressed in appropriate publications.

In the period since the publication of Jeske (2005), the importance of these types of result has only increased. Being able to place the retrenchment steps of some development inside a development methodology in a way that cleanly separates them from the more conventional refinement steps adds great clarity to the development process as it distinguishes those steps with the potential to preserve system properties in a strong manner from those steps where this capacity is curtailed. Experience has shown that in the vast majority of practical cases the integration of retrenchment and refinement could be done by hand relatively straightforwardly (some of these were reviewed in Section 2), so one view of the challenge tackled in the current paper is that it is a search for an abstract formulation of the integration phenomenon that reflects the simplicity observed in practice. Given the experience of Jeske (2005), this was not a trivial undertaking, but one that we believe has been accomplished successfully in the current paper.

References

Badeau, F. and Amelot, A. (2005) Using B as a High Level Programming Language in an Industrial Project: Riossy VAL. In: Treharne, H., King, S., Henson, M. and Schneider, S. (eds.) Proceedings ZB 2005: Formal Specification and Development in Z and B. *Springer-Verlag Lecture Notes in Computer Science* **3455** 334–354.

Banach, R. (2009) Model Based Refinement and the Design of Retrenchments. Unpublished paper.

Banach, R. (2011) Retrenchment for Event-B: UseCase-wise Development and Rodin Integration. *Formal Aspects of Computing* **23** 113–131.

Banach, R. and Jeske, C. (2010) Stronger Compositions for Retrenchments. *Journal of Logic and Algebraic Programming* **79** 215–232.

Banach, R., Jeske, C. and Poppleton, M. (2008) Composition Mechanisms for Retrenchment. *Journal of Logic and Algebraic Programming* **75** 209–229.

Banach, R., Jeske, C., Poppleton, M. and Stepney, S. (2005) Retrenching the Purse: Finite Sequence Numbers, and the Tower Pattern. In: Fitzgerald, J., Hayes, I. J. and Tarlecki, A. (eds.) FM 2005: Formal Methods. Proceedings International Symposium of Formal Methods Europe. *Springer-Verlag Lecture Notes in Computer Science* **3582** 382–398.

Banach, R., Jeske, C., Poppleton, M. and Stepney, S. (2006a) Retrenching the Purse: Finite Exception Logs, and Validating the Small. In: Hinchey, M. (ed.) *30th Annual IEEE/NASA Software Engineering Workshop, 2006 – SEW '06*. 234–245.

Banach, R., Jeske, C., Poppleton, M. and Stepney, S. (2006b) Retrenching the Purse: Hashing Injective CLEAR Codes, and Security Properties. In: Margaria, T. and Steffen, B. (eds.) *Proceedings ISoLA 2006: Second IEEE International Symposium on Leveraging Applications of Formal Methods, Verification and Validation* 82–90.

Banach, R., Jeske, C., Poppleton, M. and Stepney, S. (2007a) Retrenching the Purse: The Balance Enquiry Quandary, and Generalised and (1,1) Forward Refinements. *Fundamenta Informaticae* **77** 29–69.

Banach, R., Poppleton, M., Jeske, C. and Stepney, S. (2007b) Engineering and Theoretical Underpinnings of Retrenchment. *Science of Computer Programming* **67** 301–329.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press

Banach, R. and Schellhorn, G. (2010) Atomic Actions and their Refinements to Isolated Protocols. *Formal Aspects of Computing* **22** 33–61.

Banach, R., Zhu, H., Su, W. and Huang, R. (2014) Continuous KAOS, ASM, and Formal Control System Design Across the Continuous/Discrete Modeling Interface: A Simple Train Stopping Application. *Formal Aspects of Computing* **26** 319–366.

Behm, P., Benoit, P., Faivre, A. and Meynadier, J.-M. (1999) Météor: A Successful Application of B in a Large Project. In: Wing, J., Woodcock, J. and Davies, J. (eds.) Proceedings: World Congress on Formal Methods in the Development of Computing Systems – Volume I. *Springer-Verlag Lecture Notes in Computer Science* **1708** 369–387.

Behm, P., Benoit, P., Faivre, A. and Meynadier, J.-M. (2000) Météor: An Industrial Success in Formal Development. In: Bowen, J. P., Dunne, S., Galloway, A. and King, S. (eds.) ZB 2000: Formal Specification and Development in Z and B. Proceedings First International Conference of B and Z Users. *Springer-Verlag Lecture Notes in Computer Science* **1878** 374–393.

de Roever, W.-P. and Engelhardt, K. (1998) *Data Refinement: Model-Oriented Proof Methods and their Comparison*, Cambridge University Press.

Dijkstra, E. (1972) Notes on Structured Programming. In: Dahl, O.-J., Dijkstra, E. and Hoare, C. (eds.) *Structured Programming*, Academic Press.

Hoare, C. (1972) Proofs of Correctness of Data Representation. *Acta Informatica* **1** 271–281.

Jeffords, R., Heitmeyer, C., Archer, M. and Leonard, E. (2009) A Formal Method for Developing Provably Correct Fault-Tolerant Systems Using Partial Refinement and Composition. In: Cavalcanti, A. and Dams, D. R. (eds.) FM 2009: Formal Methods – Proceedings Second World Congress. *Springer-Verlag Lecture Notes in Computer Science* **5850** 173–189.

Jeske, C. (2005) *Algebraic Theory of Retrenchment and Refinement*, Ph.D. thesis, School of Computer Science, University of Manchester.

Jones, C., O'Hearne, P. and Woodcock, J. (2006) Verified Software: A Grand Challenge. *IEEE Computer* **39** 93–95.

Jones, C. and Woodcock, J. (2008) Special Issue on the Mondex Verification. *Formal Aspects of Computing* **20** 1–139.

Stepney, S., Cooper, D. and Woodcock, J. (1998) More Powerful Z Data Refinement: Pushing the State of the Art in Industrial Refinement. In: Bowen, J. P., Fett, A. and Hinchey, M. G. Proceedings ZUM 98: The Z Formal Specification Notation. Proceedings 11th International Conference of Z Users. *Springer-Verlag Lecture Notes in Computer Science* **1493** 284–307.

Stepney, S., Cooper, D. and Woodcock, J. (2000) An Electronic Purse: Specification, Refinement and Proof. Technical Report PRG-126, Oxford University Computing Laboratory.

Wirth, N. (1971) Program Development by Stepwise Refinement. *Communications of the ACM* **14** 221–227.

Woodcock, J. (2006) First Steps in the Verified Software Grand Challenge. *IEEE Computer* **39** 57–64.

Woodcock, J. and Banach, R. (2007) The Verification Grand Challenge. *Journal of Universal Computer Science* **13** 661–668.

https://doi.org/10.1017/S0960129514000061 Published online by Cambridge University Press